ΠΑΝΕΠΙΣΤΗΜΙΟ ΑΙΓΑΙΟΥ

ΠΟΛΥΤΕΧΝΙΚΗ ΣΧΟΛΗ

ΤΜΗΜΑ ΜΗΧΑΝΙΚΩΝ ΠΛΗΡΟΦΟΡΙΑΚΩΝ ΚΑΙ ΕΠΙΚΟΙΝΩΝΙΑΚΩΝ ΣΥΣΤΗΜΑΤΩΝ

Τρέχουσα Κατάσταση Αγοράς για Υπηρεσίες Security as a Service
(Current Market State Concerning Security as a Service)

ΔΙΠΛΩΜΑΤΙΚΗ ΕΡΓΑΣΙΑ

Ευάγγελος Ιωάννης Λάμπρου

Επιβλέπων : Κυριάκος Κρητικός

Μέλη εξεταστικής επιτροπής: Μαρία Καρύδα, Σπύρος Κοκολάκης

Σάμος, Σεπτέμβριος 2022

Η σελίδα αυτή είναι σκόπιμα λευκή.

Πρόλογος και ευχαριστίες

Θα ήθελα να εκφράσω τις βαθύτατες ευχαριστίες μου στον επιβλέποντα καθηγητή μου κύριο Κυριάκο Κρητικό. Η βοήθεια του ήταν πολύτιμη για την εκπόνηση αυτής της εργασίας, όσο και στη μετέπειτα εξέλιξη μου. Επιπρόσθετα, θα ήθελα να ευχαριστήσω την οικογένεια μου για την κατανόηση και υποστήριξή τους, χωρίς τις οποίες δεν θα ήταν δυνατή η ολοκλήρωση των σπουδών μου.

© 2022

Ευάγγελος Ιωάννης Λάμπρου
Τμήμα Μηχανικών Πληροφοριακών και Επικοινωνιακών Συστημάτων
ΠΑΝΕΠΙΣΤΗΜΙΟ ΑΙΓΑΙΟΥ

Η σελίδα αυτή είναι σκόπιμα λευκή.

Πίνακας περιεχομένων

1 Εισαγωγή 1

1.1 Εισαγωγή 1

1.2 Πρόβλημα και τρόπος αντιμετώπισης 1

1.3 Δομή εργασίας 2

2 Υπολογιστικό νέφος 3

2.1 Εισαγωγή στο υπολογιστικό νέφος 3

2.2 Μοντέλα Παράδοσης 6

2.2.1 Λογισμικό σαν υπηρεσία (Software as a service) 7

2.2.2 Υποδομή σαν υπηρεσία (Infrastructure as a service) 8

2.2.3 Πλατφόρμα σαν υπηρεσία (Platform as a service) 8

2.3 Μοντέλα Διάταξης 9

2.3.1 Δημόσιο νέφος (Public cloud) 10

2.3.2 Ιδιωτικό νέφος (Private cloud) 10

2.3.3 Υβριδικό νέφος (Hybrid cloud) 11

2.3.4 Κοινοτικό νέφος (Community cloud) 12

3 Ασφάλεια ΠΣ 13

3.1 Ορισμός 13

3.2 Ανάλυση βασικών αρχών ασφαλείας 14

3.3 Ασφάλεια στο Υπολογιστικό Νέφος 15

3.3.1 Εισαγωγή 15

3.3.2 Σύγκριση μεταξύ υπηρεσιών στο νέφος και σε επιτόπιο περιβάλλον 15

3.3.3 Απειλές στο υπολογιστικό νέφος και τρόποι αντιμετώπισης 17

3.3.3.1 Κλασσικές απειλές 17

3.3.3.2 Απειλές στο υπολογιστικό νέφος 25

4 Security as a Service 29

4.1 Εισαγωγή 29

4.2 Είδη υπηρεσιών ασφάλειας 29

4.2.1 Σύστημα διαχείρισης πληροφοριών και συμβάντων ασφαλείας (Security Information and Event Management - SIEM) 30

4.2.2 Επιχειρησιακή συνέχεια και αποκατάσταση καταστροφών (Business Continuity and Disaster Recovery) ... *32*
4.2.3 Διαχείριση εισβολής (Intrusion Management) ... *35*
4.2.4 Διαχείριση ταυτότητας και πρόσβασης (Identity and Access Management) ... *40*
4.2.5 Πρόληψη απώλειας δεδομένων (Data Loss Prevention) ... *46*
4.2.6 Κρυπτογράφηση (Encryption) ... *48*
4.2.7 Ασφάλεια ηλεκτρονικού ταχυδρομείου (Email Security) ... *51*
4.2.8 Ασφάλεια δικτύου (Network Security) ... *56*
4.2.9 Αποτίμηση ασφάλειας (Security assessment) ... *63*
4.2.10 Ασφάλεια Ιστού (Web Security) ... *67*
5 Σύγκριση Προϊόντων Υπηρεσιών SecaaS ... **70**
5.1 Εισαγωγή ... 70
5.2 Στατιστικά στοιχεία ... 77
5.2.1 Σύστημα διαχείρισης πληροφοριών και συμβάντων ασφαλείας (Security Information and Event Management - SIEM) ... *77*
5.2.2 Επιχειρησιακή συνέχεια και αποκατάσταση καταστροφών (Business Continuity and Disaster Recovery) ... *83*
5.2.3 Διαχείριση εισβολής (Intrusion Management) ... *89*
5.2.4 Διαχείριση ταυτότητας και πρόσβασης (Identity and Access Management) ... *95*
5.2.5 Πρόληψη απώλειας δεδομένων (Data Loss Prevention) ... *100*
5.2.6 Κρυπτογράφηση (Encryption) ... *105*
5.2.7 Ασφάλεια ηλεκτρονικού ταχυδρομείου (Email Security) ... *111*
5.2.8 Ασφάλεια δικτύου (Network Security) ... *117*
5.2.9 Αποτίμηση ασφάλειας (Security assessment) ... *122*
5.2.10 Ασφάλεια Ιστού (Web Security) ... *126*
5.3 Συνολικά στατιστικά στοιχεία ... 130
5.3.1 Τρόπος παράδοσης ... *131*
5.3.2 Μοντέλο διάταξης ... *133*
5.3.3 Κατηγορίες ασφαλείας ... *135*
5.3.4 Μοντέλο κόστους ... *137*
5.3.5 Μηχανισμοί / Λειτουργικότητα Ασφάλειας ... *139*
5.3.6 Μη λειτουργικές εγγυήσεις ... *140*
5.3.7 Είδος προσφερόμενης προστασίας ... *142*
5.3.8 Ιδιότητες ασφάλειας ... *145*
5.3.9 Αντιμετωπιζόμενες Απειλές ... *150*
5.3.10 Περιορισμοί Χρήσης ... *152*

5.3.11 Δοκιμαστικές εκδόσεις *154*
5.3.12 Τρόπος χρήσης *156*
5.3.13 Αγορές *160*
5.3.14 Υποστήριξη *164*
6 Συμπεράσματα και μελλοντικές κατευθύνσεις 166
6.1 Συμπεράσματα 166
6.2 Μελλοντικές κατευθύνσεις 167
Βιβλιογραφία 168
Παράρτημα Ι Πίνακες αποτίμησης κεφαλαίου 5 180

Λίστα Σχημάτων

Εικόνα 1. Διαφορές μεταξύ των 3 μοντέλων παράδοσης του υπολογιστικού νέφους.....6
Εικόνα 2. Δομικά στοιχεία της SAML [56].....43
Εικόνα 3. Διάγραμμα ροής δεδομένων της XACML [59].....45
Εικόνα 4. Πλήθος προϊόντων που υποστηρίζει τον κάθε τρόπο παράδοσης.....132
Εικόνα 5. Πλήθος προϊόντων ανά τρόπο παράδοσης και κατηγορία προϊόντων 132
Εικόνα 6. Πλήθος προϊόντων που υποστηρίζουν τις διαφορετικές τιμές για το μοντέλο διάταξης 134
Εικόνα 7. Πλήθος προϊόντων ανά τιμή του μοντέλου διάταξης και κατηγορία προϊόντων 134
Εικόνα 8. Πλήθος προϊόντων που είτε καλύπτουν επιπλέον κατηγορίες ασφαλείας είτε όχι 136
Εικόνα 9. Πλήθος προϊόντων ανά κατηγορία που είτε καλύπτουν είτε δεν καλύπτουν έξτρα κατηγορίες ασφαλείας.....136
Εικόνα 10. Πλήθος προϊόντων με είτε 1 είτε 2 ή περισσότερα πακέτα τιμολόγησης 138
Εικόνα 11. Πλήθος προϊόντων ανά κατηγορία με είτε 1 είτε 2 ή περισσότερα πακέτα τιμολόγησης 138
Εικόνα 12. Πλήθος προϊόντων που παρέχουν είτε μόνο βασική είτε και έξτρα λειτουργικότητα.140
Εικόνα 13. Πλήθος προϊόντων ανα κατηγορία που παρέχουν είτε μόνο βασική είτε και έξτρα λειτουργικότητα.....139
Εικόνα 14. Πλήθος προϊόντων στα οποία είτε υπάρχουν είτε δεν υπάρχουν εγγυήσεις..... **Error! Bookmark not defined.**
Εικόνα 15. Πλήθος προϊόντων ανά κατηγορία στα οποία είτε υπάρχουν είτε δεν υπάρχουν εγγυήσεις.....142
Εικόνα 16. Πλήθος προϊόντων ανα διαφορετική τιμή του κριτηρίου είδους προστασίας 144
Εικόνα 17. Πλήθος προϊόντων ανά κατηγορία ασφάλειας και ανά διαφορετική τιμή του κριτηρίου είδους προστασίας.....145
Εικόνα 18. Πλήθος προϊόντων ανα κατηγορία ασφαλείας και ανά διαφορετική τιμή του κριτηρίου είδους προστασίας.....147
Εικόνα 19. Πλήθος προϊόντων που υποστηρίζουν μεμονωμένα 3 διαφορετικές ιδιότητες ασφάλειας 148
Εικόνα 20. Πλήθος προϊόντων που υποστηρίζουν είτε την διαθεσιμότητα & ακεραιότητα είτε την διαθεσιμότητα, εμπιστευτικότητα & ακεραιότητα.....148
Εικόνα 21. Πλήθος προϊόντωνπου υποστηρίζουν μεμονωμένα 3 διαφορετικούς συνδυασμούς ιδιοτήτων ασφάλειας 149

Εικόνα 22. Πλήθος προϊόντων ανά κατηγορία που υποστηρίζουν διαφορετικούς συνδιασμούς ιδιοτήτων ασφαλείας .....**Error! Bookmark not defined.**
Εικόνα 23. Πλήθος προϊόντων ασφαλείας ανα κατηγορία που υποστηρίζουν είτε ξεχωριστά 3 ιδιότητες ασφάλειας είτε τον συνδυασμό μη αποποίησης και διαθεσιμότητας 151
Εικόνα 24. Πλήθος προϊόντων που είτε αντιμετωπίζουν μια απειλή είτε δύο ή παραπάνω απειλές 151
Εικόνα 25. Πλήθος προϊόντων ανά κατηγορία αντιμετωπίζουν μια απειλή είτε δύο ή παραπάνω απειλές.....153
Εικόνα 26. Πλήθος προϊόντων που είτε έχουν κάποιο περιορισμό χρήσης είτε δεν έχουν.....**Error! Bookmark not defined.**
Εικόνα 27. Πλήθος προϊόντων ανα κατηγορία που είτε έχουν κάποιο περιορισμό χρήσης είτε δεν έχουν .....**Error! Bookmark not defined.**
Εικόνα 28. Πλήθος προϊόντων που είτε προσφέρουν δωρεάν δοκιμαστική έκδοση είτε όχι.....155
Εικόνα 29. Πλήθος προϊόντων ανα κατηγορία που είτε προσφέρουν δωρεάν δοκιμαστική έκδοση είτε όχι 158
Εικόνα 30. Πλήθος προϊόντων που υποστηρίζουν μεμονωμένα έναν τρόπο χρήσης 158
Εικόνα 31. Πλήθος προϊόντων ανά κατηγορία που υποστηρίζουν συνδιασμούς τρόπων χρήσης 159
Εικόνα 32. Πλήθος προϊόντων ανά κατηγορία που υποστηρίζουν διαφορετικούς συνδυασμούς τρόπων χρήσης 159
Εικόνα 33. Πλήθος προϊόντων ανά κατηγορία που υποστηρίζουν μεμονωμένους τρόπους χρήσης 162
Εικόνα 34. Πλήθος προϊόντων που προσφέρονται σε μεμονωμένες αγορές ή σε καμία αγορά.162
Εικόνα 35. Πλήθος προϊόντων που προσφέρονται σε συνδυασμούς αγορών**Error! Bookmark not defined.**
Εικόνα 36. Πλήθος προϊόντων ανά κατηγορία που προσφέρονται σε μεμονωμένες αγορές ή σε καμία αγορά.....163
Εικόνα 37. Πλήθος προϊόντων ανά κατηγορία που προσφέρονται σε συνδυασμούς αγορών ...164
Εικόνα 38. Πλήθος προϊόντωνπου προσφέρουν είτε 1 πακέτο υποστήριξης είτε περισσότερα .165
Εικόνα 39. Πλήθος προϊόντων ανά κατηγορία που προσφέρουν είτε ένα πακέτο υποστήριξης είτε περισσότερα 165

Ακρωνύμια

ABAC	Attribute Based Access Control
AES	Advanced Encryption Standard
API	Application Programming Interface
ARP	Address Resolution Protocol
ATM	Automated Teller Machine
AWS	Amazon Web Services
BC	Business Continuity
BCDR	Business Continuity and Disaster Recovery
BYOL	Bring Your Own License
CPU	Central Processing Unit
CSS	Cascading Style Sheets
DDoS	Distributed Denial of Service
DES	Data Encryption Standard
DNS	Domain Name System
DOM	Document Object Model
DoS	Denial of Service
DR	Disaster Recovery
FAQ	Frequently Asked Questions
GB	Gigabyte
Gbps	Gigabit per second
GCP	Google Cloud Platform
GUI	Graphical User Interface
HIDS	Host Intrusion Detection System
HTML	Hypertext Markup Language
HTTP	Hypertext Transfer Protocol
IaaS	Infrastructure as a Service
IAM	Identity and Access Management
IDS	Intrusion Detection System
IPS	Intrusion Prevention System

IPSec	Internet Protocol Security
Mbps	Megabit per second
NAS	Network-attached storage
NIDS	Network Intrusion Detection System
NIST	National Institute of Standards and Technology
OS	Operating System
OTP	One Time Password
PaaS	Platform as a Service
PAP	Policy Administration Point
PDP	Policy Decision Point
PEP	Policy Enforcement Point
PGP	Pretty Good Privacy
PIN	Personal Identification Number
PIP	Policy Information Point
RAM	Random Access Memory
RBAC	Role Based Access Control
RFC	Request for Comments
RPO	Recovery Point Objective
RSA	Rivest Shamir Adleman
RTO	Recovery Time Objective
SEM	Security Event Management
SaaS	Software as a Service
SAML	Security Assertion Markup Language
SecaaS	Security as a Service
SFTP	Secure File Transfer Protocol
SIEM	Security Information and Event Management
SIM	Security Information Management
SLA	Service Level Agreement
SMTP	Simple Mail Transfer Protocol (SMTP)
SNMP	Simple Network Management Protocol
SQL	Structured Query Language

SSH	Secure Shell
TB	Terabyte
TCP/IP	Transmission Control Protocol/ Internet Protocol
TLS/SSL	Transport Layer Security/Secure Sockets Layer
UDP	User Datagram Protocol
URL	Uniform Resource Locator
VM	Virtual Machine
VPN	Virtual Private Network
XACML	eXtensible Access Control Markup Language
XML	eXtensible Markup Language
XOR	Exclusive or

Περίληψη

Η παρούσα διπλωματική εργασία αρχικά παρουσιάζει τα βασικά σημεία του υπολογιστικού νέφους και την ασφάλειας πληροφοριακών συστημάτων. Δημιουργείται με αυτό τον τρόπο το θεωρητικό υπόβαθρο ώστε στη συνέχεια να παρουσιαστούν οι κατηγορίες προϊόντων ασφάλειας σαν υπηρεσία και η τρέχουσα κατάσταση της αντίστοιχης αγοράς μέσα από τη διεξαγωγή έρευνας σε 150 προϊόντα αυτού του είδους.

Η συνεισφορά προς τους χρήστες υπηρεσιών είναι σημαντική διότι η στατιστική γνώση που παράγεται συνιστά ανεπιφύλακτα μια αρχική καθοδήγηση προς την επιλογή προϊόντων αυτού του είδους. Επιπλέον, η εργασία μπορεί να αποτελέσει την βάση ώστε να δημιουργηθεί ένας διαδικτυακός χώρος συγκέντρωσης όλων των προϊόντων ασφάλειας σαν υπηρεσία. Εκεί θα προσδιορίζονται με ακρίβεια τα χαρακτηριστικά τους με δυνατότητα εφαρμογής συνθέτων φίλτρων αναζήτησης (πχ. αναζήτηση προϊόντος διαχείρισης ταυτότητας και πρόσβασης (IAM) που να υποστηρίζει την τεχνολογία ελέγχου πρόσβασης βάσει ρόλου (RBAC)).

Η συνεισφορά προς την ακαδημαϊκή κοινότητα είναι εξίσου σημαντική για τους εξής λόγους: (α) παρέχεται ένα σύνολο από κριτήρια που μπορούν να χρησιμοποιηθούν για την περιγραφή των υπηρεσιών SecaaS, (β) παράγεται γνώση με βάση την οποία μπορεί να διεξαχθεί περαιτέρω έρευνα, πιο κατευθυνόμενη εστιάζοντας, πχ. σε συγκεκριμένες κατηγορίες προϊόντων SecaaS για να αναδειχθούν οι ιδιαιτερότητές τους καθώς και ειδικά κριτήρια περιγραφής των προϊόντων τους, και (γ) τέλος, μπορεί να αναπτυχθεί ένα εκτεταμένο μοντέλο περιγραφής υπηρεσιών SecaaS καθώς και ένα πρωτότυπο για την υποστήριξη της περιγραφής και ανακάλυψης υπηρεσιών SecaaS προς όφελος της κοινότητας των χρηστών και των ακαδημαϊκών.

Λέξεις Κλειδιά: υπολογιστικό νέφος, ασφάλεια πληροφοριακών συστημάτων, προϊόντα ασφαλείας σαν υπηρεσία, έρευνα, επισκόπηση αγοράς

Abstract

This thesis initially presents the main points of cloud computing and information system security. In this way, the theoretical background is created to then present the categories of security as a service products and the current state of the market through a survey of 150 products of this type.

The contribution to the users of such services is important because the statistical knowledge produced unreservedly constitutes an initial guidance towards the selection of products of this kind. In addition, the work can form the basis for creating an online concentration place for all security products as services. There they will be precisely characterized with the ability to apply complex search filters (e.g., search for an identity and access management (IAM) product that supports role-based access control (RBAC) technology).

The contribution to the academic community is equally important due to the following reasons: (a) a set of criteria is provided that can be used to describe SecaaS services, (b) knowledge is generated on the basis of which further research can be conducted, more directed focusing, e.g., on specific categories of SecaaS products to highlight their specificities as well as specific product description criteria, and (c) finally, an extended SecaaS service description model as well as a prototype to support the description and discovery of SecaaS services can be developed for the benefit of the user community and academia.

Keywords: cloud computing, information system security, security as a service products, market research

1 Εισαγωγή

1.1 Εισαγωγή

Σήμερα, στην εποχή της ραγδαίας τεχνολογικής εξέλιξης, παρατηρούμε πως η χρήση των πληροφοριακών συστημάτων συνεχώς αναπτύσσεται με ταχύτατους ρυθμούς. Δυστυχώς, η χρήση της τεχνολογίας, ανεξάρτητα από το είδος συσκευής χρήσης (απλό κινητό τηλέφωνο ή προσωπικός υπολογιστής) και το είδος της εφαρμογής ή πληροφοριακού συστήματος, συνοδεύεται από κινδύνους ασφάλειας (πχ. κλοπή δεδομένων). Είναι λοιπόν απαραίτητο όλοι οι χρήστες να προστατεύουν, όσο είναι δυνατόν, τις συσκευές και εφαρμογές τους χρησιμοποιώντας τα κατάλληλα προϊόντα ασφαλείας. Πλέον τα προϊόντα ασφαλείας μπορούν να παρέχονται σαν υπηρεσία (security as a service - SecaaS) και πάνω σε αυτό το δεδομένο αναπτύχθηκε η παρούσα διπλωματική εργασία. Η εργασία εξετάζει την αγορά των προϊόντων λογισμικού σαν υπηρεσία μέσα από μία μεγάλη έρευνα στις διαφορετικές κατηγορίες προϊόντων αυτής της αγοράς.

1.2 Πρόβλημα και τρόπος αντιμετώπισης

Το πρόβλημα που αντιμετωπίζει η παρούσα εργασία είναι η έλλειψη στοιχείων για την αγορά προϊόντων ασφάλειας σαν υπηρεσία, μια έλλειψη που καθιστά σχεδόν αδύνατο τον εντοπισμό και επιλογή αυτών των προϊόντων για την προστασία των πληροφοριακών συστημάτων και εφαρμογών. Παρέχονται πληροφορίες για το ποιες είναι και πως λειτουργούν οι κατηγορίες των προϊόντων ασφάλειας που προσφέρονται σαν λογισμικό. Επίσης, για κάθε μια από τις δέκα κατηγορίες προϊόντων εντοπίζονται και αποτιμώνται 15 προϊόντα με βάση συγκεκριμένα κριτήρια. Τα κριτήρια αυτά ισοδυναμούν με τις βασικές πληροφορίες τις οποίες θα αναζητούσε ένας υποψήφιος αγοραστής ο οποίος θα πραγματοποιούσε έρευνα για να επιλέξει και αποκτήσει ένα προϊόν. Επιπλέον, παρέχονται στατιστικά στοιχεία για το σύνολο των προϊόντων όλων των κατηγοριών καθώς και νικητήρια προϊόντα για κάθε κατηγορία. Όλα τα παραπάνω μπορούν να δώσουν μια πολύ καλή εικόνα για την κατάσταση της αγοράς σε όποιον ενδιαφέρεται να αποκτήσει προϊόντα ασφάλειας σαν υπηρεσία. Η παρούσα εργασία ουσιαστικά απαλλάσσει τους ενδιαφερόμενους από μία έρευνα αγοράς, η οποία θα έπαιρνε πάρα πολύ χρόνο, και βοηθά στο να δημιουργηθεί ένα ασφαλές περιβάλλον για εφαρμογές και πληροφοριακά συστήματα, νωρίτερα από το αναμενόμενο, μέσω της επιλογής και ενσωμάτωσης των κατάλληλων προϊόντων ασφάλειας ως υπηρεσία. Με αυτό τον τρόπο, μπορεί να αποτραπούν ορισμένες επιθέσεις που θα συνέβαιναν κατά το (μεγάλο) χρονικό διάστημα διεξαγωγής της ερευνάς αγοράς μεμονωμένα από τον κάθε ενδιαφερόμενο, όπου το πληροφοριακό σύστημα / εφαρμογή του θα ήταν ακόμη

απροστάτευτο/η. Επίσης η παρούσα εργασία βοηθά την ακαδημαϊκή κοινότητα καθώς παρέχει πολύτιμη γνώση και πληροφορίες ώστε μελλοντικά να διεξαχθούν έρευνες με πολύ πιο εξειδικευμένα κριτήρια. Οι έρευνες αυτές θα έχουν ως αποτέλεσμα να προσδιοριστεί μεγάλος πλήθος χαρακτηριστικών των προϊόντων λογισμικού σαν υπηρεσία και να εντοπιστούν ιδιαιτερότητες που μέχρι στιγμής δεν είναι εμφανείς και έχουν ερευνητικό ενδιαφέρον. Τέλος, με βάση την συνεισφορά της εργασίας μπορεί να αναπτυχθεί ένα εκτεταμένο μοντέλο περιγραφής υπηρεσιών SecaaS καθώς και ένα πρωτότυπο για την υποστήριξη της περιγραφής και ανακάλυψης υπηρεσιών SecaaS προς όφελος της κοινότητας των χρηστών και των ακαδημαϊκών.

1.3 Δομή εργασίας

Το υπόλοιπο μέρος της εργασία δομείται ως εξής. Στο δεύτερο κεφάλαιο καλύπτεται η εισαγωγή στο υπολογιστικό νέφος, περιγράφοντας τις βασικές έννοιες σχετικά με τα μοντέλα παράδοσης και ανάπτυξης του. Στο τρίτο κεφάλαιο αναλύονται οι βασικές έννοιες ασφάλειας των πληροφοριακών συστημάτων και τα σημαντικότερα είδη επιθέσεων. Στο τέταρτο κεφάλαιο περιγράφονται αναλυτικά οι 10 κατηγορίες υπηρεσιών ασφαλείας που παρέχονται από το υπολογιστικό νέφος σύμφωνα με την οργάνωση Cloud Security Alliance. Στο πέμπτο κεφάλαιο πραγματοποιήθηκε αποτίμηση 150 προϊόντων (15 προϊόντα για κάθε μία από τις 10 κατηγορίες υπηρεσιών ασφαλείας) με βάση συγκεκριμένα κριτήρια, τα οποία περιγράφονται στην εισαγωγή αυτού του κεφαλαίου. Στη συνέχεια παρουσιάζονται στατιστικά στοιχεία και νικητήρια προϊόντα για κάθε κατηγορία. Επίσης παρουσιάζονται καθολικά στατιστικά στοιχεία και γραφήματα ανά κριτήριο για όλα τα προϊόντα κατά μήκος όλων των κατηγοριών. Στο τελευταίο κεφάλαιο παρουσιάζονται βασικά συμπεράσματα που προέκυψαν μέσα από την εργασία και μελλοντικές κατευθύνσεις.

2 Υπολογιστικό νέφος

2.1 Εισαγωγή στο υπολογιστικό νέφος

Το υπολογιστικό νέφος είναι μια τεχνολογία στον χώρο της πληροφορικής όπου μέρα με τη μέρα ε-δραιώνεται και συγχρόνως επεκτείνεται όλο και περισσότερο. Αυτό συμβαίνει διότι έχει να προσφέρει πάρα πολλά οφέλη σε επιχειρήσεις και οργανισμούς που την υιοθετούν.

Το υπολογιστικό νέφος ορίζεται ως μια εξειδικευμένη μορφή κατανεμημένης υπολογιστικής που εισάγει διαφορετικά μοντέλα χρήσης για απομακρυσμένους, κλιμακούμενους και μετρήσιμους πόρους [1]**.** Σε πρωταρχική μορφή έκανε την εμφάνιση του τη δεκαετία του 1990, όπου δημιουργήθηκαν οι πρώτες υπηρεσίες κοινής ωφέλειας, όπως οι μηχανές αναζήτησης και οι υπηρεσίες ηλεκτρονικού ταχυδρομείου. Τα επόμενα χρόνια πολλές εταιρείες, όπως η Amazon, άρχισαν να μισθώνουν υπολογιστική ισχύ σε επιχειρήσεις για την εκτέλεση επιχειρησιακών λειτουργιών, κάτι το οποίο συνεχίζει να εφαρμόζεται μέχρι και σήμερα [2]. Η φιλοσοφία πίσω από την ανάπτυξη του νέφους είναι ότι όποιος υιοθετήσει αυτή την τεχνολογία πληρώνει μόνο για την κατανάλωση πόρων οπότε δεν χρειάζεται να επενδύσει σε αυτούς και να τους διαχειριστεί. Ένα αντίστοιχο παράδειγμα της καθημερινής ζωής είναι η υδροδότηση. Το κάθε σπίτι πληρώνει ένα χρηματικό ποσό στον δήμο για την λήψη πόσιμου νερού αντί να έχει τα δικά του μέσα συλλογής, αποθήκευσης, φιλτραρίσματος και παροχής πόσιμου νερού.

Πλεονεκτήματα

Γίνεται λοιπόν αντιληπτό ότι η χρήση νέφους μόνο ωφέλιμη μπορεί να αποδειχθεί για επιχειρήσεις και οργανισμούς. Το κύριο πλεονέκτημα είναι το οικονομικό όφελος. Μία επιτόπια εγκατάσταση θα απαιτούσε αγορά, συντήρηση και πιθανή επισκευή μηχανημάτων, τα όποια απαιτούν ένα αξιοσέβαστο αρχικό κεφάλαιο και στη συνέχεια ενέχουν λειτουργικό κόστος [2]. Επίσης, για όλες τις παραπάνω διαδικασίες είναι απαραίτητη η απασχόληση επιπλέον εξειδικευμένου προσωπικού, το οποίο σημαίνει επιπλέον κόστος μισθοδοσίας. Ταυτόχρονα, επιβαρύνεται το υπάρχον προσωπικό με επιπλέον αρμοδιότητες (πχ. διαδικασίες λογιστηρίου για μεγαλύτερο αριθμό υπαλλήλων). Μία εγκατάσταση απαιτεί τον κατάλληλο χώρο, το οποίο σημαίνει επιπλέον έξοδα για ενδεχόμενη ενοικίαση και στη συνέχεια διαμόρφωση του χώρου. Ένα παράδειγμα διαμόρφωσης ενός χώρου είναι η εγκατάσταση συστήματος συναγερμού και πυρασφάλειας. Τέλος, αυξάνονται πάγια έξοδα, όπως η κατανάλωση ηλεκτρικού ρεύματος όταν τροφοδοτείται μία ολόκληρη εγκατάσταση σε σύγκριση με τη χρήση απλών προσωπικών υπολογιστών στην περίπτωση χρήσης (υπηρεσιών) νέφους. Ένα ακόμα πάγιο το οποίο αυξάνεται είναι το κόστος ασφάλισης της επιχείρησης καθώς σε περίπτωση ατυχήματος θα πρέπει η ασφαλιστική να α-ποζημιώσει την εταιρεία για εξοπλισμό μεγάλης χρηματικής αξίας. Όταν λοιπόν όλα τα παραπάνω

κόστη και διαδικασίες μεταφερθούν σε μία τρίτη οντότητα δηλαδή στον πάροχο νέφους τότε το οικονομικό κέρδος για την επιχείρηση είναι πολύ μεγάλο. Σε αντίθεση με την επιτόπια εγκατάσταση η μοναδική οικονομική υποχρέωση είναι η καταβολή ενός (συνήθως μηνιαίου) χρηματικού ποσού προς τον πάροχο νέφους για την χρήση των πόρων και υπηρεσιών του.

Ένα ακόμα μεγάλο πλεονέκτημα είναι η ευελιξία. Όταν μία επιχείρηση μισθώνει υπολογιστικούς πόρους έχει τη δυνατότητα είτε να ζητήσει αύξηση πόρων είτε μείωση πόρων όποτε το θελήσει [2]. Αυτό είναι ένα τεράστιο πλεονέκτημα γιατί κάθε φορά μπορεί να χρησιμοποιεί όσους πόρους χρειάζεται σε αντίθεση με μία επιχείρηση που διαθέτει επιτόπια εγκατάσταση. Στην περίπτωση της επιτόπιας εγκατάστασης είτε θα υπάρχουν περισσότεροι πόροι από τους απαιτούμενους είτε λιγότεροι. Αυτό συμβαίνει διότι κάθε φορά η αγορά, η ρύθμιση και η ενσωμάτωση ενός νέου μηχανήματος ή αντίστοιχα η ρύθμιση της εγκατάστασης, η αποσύνδεση και η πώληση/αποθήκευση μηχανημάτων έχει οικονομικό κόστος και δεν μπορεί να πραγματοποιηθεί σε αυστηρά χρονικά πλαίσια. Έτσι, λοιπόν, οι επιπλέον πόροι σε μία επιτόπια εγκατάσταση μεταφράζονται σε αυξημένο κόστος αγοράς και λειτουργίας. Αντίστοιχα η έλλειψη πόρων σημαίνει περιορισμένες δυνατότητες, οι οποίες ενδεχομένως να οδηγούν σε καθυστερήσεις και αθέτηση συμφωνιών ή ακόμα και να αποτρέψουν την επιχείρηση από το να συνάψει μια μελλοντική συμφωνία για κάποιο έργο. Αυτό με τη σειρά του μεταφράζεται σε κακή φήμη στην αγορά το οποίο είναι βέβαιο πως οδηγεί σε μακροπρόθεσμη απώλεια χρημάτων.

Άλλο ένα πλεονέκτημα είναι η διαθεσιμότητα και η αξιοπιστία [2]. Αρχικά είναι λογικό είτε πρόκειται για υπηρεσίες νέφους είτε πρόκειται για επιτόπια εγκατάσταση να υπάρξουν απρόοπτα τα οποία θα διακόψουν τις λειτουργικές διαδικασίες της επιχείρησης. Το πλεονέκτημα των υπηρεσιών νέφους είναι πως παρέχουν αρκετά μεγαλύτερη διαθεσιμότητα και αξιοπιστία σε σχέση με μία επιτόπια εγκατάσταση. Αυτό συμβαίνει διότι οι πάροχοι είναι εξειδικευμένες εταιρείες με κέντρα δεδομένων διάσπαρτα σε όλο τον πλανήτη, με δυνατότητα χρήσης εξισορροπητών φορτίων πάνω από στιγμιότυπα μιας εφαρμογής, με άρτια καταρτισμένο προσωπικό και με διεθνώς αναγνωρισμένες πιστοποιήσεις. Είναι, λοιπόν, βέβαιο πως η αξιοπιστία και η διαθεσιμότητα που παρέχουν είναι μεγαλύτερη από αυτή που μπορεί να έχει μία απλή, συνήθως μικρό-μεσαία επιχείρηση στο εσωτερικό της, η οποία λειτουργεί ¨αυθαίρετα¨ χωρίς να είναι υποχρεωμένη να ακολουθήσει κάποια πρότυπα. Βέβαια ενδεχομένως να υπάρχουν και εξαιρέσεις ενώ μεγάλες εταιρείες σίγουρα ακολουθούν καλές πρακτικές & πρότυπα.

Ένα ακόμα πλεονέκτημα που προσφέρει το υπολογιστικό νέφος είναι η συνεργατικότητα [2]. Όταν όλο το προσωπικό μιας επιχείρησης χρησιμοποιεί το ίδιο λογισμικό, το οποίο προσφέρει ένας πάροχος υπηρεσιών νέφους, τότε όλοι εργάζονται πάνω στην ίδια έκδοση του προϊόντος. Έτσι, λοιπόν, αποφεύγονται πιθανά προβλήματα ασυμβατότητας ανάμεσα σε αρχεία τα οποία δημιουργήθηκαν ή επεξεργάστηκαν με διαφορετικά λογισμικά ή διαφορετικές εκδόσεις του ίδιου λογισμικού. Επιπλέον, μπορούν να δημιουργηθούν κοινόχρηστα αρχεία (πχ. Google doc) όπου εκεί γίνεται ξεκάθαρο ποια τροποποίηση πραγματοποιήθηκε, από ποιόν χρήστη και ποια χρονική στιγμή. Με αυτόν τον τρόπο, εξοικονομείται χαμένος χρόνος από της συνεχείς επαναποστολές αρχείων τηςλές εκδόσεις. Μία ακότηςπτυχή της

συνεργατικότητας είναι η από κοινού συγγραφή αρχείων και προγραμμάτων/εφαρμογών. Το νέφος προσφέρει τη δυνατότητα σε μέλη ίδιων και διαφορετικών επιχειρήσεων που βρίσκονται σε διαφορετικές περιοχές γεωγραφικά να εργάζονται πάνω στην ίδια πλατφόρμα, με τα ίδια εργαλεία και στο ίδιο περιεχόμενο. Έτσι λοιπόν μπορούν να δημιουργηθούν με ιδιαίτερη ευκολία, από άποψη πρόσβασης στο περιεχόμενο, τεράστια έργα πληροφορικής με τη συνδρομή ανθρώπων από όλο τον κόσμο και ταυτόχρονα μειώνονται τα έξοδα επιχειρήσεων για μεταφορά και διαμονή προσωπικού σε διαφορετικές περιοχές κάθε φορά.

Επιπλέον, το νέφος προσφέρει το πλεονέκτημα της φορητότητας, ειδικά στην περίπτωση του μοντέλου λογισμικού σαν υπηρεσία [2]. Οι χρήστες δεν είναι υποχρεωμένοι να εργάζονται από τον υπολογιστή του γραφείου τους. Αντίθετα μπορούν να έχουν πρόσβαση στα εργαλεία και τις εφαρμογές που τους είναι απαραίτητα όλο το 24ωρο, από οποιοδήποτε σημείο του πλανήτη μέσα από οποιαδήποτε συσκευή (ακόμα και κινητό τηλέφωνο) που τηρεί ορισμένες ελάχιστες προδιαγραφές.

Τέλος, ένα πλεονέκτημα του νέφους είναι η δυνατότητα ανάκαμψης από καταστροφές. Οι επιχειρήσεις που αποθηκεύουν τα δεδομένα τους μόνο σε επιτόπιες εγκαταστάσεις κινδυνεύουν να χάσουν τα δεδομένα αυτά σε περίπτωση φυσικής καταστροφής ή κυβερνο-επίθεσης. Αντιθέτως, όταν τα δεδομένα βρίσκονται αποθηκευμένα και στο νέφος, ανεξάρτητα από την καταστροφή που θα συμβεί, θα παραμείνουν ασφαλή. Τα αρχεία κομματιάζονται και κάθε κομμάτι αναπαράγεται και αποθηκεύεται σε διαφορετικά σημεία του πλανήτη. Οπότε, αν προκύψει κάποιο πρόβλημα σε ένα σημείο, τότε τα αντίστοιχα κομμάτια που έχουν αποθηκευτεί εκεί θα είναι ακόμη διαθέσιμα σε άλλα σημεία του πλανήτη.

Μειονεκτήματα

Από την άλλη πλευρά, ένα μειονέκτημα του νέφους είναι τα ζητήματα ασφάλειας [2]. *Όταν* χρησιμοποιούνται υπηρεσίες νέφους και άρα τα δεδομένα μεταφέρονται στο νέφος, τότε η ασφάλεια των δεδομένων θα λέγαμε ότι μοιράζεται ανάμεσα στην επιχείρηση και στον πάροχο. Το πρόβλημα σε αυτή την περίπτωση είναι πως ενδεχομένως η επιχείρηση και ο πάροχος να μην υποστηρίζουν τα ίδια ή συμβατά πλαίσια εργασίας ασφάλειας και έτσι να προκύψουν τρωτά σημεία. Άρα, λοιπόν, η ασφάλεια των δεδομένων περιορίζεται από τους μηχανισμούς ελέγχου και τις πολιτικές ασφάλειας που εφαρμόζονται από τον πάροχο νέφους και από την επιχείρηση. Επίσης, μειώνεται σημαντικά εφόσον υπάρχει ασυμβατότητα πλαισίων.

Ένα ακόμα μειονέκτημα είναι πως η επιχείρηση, η οποία έχει μισθώσει πόρους, δε μπορεί να έχει τον πλήρη έλεγχο τους [2]. Στην περίπτωση που δεν τηρείται ότι έχει συμφωνηθεί στο συμβόλαιο με τον πάροχο είναι πολύ πιθανό να διαταραχθεί η ομαλή λειτουργία της επιχείρησης. Τα συμβόλαια, συνήθως, διαθέτουν συστήματα ποινών, δηλαδή επιστρέφεται στην επιχείρηση ένα μέρος του χρηματικού ποσού της συνδρομής αν δεν τηρηθούν τα συμφωνηθέντα. Αυτό όμως δεν αλλάζει το γεγονός πως στην περίπτωση που υπάρχουν προβλήματα η επιχείρηση είναι αυτή που εκτίθεται απέναντι στους πελάτες της παρόλο που δεν φέρει την αποκλειστική ευθύνη. Επιπλέον, η ίδια η επιχείρηση θα πρέπει

να αποδείξει πως πραγματικά υπήρξε πρόβλημα ώστε να λάβει πίσω κάποιο χρηματικό ποσό ή μια προσφορά.

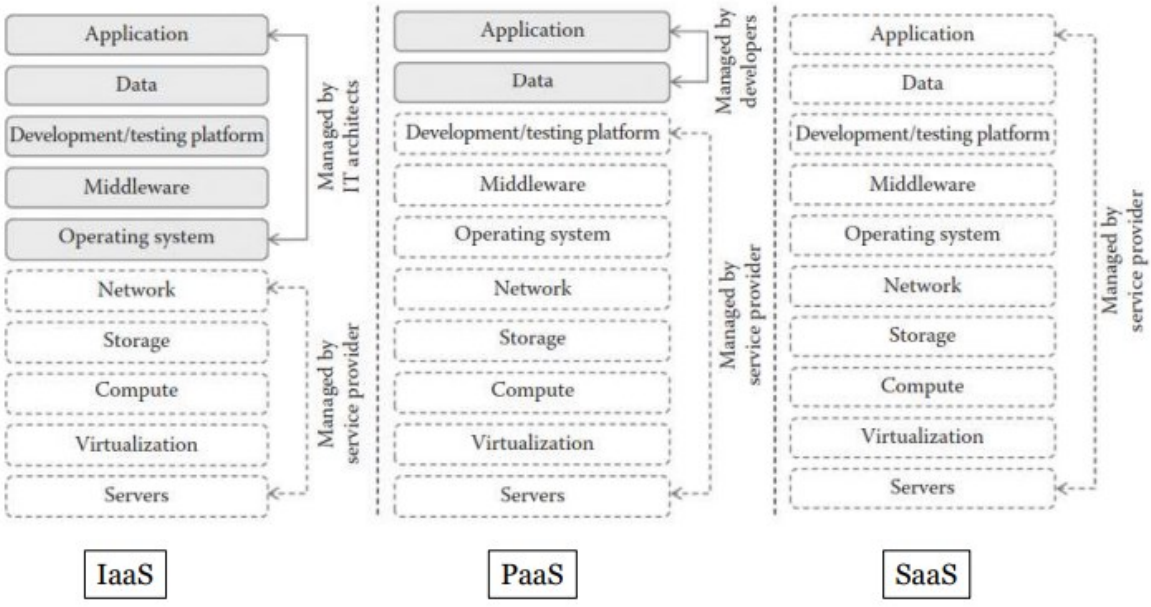
Ένα ακόμα μειονέκτημα είναι πως υπάρχει το πρόβλημα του κλειδώματος σε πάροχο [2]. Ειδικότερα, η διαδικασία μετακίνησης από έναν πάροχο σε έναν άλλο είναι μια σύνθετη διαδικασία όπου προκύπτουν ζητήματα συμβατότητας ενώ πρέπει να αντιμετωπιστούν πολλές προκλήσεις όπως η μεταφορά δεδομένων. Για παράδειγμα, ένα ζήτημα είναι πόσο γρήγορα θα μεταφερθούν τα δεδομένα, και αν θα διαγραφούν πλήρως από τον αρχικό πάροχο.

Τέλος, ένα μειονέκτημα είναι πως οι επιχειρήσεις δεν γνωρίζουν σε ποια ακριβώς τοποθεσία βρίσκονται οι πόροι του νέφους άρα και σε ποια τοποθεσία βρίσκονται αποθηκευμένα τα δεδομένα τους. Το πρόβλημα σε αυτή την περίπτωση είναι πως υπάρχουν νομικά ζητήματα, σχετικά με την ιδιωτικότητα και την πρόσβαση σε δεδομένα, τα οποία διαφέρουν από χώρα σε χώρα. Έτσι, λοιπόν, ενδεχομένως να χρειαστεί να αποκαλυφθούν δεδομένα πελατών μίας επιχείρησης σε κυβερνητικές υπηρεσίες άλλων χωρών χωρίς τη σύμφωνη γνώμη τους ή να αποθηκεύονται δεδομένα σε χώρες όπου αυτό απαγορεύεται.

2.2 Μοντέλα Παράδοσης

Το υπολογιστικό νέφος ανάλογα με το μοντέλο παράδοσης διακρίνεται στις 3 ακόλουθες κατηγορίες όπου οι διαφορές τους φαίνονται στο παρακάτω σχήμα:

- Λογισμικό σαν υπηρεσία
- Υποδομή σαν υπηρεσία
- Πλατφόρμα σαν υπηρεσία



Εικόνα 1. Διαφορές μεταξύ των 3 μοντέλων παράδοσης του υπολογιστικού νέφους

Στην παραπάνω εικόνα βλέπουμε το φόρτο εργασίας που υπάρχει σε ένα πληροφοριακό σύστημα και ποιος διαχειρίζεται αυτό το φόρτο εργασίας ανάλογα με το μοντέλο παράδοσης (και άρα το επίπεδο ελέγχου που προσφέρεται στον χρήστη/πελάτη). Παρατηρούμε πως το υψηλότερο επίπεδο ελέγχου υπάρχει στο μοντέλο IaaS όπου μόνο το 50% της διαχείρισης γίνεται από την πλευρά του παρόχου, στη συνέχεια ακολουθεί το μοντέλο PaaS όπου το 80% της διαχείρισης γίνεται από την πλευρά του παρόχου και τέλος το χαμηλότερο επίπεδο ελέγχου βρίσκεται στο μοντέλο SaaS όπου το 100% της διαχείρισης γίνεται από την πλευρά του παρόχου.

2.2.1 Λογισμικό σαν υπηρεσία (Software as a service)

Στο μοντέλο παράδοσης λογισμικού ως υπηρεσία ο πάροχος προσφέρει ένα πρόγραμμα λογισμικού σαν υπηρεσία νέφους, η οποία επικοινωνεί με τον πελάτη μέσω ενός περιβάλλοντος διαδικτύου. Χαρακτηριστικά αυτού του μοντέλου είναι η περιορισμένη δυνατότητα διαχείρισης από τους χρήστες, η πρόσβαση μέσω περιηγητή διαδικτύου, η υποστήριξη πολλαπλών συσκευών και η υψηλή διαθεσιμότητα [3]. Παραδείγματα τέτοιων υπηρεσιών είναι τα προγράμματα διαχείρισης επιχειρησιακών πόρων (π.χ Prosvasis GO) και τα προγράμματα διαχείρισης εγγράφων (πχ. Office365).

Τα πλεονεκτήματα του λογισμικού σαν υπηρεσία είναι πως δεν υπάρχει καμία εγκατάσταση συσκευής στην πλευρά του πελάτη, το οποίο ισοδυναμεί με μειωμένο κόστος. Επιπλέον, το κόστος μειώνεται διότι η χρέωση πραγματοποιείται με ευέλικτο τρόπο. Οι χρήστες πληρώνουν ένα πάγιο ποσό/συνδρομή ώστε να μπορούν να χρησιμοποιήσουν την υπηρεσία/ λογισμικό ενώ υπάρχουν πολλά διαφορετικά πακέτα συνδρομής ανάλογα με τις ανάγκες των χρηστών. Οι χρήστες δεν επιβαρύνονται με διαδικασίες συντήρησης, όπως για παράδειγμα εγκατάσταση ενημερώσεων. καθώς οποιαδήποτε διαδικασία αφορά την συντήρηση πραγματοποιείται από τον πάροχο του προϊόντος. Τέλος, δύο ακόμη πλεονεκτήματα [3], όπως αναφέρθηκε παραπάνω, είναι η δυνατότητα πρόσβασης από πολλαπλές διαφορετικής συσκευές μέσω του διαδικτύου και η υψηλή διαθεσιμότητα που εγγυώνται τις περισσότερες φορές οι πάροχοι του λογισμικού.

Τα μειονεκτήματα του λογισμικού σαν υπηρεσία είναι τα πιθανά ζητήματα ασφαλείας (πχ. διαρροή εταιρικών δεδομένων ή διαπιστευτηρίων χρηστών) που μπορεί να δημιουργηθούν αν ο πάροχος δεν είναι απολύτως αξιόπιστος. Γι' αυτό προτείνεται να μη χρησιμοποιείται αυτό το μοντέλο διάταξης αν το ρίσκο ασφάλειας είναι μεγάλο για ιδιωτικά/ευαίσθητα δεδομένα. Ένα ακόμα μειονέκτημα είναι πως για να λειτουργήσει σωστά ένα προϊόν και να υπάρξει ένα ικανοποιητικό επίπεδο παροχής υπηρεσιών, θα πρέπει πρώτα να έχει εξασφαλιστεί σύνδεση στο διαδίκτυο με κατάλληλη ταχύτητα (ανάλογα με το είδος της εφαρμογής, το όγκο των δεδομένων που πρέπει να συναλλάσσονται ανά χρονική μονάδα και πόσο συχνά πραγματοποιείται αλληλεπίδραση μεταξύ του πελάτη και της εφαρμογής) και άρα να ικανοποιούνται κατάλληλες απαιτήσεις συνδεσιμότητας. Βέβαια αυτό αποτελεί πρόβλημα και για τα άλλα είδη υπηρεσιών. Τέλος, δύο τελευταία μειονεκτήματα [3] είναι οι περιορισμένες δυνατότητες διαχείρισης λογισμικού και η απουσία ελέγχου των δεδομένων.

2.2.2 Υποδομή σαν υπηρεσία (Infrastructure as a service)

Στο μοντέλο παράδοσης υποδομής σαν υπηρεσία ο πάροχος προσφέρει ένα σύνολο πόρων υποδομής στον πελάτη, δηλαδή προσφέρει πόρους για την εκτέλεση των εφαρμογών. Η διαφορά σε σχέση με το μοντέλο ανάπτυξης λογισμικού σαν υπηρεσία είναι ότι ο χρήστης είναι υπεύθυνος για την ανάπτυξη και διαχείριση της εφαρμογής [3]. Χαρακτηριστικά αυτού του μοντέλου είναι:

α. η πρόσβαση στην υποδομή (στους πόρους), η οποία αποτελείται από εικονικές μηχανές, μέσω του διαδικτύου [3]
β. η κλιμάκωση των πόρων καθώς ένας πελάτης μπορεί ανά πάσα στιγμή να αιτηθεί αύξηση ή μείωση τον πόρων, συνεπώς και της ισχύος που ενοικιάζει [3]
γ. η δυνατότητα μέτρησης της χρήσης των υπηρεσιών ώστε να υπάρξει η αντίστοιχη χρέωση [3]

Τα πλεονεκτήματα της υποδομής σαν υπηρεσία είναι ότι μπορεί να εφαρμοστεί η τιμολόγηση με βάση τη χρήση με ακρίβεια και έτσι ο πελάτης να χρεώνεται ακριβώς για ότι χρησιμοποιεί μέσα στα πλαίσια συγκεκριμένης μοναδιαίας χρονικής διάρκειας, πολύ μικρότερης από αυτής για υπηρεσίες SaaS. Ένα ακόμα πλεονέκτημα είναι το μειωμένο κόστος χρήσης για τον πελάτη διότι οι τιμές μοναδιαίας χρέωσης είναι αρκετά φθηνές και δεν υπάρχουν έξτρα χρεώσεις που θα ίσχυαν εφόσον μιλούσαμε για επιτόπια υποδομή. Επιπλέον, η άμεση δυνατότητα για αύξηση ή μείωση πόρων δίνει τη δυνατότητα στον πελάτη να λειτουργεί ευέλικτα χωρίς να χρειάζεται εκ των προτέρων κατάλληλος προγραμματισμός και εκτιμήσεις προσδιορισμού της απαιτούμενης υπολογιστικής ισχύος [3]. Όλα τα παραπάνω συντελούν στη δημιουργία μιας ολοκληρωμένης**,** σωστά δομημένης και ευέλικτης αρχιτεκτονικής πληροφορικής για μία επιχείρηση με κατάλληλο κόστος λειτουργίας. Αυτό σίγουρα λειτουργεί θετικά καθώς εξασφαλίζει την απροβλημάτιστη ροή των επιχειρησιακών διαδικασιών και μακροπρόθεσμα ενδεχομένως αυξάνει την κερδοφορία.

Τα μειονεκτήματα της υποδομής σαν υπηρεσία είναι τα ζητήματα ασφάλειας διότι εκτός από τις κλασικές απειλές υπάρχουν και απειλές, οι οποίες έχουν ως στόχο να βλάψουν τις εικονικές μηχανές, δηλαδή την υποδομή [3]. Θα λέγαμε, λοιπόν, ότι προκύπτει ακόμα ένα ευπαθές σημείο στην εγκατάσταση πληροφορικής του πελάτη. Ένα ακόμα μειονέκτημα που προκύπτει από τη φύση αυτού του μοντέλου είναι πως οι χρήστες χρειάζονται κάποια εκπαίδευση ή τουλάχιστον είναι απαραίτητο να ακολουθήσουν μία σειρά διαδικασιών ώστε να διαχειρίζονται κατάλληλα την υποδομή, να αντλούν πόρους όταν αυτό χρειάζεται ή να αφαιρούν πόρους όταν αυτοί πλέον δεν είναι απαραίτητοι**.**

2.2.3 Πλατφόρμα σαν υπηρεσία (Platform as a service)

Στο μοντέλο παράδοσης πλατφόρμας σαν υπηρεσία ο πάροχος προσφέρει ένα περιβάλλον από ήδη ανεπτυγμένους πόρους. Πάνω στο περιβάλλον αυτό υπάρχουν προϊόντα και εργαλεία τα οποία χρησιμοποιούνται για την ανάπτυξη, δοκιμή, συντήρηση και εκτέλεση λογισμικού από προγραμματιστές.

Χαρακτηριστικά αυτού του μοντέλου είναι η πρόσβαση μέσω διαδικτύου και η δυνατότητα πρόσβασης εκτός σύνδεσης, όπου σε αυτή την περίπτωση το τοπικό ολοκληρωμένο περιβάλλον ανάπτυξης (IDE) αποθηκεύει τις αλλαγές που επιτελούνται από τον χρήστη και συγχρονίζεται με της υπηρεσίες της πλατφόρμας όταν η σύνδεση αποκαθίσταται. Τέλος, ένα χαρακτηριστικό είναι η δυνατότητα αυτό-κλιμάκωσης [3]. Δηλαδή όταν μια εφαρμογή χρειαστεί περισσότερους πόρους από όσους καταναλώνει ήδη, η διαδικασία κλιμάκωσης θα πραγματοποιηθεί αυτόματα από την πλατφόρμα, χωρίς να χρειαστεί η παρέμβαση του πελάτη στη διαδικασία.

Τα πλεονεκτήματα της πλατφόρμας σαν υπηρεσία [3] είναι το γεγονός πως προσφέρει τη δυνατότητα για γρήγορη ανάπτυξη και διάταξη εφαρμογών με μικρό κόστος χρήσης για τον πελάτη. Αυτό συμβαίνει διότι τα εργαλεία που χρησιμοποιούνται και γενικότερα το απαιτούμενο περιβάλλον για την ανάπτυξη εφαρμογών ανήκει στον πάροχο. Επιπλέον, ο πελάτης δεν επιβαρύνεται με διαδικασίες συντήρησης και διαμόρφωσης της πλατφόρμας όπως θα συνέβαινε στην περίπτωση του μοντέλου υποδομής σαν υπηρεσία, το οποίο ισοδυναμεί με κέρδος σε χρήματα και χρόνο καθώς εξοικονομούνται εργατοώρες. Επίσης, η ανάπτυξη εφαρμογών γίνεται πολύ εύκολα λόγω του πλήθους έτοιμων εργαλείων που παρέχονται. Ακόμη, υποστηρίζεται η συνεργατική ανάπτυξη του λογισμικού για περαιτέρω επιτάχυνση της κατασκευής του. Τέλος, η ευελιξία στην διάταξη εφαρμογών επιτυγχάνεται, διότι όπως αναφέρθηκε παραπάνω, υπάρχει η δυνατότητα αυτό-κλιμάκωσης.

Τα μειονεκτήματα της πλατφόρμας σαν υπηρεσία είναι ότι υπάρχουν κάποιοι περιορισμοί σχετικά με τα εργαλεία ανάπτυξης εφαρμογών [3]. Είναι λογικό η πλατφόρμα να περιέχει έναν συγκεκριμένο αριθμό από εργαλεία (και όχι άπειρα) άρα οι προγραμματιστές είναι υποχρεωμένοι να αναπτύξουν τις εφαρμογές τους σύμφωνα με τις τεχνολογίες των εργαλείων αυτών. Σε αντίθετη περίπτωση είναι αδύνατο να εργαστούν σε αυτή την πλατφόρμα. Για παράδειγμα, αν μία πλατφόρμα διαθέτει μεταγλωττιστές (compilers) μόνο για τις γλώσσες προγραμματισμού java και python, ο προγραμματιστής δεν μπορεί να αναπτύξει μία εφαρμογή σε γλώσσα C++. Βέβαια μπορεί να υπάρχει η δυνατότητα να εγκαταστήσουν τα εργαλεία οι ίδιοι αλλά αυτό έρχεται με κάποια μειονεκτήματα (χάσιμο χρόνου, συμβατότητα με άλλα εργαλεία, κα.). Επίσης, επειδή, όπως αναφέρθηκε προηγουμένως, η πλατφόρμα είναι προσβάσιμη μέσω διαδικτύου υπάρχει ο κίνδυνος χαμηλής απόδοσης όταν υπάρχει κακή ποιότητα στη σύνδεση. Άρα, λοιπόν το προαπαιτούμενο για την σωστή χρήση μιας πλατφόρμας είναι να υπάρχει καλή σύνδεση στο διαδίκτυο, όπως αντίστοιχα συμβαίνει και με το μοντέλο λογισμικού σαν υπηρεσία.

2.3 Μοντέλα Διάταξης

Το υπολογιστικό νέφος ανάλογα με το μοντέλο διάταξης διακρίνεται σε 4 κατηγορίες [3]:

- Δημόσιο νέφος
- Ιδιωτικό νέφος
- Υβριδικό νέφος

- Κοινοτικό νέφος

2.3.1 *Δημόσιο νέφος (Public cloud)*

Το δημόσιο νέφος είναι ένα δημόσιο περιβάλλον νέφους το οποίο ανήκει σε έναν πάροχο, ο οποίος είναι υπεύθυνος για την δημιουργία και την συντήρηση του νέφους και των πόρων του. Οι πελάτες αποκτούν πρόσβαση στους πόρους αυτούς με κάποια χρέωση, την οποία ορίζει ο πάροχος. Χαρακτηριστικά του δημοσίου νέφους είναι το μεγάλο μέγεθος του (ως προς την ποσότητα των πόρων που προσφέρει) καθώς και το ότι μπορεί να κλιμακώνεται ανάλογα με τις απαιτήσεις και τον αριθμό των χρηστών. Ένα ακόμα χαρακτηριστικό είναι πως πρόκειται για ένα οικονομικό μοντέλο καθώς οι χρήστες μπορούν να πληρώσουν μόνο για ότι χρησιμοποιήσουν. Τέλος, το δημόσιο νέφος είναι διαθέσιμο από οπουδήποτε και δεν υπάρχουν περιορισμοί πρόσβασης. [3]

Τα πλεονεκτήματα του δημοσίου νέφους [3] είναι ότι δεν χρειάζεται καμία υποδομή στην πλευρά του πελάτη συνεπώς μειώνεται το κόστος (για τον πελάτη). Επιπλέον, λόγω υψηλού ανταγωνισμού ανάμεσα στους παρόχους, οι προσφερόμενες υπηρεσίες είναι υψηλής ποιότητας και αξιόπιστες. Αυτό διασφαλίζεται μέσα και από τις συμφωνίες σε επίπεδο υπηρεσίας (SLAs), οι οποίες όταν παραβιαστούν αποζημιώνεται οικονομικά ο πελάτης. Τέλος, στο δημόσιο νέφος δεν υπάρχει περιορισμός σχετικά με τον αριθμό χρηστών που μπορούν να χρησιμοποιήσουν τις υπηρεσίες, το οποίο σημαίνει πως υπάρχουν μεγάλες δυνατότητες κλιμάκωσης.

Τα μειονεκτήματα του δημοσίου νέφους είναι πως πρόκειται για ένα λιγότερο ασφαλές μοντέλο ανάπτυξης σε σχέση με τα υπόλοιπα μοντέλα. Υπάρχει υψηλότερη πιθανότητα να δημιουργηθούν ζητήματα ασφαλείας και να κλαπούν/διαρρεύσουν δεδομένα. Επιπλέον, οι πελάτες που προτιμούν το δημόσιο νέφος εξαρτώνται εξ ολοκλήρου από μία τρίτη οντότητα [3]. Δηλαδή κατά κάποιο τρόπο χάνουν την αυτονομία τους και δεν μπορούν να υποστηρίξουν τις επιχειρησιακές τους λειτουργίες στην περίπτωση που η εγκατάσταση του παρόχου καταρρεύσει. Τέλος, τα δεδομένα θα πρέπει να ελέγχονται και να ασφαλίζονται διότι υπάρχει κίνδυνος έκθεσής τους (από το τρίτο μέρος ή/και από άλλους πελάτες του νέφους), πράγμα το οποίο μπορεί να μην είναι πάντοτε εύκολο ή εφικτό.

2.3.2 *Ιδιωτικό νέφος (Private cloud)*

Το ιδιωτικό νέφος είναι ένα περιβάλλον νέφους το οποίο το διαχειρίζεται είτε το προσωπικό της επιχείρησης που το χρησιμοποιεί είτε μια τρίτη οντότητα. Ουσιαστικά η επιχείρηση έχει διπλό ρόλο, λειτουργεί και σαν πάροχος και σαν καταναλωτής νέφους, δηλαδή πρώτα δημιουργεί και στη συνέχεια καταναλώνει το νέφος της. Χαρακτηριστικά αυτού του μοντέλου είναι ότι ανήκει μόνο σε μια επιχείρηση και το μικρό μέγεθος εφόσον καλύπτει μόνο μία επιχείρηση. Τέλος, η δυνατότητα του πλήρους ελέγχου ώστε να αντιμετωπιστούν ζητήματα που προκύπτουν στα υπόλοιπα, λιγότερο ελεγχόμενα μοντέλα. [3]

Τα πλεονεκτήματα του ιδιωτικού νέφους είναι το επίπεδο ασφάλειας που προσφέρει καθώς η πιθανότητα απειλής και κλοπής/διαρροής δεδομένων είναι μικρότερη σε σχέση με τα υπόλοιπα είδη νέφους [3]. Επιπλέον, η επιχείρηση μπορεί να λειτουργεί αυτόνομα χωρίς να εξαρτάται από κάποιον πάροχο και από ενδεχόμενες βλάβες και γενικότερα αστοχίες για τις οποίες δεν φέρει την παραμικρή ευθύνη. Τέλος, έχει τον πλήρη έλεγχο του νέφους της και λειτουργεί αυτοβούλως, για παράδειγμα εφαρμόζοντας δικές της πολιτικές ασφαλείας [3].

Τα μειονεκτήματα του ιδιωτικού νέφους είναι το γεγονός πως απαιτείται ένα οικονομικό κεφάλαιο για αγορά εξοπλισμού και στη συνέχεια απαιτείται ανθρώπινο δυναμικό για την διαχείριση και τη συντήρηση του νέφους [3]. Θα λέγαμε, λοιπόν, ότι εν μέρη χάνεται ένα μεγάλο πλεονέκτημα του νέφους, το οποίο είναι η απαλλαγή από το αρχικό κόστος επένδυσης και το λειτουργικό κόστος. Επίσης, εφόσον μία επιχείρηση λειτουργεί και σαν πάροχος και σαν καταναλωτής νέφους πολλές φορές δεν τηρούνται απόλυτα οι συμφωνίες σε επίπεδο υπηρεσίας (SLAs) [3]. Τέλος, ίσως και η ύπαρξη τρίτου μέρους που να λειτουργεί εκ μέρους του παρόχου του ιδιωτικού νέφους να οδηγεί σε μειονεκτήματα, όπως για παράδειγμα να μην γίνεται σωστή διαχείριση του νέφους ή να δημιουργηθούν θέματα ασφαλείας (ειδικότερα δεδομένων).

2.3.3 Υβριδικό νέφος (Hybrid cloud)

Το υβριδικό νέφος αποτελεί μία σύνθεση από διαφορετικά μοντέλα διάταξης νεφών (ιδιωτικό, δημόσιο, κοινοτικό) όπου τα νέφη αυτά αποτελούν ξεχωριστές οντότητες που συνεργάζονται μεταξύ τους με τέτοιο τρόπο ώστε να επιτυγχάνεται η φορητότητα δεδομένων και εφαρμογών. Ένα παράδειγμα υβριδικού νέφους είναι η προσθήκη πόρων από δημόσιο νέφος σε μία εγκατάσταση ιδιωτικού νέφους [3]. Σε αυτή την περίπτωση συνδυάζονται πλεονεκτήματα και των δύο μοντέλων, όπως η ασφάλεια από την πλευρά του ιδιωτικού νέφους και η κλιμάκωση από την πλευρά του δημοσίου. Βέβαια, όπως αντλούνται πλεονεκτήματα από τον συνδυασμό μοντέλων, αντίστοιχα αντλούνται και μειονεκτήματα, όπως η μειωμένη ασφάλεια από το δημόσιο νέφος και τα χαλαρά SLAs από το ιδιωτικό νέφος.

Τα πλεονεκτήματα του υβριδικού νέφους είναι ότι υπάρχει αυξημένη ασφάλεια σε σχέση με το δημόσιο νέφος διότι μπορεί να περιλαμβάνεται και το ιδιωτικό νέφος. Επιπλέον, λόγω του δημοσίου νέφους υπάρχει δυνατότητα κλιμάκωσης [3], κάτι το οποίο είναι πολύ σημαντικό καθώς οι απαιτήσεις σε πόρους μπορεί να αλλάξουν από μέρα σε μέρα (ή από ώρα σε ώρα) και η αντίδραση από την πλευρά της επιχείρησης θα πρέπει να είναι άμεση. Ένα ακόμα πλεονέκτημα είναι πως υπάρχουν αυστηρές συμφωνίες σε επίπεδο υπηρεσίας (SLAs) ανάμεσα στους κατόχους ιδιωτικού νέφους και στους παρόχους δημοσίου νέφους ώστε να διατηρείται ένα υψηλό επίπεδο παροχής υπηρεσιών [3]. Τέλος, το υβριδικό νέφος έχει την δυνατότητα να συνδυάζει στοιχεία από όλα τα μοντέλα νέφους που το συνθέτουν ώστε να επιτυγχάνεται το βέλτιστο αποτέλεσμα.

Τα μειονεκτήματα του υβριδικού νέφους είναι η λιγότερη ασφάλεια σε σχέση με το ιδιωτικό νέφος διότι (μπορεί να) συμμετέχει και το δημόσιο νέφος. Επίσης, η διαχείριση του είναι πολύπλοκη και δύσκολη

καθώς μπορεί να υπάρχει ανομοιομορφία ανάμεσα στα μοντέλα νέφους που θα συνδυαστούν [3]. Η διαχείριση, εκτός από πολυπλοκότητα και δυσκολία, προσθέτει και το μειονέκτημα του επιπλέον κόστους διότι μία επιχείρηση που έχει υιοθετήσει το υβριδικό μοντέλο είναι υπεύθυνη να συντηρεί και το ιδιωτικό νέφος της. Εξαίρεση αποτελεί η περίπτωση κατά την οποία το υβριδικό νέφος το διαχειρίζεται ένας ξεχωριστός πάροχος. Σε αυτή την περίπτωση δεν υπάρχει επιπλέον διαχειριστικό φορτίο για τους παρόχους των συντιθέμενων νεφών. Τέλος ένα μειονέκτημα είναι τα πιθανά ζητήματα απόδοσης που μπορεί να προκύψουν διότι για να συνδυαστούν και να λειτουργήσουν πολλά νέφη μαζί εμπλέκεται το διαδίκτυο [3].

2.3.4 Κοινοτικό νέφος (Community cloud)

Το κοινοτικό νέφος μοιάζει με το ιδιωτικό νέφος αλλά η διαφορά τους είναι πως στο κοινοτικό νέφος έχει πρόσβαση μόνο μια συγκεκριμένη κοινότητα καταναλωτών (πχ. ένα σύνολο επιχειρήσεων). Αυτό δεν σημαίνει βέβαια πως όλα τα μέλη της κοινότητας έχουν πλήρη δικαιώματα πρόσβασης και ελέγχου όλων των πόρων. Η κοινότητα αυτή είναι υπεύθυνη για να την ανάπτυξη του νέφους και το νέφος μπορεί να ανήκει είτε στην κοινότητα είτε σε μία τρίτη οντότητα. [3]

Τα πλεονεκτήματα του κοινοτικού νέφους [3] είναι η φιλοσοφία της κατανεμημένης λειτουργίας. Επιπλέον, οι διαδικασίες πραγματοποιούνται συνεργατικά από τα μέλη της κοινότητας και οι ευθύνες μοιράζονται. Τέλος, το κόστος είναι μειωμένο για τον κάθε συμμετέχοντα στην κοινότητα διότι διαμοιράζεται. Επίσης, υπάρχει παραπάνω ασφάλεια σε σχέση με το δημόσιο νέφος καθώς εδώ οι απειλές συνήθως προέρχονται από το εσωτερικό της κοινότητας.

Τα μειονεκτήματα του κοινοτικού νέφους [3] είναι η περιορισμένη αυτονομία διότι μία επιχείρηση που έχει υιοθετήσει αυτό το μοντέλο εξαρτάται και από τον πάροχο νέφους στην περίπτωση που ανήκει σε μία τρίτη οντότητα αλλά και από τα υπόλοιπα μέλη της κοινότητας. Βλέπουμε λοιπόν ότι το χαρακτηριστικό της αυτονομίας αποδυναμώνεται σε μεγάλο βαθμό. Επιπλέον, η ασφάλεια του κοινοτικού νέφους είναι μικρότερη σε σχέση με την ασφάλεια που παρέχει το ιδιωτικό νέφος.

3 Ασφάλεια ΠΣ

3.1 Ορισμός

Κάθε φορά που ένας οργανισμός, μια επιχείρηση ή ένα σύνολο ανθρώπων, κάνει χρήση του διαδικτύου μεταφέρει και αποθηκεύει δεδομένα και πληροφορίες ή ακόμα και λογισμικό. Οι πληροφορίες και τα δεδομένα γίνονται όλο και πιο πολύτιμα τα τελευταία χρόνια καθώς μετά από την απαραίτητη επεξεργασία μπορούν να χρησιμοποιηθούν σε πολλούς τομείς της επιστήμης, όπως η ιατρική, η πολιτική, και η οικονομία ώστε να εξάγουν συμπεράσματα, να προβλέψουν καταστάσεις και να βοηθήσουν στην λήψη αποφάσεων. Χαρακτηριστική είναι η φράση του πρωθυπουργού της Ινδίας Narendra Modi “Data is the new gold” [5]**.** Επομένως, γίνεται ολοένα και πιο έντονη η ανάγκη να τα προστατεύσουμε.

Η ασφάλεια πληροφοριακών συστημάτων [6] που συνήθως αναφέρεται ως INFOSEC αναφέρεται στις διαδικασίες και τις μεθοδολογίες που εμπλέκονται στη διατήρηση της εμπιστευτικότητας των πληροφοριών, στη διαθεσιμότητα και στη διασφάλιση της ακεραιότητάς τους. Αναφέρεται επίσης σε ελέγχους πρόσβασης, οι οποίοι έχουν σαν στόχο να εμποδίσουν τους μη εξουσιοδοτημένους χρήστες να εισέλθουν ή να έχουν πρόσβαση σε ένα σύστημα και στην προστασία των πληροφοριών ανεξάρτητα από την τοποθεσία δηλαδή από το αν βρίσκονται αποθηκευμένες, επεξεργάζονται ή μετακινούνται. Τέλος αναφέρεται στον εντοπισμό, στην αποκατάσταση και την καταγραφή παραβιάσεων ασφαλείας.

Θα μπορούσαμε να πούμε ότι υπάρχουν τέσσερις βασικοί στόχοι που σχετίζονται με τις ευαίσθητες πληροφορίες:

- Διατήρηση της εμπιστευτικότητας (confidentiality)
- Διατήρηση της ακεραιότητας (integrity)
- Διατήρηση της διαθεσιμότητάς (availability)
- Μη αποποίηση (non-repudiation)

Προσπαθώντας να δούμε την ασφάλεια από μία πιο πρακτική σκοπιά θα λέγαμε ότι πρόκειται για ένα σύνολο διαδικασιών αποτελούμενο από τρία στάδια. Το πρώτο στάδιο είναι η πρόληψη, στη συνέχεια ακολουθεί η ανίχνευση και τέλος η αντίδραση.

- Πρόληψη (prevention): Αποτροπή της κατάληξης μιας απειλής σε παραβίαση [7]**.**

- Ανίχνευση (detection): Διαπίστωση της εμφάνισης μιας παραβίασης [7].
- Αντίδραση (reaction): Εξάλειψη των αρνητικών επιπτώσεων μίας παραβίασης, αποκατάσταση των πόρων που υπέστησαν ζημιά και αντιμετώπιση των επιθέσεων που βρίσκονται σε εξέλιξη

3.2 Ανάλυση βασικών αρχών ασφαλείας

Όπως αναφέρθηκε και στην προηγούμενη ενότητα, οι τρεις θεμελιώδεις έννοιες για την ασφάλεια πληροφοριακών συστημάτων είναι η εμπιστευτικότητα (confidentiality), η ακεραιότητα (integrity) και η διαθεσιμότητα (availability).

Εμπιστευτικότητα (confidentiality): διασφαλίζει ότι η πρόσβαση σε ευαίσθητες πληροφορίες γίνεται μόνο από εξουσιοδοτημένα άτομα [8]. Δεν αφορά μόνο την προστασία απέναντι στην μη εξουσιοδοτημένη τροποποίηση δεδομένων, αλλά και στην απλή ανάγνωση. Η εμπιστευτικότητα εφαρμόζεται χρησιμοποιώντας μηχανισμούς ασφαλείας, τους ταυτοποίηση των χρηστών και κρυπτογράφηση [8].

Διαθεσιμότητα (availability): διασφαλίζει ότι οι πληροφορίες και εν γένει οι πόρους ενός δικτύου υπολογιστών είναι διαθέσιμοι όταν τους χρειάζεται κάποιος εξουσιοδοτημένος χρήστης. Μια πολύ συνηθισμένη απειλή, η οποία οδηγεί σε απώλεια διαθεσιμότητας, είναι οι επιθέσεις άρνησης υπηρεσίας (DoS attack) [8] όπου ο εξυπηρετητής (server) ενός συστήματος κατακλύζεται από ψευδή αιτήματα. Αυτό έχει ως αποτέλεσμα πως ο εξυπηρετητής δεν μπορεί πια να ανταπεξέλθει στα (νόμιμα) αιτήματα των εξουσιοδοτημένων χρηστών.

Ακεραιότητα (integrity): Πρόκειται για την επιβεβαίωση ότι τα απεσταλμένα δεδομένα έχουν παραληφθεί από τον παραλήπτη χωρίς κάποια τροποποίηση, πχ. από έναν ενδιάμεσο. Τα δεδομένα, είτε είναι αποθηκευμένα είτε μεταφέρονται, θα πρέπει να μπορούν να εγγραφούν, να διαγραφούν ή να μετατραπούν μόνο από εξουσιοδοτημένα άτομα. Η ακεραιότητα υλοποιείται χρησιμοποιώντας μηχανισμούς ασφάλειας, όπως η κρυπτογράφηση δεδομένων (encryption) και ο κατακερματισμός (hashing). [8]

Ένα παράδειγμα, το οποίο αντικατοπτρίζει πλήρως πως συνδέονται και πως εφαρμόζονται αυτές οι τρεις έννοιες, είναι η εφαρμογή των παραπάνω στα ATM (Automated Teller Machine) [9].

Υπάρχει εμπιστευτικότητα καθώς απαιτείται να εισαχθεί η κάρτα, δηλαδή να υπάρχει φυσική παρουσία του χρηστή και ταυτοποίηση με κωδικό πρόσβασης (PIN). Επιπλέον, τα δεδομένα που μεταφέρονται εντός του δικτύου είναι κρυπτογραφημένα.

Υπάρχει ακεραιότητα καθώς όλα τα δεδομένα κρυπτογραφούνται με εξαιρετικά ασφαλείς αλγορίθμους ώστε να αποκτούν μη κατανοητή μορφή και έτσι να μη μπορεί να τα κατανοήσει κάποιος ενδιάμεσος περί τίνος πρόκειται. Βέβαια, ένας ενδιάμεσος μπορεί να τα τροποποιήσει, αλλά αυτό είναι κάτι που αντιμετωπίζεται στην ιδιότητα/στόχο της μη αποποίησης .

Υπάρχει διαθεσιμότητα καθώς το ATM βρίσκεται σε δημόσιες τοποθεσίες και είναι διαθέσιμο καθ' όλη τη διάρκεια του εικοσιτετράωρου, ακόμα και όταν το κατάστημα της τράπεζας είναι κλειστό. Τέλος, ανεξάρτητα από το είδος της συναλλαγής που πραγματοποιείται, ο χρόνος απόκρισης είναι πολύ μικρός και παραμένει λίγο πολύ σταθερός. Βέβαια η διαθεσιμότητα μπορεί να επηρεαστεί από εξωτερικούς παράγοντες, όπως προβλήματα δικτύου στην ευρύτερη περιοχή ή ανάγκη για συντήρηση μετά από κάποιου είδους καταστροφή (όπως μια πλημμύρα ή πυρκαγιά).

Μη αποποίηση (non repudiation): διασφαλίζει ότι μία οντότητα δεν μπορεί να αρνηθεί το γεγονός πως πραγματοποίησε μια ενέργεια, όπως για παράδειγμα αποστολή ενός μηνύματος όταν πρόκειται για τον αποστολέα, και ότι παρέλαβε κάποια δεδομένα όταν πρόκειται για τον παραλήπτη. Ένας μηχανισμός με τον οποίο εξασφαλίζεται η μη αποποίηση είναι η χρήση ψηφιακών υπογραφών. [10]

3.3 Ασφάλεια στο Υπολογιστικό Νέφος

3.3.1 Εισαγωγή

Η ασφάλεια στα πληροφοριακά συστήματα ένα ζήτημα μείζονος σημασίας για τους χρήστες αλλά και για τους παρόχους, οι οποίοι καλούνται να αντιμετωπίσουν τις σχετικές προκλήσεις ασφάλειας. Παρακάτω θα δούμε ορισμένους λόγους για τους οποίους η χρήση υπηρεσιών στο υπολογιστικό νέφος είναι πιο ασφαλής από ένα παραδοσιακό επιτόπιο περιβάλλον για επιχειρήσεις και οργανισμούς.

3.3.2 Σύγκριση μεταξύ υπηρεσιών στο νέφος και σε επιτόπιο περιβάλλον

Εμπειρία σε τεχνικά ζητήματα

Εάν μία εταιρία ή ένας οργανισμός δεν ασχολείται ήδη με την ασφάλεια πληροφοριακών συστημάτων αφιερώνεται πολύτιμος χρόνος και χρήματα ώστε να εξασφαλιστούν τα ελάχιστα επίπεδα ασφαλείας που απαιτούνται. Οι περισσότεροι οργανισμοί πιθανότατα να μη διαθέτουν μια έμπειρη και σωστά καταρτισμένη ομάδα πάνω σε ζητήματα ασφάλειας ώστε να προστατέψουν τα δεδομένα τους. [11]

Από την άλλη πλευρά, οι πάροχοι υπολογιστικού νέφους έχουν σαν πρωταρχικό στόχο να παρέχουν στους πελάτες τους αποθηκευτικό χώρο και όλες τις απαραίτητες υπηρεσίες που χρειάζονται. Το κέρδος

αλλά και η φήμη ενός παρόχου συνδέεται σε τεράστιο βαθμό με τη δυνατότητα του να διασφαλίσει την ασφάλεια των δεδομένων των πελατών του. Οι πάροχοι, λοιπόν, μπορούν να απασχολήσουν άρτια καταρτισμένους επαγγελματίες ασφάλειας ώστε να πετύχουν τον μέγιστο βαθμό προστασίας των δεδομένων. [11]

Φυσική πρόσβαση

Τα δεδομένα στο νέφος αποθηκεύονται σε έναν διακομιστή που βρίσκεται σε φυσική παρουσία οπουδήποτε στον κόσμο, καθιστώντας μια φυσική επίθεση πολύ λιγότερο πιθανή σε σύγκριση με μία επιτόπια εγκατάσταση. Αυτό συμβαίνει διότι το να βρίσκεται κάποιος άνθρωπος, δυνητικά επιτιθέμενος, πολύ κοντά σε ένα υπολογιστικό σύστημα καθιστά πολύ πιο εύκολη της εκκίνηση μιας σχετικής επίθεσης. Επιπλέον, ακόμα και αν συμβεί επίθεση δεν θα διαρρεύσει το σύνολο των δεδομένων ενός χρήστη διότι σε πολλές περιπτώσεις γίνεται κατακερματισμός, έτσι ώστε ακόμη και αν υπάρχουν δεδομένα σε έναν εκτιθέμενο διακομιστή, αυτά θα αποτελούν ένα πολύ μικρό ποσοστό σε σχέση με αυτά που έχει αποθηκεύσει ο χρήστης στο νέφος και άρα η διαρροή θα είναι μικρή. Επίσης, οι πάροχοι προστατεύουν το χώρο στον οποίο βρίσκονται αυτοί οι εξυπηρετητές με αντικλεπτικά μέσα, όπως φράχτες ή κάμερες ασφαλείας. Γίνεται, λοιπόν, φανερό ότι το υπολογιστικό νέφος αποτελεί μια πολύ πιο ασφαλή λύση σχετικά με τα ζητήματα ασφάλειας που αφορούν την φυσική πρόσβαση. [11]

Ανεξάρτητα από το είδος της υποδομής η σημαντικότερη προϋπόθεση για ένα υψηλό επίπεδο ασφαλείας σε έναν οργανισμό είναι η εκπαίδευση του προσωπικού ώστε να αποφευχθούν φαινόμενα όπως το ηλεκτρονικό ψάρεμα (phishing) και να επιτευχθεί η προστασία από εσωτερικές επιθέσεις. [11]

Λιγότερες ευπάθειες

Όσον αφορά την προστασία των δεδομένων, η φυσική τοποθεσία έχει πολύ λιγότερη σημασία από τα μέσα πρόσβασης. Αυτό σημαίνει ότι ο κύριος στόχος των επιτιθέμενων είναι να εντοπίσουν και να αξιοποιήσουν τις υπάρχουσες ευπάθειες. Ένα παράδειγμα είναι η αποστολή μηνυμάτων ηλεκτρονικού ψαρέματος (phishing emails). [11]

Οι επιτιθέμενοι έχουν πολλούς διαφορετικούς τρόπους αξιοποίησης αυτών των ευπαθειών σε συστήματα εσωτερικής εγκατάστασης, οι οποίοι επιδιώκουν τη συλλογή κωδικών πρόσβασης και άλλων ευαίσθητων στοιχείων. Οι πάροχοι νέφους σίγουρα μπορούν να ανταπεξέλθουν σε αυτή την κατάσταση και να διορθώσουν πιθανά κενά ασφαλείας πολύ πιο γρήγορα και αποτελεσματικά σε σχέση με κάποιον απλό χρήστη ή οργανισμό διότι όπως αναφέρθηκε παραπάνω το προσωπικό που απασχολείται είναι έμπειροι επαγγελματίες με τα κατάλληλα εργαλεία στη διάθεσή τους ανά πάσα στιγμή. Επίσης, εκτός από το άρτια καταρτισμένο και έμπειρο προσωπικό, τα νέφη εφαρμόζουν καλές πρακτικές ασφάλειας και τα κατάλληλα μέτρα ασφάλειας ενώ κάνουν συχνά δοκιμές ασφάλειας και διείσδυσης. Συνεπώς, μπορεί να έχουν ένα πολύ καλύτερο επίπεδο ασφάλειας σε σχέση με επιτόπια περιβάλλοντα. [11]

3.3.3 Απειλές στο υπολογιστικό νέφος και τρόποι αντιμετώπισης

Σε υπολογιστές και δίκτυα υπολογιστών, μια επίθεση ορίζεται ως κάθε προσπάθεια έκθεσης, αλλαγής, απενεργοποίησης, καταστροφής, κλοπής ή απόκτησης πληροφοριών μέσω μη εξουσιοδοτημένης πρόσβασης ή μη εξουσιοδοτημένης χρήσης ενός υπολογιστικού πόρου. Μια επίθεση μπορεί να ξεκινήσει από οπουδήποτε από οποιοδήποτε άτομο ή ομάδα χρησιμοποιώντας μία ή περισσότερες στρατηγικές επίθεσης και να κλέψει, να τροποποιήσει, να καταστρέψει ή εν γένει να εκθέσει έναν καθορισμένο στόχο σε ένα πληροφοριακό σύστημα [12]. Οι επιθέσεις που μπορεί να γίνουν στο νέφος μπορεί να είναι είτε κλασικές είτε εξειδικευμένες στο νέφος και ειδικότερα σε ευπάθειες που αφορούν την εικονικοποίηση (virtualization).

3.3.3.1 Κλασσικές απειλές

Επιθέσεις άρνησης υπηρεσίας (Denial of Service - DoS)

Στην επίθεση άρνησης υπηρεσίας, ένας εισβολέας υπερφορτώνει το σύστημα με αιτήματα υπηρεσίας, ώστε αυτό να σταματήσει να ανταποκρίνεται σε νέα αιτήματα από νόμιμους/εξουσιοδοτημένους χρήστες. Μια παραλλαγή της είναι η κατανεμημένη επίθεση άρνησης υπηρεσίας (Distributed DoS - DDoS), η οποία είναι πιο δύσκολο να αντιμετωπιστεί καθώς υπάρχει μεγάλος αριθμός συσκευών μέσα από τις οποίες πραγματοποιείται η επίθεση [13].

Οι κατανεμημένες επιθέσεις άρνησης εξυπηρέτησης σε επίπεδο δικτύου στέλνουν τεράστιο όγκο πακέτων στο δίκτυο με στόχο να εξαντλήσουν το διαθέσιμο εύρος ζώνης ώστε να δημιουργηθεί ένα είδος συμφόρησης στο δίκτυο και παράλληλα να υπερφορτωθεί ο στόχος (target) (πχ. ένας εξυπηρετητής) καθώς και να διακοπεί η παροχή υπηρεσιών προς τους εξουσιοδοτημένους χρήστες [13]. Για να αντιμετωπιστεί αυτό το είδος το επιθέσεων και να περιοριστούν όσο το δυνατόν περισσότερο οι συνέπειες αρχικά θα πρέπει να υπάρχει πρόληψη. Η πρόληψη, όμως, δε μπορεί να εγγυηθεί πως δεν θα συμβεί ποτέ καμία επίθεση άρα είναι απαραίτητο εκτός από την πρόληψη να υπάρχουν και τεχνικές ανίχνευσης και αντιμετώπισης των επιθέσεων αυτών.

Το τείχος προστασίας (firewall) μπορεί να χρησιμοποιηθεί για να επιτρέψει ή να αρνηθεί τη μεταφορά πακέτων στο δίκτυο με βάση πρωτόκολλα πρόσβασης, θύρες ή διευθύνσεις IP. Οι μεταγωγείς (switches) έχουν δυνατότητα άρνησης εξυπηρέτησης ορισμένων αιτημάτων αν δεχτούν πολλά αιτήματα από μία συγκεκριμένη διεύθυνση IP σε μικρό χρονικό διάστημα (rate limiting) ενώ τα φιλτράρουν βάσει λίστας ελέγχου πρόσβασης (Access Control List), η οποία καθορίζει με ακρίβεια ποιος μπορεί να εκτελέσει κάποια εργασία πάνω σε ένα αντικείμενο και τι είδους εργασία θα είναι αυτή [13]. Ένα ακόμα σημαντικό εργαλείο για την αντιμετώπιση αυτών των επιθέσεων είναι το σύστημα ανίχνευσης και αποτροπής εισβολών (Intrusion Detection and Prevention System). Το σύστημα ανίχνευσης εισβολών

χρησιμοποιείται για να εντοπίσει τυχόν απειλές αναλύοντας την κίνηση του δικτύου (ή ενός μηχανήματος) και δεδομένα από τις συσκευές ενώ το σύστημα αποτροπής εισβολών για να αντιμετωπίσει τις απειλές αυτές μπλοκάροντας την κίνηση στο δίκτυο και απομονώνοντας τις.

Επιθέσεις ελέγχου ταυτότητας

Ο έλεγχος ταυτότητας είναι ένα τρωτό σημείο στο υπολογιστικό νέφος καθώς εξαρτάται από τον βαθμό καταλληλότητας των (απλών) διαπιστευτηρίων (όνομα χρήστη και κωδικός πρόσβασης) των χρηστών του.

Ορισμένες επιθέσεις ελέγχου ταυτότητας είναι οι εξής:

- Καταγραφείς πληκτρολόγησης (key loggers): Είναι προγράμματα τα οποία έχουν εγχυθεί σε ένα μηχάνημα και παρακολουθούν τις δραστηριότητες των χρηστών καταγράφοντας κάθε πλήκτρο που πατήθηκε από τον χρήστη. Έπειτα, το αρχείο καταγραφής στέλνεται στον επιτιθέμενο και αυτός με τη σειρά του εντοπίζει ευαίσθητα δεδομένα όπως κωδικούς πρόσβασης.
- Επιθέσεις ωμής βίας (brute force attacks): Σε αυτό το είδος επίθεσης δοκιμάζονται όλοι οι πιθανοί συνδυασμοί με γράμματα, σύμβολα και αριθμούς για να σπάσουν τον κωδικό πρόσβασης ενός χρήστη. Η επίθεση brute force εφαρμόζεται γενικά για να σπάσει τους κωδικούς πρόσβασης αλλά είναι πολύ χρονοβόρα ενώ αντιμετωπίζεται πολύ εύκολα [14].
- Επιθέσεις λεξικού (dictionary attacks): Αυτός ο τύπος επίθεσης είναι σχετικά γρηγορότερος από την επίθεση brute force διότι χρησιμοποιεί έναν κατάλογο από λέξεις, ο οποίος θα πρέπει να έχει καταρτισθεί εκ των προτέρων, σαν πιθανούς κωδικούς πρόσβασης [15].
- Επιθέσεις ηλεκτρονικού ψαρέματος (phishing): Είναι μια επίθεση κατά την οποία ο επιτιθέμενος προσποιείται μια έμπιστη οντότητα, συνήθως στέλνοντας κάποιο αληθοφανές μήνυμα ηλεκτρονικού ταχυδρομείου (δόλωμα), με σκοπό να εξαπατήσει το θύμα και να αποκτήσει προσωπικά του στοιχεία (πχ. κωδικούς πρόσβασης). Υπάρχουν διάφορα είδη ηλεκτρονικού ψαρέματος όπως: (α) το ηλεκτρονικό ψάρεμα ψαροντούφεκου (spear phishing) όπου ο επιτιθέμενος στοχεύει σε ένα συγκεκριμένο πρόσωπο και χρησιμοποιεί προσωπικά στοιχεία του ώστε το μήνυμα να φαίνεται όσο το δυνατόν πιο πειστικό, (β) το ηλεκτρονικό ψάρεμα φαλαινοθηρίας (whaling) όπου ο στόχος είναι κάποιο υψηλόβαθμο πρόσωπο, (γ) το ηλεκτρονικό ψάρεμα κλώνου (clone phishing) όπου ο επιτιθέμενος αντιγράφει (κλωνοποιεί) ένα μήνυμα που ήδη έχει σταλεί στο θύμα και περιέχει ένα συνημμένο αρχείο ή έναν σύνδεσμο, αντικαθιστά το αρχείο ή τον σύνδεσμο με δικό του (κακόβουλο) και στέλνει ξανά το μήνυμα στο θύμα σαν μια νέα έκδοση και (δ) το ηλεκτρονικό ψάρεμα γατόψαρου (catphising) όπου ο επιτιθέμενος δημιουργεί ένα ψεύτικο προφίλ σε διαδικτυακούς χώρους συνομιλίας και επιδιώκει την τακτική επικοινωνία με το θύμα ώστε να δημιουργήσει μια σχέση οικειότητας και εμπιστοσύνης και έτσι να μάθει προσωπικές πληροφορίες για αυτό ώστε να αποκτήσει κάποιο οικονομικό όφελος. [16]

Τρόποι αντιμετώπισης

Καθυστέρηση απάντησης: Ο εξυπηρετητής καθυστερεί να εμφανίσει μήνυμα επιβεβαίωσης για την εγκυρότητα ενός συνδυασμού ονόματος χρήστη (username) και κωδικού (password). Με αυτό τον τρόπο μειώνονται οι προσπάθειες που μπορεί να κάνει ο επιτιθέμενος σε ένα συγκεκριμένο χρονικό διάστημα.

Κλείδωμα λογαριασμού: Οι λογαριασμοί κλειδώνονται μετά από μερικές ανεπιτυχείς προσπάθειες σύνδεσης. Όπως και το προηγούμενο μέτρο, αυτό το μέτρο έχει σχεδιαστεί για να εμποδίζει τους εισβολείς να εξετάζουν πολλούς κωδικούς πρόσβασης σε μικρό χρονικό διάστημα.

Ταυτοποίηση πολλαπλών παραγόντων: Πρόκειται για έναν μηχανισμό ο οποίος συνδυάζει δύο ή περισσότερα στοιχεία για να επαληθεύσει την ταυτότητα ενός χρήστη. Το πιο κλασικό παράδειγμα είναι αυτό της τραπεζικής συναλλαγής μέσω e-banking. Ο χρήστης προσπαθεί να μπει στην εφαρμογή μέσω υπολογιστή ή laptop. Εφόσον το κατορθώσει, τότε θα πρέπει να δώσει τον κωδικό OTP για την ολοκλήρωση των συναλλαγών, ο οποίος αποστέλλεται σε μια ξεχωριστή συσκευή (το κινητό) σε σχέση με την τρέχουσα. Έτσι έχουν χρησιμοποιηθεί δύο παράγοντες ταυτοποίησης και όχι ένας. [17]

Επιβολή χρήσης ισχυρών κωδικών: Η χρήση ενός ισχυρού κωδικού πρόσβασης μπορεί να κάνει πολύ δύσκολη ή ακόμα και να αποτρέψει μια επίθεση. Οι κωδικοί πρόσβασης που μπορούν να εισάγουν οι χρήστες θα πρέπει να έχουν κάποιο ελάχιστο μήκος και να περιλαμβάνουν υποχρεωτικά κάποιους ειδικούς χαρακτήρες (!, ", #, $, %, &, ', (,), *, +). Επιπλέον, θα πρέπει και να μην περιλαμβάνουν αναγνωριστικά στοιχεία, όπως το ονοματεπώνυμο ενός χρήστη, και να αποφεύγονται κάποια μοτίβα, όπως μια λέξη ακολουθούμενη από έναν τετραψήφιο αριθμό. Τέλος, οι κωδικοί θα πρέπει μετά από κάποιο χρονικό διάστημα να αντικαθίστανται από καινούργιους (διαφορετικούς) και καλό θα ήταν να προτείνονται κάποια σύμβολα τα οποία να αντικαθιστούν κάποια γράμματα ώστε να αυξηθεί η πολυπλοκότητα των κωδικών. Αυτό όμως δεν είναι κάτι το οποίο μπορεί να τεθεί σαν υποχρεωτική οδηγία(περιορισμός) προς τους χρήστες. [18]

Επιθέσεις έγχυσης (Injection Attacks)

Οι επιθέσεις έγχυσης είναι μια κατηγορία επιθέσεων όπου ένας εισβολέας στέλνει μη αξιόπιστα δεδομένα σε μια εφαρμογή ώστε να αλλάξει το νόημα των εντολών που αποστέλλονται στον διερμηνέα και έτσι κατά την εκτέλεσή τους να επιτελεστούν μη εξουσιοδοτημένες διαδικασίες. Μια τέτοια επίθεση μπορεί να οδηγήσει σε παραβίαση και απώλεια δεδομένων, άρνηση εξυπηρέτησης και στην χειρότερη περίπτωση έλεγχο ολόκληρου του συστήματος από τον επιτιθέμενο. Παρακάτω παραθέτουμε τα πιο βασικά είδη επιθέσεων έγχυσης.

1. Έγχυση κακόβουλου λογισμικού (Malware injection)

Ως malware ορίζεται το κακόβουλο λογισμικό (malicious software), το οποίο έχει κατασκευαστεί από κάποιον επιτιθέμενο με στόχο να προκαλέσει ζημία σε ένα σύστημα ή να αποκτήσει μη εξουσιοδοτημένη πρόσβαση σε αυτό [19].

Οι βασικότερες κατηγορίες κακόβουλου λογισμικού είναι:

Ιοί (Viruses): Ένας ιός είναι ένα κακόβουλο λογισμικό το οποίο αφού μολύνει έναν υπολογιστή μία φορά έχει τη δυνατότητα να αντιγράψει τον εαυτό του και να μολύνει κι άλλα αρχεία στον ίδιο υπολογιστή ή να μεταφερθεί και να μολύνει κι άλλους υπολογιστές. [19]

Δούρειοι ίπποι (Trojans): Ένας Δούρειος Ίππος δείχνει να είναι ένα νόμιμο λογισμικό, το οποίο όμως περιέχει κακόβουλο κώδικα που έχει σκοπό να ανοίξει πίσω πόρτες για την μη εξουσιοδοτημένη πρόσβαση στον υπολογιστή στον οποίον εγκαθίσταται καθώς και να εκτελέσει διάφορες κακόβουλες ενέργειες. [19]

Σκουλήκια (Worms): Τα σκουλήκια λειτουργούν αυτόνομα δηλαδή δεν χρειάζονται κάποιο αρχείο ή πρόγραμμα ώστε να ενσωματώσουν τον κώδικά τους σε αυτό και μεταδίδονται μέσω του δικτύου μολύνοντας άλλους υπολογιστές που βρίσκονται στο ίδιο δίκτυο. [19]

Διαχειριστικά σύνεργα (Rootkits): Τα διαχειριστικά σύνεργα επιτρέπουν σε μη εξουσιοδοτημένους χρήστες να αποκτήσουν πρόσβαση σε έναν υπολογιστή αλλά και να αποκτήσουν δικαιώματα διαχειριστή (root) ενώ είναι πολύ δύσκολο να εντοπιστούν διότι ανατρέπουν το πρόγραμμα που προσπαθεί να τα ανακαλύψει. [19]

Λυτρισμικό (Ransomware): Το λυτρισμικό έχει σχεδιαστεί για να κρυπτογραφεί και να “κλειδώνει” αρχεία ώστε ο χρήστης (θύμα της επίθεσης) να μη μπορεί να αποκτήσει πρόσβαση σε αυτά έως ότου δώσει ένα χρηματικό ποσό στον επιτιθέμενο. [19]

Κατασκοπευτικό λογισμικό (Spyware): Το κατασκοπευτικό λογισμικό προσπαθεί να κλέψει προσωπικά στοιχεία, όπως τραπεζικά στοιχεία, μηνύματα ηλεκτρονικού ταχυδρομείου και κωδικούς πρόσβασης σε διάφορους λογαριασμούς και να τα στείλει σε τρίτους. [19]

Λογισμικό με διαφημίσεις (Adware): Το λογισμικό με διαφημίσεις εμφανίζει διαφημίσεις και εκτελείται στο παρασκήνιο χωρίς ο χρήστης να το γνωρίζει. Επίσης, συλλέγει δεδομένα, όπως η κίνηση στο διαδίκτυο, για να εμφανίσει πιο εξατομικευμένες διαφημίσεις. [19]

<u>Τρόποι αντιμετώπισης</u>

Το κακόβουλο λογισμικό μπορεί να αντιμετωπιστεί σε πρώτο στάδιο προληπτικά ώστε να μην υπάρξει μόλυνση από τέτοιου είδους λογισμικό και σε δεύτερο στάδιο, εφόσον ένας χρήστης κάνει κάποια λάθος ενέργεια, να αντιμετωπιστεί ανασταλτικά ώστε να περιοριστεί η δράση του.

Στο στάδιο της πρόληψης θα πρέπει να γίνεται συνεχής εκπαίδευσης των χρηστών ώστε να είναι σε θέση να αντιλαμβάνονται πιθανούς κινδύνους και ταυτόχρονα να λειτουργούν με τέτοιο τρόπο ώστε να μην εκτίθενται σε κακόβουλο λογισμικό [19]. Παρακάτω παρουσιάζονται κάποιοι απλοί τρόποι με τους οποίους οι χρήστες μπορούν να προστατευτούν. Θα πρέπει λοιπόν:

- να εγκαθιστούν τις ενημερώσεις των λειτουργικών συστημάτων που χρησιμοποιούν αμέσως μόλις γίνονται διαθέσιμες καθώς μέσω αυτών καλύπτονται πιθανά κενά ασφαλείας του λειτουργικού συστήματος [19].
- να μην εμπιστεύονται και να μην ανοίγουν συνδέσμους και συνημμένα αρχεία ηλεκτρονικού ταχυδρομείου από άγνωστους αποστολείς και γενικότερα να είναι σε θέση να “φιλτράρουν” τα μηνύματα που δέχονται (για την περίπτωση όπου δεν φαίνεται ξεκάθαρα πως η διεύθυνση ενός αποστολέα είναι ύποπτη) [19].
- να κατεβάζουν μόνο νόμιμο λογισμικό και από επίσημες πηγές [19].
- να δημιουργούν τακτικά αντίγραφα ασφαλείας ώστε σε περίπτωση μόλυνσης ενός υπολογιστή όπου θα χρειαστεί να διαγραφούν τα πάντα, να είναι όσο το δυνατόν μικρότερη η απώλεια αρχείων [19].
- όταν σε μία επιχείρηση ή οργανισμό υπάρχουν πολλοί χρήστες καλό θα είναι ο διαχειριστής του συστήματος να είναι ένας και οι υπόλοιποι λογαριασμοί να είναι λογαριασμοί χρηστών με περιορισμένες δυνατότητες (όπως για παράδειγμα αδυναμία εγκατάστασης λογισμικού χωρίς έγκριση από τον διαχειριστή) ώστε να μη δημιουργήσουν κάποιο πρόβλημα άθελα τους λόγω άγνοιας ή εσκεμμένα (πχ. για λόγους εκδίκησης) [19].

Στο στάδιο της αντιμετώπισης θα πρέπει να χρησιμοποιούνται συστήματα εντοπισμού και αποτροπής εισβολών καθώς και τείχη προστασίας, όταν αυτό είναι δυνατόν, ενώ σε επίπεδο προσωπικών υπολογιστών πρέπει να υπάρχουν εγκατεστημένα λογισμικά πρόληψης, εντοπισμού και αφαίρεσης κακόβουλου λογισμικού (anti malware ή antivirus).

2. Έγχυση SQL (SQL Injection)

Πρόκειται για μια τεχνική με την οποία πραγματοποιείται επίθεση σε εφαρμογές που χρησιμοποιούν τη γλώσσα SQL, όπως εφαρμογές ιστού (web applications), όπου το πιο απλό παράδειγμα είναι ένας ιστότοπος που συνδέεται με μία βάση δεδομένων. Όταν ένας χρήστης συμπληρώσει μια φόρμα, πχ. ταυτοποίησης, τότε δημιουργείται ένα ερώτημα (query) προς τη βάση δεδομένων. Ο επιτιθέμενος εισάγει κάποιους χαρακτήρες με τέτοιο τρόπο ώστε να “μπερδέψει” και να εμποδίσει ή να επεκτείνει την προκαθορισμένη λειτουργία του ερωτήματος για να αποκτήσει μη εξουσιοδοτημένη πρόσβαση σε αντίστοιχα αποθηκευμένα δεδομένα.

Για το παραπάνω παράδειγμα της φόρμας ταυτοποίησης με την χρήση ονόματος χρήστη (username) ένα ερώτημα SQL μπορεί να έχει την εξής μορφή:

SELECT * FROM students WHERE username='AAAA' and password='BBBB';

όπου το ΄΄ * ΄΄ συμβολίζει το ΄΄οτιδήποτε΄΄ (δηλ. οποιοδήποτε χαρακτηριστικό ενός φοιτητή) και οι τιμές 'AAAA', 'BBBB' λαμβάνονται από τα πεδία της φόρμας. Αν ο χρήστης στο πεδίο username εισάγει: ' OR 1=1 - - τότε το ερώτημα γίνεται:

SELECT * FROM students WHERE username=' ' OR 1=1 - - and password=' ';

Το τελευταίο ερώτημα θα επιστρέψει οτιδήποτε υπάρχει στον πίνακα students λόγω της χρήσης της διάζευξης με μια συνθήκη που είναι πάντοτε αληθής καθώς και της χρήσης του " - - " που δηλώνει σχόλιο ώστε ο έλεγχος για κωδικό (password) να μην πραγματοποιηθεί.

<u>Τρόποι αντιμετώπισης</u>

- *Χρήση παραμετροποιημένων ερωτημάτων*: Με αυτή την τεχνική για τα ερωτήματα είναι γραμμένος όλος ο κώδικας και το μόνο που απομένει για να εκτελεστούν είναι να καταχωρηθούν τιμές στις παραμέτρους των ερωτημάτων (όπως στην παράμετρο username στο παράδειγμα που αναφέρθηκε παραπάνω), οι οποίες δηλώνονται σαν μεταβλητές και περιμένουν να εκχωρηθεί σε αυτές μία τιμή. Ουσιαστικά έτσι έχει γίνει μια πρώτη μεταγλώττιση και η βάση δεδομένων μπορεί να ξεχωρίσει τον κώδικα από τα δεδομένα που εισάγει ο χρήστης καθώς η είσοδος του χρήστη μπαίνει μέσα σε ' " " ' και δε μπορεί να λειτουργήσει σαν κώδικας που θα δημιουργήσει πρόβλημα. [20]
- *Λίστα επιτρεπόμενης εισόδου (Whitelisting)*: Με αυτή την τεχνική μπορεί να προσδιοριστεί, συνήθως με χρήση κανονικών εκφράσεων, η μορφή που πρέπει να έχουν τα δεδομένα που εισάγει ο χρήστης σε κάθε πεδίο για να θεωρηθούν ασφαλή. Για παράδειγμα, μία φόρμα το πεδίο ονοματεπωνύμου πρέπει να περιέχει μόνο γράμματα ή το πεδίο email τον χαρακτήρα '@'. Έτσι φιλτράρεται το τι ακριβώς θα εισέλθει στη βάση και όταν εντοπιστεί κάποια ύποπτη είσοδος απορρίπτεται. [20]
- *Λίστα μη επιτρεπόμενης εισόδου (Blacklisting)*: Αυτή η τεχνική έρχεται να συμπληρώσει την προηγούμενη και αντίστοιχα εδώ υπάρχει ένας κατάλογος με εντολές ή σύμβολα τα οποία δεν επιτρέπεται να χρησιμοποιηθούν. Για παράδειγμα, δεν μπορεί ένας χρήστης σε μία φόρμα να χρησιμοποιήσει την εντολή 'DELETE' ή σύμβολα όπως ' */ '. [20]
- *Διαφυγή της εισόδου του χρήστη (Escaping user input)*: Σε αυτή την τεχνική χρησιμοποιούνται κάποιες συναρτήσεις διαφορετικές για κάθε βάση δεδομένων ώστε να αντικατασταθούν στην είσοδο του χρήστη πιθανοί χαρακτήρες που έχουν ειδική σημασία, με άλλους κατάλληλους, οι οποίοι δεν θα δημιουργούσαν πρόβλημα κατά την εκτέλεση των ερωτημάτων. Για παράδειγμα

ο χαρακτήρας " ' " (μονό εισαγωγικό) μπορεί να αντικατασταθεί από τον χαρακτήρα " '' " (διπλό εισαγωγικό). [20]

3. Δέσμη ενεργειών μεταξύ ιστότοπων (Cross-site Scripting ή XSS)

Πρόκειται για μια τεχνική, η οποία εισάγει κακόβουλο κώδικα, κυρίως σε γλώσσα JavaScript σε ιστοσελίδες. Ο κώδικας αυτός εκτελείται μέσα από τον περιηγητή του χρήστη και ο περιηγητής δεν μπορεί να εντοπίσει ότι πρόκειται για κακόβουλη ενέργεια. Εφαρμόζεται σε περιπτώσεις όπου ο χρήστης έχει εισάγει τα διαπιστευτήριά του, όπως σε φόρμες εισόδου κοινωνικών δικτύων ή φόρουμ, και ο επιτιθέμενος μπορεί να αποκτήσει πρόσβαση σε cookies ή άλλες ευαίσθητες πληροφορίες. Υπάρχουν τρεις βασικές κατηγορίες για αυτό το είδος των επιθέσεων: 1) οι μόνιμες επιθέσεις, 2) οι μη μόνιμες επιθέσεις και 3) οι επιθέσεις βασισμένες στο DOM (μοντέλο αντικειμένου εγγράφου της γλώσσας HTML). [21]

Μόνιμη επίθεση (Stored XSS)

Πρόκειται για ένα είδος επίθεσης, το οποίο πραγματοποιείται όταν η είσοδος (user input) του επιτιθέμενου αποθηκεύεται στους διακομιστές που φιλοξενούν την ιστοσελίδα μέσα στην οποία ο επιτιθέμενος πραγματοποίησε τις ενέργειες του. Μία τέτοια περίπτωση θα μπορούσε να είναι ένα φόρουμ όπου εκεί ένα μήνυμα το οποίο δημοσιεύει ο επιτιθέμενος και περιέχει κακόβουλο κώδικα αποθηκεύεται στους διακομιστές του φόρουμ. Αυτό το μήνυμα στη συνέχεια θα είναι ορατό στους χρήστες, οι οποίοι θα διαβάζουν τη συζήτηση που περιέχει και ο αντίστοιχος κώδικας θα εκτελείται στους φυλλομετρητές τους. [21]

Μη μόνιμη επίθεση (Reflected XSS)

Πρόκειται για ένα είδος επίθεσης που συμβαίνει όταν η είσοδος του χρήστη αποστέλλεται κατευθείαν στον εξυπηρετητή χωρίς πρώτα να ελεγχθεί. Ένα τέτοιο παράδειγμα συμβαίνει όταν ένας χρήστης συμπληρώνει πεδία κειμένων σε ιστοσελίδες. Ο επιτιθέμενος εκμεταλλεύεται αυτή την ευπάθεια και εισάγει κακόβουλο κώδικα σε μία μπάρα αναζήτησης ή στα πεδία εισαγωγής φίλτρων αναζήτησης σε μία ιστοσελίδα. Όταν κάνει την αναζήτηση, δημιουργείται ένας νέος σύνδεσμος (URL) τον οποίο μπορεί να κοινοποιήσει στο υποψήφιο θύμα του. Όταν το θύμα ανοίξει αυτόν τον σύνδεσμο θα εκτελεστεί ο κακόβουλος κώδικας. [21]

Επίθεση βασισμένη στο μοντέλο αντικειμένου εγγράφου (DOM-based XSS)

Πρόκειται για ένα είδος επίθεσης, η οποία τροποποιεί το μοντέλο αντικειμένου εγγράφου για μια ιστοσελίδα που επισκέπτεται ένας χρήστης (θύμα) με τέτοιο τρόπο ώστε όταν εκτελεστεί ο κώδικας της ιστοσελίδας να λειτουργήσει με διαφορετικό τρόπο από τον αναμενόμενο. Αυτό συμβαίνει μέσα στη σελίδα που εμφανίζεται στον φυλλομετρητή του χρήστη χωρίς να συμμετέχει στη διαδικασία ο εξυπηρετητής. Και σε αυτή την περίπτωση ο κακόβουλος κώδικας εισάγεται σαν είσοδος από τον επιτιθέμενο,

ο οποίος στη συνέχεια θα πρέπει με κάποιο τρόπο να στείλει τον σύνδεσμο της ιστοσελίδας στο υποψήφιο θύμα ώστε να ξεκινήσει η επίθεση. [22]

Τρόποι αντιμετώπισης

- *Απόρριψη εισαγωγής μη αξιόπιστων δεδομένων σε έγγραφο HTML*: Αρχικά, θα πρέπει να αποφεύγεται η εισαγωγή μη αξιόπιστων δεδομένων σε ένα έγγραφο HTML καθώς η λίστα με τους κανόνες κωδικοποίησης μπορεί να γίνει αρκετά περίπλοκη. Παρόλα αυτά, αν πρέπει να γίνουν αποδεκτά μη αξιόπιστα δεδομένα μπορούν να εφαρμοστούν οι λύσεις που αναφέρονται στη συνέχεια. [23]
- *Κωδικοποίηση μη αξιόπιστων δεδομένων*: Όταν εισάγονται μη αξιόπιστα δεδομένα στο σώμα και σε διάφορες ετικέτες της HTML τότε τα δεδομένα αυτά κωδικοποιούνται κατάλληλα. Αυτό όμως δεν είναι αρκετό για να αποκλείσει την πιθανότητα να εκτελεστεί κάποιος κακόβουλος κώδικας. Οι πιο σημαντικοί χαρακτήρες προς κωδικοποίηση με την κωδικοποίησή τους είναι οι εξής: [23]

  & → &

  < → <

  > → >

  " → "

  ' → '

- *Κωδικοποίηση χαρακτηριστικών*: Όταν εισάγονται μη αξιόπιστα δεδομένα σε πεδία χαρακτηριστικών, όπως length, width κλπ., θα πρέπει να κωδικοποιούνται και να βρίσκονται μέσα σε μονά ή διπλά εισαγωγικά ώστε να μη συμβεί διαφυγή χαρακτήρα. Με τη σειρά τους τα εισαγωγικά κωδικοποιούνται κατάλληλα (" → &#x22 , ' → &#x27). Επιπλέον, θα πρέπει να αποκλείονται κάποιες ετικέτες, όπως src, href, και χειριστές συμβάντων διότι έτσι μπορεί να εκχυθεί κακόβουλος κώδικας Javascript. [23]
- Όταν εισάγονται μη αξιόπιστα δεδομένα σε Javascript το μόνο σημείο στο οποίο είναι ασφαλές να εισαχθούν αφού κωδικοποιηθούν είναι σε πεδία τιμών δεδομένων τα οποία περικλείονται από εισαγωγικά. Σε οποιοδήποτε άλλο σημείο είναι αρκετά επικίνδυνο καθώς εύκολα μπορεί να εκτελεστεί κακόβουλος κώδικας Βέβαια, ορισμένες προκαθορισμένες συναρτήσεις (π.χ. <script> window.setInterval('...EVEN IF YOU ENCODE UNTRUSTED DATA YOU ARE XSSED HERE...'); </script>) σε καμία περίπτωση δε μπορούν να χρησιμοποιήσουν μη αξιόπιστα δεδομένα ως είσοδο. Τέλος, θα πρέπει να αποφεύγονται μη αξιόπιστοι ενιαίοι εντοπιστές πόρων (URLs), οι οποίοι μπορεί να εκτελέσουν κώδικα Javascript. [23]

- Όταν εισάγονται μη αξιόπιστα δεδομένα σε ετικέτες της γλώσσας CSS θα πρέπει να έχουν κωδικοποιηθεί και να εισάγονται μόνο σε πεδία τιμών και όχι σε άλλα μέρη στο έγγραφο καθώς μπορεί να γίνουν πολύ επικίνδυνα, όπως συμβαίνει με τα μη αξιόπιστα δεδομένα σε γλώσσα Javascript. [23]
- Όταν εισάγονται μη αξιόπιστα δεδομένα στην τιμή της παραμέτρου HTTP GET θα πρέπει να κωδικοποιούνται και δεν θα πρέπει να επιτρέπεται η εισαγωγή ενιαίων εντοπιστών πόρων (URLs) στην παράμετρο 'data' καθώς σε περίπτωση που περιέχουν κακόβουλο κώδικα δε μπορεί να διακοπεί η εκτέλεση του. επίσης, όταν οι ενιαίοι εντοπιστές πόρων εισάγονται σε διάφορες ετικέτες (πχ. src) θα πρέπει πρώτα να ελέγχονται για να διαπιστωθεί ότι δεν περιέχουν κώδικα Javascript και έπειτα να κωδικοποιούνται όπως όλα τα μη αξιόπιστα δεδομένα. [23]

3.3.3.2 Απειλές στο υπολογιστικό νέφος

Επιθέσεις Εικονικοποίησης

Επιθεση πειρατείας (Hyperjacking attack)

Στο εικονικό περιβάλλον ο υπερεπόπτης (hypervisor) είναι ένα επίπεδο λογισμικού που είτε τρέχει ως υλικολογισμικό (firmware) στο υλικό του ξενιστή είτε στο λειτουργικό σύστημα του ξενιστή και εξασφαλίζει την σωστή λειτουργία όλου του συστήματος μέσα από τη διαχείριση των εικονικών μηχανών και την κατάλληλη κατανομή των πόρων [24]. Όταν κάποιος κακόβουλος χρήστης αποκτήσει πρόσβαση στον υπερεπόπτη, τότε όλες οι εικονικές μηχανές που διαχειρίζεται ο υπερεπόπτης αλλά και τα δεδομένα που είναι αποθηκευμένα σε αυτές περνούν στον έλεγχο του επιτιθέμενου [25].

Αυτή η επίθεση πραγματοποιείται με τον επιτιθέμενο να εγκαθιστά ένα ειδικό λειτουργικό σύστημα σε μια εικονική μηχανή και να επιτίθεται στον υποκείμενο υπερεπόπτη (hypervisor). Έτσι μπορεί να αλλάξει τον πηγαίο κώδικα του υπερεπόπτη ώστε να έχει μη εξουσιοδοτημένη πρόσβαση σε μνήμη και δεδομένα εικονικών μηχανών [26]. Το λειτουργικό σύστημα του ξενιστή (host) δεν γνωρίζει ότι το μηχάνημα έχει παραβιαστεί γιατί το κακόβουλο λογισμικό (λειτουργικό σύστημα) λειτουργεί κρυφά, γεγονός το οποίο κάνει πολύ δύσκολη την ανίχνευσή του [25].

Διαφυγή εικονικής μηχανής (VM escape attack)

Πρόκειται για ένα είδος επίθεσης στο οποίο ο επιτιθέμενος παραβιάζει το λειτουργικό σύστημα μιας εικονικής μηχανής και αποκτά πρόσβαση στον υπερεπόπτη. Ο εισβολέας παρακάμπτει την απομόνωση που υπάρχει ανάμεσα στις εικονικές μηχανές και τα υπόλοιπα επίπεδα λογισμικού, δηλαδή τον υπερεπόπτη και το λειτουργικό σύστημα του ξενιστή οπότε μπορεί να αποκτήσει πρόσβαση σε ολόκληρο το σύστημα. Η επίθεση αυτή μπορεί να προκληθεί είτε από ευπάθειες του λειτουργικού συστήματος της

εικονικής μηχανής είτε από την εκτέλεση κακόβουλου κώδικα μέσα σε αυτήν. Η απομόνωση που αναφέρεται παραπάνω σχετίζεται με τον τρόπο λειτουργίας τον εικονικών μηχανών. Κάθε εικονική μηχανή έχει πρόσβαση μόνο στους πόρους που της έχουν ανατεθεί και δεν "βλέπει" τις υπόλοιπες εικονικές μηχανές που τρέχουν στο ίδιο φυσικό μηχάνημα. [27]

Μετανάστευση εικονικής μηχανής (VM Migration attack)

Οι εικονικές μηχανές μπορούν να μεταφερθούν από έναν φυσικό διακομιστή σε έναν άλλον αν χρειαστεί - αυτή η δυνατότητα είναι γνωστή ως μετανάστευση εικονικών μηχανών (VM migration). Η δυνατότητα αυτή αυξάνει την απόδοση και τη διαθεσιμότητα των υπηρεσιών καθώς για παράδειγμα στην περίπτωση που ένας διακομιστής έχει σχεδόν εξαντλήσει τους πόρους του ή στην περίπτωση όπου υπάρχουν προβλήματα δικτύου στην περιοχή που βρίσκεται ο διακομιστής οι εικονικές μηχανές μπορούν να μεταφερθούν σε έναν άλλο. Οι επιθέσεις κατά τη διάρκεια της μετανάστευσης προσπαθούν να πλήξουν τον υπερεπόπτη, το κομμάτι του λογισμικού που είναι υπεύθυνο για τη μετανάστευση των εικονικών μηχανών και τα δεδομένα που μεταφέρονται. [26]

Μια επίθεση στον υπερεπόπτη μπορεί να συμβεί όταν το δίκτυο εντός του οποίου μεταφέρονται οι εικονικές μηχανές δεν είναι ασφαλές, όταν οι εικονικές μηχανές φέρουν ήδη κακόβουλο κώδικα και όταν η εικονική μηχανή μεταφερθεί σε ένα μηχάνημα το οποίο έχει παραβιαστεί [26]. Οι επιθέσεις που μπορούν να συμβούν είναι:

- Επίθεση Άρνησης υπηρεσίας (DoS) σε ένα φυσικό μηχάνημα στέλνοντας προς αυτό πολλές εικονικές μηχανές. Με αυτό τον τρόπο, εξαντλούνται οι πόροι του και δεν μπορεί πλέον να δεχτεί άλλες εικονικές μηχανές που πρέπει να μεταναστεύσουν [28].
- Εφόσον ένα φυσικό μηχάνημα φέρει μολυσμένο υπερεπόπτη μπορεί να φαίνεται πως υπάρχουν διαθέσιμοι πόροι σε αυτό ενώ έχουν εξαντληθεί, αναγκάζοντας την μετανάστευση σε αυτό και άλλων εικονικών μηχανών [28].
- Επίθεση στη διεπαφή κονσόλας διοίκησης με αποτέλεσμα να πραγματοποιηθεί ανεπιθύμητη μετανάστευση σε φυσικό μηχάνημα (στόχο), το οποίο θα καθοριστεί από τον επιτιθέμενο και όχι από τον διαχειριστή του συστήματος, όπως θα έπρεπε κανονικά στην περίπτωση όπου οι διαδικασίες μετανάστευσης πραγματοποιούνται χειρωνακτικά [26].
- Επίθεση στην κατάσταση ιδεατής μηχανής κατά τη μετανάστευση όπου ο επιτιθέμενος μπορεί να αποκτήσει πρόσβαση σε ευαίσθητα δεδομένα, όπως κωδικοί πρόσβασης, δεδομένα εφαρμογών και κλειδιά κρυπτογράφησης, καθώς και να αλλάξει την κατάσταση των εφαρμογών, των διαδικασιών και της μνήμης της ιδεατής μηχανής [26].
- Επίθεση στην ενότητα μετανάστευσης με επόμενο στόχο την επίθεση στον υπερεπόπτη όπου θα έχει σαν αποτέλεσμα τον πλήρη έλεγχο ολόκληρης της διαδικασίας αλλά και των εικονικών μηχανών [26].

Επίθεση Πλευρικού Καναλιού (Side Channel Attack)

Οι επιθέσεις πλευρικού καναλιού είναι ένα είδος επιθέσεων που πραγματοποιείται σε φυσικά μηχανήματα, τα οποία φιλοξενούν πολλές εικονικές μηχανές που "μοιράζονται" το υλικό αυτού του μηχανήματος. Σε κάθε πληροφοριακό σύστημα ανάμεσα στην κεντρική μονάδα επεξεργασίας (CPU) και στη μνήμη τυχαίας προσπέλασης (RAM) υπάρχει η κρυφή μνήμη (cache), η οποία βοηθά στην αύξηση της ταχύτητας του συστήματος καθώς εκεί αποθηκεύονται δεδομένα τα οποία θα ήταν πολύ χρονοβόρο να τα αντλήσει ο επεξεργαστής από τη μνήμη τυχαίας προσπέλασης [25]. Η κρυφή μνήμη χωρίζεται σε τρία επίπεδα, το επίπεδο 1 όπου υπάρχει ένα τμήμα μνήμης πολύ γρήγορο και πολύ μικρής χωρητικότητας, το επίπεδο 2 όπου η χωρητικότητα είναι μεγαλύτερη σε σχέση με το επίπεδο 1 και τέλος το επίπεδο 3 όπου πρόκειται για ένα εξειδικευμένο τμήμα μνήμης που χρησιμοποιείται για να γίνουν ταχύτερα τα τμήματα 1 και 2. Σε ένα σύστημα με επεξεργαστές πολλαπλών πυρήνων η κρυφή μνήμη επιπέδου 1 και 2 είναι ξεχωριστή για κάθε πυρήνα αλλά η κρυφή μνήμη επιπέδου 3 είναι κοινή γεγονός το οποίο εκμεταλλεύεται αυτό το είδος επιθέσεων. Ένας επιτιθέμενος μπορεί να χρησιμοποιήσει μια μολυσμένη εικονική μηχανή η οποία να φιλοξενείται στο ίδιο κανάλι κρυφής μνήμης επιπέδου 3 με αυτό όπου φιλοξενείται η εικονική μηχανή του θύματος και έτσι να αποκτήσει μη εξουσιοδοτημένη πρόσβαση σε αντίστοιχες πληροφορίες (του θύματος) λόγω ανεπαρκούς λογικής απομόνωσης [26].

Επίθεση Εικόνας Επισκέπτη (Guest image attack)

Όταν υπάρχουν πολλές και ενδεχομένως περιττές εικόνες για φιλοξενούμενα λειτουργικά συστήματα (guest OS images) μπορεί να δημιουργηθούν προβλήματα. Εκτός από την κατανάλωση πόρων, υπάρχει και το πρόβλημα του ότι αν μία εικόνα είναι δημόσια τότε ενδεχομένως να γίνουν ορατές σε τρίτους προσωπικές πληροφορίες των χρηστών ενώ είναι πιθανό να περιέχει και τρωτότητες που θα κάνουν την χρήση της (από νέους χρήστες) ευάλωτη σε επιθέσεις [26]. Επιπλέον, αν μία εικόνα ιδεατής μηχανής είναι μολυσμένη τότε οι ιδεατές μηχανές που θα προκύψουν από αυτήν θα είναι και αυτές μολυσμένες. Συνεπώς, η μόλυνση είναι πιθανόν να μεταφερθεί και στο φυσικό μηχάνημα που τις φιλοξενεί [29]. Τέλος, οι ιδεατές μηχανές δίνουν τη δυνατότητα στους χρήστες να δημιουργήσουν στιγμιότυπα (snapshots), τα οποία αποθηκεύουν την κατάσταση της ιδεατής μηχανής οπότε, μελλοντικά, εφόσον χρειαστεί, μπορούν να την επαναφέρουν σε προηγούμενη κατάσταση. Η πρόσβαση ενός εισβολέα στα στιγμιότυπα μπορεί να του επιτρέψει να προσπελάσει κρίσιμες πληροφορίες για την ιδεατή μηχανή [26].

Τρόποι αντιμετώπισης

Για την αποφυγή ή έστω για τον περιορισμό επιθέσεων εικονικοποίησης θα πρέπει να τηρούνται κάποια μέτρα. Τον σημαντικότερο ρόλο σε ένα περιβάλλον εικονικοποίησης έχει ο υπερεπόπτης. Θα πρέπει, λοιπόν, ο κώδικάς του να προστατεύεται από μη εξουσιοδοτημένη πρόσβαση, όλες οι ενημερώσεις να εγκαθίστανται άμεσα, να προστατεύεται με τείχη προστασίας (firewalls) και IPSs, να αφαιρούνται από αυτόν κομμάτια κώδικα που είναι περιττά και να διασφαλιστεί ότι η επικοινωνία ανάμεσα στο υπερεπόπτη και στις εικονικές μηχανές γίνεται μέσω ασφαλών καναλιών επικοινωνίας [26]. Επιπλέον, ο υπερεπόπτης θα πρέπει να διασφαλίζει την λογική απομόνωση (isolation) ώστε οι εικονικές μηχανές να μη μπορούν να επικοινωνήσουν μεταξύ τους και κατά συνέπεια ούτε να μεταφέρουν κακόβουλο λογισμικό.

Επίσης, και το λειτουργικό σύστημα των εικονικών μηχανών θα πρέπει να προστατεύεται από κακόβουλο λογισμικό. Τέλος, οι εικονικές μηχανές θα πρέπει να σαρώνονται για να εντοπιστεί κακόβουλο λογισμικό και όταν μία εικόνα μεταφερθεί σε άλλο μηχάνημα θα πρέπει τα δεδομένα να διαγράφονται και να μην μένουν ‘’κατάλοιπα΄΄ στον αρχικό δίσκο και γενικότερα να μην παραμένουν στο σύστημα εικονικές μηχανές που δεν είναι απαραίτητες ή είναι ανασφαλής [26].

4 Security as a Service

4.1 Εισαγωγή

Όσο αυξάνεται η χρήση των πληροφοριακών συστημάτων και του διαδικτύου τόσο αυξάνεται και η έκθεση σε σημαντικές απειλές, οι οποίες πρέπει να αντιμετωπιστούν αποτελεσματικά. Γίνεται λοιπόν αναγκαία η λήψη κατάλληλων μέτρων προστασίας. Ένας τρόπος πρόσβασης σε μηχανισμούς και τεχνολογίες ασφάλειας είναι μέσω υπηρεσιών υπολογιστικού νέφους (Security-as-a-Service - SecaaS). Ειδικότερα, με τον όρο Security as a Service εννοούμε τη δυνατότητα ενός χρήστη, μιας επιχείρησης ή ενός οργανισμού να χρησιμοποιεί λογισμικό ασφαλείας που τρέχει στο διαδίκτυο ως μια υπηρεσία που είναι προσβάσιμη μέσω μιας τεχνικής διεπαφής ιστού (web interface). Ο χρήστης δεν εμπλέκεται καθόλου στη διαχείριση του δικτύου, των εξυπηρετητών και του αποθηκευτικού χώρου. Ο στόχος είναι να υπάρχει ποικιλία εφαρμογών ασφαλείας που βασίζονται στο υπολογιστικό νέφος ώστε ο χρήστης κάθε φορά, ανάλογα με τις ανάγκες του, να πετυχαίνει το βέλτιστο αποτέλεσμα δηλαδή τον μέγιστο βαθμό προστασίας με το λιγότερο δυνατό κόστος. Για να γίνει αυτό οι χρήστες πρέπει να είναι σε θέση να αξιολογήσουν και να δώσουν προτεραιότητα στους κινδύνους του συστήματος τους και οι πάροχοι θα πρέπει να προσφέρουν τις κατάλληλες υπηρεσίες ασφάλειας στους πελάτες τους.

4.2 Είδη υπηρεσιών ασφάλειας

Η Cloud Security Alliance [30], μία μη κερδοσκοπική οργάνωση, με αποστολή της την προώθηση της χρήσης καλών πρακτικών για την ασφάλεια συστημάτων υπολογιστικού νέφους και γενικά την επιμόρφωση χρηστών ως προς την ασφάλεια υπολογιστικών συστημάτων, δημιούργησε μία λίστα με τα κυριότερα είδη υπηρεσιών ασφάλειας υπολογιστικού νέφους. Βέβαια δεν είναι δυνατό να παρέχονται όλοι οι μηχανισμοί ασφαλείας με τη μορφή υπηρεσίας καθώς αυτό εξαρτάται από την ίδια τη φύση του μηχανισμού. Στην συνέχεια, θα αναλύσουμε διεξοδικά όλα αυτά τα είδη υπηρεσιών ασφάλειας.

4.2.1 Σύστημα διαχείρισης πληροφοριών και συμβάντων ασφαλείας (Security Information and Event Management - SIEM)

Το σύστημα διαχείρισης πληροφοριών και συμβάντων ασφαλείας (SIEM) είναι ένα ενιαίο σύστημα που προκύπτει από τον συνδυασμό δυο υποσυστημάτων, του υποσυστήματος διαχείρισης πληροφοριών ασφαλείας (SIM) και του υποσυστήματος διαχείρισης συμβάντων ασφαλείας (SEM). Τα παραπάνω συστήματα, σύμφωνα με την techopedia, ορίζονται ως εξής:

Διαχείριση πληροφοριών ασφαλείας (Security Information Management): Λογισμικό το οποίο αυτοματοποιεί τη συλλογή δεδομένων καταγραφής συμβάντων από συσκευές ασφαλείας, όπως τείχη προστασίας, διακομιστές μεσολάβησης, συστήματα ανίχνευσης εισβολών και λογισμικό προστασίας από ιούς. Αυτά τα δεδομένα στη συνέχεια μεταφράζονται σε συσχετισμένες και απλοποιημένες μορφές. [31]

Διαχείριση Συμβάντων Ασφαλείας (Security Event Management): η διαδικασία αναγνώρισης, συλλογής, παρακολούθησης και αναφοράς συμβάντων ασφάλειας σε ένα πληροφοριακό σύστημα. Η διαχείριση συμβάντων ασφαλείας επιτρέπει την καταγραφή και την αξιολόγηση συμβάντων και βοηθά τους διαχειριστές ασφάλειας και τους διαχειριστές συστημάτων να αναλύουν, να προσαρμόζουν και να διαχειρίζονται την αρχιτεκτονική, τις πολιτικές και τις διαδικασίες ασφάλειας των πληροφοριών. [32]

Διαχείριση πληροφοριών και συμβάντων ασφαλείας (Security Information and Event Management): η διαδικασία εντοπισμού, παρακολούθησης, καταγραφής και ανάλυσης γεγονότων ή συμβάντων ασφαλείας σε πληροφοριακά συστήματα σε πραγματικό χρόνο. Παρέχει μια ολοκληρωμένη άποψη του σεναρίου ασφαλείας σε ένα πληροφοριακό σύστημα. [33]

Τα συστήματα διαχείρισης πληροφοριών και συμβάντων ασφαλείας συλλέγουν πολύ μεγάλο όγκο από δεδομένα και αρχεία καταγραφής συμβάντων ασφαλείας μέσα από διαφορετικές πηγές και δημιουργούν αντίστοιχες αναφορές. Αυτό είναι πολύ χρήσιμο διότι εφόσον το σύστημα μπορεί να συνδυάσει πληροφορίες από διαφορετικές πηγές είναι σε θέση να εντοπίσει ύποπτη δραστηριότητα που δεν θα μπορούσε να εντοπίσει αν λάμβανε δεδομένα μόνο από μία πηγή [34]. Συνεπώς, είναι ένα πολύ χρήσιμο εργαλείο που θα μπορούσε να καλύψει εξ' ολοκλήρου τις ανάγκες μιας μεγάλης επιχείρησης ή ενός οργανισμού. Στους οργανισμούς το σύνολο του πληροφοριακού συστήματος αποτελείται από πολλές συσκευές και μεμονωμένα συστήματα ασφαλείας που μπορούν να εντοπίσουν και να αντιμετωπίσουν κάποια συγκεκριμένα είδη επιθέσεων. Έτσι λοιπόν γίνεται πολύ δύσκολο να παρακολουθείται η κατάσταση της ασφάλειας συνολικά. Για να γίνει αυτό απαιτείται η συλλογή όλων των δεδομένων που αφορούν την ασφάλεια σε ένα (μοναδικό) σύστημα.

Το αμέσως επόμενο βήμα είναι με βάση τα δεδομένα αυτά να πραγματοποιείται ανάλυση απειλών σε πραγματικό χρόνο, κάτι το οποίο είναι απαραίτητο ώστε μια επίθεση να αντιμετωπιστεί άμεσα και να έχει τις λιγότερες δυνατές επιπτώσεις για τον οργανισμό. Παρόλο που πρόκειται για ένα σύστημα το οποίο είναι πολύ χρήσιμο, όπως αναφέρθηκε προηγουμένως, το μεγαλύτερο μειονέκτημα είναι το κόστος του, το οποίο είναι υπέρογκο ειδικά για μικρές επιχειρήσεις. Εκτός από το κόστος της αγοράς εξοπλισμού της υλοποίησης και της συντήρησης του λογισμικού θα πρέπει να δοθεί και ένα πολύ μεγάλο ποσό για την μισθοδοσία και την εκπαίδευση προσωπικού, το οποίο πρέπει να είναι κατάλληλο και να διαθέτει εξειδικευμένες γνώσεις στον τομέα της ασφάλειας [35]. Συνεπώς η ανάπτυξη ενός εσωτερικού (on premise) συστήματος είναι ασύμφορη τις περισσότερες φορές και τη λύση έρχεται να δώσει η χρήση ενός τέτοιου συστήματος σαν υπηρεσία μέσω του νέφους**.**

Πηγές Δεδομένων

Οι πηγές από τις οποίες προέρχονται τα δεδομένα είναι το πιο σημαντικό στοιχείο όλου του συστήματος καθώς οποιαδήποτε διαδικασία που εκτελείται είναι βασισμένη σε αυτές. Γίνεται λοιπόν αντιληπτό ότι το σύστημα μπορεί να λειτουργήσει σωστά και να είναι αποτελεσματικό μόνο εάν λάβει τις κατάλληλες πληροφορίες. Όσο λιγότερες είναι οι πληροφορίες τόσο πιο μικρή προστασία θα παρέχει το σύστημα διότι δεν θα έχει λάβει το απαραίτητο υλικό ώστε να το επεξεργαστεί και να εξάγει αποτελέσματα. Υπάρχουν πολλές συσκευές που μπορούν να λειτουργήσουν σαν πηγές δεδομένων (όπως διακομιστές, τείχη προστασίας και συστήματα αποτροπής εισβολών) δηλαδή να παρέχουν αρχεία καταγραφής, τα οποία θα στη συνέχεια θα επεξεργαστούν [36]. Για τη μεταφορά των δεδομένων χρησιμοποιούνται πρωτόκολλα όπως τα SFTP [37] , SNMP [38], syslog [39],UDP [40] κ.α.

Υποσύστημα συλλογής αρχείων καταγραφής

Τα αρχεία καταγραφής παρέχονται από διάφορες πηγές και εισάγονται σε αυτό το υποσύστημα με δύο τρόπους: ο ένας είναι το υποσύστημα να αντλήσει τα δεδομένα (pull) από τις πηγές και ο άλλος οι πηγές να ωθήσουν (push) τα δεδομένα προς αυτό.

Στην περίπτωση που έχουμε ώθηση (push) τα δεδομένα τα στέλνει η ίδια η πηγή και το υποσύστημα απλά τα αποθηκεύει και προχωρά σε περαιτέρω επεξεργασία τους. Στις πηγές δεδομένων εγκαθίσταται ένα λογισμικό πράκτορα (agent) ο οποίος συλλέγει τα συμβάντα, τα φιλτράρει, δίνει μία συγκεκριμένη μορφή (κανονικοποιεί) στα αρχεία καταγραφής και τα προωθεί στον διακομιστή του συστήματος διαχείρισης πληροφοριών και συμβάντων ασφαλείας. Το πλεονέκτημα αυτής της μεθόδου είναι ότι η αποστολή των δεδομένων γίνεται σε πραγματικό χρόνο και το μειονέκτημα ότι χρησιμοποιείται το πρωτόκολλο UDP με το οποίο υπάρχει ο κίνδυνος κάποια πακέτα να μη φτάσουν ποτέ στον προορισμό τους ή να φτάσουν με λάθος σειρά. Από την άλλη πλευρά, όταν γίνεται άντληση (pull), τα δεδομένα μεταφέρονται με πιο περίπλοκο τρόπο καθώς το σύστημα θα πρέπει να αποκτήσει πρόσβαση στην πηγή ώστε να πάρει τα δεδομένα που χρειάζεται. Το πλεονέκτημα σε αυτή την περίπτωση είναι ο μεγαλύτερος βαθμός ασφάλειας διότι το υποσύστημα αντλεί και μορφοποιεί μόνο του τα δεδομένα που χρειάζεται

όποτε τα χρειαστεί και τα μειονεκτήματα είναι πως η πηγή θα πρέπει να εγγραφεί στο υποσύστημα ώστε αυτό να μπορεί να επικοινωνήσει μαζί της [36] καθώς και το γεγονός πως η πηγή θα πρέπει να είναι σε θέση να αποθηκεύει τα δεδομένα μέχρι αυτά να αντληθούν από το υποσύστημα.

Υποσύστημα συσχέτισης και ανάλυσης

Το υποσύστημα συσχέτισης και ανάλυσης θα λέγαμε ότι αποτελεί τον πυρήνα του συστήματος διαχείρισης πληροφοριών και συμβάντων ασφαλείας. Η συσχέτιση και ανάλυση πραγματοποιείται σε πραγματικό χρόνο σε δεδομένα που έχουν κανονικοποιηθεί ώστε να εντοπίζονται ύποπτα περιστατικά όσο πιο σύντομα γίνεται. Η συσχέτιση πληροφοριών βασίζεται σε κάποιους κανόνες σύμφωνα με τους οποίους αξιολογείται το κάθε συμβάν και όταν ένα συμβάν δείχνει ύποπτο, υπάρχει η δυνατότητα να ειδοποιούνται οι διαχειριστές ασφαλείας. Τέτοιοι κανόνες μπορούν να ληφθούν αυτόματα, να δημιουργηθούν από ανθρώπους ή να ανακτηθούν από άλλα συστήματα. Με αυτόν τον τρόπο δημιουργούνται συσχετίσεις έτσι ώστε το σύστημα να μπορεί να αντιληφθεί κάποιες πληροφορίες για το εσωτερικό και το εξωτερικό περιβάλλον και να εντοπίσει πιθανές απειλές. [41]

Υποσύστημα παρακολούθησης

Στο υποσύστημα παρακολούθησης, το οποίο λαμβάνει υπόψιν όλη την πληροφορία που διατηρείται από τα άλλα συστήματα, υπάρχει αλληλεπίδραση του συστήματος με τον άνθρωπο καθώς οι αναλυτές μπορούν να έχουν πρόσβαση στα συμβάντα. Το γεγονός αυτό είναι πολύ χρήσιμο καθώς μέσα από ένα περιβάλλον που παρέχει οπτική απεικόνιση των πληροφοριών [36] οι αναλυτές είναι σε θέση να παρέμβουν, να εντοπίσουν και να αξιολογήσουν κάποια απειλή που δεν έγινε αντιληπτή από το σύστημα ή ένα συμβάν που θεωρήθηκε ύποπτο και γενικότερα να εποπτεύουν το σύστημα.

Η οπτικοποίηση δίνει τη δυνατότητα στους αναλυτές να επιλέξουν αυτοί ποια δεδομένα και σε ποιο εύρος (π.χ. χρονικό) θέλουν να οπτικοποιήσουν, με ποιον γραφικό τρόπο θα απεικονίζονται τα δεδομένα αυτά (μπάρα, δεντροδιάγραμμα, κλπ.), σε πόσες διαστάσεις, καθώς και από ποιες και από πόσες πηγές θα προέρχονται [42], γεγονός το οποίο απαιτεί οι αναλυτές να έχουν κατανοήσει πολύ καλά τι είναι αυτό το οποίο θέλουν να απεικονίσουν ώστε εκμεταλλευόμενοι τις πάρα πολλές επιλογές που τους δίνονται να καταλήξουν στο καλύτερο δυνατό αποτέλεσμα.

4.2.2 Επιχειρησιακή συνέχεια και αποκατάσταση καταστροφών (Business Continuity and Disaster Recovery)

Σύμφωνα με την techopedia η επιχειρησιακή συνέχεια και η αποκατάσταση καταστροφών είναι ένα σύνολο διαδικασιών και τεχνικών που χρησιμοποιούνται για να βοηθήσουν έναν οργανισμό να ανακάμψει από μια καταστροφή και να συνεχίσει τις συνήθεις επιχειρηματικές του δραστηριότητες [43]. Η επιχειρησιακή συνέχεια και αποκατάσταση καταστροφών χωρίζεται σε δύο διαφορετικά συστατικά:

- *Επιχειρησιακή συνέχεια (Business Continuity – BC)*: ασχολείται με την επιχειρησιακή πλευρά της επιχειρησιακής συνέχειας και της αποκατάστασης καταστροφών. Περιλαμβάνει το σχεδιασμό και τη δημιουργία πολιτικών και διαδικασιών που διασφαλίζουν ότι οι βασικές επιχειρηματικές λειτουργίες/διαδικασίες είναι διαθέσιμες κατά τη διάρκεια και μετά από μια καταστροφή. Επίσης, μπορεί να περιλαμβάνει την αντικατάσταση προσωπικού, ζητήματα διαθεσιμότητας υπηρεσιών, ανάλυση επιχειρηματικού αντίκτυπου και διαχείριση αλλαγών [43].
- Αποκατάσταση καταστροφών (Disaster Recovery – DR): Η αποκατάσταση καταστροφών επικεντρώνεται κυρίως στην πλευρά της πληροφορικής του BCDR. Καθορίζει πώς το τμήμα πληροφορικής ενός οργανισμού θα ανακάμψει από μια φυσική ή τεχνητή καταστροφή. Οι διαδικασίες σε αυτή τη φάση μπορούν να περιλαμβάνουν την αποκατάσταση διακομιστή και δικτύου, την αντιγραφή δεδομένων αντιγράφων ασφαλείας και την παροχή συστημάτων αντιγράφων ασφαλείας [43].

Η αποκατάσταση καταστροφών μπορούμε να πούμε ότι αποτελεί ένα μέρος της επιχειρησιακής συνέχειας και μάλιστα το πιο απαραίτητο διότι χωρίς να παρέχονται ηλεκτρονικές υπηρεσίες που υλοποιούν τις απαραίτητες/κύριες επιχειρησιακές διαδικασίες ένας οργανισμός (π.χ. λόγω καταστροφής μηχανημάτων που τις φιλοξενεί) είναι αδύνατο να συνεχίσει να εκτελεί της βασικές του λειτουργίες.

Ο σημαντικότερος στόχος της παροχή υπηρεσιών αποκατάστασης καταστροφών είναι να υποστηρίξει την επιχειρησιακή συνέχεια με τον καλύτερο δυνατό τρόπο επιτρέποντας στο λογισμικό και γενικότερα σε όλη την τεχνολογική υποδομή να ανακάμψει πλήρως και να επιστρέψει σε λειτουργία μετά από μια αποτυχία [44]. Οι υπηρεσίες αποκατάστασης καταστροφών βασίζονται στη δημιουργία αντιγράφων ασφαλείας και σε μηχανισμούς αναπαραγωγής ώστε όταν συμβεί μία καταστροφή να επαναφέρουν τα απαραίτητα δεδομένα και γενικότερα τα περιουσιακά στοιχεία (assets), όπως για παράδειγμα ένας διακομιστής, έτσι ώστε ο οργανισμός να συνεχίσει να λειτουργεί σε έναν βαθμό.

Ο στόχος, λοιπόν, είναι η επαναφορά όσο το δυνατόν περισσότερων δεδομένων στο λιγότερο χρόνο και με το μικρότερο (δυνατόν) κόστος. Γίνεται εύκολα αντιληπτό ότι πρέπει να υπάρξει μία χρυσή τομή ανάμεσα στο κόστος, τον όγκο δεδομένων και τον χρόνο ανάκαμψης. Για να προσδιορίσουμε με μεγαλύτερη ακρίβεια πότε μια υπηρεσία αποκατάστασης καταστροφών είναι αποδοτική υπάρχουν κάποια βασικά χαρακτηριστικά τα οποία θα πρέπει να ικανοποιούνται από αυτή την υπηρεσία και θα παρουσιαστούν παρακάτω.

Χρονικό Σημείο Ανάκτησης Δεδομένων (Recovery Point Objective – RPO): Το χρονικό σημείο ανάκτησης δεδομένων είναι ένας τρόπος μέτρησης της χρονικής διάρκειας μεταξύ των αντιγράφων ασφαλείας και του όγκου δεδομένων που θα χαθούν όταν υπάρξει αστοχία και πραγματοποιηθεί ανάκαμψη [44-46]. Για παράδειγμα, σε μία εφαρμογή μπορεί να δημιουργούνται αντίγραφα ασφαλείας των δεδομένων κάθε τέσσερις ώρες και έτσι σε περίπτωση αστοχίας να χαθούν δεδομένα το πολύ

τεσσάρων ωρών ανάλογα με το πότε ακριβώς παρουσιάστηκε η αστοχία σε σχέση με το τελευταίο αντίγραφο ασφαλείας.

Χρονικός Στόχος Ανάκαμψης (Recovery Time Objective – RTO): Ο χρονικός στόχος ανάκαμψης είναι ένας τρόπος μέτρησης της διάρκειας κατά την οποία οι επιχειρησιακές λειτουργίες δεν είναι διαθέσιμες και του χρόνου που θα χρειαστεί για την επαναφορά τους μετά από μία καταστροφή. Εξαρτάται από την πολυπλοκότητα και την απόδοση των εργασιών που πρέπει να γίνουν, όπως για παράδειγμα τη μετάβαση από τον κύριο εξυπηρετητή σε έναν άλλο που περιέχει τα αντίγραφα ασφαλείας για μια υπηρεσία, η οποία για κάποιο λόγο έχει σταματήσει να λειτουργεί. [44-46]

Όσο μικρότερα είναι ο χρονικός στόχος ανάκαμψης και το χρονικό σημείο ανάκτησης δεδομένων τόσο πιο αποτελεσματικές είναι οι υπηρεσίες αποκατάστασης καταστροφών. Σαν αποτέλεσμα εξασφαλίζεται η επιχειρησιακή συνέχεια και οι επιπτώσεις ενός συμβάντος για έναν οργανισμό περιορίζονται στο ελάχιστο.

Απόδοση: Για να λειτουργεί σωστά μια υπηρεσία αποκατάστασης καταστροφών πρέπει να μην επηρεάζει την απόδοση των εφαρμογών με τις οποίες σχετίζεται, όταν αυτές λειτουργούν υπό κανονικές συνθήκες, χωρίς να υπάρχει κάποιο πρόβλημα. [44-46]

Συνοχή: Μια υπηρεσία αποκατάστασης καταστροφών θα πρέπει να εξασφαλίζει ότι μετά από μια αποτυχία μία εφαρμογή μπορεί να επανέλθει πλήρως και να λειτουργήσει σωστά. Αυτό σημαίνει ότι θα πρέπει για όλα τα δεδομένα που σχετίζονται με την εφαρμογή να υπάρχουν τα αντίστοιχα αντίγραφα ασφαλείας. [44-46]

Γεωγραφικός διαχωρισμός: Τα σημεία δημιουργίας αντιγράφων ασφαλείας θα πρέπει να βρίσκονται σε μεγάλη απόσταση (χιλιομετρικά) από τις κύριες τοποθεσίες αποθήκευσης των δεδομένων γεωγραφικά ώστε να μην υπάρχει κίνδυνος ανεπανόρθωτης απώλειας των δεδομένων σε περίπτωση που υπάρξει κάποια φυσική καταστροφή. Από την άλλη πλευρά, σε αυτή την περίπτωση το μειονέκτημα είναι ότι ίσως δημιουργηθούν καθυστερήσεις στο δίκτυο [44-46] (π.χ. λόγω του μεγάλου όγκου των δεδομένων που θα πρέπει να μετακινηθούν).

Στις υπηρεσίες αποκατάστασης καταστροφών εφαρμόζονται οι ακόλουθες τεχνικές για τη δημιουργία αντιγράφων ασφαλείας:

Κρύα Αντίγραφα Ασφαλείας (Cold backup): Πρόκειται για την πιο απλή τεχνική δημιουργίας αντιγράφων ασφαλείας. Δεν απαιτεί πρόσθετο υλικό και για αυτό και έχει το μικρότερο κόστος υλοποίησης. Από την άλλη, όμως, είναι η πιο χρονοβόρα τεχνική όταν προκύψει η ανάγκη ανάκτησης δεδομένων διότι όσο διαρκεί η ανάκτηση δεν υπάρχει η δυνατότητα πρόσβασης στη βάση δεδομένων και άρα δεν μπορούν να λειτουργήσουν οι σχετικές υπηρεσίες. Όταν χρειαστούν κάποια δεδομένα ώστε να αποκατασταθεί η λειτουργία μιας υπηρεσίας, πρώτα αντλούνται όλα τα δεδομένα και έπειτα ξεκινούν οι διαδικασίες για την επαναλειτουργία της υπηρεσίας αυτής. [44-46]

Καυτά Αντίγραφα Ασφαλείας (Hot Backup): Πρόκειται για την πιο ολοκληρωμένη αλλά και την πιο δαπανηρή τεχνική. Σε αυτήν υπάρχει ένα πρόσθετο/δευτερεύον στιγμιότυπο μιας εφαρμογής, το οποίο λειτουργεί σε πραγματικό χρόνο με όλη την απαραίτητη υποδομή υλικού. Σε αντίθεση με τις άλλες δύο τεχνικές δημιουργούνται συνεχώς αντίγραφα ασφαλείας των δεδομένων ώστε να είναι πάντοτε ενημερωμένο αυτό το στιγμιότυπο. Αυτό βρίσκεται σε αναμονή ώστε να αντικαταστήσει το πρωτεύον στιγμιότυπο όταν παρουσιαστεί κάποια αστοχία και τα δεδομένα να είναι όσο το δυνατόν πιο ενημερωμένα. Η απώλεια δεδομένων είναι ελάχιστη ενώ το δευτερεύον στιγμιότυπο μπορεί να αντικαταστήσει το πρωτεύον σε πολύ μικρό χρονικό διάστημα. [44-46]

Ζεστά Αντίγραφα Ασφαλείας (Warm backup): Πρόκειται για μία ενδιάμεση λύση. Εδώ δημιουργούνται αντίγραφα ασφαλείας με μια συγκεκριμένη χρονική συχνότητα και υπάρχει το απαραίτητο πρόσθετο υλικό, όπως διακομιστές οι οποίοι βρίσκονται σε αναμονή, ενώ οποιαδήποτε στιγμή χρειαστεί τα αντίγραφα ασφαλείας μπορούν να είναι διαθέσιμα σε μικρό χρονικό διάστημα. Όταν προκύψει κάποια αποτυχία θα αντληθούν τα δεδομένα από το πιο πρόσφατο αντίγραφο ασφαλείας ώστε να χρησιμοποιηθούν για την ανάκαμψη του συστήματος. Η διαφορά με τα κρύα αντίγραφα ασφαλείας (cold backup) είναι ότι το backup θα πραγματοποιηθεί όταν ένα σύστημα θα βρίσκεται εκτός λειτουργίας ενώ για τα ζεστά αντίγραφα ασφαλείας (warm backup) υπάρχει πρόσθετος εξοπλισμός και ανάλογα με τη χρονική συχνότητα που έχει οριστεί πραγματοποιείται η δημιουργία αντιγράφων ασφαλείας εν ώρα λειτουργίας [44-46]. Για παράδειγμα, σε μία δημόσια υπηρεσία τα κρύα αντίγραφα ασφαλείας θα δημιουργηθούν το σαββατοκύριακο ενώ τα ζεστά αντίγραφα ασφαλείας μπορούν να δημιουργούνται κάθε μέρα στις 14.00. Αν κάνουμε μια σύγκριση με τα καυτά αντίγραφα ασφαλείας υπάρχει το πλεονέκτημα ότι εδώ το κόστος είναι μικρότερο διότι η κατανάλωση ρεύματος είναι μικρότερη και το μειονέκτημα πως ο χρόνος ανάκαμψης είναι μεγαλύτερος. Από την άλλη πλευρά, αν συγκρίνουμε τα ζεστά με τα κρύα αντίγραφα ασφαλείας εδώ υπάρχει το πλεονέκτημα ότι ο χρόνος ανάκαμψης είναι μικρότερος και το μειονέκτημα πως το κόστος είναι μεγαλύτερο. Γίνεται, λοιπόν, φανερό ότι η τρέχουσα είναι μια ενδιάμεση λύση, όπως αναφέρθηκε στην αρχή.

4.2.3 Διαχείριση εισβολής (Intrusion Management)

Σύμφωνα με το NIST, το Σύστημα Ανίχνευσης Εισβολών (Intrusion Detection System – IDS) παρακολουθεί και αναλύει συμβάντα δικτύου ή συστήματος με σκοπό να εντοπίσει και να προειδοποιήσει σε πραγματικό ή σχεδόν πραγματικό χρόνο για απόπειρες πρόσβασης στους πόρους ενός πληροφοριακού συστήματος με μη εξουσιοδοτημένο τρόπο. Ο στόχος του Συστήματος Ανίχνευσης Εισβολών είναι να παρακολουθεί τις επιθέσεις παραβίασης ενός πληροφοριακού συστήματος και έμμεσα να συμβάλει στην προστασία του διότι οι πληροφορίες που παρέχει βοηθούν στη βελτίωση των μέτρων ασφάλειας. [47]

Ένα Σύστημα Ανίχνευσης Εισβολών αποτελείται από ορισμένα βασικά στοιχεία: (α) έναν ανιχνευτή συμβάντων που ανιχνεύει συμβάντα ασφαλείας (event box), (β) μια κονσόλα για την παρακολούθηση

συμβάντων και έλεγχο/διαχείριση του ανιχνευτή (analysis box), (γ) μια κεντρική μονάδα που καταχωρεί σε μία βάση δεδομένων όποιο συμβάν έχει εντοπίσει ο αισθητήρας (database box) και (δ) μία μονάδα η οποία δημιουργεί ειδοποιήσεις ασφάλειας (προς την κονσόλα), έτσι ώστε όταν συμβεί ξανά παρόμοιο περιστατικό το σύστημα να το θεωρήσει σαν απειλή και να λειτουργήσει ανάλογα (response box). [48]

Τα Συστήματα Ανίχνευσης Εισβολών, ανάλογα με το αντικείμενο το οποίο προστατεύουν, χωρίζονται σε τέσσερις βασικές κατηγορίες: συστήματα ανίχνευσης εισβολών βάσει του ξενιστή (host based IDS), συστήματα ανίχνευσης εισβολών βάσει δικτύου (network based IDS), συστήματα ανίχνευσης εισβολών βάσει εφαρμογών (application based IDS) και υβριδικά συστήματα ανίχνευσης (hybrid IDS) .

Ανάλογα με τους μηχανισμούς που χρησιμοποιούν για ανίχνευση και ανάλυση επιθέσεων, τα IDS χωρίζονται σε τέσσερις βασικές κατηγορίες: ανίχνευση κατάχρησης (misuse detection), ανίχνευση ανωμαλιών (anomaly detection), ανίχνευση βάσει προδιαγραφών (specification based) και υβριδική ανίχνευση (hybrid detection). Παρακάτω παρουσιάζονται όλες αυτές οι κατηγορίες και για τις 2 διαστάσεις κατηγοριοποίησης.

Σύστημα Ανίχνευσης Εισβολών βάσει του Ξενιστή

Ένα σύστημα Ανίχνευσης Εισβολών βάσει του ξενιστή (Host-based IDS - HIDS) συγκεντρώνει και αναλύει πληροφορίες από μία συγκεκριμένη συσκευή για να εντοπίσει πιθανές επιθέσεις. Πιο συγκεκριμένα, ένα τέτοιο σύστημα ελέγχει τα αρχεία καταγραφής (log files) της συσκευής, τυχόν αλλαγές που πραγματοποιούνται σε αρχεία καθώς και ποιες εφαρμογές προσπαθούν να χρησιμοποιήσουν πόρους του συστήματος. Με άλλα λόγια θα λέγαμε ότι παρακολουθεί όλη την κίνηση και τις αλλαγές που πραγματοποιούνται στο εσωτερικό μιας συσκευής με στόχο να εντοπιστεί κάποια ύποπτη δραστηριότητα και να σημάνει συναγερμός. [49]

Ένα σύστημα ανίχνευσης εισβολών βάσει του ξενιστή έχει τα πλεονεκτήματα πως δεν επηρεάζεται από τις αλλαγές που συμβαίνουν στο δίκτυο και από τη χρήση κρυπτογράφησης, μπορεί να εντοπίσει την πηγή της επίθεσης και τέλος λόγω του όγκου των δεδομένων η ανίχνευση γίνεται με αξιοπιστία και με μεγαλύτερη ακρίβεια σε σύγκριση με τις άλλες μεθόδους. Τα μειονεκτήματά του είναι πως καταλαμβάνει πόρους του συστήματος, η διαχείριση μεγάλου αριθμού συστημάτων είναι δύσκολη, μπορεί να επηρεαστεί (μολυνθεί) από την ίδια την επίθεση που προσπαθεί να εντοπίσει και τέλος δε μπορεί να εντοπίσει επιθέσεις που συμβαίνουν σε όλο το δίκτυο. [48-49]

Σύστημα Ανίχνευσης Εισβολών βάσει εφαρμογών

Ένα σύστημα ανίχνευσης εισβολών (Application based IDS) βάσει εφαρμογών αναλύει γεγονότα τα οποία συμβαίνουν μέσα σε μία εφαρμογή (application) χρησιμοποιώντας πληροφορίες από πηγές, όπως τα αρχεία καταγραφής και τα ημερολόγια δοσοληψιών της εφαρμογής. Συνεπώς, αποτελεί μια ειδική υποκατηγορία των συστημάτων ανίχνευσης εισβολών βάσει του ξενιστή. [48-49]

Ένα σύστημα ανίχνευσης εισβολών βάσει εφαρμογών έχει τα πλεονεκτήματα πως μπορεί να εντοπίσει έναν μεγάλο αριθμό παραβιάσεων καθώς εστιάζει σε συγκεκριμένες εφαρμογές που τις "γνωρίζει" σε βάθος σε σχέση με άλλα συστήματα ανίχνευσης εισβολών και να εντοπίσει ακόμα και περιπτώσεις κατάχρησης δικαιωμάτων. Επιπλέον, ομοίως με τα συστήματα ανίχνευσης εισβολών βάσει του ξενιστή, δεν επηρεάζεται από τη χρήση κρυπτογράφησης και λόγω του όγκου των δεδομένων η ανίχνευση γίνεται με αξιοπιστία και με μεγαλύτερη ακρίβεια. Από την άλλη πλευρά, τα μειονεκτήματα είναι πως οι επιτιθέμενοι έχουν τη δυνατότητα να αλλοιώσουν τα δεδομένα και, όπως και στα συστήματα ανίχνευσης εισβολών βάσει του ξενιστή έτσι και εδώ, η διαχείριση μεγάλου αριθμού συστημάτων είναι δύσκολη, υπάρχει πιθανότητα επηρεασμού/μόλυνσης από την ίδια την επίθεση προς εντοπισμό και τέλος δεν υπάρχει η δυνατότητα εντοπισμού επιθέσεων που συμβαίνουν σε όλο το δίκτυο. [48-49]

Σύστημα Ανίχνευσης Εισβολών Δικτύου

Ένα σύστημα ανίχνευσης εισβολών δικτύου (network-based IDS – NIDS), παρακολουθεί και αναλύει την κίνηση σε ολόκληρο το δίκτυο, συνεπώς μπορεί να προστατεύει πολλούς ξενιστές που είναι συνδεδεμένοι σε αυτό. Συνήθως αποτελείται από ένα σύνολο αισθητήρων που τοποθετούνται σε διάφορα σημεία του δικτύου, αναλύει τοπικά την κυκλοφορία και όταν εντοπίσει επίθεση ενημερώνεται η κεντρική κονσόλα παρακολούθησης συμβάντων και η επίθεση καταχωρείται στη βάση δεδομένων [50]. Συνήθως, χρησιμοποιείται ένα signature/misuse-based μοντέλο ανίχνευσης, το οποίο για να λειτουργήσει αποτελεσματικά είναι αναγκαίο η βάση δεδομένων να ενημερώνεται πολύ συχνά με νέα είδη επιθέσεων έτσι ώστε όταν συγκρίνονται τα πακέτα που μεταφέρονται στο δίκτυο με αυτά της βάσης να μπορεί να εντοπιστεί μια απειλή. Εναλλακτικά, μπορεί να χρησιμοποιηθεί το μοντέλο ανίχνευσης ανωμαλιών με βάση ένα στατιστικό ή βασικής γραμμής (baseline) μοντέλο δηλαδή να υπάρχει εστίαση σε παραβίαση πρωτοκόλλων, όπως TCP/IP και επιπέδου εφαρμογής (SMTP), ή το μοντέλο υβριδικής ανίχνευσης [48].

Ένα σύστημα ανίχνευσης εισβολών βάσει δικτύου έχει τα πλεονεκτήματα πως σε αντίθεση με τα παραπάνω συστήματα ανίχνευσης εισβολών έχει τη δυνατότητα να διαχειρίζεται μεγάλο αριθμό συστημάτων, δεν επηρεάζει σχεδόν καθόλου την απόδοση του δικτύου, μπορεί να παρακολουθεί διαφορετικές συσκευές (συνεπώς και λειτουργικά συστήματα), και σε ένα βαθμό δεν είναι εμφανές προς τους επιτιθέμενους. Τα μειονεκτήματά του είναι πως από πλευράς δικτύου επηρεάζεται από αλλαγές τοπολογίας του δικτύου, αν το δίκτυο είναι υπερφορτωμένο ενδεχομένως να μη μπορέσει να αναλύσει μια επίθεση και είναι δύσκολο να εφαρμοστεί σε δίκτυα με υψηλές ταχύτητες. Επιπλέον, εξαρτάται σε μεγάλο βαθμό από στατικούς προσδιορισμούς υπογραφών, εμφανίζει ψευδείς συναγερμούς και δεν συσχετίζει σωστά τα γεγονότα με αποτέλεσμα να εμφανίζεται παραπάνω από ένας συναγερμός για μία (μοναδική) περίπτωση. Τέλος, όπως και τα παραπάνω συστήματα, επηρεάζεται από τη χρήση κρυπτογράφησης και από την ίδια την επίθεση. [48-49]

Υβριδικά Συστήματα Ανίχνευσης

Είναι ολοφάνερο πως τα συστήματα ανίχνευσης εισβολών δικτύου και τα συστήματα ανίχνευσης εισβολών βάσει του ξενιστή και τα συστήματα ανίχνευσης εισβολών βάσει εφαρμογών διαφέρουν αρκετά μεταξύ τους καθώς το καθένα εκπληρώνει έναν διαφορετικό στόχο και το ποιο είναι πιο αποτελεσματικό εξαρτάται από τις απαιτήσεις ασφαλείας που υπάρχουν κάθε φορά. Τη λύση σε αυτό το ζήτημα έρχεται να δώσει το υβριδικό Σύστημα Ανίχνευσης Εισβολών το οποίο είναι ένας συνδυασμός αυτών των συστημάτων.

Συστήματα Ανίχνευσης Ανωμαλιών

Η ανίχνευση ανωμαλιών (anomaly detection) στηρίζεται στο γεγονός πως ένα πληροφοριακό σύστημα έχει διαφορετική συμπεριφορά όταν βρίσκεται σε μια κανονική ή συνηθισμένη κατάσταση και διαφορετική όταν βρίσκεται σε κατάσταση επίθεσης. Για αυτό, λοιπόν, εντοπίζει συμπεριφορές συστημάτων που διαφέρουν σε σχέση με την φυσιολογική τους λειτουργία. Δημιουργεί μοντέλα συμπεριφοράς για το σύστημα που παρακολουθείται, τα οποία δείχνουν τη συμπεριφορά του συστήματος κάτω από φυσιολογικές συνθήκες και λαμβάνουν υπόψη παραμέτρους, όπως ο αριθμός των διεργασιών που δημιουργούνται και εκτελούνται, ο αριθμός των συνδέσεων στο εκάστοτε δίκτυο κ.α. Η δημιουργία του μοντέλου βασίζεται σε δεδομένα που έχουν συλλεχθεί κατά το διάστημα κανονικής λειτουργίας του συστήματος. Οι αισθητήρες συλλέγουν δεδομένα συμβάντων και τα συγκρίνουν με αυτά των μοτίβων για να προσδιορίσουν πότε η δραστηριότητα που ελέγχεται διαφέρει από την κανονική [50]. Τα βασικά πλεονεκτήματα αυτού του μηχανισμού είναι πως μπορεί να εντοπίσει νέα είδη επιθέσεων και να χρησιμοποιηθεί σε ανιχνευτές κακής συμπεριφοράς ενώ τα μειονεκτήματα του είναι ότι πολλές φορές δημιουργούνται ψευδείς συναγερμοί, δηλαδή φαίνεται ότι υπάρχει εισβολή στο σύστημα ενώ κάτι τέτοιο δεν συμβαίνει στην πραγματικότητα, καθώς και το γεγονός πως απαιτούνται συχνές περίοδοι εκμάθησης. [48-49]

Παραδείγματα μη συνηθισμένων - ανώμαλων ενεργειών:

- Μεγάλος αριθμός συνδέσεων στο σύστημα [49].
- Μεγάλη κατανάλωση υπολογιστικών πόρων του εκάστοτε συστήματος σε σχέση με το συνηθισμένο [49].
- Μεγάλος αριθμός αποτυχημένων προσπαθειών εισόδου [49].

Συστήματα Ανίχνευσης Κατάχρησης

Η ανίχνευση κατάχρησης (misuse detection) σε αντίθεση με την ανίχνευση ανωμαλιών αντί να προσπαθεί να αναλύσει (κανονικές) συμπεριφορές ώστε να δημιουργήσει νέα μοτίβα αναζητά συμβάντα τα οποία να ταιριάζουν με ένα προκαθορισμένο μοτίβο που περιγράφει μια γνωστή επίθεση. Το μοτίβο που περιγράφει μια επίθεση ονομάζεται υπογραφή. Συνεπώς, αυτός ο μηχανισμός μπορεί να

χρησιμοποιηθεί μόνο στην περίπτωση που ένα σύνολο ενεργειών είναι ήδη γνωστό, έχει χαρακτηριστεί ως μια διαδικασία επίθεσης και είναι καταχωρημένο στη βάση δεδομένων με την μορφή μιας υπογραφής [49]. Ένα πλεονέκτημα αυτής της μεθόδου ανίχνευσης είναι ότι είναι εξαιρετικά ακριβής και σπάνια δημιουργεί ψευδείς συναγερμούς. Από την άλλη πλευρά, όμως, μπορεί να ανιχνεύσει μόνο συγκεκριμένα είδη απειλών. Συνεπώς, θα πρέπει να ενημερώνεται συχνά μέσα από τη βάση δεδομένων όπου καταχωρούνται τα συμβάντα με νέες υπογραφές ή με τροποποιήσεις υπαρχόντων. Επιπλέον, αν ένας επιτιθέμενος αλλάξει τον τρόπο εκτέλεσης μιας επίθεσης, αυτό σημαίνει πως η υπογραφή της δεν θα είναι πια η ίδια σε σχέση με αυτή που έχει αποθηκευτεί οπότε η επίθεση αυτή δε θα μπορεί να ανιχνευτεί ως γνωστή μέσα από βάση δεδομένων [48-49].

Συστήματα Ανίχνευσης βάσει προδιαγραφών

Η ανίχνευση βάσει προδιαγραφών (specification based) είναι μία τεχνική η οποία χρησιμοποιεί προδιαγραφές για να καθορίσει την αναμενόμενη συμπεριφορά του συστήματος και όταν εντοπίσει ένα σύνολο ενεργειών το οποίο είναι εκτός αυτών των προδιαγραφών τότε αντιλαμβάνεται μια εισβολή. Γενικότερα, θα λέγαμε ότι μοιάζει με την τεχνική ανίχνευσης ανωμαλιών αλλά εδώ το τι θεωρείται εντός των προδιαγραφών ορίζεται χειροκίνητα από τον διαχειριστή του συστήματος και όχι αυτοματοποιημένα παρακολουθώντας προηγούμενες συμπεριφορές χρηστών [49]. Πιο συγκεκριμένα, γίνεται εστίαση σε εφαρμογές και το όλο σύστημα όπου προδιαγράφεται η αναμενόμενη συμπεριφορά με χειρωνακτικό τρόπο και στη συνέχεια ελέγχεται η τρέχουσα συμπεριφορά σε σύγκριση με την αναμενόμενη με βάση ίχνη ή ακολουθίες γεγονότων που ανιχνεύονται [48]. Ένα πλεονέκτημα αυτής της μεθόδου, όπως στην περίπτωση της ανίχνευσης κατάχρησης, είναι το γεγονός πως δεν εγείρονται πολλοί ψευδείς συναγερμοί, γιατί όταν παρατηρείται ασυνήθιστη (αλλά νόμιμη) συμπεριφορά συγκρίνεται με τη συμπεριφορά που έχει προδιαγραφεί χειρωνακτικά, η οποία είναι νόμιμη. Από την άλλη πλευρά αυτή η τεχνική είναι πιο δύσκολο να υλοποιηθεί με υψηλή ακρίβεια καθώς όσο πιο ευρύ γίνεται το πεδίο το οποίο καλείται να καλύψει το σύστημα ανίχνευσης εισβολών (περισσότερα προγράμματα, πρωτόκολλα κλπ.) τόσο πιο δύσκολο γίνεται να καθοριστούν οι αναμενόμενες συμπεριφορές για όλες τις περιπτώσεις [51].

Υβριδικά Συστήματα Ανίχνευσης

Ένα υβριδικό σύστημα ανίχνευσης προκύπτει από το συνδυασμό των παραπάνω τεχνικών σε ένα ενιαίο σύστημα ώστε να καλύπτει όσο το δυνατόν περισσότερες περιπτώσεις και να παρέχει μία πιο ολοκληρωμένη λύση. Χρησιμοποιώντας την τεχνική ανίχνευσης ανωμαλιών μπορεί να ανιχνεύσει αποτελεσματικά τις επιθέσεις που εμφανίζονται για πρώτη φορά και αντίστοιχα χρησιμοποιώντας την τεχνική ανίχνευσης κατάχρησης μπορεί να εντοπίζει τις επιθέσεις που είναι ήδη γνωστές.

4.2.4 Διαχείριση ταυτότητας και πρόσβασης (Identity and Access Management)

Η διαχείριση ταυτότητας και πρόσβασης (IAM) ορίζεται ως ένα σύνολο διαδικασιών, πολιτικών και εργαλείων για τον καθορισμό και τη διαχείριση των ρόλων και των προνομίων πρόσβασης μεμονωμένων οντοτήτων δικτύου (χρήστες και συσκευές) σε μια ποικιλία εφαρμογών νέφους και εσωτερικής εγκατάστασης [52]. Πραγματοποιείται χρησιμοποιώντας διάφορες τεχνικές, όπως η υποχρεωτική χρήση κωδικού πρόσβασης στους λογαριασμούς και η παραχώρηση διαφορετικού πλήθους και είδους δικαιωμάτων στους χρήστες ανάλογα με το ρόλο τους (π.χ. χρήστης και διαχειριστής). Πιο πρακτικά, θα λέγαμε ότι ένα σύστημα IAM χρησιμοποιείται για τον έλεγχο ταυτότητας χρηστών, συσκευών ή υπηρεσιών και για την παραχώρηση ή άρνηση δικαιωμάτων πρόσβασης σε δεδομένα και άλλους πόρους του συστήματος.

Ένα σύστημα IAM αποτελείται από δύο υποσυστήματα, αυτό της διαχείρισης ταυτότητας (identity management) και αυτό της διαχείρισης πρόσβασης (access management), τα οποία συσχετίζονται με την λογική πως δεν νοείται διαχείριση πρόσβασης αν δεν υπάρχει η απαραίτητη πληροφορία ταυτοποίησης. Παρακάτω παρουσιάζεται το κάθε υποσύστημα μεμονωμένα.

Διαχείριση Ταυτότητας (Identity Management)

Το σύστημα διαχείρισης ταυτότητας είναι ένα σύνολο διαδικασιών που χρησιμοποιούνται από έναν οργανισμό για τη διαχείριση πληροφοριών σχετικά με την ταυτότητα των χρηστών. Παρέχει πληροφορίες ελέγχου που δείχνουν πώς και γιατί έχει τη δυνατότητα να αιτηθεί την είσοδο ένας χρήστης σε ένα σύστημα και ταυτόχρονα συντελεί στη μείωση των εξόδων τους οργανισμού που προκύπτουν από τις διαδικασίες για τη διαχείριση των διαπιστευτηρίων των χρηστών. Αυτό προκύπτει από το γεγονός πως περιορίζεται σε πολύ μεγάλο βαθμό ο φόρτος εργασίας για υποστηρικτικές λειτουργίες, όπως η δημιουργία λογαριασμού για έναν χρήστη και η επαναφορά κωδικού πρόσβασης, διότι αυτές οι διαδικασίες αυτοματοποιούνται. [53]

Διαχείριση πρόσβασης (Access Management)

Η διαχείριση πρόσβασης είναι η διαδικασία παραχώρησης δικαιωμάτων πρόσβασης στους εξουσιοδοτημένους χρήστες για χρήση μιας υπηρεσίας και γενικότερα πόρων του συστήματος, αποτρέποντας τη μη εξουσιοδοτημένη πρόσβαση. Το πεδίο της διαχείρισης πρόσβασης παρέχει τη δυνατότητα στον οργανισμό να διαχειρίζεται τη διαθεσιμότητα, την ακεραιότητα και την εμπιστευτικότητα των δεδομένων του. Το σύστημα διαχείρισης πρόσβασης συμπεραίνει αν ένας χρήστης μπορεί να έχει πρόσβαση ή όχι σε έναν πόρο με βάση το αίτημά του και εφαρμόζει αυτό το συμπέρασμα/απόφαση πρόσβασης. Εφόσον τα διαπιστευτήρια ενός χρήστη επαληθευτούν, εάν έχει τα κατάλληλα δικαιώματα τότε η διαχείριση πρόσβασης θα του δώσει τη δυνατότητα να χρησιμοποιήσει την υπηρεσία που επιθυμεί. [53]

Οι κυριότερες μέθοδοι διαχείρισης πρόσβασης είναι ο έλεγχος πρόσβασης βασισμένος σε ρόλους (Role Based Access Control – RBAC) και ο έλεγχος πρόσβασης βασισμένος σε ιδιότητες (Attribute Based Access Control – ABAC).

1. *Έλεγχος πρόσβασης βασισμένος σε ρόλους (RBAC)*: Πρόκειται για έναν μηχανισμό ο οποίος στηρίζεται σε κάποιους ρόλους, δηλαδή ανάλογα με τον ρόλο που έχει ένας χρήστης του ανατίθενται και τα αντίστοιχα δικαιώματα πρόσβασης από τον διαχειριστή του συστήματος [54]. Για παράδειγμα, με βάση το ρόλο του ένας διαχειριστής έχει πρόσβαση σε ειδικά αρχεία του Λειτουργικού Συστήματος ενώ ένας απλός χρήστης μόνο στα αρχεία που αντιστοιχούν στον λογαριασμό του.

2. *Έλεγχος πρόσβασης βασισμένος σε ιδιότητες (ABAC)*: Πρόκειται για έναν μηχανισμό ο οποίος στηρίζεται σε ένα σύνολο χαρακτηριστικών τα οποία σχετίζονται μέσω κανόνων πρόσβασης. Υπάρχουν τρία είδη χαρακτηριστικών: (α) τα χαρακτηριστικά του χρήστη, όπως το όνομα, ο ρόλος και το αναγνωριστικό του, (β) τα χαρακτηριστικά των πόρων, όπως η ημερομηνία δημιουργίας και το όνομα του δημιουργού τους και (γ) τέλος τα χαρακτηριστικά περιβάλλοντος, όπως η τοποθεσία και η ώρα πρόσβασης. Όταν, λοιπόν, θα πρέπει να δοθεί πρόσβαση για έναν πόρο σε έναν χρήστη αξιολογούνται όλα τα προαναφερόμενα χαρακτηριστικά και η απόφαση για πρόσβαση ή μη λαμβάνεται με πιο ολοκληρωμένο τρόπο [54]. Για παράδειγμα, ένας τραπεζικός υπάλληλος μιας πολυεθνικής τράπεζας σε κατάστημα της Ελλάδος μπορεί να έχει τη δυνατότητα μόνο για ανάγνωση του υπολειπόμενου ποσού δανείων, μόνο για πελάτες που έλαβαν το δάνειο από υποκατάστημα στην Ελλάδα και μόνο κατά το ωράριο λειτουργίας της τράπεζας.

Αν έπρεπε να επιλέξουμε ανάμεσα στις δύο μεθόδους θα λέγαμε ότι η καλύτερη μέθοδος είναι ο έλεγχος πρόσβασης βασισμένος σε ιδιότητες διότι είναι μια πιο πλήρης μέθοδος, η οποία λαμβάνει υπόψιν πολλές παραμέτρους και προσφέρει περισσότερες δυνατότητες σχετικά με μία απόφαση εξουσιοδότησης, όπως αναφέρθηκε και στο παράδειγμα παραπάνω. Από την άλλη πλευρά, όμως, επειδή είναι πιο σύνθετη έχει υψηλότερο κόστος υλοποίησης και λειτουργίας και δεν ενδείκνυται για μικρούς οργανισμούς.

Ένα σύστημα διαχείρισης ταυτότητας και πρόσβασης περιλαμβάνει ορισμένες βασικές λειτουργίες όπως:

α. *Παροχή και ανάκληση ταυτότητας (Identity provisioning)*: Με την παροχή ταυτότητας ένας νέος χρήστης εγγράφεται για πρώτη φορά στο σύστημα, και αποκτά έναν λογαριασμό που του δίνει πρόσβαση με ασφαλή τρόπο στο σύνολο του λογισμικού και των δεδομένων που καλείται να χρησιμοποιήσει εντός ενός οργανισμού. Όταν αντίστοιχα αυτός ο χρήστης πάψει να είναι μέλος ή πελάτης του οργανισμού θα πρέπει ο λογαριασμός που έχει δημιουργηθεί για εκείνον να απενεργοποιηθεί (και πιθανώς να διαγραφεί). [55]

β. *Έλεγχος ταυτότητας (Authentication)*: Ο έλεγχος ταυτότητας περιλαμβάνει την επαλήθευση της ταυτότητας των χρηστών ή των συστημάτων μέσω διαφόρων μηχανισμών (μεμονωμένα ή σε συνδυασμό), όπως οι κωδικοί πρόσβασης και τα βιομετρικά στοιχεία. [55]

γ. *Εξουσιοδότηση (Authorisation)*: Η λειτουργία εξουσιοδότησης ελέγχει ποια δικαιώματα έχει ένας χρήστης που έχει ταυτοποιηθεί και έχει εισέλθει στο σύστημα. Ειδικότερα, ελέγχει σε ποια δεδομένα και λειτουργίες εφαρμογών ή υπηρεσιών έχει πρόσβαση και ποιους πόρους του συστήματος μπορεί να χρησιμοποιήσει. [55]

δ. *Έλεγχος (Auditing)*: Η διαδικασία του ελέγχου πιστοποιεί πως εφαρμόζονται οι πολιτικές ασφαλείας που έχει ορίσει ένας οργανισμός και βοηθά να εντοπιστούν πιθανές παραβιάσεις. Για να λειτουργήσει σωστά θα πρέπει να καταχωρούνται όλες οι ενέργειες ταυτοποίησης και εξουσιοδότησης. [55]

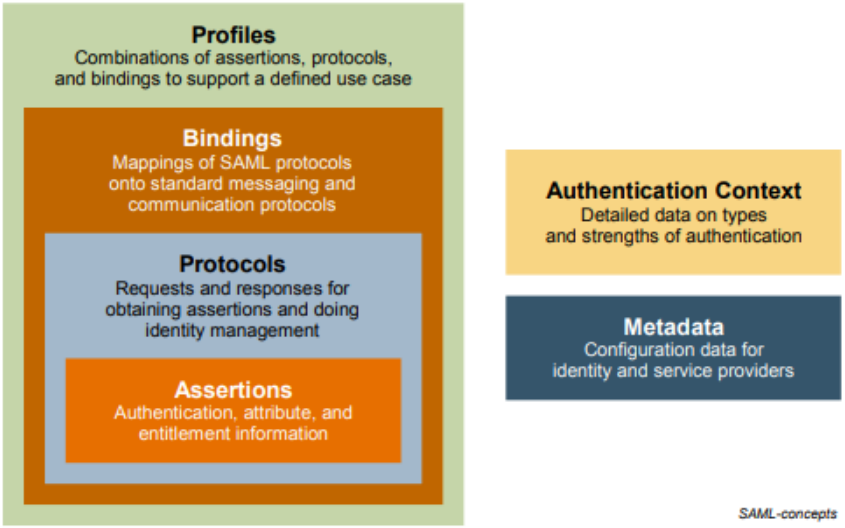
Παρακάτω παρουσιάζονται ορισμένα πρότυπα που εφαρμόζονται σε ένα σύστημα διαχείρισης ταυτότητας και πρόσβασης

Security Assertion Markup Language (SAML)

Πρόκειται για ένα πρότυπο για τον έλεγχο ταυτότητας των χρηστών το οποίο βασίζεται στη γλώσσα XML και χρησιμοποιείται για τη μεταφορά των δεδομένων αυθεντικοποίησης ενός χρήστη από τον πάροχο ταυτότητας στον πάροχο υπηρεσίας (για την οποία απαιτείται ο χρήστης να έχει ταυτοποιηθεί). Οι πληροφορίες ασφάλειας, όπως πληροφορίες για την ταυτότητα, τον έλεγχο ταυτότητας και την εξουσιοδότηση χρηστών, εκφράζονται σαν ισχυρισμοί (assertions) της SAML και οι εφαρμογές/υπηρεσίες τις οποίες ο χρήστης ζητά να χρησιμοποιήσει θεωρούν ότι οι ισχυρισμοί αυτοί είναι αληθείς. Οι ισχυρισμοί παράγονται από άλλα συστατικά/υπηρεσίες για τα οποία υπάρχει εμπιστοσύνη πως θα δημιουργήσουν έγκυρους ισχυρισμούς με βάση τα στοιχεία (πχ. διαπιστευτήρια) που παρέχονται από τον χρήστη. [56-57]

Η ανταλλαγή πληροφοριών γίνεται κάθε φορά ανάμεσα σε δύο συναλλασσόμενες οντότητες, η μία κάνει ένα αίτημα πρόσβασης σε πόρους/υπηρεσίες (asserting party) και η άλλη το λαμβάνει και στη συνέχεια είτε το δέχεται είτε το απορρίπτει (relying party). Δηλαδή η οντότητα που κάνει το αίτημα (asserting party) ζητά από την οντότητα προς την οποία στέλνεται το αίτημα (relying party) να επιτρέψει σε έναν εξουσιοδοτημένο χρήστη να χρησιμοποιήσει μία υπηρεσία. Το πρότυπο SAML αποτελείται από κάποια δομικά στοιχεία (blocks) τα οποία επιτρέπουν τη μεταφορά των πληροφοριών ασφαλείας που αναφέρθηκαν πιο πάνω μεταξύ οργανισμών που έχουν μία εδραιωμένη σχέση εμπιστοσύνης. Η δομή και το περιεχόμενο των μηνυμάτων των ισχυρισμών και του πρωτοκόλλου που χρησιμοποιείται για τη

μεταφορά τους περιγράφονται στην προδιαγραφή του προτύπου και το πως πρέπει να είναι δομημένος ένας ισχυρισμός ώστε να είναι έγκυρος περιγράφεται στο XML σχήμα των ισχυρισμών SAML. [56-57]



Εικόνα 2. Δομικά στοιχεία της SAML [56]

Οι ισχυρισμοί δημιουργούνται ως απόκριση όταν μία οντότητα έχει δημιουργήσει ένα αίτημα ενώ για την υλοποίηση τόσο των αιτημάτων αλλά και των ισχυρισμών χρησιμοποιούνται μηνύματα του πρωτοκόλλου SAML, όπου η δομή και το περιεχόμενό τους καθορίζεται από ένα πρωτόκολλο βασισμένο σε XML. [56-57]

Οι αντιστοιχίσεις (bindings) SAML χρησιμοποιούνται για να περιγράψουν πως μπορεί να γίνει μεταφορά μηνυμάτων SAML με πρωτόκολλα ανταλλαγής μηνυμάτων, όπως το HTTP. [56-57]

Τα προφίλ SAML περιγράφουν τη δομή των ισχυρισμών, των πρωτοκόλλων και των αντιστοιχίσεων για μία περίπτωση χρήσης. [56-57]

Τα μεταδεδομένα ορίζουν έναν τρόπο με τον οποίο είναι δυνατή η διατύπωση και ο διαμοιρασμός πληροφοριών ανάμεσα στους συμμετέχοντες σε ένα σύστημα που χρησιμοποιεί το πρότυπο SAML. [56-57]

Ένα πλαίσιο αυθεντικοποίησης χρησιμοποιείται όταν ένας πάροχος υπηρεσιών χρειάζεται αναλυτικές πληροφορίες σχετικά με την αυθεντικοποίηση ενός χρήστη από τον πάροχο ταυτότητας και δημιουργείται με βάση ένα σχήμα XML. [56],[57]

eXtensible Access Control Markup Language (XACML)

Πρόκειται για ένα πρότυπο που βασίζεται στη γλώσσα XML και περιγράφει μια γλώσσα πολιτικής καθώς και μια γλώσσα αίτησης/απόκρισης απόφασης ελέγχου πρόσβασης. Η γλώσσα πολιτικής χρησιμοποιείται για την περιγραφή γενικών απαιτήσεων ελέγχου πρόσβασης ενώ η γλώσσα αίτησης/απόκρισης χρησιμοποιείται για να σχηματιστεί ένα ερώτημα που αφορά το αν θα πρέπει να επιτρέπεται μία συγκεκριμένη ενέργεια, όπως για παράδειγμα πρόσβαση σε κάποιον πόρο του συστήματος. Παρακάτω υπάρχει ένα λεξικό κάποιων βασικών εννοιών ώστε στη συνέχεια να γίνει κατανοητό το διάγραμμα ροής δεδομένων. [58]

Λεξικό:

Action (Ενέργεια): Μια λειτουργία/ενέργεια πάνω σε έναν πόρο [59].

Attributes (Γνωρίσματα): Χαρακτηριστικά ενός υποκειμένου, ενός πόρου, μιας ενέργειας ή του περιβάλλοντος που αναφέρονται σε έναν στόχο [59].

Context Handler (Χειριστής Πλαισίου): Η οντότητα που μετατρέπει τα αιτήματα αποφάσεων από την αρχική τους μορφή σε κανονική μορφή XACML και τις αποφάσεις εξουσιοδότησης από κανονική μορφή XACML στην αρχική τους μορφή (δηλαδή στη μορφή που είχε το αίτημα απόφασης όταν στάλθηκε από το Κέντρο Επιβολής Πολίτικων) [59].

Environment (Περιβάλλον): Το σύνολο των γνωρισμάτων που σχετίζονται με μια απόφαση εξουσιοδότησης και είναι ανεξάρτητα από ένα συγκεκριμένο υποκείμενο, πόρο ή ενέργεια [59].

Obligation (Υποχρέωση): Μια λειτουργία που καθορίζεται σε μια πολιτική ή ένα σύνολο πολιτικών η οποία πρέπει να εκτελείται από το Κέντρο Επιβολής Πολιτικών σε συνδυασμό με την επιβολή μιας απόφασης εξουσιοδότησης [59].

Policy (Πολιτική): Ένα σύνολο κανόνων, ο καθορισμός ενός συγκεκριμένου αλγόριθμου συνδυασμού κανόνων και προαιρετικά ένα σύνολο υποχρεώσεων. Μια πολιτική μπορεί να είναι και μέρος ενός συνόλου πολιτικών [59].

Policy Administration Point (PAP) (Κέντρο Διαχείρισης Πολίτικών): Η οντότητα που δημιουργεί και διαχειρίζεται μία πολιτική ή ένα σύνολο πολιτικών [59].

Policy Decision Point (PDP) (Κέντρο Αποφάσεων Πολίτικών): Η οντότητα που αξιολογεί την πολιτική που εφαρμόζεται και ορίζει την απόφαση εξουσιοδότησης [59].

Policy Enforcement Point (PEP) (Κέντρο Επιβολής Πολιτικών): Η οντότητα που εκτελεί τον έλεγχο πρόσβασης δηλαδή δημιουργεί αιτήματα αποφάσεων και επιβάλλει τις αποφάσεις πρόσβασης που λαμβάνει [59].

Policy Information Point (PIP) (Κέντρο Πληροφοριών Πολιτικών): Η οντότητα που παρέχει τιμές για τα διάφορα γνωρίσματα [59].

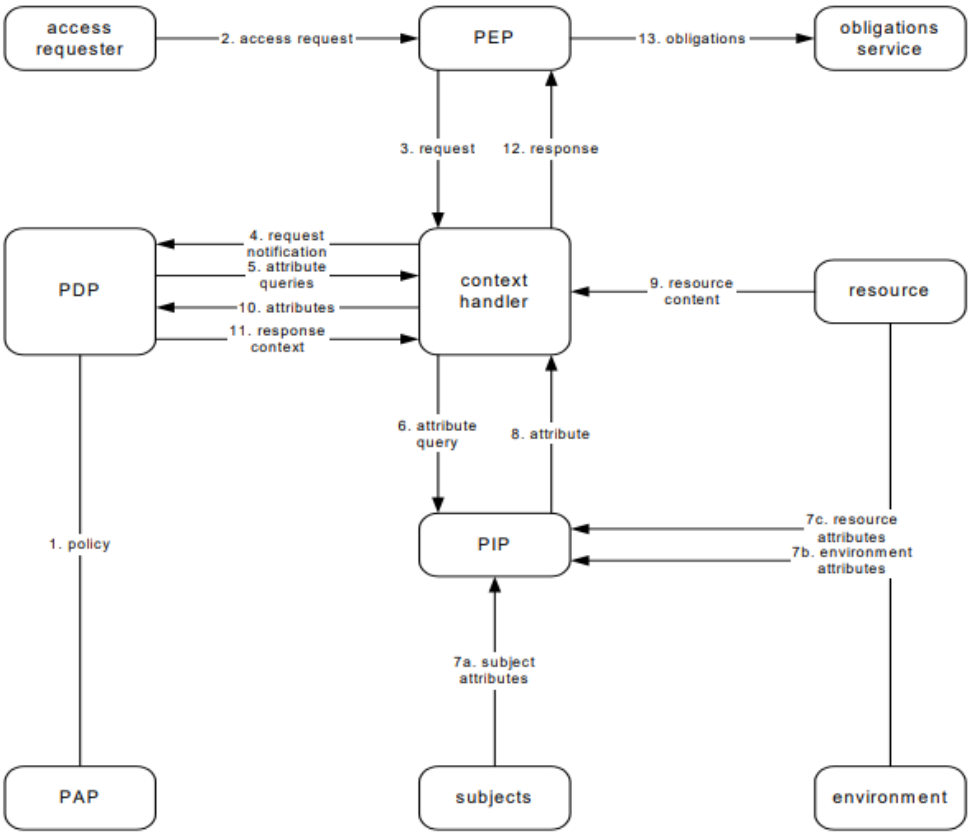
Policy Set (Σύνολο Πολιτικών): Ένα σύνολο πολιτικών το οποίο ενδεχομένως να περιέχει και άλλα σύνολα πολιτικών, ένας αλγόριθμος συνδυασμού πολιτικών και προαιρετικά ένα σύνολο υποχρεώσεων [59].

Resource (Πόρος): δεδομένα, υπηρεσίες ή συστατικά στοιχεία (components) του συστήματος [59].

Subject (Υποκείμενο): Μία οντότητα για την οποία πρέπει να αποφασιστεί εάν θα της παραχωρηθεί η πρόσβαση την οποία αιτείται [59].

Target (Στόχος): Τα αιτήματα απόφασης που ένας κανόνας, μια πολιτική ή ένα σύνολο πολιτικών πρέπει να αξιολογήσουν [59].

Παρακάτω παρατίθεται το διάγραμμα ροής δεδομένων και η περιγραφή του [59].



Εικόνα 3. Διάγραμμα ροής δεδομένων της XACML [59]

1. Το Κέντρο Διαχείρισης Πολίτικών γράφει κάποιες πολιτικές και σύνολα πολιτικών, τα οποία κοινοποιεί στο Κέντρο Αποφάσεων Πολιτικών και αποτελούν την πλήρη πολιτική για έναν καθορισμένο στόχο.
2. Ο αιτών πρόσβασης στέλνει ένα αίτημα για πρόσβαση στο Κέντρο Επιβολής Πολιτικών.
3. Το Κέντρο Επιβολής Πολιτικών στέλνει το αίτημα πρόσβασης στον Χειριστή Πλαισίου στην αρχική του μορφή δηλαδή χωρίς να έχει κάποια συγκεκριμένη μορφή (format). Προαιρετικά, το αίτημα πρόσβασης μπορεί να περιλαμβάνει γνωρίσματα για το περιβάλλον, τα υποκείμενα, τους πόρους και τις ενέργειες.
4. Ο Χειριστής Πλαισίου δημιουργεί ένα πλαίσιο αίτησης XACML, δηλαδή η αίτηση αποκτά την κατάλληλη μορφή, και το στέλνει στο Κέντρο Αποφάσεων Πολιτικών.
5. Το Κέντρο Αποφάσεων Πολιτικών ζητά από τον Χειριστή Πλαισίου τυχόν επιπλέον πληροφορίες για τα υποκείμενα, τους πόρους, τις ενέργειες και τα γνωρίσματα του περιβάλλοντος.
6. Ο Χειριστής Πλαισίου ζητά τα γνωρίσματα από το Κέντρο Πληροφοριών Πολιτικών.
7. Το Κέντρο Πληροφοριών Πολιτικών ανακτά τα γνωρίσματα που του έχουν ζητηθεί.
8. Το Κέντρο Πληροφοριών Πολιτικών στέλνει τα γνωρίσματα που του έχουν ζητηθεί στον Χειριστή Πλαισίου.
9. Προαιρετικά, ο Χειριστής Πλαισίου μπορεί να συμπεριλάβει και τον πόρο στο πλαίσιο.
10. Ο Χειριστής Πλαισίου στέλνει τα ζητούμενα γνωρίσματα και προαιρετικά τον πόρο στο Κέντρο Αποφάσεων Πολιτικών και αυτό αξιολογεί την πολιτική.
11. Το Κέντρο Αποφάσεων Πολιτικών στέλνει το πλαίσιο απόκρισης, το οποίο περιέχει την απόφαση για την εξουσιοδότηση, στον Χειριστή Πλαισίου.
12. Ο Χειριστής Πλαισίου μετατρέπει το πλαίσιο απόκρισης στη μορφή που είχε αρχικά το αίτημα όταν το έλαβε από το Κέντρο Επιβολής Πολιτικών και στη συνέχεια στέλνει την απάντηση στο Κέντρο Επιβολής Πολιτικών.
13. Το Κέντρο Επιβολής Πολιτικών εκπληρώνει τις υποχρεώσεις.
14. (Δεν φαίνεται στο διάγραμμα). Αν επιτραπεί η πρόσβαση, το Κέντρο Επιβολής Πολιτικών επιτρέπει την πρόσβαση που ζητήθηκε. Σε αντίθετη περίπτωση, την αρνείται.

4.2.5 Πρόληψη απώλειας δεδομένων (Data Loss Prevention)

Για να ελαχιστοποιηθεί ο κίνδυνος παραβίασης δεδομένων οι οργανισμοί χρησιμοποιούν συχνά μηχανισμούς προστασίας απώλειας δεδομένων (DLP). Η πρόληψη απώλειας δεδομένων είναι μια λύση που έχει σχεδιαστεί για την έγκαιρη ανίχνευση πιθανών περιστατικών παραβίασης δεδομένων και την αποτροπή τους, παρακολουθώντας δεδομένα είτε σε χρήση, είτε σε κίνηση, είτε σε κατάσταση ηρεμίας [60]. Στόχος είναι η προστασία ευαίσθητων πληροφοριών, όπως προσωπικά στοιχεία, πιστωτικές κάρτες, αριθμοί κοινωνικής ασφάλισης, οικονομικές & νομικές πληροφορίες, εταιρικά μυστικά και γενικά πληροφορίες που δημιουργούνται εντός άλλες οργανισμού.

Τα συστήματα πρόληψης απώλειας δεδομένων διακρίνουν τα δεδομένα σε τρεις κατηγορίες

Δεδομένα σε κατάσταση ηρεμίας

Τα δεδομένα σε κατάσταση ηρεμίας είναι δεδομένα που αποθηκεύονται τόσο σε συσκευές εντός του οργανισμού, όπως συστήματα διαχείρισης εγγράφων, διακομιστές email και αρχείων και προσωπικούς υπολογιστές, όσο και σε άλλες εξωτερικές συσκευές ή υπηρεσίες, όπως υπηρεσίες νέφους. Για να αποτραπεί η πρόσβαση, η τροποποίηση και ενδεχομένως η κλοπή δεδομένων σε κατάσταση ηρεμίας από μη εξουσιοδοτημένα άτομα χρησιμοποιούνται μέτρα ασφαλείας, όπως η κρυπτογράφηση δεδομένων και ο έλεγχος πρόσβασης. Απαραίτητη προϋπόθεση για αυτά τα μέτρα ασφαλείας είναι να εντοπιστεί το περιεχόμενο το οποίο είναι αναγκαίο να προστατευθεί και τα σημεία στα οποία είναι αποθηκευμένο [60-61].

Δεδομένα σε χρήση

Τα δεδομένα σε χρήση είναι δεδομένα με τα οποία αλληλοεπιδρά ένας χρήστης δηλαδή τα χρησιμοποιεί σε έγγραφα, email, εφαρμογές κ.α. Το σύστημα προστασίας, το οποίο τοποθετείται σε τελικά σημεία, αναλαμβάνει να επιτρέψει ή όχι την πρόσβαση στα δεδομένα σε συσκευές, μπορεί να μπλοκάρει την μετακίνηση των δεδομένων σε φορητές συσκευές πολυμέσων, περιορίζει την αντιγραφή, επικόλληση και τροποποίηση των εμπιστευτικών δεδομένων καθώς και την αναπαραγωγή σκληρών αντιγράφων των δεδομένων σε εκτυπωτές. Εν γένει, εφόσον γίνει προσπάθεια αποστολής ευαίσθητων δεδομένων η ενδεχόμενη διαρροή θα εντοπιστεί αμέσως και θα αντιμετωπιστεί πριν τα δεδομένα αποσταλούν εκτός του οργανισμού. [60-61]

Δεδομένα σε κίνηση

Τα δεδομένα σε κίνηση είναι δεδομένα που αποστέλλονται εντός του εσωτερικού δικτύου ενός οργανισμού ή σε ένα εξωτερικό δίκτυο. Τα συστήματα πρόληψης απώλειας δεδομένων τοποθετούνται σε σημεία του δικτύου και χρησιμοποιούνται για τον εντοπισμό και τον έλεγχο δεδομένων που μεταφέρονται στο δίκτυο ή σε κάποιο εξωτερικό δίκτυο. [60-61]

Η απώλεια δεδομένων μπορεί να περιοριστεί με τους παρακάτω τρόπους:

Ανάλυση περιβάλλοντος

Αυτή η τεχνική λαμβάνει υπόψη τα μεταδεδομένα που συνδέονται με τα ευαίσθητα δεδομένα χωρίς να δίνει ιδιαίτερη σημασία στα δεδομένα καθαυτά. Εάν ένας χρήστης προσπαθήσει να στείλει δεδομένα σε μια άλλη οντότητα, θα αναλυθούν συγκεκριμένα χαρακτηριστικά, όπως το μέγεθος, η πηγή, ο προορισμός και η μορφή του αρχείου [61], και ανάλογα το σύστημα θα αποφασίσει αν θα επιτρέψει αυτή την ενέργεια ή όχι με βάση πολιτικές που εκφράζονται μέσω αυτών των χαρακτηριστικών περιβάλλοντος.

Ανάλυση περιεχομένου

Αυτή η τεχνική λαμβάνει υπόψη μόνο τα ευαίσθητα δεδομένα και όχι το υπόλοιπο περιβάλλον και χωρίζεται σε τρεις υποκατηγορίες. Οι τεχνικές ανάλυσης περιεχομένου είναι: η χρήση αποτυπώματος δεδομένων (συμπεριλαμβανομένης της ακριβούς ή μερικής αντιστοίχισης), η χρήση κανονικών εκφράσεων (συμπεριλαμβανομένης της αντιστοίχισης με βάση λεξικό) και η στατιστική ανάλυση.

- *Αποτύπωμα δεδομένων (fingerprint)*: Αυτή είναι η πιο συνηθισμένη τεχνική που χρησιμοποιείται για την αποφυγή απώλειας δεδομένων. Ένα αποτύπωμα είναι η τιμή κατακερματισμού ενός συνόλου δεδομένων όπου οι τιμές κατακερματισμού όλων των ευαίσθητων δεδομένων αποθηκεύονται σε βάσεις δεδομένων. Όταν εντοπιστεί δραστηριότητα το σύστημα συγκρίνει αυτά τα (αποθηκευμένα) αποτυπώματα με τα αντίστοιχα αποτυπώματα των δεδομένων πάνω στα οποία προσπαθεί να πραγματοποιηθεί κάποια ενέργεια. Όταν τα δύο αποτυπώματα είναι τα ίδια τότε πρόκειται για ευαίσθητα δεδομένα και το σύστημα μπλοκάρει την οποιαδήποτε ενέργεια πάνω σε αυτά. [62]
- *Κανονικές εκφράσεις και λέξεις κλειδιά (regular expressions and keywords)*: Αυτή η τεχνική αναγνωρίζει δομημένα δεδομένα δηλαδή δεδομένα που έχουν συγκεκριμένο μήκος και μορφή, με κανονικές εκφράσεις και με λέξεις-κλειδιά [63]. Οι κανονικές εκφράσεις χρησιμοποιούνται κυρίως για την αναγνώριση δεδομένων ανά τύπο, π.χ. αριθμούς πιστωτικών καρτών, αριθμούς τηλεφώνων, ΑΦΜ, κ.α. Η αντιστοίχιση λέξεων-κλειδιών χρησιμοποιείται στην περίπτωση κατά την οποία ένας μικρός αριθμός γνωστών λέξεων-κλειδιών, που ενδεχομένως να είναι ειδικευμένος σε έναν συγκεκριμένο τομέα (π.χ. ιατρικοί όροι), μπορεί να χρησιμοποιηθεί για τον εντοπισμό ευαίσθητων δεδομένων. Ένα παράδειγμα θα μπορούσε να είναι οι λέξεις πατρώνυμο και ημερομηνία γέννησης, οι οποίες παραπέμπουν στην ταυτότητα.
- *Στατιστική ανάλυση*: Αυτή η τεχνική χρησιμοποιεί στατιστικά δεδομένα, όπως η συχνότητα εμφάνισης ενός όρου μέχρι το επίπεδο μιας λέξης σε ένα κείμενο, και μεθόδους μηχανικής μάθησης ώστε να εντοπίσει τα ευαίσθητα δεδομένα. Χρειάζεται μεγάλος όγκος δεδομένων για να εκπαιδευτεί το σύστημα αλλά είναι μια χρήσιμη τεχνική στην περίπτωση που κάποια άλλη τεχνική δεν μπορεί να αποφασίσει εάν ορισμένα δεδομένα είναι ευαίσθητα και πρέπει να προστατευθούν [61]. Συνεπώς, μπορεί να καλύψει ένα μεγαλύτερο υποσύνολο από τα ευαίσθητα/εμπιστευτικά δεδομένα σε σχέση με τις άλλες 2 τεχνικές.

4.2.6 Κρυπτογράφηση (Encryption)

Σύμφωνα με το NIST ως κρυπτογράφηση ορίζεται η μετατροπή δεδομένων (plaintext) σε μία μορφή (cipher text) η οποία αποκρύπτει την πραγματική σημασία των δεδομένων αυτών ώστε να μη μπορούν να γνωστοποιηθούν. Όταν η μετατροπή γίνεται αντίστροφα, η αντίστοιχη διαδικασία ονομάζεται αποκρυπτογράφηση και πραγματοποιείται για να μετατρέψει τα κρυπτογραφημένα δεδομένα στην αρχική τους μορφή. Υπάρχουν τρεις βασικές κατηγορίες κρυπτογράφησης, η συμμετρική κρυπτογράφηση ή

αλλιώς κρυπτογράφηση ιδιωτικού κλειδιού, η ασύμμετρη κρυπτογράφηση ή αλλιώς κρυπτογράφηση δημοσίου κλειδιού και τέλος η υβριδική κρυπτογράφηση. [64]

Για να γίνει κατανοητό πως λειτουργούν αυτές οι τρεις μέθοδοι πρέπει πρώτα να γίνουν κατανοητές κάποιες βασικές έννοιες, οι οποίες περιγράφονται παρακάτω.

- *Απλό κείμενο (plaintext)*: Τα δεδομένα τα οποία είναι σε μια αρχική (κατανοητή) μορφή και πρόκειται να κρυπτογραφηθούν [65].
- *Κρυπτογραφημένο κείμενο (ciphertext)*: Η νέα "ακατανόητη" μορφή στην οποία βρίσκονται τα δεδομένα αφού κρυπτογραφηθούν [65].
- *Κλειδί (key)*: ένας αριθμός που αποτελείται από κάποια ψηφία και χρησιμοποιείται σαν είσοδος στη συνάρτηση κρυπτογράφησης. Χρησιμοποιώντας ένα ή δύο κλειδιά κρυπτογραφείται και αποκρυπτογραφείται απλό κείμενο [65].
- *Κρυπτογραφικός αλγόριθμος (cipher)*: η μαθηματική συνάρτηση/αλγόριθμος που χρησιμοποιεί το κλειδί ως είσοδο (input) για να κρυπτογραφηθεί το απλό κείμενο δηλαδή να αλλάξει / μετασχηματίσει το περιεχόμενό του [65].

Συμμετρική κρυπτογράφηση

Στη συμμετρική κρυπτογράφηση χρησιμοποιείται ένα μοναδικό μυστικό κλειδί, τόσο για την κρυπτογράφηση όσο και την αποκρυπτογράφηση απλού κειμένου (plaintext), το οποίο γνωρίζουν μόνο ο αποστολέας και ο παραλήπτης. Τα πλεονεκτήματα αυτής της μεθόδου είναι ο υψηλός ρυθμός κρυπτογράφησης, δηλαδή μπορεί να κρυπτογραφηθεί μεγάλος όγκος δεδομένων σε μικρό χρονικό διάστημα, και οι μικρές απαιτήσεις σε υπολογιστικούς πόρους και ενέργεια, κάτι που μεταφράζεται σε μικρότερο οικονομικό κόστος. Από την άλλη πλευρά, το μεγαλύτερο μειονέκτημα αυτής της μεθόδου είναι ότι το μυστικό κλειδί θα πρέπει να διαμοιραστεί με ασφάλεια και να διατηρηθεί ασφαλές και από τις δύο πλευρές (αποστολέα και παραλήπτη) καθώς πιθανή διαρροή/απώλεια του σημαίνει δυνατότητα για αποκρυπτογράφηση των δεδομένων. Επίσης, αν η ίδια πληροφορία μεταφέρεται από τον έναν χρήστη σε πολλούς, τότε θα πρέπει να δημιουργηθούν τόσα κλειδιά όσοι οι παραλήπτες. [66]

Ο πιο ευρέως χρησιμοποιούμενος αλγόριθμος συμμετρικής κρυπτογράφησης είναι ο AES (Advanced Encryption Standard) και ανήκει στην κατηγορία αλγορίθμων κρυπτογράφησης δέσμης (block ciphers), δηλαδή χωρίζει το κείμενο που θα κρυπτογραφηθεί σε κομμάτια και το κάθε κομμάτι κρυπτογραφείται ξεχωριστά. Είναι μία παραλλαγή του παλαιότερου αλγορίθμου Rijndael και αντικαταστάτης του παλαιότερου αλγορίθμου DES (Data Encryption Standard). Στον AES κάθε δέσμη (block) κειμένου προς κρυπτογράφηση έχει μήκος 128 bit και τα κλειδιά μπορούν να έχουν μήκος 128 (AES-128),192 (AES-192) και 256 bits (AES-256). [67]

Εκτός από τους αλγορίθμους κρυπτογράφησης δέσμης που αναφέρονται παραπάνω υπάρχουν και οι αλγόριθμοι κρυπτογράφησης ροής (stream ciphers), οι οποίοι χωρίζουν το κείμενο που θα

κρυπτογραφηθεί γράμμα προς γράμμα σε δυαδικά ψηφία (bits) και έτσι δημιουργείται μία ροή. Τα ψηφία του κειμένου προς κρυπτογράφηση (plaintext) συνδυάζονται με μια ροή ψηφίων (keystream) του κρυπτογραφικού αλγορίθμου (cipher) και χρησιμοποιώντας την συνάρτηση XOR προκύπτει το κρυπτογραφημένο κείμενο. Τα πλεονεκτήματά των αλγορίθμων κρυπτογράφησης ροής είναι ότι είναι πιο γρήγοροι σε σχέση με τους αλγορίθμους κρυπτογράφησης δέσμης και απαιτούν λιγότερους πόρους καθώς κρυπτογραφείται ένα δυαδικό ψηφίο κάθε φορά ενώ σε περίπτωση που υπάρξει κάποιο πρόβλημα κατά την κρυπτογράφηση επηρεάζεται μόνο ένα bit και όχι ολόκληρο το τμήμα ενός κειμένου. Τέλος, στο κομμάτι της ασφάλειας και οι δύο εξαρτώνται από το μήκος των κλειδιών, άρα δεν μπορούμε να πούμε ότι μία κατηγορία είναι πιο ασφαλής από την άλλη. Από την παραπάνω ανάλυση, φαίνεται, λοιπόν, ότι τελικά οι καλύτεροι είναι οι αλγόριθμοι κρυπτογράφησης ροής. [68]

Ασύμμετρη κρυπτογράφηση

Στην ασύμμετρη κρυπτογράφηση χρησιμοποιείται ένα ζεύγος κλειδιών, το δημόσιο κλειδί, το οποίο χρησιμοποιείται για την κρυπτογράφηση του κειμένου και μπορεί να είναι γνωστό δημοσίως, και το ιδιωτικό κλειδί, το οποίο χρησιμοποιείται για την αποκρυπτογράφηση του κρυπτογραφημένου μηνύματος και θα πρέπει να παραμένει μυστικό. Αυτά τα δύο κλειδιά είναι διαφορετικά μεταξύ τους, γνωρίζοντας το ένα δε μπορεί να βρεθεί το άλλο οπότε θα λέγαμε ότι το ένα συμπληρώνει το άλλο αφού όταν κρυπτογραφηθούν δεδομένα με ένα δημόσιο κλειδί μπορούν να αποκρυπτογραφηθούν μόνο με το “δικό του” ιδιωτικό κλειδί [69]. Το πλεονέκτημα που έχει αυτή η μέθοδος είναι ότι σε αντίθεση με τη συμμετρική κρυπτογράφηση, το ιδιωτικό κλειδί, το οποίο πρέπει να παραμείνει μυστικό, δε χρειάζεται να μεταφερθεί ανάμεσα στον αποστολέα και τον παραλήπτη. Το μειονέκτημα αυτής της τεχνικής είναι ότι είναι πιο σύνθετη, κατά συνέπεια πιο αργή, με μεγαλύτερες απαιτήσεις σε πόρους και πιο δαπανηρή [66].

Ο πιο ευρέως χρησιμοποιούμενος αλγόριθμος συμμετρικής κρυπτογράφησης είναι ο RSA (Rivest Shamir Adleman), στηρίζεται στη θεωρία αριθμών και πιο συγκεκριμένα στη δυσκολία ανάλυσης ενός αριθμού σε γινόμενο πρώτων παραγόντων. Δημιουργείται ένα ζεύγος κλειδιών, το δημόσιο κλειδί προκύπτει από το γινόμενο δύο πρώτων αριθμών και έναν ακόμα αριθμό που προκύπτει με μαθηματικές πράξεις και το ιδιωτικό κλειδί μπορεί να προκύψει μόνο αν κάποιος γνωρίζει τους δύο πρώτους αριθμούς που χρησιμοποιήθηκαν. [70]

Υβριδική κρυπτογράφηση

Η υβριδική κρυπτογράφηση συνδυάζει τις δύο παραπάνω τεχνικές και εκμεταλλεύεται τα πλεονεκτήματά τους. Παρακάτω περιγράφονται τα βήματα της διαδικασίας.

1. Ένα απλό κείμενο (plaintext) κρυπτογραφείται χρησιμοποιώντας ένα μυστικό κλειδί που παράγεται αυτόματα για κάθε διαφορετική κρυπτογράφηση [66, 71].

2. Αυτό το μυστικό κλειδί κρυπτογραφείται χρησιμοποιώντας το δημόσιο κλειδί του παραλήπτη. Έτσι λοιπόν έχουν δημιουργηθεί δύο κρυπτογραφημένα μέρη (το αρχικό κείμενο και το μυστικό κλειδί) τα οποία αποστέλλονται στον παραλήπτη σαν ένας φάκελος [66, 71].
3. Ο παραλήπτης χρησιμοποιεί το ιδιωτικό του κλειδί για να αποκρυπτογραφήσει το μυστικό κλειδί του κρυπτογραφημένου μηνύματος [66, 71].
4. Στη συνέχεια χρησιμοποιεί το μυστικό κλειδί του κρυπτογραφημένου μηνύματος για να αποκρυπτογραφήσει το κρυπτογραφημένο μήνυμα [66, 71].

Στην υβριδική κρυπτογράφηση το μυστικό κλειδί κρυπτογραφείται συνεπώς δε μπορεί να το αξιοποιήσει κάποιος ενδιάμεσος και είναι πολύ δύσκολο να διαρρεύσει. Επιπλέον, δεν απαιτείται ανταλλαγή πληροφορίας για την παραγωγή του άρα υπάρχει περισσότερη ασφάλεια. Τέλος, έχει λυθεί το πρόβλημα της χρονικής καθυστέρησης για κρυπτογράφηση μεγάλου όγκου δεδομένων με ασύμμετρη κρυπτογράφηση αφού πλέον η ασύμμετρη κρυπτογράφηση χρησιμοποιείται για να κρυπτογραφήσει το μυστικό κλειδί των δεδομένων και όχι τα ίδια τα δεδομένα, τα οποία κρυπτογραφούνται με την πιο ταχεία μέθοδο κρυπτογράφησης [66, 71].

Το πρωτόκολλο Kerberos χρησιμοποιεί συμμετρική κρυπτογράφηση, το πρωτόκολλο SSH (Secure Shell) χρησιμοποιεί ασύμμετρη κρυπτογράφηση και το πρωτόκολλο PGP (Pretty Good Privacy) χρησιμοποιεί υβριδική κρυπτογράφηση. Τα πρωτόκολλα IPSec και TLS / SSL (Transport Layer Security / Secure Sockets Layer) χρησιμοποιούν ασύμμετρη κρυπτογράφηση για να ξεκινήσει μία σύνοδος (session) και έπειτα χρησιμοποιούν συμμετρική κρυπτογράφηση για την ανταλλαγή πληροφοριών.

4.2.7 Ασφάλεια ηλεκτρονικού ταχυδρομείου (Email Security)

Το ηλεκτρονικό ταχυδρομείο πλέον δεν αποτελεί μόνο ένα από τα πολλά μέσα επικοινωνίας για μια επιχείρηση ή έναν οργανισμό αλλά είναι ένα άκρως απαραίτητο συστατικό για τη σωστή λειτουργία του. Είναι, λοιπόν, απαραίτητο να παραμένει ασφαλές καθώς οι συνέπειες μιας επίθεσης μπορεί να είναι καταστροφικές. Η ασφάλεια ηλεκτρονικού ταχυδρομείου ορίζεται ως ένα σύνολο διαφορετικών διαδικασιών και τεχνικών για την προστασία των λογαριασμών ηλεκτρονικού ταχυδρομείου, του περιεχομένου και της επικοινωνίας από μη εξουσιοδοτημένη πρόσβαση, απώλεια ή παραβίαση (compromise) [72]. Οι τεχνικές αυτές περιλαμβάνουν την προστασία από ηλεκτρονικό ψάρεμα (phishing), όπου πληροφορίες σχετικά με αυτού του είδους προστασία βρίσκονται στο Κεφάλαιο 3, την προστασία από ανεπιθύμητη αλληλογραφία (spam), την δυνατότητα χρήσης ψηφιακών υπογραφών (digital signatures) και την κρυπτογράφηση [73], όπου πληροφορίες σχετικά με αυτήν βρίσκονται στην Ενότητα 4.2.6.

<u>Ανεπιθύμητη αλληλογραφία (Spam)</u>

Σύμφωνα με τη Wikipedia ως ανεπιθύμητη αλληλογραφία θεωρούνται τα ανεπιθύμητα μηνύματα ηλεκτρονικού ταχυδρομείου που αποστέλλονται, χρησιμοποιώντας συστήματα ανταλλαγής μηνυμάτων, σε μεγάλο αριθμό παραληπτών για διάφορους σκοπούς όπως: την εμπορική διαφήμιση, εμπορικό

προσηλυτισμό, απαγορευμένους σκοπούς ή απλά την επαναλαμβανόμενη αποστολή ενός μηνύματος στον ίδιο χρήστη. [74]

Η ανεπιθύμητη αλληλογραφία αντιμετωπίζεται χρησιμοποιώντας κατάλληλα φίλτρα, τα οποία διαχωρίζουν τα μηνύματα ηλεκτρονικού ταχυδρομείο σε επιθυμητά και μη επιθυμητά και τα διαχειρίζονται ανάλογα. Το τελευταίο σημαίνει πως ένα επιθυμητό μήνυμα φτάνει κανονικά στον παραλήπτη του ενώ ένα ανεπιθύμητο μήνυμα μπορεί είτε να καταλήξει στον αντίστοιχο φάκελο ανεπιθύμητων μηνυμάτων του παραλήπτη είτε να διαγραφεί αυτόματα. Παρακάτω παρουσιάζονται τα είδη των φίλτρων αυτών.

- *Φίλτρα περιεχομένου (content filters)*: Τα φίλτρα περιεχομένου διαχωρίζουν την αλληλογραφία σε επιθυμητή και ανεπιθύμητη βασιζόμενα σε λέξεις-κλειδιά, στις επισυναπτόμενες εικόνες και τα τμήματα ενός κειμένου και χρησιμοποιώντας είτε απλές είτε πολύπλοκες τεχνικές φιλτραρίσματος από την περιοχή της Ανάκτησης Πληροφορίας (Information Retrieval). Το πλεονέκτημά τους είναι πως μπορούν να ρυθμιστούν, αν και δύσκολα, με ακρίβεια ώστε να εντοπίζουν το κατάλληλο περιεχόμενο και το μειονέκτημά τους είναι ότι χρειάζονται διαρκή ενημέρωση καθώς είναι εύκολο να παρακαμφθούν εάν ο αποστολέας του (ανεπιθύμητου) μηνύματος τροποποιήσει τις λέξεις κλειδιά χρησιμοποιώντας, π.χ. ειδικούς χαρακτήρες ($p@m αντί της λέξης spam). [75]
- *Φίλτρα περιεχομένου Bayes (Bayes content filters)*: Πρόκειται για ένα φίλτρο περιεχομένου το οποίο δεν αναλύει λέξεις μία προς μία αλλά εκπαιδεύεται ανάλογα με το περιεχόμενο των μηνυμάτων, το οποίο συνήθως δέχεται ένας χρήστης, και λειτουργεί ανάλογα. Η εκπαίδευση γίνεται χειροκίνητα από τον χρήστη, ο οποίος υποδεικνύει ποια μηνύματα είναι ανεπιθύμητα και ποια όχι. Έτσι το φίλτρο δημιουργεί λίστες με επιθυμητές και ανεπιθύμητες λέξεις, οι οποίες συνεχώς εμπλουτίζονται με την ανάλυση νέων (εισερχόμενων) μηνυμάτων. Όταν λοιπόν φτάσει ένα μήνυμα προς εξέταση, ανάλογα με το αν οι λέξεις του αντιστοιχίζονται περισσότερο με τη λίστα επιθυμητών ή ανεπιθύμητων λέξεων, του δίνεται ο αντίστοιχος χαρακτηρισμός [76]. Για παράδειγμα, όταν ένας φοιτητής πληροφορικής δέχεται ενημερωτικά μηνύματα για επιστημονικά συνέδρια πληροφορικής το φίλτρο “μαθαίνει” να τα θεωρεί επιθυμητά ενώ αντίστοιχα αν το ίδιο μήνυμα αποσταλεί σε έναν γυμναστή, ο οποίος υπό φυσιολογικές συνθήκες δεν δέχεται τέτοιου είδους μηνύματα, θα θεωρηθεί ανεπιθύμητο. Το πλεονέκτημα αυτού του φίλτρου είναι πως μπορεί να προσαρμοστεί σε κάθε χρήστη μεμονωμένα και το μειονέκτημά του πως δεν μπορεί να δουλέψει απόλυτα σωστά πάνω σε διακομιστές με πολύ μεγάλο αριθμό μηνυμάτων. Αυτό συμβαίνει διότι οι αποστολείς των μηνυμάτων προσθέτουν λέξεις ώστε να μεγαλώνει αρκετά το κείμενο του μηνύματος και το ποσοστό των “ανεπιθύμητων” λέξεων να παραμένει αρκετά χαμηλό και σαν αποτέλεσμα το μήνυμα να διαβάζεται σαν επιθυμητό [76]. Συνεπώς όσο μεγαλύτερος είναι ο όγκος των μεγάλων μηνυμάτων σε έναν διακομιστή τόσο περισσότερα θα είναι και τα ανεπιθύμητα μηνύματα τα οποία θα διαβαστούν ως επιθυμητά εφόσον δεν είναι κατάλληλη η αντιμετώπιση των μεγάλων, ανεπιθύμητων μηνυμάτων.
- *Graylisting*: Αυτή η τεχνική βασίζεται στην παραδοχή ότι τα μηνύματα ηλεκτρονικού ταχυδρομείου αποστέλλονται μαζικά από μηχανήματα τα οποία εξυπηρετούν μόνο αυτό τον σκοπό. Πιο

συγκεκριμένα, όταν ένα μηχάνημα στέλνει μαζικά μηνύματα ηλεκτρονικού ταχυδρομείου και αυτά δεν γίνονται δεκτά από τον αποστολέα τότε δεν τα στέλνει ξανά για δεύτερη φορά, ενώ αντιθέτως τα "πραγματικά" συστήματα (ηλεκτρονικού ταχυδρομείου) λειτουργούν με την πολιτική της επαναποστολής (χωρίς την επέμβαση του χρήστη-αποστολέα). Έτσι λοιπόν αυτή η τεχνική μπλοκάρει τα μηνύματα την πρώτη φορά που έρχονται, περιμένει να σταλούν ξανά και όταν έρθουν τότε τα εγκρίνει σαν επιθυμητά. Αυτό γίνεται ώστε να εντοπιστεί εάν το μήνυμα προέρχεται από πραγματικό ή κακόβουλο χρήστη. Τα μειονεκτήματα της τεχνικής αυτής είναι ότι δημιουργούνται καθυστερήσεις και οπότε αυτή δεν είναι αποδεκτή από πολλά άτομα. Επιπλέον, αν ένα κακόβουλο σύστημα προσομοιώσει την συμπεριφορά ενός εξυπηρετητή ηλεκτρονικού ταχυδρομείου, τότε θα στείλει ξανά τα μαζικά μηνύματα. Οπότε, το πρόβλημα ουσιαστικά δεν θα αντιμετωπιστεί και θα υπάρχει επιπλέον και καθυστέρηση στην λήψη των μηνυμάτων. [77]

- *Φίλτρα κεφαλίδων (header filters)*: Τα φίλτρα κεφαλίδων αναλύουν τις κεφαλίδες των μηνυμάτων ώστε να εντοπίσουν τυχόν λάθη και έτσι να μαρκάρουν το αντίστοιχο μήνυμα ως ανεπιθύμητο [78]. Τα λάθη υπάρχουν διότι οι αποστολείς μηνυμάτων ανεπιθύμητης αλληλογραφίας τροποποιούν τις κεφαλίδες των μηνυμάτων, οι οποίες περιέχουν τις απαραίτητες πληροφορίες για το μήνυμα, με σκοπό να μην γίνουν αντιληπτοί. Ένα παράδειγμα είναι το να υπάρχει διαφορετική διεύθυνση στο πεδίο για τον αποστολέα του μηνύματος (from) και στο πεδίο για τον παραλήπτη (reply to) στον οποίο θα καταλήξει η απάντηση στο μήνυμα με αποτέλεσμα η απάντηση του χρήστη σε αυτό το μήνυμα να μην καταλήγει στον αποστολέα του μηνύματος άλλα σε κάποιον άλλο χρήστη. Αυτές οι τροποποιήσεις έχουν σαν αποτέλεσμα πολλές φορές να μην τηρείται το πρότυπο [79] RFC 5322 [80], το οποίο χρησιμοποιείται για τις κεφαλίδες μηνυμάτων ηλεκτρονικού ταχυδρομείου. Το πλεονέκτημα αυτής της μεθόδου είναι ότι είναι αρκετά αξιόπιστη καθώς στηρίζεται σε ένα παγκόσμιο πρότυπο και το μειονέκτημά της είναι ότι μπορεί να εντοπίζει ανεπιθύμητα μηνύματα μόνο από αποστολείς που κάνουν αυτά τα λάθη (μικρότερη ακρίβεια ανάκλησης - recall), τα οποία μπορεί να μην είναι εσκεμμένα και άρα να πραγματοποιούνται από μη κακόβουλους χρήστες (μικρότερο precision).
- *Φίλτρα μαύρης λίστας (blacklist filter)*: Αυτά τα φίλτρα αντιμετωπίζουν τα ανεπιθύμητα μηνύματα ηλεκτρονικού ταχυδρομείου μπλοκάροντας συνήθως διευθύνσεις email και σε ορισμένες περιπτώσεις ονόματα τομέων και IPs εφόσον αποτελούν πηγές ανεπιθύμητων μηνυμάτων. Για να ελεγχθεί αν μια πηγή μηνυμάτων είναι ανεπιθύμητη αναζητείται μέσα σε λίστες που διατίθενται δημόσια από παρόχους/οργανισμούς (π.χ. Spamhaus, Spam Comp, Barracuda), οι οποίες περιλαμβάνουν διευθύνσεις που έχουν χαρακτηριστεί ως ανεπιθύμητες. Έτσι, λοιπόν, όταν φτάνει ένα μήνυμα ηλεκτρονικού ταχυδρομείου από αποστολέα που βρίσκεται σε αυτή τη λίστα είτε τοποθετείται στο φάκελο ανεπιθύμητων μηνυμάτων είτε απορρίπτεται ανάλογα με την αυστηρότητα που επιθυμεί ο χρήστης (ή γενικότερα ο διαχειριστής ασφάλειας) [81]. Το πλεονέκτημα αυτής της μεθόδου είναι πως μπορεί να φιλτράρει όλα τα εισερχόμενα μηνύματα με ακρίβεια χωρίς κάποιο να διαφύγει του ελέγχου και το μειονέκτημά της είναι πως μπορεί να έχει

μικρή κάλυψη ακόμη και αν χρησιμοποιηθούν πολλαπλές μαύρες λίστες [82]. Μια παραλλαγή αυτής της τεχνικής είναι το μπλοκάρισμα με βάση τη χώρα του αποστολέα [83]. Οι λίστες που αναφέρονται παραπάνω υπάρχουν ελεύθερα στο διαδίκτυο (π.χ. rbl.mailspike.org) ενώ υπάρχουν και μηχανές αναζήτησης (π.χ. https://mxtoolbox.com/blacklists.aspx) όπου κάποιος χρήστης μπορεί να ελέγξει αν η IP διεύθυνσή του βρίσκεται σε μαύρη λίστα.

Ηλεκτρονικό ψάρεμα (Phishing)

Στο ηλεκτρονικό ψάρεμα το οποίο πραγματοποιείται κατά κόρον μέσω ηλεκτρονικού ταχυδρομείου, όπως έχει αναφερθεί και στο Κεφάλαιο 3, ο επιτιθέμενος προσποιείται μια έμπιστη οντότητα, συνήθως στέλνοντας κάποιο αληθοφανές μήνυμα ηλεκτρονικού ταχυδρομείου (δόλωμα), με σκοπό να εξαπατήσει το θύμα και να αποκτήσει προσωπικά του στοιχεία (π.χ. κωδικούς πρόσβασης). Οι τεχνικές αντιμετώπισης της ηλεκτρονικής αλληλογραφίας που έχει ως στόχο το ηλεκτρονικό ψάρεμα μοιάζουν με τις τεχνικές αντιμετώπισης των ανεπιθύμητων μηνυμάτων που αναφέρονται παραπάνω και αναλύονται παρακάτω.

- *Ενιαίοι Εντοπιστές Πόρων (URLs) βασισμένοι στις διευθύνσεις IP*: Πολλές φορές τα μηνύματα ηλεκτρονικού ταχυδρομείου που έχουν ως στόχο το ηλεκτρονικό ψάρεμα περιέχουν συνδέσμους, οι οποίοι χρησιμοποιούν την IP διεύθυνση τους και όχι έναν διακομιστή συστήματος ονομάτων τομέων (DNS server). Όταν λοιπόν ένα μήνυμα ηλεκτρονικού ταχυδρομείου περιέχει έναν τέτοιο σύνδεσμο είναι από πολύ σπάνιο έως αδύνατον να προέρχεται από κάποια “νόμιμη” οντότητα και συνεπώς θεωρείται ύποπτο. [84]
- *Μηνύματα ηλεκτρονικού ταχυδρομείου που περιέχουν Γλώσσα Σήμανσης Υπερκειμένου (HTML)*: Τα μηνύματα ηλεκτρονικού ταχυδρομείου αποτελούνται είτε από απλό κείμενο, είτε από συνδυασμό απλού κειμένου μαζί με τμήματα γλώσσας σήμανσης υπερκειμένου (HTML). Όταν ένα μήνυμα ηλεκτρονικού ταχυδρομείου περιέχει κομμάτια γλώσσας σήμανσης υπερκειμένου (HTML) δεν σημαίνει απαραίτητα ότι έχει ως στόχο το ηλεκτρονικό ψάρεμα αλλά είναι άξιο προσοχής διότι χρησιμοποιώντας γλώσσα σήμανσης υπερκειμένου μπορεί να παραμείνει κρυφό το “ασυνήθιστο” τμήμα ενός συνδέσμου, ο οποίος με μία πρώτη ματιά φαίνεται φυσιολογικός. [84]
- *Ενιαίοι Εντοπιστές Πόρων (URLs) χωρίς αντιστοιχία*: Στα μηνύματα ηλεκτρονικού ταχυδρομείου, τα οποία περιέχουν γλώσσας σήμανσης υπερκειμένου (HTML), πραγματοποιείται έλεγχος για να διαπιστωθεί εάν υπάρχει κάποιος σύνδεσμος ο οποίος οδηγεί σε μια άλλη ιστοσελίδα από αυτήν που εμφανίζεται σε αυτό, ενδεχομένως επιβλαβή, μέσω της γλώσσας σήμανσης υπερκειμένου και χωρίς αυτό να γίνεται ξεκάθαρο προς τον χρήστη. Κάτι τέτοιο μπορεί να συμβεί χρησιμοποιώντας την ετικέτα href [84]. Στο παρακάτω παράδειγμα ο χρήστης θα βλέπει έναν σύνδεσμο με τίτλο “https://www.icsd.com“ αλλά μόλις πατήσει πάνω θα ανακατευθυνθεί στην ιστοσελίδα "https://www.icsd16087.com" : ** https://www.icsd.com **

Η παρούσα τεχνική σε συνδυασμό με τις δύο παραπάνω τεχνικές είναι συμπληρωματικές και μπορούν να χρησιμοποιηθούν ταυτόχρονα. Σε ορισμένες περιπτώσεις η ταυτόχρονη χρήση τους μπορεί να οδηγήσει σε περισσότερη ακρίβεια. Παραδείγματος χάριν, στο παράδειγμα που αναφέρεται παραπάνω έστω ότι ο σύνδεσμος με τίτλο "https://www.icsd.com" είχε σταλεί μέσω ενός μηνύματος ηλεκτρονικού ταχυδρομείου το οποίο περιείχε γλώσσα HTML από έναν αποστολέα με διεύθυνση IP αντί για κάποιο όνομα. Τότε θα υπήρχε μία πρώτη ένδειξη ότι κάτι περίεργο συμβαίνει αφού η διεύθυνση ηλεκτρονικού ταχυδρομείου του είναι μία IP διεύθυνση και όχι κάποιο όνομα, η δεύτερη ένδειξη θα ήταν η ύπαρξη γλώσσας html μέσα στο κείμενο και η τρίτη και τελευταία ένδειξη θα ήταν ο εντοπισμός της ανακατεύθυνσης. Είναι λοιπόν φανερό ότι ο συνδυασμός αυτών των τεχνικών ξεκάθαρα λειτουργεί πιο αποτελεσματικά σε σχέση με την περίπτωση που θα είχε χρησιμοποιηθεί μόνο μία τεχνική.

- *Αριθμός από τελείες ("."*): Πολλές φορές στα μηνύματα ηλεκτρονικού ταχυδρομείου περιέχονται κακόβουλοι σύνδεσμοι, οι οποίοι θα πρέπει να δείχνουν νόμιμοι. Ένας τρόπος για να γίνει αυτό είναι να κατασκευάζονται ενιαίοι εντοπιστές πόρων (URLs) με μεγάλο μήκος όπου ενώ το αρχικό τους κομμάτι μοιάζει φυσιολογικό στη συνέχεια χρησιμοποιούνται πολλοί υποτομείς (subdomains) ή γίνεται ανακατεύθυνση σε άλλες ιστοσελίδες. Για αυτό το λόγο σύνδεσμοι με πολλές τελείες (συνήθως πέντε ή περισσότερες) θεωρούνται ύποπτοι. [84]
- *Μηνύματα ηλεκτρονικού ταχυδρομείου που περιέχουν κώδικα Javascript*: Τα μηνύματα ηλεκτρονικού ταχυδρομείου στα οποία εντοπίζεται κώδικας Javascript είτε στο κυρίως μέρος τους είτε σε κάποιον σύνδεσμο θεωρούνται ύποπτα καθώς μέσω αυτού του κώδικα μπορούν να πραγματοποιηθούν κακόβουλες ενέργειες, οι οποίες μπορεί να περιλαμβάνουν από μία ανακατεύθυνση σε κάποια ιστοσελίδα με στόχο το ηλεκτρονικό ψάρεμα έως μία κακόβουλη επίθεση με στόχο κάποιον χρήστη ή κάποιο μηχάνημα. [84]

Ψηφιακές Υπογραφές

Οι ψηφιακές υπογραφές στηρίζονται στην ασύμμετρη κρυπτογράφηση και χρησιμοποιούνται για να αποδειχθεί η γνησιότητα ενός εγγράφου, δηλαδή ότι το έστειλε ο πραγματικός αποστολέας του και ότι το περιεχόμενό του είναι ίδιο με αυτό που έστειλε ο αποστολέας χωρίς να γίνει κάποια αλλαγή κατά τη μεταφορά. Για να πραγματοποιηθεί αυτή η διαδικασία εκτός από τα κλειδιά ασύμμετρης κρυπτογράφησης, όπου εξηγείται στο προηγούμενο κεφάλαιο πως λειτουργούν, χρησιμοποιείται και μία συνάρτηση κατακερματισμού (hash function), δηλαδή μία συνάρτηση η οποία αντιστοιχίζει δεδομένα οποιουδήποτε μήκους (στην περίπτωσή μας τα δεδομένα αυτά είναι οι συμβολοσειρές του εγγράφου) σε μοναδικές τιμές σταθερού μήκους. [85]

Η διαδικασία που ακολουθείται είναι η εξής:

- Ο αποστολέας χρησιμοποιώντας κάποιον αλγόριθμο κερματισμού δημιουργεί μία σύνοψη δηλαδή έναν αριθμό σταθερού μήκους που προέκυψε από τον κατακερματισμό του εγγράφου [86].

- Με το ιδιωτικό του κλειδί κρυπτογραφεί αυτή τη σύνοψη και έτσι δημιουργείται η ψηφιακή υπογραφή [86].
- Στέλνει στον παραλήπτη το αρχικό έγγραφο μαζί με την ψηφιακή υπογραφή [86].
- Ο παραλήπτης χρησιμοποιώντας το δημόσιο κλειδί του αποστολέα αποκρυπτογραφεί την ψηφιακή υπογραφή και μπορεί πλέον να δει ποια είναι η σύνοψη. Αφού ο παραλήπτης καταφέρει να αποκρυπτογραφήσει χρησιμοποιώντας το δημόσιο κλειδί του αποστολέα έχει διασφαλιστεί και η ταυτότητά του αποστολέα αυτού, δηλαδή ότι αυτός έστειλε το μήνυμα [86].
- Στο έγγραφο που έλαβε αφαιρεί την ψηφιακή υπογραφή και εφαρμόζει τον ίδιο αλγόριθμο κατακερματισμού που εφάρμοσε ο αποστολέας στην αρχή. Εάν η σύνοψη που προκύπτει είναι ίδια με την σύνοψη που προέκυψε αποκρυπτογραφώντας την ψηφιακή υπογραφή τότε το έγγραφο δεν έχει τροποποιηθεί κατά τη μεταφορά του άρα διασφαλίζεται η ακεραιότητα [86].

4.2.8 Ασφάλεια δικτύου (Network Security)

Η ασφάλεια δικτύου περιλαμβάνει στις μεθόδους που χρησιμοποιούνται για την αντιμετώπισης της μη εξουσιοδοτημένης πρόσβασης σε ένα δίκτυο και γενικότερα για την προστασία των δεδομένων τα οποία μεταφέρονται μέσα στο δίκτυο αλλά και των τμημάτων από τα οποία αποτελείται το δίκτυο αυτό απέναντι στις επιθέσεις που μπορούν να πραγματοποιηθούν. Πιο συγκεκριμένα αυτή η κατηγορία περιλαμβάνει τα αναχώματα ασφαλείας και την προστασία από κατανεμημένες επιθέσεις άρνησης εξυπηρέτησης. Επιπλέον, στην ασφάλεια δικτύου συμμετέχουν και ορισμένες από τις υπόλοιπες υπηρεσίες που έχουν αναφερθεί σε αυτό το κεφάλαιο όπως το σύστημα διαχείρισης εισβολών (Ενότητα 4.2.3), το σύστημα διαχείρισης ταυτότητας και πρόσβασης (Ενότητα 4.2.4) και το σύστημα πρόληψης απώλειας δεδομένων (Ενότητα 4.2.5).

Αναχώματα ασφαλείας (firewalls)

Σύμφωνα με το NIST ένα ανάχωμα ασφαλείας ορίζεται ως μια δια-δικτυακή (inter-network) πύλη, η οποία περιορίζει την κίνηση των δεδομένων προς και από το δίκτυο που βρίσκεται "μέσα" στο ανάχωμα ασφαλείας και έτσι προστατεύει τους πόρους του δικτύου αυτού του συστήματος από απειλές προερχόμενες από το δίκτυο που βρίσκεται "έξω" από το ανάχωμα ασφαλείας. [87]

Τα αναχώματα ασφαλείας έχουν ως στόχο να προστατεύσουν τα δεδομένα και τους πόρους ενός οργανισμού από επιτιθέμενους, οι οποίοι βρίσκονται εκτός του οργανισμού, προστατεύοντας τα (δηλ. τα δεδομένα και τους πόρους) από μη εξουσιοδοτημένη πρόσβαση ενός επιτιθέμενου σε αυτά και από ενέργειες για μη εξουσιοδοτημένη έξοδο κάποιας πληροφορίας. Είναι υπεύθυνα για τη λήψη αποφάσεων σχετικά με το δίκτυο και πραγματοποιούν έλεγχο προσπέλασης αφού μέσα από αυτό περνά όλος ο όγκος των δεδομένων που μεταφέρονται από και προς το δίκτυο το οποίο προστατεύεται. Επιπλέον, έχουν τη δυνατότητα να προστατέψουν ένα μόνο τμήμα του εσωτερικού δικτύου, το οποίο ενδεχομένως

να είναι πιο ευαίσθητο από το τα υπόλοιπα, και να ορίσουν πως θα κατευθυνθεί η κίνηση του δικτύου. Τέλος, μπορούν να διατηρούν αρχεία καταγραφής της κίνησης του δικτύου και να αποκρύπτουν στοιχεία, όπως ονόματα συστημάτων, διευθύνσεις υπολογιστών και αναγνωριστικά χρηστών. [48]

Οι τρεις κατηγορίες αναχωμάτων ασφαλείας είναι (α) τα αναχώματα επιπέδου εφαρμογής, (β) τα αναχώματα επιπέδου μεταφοράς/δικτύου και (γ) τα υβριδικά αναχώματα

- *Αναχώματα ασφαλείας επιπέδου μεταφοράς/δικτύου*: Τα αναχώματα ασφαλείας επιπέδου μεταφοράς/δικτύου είναι δρομολογητές, οι οποίοι έχουν τη δυνατότητα να φιλτράρουν τα εισερχόμενα πακέτα και να εξετάζουν αν μπορούν και αν πρέπει να δρομολογηθούν προς τον προορισμό τους [48]. Το φιλτράρισμα αυτό γίνεται ελέγχοντας τις πληροφορίες που υπάρχουν στις κεφαλίδες των πακέτων, όπως οι IP διευθύνσεις του αποστολέα και του παραλήπτη, οι θύρες πρωτοκόλλου ελέγχου μεταφοράς (TCP) και πρωτοκόλλου επιστολής δεδομένων χρήστη (UDP) της πηγής και του προορισμού του πακέτου και ο αριθμός που δηλώνει το πρωτόκολλο που χρησιμοποιείται. Τα πακέτα ελέγχονται ένα προς ένα ξεχωριστά και δεν υπάρχει κάποιου είδους σύνδεση ανάμεσα σε ένα προηγούμενο με ένα επόμενο πακέτο. Μία υποκατηγορία των αναχωμάτων ασφαλείας αυτού του επιπέδου είναι τα φίλτρα συνόδου, τα οποία δεν εξετάζουν το κάθε πακέτο ένα προς ένα ξεχωριστά αλλά κρατάνε πληροφορίες για τη σύνοδο και την κατάσταση των πακέτων και έτσι επιτρέπουν σε πακέτα να εισέρχονται ή να εξέρχονται χωρίς να τα ελέγξουν ολοκληρωτικά, όπως περιγράφεται παραπάνω, αλλά συσχετίζοντας τα με τα προηγούμενα πακέτα που έχουν επιτραπεί [88]. Δηλαδή υπάρχει ένα είδος “μνήμης” ώστε να γίνεται αντιληπτό πως ένα σύνολο πακέτων αφορά την ίδια σύνοδο

  Τα πλεονεκτήματα των αναχωμάτων ασφαλείας επιπέδου μεταφοράς/δικτύου είναι το χαμηλό κόστος, η εύκολη εγκατάσταση και ρύθμιση τους και η γρήγορη ταχύτητα καθώς φιλτράρονται μόνο οι κεφαλίδες και όχι το περιεχόμενο των πακέτων. Επιπλέον, δεν χρησιμοποιείται κάποιο λογισμικό το οποίο να απαιτεί τη συμμετοχή των χρηστών, συνεπώς οι χρήστες δεν εμπλέκονται στη διαδικασία του ελέγχου των πακέτων και ενδεχομένως να μη γνωρίζουν καν ότι αυτή η διαδικασία πραγματοποιείται [48, 88]. Από την άλλη πλευρά, τα μειονεκτήματα τους είναι πως έχουν σχετικά περιορισμένες δυνατότητες καταγραφής περιστατικών, δεν διαθέτουν μηχανισμούς για την αυθεντικοποίηση των χρηστών και δεν μπορούν να αντιμετωπίσουν επιθέσεις, οι οποίες αφορούν το περιεχόμενο των πακέτων (π.χ. πλαστογράφηση διεύθυνσης IP) διότι δεν ελέγχεται το περιεχόμενο τους. Τέλος, είναι αρκετά δύσκολο να οριστούν οι κανόνες φιλτραρίσματος διότι μπορεί να είναι αρκετά περίπλοκοι και ενδεχομένως να πρέπει να προστεθούν εξαιρέσεις για ορισμένους χρήστες, γεγονός που αυξάνει ακόμα περισσότερο την πολυπλοκότητα της διαδικασίας [48].
- *Αναχώματα ασφαλείας επιπέδου εφαρμογής:* Τα αναχώματα ασφαλείας επιπέδου εφαρμογής είναι αναχώματα ασφαλείας, τα οποία χρησιμοποιούνται ξεχωριστά για κάθε υπηρεσία και εφαρμογή που θέλει να χρησιμοποιήσει ένας χρήστης, και ελέγχουν την είσοδο (input) και την

έξοδο (output) δεδομένων και την πρόσβαση ή μη σε μία εφαρμογή ή υπηρεσία. Η διαφορά τους σε σχέση με τα αναχώματα ασφαλείας επιπέδου μεταφοράς / δικτύου είναι πως εκείνα χρησιμοποιούνται για να ελέγξουν την κίνηση ολόκληρου του δικτύου ενώ αυτά χρησιμοποιούνται για μία συγκεκριμένη εφαρμογή ή υπηρεσία, έτσι λοιπόν μπορεί να υπάρξει καλύτερο (αυστηρότερο) επίπεδο ασφάλειας. [88]

Το ανάχωμα ασφαλείας λειτουργεί σαν ένας ενδιάμεσος ανάμεσα σε έναν χρήστη που ζητά να χρησιμοποιήσει μία υπηρεσία και στον εξυπηρετητή ο οποίος θα προσφέρει την υπηρεσία αυτή [88]. Πιο συγκεκριμένα, όταν ένας χρήστης προσπαθεί να επικοινωνήσει με έναν εξυπηρετητή για να χρησιμοποιήσει μια εφαρμογή ή υπηρεσία, το ανάχωμα ασφαλείας λειτουργεί σαν να ήταν αυτό ο εξυπηρετητής, δέχεται το αίτημα και διαχειρίζεται όλη τη διαδικασία χωρίς αυτό να γίνεται αντιληπτό από τον χρήστη. Οπότε, έρχεται μόνο αυτό (το ανάχωμα) σε επαφή με άλλα δίκτυα και ο χρήστης παραμένει ανώνυμος και προστατευμένος. Ομοίως, όταν ένας εξυπηρετητής στέλνει μια απάντηση προς τον χρήστη, το ανάχωμα ασφαλείας λειτουργεί ως χρήστης και έτσι είναι ξανά το μοναδικό συστατικό του δικτύου το οποίο έρχεται σε επαφή με εξωτερικά δίκτυα. Το ανάχωμα ασφαλείας φιλοξενείται σαν λογισμικό σε έναν υπολογιστή έπαλξη (bastion host), ο οποίος αποτελεί και το σημείο μέσω του οποίου το εσωτερικό δίκτυο επικοινωνεί με εξωτερικά δίκτυα, όπως το διαδίκτυο. Εκεί στεγάζονται οι πληρεξούσιοι εξυπηρετητές (proxy servers), οι οποίοι πραγματοποιούν τη λειτουργία της μεσολάβησης που περιγράφεται παραπάνω και εξασφαλίζουν την ανωνυμία των χρηστών καθώς αντικαθιστούν τις IP διευθύνσεις τις οποίες χρησιμοποιούν εντός του προστατευμένου δικτύου με τις δικές τους ώστε να μην βρεθούν εκτεθειμένες. Επομένως, προστατεύονται δημόσια δεδομένα που αφορούν το προστατευόμενο δίκτυο και που μπορούν να αποτελέσουν πηγή πληροφόρησης ώστε να πραγματοποιηθεί μια επίθεση [48].

Ο υπολογιστής έπαλξη που αναφέρθηκε στην προηγούμενη παράγραφο πρέπει να είναι ιδιαίτερα ασφαλής καθώς είναι το σημείο επικοινωνίας του εσωτερικού δικτύου με το διαδίκτυο άρα θα λέγαμε ότι αποτελεί και το πιο εκτεθειμένο τμήμα του δικτύου. Θα πρέπει να τρέχει ένα λειτουργικό σύστημα χωρίς γνωστές ευπάθειες και οι δυνατότητες του να είναι περιορισμένες στις ελάχιστες που απαιτούνται ώστε να επιτελέσει το σκοπό του. Επίσης, θα πρέπει να διατηρεί αρχεία καταγραφής και να αυθεντικοποιεί τους χρήστες που τον χρησιμοποιούν σε επίπεδο δικτύου. [48]

Τα πλεονεκτήματα των αναχωμάτων ασφαλείας επιπέδου εφαρμογής είναι ότι μπορούν να καταγράψουν με λεπτομέρειες τα γεγονότα που συμβαίνουν στο δίκτυο, οι κανόνες φιλτραρίσματος δεν είναι το τόσο σύνθετοι όσο στα αναχώματα επιπέδου μεταφοράς/δικτύου και παρέχουν μεγαλύτερη ασφάλεια καθώς μπορεί να γίνει κάποιο είδος αυθεντικοποίησης πριν χρησιμοποιηθεί μία υπηρεσία από κάποιον χρήστη και υπάρχει μόνο μία οντότητα (ο πληρεξούσιος εξυπηρετητής) που προσπελαύνει το εσωτερικό δίκτυο. Από την άλλη πλευρά, τα μειονεκτήματα είναι πως είναι πιο δύσκολη η υλοποίησή τους, πολλές φορές λειτουργούν με τέτοιο τρόπο που να γίνονται αντιληπτά από τον χρήστη (μη διαφανή) και σε σχέση με τα αναχώματα επιπέδου

μεταφοράς/δικτύου η ταχύτητά τους και η απόδοσή τους είναι μικρότερη ενώ η ανάγκη για πόρους μεγαλύτερη. [48]

- *Υβριδικά αναχώματα ασφαλείας*: Τα υβριδικά αναχώματα ασφαλείας συνδυάζουν και τις δύο τεχνικές και έτσι σε ένα σύστημα ενσωματώνονται τα πλεονεκτήματα και το πεδίο δράσης και των δύο αυτών τεχνικών. Τα υβριδικά αναχώματα, ανάλογα με την αρχιτεκτονική τους, χωρίζονται σε τρεις κατηγορίες: τα διπλοσυνδεδεμένα αναχώματα ασφάλειας, τα αναχώματα ασφάλειας υπολογιστή διαλογής και τα αναχώματα ασφάλειας υποδικτύου διαλογής.
    - *Διπλοσυνδεδεμένα αναχώματα ασφάλειας (Simple Dual-homed Gateway)*: Τα διπλοσυνδεδεμένα αναχώματα ασφαλείας, όπως όλα τα υβριδικά αναχώματα, συνδυάζουν τα αναχώματα επιπέδου εφαρμογής και επιπέδου μεταφοράς δικτύου. Υπάρχει ένας υπολογιστής έπαλξη, ο οποίος είναι ταυτόχρονα συνδεδεμένος και με το ιδιωτικό δίκτυο το οποίο προστατεύεται και με το διαδίκτυο. Ο υπολογιστής αυτός βρίσκεται ανάμεσα στα δύο δίκτυα, συνεπώς η κίνηση μεταξύ των δύο δικτύων ελέγχεται και δεν είναι δυνατόν να δρομολογηθούν πακέτα απευθείας από το διαδίκτυο προς το εσωτερικό δίκτυο, γεγονός που αποτελεί μιας μορφής ασφάλεια. Επιπλέον, μπορούν να χρησιμοποιήσουν υπηρεσίες και κατά συνέπεια να δοθεί σε αυτές η δυνατότητα να επικοινωνήσουν με το εσωτερικό του δικτύου μόνο εάν παρέχονται μέσω πληρεξούσιων εφαρμογών, σε αντίθετη περίπτωση απορρίπτονται. Με αυτόν τον τρόπο, αυξάνεται ακόμα περισσότερο το επίπεδο ασφάλειας καθώς η πρόσβαση στο προστατευόμενο δίκτυο πραγματοποιείται με απόλυτα ελεγχόμενο τρόπο [88]. Το πλεονέκτημά αυτού του είδους αναχώματος είναι ότι έχει το μικρότερο κόστος σε σχέση με τα άλλα είδη και το μειονέκτημά του είναι πως σε περίπτωση που ένας επιτιθέμενος καταφέρει να τα παραβιάσει τότε θα βρεθεί εκτεθειμένο σε αυτόν ολόκληρο το προστατευόμενο δίκτυο [48, 88].
    - *Αναχώματα ασφάλειας υπολογιστή διαλογής (Screened Host)*: Τα αναχώματα ασφαλείας υπολογιστή διαλογής παρέχουν υπηρεσίες μέσω ενός υπολογιστή έπαλξη, ο οποίος είναι συνδεδεμένος μόνο στο εσωτερικό δίκτυο. Για την επικοινωνία του εσωτερικού δικτύου με το διαδίκτυο υπάρχει ένας δρομολογητής διαλογής όπου αρχικά φιλτράρει τα εισερχόμενα πακέτα και στη συνέχεια στέλνει όλη την κίνηση, που προέρχεται από το διαδίκτυο και έγινε αποδεκτή κατά τη διαδικασία του φιλτραρίσματος, στον υπολογιστή έπαλξη. [88] Τα πλεονεκτήματα αυτού του είδους είναι η μεγαλύτερη ευχρηστία, καθώς δεν είναι απαραίτητο να χρησιμοποιούνται συνεχώς πληρεξούσιοι εξυπηρετητές, και υπάρχει αυξημένη ασφάλεια διότι εδώ έρχεται σε επαφή με το διαδίκτυο ένας δρομολογητής και όχι υπολογιστής και ο δρομολογητής αυτός είναι πιο εύκολο να προστατευθεί καθώς προσφέρει λιγότερες υπηρεσίες άρα μπορούν να προκύψουν και λιγότερες ευπάθειες [48]. Τα μειονεκτήματα αυτού του είδους είναι πως, όπως και στην προηγούμενη τεχνική, αν παραβιαστεί είτε ο υπολογιστής έπαλξη είτε ο δρομολογητής διαλογής τότε θα βρεθεί εκτεθειμένο ολόκληρο το δίκτυο. Επιπλέον, χρησιμοποιούνται δύο συσκευές (υπολογιστής έπαλξη και δρομολογητής) αντί για μία, από τις οποίες μπορεί να ξεκινήσει μία επίθεση [48, 88]. Ακόμα και αν δεν έχει δεχτεί

επίθεση ο υπολογιστής έπαλξη σε περίπτωση που ένας επιτιθέμενος αποκτήσει πρόσβαση στους πίνακες δρομολόγησης του δρομολογητή διαλογής μπορεί να τροποποιήσει τις IP διευθύνσεις ώστε ο υπολογιστής έπαλξη να παρακάμπτεται και να υπάρχει πρόσβαση απευθείας στο εσωτερικό του δικτύου.

- *Αναχώματα ασφάλειας υποδικτύου διαλογής (Screened Subnet)*: Τα αναχώματα ασφαλείας υποδικτύου διαλογής είναι η πιο ευρέως χρησιμοποιούμενη και η πιο ασφαλής λύση. Αποτελούνται από δύο δρομολογητές διαλογής, τον εσωτερικό και τον εξωτερικό, και ανάμεσα στους βρίσκεται ο υπολογιστής έπαλξη, έτσι λοιπόν δημιουργείται ένα μικρό δίκτυο. Το δίκτυο αυτό ονομάζεται περιμετρικό δίκτυο και παρεμβάλλεται ανάμεσα στο εσωτερικό δίκτυο και στο διαδίκτυο δημιουργώντας μία επιπλέον ζώνη προστασίας. Αυτή η επιπλέον ζώνη προστασίας είναι σε θέση να κρατήσει ασφαλές το εσωτερικό δίκτυο στην περίπτωση που έχει γίνει επίθεση στον υπολογιστή έπαλξη. [48, 88] Ο εσωτερικός δρομολογητής είναι αυτός που βρίσκεται από την πλευρά του εσωτερικού δικτύου και προστατεύει το εσωτερικό δίκτυο από τα υπόλοιπα, δηλαδή από το περιμετρικό δίκτυο και από το διαδίκτυο. Αναλαμβάνει σε μεγαλύτερο βαθμό το φιλτράρισμα των πακέτων και ελέγχει ποιες υπηρεσίες θα περάσουν από το εσωτερικό δίκτυο προς το διαδίκτυο απευθείας χωρίς τη χρήση πληρεξούσιων εξυπηρετητών [48, 88]. Ο υπολογιστής έπαλξη, όπως και στα άλλα δύο υποείδη (υβριδικών αναχωμάτων) φιλοξενεί τους πληρεξούσιους εξυπηρετητές ώστε να παρέχονται υπηρεσίες στους εσωτερικούς χρήστες και αποτελεί σημείο επικοινωνίας του εσωτερικού δικτύου με το διαδίκτυο [48]. Ο εξωτερικός δρομολογητής ο οποίος βρίσκεται στην πλευρά του διαδικτύου, προστατεύει το εσωτερικό και το περιμετρικό δίκτυο από το διαδίκτυο και επιτρέπει σε όλα τα πακέτα να μεταφέρονται από το περιμετρικό δίκτυο προς το διαδίκτυο. Οι κανόνες ασφαλείας του θα πρέπει να είναι ίδιοι με αυτούς του εσωτερικού δρομολογητή [48, 88] και οι κανόνες φιλτραρίσματος που εφαρμόζονται σε αυτόν είναι ο μόνος τρόπος να προστατευθεί ο υπολογιστής έπαλξη διότι δεν υπάρχει άλλο συστατικό του δικτύου το οποίο να βρίσκεται προς την πλευρά του διαδικτύου ώστε να τον προστατεύσει [88].Τα πλεονεκτήματα αυτής της λύσης είναι ότι για να φτάσει να παραβιαστεί το εσωτερικό δίκτυο θα πρέπει να έχουν παραβιαστεί τρία διαφορετικά συστατικά του δικτύου, οι δυο δρομολογητές και ο υπολογιστής έπαλξη, άρα το επίπεδο ασφάλειας είναι αυξημένο και ότι δεν υπάρχει καμία απευθείας σύνδεση με το διαδίκτυο καθώς, ανεξάρτητα από το αν χρησιμοποιείται πληρεξούσιος εξυπηρετητής, παρεμβάλλεται το περιμετρικό δίκτυο. Τελευταίο και σημαντικότερο είναι το γεγονός το ότι καταφέρνει να αντιμετωπίσει το πρόβλημα του μοναδικού σημείου αποτυχίας όπου αν παραβιαστεί ο υπολογιστής έπαλξη ή ο δρομολογητής διαλογής βρίσκεται εκτεθειμένο όλο το δίκτυο. Εδώ ακόμα και να παραβιαστεί ο υπολογιστής έπαλξη δεν απειλείται το εσωτερικό του δικτύου καθώς υπάρχουν οι δύο δρομολογητές, οι οποίοι μπορούν να τον παρακάμψουν και να ανακατευθύνουν την κίνηση. Από την άλλη πλευρά, τα μειονεκτήματα είναι το υψηλό κόστος υλοποίησης και συντήρησης και η μεγάλη πολυπλοκότητα. [48]

Πρόληψη κατανεμημένων επιθέσεων άρνησης εξυπηρέτησης

Για την πρόληψη κατά των κατανεμημένων επιθέσεων άρνησης εξυπηρέτησης μπορούν να χρησιμοποιηθούν τεχνικές, όπως το φιλτράρισμα της κίνησης, η αλλαγή διευθύνσεων IP, η εξισορρόπηση φορτίου, ο περιορισμός μη χρησιμοποιούμενων πόρων και η έγκαιρη εγκατάσταση ενημερώσεων. [89]

Το φιλτράρισμα της εισερχόμενης κίνησης είναι μία τεχνική που πραγματοποιείται ώστε να παρακολουθείται και να ελέγχεται η κίνηση στο δίκτυο και να εμποδίζεται η παράνομη κίνηση [89]. Το φιλτράρισμα της κίνησης συμβάλλει στην πρόληψη κατά των κατανεμημένων επιθέσεων άρνησης εξυπηρέτησης διότι εντοπίζονται και αποκλείονται πακέτα με πλαστογραφημένη διεύθυνση IP. Με αυτόν τον τρόπο, πέρα από την προστασία από κακόβουλα πακέτα, περιορίζεται και ο αριθμός των συνολικών πακέτων που τελικά εισέρχονται στο δίκτυο, ο οποίος αν αυξηθεί σε πολύ μεγάλο βαθμό θα δημιουργηθεί συμφόρηση. Επιπλέον, μπορεί να γίνεται και φιλτράρισμα της εξερχόμενης κίνησης δηλαδή να ελέγχονται τα πακέτα τα οποία εξέρχονται από το σύστημα. Αυτό δεν βοηθά άμεσα το ίδιο το σύστημα ως προς την δική του προστασία αλλά είναι χρήσιμο στην περίπτωση όπου ένα μηχάνημα του συστήματος έχει καταληφθεί από επιτιθέμενους, οι οποίοι προσπαθούν να στείλουν κακόβουλα πακέτα προς κάποιο άλλο δίκτυο. Αυτά τα πακέτα θα μπλοκαριστούν και έτσι δεν θα επεκταθεί ακόμη περισσότερο η κακόβουλη δράση των επιτιθέμενων [89].

Η εξισορρόπηση φορτίου είναι μία χρήσιμη τεχνική ώστε να προσαρμόζεται (αυξάνεται) το εύρος ζώνης όταν υπάρχει αυξημένη ζήτηση και η κίνηση να κατανέμεται ομοιόμορφα στο σύνολο των διαθέσιμων εξυπηρετητών στο δίκτυο [89]. Έτσι σε ενδεχόμενη επίθεση αντιμετωπίζεται το πρόβλημα του μοναδικού σημείου αποτυχίας και ακόμα και στην περίπτωση που ένας εξυπηρετητής καταρρεύσει η κίνηση του δικτύου θα ανακατευθυνθεί στους υπόλοιπους ώστε να μην υπάρξει άρνηση εξυπηρέτησης.

Η αλλαγή διευθύνσεων IP χρησιμοποιείται σε περιπτώσεις όπου ο επιτιθέμενος έχει εντοπίσει μια IP διεύθυνση του δικτύου και προσπαθεί να “μπλοκάρει” την κίνηση με πολλά πακέτα προς το προστατευόμενο δίκτυο. Αν γίνεται αλλαγή διευθύνσεων περιοδικά για την συσκευή της οποίας την αρχική διεύθυνση γνωρίζει ο επιτιθέμενος τότε τα πακέτα που αυτός στέλνει θα απορρίπτονται [89]. Η περιοδικότητα (αλλαγής) έγκειται στο γεγονός πως εφόσον η IP διεύθυνση μιας συσκευής αποκαλύφθηκε μια φορά, είναι πιθανόν να αποκαλυφθεί και στο μέλλον.

Δύο ακόμα τεχνικές είναι: (α) ο περιορισμός των ενεργών συνδέσεων/πόρων, όταν δεν χρησιμοποιούνται, ώστε εφόσον θα βρίσκονται εκτός λειτουργίας να παύουν να αποτελούν έναν ακόμα στόχο για τον επιτιθέμενο και (β) η διαρκής ενημέρωση του υλικού και του λογισμικού του δικτύου άλλα και του συνόλου της υποδομής με τις πιο πρόσφατες ενημερώσεις ώστε να μην υπάρχουν τρωτά σημεία τα οποία να μπορεί να εκμεταλλευτεί κάποιος επιτιθέμενος [89].

Ανίχνευση επιθέσεων

Οι επιθέσεις ανιχνεύονται με τις τεχνικές ανίχνευσης ανωμαλιών, ανίχνευσης κατάχρησης, ανίχνευσης υπογραφής καθώς και με υβριδικές τεχνικές. Όλες αυτές οι τεχνικές περιγράφονται στην ενότητα των συστημάτων ανίχνευσης εισβολών (Ενότητα 4.2.3).

Αντιμετώπιση

Εφόσον ανιχνευθεί μία επίθεση θα πρέπει να γίνει προσπάθεια για να περιοριστούν στο ελάχιστο δυνατό οι συνέπειές που θα επιφέρει στο προστατευόμενο σύστημα. Παρακάτω αναφέρονται τεχνικές περιορισμού που μπορούν να εφαρμοστούν για αυτό τον σκοπό.

- ***Μαύρη τρύπα (Blackholing)***: Αυτή η τεχνική χρησιμοποιείται για να ελέγξει την εισερχόμενη κίνηση σε ένα δίκτυο και να την ανακατευθύνει με τέτοιο τρόπο ώστε να "χαθεί" και να μην καταλήξει σε κανέναν προορισμό, δημιουργώντας IP διευθύνσεις που δεν αντιστοιχούν κάπου και ανακατευθύνοντας την κίνηση εκεί [90]. Το πλεονέκτημα αυτής της τεχνικής είναι πως μπορεί να αντιμετωπίσει την επίθεση άμεσα και ολοσχερώς. Από την άλλη πλευρά, αυτή η τεχνική έχει σημαντικό αρνητικό αντίκτυπο ως προς τα νόμιμα αιτήματα που και αυτά εν τέλει χάνονται δίνοντας την εντύπωση πως το όλο σύστημα δεν είναι διαθέσιμο [90].
- *Καταβόθρισμος (Sinkholing)*: Αυτή η τεχνική χρησιμοποιείται για να ελέγξει την εισερχόμενη κίνηση σε ένα δίκτυο και να την ανακατευθύνει σε έναν προκαθορισμένο και διαφορετικό προορισμό από τον αρχικό με στόχο να αποφευχθεί η συμφόρηση, όταν στέλνονται πολλά πακέτα προς έναν συγκεκριμένο στόχο, καθώς και η μόλυνση, εάν πρόκειται και για κακόβουλα πακέτα. Έτσι, λοιπόν, μία επίθεση αντιμετωπίζεται καθώς τα αιτήματα των επιτιθέμενων, ακόμη και αν στέλνονται συνεχώς, δεν προκαλούν κάποιο σοβαρό πρόβλημα στο σύστημα διότι καταλήγουν σε ένα προκαθορισμένο σημείο (το οποίο μπορεί να είναι ένα ή περισσότερα μηχανήματα) του προστατευόμενου συστήματος που εις γνώση των διαχειριστών θα βρεθεί αντιμέτωπο με την επίθεση και την ενδεχόμενη μόλυνση [90]. Το πλεονέκτημα αυτής της τεχνικής είναι ότι αφού διατίθεται ένα σημείο το οποίο θα δεχθεί όλη την επιβλαβή κίνηση δεν δημιουργείται πρόβλημα σε άλλα σημεία του δικτύου. Από την άλλη πλευρά δεν είναι σε θέση να σταματήσει μία επίθεση παρά μόνο να την περιορίσει προσπαθώντας να μετριάσει τις συνέπειες [90].
- *Περιορισμός ρυθμού (Rate limiting)*: Αυτή η τεχνική χρησιμοποιείται για να περιορίσει την κίνηση του δικτύου, δηλαδή να θέσει περιορισμό στο πόσες φορές μπορεί να συμβεί κάποια ενέργεια σε ένα συγκεκριμένο χρονικό διάστημα. Δηλαδή μετριούνται τα αιτήματα που φτάνουν για τη χρήση μιας υπηρεσίας αλλά και αυτά που φτάνουν από κάθε IP διεύθυνση ξεχωριστά σε ένα χρονικό πλαίσιο και τα αιτήματα εξυπηρετούνται ανάλογα με τον ρυθμό που έχει καθοριστεί. Το τελευταίο σημαίνει πως με βάση την τεχνική του throttling, τα αιτήματα που είναι πέραν του ρυθμού θα απορρίπτονται άμεσα. Σαν αποτέλεσμα δεν δημιουργείται συμφόρηση στο δίκτυο. Το πλεονέκτημα αυτής της τεχνικής είναι πως μπορεί να περιορίσει τις βλαβερές συνέπειες πολλών ειδών επιθέσεων, όπως επιθέσεις ωμής βίας, άρνησης εξυπηρέτησης και εξαγωγής δεδομένων ιστού, ενώ το μειονέκτημά της είναι πως εφόσον ξεπεραστεί το όριο ρυθμού που

έχει οριστεί είναι πολύ πιθανό εκτός από τα μη νόμιμα να απορριφθούν και νόμιμα μηνύματα. [91]

4.2.9 Αποτίμηση ασφάλειας (Security assessment)

Σύμφωνα με τον οργανισμό NIST (National Institute of Standards and Technology) ως αποτίμηση ασφαλείας ορίζεται η διαδικασία που εξετάζει το πόσο αποτελεσματικά μια οντότητα προς αξιολόγηση εκπληρώνει συγκεκριμένους στόχους ασφαλείας [92].

Μεθοδολογία αποτίμησης ασφάλειας

Οι μέθοδοι που μπορούν να χρησιμοποιηθούν για την αποτίμηση είναι η δοκιμή (testing), η εξέταση (examination) και η συνέντευξη (interviewing).

- *Δοκιμή*: είναι η διαδικασία όπου οι προς αξιολόγηση οντότητες δοκιμάζονται υπό καθορισμένες συνθήκες ώστε να συγκριθούν η πραγματική και η αναμενόμενη συμπεριφορά τους ως προς την ασφάλεια. [92]
- *Εξέταση*: είναι η διαδικασία που περιλαμβάνει: έλεγχο, επιθεώρηση, επανεξέταση, παρατήρηση, μελέτη και ανάλυση των οντοτήτων προς αξιολόγηση ώστε να γίνει πιο εύκολη η κατανόηση, να επιτευχθεί διευκρίνιση ή να αποκτηθούν αποδεικτικά στοιχεία για το αν εκπληρώνονται οι στόχοι ασφαλείας. [92]
- *Συνέντευξη*: είναι η μια εναλλακτική διαδικασία σε σχέση με αυτήν της εξέτασης με τον ίδιο στόχο. Κατά την διαδικασία αυτή πραγματοποιούνται συζητήσεις μεταξύ των ατόμων ενός οργανισμού ώστε να γίνει ευκολότερη η κατανόηση, να επιτευχθεί διευκρίνιση ή να εντοπιστεί η τοποθεσία των αποδεικτικών στοιχείων, όπως συμβαίνει και με την μέθοδο της εξέτασης. [92]

Η εξέταση (examination) περιλαμβάνει κυρίως την ανασκόπηση (review) διαφόρων εγγράφων, όπως έγγραφα για τις πολιτικές, τις διαδικασίες, σχέδια ασφαλείας κ.α. Πραγματοποιείται για να διαπιστωθεί εάν η τεκμηρίωση (documentation) ενός συστήματος έχει γίνει σωστά, για να εντοπιστούν ευπάθειες και για να αποκτηθούν πληροφορίες που μπορούν να βρεθούν μόνο μέσα στα έγγραφα της τεκμηρίωσης. Δίνεται σημασία στην τεκμηρίωση διότι με βάση αυτή προκύπτει ο σχεδιασμός, η διαμόρφωση, και η λειτουργία και η συντήρηση του συνόλου του πληροφοριακού συστήματος ενός οργανισμού και είναι απαραίτητο να ακολουθείται απόλυτα, χωρίς αποκλίσεις. Η μέθοδος της εξέτασης δεν επιφέρει συνέπειες για τα συστήματα τα οποία εξετάζονται διότι δεν χρειάζεται να εκτελέσουν κάποια λειτουργία ενώ οι υπεύθυνοι απλά αποκτούν πρόσβαση στα έγγραφα τεκμηρίωσης και ενδεχομένως σε αρχεία καταγραφής, εάν υπάρχουν. Επιπλέον, το γεγονός πως οι αποτιμήσεις ασφαλείας πραγματοποιούνται από άτομα με την κατάλληλη εκπαίδευση και τις απαραίτητες γνώσεις διασφαλίζει σε πολύ μεγάλο βαθμό ότι δε μπορεί να συμβεί κάποια επιβλαβής ενέργεια από αμέλεια. [92]

Η μέθοδος της δοκιμής (testing) είναι μία πιο πρακτική διαδικασία σε σύγκριση με τη μέθοδο της εξέτασης (examination) διότι περιλαμβάνει την εκτέλεση διαφόρων ενεργειών πάνω σε ολόκληρα πληροφοριακά συστήματα ή σε μεμονωμένα κομμάτια τους ώστε να εντοπιστούν ευπαθή σημεία. Η χρήση των τεχνικών της ανίχνευσης (vulnerability testing) και της διείσδυσης (penetration testing) προσφέρουν χρήσιμες πληροφορίες για ενδεχόμενα ευάλωτα σημεία και μπορούν να προβλέψουν αν τις επιτιθέμενος είναι σε θέση να εκμεταλλευτεί τις ευπάθειες του συστήματος. Επιπλέον, η μέθοδος αυτή προσφέρει τη δυνατότητα σε οργανισμούς να ελέγξουν κατά πόσο είναι συμμορφωμένοι με αντικείμενα, όπως οι πολιτικές κωδικών πρόσβασης και διαχείρισης ενημερώσεων. επίσης, μπορεί να προσφέρει μία πιο ακριβή εικόνα για τα επίπεδα ασφαλείας ενός οργανισμού σε σχέση με τη μέθοδο της εξέτασης αλλά ενδεχομένως να επηρεάσει τα πληροφοριακά συστήματα καθώς πραγματοποιούνται διάφορες ενέργειες που μπορούν να επιφέρουν συνέπειες, όπως για παράδειγμα ακούσια διαγραφή αρχείων και απώλεια δεδομένων. Θα πρέπει, λοιπόν, οι ενέργειες αυτές να πραγματοποιούνται σε περιόδους που το σύστημα ή το αντίστοιχο μέρος του συστήματος δεν είναι υπό κανονική λειτουργία (αλλά πχ. υπό συντήρηση) και ενδεχομένως να απενεργοποιούνται και κάποιοι μηχανισμοί ασφάλειας ή να διαμορφώνονται με διαφορετικό τρόπο ώστε να μπορέσει να εκτελεστεί σωστά η δοκιμή. Βέβαια, ο διαθέσιμος χρόνος για να γίνουν οι δοκιμές είναι περιορισμένος και οι υπεύθυνοι δεν φτάνουν το σύστημα στα όρια του, σε αντίθεση με έναν πραγματικό επιτιθέμενο. Γι' αυτό λοιπόν η καλύτερη λύση είναι ο συνδυασμός των δύο μεθόδων (δοκιμής και εξέτασης). [92]

Η διεξαγωγή της διαδικασίας αποτίμησης χωρίζεται σε τρία στάδια: (α) το στάδιο του σχεδιασμού, (β) το στάδιο της εκτέλεσης και (γ) το στάδιο της μετα-εκτέλεσης.

- *Σχεδιασμός*: Το στάδιο του σχεδιασμού είναι πολύ σημαντικό για να γίνει σωστά η αποτίμηση ασφάλειας. Συγκεντρώνονται πληροφορίες που χρειάζονται, όπως οι οντότητες που θα αξιολογηθούν, οι απειλές ως προς αυτές και τα μέτρα ασφαλείας που θα χρησιμοποιηθούν ώστε να περιοριστούν οι συνέπειες των απειλών. Η αποτίμηση ασφάλειας θα πρέπει να αντιμετωπίζεται σαν ένα έργο πληροφορικής και να υπάρχει το αντίστοιχο σχέδιο διαχείρισης έργου, όπως συμβαίνει με όλα τα έργα (λογισμικού) ώστε να ορίζονται στόχοι, απαιτήσεις, ρόλοι χρηστών, ευθύνες, πόροι, περιορισμοί, χρονοδιαγράμματα και παραδοτέα στα πλαίσια της αποτίμησης της ασφάλειας. [92]
- *Εκτέλεση*: Το στάδιο της εκτέλεσης περιλαμβάνει τον εντοπισμό των ευπαθειών και την επικύρωσή τους, όποτε χρειάζεται. Αυτό το στάδιο εξετάζει τις δραστηριότητες που συνδέονται με τη μέθοδο αξιολόγησης που ακολουθείται. Παρόλο που οι δραστηριότητες ενδεχομένως να διαφέρουν ανάλογα με τον τύπο αξιολόγησης, στο τέλος αυτού του σταδίου θα έχουν εντοπιστεί ευπάθειες στο σύστημα, στο δίκτυο και στις οργανωτικές διαδικασίες ενώ θα έχουν αποτιμηθεί και άλλα στοιχεία, όπως η επάρκεια των πολιτικών, μηχανισμών & διαδικασιών ασφάλειας που εφαρμόζονται. [92]

- *Μετα-εκτέλεση*: Το στάδιο της μετα-εκτέλεσης περιλαμβάνει την ανάλυση των ευπαθειών που εντοπίστηκαν ώστε να ανιχνευθούν οι αιτίες του προβλήματος και να ληφθούν μέτρα αντιμετώπισης αυτών των ευπαθειών ώστε να αυξηθεί το επίπεδο ασφάλειας. Επιπλέον, δημιουργείται μια αναφορά που περιέχει όλες τις προτάσεις ώστε να βελτιωθεί το επίπεδο της ασφάλειας. [92]

Τεχνικές αποτίμησης ασφάλειας

Υπάρχουν πάρα πολλές και διαφορετικές τεχνικές που μπορούν να χρησιμοποιηθούν για την αποτίμηση ασφάλειας. Οι πιο ευρέως χρησιμοποιούμενες τεχνικές χωρίζονται σε τρεις κατηγορίες: τις τεχνικές ανασκόπησης, τις τεχνικές εντοπισμού & ανάλυσης στόχων και τις τεχνικές επικύρωσης ευπάθειας στόχου. [92]

Τεχνικές ανασκόπησης (Review techniques)

Οι τεχνικές ανασκόπησης ανήκουν στη μέθοδο της εξέτασης (examination) και αξιολογούν συστήματα, εφαρμογές, δίκτυα, και διαδικασίες ώστε να εντοπίσουν πιθανά ευάλωτα σημεία ενώ συλλέγουν πληροφορίες οι οποίες μπορεί να είναι χρήσιμες και για άλλες τεχνικές αξιολόγησης. Οι τεχνικές οι οποίες εντάσσονται σε αυτή την κατηγορία είναι οι εξής:

- *Ανασκόπηση τεκμηρίωσης (Documentation review)*: Αξιολογεί πολιτικές και διαδικασίες για να διαπιστωθεί σε τι βαθμό υπάρχει τεχνική ακρίβεια και πληρότητα [92].
- *Ανασκόπηση καταγραφής (Log review)*: Παρέχει πληροφορίες που έχουν καταγραφεί και σχετίζονται με τη χρήση, τη διαμόρφωση και την τροποποίηση του συστήματος και μπορεί να φανερώσει προβλήματα και στοιχεία μη-συμμόρφωσης με τις πολιτικές που εφαρμόζεται [92].
- *Ανασκόπηση του συνόλου κανόνων (Ruleset review)*: Εντοπίζει κενά σε ελέγχους ασφαλείας που βασίζονται σε σύνολα κανόνων (ruleset) δηλαδή σε έναν αριθμό από κανόνες που εφαρμόζονται για την κίνηση του δικτύου και τη δραστηριότητα των συστημάτων [92].
- *Ανασκόπηση Διαμόρφωσης Συστημάτων (System configuration review)*: Αξιολογεί πόσο ισχυρά έχει διαμορφωθεί το σύστημα και επικυρώνει ότι το σύστημα έχει συμμορφωθεί με τις πολιτικές σκλήρυνσης (hardening) που εφαρμόζονται [92].
- *Παρακολούθηση δικτύου (Network sniffing)*: Παρακολουθεί την κυκλοφορία σε ένα τμήμα του δικτύου για να εντοπίσει ποιά συστήματα είναι ενεργά καθώς και πληροφορίες, όπως τα πρωτόκολλα επικοινωνίας οι υπηρεσίες και εφαρμογές που χρησιμοποιούνται, και επαληθεύει την κρυπτογράφηση των επικοινωνιών.
- *Έλεγχος ακεραιότητας αρχείων (File integrity checking)*: Εντοπίζει αλλαγές σε σημαντικά αρχεία και αναγνωρίζει διάφορους τύπους ανεπιθύμητων αρχείων [92].

Τεχνικές εντοπισμού και ανάλυσης στόχων (Target identification and analysis techniques)

Οι τεχνικές εντοπισμού και ανάλυσης στόχων αποτελούν υποκατηγορία της μεθόδου δοκιμής (testing). Αποσκοπούν στο να εντοπίσουν ενεργές συσκευές, θύρες και υπηρεσίες και να τις αναλύσουν ώστε να εντοπίσουν πιθανές ευπάθειες, χρησιμοποιώντας κατά κύριο λόγο αυτοματοποιημένα εργαλεία. Οι τεχνικές που εντάσσονται σε αυτή την κατηγορία είναι οι εξής:

- *Ανακάλυψη δικτύου (Network discovery)*: Ανακαλύπτει ενεργές συσκευές, εντοπίζει τα μονοπάτια (paths) επικοινωνίας και συμβάλλει στο να προσδιοριστούν οι αρχιτεκτονικές του δικτύου [92].
- *Εντοπισμός υπηρεσιών και θυρών δικτύου (Network port and service identification)*: Ανακαλύπτει ανοιχτές θύρες και τις αντίστοιχες εφαρμογές και υπηρεσίες [92].
- *Ανίχνευση ευπαθειών (Vulnerability scanning)*: Χρησιμοποιεί χρήσιμα αποτελέσματα που προκύπτουν από τις δύο προηγούμενες τεχνικές (πχ. εντοπισμένες συσκευές), εντοπίζει γνωστές ευπάθειες και τέλος προτείνει κάποια μέτρα ώστε να περιοριστούν όσο το δυνατόν περισσότερο οι συνέπειες που προκύπτουν από τις ευπάθειες αυτές [92].
- *Ανίχνευση ασύρματων επικοινωνιών (Wireless scanning)*: Εντοπίζει συσκευές ασύρματων επικοινωνιών, οι οποίες δεν είναι εξουσιοδοτημένες, χρησιμοποιώντας κατάλληλους ανιχνευτές, ανακαλύπτει ασύρματα σήματα έξω από την περίμετρο του οργανισμού και ανιχνεύει παραβιάσεις ασφάλειας. Περιλαμβάνει τις τεχνικές: παθητικής ανίχνευσης ασύρματων επικοινωνιών (passive wireless scanning), ενεργής ανίχνευσης ασύρματων επικοινωνιών (active wireless scanning), εντοπισμού θέσης συσκευών ασύρματων επικοινωνιών (wireless device location tracking) και ανίχνευσης bluetooth (bluetooth scanning) [92].
- *Έλεγχος ασφάλειας εφαρμογών (Application security testing)*: Εντοπίζει πιθανές ευπάθειες σε εξατομικευμένα λογισμικά (custom software) που χρησιμοποιούνται μέσα σε έναν οργανισμό και ελέγχει αν τα λογισμικά αυτά αλληλοεπιδρούν με ασφαλή τρόπο με τους χρήστες και με άλλες εφαρμογές [92].

Τεχνικές επικύρωσης ευπάθειας στόχου (Target Vulnerability Validation Techniques)

Οι τεχνικές επικύρωσης ευπάθειας στόχου αποτελούν υποκατηγορία της μεθόδου της δοκιμής (testing). Χρησιμοποιούν πληροφορίες που προκύπτουν από τις τεχνικές εντοπισμού και ανάλυσης στόχων ώστε να εξετάσουν σε μεγαλύτερο βαθμό αν υπάρχει κάποιο ευάλωτο σημείο και αν τελικά υπάρχει, τότε να το επιβεβαιώσουν. Οι τεχνικές που εντάσσονται σε αυτή την κατηγορία είναι οι εξής:

- *Παραβίαση κωδικού πρόσβασης (Password Cracking)*: Εντοπίζει τους μη ισχυρούς κωδικούς πρόσβασης και τις μη ισχυρές πολιτικές (δημιουργίας & διατήρησης) κωδικών πρόσβασης [92] .

- *Έλεγχος διείσδυσης (Penetration testing)*: Ελέγχει την ασφάλεια χρησιμοποιώντας τις τεχνικές και τα εργαλεία που θα χρησιμοποιούσε ένας επιτιθέμενος, επαληθεύει τις ευπάθειες και εντοπίζει πως οι ευπάθειες μπορούν να χρησιμοποιηθούν συνδυαστικά ώστε μια επίθεση να έχει μεγαλύτερη επιτυχία [92].
- *Κοινωνική μηχανική (Social engineering)*: Ελέγχει τις διαδικασίες και την ευαισθητοποίηση των ανθρώπων (user awareness) στα ζητήματα ασφάλειας [92].

4.2.10 Ασφάλεια Ιστού (Web Security)

Η ασφάλεια ιστού προσφέρει προστασία σε πραγματικό χρόνο ώστε να προστατεύονται οι χρήστες μίας επιχείρησης ή ενός οργανισμού από πιθανές απειλές που δημιουργούνται κατά την πλοήγησή τους στο διαδίκτυο. Οι υπηρεσίες που παρέχονται είναι: (α) φιλτράρισμα ιστοσελίδων, (β) προστασία από κακόβουλο λογισμικό (anti-malware) και (γ) απεικόνιση των αρχείων καταγραφής [93-94]. Όταν η ασφάλεια ιστού συνδυάζεται και με άλλες υπηρεσίες που αναλύθηκαν σε προηγούμενα κεφάλαια, όπως για παράδειγμα η προστασία ηλεκτρονικού ταχυδρομείου και η ασφάλεια δικτύου, δημιουργείται ένα ολοκληρωμένο και ασφαλές αποτέλεσμα.

Φιλτράρισμα ιστοσελίδων

Το φιλτράρισμα είναι μία απαραίτητη διαδικασία διότι προσφέρει πάρα πολλά πλεονεκτήματα, όπως η προστασία από κακόβουλες ιστοσελίδες και από λήψη κακόβουλων αρχείων, προστασία από ηλεκτρονικό ψάρεμα και ανεπιθύμητο περιεχόμενο (spam), σωστή διαχείριση του διαθέσιμου εύρους ζώνης καθώς μπορεί να περιοριστεί η πρόσβαση σε ιστοσελίδες που καταναλώνουν μεγάλο εύρος ζώνης, όπως για παράδειγμα ιστοσελίδες μετάδοσης βίντεο, και τέλος αύξηση της παραγωγικότητας του προσωπικού, εφόσον δεν επιτρέπεται η πρόσβαση σε ιστοσελίδες που θα τους αποσπούσαν από το έργο τους. Οι τεχνικές φιλτραρίσματος ιστοσελίδων είναι οι εξής: (α) φιλτράρισμα περιεχομένου, (β) φιλτράρισμα ενιαίων εντοπιστών πόρων (urls) και (γ) φιλτράρισμα συστήματος ονομάτων τομέων (dns). [95]

- *Φιλτράρισμα περιεχομένου (content filtering)*: Το φιλτράρισμα περιεχομένου, όπως έχει αναφερθεί και σε προηγούμενη ενότητα, ελέγχει το περιεχόμενο μιας ιστοσελίδας βασιζόμενο σε λέξεις-κλειδιά, επισυναπτόμενες εικόνες και τμήματα ενός κειμένου, χρησιμοποιώντας είτε απλές είτε πολύπλοκες τεχνικές φιλτραρίσματος από την περιοχή της Ανάκτησης Πληροφορίας (Information Retrieval) ώστε να διαχωρίζει τις κατάλληλες από τις ακατάλληλες ιστοσελίδες. Παραδείγματος χάριν, όταν μια σελίδα περιέχει κακές λέξεις, τότε θα χαρακτηρίζεται ακατάλληλη και θα φιλτράρεται. Επιπλέον, οι ιστοσελίδες μπορούν να κατηγοριοποιούνται σε λίστες ανάλογα με το θέμα τους (π.χ. μέσα κοινωνικής δικτύωσης, ειδησεογραφικές, μετεωρολογικές, ηλεκτρονικά καταστήματα κλπ). Σε αυτή την περίπτωση, μπορεί να χρησιμοποιούνται κανόνες καταλληλότητας που να προσδιορίζουν πως ιστοσελίδες με συγκεκριμένη θεματική κατηγορία θεωρούνται ακατάλληλες όταν ισχύουν κάποιοι περιορισμοί περιβάλλοντος [95]. Για παράδειγμα,

οι ιστοσελίδες των μέσων κοινωνικής δικτύωσης θα μπορούσαν να χαρακτηρίζονται ως ακατάλληλες κατά τη διάρκεια του ωραρίου εργασίας σε μία επιχείρηση. Για αυτόν τον λόγο μπορεί να μπλοκάρονται τάχιστα με βάση μία λίστα, η οποία περιλαμβάνει όλες τις σελίδες μέσων κοινωνικής δικτύωσης αντί να μπλοκάρεται το κάθε μέσο μεμονωμένα.

- *Φιλτράρισμα ενιαίων εντοπιστών πόρων και συστήματος ονομάτων τομέων (URL filtering & DNS filtering)*: Το φιλτράρισμα ενιαίων εντοπιστών πόρων είναι μια τεχνική φιλτραρίσματος όπου και εδώ μπλοκάρονται διάφορες ιστοσελίδες χρησιμοποιώντας τον ενιαίο εντοπιστή πόρων (URL) της ιστοσελίδας (περισσότερες λεπτομέρειες υπάρχουν στην Ενότητα 4.2.7). Η διαφορά της με το φιλτράρισμα συστήματος ονομάτων τομέων (DNS) είναι πως μπλοκάροντας έναν τομέα μπλοκάρονται όλες οι ιστοσελίδες που περιέχονται σε αυτόν και όχι μεμονωμένες ιστοσελίδες [96]. Για παράδειγμα, σε μία ειδησεογραφική ιστοσελίδα χρησιμοποιώντας φιλτράρισμα ενιαίων εντοπιστών πόρων θα μπορούσαν να μπλοκαριστούν όλες οι αθλητικές ειδήσεις αλλά να επιτρέπονται οι οικονομικές ενώ αντίστοιχα χρησιμοποιώντας φιλτράρισμα συστήματος ονομάτων τομέων κάτι τέτοιο δεν είναι δυνατό. Αλλά στην περίπτωση ενός κακόβουλου ιστότοπου, είναι πιο βολικό και ταχύ να υποστηριχθεί φιλτράρισμα ονομάτων τομέων ώστε να αποκλειστούν όλες οι ιστοσελίδες του ιστότοπου.

Απεικόνιση αρχείων καταγραφής (Log files monitoring)

Τα αρχεία καταγραφής παρέχουν σημαντικές πληροφορίες σχετικά με τα συμβάντα που δημιουργούνται κατά την πλοήγηση των χρηστών στο διαδίκτυο και διαβάζονται ώστε να εντοπιστούν απειλές. Οι πληροφορίες που καταγράφονται αφορούν το αναγνωριστικό του χρήστη (user ID), τον περιηγητή που χρησιμοποιήθηκε, το είδος, την προέλευση και τον χρόνο κατά τα οποία εντοπίστηκε μία απειλή. Η απεικόνιση των αρχείων πραγματοποιείται σε γραφικό περιβάλλον μέσω διαγραμμάτων ώστε το περιεχόμενο των αρχείων να είναι ευανάγνωστο και φιλικό προς κάθε χρήστη του πληροφοριακού συστήματος. [93]

Λογισμικό προστασίας από κακόβουλο λογισμικό (Anti-malware software)

Το λογισμικό προστασίας από κακόβουλο λογισμικό χρησιμοποιείται για να παρέχει προστασία από κακόβουλο λογισμικό, το οποίο τις περισσότερες φορές προέρχεται από ενέργειες που πραγματοποιούνται κατά την πλοήγηση στο διαδίκτυο και εστιάζουν σε: (α) αρχεία που κατεβάζονται με ή χωρίς την θέληση του χρήστη (π.χ. στα πλαίσια φόρτωσης μιας ιστοσελίδας), (β) κώδικα που ο χρήστης προσπαθεί να κατεβάσει, (γ) σε κώδικα Javascript μιας ιστοσελίδας. Το λογισμικό προστασίας από κακόβουλο λογισμικό μπορεί να εντοπίζει απειλές χρησιμοποιώντας υπογραφές ή χρησιμοποιώντας συμπεριφορές και τέλος χρησιμοποιώντας την τεχνική περιορισμού λογισμικού (sandboxing). Η ανίχνευση βασισμένη σε υπογραφές, όπως έχει αναφερθεί και σε προηγούμενο κεφάλαιο, συγκρίνει υπογραφές αρχείων με υπογραφές που είναι καταχωρημένες στη βάση δεδομένων ως κακόβουλα αρχεία και αν οι δύο υπογραφές ταιριάζουν τότε το αρχείο που ελέγχεται χαρακτηρίζεται ως κακόβουλο. Η ανίχνευση βασισμένη σε συμπεριφορές, χρησιμοποιώντας τεχνικές μηχανικής μάθησης εκπαιδεύεται και παρατηρεί τον τρόπο λειτουργίας των συστατικών του πληροφοριακού συστήματος με σκοπό να εντοπίσει ύποπτη

συμπεριφορά (όπως για παράδειγμα η προσπάθεια διαγραφής αρχείων συστήματος) κατά τη διάρκεια που το κακόβουλο λογισμικό βρίσκεται σε λειτουργία. Έτσι, λοιπόν, ο “παραβατικός” τρόπος δράσης του κακόβουλου λογισμικού προδίδει την ταυτότητά του. [97]

Μία ακόμα τεχνική που χρησιμοποιείται από τα λογισμικά προστασίας απέναντι στο κακόβουλο λογισμικό είναι ο περιορισμός λογισμικού (sandboxing). Χρησιμοποιείται ώστε να απομονώσει το ενδεχομένως κακόβουλο λογισμικό, όπως για παράδειγμα ένα εκτελέσιμο αρχείο, και έτσι να περιοριστεί η δράση του και να μη βλάψει το υπόλοιπο σύστημα. Ειδικότερα, όταν πρέπει να εκτελεστεί ένα αρχείο το οποίο δεν είναι βέβαιο πως είναι ασφαλές τότε εκτελείται έχοντας διαθέσιμους τους ελάχιστους δυνατούς πόρους που απαιτούνται ώστε να εκτελεστεί και χωρίς να επικοινωνεί με το υπόλοιπο σύστημα. [97]

5 Σύγκριση Προϊόντων Υπηρεσιών SecaaS

5.1 Εισαγωγή

Για τη σύνταξη αυτού του κεφαλαίου έχουν μελετηθεί 15 προϊόντα ανά κατηγορία υπηρεσίας ασφαλείας (σε αντιστοιχία με τις κατηγορίες του Κεφαλαίου 4) τα οποία εντοπίστηκαν στις αγορές υπηρεσιών νέφους Amazon web services, Google cloud platform, Microsoft Azure αλλά και στο διαδίκτυο. Οπότε, θα γίνει μία παρουσίαση των αποτελεσμάτων/συμπερασμάτων που προκύπτουν μέσα από αυτή την έρευνα. Οι κύριες ερωτήσεις που καλύπτονται από αυτήν την έρευνα είναι η ανάδειξη ιδιαιτεροτήτων ανά κατηγορία υπηρεσιών ασφαλείας, προϊόντων που ξεχωρίζουν, αναμενόμενων λειτουργικών χαρακτηριστικών που δεν καλύπτονται από τα επιλεγμένα προϊόντα καθώς και ο εντοπισμός εταιριών που είτε παρέχουν προϊόντα για παραπάνω από μία κατηγορία ασφάλειας είτε παρέχουν προϊόντα που είναι νεωτεριστικά και αρκετά αποδοτικά ως προς τα κριτήρια που έχουν τεθεί. Η μελέτη πραγματοποιήθηκε με βάση μια σειρά από κριτήρια ανάλυσης ενώ το κριτήριο για την επιλογή/απόρριψη ενός προϊόντος ήταν η ύπαρξη επαρκούς τεκμηρίωσης ώστε να καλύπτονται όσο το δυνατόν περισσότερα από τα κριτήρια ανάλυσης (75% των κριτηρίων). Σε αυτό το σημείο θα πρέπει να τονιστεί ότι σε ορισμένα προϊόντα δεν ήταν δυνατόν να εντοπιστούν όλα τα κριτήρια, για αυτό και ορισμένες τιμές αποτίμησης για κάποια προϊόντα έμειναν κενές. Σαν πόροι πληροφορίας χρησιμοποιήθηκαν κατά κύριο λόγο ιστοσελίδες αγορών (marketplaces), ιστοσελίδες των ίδιων των προϊόντων συμπεριλαμβανομένων φύλλων δεδομένων (datasheets) καθώς και κάποιες ιστοσελίδες που παρουσιάζουν ή συγκρίνουν προϊόντα, οι οποίες βρέθηκαν κατά την διάρκεια της επεξεργασίας των αποτελεσμάτων της αναζήτησης και παρείχαν δυνατότητες αναζήτησης και μια καλή κατηγοριοποίηση των προϊόντων.

Τα κριτήρια που χρησιμοποιήθηκαν είναι τα εξής:

(α) τρόπος παράδοσης

Ανάλυση: Οι τιμές αυτού του κριτηρίου είναι: λογισμικό σαν υπηρεσία (SaaS), πλατφόρμα σαν υπηρεσία (PaaS), υποδομή σαν υπηρεσία (IaaS). Το κύριο όφελος υποστήριξης άνω του ενός τρόπου παράδοσης είναι πως με αυτό τον τρόπο ικανοποιείται μεγαλύτερη μερίδα πελατών ανάλογα με το ποιό είδος ταιριάζει στον καθένα, γεγονός που μεταφράζεται σε αύξηση των πωλήσεων και λογικά των κερδών.

Τα πλεονεκτήματα του λογισμικού σαν υπηρεσία (SaaS) είναι:

- το μικρό κόστος άρα και η εύκολη απόκτηση του για οποιαδήποτε επιχείρηση, ακόμη και για πιο μικρές επιχειρήσεις που τώρα μεταβαίνουν στο νέφος, διότι το μόνο που απαιτείται είναι η δυνατότητα (άδεια) να χρησιμοποιηθεί το λογισμικό χωρίς κάποια α-νάγκη επένδυσης σε λογισμικό & υλικό,
- το κέρδος χρόνου διότι το προσωπικό μιας εταιρείας δεν χρειάζεται να καταναλώσει κάποια προσπάθεια για την εγκατάσταση και ρύθμιση του λογισμικού,
- η εύκολη επέκταση δυνατοτήτων (πχ. μέσω μετάβασης σε αντίστοιχο πακέτο προϊόντος με περισσότερες δυνατότητες),
- και τέλος, η έλλειψη ζητημάτων συμβατότητας λόγω της μη ανάγκης ύπαρξης επιτόπιου φυσικού μηχανήματος για την εγκατάσταση και εκτέλεση του λογισμικού.

Από την άλλη πλευρά τα μειονεκτήματα είναι πιθανά ζητήματα ασφαλείας καθώς όλος ο έλεγχος και η φιλοξενία του λογισμικού άρα και των δεδομένων των χρηστών γίνεται από τον πάροχο και η απαίτηση για πολύ καλή σύνδεση διαδικτύου ώστε η υπηρεσία να μπορεί να καταναλώνεται χωρις προβλήματα/καθυστερήσεις.

Τα πλεονεκτήματα της υποδομής σαν υπηρεσία (IaaS) είναι ο περισσότερος έλεγχος της υποδομής της υπηρεσίας και η δυνατότητα προσωποποιημένης διαμόρφωσης τόσο της υποδομής όσο και της υπηρεσίας ώστε να ανταποκρίνεται στις απαιτήσεις του πελάτη.

Τα μειονεκτήματα είναι και εδώ πιθανά ζητήματα ασφάλειας, πιθανόν υψηλότερο κόστος για την φιλοξενία της υπηρεσίας σε κατάλληλη υποδομή σε σχέση με το μοντέλο SaaS, ενδεχόμενη δυσκολία συνεργασίας & συμβατότητας με ήδη υπάρχοντα συστήματα μιας επιχείρησης, και τέλος το γεγονός πως για τη σωστή λειτουργία της υπηρεσίας μία επιχείρηση εξαρτάται από δύο διαφορετικές οντότητες, και από τον πάροχο του λογισμικού (δηλ. του προϊόντος) και από τον πάροχο των μηχανημάτων (δηλ. υπηρεσιών IaaS για την φιλοξενία του λογισμικού).

Ένα πλεονέκτημα της πλατφόρμας σαν υπηρεσία (PaaS) είναι η ευκολία χρήσης συγκριτικά με την υποδομή σαν υπηρεσία καθώς παρέχονται διάφορα εργαλεία ανάπτυξης & εκτέλεσης ενώ δεν απαιτείται πλήρης παραμετροποίηση του περιβάλλοντος που θα χρησιμοποιηθεί. Από την άλλη πλευρά, μειονεκτήματα είναι ότι δε μπορεί να γίνει εύκολη μετάβαση από έναν πάροχο σε έναν άλλον και πως η δυνατότητα ευέλικτης επιλογής πόρων είναι μικρότερη σε σχέση με την υποδομή σαν υπηρεσία. Βλέπουμε, λοιπόν, ότι η πλατφόρμα σαν υπηρεσία είναι μια ενδιάμεση επιλογή σε σχέση με τις άλλες δύο.

Αν προσπαθήσουμε να ιεραρχήσουμε τα μοντέλα παράδοσης με βάση το σύνολο των παροχών προς τον χρήστη και των σχετικών πλεονεκτημάτων θα λέγαμε ότι πρώτο έρχεται το λογισμικό, μετά η υποδομή και τέλος η πλατφόρμα σαν υπηρεσία. Η πλατφόρμα σαν υπηρεσία βρίσκεται τελευταία διότι παρά τα σχετικά πλεονεκτήματα σε σχέση με το IaaS χρησιμοποιείται κυρίως για την ανάπτυξη εφαρμογών - άρα δεν έχει νόημα να χρησιμοποιηθεί για την παροχή έτοιμων εφαρμογών.

(β) μοντέλο διάταξης

Ανάλυση: Σκοπός του κριτηρίου είναι να ανιχνεύσει ποιο είδος μοντέλου διάταξης προσφέρεται από το κάθε προϊόν, ποιο είναι το πιο συνηθισμένο και για ποιο λόγο καθώς και αν υπάρχουν προϊόντα που προσφέρουν πάνω από ένα είδη μοντέλων διάταξης. Οι τιμές του κριτηρίου είναι: δημόσιο νέφος, ιδιωτικό νέφος, υβριδικό νέφος. Να τονιστεί πως ένα προϊόν μπορεί δυνητικά να αποτιμηθεί με πολλαπλές και όχι μόνο μια τιμή για αυτό το κριτήριο.
Σχετικά με τη σειρά προτίμησης (των τιμών αποτίμησης) το προτιμότερο είναι να υπάρχουν παραπάνω από ένας τρόπος διάταξης ώστε κάθε πελάτης να μπορεί να επιλέξει αυτόν που ταιριάζει καλύτερα στις ανάγκες του. Στη συνέχεια ακολουθεί το δημόσιο νέφος λόγω των πλεονεκτημάτων που έχει και της ευελιξίας που προσφέρει. Μετά ακολουθεί το υβριδικό νέφος, το οποίο δίνει τη δυνατότητα για ταυτόχρονη χρήση και ιδιωτικού και δημόσιου νέφους ανάλογα με την υπηρεσία. Τέλος, αυτό που απομένει είναι το ιδιωτικό νέφος

(γ) κατηγορία ασφάλειας

Ανάλυση: Ουσιαστικά οι τιμές που μπορεί να πάρει αυτό το κριτήριο αφορούν τις δέκα κατηγορίες ασφαλείας που περιγράφονται στο Κεφάλαιο 4. Το γεγονός ότι υπάρχουν επιπλέον μηχανισμοί ασφάλειας σε κάποια προϊόντα, οι οποίοι μπορεί να ανήκουν σε διαφορετικές κατηγορίες ασφάλειας, σε σύγκριση με ένα προϊόν το οποίο έχει σχεδιαστεί συγκεκριμένα για μια μόνο κατηγορία, μπορεί να λειτουργήσει θετικά για κάποιον υποψήφιο αγοραστή και να αυξήσει τις πιθανότητες επιλογής αυτού προϊόντος. Αυτό συμβαίνει διότι ένας πελάτης μπορεί να καλύψει περισσότερες ανάγκες (ασφάλειας) με μόνο ένα προϊόν και να μη χρειαστεί να ψάξει για ξεχωριστά προϊόντα για κάθε κατηγορία (ασφάλειας), κάτι που μεταφράζεται σε οικονομικό όφελος για αυτόν και λιγότερο κόπο. Επομένως, για ένα προϊόν μπορούμε να έχουμε περισσότερες από μια τιμές αποτίμησης, πράγμα το οποίο σημαίνει πως θα καλύπτει περισσότερες κατηγορίες ασφάλειας σε σχέση με αυτήν που ανήκει.

(δ) μοντέλο κόστους

Ανάλυση: Η τιμολόγηση είναι η διαδικασία κατά την οποία μια επιχείρηση ορίζει μια μαθηματική έκφραση ή μοντέλο της τιμής στην οποία θα πουλήσει τα προϊόντα και τις υπηρεσίες της και μπορεί να αποτελεί μέρος του σχεδίου μάρκετινγκ της επιχείρησης. Κοιτάμε το κριτήριο αυτό με βάση 3 διαστάσεις: (α) τον τρόπο χρέωσης (β) τη συχνότητα χρέωσης και (γ) την ύπαρξη διαφορετικών πακέτων χρέωσης. Συνεπώς, ένα προϊόν αποτιμάται με 3 διαφορετικές τιμές για αυτό το κριτήριο, μια για κάθε διάσταση.
Ο τρόπος χρέωσης είναι το κριτήριο με βάση το οποίο η εταιρεία χρεώνει τους πελάτες της δηλαδή τους υποχρεώνει να πληρώσουν για ένα συγκεκριμένο αγαθό ή υπηρεσία χρησιμοποιώντας κάποια μετρήσιμη μετρική (π χ. όγκος δεδομένων).
Η συχνότητα χρέωσης είναι ο αριθμός των περιπτώσεων κατά τις οποίες πραγματοποιείται πληρωμή από τον πελάτη για ένα προϊόν/υπηρεσία σε ένα δεδομένο χρονικό διάστημα (π χ. μία φορά το μήνα).
Τα πακέτα χρέωσης (tiers) είναι διαφορετικές λύσεις υπηρεσιών που προσφέρονται στους πελάτες με διαφορετικά σημεία τιμολόγησης ανεξάρτητα από τον τρόπο χρέωσης που χρησιμοποιείται (πχ πακέτο standard και premium). Μπορεί να έχουμε διαφορετικά επίπεδα εγγυήσεων, όπου κάθε ένα αντιστοιχεί

σε διαφορετικό σημείο τιμολόγησης και άρα κόστος, ενώ λογικά, ο τρόπος χρέωσης θα είναι ο ίδιος. Για έναν υποψήφιο αγοραστή, οι διαφορετικοί τρόποι χρέωσης και πληρωμής ενός προϊόντος μπορούν να λειτουργήσουν πολύ θετικά καθώς έτσι ο αγοραστής θα διαλέξει την επιλογή που του ταιριάζει περισσότερο ανάλογα με τις ανάγκες και τις δυνατότητές του. Επίσης, μας ενδιαφέρει να εφαρμόζεται ένας μόνο αλλά ευέλικτος τρόπος/κριτήριο χρέωσης που να αντιστοιχεί σε χρέωση με βάση την πραγματική χρήση ενός προϊόντος. Το κριτήριο αυτό μπορεί να διαφέρει από μια κατηγορία σε μια άλλη. Στο μοντέλο κόστους όσο περισσότερες είναι οι επιλογές τιμολόγησης (για τις 2 τελευταίες διαστάσεις του κριτηρίου) που προσφέρει ένα προϊόν τόσο το καλύτερο για τους υποψήφιους αγοραστές καθώς έτσι υπάρχει η δυνατότητα να αναπτυχθεί ένα τιμολογιακό πλάνο εξειδικευμένο στις ανάγκες τους.

(ε) μηχανισμοί ασφάλειας

Ανάλυση: το κριτήριο αυτό έχει ως στόχο να ανιχνευθεί πόσοι από τους αναμενόμενους μηχανισμούς ασφάλειας της κατηγορίας έχουν καλυφθεί από το προϊόν και αν παρέχονται από το προϊόν και έξτρα μηχανισμοί ασφάλειας για την ίδια κατηγορία. Δηλαδή υπάρχουν δύο διαστάσεις όπου η πρώτη αποτιμάται σε ποσοστό και η δεύτερη σε σχέση με το πλήθος των επιπλέον μηχανισμών δηλαδή όσο μεγαλύτερο το ποσοστό κάλυψης ή το πλήθος μηχανισμών τόσο το καλύτερο.

(στ) μη λειτουργικές εγγυήσεις

Ανάλυση: Οι μη λειτουργικές εγγυήσεις είναι ένα βασικό στοιχείο μιας συμφωνίας επιπέδου υπηρεσίας (SLA) μεταξύ ενός παρόχου υπηρεσιών και ενός πελάτη. Συμφωνούνται ως μέσο μέτρησης της απόδοσης & αξιοπιστίας της προσφερόμενης υπηρεσίας και περιγράφονται με τέτοιο τρόπο ώστε να αποφεύγονται οι διαφορές μεταξύ των δύο μερών λόγω παρεξήγησης. Ο στόχος αυτού του κριτηρίου είναι να εντοπιστούν μη λειτουργικές εγγυήσεις (όταν υπάρχουν) για ένα προϊόν προς αποτίμηση και πιθανές ποινές που εφαρμόζει ο πάροχός του (στον εαυτό του) εάν δεν τις τηρήσει.

Οι προτιμήσεις ως προς τις τιμές αποτίμησης εξαρτώνται από το είδος του μη λειτουργικού χαρακτηριστικού/ιδιότητας που εμπλέκεται. Εδώ έχουμε να κάνουμε με 2 είδη τέτοιων ιδιοτήτων: (α) με θετική κατεύθυνση δηλαδή όσο πιο μεγάλη τιμή εγγυάται από το προϊόν, τόσο το καλύτερο (π χ. διαθεσιμότητα) και (β) με αρνητική κατεύθυνση δηλαδή όσο πιο χαμηλή τιμή εγγυάται από το προϊόν, τόσο το καλύτερο (π.χ. χρόνος ανάκαμψης από καταστροφές). Το αν οι καλύτερες τιμές για τις ιδιότητες αυτές (κατά μήκος των προϊόντων μιας κατηγορίας) είναι επαρκείς μπορεί να εξαρτάται από την αντίστοιχη κατηγορία ασφάλειας.

Μια συχνή εγγύηση που παρέχεται από υπηρεσίες νέφους αφορά την διαθεσιμότητά τους. Στο πεδίο της ασφάλειας, η διαθεσιμότητα δεν θα πρέπει να είναι μικρότερη του 99.9% διότι δεν κρίνεται αρκετά επαρκής για οποιοδήποτε είδος υπηρεσιών ασφαλείας, οπότε θα πρέπει να ξεπερνά το 99.9% ώστε το σύστημα που προστατεύεται να παραμένει ασφαλές. Όμως, η απαιτούμενη διαθεσιμότητα ενδεχομένως να εξαρτάται από τις ανάγκες ενός οργανισμού και από το πόσο ασφαλές είναι ήδη το σύστημά του. Επίσης, αναμένεται πως το κατώφλι στο ποσοστό διαθεσιμότητας μπορεί να διαφέρει από μια κατηγορία ασφάλειας σε μια άλλη.

(ζ) είδος προσφερόμενης προστασίας

Ανάλυση: Οι υπηρεσίες ασφαλείας ανάλογα με τον τρόπο λειτουργίας τους και τον σκοπό για τον οποίο έχουν σχεδιαστεί προσφέρουν προληπτική (preventive), αντιδραστική (reactive) ή ανιχνευτική (detective) προστασία άρα λοιπόν οι τιμές του κριτηρίου είναι αυτές. Η προληπτική προστασία αφορά υπηρεσίες που λειτουργούν με στόχο να αποτρέψουν μία επίθεση πριν ακόμα αυτή συμβεί, η αντιδραστική αφορά υπηρεσίες οι οποίες αφού συμβεί μία επίθεση έχουν ως στόχο να μετριάσουν τις συνέπειες και να επαναφέρουν το σύστημα σε κανονική ροή λειτουργίας και η ανιχνευτική υπηρεσίες που έχουν ως στόχο να εντοπίσουν μία πιθανή επίθεση ακόμα και αν αυτή βρίσκεται σε εξέλιξη.

Η προληπτική προστασία είναι προτιμότερη από την αντιδραστική διότι προλαβαίνει μία επίθεση πριν ακόμα αυτή συμβεί και η ανιχνευτική προστασία είναι προϋπόθεση για την επίτευξη προληπτικής και αντιδραστικής προστασίας οπότε είναι τελευταία σε κατάταξη.

Το ποιο από τα τρία είδη προστασίας προσφέρεται αναμένεται να εξαρτάται από το είδος του προϊόντος δηλαδή από την κατηγορία ασφάλειας την οποία καλύπτει το προϊόν. Βέβαια μπορεί ορισμένα προϊόντα να ξεπερνούν τα στεγανά μιας κατηγορίας προσφέροντας επιπρόσθετες λειτουργίες ή μηχανισμούς, οι οποίοι μπορεί να εμπίπτουν και σε κάποια άλλη κατηγορία. Σε αυτή την περίπτωση, μπορεί τα προϊόντα αυτά να εμφανίζουν πολλαπλές τιμές για αυτό το κριτήριο, κάτι που είναι περισσότερο προτιμότερο σε σχέση με την εμφάνιση μόνο μιας τιμής.

Τέλος, θεωρούμε πως αν παρέχεται ταυτόχρονα αντιδραστική και προληπτική προστασία για ένα προϊόν, τότε παρέχεται η καλύτερη δυνατή προστασία για αυτό.

(η) ιδιότητες ασφάλειας

Ανάλυση: οι τιμές αυτού του κριτηρίου είναι: ακεραιότητα, εμπιστευτικότητα, διαθεσιμότητα, μη αποποίηση. Οι παραπάνω τιμές αποτελούν τις βασικές ιδιότητες της ασφάλειας, οι οποίες έχουν οριστεί λεπτομερώς στο Κεφάλαιο 3. Όσες περισσότερες ιδιότητες ασφαλείας καλύπτονται από ένα προϊόν τόσο το καλύτερο διότι έτσι λειτουργεί με ασφαλή τρόπο και οι πιθανοί αγοραστές μπορούν να το εμπιστευτούν περισσότερο και κατά συνέπεια να το αγοράσουν.

(θ) προστατευόμενα αντικείμενα

Ανάλυση: Τα αντικείμενα που προστατεύονται είναι ένας σημαντικός παράγοντας για την επιλογή ενός προϊόντος. Όσο περισσότερα είναι τα αντικείμενα που προστατεύονται (πχ. δίκτυο, δεδομένα, εξυπηρετητές) από ένα προϊόν ασφάλειας τόσο το καλύτερο για έναν πελάτη διότι μειώνεται η πολυπλοκότητα και η απαιτούμενη τεχνική κατάρτιση του προσωπικού, τα οποία μεταφράζονται σε μείωση των απαιτούμενων πόρων και άρα του κόστους. Αντιθέτως, αν έπρεπε να χρησιμοποιηθεί ξεχωριστό προϊόν για κάθε αντικείμενο που προστατεύεται, τότε το κόστος θα ήταν από δυσβάσταχτο έως απαγορευτικό, ειδικότερα για μικρές ή ακόμη και μεσαίες επιχειρήσεις.

(ι) αντιμετωπιζόμενες απειλές

Ανάλυση: μια απειλή ορίζεται ως μια πιθανή αρνητική ενέργεια ή συμβάν που διευκολύνεται από μια ευπάθεια που οδηγεί σε ανεπιθύμητη επίδραση σε ένα σύστημα ή εφαρμογή υπολογιστή [98]. Η αποτίμηση των απειλών για ένα προϊόν αφορά την καταγραφή όλων των απειλών που αυτό μπορεί να αντιμετωπίσει. Στόχος μιας τέτοιας καταγραφής είναι να ανιχνευθεί ο αριθμός των απειλών ανά προϊόν αλλά και εκείνες οι απειλές που αντιμετωπίζονται από την πλειονότητα των προϊόντων. Προφανώς, όσες περισσότερες απειλές αντιμετωπίζει ένα προϊόν τόσο το καλύτερο και τόσο πιο ελκυστικό θα είναι στους δυνητικούς του πελάτες.

(ια) περιορισμοί χρήσης

Ανάλυση: Οι περιορισμοί ως προς τη χρήση των προϊόντων αφορούν οτιδήποτε περιορίζει, ελαττώνει, μετριάζει ή εμποδίζει τη λειτουργία ενός προϊόντος πληροφορικής/λογισμικού. Οι περιορισμοί είναι απόλυτα λογικό να υφίστανται καθώς όλα τα προϊόντα πληροφορικής/λογισμικού σε οποιαδήποτε μορφή και αν παρέχονται έχουν κάποια ορισμένη απαίτηση σε υπολογιστική ισχύ. Επομένως, ακόμη και αν η ισχύς που τους παρέχεται ξεπεράσει την μέγιστη απαιτούμενη, λόγω της αρχιτεκτονικής ή/και τις υλοποίησής τους δε μπορούν να την εκμεταλλευτούν. Στόχος του κριτηρίου είναι να εντοπίσει τους περιορισμούς αυτούς (αν αναφέρονται). Είναι αναμενόμενο πως όσο περισσότερους περιορισμούς εμφανίζει ένα προϊόν τόσο μικραίνει η πιθανότητα να ταιριάζει με τις απαιτήσεις και προσδοκίες των δυνητικών του πελατών. Από την άλλη μεριά, όσο πιο μεγάλος είναι ο αριθμός των περιορισμών, τόσο περισσότερη πληροφορία αποκαλύπτεται για ένα προϊόν οπότε και ο πάροχός του μπορεί να θεωρηθεί πιο αξιόπιστος. Ενώ προλαμβάνεται πιθανή απογοήτευση ενός δυνητικού πελάτη κατά την χρήση ενός προϊόντος εφόσον το έχει επιλέξει μη γνωρίζοντας περιορισμούς που δεν έχουν αποκαλυφθεί για αυτό από τον πάροχό του.

(ιβ) δοκιμαστικές εκδόσεις

Ανάλυση: Η δοκιμαστική έκδοση είναι αρκετά σημαντική για τους υποψήφιους αγοραστές και όσο παραπάνω διαρκεί τόσο το καλύτερο διότι ο υποψήφιος αγοραστής μπορεί να χρησιμοποιήσει πιο ολοκληρωμένα το προϊόν και να διαπιστώσει αν ικανοποιεί τις ανάγκες του πριν επενδύσει ένα χρηματικό ποσό για την αγορά του. Επιπλέον, μέσω του κριτηρίου αυτού ελέγχεται και αν ένα προϊόν παρέχεται ελεύθερα, δηλαδή χωρίς κάποια χρέωση. Προφανώς, είναι προτιμότερο για έναν δυνητικό πελάτη/καταναλωτή ένα προϊόν να προσφέρεται ελεύθερα παρά να του παρέχεται μια ελεύθερη δοκιμαστική έκδοση για αυτό που θα λήξει μετά από κάποια προκαθορισμένη περίοδο.

(ιγ) τρόπος χρήσης

Ανάλυση: Η δυνατότητα χρήσης διαφόρων τεχνολογιών αποτελεί όφελος για τα προϊόντα διότι έτσι μπορούν να εκτελέσουν τις υπάρχουσες, προσφερόμενες λειτουργίες με διαφορετικούς τρόπους ανάλογα με την περίπτωση, καλύπτοντας με αυτό τον τρόπο τις διαφορετικές ανάγκες που μπορεί να έχουν οι δυνητικοί πελάτες τους. Ο σκοπός αυτού του κριτηρίου είναι να εντοπίσει εάν, και σε πόσα προϊόντα προσφέρονται διαφορετικοί τρόποι χρήσης τους, οι οποίοι περιλαμβάνουν τις τεχνολογίες

διεπαφής προγραμματισμού εφαρμογών μεταφοράς αναπαραστατικής κατάστασης (RESTful API), την χρήση γραμμής εντολών (command line interface – CLI) και την παροχή γραφικού περιβάλλοντος εργασίας (Graphical User Interface - GUI) μέσω διαδικτύου (web-based GUI).

(ιδ) παροχος

Ανάλυση: σκοπός αυτού του κριτηρίου είναι να δούμε ποια εταιρία παρέχει το κάθε προϊόν και να εντοπιστούν εταιρείες που παρέχουν προϊόντα για περισσότερες από μια κατηγορίες ασφαλείας.

(ιε) αγορές

Ανάλυση: Ο στόχος του κριτηρίου αυτού είναι να εντοπιστεί η αγορά που προσφέρει τον μεγαλύτερο αριθμό προϊόντων και η ύπαρξη προϊόντων που προσφέρονται/διαφημίζονται σε περισσότερες από μια αγορές. Οπότε, οι τιμές αυτού του κριτηρίου είναι: Amazon web services, Google cloud platform, Microsoft Azure καθώς και συνδυασμοί των παραπάνω αγορών αλλά και η «καμία» (δηλ. εντοπίστηκαν στο διαδίκτυο). Σε μία αγορά μπορεί να εμφανίζονται περισσότερα προϊόντα σε σχέση με τις υπόλοιπες για διάφορους λόγους, όπως καλύτερη προσέλκυση παρόχων SecaaS και καλύτερη προσέγγιση στην διαφήμιση τρίτων παρόχων. Επίσης, αναμένουμε πως πολλά προϊόντα μπορούν να εντοπιστούν σε πάνω από μία αγορά, γεγονός που δείχνει ότι οι πάροχοι υπηρεσιών προσπαθούν να πετύχουν τη μέγιστη δυνατή κάλυψη τους αγοράς με τα προϊόντουςους, παρέχοντάς τα μέσα από πολλές αγορές ώστε να προσεγγίσουν μεγάλο αριθμό πελατών.

(ιστ) επίπεδο/είδος υποστήριξης

Ανάλυση:

Ως είδη υποστήριξης για ένα προϊόν θεωρούνται τα μέσα τα οποία χρησιμοποιεί μία εταιρία ώστε να παρέχει υποστήριξη προς τους πελάτες της. Ορισμένα από αυτά τα μέσα απαιτούν ανθρώπους για να χρησιμοποιηθούν (π.χ. τηλέφωνο, emails) ενώ ορισμένα όχι (π.χ. τεκμηρίωση, βίντεο). Το επίπεδο υποστήριξης είναι η ημερολογιακή/χρονική διάρκεια (π.χ. 24 ώρες την ημέρα, 7 ημέρες την εβδομάδα) κατά την οποία προσφέρονται είδη υποστήριξης τα οποία απαιτούν ανθρώπινη παρουσία ώστε να λειτουργήσουν. Όσο υψηλότερο το επίπεδο υποστήριξης τόσο το καλύτερο διότι αυξάνονται οι μέρες και ώρες που υπάρχει κάποιος άνθρωπος διαθέσιμος να μας εξυπηρετήσει. Ο στόχος αυτού του κριτηρίου είναι να εντοπίσει ποια είδη υποστήριξης παρέχονται, αν υπάρχουν πακέτα υποστήριξης όπου το καθένα να προσφέρει και διαφορετικό επίπεδο υποστήριξης και τέλος να εντοπίσει το προϊόν που προσφέρει την καλύτερη δυνατή υποστήριξη (δηλ. υψηλότερο επίπεδο, περισσότερα πακέτα και περισσότερα είδη υποστήριξης).

5.2 Στατιστικά στοιχεία

Παρακάτω παρουσιάζονται τα στατιστικά στοιχεία ανά κριτήριο και τα νικητήρια προϊόντα που προκύπτουν από την αποτίμηση για κάθε κατηγορία προϊόντων SecaaS. Επιπλέον, παρουσιάζονται (καθολικά) στατιστικά και γραφήματα ανά κριτήριο κατά μήκος όλων των κατηγοριών προϊόντων SecaaS

5.2.1 Σύστημα διαχείρισης πληροφοριών και συμβάντων ασφαλείας (Security Information and Event Management - SIEM)

Για αυτή την κατηγορία προϊόντων SecaaS βρέθηκαν 15 προϊόντα με επαρκή τεκμηρίωση, τα οποία αποτιμήθηκαν. Τα αποτελέσματα αποτίμησης εμφανίζονται στον Πίνακα 1 του παραρτήματος. Παρακάτω παρέχουμε μια στατιστική ανάλυση των αποτελεσμάτων αυτών ανά κριτήριο.

Τρόπος παράδοσης: 6 προϊόντα (40%) προσφέρονται σαν λογισμικό, 7 προϊόντα (46.6%) προσφέρονται σαν υποδομή, δηλαδή υπάρχει ένα ολοκληρωμένο περιβάλλον εκτέλεσης της υπηρεσίας, το οποίο είναι ήδη προ εγκατεστημένο σε ιδεατή μηχανή, της οποίας η εικόνα προσφέρεται, και 2 προϊόντα (26.6%) προσφέρονται και σαν λογισμικό και σαν υποδομή. Τα τελευταία δύο προϊόντα είναι το IBM Qradar και το LogRhythm nextgen siem platform, τα οποία είναι τα νικητήρια για το κριτήριο αυτό. Τα παραπάνω αποτελέσματα δεν είναι καθόλου ικανοποιητικά. Σίγουρα περισσότερα προϊόντα θα μπορούσαν να παρέχονται με πάνω από έναν τρόπο ώστε να δώσουν τη δυνατότητα στον υποψήφιο πελάτη να επιλέξει τον τρόπο παράδοσης που ταιριάζει καλύτερα στις ανάγκες του.

Μοντέλο διάταξης: 13 προϊόντα (86.6%) υποστηρίζουν δημόσιο νέφος, 1 προϊόν (6.6%) υποστηρίζει δημόσιο και ιδιωτικό νέφος και 1 προϊόν (6.6%), το Splunk Enterprise Security SIEM, υποστηρίζει δημόσιο, ιδιωτικό και υβριδικό νέφος. Άρα, το τελευταίο προϊόν είναι και το νικητήριο για αυτό το κριτήριο. Από τα αποτελέσματα παρατηρούμε πως υπάρχει προτίμηση προς το δημόσιο νέφος λόγω των πλεονεκτημάτων που αυτό προσφέρει.

Κατηγορία ασφάλειας: 13 προϊόντα (86.6%) δεν καλύπτουν κάποια επιπλέον κατηγορία εκτός από την τρέχουσα. Επίσης, 1 προϊόν (6.6%), το Solarwinds Security Event Manager, προσφέρει επιπρόσθετα υπηρεσίες πρόληψης απώλειας δεδομένων και 1 προϊόν (6.6%), το Alienvault Unified Security Management Anyware, προσφέρει επιπρόσθετα υπηρεσίες ανίχνευσης εισβολών και ασφάλειας δικτύου. Συνεπώς, το τελευταίο προϊόν είναι το νικητήριο για αυτό το κριτήριο. Όμως, θα πρέπει να τονιστεί πως το ποσοστό προϊόντων το οποίο καλύπτει παραπάνω από μία έξτρα κατηγορία ασφάλειας είναι μικρό και θα μπορούσε να ήταν υψηλότερο.

Μοντέλο κόστους: Σχετικά με την τιμολόγηση, 8 προϊόντα (53.3%) τιμολογούνται με βάση τον όγκο των δεδομένων που επεξεργάζονται, 3 προϊόντα (20%) τιμολογούνται ανάλογα με το φόρτο εργασίας (workload), δηλαδή τις εικονικές μηχανές ή τους επεξεργαστές που απαιτούνται για να λειτουργήσει το λογισμικό, 2 προϊόντα (13.3%) με βάση τις συσκευές από τις οποίες μπορούν να συλλέξουν αρχεία καταγραφής και πληροφορίες και 1 προϊόν (6.6%) με βάση τους λογαριασμούς χρηστών.
Επιπλέον, υπάρχει 1 προϊόν (6.6%), το Elastic Security solution SIEM , που δίνει τη δυνατότητα επιλογής τεσσάρων πακέτων πληρωμής (standard, gold, platinum, enterprise) και 1 προϊόν (6.6%), το Alienvault Unified Security Management Anyware, που δίνει τη δυνατότητα επιλογής τριών πακέτων πληρωμής (essentials, standard, premium).
Τέλος, σχετικά με τη χρονική συνιστώσα των πληρωμών, 4 προϊόντα (20%) δίνουν τη δυνατότητα πληρωμής ανά μήνα, και 1 προϊόν (6.6%) πληρωμή ανά μήνα ή ανά έτος. Για ένα προϊόν δεν βρέθηκαν πληροφορίες.
Φαίνεται ότι ο τρόπος τιμολόγησης που χρησιμοποιείται περισσότερο είναι η τιμολόγηση με βάση τον όγκο δεδομένων, κάτι που ήταν αναμενόμενο διότι ο τρόπος λειτουργίας των SIEMs βασίζεται στον έλεγχο δεδομένων (όπως, πχ. αρχεία καταγραφής) από πηγές του συστήματος. Σχετικά με την προσφορά πακέτων μόνο 2 προϊόντα (13.3%) προσφέρουν πολλαπλά πακέτα, αριθμός ο οποίος δεν κρίνεται ικανοποιητικός για την τρέχουσα κατηγορία ασφάλειας, αν λάβουμε υπόψιν ότι τα πολλαπλά πακέτα σημαίνει ευελιξία και όφελος για τον πελάτη. Τέλος, μόνο 5 προϊόντα (33.3%) παρέχουν επιλογές σχετικές με τη συχνότητα πληρωμής το οποίο και πάλι δεν είναι ικανοποιητικό. Κανονικά θα έπρεπε περισσότερα προϊόντα να δίνουν επιλογές σχετικά με τη χρονική συχνότητα διότι τις περισσότερες φορές ο καθορισμός μιας χρονικής συχνότητας (π.χ. πληρωμή ανά έτος) συνοδεύεται και με αντίστοιχες εκπτώσεις στην τιμή. Άρα, λοιπόν, θα έπρεπε να δίνεται η επιλογή είτε για πληρωμή σε τακτά χρονικά διαστήματα για πελάτες με ενδεχομένως μικρή οικονομική δυνατότητα είτε η επιλογή για πληρωμή σε αραιά χρονικά διαστήματα σε συνδυασμό με πιθανή έκπτωση για πελάτες με μεγαλύτερη οικονομική δυνατότητα. Από την παραπάνω ανάλυση προκύπτει πως το Alienvault Unified Security Management Anyware είναι το καλύτερο προϊόν καθώς προσφέρει διαφορετικά πακέτα και έχει έναν ευέλικτο τρόπο χρέωσης που ανταποκρίνεται στην πραγματική χρήση του.

Μηχανισμοί ασφάλειας: Σχετικά με τη λειτουργικότητα που καλύπτεται (δηλ. τους μηχανισμούς ασφάλειας) υπάρχουν 13 προϊόντα (86.6%) που υποστηρίζουν έξτρα λειτουργικότητα πέρα από τη βασική. Υπάρχει 1 προϊόν (6.6%), το Sumo Logic Cloud SIEM Powered by AWS, το οποίο υποστηρίζει μόνο τη βασική λειτουργικότητα και τέλος 1 προϊόν (6.6), το Blumira Modern Cloud SIEM, το οποίο είναι ελλιπές δηλαδή δεν υποστηρίζει πλήρως τη βασική λειτουργικότητα. Τα δύο προϊόντα τα οποία προσφέρουν τις περισσότερες έξτρα λειτουργικότητες είναι τα Alienvault Unified Security Management Anyware και McAfee Enterprise Security Manager SIEM. Τα αποτελέσματα κρίνονται αρκετά ικανοποιητικά καθώς η πλειοψηφία των προϊόντων καλύπτει έξτρα λειτουργικότητες. Αυτό είναι λογικό διότι εφόσον η βασική λειτουργικότητα είναι λίγο πολύ καλυμμένη από όλους τους ανταγωνιστές, θα πρέπει να γίνει κάποια

διαφοροποίηση μέσω έξτρα λειτουργικότητας ώστε να ξεπεραστεί ο ανταγωνισμός. Αποτέλεσμα λοιπόν αυτής της συνεχούς βελτίωσης που προκύπτει από την προσπάθεια για διαφοροποίηση είναι το σημείο στο οποίο βρισκόμαστε, δηλαδή προϊόντα με πολλές λειτουργικότητες.

Μη λειτουργικές εγγυήσεις: Για όλα τα προϊόντα, η διαθεσιμότητα, δηλαδή ο χρόνος που ένα προϊόν είναι πλήρως διαθέσιμο, κυμαίνεται σε ποσοστά από 99.5% έως 100%. Υπάρχει 1 προϊόν με διαθεσιμότητα 100%, 5 προϊόντα με διαθεσιμότητα 99.90% έως 99.99%, 2 προϊόντα με διαθεσιμότητα από 99.5% έως 99.9% και 1 προϊόν με διαθεσιμότητα 99.8%. Για 5 προϊόντα δεν βρέθηκαν πληροφορίες Όταν τα ποσοστά διαθεσιμότητας δεν τηρούνται, ορισμένοι πάροχοι εφαρμόζουν ένα σύστημα ποινών, δηλαδή αποζημιώνουν τον πελάτη διότι δεν τηρήθηκαν τα συμφωνηθέντα. Πιο συγκεκριμένα, τα LogRhythm nextgen siem platform και IBM Qradar για διαθεσιμότητα < 99,9% προσφέρουν 2% πίστωση, για διαθεσιμότητα < 99,0% προσφέρουν 5% πίστωση και για διαθεσιμότητα < 95% προσφέρουν 10% πίστωση της μηνιαίας χρέωσης συνδρομής. Το Datadog cloud siem αν υπάρξει διαθεσιμότητα < 99.8% για δύο διαδοχικούς μήνες δίνει τη δυνατότητα στον πελάτη να διακόψει το συμβόλαιό του. Το Splunk Enterprise Security SIEM για διαθεσιμότητα 99.99-99.999% σε χρονική διάρκεια τριών μηνών πιστώνει το κόστος χρήσης 2 ωρών, για 99.9-99.99% το κόστος χρήσης 8 ωρών, για 95.0-99.0% το κόστος χρήσης 24 ωρών και για διαθεσιμότητα διαθεσιμότητα 0-95.0% το κόστος χρήσης ενός μήνα.
Τα αποτελέσματα φαίνεται πως είναι κάπως ικανοποιητικά και θα μπορούσαν να βελτιωθούν. Η εγγύηση διαθεσιμότητας εξαρτάται από το είδος χρήσης που επιθυμεί να κάνει ένας οργανισμός, τις απαιτήσεις του και από το αναμενόμενο κόστος της υπηρεσίας. Οπότε, το επίπεδο του 99.9% το οποίο εμφανίζεται σε μόνο 6 προϊόντα (40%) μπορεί να είναι ικανοποιητικό για ορισμένους οργανισμούς και ίσως όχι ικανοποιητικό ή αρκετά υψηλό για άλλους. Τέλος, τα συστήματα ποινών μπορούν να λειτουργήσουν θετικά για υποψήφιους πελάτες και να αυξήσουν το επίπεδο εμπιστοσύνης σε έναν πάροχο καθώς ο πάροχος “τιμωρεί τον εαυτό του” αν δεν τηρήσει τα συμφωνηθέντα. Το νικητήριο προϊόν σε αυτό το κριτήριο είναι το Splunk Enterprise Security SIEM το οποίο προσφέρει 100% διαθεσιμότητα. Ταυτόχρονα παρέχει το πιο αυστηρό σύστημα ποινών διότι αρχίζει να αποζημιώνει τους πελάτες για διαθεσιμότητα μικρότερη του 99.999%

Είδος προσφερόμενης προστασίας: Η κύρια λειτουργικότητα σε όλα τα προϊόντα (100%) είναι ανιχνευτική (detective). Αυτό συμβαίνει λόγω της φύσης των προϊόντων σε αυτή την κατηγορία διότι τα SIEM αναλύουν συνεχώς συμβάντα και αρχεία καταγραφής σε πραγματικό χρόνο ώστε να εντοπίζουν μη εξουσιοδοτημένη δραστηριότητα και να δημιουργηθεί μια ειδοποίηση προς τους υπεύθυνους. Βέβαια, η κάλυψη επιπλέον κατηγοριών ασφάλειας τείνει να προσθέσει ένα δεύτερο είδος προστασίας στα προϊόντα ανάλογα βέβαια με την βαρύτητα, καταλληλότητα και έκταση της προσφερόμενης λειτουργικότητας ως προς τις επιπλέον κατηγορίες ασφάλειας. Στην περίπτωση της κατηγορίας SIEM, φαίνεται πως τα 3 προϊόντα που δραστηριοποιούνται σε άλλες κατηγορίες ασφάλειας δεν προσφέρουν κατάλληλο επίπεδο βαρύτητας και έκτασης κάλυψης των αναμενόμενων λειτουργιών σε αυτές τις κατηγορίες. Οπότε,

δεν μπορεί να προστεθεί κάποιος επιπλέον χαρακτηρισμός σε αυτά ως προς επιπλέον είδη προστασίας που μπορεί να προσφέρονται.

Ιδιότητες ασφάλειας: 9 προϊόντα (60%) διασφαλίζουν την ακεραιότητα, 2 προϊόντα (13.3%) διασφαλίζουν την ακεραιότητα, τη διαθεσιμότητα και την εμπιστευτικότητα, 1 προϊόν (6.6%) διασφαλίζει την ακεραιότητα και τη μη αποποίηση, και 1 προϊόν (6.6%) εξασφαλίζει τη διαθεσιμότητα και τη μη αποποίηση. Τέλος, για 2 προϊόντα (13.3%) δε βρέθηκαν πληροφορίες. Παρατηρούμε ότι στα περισσότερα προϊόντα καλύπτεται η ακεραιότητα. Αυτό είναι αναμενόμενο διότι η παρακολούθηση η ίδια είναι ένας παθητικός μηχανισμός, ο οποίος σίγουρα θα εστιάζει στον εντοπισμό μη κανονικών συνθηκών ειδικά ως προς την ακεραιότητα συστημάτων ή δεδομένων που μπορεί να είναι απόρροια κάποιας επίθεσης. Σύμφωνα με τα παραπάνω, τα αποτελέσματα θεωρούνται αναμενόμενα αλλά το ποσοστό των προϊόντων που καλύπτει πάνω από μία ιδιότητα είναι σχετικά μικρό. Οπότε, εδώ η εν λόγω κατηγορία προϊόντων SecaaS χρήζει βελτίωσης. Τα προϊόντα με τον μεγαλύτερο αριθμό από καλυμμένες ιδιότητες είναι τα: Alienvault Unified Security Management Anyware & ClearSkies NG SIEM. Συνεπώς, είναι και τα νικητήρια προϊόντα.

Προστατευόμενα αντικείμενα: 12 προϊόντα (80%) προστατεύουν όλα τα αντικείμενα χωρίς να υπάρχει κάποια συγκεκριμένη πληροφορία, 1 προϊόν (6.6%) προστατεύει τα δεδομένα, 1 προϊόν (6.6%) προστατεύει τα δεδομένα, το δίκτυο και τους ξενιστές (hosts) και 1 προϊόν (6.6%) προστατεύει τα δεδομένα, τα άκρα του δικτύου, την υποδομή και άλλες εφαρμογές. Τα παραπάνω αποτελέσματα θεωρούνται ικανοποιητικά καθώς σε κάθε περίπτωση προστατεύονται τμήματα του πληροφοριακού συστήματος (αν όχι όλο) - αυτό είναι λογικό λόγω της φύσης των προϊόντων αυτής της κατηγορία που δυνητικά μπορούν να παρακολουθήσουν/ανιχνεύσουν γεγονότα ασφάλειας που μπορεί να αφορούν οποιοδήποτε αντικείμενο ενός πληροφοριακού συστήματος. Το προϊόν Alienvault Unified Security Management Anyware, το οποίο προστατεύει τα δεδομένα, το δίκτυο και τους ξενιστές καλύπτει την κατηγορία Siem, την κατηγορία IDS (καθώς περιλαμβάνει network based και host based ids) καθώς και την κατηγορία της ασφάλειας δικτύου (λόγω του προσφερόμενου network based ids). Συνεπώς, εδώ βλέπουμε μια συσχέτιση μεταξύ του αντικειμένου που προστατεύεται με την κατηγορία υπηρεσιών ασφάλειας που προσφέρει την σχετική προστασία σε ένα τέτοιο αντικείμενο.

Αντιμετωπιζόμενες απειλές: 5 προϊόντα προστατεύουν από κακόβουλο λογισμικό, 4 προϊόντα (26.6%) προστατεύουν από λυτρισμικό, 2 προϊόντα (13.3%) προστατεύουν από κακόβουλη δραστηριότητα στα τελικά σημεία, 4 προϊόντα προστατεύουν από παραβιάσεις δεδομένων, 1 προϊόν (6.6%) προστατεύει από απώλεια δεδομένων, κλοπή και απάτη, 2 προϊόντα (13.3%) προστατεύουν από σφάλματα χρηστών, 2 προϊόντα (13.3%) προστατεύουν από πρόσβαση μη εξουσιοδοτημένων χρηστών και τέλος 2 προϊόντα (13.3%) προστατεύουν από ηλεκτρονικό ψάρεμα. Για 8 προϊόντα δεν βρέθηκαν πληροφορίες. Από τις παραπάνω πληροφορίες προκύπτει πως οι πιο συχνά αντιμετωπίσιμες απειλές είναι το κακόβουλο λογισμικό, το λυτρισμικό και οι παραβιάσεις δεδομένων. Τα αποτελέσματα κρίνονται

ικανοποιητικά καθώς βλέπουμε να αντιμετωπίζονται εν γένει αρκετά είδη απειλών ανά προϊόν. Το νικητήριο προϊόν είναι το Alienvault Unified Security Management Anyware γιατί αντιμετωπίζει 7 είδη απειλών την ίδια στιγμή που τα υπόλοιπα προϊόντα αντιμετωπίζουν από 2 έως 5 είδη.

Περιορισμοί χρήσης: υπάρχουν 4 προϊόντα (26.6%) με περιορισμό στον όγκο των δεδομένων που μπορούν να επεξεργαστούν με τιμές από 2500 έως 100.000 γεγονότα ανά δευτερόλεπτο. επίσης, υπάρχει ένα προϊόν (6.6%) με περιορισμό στον όγκο των δεδομένων που εξέρχονται από το σύστημα ανά μήνα, ένα προϊόν (6.6%) με περιορισμό το γεγονός ότι για την απόκτηση του προϊόντος απαιτείται να συμπληρωθεί μια αίτηση, η οποία μπορεί να περιλαμβάνει μόνο επαγγελματικό λογαριασμό ηλεκτρονικού ταχυδρομείου, και τέλος ένα προϊόν (6.6%) έχει ελάχιστη διάρκεια χρήσης το ένα έτος. Για 8 προϊόντα δεν βρέθηκαν πληροφορίες.
Οι περιορισμοί αυτοί θεωρούνται λογικοί - οφείλονται στον τρόπο κατασκευής των προϊόντων και στα είδη υποκείμενων υπηρεσιών νέφους που μπορεί να χρησιμοποιούν. Αντίθετα ο περιορισμός που απαιτεί επαγγελματικό λογαριασμό ηλεκτρονικού ταχυδρομείου και ο περιορισμός που απαιτεί ελάχιστη διάρκεια χρήσης ενός έτους δεν θεωρούνται λογικοί. Ο πρώτος από τους δύο υποχρεώνει τον ενδιαφερόμενο να δημιουργήσει τέτοιου είδους λογαριασμό άρα επεμβαίνει στον τρόπο λειτουργίας της επιχείρησης. Ο δεύτερος δεν δίνει την δυνατότητα για χρήση μικρής χρονικής διάρκειας συνεπώς θέτει μία ελάχιστη οικονομική άνεση την όποια θα πρέπει να έχει μία επιχείρηση ώστε να μπορεί να πληρώσει για δώδεκα μήνες χρήσης.

Δοκιμαστικές εκδόσεις: 6 προϊόντα (40%) παρέχουν δωρεάν δοκιμαστική έκδοση για 14 ή 15 ημέρες, 3 προϊόντα (20%) παρέχουν δωρεάν δοκιμαστική έκδοση για 30 ημέρες, 1 προϊόν (6.6%) παρέχει δοκιμαστική έκδοση από τη μέρα ενεργοποίησης έως το τέλος του επόμενου μήνα (31 έως 60 ημέρες), 1 προϊόν (6.6%) παρέχει δοκιμαστική έκδοση χωρίς να αναφέρεται η χρονική διάρκεια και 4 προϊόντα (26.6%) δεν παρέχουν καμία δωρεάν έκδοση.
Βλέπουμε πως 4 προϊόντα (περίπου 1/4) προσφέρουν δοκιμαστική έκδοση για 1 μήνα ή παραπάνω ενώ υπάρχουν και 4 προϊόντα που δεν προσφέρουν καμία δωρεάν έκδοση. Αυτό σημαίνει πως η απόδοση για αυτό το κριτήριο θα μπορούσε να είναι καλύτερη για αυτή την κατηγορία προϊόντων. Από την άλλη, περίπου ένα 75% δίνει κάποια δοκιμαστική έκδοση, ακόμη και μικρής διάρκειας, το οποίο θα μπορούσε να χαρακτηριστεί κάτι καλό αλλά όχι αρκετά ικανοποιητικό.

Τρόπος χρήσης: 6 προϊόντα (40%) υποστηρίζουν διεπαφή προγραμματισμού εφαρμογών μεταφοράς αναπαραστατικής κατάστασης (RESTful API), χρήση γραμμής εντολών και γραφικό περιβάλλον εργασίας μέσω διαδικτύου. 5 προϊόντα (33.3%) υποστηρίζουν διεπαφή προγραμματισμού εφαρμογών μεταφοράς αναπαραστατικής κατάστασης (RESTful API) και γραφικό περιβάλλον εργασίας μέσω διαδικτύου. 1 προϊόν (6.6%) υποστηρίζει χρήση γραμμής εντολών και διεπαφή προγραμματισμού εφαρμογών μεταφοράς αναπαραστατικής κατάστασης (RESTful API). 1 προϊόν (6.6%) υποστηρίζει χρήση γραμμής εντολών και γραφικό περιβάλλον εργασίας μέσω διαδικτύου. 1 προϊόν (6.6%)

υποστηρίζει γραφικό περιβάλλον εργασίας μέσω διαδικτύου και τέλος για 2 προϊόντα (13.3%) δεν βρέθηκαν πληροφορίες.
Αν δούμε τις τιμές αποτίμησης μεμονωμένα η διεπαφή προγραμματισμού εφαρμογών μεταφοράς αναπαραστατικής κατάστασης (RESTful API) και το γραφικό περιβάλλον εργασίας μέσω διαδικτύου εμφανίζονται σε 12 προϊόντα (80%). Η γραμμή εντολών εμφανίζεται σε 7 προϊόντα (46.6%). Τα αποτελέσματα θεωρούνται ικανοποιητικά καθώς παρατηρούμε πως όλα τα προϊόντα, εκτός από ένα, υποστηρίζουν δύο ή τρεις τεχνολογίες.

Αγορές: 1 προϊόν (6.6%) εντοπίστηκε στο Amazon web services, 1 προϊόν (6.6%) στο Google cloud platform και 4 προϊόντα (26.6%) στο Microsoft Azure. 1 προϊόν (6.6%) εντοπίστηκε σε Amazon web services και Google cloud platform, 2 προϊόντα (13,3%) εντοπίστηκαν σε Amazon web services και Microsoft Azure, 2 προϊόντα (13,3%) εντοπίστηκαν σε Amazon web services, Microsoft Azure και Google cloud platform και τέλος 4 προϊόντα (26.6%) εντοπίστηκαν στο διαδίκτυο και όχι σε κάποια αγορά.
Σαν συνολικό αποτέλεσμα από τα παραπάνω προκύπτει ότι στο Microsoft Azure βρέθηκαν 8 από τα προϊόντα (53.3%), στο Amazon web services βρέθηκαν 6 από τα προϊόντα (40%) και τέλος στο Google cloud βρέθηκαν 4 από τα προϊόντα (26.6%). Γίνεται, λοιπόν, φανερό ότι τα περισσότερα προϊόντα είναι διαθέσιμα στην αγορά της Microsoft Azure.
Όμως, μόνο 5 προϊόντα βρέθηκαν σε παραπάνω από μία αγορές άρα τα αποτελέσματα δεν είναι πολύ ικανοποιητικά. Απεναντίας, περισσότερα προϊόντα θα μπορούσαν να συμμετέχουν σε πολλαπλές αγορές και έτσι να μπορούν να εντοπιστούν πιο εύκολα από τους μελλοντικούς αγοραστές. Νικητήρια προϊόντα για αυτή την κατηγορία είναι αυτά που εμφανίζονται και στις τρεις αγορές, δηλαδή το IBM Qradar και το Elastic Security solution SIEM

Επίπεδο/είδος υποστήριξης: Σχετικά με το είδος υποστήριξης, 13 προϊόντα (86.6%) προσφέρουν υποστήριξη μέσω τηλεφώνου, 9 προϊόντα (60%) μέσω email, 8 προϊόντα (53.3%) μέσω δελτίων (tickets), 4 προϊόντα (26.6%) διαθέτουν κοινότητα (community), 6 προϊόντα (40%) διαθέτουν τεκμηρίωση (documentation), 4 προϊόντα (26.6%) διαθέτουν πύλη υποστήριξης (portal), 4 προϊόντα (26.6%) διαθέτουν έγγραφα με πληροφορίες, 3 προϊόντα (20%) διαθέτουν forum, 3 προϊόντα (20%) διαθέτουν βίντεο, 3 προϊόντα (20%) διαθέτουν πιθανές ερωτήσεις και τις απαντήσεις τους και 2 προϊόντα (13,3%) προσφέρουν ενημέρωση για νέες εκδόσεις. Τέλος υπάρχουν διάφοροι τρόποι υποστήριξης που παρέχονται από μεμονωμένα προϊόντα όπως χάρτης προϊόντων, blog, επικοινωνία μέσω μηνυμάτων (chat), κέντρο επιδιόρθωσης προβλημάτων και λογαριασμός στο twitter.
Υπάρχουν τρία προϊόντα τα οποία παρέχουν πακέτα υποστήριξης. Το Elastic security solution siem προσφέρει 4 πακέτα. Το πακέτο standard προσφέρει επικοινωνία μέσω διαδικτύου και απάντηση σε 3 εργάσιμες ημέρες. Το πακέτο gold προσφέρει επικοινωνία μέσω διαδικτύου και τηλεφώνου σε ώρες καταστημάτων. Τα πακέτα Platinum και Enterprise προσφέρουν επικοινωνία μέσω διαδικτύου και τηλεφώνου 24 ώρες την ημέρα, 365 μέρες το χρόνο. Για επείγον περιστατικό ο χρόνος απάντησης είναι 4

ώρες, για υψηλό περιστατικό ο χρόνος απάντηση είναι 1 ημέρα και για κανονικό περιστατικό ο χρόνος απάντησης είναι 2 εργάσιμες ημέρες.
Το Splunk Enterprise Security SIEM προσφέρει 2 πακέτα, το standard και το premium, με τη διαφορά να βρίσκεται πως στο premium υπάρχει γρηγορότερη απόκριση και ομάδα υποστήριξης.
Το Alienvault Unified Security Management Anyware προσφέρει 2 πακέτα υποστήριξης. Το standard παρέχει υποστήριξη 10 ώρες την ημέρα, 5 ημέρες την εβδομάδα ενώ το premium παρέχει υποστήριξη 24 ώρες την ημέρα, 7 ημέρες την εβδομάδα.
Για την ημερολογιακή/χρονική διάρκεια κατά την οποία παρέχεται υποστήριξη βρέθηκαν πληροφορίες μόνο σε 5 προϊόντα. Υπάρχουν 3 προϊόντα που παρέχουν τηλεφωνική υποστήριξη 24 ώρες την ημέρα, 7 ημέρες την εβδομάδα. Τα άλλα 2 προϊόντα που απομένουν είναι τα Alienvault Unified Security Management Anyware και Elastic security solution siem. Οι πληροφορίες σχετικά με την ημερολογιακή/χρονική διάρκεια υποστήριξης για αυτά τα 2 προϊόντα έχουν αναφερθεί στην προηγούμενη παράγραφο. Για τα υπόλοιπα προϊόντα για τα οποία δεν υπάρχουν πληροφορίες θεωρούμε ότι ακολουθούν εργάσιμο ωράριο άρα η ημερολογιακή/χρονική διάρκεια δεν καλύπτεται επαρκώς.
Τα αποτελέσματα μπορούν να χαρακτηριστούν παραπάνω από ικανοποιητικά αν εξετάσουμε την ποικιλία που υπάρχει σχετικά με τους τρόπους υποστήριξης σε αυτή την κατηγορία προϊόντων. Βέβαια υπάρχουν μόνο 3 προϊόντα που παρέχουν διαφορετικά πακέτα υποστήριξης και αυτό δεν είναι ικανοποιητικό. Θα έπρεπε να υπάρχουν περισσότερα προϊόντα με αυτή τη δυνατότητα ώστε ο κάθε πελάτης να έχει τη δυνατότητα να επιλέξει το αντίστοιχο επίπεδο υποστήριξης ανάλογα με τους οικονομικούς πόρους που διαθέτει. Το νικητήριο προϊόν σε αυτή την κατηγορία είναι το Alienvault Unified Security Management Anyware διότι προσφέρει 10 διαφορετικούς τρόπους/είδη υποστήριξης και τη δυνατότητα επιλογής ανάμεσα σε διαφορετικά πακέτα.

Νικητήριο προϊόν για ολόκληρη την κατηγορία είναι το Alienvault Unified Security Management Anyware το οποίο εμφανίζεται ως νικητήριο 6 φορές.

5.2.2 Επιχειρησιακή συνέχεια και αποκατάσταση καταστροφών (Business Continuity and Disaster Recovery)

Για αυτή την ενότητα βρέθηκαν 15 προϊόντα με επαρκή τεκμηρίωση, τα οποία αποτιμήθηκαν. Τα αποτελέσματα αποτίμησης εμφανίζονται στον Πίνακα 2 του παραρτήματος. Παρακάτω παρέχουμε μια στατιστική ανάλυση των αποτελεσμάτων αυτών ανά κριτήριο.

Τρόπος παράδοσης: 4 προϊόντα (26.6%) προσφέρονται σαν λογισμικό, 7 προϊόντα (46.6%) προσφέρονται σαν υποδομή και 4 προϊόντα (26.6%) (δείτε πίνακα αποτίμησης) προσφέρονται και σαν λογισμικό και σαν υποδομή, τα οποία είναι και τα νικητήρια. Τα παραπάνω αποτελέσματα θα λέγαμε ότι δεν θεωρούνται ούτε ικανοποιητικά αλλά ούτε και μη ικανοποιητικά. Σίγουρα περισσότερα προϊόντα θα μπορούσαν να παρέχονται με πάνω από έναν τρόπο αλλά βλέπουμε μία σχετική “διασπορά” στους

τρόπους παράδοσης. Δηλαδή δεν κυριαρχεί με μεγάλη διαφορά μόνο ένας τρόπος ώστε αυτό να είναι ένα δεσμευτικό (με αρνητικό πρόσημο) για τον υποψήφιο αγοραστή.

Μοντέλο διάταξης: 12 προϊόντα (80%) υποστηρίζουν δημόσιο νέφος, 2 προϊόντα (13.3%) υποστηρίζουν δημόσιο και ιδιωτικό νέφος και 1 προϊόν (6.6%) υποστηρίζει ιδιωτικό νέφος. Τα νικητήρια προϊόντα είναι τα Axcient x360 recover d2c και Arcserve UDP Cloud Hybrid, τα οποία υποστηρίζουν δύο μοντέλα διάταξης. Από τα αποτελέσματα παρατηρούμε πως υπάρχει προτίμηση προς το δημόσιο νέφος λόγω των πλεονεκτημάτων που αυτό προσφέρει.

Κατηγορία ασφάλειας: 7 προϊόντα (46.6%) δεν καλύπτουν κάποια επιπλέον κατηγορία και 8 προϊόντα (53.3%) καλύπτουν επιπρόσθετα την κατηγορία της κρυπτογράφησης. Τα νικητήρια προϊόντα είναι αυτά που καλύπτουν δύο κατηγορίες. Τα αποτελέσματα είναι πολύ ικανοποιητικά καθώς βλέπουμε ότι σχεδόν τα μισά προϊόντα καλύπτουν μία επιπλέον κατηγορία. Η κρυπτογράφηση είναι ένα απαραίτητο χαρακτηριστικό των προϊόντων διότι τα δεδομένα και ειδικότερα τα ευαίσθητα/προσωπικά δεδομένα θα πρέπει οπωσδήποτε να κρυπτογραφούνται ώστε να παραμένουν προστατευμένα. Επομένως, θα πρέπει να υπάρχει βελτίωση ως προς αυτή την πλευρά για τα προϊόντα αυτής της κατηγορίας.

Μοντέλο κόστους: Σχετικά με την τιμολόγηση, για 1 προϊόν δεν βρέθηκαν πληροφορίες. 4 προϊόντα (26.6%) τιμολογούνται με βάση τον όγκο των δεδομένων που χρησιμοποιούνται ενώ 5 προϊόντα (33.3%) τιμολογούνται ανάλογα με το φόρτο εργασίας (workload), δηλαδή τις εικονικές μηχανές ή τους επεξεργαστές που απαιτούνται για να λειτουργήσει το λογισμικό. 1 προϊόν (6.6%) τιμολογείται με βάση με βάση τον όγκο των δεδομένων ή τις εικονικές μηχανές και 1 προϊόν (6.6%) τιμολογείται με βάση το μοντέλο tailored fit pricing.
Σχετικά με την ύπαρξη πακέτων, 2 προϊόντα (13.3%) παρέχουν τέσσερα πακέτα τιμολόγησης με διαφορές ως προς τα στιγμιότυπα εικονικών μηχανών, τους λογαριασμούς ως προς τον αντίστοιχο πάροχο και τον αριθμό χρηστών. 1 προϊόν (6.6%) προσφέρει ένα πακέτο χρέωσης αν χρησιμοποιηθεί πάνω σε εφαρμογές SaaS, δύο πακέτα χρέωσης αν χρησιμοποιηθεί πάνω σε σύμπλεγμα Kubernetes και τρία πακέτα χρέωσης αν χρησιμοποιηθεί πάνω σε εικονικές μηχανές. Συνεπώς, ανάλογα με το σημείο πάνω στο οποίο εφαρμόζεται αλλάζει και το κριτήριο με το οποίο γίνεται η χρέωση των πακέτων. Τέλος, 1 προϊόν (6.6%), το οποίο εφαρμόζει τιμολόγηση με βάση το φόρτο εργασίας, προσφέρει πέντε διαφορετικά πακέτα με τις αντίστοιχες παροχές.
Τέλος, σχετικά με τη χρονική συνιστώσα των πληρωμών, 3 προϊόντα (20%) δίνουν τη δυνατότητα πληρωμής ανά μήνα, και 1 προϊόν (6.6%) πληρωμή ανά μήνα ή ανά έτος ή ανά δύο έτη με τις αντίστοιχες εκπτώσεις.
Φαίνεται ότι οι τρόποι τιμολόγησης που χρησιμοποιούνται περισσότερο είναι η τιμολόγηση με βάση τον όγκο δεδομένων και η τιμολόγηση με βάση το φόρτο εργασίας. Σχετικά με την προσφορά πακέτων 4 προϊόντα προσφέρουν πολλαπλά πακέτα, αριθμός ο οποίος δεν είναι ούτε ικανοποιητικός αλλά ούτε και απογοητευτικός. Το ίδιο ισχύει για την συχνότητα πληρωμής όπου μόνο 4 προϊόντα προσφέρουν

σχετικές πληροφορίες. Επιπλέον, όπως έχει αναφερθεί, ο καθορισμός μιας χρονικής συχνότητας (π.χ. πληρωμή ανά έτος) είναι καλό να συνοδεύεται και με αντίστοιχες εκπτώσεις στην τιμή. Κάτι τέτοιο βλέπουμε ότι εδώ εφαρμόζεται μόνο για ένα προϊόν. Από την παραπάνω ανάλυση προκύπτει πως το Cloud Daddy Secure Backup Enterprise Edition είναι το καλύτερο προϊόν καθώς προσφέρει τέσσερα διαφορετικά πακέτα χρέωσης και την ίδια στιγμή προσφέρει τρεις διαφορετικές επιλογές χρονικής συχνότητας, οι οποίες συνοδεύονται και από εκπτώσεις.

Μηχανισμοί ασφάλειας: Υπάρχουν 13 προϊόντα (86.6%) τα οποία καλύπτουν τη βασική αλλά και έξτρα λειτουργικότητα και 2 προϊόντα (13.3%) τα οποία καλύπτουν μόνο τη βασική λειτουργικότητα, το Commvault backup and recovery και το Hystax Backup and Disaster Recovery to AWS. Το προϊόν το οποίο παρέχει τις περισσότερες έξτρα λειτουργικότητες είναι το Cloud Daddy Secure Backup Enterprise Edition, το οποίο είναι και το νικητήριο. Τέλος, μία διευκρίνιση που αφορά τον πίνακα αποτίμησης είναι πως τα προϊόντα cohesity dataplatform dataprotect (για backup) και cohesity dataplatform sitecontinuity (για disaster recovery) είναι δύο διαφορετικά προϊόντα τα οποία λήφθηκαν υπόψη σαν ένα προϊόν. Αυτό συνέβη διότι είναι προϊόντα της ίδιας εταιρείας που πρέπει να συνδυαστούν για να προκύψει μία λύση BCDR.
Τα αποτελέσματα για αυτή την κατηγορία κρίνονται πολύ ικανοποιητικά καθώς δεν υπάρχει ούτε ένα προϊόν που να μην καλύπτει τη βασική λειτουργικότητα. Αντιθέτως σχεδόν όλα τα προϊόντα καλύπτουν και επιπλέον λειτουργικότητες.

Μη λειτουργικές εγγυήσεις: Υπάρχει 1 προϊόν (6.6%) με διαθεσιμότητα 99.9999% και επιτυχία δημιουργίας αντιγράφων ασφαλείας 97.5%. Υπάρχουν 4 προϊόντα (26.6%) με διαθεσιμότητα 99.9% και 1 προϊόν με διαθεσιμότητα 99%.
επίσης, υπάρχει 1 προϊόν (6.6%) με Χρονικό Σημείο Ανάκτησης Δεδομένων (RPO) 5 λεπτά και Χρονικό Στόχο Ανάκαμψης (RTO) μικρότερο των 30 δευτερολέπτων. Υπάρχει 1 προϊόν (6.6%) με Χρονικό Σημείο Ανάκτησης Δεδομένων (RPO) 1 ώρα και Χρονικό Στόχο Ανάκαμψης (RTO) από 15 έως 20 λεπτά. Υπάρχει 1 προϊόν (6.6%) με Χρονικό Σημείο Ανάκτησης Δεδομένων (RPO) μικρότερο από 15 λεπτά και Χρονικό Στόχο Ανάκαμψης (RTO) μικρότερο των 5 λεπτών. Τέλος, υπάρχει 1 προϊόν (6.6%) με Χρονικό Σημείο Ανάκτησης Δεδομένων (RPO) 15 λεπτά και Χρονικό Στόχο Ανάκαμψης (RTO) 1 ώρα. Για 5 προϊόντα δεν βρέθηκαν πληροφορίες. Παρατηρούμε πως μόνο 4 προϊόντα παρέχουν πληροφορίες για τα RTO και RPO. Αυτό δεν είναι ικανοποιητικό διότι αυτές οι εγγυήσεις είναι πολύ κρίσιμες για αυτή την κατηγορία και ενδεχομένως να αποτελούν και ένα από τα κριτήρια αξιολόγησης για την αγορά ενός προϊόντος. Το ίδιο ισχύει για τις εγγυήσεις διαθεσιμότητας που διατίθενται μόνο σε 5 προϊόντα.
Όταν τα ποσοστά διαθεσιμότητας δεν τηρούνται, ορισμένοι πάροχοι εφαρμόζουν ένα σύστημα ποινών, δηλαδή αποζημιώνουν τον πελάτη διότι δεν τηρήθηκαν τα συμφωνηθέντα. Πιο συγκεκριμένα, το Appranix Cloud Application Resilience για κάθε διακοπή μεγαλύτερη από 1 ώρα, πιστώνει το 2% των τελών υπηρεσίας για κάθε περίοδο 30 ή περισσότερων διαδοχικών λεπτών διακοπής λειτουργίας. Το Commvault Backup & Recovery, αν το μηνιαίο ποσοστό προσβασιμότητας είναι μικρότερο από 99,9%,

τότε ισχύει πίστωση 10% των τελών υπηρεσίας και αν είναι μικρότερο του 99% ισχύει πίστωση 25% των τελών υπηρεσίας για τον τρέχων μήνα. Το Barracuda Backup προσφέρει επιστροφή χρημάτων σε αναλογική βάση για το ποσό του επιπλέον χρόνου διακοπής λειτουργίας, πάνω από τη δέσμευση χρόνου λειτουργίας.

Τα αποτελέσματα φαίνεται πως δεν είναι ικανοποιητικά και θα μπορούσαν να βελτιωθούν. Η εγγύηση διαθεσιμότητας όπως και το χρονικό σημείο ανάκτησης δεδομένων και ο χρονικός στόχος ανάκαμψης εξαρτώνται από το είδος χρήσης που επιθυμεί να κάνει ένας οργανισμός, τις απαιτήσεις του και από το αναμενόμενο κόστος της υπηρεσίας. Οπότε, το επίπεδο διαθεσιμότητας του 99.9% και άνω, το οποίο εμφανίζεται σε μόνο 5 προϊόντα (40%), μπορεί να είναι ικανοποιητικό για ορισμένους οργανισμούς και ίσως όχι ικανοποιητικό ή αρκετά υψηλό για άλλους. Παρόλα αυτά το κύριο μειονέκτημα είναι πως δεν υπάρχει κανένα προϊόν το οποίο να συνδυάζει υψηλή διαθεσιμότητα και εγγυήσεις για Χρονικό Σημείο Ανάκτησης Δεδομένων (RPO) και Χρονικό Στόχο Ανάκαμψης (RTO). Αυτό θα έπρεπε να συμβαίνει ώστε η υπηρεσία να είναι συνεχώς διαθέσιμη και ταυτόχρονα να ικανοποιεί τις αντίστοιχες απαιτήσεις των χρηστών (για RTO & RPO).

Το νικητήριο προϊόν ως προς την εγγύηση της διαθεσιμότητας και την ύπαρξη συστήματος ποινών είναι το Barracuda Backup διότι είναι ένα από τα τρία προϊόντα με εγγύηση διαθεσιμότητας 99.9% και διαθέτει το πιο δίκαιο σύστημα ποινών. Ο χρήστης δεν αποζημιώνεται με κάποιο προκαθορισμένο ποσοστό αλλά με το ακριβές ποσό για τον χρόνο διακοπής. Ως πρός το χρονικό σημείο ανάκτησης δεδομένων και το χρονικό στόχο ανάκαμψης το νικητήριο προϊόν είναι το N2WS Backup & Recovery for AWS Standard Edition διότι προσφέρει τις ελάχιστες τιμές και για τις δύο αυτές παραμέτρους.

Είδος προσφερόμενης προστασίας: Η κύρια λειτουργικότητα σε όλα τα προϊόντα (100%) είναι προληπτική (proactive) και αντιδραστική (reactive). Αυτό συμβαίνει διότι η επιχειρησιακή συνέχεια είναι ένας προληπτικός μηχανισμός. Η δημιουργία αντιγράφων ασφαλείας πραγματοποιείται κατά το διάστημα κανονικής λειτουργίας ενός οργανισμού. Ένας από τους διάφορους λόγους που δημιουργούνται είναι για να αντιμετωπιστεί το ενδεχόμενο του να υπάρξει κάποια επίθεση/καταστροφή, η οποία θα διαταράξει την ομαλή λειτουργία του οργανισμού. Σε αυτή την περίπτωση τα αντίγραφα ασφαλείας θα χρησιμοποιηθούν ώστε να περιοριστεί στο ελάχιστο η απώλεια δεδομένων. Μπορούμε να πούμε, λοιπόν, ότι πρόκειται για πρόληψη, δηλαδή γίνεται προσπάθεια για να προλάβουμε εκ των προτέρων και να αποτρέψουμε κάποιες αρνητικές ή ανεπιθύμητες καταστάσεις, ενέργειες ή συνέπειες [99]. Η ανάκαμψη από καταστροφές είναι ένας αντιδραστικός μηχανισμός. Δηλαδή είναι ένας μηχανισμός ο οποίος ενεργοποιείται αφού έχει συμβεί η καταστροφή. Έχει ως στόχο να επαναφέρει την ομαλή λειτουργία του οργανισμού όσο αυτό είναι δυνατόν και γενικότερα να μετριάσει τις συνέπειες. Άρα, λοιπόν, αντιδρά στην καταστροφή, η οποία έχει συμβεί προηγουμένως.

Ιδιότητες ασφάλειας: Όλα τα προϊόντα (100%) εξασφαλίζουν τη διαθεσιμότητα και 8 προϊόντα (53.3%) εκτός από την διαθεσιμότητα εξασφαλίζουν και την εμπιστευτικότητα. Αυτό είναι αναμενόμενο λόγω της φύσης των προϊόντων. Είτε πρόκειται για επιχειρησιακή συνέχεια είτε πρόκειται για ανάκαμψη από

καταστροφές και στις δύο περιπτώσεις το κύριο ζητούμενο είναι να εξασφαλιστεί η διαθεσιμότητα. Η διαφορά είναι πως ο ένας μηχανισμός λειτουργεί προληπτικά και ο άλλος αντιδραστικά όπως έχει αναφερθεί στο προηγούμενο κριτήριο. Η εμπιστευτικότητα είναι επακόλουθο της κρυπτογράφησης, η οποία προσφέρεται ως έξτρα λειτουργικότητα από τα 8 προαναφερθέντα προϊόντα. Όταν τα δεδομένα κρυπτογραφούνται υπάρχει εμπιστευτικότητα διότι ακόμα και αν κάποιος τρίτος καταφέρει να τα αναγνώσει (λόγω της κρυπτογραφημένης μορφής τους) δεν θα καταλάβει περί τίνος πρόκειται. Σύμφωνα με τα παραπάνω, τα αποτελέσματα θεωρούνται αναμενόμενα και ικανοποιητικά καθώς πάνω από τα μισά προϊόντα καλύπτουν δύο ιδιότητες. Τα προϊόντα που καλύπτουν δύο ιδιότητες (δείτε πίνακα αποτίμησης) είναι και τα νικητήρια.

Προστατευόμενα αντικείμενα: 9 προϊόντα (60%) προστατεύουν όλα τα αντικείμενα χωρίς να υπάρχει κάποια πιο συγκεκριμένη πληροφορία, 2 προϊόντα (13.3%) προστατεύουν τα δεδομένα, 2 προϊόντα (13.3%) προστατεύουν ολόκληρα περιβάλλοντα εφαρμογών, 1 προϊόν (6.6%) προστατεύει κρίσιμα δεδομένα για τις επιχειρήσεις, 1 προϊόν (6.6%) προστατεύει αρχεία που βρίσκονται σε φυσικά περιβάλλοντα, εικονικές συσκευές ή στο δημόσιο νέφος. Τα παραπάνω αποτελέσματα θεωρούνται ικανοποιητικά καθώς σε κάθε περίπτωση προστατεύονται τμήματα του πληροφοριακού συστήματος. Νικητήρια προϊόντα είναι τα Appranix Cloud Application Resilience και Commvault Backup & Recovery, τα οποία προστατεύουν ολόκληρα περιβάλλοντα εφαρμογών.

Αντιμετωπίζόμενες απειλές: Για 3 προϊόντα δεν βρέθηκαν πληροφορίες. 12 προϊόντα (80%) προστατεύουν από το λυτρισμικό, 4 προϊόντα (26.6%) προστατεύουν από διακοπές λειτουργίας, 2 προϊόντα (13.3%) προστατεύουν από ανθρώπινα λάθη, 2 προϊόντα (13.3%) προστατεύουν από απώλεια δεδομένων, 2 προϊόντα (13.3%) προστατεύουν από κακόβουλες ενέργειες, 1 προϊόν (6.6%) προστατεύει από παραβιάσεις, 1 προϊόν (6.6%) προστατεύει από αστοχίες υλικού ενώ 4 προϊόντα (26.6%) προστατεύουν από καταστροφές. Βλέπουμε ότι όλα τα προϊόντα καλύπτουν το λυτρισμικό γιατί εφόσον δημιουργούνται αντίγραφα ασφαλείας τα δεδομένα δεν μπορούν να χαθούν. Ως προς τον αριθμό απειλών που καλύπτονται ανά προϊόν 2 προϊόντα (13.3%) καλύπτουν μία απειλή, 5 προϊόντα (33.3%) καλύπτουν 2 απειλές, 4 προϊόντα (26.6%) καλύπτουν τρεις απειλές και 1 προϊόν (6.6%) καλύπτει τέσσερις απειλές. Νικητήριο προϊόν είναι το Zerto platform το οποίο προσφέρει προστασία απέναντι σε τέσσερα είδη απειλών την ίδια στιγμή που τα υπόλοιπα προϊόντα προσφέρουν προστασία απέναντι σε ένα έως τρία είδη.

Περιορισμοί χρήσης: 1 προϊόν (6.6%) έχει μέγιστη συχνότητα δημιουργίας αντιγράφων ασφαλείας ανά 5 λεπτά και 1 προϊόν (6.6%) μέγιστη συχνότητα τα 15 λεπτά. Υπάρχει 1 προϊόν όπου η επιστροφή σε κανονική λειτουργία (failback) διαρκεί από 1 ώρα έως 1 με 2 ημέρες. Υπάρχει 1 προϊόν (6.6%) όπου υπάρχουν έως 4000 σημεία επαναφοράς για κάθε αντίγραφο ασφαλείας. Υπάρχει 1 προϊόν (6.6%) για το οποίο πωλείται μία άδεια χρήσης, η οποία είναι ένα πακέτο το οποίο μπορεί να καλύψει 10 φορτία

εργασίας. Ένα φορτίο εργασίας μπορεί να είναι: 1 εικονική μηχανή (VM), 1 φυσικός διακομιστής, ένα πακέτο 3 σταθμών εργασίας ή 500GB δεδομένων NAS. Για 10 προϊόντα δεν βρέθηκαν πληροφορίες.
Οι παραπάνω περιορισμοί είναι αναμενόμενοι για αυτό το είδος των προϊόντων με βάση την αναμενόμενη λειτουργία τους με εξαίρεση τον τελευταίο περιορισμό. Ο τελευταίος περιορισμός δεν θεωρείται αναμενόμενος καθώς δεν πρόκειται για κάτι που αφορά τον τρόπο λειτουργίας του λογισμικού αλλά τον τρόπο χρέωσής του. Αντιθέτως, σε ένα προϊόν που δημιουργεί αντίγραφα ασφαλείας είναι λογικό να υπάρχει ένας περιορισμός, πχ. σχετικά με το πόσα αντίγραφα μπορούν να δημιουργηθούν σε ένα συγκεκριμένο χρονικό διάστημα, σχετικός με τη βασική του λειτουργία.

Δοκιμαστικές εκδόσεις: 2 προϊόντα (13.3%) δεν παρέχουν δωρεάν δοκιμαστική έκδοση, 6 προϊόντα (40%) παρέχουν δωρεάν δοκιμαστική έκδοση για 30 ημέρες, 5 προϊόντα (33.3%) παρέχουν δωρεάν δοκιμαστική έκδοση για 14 ημέρες, 1 προϊόν (6.6%) παρέχει δωρεάν δοκιμαστική έκδοση για 30 ημέρες ή χρήση κόστους 300$ ανάλογα με το τι θα έρθει πρώτο, και 1 προϊόν (6.6%) παρέχει δωρεάν δοκιμαστική έκδοση για 60 ημέρες. Τα αποτελέσματα είναι πολύ ικανοποιητικά καθώς βλέπουμε ότι τα 13 από τα 15 προϊόντα προσφέρουν δοκιμαστικές εκδόσεις χρονικής διάρκειας μεγαλύτερης ή ίσης με δύο εβδομάδες. Νικητήριο προϊόν για αυτή την κατηγορία είναι το Barracuda Backup, το οποίο προσφέρει 60 ημέρες δωρεάν χρήσης

Τρόπος χρήσης: 8 προϊόντα (53.3%) υποστηρίζουν και τα 3 είδη διεπαφών. 2 προϊόντα (13.3%) υποστηρίζουν διεπαφή προγραμματισμού εφαρμογών μεταφοράς αναπαραστατικής κατάστασης και γραφικό περιβάλλον εργασίας μέσω διαδικτύου. 2 προϊόντα (13.3%) υποστηρίζουν χρήση γραμμής εντολών και διεπαφή προγραμματισμού εφαρμογών μεταφοράς αναπαραστατικής κατάστασης. 3 προϊόντα (20%) υποστηρίζουν γραφικό περιβάλλον εργασίας μέσω διαδικτύου. Αν δούμε τις τιμές αποτίμησης μεμονωμένα η διεπαφή προγραμματισμού εφαρμογών μεταφοράς αναπαραστατικής κατάστασης εμφανίζεται σε 12 προϊόντα (80%). Το γραφικό περιβάλλον εργασίας μέσω διαδικτύου εμφανίζεται σε 13 προϊόντα (86.6%). Η γραμμή εντολών εμφανίζεται σε 10 προϊόντα (66.6%).
Τα αποτελέσματα θεωρούνται ικανοποιητικά καθώς παρατηρούμε πως 12 από τα 15 προϊόντα υποστηρίζουν δύο ή τρεις τεχνολογίες. Αυτά τα σχετικά υψηλά ποσοστά ήταν αναμενόμενα λόγω της φύσης των προϊόντων όπου μπορούν να χρησιμοποιηθούν εύκολα ακόμη και με όλους τους τρόπους.

Αγορές: 5 προϊόντα (33.3%) εντοπίστηκαν στο Amazon web services, 2 προϊόντα (13.3%) εντοπίστηκαν στο Google cloud platform και 3 προϊόντα (26.6%) εντοπίστηκαν στο Microsoft Azure. 2 προϊόντα (13,3%) εντοπίστηκαν σε Amazon web services και Microsoft Azure, και τελος 3 προϊόντα (20%) εντοπίστηκαν στο διαδίκτυο και όχι σε κάποια αγορά. Σαν συνολικό αποτέλεσμα από τα παραπάνω προκύπτει ότι στο Microsoft Azure βρέθηκαν 5 από τα προϊόντα (33.3%), στο Amazon web services βρέθηκαν 7 από τα προϊόντα (46.6%) και τέλος στο Google cloud βρέθηκαν 2 από τα προϊόντα (13.3%). Γίνεται, λοιπόν, φανερό ότι τα περισσότερα προϊόντα είναι διαθέσιμα στην αγορά της Amazon web services. Μόνο 2 προϊόντα βρέθηκαν σε παραπάνω από μία αγορές, άρα τα αποτελέσματα δεν είναι

ικανοποιητικά. Αντίθετα, περισσότερα προϊόντα θα μπορούσαν να συμμετέχουν σε πολλαπλές αγορές και έτσι να μπορούν να εντοπιστούν πιο εύκολα από τους μελλοντικούς αγοραστές. Νικητήρια προϊόντα για αυτό το κριτήριο είναι αυτα που εμφανίζονται σε δύο αγορές, δηλαδή τα Commvault Backup & Recovery και Nakivo Backup & Replication.

Επίπεδο/είδος υποστήριξης: 15 προϊόντα (100%) προσφέρουν υποστήριξη μέσω τηλεφώνου, 15 προϊόντα (100%) μέσω email, 10 προϊόντα (66.6) μέσω δελτίων (tickets), και 6 προϊόντα (40%) μέσω μηνυμάτων (chat). 12 προϊόντα (80%) διαθέτουν υποστήριξη κοινοτήτων χρηστών (κοινοτητα, φόρουμ, blog), 12 προϊόντα (80%) διαθέτουν τεκμηρίωση (documentation), 6 προϊόντα (40%) διαθέτουν πύλη υποστήριξης (portal), 11 προϊόντα (73.3%) διαθέτουν υποστηρικτικό υλικό (έγγραφα με πληροφορίες & βίντεο & FAQ) και 6 προϊόντα (40%) διαθέτουν βάση γνώσης (knowledge base). Τέλος υπάρχουν διάφοροι τρόποι υποστήριξης που παρέχονται από μεμονωμένα προϊόντα, ενός εκπαίδευση, ενημέρωση για συνδρομές, εργαλείο εκτίμησης κόστους ενός προϊόντος και ιστορικό λογαριασμού υποστήριξης.
Επιπλέον, υπάρχουν 5 προϊόντα (33.3%) τα οποία παρέχουν πακέτα υποστήριξης. Υπάρχουν δύο προϊόντα τα οποία προσφέρουν 3 πακέτα υποστήριξης, και τρία προϊόντα τα οποία προσφέρουν αντίστοιχα δυο, τέσσερα και πέντε διαφορετικά πακέτα. Το προϊόν, το οποίο προσφέρει τα περισσότερα (πέντε) πακέτα, είναι το Commvault Backup & Recovery.
Για την ημερολογιακή/χρονική διάρκεια κατά την οποία παρέχεται υποστήριξη υπάρχουν 7 προϊόντα που παρέχουν υποστήριξη 24 ώρες την ημέρα, 7 ημέρες την εβδομάδα.
Τα αποτελέσματα κρίνονται αρκετά ικανοποιητικά καθώς παρατηρούμε πως αρκετά προϊόντα προσφέρουν πολλαπλά είδη υποστήριξης και επικοινωνίας. Επιπλέον το ⅓ των προϊόντων προσφέρει διαφορετικά πακέτα υποστήριξης ώστε να προσαρμόζονται στις ανάγκες των πελατών και σχεδόν τα μισά προϊόντα παρέχουν υποστήριξη 24/7. Νικητήριο προϊόν για αυτό το κριτήριο είναι το Commvault Backup & Recovery, το οποίο συγχρόνως είναι ένα από τα προϊόντα με τα περισσότερα είδη υποστήριξης και την ίδια στιγμή διαθέτει πέντε διαφορετικά πακέτα.

Νικητήριο προϊόν για ολόκληρη την κατηγορία είναι το Commvault Backup & Recovery, το οποίο εμφανίζεται ως νικητήριο 4 φορές.

5.2.3 Διαχείριση εισβολής (Intrusion Management)

Για αυτή την ενότητα βρέθηκαν 15 προϊόντα με επαρκή τεκμηρίωση, τα οποία αποτιμήθηκαν. Τα αποτελέσματα αποτίμησης εμφανίζονται στον Πίνακα 3 του παραρτήματος. Παρακάτω παρέχουμε μια στατιστική ανάλυση των αποτελεσμάτων αυτών ανά κριτήριο.

Τρόπος παράδοσης: 3 προϊόντα (20%) προσφέρονται σαν λογισμικό, 11 προϊόντα (73.3%) προσφέρονται σαν υποδομή και 1 προϊόν (6,6%) σαν υποδομή και σαν λογισμικό. Νικητήριο προϊόν είναι το Atomic Enterprise OSSEC το οποίο υποστηρίζει δύο τρόπους παράδοσης. Τα παραπάνω

αποτελέσματα θα λέγαμε ότι δεν θεωρούνται ικανοποιητικά καθώς τα περισσότερα προϊόντα προσφέρονται με έναν μόνο τρόπο. Βέβαια αυτό είναι φυσιολογικό για την παρούσα κατηγορία καθώς αρκετά προϊόντα παρέχονται ως δωρεάν λογισμικό. Στην περίπτωση αυτή οι χρήστες υποχρεωτικά οδηγούνται σε τρόπο παράδοσης IaaS διότι αποκτούν το προϊόν και είτε το χρησιμοποιούν σε δικά τους μηχανήματα είτε μισθώνουν πόρους στο νέφος για να το φιλοξενήσουν.

Μοντέλο διάταξης: Όλα τα προϊόντα (100%) υποστηρίζουν δημόσιο νέφος. Σίγουρα, δεν είναι ικανοποιητικό πως όλα τα προϊόντα υποστηρίζουν μόνο ένα μοντέλο διάταξης. Από την άλλη πλευρά, όμως, αυτό είναι αναμενόμενο καθώς και τα προϊόντα με μοντέλο διάταξης SaaS και με μοντέλο διάταξης IaaS καλύπτονται πλήρως από τις δυνατότητες-πλεονεκτήματα του δημόσιου νέφους.

Κατηγορία ασφαλείας: 5 προϊόντα (33.3%) καλύπτουν επιπλέον την κατηγορία της ασφάλειας δικτύου, 1 προϊόν (6.6%) καλύπτει επιπλέον την ασφάλεια ιστού και 3 προϊόντα (20%) καλύπτουν επιπλέον και την ασφάλεια ιστού και την ασφάλεια δικτύου, τα οποία είναι και τα νικητήρια εφόσον καλύπτουν παραπάνω από 1 έξτρα κατηγορία. Τα αποτελέσματα είναι πολύ ικανοποιητικά καθώς βλέπουμε ότι πάνω από τα μισά προϊόντα καλύπτουν μία ή δύο επιπλέον κατηγορίες. Αυτό συμβαίνει διότι τα πιο πολλά προϊόντα δεν είναι μόνο συστήματα ανίχνευσης ή αποτροπής εισβολών. Αντιθέτως είναι πιο σύνθετα προϊόντα, τα οποία καλύπτουν πολλούς επιπλέον μηχανισμούς (π.χ. τείχος προστασίας), οι οποίοι εντάσσονται στις επιπλέον κατηγορίες που αναφέρθηκαν προηγουμένως.

Μοντέλο κόστους: Σχετικά με την τιμολόγηση, 1 προϊόν (6.6%) παρέχει πληροφορίες τιμολόγησης μόνο μέσω επικοινωνίας με την εταιρία. 8 προϊόντα (53.3%) είναι δωρεάν λογισμικό, 1 προϊόν (6.6%) τιμολογείται με βάση τις ώρες χρήσης του AWS Sagemaker, 3 προϊόντα (20%) τιμολογούνται με βάση το φόρτο εργασίας (συνήθως με βάση τον αριθμό των VM που χρησιμοποιούνται) στο νέφος, 1 προϊόν (6.6%) τιμολογείται με βάση τον όγκο των δεδομένων (εύρος ζώνης) και 1 προϊόν (6.6%) τιμολογείται αναλογικά με βάση τον αριθμό των λογαριασμών (accounts) που δημιουργούνται στο νέφος, όπου κάθε λογαριασμός υποστηρίζει έως 200 αντικείμενα (assets).
Σχετικά με την ύπαρξη πακέτων, δεν υπάρχουν διαφορετικά πακέτα πληρωμής για κάποιο προϊόν. Τέλος, σχετικά με τη χρονική συνιστώσα των πληρωμών, 1 προϊόν (6.6%) προσφέρει δυνατότητα πληρωμής ετησίως, 1 προϊόν (6.6%) προσφέρει δυνατότητα πληρωμής είτε μηνιαίως, είτε ανά τρίμηνο ή ετησίως και τέλος 2 προϊόντα (13.3%) προσφέρουν δυνατότητα πληρωμής μηνιαίως ή αγορά άδειας χρήσης (στις αγορές αναφέρεται ως bring your own license), οι οποίες ανά κάποιο χρονικό διάστημα χρήζουν ανανέωσης. Συνεπώς, για 2 προϊόντα υπό πληρωμή δεν αναφέρεται η χρονική συνιστώσα.
Φαίνεται ότι τα περισσότερα προϊόντα είναι δωρεάν συνεπώς δεν μπορούμε να περιμένουμε πολλές πληροφορίες στην κατηγορία αυτή. Στα 6 προϊόντα τα οποία δεν είναι δωρεάν, οι τρόποι πληρωμής είναι διαφορετικοί ανάμεσα στα προϊόντα χωρίς να ξεχωρίζει κάποιος τρόπος. Δεν προσφέρονται πακέτα πληρωμής ενώ σχετικά με τη χρονική συνιστώσα μόνο 4 προϊόντα προσφέρουν κάποια πληροφορία. Γίνεται, λοιπόν, φανερό πως τα αποτελέσματα δεν είναι ικανοποιητικά. Νικητήριο προϊόν για αυτή

την κατηγορία είναι το Big HIDS SaaS, το οποίο παρέχει τον πιο ευέλικτο χρονικά τρόπο πληρωμής με τρεις επιλογές.

Μηχανισμοί ασφάλειας: Υπάρχουν 13 προϊόντα (86.6%) που υποστηρίζουν έξτρα λειτουργικότητα πέρα από τη βασική και 2 προϊόντα (13.3%) που υποστηρίζουν μόνο τη βασική λειτουργικότητα. Τα προϊόντα τα οποία προσφέρουν τις περισσότερες έξτρα λειτουργικότητες είναι το Wazuh All-In-One Deployment και το OPNsense Firewall/Router/VPN/IDPS, τα οποία είναι και τα νικητήρια.
Τα αποτελέσματα είναι πολύ ικανοποιητικά καθώς σχεδόν όλα τα προϊόντα καλύπτουν έξτρα λειτουργικότητες. Αυτό συμβαίνει διότι σχεδόν κανένα προϊόν δεν λειτουργεί μόνο σαν σύστημα ανίχνευσης/αποτροπής εισβολών, Αντίθετα είναι ολοκληρωμένα προϊόντα, τα οποία προσφέρουν πολλές υπηρεσίες ταυτόχρονα ώστε να δημιουργηθεί μία πιο ολοκληρωμένη λύση ασφάλειας (σε σύγκριση με ένα σκέτο IDS). Αυτή η λύση δυνητικά καλύπτει πολλές κατηγορίες ασφάλειας, όπως φάνηκε και στην ανάλυση του κριτηρίου που αφορά τις καλυπτόμενες κατηγορίες ασφάλειας. Κάτι τέτοιο ωφελεί και τους αγοραστές διότι όταν ένα μόνο προϊόν αντικαθιστά δυο ή τρία μεμονωμένα προϊόντα, το συνολικό κόστος απόκτησης και λειτουργίας είναι σαφώς μικρότερο.

Μη λειτουργικές εγγυήσεις: Βρέθηκαν πληροφορίες μόνο σε 1 από τα 7 προϊόντα (6.6%) που προσφέρονται επί πληρωμή. Προφανώς, τα δωρεάν προϊόντα συνήθως δεν συνοδεύονται από κάποιες εγγυήσεις. Στο Lacework Cloud Security, αν η υπηρεσία δεν λειτουργήσει όπως περιγράφεται στην τεκμηρίωση (αξιοπιστία), ο πελάτης μπορεί να διακόψει τη συνδρομή και να του επιστραφεί μέρος του προπληρωμένου ποσού που αντιστοιχεί στο υπολειπόμενο χρονικό διάστημα (για το οποίο δεν θα χρησιμοποιηθεί το προϊόν).
Τα αποτελέσματα δεν είναι ικανοποιητικά διότι δεν δίνονται εγγυήσεις για τα περισσότερα προϊόντα ενώ και οι εγγυήσεις που παρέχονται είναι τις περισσότερες φορές μη ουσιαστικές. Το νικητήριο προϊόν είναι το Lacework Cloud Security, το οποίο προσφέρει την πιο χρήσιμη/απαραίτητη εγγύηση.

Είδος προσφερόμενης προστασία: Η κύρια λειτουργικότητα σε 8 προϊόντα (53,3%) είναι ανιχνευτική (detective) και σε 7 προϊόντα (46.6%) είναι ανιχνευτική και προληπτική. Για τα παραπάνω αποτελέσματα λήφθηκε υπόψη μόνο η αντιμετώπιση εισβολών που είναι και η κύρια λειτουργικότητα αυτής της κατηγορίας και όχι οι υπόλοιποι μηχανισμοί. Τα προϊόντα με ανιχνευτική προστασία είναι εκείνα που προσφέρουν ανίχνευση εισβολών (Intrusion Detection System). Όπως λέει και το όνομά τους ανιχνεύουν (detect) εισβολές και εγείρουν συναγερμούς, δεν εκτελούν κάποια λειτουργία που να “πολεμήσει” την εισβολή. Τα προϊόντα με προληπτική και ανιχνευτική προστασία είναι εκείνα τα οποία προσφέρουν συνδυασμό ανίχνευσης και αποτροπής εισβολών (Intrusion Prevention System). Η διαφορά τους με τα προηγούμενα προϊόντα είναι πως αρχικά ανιχνεύουν την εισβολή και στη συνέχεια έχουν τη δυνατότητα να την αποτρέψουν. Η αποτροπή μιας εισβολής είναι προληπτικό μέτρο διότι προσπαθεί να αντιμετωπίσει έναν συμβάν (την εισβολή) προτού αυτό συμβεί και προκληθούν δυσάρεστες συνέπειες. Τα

αποτελέσματα είναι ικανοποιητικά καθώς βλέπουμε ότι το ½ των προϊόντων συνδυάζει δύο κατηγορίες. Τα προϊόντα αυτά (δείτε πίνακα αποτίμησης) είναι και τα νικητήρια.

Ιδιότητες ασφάλειας: Βρέθηκαν πληροφορίες σε 12 προϊόντα (80%). 5 προϊόντα (33.3%) εξασφαλίζουν την ακεραιότητα, 5 προϊόντα (33.3%) εξασφαλίζουν τη διαθεσιμότητα και 2 προϊόντα (13.3%) εξασφαλίζουν ακεραιότητα και διαθεσιμότητα. Τα προϊόντα που εξασφαλίζουν τη ακεραιότητα υλοποιούν μηχανισμό για έλεγχο της ακεραιότητας των αρχείων (file integrity monitoring). Τα προϊόντα που εξασφαλίζουν τη διαθεσιμότητα ή τη διαθεσιμότητα και την ακεραιότητα είναι συστήματα αποτροπής εισβολών. Ουσιαστικά, η διαθεσιμότητα παρέχεται μέσα από την αποτροπή εισβολής διότι το σύστημα δεν καταρρέει (άρα παραμένει διαθέσιμο – π.χ. μετά από μια επίθεση τύπου DoS).
Σύμφωνα με τα παραπάνω, τα αποτελέσματα δεν θεωρούνται ικανοποιητικά καθώς μόνο δύο προϊόντα καλύπτουν πάνω από μία ιδιότητα ασφάλειας, Τα προϊόντα αυτά είναι τα Trend Micro Deep Security και Anhlab CPP, τα οποία είναι και τα νικητήρια.

Προστατευόμενα αντικείμενα: 10 προϊόντα (66.6%) προστατεύουν οποιοδήποτε συστατικό του πληροφοριακού συστήματος, 4 προϊόντα (26.6%) προστατεύουν τους ξενιστές και 1 προϊόν (6,6%) προστατεύει το δίκτυο. Η προστασία ολόκληρων συστημάτων οφείλεται στον μεγάλο αριθμό μηχανισμών ασφαλείας που προσφέρονται από τα αντίστοιχα προϊόντα της κατηγορίας (66,6%). Δηλαδή όταν ένα προϊόν προσφέρει διάφορους μηχανισμούς όπου ο καθένας προστατεύει και ένα διαφορετικό τμήμα του πληροφοριακού συστήματος, τότε θεωρούμε πως προστατεύεται όλο το σύστημα. Τα προϊόντα που προσφέρουν σύστημα εντοπισμού εισβολών βάσει δικτύου προστατεύουν το δίκτυο και βάσει ξενιστή τους ξενιστές, αντίστοιχα.
Τα αποτελέσματα θεωρούνται ικανοποιητικά καθώς περισσότερα από τα μισά προϊόντα προσφέρουν συνολική προστασία. Επίσης, παρατηρούμε πως ανάμεσα στα 10 προϊόντα που προσφέρουν πλήρη προστασία τα 6 είναι δωρεάν προϊόντα και τα 4 είναι επί πληρωμή, Αυτό δεν είναι απόλυτα αναμενόμενο διότι κάποιος θα περίμενε πως πλήρης προστασία παρέχεται κατά κύριο λόγο από επί πληρωμή προϊόντα.

Αντιμετωπιζόμενες απειλές: Για 3 προϊόντα δεν βρέθηκαν πληροφορίες. 9 προϊόντα (46.6%) αντιμετωπίζουν το κακόβουλο λογισμικό, 2 προϊόντα (13.3%) αντιμετωπίζουν επιθέσεις ωμής βίας, 2 προϊόντα (13.3%) αντιμετωπίζουν επιθέσεις άρνησης εξυπηρέτησης και κατανεμημένης άρνησης εξυπηρέτησης. 2 προϊόντα (13.3%) αντιμετωπίζουν απειλές διαδικτύου, 1 προϊόν (6.6%) αντιμετωπίζει διαχειριστικά σύνεργα (rootkits), και 1 προϊόν (6.6%) αντιμετωπίζει επιθέσεις Zero Hour, λυτρισμικό και διαρροές δεδομένων. 1 προϊόν (6.6%) αντιμετωπίζει κανάλια command and control, 1 προϊόν αντιμετωπίζει κακόβουλο κώδικα και 1 προϊόν (6.6%) αντιμετωπίζει επιθέσεις κοινής διεπαφής πύλης (Common Gateway Interface), υπερχείλιση προσωρινής μνήμης, και σάρωση λαθραίων πυλών (stealth port scan). Ως προς τον αριθμό απειλών που καλύπτονται ανά προϊόν, 1 προϊόν (6.6%) καλύπτει μία απειλή, 8

προϊόντα (53.3%) καλύπτουν δύο απειλές, 1 προϊόν (6.6%) καλύπτει τρεις απειλές και 2 προϊόντα (13.3%) καλύπτουν 5 απειλές. Τα αποτελέσματα είναι ικανοποιητικά καθώς σχεδόν όλα τα προϊόντα καλύπτουν δύο ή περισσότερα είδη απειλών. Νικητήρια προϊόντα είναι τα Heimdal Threat Prevention και Snort που καλύπτουν τα περισσότερα (πέντε) είδη απειλών.

Περιορισμοί χρήσης: Βρέθηκαν περιορισμοί μόνο σε 7 προϊόντα (46.6%). 1 προϊόν (6.6%) υποστηρίζεται μόνο σε linux περιβάλλοντα ενώ 2 προϊόντα (13.3%) έχουν περιορισμό στον αριθμό κανόνων που υποστηρίζονται για το IDS (το ένα 100 έως 999 και το άλλο 5000). Σε 1 προϊόν (6.6%) το μέγιστο μέγεθος δεδομένων εισόδου ανά εκτέλεση του προγράμματος (per invocation) είναι 25MB και προσφέρει: συνολική ακρίβεια (δυαδική ανίχνευση): 84%, συνολική ανάκληση (δυαδική ανίχνευση): 84%, ακρίβεια πολλαπλών κλάσεων (ανίχνευση πολλαπλών κλάσεων): 78%. 1 προϊόν (6.6%) έχει απόδοση έως 10 Gbps. 1 προϊόν (6.6%) με μία άδεια για κάθε λογαριασμό που καλύπτει μέχρι 200 αντικείμενα στο νέφος και τέλος για 1 προϊόν (6.6%) δεν υποστηρίζονται περιβάλλοντα windows.
Τα αποτελέσματα δεν είναι ικανοποιητικά καθώς βρέθηκαν πληροφορίες μόνο στα μισά προϊόντα. Από πλευράς περιορισμών όλοι θεωρούνται αναμενόμενοι καθώς βρίσκονται στα πλαίσια της φυσιολογικής λειτουργίας των προϊόντων.

Δοκιμαστικές εκδόσεις: 3 προϊόντα (20%) δεν παρέχουν δωρεάν δοκιμαστική έκδοση, 8 προϊόντα (53.3%) είναι δωρεάν λογισμικό, 1 προϊόν (6.6%) παρέχει δωρεάν δοκιμαστική έκδοση για 5 ημέρες και 3 προϊόντα (20%) παρέχουν δωρεάν δοκιμαστική έκδοση 30 ημερών.
Τα αποτελέσματα είναι ικανοποιητικά καθώς πάνω από τα μισά προϊόντα είναι δωρεάν όπως αναφέρθηκε και στο κριτήριο της τιμολόγησης. Βέβαια, υπάρχει περιθώριο βελτίωσης καθώς από τα επι πληρωμή προϊόντα σχεδόν τα μισά δεν διαθέτουν δωρεάν δοκιμαστική έκδοση.

Τρόπος χρήσης: 5 προϊόντα (33.3%) υποστηρίζουν και τα 3 είδη διεπαφών. 2 προϊόντα (13.3%) υποστηρίζουν διεπαφή προγραμματισμού εφαρμογών μεταφοράς αναπαραστατικής κατάστασης και γραφικό περιβάλλον εργασίας μέσω διαδικτύου. 4 προϊόντα (26.6%) υποστηρίζουν χρήση γραμμής εντολών και διεπαφή προγραμματισμού εφαρμογών μεταφοράς αναπαραστατικής κατάστασης. 4 προϊόντα (26.6%%) υποστηρίζουν χρήση γραμμής εντολών.
Αν δούμε τις τιμές αποτίμησης μεμονωμένα η διεπαφή προγραμματισμού εφαρμογών μεταφοράς αναπαραστατικής κατάστασης εμφανίζεται σε 7 προϊόντα (46.6%). Το γραφικό περιβάλλον εργασίας μέσω διαδικτύου εμφανίζονται σε 11 προϊόντα (73.3%). Η γραμμή εντολών, που είναι και ο κλασσικός τρόπος χρήσης ενός συστήματος ανίχνευσης εισβολών, εμφανίζεται σε 13 προϊόντα (86.6%).
Τα αποτελέσματα θεωρούνται ικανοποιητικά καθώς παρατηρούμε πως 11 από τα 15 προϊόντα υποστηρίζουν δύο ή τρεις τεχνολογίες. Νικητήρια είναι τα 4 προϊόντα (δείτε πίνακα αποτίμησης), τα οποία υποστηρίζουν και τις 3 τεχνολογίες.

Αγορές: 4 προϊόντα (26.6%) εντοπίστηκαν στο Amazon web services και 1 προϊόν (6.6%) στο Microsoft Azure. 5 προϊόντα (33,3%) εντοπίστηκαν σε Amazon web services και Microsoft Azure. 1 προϊόν (6.6%) εντοπίστηκε σε Amazon web services και Google cloud platform. 1 προϊόν (6.6%) εντοπίστηκε σε Amazon web services, Google cloud platform και Microsoft Azure. Τέλος, 3 προϊόντα (20%) εντοπίστηκαν στο διαδίκτυο και όχι σε κάποια αγορά.

Σαν συνολικό αποτέλεσμα από τα παραπάνω προκύπτει ότι στο Microsoft Azure βρέθηκαν 7 από τα προϊόντα (46.6%), στο Amazon web services βρέθηκαν 11 από τα προϊόντα (73.3%) και τέλος στο Google cloud βρέθηκαν 2 από τα προϊόντα (13.3%). Γίνεται, λοιπόν, φανερό ότι τα περισσότερα προϊόντα είναι διαθέσιμα στην αγορά της Amazon web services.

Τα αποτελέσματα είναι οριακά αποδεκτά διότι 7 από τα 15 προϊόντα δηλαδή κάτι λιγότερο από τα μισά βρέθηκαν σε παραπάνω από μία αγορές. Νικητήριο προϊόν είναι το Atomic Enterprise OSSEC, το οποίο βρέθηκε και στις 3 αγορές (που προσφέρονται από παρόχους νέφους).

Επίπεδο/είδος υποστήριξης: 8 προϊόντα (53.3%) προσφέρουν υποστήριξη μέσω τηλεφώνου, 15 προϊόντα (100%) μέσω email, 5 προϊόντα (33.3%) μέσω δελτίων (tickets), και 7 προϊόντα (46.6%) μέσω μηνυμάτων (chat). 10 προϊόντα (66.6%) διαθέτουν υποστήριξη κοινοτήτων χρηστών (κοινότητα, φόρουμ), 10 προϊόντα (66.6%) διαθέτουν τεκμηρίωση (documentation), 2 προϊόντα (13.3%) διαθέτουν πύλη υποστήριξης (portal), 15 προϊόντα (100%) διαθέτουν έγγραφα με πληροφορίες, 2 προϊόντα (13.3%) διαθέτουν βίντεο, 8 προϊόντα (53.3%) διαθέτουν πιθανές ερωτήσεις και τις απαντήσεις τους, 3 προϊόντα (20%) διαθέτουν βάση γνώσης (knowledge base), 3 προϊόντα (20%) προσφέρουν ενημέρωση για νέες εκδόσεις και 3 προϊόντα (20%) διαθέτουν κέντρο αυτοβοήθειας. Τέλος, υπάρχουν διάφοροι τρόποι υποστήριξης που παρέχονται από μεμονωμένα προϊόντα, όπως λογαριασμοί σε διάφορα μέσα κοινωνικής δικτύωσης (github, discord, slack, github, Google group), κέντρο υποστήριξης και διαχείριση συνδρομής.

Επιπλέον, υπάρχουν 8 προϊόντα (53.3%) τα οποία παρέχουν πακέτα υποστήριξης. Υπάρχουν 4 προϊόντα τα οποία προσφέρουν δύο πακέτα υποστήριξης, 3 προϊόντα τα οποία προσφέρουν τρία πακέτα υποστήριξης και 1 προϊόν το οποίο προσφέρει πέντε πακέτα υποστήριξης. Το προϊόν το οποίο προσφέρει τα περισσότερα (πέντε) πακέτα είναι το Big HIDS SaaS.

Για την ημερολογιακή/χρονική διάρκεια κατά την οποία παρέχεται υποστήριξη υπάρχουν 3 προϊόντα (20%) όπου η ελάχιστη υποστήριξη είναι σε εργάσιμες ώρες και η μέγιστη είναι 24/7, 4 προϊόντα (26.6%) παρέχουν υποστήριξη 24/7 και τέλος 1 προϊόν (6.6%) προσφέρει υποστήριξη από 12/5 έως 24/7 ανάλογα με την κρισιμότητα των συμβάντων.

Τα αποτελέσματα κρίνονται αρκετά ικανοποιητικά καθώς παρατηρούμε πως υπάρχουν πολλά προϊόντα που προσφέρουν πολλαπλά είδη υποστήριξης και επικοινωνίας. Επιπλέον, πάνω από τα μισά προϊόντα προσφέρουν διαφορετικά πακέτα υποστήριξης. Ένας ακόμα λόγος που τα αποτελέσματα είναι πολύ ικανοποιητικά είναι πως υπάρχουν 8 δωρεάν προϊόντα τα οποία θα μπορούσαν να έχουν μηδαμινή υποστήριξη αφού είναι δωρεάν και να επηρεάσουν αρνητικά τα συνολικά αποτελέσματα της κατηγορίας.

Κάτι τέτοιο, όμως, δεν ισχύει. Νικητήριο προϊόν για αυτή την κατηγορία είναι το Big HIDS SaaS, το οποίο παρέχει 5 πακέτα υποστήριξης, εκ των οποίων τα 4 παρέχουν 24/7 υποστήριξη.

Νικητήρια προϊόντα για ολόκληρη την κατηγορία είναι τα Trend Micro Deep Security και OPNsense Firewall/Router/VPN/IDPS, τα οποία εμφανίζεται ως νικητήρια από 3 φορές.

5.2.4 Διαχείριση ταυτότητας και πρόσβασης (Identity and Access Management)

Για αυτή την ενότητα βρέθηκαν 15 προϊόντα με επαρκή τεκμηρίωση, τα οποία αποτιμήθηκαν. Τα αποτελέσματα αποτίμησης εμφανίζονται στον Πίνακα 4 του παραρτήματος. Παρακάτω παρέχουμε μια στατιστική ανάλυση των αποτελεσμάτων αυτών ανά κριτήριο.

Τρόπος παράδοσης: 13 προϊόντα (86.6%) προσφέρονται σαν λογισμικό και 2 προϊόντα (13.3%) προσφέρονται σαν υποδομή. Παρατηρούμε πως κυριαρχεί ο τρόπος παράδοσης ως λογισμικό λόγω των πλεονεκτημάτων που έχει απέναντι στους υπόλοιπους τρόπους παράδοσης. Επίσης, αυτά τα προϊόντα παραδοσιακά τις περισσότερες φορές προσφέρονται με την μορφή μιας υπηρεσίας/εφαρμογής λογισμικού Τα αποτελέσματα δεν θεωρούνται ικανοποιητικά διότι κανένα προϊόν δεν προσφέρεται με δύο ή περισσότερους τρόπους.

Μοντέλο διάταξης: 14 προϊόντα (93.3%) υποστηρίζουν δημόσιο νέφος και 1 προϊόν (6.6%) υποστηρίζει δημόσιο ή ιδιωτικό νέφος. Σίγουρα δεν είναι ικανοποιητικό πως όλα τα προϊόντα εκτός από ένα υποστηρίζουν μόνο ένα μοντέλο διάταξης. Από την άλλη πλευρά, όμως, αυτό είναι αναμενόμενο καθώς σχεδόν όλα τα προϊόντα υποστηρίζουν τρόπο παράδοσης SaaS, συνεπώς το μοντέλο διάταξης είναι λογικά το δημόσιο νέφος. Νικητήριο προϊόν είναι το WSO2 Identity Server, το οποίο υποστηρίζει δημόσιο ή ιδιωτικό νέφος.

Κατηγορία ασφάλειας: Τα 14 από τα 15 προϊόντα (93.3%) καλύπτουν μόνο την κατηγορία της Διαχείρισης ταυτότητας και πρόσβασης, δηλαδή την τρέχουσα κατηγορία υπό ανάλυση, χωρίς να καλύπτουν κάποια επιπλέον κατηγορία. Υπάρχει 1 προϊόν (6.6), το ForgeRock Identity Cloud, το οποίο εν μέρη υποστηρίζει την κατηγορία BCDR καθώς έχει την ικανότητα να δημιουργεί αντίγραφα ασφαλείας για τα δεδομένα. Το προϊόν αυτό είναι και το νικητήριο.
Τα αποτελέσματα, όπως είναι λογικό, δεν είναι καθόλου ικανοποιητικά. Βέβαια αυτό το αποτέλεσμα θα μπορούσε να θεωρηθεί και αναμενόμενο. Τα προϊόντα αυτής της κατηγορίας έχουν έναν πολύ συγκεκριμένο σκοπό (τη διαχείριση ταυτοτήτων/δικαιωμάτων). Έτσι, λοιπόν, δεν υπάρχει ευελιξία ώστε ένα προϊόν να καλύψει επιπλέον κατηγορίες. Δηλαδή, για παράδειγμα, ένα σύστημα αποτροπής εισβολών θα μπορούσε να αντιμετωπίζει διαδικτυακές απειλές άρα να καλύπτει την ασφάλεια ιστού διότι εξ' ορισμού αντιμετωπίζει απειλές. Από την άλλη πλευρά, ένα σύστημα διαχείρισης ταυτότητας και

πρόσβασης δεν μπορεί παράλληλα να εκτελεί μία εντελώς διαφορετική λειτουργία από τις αναμενόμενες της κατηγορίας του και έτσι να καλύπτει πολλαπλές κατηγορίες.

Μοντέλο κόστους: Σχετικά με την τιμολόγηση, αν δούμε τις συνιστώσες τιμολόγησης μεμονωμένα 10 προϊόντα (66.6%) τιμολογούν με βάση τον αριθμό των χρηστών, 6 προϊόντα (40%) τιμολογούν με βάση τα χαρακτηριστικά, 4 προϊόντα (26.6%) τιμολογούν με βάση τα βασικά χαρακτηριστικά και υπό χαρακτηριστικά, 1 προϊόν (6.6%) τιμολογεί με βάση τη χρήση, 1 προϊόν (6.6%) τιμολογεί με βάση το χρονικό διάστημα σε μήνες που θα είναι ενεργοί οι χρήστες. επίσης, δύο προϊόντα (13.3%) έχουν ελάχιστη τιμή ετήσιου συμβολαίου. Πιο συγκεκριμένα, σε 1 προϊόν το ελάχιστο κόστος πρέπει να είναι 1500 δολάρια ενώ σε ένα άλλο 500 δολάρια

Αν δούμε τον αριθμό των συνιστωσών, 7 προϊόντα (46.6%) τιμολογούν με 2 τρόπους, 1 προϊόν (6.6%) τιμολογεί με 3 τρόπους, ενώ 4 προϊόντα (26.6%) τιμολογούν με 1 τρόπο.

Ένα παράδειγμα για την περίπτωση τιμολόγησης με βάση τα βασικά χαρακτηριστικά και υπόχαρακτηριστικά μπορεί να αντληθεί από το προϊόν JumpCloud Directory-as-a-Service όπου ένα από τα βασικά χαρακτηριστικά του είναι η διαχείριση πρόσβασης και η καταγραφή. Υπόχαρακτηριστικά του χαρακτηριστικού αυτού είναι τα Cloud LDAP (για την αποθήκευση χρηστών), Cloud Radius (λύση ταυτοποίησης χρηστών χωρίς την χρήση κωδικών μέσω OAuth & ψηφιακών πιστοποιητικών) και Directory Insights (για την καταχώρηση διαφόρων ειδών γεγονότων σχετιζόμενων με την ταυτοποίηση & την διαχείριση χρηστών). Στην περίπτωση του JumpCloud Directory-as-a-Service, ένα πακέτο δεν υποστηρίζει αυτό το χαρακτηριστικό αλλά τα υπόλοιπα το υποστηρίζουν. Τα τελευταία αυτά πακέτα υποστηρίζουν πλήρως όλα τα υποχαρακτηριστικά αυτού του χαρακτηριστικού. Αυτό, όμως, δεν συμβαίνει για ένα άλλο χαρακτηριστικό, το Device Management & Telemetry (Διαχείριση Συσκευών & Τηλεμετρία), όπου ένα πακέτο δεν το υποστηρίζει καθόλου, ένα άλλο πακέτο υποστηρίζει 2 υποχαρακτηριστικά του μόνο μέσω έξτρα πληρωμής, και δύο άλλα πακέτα υποστηρίζουν πάντοτε 3 υποχαρακτηριστικά του καθώς και το τελευταίο μόνο μέσω έξτρα πληρωμής.

Σχετικά με την ύπαρξη πακέτων, υπάρχουν 7 προϊόντα που προσφέρουν διαφορετικά πακέτα πληρωμής. Ειδικότερα, υπάρχουν 4 προϊόντα (26.6%) που προσφέρουν 3 πακέτα, 1 προϊόν (6.6%) που προσφέρει 4 πακέτα, 1 προϊόν (6.6%) που προσφέρει 5 πακέτα, και 1 προϊόν (6.6%) που προσφέρει 2 πακέτα.

Τέλος, σχετικά με τη χρονική συνιστώσα των πληρωμών, 5 προϊόντα (33.3%) έχουν μηνιαία χρέωση, 1 προϊόν (6.6%) ετήσια χρέωση, 2 προϊόντα (13.3%) ετήσια ή μηνιαία χρέωση και 1 προϊόν (6.6%) χρέωση ετησίως ή ανά τρία έτη.

Τα αποτελέσματα είναι πολύ ικανοποιητικά καθώς σχεδόν τα μισά προϊόντα παρέχουν διαφορετικά πακέτα πληρωμής και πληροφορίες για τη χρονική συχνότητα. Η ύπαρξη πακέτων ήταν κάτι αναμενόμενο εφόσον υπάρχει τιμολόγηση με βάση τα χαρακτηριστικά διότι κάθε πακέτο αντιστοιχεί και σε διαφορετικά χαρακτηριστικά. Νικητήριο προϊόν είναι το JumpCloud Directory-as-a-Service, το οποίο προσφέρει 4 διαφορετικά πακέτα και δύο διαφορετικές χρονικές επιλογές (μηνιαίως ή ετησίως).

Μηχανισμοί ασφάλειας: Όλα τα προϊόντα υποστηρίζουν έξτρα λειτουργικότητα πέρα από τη βασική. Τα προϊόντα τα οποία προσφέρουν τις περισσότερες έξτρα λειτουργικότητες είναι το Entrust Identity as a Service και το Cloud Identity Premium, τα οποία είναι και τα νικητήρια.
Τα αποτελέσματα είναι πολύ ικανοποιητικά καθώς όλα τα προϊόντα καλύπτουν έξτρα λειτουργικότητες. Αυτό συμβαίνει γιατί όλα τα προϊόντα σαν ελάχιστη προϋπόθεση για να προσφέρουν μία σωστή λύση ασφάλειας οφείλουν να καλύψουν τις βασικές λειτουργικότητες, οι οποίες είναι παροχή και έλεγχος ταυτότητας, εξουσιοδοτήσεις και έλεγχος. Πέρα από αυτές τις πολύ βασικές λειτουργίες, το κάθε προϊόν έχει κατασκευαστεί με τις αντίστοιχες διαφοροποιήσεις/ επιπλέον λειτουργικότητες ώστε να προκύψει ένα πιο ολοκληρωμένο & ελκυστικό αποτέλεσμα.

Μη λειτουργικές εγγυήσεις: Για 5 προϊόντα δεν βρέθηκαν πληροφορίες. 3 προϊόντα προσφέρουν διαθεσιμότητα 99.9% και 7 προϊόντα προσφέρουν διαθεσιμότητα 99.99%.
6 προϊόντα διαθέτουν σύστημα ποινών αν δεν τηρήσουν τη διαθεσιμότητα που αναφέρουν. 2 προϊόντα για διαθεσιμότητα από 99% έως 99.9% επεκτείνουν τη μηνιαία συνδρομή ή πιστώνεται το αντίστοιχο χρηματικό ποσό αναλογικά ως προς την μηνιαία συνδρομή για τις 3 ημέρες μη διαθεσιμότητας, για 95% έως 99% για 5 μέρες και για μικρότερη του 95% για 15 μέρες. 1 προϊόν για διαθεσιμότητα μικρότερη από 99% επιστρέφει το 10% της μηνιαίας συνδρομής. 1 προϊόν για διαθεσιμότητα 99% έως 99.99% επιστρέφει 5% της μηνιαίας συνδρομής, για 95% έως 99% επιστρέφει το 10%, και για μικρότερη του 95% επιστρέφει το 25%. Σε 1 προϊόν για διαθεσιμότητα μικρότερη 99.9% η διάρκεια της συνδρομής θα παρατείνεται κατά μία επιπλέον ημέρα για κάθε μισό τοις εκατό (0,5%) κατά την οποία η συνδρομητική υπηρεσία απέτυχε να πετύχει αυτό το επίπεδο για αυτόν τον μήνα (δηλ. αριθμός ημερών = (99.9-X) / 0,5 όπου X η πραγματική διαθεσιμότητα). Για 2 ή περισσότερους συνεχόμενους μήνες ή για 3 μήνες σε ένα έτος πραγματοποιείται αναλογική επιστροφή των προπληρωμένων αχρησιμοποίητων τελών από την ημερομηνία της καταγγελίας. Τέλος, 1 προϊόν απλά αναφέρει ότι διαθέτει σύστημα ποινών χωρίς να αναφέρονται λεπτομέρειες.
Τα αποτελέσματα δεν θεωρούνται ιδιαίτερα ικανοποιητικά καθώς στα 10 προϊόντα που βρέθηκαν πληροφορίες, όλα παρέχουν μόνο την εγγύηση της διαθεσιμότητας. Επιπλέον, μόνο 3 προϊόντα έχουν διαθεσιμότητα 99.99%. Οποιοσδήποτε αριθμός χαμηλότερος από αυτό δεν θεωρείται ικανοποιητικός. Ανεξάρτητα από το μέγεθος ή τις ανάγκες ενός οργανισμού, θα πρέπει ανά πάσα στιγμή να λειτουργούν οι λογαριασμοί των χρηστών ώστε να μπορούν να εισέλθουν στο πληροφοριακό σύστημα για να αντιμετωπίσουν το οποιοδήποτε ζήτημα (βλάβη, επίθεση, κλπ.), ειδικότερα για αυτούς με ρόλο διαχειριστή. Νικητήριο προϊόν για αυτή την κατηγορία είναι το The OptimalCloud καθώς διαθέτει 99.99% διαθεσιμότητα και σύστημα ποινών.

Είδος προσφερόμενες προστασίας: η κύρια λειτουργικότητα σε όλα τα προϊόντα (100%) είναι προληπτική (preventive). Αυτό είναι αναμενόμενο και οφείλεται στη φύση των προϊόντων διαχείρισης ταυτότητας και πρόσβασης. Το σύστημα αυτό διαχειρίζεται τους λογαριασμούς χρηστών και τα δικαιώματα τους και έτσι ελέγχει εάν κάποιος χρήστης έχει τη δυνατότητα να πραγματοποιήσει μια ενδεχομένως

επιβλαβή ενέργεια που κανονικά δεν θα έπρεπε. Άρα, λοιπόν, πρόκειται για πρόληψη απέναντι στην πραγματοποίηση κάποιας ενέργειας που θα επιφέρει δυσάρεστες συνέπειες.

Ιδιότητες ασφάλειας: Βρέθηκαν πληροφορίες μόνο σε 2 προϊόντα (13.3%). Όλα τα προϊόντα εξασφαλίζουν την εμπιστευτικότητα λόγω της φύσης των προϊόντων και μόνο ένα προϊόν εξασφαλίζει και επιπλέον ιδιότητες (διαθεσιμότητα, ακεραιότητα) λόγω της ικανότητάς του να διενεργεί και να ελέγχει την ακεραιότητα των backups στα δεδομένα. Τα αποτελέσματα δεν θεωρούνται ικανοποιητικά διότι μόνο ένα προϊόν εξασφαλίζει παραπάνω από μία ιδιότητα.

Προστατευόμενα αντικείμενα: Από την φύση τους τα προϊόντα αυτά προστατεύουν την ταυτότητα των χρηστών και την πρόσβαση σε δεδομένα. Συγκεκριμένες πληροφορίες βρέθηκαν μόνο σε 2 προϊόντα σύμφωνα με τις οποίες το ένα προϊόν προστατεύει ταυτότητες χρηστών και δεδομένα και το άλλο λογαριασμούς χρηστών και εταιρικά δεδομένα.

Αντιμετωπιζόμενες απειλές: Βρέθηκαν πληροφορίες μόνο σε 5 προϊόντα. Αρχικά, λόγω της φύσης τους, όλα τα προϊόντα αντιμετωπίζουν τη μη εξουσιοδοτημένη και επιβλαβή πρόσβαση τρίτων καθώς και επιθέσεις και παραβάσεις που σχετίζονται με τα διαπιστευτήρια των χρηστών. Σύμφωνα με τις πληροφορίες οι οποίες βρέθηκαν στα προϊόντα, έχουμε τις ακόλουθες επιπλέον απειλές που αντιμετωπίζονται: 1 προϊόν (6.6%) αντιμετωπίζει το ηλεκτρονικό ψάρεμα και την κατάληψη πόρων (αεροπειρατεία-hijacking), 1 προϊόν (6.6%) αντιμετωπίζει τις απάτες (frauds), και 2 προϊόντα (20%) αντιμετωπίζουν επιθέσεις και παραβάσεις που σχετίζονται με τα διαπιστευτήρια των χρηστών.
Τα αποτελέσματα δεν είναι ικανοποιητικά καθώς βρέθηκαν πληροφορίες σε αρκετά μικρό αριθμό προϊόντων και όλα τα προϊόντα καλύπτουν δύο έως τέσσερις απειλές. Βέβαια είναι αναμενόμενο να μην αντιμετωπίζονται πολλά και διαφορετικά είδη απειλών. Όπως έχει αναφερθεί και παραπάνω, αυτό το είδος των προϊόντων έχει πολύ συγκεκριμένη δράση συνεπώς περιμένουμε να αντιμετωπίζει μόνο απειλές που σχετίζονται με την ταυτότητα και την διαχείριση πρόσβασης. Νικητήριο προϊόν είναι το Cloud Identity Premium, το οποίο αντιμετωπίζει δύο είδη απειλών σε αντίθεση με τα υπόλοιπα προϊόντα που αντιμετωπίζουν μόνο ένα.

Περιορισμοί χρήσης: Βρέθηκαν περιορισμοί μόνο σε 5 προϊόντα (33.3%) . 3 προϊόντα (20%) εμφανίζουν περιορισμούς ως προς τον αριθμό χρηστών. Πιο συγκεκριμένα, 1 προϊόν μπορεί να υποστηρίζει έως 50.000 χρήστες, 1 προϊόν μπορεί να υποστηρίξει μέχρι 1 εκατομμύριο ταυτότητες (χρήστες) και σε 1 προϊόν μία άδεια χρήσης υποστηρίζει έως 500 χρήστες. 1 προϊόν (6.6%) υποστηρίζει έως 3 συσκευές ανά χρήστη και σε 1 προϊόν (6.6%) υποστηρίζεται ένας συνολικός αριθμός συναλλαγών για κάθε πελάτη (στιγμιότυπο πελάτη) ο οποίος είναι 400 ανά δευτερόλεπτο . Αυτό το όριο είναι μια συγκέντρωση όλων των σεναρίων που υποστηρίζονται από την πλατφόρμα.
Τα αποτελέσματα δεν είναι ικανοποιητικά καθώς βρέθηκαν πληροφορίες σχεδόν στα μισά προϊόντα. Από πλευράς περιορισμών όλοι θεωρούνται αναμενόμενοι καθώς βρίσκονται στα πλαίσια της

φυσιολογικής λειτουργίας των προϊόντων με εξαίρεση τους περιορισμούς των συμβολαίων. Δεν είναι δυνατόν μία εταιρία να υποχρεώνει τους αγοραστές να κάνουν “ελάχιστη παραγγελία”. Με αυτό τον τρόπο υποψήφιοι αγοραστές με μικρές επιχειρήσεις και μικρές ανάγκες αυτόματα απορρίπτουν τα προϊόντα αυτά λόγω της τιμολογιακής τους πολιτικής.

Δοκιμαστικές εκδόσεις: 3 προϊόντα (20%) δεν παρέχουν δωρεάν δοκιμαστική έκδοση, 2 προϊόντα (13.3%) είναι δωρεάν, 6 προϊόντα (40%) παρέχουν δωρεάν δοκιμαστική έκδοση 30 ημερών. 1 προϊόν (6.6%) παρέχει μόνιμη δωρεάν έκδοση για 10 χρήστες και 10 συσκευές, 1 προϊόν (6.6%) παρέχει 14 μέρες δωρεάν ή μόνιμη δωρεάν έκδοση με περιορισμένα χαρακτηριστικά, 1 προϊόν (6.6%) παρέχει 60 μέρες δωρεάν και τέλος 1 προϊόν (6.6%) παρέχει 90 μέρες δωρεάν.
Τα αποτελέσματα είναι ικανοποιητικά καθώς 2 προϊόντα είναι δωρεάν, 2 προϊόντα παρέχουν δωρεάν έκδοση με περιορισμένους πόρους και τα περισσότερα προϊόντα προσφέρουν δοκιμαστική έκδοση με διάρκεια μεγαλύτερη ή ίση των 30 ημερών. Νικητήρια προϊόντα σε αυτή την κατηγορία είναι το Cloud Identity Premium και το JumpCloud Directory-as-a-Service, τα οποία προσφέρουν μόνιμες δωρεάν εκδόσεις με περιορισμένες δυνατότητες.

Τρόπος χρήσης: 5 προϊόντα (33.3%) υποστηρίζουν και τα 3 είδη διεπαφών. 8 προϊόντα (13.3%) υποστηρίζουν διεπαφή προγραμματισμού εφαρμογών μεταφοράς αναπαραστατικής κατάστασης και γραφικό περιβάλλον εργασίας μέσω διαδικτύου και τέλος 3 προϊόντα (20%) υποστηρίζουν γραφικό περιβάλλον εργασίας μέσω διαδικτύου. Αν δούμε τις τιμές αποτίμησης μεμονωμένα η διεπαφή προγραμματισμού εφαρμογών μεταφοράς αναπαραστατικής κατάστασης εμφανίζεται σε 13 προϊόντα (86.6%). Το γραφικό περιβάλλον εργασίας μέσω διαδικτύου εμφανίζονται σε 15 προϊόντα (100%) και η γραμμή εντολών εμφανίζεται σε 5 προϊόντα (33.3%).
Είναι αναμενόμενο μεγάλος αριθμός προϊόντων να υποστηρίζει διεπαφή προγραμματισμού εφαρμογών μεταφοράς αναπαραστατικής κατάστασης και γραφικό περιβάλλον εργασίας μέσω διαδικτύου διότι σχεδόν όλα τα προϊόντα προσφέρονται σαν λογισμικό. Τα αποτελέσματα θεωρούνται ικανοποιητικά καθώς παρατηρούμε πως 13 από τα 15 προϊόντα υποστηρίζουν δύο ή τρεις τεχνολογίες.

Αγορές: 5 προϊόντα (33.3%) εντοπίστηκαν στο Amazon web services, 4 προϊόντα (26.6%) εντοπίστηκαν στο Google cloud platform και 5 προϊόντα (33.3%) εντοπίστηκαν στο Microsoft Azure. 1 προϊόν (6.6%) εντοπίστηκε στο διαδίκτυο και όχι σε κάποια αγορά. Κανένα προϊόν δεν βρέθηκε σε παραπάνω από μία αγορές, συνεπώς τα αποτελέσματα δεν είναι ικανοποιητικά.

Επίπεδο/είδος υποστήριξης: 14 προϊόντα (93.3%) προσφέρουν υποστήριξη μέσω τηλεφώνου, 15 προϊόντα (100%) μέσω email, 8 προϊόντα (53.3%) μέσω δελτίων (tickets), και 3 προϊόντα (20%) μέσω μηνυμάτων (chat). 15 προϊόντα (100%) διαθέτουν υποστήριξη κοινοτήτων χρηστών (κοινότητα, φόρουμ, blog, αποθετήριο κώδικα στο github), 13 προϊόντα (86.6%) διαθέτουν τεκμηρίωση (documentation), 7 προϊόντα (46.6%) διαθέτουν πύλη υποστήριξης (portal), 15 προϊόντα (100%) διαθέτουν υποστηρικτικό

υλικό (έγγραφα με πληροφορίες & βίντεο & FAQ). 7 προϊόντα (46.6%) διαθέτουν βάση γνώσης (knowledge base). 4 προϊόντα (26.6%) διαθέτουν ενημέρωση για νέα προϊόντα και 2 προϊόντα (13.3%) διαθέτουν κέντρο βοήθειας. Τέλος, ένα προϊόν (6.6%) διαθέτει εκπαιδευτικό υλικό .

Επιπλέον, υπάρχουν 11 προϊόντα (73.3%) τα οποία παρέχουν πακέτα υποστήριξης. 5 προϊόντα (33.3%) προσφέρουν τρία πακέτα, 4 προϊόντα (26.6%) προσφέρουν δυο πακέτα, 1 προϊόν (6.6%) προσφέρει τέσσερα πακέτα και 1 προϊόν (6.6%) προσφέρει πέντε πακέτα. Το προϊόν που προσφέρει τα περισσότερα (πέντε) πακέτα είναι το Okta Identity Platform.

Για την ημερολογιακή/χρονική διάρκεια κατά την οποία παρέχεται υποστήριξη 5 προϊόντα (33.3%) προσφέρουν υποστήριξη 24/7, 6 προϊόντα (40%) προσφέρουν υποστήριξη από 8/5 (εργάσιμες ώρες) έως 24/7 και τέλος 1 προϊόν (6.6) προσφέρει υποστήριξη από 24/5 έως 24/7.

Τα αποτελέσματα κρίνονται αρκετά ικανοποιητικά καθώς παρατηρούμε πως αρκετά προϊόντα προσφέρουν πολλαπλά είδη υποστήριξης και επικοινωνίας. Επιπλέον, σχεδόν τα ⅔ των προϊόντων προσφέρουν διαφορετικά πακέτα υποστήριξης ώστε να προσαρμόζονται στις ανάγκες των πελατών και το ⅓ των προϊόντων παρέχουν υποστήριξη 24/7. Νικητήριο προϊόν για αυτή την κατηγορία είναι το Okta Identity Platform, το οποίο προσφέρει 5 διαφορετικά πακέτα και υποστήριξη 24/7.

Νικητήριο προϊόν για ολόκληρη την κατηγορία είναι το Cloud Identity Premium, το οποίο εμφανίζεται ως νικητήριο 3 φορές.

5.2.5 Πρόληψη απώλειας δεδομένων (Data Loss Prevention)

Για αυτή την ενότητα βρέθηκαν 15 προϊόντα με επαρκή τεκμηρίωση, τα οποία αποτιμήθηκαν. Τα αποτελέσματα αποτίμησης εμφανίζονται στον Πίνακα 5 του παραρτήματος. Παρακάτω παρέχουμε μια στατιστική ανάλυση των αποτελεσμάτων αυτών ανά κριτήριο.

Τρόπος παράδοσης: 8 προϊόντα (53.3%) προσφέρονται σαν λογισμικό, 4 προϊόντα (26.6%) προσφέρονται σαν υποδομή και 3 προϊόντα (20%) προσφέρονται σαν υποδομή και σαν λογισμικό. Παρατηρούμε πως κυριαρχεί ο τρόπος παράδοσης ως λογισμικό λόγω των πλεονεκτημάτων που έχει απέναντι στους υπόλοιπους τρόπους παράδοσης. Βέβαια, όσο περισσότεροι τρόποι παράδοσης υποστηρίζονται τόσο το καλύτερο διότι υπάρχει μεγαλύτερη ευελιξία. Τα αποτελέσματα δεν είναι ιδιαίτερα ικανοποιητικά καθώς μόνο 3 προϊόντα υποστηρίζουν δύο τρόπους παράδοσης. Τα προϊόντα αυτά (δείτε πίνακα αποτίμησης) είναι και τα νικητήρια.

Μοντέλο διάταξης: Για 3 προϊόντα δεν βρέθηκαν πληροφορίες. 11 προϊόντα (73.3%) υποστηρίζουν δημόσιο νέφος και 1 προϊόν (6.6%) υποστηρίζει δημόσιο ή ιδιωτικό νέφος. Δεν είναι ικανοποιητικό πως μόνο ένα προϊόν διατίθεται με δύο τρόπους. Αυτό είναι αναμενόμενο διότι τα περισσότερα προϊόντα στα οποία βρέθηκαν πληροφορίες υποστηρίζουν τρόπο παράδοσης SaaS συνεπώς το μοντέλο διάταξης

είναι λογικά το δημόσιο νέφος. Νικητήριο προϊόν είναι το Endpoint Protector, το οποίο υποστηρίζει δημόσιο ή ιδιωτικό νέφος.

Κατηγορία ασφάλειας: 9 προϊόντα (60%) καλύπτουν επιπλέον την κατηγορία της κρυπτογράφησης. Αυτό συμβαίνει διότι τα προϊόντα πρόληψης απώλειας δεδομένων κρυπτογραφούν τα δεδομένα για να ενισχύσουν ακόμη περισσότερο την ασφάλεια του πληροφοριακού συστήματος. Έτσι εξασφαλίζουν πως ακόμα και αν υπάρξει κάποια διαρροή δεδομένων/πληροφοριών, αυτά θα βρίσκονται σε μη αναγνώσιμη μορφή, συνεπώς το πιθανότερο είναι πως δε θα μπορούν να αξιοποιηθούν από κάποιον τρίτο. Τα αποτελέσματα είναι οριακά ικανοποιητικά καθώς παραπάνω προϊόντα θα έπρεπε να έχουν τη δυνατότητα της κρυπτογράφησης με βάση την αναγκαιότητα της λειτουργίας αυτής για την τρέχουσα κατηγορία προϊόντος.

Μοντέλο κόστους: Σχετικά με την τιμολόγηση, για 2 προϊόντα (13.3%) δεν βρέθηκαν πληροφορίες. 3 προϊόντα (20%) παρέχουν πληροφορίες τιμολόγησης μόνο με επικοινωνία με την εταιρία. 8 προϊόντα (53.3%) τιμολογούν με βάση τον αριθμό των χρηστών, 1 προϊόν (6.6%) τιμολογεί με άδεια χρήσης τόσο για μεμονωμένες μονάδες (modules) όσο και για συγκεκριμένο αριθμό ελεγχόμενων χρηστών και τέλος 1 προϊόν (6.6%) τιμολογεί με βάση τον όγκο δεδομένων που επεξεργάζονται. Επίσης, 1 προϊόν (6.6%) έχει ελάχιστο ποσό χρέωσης, το οποίο οφείλεται στον περιορισμό πως τουλάχιστον 5 χρήστες θα πρέπει να προστατεύονται ανά πελάτη.
Σχετικά με την ύπαρξη πακέτων δεν εντοπίστηκαν διαφορετικά πακέτα τιμολόγησης σε κάποιο προϊόν, πράγμα που χρήζει βελτίωσης.
Τέλος, σχετικά με τη χρονική συνιστώσα των πληρωμών 2 προϊόντα (13.3%) έχουν μηνιαία χρέωση, 2 προϊόντα (13.3%) έχουν ετήσια χρέωση, και 1 προϊόν (6.6%) έχει χρέωση ανά 12,18 ή 36 μήνες.
Τα αποτελέσματα δεν είναι ικανοποιητικά καθώς σχεδόν κανένα προϊόν δεν προσφέρει διαφορετικά πακέτα πληρωμής ενώ πληροφορίες για τη χρονική συχνότητα βρέθηκαν μόνο στο ⅓ των προϊόντων. Νικητήριο προϊόν είναι το Forcepoint DLP, το οποίο προσφέρει τρεις επιλογές σχετικά με το χρονικό διάστημα χρέωσης.

Μηχανισμοί ασφάλειας: Υπάρχει 1 προϊόν (6.6%) το οποίο υποστηρίζει μόνο τη βασική λειτουργικότητα, το Digital Guardian Data Loss Prevention. Επίσης, υπάρχουν 14 προϊόντα (93.3%) με έξτρα λειτουργικότητα πέρα από τη βασική. Τα προϊόντα που προσφέρουν τη λιγότερη από την έξτρα λειτουργικότητα είναι τα Somansa SaaS Endpoint DLP και SecureTower DLP, τα οποία προσφέρουν από 1 έξτρα λειτουργικότητα. Από την άλλη πλευρά, τα προϊόντα με τις περισσότερες έξτρα λειτουργικότητες είναι τα Endpoint Protector και Zecurion DLP που προσφέρουν 6 και 5 έξτρα λειτουργικότητες, αντίστοιχα. Τα προϊόντα αυτά είναι και τα νικητήρια για αυτό το κριτήριο.
Κάποιες από τις λειτουργικότητες των νικητήριων προϊόντων που φαίνονται ενδιαφέρουσες είναι η ελαχιστοποίηση ψευδών θετικών στοιχείων, ο περιορισμός σπατάλης πόρων και η ενσωμάτωση με

συστήματα SIEM για το Endpoint Protector. Αντίστοιχα, στο Zecurion DLP οι πιο ενδιαφέρουσες είναι η μελέτη του συναισθηματικού προφίλ των χρηστών και ο χάρτης συνδέσεων χρηστών.
Σχετιζόμενα με τις επιπλέον κατηγορίες που καλύπτονται, θα πρέπει να τονιστεί πως πολλά από τα προϊόντα προσφέρουν την έξτρα λειτουργικότητα κρυπτογράφησης των δεδομένων, που είναι και ο λόγος για τον οποίο καλύπτεται η έξτρα κατηγορία της κρυπτογράφησης. Τα αποτελέσματα είναι ικανοποιητικά καθώς σχεδόν όλα τα προϊόντα καλύπτουν επιπλέον λειτουργικότητες.

Μη λειτουργικές εγγυήσεις: Βρέθηκαν πληροφορίες μόνο για 4 προϊόντα. 1 προϊόν (6.6) παρέχει συμβόλαιο συμφωνίας επιπέδου υπηρεσιών μόνο με επικοινωνία με την εταιρία. Ένα άλλο προϊόν (6.6%) προσφέρει διαθεσιμότητα 99.5% και το εξής σύστημα ποινών: για διαθεσιμότητα από 99.5% έως 99% επιστροφή 10% του κόστους της μηνιαίας συνδρομής, για 95% έως 99% επιστροφή 25% του κόστους και για μικρότερη του 95% επιστροφή 50% του κόστους.
1 προϊόν (6.6%) προσφέρει διαθεσιμότητα 99%. Για διαθεσιμότητα από 95% έως 99% επιστρέφεται το χρηματικό για 3 ημέρες χρήσης, για 95% έως 90% για 5 μέρες και για μικρότερη του 90% για 10 μέρες.
1 προϊόν (6.6%) προσφέρει χαμηλή αναλογία ψευδώς θετικών συμβάντων με 2 περιπτώσεις (συμβάντα) την εβδομάδα για κάθε 500 χρήστες με επίπεδο κινδύνου > 1.
Νικητήρια προϊόντα είναι το Cloud Data Loss Prevention, το οποίο προσφέρει 99.5% διαθεσιμότητα με σύστημα ποινών, και το Beyond DLP που προσφέρει υψηλή ακρίβεια έχοντας χαμηλή αναλογία ψευδώς θετικών συμβάντων. Τα αποτελέσματα δεν είναι καθόλου ικανοποιητικά διότι βρέθηκαν πληροφορίες σε λιγότερο από το ⅓ των προϊόντων.

Είδος προσφερόμενης προστασίας: Η κύρια λειτουργικότητα σε όλα τα προϊόντα (100%) είναι ανιχνευτική (detective) και προληπτική (preventive). Αυτό είναι αναμενόμενο και οφείλεται στη φύση των προϊόντων πρόληψης απώλειας δεδομένων. Έχουν τη δυνατότητα να πραγματοποιούν ελέγχους και να σαρώνουν τα δεδομένα με σκοπό να εντοπιστεί κάποια ύποπτη δραστηριότητα, άρα λειτουργούν ανιχνευτικά. Επίσης, έχουν τη δυνατότητα να εμποδίσουν τη μετακίνηση αρχείων/δεδομένων, το οποίο είναι ένα προληπτικό μέτρο διότι εκτελείται μια προληπτική ενέργεια που προλαμβάνει τις δυσάρεστες συνέπειες που θα προκαλούσε η διαρροή/απώλεια αρχείων/δεδομένων. Έτσι, λοιπόν, βλέπουμε πως αυτή η κατηγορία προϊόντων συνδυάζει δύο είδη προστασίας, πράγμα που είναι ικανοποιητικό.

Ιδιότητες ασφάλειας: Όλα τα προϊόντα (100%) εξασφαλίζουν την διαθεσιμότητα διότι ο στόχος των προϊόντων πρόληψης απώλειας δεδομένων είναι από τη φύση τους να εμποδίζουν την απώλεια και διαρροή δεδομένων. Όπως είναι λογικό, όταν υπάρχει απώλεια δεδομένων, παύει να υπάρχει διαθεσιμότητα. Επιπλέον, τα 9 προϊόντα (60%), τα οποία υποστηρίζουν την κρυπτογράφηση, εξασφαλίζουν την εμπιστευτικότητα διότι όταν ένας τρίτος αποκτήσει πρόσβαση σε αρχεία αυτά δεν θα βρίσκονται σε αναγνώσιμη/αξιοποιήσιμη μορφή, εφόσον το περιεχόμενό τους θα είναι κρυπτογραφημένο.

Προστατευόμενα αντικείμενα: Από την φύση τους τα προϊόντα αυτά προστατεύουν τα δεδομένα. Συνεπώς, όλα τα προϊόντα (100%) προστατεύουν δεδομένα / πληροφορίες εντός του πληροφοριακού συστήματος. Αν τα δούμε πιο αναλυτικά, 12 προϊόντα (80%) προστατεύουν δεδομένα (ευαίσθητα ,προσωπικά, εταιρικά) 4 προϊόντα (26.6%) προστατεύουν πληροφορίες (κρίσιμες, εμπιστευτικές, ευαίσθητες), 2 προϊόντα (13.3%) προστατεύουν προσωπικά στοιχεία ταυτοποίησης (PII). 1 προϊόν (6.6%) προστατεύει ιδιωτικά αρχεία δεδομένων, 1 προϊόν (6.6%) προστατεύει συσκευές usb & πνευματική ιδιοκτησία και τέλος 1 προϊόν (6.6%) προστατεύει πληροφορίες υγείας, οικονομικά στοιχεία της εταιρείας, εμπορικά μυστικά, και δεδομένα πιστωτικών καρτών. Τα παραπάνω αποτελέσματα θεωρούνται ικανοποιητικά, αν λογαριάσουμε και την φύση των εν λόγω προϊόντων.

Αντιμετωπιζόμενες απειλές: Όλα τα προϊόντα (100%), λόγω της φύσης τους, αντιμετωπίζουν την διαρροή/απώλεια δεδομένων. 4 προϊόντα (26.6%) αντιμετωπίζουν κακόβουλες δραστηριότητες που μπορεί να επιτελούνται είτε από λογισμικό είτε από χρήστες άρα προστατεύουν τόσο από εξωτερικές όσο και από εσωτερικές απειλές. 5 προϊόντα (30%) αντιμετωπίζουν εσωτερικές απειλές (π.χ. κλοπή και πώληση δεδομένων από κάποιον υπάλληλο με στόχο το οικονομικό όφελος, ακούσια αποστολή μηνύματος ηλεκτρονικού ταχυδρομείου με ευαίσθητες πληροφορίες σε λάθος παραλήπτη), 2 προϊόντα (13.3%) αντιμετωπίζουν το λυτρισμικό, 2 προϊόντα (13.3%) αντιμετωπίζουν τις εξωτερικές απειλές (π.χ. επιθέσεις άρνησης υπηρεσίας, ηλεκτρονικό ψάρεμα, κακόβουλο λογισμικό), 1 προϊόν (6.6%) αντιμετωπίζει τα ανθρώπινα λάθη και τέλος 1 προϊόν (6.6%) αντιμετωπίζει την κλοπή δεδομένων. Αν δούμε τον αριθμό απειλών ανά προϊόν υπάρχουν 8 προϊόντα (53.3%) που αντιμετωπίζουν μία απειλή (τη διαρροή/απώλεια δεδομένων), υπάρχουν 6 προϊόντα (40%) που αντιμετωπίζουν από δύο έως τέσσερις απειλές και τέλος υπάρχει 1 προϊόν (6.6%) το οποίο αντιμετωπίζει πέντε απειλές. Το προϊόν αυτό, το SecurEnvoy DLP, είναι και το νικητήριο.

Περιορισμοί χρήσης: Βρέθηκαν περιορισμοί σε 6 προϊόντα (40%). Για 1 προϊόν (6.6%) η εταιρία δεν είναι σε θέση να υποστηρίζει συνεχώς παλαιότερες, ξεπερασμένες εκδόσεις του προϊόντος αυτού, 1 προϊόν (6.6%) υποστηρίζει μόνο Windows και Linux, και 2 προϊόντα (13.3%) υποστηρίζουν μόνο Windows. 1 προϊόν (6.6%) μπορεί να υποστηρίξει έως 1 εκατομμύριο χρήστες και τέλος 1 προϊόν (6.6%) αποτρέπει έως και το 98% των διαρροών δεδομένων και προστατεύει έως περίπου 200.000 υπολογιστές. 1 προϊόν (6.6%) στην μεγαλύτερη έκδοση του υποστηρίζει έως 299 χρήστες.
Όλοι σχεδόν οι περιορισμοί θεωρούνται αναμενόμενοι καθώς βρίσκονται στα πλαίσια της φυσιολογικής λειτουργίας των προϊόντων. Το μόνο που δεν ήταν αναμενόμενο είναι ο περιορισμός που αναφέρει πως δεν υποστηρίζονται παλαιότερες εκδόσεις ενός προϊόντος. Αυτό μπορεί να λειτουργήσει αρνητικά και να απωθήσει κάποιον ενδιαφερόμενο αγοραστή, διότι μία μελλοντική αναβάθμιση προϊόντος ίσως να έχει κάποιο χρηματικό κόστος. Επιπλέον ίσως να αλλάξει ο τρόπος χρήσης του προϊόντος οδηγώντας σε έξτρα κόστος & χρόνο για τον πελάτη για την εκμάθησή του. Επιπλέον, δεν είναι δυνατόν να υπάρχει αυτή η πολιτική σε μία εταιρία χωρίς να προσδιορίζεται ακριβώς ποια είναι η εναπομένουσα χρονική διάρκεια για την οποία θα υποστηρίζεται η τρέχουσα έκδοση ενός προϊόντος.

Δοκιμαστικές εκδόσεις: 4 προϊόντα (26.6%) δεν παρέχουν δωρεάν δοκιμαστική έκδοση, 2 προϊόντα (13.3%) παρέχουν δωρεάν δοκιμαστική έκδοση χωρίς να αναφέρουν την χρονική διάρκεια, 6 προϊόντα (40%) παρέχουν δωρεάν δοκιμαστική έκδοση 30 ημερών. 1 προϊόν (6.6%) παρέχει δωρεάν έκδοση για 10 ημέρες, 1 προϊόν (6.6%) παρέχει δωρεάν έκδοση για 5 ημέρες και τέλος 1 προϊόν (6.6%) παρέχει 90 ημέρες ή 300$ κόστους χρήσης (ότι έρθει πρώτο) δωρεάν.
Τα αποτελέσματα είναι οριακά ικανοποιητικά καθώς 4 προϊόντα δεν διαθέτουν δωρεάν έκδοση και σε 2 προϊόντα η διάρκεια δοκιμαστικής έκδοσης είναι έως 10 ημέρες που θεωρούνται λίγες. Νικητήριο προϊόν σε αυτή την κατηγορία είναι το Cloud Data Loss Prevention, το οποίο προσφέρει δωρεάν έκδοση με τη μεγαλύτερη διάρκεια (90 ημέρες).

Τρόπος χρήσης: 3 προϊόντα (20%) υποστηρίζουν και τα τρία είδη διεπαφών. 3 προϊόντα (20%) υποστηρίζουν διεπαφή προγραμματισμού εφαρμογών μεταφοράς αναπαραστατικής κατάστασης και γραφικό περιβάλλον εργασίας μέσω διαδικτύου, 3 προϊόντα (20%) διεπαφή προγραμματισμού εφαρμογών μεταφοράς αναπαραστατικής κατάστασης και χρήση γραμμής εντολών, 1 προϊόν (6.6%) υποστηρίζει γραφικό περιβάλλον εργασίας μέσω διαδικτύου και χρήση γραμμής εντολών, 5 προϊόντα (33.3%) υποστηρίζουν μόνο γραφικό περιβάλλον εργασίας μέσω διαδικτύου.
Αν δούμε τις τιμές αποτίμησης μεμονωμένα, η διεπαφή προγραμματισμού εφαρμογών μεταφοράς αναπαραστατικής κατάστασης εμφανίζεται σε 9 προϊόντα (60%). Το γραφικό περιβάλλον εργασίας μέσω διαδικτύου εμφανίζονται σε 12 προϊόντα (80%) και η γραμμή εντολών εμφανίζεται σε 7 προϊόντα (46.6%).
Βλέπουμε να κυριαρχεί το γραφικό περιβάλλον εργασίας μέσω διαδικτύου. Αυτό συμβαίνει διότι τα περισσότερα προϊόντα διατίθενται σαν λογισμικό. Στην περίπτωση αυτή ο χρήστης συνδέεται σε ένα γραφικό περιβάλλον εργασίας μέσω διαδικτύου ώστε να χρησιμοποιήσει το προϊόν. Θα λέγαμε δηλαδή ότι από τη φύση του όταν ένα προϊόν διατίθεται σαν λογισμικό περιλαμβάνει γραφικό περιβάλλον εργασίας μέσω διαδικτύου. Επιπλέον, ίσως χρειάζεται κατάλληλη διαμόρφωση για την σωστή χρήση των προϊόντων και ένα γραφικό περιβάλλον βοηθά προς αυτή την κατεύθυνση. Τα αποτελέσματα θεωρούνται ικανοποιητικά καθώς τα ⅔ των προϊόντων υποστηρίζουν δύο ή τρεις τεχνολογίες.

Αγορές: Μόνο 5 προϊόντα (33.3%) εντοπίστηκαν στις αγορές.1 προϊόν (6.6%) εντοπίστηκε στο Amazon web services και στο Microsoft Azure, 1 προϊόν (6.6%) εντοπίστηκε στο Google cloud platform και 3 προϊόντα (20%) εντοπίστηκαν στο Microsoft Azure. 10 προϊόντα (66.6%) εντοπίστηκαν στο διαδίκτυο και όχι σε κάποια αγορά.
Τα αποτέλεσμα δεν είναι καθόλου ικανοποιητικά διότι μόνο το ⅓ των προϊόντων εντοπίστηκε στις αγορές. Το γεγονός πως τα προϊόντα δεν βρίσκονται στις αγορές ίσως να σημαίνει πως δεν πληρούν ορισμένες προϋποθέσεις για να μπουν σε κάποια αγορά. Άρα, λοιπόν, είναι πιο ανεπαρκή σε σχέση με αυτά που βρίσκονται στις αγορές. Αυτή η εικασία επιβεβαιώθηκε στην περίπτωση μας ως προς την πλευρά της πληροφόρησης καθώς σε ορισμένα κριτήρια έχουν βρεθεί πληροφορίες για πολύ λίγα

προϊόντα. Συνεπώς, η ελάχιστη πληροφόρηση και τεκμηρίωση μπορεί να θεωρηθεί ως ένας ανασταλτικός παράγοντας για την εγγραφή και δημοσίευση ενός προϊόντος σε μια αγορά. Νικητήριο προϊόν είναι το Teramind καθώς είναι το μοναδικό που εντοπίστηκε σε δύο αγορές.

Επίπεδο/είδος υποστήριξης: Όλα τα προϊόντα (100%) προσφέρουν υποστήριξη μέσω τηλεφώνου και email και 7 προϊόντα (46,6%) μέσω δελτίων (tickets). 6 προϊόντα (40%) διαθέτουν υποστήριξη κοινοτήτων χρηστών (κοινότητα, φόρουμ, blog), 11 προϊόντα (73.3%) διαθέτουν τεκμηρίωση (documentation), 2 προϊόντα (13.3%) διαθέτουν κέντρο υποστήριξης, 14 προϊόντα (93.3%) διαθέτουν υποστηρικτικό υλικό (έγγραφα με πληροφορίες, βίντεο, FAQ). 9 προϊόντα (60%) διαθέτουν βάση γνώσης (knowledge base). 3 προϊόντα (20%) διαθέτουν ενημέρωση για νέα προϊόντα και 5 προϊόντα (33.3%) διαθέτουν εκπαίδευση/εκπαιδευτικό υλικό. Τέλος, υπάρχουν διάφοροι τρόποι υποστήριξης που παρέχονται από μεμονωμένα προϊόντα όπως πύλη συνεργατών, ιστοσελίδα βοήθειας, ειδοποιήσεις και εργαλείο testing Σχετικά με τα πακέτα υποστήριξης, αυτά προσφέφονται από 5 προϊόντα (33.3%). Ειδικότερα, 3 προϊόντα (20%) προσφέρουν τρία πακέτα, 1 προϊόν (6.6%) προσφέρει δύο πακέτα και 1 προϊόν (6.6%) προσφέρει τέσσερα πακέτα.
Για την ημερολογιακή/χρονική διάρκεια κατά την οποία παρέχεται υποστήριξη, υπάρχουν 5 προϊόντα (33.3%) τα οποία προσφέρουν υποστήριξη 24/7, 1 προϊόν (6.6%) το οποίο προσφέρει υποστήριξη 8/5 και 1 προϊόν (6.6%) το οποίο προσφέρει υποστήριξη από 8/5 έως 24/7
Τα αποτελέσματα κρίνονται μη ικανοποιητικά καθώς παρατηρούμε πως μόνο το ⅓ των προϊόντων προσφέρει διαφορετικά πακέτα υποστήριξης ώστε να προσαρμόζονται επίσης ανάγκες των πελατών. Επίσης, το ⅓ των προϊόντων προσφέρει υποστήριξη 24/7. Νικητήριο προϊόν για αυτή την κατηγορία είναι το GTB Technologies DLP SaaS, το οποίο προσφέρει τα περισσότερα πακέτα (4 πακέτα) και όλα αυτά διαθέτουν υποστήριξη 24/7.

Νικητήριο προϊόν για ολόκληρη την κατηγορία είναι το Endpoint Protector, το οποίο εμφανίζεται ως νικητήριο 3 φορές.

5.2.6 Κρυπτογράφηση (Encryption)

Για αυτή την ενότητα βρέθηκαν 15 προϊόντα με επαρκή τεκμηρίωση, τα οποία αποτιμήθηκαν. Τα αποτελέσματα αποτίμησης εμφανίζονται στον Πίνακα 6 του παραρτήματος. Παρακάτω παρέχουμε μια στατιστική ανάλυση των αποτελεσμάτων αυτών ανά κριτήριο.

Τρόπος παράδοσης: 10 προϊόντα (66.6%) προσφέρονται σαν λογισμικό, 4 προϊόντα (26.6%) προσφέρονται σαν υποδομή και 1 προϊόν (6.6%) προσφέρεται σαν υποδομή και σαν λογισμικό. Παρατηρούμε πως τα περισσότερα προϊόντα είναι διαθέσιμα σαν λογισμικό λόγω των πλεονεκτημάτων που προσφέρει αυτός ο τρόπος σε σχέση με τους υπόλοιπους τρόπους παράδοσης. Παρόλα αυτά, όσο περισσότεροι τρόποι παράδοσης υποστηρίζονται τόσο το καλύτερο καθώς ο αγοραστής έχει τη δυνατότητα να

επιλέξει ότι ακριβώς ταιριάζει στις ανάγκες του. Τα αποτελέσματα δεν είναι ιδιαίτερα ικανοποιητικά καθώς μόνο 1 προϊόν υποστηρίζει δύο τρόπους παράδοσης. Το προϊόν αυτό, το Fortanix Data Security Manager, είναι και το νικητήριο.

Μοντέλο διάταξης: Για 1 προϊόν δεν βρέθηκαν πληροφορίες. 12 προϊόντα (80%) υποστηρίζουν δημόσιο νέφος και 2 προϊόντα (13.3%) υποστηρίζουν δημόσιο ή ιδιωτικό νέφος. Δεν είναι ικανοποιητικό πως μόνο δύο προϊόντα υποστηρίζουν 2 διαφορετικά είδη νεφών. Από την άλλη πλευρά, το αποτέλεσμα είναι αναμενόμενο καθώς τα περισσότερα προϊόντα υποστηρίζουν τρόπο παράδοσης SaaS συνεπώς το μοντέλο διάταξης είναι λογικά το δημόσιο νέφος. Νικητήρια προϊόντα είναι τα Fortanix Data Security Manager και Entrust DataControl, τα οποία υποστηρίζουν δημόσιο ή ιδιωτικό νέφος.

Κατηγορία ασφάλειας: 3 προϊόντα (20%) καλύπτουν επιπρόσθετα την κατηγορία της διαχείρισης ταυτότητας και πρόσβασης διότι υλοποιούν μηχανισμούς διαχείρισης πρόσβασης. 1 προϊόν (6.6%) καλύπτει επιπρόσθετα την κατηγορία της πρόληψης απώλειας δεδομένων διότι πραγματοποιεί ελέγχους για να προστατεύσει τα δεδομένα που μπορούν να μεταφερθούν εκτός του οργανισμού. 1 προϊόν (6.6%) καλύπτει επιπρόσθετα την κατηγορία της επιχειρησιακής συνέχειας και αποκατάστασης καταστροφών διότι δημιουργεί αντίγραφα ασφαλείας των δεδομένων.
Τα αποτελέσματα δεν είναι αρκετά ικανοποιητικά καθώς μόνο το ⅓ των προϊόντων καλύπτει παραπάνω από μία κατηγορία. Νικητήριο προϊόν είναι το DSaaS_Masking_Tokenization_Encryption_API, το οποίο καλύπτει 2 επιπλέον κατηγορίες (IAM, DLP), την ίδια στιγμή που ορισμένα από τα υπόλοιπα προϊόντα καλύπτουν μόνο μία έξτρα κατηγορία.

Μοντέλο κόστους: Σχετικά με την τιμολόγηση, για 2 προϊόντα (13.3%) δεν βρέθηκαν πληροφορίες. Για 3 προϊόντα (20%) η μόνη πληροφορία που βρέθηκε είναι ότι διατίθενται με άδεια χρήσης BYOL (bring your own license). 3 προϊόντα (20%) τιμολογούν με βάση τον όγκο των δεδομένων, 5 προϊόντα (33.3%) τιμολογούν με βάση τα χαρακτηριστικά. 2 προϊόντα (13.3%) τιμολογούν με βάση τον αριθμό χρηστών, 3 προϊόντα (13.3%) τιμολογούν με βάση τη χρήση και 1 προϊόν (6.6%) τιμολογεί με βάση το φόρτο εργασίας.
Σχετικά με την ύπαρξη πακέτων, 2 προϊόντα (13.3%) διαθέτουν δύο διαφορετικά πακέτα, 2 προϊόντα (13.3%) διαθέτουν τρία διαφορετικά πακέτα και 1 προϊόν (6.6%), το StrongSalt API, διαθέτει 12 διαφορετικά πακέτα (4 πακέτα σχετικά με τον όγκο των δεδομένων και 3 πακέτα σχετικά με τα χαρακτηριστικά).
Τέλος, σχετικά με τη χρονική συνιστώσα των πληρωμών, 4 προϊόντα (26.6%) έχουν μηνιαία χρέωση και 4 προϊόντα (26.6%) έχουν ως ελάχιστη χρονική διάρκεια συμβολαίου το ένα έτος, όπου τα 2 από αυτά (13.3%) επιτρέπουν στον χρήστη να διαλέξει μεταξύ ετήσιου & τριετούς συμβολαίου. 1 προϊόν (6.6%) επιβάλει πληρωμή μηνιαίως ή ετησίως και 1 προϊόν (6.6%) μηνιαίως ή εφάπαξ.
Τα αποτελέσματα δεν είναι αρκετά ικανοποιητικά καθώς μόνο 5 προϊόντα διαθέτουν διαφορετικά πακέτα πληρωμής και μόνο 4 προϊόντα επιτρέπουν στον χρήστη να επιλέξει τη συχνότητα πληρωμής. Νικητήριο προϊόν είναι το StrongSalt API, το οποίο διαθέτει 12 διαφορετικά πακέτα.

Μηχανισμοί ασφάλειας: Υπάρχει 1 προϊόν (6.6%) που υποστηρίζει μόνο τη βασική λειτουργικότητα, το Encrypted ecosystem for truly private data (usecrypt safe). Υπάρχουν 14 προϊόντα (93.3%) τα οποία υποστηρίζουν έξτρα λειτουργικότητα πέρα από τη βασική. Ενδεικτικά δύο έξτρα λειτουργικότητες που εντάσσονται στην τρέχουσα κατηγορία και δείχνουν ενδιαφέρουσες είναι η απόκριση σε παραβίαση δεδομένων με ένα μόνο κλικ στο προϊόν Crypteron Data Security και η προβολή αρχείων καταγραφής, έλεγχος ακεραιότητας αρχείων καταγραφής και δυνατότητες εναλλαγής αρχείων καταγραφής στο προϊόν D'Amo.

Το ⅓ των προϊόντων που καλύπτουν επιπλέον κατηγορίες καλύπτουν έξτρα λειτουργικότητες από τις κατηγορίες αυτές. Τα υπόλοιπα ⅔ καλύπτουν έξτρα λειτουργικότητες μόνο από την κατηγορία της κρυπτογράφησης. Τα προϊόντα που προσφέρουν τη λιγότερη λειτουργικότητα στην κατηγορία τους είναι τα File Vault API και Data Vault API, τα οποία προσφέρουν συνολικά από 4 λειτουργικότητες. Από την άλλη πλευρά, το προϊόν με την περισσότερη έξτρα λειτουργικότητα είναι το D' Amo που προσφέρει συνολικά 19 λειτουργικότητες. Οπότε, πρόκειται για ένα αρκετά σύνθετο προϊόν με πολλές δυνατότητες. Τα προϊόν αυτό είναι και το νικητήριο για αυτή την κατηγορία.

Τα αποτελέσματα είναι ικανοποιητικά καθώς σχεδόν όλα τα προϊόντα καλύπτουν επιπλέον λειτουργικότητες.

Μη λειτουργικές εγγυήσεις: Βρέθηκαν πληροφορίες μόνο για 5 προϊόντα. Ειδικότερα, 2 προϊόντα (13.3%) προσφέρουν 99.95% διαθεσιμότητα, 2 προϊόντα (13.3%) προσφέρουν 99.9% διαθεσιμότητα και 1 προϊόν (6.6%) προσφέρει διαθεσιμότητα 99.5%. Το ένα προϊόν με 99.95% διαθεσιμότητα, το Crypteron Data Security, διαθέτει σύστημα ποινών όπου αν η μηνιαία διαθεσιμότητά της είναι μικρότερη από 99,95%, τότε αυτό το ποσοστό διαθεσιμότητας θα πολλαπλασιαστεί με την κανονική χρέωση για τον συγκεκριμένο μήνα (για παράδειγμα, αν εντός ενός μήνα το προϊόν παρουσιάσει 80% διαθεσιμότητα, ο χρήστης θα πληρώσει το 80% της μηνιαίας συνδρομής). Επιπλέον, πέρα από τη διαθεσιμότητα, παρέχει και την εγγύηση πως το ενδιάμεσο λογισμικό (middleware) cipherDB, το οποίο αποτελεί μέρος του προϊόντος, έχει καθυστέρηση περίπου 1ms ανά εγγραφή δεδομένων προς κρυπτογράφηση. Νικητήριο προϊόν είναι το Crypteron Data Security, το οποίο προσφέρει 99.95% διαθεσιμότητα με σύστημα ποινών καθώς και εγγύηση που αφορά τη χρονική διάρκεια κρυπτογράφησης ανά εγγραφή δεδομένων του προϊόντος.

Τα αποτελέσματα δεν είναι ικανοποιητικά καθώς βρέθηκαν πληροφορίες μόνο στο ⅓ των προϊόντων. Κανένα προϊόν δεν προσφέρει αξιόλογες εγγυήσεις με εξαίρεση το Crypteron data security. Η κρυπτογράφηση είναι μία διαδικασία που θα πρέπει να πραγματοποιείται διαρκώς. Βέβαια το αν η διαθεσιμότητα είναι επαρκής ή όχι μπορεί να εξαρτάται από την περίπτωση και τις ανάγκες της κάθε επιχείρησης. Άρα, λοιπόν, οποιαδήποτε εγγύηση μικρότερη του 99.95% (η μέγιστη στα προϊόντα που εξετάστηκαν) δεν θεωρείται επαρκής για μια επιχείρηση με υψηλές απαιτήσεις.

Είδος προσφερόμενης προστασίας: Η κύρια λειτουργικότητα σε όλα τα προϊόντα (100%) είναι προληπτική (preventive). Αυτό είναι αναμενόμενο και οφείλεται στη φύση των προϊόντων κρυπτογράφησης. Η κρυπτογράφηση των αρχείων είναι μια διαδικασία που πραγματοποιείται προληπτικά ώστε να ενισχυθεί η ασφάλεια ενός πληροφοριακού συστήματος ανεξάρτητα με το αν θα συμβεί κάποια απειλή στο μέλλον ή όχι. Επιπλέον, η κρυπτογράφηση δεν έχει τη δυνατότητα να εντοπίσει κάποιο ύποπτο συμβάν συνεπώς δε μπορεί να προσφέρει ανιχνευτική προστασία. Υπάρχει 1 προϊόν (6.6%), το DSaaS_Masking_Tokenization_Encryption_API που υλοποιεί μηχανισμούς της κατηγορίας πρόληψης απώλειας δεδομένων. Έτσι, λοιπόν, παρέχει επιπλέον ανιχνευτική προστασία (detective). Το προϊόν αυτό είναι και το νικητήριο.
Τα αποτελέσματα δεν είναι καθόλου ικανοποιητικά καθώς μόνο ένα προϊόν προσφέρει δύο είδη προστασίας.

Ιδιότητες ασφάλειας: Όλα τα προϊόντα (100%) εξασφαλίζουν την εμπιστευτικότητα. Αυτό συμβαίνει λόγω της φύσης των προϊόντων, τα οποία μετατρέπουν αρχεία σε μη αναγνώσιμη/μη αντιληπτή μορφή. Έτσι, λοιπόν, ακόμη και αν ένας τρίτος αποκτήσει πρόσβαση σε τέτοια αρχεία, αυτά δεν θα βρίσκονται σε αναγνώσιμη μορφή εφόσον το περιεχόμενό τους θα είναι κρυπτογραφημένο. Συνεπώς δεν θα είναι σε θέση να αναγνώσει/να αξιοποιήσει κάποια πληροφορία στην οποία υπό κανονικές συνθήκες δεν θα έπρεπε να έχει πρόσβαση. Επιπλέον, 2 προϊόντα (13.3%) εξασφαλίζουν τη διαθεσιμότητα. Το ένα προϊόν υλοποιεί μηχανισμούς της κατηγορίας πρόληψης απώλειας δεδομένων. Το άλλο προϊόν υλοποιεί μηχανισμούς της κατηγορίας επιχειρησιακής συνέχειας και αποκατάστασης καταστροφών. Κοινό στοιχείο αυτών των δύο κατηγοριών είναι ότι εξασφαλίζουν τη διαθεσιμότητα.
Τα αποτελέσματα δεν είναι ικανοποιητικά καθώς μόνο δύο προϊόντα καλύπτουν πάνω από μία ιδιότητα ασφαλείας. Τα προϊόντα αυτά, τα DSaaS_Masking_Tokenization_Encryption_API και Nordlocker, είναι και τα νικητήρια.

Προστατευόμενα αντικείμενα: Όλα τα προϊόντα (100%) προστατεύουν τα δεδομένα λόγω της φύσης των προϊόντων της κρυπτογράφησης. Πιο συγκεκριμένα, 1 προϊόν (6.6%) προστατεύει αρχεία, ροές δεδομένων και γενικά αντικείμενα. 1 προϊόν (6.6%) προστατεύει ευαίσθητα αρχεία εφαρμογών, 1 προϊόν (6.6%) προστατεύει το φόρτο εργασίας, δηλαδή τις εικονικές μηχανές, 1 προϊόν (6.6%) προστατεύει βάσεις δεδομένων και τέλος 1 προϊόν (6.6%) προστατεύει σκληρούς δίσκους. Τα αποτελέσματα είναι ικανοποιητικά και αναμενόμενα για την τρέχουσα κατηγορία.
Ενώ όλα τα προϊόντα προστατεύουν δεδομένα ανεξάρτητα από τη μορφή την οποία έχουν ή το υλικό στο οποίο βρίσκονται ο βαθμός προστασίας αλλάζει. Η προστασία των σκληρών δίσκων είναι πιο ισχυρή από την προστασία φόρτου εργασίας. Με τη σειρά της η προστασία φόρτου εργασίας είναι ισχυρότερη από την προστασία απλών αρχείων. Τέλος, η προστασία αρχείων είναι πιο ισχυρή από την προστασία βάσεων δεδομένων και προστασία αρχείων εφαρμογών.
Επομέμως, αν επιθεωρήσουμε τον αριθμό αντικειμένων που προστατεύονται, 1 προϊόν (6.6%) (Crypteron Data Security) προστατεύει τέσσερα είδη αντικειμένων (δεδομένα, αρχεία, ροές αρχείων,

γενικά αντικείμενα) ενώ όλα τα υπόλοιπα προϊόντα από ένα είδος. Επιπλέον, αν ελέγξουμε τον βαθμό προστασίας, το νικητήριο προϊόν είναι το Sophos Central Device Encryption, το οποίο προστατεύει τους σκληρούς δίσκους, δηλαδή παρέχει τον υψηλότερο βαθμό προστασίας. Συνεπώς, τα νικητήρια προϊόντα με βάση τις 2 προαναφερόμενες διαστάσεις είναι το Crypteron Data Security και το Sophos Central Device Encryption

Αντιμετωπιζόμενες απειλές: Όλα τα προϊόντα (100%) παρέχουν προστασία από μη εξουσιοδοτημένη πρόσβαση με την συνθήκη πως δεν χρησιμοποιούνται αδύναμα κλειδιά κρυπτογράφησης. 1 προϊόν (6.6%) προστατεύει από κλοπή διαπιστευτηρίων, πειρατεία λογαριασμών, μη ασφαλή API, κακόβουλους εσωτερικούς χρήστες ή αναγκαστική αποκάλυψη δεδομένων σε χρήση. 1 προϊόν (6.6%) προστατεύει από λυτρισμικό. 1 προϊόν (6.6%) προστατεύει από κακόβουλο κώδικα και απώλεια δεδομένων. 1 προϊόν (6.6%) προστατεύει από παραβιάσεις δεδομένων. 1 προϊόν (6.6%) προστατεύει από επιθέσεις ωμής βίας. Τέλος, 1 προϊόν (6.6%) προστατεύει από απειλές που δημιουργούνται από χακερς.
Αν εξετάσουμε τον αριθμό απειλών που αντιμετωπίζονται ανά προϊόν, συμπεριλαμβανομένης της μη εξουσιοδοτημένης πρόσβασης, υπάρχει 1 προϊόν (6.6%) το οποίο καλύπτει έξι είδη απειλών, 4 προϊόντα (26.6%) που καλύπτουν δύο είδη απειλών, 1 προϊόν (6.6%) που καλύπτει τρία είδη απειλών και 9 προϊόντα (60%) που καλύπτουν ένα είδος απειλών.
Τα αποτελέσματα δεν είναι ιδιαίτερα ικανοποιητικά καθώς σχεδόν μόνο το ⅓ των προϊόντων καλύπτει παραπάνω από ένα είδος απειλών. Νικητήριο προϊόν είναι το DSaaS_Masking_Tokenization_Encryption_API, το οποίο καλύπτει έξι είδη απειλών.

Περιορισμοί χρήσης: Βρέθηκαν περιορισμοί σε 4 προϊόντα (26,6%). Σε 3 προϊόντα (20%) υπάρχουν περιορισμοί σχετικά με τον αποθηκευτικό χώρο. Πιο συγκεκριμένα, σε 1 προϊόν σε κάθε χρήστη αντιστοιχεί αποθηκευτικός χώρος 100gb, 1 προϊόν έχει ως περιορισμό 1TB αποθηκευτικό χώρο ανά χρήστη ανά μήνα και 1 προϊόν έχει μέγιστο αποθηκευτικό χώρο 2TB.
Ένα άλλο είδος περιορισμού που βρέθηκε σε 1 προϊόν (6.6%) είναι ως προς τον αριθμό χρηστών, όπου στη μία από τις δύο εκδόσεις του υποστηρίζονται έως 25 χρήστες. Σε 1 προϊόν (6.6%) βρέθηκε περιορισμός σχετικά με το μέγιστο μέγεθος αρχείου προς κρυπτογράφηση το οποίο είναι 5GB. Τέλος, σε 1 προϊόν (6.6%) βρέθηκε ο περιορισμός πως μπορεί να δεχτεί έως 400.000 αιτήματα (requests) ανά μήνα.
Σχετικά με το πλήθος περιορισμών 2 προϊόντα (13.3%) έχουν από δύο περιορισμούς και 2 προϊόντα (13.3%) έχουν από έναν περιορισμό.
Οι παραπάνω περιορισμοί θεωρούνται αναμενόμενοι καθώς βρίσκονται στα πλαίσια της φυσιολογικής λειτουργίας των προϊόντων. Δηλαδή ανεξάρτητα από το αν κάποιος περιορισμός είναι δεσμευτικός ή όχι θα μπορούσε να υφίσταται σε αυτού του είδους τα προϊόντα.

Δοκιμαστικές εκδόσεις: 6 προϊόντα (40%) δεν παρέχουν δωρεάν δοκιμαστική έκδοση, 1 προϊόν (6.6%) παρέχει δωρεάν δοκιμαστική έκδοση χωρίς να αναφέρει την χρονική διάρκεια και 6 προϊόντα (40%)

παρέχουν δωρεάν δοκιμαστική έκδοση 30 ημερών. 4 προϊόντα (20%) παρέχουν μόνιμη δωρεάν έκδοση με περιορισμένες δυνατότητες (1 προϊόν με 5gb ανά μήνα αποθηκευτικό χώρο, 1 προϊόν με 1500 αιτήματα ανά μήνα και 1 προϊόν με 3gb αποθηκευτικό χώρο).
Τα αποτελέσματα είναι μεν ικανοποιητικά καθώς τα ⅔ των προϊόντων διαθέτουν κάποιο είδος δοκιμαστικής έκδοσης αλλά χρήζουν βελτίωσης. Ιδανικά όλα τα προϊόντα θα έπρεπε να διαθέτουν κάποιο είδος δωρεάν δοκιμαστικής έκδοσης ακόμα και αν ήταν μικρής χρονικής διάρκειας.

Τρόπος χρήσης: 3 προϊόντα (20%) υποστηρίζουν και τα τρία είδη διεπαφών. 6 προϊόντα (40%) υποστηρίζουν διεπαφή προγραμματισμού εφαρμογών μεταφοράς αναπαραστατικής κατάστασης και γραφικό περιβάλλον εργασίας μέσω διαδικτύου, 1 προϊόν (6.6%) διεπαφή προγραμματισμού εφαρμογών μεταφοράς αναπαραστατικής κατάστασης και χρήση γραμμής εντολών, 1 προϊόν (6.6%) υποστηρίζει γραφικό περιβάλλον εργασίας μέσω διαδικτύου και χρήση γραμμής εντολών, 4 προϊόντα (33.3%) υποστηρίζουν μόνο γραφικό περιβάλλον εργασίας μέσω διαδικτύου.
Αν δούμε τις τιμές αποτίμησης μεμονωμένα, η διεπαφή προγραμματισμού εφαρμογών μεταφοράς αναπαραστατικής κατάστασης εμφανίζεται σε 9 προϊόντα (60%). Το γραφικό περιβάλλον εργασίας μέσω διαδικτύου εμφανίζονται σε 14 προϊόντα (93.3%) και η γραμμή εντολών εμφανίζεται σε 5 προϊόντα (33.3%). Τη μεγαλύτερη συχνότητα εμφάνισης έχει το γραφικό περιβάλλον εργασίας μέσω διαδικτύου. Αυτό συμβαίνει γιατί τα περισσότερα προϊόντα διατίθενται σαν λογισμικό και ενδεχομένως να απαιτείται εκτεταμένη διαμόρφωση για την εφαρμογή της κρυπτογράφησης, οπότε η χρήση γραφικής διεπαφής είναι ενδεδειγμένη σε αυτή την περίπτωση.
Τα αποτελέσματα θεωρούνται ικανοποιητικά καθώς πάνω από τα ⅔ των προϊόντων υποστηρίζουν δύο ή τρεις τεχνολογίες.

Αγορές: 11 προϊόντα (73.3%) εντοπίστηκαν στις αγορές. Ειδικότερα, 3 προϊόντα (20%) εντοπίστηκαν στο Amazon web services και στο Microsoft Azure, 1 προϊόν (6.6%) εντοπίστηκε και στις τρεις, 3 προϊόντα (20%) εντοπίστηκαν στο Microsoft Azure, 4 προϊόντα (26.6%) εντοπίστηκαν στο Amazon web services και 4 προϊόντα (26.6%) εντοπίστηκαν στο διαδίκτυο και όχι σε κάποια αγορά. Συνολικά, 8 προϊόντα (53.3%) εντοπίστηκαν στο Amazon web services, 7 προϊόντα (46.6%) στο Microsoft Azure και 1 προϊόν (6.6%) στο Google cloud platform.
Τα αποτελέσματά δεν είναι αρκετά ικανοποιητικά διότι μόνο 4 προϊόντα εντοπίστηκαν σε πάνω από δύο αγορές και 4 προϊόντα εντοπίστηκαν εκτός αγορών. Νικητήριο προϊόν είναι το Fortanix Data Security Manager, το οποίο εντοπίστηκε σε όλες τις αγορές.

Επίπεδο/είδος υποστήριξης: 15 προϊόντα (100%) προσφέρουν υποστήριξη μέσω email, 12 προϊόντα (80%) μέσω τηλεφώνου, 5 προϊόντα (33.3%) μέσω δελτίων (tickets) και 3 προϊόντα (20%) μέσω μηνυμάτων (chat). 3 προϊόντα (20%) διαθέτουν υποστήριξη κοινοτήτων χριστών (κοινότητα, φόρουμ, blog), 8 προϊόντα (53.3%) διαθέτουν τεκμηρίωση (documentation), 2 προϊόντα (13.3%) διαθέτουν πύλη

υποστήριξης, 14 προϊόντα (93.3%) διαθέτουν υποστηρικτικό υλικό (έγγραφα με πληροφορίες, βίντεο, FAQ). 6 προϊόντα (40%) διαθέτουν βάση γνώσης (knowledge base). 2 προϊόντα (13.3%) διαθέτουν ενημέρωση για νέα προϊόντα και 1 προϊόν (6.6%) διαθέτει εκπαιδευτικό υλικό. 2 προϊόντα (13.3 %) διαθέτουν λογαριασμούς σε μέσα κοινωνικής δικτύωσης (twitter, slack) και 3 προϊόντα (20%) διαθέτουν κέντρο βοήθειας.

Για την ημερολογιακή/χρονική διάρκεια κατά την οποία παρέχεται υποστήριξη, υπάρχουν 3 προϊόντα (20%) τα οποία προσφέρουν υποστήριξη 24/7 και δύο προϊόντα (13.3%) τα οποία προσφέρουν δύο πακέτα υποστήριξης, 10/5 και 24/7.

Τα αποτελέσματα κρίνονται μη ικανοποιητικά διότι μόνο δύο προϊόντα προσφέρουν διαφορετικά πακέτα υποστήριξης και μόνο το ⅓ των προϊόντων προσφέρει υποστήριξη 24/7. Νικητήρια προϊόντα για αυτή την κατηγορία είναι το Bloombase storasafe και το Fabasoft Secomo, τα οποία παρέχουν διαφορετικά πακέτα υποστήριξης και υποστήριξη 24/7.

Νικητήριο προϊόν για ολόκληρη την κατηγορία είναι το DSaaS_Masking_Tokenization_Encryption_API, το οποίο εμφανίζεται ως νικητήριο 4 φορές.

5.2.7 Ασφάλεια ηλεκτρονικού ταχυδρομείου (Email Security)

Για αυτή την ενότητα βρέθηκαν 15 προϊόντα με επαρκή τεκμηρίωση, τα οποία αποτιμήθηκαν. Τα αποτελέσματα αποτίμησης εμφανίζονται στον Πίνακα 7 του παραρτήματος. Παρακάτω παρέχουμε μια στατιστική ανάλυση των αποτελεσμάτων αυτών ανά κριτήριο.

Τρόπος παράδοσης: 9 προϊόντα (60%) προσφέρονται σαν λογισμικό, 5 προϊόντα (26.6%) προσφέρονται σαν υποδομή και 1 προϊόν (6.6%) προσφέρεται σαν υποδομή και σαν λογισμικό. Τα περισσότερα προϊόντα προσφέρονται σαν λογισμικό λόγω των πλεονεκτημάτων που προσφέρει αυτός ο τρόπος συγκριτικά με τους άλλους τρόπους παράδοσης. Βέβαια, όσο περισσότεροι τρόποι παράδοσης υποστηρίζονται τόσο το καλύτερο για τον υποψήφιο αγοραστή. Τα αποτελέσματα δεν είναι ιδιαίτερα ικανοποιητικά διότι μόνο 1 προϊόν υποστηρίζει δύο τρόπους παράδοσης. Το προϊόν αυτό είναι το Forcepoint Email Security που είναι και το νικητήριο.

Μοντέλο διάταξης: 13 προϊόντα (86.6%) υποστηρίζουν δημόσιο νέφος και 2 προϊόντα (13.3%) υποστηρίζουν δημόσιο ή ιδιωτικό νέφος. Το γεγονός πως μόνο δύο προϊόντα υποστηρίζουν παραπάνω από ένα είδος νέφους δεν είναι καθόλου ικανοποιητικό. Βέβαια, το αποτέλεσμα αυτό είναι αναμενόμενο καθώς τα περισσότερα προϊόντα υποστηρίζουν τρόπο παράδοσης SaaS όπου το μοντέλο διάταξης είναι λογικά το δημόσιο νέφος. Νικητήρια προϊόντα είναι τα Libraesva Email Security Gateway και Clearswift Secure Email Gateway, τα οποία υποστηρίζουν δημόσιο ή ιδιωτικό νέφος.

Κατηγορία ασφάλειας: 2 προϊόντα (13.3%) καλύπτουν επιπλέον την κατηγορία της επιχειρησιακής συνέχειας και αποκατάστασης καταστροφών. 6 προϊόντα (40%) καλύπτουν επιπρόσθετα την κατηγορία

της διαχείρισης ταυτότητας και πρόσβασης και 7 προϊόντα (46.6%) καλύπτουν επιπρόσθετα την κατηγορία της κρυπτογράφησης.
Αν δούμε τον αριθμό επιπλέον κατηγοριών που καλύπτονται ανά προϊόν, 3 προϊόντα (20%) καλύπτουν μία επιπλέον κατηγορία και 6 προϊόντα (40%) καλύπτουν δύο επιπλέον κατηγορίες.
Τα αποτελέσματα είναι αρκετά ικανοποιητικά καθώς σχεδόν τα ⅔ των προϊόντων καλύπτουν παραπάνω από μία έξτρα κατηγορία. Νικητήρια προϊόντα είναι τα προϊόντα εκείνα τα οποία καλύπτουν δύο επιπλέον κατηγορίες (δείτε πίνακα αποτίμησης).

Μοντέλο κόστους: Σχετικά με την τιμολόγηση για 4 προϊόντα (26.6%) δεν βρέθηκαν πληροφορίες. 2 προϊόντα (13.3%) παρέχουν πληροφορίες τιμολόγησης μόνο με επικοινωνία με την εταιρία. 1 προϊόν (6.6%) διατίθεται με άδεια χρήσης bring your own license (BYOL) στο Microsoft Azure. 6 προϊόντα (40%) τιμολογούνται με βάση τον αριθμό χρηστών και σε ένα προϊόν υπάρχει ελάχιστη χρέωση που αντιστοιχεί σε 10 χρήστες. 2 προϊόντα (13.3%) τιμολογούνται με βάση το φόρτο εργασίας. 1 προϊόν (6.6%) τιμολογείται με βάση τα βασικά χαρακτηριστικά.
Σχετικά με την ύπαρξη πακέτων, υπάρχει μόνο 1 προϊόν (GreatHorn Cloud Email Security) (6.6%), το οποίο παρέχει τρία διαφορετικά πακέτα τιμολόγησης.
Τέλος, σχετικά με τη χρονική συνιστώσα των πληρωμών, 1 προϊόν (6.6%) έχει μηνιαία χρέωση και 4 προϊόντα (26,6%) έχουν συμβόλαια με διάρκεια μεγαλύτερη ή ίση του ενός μήνα. Πιο συγκεκριμένα, 1 προϊόν (6.6%) έχει ετήσιο ή διετές συμβόλαιο, 2 προϊόντα (13.3%) έχουν ετήσιο συμβόλαιο, και 1 προϊόν (6.6%) συμβόλαιο διάρκειας 1,12,24 ή 36 μηνών.
Τα αποτελέσματα δεν είναι ικανοποιητικά καθώς σχεδόν στο ⅓ των προϊόντων δεν βρέθηκαν πληροφορίες, μόνο ένα προϊόν προσφέρει διαφορετικά πακέτα πληρωμής και μόνο δύο προϊόντα προσφέρουν επιλογές σχετικά με τη χρονική συνιστώσα. Νικητήρια προϊόντα είναι τα GreatHorn Cloud Email Security με τα τρία πακέτα τιμολόγησης και Advanced Threat Protection for Email and Collaboration με τα τέσσερα χρονικά διαστήματα χρέωσης.

Μηχανισμοί ασφάλειας: Όλα τα προϊόντα (100%) υποστηρίζουν βασική και έξτρα λειτουργικότητα. Το προϊόν που διαθέτει τη λιγότερη λειτουργικότητα είναι το Vircom modusGate Email Security Gateway, το οποίο καλύπτει 5 λειτουργικότητες, οι οποίες αφορούν μόνο την τρέχουσα κατηγορία. Αντίθετα, τα προϊόντα που διαθέτουν τη περισσότερη λειτουργικότητα είναι τα Clearswift Secure Email Gateway και Barracuda Email Security Gateway, τα οποία προσφέρουν 12 λειτουργικότητες, οι οποίες αφορούν και την τρέχουσα και επιπλέον κατηγορίες (π.χ. υπάρχει η λειτουργικότητα της κρυπτογράφησης). Τα δύο αυτά προϊόντα είναι και τα νικητήρια.
Τα αποτελέσματα είναι ικανοποιητικά καθώς όλα τα προϊόντα καλύπτουν έξτρα λειτουργικότητα, κατι που εν μέρη ήταν αναμενόμενο καθώς αρκετά προϊόντα καλύπτουν επιπλέον κατηγορίες ασφάλειας, όπως αναφέρθηκε παραπάνω.

Μη λειτουργικές εγγυήσεις: 3 προϊόντα (20%) διαθέτουν εγγύηση διαθεσιμότητας (99.9%, 99.999% και 99.99%) με τα δύο πρώτα να διαθέτουν και συστήματα ποινών. Το προϊόν με 99.9% εγγύηση διαθεσιμότητας εφαρμόζει το παρακάτω σύστημα ποινών: για 99.8% - 97% επιστροφή 5% της μηνιαίας συνδρομής, για 96.9% - 93.0% επιστροφή 10% της μηνιαίας συνδρομής, για 92.9% - 90.0% επιστροφή 20% της μηνιαίας συνδρομής, για <90% επιστροφή 30% της μηνιαίας συνδρομής. Το προϊόν με 99.999% εγγύηση διαθεσιμότητας εφαρμόζει το παρακάτω σύστημα ποινών: για περισσότερο από 0,001% μη διαθεσιμότητα οποιουδήποτε ημερολογιακού μήνα, ο πελάτης δικαιούται πίστωση υπηρεσίας ίση με 1 ημέρα για κάθε περίοδο 2 ωρών μη διαθεσιμότητας υπηρεσίας, με μέγιστη πίστωση 5 ημερών ανά 1 μήνα.

Επίσης, 3 προϊόντα (20%) διαθέτουν εγγύηση περιορισμού των μηνυμάτων ηλεκτρονικού ψαρέματος (99.2%, 99.9%, πάνω από 99.9%). 7 προϊόντα (43.3%) διαθέτουν εγγύηση περιορισμού των ανεπιθύμητων μηνυμάτων (99.91%, 99.9%, 95% με 0.01% ψευδώς θετικά, 99.9%, 99.9% με 0% ψευδώς θετικά, 99,93%, 99.78%).

Ακόμη, 1 προϊόν διαθέτει 100% ποσοστό σάρωσης αρχείων, 99.99% διαθεσιμότητα παράδοσης μηνυμάτων ηλεκτρονικού ταχυδρομείου, 99.99% διαθεσιμότητα προστασίας περιεχομένου, 99.99% διαθεσιμότητα σάρωσης μηνυμάτων και ποσοστό εντοπισμού ψευδώς θετικών < 0.0001%. Οι εγγυήσεις του παραπάνω προϊόντος διαθέτουν η κάθε μία το δικό της της σύστημα ποινών.

Επιπρόσθετα, 1 προϊόν (6.6%) διαθέτει 100% παραμονή δεδομένων στο περιβάλλον του χρήστη, εξάλειψη του 100% των εξαγορών λογαριασμού, μείωση της αλληλεπίδρασης των χρηστών με ύποπτα email κατά 60%. 1 προϊόν (6.6%) διαθέτει ποσοστό εντοπισμού κακόβουλου λογισμικού 99,91% και μπλοκαρίσματος 100%. 1 προϊόν (6.6%) διαθέτει εγγύηση εξάλειψη του 99,9% των ιών. 1 προϊόν (6.6%) διαθέτει 99.9% ανίχνευση κακόβουλων μηνυμάτων ηλεκτρονικού ταχυδρομείου, 94% συνολικό ποσοστό ανίχνευσης απειλής, 100% ποσοστό ανίχνευσης Wildlist. 1 προϊόν (6.6%) διαθέτει αφαίρεση του 97% των επιθέσεων από όλα τα επηρεαζόμενα γραμματοκιβώτια (mailboxes).

Αν δούμε τον αριθμό εγγυήσεων ανά προϊόν, 8 προϊόντα (53.3%) διαθέτουν μία εγγύηση, 2 προϊόντα (13.3%) διαθέτουν τρεις εγγυήσεις, 2 προϊόντα (13.3%) διαθέτουν δύο εγγυήσεις, 1 προϊόν (6.6%) διαθέτει τέσσερις εγγυήσεις και 1 προϊόν (6.6%) διαθέτει πέντε εγγυήσεις.

Τα αποτελέσματα είναι πολύ ικανοποιητικά καθώς πάνω από το ⅓ των προϊόντων διαθέτουν δύο ή περισσότερες εγγυήσεις. Νικητήριο είναι το προϊόν το οποίο διαθέτει 5 διαφορετικές εγγυήσεις με συστήματα ποινών, το Advanced Threat Protection for Email and Collaboration

Είδος προσφερόμενης προστασίας: Η κύρια λειτουργικότητα σε 13 προϊόντα (86.6%) είναι προληπτική, ανιχνευτική και αντιδραστική. Σε 1 προϊόν (6.6%) είναι προληπτική και σε 1 προϊόν (6.6%) είναι προληπτική και αντιδραστική. Το γεγονός πως σχεδόν όλα τα προϊόντα παρέχουν και τα τρία είδη προστασίας οφείλεται στους μηχανισμούς τους οποίους υλοποιούν τα προϊόντα αυτά. Δηλαδή είναι τόσες πολλές και διαφορετικές οι λειτουργίες που επιτελούν αυτά τα προϊόντα που κάθε λειτουργία μπορεί να προσφέρει και διαφορετικό είδος προστασίας. Έτσι προκύπτει ένα προϊόν το οποίο προσφέρει και τα τρία είδη προστασίας. Πιο συγκεκριμένα, ένα προϊόν προστασίας ηλεκτρονικού ταχυδρομείου μπορεί, για

παράδειγμα, να προσφέρει προστασία από ανεπιθύμητα μηνύματα. Τα μηνύματα ελέγχονται πριν φτάσουν στον παραλήπτη άρα η προστασία είναι προληπτική. Επιπλέον, το ίδιο προϊόν μπορεί να προσφέρει προστασία από κακόβουλο λογισμικό σαρώνοντας τα αρχεία άρα προσφέρει ανιχνευτική προστασία λόγω της σάρωσης. Τέλος, το ίδιο προϊόν μπορεί να μπλοκάρει μία απειλή που εντοπίστηκε. Εφόσον η απειλή έχει ήδη εισέλθει στο σύστημα μας και το προϊόν τερματίζει τη λειτουργία της πρόκειται για αντιδραστική προστασία.
Τα παραπάνω αποτελέσματα είναι πάρα πολύ ικανοποιητικά καθώς όλα σχεδόν τα προϊόντα καλύπτουν και τα τρία είδη προστασίας.

Ιδιότητες ασφάλειας: Σε 6 προϊόντα (40%) δε βρέθηκε κάποια πληροφορία. 8 προϊόντα (53.3%) εξασφαλίζουν τη διαθεσιμότητα και 7 προϊόντα (46.6%) εξασφαλίζουν την εμπιστευτικότητα. Τα προϊόντα που υλοποιούν μηχανισμούς της κατηγορίας πρόληψης απώλειας δεδομένων και της κατηγορίας επιχειρησιακής συνέχειας και αποκατάστασης καταστροφών εξασφαλίζουν τη διαθεσιμότητα. Τα προϊόντα που υλοποιούν μηχανισμούς της κατηγορίας κρυπτογράφησης εξασφαλίζουν την εμπιστευτικότητα.
Αν δούμε τον αριθμό ιδιοτήτων ανά προϊόν, 6 προϊόντα (40%) καλύπτουν δύο ιδιότητες και 3 προϊόντα (20%) καλύπτουν μία ιδιότητα.
Τα αποτελέσματα είναι οριακά ικανοποιητικά καθώς σχεδόν τα ⅔ των προϊόντων καλύπτουν μία ή δύο ιδιότητες ασφαλείας. Νικητήρια είναι τα προϊόντα τα οποία καλύπτουν δύο κατηγορίες (δείτε πίνακα αποτίμησης)

Προστατευόμενα αντικείμενα: Όλα τα προϊόντα (100%) προστατεύουν τόσο την υπηρεσία email όσο και τους πελάτες της στον οργανισμό, κάτι το οποίο είναι αναμενόμενο λόγω της φύσης των προϊόντων. Επιπλέον, υπάρχει ένα προϊόν (6.6%) το οποίο προστατεύει υπηρεσίες κοινής χρήσης αρχείων και εφαρμογές συνεργασίας. Το προϊόν αυτό, το Harmony Email & Collaboration, είναι και το νικητήριο. Τα αποτελέσματα είναι ικανοποιητικά όπως ήταν αναμενόμενο για την τρέχουσα κατηγορία.

Αντιμετωπιζόμενες απειλές: 13 προϊόντα (86.6%) αντιμετωπίζουν επιθέσεις κοινωνικής μηχανικής και πιο συγκεκριμένα τα 11 από αυτά (73.3%) αντιμετωπίζουν το ηλεκτρονικό ψάρεμα (συμπεριλαμβανομένου του στοχευμένου ψαρέματος (spearphising), ψαρέματος διαπιστευτηρίων, φαλαινοθηριας (whaling), νέων επιθέσεων (zero day), πλευρικού ψαρέματος). 7 προϊόντα (46.6%) αντιμετωπίζουν την παραβίαση επιχειρηματικού ηλεκτρονικού ταχυδρομείου (business email compromise). 8 προϊόντα (53.3%) αντιμετωπίζουν την ανεπιθύμητη αλληλογραφία. 8 προϊόντα (53.3%) αντιμετωπίζουν το κακόβουλο λογισμικό. 6 προϊόντα (40%) αντιμετωπίζουν κακόβουλα συνημμένα και URLs. 5 προϊόντα (33.3%) αντιμετωπίζουν τους ιούς. 6 προϊόντα (40%) αντιμετωπίζουν το λυτρισμικό. 6 προϊόντα (40%) αντιμετωπίζουν την πλαστογράφηση/πλαστοπροσωπία (συμπεριλαμβανομένης της πλαστογράφησης τομέα (domain), email και μηνυμάτων). 4 προϊόντα (26.6%) αντιμετωπίζουν τις απειλές μηδενικής ημέρας. 3 προϊόντα (20%) αντιμετωπίζουν την κατάληψη λογαριασμών (account takeover). 2 προϊόντα (13.3%) αντιμετωπίζουν την κλοπή διαπιστευτηρίων. 3 προϊόντα (20%) αντιμετωπίζουν τις απάτες και

τους εκβιασμούς. 1 προϊόν (6.6%) αντιμετωπίζει εκμεταλλεύσεις ηλεκτρονικού ταχυδρομείου & επιθέσεις botnet, ανεπιθύμητο περιεχόμενο, και μηνύματα ηλεκτρονικού ταχυδρομείου που προέρχονται από μολυσμένες IP ή/και τομείς. 1 προϊόν (6.6%) αντιμετωπίζει προηγμένες μόνιμες απειλές. 1 προϊόν (6.6%) αντιμετωπίζει το κατασκοπευτικό λογισμικό και τις επιθέσεις άρνησης υπηρεσίας. 1 προϊόν (6.6%) αντιμετωπίζει απειλές βασισμένες σε αρχεία. 1 προϊόν (6.6%) αντιμετωπίζει τη διαρροή δεδομένων και την κατάληψη λογαριασμών. 1 προϊόν (6.6%) αντιμετωπίζει εσωτερικές και εξωτερικές απειλες.1 προϊόν (6.6%) αντιμετωπίζει επιθέσεις υπεκφυγής (evasion). 1 προϊόν (6.6%) αντιμετωπίζει την παρακολούθηση εσωτερικού email.

Αν δούμε τις απειλές που αντιμετωπίζονται ανά προϊόν 3 προϊόντα (20%) αντιμετωπίζουν εννέα απειλές, 3 προϊόντα (20%) αντιμετωπίζουν έξι απειλές, 2 προϊόντα (13.3%) αντιμετωπίζουν οχτώ απειλές, 2 προϊόντα (13.3%) αντιμετωπίζουν 7 απειλές, 2 προϊόντα (13.3%) αντιμετωπίζουν 10 απειλές. Από 1 προϊόν (6.6%) αντιμετωπίζει 3, 4, και 5 απειλές.

Τα αποτελέσματα είναι πάρα πολύ ικανοποιητικά καθώς 12 από τα 15 προϊόντα αντιμετωπίζουν έξι ή περισσότερες απειλές. Νικητήρια είναι τα δύο προϊόντα που αντιμετωπίζουν από 10 απειλές, τα Vircom modusGate Email Security Gateway και FortiMail Secure Email Gateway

Περιορισμοί χρήσης: Βρέθηκαν πληροφορίες μόνο σε 6 προϊόντα (40%). 2 προϊόντα παρέχουν αρχειοθέτηση των μηνυμάτων ηλεκτρονικού ταχυδρομείου έως 10 έτη. 1 προϊόν (6.6%) έχει ανώτατο όριο τους 30.000 χρήστες. 1 προϊόν (6.6%) έχει ποσοστό ανίχνευσης ανεπιθύμητης αλληλογραφίας έως 99.99%, 1 προϊόν (6.6%) αποτρέπει έως και το 75% των παραβιάσεων επαγγελματικών email ή ηλεκτρονικού ψαρέματος που χρησιμοποιούν πλαστογράφηση τομέα (domain) και ηλεκτρονικού ταχυδρομείου. Τέλος, 1 προϊόν (6.6%) έχει ελάχιστο αριθμό χρηστών τους 10 χρήστες. Τα αποτελέσματα είναι ικανοποιητικά καθώς όλοι οι περιορισμοί βρίσκονται μέσα στα πλαίσια της φυσιολογικής λειτουργίας των προϊόντων.

Δοκιμαστικές εκδόσεις: 3 προϊόντα (20%) δεν παρέχουν δωρεάν δοκιμαστική έκδοση, 3 προϊόντα (20%) παρέχουν δωρεάν δοκιμαστική έκδοση χωρίς να αναφέρουν την χρονική διάρκεια, 8 προϊόντα (53.3%) παρέχουν δωρεάν δοκιμαστική έκδοση 30 ημερών, 1 προϊόν (6.6%) παρέχει δωρεάν δοκιμαστική έκδοση 90 ημερών.

Τα αποτελέσματα είναι ικανοποιητικά καθώς τα περισσότερα προϊόντα διαθέτουν δωρεάν δοκιμαστική έκδοσης και στα ⅔ η διάρκεια είναι μεγαλύτερη ή ίση των 30 ημερών. Νικητήριο είναι το προϊόν με τη μεγαλύτερη σε διάρκεια δοκιμαστική έκδοση, το Armorblox Email Protection.

Τρόπος χρήσης: 5 προϊόντα (33.3%) υποστηρίζουν διεπαφή προγραμματισμού εφαρμογών μεταφοράς αναπαραστατικής κατάστασης και γραφικό περιβάλλον εργασίας μέσω διαδικτύου. 3 προϊόντα (20%) υποστηρίζουν γραφικό περιβάλλον εργασίας μέσω διαδικτύου και χρήση γραμμής εντολών. 7 προϊόντα (46.6%) υποστηρίζουν μόνο γραφικό περιβάλλον εργασίας μέσω διαδικτύου.

Αν δούμε τις τιμές αποτίμησης μεμονωμένα, η διεπαφή προγραμματισμού εφαρμογών μεταφοράς αναπαραστατικής κατάστασης εμφανίζεται σε 5 προϊόντα (33.3%). Το γραφικό περιβάλλον εργασίας μέσω διαδικτύου εμφανίζεται σε όλα τα προϊόντα (100%) και η γραμμή εντολών εμφανίζεται σε 3 προϊόντα (20%). Παρατηρούμε πως μόνο το γραφικό περιβάλλον εργασίας μέσω διαδικτύου εμφανίζεται σε όλα τα προϊόντα. Αυτό συμβαίνει διότι η πλειοψηφία των προϊόντων διατίθεται σαν λογισμικό και ενδεχομένως να απαιτείται γραφικό περιβάλλον εργασίας για την απαραίτητη ρύθμιση/παραμετροποίηση τους. Μία άλλη περίπτωση κατά την οποία χρειάζεται το γραφικό περιβάλλον είναι η εμφάνιση των μηνυμάτων που μπλοκάρονται και η δυνατότητα του χρήστη να ξεμπλοκάρει εκείνα που θεωρεί πως δεν είναι ανεπιθύμητα.
Τα αποτελέσματα θεωρούνται ικανοποιητικά καθώς σχεδόν τα ⅔ των προϊόντων υποστηρίζουν δύο τεχνολογίες.

Αγορές: 13 προϊόντα (86.6%) εντοπίστηκαν στις αγορές. 2 προϊόντα (13.3%) εντοπίστηκαν στο Amazon web services και στο Microsoft Azure, 1 προϊόν (6.6%) εντοπίστηκε στο Google cloud platform και στο Microsoft Azure, 8 προϊόντα (53.3%) εντοπίστηκαν στο Microsoft Azure, 2 προϊόντα (26.6%) εντοπίστηκαν στο Amazon web services και 2 προϊόντα (26.6%) εντοπίστηκαν στο διαδίκτυο και όχι σε κάποια αγορά. Συνολικά, 11 προϊόντα (73.3%) εντοπίστηκαν στο Microsoft Azure, 4 προϊόντα (26.6%) στο Amazon web services και 1 προϊόν (6.6%) στο Google cloud platform. Τα αποτελέσματά δεν είναι ιδιαίτερα ικανοποιητικά καθώς μόνο 3 προϊόντα εντοπίστηκαν σε δύο αγορές. Τα προϊόντα αυτά (δείτε πίνακα αποτίμησης) είναι και τα νικητήρια.

Επίπεδο/είδος υποστήριξης: Σχετικά με το είδος υποστήριξης, 14 προϊόντα (93,3%) προσφέρουν υποστήριξη μέσω τηλεφώνου και μέσω email, 7 προϊόντα (46.6%) μέσω δελτίων (tickets) και 4 προϊόντα (26.6%) μέσω μηνυμάτων (chat). 6 προϊόντα (40%) διαθέτουν υποστήριξη κοινοτήτων χρηστών (κοινότητα, φόρουμ, blog), 9 προϊόντα (60%) διαθέτουν τεκμηρίωση (documentation), 5 προϊόντα (33.3%) διαθέτουν πύλη υποστήριξης, και 12 προϊόντα (80%) διαθέτουν υποστηρικτικό υλικό (έγγραφα με πληροφορίες, βίντεο, FAQ). 9 προϊόντα (60%) διαθέτουν βάση γνώσης (knowledge base). 4 προϊόντα (26.6%) διαθέτουν ενημερώσεις για νέα προϊόντα και συνδρομές. 2 προϊόντα (13.3%) διαθέτουν εκπαιδευτικό υλικό. 4 προϊόντα (26.6%) διαθέτουν κέντρο βοήθειας, 1 προϊόν (6.6%) διαθέτει λεξικό και 1 προϊόν (6.6%) διαθέτει πρόσβαση σε εργαλεία
Σχετικά με τα πακέτα υποστήριξης, υπάρχουν 3 προϊόντα (20%) που παρέχουν δύο πακέτα, 1 προϊόν (6.6%) το οποίο προσφέρει τρία πακέτα και 1 προϊόν (6.6%) το οποίο προσφέρει τέσσερα πακέτα.
Για την ημερολογιακή/χρονική διάρκεια κατά την οποία παρέχεται υποστήριξη, υπάρχουν 6 προϊόντα (40%) που προσφέρουν υποστήριξη 24/7, 2 προϊόντα (13.3%) τα οποία προσφέρουν υποστήριξη 8.5/5 και 1 προϊόν (6.6%) το οποίο παρέχει υποστήριξη 9/5. Επίσης, υπάρχει 1 προϊόν (6.6%) το οποίο παρέχει υποστήριξη 8/5 έως 24/7, 1 προϊόν (6.6%) από 9/5 έως 24/7 και 1 προϊόν (6.6%) από 10/5 έως 24/7.

Τα αποτελέσματα είναι ικανοποιητικά διότι 6 προϊόντα προσφέρουν υποστήριξη 24/7 και 3 προϊόντα παρέχουν υποστήριξη 24/7 στο πιο "πλούσιο" πακέτο τους. Επιπλέον, το 1/3 των προϊόντων προσφέρει διαφορετικά πακέτα υποστήριξης. Νικητήριο προϊόν είναι το Harmony Email & Collaboration, το οποίο παρέχει 4 πακέτα υποστήριξης καθώς και υποστήριξη 24/7.

Νικητήρια προϊόντα για ολόκληρη την κατηγορία είναι τα Harmony Email & Collaboration και Clearswift Secure Email Gateway, τα οποία εμφανίζονται ως νικητήρια από 3 φορές.

5.2.8 Ασφάλεια δικτύου (Network Security)

Για αυτή την ενότητα βρέθηκαν 15 προϊόντα με επαρκή τεκμηρίωση, τα οποία αποτιμήθηκαν. Τα αποτελέσματα αποτίμησης εμφανίζονται στον Πίνακα 8 του παραρτήματος. Παρακάτω παρέχουμε μια στατιστική ανάλυση των αποτελεσμάτων αυτών ανά κριτήριο.

Τρόπος παράδοσης: 13 προϊόντα (86.6%) προσφέρονται σαν υποδομή και 2 προϊόντα (13.3%) προσφέρονται σαν υποδομή και σαν λογισμικό. Τα περισσότερα προϊόντα προσφέρονται σαν υποδομή διότι η βασικότερη λειτουργία τους είναι το τείχος προστασίας. Το τείχος προστασίας σαν τεχνολογία είναι μία λειτουργικότητα που ενσωματώνεται σε μία συσκευή οπότε είναι πιο λογικό να προσφέρεται με την μορφή μιας ιδεατής υποδομής. Τα αποτελέσματα δεν είναι ιδιαίτερα ικανοποιητικά διότι μόνο 2 προϊόντα υποστηρίζουν δύο τρόπους παράδοσης. Τα προϊόντα αυτά, το Deep Learning-Powered Network Malware Protection και το Trend Micro Cloud One – Network Security, είναι και τα νικητήρια.

Μοντέλο διάταξης: 10 προϊόντα (66.6%) υποστηρίζουν δημόσιο νέφος; 4 προϊόντα (26.6%) υποστηρίζουν δημόσιο ή ιδιωτικό νέφος και ένα προϊόν (6.6%) υποστηρίζει δημόσιο, ιδιωτικό ή υβριδικό νέφος. Το γεγονός πως 5 προϊόντα υποστηρίζουν πάνω από ένα μοντέλο διάταξης οφείλεται στο ότι τα πιο πολλά προϊόντα διατίθενται σαν υποδομή. Όταν ένα προϊόν διατίθεται σαν υποδομή μπορεί να υποστηρίξει και το ιδιωτικό αλλά και το δημόσιο νέφος ανάλογα με την προτίμηση του κάθε αγοραστή. Αντίθετα τα προϊόντα που διατίθενται σαν λογισμικό υποστηρίζουν μόνο ένα μοντέλο διάταξης, το δημόσιο νέφος. Έτσι, λοιπόν, ο χρήστης έχει τη δυνατότητα επιλογής ανάμεσα στα προσφερόμενα μοντέλα διάταξης. Τα αποτελέσματα δεν είναι ιδιαίτερα ικανοποιητικά καθώς, όπως αναφέρθηκε παραπάνω, μόνο το ⅓ των προϊόντων υποστηρίζουν δύο ή περισσότερα μοντέλα διάταξης. Νικητήριο προϊόν είναι το SonicWall NSv (Firewall/Security/VPN/Router), το οποίο υποστηρίζει και τα τρία μοντέλα διάταξης.

Κατηγορία ασφάλειας: 13 προϊόντα (86.6%) καλύπτουν επιπλέον την κατηγορία της διαχείριση εισβολής, 12 προϊόντα (80%) καλύπτουν επιπρόσθετα την κατηγορία της ασφάλειας ιστού, 4 προϊόντα (26.6%) καλύπτουν επιπλέον την κατηγορία της πρόληψης απώλειας δεδομένων, 2 προϊόντα (13.3%) καλύπτουν έξτρα την κατηγορία της διαχείρισης ταυτότητας και πρόσβασης και 1 προϊόν (6.6%) καλύπτει επιπλέον την κατηγορία της ασφάλειας ηλεκτρονικού ταχυδρομείου.

Η ασφάλεια ιστού καλύπτεται από 12 προϊόντα διότι σχετίζεται άμεσα με την ασφάλεια δικτύου. Το διαδίκτυο μπορεί να θεωρηθεί ένα μεγάλο δίκτυο που συνδέει πολλά μικρότερα δίκτυα. Οπότε, όταν ένα προϊόν καλύπτει την ασφάλεια δικτύου, τότε καλύπτει και την ασφάλεια διαδικτύου εντός όμως των πλαισίων ενός οργανισμού, προστατεύοντας εσωτερικά σημεία πρόσβασης με το διαδίκτυο.
Αν δούμε τον αριθμό επιπλέον κατηγοριών που καλύπτονται ανά προϊόν, 2 προϊόντα (26.6%) καλύπτουν μία επιπλέον κατηγορία, 5 προϊόντα (33.3) καλύπτουν δύο επιπλέον κατηγορίες και 7 προϊόντα (46.6%) καλύπτουν τρεις επιπλέον κατηγορίες.
Τα αποτελέσματα είναι πολύ ικανοποιητικά καθώς σχεδόν όλα τα προϊόντα καλύπτουν παραπάνω από μία κατηγορία. Νικητήρια προϊόντα είναι τα προϊόντα εκείνα τα οποία καλύπτουν τρείς επιπλέον κατηγορίες (δείτε πίνακα αποτίμησης).

Μοντέλο κόστους: Σχετικά με την τιμολόγηση για 2 προϊόντα (13.3%) δεν βρέθηκαν πληροφορίες. 1 προϊόν (6.6%) είναι δωρεάν, 1 προϊόν (6.6%) παρέχει πληροφορίες τιμολόγησης μόνο μετα από επικοινωνία με την εταιρία ενώ 2 προϊόντα (13.3%) τιμολογούνται με άδεια bring your own license. 5 προϊόντα (33.3%) τιμολογούνται με βάση το φόρτο εργασίας, 6 προϊόντα (40%) τιμολογούνται με βάση τις ώρες χρήσης, 1 προϊόν (6.6%) τιμολογείται με βάση τον όγκο δεδομένων, 1 προϊόν (6.6%) τιμολογείται με βάση τον αριθμό χρηστών και απαιτεί ο ελάχιστος αριθμός χρηστών να είναι 25, 1 προϊόν (6.6%) τιμολογείται με βάση τον αριθμό συσκευών & τα πρόσθετα και 1 προϊόν τιμολογείται με βάση τα βασικά χαρακτηριστικά.
Υπάρχουν 3 προϊόντα (20%) τα οποία τιμολογούνται με δύο διαφορετικούς τρόπους ανάλογα με την προτίμηση του αγοραστή. Για παράδειγμα, το προϊόν SonicWall NSv (Firewall/Security/VPN/Router) υποστηρίζει τιμολόγηση με βάση τον αριθμό χρηστών (sso users) ή τιμολόγηση με βάση τη χρήση.
Σχετικά με την ύπαρξη πακέτων υπάρχει μόνο 1 προϊόν (6.6%), το Hillstone CloudEdge Virtual-Firewall, το οποίο προσφέρει 5 διαφορετικά πακέτα (3 πακέτα στην βασική έκδοση και 2 πακέτα στην προχωρημένη).
Σχετικά με τη χρονική συνιστώσα, 2 προϊόντα (13.3%) διαθέτουν ετήσια συνδρομή, 3 προϊόντα (13.3%) διαθέτουν χρέωση ανά ώρα ή ανά έτος και ένα προϊόν διαθέτει μηνιαία, ετήσια και τριετή χρέωση.
Τα αποτελέσματα δεν είναι ιδιαίτερα ικανοποιητικά καθώς μόνο 1 προϊόν διαθέτει πακέτα και μόνο 4 προϊόντα διαθέτουν πάνω από μία επιλογή στη χρονική συνιστώσα των πληρωμών. Νικητήρια είναι το προϊόν με τα 5 πακέτα, το Hillstone CloudEdge Virtual-Firewall, το προϊόν με τις τρεις επιλογές χρονικής συνιστώσας, το Untangle NG Firewall, και τα 3 προϊόντα τα οποία διαθέτουν δυνατότητα επιλογής ανάμεσα σε δύο τρόπους χρέωσης

Μηχανισμοί ασφάλειας: 13 προϊόντα (86.6%) υποστηρίζουν τόσο βασική όσο και επιπλέον λειτουργικότητα ενώ δυο προϊόντα (13.3%) υποστηρίζουν μόνο τη βασική λειτουργικότητα. Τα προϊόντα με τον μεγαλύτερο αριθμό από λειτουργικότητες είναι τα Barracuda CloudGen Firewall και Hillstone CloudEdge Virtual-Firewall, τα οποία καλύπτουν 16 και 17 λειτουργικότητες, αντίστοιχα. Για παράδειγμα, το

φιλτράρισμα URL είναι μία επιπλέον λειτουργικότητα, η οποία εντάσσεται στην κατηγορία της ασφάλειας ιστού. Τα δύο αυτά προϊόντα είναι και τα νικητήρια.
Τα αποτελέσματα είναι ικανοποιητικά καθώς σχεδόν όλα τα προϊόντα καλύπτουν έξτρα λειτουργικότητα και στις περισσότερες περιπτώσεις καλύπτουν επιπλέον κατηγορίες ασφαλείας. Νικητήριο προϊόν είναι το Hillstone CloudEdge Virtual-Firewall, το οποίο καλύπτει τις περισσότερες λειτουργικότητες.

Μη λειτουργικές εγγυήσεις: Βρέθηκαν πληροφορίες μόνο σε 4 προϊόντα. 1 προϊόν (6.6%) προσφέρει προηγμένη πρόληψη απειλών με 100% ποσοστό αποκλεισμού, 100% πρόληψη κακόβουλου λογισμικού, 100% αντίσταση εκμετάλλευσης (exploit resistance) και 0% ψευδώς θετικά. 1 προϊόν (6.6%) προσφέρει ακρίβεια 96% στον εντοπισμό και την πρόβλεψη μελλοντικών επιθέσεων καθώς και ανίχνευση απειλών σε λιγότερο από ένα δευτερόλεπτο, με αποτελεσματικότητα μεγαλύτερη από 99,5%. Τέλος, 1 προϊόν έχει στόχος χρόνου αποκατάστασης (RTO) έως 5 ώρες και στόχο σημείου αποκατάστασης (RPO) έως 24 ώρες. Οι παραπάνω στόχοι αφορούν το ίδιο το λογισμικό/προϊόν σε περίπτωση αστοχίας και όχι κάποια λειτουργικότητα.
Τα αποτελέσματα δεν είναι ικανοποιητικά διότι βρέθηκαν εγγυήσεις μόνο σε 4 προϊόντα ενώ και οι εγγυήσεις που προσφέρονται ποικίλουν και άρα δεν είναι κοινές (ως προς τι ακριβώς εγγυάται). Νικητήριο είναι το πρώτο προϊόν που αναφέρθηκε, το CloudGuard Network Security All-In-One, διότι προσφέρει τέσσερις διαφορετικές εγγυήσεις.

Είδος προσφερόμενης προστασίας: Είναι προληπτική (preventive) και ανιχνευτική σε 14 προϊόντα (93.3%). Σε 1 προϊόν (6.6%) είναι μόνο προληπτική (preventive) καθώς αυτό καλύπτει μόνο την κατηγορία της ασφάλειας δικτύου. Σε αυτή την κατηγορία, το τείχος προστασίας αποτελεί την βασική λειτουργικότητα, το οποίο προσφέρει προληπτική προστασία. Τα άλλα προϊόντα, όμως, διαθέτουν σύστημα ανίχνευσης ή αποτροπής εισβολών, το οποίο προσφέρει ανιχνευτική προστασία. Επιπλέον, η προληπτική προστασία για αυτά προσφέρεται και μέσω υλοποίησης μηχανισμών από τις κατηγορίες πρόληψης απώλειας δεδομένων και διαχείρισης ταυτότητας και πρόσβασης. Συνεπώς, τα αποτελέσματα θεωρούνται τόσο αναμενόμενα όσο και αρκετά ικανοποιητικά.

Ιδιότητες ασφάλειας: Βρέθηκαν πληροφορίες σε 6 προϊόντα. 6 προϊόντα (40%) καλύπτουν τη διαθεσιμότητα και 1 προϊόν (6.6%) καλύπτει την εμπιστευτικότητα. Σχετικά με τον αριθμό ιδιοτήτων ανά προϊόν, 1 προϊόν (6.6%) καλύπτει δύο ιδιότητες και 5 προϊόντα (33.3%) καλύπτουν 2 ιδιότητες. Η ιδιότητα της διαθεσιμότητας προσφέρεται και μέσω υλοποίησης μηχανισμών από την κατηγορία πρόληψης απώλειας δεδομένων.
Τα αποτελέσματα δεν είναι καθόλου ικανοποιητικά καθώς βρέθηκαν πληροφορίες μόνο σε 6 προϊόντα και μόνο 3 προϊόντα καλύπτουν δύο ή περισσότερες ιδιότητες. Νικητήριο προϊόν είναι το SonicWall NSv (Firewall/Security/VPN/Router), το οποίο καλύπτει και τις τρεις ιδιότητες.

Προστατευόμενα αντικείμενα: Όλα τα προϊόντα (100%) προστατεύουν σε μεγαλύτερο βαθμό το δίκτυο και κατά συνέπεια σε λιγότερο βαθμό οποιοδήποτε συστατικό του πληροφοριακού συστήματος καθώς όλα τα συστατικά του πληροφοριακού συστήματος είναι συνδεδεμένα στο δίκτυο. Ο λιγότερος βαθμός προστασίας για τα υπόλοιπα συστατικά οφείλεται στο γεγονός πως μπορεί να υπάρχουν επιθέσεις, π.χ. σε μηχανήματα, που να μην καλύπτονται από την προστασία δικτύου. 4 προϊόντα (26.6%) προστατεύουν τους ξενιστές. Τα αποτελέσματα θεωρούνται ικανοποιητικά και αναμενόμενα.

Αντιμετωπιζόμενες απειλές: 11 προϊόντα (73.3%) αντιμετωπίζουν το κακόβουλο λογισμικό συμπεριλαμβανομένων του λογισμικού διαφημίσεων και των keyloggers. 4 προϊόντα (26.6%) αντιμετωπίζουν τις απειλές διαδικτύου, συμπεριλαμβανομένων του κακόβουλου περιεχομένου ιστού, των κακόβουλων URL και της ακούσιας ή κακόβουλης μετάδοσης αρχείων. 3 προϊόντα (20%) αντιμετωπίζουν το λυτρισμικό, 3 προϊόντα (20%) αντιμετωπίζουν τις επιθέσεις command and control και 3 προϊόντα (20%) αντιμετωπίζουν το κατασκοπευτικό λογισμικό. 4 προϊόντα (26.6%) αντιμετωπίζουν επιθέσεις άρνησης και κατανεμημένης άρνησης εξυπηρέτησης, 5 προϊόντα (33.3%) αντιμετωπίζουν τις προηγμένες επίμονες απειλές, 5 προϊόντα (33.3%) αντιμετωπίζουν τους ιούς και 6 προϊόντα (40%) αντιμετωπίζουν τις απειλές δικτύου, συμπεριλαμβανομένων των επιθέσεων επίλυσης πρωτοκόλλου δικτύου (ARP attack). 2 προϊόντα (13.3%) αντιμετωπίζουν τις επιθέσεις μηδενικής μέρας, 3 προϊόντα (20%) αντιμετωπίζουν τις επιθέσεις botnet, 2 προϊόντα (13.3%) αντιμετωπίζουν το ηλεκτρονικό ψάρεμα και 3 προϊόντα (20%) αντιμετωπίζουν ευπάθειες και εκμεταλλεύσεις. 3 προϊόντα (20%) αντιμετωπίζουν την κλοπή δεδομένων συμπεριλαμβανομένης της διήθησης δεδομένων (data extrafiltration). 1 προϊόν (6.6%) αντιμετωπίζει τις απόπειρες hacking και 1 προϊόν (6.6%) αντιμετωπίζει τις επιθέσεις πλευρικού καναλιού, τις επιθέσεις cross virtual machine και τις ευπάθειες εφαρμογών και πρωτοκόλλων. 1 προϊόν (6.6%) αντιμετωπίζει οποιαδήποτε γνωστή και άγνωστη απειλή και τέλος 2 προϊόντα (13.3%) αντιμετωπίζουν εισβολές και ανεπιθύμητο περιεχόμενο.
Αν δούμε τον αριθμό απειλών που αντιμετωπίζονται ανά προϊόν, 2 προϊόντα (13.3%) αντιμετωπίζουν μια απειλή, 2 προϊόντα (13.3%) αντιμετωπίζουν τρεις απειλές, 2 προϊόντα (13.3%) αντιμετωπίζουν πέντε απειλές και 2 προϊόντα (13.3%) αντιμετωπίζουν δεκατρείς απειλές, 1 προϊόν (6.6%) αντιμετωπίζει τέσσερις απειλές, 1 προϊόν (6.6%) αντιμετωπίζει έξι απειλές, 1 προϊόν (6.6%) αντιμετωπίζει επτά απειλές, 1 προϊόν (6.6%) αντιμετωπίζει εννέα απειλές και 3 προϊόντα (20%) αντιμετωπίζουν δύο απειλές.
Τα αποτελέσματα είναι αρκετά ικανοποιητικά καθώς τα ⅔ των προϊόντων αντιμετωπίζουν από τρεις έως 13 απειλές. Τα νικητήρια προϊόντα είναι τα SonicWall NSv (Firewall/Security/VPN/Router) και vSRX Next Generation Firewall, τα οποία αντιμετωπίζουν 13 είδη απειλών.

Περιορισμοί χρήσης: Βρέθηκαν πληροφορίες σε 5 προϊόντα. 1 προϊόν (6.6%) λειτουργεί με ταχύτητες δικτύου έως και 100 Gbps. 1 προϊόν (6.6%) στη μέγιστη έκδοση έχει ρυθμοαπόδοση 15.5Gbps, έως 2 εκ. ταυτόχρονες συνδέσεις και 10 χιλιάδες συνδέσεις vpn (vpn peers). 1 προϊόν (6.6%) στη μέγιστη έκδοση υποστηρίζει έως 20 χιλιάδες χρήστες. 1 προϊόν (6.6%) έχει απόδοση έως 10 Gbps. Τέλος, 1 προϊόν (6.6%) στη μεγαλύτερη έκδοση υποστηρίζει έως και 5 εκατομμύρια ταυτόχρονες συνεδρίες, έως

10000 σήραγγες VPN IPSec και έως 2000 χρήστες SSL VPN. Οι παραπάνω περιορισμοί είναι αναμενόμενοι διότι αφορούν κάποια όρια σχετικά με τη λειτουργία των προϊόντων. Τα αποτελέσματα δεν είναι ικανοποιητικά διότι βρέθηκαν πληροφορίες μόνο στο ⅓ των προϊόντων.

Δοκιμαστικέ εκδόσεις: 1 προϊόν (6.6%) δεν παρέχει δωρεάν δοκιμαστική έκδοση, 1 προϊόν 96.6%) είναι δωρεάν, 11 προϊόντα (73.3%) παρέχουν δωρεάν δοκιμαστική έκδοση 30 ημερών, 1 προϊόν (6.6%) παρέχει δωρεάν δοκιμαστική έκδοση 14 ημερών και 1 προϊόν (6.6%) παρέχει δωρεάν δοκιμαστική έκδοση 7 ημερών. Τα αποτελέσματα είναι ικανοποιητικά καθώς πάνω από το ⅔ των προϊόντων παρέχει δωρεάν δοκιμαστική έκδοση 30 ημερών. Τα προϊόντα αυτά είναι και τα νικητήρια (δείτε πίνακα αποτίμησης)

Τρόπος χρήσης: 2 προϊόντα (13.3%) υποστηρίζουν διεπαφή προγραμματισμού εφαρμογών μεταφοράς αναπαραστατικής κατάστασης και γραφικό περιβάλλον εργασίας μέσω διαδικτύου. 2 προϊόντα (13.3%) υποστηρίζουν γραφικό περιβάλλον εργασίας μέσω διαδικτύου και χρήση γραμμής εντολών. 9 προϊόντα (60%) υποστηρίζουν και τις τρεις τεχνολογίες και 1 προϊόν (6.6%) υποστηρίζει μόνο γραμμή εντολών.
Αν δούμε τις τιμές αποτίμησης μεμονωμένα, η διεπαφή προγραμματισμού εφαρμογών μεταφοράς αναπαραστατικής κατάστασης εμφανίζεται σε 11 προϊόντα (73.3%). Το γραφικό περιβάλλον εργασίας μέσω διαδικτύου εμφανίζεται σε 13 προϊόντα (86.6%) και η γραμμή εντολών εμφανίζεται σε 12 προϊόντα (80%).
Τα αποτελέσματα θεωρούνται ικανοποιητικά καθώς σχεδόν τα ⅔ των προϊόντων υποστηρίζουν και τις τρεις τεχνολογίες. Αυτό συμβαίνει λόγω της ποικιλομορφίας στις λειτουργικότητες των προϊόντων. Υπάρχουν περιπτώσεις όπου η κάθε λειτουργικότητα απαιτεί και μία διαφορετική τεχνολογία για να εφαρμοστεί σωστά. Για παράδειγμα, τα συστήματα εντοπισμού/αποτροπής εισβολών, τα οποία εμφανίζονται σε 13 προϊόντα, υλοποιούνται κατά κόρον με χρήση τους γραμμής εντολών. Ένα ακόμα παράδειγμα είναι η ασφάλεια ιστού, η οποία εμφανίζεται σε 12 προϊόντα. Για την ασφάλεια ιστού είναι απαραίτητο ένα γραφικό περιβάλλον εργασίας ώστε να γίνονται οι κατάλληλες ρυθμίσεις και γενικότερα να υπάρχει μία απεικόνιση φιλική ως προς τους χρήστες. Έτσι, λοιπόν, φτάνουμε στο συμπέρασμα πως είναι λογικό να υποστηρίζονται και οι τρεις τεχνολογίες.

Αγορές: 7 προϊόντα (46.6%) εντοπίστηκαν στο Amazon web services και στο Microsoft Azure, 1 προϊόν (6.6%) εντοπίστηκε στο Google cloud platform και στο Amazon web services, 2 προϊόντα (13.3%) εντοπίστηκαν στο Microsoft Azure, 1 προϊόν (6.6%) εντοπίστηκε στο Amazon web services και 3 προϊόντα (20%) εντοπίστηκαν και στις τρεις αγορές. Συνολικά, 12 προϊόντα (80%) εντοπίστηκαν στο Microsoft Azure, 12 προϊόντα (80%) εντοπίστηκαν στο Amazon web services και 4 προϊόντα (26.6%) εντοπίστηκαν στο Google cloud platform.
Τα αποτελέσματά είναι ιδιαίτερα ικανοποιητικά καθώς 9 προϊόντα εντοπίστηκαν σε δύο αγορές και 3 προϊόντα εντοπίστηκαν σε όλες τις αγορές. Τα προϊόντα τα οποία εντοπίστηκαν σε όλες τις αγορές (δείτε πίνακα αποτίμησης) είναι και τα νικητήρια.

Επίπεδο/είδος υποστήριξης: Σχετικά με το είδος υποστήριξης, 14 προϊόντα (93,3%) προσφέρουν υποστήριξη μέσω email, 15 προϊόντα (70%) μέσω τηλεφώνου, 11 προϊόντα (73.3%) μέσω δελτίων (tickets) και 7 προϊόντα (46.6%) μέσω μηνυμάτων (chat). 13 προϊόντα (86.6%) διαθέτουν υποστήριξη κοινοτήτων χρηστών (κοινότητα, φόρουμ, blog), 12 προϊόντα (80%) διαθέτουν τεκμηρίωση (documentation), 5 προϊόντα (33.3%) διαθέτουν πύλη υποστήριξης και 15 προϊόντα (100%) διαθέτουν υποστηρικτικό υλικό (έγγραφα με πληροφορίες, βίντεο, FAQ). 4 προϊόντα (26.6%) διαθέτουν βάση γνώσης (knowledge base). 6 προϊόντα (40%) διαθέτουν ενημερώσεις για νέα προϊόντα και 3 προϊόντα (20%) διαθέτουν κέντρο βοήθειας. 1 προϊόν (6.6%) διαθέτει εκπαίδευση, 1 προϊόν (6.6%) διαθέτει βοηθητικές παροχές (utility services) και 1 προϊόν (6.6%) διαθέτει ενημέρωση για συνδρομές, κέντρο γνώσης και λεξικό.

Υπάρχουν 3 προϊόντα (20%) τα οποία διαθέτουν τρία πακέτα: 1 προϊόν (6.6%) διαθέτει τέσσερα πακέτα και 2 προϊόντα (13.3%) διαθέτουν δύο πακέτα υποστήριξης.

Για την ημερολογιακή/χρονική διάρκεια κατά την οποία παρέχεται υποστήριξη, υπάρχουν 8 προϊόντα (80%) τα οποία προσφέρουν υποστήριξη 24/7 και 2 προϊόντα (13.3%) τα οποία παρέχουν υποστήριξη από 9/5 έως 24/7.

Τα αποτελέσματα είναι οριακά ικανοποιητικά διότι ναι μεν είναι ικανοποιητικό πως πάνω από τα μισά προϊόντα διαθέτουν 24/7 υποστήριξη αλλά δεν είναι ικανοποιητικό πως μόνο 6 προϊόντα διαθέτουν διαφορετικά πακέτα. Νικητήριο προϊόν είναι το CloudGuard Network Security All-In-One, το οποίο διαθέτει 4 πακέτα και υποστήριξη 24/7.

Νικητήρια προϊόντα για ολόκληρη την κατηγορία είναι τα CloudGuard Network Security All-In-One και SonicWall NSv (Firewall/Security/VPN/Router), τα οποία εμφανίζονται ως νικητήρια από 4 φορές.

5.2.9 Αποτίμηση ασφάλειας (Security assessment)

Για αυτή την ενότητα βρέθηκαν 15 προϊόντα με επαρκή τεκμηρίωση, τα οποία αποτιμήθηκαν. Τα αποτελέσματα αποτίμησης εμφανίζονται στον Πίνακα 9 του παραρτήματος. Παρακάτω παρέχουμε μια στατιστική ανάλυση των αποτελεσμάτων αυτών ανά κριτήριο.

Τρόπος παράδοσης: 3 προϊόντα (20%) διατίθενται σαν υποδομή και 12 προϊόντα (80%) διατίθεται σαν λογισμικό. Τα περισσότερα προϊόντα διατίθενται σαν λογισμικό λόγω των πλεονεκτημάτων που έχει αυτός ο τρόπος παράδοσης σε σχέση με τους υπόλοιπους. Τα αποτελέσματα δεν είναι ικανοποιητικά διότι κανένα προϊόν δεν υποστηρίζει δύο τρόπους παράδοσης.

Μοντέλο διάταξης: όλα τα προϊόντα (100%) υποστηρίζουν το δημόσιο νέφος. Αυτό είναι λογικό διότι 12 προϊόντα διατίθενται σαν λογισμικό, συνεπώς το μοντέλο διάταξης είναι το δημόσιο νέφος. Επίσης, τα 3 προϊόντα που διατίθενται σαν υποδομή υποστηρίζουν και αυτά το δημόσιο νέφος λόγω των πλεονεκτημάτων που υπάρχουν συγκριτικά με τα υπόλοιπα μοντέλα διάταξης. Από την άλλη πλευρά, τα αποτελέσματα δεν είναι ικανοποιητικά διότι κανένα προϊόν δεν υποστηρίζει παραπάνω από ένα μοντέλο διάταξης.

Κατηγορία ασφάλειας: Όλα τα προϊόντα (100%) καλύπτουν μόνο την τρέχουσα κατηγορία. Βέβαια, θα μπορούσε κανείς να πει πως καλύπτεται και η ασφάλεια δικτύου διότι τα προϊόντα αποτίμησης ασφάλειας ενδεχομένως να χρησιμοποιούν παρόμοιους μηχανισμούς με τα προϊόντα ασφάλειας δικτύου. Η αξιολόγηση ασφάλειας περιλαμβάνει την δοκιμή, η οποία σχετίζεται με την διενέργεια δοκιμών για να εντοπιστούν ευπάθειες. Εκεί χρησιμοποιούνται εργαλεία που σχετίζονται με την ασφάλεια δικτύου και την ανίχνευση τρωτοτήτων. Βέβαια, τα εργαλεία αυτά δεν αναφέρονται ρητά ώστε να μπορέσουμε να θεωρήσουμε πως καλύπτονται επιπλέον κατηγορίες ασφαλείας. Υπάρχει συσχέτιση με τις κατηγορίες ασφάλειας δικτύου και διαδικτύου αλλά μπορεί να θεωρηθεί πως οι μηχανισμοί της τρέχουσας κατηγορίας επαναχρησιμοποιούνται σε αυτές τις κατηγορίες.

Μοντέλο κόστους: Σχετικά με την τιμολόγηση, δεν βρέθηκαν πληροφορίες για 5 προϊόντα (33.3%) και 1 προϊόν (6.6%) διατίθεται με άδεια bring your own license. 2 προϊόντα (13.3%) παρέχουν πληροφορίες τιμολόγησης μόνο με επικοινωνία με την εταιρία. 3 προϊόντα (20%) τιμολογούν με βάση τους πόρους (resources), 3 προϊόντα (20%) τιμολογούν με βάση τα χαρακτηριστικά. 1 προϊόν τιμολογεί με βάση τα υποσυστήματα (modules) που χρησιμοποιούνται όπου το υποσύστημα των επιθεωρήσεων και δοκίμων (assessment and testing) έχει κόστος 300$/μήνα. Σχετικά με την ύπαρξη πακέτων, 4 προϊόντα (26.6%) διαθέτουν 2 πακέτα και 1 προϊόν (6.6%) διαθέτει 4 πακέτα. Η μόνιμη δωρεάν έκδοση που διαθέτουν κάποια προϊόντα δεν μετρήθηκε ως πακέτο. Σχετικά με τη χρονική συνιστώσα, 2 προϊόντα (13.3%) υποστηρίζουν μηνιαία ή ετήσια πληρωμή και 1 προϊόν διαθέτει ετήσια, διετή ή τριετή άδεια χρήσης.

Τα αποτελέσματα δεν θεωρούνται ικανοποιητικά διότι δεν βρέθηκαν πληροφορίες για 5 προϊόντα (33.3%) και μόνο 3 προϊόντα (20%) διαθέτουν επιλογή χρονικής συνιστώσας. Από την άλλη πλευρά, το θετικό στοιχείο είναι πως τα μισά προϊόντα από τα οποία αντλήθηκαν πληροφορίες διαθέτουν δύο ή περισσότερα διαφορετικά πακέτα τιμολόγησης. Νικητήριο προϊόν είναι το ValuRisQ CCPA Automated Compliance for Small and Medium Businesses, το οποίο διαθέτει 4 πακέτα, και το Tenable Nessus, το οποίο διαθέτει τις περισσότερες επιλογές χρονικής συνιστώσας.

Μηχανισμοί ασφάλειας: 10 προϊόντα (66.6%) υποστηρίζουν τόσο βασική όσο και επιπλέον λειτουργικότητα εντός της κατηγορίας ενώ 5 προϊόντα (33.3%) υποστηρίζουν μόνο τη βασική λειτουργικότητα. Τα προϊόντα με τον μικρότερο αριθμό από λειτουργικότητες είναι τα Cymetrics SaaS platform - Cyber Assessment και QS solutions Cyber Security Assessment Tool (CSAT), τα οποία καλύπτουν 3 λειτουργικότητες. Το προϊόν με τον μεγαλύτερο αριθμό από λειτουργικότητες είναι το Qualys Cloud Security Assessment με 10 λειτουργικότητες, το οποίο είναι και το νικητήριο. Τα αποτελέσματα δεν είναι ιδιαίτερα ικανοποιητικά διότι μόνο τα ⅔ των προϊόντων υποστηρίζουν επιπλέον λειτουργικότητα.

Μη λειτουργικές εγγυήσεις: Βρέθηκαν πληροφορίες μόνο σε 3 προϊόντα. Ειδικότερα, το Qualys Security Configuration Assessment διαθέτει 99.5% διαθεσιμότητα και 99.99966% ακρίβεια εντοπισμού ευπαθειών. Το Qualys Cloud Security Assessment διαθέτει 99.5% διαθεσιμότητα και το Tennable Nessus διαθέτει 99.95% διαθεσιμότητα με σύστημα ποινών. Πιο συγκεκριμένα, για 95.00% έως 99.94% επιστροφή 10% της μηνιαίας συνδρομής, για 90.00% έως 94.99% επιστροφή 15% και για <90% επιστροφή

20%. Τα αποτελέσματα είναι πολύ απογοητευτικά διότι βρέθηκαν εγγυήσεις μόνο στο ⅕ των προϊόντων. Νικητήριο προϊόν ως προς το σύστημα ποινών είναι το Tennable Nessus και ως προς τον αριθμό εγγυήσεων το Qualys Security Configuration Assessment.

Είδος προσφερόμενης προστασίας: Όλα τα προϊόντα (100%) προσφέρουν προληπτική και ανιχνευτική προστασία. Αυτό είναι αναμενόμενο διότι οι αξιολογήσεις ασφαλείας έχουν σαν στόχο να καταγράψουν την υπάρχουσα κατάσταση, να εντοπίσουν ευπάθειες και έπειτα να παρουσιάσουν τα ευρήματα και να προτείνουν λύσεις. Οι οδηγίες/λύσεις που προτείνονται, εάν εφαρμοστούν, θα αυξήσουν το επίπεδο ασφάλειας του οργανισμού και θα ενισχυθεί η προστασία από μελλοντικές επιθέσεις. Άρα, λοιπόν, τα μέτρα που λαμβάνονται λειτουργούν προληπτικά με στόχο την καλύτερη προστασία στο μέλλον. Επιπλέον, αν ελέγχοντας ένα αρχείο καταχωρήσεων (log file) εντοπιστεί κάποιο πραγματικό συμβάν ασφάλειας, τότε υπάρχει ανιχνευτική προστασία ανεξάρτητα από τον χρόνο κατά τον οποίο εντοπίστηκε το συμβάν.

Ιδιότητες ασφαλείας: Δεν βρέθηκαν πληροφορίες σε κανένα προϊόν. Αυτό είναι πολύ απογοητευτικό αλλά αναμενόμενο διότι οι αξιολογήσεις ασφαλείας ουσιαστικά πραγματοποιούν μια επιθεώρηση της υπάρχουσας κατάστασης, παρουσιάζονται αποτελέσματα και προτείνονται πιθανές λύσεις για να αυξηθεί το επίπεδο ασφάλειας. Εφόσον, λοιπόν, απλά προτείνονται κάποια μέτρα αλλά δεν είναι απόλυτα βέβαιο πως θα εφαρμοστούν είναι λογικό να μην εξασφαλίζεται κάποια ιδιότητα ασφάλειας

Προστατευόμενα αντικείμενα: 11 προϊόντα (40%) προστατεύουν ολόκληρο τον οργανισμό. Επιπλέον, 3 προϊόντα (20%) προστατεύουν δημόσια νέφη. Πιο συγκεκριμένα, 1 προϊόν προστατεύει μόνο το νέφος του Amazon web services και 2 προϊόντα προστατεύουν το νέφος γενικά, ανεξαρτήτως παρόχου. Τέλος, 1 προϊόν (6.6%) προστατεύει τις εφαρμογές, τις επιτόπιες υποδομές και το νέφος των οργανισμών, συνεπώς σχεδόν όλο τον οργανισμό.
Τα αποτελέσματα είναι ικανοποιητικά καθώς 12 προϊόντα σίγουρα παρέχουν συνολική προστασία σε ολόκληρο τον οργανισμό. Επιπλέον, δυνητικά ένας οργανισμός ενδεχομένως να προστατεύεται και από τα άλλα 3 προϊόντα είτε πλήρως είτε εν μέρει ανάλογα με το που βρίσκονται όλα τα ψηφιακά του αγαθά (στο νέφος ή/και σε επιτόπιες υποδομές). Άρα, τελικά στη βέλτιστη περίπτωση όλα τα προϊόντα δύναται να προστατέψουν ολόκληρο τον οργανισμό.

Αντιμετωπιζόμενες απειλές: Όλα τα προϊόντα (100%) δυνητικά μπορούν να παρέχουν υποστήριξη προστασίας για οποιαδήποτε απειλή. Αυτό είναι αναμενόμενο διότι ο ρόλος των αξιολογήσεων δεν είναι να προστατεύσουν άμεσα από κάποια συγκεκριμένη απειλή αλλά να την ανιχνεύσουν και να προτείνουν λύσεις αντιμετώπισής της, οπότε συμβάλλουν συμβουλευτικά στη βελτίωση του επιπέδου ασφαλείας συνολικά. Οι ευπάθειες που μπορεί να εντοπιστούν μπορεί να περιλαμβάνουν πάρα πολλά είδη, οπότε δυνητικά θα μπορούσαν να καλυφθούν πάρα πολλές απειλές (έστω και ανιχνευτικά και όχι πλήρως).

Περιορισμοί χρήσης: Βρέθηκαν πληροφορίες μόνο σε 2 προϊόντα. Σε 1 προϊόν (6.6%) στη μέγιστη έκδοση αξιολογούνται έως 200 συστήματα και σε 1 προϊόν στη μέγιστη έκδοση υποστηρίζονται έως 500 αιτήματα πρόσβασης στα δεδομένα (data requests) ανά έτος. Από την φύση των προϊόντων, δεν δύναται να παρέχονται περιορισμοί διότι αυτοί εμποδίζουν την ελκυστικότητα του προσφερόμενου προϊόντος. Οι περιορισμοί που βρέθηκαν σε δύο προϊόντα είναι φυσιολογικοί διότι αφορούν τον τρόπο λειτουργίας των προϊόντων.

Δοκιμαστικές εκδόσεις: 8 προϊόντα (53.3%) δεν διαθέτουν δωρεάν δοκιμαστική έκδοση. 2 προϊόντα (13.3%) διαθέτουν δωρεάν δοκιμαστική έκδοση 30 ημερών, 1 προϊόν (6.6%) διαθέτει δωρεάν δοκιμαστική έκδοση 14 ημερών και 1 προϊόν (6.6%) διαθέτει δωρεάν δοκιμαστική έκδοση 7 ημερών. 3 προϊόντα (20%) διαθέτουν μόνιμη δωρεάν έκδοση με περιορισμένες δυνατότητες.
Το αποτέλεσμα είναι απογοητευτικό διότι μόνο 5 προϊόντα διαθέτουν δωρεάν δοκιμαστική έκδοση διάρκειας μεγαλύτερης ή ίσης των 30 ημερών. Τα προϊόντα αυτά είναι και τα νικητήρια (δείτε πίνακα αποτίμησης)

Τρόπος χρήσης: 1 προϊόν (6.6%) δεν υποστηρίζει κάποια τεχνολογία. 14 προϊόντα (93.3%) υποστηρίζουν το γραφικό περιβάλλον εργασίας μέσω διαδικτύου. 4 προϊόντα (26.6%) υποστηρίζουν χρήση γραμμής εντολών και 4 προϊόντα (26.6%) υποστηρίζουν διεπαφή προγραμματισμού εφαρμογών μεταφοράς αναπαραστατικής κατάστασης.
Αν δούμε τον αριθμό τεχνολογιών ανά προϊόν 9 προϊόντα (60%) υποστηρίζουν μία τεχνολογία, 2 προϊόντα (13.3%) υποστηρίζουν δύο τεχνολογίες και 3 προϊόντα (20%) υποστηρίζουν και τις τρεις τεχνολογίες. Αυτά τα τρία προϊόντα (δείτε πίνακα αποτίμησης) είναι και τα νικητήρια.
Το αποτέλεσμα είναι αναμενόμενο διότι τα προϊόντα αυτής της κατηγορίας διατίθενται σαν λογισμικό – άρα, για να αποκτήσουν πρόσβαση οι χρήστες είναι απαραίτητη η χρήση του γραφικού περιβάλλοντος εργασίας. Επιπλέον, οι χρήστες έχουν τη δυνατότητα να πραγματοποιήσουν τις απαραίτητες ενέργειες και να παραμετροποιήσουν κατάλληλα το προϊόν με σχετική ευκολία. Τα αποτελέσματα δεν είναι ικανοποιητικά διότι μόνο το ⅓ των προϊόντων υποστηρίζει παραπάνω από μία τεχνολογία.

Αγορές: 5 προϊόντα (33.3%) εντοπίστηκαν στο Microsoft Azure, 4 προϊόντα (66.6%) εντοπίστηκαν στο Amazon web services και 7 προϊόντα δεν εντοπίστηκαν σε καμία από τις τρεις αγορές. Το μοναδικό προϊόν το οποίο εντοπίστηκε σε δύο αγορές είναι το Tennable Nessus, το οποίο είναι και το νικητήριο. Τα αποτελέσματα δεν είναι ικανοποιητικά.

Επίπεδο/είδος υποστήριξης: Όλα τα προϊόντα (100%) προσφέρουν επικοινωνία μέσω email, 9 προϊόντα (60%) μέσω τηλεφώνου, 3 προϊόντα (20%) μέσω δελτίων (tickets) και 5 προϊόντα (33.3%) μέσω μηνυμάτων (chat). 15 προϊόντα (100%) διαθέτουν υποστηρικτικό υλικό (έγγραφα με πληροφορίες, βίντεο, FAQ). 4 προϊόντα (26.6%) διαθέτουν εκπαίδευση. 3 προϊόντα (20%) διαθέτουν υποστήριξη κοινοτήτων χρηστών (κοινότητα, φόρουμ, blog). 6 προϊόντα (40%) διαθέτουν τεκμηρίωση. 5 προϊόντα

(33.3%) διαθέτουν ενημερώσεις. 2 προϊόντα (13.3%) διαθέτουν κέντρο βοήθειας και 2 προϊόντα (13.3%) διαθέτουν βάση γνώσης.
Σχετικά με την ύπαρξη πακέτων, 1 προϊόν (6.6%), το Tenable Nessus διαθέτει 4 πακέτα.
Σχετικά με τη χρονική συνιστώσα, 4 προϊόντα διαθέτουν υποστήριξη 24/7.
Νικητήριο προϊόν είναι το Tenable Nessus, το οποίο διαθέτει και υποστήριξη 24/7 και 4 διαφορετικά πακέτα. Τα αποτελέσματα δεν είναι ιδιαίτερα ικανοποιητικά καθώς μόνο 4 προϊόντα διαθέτουν υποστήριξη 24/7 και μόνο 1 προϊόν διαθέτει διαφορετικά πακέτα.

Νικητήριο προϊόν για ολόκληρη την κατηγορία είναι το Tenable Nessus, το οποίο εμφανίζεται ως νικητήριο 5 φορές

5.2.10 Ασφάλεια Ιστού (Web Security)

Για αυτή την ενότητα βρέθηκαν 15 προϊόντα με επαρκή τεκμηρίωση, τα οποία αποτιμήθηκαν. Τα αποτελέσματα αποτίμησης εμφανίζονται στον Πίνακα 10 του παραρτήματος. Παρακάτω παρέχουμε μια στατιστική ανάλυση των αποτελεσμάτων αυτών ανά κριτήριο.

Τρόπος παράδοσης: 3 προϊόντα (20%) διατίθενται σαν λογισμικό, 10 προϊόντα (60%) διατίθενται σαν υποδομή και 2 προϊόντα (13.3%) διατίθεται και σαν λογισμικό και σαν υποδομή. Τα περισσότερα προϊόντα προσφέρονται σαν υποδομή διότι διατίθενται στην αγορά σαν τείχη προστασίας εφαρμογών ιστού (web application firewall). Το τείχος προστασίας γενικότερα σαν τεχνολογία είναι μία λειτουργικότητα που ενσωματώνεται σε μία συσκευή οπότε είναι πιο λογικό να προσφέρεται με την μορφή μιας ιδεατής υποδομής. Τα αποτελέσματα δεν είναι ιδιαίτερα ικανοποιητικά διότι μόνο 2 προϊόντα υποστηρίζουν δύο τρόπους παράδοσης. Τα προϊόντα αυτά, το Fastly next-gen WAF and RASP και το Reblaze, είναι τα νικητήρια.

Μοντέλο διάταξης: 13 προϊόντα (86,6%) υποστηρίζουν το δημόσιο νέφος και 2 προϊόντα (13.3%) υποστηρίζουν δημόσιο ή ιδιωτικό νέφος. Το γεγονός πως τα περισσότερα προϊόντα διατίθενται σαν υποδομή λογικά θα έπρεπε να μας οδηγήσει σε μοντέλο διάταξης με ιδιωτικό ή δημόσιο νέφος. Κάτι τέτοιο, όμως, δεν συνέβη διότι δεν βρέθηκαν πληροφορίες που να αναφέρουν ξεκάθαρα πως τα προϊόντα υποστηρίζουν το ιδιωτικό νέφος. Τα αποτελέσματα δεν είναι ικανοποιητικά διότι μόνο δύο προϊόντα υποστηρίζουν παραπάνω από ένα μοντέλο διάταξης. Τα προϊόντα αυτά, το Penta Security - WAPPLES SA (WAF) και το WEBFRONT-KS, είναι τα νικητήρια

Κατηγορία ασφάλειας: 5 προϊόντα (33.3%) καλύπτουν επιπλέον την κατηγορία πρόληψης και απώλειας δεδομένων και 1 προϊόν (6.6%) καλύπτει επιπρόσθετα την κατηγορία της ασφάλειας δικτύου και της διαχείρισης ταυτότητας και πρόσβασης. Τα αποτελέσματα δεν είναι ιδιαίτερα ικανοποιητικά διότι μόνο 6 προϊόντα καλύπτουν κάποια επιπλέον κατηγορία. Νικητήριο προϊόν είναι το Barracuda CloudGen WAF, το οποίο καλύπτει δύο επιπλέον κατηγορίες.

Μοντέλο κόστους: Σχετικά με την τιμολόγηση, 10 προϊόντα (66.6%) τιμολογούν με βάση το φόρτο εργασίας και τις ώρες χρήσης. 2 προϊόντα (13.3%) τιμολογούν με βάση την μηνιαία κίνηση, 2 προϊόντα (13.3%) τιμολογούν με βάση τον αριθμό αιτημάτων (requests) και 3 προϊόντα (20%) τιμολογούν με βάση τον αριθμό εφαρμογών που προστατεύονται. 1 προϊόν (6.6%) τιμολογεί με βάση τα χαρακτηριστικά και 1 προϊόν (6.6%) τιμολογεί με βάση το εύρος ζώνης που χρησιμοποιείται από όλες τις διαμορφωμένες εφαρμογές και τον αριθμό αρχείων που σαρώνονται. 1 προϊόν (6.6%) τιμολογεί με βάση τον αριθμό των εικονικών συσκευών που προστατεύονται. 1 προϊόν (6.6%) τιμολογεί με βάση τον αριθμό workspaces (σύνολο κανόνων και ρυθμίσεων που καθορίζεται από το χρήστη για εφαρμογές και διακομιστές προέλευσης) και τον μέσο όρο αιτημάτων ανά δευτερόλεπτο (RPS) που επεξεργάζεται το τείχος προστασίας εφαρμογών διαδικτύου. Τέλος, 1 προϊόν (6.6%) τιμολογεί με βάση τον αριθμό των τομέων (domains).

Σχετικά με την ύπαρξη πακέτων, 4 προϊόντα (26.6%) διαθέτουν 3 πακέτα, 2 προϊόντα (13.3%) διαθέτουν 4 πακέτα, 1 προϊόν (6.6%) διαθέτει 5 πακέτα και 1 προϊόν (6.6%) διαθέτει 2 πακέτα στην περίπτωση που διατίθεται σαν λογισμικό. Σχετικά με τη χρονική συνιστώσα, 1 προϊόν (6.6%) διαθέτει χρέωση ανά ώρα ή ανά έτος και 2 προϊόντα (13.3%) διαθέτουν μηνιαίο, ετήσιο, διετές και τριετές συμβόλαιο.

Τα αποτελέσματα είναι αρκετά ικανοποιητικά διότι 8 προϊόντα διαθέτουν πάνω από δύο πακέτα πληρωμής. Νικητήριο προϊόν είναι το MONITORAPP AIWAF-VE for Azure, το οποίο διαθέτει 5 διαφορετικά πακέτα τιμολόγησης και νικητήριο προϊόν ως προς την ποικιλία συστατικών τιμολόγησης είναι το Reblaze με 5 διαφορετικά συστατικά.

Μηχανισμοί ασφάλειας: Όλα τα προϊόντα (100%) υποστηρίζουν τόσο βασική όσο και έξτρα λειτουργικότητα, η οποία εμπίπτει κυρίως στην τρέχουσα κατηγορία με ορισμένες εξαιρέσεις. Τα προϊόντα με τον μικρότερο αριθμό από λειτουργικότητες είναι τα προϊόντα Fastly next-gen WAF and RASP, Akamai Web Application Protector και Edgenexus Web Application Firewall (WAF), τα οποία καλύπτουν 6 λειτουργικότητες. Τα προϊόντα με τον μεγαλύτερο αριθμό από λειτουργικότητες είναι τα Barracuda CloudGen WAF και MONITORAPP AIWAF-VE for Azure με 14 λειτουργικότητες και το Penta Security - WAPPLES SA (WAF) με 16 λειτουργικότητες, το οποίο είναι και το νικητήριο.

Μη λειτουργικές εγγυήσεις: Βρέθηκαν πληροφορίες σε 5 προϊόντα (33.3%). 1 προϊόν (6.6%) διαθέτει καθυστέρηση κίνησης του δικτύου < 1.5ms και καθυστέρηση επεξεργασίας ~0.5ms.

1 προϊόν (6.6%) διαθέτει διαθεσιμότητα ροής της κίνησης (traffic flow) 99.999% με σύστημα ποινών. Για <99.999% έως 99.9% επιστροφή 10% της μηνιαίας συνδρομής, για < 99.9% έως 98% επιστροφή 20% , για <98% έως 97% επιστροφή 30%, για <97% έως 96% επιστροφή 40%, για <96% έως επιστροφή 50%. Επιπλέον, διαθέτει διαθεσιμότητα πρόσβασης (web access) 99.9% με σύστημα ποινών. Για <99.9% έως 98% επιστροφή 10%, για <98% έως 97% επιστροφή 20%, για <97% έως 96% επιστροφή 30%, για <96% έως επιστροφή 40%.

1 προϊόν (6.6%) διαθέτει διαθεσιμότητα 99,9% με σύστημα ποινών. Για <99,9-99,0 επιστροφή 5% της μηνιαίας συνδρομής, για <99,0%-98,5% επιστροφή 10%, για <98.5%-98,0% επιστροφή 15%, για <98,0% επιστροφή 20%.

1 προϊόν (6.6%) διαθέτει διαθεσιμότητα 100%. 1 προϊόν (6.6%) διαθέτει διαθεσιμότητα 99.9% με σύστημα ποινών το οποίο προκύπτει από τον μαθηματικό τύπο: Service Credits = (30* Downtime Period Minutes * Affected Customer Ratio) / Scheduled Availability Minutes.

Τα αποτελέσματα δεν είναι ιδιαίτερα ικανοποιητικά καθώς μόνο το ⅓ των προϊόντων διαθέτει εγγυήσεις. Νικητήριο προϊόν, με επιφυλάξεις διότι η πράξη αποδεικνύει πως ποτέ ένα προϊόν δεν μπορεί να έχει 100% διαθεσιμότητα, είναι το Akamai Web Application Protector με την υψηλότερη (100%) διαθεσιμότητα. Άλλο ένα νικητήριο προϊόν, το οποίο διαθέτει δύο διαφορετικές εγγυήσεις με συστήματα ποινών είναι το Barracuda CloudGen WAF as a service.

Είδος παρεχόμενης προστασίας: Όλα τα προϊόντα (100%) προσφέρουν προληπτική προστασία. Η κύρια λειτουργία των προϊόντων είναι το τείχος προστασίας εφαρμογών διαδικτύου. Η προστασία που παρέχει είναι προληπτική γιατί εντοπίζονται νέες απειλές και προληπτική διότι οι απειλές αυτές μπλοκάρονται. Έτσι, λοιπόν, το πληροφοριακό σύστημα θα είναι προστατευμένο προληπτικά από τη στιγμή που θα εντοπιστεί και μπλοκαριστεί μια απειλή και έπειτα.

Ιδιότητες ασφάλειας: Όλα τα προϊόντα (100%) εξασφαλίζουν τη διαθεσιμότητα. Αυτό συμβαίνει διότι όλα τα προϊόντα προσφέρουν προστασία από επιθέσεις (ή κατανεμημένες επιθέσεις) άρνησης εξυπηρέτησης. επίσης, 10 προϊόντα (66.6%) αντιμετωπίζουν διάφορα άλλα είδη επιθέσεων διαδικτύου, όπως οι επιθέσεις της λίστας Owasp top 10 και έτσι εξασφαλίζεται η εμπιστευτικότητα και η ακεραιότητα. Τα αποτελέσματα είναι ιδιαίτερα ικανοποιητικά καθώς τα ⅔ των προϊόντων καλύπτουν και τις τρεις ιδιότητες ασφαλείας. Νικητήρια είναι τα προϊόντα που καλύπτουν και τις τρεις ιδιότητες (δείτε πίνακα αποτίμησης).

Προστατευόμενα αντικείμενα: Όλα τα προϊόντα (100%) προστατεύουν τις διαδικτυακές εφαρμογές. 9 προϊόντα (60%) προστατεύουν τις διεπαφές προγραμματισμού εφαρμογών (APIs). 1 προϊόν (6.6%) προστατεύει τις ιστοσελίδες. Αν δούμε τον αριθμό αντικειμένων ανά προϊόν, 9 προϊόντα (60%) προστατεύουν δύο αντικείμενα, 2 προϊόντα (13.3%) προστατεύουν 3 αντικείμενα και 4 προϊόντα (26.6%) προστατεύουν 1 αντικείμενο.

Τα αποτελέσματα είναι ικανοποιητικά καθώς πάνω από τα ⅔ των προϊόντων προστατεύουν δύο ή περισσότερα αντικείμενα. Νικητήρια προϊόντα είναι τα Penta Security - WAPPLES SA (WAF) και Barracuda CloudGen WAF, τα οποία προστατεύουν 3 αντικείμενα. Στα παραπάνω αποτελέσματα υπάρχει διαφοροποίηση ανάλογα με τον τρόπο που εκτελείται μια εφαρμογή. Πιο συγκεκριμένα, η διαφοροποίηση στηρίζεται στο ότι οι εφαρμογές μπορεί να εκτελούνται είτε στο κινητό τηλέφωνο είτε στον φυλλομετρητή οποιασδήποτε συσκευής.

Αντιμετωπιζόμενες απειλές: Όλα τα προϊόντα (100%) προσφέρουν εν γένει προστασία για απειλές διαδικτύου και διαδικτυακών εφαρμογών. Οι απειλές αυτές είναι πάρα πολλές και συνεχώς δημιουργούνται νέες γι' αυτό δεν μπορούν να προσδιοριστούν με ακρίβεια. Οι πιο σημαντικές είναι: shellcode, απόξεση ιστού, γέμισμα διαπιστευτηρίων, κατάληψη λογαριασμών, κλοπή δεδομένων, απομακρυσμένη εκτέλεση κώδικα και ανίχνευση σαρωτών, οι οποίες εμφανίστηκαν σε 4 προϊόντα. Παραβίαση/δηλητηρίαση cookie ή φορμών και επιθέσεις σε APIs που εμφανίστηκαν σε 5 προϊόντα. Επιθέσεις μηδενικής μέρας, επιθέσεις έγχυσης (κώδικα, ιστού, LDAP/Xpath, server side) και επιθέσεις bots που εμφανίστηκαν σε 6 προϊόντα. Οι επιθέσεις που συμπεριλαμβάνονται στη λίστα Owasp top 10 που εμφανίστηκαν σε 8 προϊόντα. Οι επιθέσεις άρνησης και κατανεμημένης άρνησης εξυπηρέτησης που εμφανίστηκαν σε 10 προϊόντα. Οι επιθέσεις έγχυσης κώδικα sql που εμφανίστηκαν σε 11 προϊόντα και τέλος οι επιθέσεις cross site scripting (xss) που εμφανίστηκαν σε 12 προϊόντα.

Σχετικά με τον αριθμό απειλών ανά προϊόν 6 προϊόντα (40%) καλύπτουν 3 έως 9 απειλές. 5 προϊόντα (33.3%) καλύπτουν 10 έως 14 απειλές και 4 προϊόντα (26.6%) καλύπτουν από 15 έως 19 απειλές. Στην καταμέτρηση οι απειλές της λίστας Owasp top 10 μετρήθηκαν σαν μία απειλή. Νικητήρια είναι τα προϊόντα Penta Security - WAPPLES SA (WAF) και MONITORAPP AIWAF-VE for Azure με 18 και 19 απειλές αντίστοιχα. Τα αποτελέσματα είναι αρκετά ικανοποιητικά διότι καλύπτεται μεγάλος αριθμός απειλών από τα προϊόντα.

Περιορισμοί χρήσης: Βρέθηκαν πληροφορίες σε 5 προϊόντα. Σε 1 προϊόν (6.6%) στη μέγιστη έκδοση υποστηρίζεται ρυθμοαποδοση (throughput) έως 750 mbps και έως 14.000 συνδέσεις/αιτήματα http ανά δευτερόλεπτο. Σε 1 προϊόν (6.6%) στη μέγιστη έκδοση υποστηρίζεται ρυθμοαποδοση (throughput) έως 1 gbps και σε ένα 1 προϊόν (6.6%) έως 6 gbps. Σε 1 προϊόν (6.6%) στη μέγιστη έκδοση υποστηρίζονται έως 300 εκατομμύρια αιτήματα ανά μήνα. Σε 1 προϊόν (6.6%) στη μέγιστη έκδοση υποστηρίζεται ρυθμοαπόδοση (throughput) έως 2.5 gbps και έως 100 χιλιάδες συναλλαγές (transactions) ανά δευτερόλεπτο. Οι περιορισμοί είναι φυσιολογικοί διότι πρόκειται για κάποια όρια σχετικά με τη λειτουργία των προϊόντων. Τα αποτελέσματα δεν είναι ικανοποιητικά καθώς βρέθηκαν πληροφορίες μόνο στο ⅓ των προϊόντων.

Δοκιμαστικές εκδόσεις: 2 προϊόντα (13.3%) διαθέτουν δωρεάν δοκιμαστική έκδοση χωρίς να αναφέρεται χρονική διάρκεια. 2 προϊόντα (13.3%) διαθέτουν δωρεάν δοκιμαστική έκδοση 14 ημερών. 7 προϊόντα (46.6%) διαθέτουν δωρεάν δοκιμαστική έκδοση 30 ημερών και τέλος 4 προϊόντα (26.6) δεν διαθέτουν κάποια δοκιμαστική έκδοση. Τα αποτελέσματα είναι κάπως ικανοποιητικά διότι σχεδόν τα μισά προϊόντα διαθέτουν δωρεάν δοκιμαστική έκδοση 30 ημερών.

Τρόπος χρήσης: 10 προϊόντα (66.6%) υποστηρίζουν το γραφικό περιβάλλον εργασίας μέσω διαδικτύου. 8 προϊόντα (53.3%) υποστηρίζουν χρήση γραμμής εντολών και 11 προϊόντα (73.3%) υποστηρίζουν διεπαφή προγραμματισμού εφαρμογών μεταφοράς αναπαραστατικής κατάστασης. Αν δούμε τον αριθμό τεχνολογιών ανά προϊόν 4 προϊόντα (26.6%) υποστηρίζουν μία τεχνολογία, 5 προϊόντα (33.3%)

υποστηρίζουν δύο τεχνολογίες και 5 προϊόντα (33.3%) υποστηρίζουν και τις τρεις τεχνολογίες. Τα προϊόντα τα οποία υποστηρίζουν και τις τρεις τεχνολογίες (δείτε πίνακα αποτίμησης) είναι τα νικητήρια. Τα αποτελέσματα είναι ικανοποιητικά διότι τα 2/3 των προϊόντων υποστηρίζουν δύο ή περισσότερες τεχνολογίες.

Αγορές: 13 προϊόντα (86.6%) εντοπίστηκαν στο Microsoft Azure, 12 προϊόντα (80%) εντοπίστηκαν στο Amazon web services και 6 προϊόντα (40%) εντοπίστηκαν στο Google cloud platform. Αν δούμε τον αριθμό αγορών ανά προϊόν, 4 προϊόντα (26.6%) εντοπίστηκαν σε δύο αγορές, 5 προϊόντα (33.3%) εντοπίστηκαν σε μία αγορά ενώ 6 προϊόντα (40%) εντοπίστηκαν και στις τρεις αγορές. Τα προϊόντα αυτά (δείτε πίνακα αποτίμησης) είναι και τα νικητήρια. Τα αποτελέσματα είναι αρκετά ικανοποιητικά καθώς όλα τα προϊόντα βρέθηκαν στις αγορές με τα ⅔ των προϊόντων να εντοπίζονται σε δύο ή περισσότερες αγορές.

Επίπεδο/είδος υποστήριξης: Σχετικά με τα είδη υποστήριξης, όλα τα προϊόντα (100%) προσφέρουν επικοινωνία μέσω email, 14 προϊόντα (93.3%) μέσω τηλεφώνου, 8 προϊόντα (53.3%) μέσω δελτίων (tickets) και 4 προϊόντα (26.6%) μέσω μηνυμάτων (chat). 12 προϊόντα (80%) διαθέτουν υποστηρικτικό υλικό (έγγραφα με πληροφορίες, βίντεο, FAQ). 2 προϊόντα (13.3%) διαθέτουν εκπαιδευτικό υλικό. 14 προϊόντα (93.3%) διαθέτουν υποστήριξη κοινοτήτων χρηστών (κοινότητα, φόρουμ, blog). 10 προϊόντα (66.6%) διαθέτουν τεκμηρίωση. 2 προϊόντα (13.3%) διαθέτουν ενημερώσεις. 5 προϊόντα (33.3%) διαθέτουν κέντρο βοήθειας και 3 προϊόντα (20%) διαθέτουν βάση γνώσης. 3 προϊόντα (20%) διαθέτουν πύλη υποστήριξης, 2 προϊόντα (13.3%) διαθέτουν κανάλι στο μέσο κοινωνικής δικτύωσης slack, ενώ 2 προϊόντα (13.3%) διαθέτουν ενημέρωση για συνδρομές, κέντρο γνώσης και λεξικό.
Σχετικά με την ύπαρξη πακέτων 3 προϊόντα (20%) διαθέτουν 3 πακέτα, 2 προϊόντα (13.3%) διαθέτουν 5 πακέτα και 1 προϊόν (6.6%) διαθέτει 2 πακέτα.
Σχετικά με τη χρονική συνιστώσα 8 προϊόντα (53.3%) διαθέτουν υποστήριξη 24/7 και 2 προϊόντα (13.3%) διαθέτουν υποστήριξη από 9/5 έως 24/7.
Τα αποτελέσματα δεν είναι ιδιαίτερα ικανοποιητικά διότι μόνο 6 προϊόντα διαθέτουν διαφορετικά πακέτα. Βέβαια, το γεγονός πως πάνω από τα μισά προϊόντα διαθέτουν υποστήριξη 24/7 είναι ικανοποιητικό. Νικητήριο προϊόν είναι το Big WAF, το οποίο διαθέτει 5 πακέτα και υποστήριξη 24/7 στα 4 από τα 5 πακέτα του.

Νικητήριο προϊόν για ολόκληρη την κατηγορία είναι το Penta Security - WAPPLES SA (WAF), το οποίο εμφανίζεται ως νικητήριο 6 φορές

5.3 Συνολικά στατιστικά στοιχεία

Πριν προχωρήσουμε στην παροχή & ανάλυση καθολικών στατιστικών στοιχείων, επιθυμούμε να τονίσουμε το εξής. Ορισμένες φορές δεν ήταν δυνατό να αποτιμήσουμε ορισμένα προϊόντα με βάση κάποιο

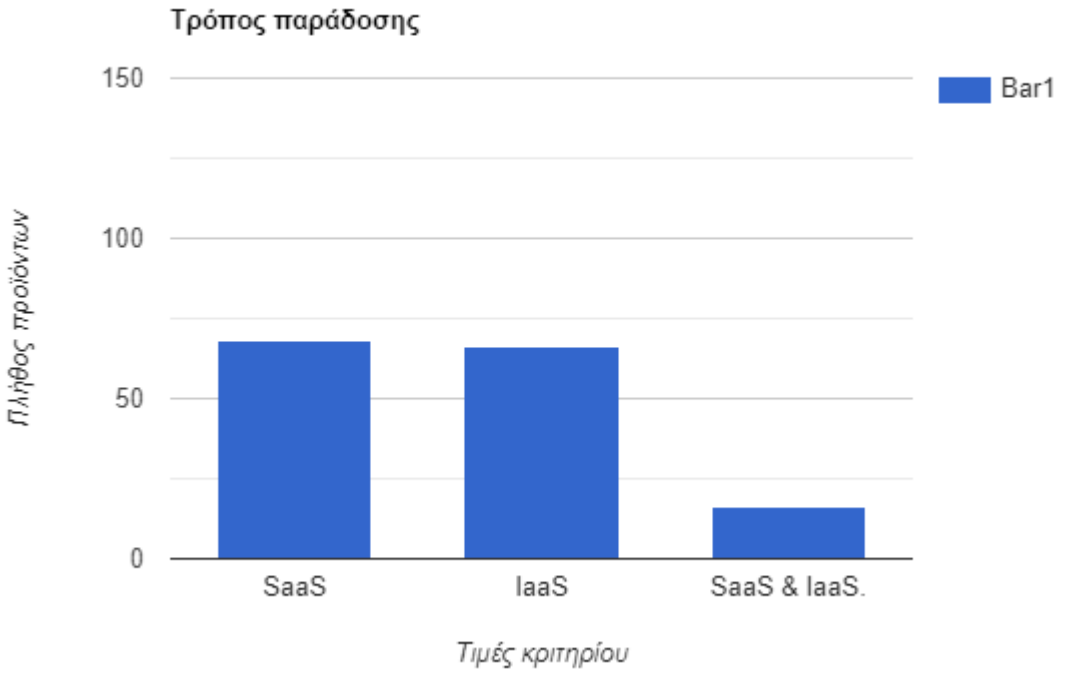
κριτήριο λόγω έλλειψης πληροφορίας. Για αυτό και το άθροισμα των προϊόντων με τις διαφορετικές τιμές αποτίμησης μπορεί να είναι μικρότερο από 150.

5.3.1 Τρόπος παράδοσης

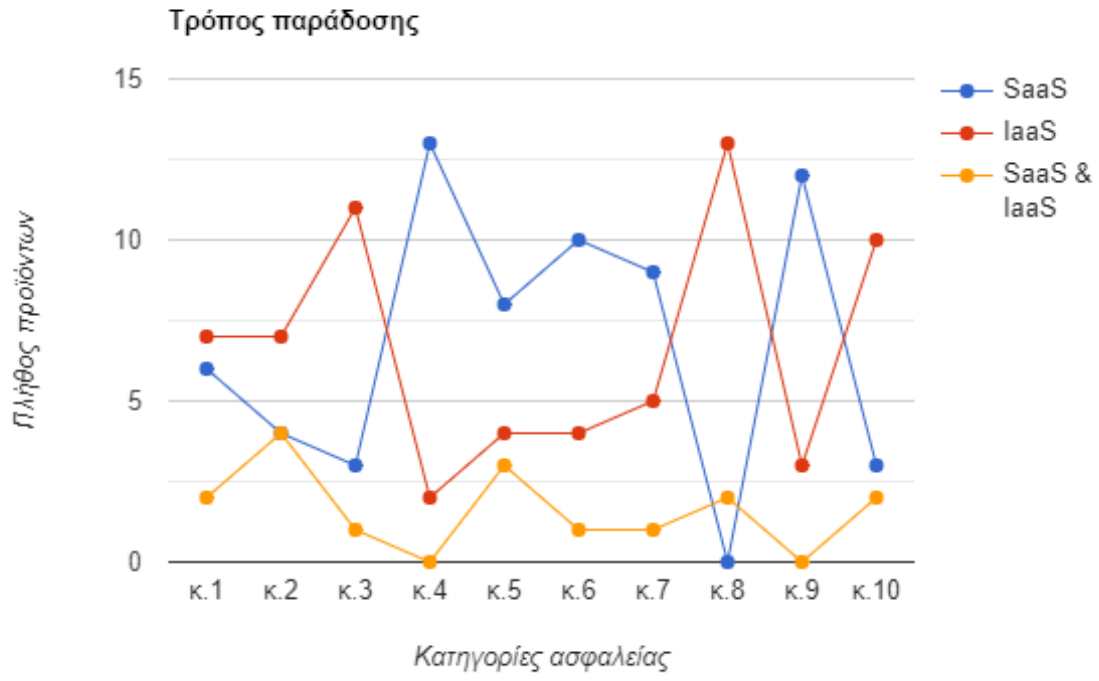
Οι τιμές που προέκυψαν κατά τη διάρκεια της έρευνας για αυτό το κριτήριο ήταν 1.SaaS, 2. IaaS, 3. SaaS & IaaS. Τα συνολικά αποτελέσματα είναι τα εξής:

- Σε σύνολο 150 προϊόντων η τιμή (μόνο) SaaS εμφανίστηκε 68 φορές (45.3%). Συνεπώς, εφόσον έχουμε 10 κατηγορίες, ο μέσος όρος εμφάνισης (μόνο) SaaS προϊόντων είναι 6.8 φορές στην κάθε κατηγορία. Η μέγιστη τιμή εμφάνισης σε μία κατηγορία ήταν 13 φορές (86.6%) και η ελάχιστη τιμή εμφάνισης σε μία κατηγορία ήταν 0 φορές (0%).
- Σε σύνολο 150 προϊόντων η τιμή (μόνο) IaaS εμφανίστηκε 66 φορές (44%). Συνεπώς, εφόσον έχουμε 10 κατηγορίες, ο μέσος όρος εμφάνισης προϊόντων (μόνο) IaaS είναι 6.6 φορές σε κάθε κατηγορία. Η μέγιστη τιμή εμφάνισης σε μία κατηγορία ήταν 13 φορές (86.6%) και η ελάχιστη τιμή εμφάνισης σε μία κατηγορία ήταν 3 φορές (20%).
- Σε σύνολο 150 προϊόντων η τιμή SaaS & IaaS εμφανίστηκε 16 φορές (10.6%). Συνεπώς, εφόσον έχουμε 10 κατηγορίες, ο μέσος όρος εμφάνισης προϊόντων SaaS & IaaS είναι 1.6 φορά σε κάθε κατηγορία. Η μέγιστη τιμή εμφάνισης σε μία κατηγορία ήταν 4 φορές (26.6%) και η ελάχιστη τιμή εμφάνισης σε μία κατηγορία ήταν 0 φορές (0%).

Παρατηρούμε πως οι δύο τρόποι παράδοσης είναι σχεδόν ισοδύναμοι αλλά ο συνδυασμός τους δεν υποστηρίζεται σε ικανοποιητικό βαθμό. Τα αποτελέσματα δεν είναι ικανοποιητικά διότι μόνο σχεδόν το 10% των προϊόντων υποστηρίζει δύο τρόπους παράδοσης



Εικόνα 5. Πλήθος προϊόντων που υποστηρίζει τον κάθε τρόπο παράδοσης



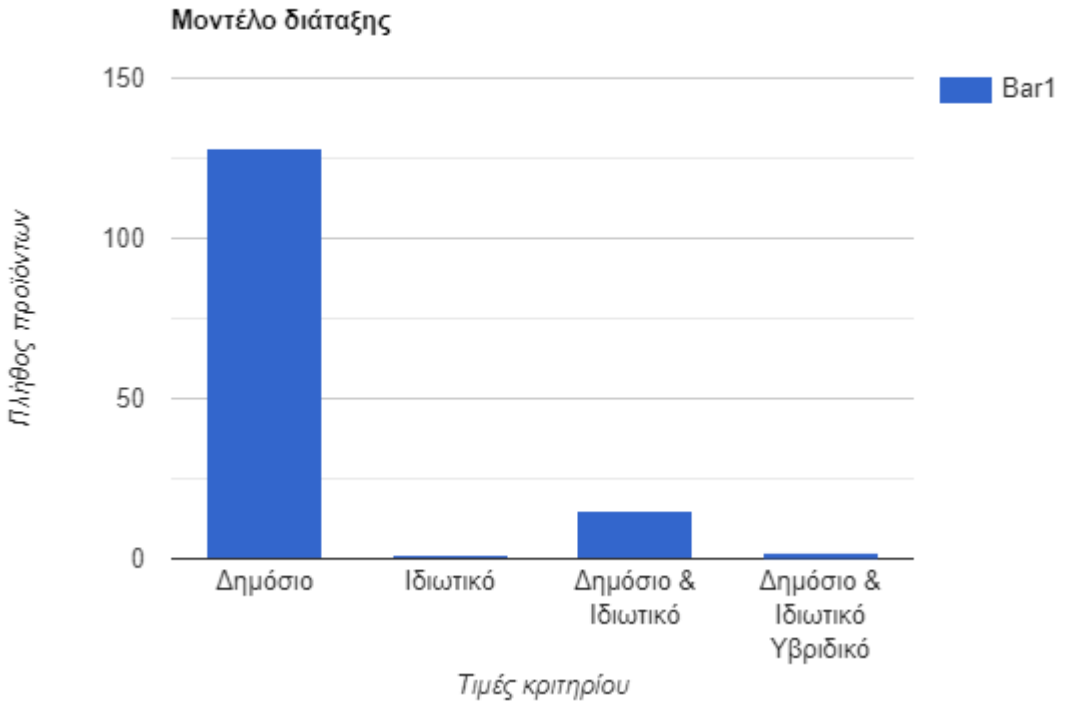
Εικόνα 4. Πλήθος προϊόντων ανά τρόπο παράδοσης και κατηγορία προϊόντων

5.3.2 Μοντέλο διάταξης

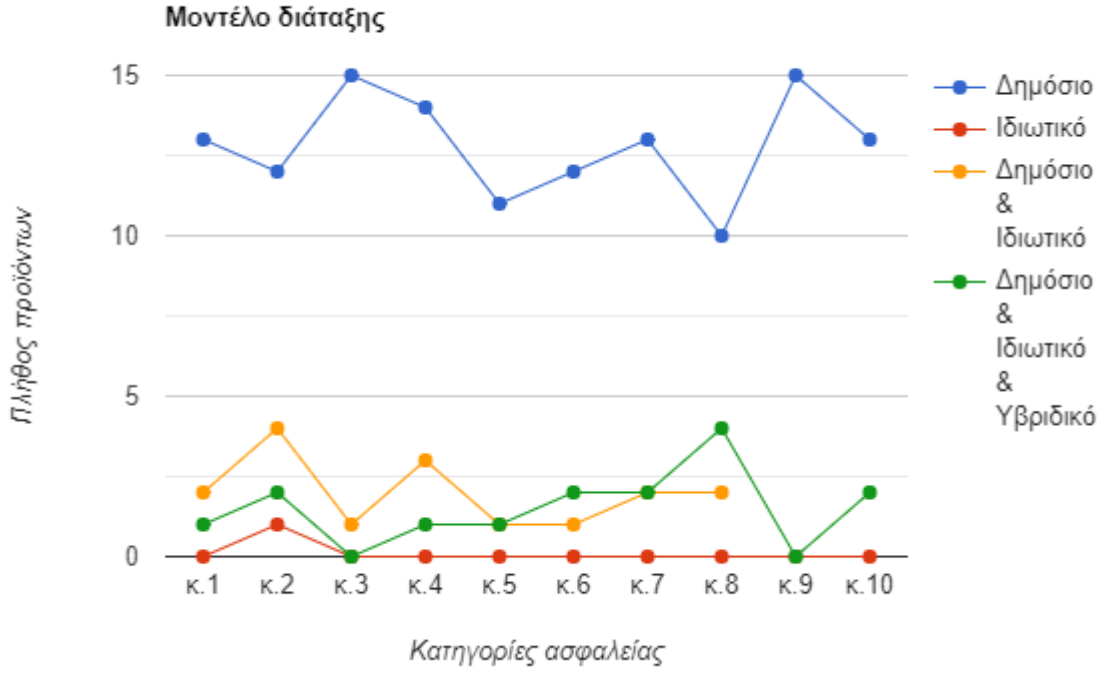
Οι τιμές που προέκυψαν κατά τη διάρκεια της έρευνας για αυτό το κριτήριο ήταν 1.ιδιωτικό νέφος, 2. δημόσιο νέφος, 3. δημόσιο & ιδιωτικό νέφος, και 4. δημόσιο & ιδιωτικό & υβριδικό νέφος. Τα συνολικά αποτελέσματα είναι τα εξής:

- Σε σύνολο 146 προϊόντων η τιμή (μόνο) ιδιωτικό νέφος εμφανίστηκε 1 φορά (0.7%). Συνεπώς, εφόσον έχουμε 10 κατηγορίες, ο μέσος όρος εμφάνισης προϊόντων μόνο ιδιωτικού νέφους είναι 0.1 φορές σε κάθε κατηγορία. Η μέγιστη τιμή εμφάνισης σε μία κατηγορία ήταν 1 φορά (6.6%) και η ελάχιστη τιμή εμφάνισης σε μία κατηγορία ήταν 0 φορές (0%).
- Σε σύνολο 146 προϊόντων η τιμή (μόνο) δημόσιο νέφος εμφανίστηκε 128 φορές (87.7%). Συνεπώς, εφόσον έχουμε 10 κατηγορίες, ο μέσος όρος εμφάνισης προϊόντων μόνο δημοσίου νέφους είναι 12.8 φορές σε κάθε κατηγορία. Η μέγιστη τιμή εμφάνισης σε μία κατηγορία ήταν 15 φορές (100%) και η ελάχιστη τιμή εμφάνισης σε μία κατηγορία ήταν 10 φορές (66.6%).
- Σε σύνολο 146 προϊόντων η τιμή (μόνο) υβριδικό νέφος εμφανίστηκε 0 φορές (0%).
- Σε σύνολο 146 προϊόντων, η τιμή δημόσιο & ιδιωτικό νέφος εμφανίστηκε 15 φορές (10.2%). Συνεπώς, εφόσον έχουμε 10 κατηγορίες, ο μέσος όρος εμφάνισης προϊόντων δημόσιου & ιδιωτικού νέφους είναι 1.5 φορές σε κάθε κατηγορία. Η μέγιστη τιμή εμφάνισης σε μία κατηγορία ήταν 4 φορές (26.6%) και η ελάχιστη τιμή εμφάνισης σε μία κατηγορία ήταν 0 φορές (0%).
- Σε σύνολο 146 προϊόντων η τιμή δημόσιο & ιδιωτικό & υβριδικό νέφος εμφανίστηκε 2 φορές (1.4%). Συνεπώς, εφόσον έχουμε 10 κατηγορίες, ο μέσος όρος εμφάνισης προϊόντων ιδιωτικού νέφους είναι 0.2 φορές σε κάθε κατηγορία. Η μέγιστη και η ελάχιστη τιμή εμφάνισης σε μία κατηγορία ήταν 1 φορά (6.6%).

Παρατηρούμε πως με μεγάλη διαφορά έρχεται πρώτο σε προτίμηση το δημόσιο νέφος. Στη συνέχεια ακολουθεί το δημόσιο & ιδιωτικό νέφος. Τέλος, το ιδιωτικό νέφος και ο συνδυασμός των τριών νεφών εμφανίζονται μόνο μία και δύο φορές αντίστοιχα. Τα αποτελέσματα δεν είναι ικανοποιητικά διότι περίπου μόνο το 10% των προϊόντων υποστηρίζει δύο η περισσότερα μοντέλα διάταξης.



Εικόνα 6. Πλήθος προϊόντων που υποστηρίζουν τις διαφορετικές τιμές για το μοντέλο διάταξης



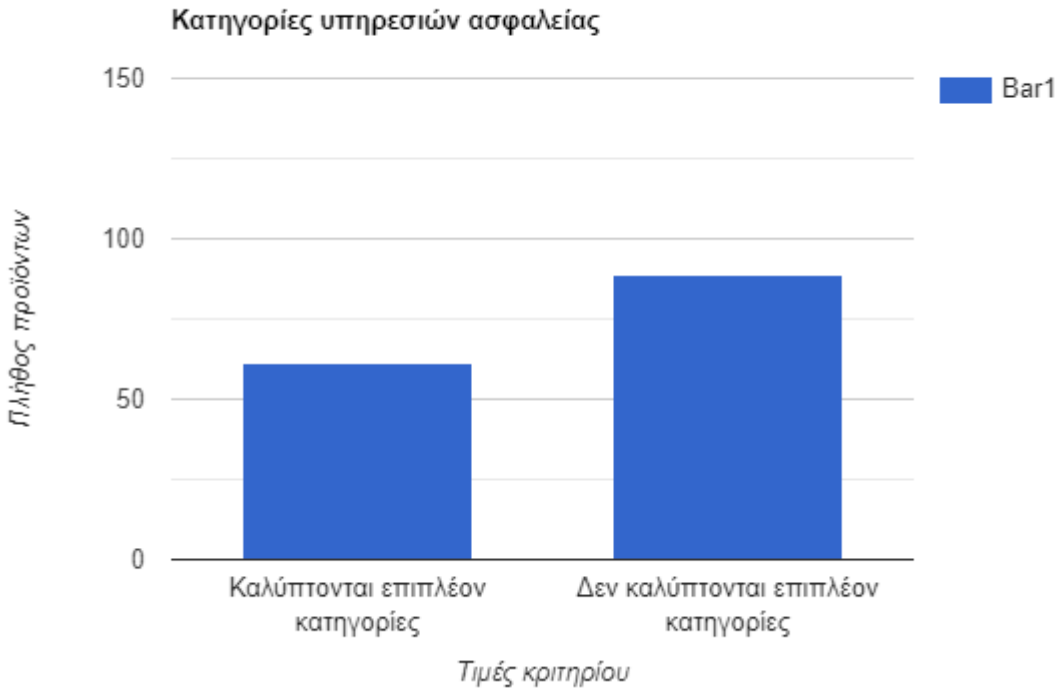
Εικόνα 7. Πλήθος προϊόντων ανά τιμή του μοντέλου διάταξης και κατηγορία προϊόντων

5.3.3 Κατηγορίες ασφαλείας

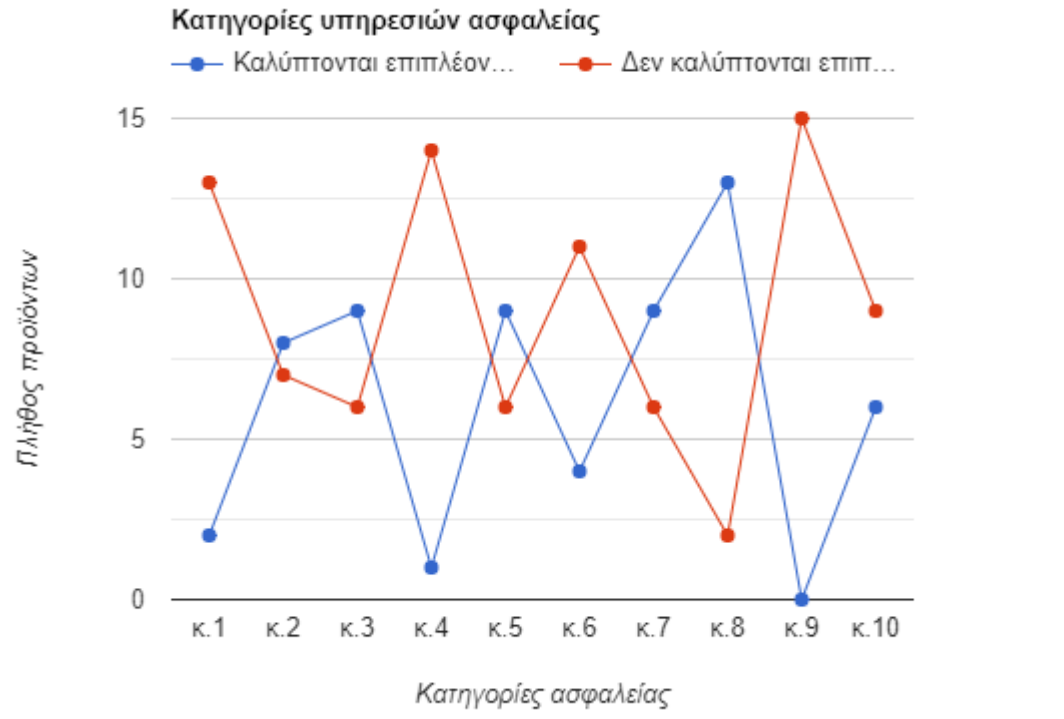
Αυτό το κριτήριο λόγω της φύσης των αποτελεσμάτων δεν διαθέτει διακριτές τιμές. Γι΄αυτό θεωρούμε πως υπάρχουν οι δύο παρακάτω τιμές: 1. προϊόντα που καλύπτουν επιπλέον κατηγορίες ασφαλείας και 2. προϊόντα που δεν καλύπτουν επιπλέον κατηγορίες ασφαλείας. Τα συνολικά αποτελέσματα είναι τα εξής:

- Σε σύνολο 150 προϊόντων εντοπίστηκαν 61 προϊόντα (40.7%) που καλύπτουν επιπλέον κατηγορίες ασφαλείας. Συνεπώς, εφόσον έχουμε 10 κατηγορίες, κατά μέσο όρο 6.1 προϊόντα σε κάθε κατηγορία καλύπτουν επιπλέον κατηγορίες ασφαλείας. Ο μεγαλύτερος αριθμός προϊόντων που καλύπτουν επιπλέον κατηγορίες ασφαλείας σε μία κατηγορία ήταν 13 (86.6%) και ο μικρότερος αριθμός προϊόντων που καλύπτουν επιπλέον κατηγορίες ασφαλείας σε μία κατηγορία ήταν 0 (0%).
- Σε σύνολο 150 προϊόντων εντοπίστηκαν 89 προϊόντα (59.3%) που δεν καλύπτουν επιπλέον κατηγορίες ασφαλείας. Συνεπώς, εφόσον έχουμε 10 κατηγορίες, κατά μέσο όρο 8.9 προϊόντα σε κάθε κατηγορία δεν καλύπτουν επιπλέον κατηγορίες ασφαλείας. Ο μεγαλύτερος αριθμός προϊόντων που δεν καλύπτουν επιπλέον κατηγορίες ασφαλείας σε μία κατηγορία ήταν 15 (100%) και ο μικρότερος αριθμός προϊόντων που δεν καλύπτουν επιπλέον κατηγορίες ασφαλείας σε μία κατηγορία ήταν 2 (13.3%).

Παρατηρούμε πως σχεδόν τα ⅖ των προϊόντων καλύπτουν επιπλέον κατηγορίες ασφαλείας ενώ τα ⅗ των προϊόντων δεν καλύπτουν κάποια επιπλέον κατηγορία ασφαλείας. Το αποτέλεσμα αυτό είναι οριακά μη ικανοποιητικό.



Εικόνα 8. Πλήθος προϊόντων που είτε καλύπτουν επιπλέον κατηγορίες ασφάλειας είτε όχι



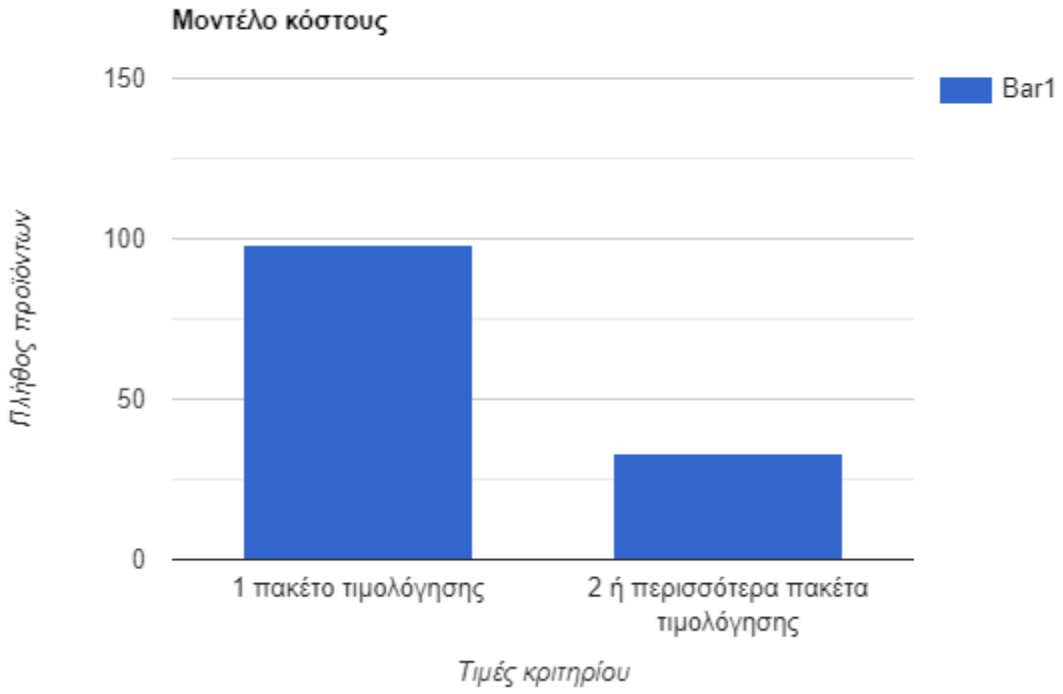
Εικόνα 8. Πλήθος προϊόντων ανά κατηγορία που είτε καλύπτουν είτε δεν καλύπτουν έξτρα κατηγορίες ασφάλειας

5.3.4 Μοντέλο κόστους

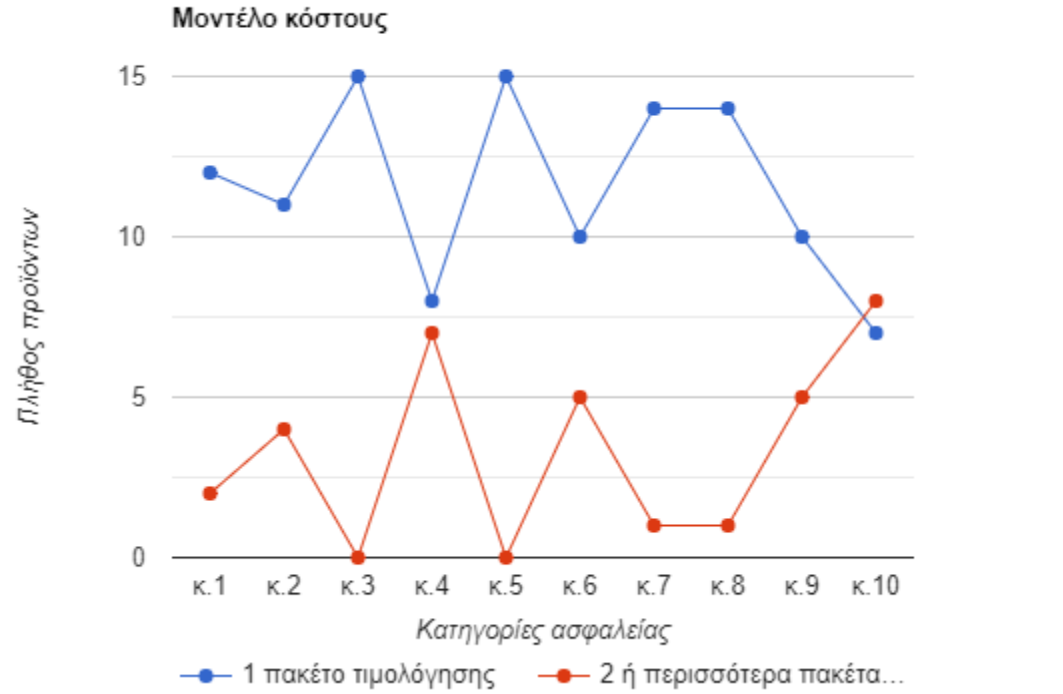
Αυτό το κριτήριο λόγω της φύσης των αποτελεσμάτων δεν διαθέτει διακριτές τιμές. Γι΄αυτό θεωρούμε πως υπάρχουν οι δύο παρακάτω τιμές: 1. προϊόντα με 2 ή περισσότερα πακέτα τιμολόγησης και 2. προϊόντα με 1 πακέτο τιμολόγησης. Τα συνολικά αποτελέσματα είναι τα εξής:

- Σε σύνολο 131 προϊόντων εντοπίστηκαν 33 προϊόντα (25.2%) με 2 ή περισσότερα πακέτα τιμολόγησης. Συνεπώς, εφόσον έχουμε 10 κατηγορίες, κατά μέσο όρο 3.3 προϊόντα σε κάθε κατηγορία διαθέτουν 2 ή περισσότερα πακέτα τιμολόγησης. Ο μεγαλύτερος αριθμός προϊόντων με 2 ή περισσότερα πακέτα τιμολόγησης σε μία κατηγορία ήταν 8 (53.3%) και ο μικρότερος αριθμός προϊόντων με 2 ή περισσότερα πακέτα τιμολόγησης σε μία κατηγορία ήταν 0 (0%).
- Σε σύνολο 131 προϊόντων εντοπίστηκαν 98 προϊόντα (74.8%) με 1 πακέτο τιμολόγησης. Συνεπώς, εφόσον έχουμε 10 κατηγορίες, κατά μέσο όρο 9.8 προϊόντα σε κάθε κατηγορία διαθέτουν 1 πακέτο τιμολόγησης. Ο μεγαλύτερος αριθμός προϊόντων με 1 πακέτο τιμολόγησης σε μία κατηγορία ήταν 15 (100%) και ο μικρότερος αριθμός προϊόντων με 1 πακέτο τιμολόγησης σε μία κατηγορία ήταν 5 (33.3%).

Παρατηρούμε ότι μόνο το ¼ των προϊόντων διαθέτει δύο ή περισσότερα πακέτα τιμολόγησης, ενώ τα ¾ των προϊόντων διαθέτουν μόνο ένα πακέτο τιμολόγησης. Επιπλέον ένας σεβαστός αριθμός προϊόντων (19 προϊόντα) δεν διαθέτουν καμία πληροφορία τιμολόγησης. Το αποτέλεσμα δεν είναι ικανοποιητικό.



Εικόνα 10. Πλήθος προϊόντων με είτε 1 είτε 2 ή περισσότερα πακέτα τιμολόγησης



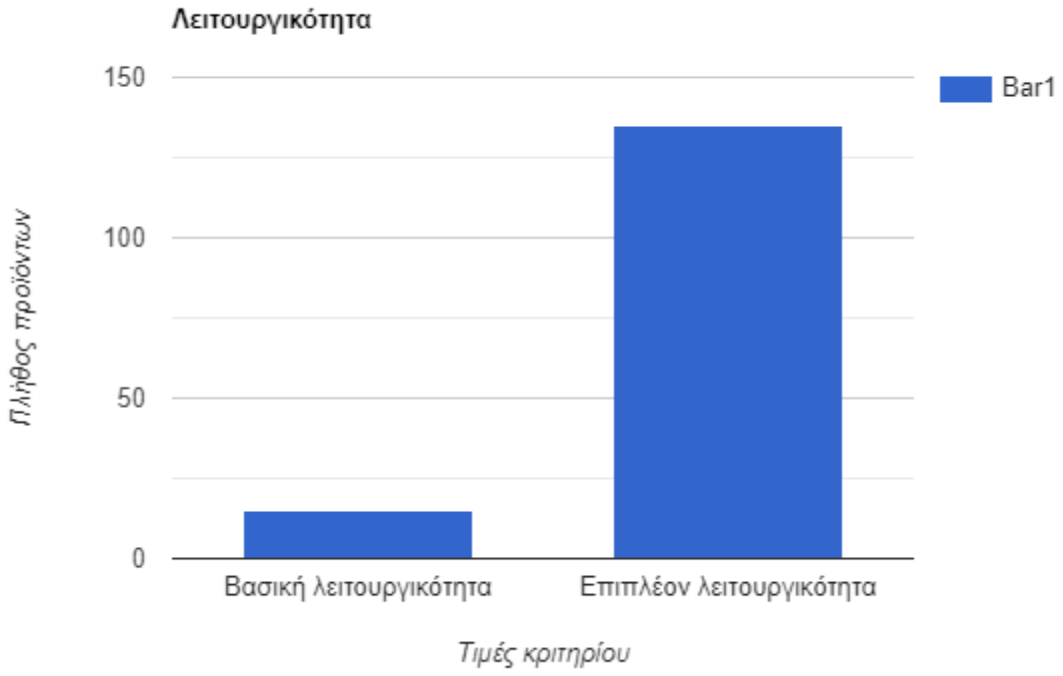
Εικόνα 9. Πλήθος προϊόντων ανά κατηγορία με είτε 1 είτε 2 ή περισσότερα πακέτα τιμολόγησης

5.3.5 Μηχανισμοί / Λειτουργικότητα Ασφάλειας

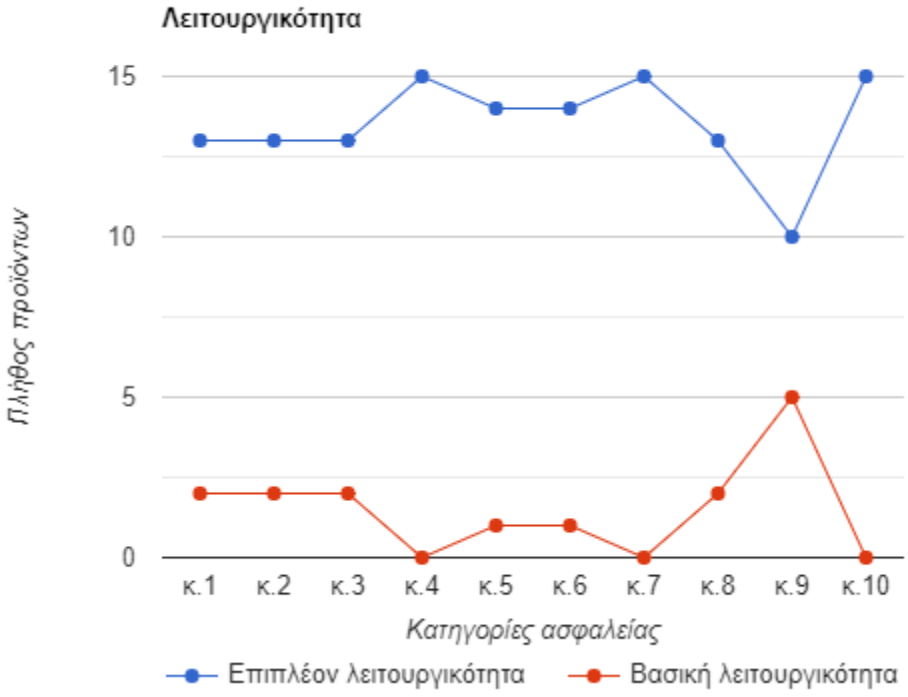
Αυτό το κριτήριο λόγω της φύσης των αποτελεσμάτων δεν διαθέτει διακριτές τιμές. Γι΄αυτό θεωρούμε πως υπάρχουν οι δύο παρακάτω τιμές: 1. προϊόντα που καλύπτουν μόνο τη βασική λειτουργικότητα και 2. προϊόντα που καλύπτουν επιπλέον λειτουργικότητα. Τα συνολικά αποτελέσματα είναι τα εξής:

- Σε σύνολο 150 προϊόντων εντοπίστηκαν 135 προϊόντα (90%), τα οποία καλύπτουν επιπλέον λειτουργικότητα. Συνεπώς, εφόσον έχουμε 10 κατηγορίες, κατά μέσο όρο 13.5 προϊόντα σε κάθε κατηγορία καλύπτουν επιπλέον λειτουργικότητα. Ο μεγαλύτερος αριθμός προϊόντων τα οποία καλύπτουν επιπλέον λειτουργικότητα σε μία κατηγορία ήταν 15 (100%) και ο μικρότερος αριθμός προϊόντων τα οποία καλύπτουν επιπλέον λειτουργικότητα σε μία κατηγορία ήταν 10 (66.6%).
- Σε σύνολο 150 προϊόντων εντοπίστηκαν 15 προϊόντα (10%), τα οποία καλύπτουν μόνο τη βασική λειτουργικότητα. Συνεπώς, εφόσον έχουμε 10 κατηγορίες, κατά μέσο όρο 1.5 προϊόντα σε κάθε κατηγορία καλύπτουν μόνο τη βασική λειτουργικότητα. Ο μεγαλύτερος αριθμός προϊόντων τα οποία καλύπτουν μόνο τη βασική λειτουργικότητα σε μία κατηγορία ήταν 5 (33.3%) και ο μικρότερος αριθμός προϊόντων τα οποία καλύπτουν μόνο τη βασική λειτουργικότητα σε μία κατηγορία ήταν 0 (0%).

Παρατηρούμε πως τα περισσότερα προϊόντα (90%) καλύπτουν και βασική και επιπλέον λειτουργικότητα. Το αποτέλεσμα αυτό είναι ιδιαίτερα ικανοποιητικό.



Εικόνα 11. Πλήθος προϊόντων που παρέχουν είτε μόνο βασική είτε και έξτρα λειτουργικότητα



Εικόνα 12. Πλήθος προϊόντων ανά κατηγορία που παρέχουν είτε μόνο βασική είτε και έξτρα λειτουργικότητα

5.3.6 Μη λειτουργικές εγγυήσεις

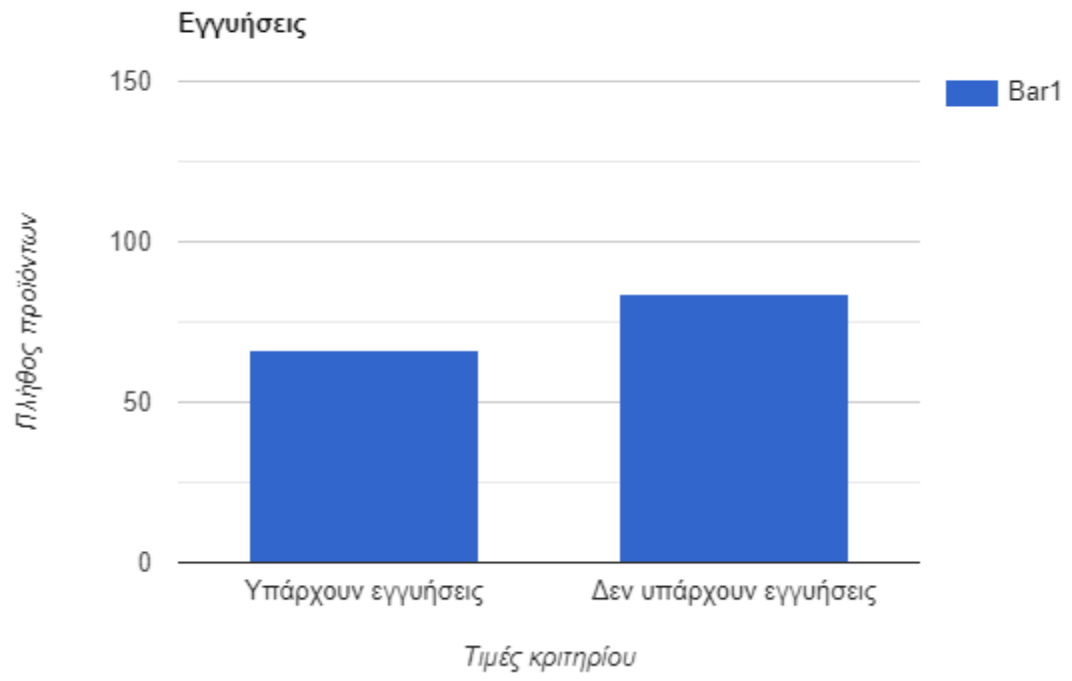
Αυτό το κριτήριο λόγω της φύσης των αποτελεσμάτων δεν διαθέτει διακριτές τιμές. Γι΄αυτό θεωρούμε πως υπάρχουν οι δύο παρακάτω τιμές: 1. προϊόντα που διαθέτουν εγγυήσεις και 2. προϊόντα που δεν διαθέτουν εγγυήσεις. Τα συνολικά αποτελέσματα είναι τα εξής:

- Σε σύνολο 150 προϊόντων εντοπίστηκαν 66 προϊόντα (44%), τα οποία διαθέτουν μη λειτουργικές εγγυήσεις. Συνεπώς, εφόσον έχουμε 10 κατηγορίες, κατά μέσο όρο 4.4 προϊόντα σε κάθε κατηγορία διαθέτουν μη λειτουργικές εγγυήσεις. Ο μεγαλύτερος αριθμός προϊόντων τα οποία διαθέτουν μη λειτουργικές εγγυήσεις σε μία κατηγορία ήταν 14 (93.3%) και ο μικρότερος αριθμός προϊόντων τα οποία διαθέτουν μη λειτουργικές εγγυήσεις σε μία κατηγορία ήταν 1 (6.6%).
    - Σε σύνολο 66 προϊόντων τα οποία διαθέτουν εγγυήσεις, τα 44 από αυτά (66.6%) δεν διαθέτουν συστήματα ποινών. Συνεπώς, εφόσον έχουμε 10 κατηγορίες, κατά μέσο όρο 4.4 προϊόντα σε κάθε κατηγορία διαθέτουν μη λειτουργικές εγγυήσεις χωρίς συστήματα ποινών. Ο μεγαλύτερος αριθμός προϊόντων τα οποία διαθέτουν εγγυήσεις χωρίς συστήματα ποινών σε μία κατηγορία ήταν 11 (73.3%) και ο μικρότερος αριθμός προϊόντων τα οποία διαθέτουν εγγυήσεις χωρίς συστήματα ποινών σε μία κατηγορία ήταν 0 (0%).

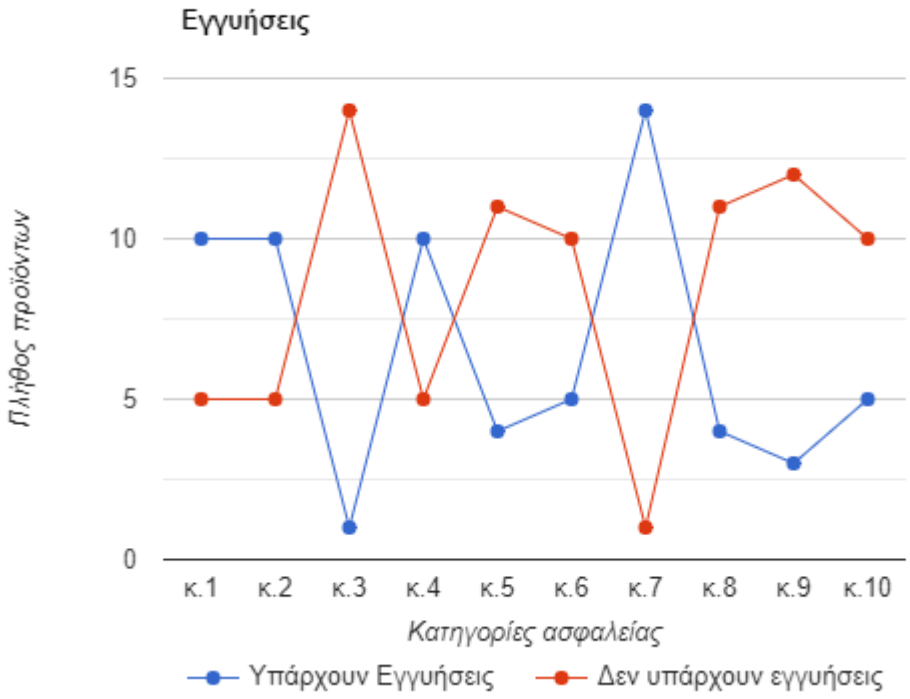
- Σε σύνολο 66 προϊόντων τα οποία διαθέτουν εγγυήσεις, τα 22 από αυτά (33.3%) διαθέτουν συστήματα ποινών. Συνεπώς, εφόσον έχουμε 10 κατηγορίες, κατά μέσο όρο 2.2 προϊόντα σε κάθε κατηγορία διαθέτουν μη λειτουργικές εγγυήσεις με συστήματα ποινών. Ο μεγαλύτερος αριθμός προϊόντων τα οποία διαθέτουν εγγυήσεις με συστήματα ποινών σε μία κατηγορία ήταν 6 (40%) και ο μικρότερος αριθμός προϊόντων τα οποία διαθέτουν εγγυήσεις με συστήματα ποινών σε μία κατηγορία ήταν 0 (0%).

- Σε σύνολο 150 προϊόντων εντοπίστηκαν 84 προϊόντα (56%), τα οποία δεν διαθέτουν μη λειτουργικές εγγυήσεις. Συνεπώς, εφόσον έχουμε 10 κατηγορίες, κατά μέσο όρο 5.6 προϊόντα σε κάθε κατηγορία δεν διαθέτουν μη λειτουργικές εγγυήσεις. Ο μεγαλύτερος αριθμός προϊόντων τα οποία δεν διαθέτουν μη λειτουργικές εγγυήσεις σε μία κατηγορία ήταν 14 (93.3%) και ο μικρότερος αριθμός προϊόντων τα οποία δεν διαθέτουν μη λειτουργικές εγγυήσεις σε μία κατηγορία ήταν 1 (6.6%). Κατά μέσο όρο 5.6 προϊόντα σε κάθε κατηγορία δεν διαθέτουν μη λειτουργικές εγγυήσεις.

Παρατηρούμε πως ως προς την ύπαρξη ή μη ύπαρξη εγγυήσεων τα αποτελέσματα είναι κάπως μοιρασμένα. Επιπλέον, για τα προϊόντα που διαθέτουν εγγυήσεις το ⅓ των προϊόντων διαθέτουν σύστημα ποινών ενώ τα ⅔ δεν διαθέτουν. Ως προς την ύπαρξη ή μη ύπαρξη εγγυήσεων το αποτέλεσμα μπορεί να χαρακτηριστεί ουδέτερο, Ως προς την ύπαρξη συστήματος ποινών το αποτέλεσμα είναι απογοητευτικό.



Εικόνα 13. Πλήθος προϊόντων στα οποία είτε υπάρχουν είτε δεν υπάρχουν εγγυήσεις



Εικόνα 15. Πλήθος προϊόντων ανά κατηγορία στα οποία είτε υπάρχουν είτε δεν υπάρχουν εγγυήσεις

5.3.7 Είδος προσφερόμενης προστασίας

Οι τιμές που προέκυψαν κατά τη διάρκεια της έρευνας για αυτό το κριτήριο ήταν 1.προληπτική προστασία, 2. ανιχνευτική προστασία, 3. αντιδραστική προστασία, 4. προληπτική & αντιδραστική & ανιχνευτική προστασία, 5. προληπτική και ανιχνευτική προστασία, 6. προληπτική και αντιδραστική προστασία. Τα συνολικά αποτελέσματα είναι τα εξής:

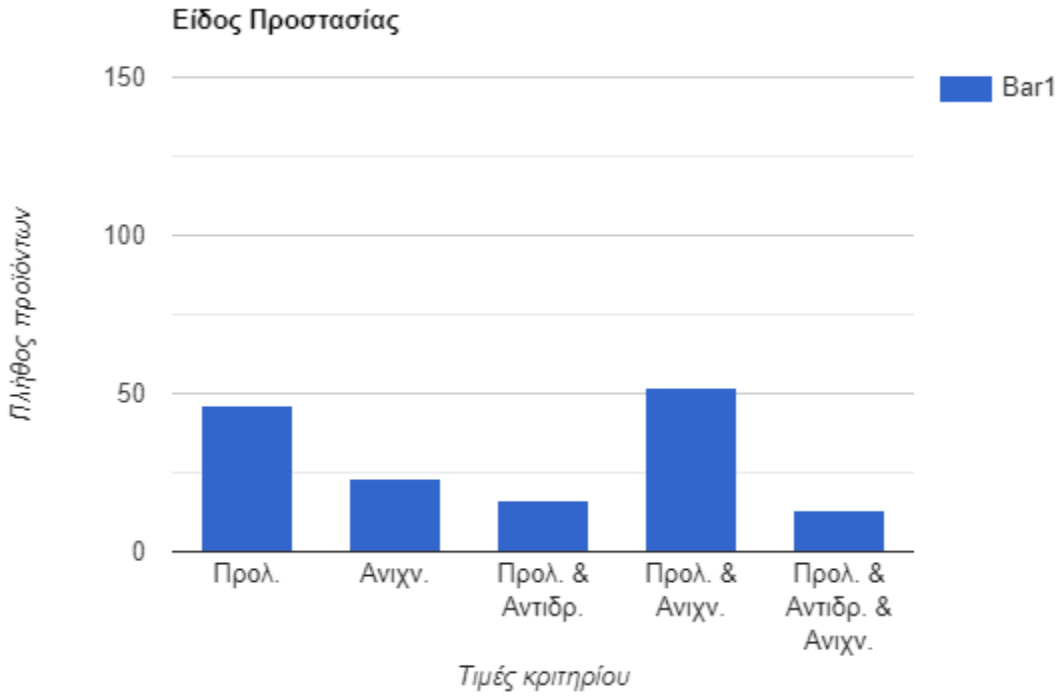
- Σε σύνολο 150 προϊόντων εντοπίστηκαν 46 προϊόντα (30.7%), τα οποία διαθέτουν μόνο προληπτική προστασία. Συνεπώς, εφόσον έχουμε 10 κατηγορίες, κατά μέσο όρο 4.6 προϊόντα σε κάθε κατηγορία διαθέτουν μόνο προληπτική προστασία. Ο μεγαλύτερος αριθμός προϊόντων τα οποία διαθέτουν μόνο προληπτική προστασία σε μία κατηγορία ήταν 15 (100%) και ο μικρότερος αριθμός προϊόντων τα οποία διαθέτουν μόνο προληπτική προστασία σε μία κατηγορία ήταν 0 (0%).
- Σε σύνολο 150 προϊόντων εντοπίστηκαν 23 προϊόντα (15.3%), τα οποία διαθέτουν μόνο ανιχνευτική προστασία. Συνεπώς, εφόσον έχουμε 10 κατηγορίες, κατά μέσο όρο 2.3 προϊόντα σε κάθε κατηγορία διαθέτουν μόνο ανιχνευτική προστασία. Ο μεγαλύτερος αριθμός προϊόντων τα οποία διαθέτουν μόνο ανιχνευτική προστασία σε μία κατηγορία ήταν 15 (100%) και ο μικρότερος

αριθμός προϊόντων τα οποία διαθέτουν μόνο ανιχνευτική προστασία σε μία κατηγορία ήταν 0 (0%).

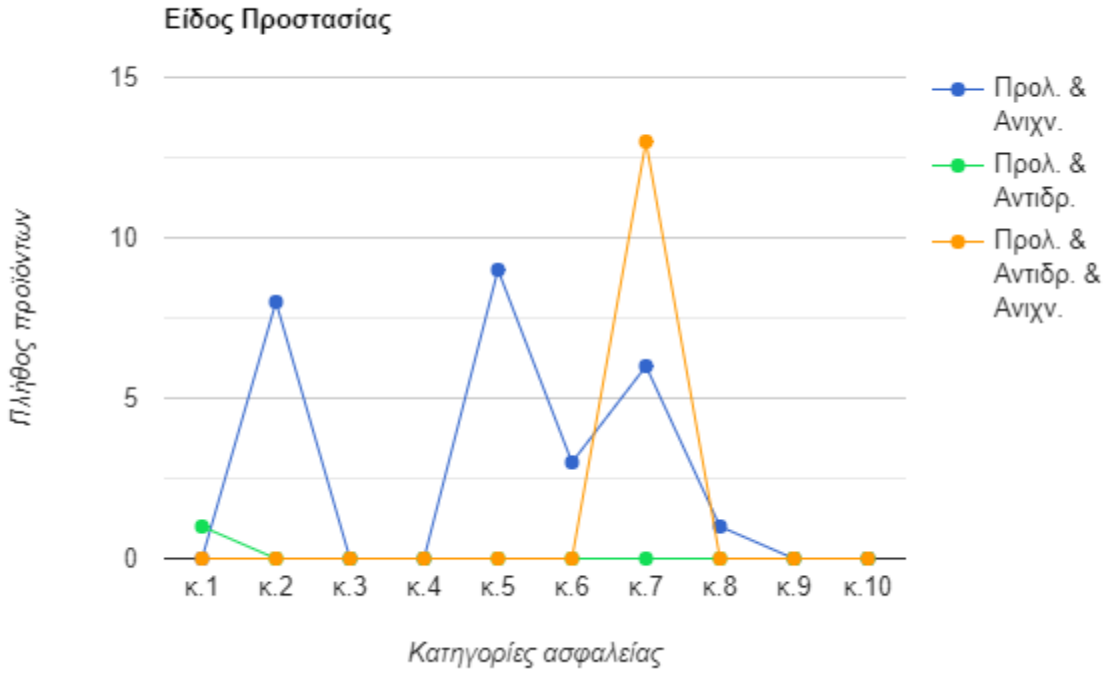
- Σε σύνολο 150 προϊόντων εντοπίστηκαν 0 προϊόντα (0%), τα οποία διαθέτουν μόνο αντιδραστική προστασία.
- Σε σύνολο 150 προϊόντων εντοπίστηκαν 13 προϊόντα (8.7%), τα οποία διαθέτουν προληπτική & αντιδραστική & ανιχνευτική προστασία. Συνεπώς, εφόσον έχουμε 10 κατηγορίες, κατά μέσο όρο 1.3 προϊόντα (8.7%) σε κάθε κατηγορία διαθέτουν προληπτική & αντιδραστική & ανιχνευτική προστασία. Ο μεγαλύτερος αριθμός προϊόντων τα οποία διαθέτουν προληπτική & αντιδραστική & ανιχνευτική σε μία κατηγορία ήταν 13 (86.6%) και ο μικρότερος αριθμός προϊόντων τα οποία διαθέτουν προληπτική & αντιδραστική & ανιχνευτική προστασία σε μία κατηγορία ήταν 0 (0%).
- Σε σύνολο 150 προϊόντων εντοπίστηκαν 16 προϊόντα (10.6%), τα οποία διαθέτουν προληπτική & αντιδραστική προστασία. Συνεπώς, εφόσον έχουμε 10 κατηγορίες, κατά μέσο όρο 1.6 προϊόντα σε κάθε κατηγορία διαθέτουν προληπτική & αντιδραστική προστασία. Ο μεγαλύτερος αριθμός προϊόντων τα οποία διαθέτουν προληπτική & αντιδραστική προστασία σε μία κατηγορία ήταν 15 (86.6%) και ο μικρότερος αριθμός προϊόντων τα οποία διαθέτουν προληπτική & αντιδραστική & προστασία σε μία κατηγορία ήταν 0 (0%).
- Σε σύνολο 150 προϊόντων εντοπίστηκαν 52 προϊόντα (34.6%), τα οποία διαθέτουν προληπτική & ανιχνευτική προστασία. Συνεπώς, εφόσον έχουμε 10 κατηγορίες, κατά μέσο όρο 5.2 προϊόντα σε κάθε κατηγορία διαθέτουν προληπτική & ανιχνευτική προστασία. Ο μεγαλύτερος αριθμός προϊόντων τα οποία διαθέτουν προληπτική & ανιχνευτική προστασία σε μία κατηγορία ήταν 15 (100%) και ο μικρότερος αριθμός προϊόντων τα οποία διαθέτουν προληπτική & ανιχνευτική προστασία σε μία κατηγορία ήταν 0 (0%).
- Σε σύνολο 150 προϊόντων εντοπίστηκαν 127 προϊόντα (84.6%), τα οποία διαθέτουν τουλάχιστον προληπτική προστασία. Συνεπώς, εφόσον έχουμε 10 κατηγορίες, κατά μέσο όρο 12.7 προϊόντα σε κάθε κατηγορία διαθέτουν τουλάχιστον προληπτική προστασία. Ο μεγαλύτερος αριθμός προϊόντων τα οποία διαθέτουν τουλάχιστον προληπτική προστασία σε μία κατηγορία ήταν 15 (100%) και ο μικρότερος αριθμός προϊόντων τα οποία διαθέτουν τουλάχιστον προληπτική προστασία σε μία κατηγορία ήταν 0 (0%).
- Σε σύνολο 150 προϊόντων εντοπίστηκαν 88 προϊόντα (58.6%), τα οποία διαθέτουν τουλάχιστον ανιχνευτική προστασία. Συνεπώς, εφόσον έχουμε 10 κατηγορίες, κατά μέσο όρο 8.8 προϊόντα σε κάθε κατηγορία διαθέτουν τουλάχιστον ανιχνευτική προστασία. Ο μεγαλύτερος αριθμός προϊόντων τα οποία διαθέτουν τουλάχιστον ανιχνευτική προστασία σε μία κατηγορία ήταν 15 (100%) και ο μικρότερος αριθμός προϊόντων τα οποία διαθέτουν τουλάχιστον ανιχνευτική προστασία σε μία κατηγορία ήταν 0 (0%).

Παρατηρούμε πως τα περισσότερα προϊόντα διαθέτουν είτε μόνο προληπτική προστασία είτε προληπτική & ανιχνευτική προστασία. Στη συνέχεια ακολουθούν τα προϊόντα με ανιχνευτική προστασία, προληπτική & αντιδραστική προστασία και προληπτική & αντιδραστική & ανιχνευτική προστασία. Τέλος,

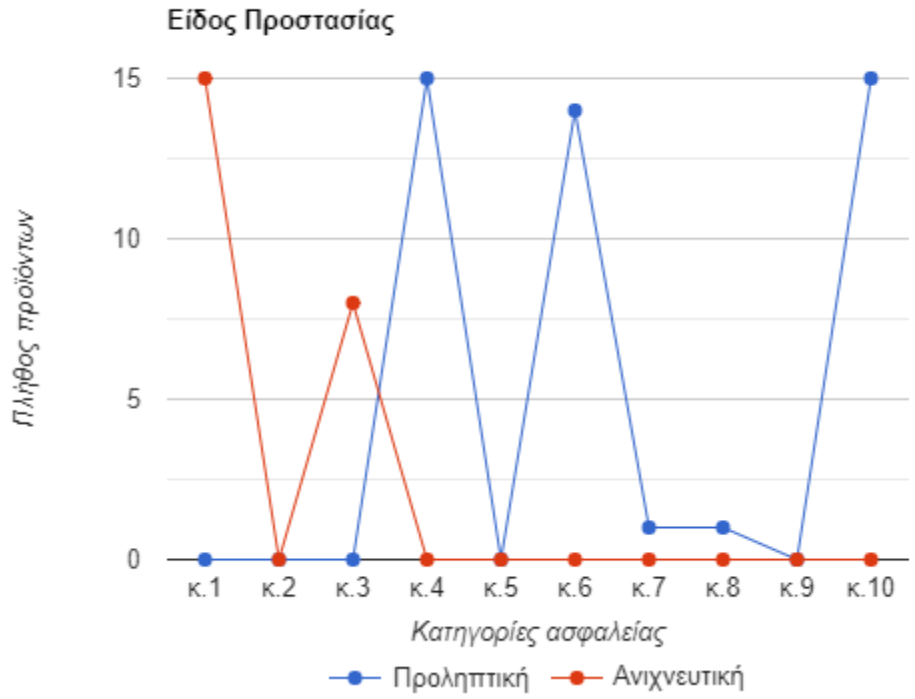
δεν βρέθηκε κανένα προϊόν που να προσφέρει μόνο ανιχνευτική προστασία. Τα αποτελέσματα είναι οριακά ικανοποιητικά διότι σχεδόν τα μισά προϊόντα υποστηρίζουν δύο ή τρία είδη προστασίας.



Εικόνα 14. Πλήθος προϊόντων ανά διαφορετική τιμή του κριτηρίου είδους προστασίας



Εικόνα 17. Πλήθος προϊόντων ανά κατηγορία ασφάλειας και ανά διαφορετική τιμή του κριτηρίου είδους προστασίας



Εικόνα 18. Πλήθος προϊόντων ανά κατηγορία ασφάλειας και ανά διαφορετική τιμή του κριτηρίου είδους προστασίας

5.3.8 Ιδιότητες ασφάλειας

Οι τιμές που προέκυψαν κατά τη διάρκεια της έρευνας για αυτό το κριτήριο ήταν 1.εμπιστευτικότητα, 2. ακεραιότητα, 3. διαθεσιμότητα, 4. ακεραιότητα & μη αποποίηση, 5. διαθεσιμότητα & μη αποποίηση, 6. διαθεσιμότητα & εμπιστευτικότητα, 7. διαθεσιμότητα & ακεραιότητα, 8. διαθεσιμότητα & εμπιστευτικότητα & ακεραιότητα. Τα συνολικά αποτελέσματα είναι τα εξής:

- Σε σύνολο 102 προϊόντων εντοπίστηκαν 14 προϊόντα (13.7%), τα οποία εξασφαλίζουν μόνο την ακεραιότητα. Συνεπώς, εφόσον έχουμε 10 κατηγορίες, κατά μέσο όρο 2.1 προϊόντα σε κάθε κατηγορία εξασφαλίζουν μόνο την ακεραιότητα. Ο μεγαλύτερος αριθμός προϊόντων τα οποία εξασφαλίζουν μόνο την ακεραιότητα σε μία κατηγορία ήταν 12 (80%) και ο μικρότερος αριθμός προϊόντων τα οποία εξασφαλίζουν μόνο την ακεραιότητα σε μία κατηγορία ήταν 0 (0%).
- Σε σύνολο 102 προϊόντων εντοπίστηκαν 29 προϊόντα (28.4%), τα οποία εξασφαλίζουν μόνο την διαθεσιμότητα. Συνεπώς, εφόσον έχουμε 10 κατηγορίες, κατά μέσο όρο 2.8 προϊόντα σε κάθε κατηγορία εξασφαλίζουν μόνο την διαθεσιμότητα. Ο μεγαλύτερος αριθμός προϊόντων τα οποία εξασφαλίζουν μόνο την διαθεσιμότητα σε μία κατηγορία ήταν 15 (100%) και ο μικρότερος αριθμός προϊόντων τα οποία εξασφαλίζουν μόνο την διαθεσιμότητα σε μία κατηγορία ήταν 0 (0%).

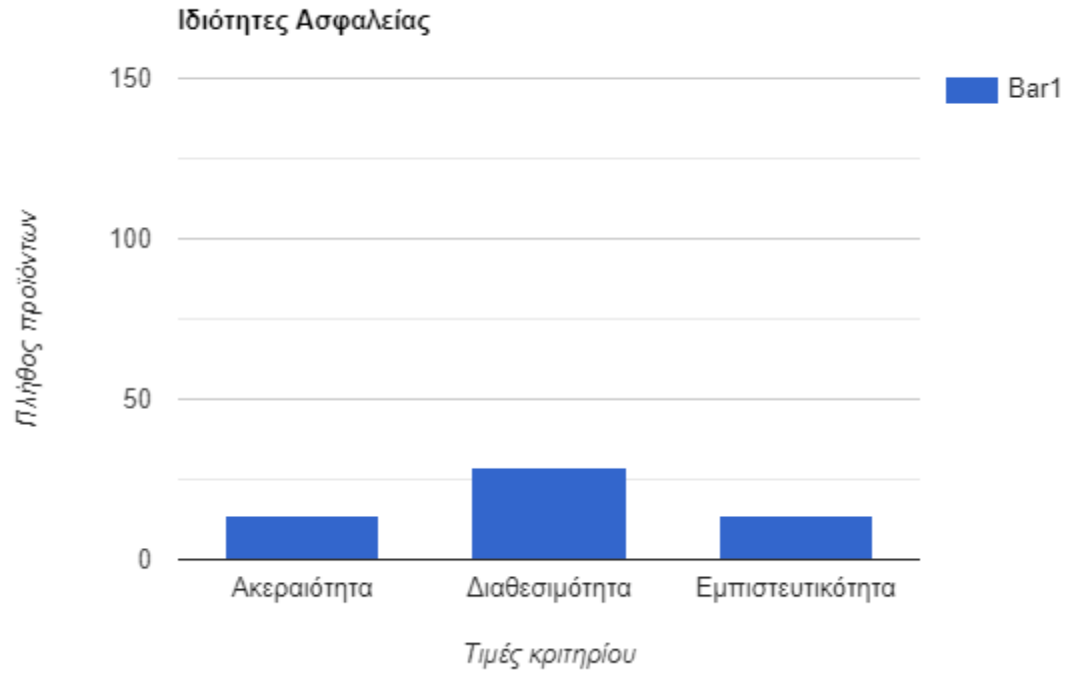
- Σε σύνολο 102 προϊόντων εντοπίστηκαν 14 προϊόντα (13.7%), τα οποία εξασφαλίζουν μόνο την εμπιστευτικότητα. Συνεπώς, εφόσον έχουμε 10 κατηγορίες, κατά μέσο όρο 1.3 προϊόντα σε κάθε κατηγορία εξασφαλίζουν μόνο την εμπιστευτικότητα. Ο μεγαλύτερος αριθμός προϊόντων τα οποία εξασφαλίζουν μόνο την εμπιστευτικότητα σε μία κατηγορία ήταν 12 (80%) και ο μικρότερος αριθμός προϊόντων τα οποία εξασφαλίζουν μόνο την εμπιστευτικότητα σε μία κατηγορία ήταν 0 (0%).

- Σε σύνολο 102 προϊόντων εντοπίστηκαν 0 προϊόντα (0%), τα οποία εξασφαλίζουν μόνο την μη αποποίηση.
- Σε σύνολο 102 προϊόντων εντοπίστηκε 1 προϊόν (0.98%), το οποίο εξασφαλίζει ακεραιότητα & μη αποποίηση. Συνεπώς, εφόσον έχουμε 10 κατηγορίες, κατά μέσο όρο 0.1 προϊόντα σε κάθε κατηγορία εξασφαλίζουν ακεραιότητα & μη αποποίηση.
- Σε σύνολο 102 προϊόντων εντοπίστηκε 1 προϊόν (0.98%), το οποίο εξασφαλίζει διαθεσιμότητα & μη αποποίηση. Συνεπώς, εφόσον έχουμε 10 κατηγορίες, κατά μέσο όρο 0.1 προϊόντα σε κάθε κατηγορία εξασφαλίζουν διαθεσιμότητα & μη αποποίηση.
- Σε σύνολο 102 προϊόντων εντοπίστηκαν 27 προϊόντα (26.5%), τα οποία εξασφαλίζουν διαθεσιμότητα & εμπιστευτικότητα. Συνεπώς, εφόσον έχουμε 10 κατηγορίες, κατά μέσο όρο 2.7 προϊόντα σε κάθε κατηγορία εξασφαλίζουν διαθεσιμότητα & εμπιστευτικότητα. Ο μεγαλύτερος αριθμός προϊόντων τα οποία εξασφαλίζουν διαθεσιμότητα & εμπιστευτικότητα σε μία κατηγορία ήταν 10 (66.6%) και ο μικρότερος αριθμός προϊόντων τα οποία εξασφαλίζουν διαθεσιμότητα & εμπιστευτικότητα σε μία κατηγορία ήταν 0 (0%).
- Σε σύνολο 102 προϊόντων εντοπίστηκαν 2 προϊόντα (2%), τα οποία εξασφαλίζουν διαθεσιμότητα & ακεραιότητα. Συνεπώς, εφόσον έχουμε 10 κατηγορίες, κατά μέσο όρο 0.2 προϊόντα σε κάθε κατηγορία εξασφαλίζουν διαθεσιμότητα & ακεραιότητα. Ο μεγαλύτερος και ο μικρότερος αριθμός προϊόντων τα οποία εξασφαλίζουν διαθεσιμότητα & ακεραιότητα σε μία κατηγορία ήταν 2 (13.3%).
- Σε σύνολο 102 προϊόντων εντοπίστηκαν 14 προϊόντα (13.7%), τα οποία εξασφαλίζουν διαθεσιμότητα & ακεραιότητα & εμπιστευτικότητα. Συνεπώς, εφόσον έχουμε 10 κατηγορίες, κατά μέσο όρο 1.4 προϊόντα σε κάθε κατηγορία εξασφαλίζουν διαθεσιμότητα & ακεραιότητα & εμπιστευτικότητα. Ο μεγαλύτερος αριθμός προϊόντων τα οποία εξασφαλίζουν διαθεσιμότητα & ακεραιότητα & εμπιστευτικότητα σε μία κατηγορία ήταν 10 (66.6%) και ο μικρότερος αριθμός προϊόντων τα οποία εξασφαλίζουν διαθεσιμότητα & ακεραιότητα & εμπιστευτικότητα σε μία κατηγορία ήταν 0 (0%).

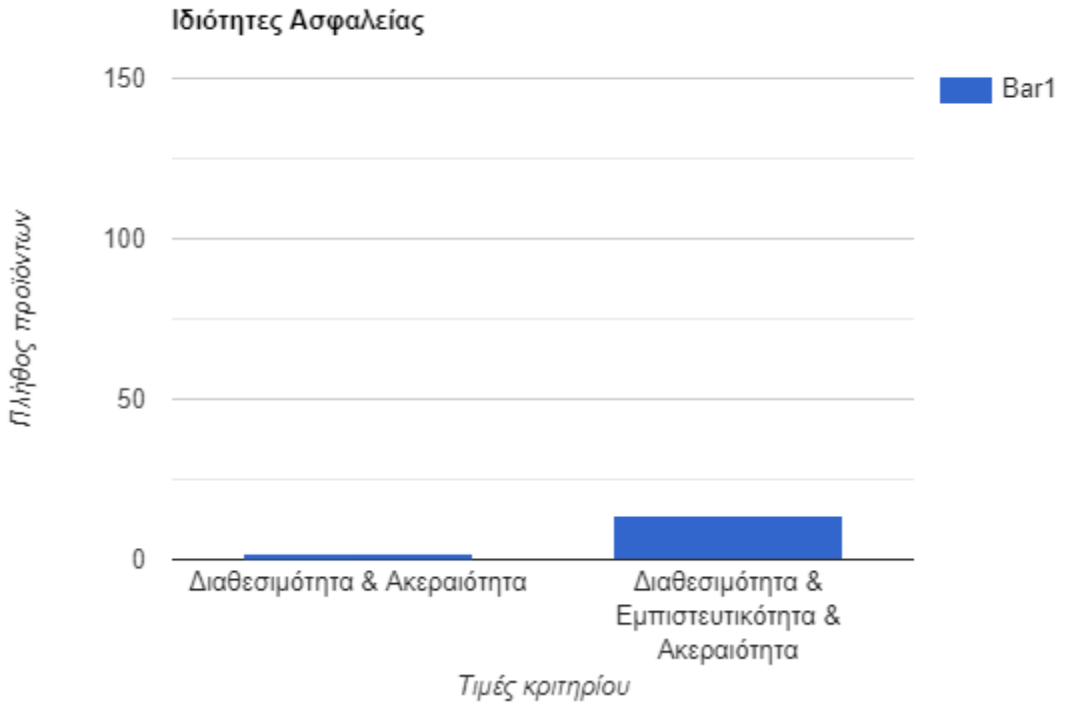
Επίσης, εξετάσαμε τα συνολικά στατιστικά όσον αφορά τον αριθμό των ιδιοτήτων ανά προϊόν με δύο διαφορετικές τιμές: προϊόντα με υποστηρίζουν 2 ή παραπάνω ιδιότητες και προϊόντα που υποστηρίζουν μόνο 1 ιδιότητα. Τα αποτελέσματα που προέκυψαν είναι τα εξής:

- Σε σύνολο 102 προϊόντων τα 45 προϊόντα (44.1%) υποστηρίζουν 2 ή παραπάνω ιδιότητες. Συνεπώς, εφόσον έχουμε 10 κατηγορίες, κατά μέσο όρο 4.5 προϊόντα σε κάθε κατηγορία υποστηρίζουν 2 ή παραπάνω ιδιότητες. Ο μεγαλύτερος αριθμός προϊόντων τα οποία υποστηρίζουν 2 ή παραπάνω ιδιότητες σε μία κατηγορία είναι 10 (66.%) και ο μικρότερος αριθμός προϊόντων τα οποία υποστηρίζουν 2 ή παραπάνω ιδιότητες σε μία κατηγορία είναι 0 (0%).
- Σε σύνολο 102 προϊόντων τα 57 προϊόντα (55.9%) υποστηρίζουν 1 ιδιότητα. Συνεπώς, εφόσον έχουμε 10 κατηγορίες, κατά μέσο όρο 4.5 προϊόντα σε κάθε κατηγορία υποστηρίζουν 2 ή παραπάνω ιδιότητες. Ο μεγαλύτερος αριθμός προϊόντων τα οποία υποστηρίζουν 1 ιδιότητα σε μία κατηγορία είναι 12 (80%) και ο μικρότερος αριθμός προϊόντων τα οποία υποστηρίζουν 1 ιδιότητα σε μία κατηγορία είναι 1 (6.6%).

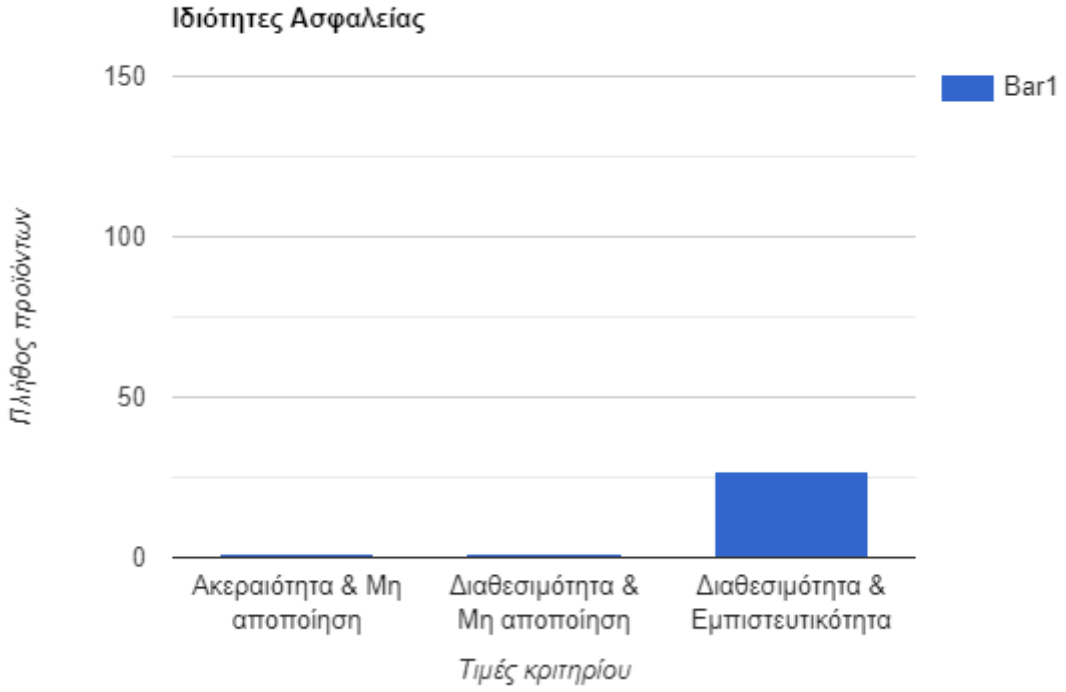
Παρατηρούμε πως τα περισσότερα προϊόντα προστατεύουν είτε μόνο την διαθεσιμότητα ή την διαθεσιμότητα & εμπιστευτικότητα. Στη συνέχεια ακολουθούν τα προϊόντα με ακεραιότητα, τα προϊόντα με εμπιστευτικότητα και τα προϊόντα με ακεραιότητα & εμπιστευτικότητα & διαθεσιμότητα. Τελευταία βρίσκονται τα προϊόντα με διαθεσιμότητα & μη αποποίηση, με ακεραιότητα & μη αποποίηση. Τέλος δε βρέθηκαν προϊόντα που να διαθέτουν μόνο μη αποποίηση. Επιπλέον παρατηρούμε πως σχεδόν ίδιος αριθμός από προϊόντα υποστηρίζουν είτε μία ιδιότητα είτε δύο ή περισσότερες ιδιότητες. Επομένως, τα αποτελέσματα θεωρούνται ουδέτερα.



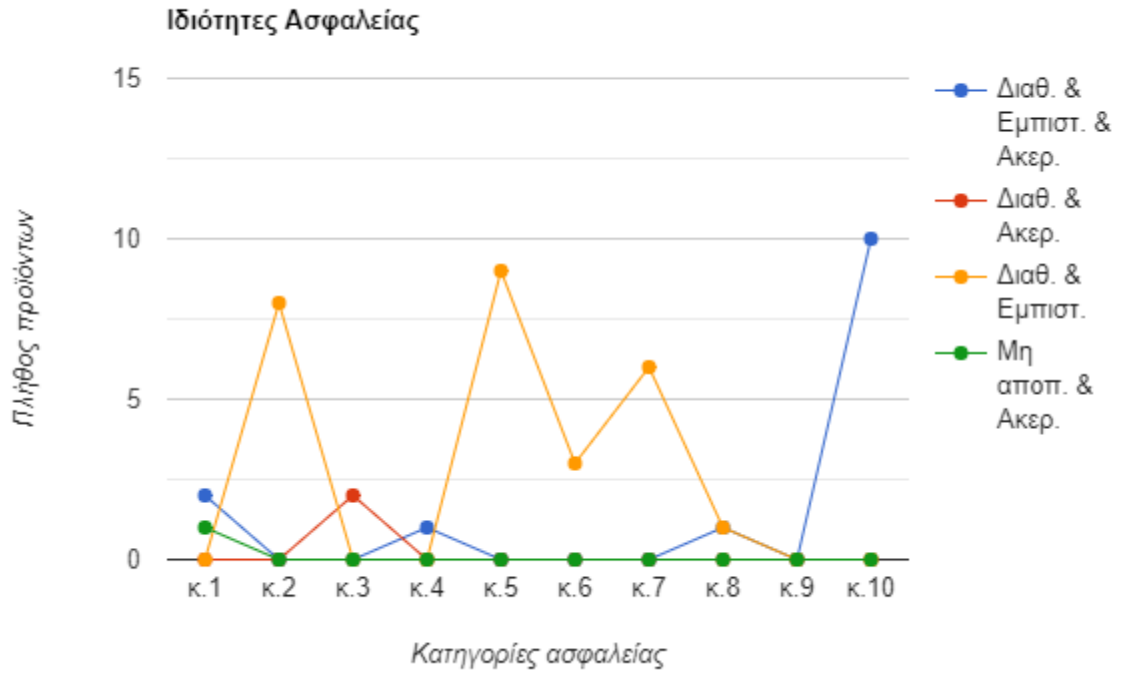
Εικόνα 19. Πλήθος προϊόντων που υποστηρίζουν μεμονωμένα 3 διαφορετικές ιδιότητες ασφάλειας



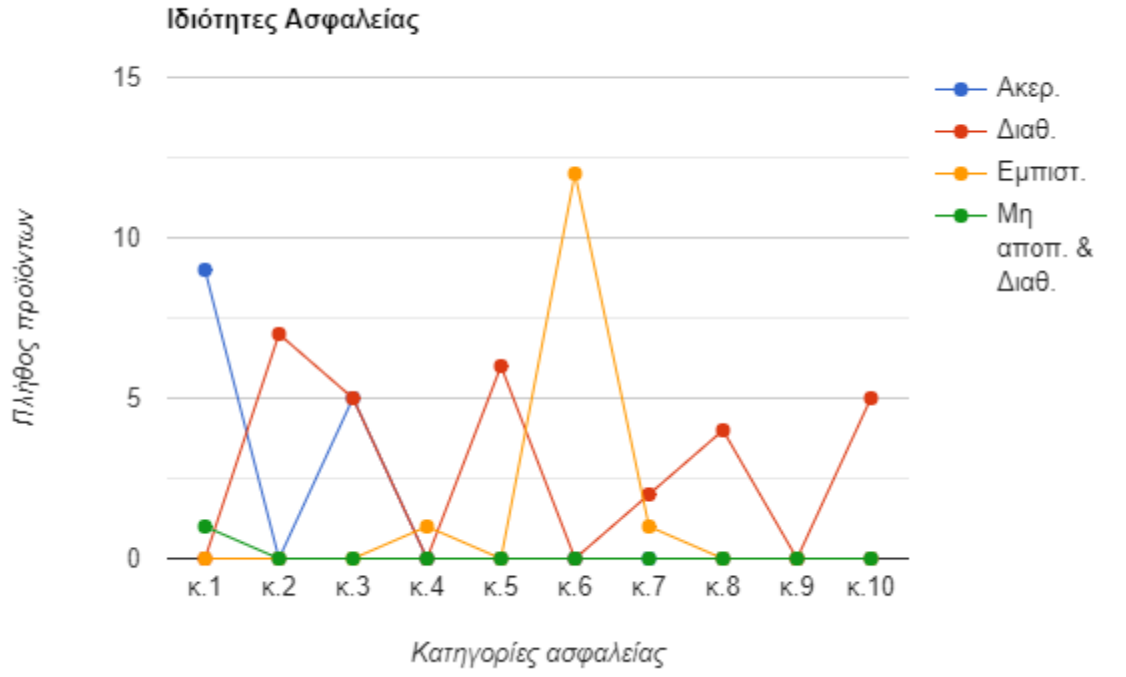
Εικόνα 20. Πλήθος προϊόντων που υποστηρίζουν είτε την διαθεσιμότητα & ακεραιότητα είτε την διαθεσιμότητα, εμπιστευτικότητα & ακεραιότητα



Εικόνα 21. Πλήθος προϊόντων που υποστηρίζουν μεμονωμένα 3 διαφορετικούς συνδυασμούς ιδιοτήτων ασφάλειας



Εικόνα 22. Πλήθος προϊόντων ανά κατηγορία που υποστηρίζουν διαφορετικούς συνδυασμούς ιδιοτήτων ασφάλειας



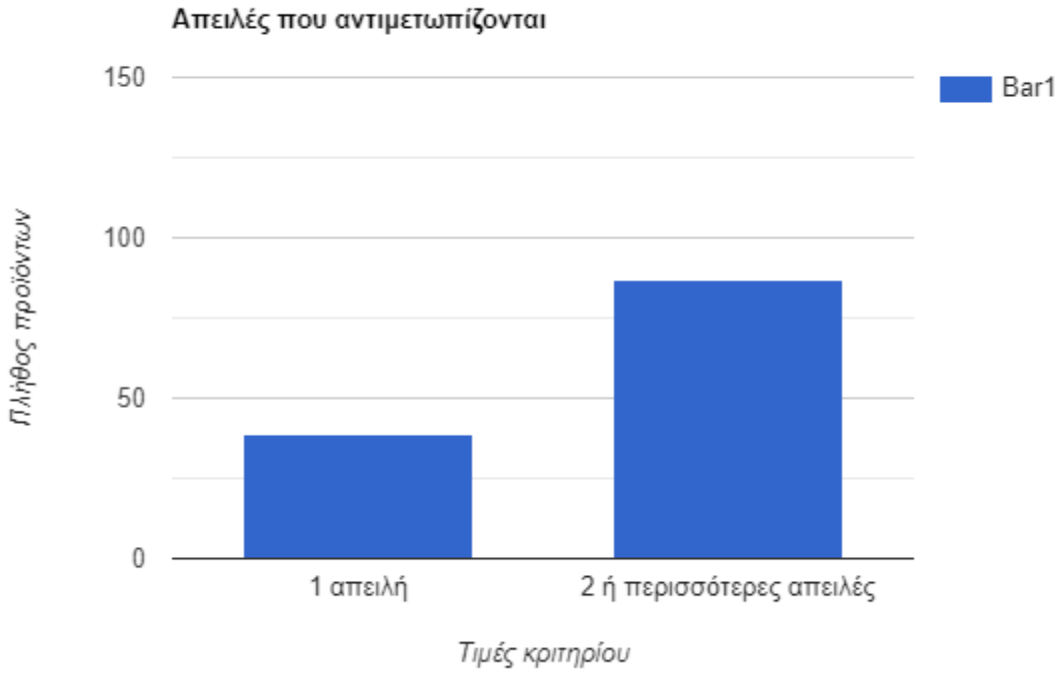
Εικόνα 23. Πλήθος προϊόντων ασφάλειας ανά κατηγορία που υποστηρίζουν είτε ξεχωριστά 3 ιδιότητες ασφάλειας είτε τον συνδυασμό μη αποποίησης και διαθεσιμότητας

5.3.9 Αντιμετωπιζόμενες Απειλές

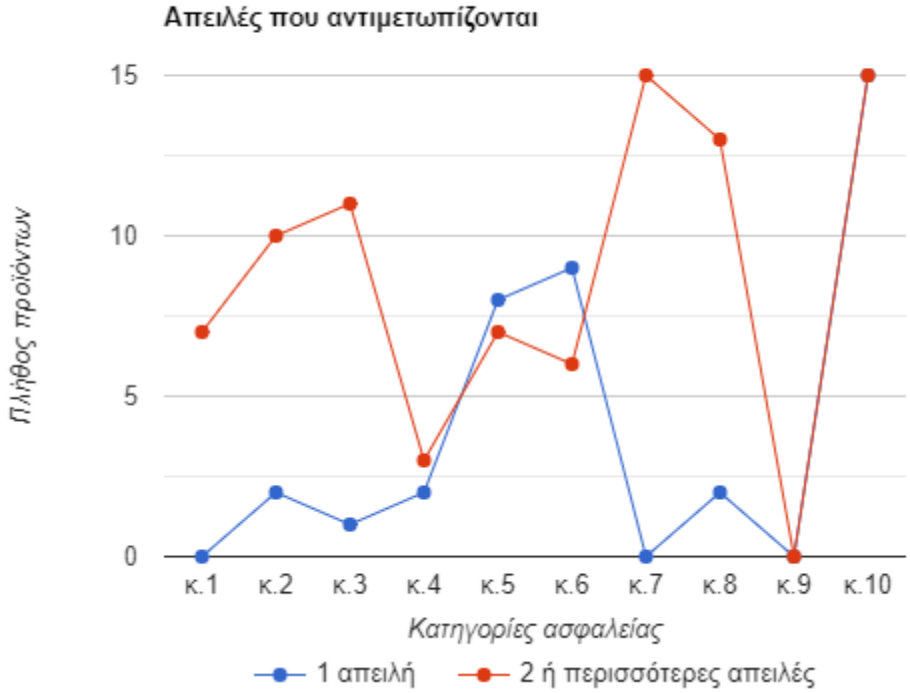
Για αυτό το κριτήριο είναι σχεδόν ανθρωπίνως αδύνατο να βγουν στατιστικά για κάθε πιθανή απειλή. Οπότε, επικεντρωθήκαμε στο πλήθος των απειλών που αντιμετωπίζονται ανά προϊόν και κατηγορία. Οπότε, θα προσδιοριστεί ελάχιστη, μέγιστη και μέση τιμή του πλήθους απειλών που καλύπτονται από τα προϊόντα. Τα συνολικά αποτελέσματα είναι τα εξής:

- Σε σύνολο 126 προϊόντων και 517 απειλών, ο μέσος όρος απειλών που αντιμετωπίζονται από ένα προϊόν είναι 4.1 απειλές. Ο μέγιστος αριθμός απειλών που αντιμετωπίζονται από ένα προϊόν είναι 19 απειλές. Ο ελάχιστος αριθμός απειλών που αντιμετωπίζονται από ένα προϊόν είναι 1 απειλή.
- Σε σύνολο 126 προϊόντων υπάρχουν 39 προϊόντα (31%), τα οποία αντιμετωπίζουν μόνο μία απειλή. Συνεπώς, εφόσον έχουμε 10 κατηγορίες, κατά μέσο όρο 3.9 προϊόντα σε κάθε αντιμετωπίζουν μόνο μία απειλή. Ο μεγαλύτερος αριθμός προϊόντων τα οποία αντιμετωπίζουν μόνο μία απειλή σε μία κατηγορία ήταν 15 (100%) και ο μικρότερος αριθμός προϊόντων τα οποία αντιμετωπίζουν μόνο μία απειλή σε μία κατηγορία ήταν 0 (0%).
- Σε σύνολο 126 προϊόντων υπάρχουν 87 προϊόντα (69%), τα οποία αντιμετωπίζουν δύο ή περισσότερες απειλές. Συνεπώς, εφόσον έχουμε 10 κατηγορίες, κατά μέσο όρο 8.7 προϊόντα σε κάθε κατηγορία αντιμετωπίζουν δύο ή περισσότερες απειλές. Ο μεγαλύτερος αριθμός προϊόντων τα οποία αντιμετωπίζουν δύο ή περισσότερες απειλές σε μία κατηγορία ήταν 15 (100%) και ο μικρότερος αριθμός προϊόντων τα οποία αντιμετωπίζουν δύο ή περισσότερες απειλές σε μία κατηγορία ήταν 0 (0%).

Παρατηρούμε ότι περίπου τα ⅔ των προϊόντων στα οποία βρέθηκαν πληροφορίες αντιμετωπίζουν 2 ή περισσότερες απειλές και περίπου το ⅓ των προϊόντων αντιμετωπίζει μία απειλή. Τα αποτελέσματα θεωρούνται ικανοποιητικά.



Εικόνα 24. Πλήθος προϊόντων που είτε αντιμετωπίζουν μια απειλή είτε δύο ή παραπάνω απειλές



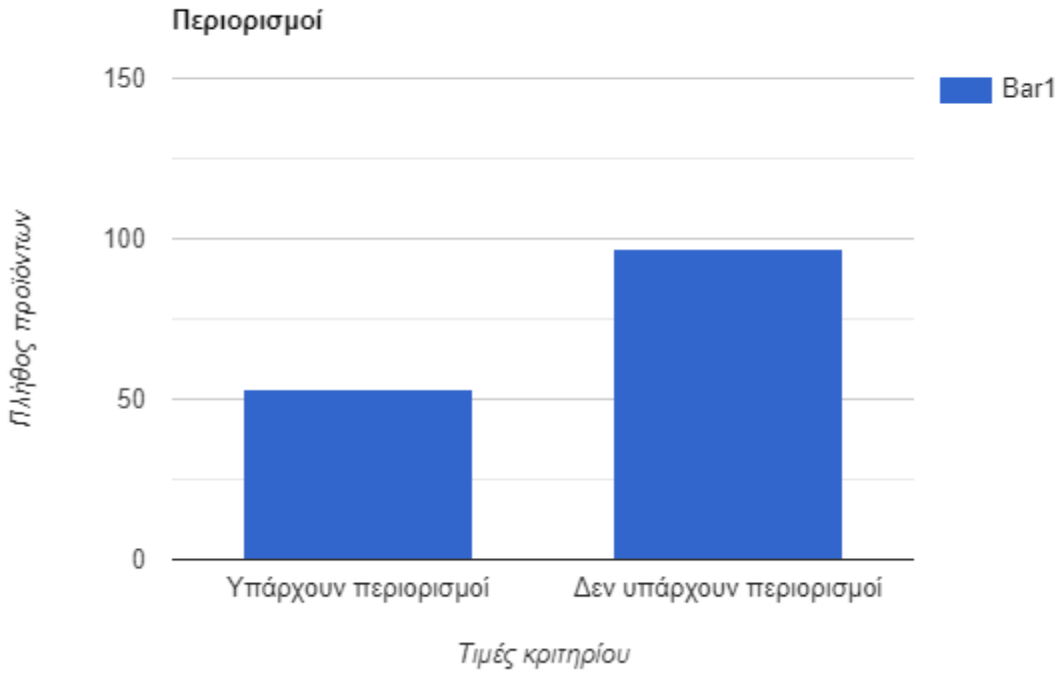
Εικόνα 25. Πλήθος προϊόντων ανά κατηγορία που είτε αντιμετωπίζουν μια απειλή είτε δύο ή παραπάνω απειλές

5.3.10 Περιορισμοί Χρήσης

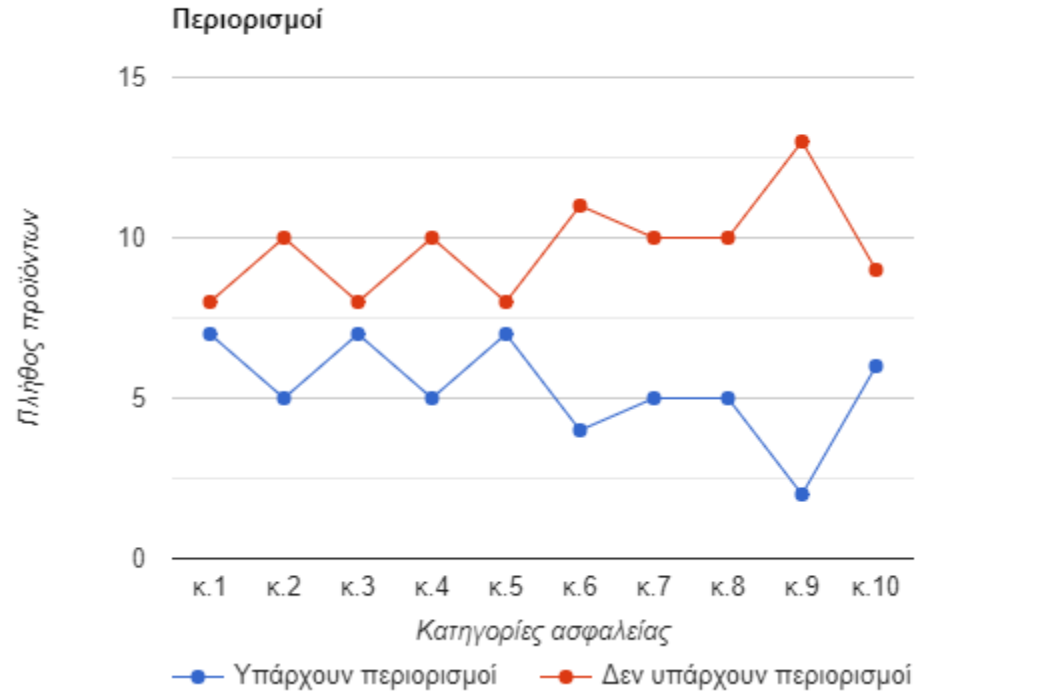
Αυτό το κριτήριο λόγω της φύσης των αποτελεσμάτων δεν διαθέτει διακριτές τιμές. Γι΄αυτό θεωρούμε πως υπάρχουν οι δύο παρακάτω τιμές: 1. προϊόντα με περιορισμούς και 2. προϊόντα χωρίς περιορισμούς. Τα συνολικά αποτελέσματα είναι τα εξής:

- Σε σύνολο 150 προϊόντων εντοπίστηκαν 97 προϊόντα (64.6%) χωρίς περιορισμούς. Συνεπώς, εφόσον έχουμε 10 κατηγορίες, κατά μέσο όρο 9.7 προϊόντα σε κάθε κατηγορία δεν διαθέτουν περιορισμούς. Ο μεγαλύτερος αριθμός προϊόντων τα οποία δεν διαθέτουν περιορισμούς σε μία κατηγορία ήταν 13 (86.6%) και ο μικρότερος αριθμός προϊόντων τα οποία δεν διαθέτουν περιορισμούς σε μία κατηγορία ήταν 8 (53.3%).
- Σε σύνολο 150 προϊόντων εντοπίστηκαν 53 προϊόντα (35.3%) με περιορισμούς. Συνεπώς, εφόσον έχουμε 10 κατηγορίες, κατά μέσο όρο 5.3 προϊόντα σε κάθε κατηγορία διαθέτουν περιορισμούς. Ο μεγαλύτερος αριθμός προϊόντων τα οποία διαθέτουν περιορισμούς σε μία κατηγορία ήταν 7 (46.6%) και ο μικρότερος αριθμός προϊόντων τα οποία διαθέτουν περιορισμούς σε μία κατηγορία ήταν 2 (13.3%).
    - Σε σύνολο 53 προϊόντων εντοπίστηκαν 44 προϊόντα (83%) με έναν περιορισμό. Συνεπώς, εφόσον έχουμε 10 κατηγορίες, κατά μέσο όρο 4.4 προϊόντα (83%) σε κάθε κατηγορία διαθέτουν έναν περιορισμό. Ο μεγαλύτερος αριθμός προϊόντων τα οποία διαθέτουν έναν περιορισμό σε μία κατηγορία ήταν 6 (40%) και ο μικρότερος αριθμός προϊόντων τα οποία διαθέτουν έναν περιορισμό σε μία κατηγορία ήταν 2 (13.3%).
    - Σε σύνολο 53 προϊόντων εντοπίστηκαν 9 προϊόντα (17%) με 2 ή περισσότερους περιορισμούς. Συνεπώς, εφόσον έχουμε 10 κατηγορίες, κατά μέσο όρο 0.9 προϊόντα σε κάθε κατηγορία διαθέτουν 2 ή περισσότερους περιορισμούς. Ο μεγαλύτερος αριθμός προϊόντων τα οποία διαθέτουν 2 ή περισσότερους περιορισμούς σε μία κατηγορία ήταν 2 (13.3%) και ο μικρότερος αριθμός προϊόντων τα οποία διαθέτουν 2 ή περισσότερους περιορισμούς σε μία κατηγορία ήταν 0 (0%).

Παρατηρούμε πως το 1/3 των προϊόντων διαθέτουν περιορισμούς. Από τα προϊόντα τα οποία διαθέτουν περιορισμούς, μόνο σχεδόν το ⅕ διαθέτει δύο ή περισσότερους περιορισμούς. Τα αποτελέσματα θεωρούνται απογοητευτικά καθώς μόνο σε 9 προϊόντα εντοπίστηκαν δύο ή περισσότεροι περιορισμοί.



Εικόνα 26. Πλήθος προϊόντων που είτε έχουν κάποιο περιορισμό χρήσης είτε δεν έχουν



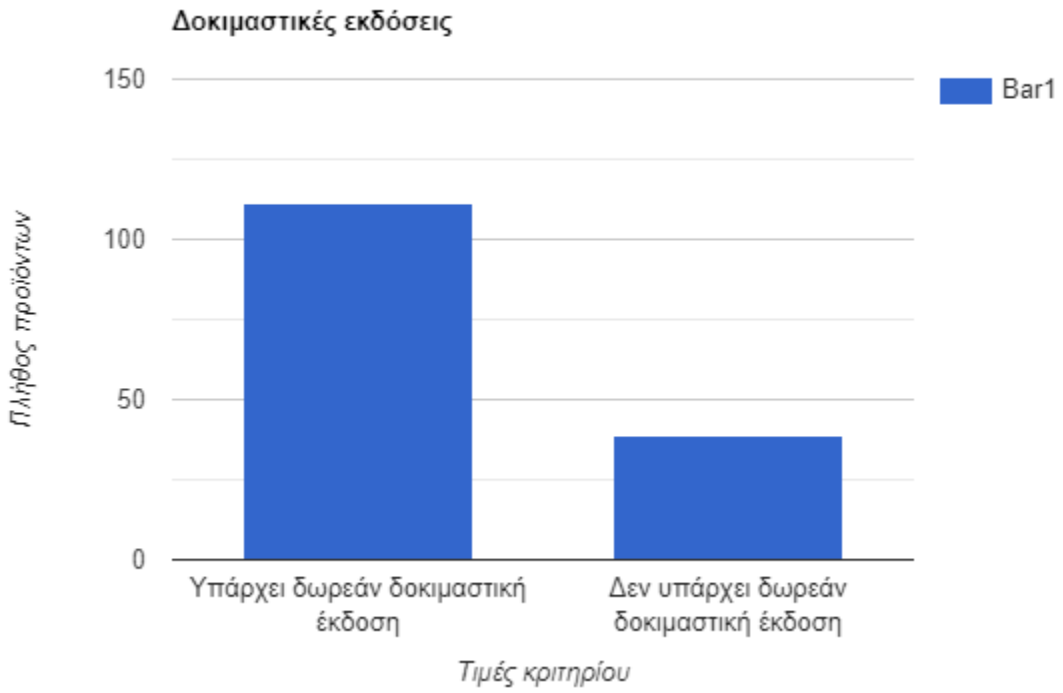
Εικόνα 27. Πλήθος προϊόντων που είτε έχουν κάποιο περιορισμό χρήσης είτε δεν έχουν

5.3.11 Δοκιμαστικές εκδόσεις

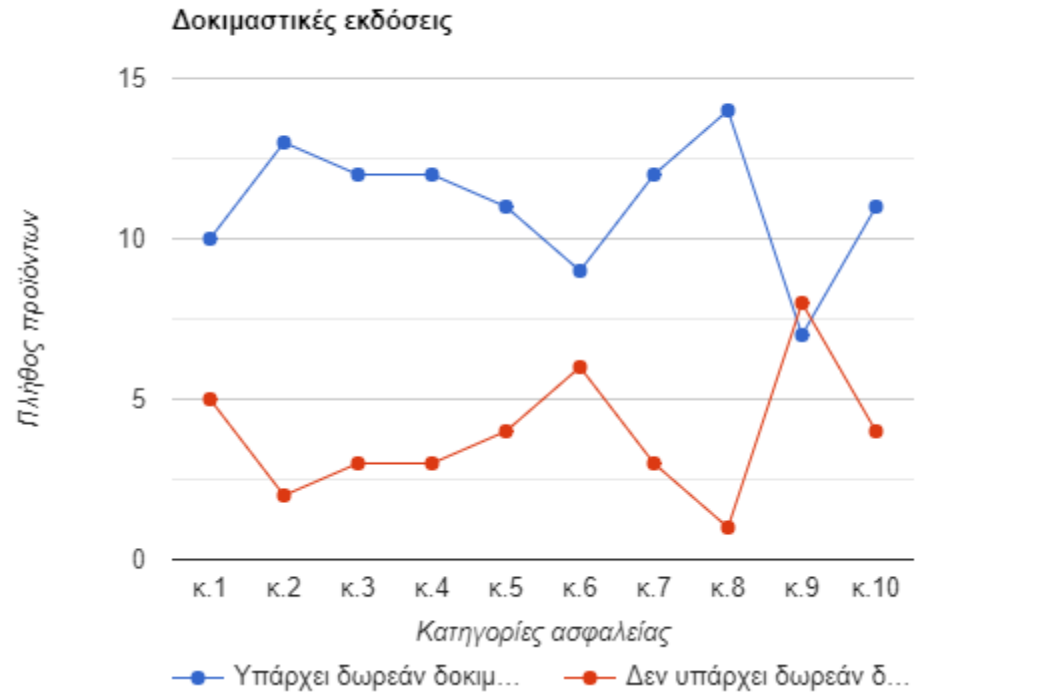
Αυτό το κριτήριο λόγω της φύσης των αποτελεσμάτων δεν διαθέτει διακριτές τιμές. Γι΄αυτό θεωρούμε πως υπάρχουν οι δύο παρακάτω τιμές: 1. προϊόντα με δωρεάν δοκιμαστική έκδοση και 2. προϊόντα χωρίς δωρεάν δοκιμαστική έκδοση. Τα συνολικά αποτελέσματα είναι τα εξής:

- Σε σύνολο 150 προϊόντων εντοπίστηκαν 38 προϊόντα (25.3%) χωρίς δωρεάν δοκιμαστική έκδοση. Συνεπώς, εφόσον έχουμε 10 κατηγορίες, κατά μέσο όρο 3.8 προϊόντα σε κάθε κατηγορία δεν διαθέτουν δωρεάν δοκιμαστική έκδοση. Ο μεγαλύτερος αριθμός προϊόντων τα οποία δεν διαθέτουν δωρεάν δοκιμαστική έκδοση σε μία κατηγορία ήταν 8 (56.6%) και ο μικρότερος αριθμός προϊόντων τα οποία δεν διαθέτουν δωρεάν δοκιμαστική έκδοση σε μία κατηγορία ήταν 1 (6.6%).
- Σε σύνολο 150 προϊόντων εντοπίστηκαν 112 προϊόντα (74.7%) με δωρεάν δοκιμαστική έκδοση. Συνεπώς, εφόσον έχουμε 10 κατηγορίες, κατά μέσο όρο 11.1 προϊόντα σε κάθε κατηγορία διαθέτουν δωρεάν δοκιμαστική έκδοση. Ο μεγαλύτερος αριθμός προϊόντων τα οποία διαθέτουν δωρεάν δοκιμαστική έκδοση σε μία κατηγορία ήταν 14 (93.3%) και ο μικρότερος αριθμός προϊόντων τα οποία διαθέτουν δωρεάν δοκιμαστική έκδοση σε μία κατηγορία ήταν 7 (46.6%).
    - Σε σύνολο 112 προϊόντων εντοπίστηκαν 83 προϊόντα (74.1%) με δωρεάν έκδοση διάρκειας μεγαλύτερης ή ίσης με 30 ημέρες. Συνεπώς, εφόσον έχουμε 10 κατηγορίες, κατά μέσο όρο 8.3 προϊόντα σε κάθε κατηγορία διαθέτουν δωρεάν έκδοση διάρκειας μεγαλύτερης ή ίσης με 30 ημέρες. Ο μεγαλύτερος αριθμός προϊόντων τα οποία διαθέτουν δωρεάν έκδοση διάρκειας μεγαλύτερης ή ίσης με 30 ημέρες ήταν 12 (80%) και ο μικρότερος αριθμός προϊόντων δωρεάν έκδοση διάρκειας μεγαλύτερης ή ίσης με 30 ημέρες ήταν 5 (33.3%).
        - Σε σύνολο 53 προϊόντων εντοπίστηκαν 29 προϊόντα (25.9%) με δωρεάν έκδοση διάρκειας μικρότερης από 30 ημέρες. Συνεπώς, εφόσον έχουμε 10 κατηγορίες, κατά μέσο όρο 2.9 προϊόντα σε κάθε κατηγορία διαθέτουν δωρεάν έκδοση διάρκειας μικρότερης από 30 ημέρες. Ο μεγαλύτερος αριθμός προϊόντων με δωρεάν έκδοση διάρκειας μικρότερης από 30 ημέρες σε μία κατηγορία ήταν 6 (40%) και ο μικρότερος αριθμός προϊόντων με δωρεάν έκδοση διάρκειας μικρότερης από 30 ημέρες σε μία κατηγορία ήταν 1 (6.6%).

Παρατηρούμε πως σχεδόν τα 3/4 των προϊόντων διαθέτουν δωρεάν δοκιμαστικές εκδόσεις και πως σχεδόν τα ¾ των προϊόντων αυτών διαθέτουν δωρεάν εκδόσεις με διάρκεια μεγαλύτερη ή ίση των 30 ημερών. Τα αποτελέσματα θεωρούνται ικανοποιητικά καθώς τελικά περισσότερα από τα μισά προϊόντα διαθέτουν δωρεάν έκδοση διάρκειας μεγαλύτερης ή ίσης με 30 ημέρες.



Εικόνα 28. Πλήθος προϊόντων που είτε προσφέρουν δωρεάν δοκιμαστική έκδοση είτε όχι



Εικόνα 29. Πλήθος προϊόντων ανά κατηγορία που είτε προσφέρουν δωρεάν δοκιμαστική έκδοση είτε όχι

5.3.12 Τρόπος χρήσης

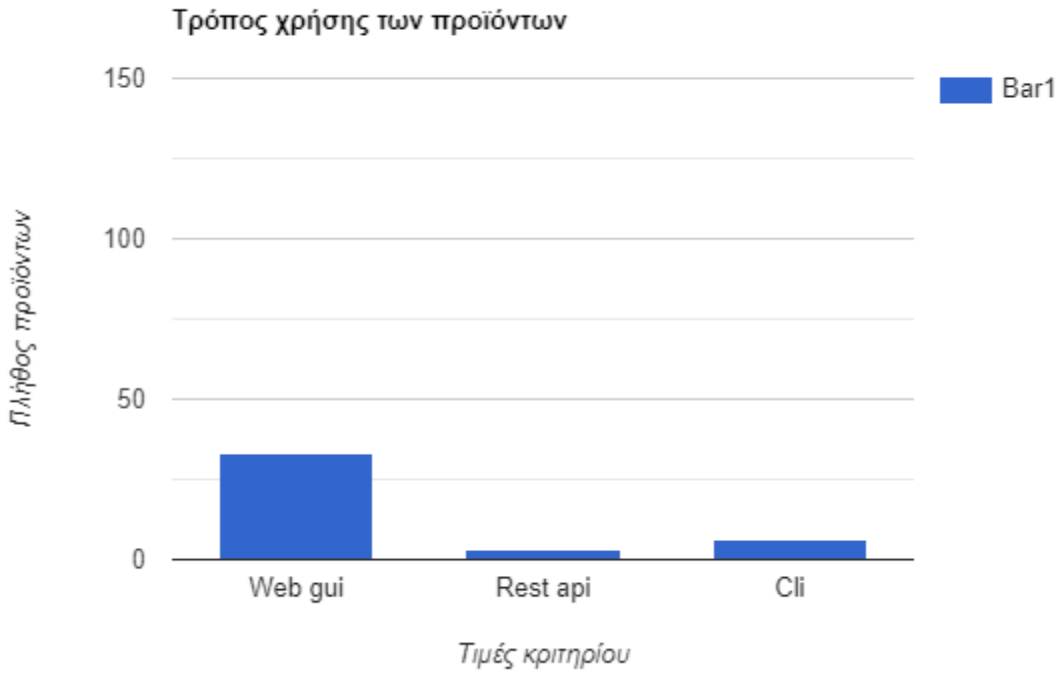
Οι τιμές που προέκυψαν κατά τη διάρκεια της έρευνας για αυτό το κριτήριο ήταν 1.Web gui, 2. Rest api, 3. Cli, 4. Web gui & Rest api & Cli, 5. Web gui & Rest api, 6. Rest api & Cli, 7. Web gui & Cli. Τα συνολικά αποτελέσματα είναι τα εξής:

- Σε σύνολο 147 προϊόντων εντοπίστηκαν 33 προϊόντα (22.4%), τα οποία υποστηρίζουν μόνο την τεχνολογία Web gui. Συνεπώς, εφόσον έχουμε 10 κατηγορίες, κατά μέσο όρο 3.3 προϊόντα σε κάθε κατηγορία υποστηρίζουν μόνο την τεχνολογία Web gui. Ο μεγαλύτερος αριθμός προϊόντων τα οποία υποστηρίζουν μόνο την τεχνολογία Web gui σε μία κατηγορία ήταν 9 (60%) και ο μικρότερος αριθμός προϊόντων τα οποία υποστηρίζουν μόνο την τεχνολογία Web gui σε μία κατηγορία ήταν 0 (0%).
- Σε σύνολο 147 προϊόντων εντοπίστηκαν 3 προϊόντα (2%), τα οποία υποστηρίζουν μόνο την τεχνολογία Rest api. Συνεπώς, εφόσον έχουμε 10 κατηγορίες, κατά μέσο όρο 0.3 προϊόντα σε κάθε κατηγορία υποστηρίζουν μόνο την τεχνολογία Rest api. Ο μεγαλύτερος αριθμός προϊόντων τα οποία υποστηρίζουν μόνο την τεχνολογία Rest api σε μία κατηγορία ήταν 3 (20%) και ο μικρότερος αριθμός προϊόντων τα οποία υποστηρίζουν μόνο την τεχνολογία Rest api σε μία κατηγορία ήταν 0 (0%).
- Σε σύνολο 147 προϊόντων εντοπίστηκαν 6 προϊόντα (4.1%), τα οποία υποστηρίζουν μόνο την τεχνολογία Cli. Συνεπώς, εφόσον έχουμε 10 κατηγορίες, κατά μέσο όρο 0.6 προϊόντα σε κάθε κατηγορία υποστηρίζουν μόνο την τεχνολογία Cli. Ο μεγαλύτερος αριθμός προϊόντων τα οποία υποστηρίζουν μόνο την τεχνολογία Cli σε μία κατηγορία ήταν 4 (26.6%) και ο μικρότερος αριθμός προϊόντων τα οποία υποστηρίζουν μόνο την τεχνολογία Cli σε μία κατηγορία ήταν 0 (0%).
- Σε σύνολο 147 προϊόντων εντοπίστηκαν 48 προϊόντα (32.6%), τα οποία υποστηρίζουν και τις τρεις τεχνολογίες. Συνεπώς, εφόσον έχουμε 10 κατηγορίες, κατά μέσο όρο 4.8 προϊόντα σε κάθε κατηγορία υποστηρίζουν και τις τρεις τεχνολογίες. Ο μεγαλύτερος αριθμός προϊόντων τα οποία υποστηρίζουν και τις τρεις τεχνολογίες σε μία κατηγορία ήταν 9 (60%) και ο μικρότερος αριθμός προϊόντων τα οποία υποστηρίζουν και τις τρεις τεχνολογίες σε μία κατηγορία ήταν 0 (0%).
- Σε σύνολο 147 προϊόντων εντοπίστηκαν 34 προϊόντα (23.1%), τα οποία υποστηρίζουν τις τεχνολογίες Web gui & Rest api. Συνεπώς, εφόσον έχουμε 10 κατηγορίες, κατά μέσο όρο 3.4 προϊόντα σε κάθε κατηγορία υποστηρίζουν τις τεχνολογίες Web gui & Rest api. Ο μεγαλύτερος αριθμός προϊόντων τα οποία υποστηρίζουν τις τεχνολογίες Web gui & Rest api σε μία κατηγορία ήταν 8 (53.3%) και ο μικρότερος αριθμός προϊόντων τα οποία υποστηρίζουν τις τεχνολογίες Web gui & Rest api σε μία κατηγορία ήταν 1 (6.6%).
- Σε σύνολο 147 προϊόντων εντοπίστηκαν 13 προϊόντα (8.8%), τα οποία υποστηρίζουν τις τεχνολογίες Web gui & Cli. Συνεπώς, εφόσον έχουμε 10 κατηγορίες, κατά μέσο όρο 1.3 προϊόντα σε κάθε κατηγορία υποστηρίζουν τις τεχνολογίες Web gui & Cli. Ο μεγαλύτερος αριθμός προϊόντων

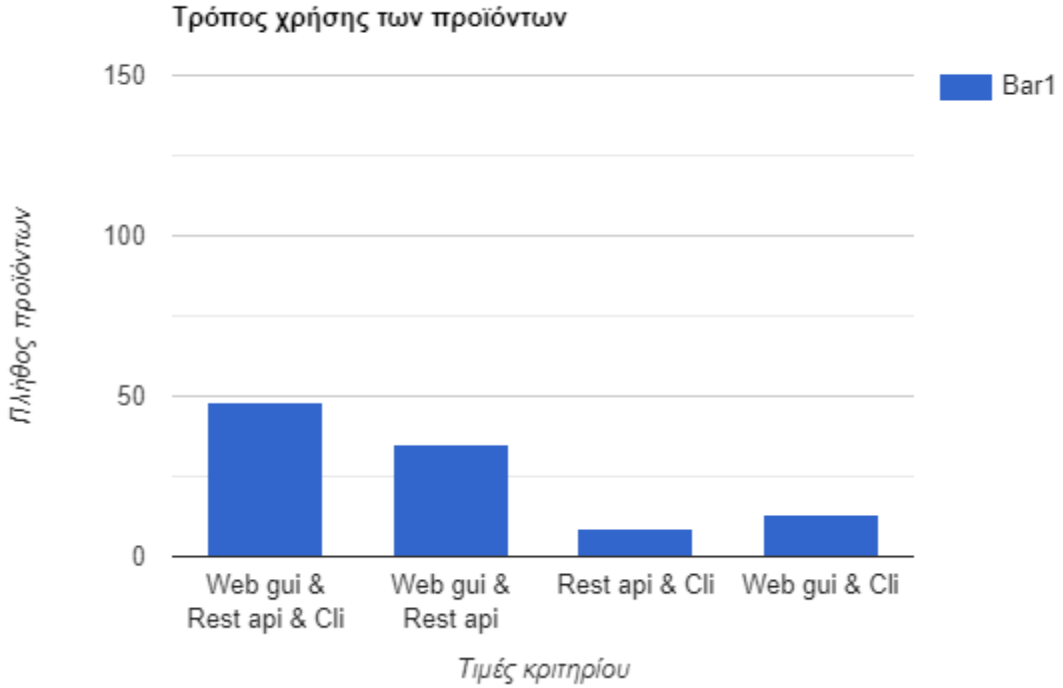
τα οποία υποστηρίζουν τις τεχνολογίες Web gui & Cli σε μία κατηγορία ήταν 4 (26.6%) και ο μικρότερος αριθμός προϊόντων τα οποία υποστηρίζουν τις τεχνολογίες Web gui & Cli σε μία κατηγορία ήταν 0 (0%).

- Σε σύνολο 147 προϊόντων εντοπίστηκαν 8 προϊόντα (5.4%), τα οποία υποστηρίζουν τις τεχνολογίες Rest api & Cli. Συνεπώς, εφόσον έχουμε 10 κατηγορίες, κατά μέσο όρο 0.8 προϊόντα σε κάθε κατηγορία υποστηρίζουν τις τεχνολογίες Rest api & Cli. Ο μεγαλύτερος αριθμός προϊόντων τα οποία υποστηρίζουν τις τεχνολογίες Rest api & Cli σε μία κατηγορία ήταν 3 (20%) και ο μικρότερος αριθμός προϊόντων τα οποία υποστηρίζουν τις τεχνολογίες Rest api & Cli σε μία κατηγορία ήταν 0 (0%).
- Σε σύνολο 147 προϊόντων εντοπίστηκαν 129 προϊόντα (87.7%), τα οποία υποστηρίζουν τουλάχιστον την τεχνολογία Web gui. Συνεπώς, εφόσον έχουμε 10 κατηγορίες, κατά μέσο όρο 12.9 προϊόντα σε κάθε κατηγορία υποστηρίζουν τουλάχιστον την τεχνολογία Web gui. Ο μεγαλύτερος αριθμός προϊόντων τα οποία υποστηρίζουν τουλάχιστον την τεχνολογία Web gui σε μία κατηγορία ήταν 15 (100%) και ο μικρότερος αριθμός προϊόντων τα οποία υποστηρίζουν τουλάχιστον την τεχνολογία Web gui σε μία κατηγορία ήταν 10 (66.6%).
- Σε σύνολο 147 προϊόντων εντοπίστηκαν 95 προϊόντα (64.6%), τα οποία υποστηρίζουν τουλάχιστον την τεχνολογία Rest api. Συνεπώς, εφόσον έχουμε 10 κατηγορίες, κατά μέσο όρο 9.5 προϊόντα σε κάθε κατηγορία υποστηρίζουν τουλάχιστον την τεχνολογία Rest api. Ο μεγαλύτερος αριθμός προϊόντων τα οποία υποστηρίζουν τουλάχιστον την τεχνολογία Rest api σε μία κατηγορία ήταν 13 (86.6%) και ο μικρότερος αριθμός προϊόντων τα οποία υποστηρίζουν τουλάχιστον την τεχνολογία Rest api σε μία κατηγορία ήταν 4 (26.6%).

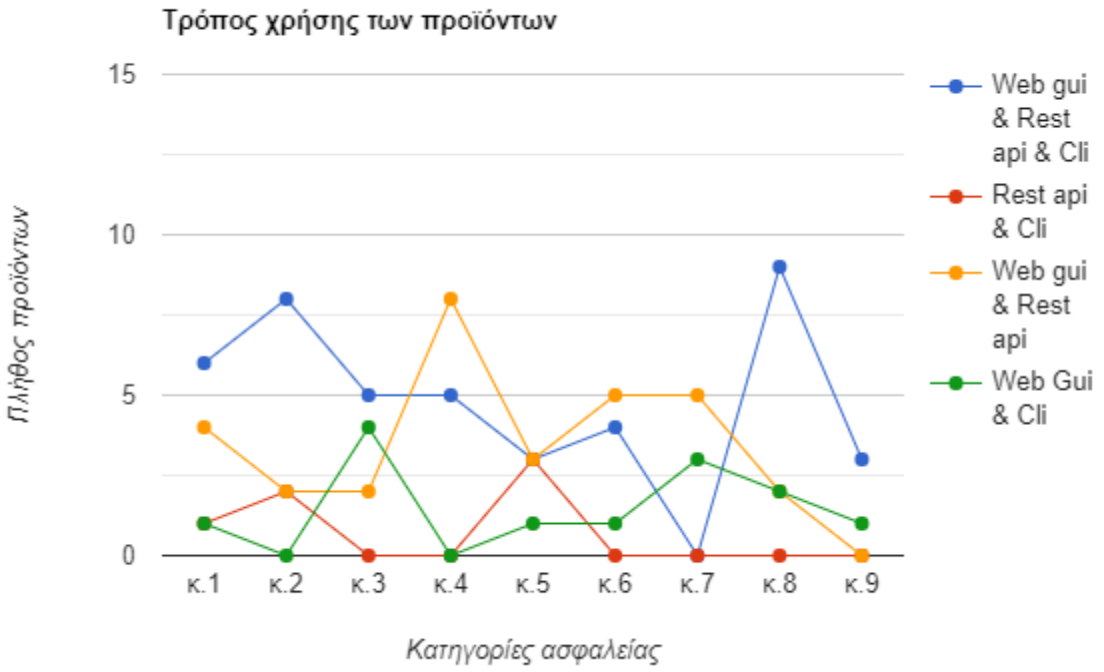
Παρατηρούμε ότι τα περισσότερα προϊόντα υποστηρίζουν είτε τις τεχνολογίες Web gui & Rest api είτε τον συνδυασμό των τριών τεχνολογιών. Στη συνέχεια ακολουθεί η τεχνολογία Cli και οι συνδυασμοί στους οποίους περιέχεται. Τα αποτελέσματα είναι ικανοποιητικά διότι πάνω από τα ⅔ των προϊόντων υποστηρίζουν δύο ή περισσότερες τεχνολογίες.



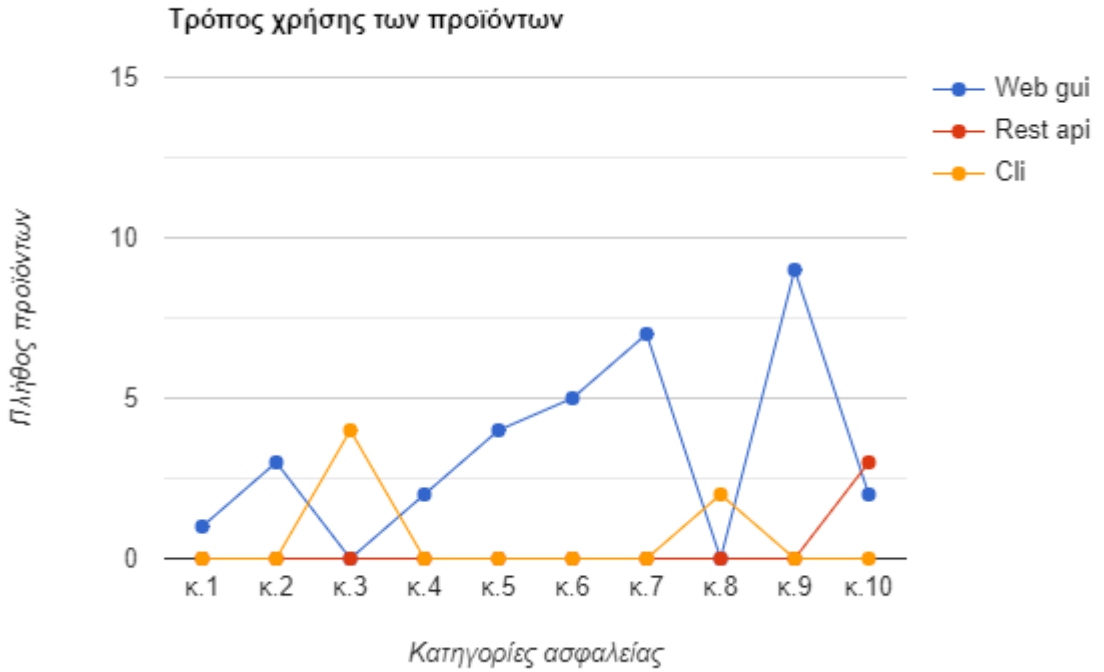
Εικόνα 30. Πλήθος προϊόντων που υποστηρίζουν μεμονωμένα έναν τρόπο χρήσης



Εικόνα 31. Πλήθος προϊόντων που υποστηρίζουν συνδυασμούς τρόπων χρήσης



Εικόνα 32. Πλήθος προϊόντων ανά κατηγορία που υποστηρίζουν διαφορετικούς συνδυασμούς τρόπων χρήσης



Εικόνα 33. Πλήθος προϊόντων ανά κατηγορία που υποστηρίζουν διαφορετικούς μεμονωμένους τρόπους χρήσης

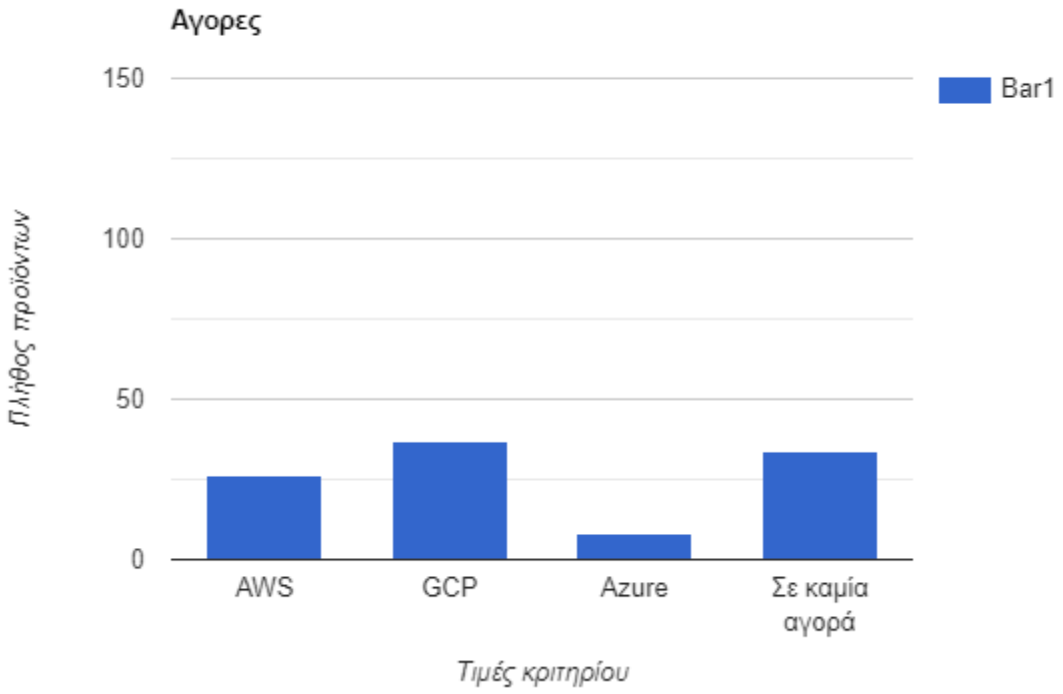
5.3.13 Αγορές

Οι τιμές που προέκυψαν κατά τη διάρκεια της έρευνας για αυτό το κριτήριο ήταν 1.Amazon web services, 2. Google cloud platform, 3. Microsoft Azure, 4. Amazon web services & Microsoft Azure & Google cloud platform, 5. Amazon web services & Microsoft Azure, 6. Amazon web services & Google cloud platform, 7. Microsoft Azure & Google cloud platform, 8. καμία από τις τρεις αγορές. Τα συνολικά αποτελέσματα είναι τα εξής:

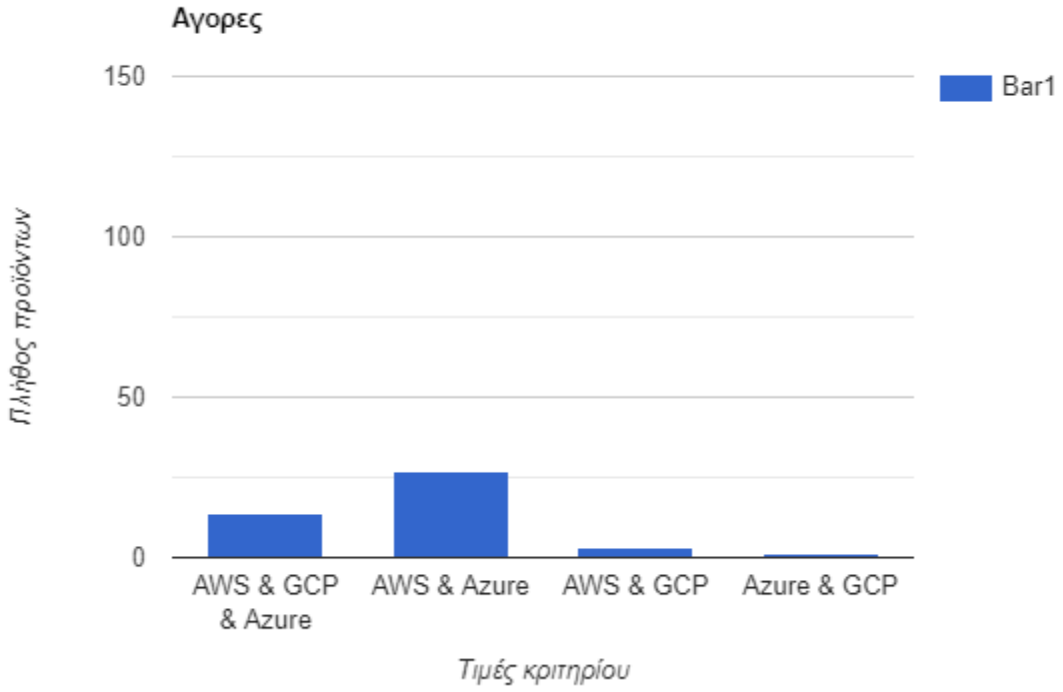
- Σε σύνολο 150 προϊόντων 26 προϊόντα (17.3%) εντοπίστηκαν μόνο στο Amazon web services. Συνεπώς, εφόσον έχουμε 10 κατηγορίες, κατά μέσο όρο 2.6 προϊόντα σε κάθε κατηγορία εντοπίστηκαν μόνο στο Amazon web services. Ο μεγαλύτερος αριθμός προϊόντων τα οποία εντοπίστηκαν μόνο στο Amazon web services σε μία κατηγορία ήταν 5 (33.3%) και ο μικρότερος αριθμός προϊόντων τα οποία εντοπίστηκαν μόνο στο Amazon web services σε μία κατηγορία ήταν 0 (0%).
- Σε σύνολο 150 προϊόντων 36 προϊόντα (24.4%) εντοπίστηκαν μόνο στο Microsoft Azure. Συνεπώς, εφόσον έχουμε 10 κατηγορίες, κατά μέσο όρο 3.6 προϊόντα σε κάθε κατηγορία εντοπίστηκαν μόνο στο Microsoft Azure. Ο μεγαλύτερος αριθμός προϊόντων τα οποία εντοπίστηκαν μόνο στο Amazon web services σε μία κατηγορία ήταν 5 (33.3%) και ο μικρότερος αριθμός προϊόντων τα οποία εντοπίστηκαν μόνο στο Microsoft Azure σε μία κατηγορία ήταν 1 (6.6%).
- Σε σύνολο 150 προϊόντων 8 προϊόντα (5.3%) εντοπίστηκαν μόνο στο Google cloud platform. Συνεπώς, εφόσον έχουμε 10 κατηγορίες, κατά μέσο όρο 0.8 προϊόντα σε κάθε κατηγορία εντοπίστηκαν στο Google cloud platform. Ο μεγαλύτερος αριθμός προϊόντων τα οποία εντοπίστηκαν μόνο στο Google cloud platform σε μία κατηγορία ήταν 4 (26.6%) και ο μικρότερος αριθμός προϊόντων τα οποία εντοπίστηκαν μόνο στο Google cloud platform σε μία κατηγορία ήταν 0 (0%).
- Σε σύνολο 150 προϊόντων 34 προϊόντα (22.6%) δεν εντοπίστηκαν σε καμία από τις τρεις αγορές. Συνεπώς, εφόσον έχουμε 10 κατηγορίες, κατά μέσο όρο 3.4 προϊόντα σε κάθε κατηγορία δεν εντοπίστηκαν σε καμία από τις τρεις αγορές. Ο μεγαλύτερος αριθμός προϊόντων τα οποία δεν εντοπίστηκαν σε καμία από τις τρεις αγορές σε μία κατηγορία ήταν 10 (66.6%) και ο μικρότερος αριθμός προϊόντων τα οποία δεν εντοπίστηκαν σε καμία από τις τρεις αγορές σε μία κατηγορία ήταν 0 (0%).
- Σε σύνολο 150 προϊόντων 14 προϊόντα (9.3%) εντοπίστηκαν και στις τρεις αγορές. Συνεπώς, εφόσον έχουμε 10 κατηγορίες, κατά μέσο όρο 1.4 προϊόντα σε κάθε κατηγορία εντοπίστηκαν και στις τρεις αγορές. Ο μεγαλύτερος αριθμός προϊόντων τα οποία εντοπίστηκαν και στις τρεις αγορές σε μία κατηγορία ήταν 6 (40%) και ο μικρότερος αριθμός προϊόντων τα οποία εντοπίστηκαν και στις τρεις αγορές σε μία κατηγορία ήταν 0 (0%).

- Σε σύνολο 150 προϊόντων 27 προϊόντα (18%) εντοπίστηκαν στις αγορές Amazon web services & Microsoft Azure. Συνεπώς, εφόσον έχουμε 10 κατηγορίες, κατά μέσο όρο 2.7 προϊόντα σε κάθε κατηγορία εντοπίστηκαν στις αγορές Amazon web services & Microsoft Azure. Ο μεγαλύτερος αριθμός προϊόντων τα οποία εντοπίστηκαν στις αγορές Amazon web services & Microsoft Azure σε μία κατηγορία ήταν 6 (40%) και ο μικρότερος αριθμός προϊόντων εντοπίστηκαν στις αγορές Amazon web services & Microsoft Azure σε μία κατηγορία ήταν 0 (0%).
- Σε σύνολο 150 προϊόντων 3 προϊόντα (2%) εντοπίστηκαν στις αγορές Amazon web services & Google cloud platform. Συνεπώς, εφόσον έχουμε 10 κατηγορίες, κατά μέσο όρο 0.3 προϊόντα σε κάθε κατηγορία δεν εντοπίστηκαν στις αγορές Amazon web services & Google cloud platform. Ο μεγαλύτερος αριθμός προϊόντων τα οποία εντοπίστηκαν στις αγορές Amazon web services & Google cloud platform σε μία κατηγορία ήταν 1 (6.6%) και ο μικρότερος αριθμός προϊόντων τα οποία εντοπίστηκαν στις αγορές Amazon web services & Google cloud platform σε μία κατηγορία ήταν 0 (0%).
- Σε σύνολο 150 προϊόντων 1 προϊόν (0.66%) εντοπίστηκε στις αγορές Microsoft Azure & Google cloud platform.
- Σε σύνολο 150 προϊόντων εντοπίστηκαν 70 προϊόντα (46.6%) τουλάχιστον στο Amazon web services. Συνεπώς, εφόσον έχουμε 10 κατηγορίες, κατά μέσο όρο 7 προϊόντα σε κάθε κατηγορία εντοπίστηκαν στο Amazon web services. Ο μεγαλύτερος αριθμός προϊόντων τα οποία εντοπίστηκαν στο Amazon web services σε μία κατηγορία ήταν 13 (86.6%) και ο μικρότερος αριθμός προϊόντων τα οποία εντοπίστηκαν στο Amazon web services σε μία κατηγορία ήταν 1 (6.6%).
- Σε σύνολο 150 προϊόντων εντοπίστηκαν 79 προϊόντα (52.6%) τουλάχιστον στο Microsoft Azure. Συνεπώς, εφόσον έχουμε 10 κατηγορίες, κατά μέσο όρο 7.9 προϊόντα σε κάθε κατηγορία εντοπίστηκαν στο Amazon web services. Ο μεγαλύτερος αριθμός προϊόντων τα οποία εντοπίστηκαν στο Amazon web services σε μία κατηγορία ήταν 13 (86.6%) και ο μικρότερος αριθμός προϊόντων τα οποία εντοπίστηκαν στο Microsoft Azure σε μία κατηγορία ήταν 4 (26.6%).

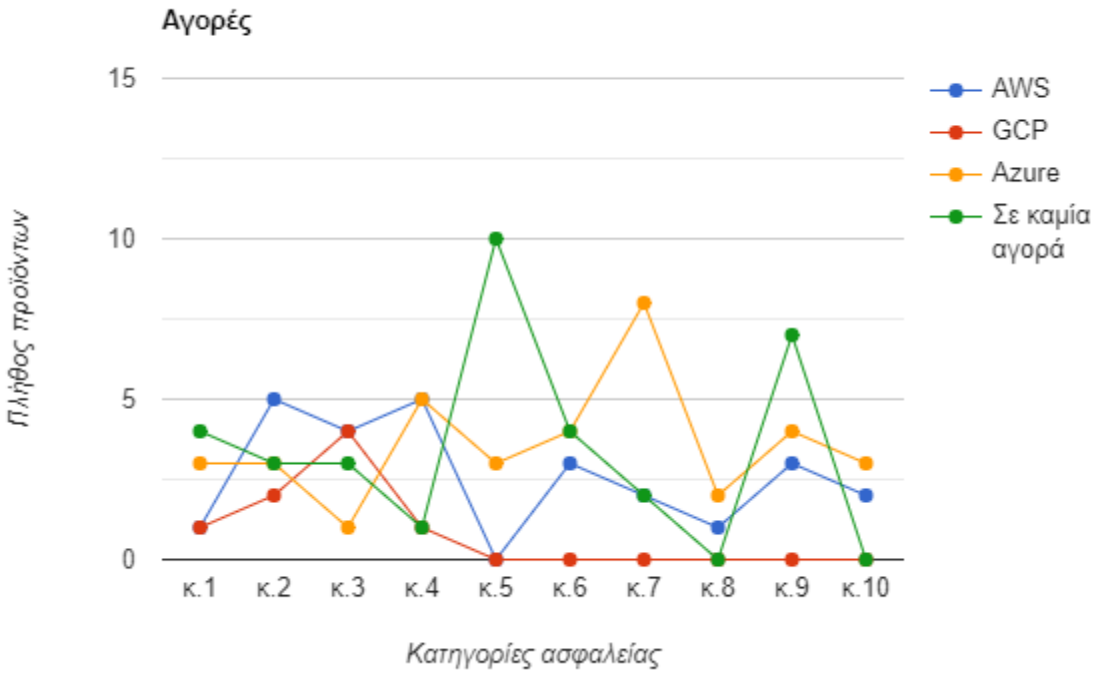
Παρατηρούμε πως οι πιο πλήρεις αγορές είναι η Microsoft Azure και Amazon web services καθώς και ο συνδυασμός τους. Στη συνέχεια ακολουθεί το Google cloud platform. Τέλος παρατηρούμε ότι ⅕ των προϊόντων δεν εντοπίστηκε σε κάποια αγορά. Τα αποτελέσματα είναι οριακά απογοητευτικά διότι μόνο σχεδόν το ⅓ των προϊόντων εντοπίστηκε σε 2 ή περισσότερες αγορές.



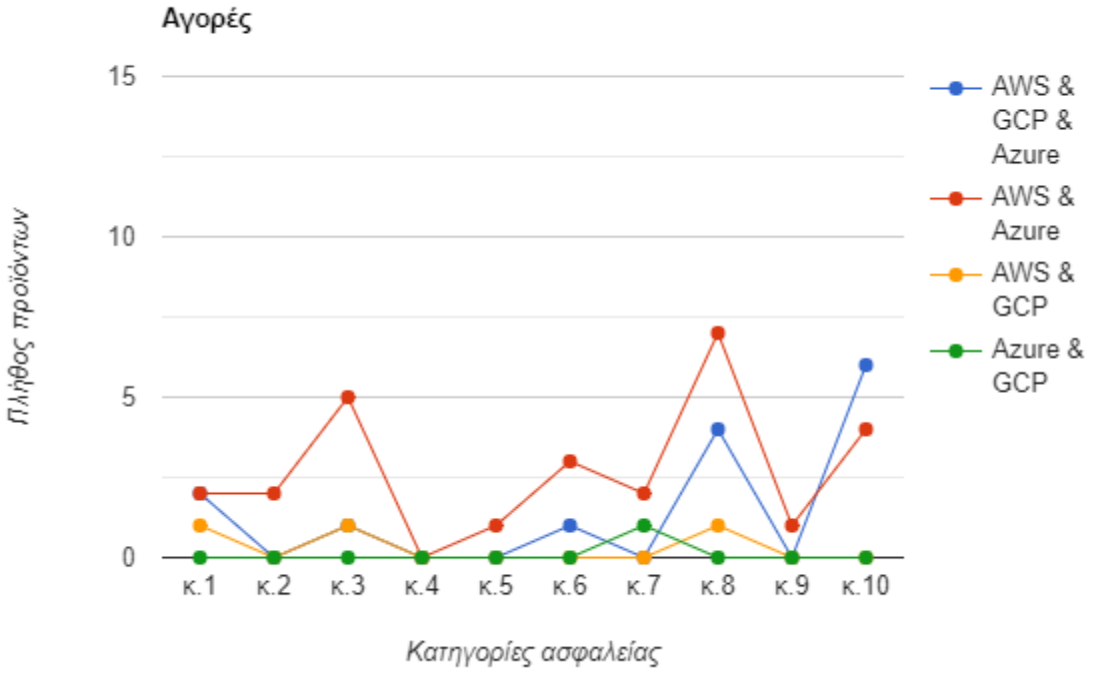
Εικόνα 15. Πλήθος προϊόντων που προσφέρονται σε μεμονωμένες αγορές ή σε καμία αγορά



Εικόνα 35. Πλήθος προϊόντων που προσφέρονται σε συνδυασμούς αγορών



Εικόνα 36. Πλήθος προϊόντων ανά κατηγορία που προσφέρονται σε μεμονωμένες αγορές ή σε καμία αγορά



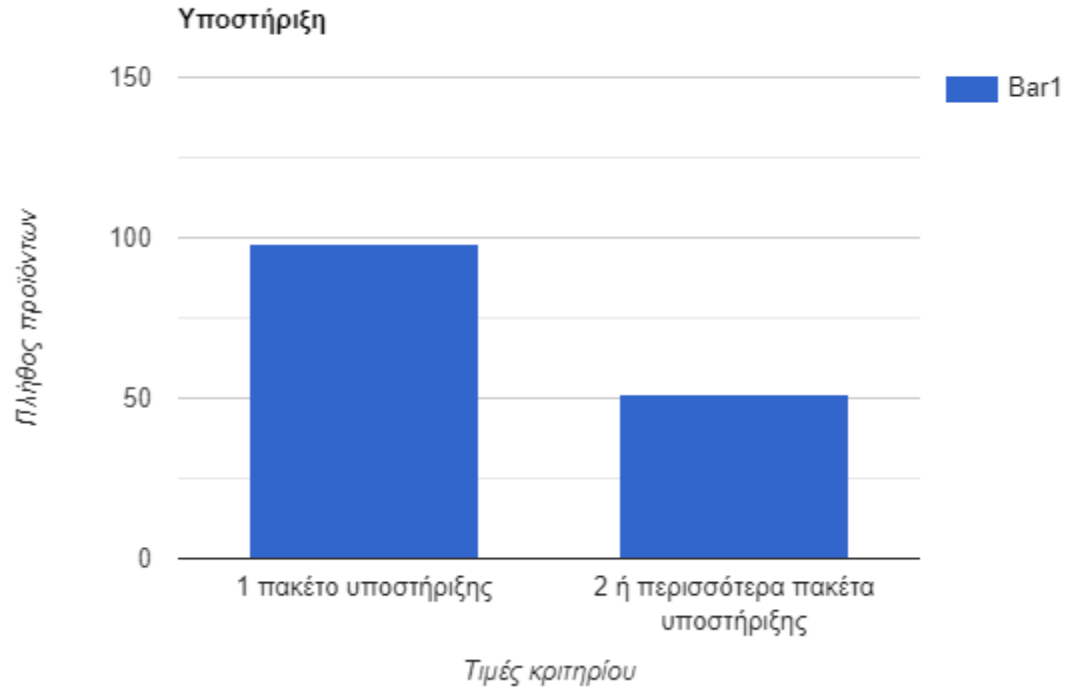
Εικόνα 37. Πλήθος προϊόντων ανά κατηγορία που προσφέρονται σε συνδυασμούς αγορών

5.3.14 Υποστήριξη

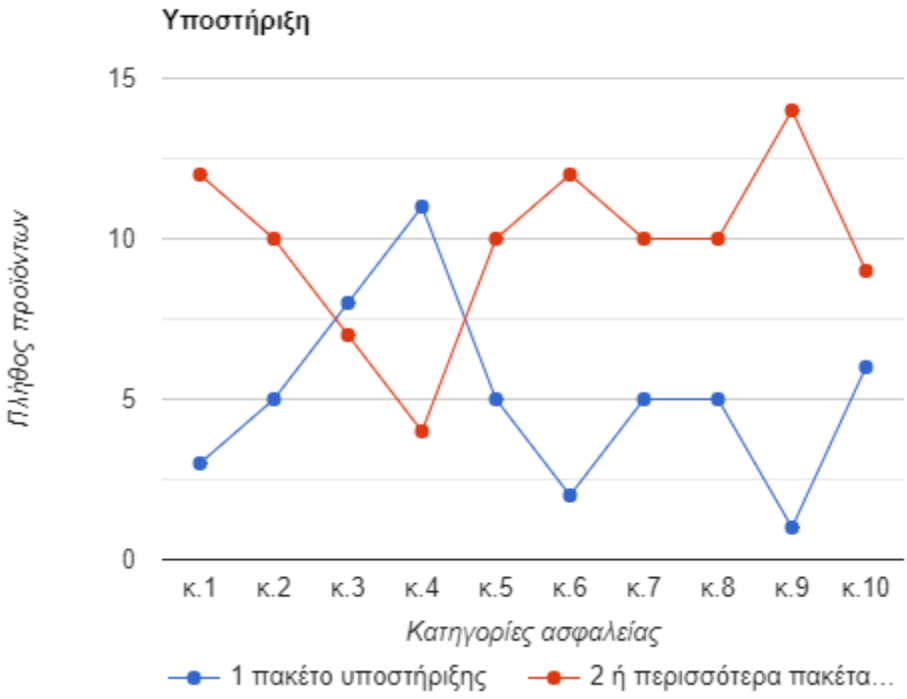
Αυτό το κριτήριο λόγω της φύσης των αποτελεσμάτων δεν διαθέτει διακριτές τιμές. Γι΄αυτό θεωρούμε πως υπάρχουν οι δύο παρακάτω τιμές: 1. προϊόντα με 2 ή περισσότερα πακέτα υποστήριξης και 2. προϊόντα με 1 πακέτο υποστήριξης. Τα συνολικά αποτελέσματα είναι τα εξής:

- Σε σύνολο 150 προϊόντων εντοπίστηκαν 51 προϊόντα (34%) με 2 ή περισσότερα πακέτα υποστήριξης. Ο μεγαλύτερος αριθμός προϊόντων με 2 ή περισσότερα πακέτα υποστήριξης σε μία κατηγορία ήταν 11 (73.3%) και ο μικρότερος αριθμός προϊόντων με 2 ή περισσότερα πακέτα υποστήριξης σε μία κατηγορία ήταν 1 (6.6%). Κατά μέσο όρο 5.1 προϊόντα σε κάθε κατηγορία διαθέτουν 2 ή περισσότερα πακέτα υποστήριξης.
- Σε σύνολο 150 προϊόντων εντοπίστηκαν 99 προϊόντα (66%) με 1 πακέτο υποστήριξης. Ο μεγαλύτερος αριθμός προϊόντων με 1 πακέτο υποστήριξης σε μία κατηγορία ήταν 14 (93.3%) και ο μικρότερος αριθμός προϊόντων με 1 πακέτο υποστήριξης σε μία κατηγορία ήταν 4 (26.6%). Κατά μέσο όρο 9.8 προϊόντα σε κάθε κατηγορία διαθέτουν 1 πακέτο υποστήριξης.

Παρατηρούμε ότι το ⅓ των προϊόντων προσφέρει δύο ή περισσότερα πακέτα υποστήριξης ενώ τα ⅔ των προϊόντων προσφέρουν μόνο ένα πακέτο. Τα αποτελέσματα είναι οριακά μη ικανοποιητικά.



Εικόνα 38. Πλήθος προϊόντων που προσφέρουν είτε 1 πακέτο υποστήριξης είτε περισσότερα



Εικόνα 39. Πλήθος προϊόντων ανά κατηγορία που προσφέρουν είτε ένα πακέτο υποστήριξης είτε περισσότερα

6 Συμπεράσματα και μελλοντικές κατευθύνσεις

6.1 Συμπεράσματα

Σε αυτή την εργασία παρουσιάστηκαν οι βασικές έννοιες για το υπολογιστικό νέφος και την ασφάλεια πληροφοριακών συστημάτων. Επίσης, παρουσιάστηκαν και αναλύθηκαν οι δέκα κατηγορίες προϊόντων λογισμικού σαν υπηρεσία ενώ με αφορμή την έλλειψη στοιχείων για αυτό το κομμάτι της αγοράς πραγματοποιήθηκε μια μεγάλη έρευνα σε 150 προϊόντα (15 ανά κατηγορία). Μέσα από την έρευνα προέκυψε ενδιαφέρουσα γνώση για τα προϊόντα και για τις κατηγορίες στις οποίες ανήκουν αλλά και συνολικά κατά μήκος όλων των κατηγοριών. Επιπλέον, δημιουργήθηκαν ορισμένα γραφήματα με στόχο την οπτική απεικόνιση των καθολικών αποτελεσμάτων.

Τα πολύ θετικά σημεία/συμπεράσματα που εντοπίστηκαν ήταν τα παρακάτω:

- 135 προϊόντα (90%) υποστηρίζουν βασική & επιπλέον λειτουργικότητα
- 112 προϊόντα (74.6%) διαθέτουν δωρεάν δοκιμαστική έκδοση. Από τα προϊόντα με δωρεάν δοκιμαστική έκδοση τα 83 (55.3%) έχουν χρονική διάρκεια μεγαλύτερη ή ίση των 30 ημερών
- 103 προϊόντα (68.6%) υποστηρίζουν δύο ή περισσότερους τρόπους χρήσης

Επίσης, η κατηγορία που έχει την καλύτερη απόδοση στα προϊόντα της ως προς τα κριτήρια που έχουν τεθεί είναι η ασφάλεια δικτύου.

Τα πολύ αρνητικά σημεία/συμπεράσματα που εντοπίστηκαν ήταν τα παρακάτω:

- Μόνο 16 προϊόντα (22%) υποστηρίζουν δύο ή περισσότερους τρόπους παράδοσης
- Μόνο 17 προϊόντα (11.3%) υποστηρίζουν δύο ή περισσότερα μοντέλα διάταξης
- Μόνο 33 προϊόντα (22%) υποστηρίζουν δύο ή περισσότερα πακέτα τιμολόγησης

Επιπλέον, η κατηγορία που έχει την χειρότερη απόδοση στα προϊόντα της ως προς τα κριτήρια που έχουν τεθεί είναι η αποτίμηση ασφαλείας.

6.2 Μελλοντικές κατευθύνσεις

Στα πλαίσια της εργασίας πραγματοποιήθηκε αποτίμηση προϊόντων με ορισμένες παραδοχές ως προς την έκταση και τη μεθοδολογία, οι οποίες μελλοντικά θα μπορούσαν να αλλάξουν. Παρακάτω παρουσιάζονται οι αλλαγές που θα μπορούσαν να πραγματοποιηθούν μελλοντικά:

1. Θα μπορούσε να αυξηθεί ο αριθμός των προϊόντων τα οποία αποτιμήθηκαν (ανά κατηγορία)
2. Θα μπορούσαν να εξεταστούν και άλλες αγορές (πχ Oracle Cloud Marketplace, Alibaba) εκτός από τις Amazon web services, Microsoft Azure και Google cloud platform
3. Θα μπορούσαν να δημιουργηθούν στατιστικά στοιχεία για κάθε μια από τις λειτουργικότητες που εντοπίζεται σε κάθε ένα προϊόν μιας κατηγορίας και να δημιουργηθούν ειδικές ταξινομίες λειτουργικότητας για κάθε κατηγορία προϊόντων.
4. Θα μπορούσαν να δημιουργηθούν συνολικά στατιστικά για τα αντικείμενα που προστατεύονται ένα προς ένα.
5. Θα μπορούσαν να δημιουργηθούν συνολικά στατιστικά για τις απειλές που αντιμετωπίζονται μία προς μία και να γίνουν κατάλληλες ομαδοποιήσεις όπου είναι εφικτό (πχ απειλές, αντικείμενα) ώστε να προκύψουν ακόμη πιο ενδιαφέροντα αποτελέσματα.

Μια ακόμα πρόταση σχετικά με τον τρόπο διεξαγωγής της έρευνας είναι η παρακάτω:

Στην παρούσα έρευνα ως νικητήριο προϊόν για κάθε κατηγορία θεωρείται το προϊόν με τη μεγαλύτερη συχνότητα εμφάνισης ως νικητήριο στα κριτήρια για την κάθε κατηγορία. Ένας άλλος τρόπος για να προκύψουν νικητήρια προϊόντα θα ήταν να μοιραστούν ερωτηματολόγια σε εταιρείες/εν δυνάμει αγοραστές όπου να τους ζητείται να κατατάξουν τα κριτήρια της έρευνας με φθίνουσα σειρά σπουδαιότητας. Στη συνέχεια για να βγει το νικητήριο προϊόν για κάθε κατηγορία μπορούν να ελέγχονται τα κριτήρια με βάση τον βαθμό σημαντικότητας, ο οποίος προσδιορίζεται με σχετικά βάρη για κάθε κριτήριο.
Έτσι, λοιπόν, θα προκύπταν νικητήρια προϊόντα τα οποία είναι νικητήρια και μέσα από τη ματιά ενός ερευνητή αλλά κυρίως μέσα από τη ματιά ενός υποψήφιου αγοραστή, ο οποίος είναι και ο άμεσα ενδιαφερόμενος για να αποκτήσει ένα προϊόν.

Τέλος, θα μπορούσε να δημιουργηθεί ένα μοντέλο περιγραφής για αυτό το είδος υπηρεσιών, το οποίο να διευκολύνει την περιγραφή και την αναζήτησή τους. Αυτό το μοντέλο μπορεί να εφαρμοστεί σε μία εφαρμογή ιστού για την περιγραφή/παρουσίαση και ανακάλυψη/αναζήτηση προϊόντων SecaaS. Το πλεονέκτημα αυτού του μοντέλου σε σχέση με ένα απλό marketplace είναι πως οι χρήστες θα έχουν τη δυνατότητα να εφαρμόσουν σύνθετα φίλτρα αναζήτησης ώστε να βρουν τα προϊόντα που ταιριάζουν καλύτερα στις ανάγκες τους (π.χ. αναζήτηση προϊόντων της κατηγορίας ασφάλειας ιστού, τα οποία να προστατεύουν από λυτρισμικό).

Βιβλιογραφία

[1] T. Erl, R. Puttini, και Z. Mahmood, *Cloud computing: concepts, technology, & architecture*. Upper Saddle River, NJ: Prentice Hall, 2013.

[2] Κ. Κρητικός, '321-11001 – Τεχνολογίες Νέφους, ΕΙΣΑΓΩΓΗ ΣΤΟ ΥΠΟΛΟΓΙΣΤΙΚΟ ΝΕΦΟΣ'. 2021.

[3] Κ. Κρητικός, '321-11001 – Τεχνολογίες Νέφους, 2η ΔΙΑΛΕΞΗ – ΘΕΜΕΛΙΩΔΗΣ ΑΡΧΕΣ & ΜΟΝΤΕΛΑ'. 2021.

[4] K. Chandrasekaran, *Essentials of cloud computing*. Boca Raton London New York: CRC Press Taylor & Francis Group, 2015.

[5] ''Data is the new oil, new gold,' says PM Modi in Houston', *Hindustan Times*, 23 Σεπτέμβριος 2019. https://www.hindustantimes.com/india-news/data-is-the-new-oil-new-gold-says-pm-modi-in-houston/story-SphHDPQadvF1dJRMXHCkwK.html (ημερομηνία πρόσβασης 29 Αύγουστος 2022).

[6] 'What is Information Systems Security (INFOSEC)? - Definition from Techopedia', *Techopedia.com*. http://www.techopedia.com/definition/24840/information-systems-security-infosec (ημερομηνία πρόσβασης 29 Αύγουστος 2022).

[7] 'Ασφάλεια Πληροφοριακών Συστημάτων και Υποδομών: Εννοιολογική Θεμελίωση - PDF Free Download'. https://docplayer.gr/2042262-Asfaleia-pliroforiakon-systimaton-kai-ypodomon-ennoiologiki-themeliosi.html (ημερομηνία πρόσβασης 29 Αύγουστος 2022).

[8] 'Confidentiality, Integrity, and Availability (CIA) triad | CCNA Security#'. https://geek-university.com/confidentiality-integrity-and-availability-cia-triad/ (ημερομηνία πρόσβασης 29 Αύγουστος 2022).

[9] 'The CIA triad: Definition, components and examples | CSO Online'. https://www.csoonline.com/article/3519908/the-cia-triad-definition-components-and-examples.html (ημερομηνία πρόσβασης 29 Αύγουστος 2022).

[10] ‘Information security’, *Wikipedia*. 20 Αύγουστος 2022. Ημερομηνία πρόσβασης: 29 Αύγουστος 2022. [Έκδοση σε ψηφιακή μορφή]. Διαθέσιμο στο: https://en.wikipedia.org/w/index.php?title=Information_security&oldid=1105432432

[11] T. Cameron, ‘Security: Public Cloud vs On-Premise Data Center’, *Eplexity*, 3 Νοέμβριος 2019. https://eplexity.com/blog/why-the-public-cloud-is-more-secure-than-an-on-premises-data-center/ (ημερομηνία πρόσβασης 29 Αύγουστος 2022).

[12] ‘What is a Cyber Attack? Definition, Examples and Prevention TechTarget’. https://www.techtarget.com/searchsecurity/definition/cyber-attack (ημερομηνία πρόσβασης 29 Αύγουστος 2022).

[13] ‘Denial-of-service attack’, *Wikipedia*. 19 Αύγουστος 2022. Ημερομηνία πρόσβασης: 29 Αύγουστος 2022. [Έκδοση σε ψηφιακή μορφή]. Διαθέσιμο στο: https://en.wikipedia.org/w/index.php?title=Denial-of-service_attack&oldid=1105366497

[14] ‘Brute-force attack’, *Wikipedia*. 25 Αύγουστος 2022. Ημερομηνία πρόσβασης: 29 Αύγουστος 2022. [Έκδοση σε ψηφιακή μορφή]. Διαθέσιμο στο: https://en.wikipedia.org/w/index.php?title=Brute-force_attack&oldid=1106615052

[15] ‘Dictionary attack’, *Wikipedia*. 19 Φεβρουάριος 2022. Ημερομηνία πρόσβασης: 29 Αύγουστος 2022. [Έκδοση σε ψηφιακή μορφή]. Διαθέσιμο στο: https://en.wikipedia.org/w/index.php?title=Dictionary_attack&oldid=1072762838

[16] Κ. Κρητικός, ‘321-9703 — Ασφάλεια Δικτύων Υπολογιστών & Τεχνολογίες Προστασίας της Ιδιωτικότητας, 1η ΔΙΑΛΕΞΗ –ΕΙΣΑΓΩΓΗ’. 2021.

[17] ‘What is multifactor authentication (MFA) and how does it work?’, *SearchSecurity*. https://www.techtarget.com/searchsecurity/definition/multifactor-authentication-MFA (ημερομηνία πρόσβασης 29 Αύγουστος 2022).

[18] ΝΟΥΣΚΑΛΗΣ ΓΕΩΡΓΙΟΣ, ‘Πρόγραμμα Ενημερότητας στην Ασφάλεια Πληροφοριών Δημόσιων Οργανισμών’, Μεταπτυχιακή εργασία, ΠΑΝΕΠΙΣΤΗΜΙΟ ΑΙΓΑΙΟΥ, Σάμος, 2019. [Έκδοση σε ψηφιακή μορφή]. Διαθέσιμο στο: https://hellanicus.lib.aegean.gr/bitstream/handle/11610/18584/Nouskalis%20Georgios%20Infromation%20Security%20Awareness.pdf?sequence=5

[19] S. Security, ‘How to Prevent Malware Attacks (7 Ways)’, *Savvy Security*, 29 Μάιος 2021. https://cheapsslsecurity.com/blog/how-to-prevent-malware-attacks/ (ημερομηνία πρόσβασης 29 Αύγουστος 2022).

[20] ΠΑΝΑΓΙΩΤΟΠΟΥΛΟΣ ΕΥΑΓΓΕΛΟΣ, ‘ΠΡΟΣΤΑΣΙΑ ΚΑΙ ΑΝΙΧΝΕΥΣΗ ΑΠΟ ΕΠΙΘΕΣΕΙΣ ΤΥΠΟΥ SQL INJECTION’, Προπτυχιακή εργασία, ΠΑΝΕΠΙΣΤΗΜΙΟ ΔΥΤΙΚΗΣ ΑΤΤΙΚΗΣ, Αθήνα, 2021. [Έκδοση σε ψηφιακή μορφή]. Διαθέσιμο στο: https://polynoe.lib.uniwa.gr/xmlui/bitstream/handle/11400/936/Panagiotopoulos_44003.pdf?sequence=3&isAllowed=y

[21] ‘Cross Site Scripting (XSS) | OWASP Foundation’. https://owasp.org/www-community/attacks/xss/ (ημερομηνία πρόσβασης 29 Αύγουστος 2022).

[22] ‘DOM Based XSS | OWASP Foundation’. https://owasp.org/www-community/attacks/DOM_Based_XSS (ημερομηνία πρόσβασης 29 Αύγουστος 2022).

[23] ‘Cross Site Scripting Prevention · OWASP Cheat Sheet Series’. https://owasp.deteact.com/cheat/cheatsheets/Cross_Site_Scripting_Prevention_Cheat_Sheet.html (ημερομηνία πρόσβασης 29 Αύγουστος 2022).

[24] Κ. Κρητικός, ‘321-11001 – Τεχνολογίες Νέφους, 3η ΔΙΑΛΕΞΗ – ΑΡΧΙΤΕΚΤΟΝΙΚΗ & ΤΕΧΝΟΛΟΓΙΑ ΕΝΕΡΓΟΠΟΙΗΣΗΣ ΝΕΦΟΥΣ’. 2021.

[25] Μήλιος Αθανάσιος, ‘ΜΕΛΕΤΗ ΖΗΤΗΜΑΤΩΝ ΙΔΙΩΤΙΚΟΤΗΤΑΣ ΣΕ ΥΠΟΛΟΓΙΣΤΙΚΑ ΝΕΦΗ’, Μεταπτυχιακή εργασία, ΜΑΚΕΔΟΝΙΑΣ, Θεσσαλονίκη, 2020. [Έκδοση σε ψηφιακή μορφή]. Διαθέσιμο στο: https://dspace.lib.uom.gr/bitstream/2159/24568/4/MiliosAthanasiosMsc2020.pdf

[26] Κ. Κρητικός, ‘321-11001 – Τεχνολογίες Δικτύων και Νέφους, ΘΕΜΑΤΑ & ΜΗΧΑΝΙΣΜΟΙ ΑΣΦΑΛΕΙΑΣ ΣΤΟ ΝΕΦΟΣ’. 2021.

[27] N. M. Almutairy και K. H. A. Al-Shqeerat, ‘A Survey on Security Challenges of Virtualization Technology in Cloud Computing’, *IJCSIT*, τ. 11, τχ. 03, σσ. 95–105, Ιουνίου 2019, doi: 10.5121/ijcsit.2019.11308.

[28] Κολόμβος Ιωάννης, ‘Examination of cloud systems’ security from virtualization perspective’, Προπτυχιακή εργασία, ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΕΙΡΑΙΩΣ, Πειραιάς, 2017. [Έκδοση

σε ψηφιακή μορφή]. Διαθέσιμο στο: https://dione.lib.unipi.gr/xmlui/bitstream/handle/unipi/10540/Kolomvos_Ioannis.pdf?sequence=1&isAllowed=y

[29] M. Kazim, R. Masood, M. A. Shibli, και A. G. Abbasi, 'Security Aspects of Virtualization in Cloud Computing', στο *Computer Information Systems and Industrial Management*, τ. 8104, K. Saeed, R. Chaki, A. Cortesi, και S. Wierzchoń, Επιμ. Berlin, Heidelberg: Springer Berlin Heidelberg, 2013, σσ. 229–240. doi: 10.1007/978-3-642-40925-7_22.

[30] 'Security as a Service Working Group | CSA'. https://cloudsecurityalliance.org/research/working-groups/security-as-a-service/ (ημερομηνία πρόσβασης 29 Αύγουστος 2022).

[31] 'What is Security Information Management (SIM)? - Definition from Techopedia', *Techopedia.com*. http://www.techopedia.com/definition/4098/security-information-management (ημερομηνία πρόσβασης 29 Αύγουστος 2022).

[32] 'What is Security Information Management (SIM)? - Definition from Techopedia', *Techopedia.com*. http://www.techopedia.com/definition/4098/security-information-management (ημερομηνία πρόσβασης 29 Αύγουστος 2022).

[33] 'What is Security Incident and Event Management (SIEM)? - Definition from Techopedia', *Techopedia.com*. http://www.techopedia.com/definition/4097/security-incident-and-event-management-siem (ημερομηνία πρόσβασης 29 Αύγουστος 2022).

[34] 'Security Information and Event Management (SIEM)', *IT SECURITY PRO: Περιοδικό για το Business IT και την ασφάλεια πληροφοριών!*, 21 Μάρτιος 2017. https://www.itsecuritypro.gr/security-information-event-management-siem/ (ημερομηνία πρόσβασης 29 Αύγουστος 2022).

[35] Datashield, 'On-Premise vs Cloud SIEM - Advantages & Disadvantages, SaaS, Gartner'. https://www.datashieldprotect.com/blog/on-premises-vs-cloud-siem (ημερομηνία πρόσβασης 29 Αύγουστος 2022).

[36] J. Pavlik, A. Komarek, και V. Sobeslav, 'Security information and event management in the cloud computing infrastructure', στο *2014 IEEE 15th International Symposium on*

Computational Intelligence and Informatics (CINTI), Budapest, Νοεμβρίου 2014, σσ. 209–214. doi: 10.1109/CINTI.2014.7028677.

[37] 'SFTP protocol, clients, servers etc. Page by the original author of SFTP.' https://www.ssh.com/academy/ssh/sftp (ημερομηνία πρόσβασης 29 Αύγουστος 2022).

[38] 'Net-SNMP'. http://www.net-snmp.org/ (ημερομηνία πρόσβασης 29 Αύγουστος 2022).

[39] R. Gerhards, 'The Syslog Protocol', Internet Engineering Task Force, Request for Comments RFC 5424, Νοεμβρίου 2009. doi: 10.17487/RFC5424.

[40] 'User Datagram Protocol', Internet Engineering Task Force, Request for Comments RFC 768, Δεκεμβρίου 1980. doi: 10.17487/RFC0768.

[41] M. Vielberth και G. Pernul, 'A Security Information and Event Management Pattern', σ. 12.

[42] A. Majeed, R. ur Rasool, F. Ahmad, M. Alam, και N. Javaid, 'Near-miss situation based visual analysis of SIEM rules for real time network security monitoring', *J Ambient Intell Human Comput*, τ. 10, τχ. 4, σσ. 1509–1526, Απριλίου 2019, doi: 10.1007/s12652-018-0936-7.

[43] 'What is Business Continuity and Disaster Recovery (BCDR)? - Definition from Techopedia', *Techopedia.com*. http://www.techopedia.com/definition/13767/business-continuity-and-disaster-recovery-bcdr (ημερομηνία πρόσβασης 29 Αύγουστος 2022).

[44] T. Wood, E. Cecchet, K. Ramakrishnan, P. Shenoy, και J. Merwe, 'Disaster Recovery as a Cloud Service: Economic Benefits & Deployment Challenges', Αυγούστου 2010.

[45] S. Suguna και A. Suhasini, 'Overview of data backup and disaster recovery in cloud', στο *International Conference on Information Communication and Embedded Systems (ICICES2014)*, Οκτωβρίου 2014, σσ. 1–7. doi: 10.1109/ICICES.2014.7033804.

[46] M. A. Srinivas, Y. S. Ramayya, και H. B. Venkatesh, 'A Study on Cloud Computing Disaster Recovery'.

[47] C. C. Editor, ‘intrusion detection system (IDS) - Glossary | CSRC’. https://csrc.nist.gov/glossary/term/intrusion_detection_system (ημερομηνία πρόσβασης 29 Αύγουστος 2022).

[48] Κ. Κρητικός, ‘321-9703 — Ασφάλεια Δικτύων Υπολογιστών & Τεχνολογίες Προστασίας της Ιδιωτικότητας, ΔΙΑΛΕΞΗ 7 – Αναχώματα Ασφάλειας & Συστήματα Ανίχνευσης Εισβολών’. 2021.

[49] Β. Ρούσσος, ‘ΣΥΣΤΗΜΑΤΑ ΑΝΙΧΝΕΥΣΗΣ & ΔΙΑΧΕΙΡΙΣΗΣ ΕΙΣΒΟΛΩΝ ΔΙΑΧΕΙΡΙΣΗ LOGS’, Μεταπτυχιακή εργασία, Πανεπιστήμιο Πειραιώς, Πειραιάς, 2012. [Έκδοση σε ψηφιακή μορφή]. Διαθέσιμο στο: https://dione.lib.unipi.gr/xmlui/bitstream/handle/unipi/5824/Roussos.pdf?sequence=2&isAllowed=y

[50] A. Zarrabi και A. Zarrabi, ‘Internet Intrusion Detection System Service in a Cloud’.

[51] R. Sekar *κ.ά.*, ‘Specification-based anomaly detection: a new approach for detecting network intrusions’, στο *Proceedings of the 9th ACM conference on Computer and communications security - CCS ’02*, Washington, DC, USA, 2002, σ. 265. doi: 10.1145/586110.586146.

[52] D. Strom, ‘What is IAM? Identity and access management explained’, *CSO Online*, 8 Απρίλιος 2021. https://www.csoonline.com/article/2120384/what-is-iam-identity-and-access-management-explained.html (ημερομηνία πρόσβασης 29 Αύγουστος 2022).

[53] M. A. Thakur και R. Gaikwad, ‘User identity and Access Management trends in IT infrastructure- an overview’, στο *2015 International Conference on Pervasive Computing (ICPC)*, Ιανουαρίου 2015, σσ. 1–4. doi: 10.1109/PERVASIVE.2015.7086972.

[54] ‘RBAC vs. ABAC Access Control: What’s the Difference? - DNSstuff’, *Software Reviews, Opinions, and Tips - DNSstuff*, 31 Οκτώβριος 2019. https://www.dnsstuff.com/rbac-vs-abac-access-control (ημερομηνία πρόσβασης 29 Αύγουστος 2022).

[55]

L. Brad και A. Munteanu, *AN ADJUSTMENT MODEL FOR EVA COMPUTATION IN FINANCIAL INSTITUTIONS AND NON-FINANCIAL COMPANIES*. 2012.

[56] Ν. Μαούνης, 'Αυθεντικοποίηση στο διαδίκτυο (με έμφαση στην Ελλάδα)', Προπτυχιακή εργασία, Πανεπιστήμιο Πειραιώς, Πειραιάς, 2011. [Έκδοση σε ψηφιακή μορφή]. Διαθέσιμο στο: https://dione.lib.unipi.gr/xmlui/bitstream/handle/unipi/4053/Maounis.pdf?sequence=2&isAllowed=y

[57] Nick Ragouzis, Enosis Group LLC, John Hughes, PA Consulting, Rob Philpott, EMC Corporation, Eve Maler, Sun Microsystems, Paul Madsen, NTT, και om Scavo, NCSA/University of Illinois, 'Security Assertion Markup Language (SAML) V2.0 Technical Overview', 25 Μάρτιος 2008. http://docs.oasis-open.org/security/saml/Post2.0/sstc-saml-tech-overview-2.0-cd-02.html (ημερομηνία πρόσβασης 29 Αύγουστος 2022).

[58] 'A Brief Introduction to XACML'. https://www.oasis-open.org/committees/download.php/2713/Brief_Introduction_to_XACML.html (ημερομηνία πρόσβασης 29 Αύγουστος 2022).

[59] Tim Moses, Entrust Inc., 'oasis-access_control-xacml-2.0-core-spec-os'. 1 Φεβρουάριος 2005. [Έκδοση σε ψηφιακή μορφή]. Διαθέσιμο στο: https://docs.oasis-open.org/xacml/2.0/access_control-xacml-2.0-core-spec-os.pdf

[60] R. Tahboub και Y. Saleh, 'Data Leakage/Loss Prevention Systems (DLP)', στο *2014 World Congress on Computer Applications and Information Systems (WCCAIS)*, Ιανουαρίου 2014, σσ. 1–6. doi: 10.1109/WCCAIS.2014.6916624.

[61] Κ. Τσιμπερδώνης, 'Προστασία Εμπιστευτικών Πληροφοριών: Η Τεχνολογία Πρόληψης Διαρροής Δεδομένων - (Data Leakage Prevention- DLP)- στην υπηρεσία της Ασφάλειας Πληροφοριών', Μεταπτυχιακή εργασία, Πανεπιστήμιο Πειραιώς, ΑΘΗΝΑ, 2013. [Έκδοση σε ψηφιακή μορφή]. Διαθέσιμο στο: https://dione.lib.unipi.gr/xmlui/bitstream/handle/unipi/8472/Tsimberdonis_Konstantinos.pdf?sequence=5&isAllowed=y

[62] E. Costante, D. Fauri, S. Etalle, J. den Hartog, και N. Zannone, 'A Hybrid Framework for Data Loss Prevention and Detection', στο *2016 IEEE Security and Privacy Workshops (SPW)*, Φεβρουαρίου 2016, σσ. 324–333. doi: 10.1109/SPW.2016.24.

[63] Θ. Β. Δημητρίου, 'ΑΠΟΤΡΟΠΗ ΔΙΑΡΡΟΗΣ ΔΕΔΟΜΕΝΩΝ', Προπτυχιακή εργασία, ΠΑΝΕΠΙΣΤΗΜΙΟ ΜΑΚΕΔΟΝΙΑΣ, Θεσσαλονίκη, 2017. [Έκδοση σε ψηφιακή μορφή]. Διαθέσιμο στο: https://dspace.lib.uom.gr/bitstream/2159/24705/1/DimitriouTheofanisMsc2017.pdf

[64] C. C. Editor, 'encryption - Glossary | CSRC'. https://csrc.nist.gov/glossary/term/encryption (ημερομηνία πρόσβασης 29 Αύγουστος 2022).

[65] 'Κρυπτογραφία', *Βικιπαίδεια*. 10 Ιανουάριος 2022. Ημερομηνία πρόσβασης: 29 Αύγουστος 2022. [Έκδοση σε ψηφιακή μορφή]. Διαθέσιμο στο: https://el.wikipedia.org/w/index.php?title=%CE%9A%CF%81%CF%85%CF%80%CF%84%CE%BF%CE%B3%CF%81%CE%B1%CF%86%CE%AF%CE%B1&oldid=9243075

[66] Κ. ΑΠΟΣΤΟΛΙΔΟΥ, 'ΕΦΑΡΜΟΓΕΣ ΤΗΣ ΚΡΥΠΤΟΓΡΑΦΙΑΣ', Μεταπτυχιακή εργασία, ΠΑΝΕΠΙΣΤΗΜΙΟ ΜΑΚΕΔΟΝΙΑΣ, ΚΟΖΑΝΗ, 2008. [Έκδοση σε ψηφιακή μορφή]. Διαθέσιμο στο: https://dspace.lib.uom.gr/bitstream/2159/13357/2/ApostolidouMsc2008.pdf

[67] 'Advanced Encryption Standard', *Wikipedia*. 8 Ιούλιος 2022. Ημερομηνία πρόσβασης: 29 Αύγουστος 2022. [Έκδοση σε ψηφιακή μορφή]. Διαθέσιμο στο: https://en.wikipedia.org/w/index.php?title=Advanced_Encryption_Standard&oldid=1097012804

[68] C. Crane, 'Block Cipher vs Stream Cipher: What They Are & How They Work', *Hashed Out by The SSL Store™*, 14 Ιανουάριος 2021. https://www.thesslstore.com/blog/block-cipher-vs-stream-cipher/ (ημερομηνία πρόσβασης 29 Αύγουστος 2022).

[69] 'Public-key cryptography', *Wikipedia*. 26 Αύγουστος 2022. Ημερομηνία πρόσβασης: 29 Αύγουστος 2022. [Έκδοση σε ψηφιακή μορφή]. Διαθέσιμο στο: https://en.wikipedia.org/w/index.php?title=Public-key_cryptography&oldid=1106743096

[70] 'RSA (cryptosystem)', *Wikipedia*. 22 Αύγουστος 2022. Ημερομηνία πρόσβασης: 29 Αύγουστος 2022. [Έκδοση σε ψηφιακή μορφή]. Διαθέσιμο στο: https://en.wikipedia.org/w/index.php?title=RSA_(cryptosystem)&oldid=1106002202

[71] Α. ΠΑΠΑΔΟΠΟΥΛΟΣ, 'ΤΕΧΝΙΚΕΣ ΔΙΑΧΕΙΡΙΣΗΣ ΚΛΕΙΔΙΩΝ ΣΕ ΠΕΡΙΒΑΛΛΟΝ ΥΠΟΛΟΓΙΣΤΙΚΗΣ ΝΕΦΟΥΣ', Προπτυχιακή εργασία, ΑΛΕΞΑΝΔΡΕΙΟ Τ.Ε.Ι. ΘΕΣΣΑΛΟΝΙΚΗΣ, Θεσσαλονίκη, 2013. [Έκδοση σε ψηφιακή μορφή]. Διαθέσιμο στο: http://eureka.teithe.gr/jspui/bitstream/123456789/10789/1/Papadopoulos_Andreas.pdf

[72] 'What is Email Security? - Defining Security of Email | Proofpoint US', *Proofpoint*, 24 Φεβρουάριος 2021. https://www.proofpoint.com/us/threat-reference/email-security (ημερομηνία πρόσβασης 29 Αύγουστος 2022).

[73] W. Stallings και L. Brown, *Computer security: principles and practice*, Third edition. Boston: Pearson, 2015.

[74] 'Spamming', *Wikipedia*. 15 Αύγουστος 2022. Ημερομηνία πρόσβασης: 29 Αύγουστος 2022. [Έκδοση σε ψηφιακή μορφή]. Διαθέσιμο στο: https://en.wikipedia.org/w/index.php?title=Spamming&oldid=1104596611

[75] 'Spam protection technologies'. https://encyclopedia.kaspersky.com/knowledge/spam-protection-technologies/ (ημερομηνία πρόσβασης 29 Αύγουστος 2022).

[76] 'Naive Bayes spam filtering', *Wikipedia*. 14 Ιούνιος 2022. Ημερομηνία πρόσβασης: 29 Αύγουστος 2022. [Έκδοση σε ψηφιακή μορφή]. Διαθέσιμο στο: https://en.wikipedia.org/w/index.php?title=Naive_Bayes_spam_filtering&oldid=1093067172

[77] E. P. Sanz, J. M. Gómez Hidalgo, και J. C. Cortizo Pérez, 'Chapter 3 Email Spam Filtering', στο *Advances in Computers*, τ. 74, Elsevier, 2008, σσ. 45–114. doi: 10.1016/S0065-2458(08)00603-7.

[78] 'What is a spam filter?', *SearchSecurity*. https://www.techtarget.com/searchsecurity/definition/spam-filter (ημερομηνία πρόσβασης 29 Αύγουστος 2022).

[79] 'What is Email Spoofing? Definition & Examples | Proofpoint US', *Proofpoint*, 26 Φεβρουάριος 2021. https://www.proofpoint.com/us/threat-reference/email-spoofing (ημερομηνία πρόσβασης 29 Αύγουστος 2022).

[80] P. Resnick, 'Internet Message Format', Internet Engineering Task Force, Request for Comments RFC 5322, Ιουλίου 2008. doi: 10.17487/RFC5322.

[81] 'What is a DNSBL?', *GlockApps*. https://glockapps.com/blacklist/ (ημερομηνία πρόσβασης 29 Αύγουστος 2022).

[82] M. Kührer, C. Rossow, και T. Holz, 'Paint It Black: Evaluating the Effectiveness of Malware Blacklists', στο *Research in Attacks, Intrusions and Defenses*, Cham, 2014, σσ. 1–21. doi: 10.1007/978-3-319-11379-1_1.

[83] 'ANTI SPAM: Country-based filtering', *ANTI SPAM*. http://antispamkill.blogspot.com/2007/07/country-based-filtering.html (ημερομηνία πρόσβασης 29 Αύγουστος 2022).

[84] I. Fette, N. Sadeh, και A. Tomasic, 'Learning to detect phishing emails', στο *Proceedings of the 16th international conference on World Wide Web - WWW '07*, Banff, Alberta, Canada, 2007, σ. 649. doi: 10.1145/1242572.1242660.

[85] 'Ψηφιακή υπογραφή', *Βικιπαίδεια*. 28 Ιανουάριος 2022. Ημερομηνία πρόσβασης: 29 Αύγουστος 2022. [Έκδοση σε ψηφιακή μορφή]. Διαθέσιμο στο: https://el.wikipedia.org/w/index.php?title=%CE%A8%CE%B7%CF%86%CE%B9%CE%B1%CE%BA%CE%AE_%CF%85%CF%80%CE%BF%CE%B3%CF%81%CE%B1%CF%86%CE%AE&oldid=9285815

[86] Ν. ΑΠΟΣΤΟΛΟΠΟΥΛΟΥ και Β. ΔΑΡΑΜΟΥΣΚΑΣ, 'Προστασία Προσωπικών Δεδομένων στο Διαδίκτυο', Προπτυχιακή εργασία, ΤΕΧΝΟΛΟΓΙΚΟ ΕΚΠΑΙΔΕΥΤΙΚΟ ΙΔΡΥΜΑ ΜΕΣΟΛΟΓΓΙΟΥ, ΜΕΣΟΛΟΓΓΙ, 2008. [Έκδοση σε ψηφιακή μορφή]. Διαθέσιμο στο: https://www.ebusiness-lab.gr/files/dmdocuments/Ptyxiakes-old/PDFs/apostolo_daramou_prostasia_proswpikwn.pdf

[87] C. C. Editor, 'firewall - Glossary | CSRC'. https://csrc.nist.gov/glossary/term/firewall (ημερομηνία πρόσβασης 29 Αύγουστος 2022).

[88] Φ. Βουλγαράκη και Π.-Χ. Μπαμπέκος, ‘Ανάπτυξη και διαχείριση ενός αναχώματος ασφαλείας επιπέδου εφαρμογής (application level firewall) το οποίο θα δίνει τη δυνατότητα δημιουργίας αποστρατικοποιημένων ζωνών (demilitarized zones – DMZ)’, Προπτυχιακή εργασία, ΤΕΧΝΟΛΟΓΙΚΟ ΕΚΠΑΙΔΕΥΤΙΚΟ ΙΔΡΥΜΑ ΚΑΒΑΛΑΣ, ΚΑΒΑΛΑ, 2011. [Έκδοση σε ψηφιακή μορφή]. Διαθέσιμο στο: http://digilib.teiemt.gr/jspui/bitstream/123456789/2222/1/012011133.pdf

[89] Ι. ΑΝΤΩΝΑΤΟΣ και Β. ΚΡΙΚΑΣ, ‘ΑΣΦΑΛΕΙΑ ΔΙΚΤΥΩΝ ΚΑΙ ΣΥΣΤΗΜΑΤΑ ΑΝΙΧΝΕΥΣΗΣ ΚΑΙ ΑΠΟΚΡΙΣΗΣ ΕΠΙΘΕΣΕΩΝ’, Προπτυχιακή εργασία, ΤΕΧΝΟΛΟΓΙΚΟ ΕΚΠΑΙΔΕΥΤΙΚΟ ΙΔΡΥΜΑ ΔΥΤΙΚΗΣ ΕΛΛΑΔΑΣ, ΠΑΤΡΑ, 2016. [Έκδοση σε ψηφιακή μορφή]. Διαθέσιμο στο: http://repository.teiwest.gr/xmlui/bitstream/handle/123456789/5137/%CE%91%CE%A3%CE%A6%CE%91%CE%9B%CE%95%CE%99%CE%91%20%CE%94%CE%99%CE%9A%CE%A4%CE%A5%CE%A9%CE%9D%20%CE%9A%CE%91%CE%99%20%CE%A3%CE%A5%CE%A3%CE%A4%CE%97%CE%9C%CE%91%CE%A4%CE%91%20%CE%91%CE%9D%CE%99%CE%A7%CE%9D%CE%95%CE%A5%CE%A3%CE%97%CE%A3%20%CE%9A%CE%91%CE%99%20%CE%91%CE%A0%CE%9F%CE%9A%CE%A1%CE%99%CE%A3%CE%97%CE%A3%20%CE%95%CE%A0%CE%99%CE%98%CE%95%CE%A3%CE%95%CE%A9%CE%9D..pdf?sequence=1&isAllowed=y

[90] A. B. Kaimal, A. Unnikrishnan, και L. V. Namboothiri, ‘Blackholing VS. Sinkholing: a Comparative Analysis’, τ. 8, τχ. 7, σ. 3, 2019.

[91] ‘What is rate limiting? | Rate limiting and bots’, *Cloudflare*. https://www.cloudflare.com/learning/bots/what-is-rate-limiting/ (ημερομηνία πρόσβασης 29 Αύγουστος 2022).

[92] K. A. Scarfone, M. P. Souppaya, A. Cody, και A. D. Orebaugh, ‘Technical guide to information security testing and assessment.’, National Institute of Standards and Technology, Gaithersburg, MD, NIST SP 800-115, 2008. doi: 10.6028/NIST.SP.800-115.

[93] VMware, ‘VMware Cloud Web Security’. 20 Σεπτέμβριος 2021. [Έκδοση σε ψηφιακή μορφή]. Διαθέσιμο στο: https://www.vmware.com/content/dam/digitalmarketing/vmware/en/pdf/docs/vmware-sdwan-cloud-web-security.pdf

[94] ‘Web Security as a Service’, *Trend Micro*. https://www.trendmicro.com/en_vn/business/products/user-protection/sps/web-security/interscan-web-as-a-service.html (ημερομηνία πρόσβασης 29 Αύγουστος 2022).

[95] D. Strickland, ‘Web Content Filtering—What’s the Best Way to Block Websites?’, *CurrentWare*, 24 Μάρτιος 2021. https://www.currentware.com/blog/web-content-filtering/ (ημερομηνία πρόσβασης 29 Αύγουστος 2022).

[96] ‘What is URL filtering? | Web filtering’, *Cloudflare*. https://www.cloudflare.com/learning/access-management/what-is-url-filtering/ (ημερομηνία πρόσβασης 29 Αύγουστος 2022).

[97] ‘Malware Protection: Types, Tools and Best Practices’, *Hysolate*, 23 Σεπτέμβριος 2021. https://www.hysolate.com/learn/malware-protection/malware-protection-types-tools-and-best-practices/ (ημερομηνία πρόσβασης 29 Αύγουστος 2022).

[98] ‘Threat (computer)’, *Wikipedia*. 23 Μάιος 2022. Ημερομηνία πρόσβασης: 29 Αύγουστος 2022. [Έκδοση σε ψηφιακή μορφή]. Διαθέσιμο στο: https://en.wikipedia.org/w/index.php?title=Threat_(computer)&oldid=1089354429

[99] ‘πρόληψη’, *Βικιλεξικό*. 3 Φεβρουάριος 2022. Ημερομηνία πρόσβασης: 29 Αύγουστος 2022. [Έκδοση σε ψηφιακή μορφή]. Διαθέσιμο στο: https://el.wiktionary.org/w/index.php?title=%CF%80%CF%81%CF%8C%CE%BB%CE%B7%CF%88%CE%B7&oldid=5508433

Παράρτημα Ι Πίνακες αποτίμησης κεφαλαίου 5

Πίνακας Αποτίμησης 1 – Προϊόντα SIEM

ΚΡΙΤΗΡΙΑ/ΠΡΟΙΟΝΤΑ	**QRADAR**
α. τρόπος παράδοσης	SaaS, IaaS
β. μοντέλο διάταξης	δημόσιο
γ. κατηγορία υπηρεσιών στην οποία ανήκει	SIEM
δ. μοντέλο κόστους	τιμολόγηση με βάση τον όγκο των δεδομένων και χρέωση ανά μήνα
ε. μηχανισμοί ασφάλειας που υλοποιούνται	**Βασική λειτουργικότητα:** -Παρακολούθηση εσωτερικών απειλών με τον εντοπισμό αποκλίσεων από την κανονική συμπεριφορά των χρηστών -Αναφορές απειλών με προτεραιότητα σε πραγματικό χρόνο, με βάση τα επιχειρησιακά στοιχεία -Ανίχνευση απειλών με χρήση αναλυτικών στοιχείων σε πραγματικό χρόνο σε αρχεία καταγραφής -Αναγνώριση απειλών με τεχνητή νοημοσύνη με χρήση του επεξεργαστή ανάλυσης δεδομένων IBM Watson για την ασφάλεια στον κυβερνοχώρο **Επιπλέον λειτουργικότητα:** -Σάρωση και ιεράρχηση της διαχείρισης ευπάθειας για τη βελτίωση της διαχείρισης ενημερώσεων κώδικα -Το εργαλείο διαχείρισης κινδύνων δικτύου (Network Risk Manager) ποσοτικοποιεί και ιεραρχεί τους πιθανούς κινδύνους που προέρχονται από τα μοτίβα κίνησης του δικτύου
στ. μη λειτουργικές εγγυήσεις	Για διαθεσιμότητα χαμηλότερη από 99,9% πίστωση 2% της μηνιαίας χρέωσης συνδρομής, για < 99,0% πίστωση 5% και για < 95% πίστωση 10%.
ζ. είδος προσφερόμενης προστασίας	ανιχνευτική
η. ιδιότητες ασφάλειας	ακεραιότητα
θ. αντικείμενα που προστατεύονται	δεδομένα του οργανισμού

ι. απειλές που αντιμετωπίζονται	απώλεια δεδομένων, κλοπή ή απάτη
ια. περιορισμοί	συλλογή έως 20000 γεγονότα/δευτ.
ιβ. ύπαρξη δωρεάν εκδόσεων	14 μέρες δωρεάν
ιγ. τρόπος χρήσης προϊόντος	Rest api,Cli, , Web based gui
ιδ. εταιρεία που προσφέρει το προϊόν	IBM
ιε. marketplace(s) όπου προσφέρεται το προϊόν	AWS, GCP , Azure
ιστ. επίπεδο/είδος υποστήριξης για το προϊόν	επικοινωνία με τηλέφωνο, email, συχνές ερωτήσεις, τεκμηρίωση, έγγραφα, πύλη (portal) υποστήριξης, κέντρο επιδιόρθωσης προβλημάτων, λίστα με όλες τις διαθέσιμες εκδόσεις λογισμικού, βίντεο, λογαριασμός στο Twitter

Elastic Security solution SIEM	**SPLUNK Enterprise Security SIEM**
SaaS	IaaS
δημόσιο	δημόσιο, ιδιωτικό, υβριδικό
SIEM	SIEM
4 πακέτα, τιμολόγηση με βάση τους πόρους υλικού	τιμολόγηση με βάση το φόρτο εργασίας
Βασική λειτουργικότητα: -Ενσωματώσεις cloud και δυνατότητες παρακολούθησης -Ενσωμάτωση με τα οικοσυστήματα ασφάλειας -Ανίχνευση ανωμαλιών -Κανόνες ανίχνευσης απειλών -Κανόνες μηχανικής εκμάθησης -Συσχετισμός γεγονότων -Προκατασκευασμένοι κανόνες ανίχνευσης **Επιπλέον λειτουργικότητα:** -Προσαρμοσμένα ερωτήματα για ανίχνευση συμβάντων -Κανόνες κατωφλίου για ειδοποιήσεις -Εντοπισμός με δεδομένα τρίτων (ευφυΐα απειλών) -Μηχανισμός ανίχνευσης που βασίζεται σε	**Βασική λειτουργικότητα:** -Συλλογή αρχείων καταγραφής και συμβάντων -Εφαρμογή κανόνων συσχέτισης σε πραγματικό χρόνο -Εφαρμογή προηγμένων αναλυτικών στοιχείων και μηχανικής μάθησης σε πραγματικό χρόνο -Αναζήτηση και αναφορά κανονικοποιημένων δεδομένων -Αναζήτηση και αναφορά σε ανεπεξέργαστα δεδομένα **Επιπλέον λειτουργικότητα:** -Μακροπρόθεσμες ιστορικές αναλύσεις και μηχανική μάθηση -Μακροπρόθεσμη αποθήκευση συμβάντων -Απορρόφηση δεδομένων περιβάλλοντος για επιπλέον συσχέτιση και ανάλυση

ένα τυποποιημένο πλαίσιο κυβερνοασφάλειας (MITTRe ATT&CK)	
---	100% Διαθεσιμότητα Για 99.99-99.999% διαθεσιμότητα ανά τρίμηνο πίστωση του κόστους συνδρομής για 2 ώρες χρήσης Για 99.9-99.99% διαθεσιμότητα πίστωση για 4 ώρες Για 99.0-99.9% διαθεσιμότητα πίστωση για 8 ώρες Για 95.0-99.0% διαθεσιμότητα πίστωση για 1 μέρα Για 0-95.0% διαθεσιμότητα πίστωση για 1 μήνα
ανιχνευτική	ανιχνευτική
ακεραιότητα	ακεραιότητα
οτιδήποτε	οτιδήποτε
κακόβουλο λογισμικό, λυτρισμικό, πρόσβαση σε μη εξουσιοδοτημένους χρήστες και τροποποιήσεις καταλαθος	---
---	---
14 μέρες δωρεάν	15 μέρες δωρεάν
Rest api, Web gui	Rest api, Cli, Web gui
Elastic	Splunk
AWS, GCP, Azure (Elasticsearch)	AWS,GCP
2 πακέτα (1 24/7 και 1 8/5), επικοινωνία με τηλέφωνο, email	επικοινωνία με τηλέφωνο, email, cases/tickets, ενημερώσεις, τεκμηρίωση, συχνές ερωτήσεις, χάρτης προϊόντων (product roadmap), παρακολούθηση πορείας tickets

FortiSIEM	**Datadog Cloud SIEM**
IaaS	SaaS
δημόσιο, ιδιωτικό	δημόσιο
SIEM	SIEM
τιμολόγηση με βάση τον αριθμό συσκευών απ’ τις οποίες αντλούνται δεδομένα	τιμολόγηση με βάση τον όγκο των δεδομένων, ανά μήνα

Βασική λειτουργικότητα: -Συνδυασμένη παρακολούθηση ασφάλειας και λειτουργίας δικτύου -Παρακολούθηση αλλαγών διαμόρφωσης συσκευής και λογισμικού -Ανάπτυξη τεχνικών μηχανικής μάθησης τεχνητής νοημοσύνης -Βαθμολόγηση κινδύνου -Συσχέτιση κατανεμημένων γεγονότων σε πραγματικό χρόνο **Επιπλέον λειτουργικότητα:** -Ύπαρξη βάσης δεδομένων για αυτόματη ανακάλυψη συσκευών του δικτύου -Αντιστοίχιση ταυτότητας χρηστών -Χρήση δεδομένων για περαιτέρω ανάλυση ώστε να συμβάλλουν στον εντοπισμό νέων απειλών	**Βασική λειτουργικότητα:** -Εισαγωγή, κανονικοποίηση και εμπλουτισμός αρχείων καταγραφής, καθώς και ειδοποιήσεων ασφαλείας τρίτων, για τον εντοπισμό απειλών και την επιτάχυνση των ερευνών -Αξιοποίηση ενσωματωμένων κανόνων ανίχνευσης κατωφλίου και ανωμαλιών για τον γρήγορο εντοπισμό απειλών, με ελάχιστη διαμόρφωση -Εντοπισμός κοινών απειλών ή επιθέσεων εντός του πλαισίου MITER ATT&CK® -Ανακάλυψη ζητημάτων ασφαλείας κατά την απορρόφηση αρχείων καταγραφής και όχι μετά από δαπανηρή ευρετηρίαση -Γρήγορη ανίχνευση απειλών, ακόμη και αν οι κανόνες είναι περίπλοκοι ή απορροφούν μεγάλο όγκο δεδομένων **Επιπλέον λειτουργικότητα:** - 500+ ενσωματωμένες ενσωματώσεις της Datadog για πλήρη ορατότητα στο δίκτυο, τους παρόχους ταυτότητας, τα τελικά σημεία και τις εφαρμογές SaaS -Συνεργασία με πολλές ομάδες μέσω ενσωματώσεων με δελτία, συστήματα συνομιλίας και εργαλεία αποκατάστασης -Δημιουργία από τους χρήστες προσαρμοσμένων κανόνων χωρίς να χρειάζεται μια ιδιόκτητη (propriatary) γλώσσα ερωτημάτων -Εμπλουτισμός σημάτων ασφαλείας με ροές πληροφοριών απειλών που διαχειρίζονται το Datadog
--- [1]	Αν η διαθεσιμότητα είναι μικρότερη από 99.8% για δυο διαδοχικούς μήνες τότε ο πελάτης μπορεί τον επόμενο μήνα να διακόψει το συμβόλαιο
ανιχνευτική	ανιχνευτική
διαθεσιμότητα, μη αποποίηση	---
δεδομένα κρίσιμα για τις επιχειρήσεις, τα άκρα του δικτύου, την υποδομή και άλλες εφαρμογές	οτιδήποτε
Σφάλματα χρηστών, παραβάσεις πολιτικών,	---

κακόβουλες δραστηριότητες, παραβιασμένοι λογαριασμοί	
---	---
τίποτα δωρεάν	14 μέρες δωρεάν
Rest api, Cli, Web gui	Rest api ,Web gui
Fortinet	Datadog
AWS,Azure	AWS,Azure
υποστήριξη 24/7 με τηλέφωνο και tickets, έγγραφα, forum τεκμηρίωση, βίντεο, πύλη ασφαλείας(security portal)	επικοινωνία με mail, chat, τεκμηρίωση, forum

Solarwinds Security Event Manager	**McAfee Enterprise Security Manager SIEM**
IaaS	IaaS
δημόσιο	δημόσιο
SIEM,DLP	SIEM
τιμολόγηση με βάση τις συσκευές (κόμβους) που παρακολουθούνται, Per Feature	τιμολόγηση με βάση το φόρτο εργασίας
Βασικοί μηχανισμοί: -Συλλέγει, ενοποιεί, κανονικοποιεί και οπτικοποιεί αρχεία καταγραφής και συμβάντα από τείχη προστασίας, συσκευές και εφαρμογές IDS/IPS, διακόπτες, δρομολογητές, διακομιστές, λειτουργικό σύστημα και άλλες εφαρμογές -Πραγματοποιεί συσχετισμό δεδομένων μηχανής σε πραγματικό χρόνο για τον εντοπισμό απειλών και μοτίβων επιθέσεων -Προσφέρει μια διαισθητική διεπαφή (intuitive interface) και άφθονη επιλογή καινοτόμου περιεχομένου **Επιπλέον λειτουργικότητα:** -Αποκρίνεται αυτόματα σε ύποπτη δραστηριότητα με την Ενεργή απόκριση, συμπεριλαμβανομένου του αποκλεισμού συσκευών USB, της θανάτωσης κακόβουλων διαδικασιών, της αποσύνδεσης χρηστών και πολλά άλλα	**Βασική λειτουργικότητα:** -Πίνακες εργαλείων, αναφορές, κριτικές, κανόνες και ειδοποιήσεις με επίκεντρο τους αναλυτές -Πακέτα περιεχομένου - προ συσκευασμένα σύνολα συναγερμών, προβολών, αναφορών, μεταβλητών, κανόνων συσχέτισης και λιστών παρακολούθησης που αντιμετωπίζουν κοινές περιπτώσεις χρήσης ασφαλείας. -Σχεδόν σε πραγματικό χρόνο ή συγκέντρωση και συσχέτιση ύποπτων ή επιβεβαιωμένων απειλών με δεδομένα συμβάντων -Δυνατότητα συλλογής δεδομένων από συσκευές προμηθευτών ασφαλείας τρίτων και ροές απειλών -Κλιμακούμενη αρχιτεκτονική δεδομένων που συλλέγει και συσχετίζει συμβάντα καταγραφής πολλών ετών **Επιπλέον λειτουργικότητα:** -Δυνατότητα εμπλουτισμού συμβάντων με πληροφορίες συμφραζομένων (όπως λύσεις απορρήτου, δεδομένα απειλών και συστήματα διαχείρισης

- Διευκολύνει τις αναφορές συμμόρφωσης και ελέγχει μέσα σε καινοτόμες αναφορές και φίλτρα για HIPAA, PCI DSS, SOX, ISO, DISA STIG, FISMA, FERPA, NERC CIP, GLBA και άλλα	ταυτότητας και πρόσβασης) -Προκαθορισμένοι πίνακες εργαλείων, ίχνη ελέγχου και αναφορές για παγκόσμιους κανονισμούς και πλαίσια ελέγχου -Προσαρμόσιμες αναφορές συμμόρφωσης, κανόνες και πίνακες εργαλείων. -Ταχεία πρόσβασης σε μακροπρόθεσμη αποθήκευση δεδομένων συμβάντων -Κατ' απαίτηση: ερωτήματα, ανάλυση στοιχειών (forensics), επικύρωση κανόνων και συμμόρφωση
---	ενσωματωμένα δεδομένα 99.999%, πρόσβαση στη διαχείριση 99.9%
ανιχνευτική	ανιχνευτική
ακεραιότητα	ακεραιότητα
οτιδήποτε	οτιδήποτε
Επιθέσεις, λυτρισμικό, κακόβουλο λογισμικό, ηλεκτρονικό ψάρεμα, απώλεια δεδομένων τελικού σημείου και προστασία ευαίσθητων δεδομένων	αρχεία κακόβουλου λογισμικού, παρακολουθούνται τα τελικά σημεία (endpoints) για δεδομένα τα οποία προσδιορίζουν δυνητικά κακόβουλη δραστηριότητα στο σύστημα (indicators of compromise)
δυνατότητα για επεξεργασία μέχρι 2500 γεγονότα/δευτερόλεπτο ((EPS) και ενεργοποίηση 5000 κανόνων/ημέρα	---
30 μέρες δωρεάν	δωρεάν δοκιμαστική έκδοση από τη μέρα ενεργοποίησης έως το τέλος του επόμενου μήνα (31-60 μέρες διάρκεια)
Cli, Web gui	Rest api, Cli, Web gui
Solarwinds	McAfee
κανένα	κανένα
επικοινωνία με τηλέφωνο, tickets, forum	επικοινωνία με τηλέφωνο, email, έγγραφα, ειδοποιήσεις υποστήριξης, κοινότητα

Arcsight Enterprise Security Manager	**Exabeam Fusion SIEM**
SaaS	SaaS
δημόσιο	δημόσιο
SIEM	SIEM
τιμολόγηση με βάση τον όγκο των δεδομένων που λαμβάνονται και τα συμβάντα ασφαλείας που συσχετίζονται ανά δευτερόλεπτο	τιμολόγηση με βάση τον όγκο των δεδομένων που λαμβάνονται

Βασική λειτουργικότητα: -Ισχυρή συσχέτιση σε πραγματικό χρόνο -Κατηγοριοποίηση και Κανονικοποίηση -Ενσωμάτωση με άλλες εφαρμογές -Οπτικοποίηση δεδομένων -Αυτόματη απόκριση εντός της Κονσόλας ή ως Ενέργεια κανόνων **Επιπλέον λειτουργικότητα:** -Κοινή χρήση περιεχομένου με άλλα συστήματα - Αυτοματισμός ροής εργασίας -Το ArcSight ESM επιτρέπει στις κατανεμημένες επιχειρηματικές μονάδες να χρησιμοποιούν μία απλοποιημένη προβολή SecOps -Πακέτα συμμόρφωσης	**Βασική λειτουργικότητα:** -Αυτόματη ανίχνευση συμπεριφορών ενδεικτικών απειλών -Μείωση ψευδώς θετικών συναγερμών που σχετίζονται με τους κανόνες συσχέτισης -Οι προκατασκευασμένες ενσωματώσεις απορροφούν εύκολα δεδομένα από δημοφιλείς υπηρεσίες που βασίζονται σε cloud -Η ανάλυση συμπεριφοράς αναλύει δεδομένα από οποιαδήποτε πηγή cloud ή εσωτερικής εγκατάστασης - Τα σχέδια απόκρισης αυτοματοποιούν τη διερεύνηση, τον περιορισμό και τον μετριασμό περιστατικών **Επιπλέον λειτουργικότητα:** -Οι έλεγχοι ασφαλείας διασφαλίζουν ότι τα δεδομένα χειρίζονται σύμφωνα με τις βέλτιστες πρακτικές
---	99.5% διαθεσιμότητα
ανιχνευτική	ανιχνευτική
ακεραιότητα, μη αποποίηση	ακεραιότητα
οτιδήποτε	οτιδήποτε
---	---
δυνατότητα για επεξεργασία έως 100.000 γεγονότα/δευτερόλεπτο	---
30 μέρες δωρεάν	δωρεάν δοκιμαστική έκδοση χωρίς να αναφέρονται μέρες
Rest api, Web gui	Web gui
Micro focus και HP (ενώθηκαν)	Exabeam
Azure	GCP
επικοινωνία με τηλέφωνο, email	υποστήριξη 24/7 μέσω τηλεφώνου, επικοινωνία με τηλέφωνο, email, tickets

Alienvault Unified Security Management Anyware	**Blumira Modern Cloud SIEM**
IaaS	SaaS
δημόσιο	δημόσιο
SIEM,IDS, ασφάλεια δικτύου	SIEM

Τρία πακέτα με διαφορετικές παροχές και τιμές και τιμολόγηση με βάση τον όγκο των δεδομων για μηνιαία συνδρομή	τιμολόγηση με βάση τον αριθμό χρηστών
Βασική λειτουργικότητα: **-**Κεντρική ανίχνευση απειλών και απόκριση συμβάντων σε περιβάλλοντα cloud, υποδομές εσωτερικής εγκατάστασης και εφαρμογές cloud -Διαχείριση ημερολογίου για συνεχείς έρευνες συμμόρφωσης και foresincs -Προηγμένη ανίχνευση απειλών με συναγερμούς σε πραγματικό χρόνο, με προτεραιότητα και ελάχιστα ψευδώς θετικά -Συνεχείς ενημερώσεις πληροφοριών απειλών από την AlienVault Labs Security **Εξτρά λειτουργικότητες:** -Ενημερώσεις της ερευνητικής ομάδας για αναδυόμενες απειλές -Προκατασκευασμένες αναφορές συμμόρφωσης για PCI DSS, HIPAA, NIST CSF και άλλα -ενορχήστρωση και αυτοματισμός ασφάλειας -Ενσωμάτωση με λογισμικό ticketing τρίτων -Ανακάλυψη περιουσιακών στοιχείων -Αξιολόγηση της ευπάθειας -Ανίχνευση εισβολής -Παρακολούθηση συμπεριφοράς	**Βασική λειτουργικότητα** -Απεριόριστη απορρόφηση δεδομένων -Ανιχνεύσεις & Απόκριση -Βασικές Αναφορές -Σύνοψη στο Ταμπλό -Πληροφορίες για τους κανόνες
99.99% διαθεσιμότητα με εξαίρεση τις προγραμματισμένες ώρες συντήρησης	99.99% διαθεσιμότητα
ανιχνευτική	ανιχνευτική
ακεραιότητα, διαθεσιμότητα, εμπιστευτικότητα	ακεραιότητα
δεδομένα, δίκτυο, ξενιστές	οτιδήποτε
-Παραβιάσεις δεδομένων -λυτρισμικό -Προηγμένο κακόβουλο λογισμικό -δούρειοι ίπποι απομακρυσμένης πρόσβασης -Εσωτερικές απειλές	λυτρισμικό και παραβιάσεις δεδομένων

-Επιθέσεις ηλεκτρονικού ψαρέματος -Επιθέσεις κατανεμημένης άρνησης υπηρεσίας	
δυνατότητα για επεξεργασία έως 15.000 γεγονότα/δευτερόλεπτο και 5000mb ρυθμοαποδοση	---
14 μέρες δωρεάν	14 μέρες δωρεάν
Rest api, Cli	---
AT&T και Alievault (ενώθηκαν)	Blumira
Azure	κανένα
2 πακέτα (10/5 και 24/7), επικοινωνία με τηλέφωνο ,email, tickets, τεκμηρίωση, έγγραφα, απαντήσεις σε ερωτήματα, πύλη υποστήριξης, κοινότητα, βίντεο, blog	υποστήριξη μέσω τηλεφώνου, mail, tickets/cases (case management)

LogRhythm nextgen SIEM platform	**Netwitness cloud SIEM platform**
SaaS, IaaS	IaaS
δημόσιο	δημόσιο
SIEM	SIEM
τιμολόγηση με βάση τον όγκο δεδομένων, με συνδρομή	τιμολόγηση με βάση των όγκο των δεδομένων τριμήνου
Βασική λειτουργικότητα: -Παρακολούθηση Δικτύου -Παρακολούθηση σε πραγματικό χρόνο -Διαχείριση αρχείων καταγραφής -Παρακολούθηση δραστηριότητας χρηστών -Αναλυτικά στοιχεία συμπεριφοράς **Επιπλέον λειτουργικότητα:** -Ευφυΐα απειλών -Διαχείριση τελικού σημείου -Παρακολούθηση ακεραιότητας αρχείων -Εγκληματολογική ανάλυση (forensics) -Αναφορές συμμόρφωσης	**Βασική λειτουργικότητα:** -συλλέγει, αναλύει, αναφέρει και αποθηκεύει δεδομένα καταγραφής από διάφορες πηγές για να υποστηρίξει πρωτοβουλίες πολιτικής ασφάλειας και κανονιστικής συμμόρφωσης. -καταλαμβάνει αρχεία καταγραφής από περισσότερες από 350 πηγές συμβάντων, καθώς και παρακολούθηση αρχείων καταγραφής για δημόσια νέφη **Επιπλέον λειτουργικότητα:** -Εξυπηρετεί περιπτώσεις χρήσης συμμόρφωσης με προκατασκευασμένες αναφορές, συμπεριλαμβανομένων των Basel II, Bill 198, FERPA, FFIEC, FISMA, GLBA, GPG13, HIPAA, ISO 27002, NERC CIP, NISPOM, PCI, SOX και SSAE. -χρησιμοποιεί πατενταρισμένη τεχνολογία για δυναμική ανάλυση και εμπλουτισμό των δεδομένων καταγραφής κατά το χρόνο λήψης, δημιουργώντας

	πλούσια μεταδεδομένα που επιταχύνουν δραματικά τις έρευνες και την απόκριση.
Για διαθεσιμότητα χαμηλότερη από 99,9% πίστωση 2% της μηνιαίας χρέωσης συνδρομής, για < 99,0% πίστωση 5% και για < 95% πίστωση 10%.	πληροφορίες μόνο με αίτηση στην εταιρία
ανιχνευτική	ανιχνευτική
ακεραιότητα	ακεραιότητα
οτιδήποτε	οτιδήποτε
---	---
---	όγκος δεδομένων που βγαίνουν από το σύστημα (data egress) έως 2TB/μήνα
τίποτα δωρεάν	τίποτα δωρεάν
Rest api, Web gui	Rest api, Cli, Web gui
LogRhythm	Rsa και Netwitness (ενώθηκαν)
κανένα	Azure
επικοινωνία με τηλέφωνο, email, tickets	επικοινωνία με τηλέφωνο, email, tickets/cases, κοινότητα

Sumo Logic Cloud SIEM Powered by AWS	**ClearSkies NG SIEM**
SaaS	IaaS
δημόσιο	δημόσιο
SIEM	SIEM
τιμολόγηση με βάση τον όγκο των δεδομένων που λαμβάνονται ανά ημέρα και τον χρόνο διατήρησης, μηνιαία ή ετήσια συνδρομή,	---
Βασική λειτουργικότητα: -Κλιμακούμενη συλλογή δεδομένων και αρχείων καταγραφής (και ανάλυση δεδομένων) -Απόκριση συμβάντων (και δημιουργία συναγερμών) -Οπτικοποίηση δεδομένων	**Βασική λειτουργικότητα:** -Συλλέγει, αποθηκεύει, επεξεργάζεται, συγκεντρώνει και αναλύει τεράστιους όγκους ιστορικών και τρεχόντων δεδομένων καταγραφής από ετερογενείς πηγές δεδομένων -Επιτυγχάνει μείωση έως και 95% στον αριθμό των ψευδώς θετικών ειδοποιήσεων συνδυάζοντας προηγμένες αναλυτικές δυνατότητες και δυνατότητες προσαρμοστικής συσχέτισης -Δημιουργεί ειδοποιήσεις εμπλουτισμένες με

	γνώσεις που βασίζονται σε στοιχεία και πληροφορίες σχετικά με τα συμφραζόμενα -Αναλύει και συσχετίζει έξυπνα δεδομένα ενσωματώνοντας γνώσεις βασισμένες σε στοιχεία και πληροφορίες σχετικά με τα συμφραζόμενα σχετικά με τους χρήστες, τα περιουσιακά στοιχεία, τις απειλές και τα τρωτά σημεία **Επιπλέον λειτουργικότητα:** -Ψηφιακά υπογράφει και κρυπτογραφεί ακατέργαστα δεδομένα καταγραφής, προστατεύοντας την εμπιστευτικότητα και την ακεραιότητα των ευαίσθητων πληροφοριών
99.5%-99.9% διαθεσιμότητα	---
ανιχνευτική	ανιχνευτική
---	ακεραιότητα, εμπιστευτικότητα, διαθεσιμότητα
οτιδήποτε	οτιδήποτε
---	---
για να αποκτηθεί και να πληρωθεί το προϊόν γίνονται δέκτες μόνο διευθύνσεις ηλεκτρονικού ταχυδρομείου επιχειρήσεων (πχ απορρίπτονται gmail, yahoo)	ελάχιστη διάρκεια αδείας χρήσης 12 μήνες
30 μέρες δωρεάν	τίποτα δωρεάν
Rest api, Cli, Web gui	---
Sumo logic	Cleaskies
AWS	Azure
επικοινωνία με email, κοινότητα, τεκμηρίωση	υποστήριξη 24/7 μέσω τηλεφώνου, επικοινωνία με τηλέφωνο, email, tickets

Πίνακας Αποτίμησης 2 – Προϊόντα BCDR

ΚΡΙΤΗΡΙΑ/ΠΡΟΙΟΝΤΑ	**Appranix Cloud Application Resilience**
α. τρόπος παράδοσης	SaaS
β. μοντέλο διάταξης	δημόσιο
γ. κατηγορία υπηρεσιών στην οποία ανήκει	BCDR

δ. μοντέλο κόστους	τιμολόγηση με βάση τα στιγμιότυπα (AWS instances)
ε. μηχανισμοί ασφάλειας που υλοποιούνται	**Βασική λειτουργικότητα:** -Προσαρμόσιμα και συνεχώς ενημερωμένα σχέδια DR Infrastructure-as-Code βασισμένα σε αλλαγές περιβάλλοντος παραγωγής -Δημιουργία αντιγράφων ασφαλείας ολόκληρου του περιβάλλοντος cloud χωρίς πράκτορες, ανάκτηση και DR για γρήγορες ανακτήσεις -Υπάρχουν εξαρτήσεις για κάθε πόρο cloud, σε οποιαδήποτε περιοχή, σε οποιαδήποτε στιγμή ανάκτησης Γεωγραφικά διάσπαρτα τοποθεσίες για αντίγραφα ασφαλείας διαχείριση και παρακολούθηση **Εξτρά λειτουργικότητα** -Προστασία και ανάκτηση υπηρεσιών δικτύου -Συνεχής αντίστροφη μηχανική περιβαλλόντων εφαρμογών cloud -Αυτοματοποιημένες εξαρτήσεις με επίκεντρο την εφαρμογή χαρτογράφησης όλων των πόρων cloud - Αυτοματοποιημένη για πάντα επαυξητική διαχείριση κύκλου ζωής δεδομένων των RDS στιγμιότυπων
στ. μη λειτουργικές εγγυήσεις	διαθεσιμότητα 99.9% και για κάθε διακοπή μεγαλύτερη από 1 ώρα, πίστωση 2% των τελών υπηρεσίας για κάθε περίοδο 30 ή περισσότερων διαδοχικών λεπτών διακοπής λειτουργίας και έως μία πίστωση ανά ημέρα
ζ. είδος προσφερόμενης προστασίας	προληπτική (BC), αντιδραστική (DR)
η. ιδιότητες ασφάλειας	διαθεσιμότητα
θ. αντικείμενα που προστατεύονται	ολόκληρα περιβάλλοντα εφαρμογών (εικονικές μηχανές, containers , εξισορροπητές φορτίου, βάσεις δεδομένων, το εικονικό ιδιωτικό νέφος (vpc))
ι. απειλές που αντιμετωπίζονται	---
ια. περιορισμοί	---
ιβ. ύπαρξη δωρεάν εκδόσεων	14 μέρες δωρεάν
ιγ. τρόπος χρήσης προϊόντος	Rest api, Cli, Web based gui

ιδ. εταιρεία που προσφέρει το προϊόν	Appranix
ιε. marketplace(s) όπου προσφέρεται το προϊόν	AWS
ιστ. επίπεδο/είδος υποστήριξης για το προϊόν	υποστήριξη 24/7, επικοινωνία με τηλέφωνο, email, tickets, εξυπηρέτηση πελατών, τεκμηρίωση, έγγραφα, forum, συχνές ερωτήσεις και βάση γνώσεων (knowledge base)

Datto SIRIS στο Datto cloud	**DRuva: AWS Backup and Disaster Recovery**
SaaS, IaaS	SaaS
ιδιωτικό	δημόσιο (vpc)
BCDR, κρυπτογράφηση	BCDR
τιμολόγηση με βάση την περίπτωση (tailored pricing)	τιμολόγηση με βάση τον όγκο δεδομένων (consumption based)
Βασική λειτουργικότητα: -Προαιρετική άπειρη διατήρηση αντιγράφων ασφαλείας -Ανάκτηση καταστροφών ως υπηρεσία (DRaaS) -Εύκολη στη χρήση διεπαφή επαναφοράς αρχείων -Γεωγραφικά διάσπαρτες τοποθεσίες για δημιουργία αντιγράφων ασφαλείας -Πρωτοποριακή πύλη διαχείρισης -Πρωτοποριακή διεπαφή ελέγχου αντιγράφων ασφαλείας **Εξτρά λειτουργικότητα** -προστασία διαγράφης αρχείων -Αμετάβλητος σχεδιασμός για ασφάλεια (προστασία ransomware) -Κρυπτογράφηση κατά την αναπαραγωγή και σε κατάσταση ηρεμίας -Υποχρεωτική πρόσβαση δύο παραγόντων (2FA) -Προαιρετική άπειρη διατήρηση αντιγράφων ασφαλείας	**Βασική λειτουργικότητα:** -Ενοποίηση δημιουργίας αντιγράφων ασφαλείας και ανάκτησης από καταστροφές στο cloud σε πρότυπα πολιτικής μιας ενιαίας πλατφόρμας για αξιόπιστες λειτουργίες DR -Αυτοματοποίηση διαδικασιών DR -Εύκολη επαναφορά σε οποιαδήποτε χρονική στιγμή — με βάση τα πιο πρόσφατα αντίγραφα ασφαλείας -Γρήγορη ανάκαμψη από διακοπές λειτουργίας, φυσικές καταστροφές και επιθέσεις λυτρισμικού -Αποφυγή διακοπής λειτουργίας με απλή, αυτοματοποιημένη εκτέλεση failback/failover -Γρήγορη επαναφορά (failback) στο VMware Cloud στο AWS ή απευθείας επιστροφή στην εσωτερική εγκατάσταση -Κατανομή του φόρτου εργασίας μιας αποτυχίας (workload failover) στο AWS σε άλλη περιοχή (region) ή λογαριασμό **Επιπλέον λειτουργικότητα:** -Εύκολη κλωνοποίηση ρυθμίσεων εικονικού ιδιωτικού νέφους (vpc) στο περιβάλλον στόχο για ετοιμότητα DR

	-Μετριασμός του κινδύνου λυτρισμικό με ασφαλή αντίγραφα ασφαλείας
διαθεσιμότητα 99.99999% και 97.5% επιτυχία backup	RTO 15 έως 20 λεπτά, RPO 1 ώρα
προληπτική (BC), αντιδραστική (DR)	προληπτική (BC), αντιδραστική (DR)
διαθεσιμότητα και (λόγω κρυπτογράφησης) εμπιστευτικότητα	διαθεσιμότητα
οτιδήποτε	δεδομένα κρίσιμα για τις επιχειρήσεις
λυτρισμικό, ανθρώπινες και κακόβουλες ενέργειες (πχ διαγραφή αρχείων)	διακοπές λειτουργίας, φυσικές καταστροφές και επιθέσεις, λυτρισμικό
μέγιστη συχνότητα δημιουργίας αντιγράφων ασφαλείας 5 λεπτά	---
τίποτα δωρεάν	30 μέρες δωρεάν
Rest api, Cli, Web based gui	Rest api, Web based gui
Datto	Druva
κανένα	AWS
υποστήριξη 24/7, επικοινωνία με τηλέφωνο, email, chat, tickets και forum	24/7 υποστήριξη, 2 πακέτα, επικοινωνία μέσω chat, email και τηλεφώνου, cases (tickets), πύλη υποστήριξης (portal), βάση γνώσης, κοινότητα, εκπαίδευση, τεκμηρίωση, forum, blog
Commvault Backup & Recovery	Barracuda Backup
IaaS	SaaS, IaaS
δημόσιο	δημόσιο
BCDR, κρυπτογράφηση	BCDR, κρυπτογράφηση
τιμολόγηση με βάση τον όγκο των δεδομένων ή με βάση τις εικονικές μηχανές	τιμολόγηση ανάλογα με τους πόρους που χρησιμοποιούνται (per-socket subscription for virtual hosts)
Βασική λειτουργικότητα: -Αντίγραφα ασφαλείας -Προστασία εικονικών μηχανών, εφαρμογών (συμπεριλαμβανομένου του cloud), βάσεων δεδομένων, τελικών σημείων, αρχείων Ανάκτηση εικονικών μηχανών, εφαρμογών (συμπεριλαμβανομένου του cloud), βάσεων	Βασική λειτουργικότητα: -Άμεση αντικατάσταση: Σε περίπτωση πλήρους καταστροφής, το Barracuda θα προφορτώσει τα πιο πρόσφατα δεδομένα και ρυθμίσεις διαμόρφωσης που είναι αποθηκευμένα στο Barracuda Cloud Storage σε μια μονάδα αντικατάστασης για επαναφορά έκτακτης

δεδομένων, τελικών σημείων, αρχείων -Μετάβαση φόρτου εργασίας από τις εγκαταστάσεις στο cloud, ή ανάμεσα στα νέφη -Αξιοποίηση στιγμιότυπων υλικού για σχεδόν άμεση ανάκτηση ολόκληρων όγκων δεδομένων Ενσωμάτωση στο cloud -Χρήση του cloud για επεκτασιμότητα, κινητικότητα, διαθεσιμότητα και μείωση κόστους για φόρτους εργασίας παραγωγής -Διατήρηση αντιγράφων προστατευμένων δεδομένων σε μία ή περισσότερες τοποθεσίες	ανάγκης. -Δημιουργία αντιγράφων ασφαλείας -Απεριόριστη χωρητικότητα και γεωγραφική κατανομή σημείων αποθήκευσης -Ανάκτηση δεδομένων: Οι φυσικοί διακομιστές είναι σε θέση να εκτελούν αποκαταστάσεις γυμνού μετάλλου σε περίπτωση καταστροφικής αποτυχίας, ενώ τα εικονικά περιβάλλοντα επωφελούνται από γρήγορες αποκαταστάσεις που βασίζονται σε εικόνες. Εξτρά λειτουργικότητα -Κρυπτογραφία δεδομένων -Αφαίρεση διπλότυπων για εξοικονόμηση πόρων -LiveBoot: Το Barracuda LiveBoot προσφέρει στους οργανισμούς που προστατεύουν τα περιβάλλοντα VMware και Microsoft Hyper-V με το Barracuda Backup την επιλογή να αξιοποιήσουν το Barracuda Cloud Storage εάν το δικό τους εικονικό περιβάλλον πέσει. -Διαχείριση πολλών τοποθεσιών από μια απλή στη χρήση διεπαφή -Μεταφορά τοπικών αντιγράφων αντιγράφων ασφαλείας από τοπικές συσκευές στο Barracuda Cloud
Εάν το μηνιαίο ποσοστό προσβασιμότητας είναι μικρότερο από 99,9%, τότε ισχύει πίστωση 10% των τελών υπηρεσίας και αν είναι μικρότερο του 99% ισχύει πίστωση 25% των τελών υπηρεσίας για τον τρέχων μήνα	διαθεσιμότητα 99.9% και επιστροφή χρημάτων σε αναλογική βάση για το ποσό του επιπλέον χρόνου διακοπής λειτουργίας, πάνω από τη δέσμευση χρόνου λειτουργίας
προληπτική (BC), αντιδραστική (DR)	προληπτική (BC), αντιδραστική (DR)
διαθεσιμότητα και (λόγω κρυπτογράφησης) εμπιστευτικότητα	διαθεσιμότητα και (λόγω κρυπτογράφησης) εμπιστευτικότητα
εικονικές μηχανές, κοντέινερ, βάσεις δεδομένων, εφαρμογές (συμπεριλαμβανομένου του cloud), τελικά σημεία και αρχεία	Αρχεία που βρίσκονται σε φυσικές συσκευές, εικονικά περιβάλλοντα ή στο δημόσιο νέφος
λυτρισμικό	καταστροφές, λυτρισμικό και κακόβουλες ενέργειες
---	---
30 μέρες δωρεάν	60 μέρες δωρεάν
Rest api, Cli, Web based gui	Web based gui

Commvault	Barracuda
AWS,Azure	Azure
5 πακέτα, υποστήριξη 8/5, επικοινωνία με τηλέφωνο, emails, πύλη υποστήριξης, συχνές ερωτήσεις, έγγραφα, ενημέρωση για αναβαθμίσεις και νέα προϊόντα, βάση γνώσης, τεκμηρίωση, κοινότητα, πρόσβαση στο ιστορικό υποστήριξης του λογαριασμού	3 πακέτα και υποστήριξη 24/7, επικοινωνία με tickets, emails, τηλέφωνο, chat, πύλη (portal), τεχνικά έγγραφα, forum, ενημέρωση για συνδρομές, κοινότητα, κέντρο γνώσης, τεκμηρίωση, λεξικο

Veeam Backup and Replication	**Cloud Daddy Secure Backup Enterprise Edition**
IaaS	IaaS
δημόσιο	δημόσιο
BCDR	BCDR
τιμολόγηση με βάση τους πόρους	4 πακέτα τιμολόγησης με αντίστοιχες παροχές (στιγμιότυπα AWS, λογαριασμοί AWS ,αριθμός χρηστών) και δυνατότητα πληρωμής ανά μήνα, έτος, διετία με τις αντίστοιχες εκπτώσεις
Βασική λειτουργικότητα: -Αντίγραφα ασφαλείας: Γρήγορη, φορητή και ολοκληρωμένη κάλυψη -Ανάκτηση: Εκπλήρωση στόχων ανάκτησής άμεσα -Νέφος: Ασφαλής δημιουργία αντιγράφων ασφαλείας, αποκατάσταση από καταστροφή (DR) και αρχειοθέτηση -Αποθήκευση: Ταχύτερα αντίγραφα ασφαλείας και άπειρη επεκτασιμότητα -Ενσωματωμένη ανάκτηση καταστροφών εκτός τοποθεσίας **Επιπλέον λειτουργικότητα:** -Ασφάλεια: Προστασία από λυτρισμικό και κυβερνοαπειλές -Αυτοματοποίηση: Επίτευξη διαχείρισης σε κλίμακα -Επαναχρησιμοποίηση δεδομένων: Επιτάχυνση δοκιμών, εξόρυξης και DevOps	**Βασική λειτουργικότητα** Backup And Disaster Recovery -Ολοκληρωμένα αντίγραφα ασφαλείας -Κρυπτογραφημένη δημιουργία αντιγράφων ασφαλείας και επαναφορά μεταξύ περιοχών/λογαριασμών -Ανάκτηση σε επίπεδο αρχείου -Δημιουργία αντιγράφων ασφαλείας και αναπαραγωγή με γνώση κόστους -Αυτόματη αφαίρεση παλιών στιγμιότυπων -Αρχειοθέτηση αντιγράφων ασφαλείας στο Amazon S3 -Δεδομένα επί τόπου στο AWS **Επιπλέον λειτουργικότητα:** Προηγμένα αντίμετρα κυβερνοασφάλειας -Διαχείριση τείχους προστασίας -Μετριασμός των επιθέσεων -Security Analytics -Ενσωμάτωση Amazon GuardDuty -Αλγόριθμοι AI -Πυροδοτούμενα συμβάντα και αντίγραφα

	ασφαλείας Διαχείριση Υποδομών AWS -Κεντρική διαχείριση από ένα σημείο -Ετικέτες AWS -Πλήρης υποστήριξη μοντέλου πολλαπλών ενοικιαστών -Χειροκίνητος έλεγχος και προγραμματισμός στιγμιοτύπων
---	---
προληπτική (BC), αντιδραστική (DR)	προληπτική (BC), αντιδραστική (DR)
διαθεσιμότητα	διαθεσιμότητα
οτιδήποτε	οτιδήποτε
καταστροφές και λυτρισμικό	---
Η Veeam πουλά το VUL (άδεια χρήσης - license) σε πακέτα των 10. Καταναλώνεται 1 άδεια για καθένα από τα ακόλουθα προστατευμένα φορτία εργασίας: 1 εικονική μηχανή (VM), 1cloudInstance/VM, 1 φυσικός διακομιστής, ένα πακέτο 3 σταθμών εργασίας ή 500 GB δεδομένων NAS .	---
30 μέρες δωρεάν	14 μέρες δωρεάν
Rest api,Cli, Web based gui	Web based gui
Veeam	Cloud Daddy
Google	AWS
επικοινωνία με email, τηλέφωνο, tickets, κοινότητα, πύλη υποστήριξης, τεκμηρίωση και τεχνικά έγγραφα, βάση γνώσης, συχνές ερωτήσεις. Υπάρχουν 3 πακέτα υποστήριξης με διαφορετικές παροχές	υποστήριξη 24/7, επικοινωνία με τηλέφωνο, email, συχνές ερωτήσεις, τεκμηρίωση

Cohecity DataPlatform DataProtect Cloud Edition (για BC) και Cohecity SiteContiunity (για DR)	**NAKIVO Backup & Replication**
SaaS, IaaS	SaaS, IaaS
δημόσιο	δημόσιο
BCDR, κρυπτογράφηση	BCDR, κρυπτογράφηση
τιμολόγηση με βάση τον όγκο των δεδομένων (front end capacity pricing)	-τιμολόγηση με βάση το τους πόρους (workload) με άδειες χρήσης και υπάρχουν πέντε πακέτα με αντίστοιχες τιμές και παροχές. Ένα workload είναι ένα

	VMware VM, Hyper-V VM, Nutanix AHV VM, ένα φυσικό μηχάνημα (1 διακομιστής ή 3 σταθμοί εργασίας), μια βάση δεδομένων Oracle (μόνο Enterprise Plus) ή ένα AWS EC2 instance.
DataProtect **Βασική λειτουργικότητα:** -Ενιαία δημιουργία αντιγράφων ασφαλείας και ανάκτηση -Σημεία Γρήγορης Ανάκτησης -Άμεση μαζική επαναφορά αρχείων -Αξιοποίηση αποθηκευτικού χώρου με την αφαίρεση διπλότυπων **Επιπλέον λειτουργικότητα:** -Ενοποιημένη εμπειρία χρήστη ελέγχοντας τα πάντα μέσα από ενα γραφικό περιβάλλον -Εφαρμογή πολίτικων για να αυτοματοποιηθούν διαδικασίες -Κρυπτογράφηση αρχείων στο δημόσιο νέφος -Προστασία από λυτρισμικό -Ανθεκτικότητα δεδομένων σε κλίμακα **SiteContinuity** **Βασική λειτουργικότητα:** -Ενοποιημένο Backup και DR Αυτόματη ενορχήστρωση για failover και failback σε περιβάλλοντα πολλαπλών cloud. -Ευέλικτη επαναφορά αρχείων -Ταχεία διαθεσιμότητα -Επαναφορά σε παλαιοτέρα χρονικά σημεία χρησιμοποιώντας μηχανική μάθηση για να επιλεχθούν τα σημεία αυτά **Επιπλέον λειτουργικότητα** -Ικανοποίηση αναγκών συμμόρφωσης και διασφάλιση ετοιμότητας DR με λεπτομερή ίχνη ελέγχου, υποβολή εκθέσεων και δοκιμές χωρίς προβλήματα. -Αναλυτικό ταμπλό που δίνει την κατάσταση	**Βασική λειτουργικότητα:** -Αποκατάσταση καταστροφών: αναπαραγωγή εικονικών μηχανών σχεδόν σε πραγματικό χρόνο και ενορχήστρωση διαδικασίας αποκατάστασης από καταστροφή με την Ανάκτηση τοποθεσίας. -Αντίγραφα ασφαλείας: αξιόπιστη προστασία για εικονικά, φυσικά περιβάλλοντα, cloud και SaaS, να διασφάλιση συνέπειας των δεδομένων των εφαρμογών, αύξηση απόδοσης και μείωση μεγέθους του backup - Άμεση αποκατάσταση: άμεση ανάκτηση VM, αρχείων και αντικείμενων εφαρμογών απευθείας από αντίγραφα αντιγράφων ασφαλείας. **Επιπλέον λειτουργικότητα:** -Προστασία από λυτρισμικό: προστασία από λυτρισμικό, βελτίωση αξιοπιστίας του backup και παροχή άμεσης ανάκτησης σε περίπτωση επίθεσης . -Διαχείριση μέσω μιας απλής διεπαφής ιστού -Παρακολούθηση VMware: Ισχυρό σύνολο εργαλείων για την παρακολούθηση της υποδομής VM.

υγείας και τον δείκτη ανακτησιμότητας των ε-φεδρικών στιγμιότυπων.	
διαθεσιμότητα 99.9%	---
προληπτική (BC), αντιδραστική (DR)	προληπτική (BC), αντιδραστική (DR)
διαθεσιμότητα και (λόγω κρυπτογράφησης) ε-μπιστευτικότητα	διαθεσιμότητα και (λόγω κρυπτογράφησης) εμπι-στευτικότητα
οτιδήποτε	οτιδήποτε
λυτρισμικό, παραβιάσεις, διακοπές λειτουργίας	λυτρισμικό
---	δημιουργία έως 4000 σημεία επαναφοράς για κάθε αντίγραφο ασφαλείας
30 μέρες δωρεάν	15 μέρες δωρεάν
Rest api, Cli, Web gui	Rest api, Cli, Web gui
Cohecity	Nakivo
Azure	AWS,Azure
υποστήριξη 24/7,επικοινωνια με τηλέφωνο, emails, chat	Επικοινωνία με τηλέφωνο emails και μηνύματα (Chat), forum, blog, βάση γνώσης, τεκμηρίωση

Arcserve UDP Cloud Direct	**N2WS Backup & Recovery for AWS Standard Edition**
IaaS	IaaS
ιδιωτικό, δημόσιο	δημόσιο
BCDR, κρυπτογράφηση	BCDR, κρυπτογράφηση
τιμολόγηση με βάση τον όγκο των δεδομένων και πληρωμή μηνιαίως	τιμολόγηση με βάση τα πακέτα (υπάρχουν 4 πα-κέτα) και πληρωμή μηνιαίως
Βασική λειτουργικότητα: Αντίγραφα ασφαλείας -Ρύθμιση και διαχείριση όλων των αναπτύξεων αντιγράφων ασφαλείας με μερικά κλικ και κλι-μάκωση απεριόριστα -Αυτόματη μεταφορά μεγάλων συνόλων δεδο-μένων με ασφάλεια εκτός τοποθεσίας με ελάχι-στη έως καθόλου ανάγκη για τακτική	**Βασική λειτουργικότητα** -Αυτοματοποιημένα αντίγραφα ασφαλείας -Επαναφορά μεμονωμένων αρχείων ή φακέλων χωρίς να χρειάζεται ανάκτηση του πλήρη όγκου. -Δημιουργία αντιγράφων ασφαλείας μεταξύ περιο-χών και ανάκτηση καταστροφών **Επιπλέον λειτουργικότητα:**

ανθρώπινη επίβλεψη -Λήψη όλων των δεδομένων σε διακομιστές με αντίγραφα ασφαλείας εικόνων. -Επιστροφή στο χρόνο σε πολλά σημεία ανάκτησης και επαναφορά χωρίς σφάλματα μέσα σε λίγα λεπτά Αποκατάσταση καταστροφών -Διαχείριση χρηστών και αναφορών και δημιουργία αντιγράφων ασφαλείας, επαναφορά και ανάκτηση συστημάτων και εφαρμογών προς/από οπουδήποτε με σύνδεση στο διαδίκτυο -Εγγύηση μεμονωμένων συστημάτων ή ολόκληρων περιβαλλόντων συνεχίζουν να λειτουργούν κατά τη διάρκεια μιας διακοπής λειτουργίας **Επιπλέον λειτουργικότητα:** Αντίγραφα ασφαλείας -Εξάλειψη των επιπτώσεων του ransomware με συνεχείς σαρώσεις ευπάθειας τρίτων, κρυπτογράφηση SSL και άλλους τεχνικούς ελέγχους. -Ελαχιστοποίηση της άντλησης πόρων του συστήματος με προηγμένη ανίχνευση αλλαγών και μεταφορά πολλαπλών νημάτων Αποκατάσταση καταστροφών -Ενεργοποίηση και αναπαραγωγή του δικτύου στο cloud και αστοχία για -συνέχιση των εργασιών ως συνήθως -Παροχή αντιγράφων ασφαλείας χωρίς πράκτορα για συμπλέγματα VMware με το Virtual Appliance της Arcserve για VMware.	-Αντιγραφή στιγμιότυπων σε άλλη περιοχή ή λογαριασμό AWS για προηγμένη προστασία δεδομένων. - Προγραμματισμός αυτοματοποιημένων σεναρίων DR -Δημιουργία αντιγράφων ασφαλείας μεταξύ λογαριασμών και ανάκτηση καταστροφών για την προστασία των δεδομένων από ευπάθειες λογαριασμού, όπως ransomware. -Υποστήριξη κλειδιού κρυπτογράφησης για ανάκτηση καταστροφών
RPO < 15 λεπτά, RTO < 5 λεπτά	RTO < 30 δευτερόλεπτα, RPO 5 λεπτά
προληπτική (BC), αντιδραστική (DR)	προληπτική (BC), αντιδραστική (DR)
διαθεσιμότητα και (λόγω κρυπτογράφησης) εμπιστευτικότητα	διαθεσιμότητα και (λόγω κρυπτογράφησης) εμπιστευτικότητα
οτιδήποτε	οτιδήποτε
λυτρισμικό, απώλεια δεδομένων	λυτρισμικό και ανθρώπινα λάθη
---	---

30 μέρες δωρεάν	30 μέρες δωρεάν
Web gui	Rest api, Cli, Web gui
Arcserve	N2W Software
κανένα	AWS
επικοινωνία με email ,τηλέφωνο, chat, tickets, κέντρο γνώσης, τεκμηρίωση, συζητήσεις, βίντεο	επικοινωνία μέσω email και τηλεφώνου, tickets, βάση γνώσης (knowledge base), έγγραφα, τεκμηρίωση, βίντεο, εκτιμητής κόστους

Actifio GO	**Hystax Backup and Disaster Recovery to AWS**
SaaS	IaaS
δημόσιο	δημόσιο
BCDR, κρυπτογράφηση	BCDR
τιμολόγηση με βάση τον όγκο των δεδομένων και πληρωμή μηνιαίως	τιμολόγηση με βάση τους πόρους που χρησιμοποιούνται (VMs)
Βασική λειτουργικότητα -Αντίγραφα ασφαλείας της μορφής Incremental-Forever τα οποία βελτιστοποιούν το εύρος ζώνης και τη χρήση αποθήκευσης -Γεωγραφικά διάσπαρτες τοποθεσίες για αποκατάσταση από καταστροφές -Δημιουργία αντιγράφων ασφαλείας VM χωρίς πράκτορα - Άμεση τοποθέτηση και ανάκτηση εικονικών μηχανών και βάσεων δεδομένων από οποιαδήποτε στιγμή σε πρωτεύουσες ή δευτερεύουσες περιοχές cloud ή υβριδικές περιοχές -Αντίγραφα ασφαλείας συνεπών και ενήμερων εφαρμογών **Επιπλέον λειτουργικότητα:** -Ευρεία υποστήριξη βάσεων δεδομένων -Τα backup for VMware δεν απαιτούν αποθηκευτικό χώρο κέντρου δεδομένων και μεταφέρονται απευθείας στο νέφος	**Βασική λειτουργικότητα:** -Ανάκτηση καταστροφών σε δημόσιο ή ιδιωτικό σύννεφο -Υποστήριξη ιδιωτικού ή δημόσιου νέφους. - Αποκατάσταση καταστροφών σε πολλαπλά νέφη -Δημιουργία αντιγράφων ασφαλείας στο νέφος -Επίπεδα αποκατάστασης καταστροφών
99% διαθεσιμότητα	---
προληπτική (BC), αντιδραστική (DR)	προληπτική (BC), αντιδραστική (DR)
διαθεσιμότητα και (λόγω κρυπτογράφησης) εμπιστευτικότητα	διαθεσιμότητα
δεδομένα	δεδομένα

λυτρισμικό, διακοπές λειτουργίας (disruptions)	---
μέγιστη συχνότητα δημιουργίας αντιγράφων ασφαλείας 15 λεπτά	η επιστροφή σε κανονική λειτουργία (failback) διαρκεί από 1 ωρα έως 1,2 ημέρες
30 μέρες ή 300$ όγκο δεδομένων (ότι έρθει πρώτο) δωρεάν	τίποτα δωρεάν
Rest api, Cli	Rest api, Web gui
Actifio	Hystax
GCP	AWS
υποστήριξη 24/7 ,επικοινωνία με τηλέφωνο και email και ύπαρξη πύλης (portal), ενημερώσεις λογισμικου	επικοινωνία με email, tickets, τηλέφωνο, έγγραφα, τεκμηρίωση, βάση γνώσης, συχνές ερωτήσεις, βίντεο

Zerto platform	**Axcient x360 recover d2c**
SaaS	IaaS
δημόσιο	ιδιωτικό, δημόσιο
BCDR	BCDR
3 εκδόσεις του προϊόντος, για SaaS 1 πακέτο πληρωμής (license) , για kubernetes 2 πακέτα πληρωμής και για εικονικές μηχανές 3 πακέτα πληρωμής, κάθε κατηγορία (SaaS, kubenrnetes, vm) έχει διαφορετικό τρόπο χρέωσης	---
Βασική λειτουργικότητα -Αποκατάστασης καταστροφών -Συνεχές Backup **Επιπλέον λειτουργικότητα:** -Μακροχρόνια διατήρηση -Κινητό ήτα δεδομένων και μεταναστεύσεις -Δοκιμή και ανάπτυξη -Ασφάλεια -Συμμόρφωση	**Βασική λειτουργικότητα** -Αντίγραφα ασφαλείας και αποκατάστασης καταστροφών απευθείας στο νέφος -Άμεση ανάκτηση **Επιπλέον λειτουργικότητα:** -Προστασία από κακόβουλο λογισμικό -Έλεγχος αν τα αρχεία αντίγραφα ασφαλείας μπορούν να ανακτηθούν και λήψη στιγμιότυπου οθόνης για το προστατευόμενο σύστημα
---	RTO 1 ώρα, RPO 15 λεπτά
προληπτική (BC), αντιδραστική (DR)	προληπτική (BC), αντιδραστική (DR)
διαθεσιμότητα	διαθεσιμότητα
οτιδήποτε	οτιδήποτε
φυσικές καταστροφές, αστοχίες υλικού, λυτρισμικό και διακοπές λειτουργίας	λυτρισμικό ή κατάρρευση δεδομένων
---	---

14 μέρες δωρεάν	14 μέρες δωρεάν
Rest api, Cli, Web gui	Rest api, Cli
Zerto	Axcient
Azure	κανένα
επικοινωνία μέσω τηλεφώνου, email και δημιουργίας αιτημάτων (cases), τεκμηρίωση, έγγραφα, forum, βάση γνώσης, πύλη (portal)	επικοινωνία με τηλέφωνο, emails, tickets, βάση γνώσης, συχνές ερωτήσεις, τεκμηρίωση

Πίνακας Αποτίμησης 3 – Προϊόντα IDS

ΚΡΙΤΗΡΙΑ/ΠΡΟΙΟΝΤΑ	**Security Onion 2**
α. τρόπος παράδοσης	IaaS
β. μοντέλο διάταξης	δημόσιο
γ. κατηγορία υπηρεσιών στην οποία ανήκει	IDS, ασφάλεια δικτύου
δ. μοντέλο κόστους	δωρεάν λογισμικό
ε. μηχανισμοί ασφάλειας που υλοποιούνται	**Βασική λειτουργικότητα** -NIDS: Συλλογή συμβάντων δικτύου για πλήρη κάλυψη του δικτύου -HIDS: Υποστηρίζει πολλούς πράκτορες συλλογής συμβάντων που βασίζονται σε ξενιστές -Διεπαφή για έλεγχο και διαχείριση των συναγερμών -Διεπαφή για διερεύνηση γεγονότων γρήγορα και εύκολα **Επιπλέον λειτουργικότητα:** -Στατική ανάλυση με εισαγωγή PCAP (διεπαφή προγραμματισμού εφαρμογών για την καταγραφή της κίνησης του δικτύου): εισαγωγή αρχείων PCAP για γρήγορη στατική ανάλυση και μελέτες περιπτώσεων. -Σταθμός εργασίας SOC (security onion console) : χρήση τοπικών εργαλείων Linux για την εκτέλεση ανάλυσης συμβάντων δικτύου και κεντρικού υπολογιστή. -Διεπαφή για απόκριση σε συμβάντα

στ. μη λειτουργικές εγγυήσεις	---
ζ. είδος προσφερόμενης προστασίας	ανιχνευτική
η. ιδιότητες ασφάλειας	---
θ. αντικείμενα που προστατεύονται	οτιδήποτε
ι. απειλές που αντιμετωπίζονται	---
ια. περιορισμοί	Υποστηρίζονται μόνο linux
ιβ. ύπαρξη δωρεάν εκδόσεων	δωρεάν λογισμικό
ιγ. τρόπος χρήσης προϊόντος	Cli, Web based gui
ιδ. εταιρεία που προσφέρει το προϊόν	Security Onion Solutions
ιε. marketplace(s) όπου προσφέρεται το προϊόν	AWS,Azure
ιστ. επίπεδο/είδος υποστήριξης για το προϊόν	2 πακέτα, επικονωνια μέσω emails

OSSEC HIDS Open Source Distribution from Atomicorp	**Atomic Enterprise OSSEC**
IaaS	SaaS, IaaS
δημόσιο	δημόσιο
IDS	IDS
δωρεάν λογισμικό	τιμολόγηση με βάση το φόρτο εργασίας
Βασική λειτουργικότητα: -Ανίχνευση εισβολής βάσει κεντρικού υπολογιστή -Ανίχνευση εισβολής βάσει αρχείων καταγραφής **Επιπλέον λειτουργικότητα** -Παρακολούθηση ακεραιότητας αρχείων -Ανίχνευση Rootkit -Ενεργή απόκριση	**Βασική λειτουργικότητα:** -Ανίχνευση εισβολής βάσει κεντρικού υπολογιστή - Ανίχνευση εισβολής βάσει αρχείων καταγραφής **Επιπλέον λειτουργικότητα** -Παρακολούθηση ακεραιότητας αρχείων -Ανίχνευση Rootkit -Ενεργή απόκριση -Ευφυία απειλών -Αναφορά συμμόρφωσης (PCI, DISA, άλλα) -Γραφικό περιβάλλον για διαχείριση κανόνων -Υποστήριξη Ανάπτυξης Κανόνων -Προσαρμοσμένες ειδοποιήσεις για παρακολούθηση ακεραιότητας αρχείων -Γραφικό περιβάλλον για διαχείριση επαναφοράς (rollback) -Διαχείριση Ενεργητικής Απόκρισης
---	---
ανιχνευτική	ανιχνευτική

ακεραιότητα	ακεραιότητα
ξενιστές	ξενιστές
rootkits, κακόβουλο λογισμικό	rootkits, κακόβουλο λογισμικό
υποστηρίζονται 100-999 κανόνες (100΄s rules)	υποστηρίζονται έως περίπου 5000 κανόνες
δωρεάν λογισμικό	30 μέρες δωρεάν στο Azure
Cli	Cli, Web based gui
Atomicorp	Atomicorp
AWS,GCP	AWS, GCP, Azure
επικοινωνία με mail, τηλέφωνο	2 πακέτα (1 8/5 και 1 24/7) επικοινωνία με τηλέφωνο, email, tickets, πύλη υποστήριξης, διαχείριση συνδρομής, τεκμηρίωση, έγγραφα, συχνές ερωτήσεις, βάση γνώσης, forum, ενημέρωση για νέες εκδόσεις, κέντρο αυτο βοήθειας

Flow Threat Detection	**Big HIDS SaaS**
SaaS	SaaS
δημόσιο	δημόσιο
IDS, ασφάλεια δικτύου	IDS
τιμολόγηση με βάση τις ώρες χρήσης του AWS sagemaker	τιμολόγηση με βάση τον όγκο των δεδομένων (εύρος ζώνης), μηνιαία, τρίμηνη ή ετήσια πληρωμή
Βασική λειτουργικότητα -Σύστημα ανίχνευσης εισβολών στο δίκτυο -Ανάλυση δικτύου -Ανίχνευση απειλών	**Βασική λειτουργικότητα:** -Ανίχνευση εισβολών **Επιπλέον λειτουργικότητα** - Άμυνα σε πραγματικό χρόνο - Προσδιορισμός κινδύνων - Ιχνηλασιμότητα επιθέσεων -24/7 παρακολούθηση και αναφορά συναγερμών έκτακτης ανάγκης μέσω email, SMS κ.λπ
---	---
ανιχνευτική	ανιχνευτική
---	---
δίκτυο	οτιδήποτε
εντοπισμός επιθέσεων ωμής βίας, DDos, and DoS	κακόβουλος κώδικας και επιθέσεις ωμής βίας
το μέγιστο μέγεθος δεδομένων εισόδου ανά εκτέλεση του προγράμματος (per invocation) είναι 25mb συμφωνα με το AWS, Συνολική ακρίβεια (δυαδική ανίχνευση): 84%	---

Συνολική ανάκληση (δυαδική ανίχνευση): 84% Ακρίβεια πολλαπλών κλάσεων (ανίχνευση πολλαπλών κλάσεων): 78%	
5 μέρες	τίποτα δωρεάν
Cli	Cli
VyoPath	HONGKONG SEAGA TECHNOLOGY LIMITED (en.wangsu.com)
AWS	AWS
επικοινωνία μέσω τηλεφώνου, email και chat	5 πακέτα υποστήριξης (4 24/7 και 1 9.00-24.00). Επικοινωνία με τηλέφωνο, email, tickets, chat , κέντρο αυτοβοήθειας, τεκμηρίωση

Trend Micro Deep Security	**Netgate pfSense Plus Firewall/VPN/Router**
IaaS	IaaS
δημόσιο	δημόσιο
IDS, ασφάλεια δικτύου, ασφάλεια ιστού	IDS, ασφάλεια ασφάλεια δικτύου, ασφάλεια ιστού
τιμολόγηση με βάση το φόρτο εργασίας μηνιαία ή με άδεια χρήσης (BYOL)	δωρεάν λογισμικό
Βασική λειτουργικότητα -Αποτροπή εισβολών **Επιπλέον λειτουργικότητα:** -Προστασία από κακόβουλο λογισμικό -Τείχος προστασίας -Φιλτράρισμα περιεχομένου και μαρκάρισμα επικίνδυνων url -Παρακολούθηση ακεραιότητας -Επιθεώρηση αρχείων καταγραφής -Έλεγχος εφαρμογών για αλλαγές	**Βασική λειτουργικότητα:** -Αποτροπή επιθέσεων (IDS/IPS) **Επιπλέον λειτουργικότητα:** - Τείχος προστασίας -Δρομολογητής -VPN -Φιλτράρισμα διακομιστή μεσολάβησης και περιεχομένου -Υπηρεσίες Δικτύου -Αναφορά/παρακολούθηση συστήματος -Διαχείριση Ασφάλειας Συστήματος -Διαχείριση Αξιοπιστίας/Ανθεκτικότητας
---	---
ανιχνευτική, προληπτική	ανιχνευτική, προληπτική
ακεραιότητα, διαθεσιμότητα	διαθεσιμότητα
οτιδήποτε	οτιδήποτε
κακόβουλο λογισμικό, απειλές διαδικτύου	κακόβουλο λογισμικό, απειλές διαδικτύου
---	απόδοση έως 10 Gbps
30 μέρες δωρεάν	δωρεάν λογισμικό
Rest api, Cli, Web gui	Cli, Web gui

Trend micro	Netgate
AWS, Azure	AWS, Azure
2 πακέτα, επικοινωνία μέσω τηλεφώνου 24/7 ,email, tickets, chat, κέντρο βοήθειας, συχνές ερωτήσεις, τεκμηρίωση, έγγραφα, ενημερώσεις και αναβαθμίσεις προϊόντων, κοινότητα, forum	3 πακέτα, υποστήριξη 24/7, επικοινωνία με email, τηλέφωνο, κοινότητα, έγγραφα, τεκμηρίωση, συχνές ερωτήσεις

Wazuh All-In-One Deployment	**OPNsense Firewall/Router/VPN/IDPS**
IaaS	IaaS
δημόσιο	δημόσιο
IDS	IDS, ασφάλεια δικτύου, ασφάλεια ιστού
δωρεάν λογισμικό	δωρεάν λογισμικό
Βασική λειτουργικότητα: -Σύστημα ανίχνευσης εισβολής **Επιπλέον λειτουργικότητα:** -Ανάλυση δεδομένων καταγραφής -Παρακολούθηση ακεραιότητας αρχείων -Rootkits και εντοπισμός κακόβουλου λογισμικού -Αξιολόγηση Διαμόρφωσης Ασφαλείας -Παρακολούθηση πολιτικών ασφαλείας, κλήσεις συστήματος, εντολές -Ενεργή ανταπόκριση -Παρακολούθηση συστημάτων και δεδομένων χωρίς πράκτορες -Μηχανισμός αποτροπής πλημμυρίσματος από δεδομένα -Απογραφή συστήματος -Ανίχνευση τρωτών σημείων	**Βασική λειτουργικότητα:** -Ανίχνευση & αποτροπή εισβολών **Επιπλέον λειτουργικότητα:** - Τείχος προστασίας -Διαμόρφωση κίνησης δικτύου -Πιστοποίηση ταυτότητας δύο παραγόντων -Εικονικό ιδιωτικό δίκτυο -Υψηλή διαθεσιμότητα / Ανακατεύθυνση αποτυχίας υλικού -Φιλτράρισμα ιστού βάσει κατηγορίας, εκτενείς λίστες ελέγχου πρόσβασης -Δημιουργία αντιγράφων ασφαλείας και επαναφορά των ρυθμίσεων διαμόρφωσης -Αναφορά & Παρακολούθηση του συστήματος -Αναβαθμίσεις και προσθετά
---	---
ανιχνευτική	ανιχνευτική, προληπτική
ακεραιότητα	διαθεσιμότητα
οτιδήποτε	οτιδήποτε
κακόβουλο λογισμικό, rootkits	κακόβουλο λογισμικό, απειλές διαδικτύου
---	---
δωρεάν λογισμικό	δωρεάν λογισμικό
Rest api, Cli, Web gui	Rest api, Cli, Web gui
Wazuh	Deciso Sales B.V.

AWS	AWS,Azure
2 πακέτα (8/5 και 24/7) επικοινωνία με email, slack, github ,Google group, τεκμηρίωση	επικοινωνία μέσω email, κοινότητα, forum, τεκμηρίωση, έγγραφα, επικοινωνία μεταξύ των χρηστών

Heimdal Threat Prevention-Endpoint	**Lacework Cloud Security Platform**
IaaS	SaaS
δημόσιο	δημόσιο
IDS, ασφάλεια ιστού	IDS
πληροφορίες τιμολόγησης μόνο μέσω επικοινωνίας με την εταιρία	τιμολόγηση με βάση τον αριθμό λογαριασμών χρηστών στο νέφος, πληρωμή ετησίως, και κάθε λογαριασμός υποστηρίζει έως 200 αντικείμενα (assets).
Βασική λειτουργικότητα: -Σύστημα αποτροπής εισβολής βασισμένο σε κεντρικούς υπολογιστές **Επιπλέον λειτουργικότητα:** - Εργαλεία κυνηγιού απειλών για τη χαρτογράφηση των κρίσιμων για την ασφάλεια σημείων -Αλγόριθμος AI & ML που προβλέπει εάν ένας τομέας είναι κακόβουλος προτού φιλοξενήσει οποιοδήποτε κακόβουλο περιεχόμενο. -Προηγμένα νευρωνικά δίκτυα και γλωσσική ανάλυση AI για έξυπνη πρόληψη -Μηχανική εκμάθηση για την καθιέρωση μοτίβων ευπάθειας και προσφορά δεικτών τρωτότητας/επίθεσης (IOA/IOC)	**Βασική λειτουργικότητα:** -Ανίχνευση εισβολής βάσει κεντρικού υπολογιστή -Ανίχνευση ανωμαλιών συμπεριφοράς **Επιπλέον λειτουργικότητα:** - Παρακολούθηση ακεραιότητας αρχείων - Συμμόρφωση με τη διαμόρφωση του cloud - Προστασία από απειλές χρόνου εκτέλεσης (runtime) - Container & Kubernetes Security: Το Lacework παρέχει βαθιά ορατότητα στην ανάπτυξη του Kubernetes.
---	Αν η υπηρεσία δεν λειτουργήσει όπως περιγράφεται στην τεκμηρίωση ο πελάτης μπορεί να διακόψει τη συνδρομή και να πάρει πίσω πιθανό προπληρωμένο ποσό
ανιχνευτική, προληπτική	ανιχνευτική
διαθεσιμότητα	ακεραιότητα
ξενιστές	οτιδήποτε
Επιθέσεις μηδενικής ώρας, λυτρισμικό, διαρροές δεδομένων, απειλές διαδικτύου, κακόβουλο λογισμικό	---
---	με μία άδεια για κάθε λογαριασμό καλύπτονται μέχρι 200 αντικείμενα στο νέφος
30 μέρες δωρεάν	τίποτα δωρεάν

Rest api, Web gui	Rest api, Cli, Web gui
Heimdal security	Lacework
Azure	AWS
24/7 υποστήριξη, επικοινωνία με τηλέφωνο, email, tickets, βάση γνώσης, συχνές ερωτήσεις, τεκμηρίωση	3 πακέτα, υποστήριξη από 12/5 έως 24/7, επικοινωνία μέσω email, chat, τεκμηρίωση, συχνές ερωτήσεις, κοινότητα, πύλη υποστήριξης, βάση γνώσης

Suricata	**Advanced Intrusion Detection Environment**
IaaS	IaaS
δημόσιο	δημόσιο
IDS, ασφάλεια ασφάλεια δικτύουυ	IDS
δωρεάν λογισμικό	δωρεάν λογισμικό
Βασική λειτουργικότητα: -IDS / IPS -Υψηλή απόδοση: Μια μεμονωμένη παρουσία Suricata είναι ικανή να επιθεωρεί κυκλοφορία πολλών gigabit. **Επιπλέον λειτουργικότητα:** - Καταγραφή και ανάλυση TLS/SSL - Καταγραφή HTTP - Καταγραφή DNS -Αυτόματη ανίχνευση πρωτοκόλλων -Lua Scripting: Προηγμένη ανάλυση και λειτουργικότητα διαθέσιμη για τον εντοπισμό πραγμάτων που δεν είναι δυνατά στη σύνταξη του συνόλου κανόνων. -Έξοδος σε συγκεκριμένη μορφή που επιτρέπει την εύκολη ενσωμάτωση με άλλα εργαλεία	**Βασική λειτουργικότητα:** -Ανίχνευση εισβολής βάσει κεντρικού υπολογιστή ελέγχοντας την ακεραιότητα των αρχείων
---	---
ανιχνευτική, προληπτική	ανιχνευτική
διαθεσιμότητα	ακεραιότητα
οτιδήποτε	ξενιστές
κακόβουλο λογισμικό και κανάλια command and control	---
---	δεν υποστηρίζονται windows
δωρεάν λογισμικό	δωρεάν λογισμικό
Rest api, Cli, Web gui	Cli
Open Information Security Foundation (OISF)	GNU General Public License

σε κανένα	σε κανένα
επικοινωνία μέσω email και chat, έγγραφα, τεκμηρίωση, βίντεο, κοινότητα, forum, συχνές ερωτήσεις	επικοινωνία μέσω email, μηνυμάτων, github

Snort	**AhnLab CPP**
IaaS	IaaS
δημόσιο	δημόσιο
IDS, ασφάλεια ασφάλεια δικτύουυ	IDS, ασφάλεια ασφάλεια δικτύου
δωρεάν λογισμικό	τιμολόγηση με βάση το φόρτο εργασίας και πληρωμή ανά μήνα, υπάρχει και η επιλογή BYOL
Βασική λειτουργικότητα: -NIPDS (Σύστημα ανίχνευσης και αποτροπής εισβολής βάσει δικτύου) **Επιπλέον λειτουργικότητα:** -Λειτουργία Packet Sniffer: το λογισμικό θα διαβάζει πακέτα IP και στη συνέχεια θα τα εμφανίζει στον χρήστη στην κονσόλα του. -Λειτουργία καταγραφής πακέτων - Παρακολούθηση κυκλοφορίας σε πραγματικό χρόνο - Καταγραφή πακέτων -Ανάλυση Πρωτοκόλλων - Αντιστοίχιση περιεχομένου -Το SNORT μπορεί να χρησιμοποιηθεί για τον προσδιορισμό της πλατφόρμας λειτουργικού συστήματος που χρησιμοποιείται από ένα σύστημα που έχει πρόσβαση σε ένα δίκτυο.	**Βασική λειτουργικότητα:** Εντοπισμός και αποτροπή εισβολής (IDS και IPS) **Επιπλέον λειτουργικότητα:** -Ενιαία Λειτουργία και Διαχείριση -Έλεγχος Εφαρμογών -Τείχος προστασίας -Προστασία από κακόβουλο λογισμικό -Παρακολούθηση ακεραιότητας
---	---
ανιχνευτική, προληπτική	ανιχνευτική, προληπτική
διαθεσιμότητα	ακεραιότητα, διαθεσιμότητα
οτιδήποτε	οτιδήποτε
επιθέσεις DoS, DDos, κοινής διεπαφής πύλης (Common Gateway Interface), υπερχείλιση προσωρινής μνήμης, και σάρωση λαθραίων πυλών (stealth port scan)	κακόβουλο λογισμικό
---	---
δωρεάν λογισμικό	τίποτα δωρεάν

Cli, Web gui	Rest api, Web gui
Cisco	AhnLab, Inc.
σε κανένα	AWS, Azure
επικοινωνία μέσω email και discord, έγγραφα, συχνές ερωτήσεις, τεκμηρίωση, κοινότητα, βίντεο	3 πακέτα και υποστήριξη σε εργάσιμο ωράριο, εργάσιμο και σαββατοκύριακα, 24/7 αντίστοιχα, επικοινωνία μέσω email, τηλεφώνου, chat, tickets (TAC portal), συχνές ερωτήσεις, κέντρο υποστήριξης

Πίνακας Αποτίμησης 4 – Προϊόντα IAM

ΚΡΙΤΗΡΙΑ/ΠΡΟΙΟΝΤΑ	**JumpCloud Directory-as-a-Service**
α. τρόπος παράδοσης	SaaS
β. μοντέλο διάταξης	δημόσιο
γ. κατηγορία υπηρεσιών στην οποία ανήκει	IAM
δ. μοντέλο κόστους	4 πακέτα τιμολόγησης ανά χρήστη, βασικά χαρακτηριστικά με τα υπό-χαρακτηριστικά τους και πληρωμή μηνιαία ή ετήσια.
ε. μηχανισμοί ασφάλειας που υλοποιούνται	**Βασική λειτουργικότητα:** -Διαχείριση Ταυτότητας: Υπηρεσία καταλόγου που βασίζεται στο νέφος Διαχείριση χρηστών Διαχείριση Γκρουπ -Έλεγχος πρόσβασης και υποστήριξη πρωτοκόλλων LDAP που βασίζεται στο νέφος RADIUS που βασίζεται στο νέφος SAML 2.0 **Επιπλέον λειτουργικότητα:** -Διαχείριση Ταυτότητας Πολυπλοκότητα κωδικού πρόσβασης και διαχείριση κλειδιών SSH Έλεγχος ταυτότητας πολλαπλών παραγόντων -Έλεγχος πρόσβασης και υποστήριξη πρωτοκόλλων

	Πολυπλοκότητα κωδικού πρόσβασης και διαχείριση κλειδιών SSH Σταθμός εργασίας Mac, Windows και Linux που βασίζεται σε πράκτορες και σύνδεση διακομιστή
στ. μη λειτουργικές εγγυήσεις	---
ζ. είδος προσφερόμενης προστασίας	προληπτική
η. ιδιότητες ασφάλειας	---
θ. αντικείμενα που προστατεύονται	ταυτότητες χρηστών
ι. απειλές που αντιμετωπίζονται	---
ια. περιορισμοί	σε κάθε χρήστη αντιστοιχούν έως 3 συσκευές
ιβ. ύπαρξη δωρεάν εκδόσεων	μόνιμη δωρεάν έκδοση για 10 χρήστες και 10 συσκευές
ιγ. τρόπος χρήσης προϊόντος	Rest api, Cli, Web gui
ιδ. εταιρεία που προσφέρει το προϊόν	Jumpcloud
ιε. marketplace(s) όπου προσφέρεται το προϊόν	GCP
ιστ. επίπεδο/είδος υποστήριξης για το προϊόν	3 πακέτα (1 πακέτο 8/5 και 2 πακέτα 24/7) επικοινωνία με τηλέφωνο, email, chat, tickets, βάση γνώσης, κοινότητα, έγγραφα, κέντρο βοήθειας

Evidian IDaaS (Identity as a Service)	**Cloud Identity Premium**
SaaS	SaaS
δημόσιο	δημόσιο
IAM	IAM
τιμολόγηση με βάση τον αριθμό χρηστών και τα χαρακτηριστικά, δυνατότητα αγοράς για 1 χρόνο ή 3 χρονιά με έκπτωση και πληρωμή ανά έτος ή ανά τριετία	τιμολόγηση με βάση τα χαρακτηριστικά και τον αριθμό χρηστών και πληρωμή μηνιαίως ή ετησίως
Βασική λειτουργικότητα: -SSO -Γενικά πρότυπα SAML -Ισχυρός έλεγχος ταυτότητας & έλεγχος ταυτότητας πολλαπλών παραγόντων -Διαχείριση χρηστών -Πίνακες ελέγχου & αναφορές **Επιπλέον λειτουργικότητα:** -Identity Federation & Προ-ενσωματωμένες	**Βασική λειτουργικότητα:** -Ασφάλεια λογαριασμού και MFA -Εύκολη πρόσβαση σε εφαρμογές με SSO -Ενοποιημένη κονσόλα διαχείρισης -εφαρμογές που προστατεύονται με κωδικό πρόσβασης -Γρήγορη και εύκολη ανάπτυξη διαχείρισης τελικού σημείου **Επιπλέον λειτουργικότητα:**

εφαρμογές SAML -Σύνθετες αναφορές & Πίνακας ελέγχου (προ-αιρετικό πρόσθετο)	-Ασφάλεια συσκευής με διαχείριση τελικού σημείου -Ενσωμάτωση με εφαρμογές -Διαχείριση υβριδικής ταυτότητας -Πρόσβαση με επίγνωση του περιβάλλοντος -Εύκολη πρόσβαση σε εφαρμογές εσωτερικής ε-γκατάστασης -Αυτόματη διαχείριση του κύκλου ζωής -Αυτοματοποιημένη παροχή χρηστών -Προστασία από κλοπή λογαριασμού -έλεγχος και αναφορά μεθόδων MFA
99.9%διαθεσιμοτητα	99.9% διαθεσιμότητα, για 99% έως 99.9% 3 μέρες χρήσης ή πιστώνουν το αντίστοιχο χρηματικό ποσό, για 95% έως 99% 5 μέρες και για <95% 15 μέρες
προληπτική	προληπτική
εμπιστευτικότητα	---
ταυτότητες χρηστών	λογαριασμοί χρηστών και εταιρικά δεδομένα
---	ηλεκτρονικό ψάρεμα, hijacking
διαχείριση έως 1 εκατομμυριο ταυτότητες	---
τίποτα δωρεάν	14 μέρες δωρεάν ή μόνιμη δωρεάν έκδοση με περιορισμένες δυνατότητες
Web gui	Rest api, Web gui
Atos	Google Enterprise API
GCP	GCP
2 πακέτα, επικοινωνία με τηλέφωνο, mail, tickets, βάση γνώσης, πύλη υποστήριξης, τεκμηρίωση, έγγραφα, βίντεο	3 πακέτα (1 8/5 και 2 24/7) επικοινωνία με chat, email, τηλέφωνο σε 14 γλώσσες, τεκμηρίωση, κέντρο βοήθειας, κοινότητα, συχνές ερωτήσεις)

ForgeRock Identity Cloud	**Entrust Identity as a Service**
SaaS	SaaS
δημόσιο	δημόσιο
IAM,BCDR	IAM
5 πακέτα τιμολόγησης με βάση τα χαρακτηριστικά	3 πακέτα τιμολόγησης με βάση τα χαρακτηριστικά και τον αριθμό χρηστών, μηνιαία χρέωση
Βασική λειτουργικότητα: -Διαχείριση ταυτότητας -Διαχείριση Πρόσβασης -single sign-on (SSO) και ομοσπονδιακό SSO -Προσαρμοστικός έλεγχος ταυτότητας και	**Βασική λειτουργικότητα:** -Ταυτοποίηση πολλαπλών παραγόντων -Ενιαίο SSO -Εξουσιοδότηση και διαχείριση πρόσβασης -Πρόσβαση βασισμένη σε διαπιστευτήρια υψηλής

πολλαπλών παραγόντων (MFA) **Επιπλέον λειτουργικό-** **τητα:** -Ισχυροί παράγοντες ελέγχου ταυτότητας, ό-πως κωδικός πρόσβασης μίας χρήσης (OTP), επιβεβαίωση μέσω email, Mobile Push, Magic Link. -Ενσωμάτωση με τα κιτ ανάπτυξης λογισμικού της ForgeRock (SDK)	διασφάλισης -Έλεγχος ταυτότητας και εξουσιοδότηση εφαρμογής ενσωματωμένης συσκευής **Επιπλέον λειτουργικότητα:** -Επιλογές χωρίς κωδικό πρόσβασης – προώθηση για κινητά, FIDO και βάσει διαπιστευτηρίων -Προσαρμοστικός έλεγχος ταυτότητας βάσει κινδύ-νου -Ανίχνευση και πρόληψη απάτης -Ενορχήστρωση ταυτότητας -Επαναφορά κωδίκων πρόσβασης με αυτοεξυπη-ρέτηση -Ενσωματώσεις, API και SDK -Κρυπτογράφηση email και αρχείων, υπογραφή εγ-γράφων
99.99% διαθεσιμότητα, για 99-99.99% επι-στροφή 5% της μηνιαίας συνδρομής, για 95-99% επιστροφή 10%, για <95% επιστροφή 25%	99.9% διαθεσιμότητα, για 99% έως 99.9% 3 μέρες χρήσης ή πιστώνουν το αντίστοιχο χρηματικό ποσό , για 95% έως 99% 5 μέρες και για <95% 15 μέρες
προληπτική	προληπτική
εμπιστευτικότητα, ακεραιότητα και διαθεσιμό-τητα	---
ταυτότητες χρηστών	ταυτότητες χρηστών
---	απάτες (frauds)
---	---
τίποτα δωρεάν	60 μέρες δωρεάν
Rest api, Web gui	Web gui, Rest api
ForgeRock	Entrust
GCP	Azure
2 πακέτα, επικοινωνία με τηλέφωνο email, tickets, πύλη υποστήριξης, βάση γνώσης, τεκ-μηρίωση, κοινότητα	2 πακέτα (24/5 και 24/7)) επικοινωνία με τηλέφωνο, email, chat, τεκμηρίωση, συχνές ερωτήσεις, έγ-γραφα, πύλη υποστήριξης

Compact Identity - The Ultimate IAM Solu-tion	**HelloID**
SaaS	SaaS
δημόσιο	δημόσιο
IAM	IAM

τιμολόγηση με βάση τη χρήση (pay per use)	3 πακέτα τιμολόγησης με βάση τα βασικά χαρακτηριστικά με τα υπό-χαρακτηριστικά τους και τον αριθμό χρηστών, χρέωση ανά μήνα
Βασική λειτουργικότητα: -Προσαρμοστικός έλεγχος ταυτότητας πολλαπλών παραγόντων -Διαχείριση κωδικών πρόσβασης -Διαχείριση Πρόσβασης -Διαχείριση Ταυτότητας -Αναλυτικά στοιχεία ταυτότητας **Επιπλέον λειτουργικότητα:** -Διακυβέρνηση ταυτότητας -Διαχείριση πρόσβασης με προνόμια	**Βασική λειτουργικότητα:** -Παροχή ταυτότητας -Διαχείριση πρόσβασης **Επιπλέον λειτουργικότητα:** -Αυτοματοποίηση Υπηρεσιών: Το Service Automation συνδέεται απρόσκοπτα με την παροχή ταυτότητας.
99.9%διαθεσιμοτητα	99.9%διαθεσιμοτητα
προληπτική	προληπτική
---	---
ταυτότητες χρηστών	ταυτότητες χρηστών
---	---
---	υποστηρίζονται έως 50000 χρήστες
30 μέρες δωρεάν	30 μέρες δωρεάν
Web gui	Web gui, Rest api
Ilantus technologies	Tools4ever B.V.
Azure	Azure
4 πακέτα, υποστήριξη από 8/5 έως 24/7, επικοινωνία με emails τηλέφωνο, βάση γνώσης, αναβαθμίσεις, εκπαιδευτικό υλικό	2 πακέτα (8/5 και 24/7),επικοινωνία με τηλέφωνο, emails, πύλη υποστήριξης, forum, έγγραφα, τεκμηρίωση, συχνές ερωτήσεις

DoubleClue	**WSO2 Identity Server**
SaaS	IaaS
δημόσιο	δημόσιο, ιδιωτικό
IAM	IAM
---	δωρεάν προιον
Βασική λειτουργικότητα: -8 διαφορετικές μέθοδοι ελέγχου ταυτότητας -Διαχείριση ταυτότητας και πρόσβασης -Ενιαία σύνδεση (SSO) -Ταυτοποίηση δυο παραγόντων -Διαχείριση πολλαπλών κωδικών πρόσβασης	**Βασική λειτουργικότητα:** -Ομοσπονδία Ταυτότητας και SSO -Ισχυρός και προσαρμοστικός έλεγχος ταυτότητας -Διαχείριση λογαριασμού και παροχή ταυτότητας -Έλεγχος πρόσβασης -Αναλυτικά στοιχεία ταυτότητας

με MFA -Ενσωμάτωση RADIUS, OpenID, SAML και Rest **Επιπλέον λειτουργικότητα:** -Έκδοση εφαρμογής Android & iOS -Νέφος υψηλής ασφάλειας -Συγχρονισμός Azure, AD και LDAP	 **Επιπλέον λειτουργικότητα:** -Γεφύρωση Ταυτότητας -APIs και Microservices Security -Συμμόρφωση με το απόρρητο
---	---
προληπτική	προληπτική
---	---
ταυτότητες χρηστών, δεδομένα	ταυτότητες χρηστών
μη εξουσιοδοτημένη και επιβλαβή πρόσβαση τρίτων	---
---	---
30 μέρες δωρεάν	δωρεάν προιον
Web gui,Rest api	Rest api, Cli, Web gui
HWS Informationssysteme GmbH	WSO2
Azure	Azure
υποστήριξη 24/7, επικοινωνία με email, τηλέφωνο, τεκμηρίωση, τεχνικά έγγραφα	υποστήριξη 24/7, επικοινωνία με τηλέφωνο, email, tickets, τεκμηρίωση, έγγραφα, πύλη υποστήριξης, blog, forum, κοινότητα, ενημερώσεις προϊόντων

DoubleClue	**WSO2 Identity Server**
SaaS	IaaS
δημόσιο	δημόσιο, ιδιωτικό
IAM	IAM
---	δωρεάν προιον
Βασική λειτουργικότητα: -8 διαφορετικές μέθοδοι ελέγχου ταυτότητας -Διαχείριση ταυτότητας και πρόσβασης -Ενιαία σύνδεση (SSO) -Ταυτοποίηση δυο παραγόντων -Διαχείριση πολλαπλών κωδικών πρόσβασης με MFA -Ενσωμάτωση RADIUS, OpenID, SAML και Rest **Επιπλέον λειτουργικότητα:**	**Βασική λειτουργικότητα:** -Ομοσπονδία Ταυτότητας και SSO -Ισχυρός και προσαρμοστικός έλεγχος ταυτότητας -Διαχείριση λογαριασμού και παροχή ταυτότητας -Έλεγχος πρόσβασης -Αναλυτικά στοιχεία ταυτότητας **Επιπλέον λειτουργικότητα:** -Γεφύρωση Ταυτότητας

-Έκδοση εφαρμογής Android & iOS -Νέφος υψηλής ασφάλειας -Συγχρονισμός Azure, AD και LDAP	-APIs και Microservices Security -Συμμόρφωση με το απόρρητο
---	---
προληπτική	προληπτική
---	---
ταυτότητες χρηστών, δεδομένα	ταυτότητες χρηστών
μη εξουσιοδοτημένη και επιβλαβή πρόσβαση τρίτων	---
---	---
30 μέρες δωρεάν	δωρεάν προϊόν
Web gui, Rest api	Rest api, Cli, Web gui
HWS Informationssysteme GmbH	WSO2
Azure	Azure
υποστήριξη 24/7, επικοινωνία με email, τηλέφωνο, τεκμηρίωση, τεχνικά έγγραφα	υποστήριξη 24/7, επικοινωνία με τηλέφωνο, email, tickets τεκμηρίωση, έγγραφα, πύλη υποστήριξης, blog, forum, κοινότητα, ενημερώσεις προϊόντων

Okta Identity Platform (okta workforce identity)	**Workforce Identity Solutions (ping one)**
SaaS	SaaS
δημόσιο	δημόσιο
IAM	IAM
2 πακέτα, τιμολόγηση με βάση τα βασικά χαρακτηριστικά με τα υπό-χαρακτηριστικά τους και τον αριθμό χρηστών ,χρέωση μηνιαίως, ελάχιστη τιμή ετήσιου συμβολαίου 1500$	3 πακέτα, τιμολόγηση με βάση τον αριθμό χρηστών και τα χαρακτηριστικά, πληρωμή ετησίως

Βασική λειτουργικότητα: -SSO -Καθολικός κατάλογος: Ένας κατάλογος για όλους τους χρήστες, τις ομάδες και τις συσκευές -Προσαρμοστικός έλεγχος ταυτότητας πολλαπλών παραγόντων **Επιπλέον λειτουργικότητα:** -Διαχείριση Κύκλου Ζωής: Διαχείριση της παροχή ταυτότητας με εύκολο στην εφαρμογή αυτοματισμό -Access Gateway: Επέκταση της σύγχρονη ταυτότητας σε on-premium εφαρμογές και προστασία του υβριδικού νέφους -Διαχείριση πρόσβασης API -Προηγμένη πρόσβαση διακομιστή: Τα στοιχεία ελέγχου πρόσβασης διακομιστή είναι τόσο δυναμικά όσο η υποδομή πολλαπλών νέφους	**Βασική λειτουργικότητα:** -Ενιαία σύνδεση για όλες τις εφαρμογές -Κεντρική ασφάλεια πρόσβασης -Προσαρμοστικός έλεγχος ταυτότητας πολλαπλών παραγόντων **Επιπλέον λειτουργικότητα:** -Ενορχήστρωση ταυτότητας χωρίς κώδικα -Ενιαία διαχείριση -Ενιαία πηγή καταλόγου & πηγή δεδομένων
99.99% διαθεσιμότητα	---
προληπτική	προληπτική
---	---
ταυτότητες χρηστών	ταυτότητες χρηστών
επιθέσεις εστιασμένες σε διαπιστευτήρια	**---**
---	---
30 μέρες δωρεάν	30 μέρες δωρεάν
Rest api, Cli, Web gui	Rest api, Cli, Web gui
Okta	Ping Identity
AWS	AWS
5 πακέτα (3 24/7 και 2 12/5), επικοινωνία με τηλέφωνο, email, tickets, τεκμηρίωση, βάση γνώσης, τεχνικά έγγραφα, κοινότητα	3 πακέτα, υποστήριξη 24/7, επικοινωνία με τηλέφωνο, emails, tickets, forum, συχνές ερωτήσεις,, έγγραφα, κοινότητα, τεκμηρίωση, πύλη υποστήριξης, βάση γνώσης, βίντεο

SecureAuth Identity Platform	**KeyCloak: Identity and Access Management**
SaaS	IaaS
δημόσιο	δημόσιο
IAM	IAM

τιμολόγηση με βάση τον αριθμό χρηστών και πληρωμή ετησιως	δωρεάν προιον
Βασική λειτουργικότητα: -Προσαρμοστικός έλεγχος ταυτότητας -Έλεγχος ταυτότητας πολλαπλών παραγόντων -Single Sign-on -Ευφυΐα ελέγχου ταυτότητας -Έλεγχος ταυτότητας βάσει κινδύνου -Απλή Διαχείριση **Επιπλέον λειτουργικότητα:** -Έλεγχος ταυτότητας χωρίς κωδικό πρόσβασης -Διαχείριση κύκλου ζωής χρήστη -Επέκταση ασφάλειας σύνδεσης -Ενοποίηση καταλόγου -Αυτοεξυπηρέτηση χρήστη	**Βασική λειτουργικότητα:** -Single-Sign On -Υπηρεσίες εξουσιοδότησης -Κονσόλα διαχειριστή: Μέσω της κονσόλας διαχειριστή, οι διαχειριστές μπορούν να διαχειρίζονται κεντρικά όλες τις πτυχές του διακομιστή Keycloak. -πρωτόκολλα: OpenID Connect, Auth 2.0, SAML **Επιπλέον λειτουργικότητα:** -Σύνδεση κοινωνικής δικτύωσης: Ενεργοποίηση σύνδεσης με Google, GitHub, Facebook, Twitter και άλλα κοινωνικά δίκτυα -Μεσιτεία ταυτότητας: Έλεγχος ταυτότητας με εξωτερικούς παρόχους OpenID Connect ή SAML Identity Providers -Ομοσπονδία χρηστών: Συγχρονισμός χρηστών από LDAP και Active Directory -Κονσόλα διαχείρισης λογαριασμού: Μέσω της κονσόλας διαχείρισης λογαριασμού, οι χρήστες μπορούν να διαχειρίζονται τους δικούς τους λογαριασμούς.
99.9% διαθεσιμότητα. Για <99.9% η διάρκεια της Συνδρομής θα παρατείνεται κατά μία επιπλέον ημέρα για κάθε μισό τοις εκατό (0,5%) κατά την οποία η Συνδρομήτική Υπηρεσία απέτυχε να επιτύχει αυτό το επίπεδο για αυτόν τον μήνα. Για 2 ή περισσότερους συνεχόμενους μήνες ή για 3 μήνες σε ενα έτος αναλογική επιστροφή των προπληρωμένων αχρησιμοποίητων τελών από την ημερομηνία της καταγγελίας.	---
προληπτική	προληπτική
---	---
ταυτότητες χρηστών	ταυτότητες χρηστών
κατάχρηση διαπιστευτηρίων και εξάλειψη των παραβιάσεων που σχετίζονται με την ταυτότητα.	---

μια άδεια χρήσης υποστηρίζει έως 500 χρήστες	---
τίποτα δωρεάν	δωρεάν προϊόν
Web gui, Rest api	Rest api, Cli, Web gui
SecureAuth	KeyCloak
AWS	AWS
3 πακέτα (2 πακέτα 12/5 και 1 πακετο24/7), επικοινωνία με τηλέφωνο, email, tickets, τεκμηρίωση, πύλη υποστήριξης, κοινότητα, ενημερώσεις προιοντων	επικοινωνία με email, τεκμηρίωση, κοινότητα, gtihub, blog, έγγραφα, forum

IBM Security Verify SaaS	**The OptimalCloud**
SaaS	SaaS
δημόσιο	δημόσιο
IAM	IAM
τιμολόγηση με βάση τον αριθμό χρηστών, ο χρονικό διάστημα σε μήνες που θα είναι ενεργοί οι χρήστες και τα βασικά χαρακτηριστικά με τα υπο-χαρακτηριστικά τους, μηναια χρέωση	3 πακέτα, τιμολόγηση με βάση τον αριθμό χρηστών και τα χαρακτηριστικά, μηνιαία χρέωση, ελάχιστη τιμή ετήσιου συμβολαίου 500$
Βασική λειτουργικότητα: -Single sign-on -Σύνθετος έλεγχος ταυτότητας: Προσθήκη επιπέδου ασφαλείας όπως το MFA ή η μετάβαση χωρίς κωδικό πρόσβασης για ταχύτερη πρόσβαση σε δεδομένα και εφαρμογές. -Αναλυτικά στοιχεία ταυτότητας: Σάρωση για κινδύνους μεταξύ χρηστών, δικαιωμάτων και εφαρμογών. **Επιπλέον λειτουργικότητα:** -Προσαρμοστική πρόσβαση: Συνεχής αξιολόγηση του κινδύνου χρήστη με εφαρμογή μηχανικής μάθησης για μεγαλύτερη ακρίβεια. -Διαχείριση συναίνεσης: Χρήση προτύπων για λεπτομερείς απαιτήσεις που βοηθούν στην αντιμετώπιση των νόμων περί απορρήτου και της αυτοεξυπηρέτησης. -Διαχείριση κύκλου ζωής: Σύνδεση πρόσβασης	**Βασική λειτουργικότητα:** -Single Sign On (SSO) - Έλεγχος ταυτότητας πολλαπλών παραγόντων (MFA) -Περιλαμβάνεται υποστήριξη για ΟΛΑ τα πρότυπα, συμπεριλαμβανομένων των WS-Federation, WS Trust, SAML, Shibboleth, OpenID Connect, OAuth2, SCIM & Rest -Υποστήριξη ελέγχου ταυτότητας KBA, Email, SMS, Voice Authentication, TOTP και PUSH. **Επιπλέον λειτουργικότητα:** -Συγκεκριμένη εξουσιοδότηση διαχείρισης που μπορεί να συνδεθεί με χρήστες ή/και οργανισμούς -Ενσωματώσεις OAuth2, OpenID Connect & SAML με πρόσβαση στην πύλη προγραμματιστών και ολοκληρωμένα έργα εργασίας -Εφαρμογή για φορητές συσκευές που διευκολύνει το MFA χωρίς κωδικό πρόσβασης με αναγνώριση δακτυλικών αποτυπωμάτων ή προσώπου

εφαρμογών με ροές εργασιών επιχειρηματικής διακυβέρνησης.	-Ολοκληρωμένη λύση cloud που περιλαμβάνει επαναφορά κωδικού πρόσβασης αυτοεξυπηρέτησης, αυτοεγγραφή, ανάθεση διαχείρισης, πλήρη διαχείριση ταυτότητας και εγκρίσεις ροής εργασίας με ένα κλικ
99.9% διαθεσιμότητα, για μικρότερη επιστρέφεται το 10% της μηνιαίας συνδρομής	99.99% διαθεσιμότητα με σύστημα ποινών
προληπτική	προληπτική
---	---
ταυτότητες χρηστών	ταυτότητες χρηστών
---	---
Τα στιγμιότυπα πελάτων έχουν μέγιστο όριο συνολικού ποσοστού συναλλαγών (Συμβάντα) 400 ανά δευτερόλεπτο για κάθε στιγμιότυπο παραγωγής. Αυτό το όριο είναι μια συγκέντρωση όλων των σεναρίων που υποστηρίζονται από την πλατφόρμα.	---
90 μέρες δωρεάν	30 μέρες δωρεάν
Web gui, Rest api	Web gui, Rest api
IBM	Optimal IdM
AWS	κανένα
3 πακέτα (τα 2 έχουν 24/7 υποστήριξη) επικοινωνία με τηλέφωνο, emails, tickets, τεκμηρίωση, βάση γνώσης, forum, συχνές ερωτήσεις, κοινότητα, ενημερώσεις,	24/7 υποστήριξη, επικοινωνία με emails, τηλέφωνο, τεκμηρίωση, ιστοσελίδα υποστήριξης

Πίνακας Αποτίμησης 5 – Προϊόντα DLP

ΚΡΙΤΗΡΙΑ/ΠΡΟΙΟΝΤΑ	**Cloud Data Loss Prevention**
α. τρόπος παράδοσης	SaaS
β. μοντέλο διάταξης	δημόσιο
γ. κατηγορία υπηρεσιών στην οποία ανήκει	DLP
δ. μοντέλο κόστους	τιμολόγηση με βάση τον όγκο δεδομένων που επεξεργάζονται
ε. μηχανισμοί ασφάλειας που υλοποιούνται	**Βασική λειτουργικότητα:** -Αυτόματη ανακάλυψη, επιθεώρηση και ταξινόμηση δεδομένων

	-Ευέλικτη ταξινόμηση δεδομένων -Απλή και ισχυρή διασκευή (Κατάργηση ταυτότητας των δεδομένων) -Χωρίς διακομιστή -Ασφαλής χειρισμός δεδομένων **Επιπλέον λειτουργικότητα:** -Αναλυτικά ευρήματα με επιθεώρηση κατά παραγγελία -Εύκολη ενσωμάτωση φόρτου εργασίας -Προσαρμοσμένοι κανόνες
στ. μη λειτουργικές εγγυήσεις	διαθεσιμότητα 99.5%, για 99.5%-99% επιστροφή 10% της μηνιαίας συνδρομής, για 95%-99% επιστροφή 25%, για <95% επιστροφή 50%
ζ. είδος προσφερόμενης προστασίας	ανιχνευτική, προληπτική
η. ιδιότητες ασφάλειας	διαθεσιμότητα
θ. αντικείμενα που προστατεύονται	δεδομένα
ι. απειλές που αντιμετωπίζονται	διαρροή/απώλεια δεδομένων
ια. περιορισμοί	---
ιβ. ύπαρξη δωρεάν εκδόσεων	90 μέρες ή 300$ δωρεάν
ιγ. τρόπος χρήσης προϊόντος	Web gui, Rest api
ιδ. εταιρεία που προσφέρει το προϊόν	Google
ιε. marketplace(s) όπου προσφέρεται το προϊόν	GCP
ιστ. επίπεδο/είδος υποστήριξης για το προϊόν	3 πακέτα (1 8/5 και 2 24/7) επικοινωνία με tickets, email, τηλέφωνο, τεκμηρίωση, κοινότητα, συχνές ερωτήσεις, έγγραφα

Safetica NXT	**Teramind DLP**
SaaS	IaaS
δημόσιο	δημόσιο, ιδιωτικό
DLP	DLP
τιμολόγηση με βάση τον αριθμό χρηστών που προστατεύονται, πληρωμή μηνιαίως	τιμολόγηση με βάση τον αριθμό χρηστών (seat), πληρωμή ετησίως και ελάχιστο 5 χρήστες
Βασική λειτουργικότητα: -Τυποποιημένη ταξινόμηση δεδομένων -Ανίχνευση και απόκριση συμβάντων -Προστασία πνευματικής ιδιοκτησίας και ευαίσθητων δεδομένων	**Βασική λειτουργικότητα:** -Ανίχνευση απάτης από εσωτερικές πληροφορίες -Πρόληψη απειλών από εσωτερικές πληροφορίες -Πρόληψη απώλειας δεδομένων -Παρακολούθηση δραστηριότητας χρήστη

-Εντοπισμός & μετριασμός παραβάσεων συμμόρφωσης -Αναφορές -Εύχρηστη διαχείριση **Επιπλέον λειτουργικότητα:** -Ανίχνευση συμβάντων με γνώμονα τον κίνδυνο	-Διαχείριση Πολιτικών και Κανόνων **Επιπλέον λειτουργικότητα:** -Αναλύσεις συμπεριφοράς χρηστών και οντοτήτων -Βελτιστοποίηση Παραγωγικότητας -Μηχανική Επιχειρηματικών Διαδικασιών -Παρακολούθηση Εργαζομένων -Έλεγχος & Ιατροδικαστική (forensics) -Συμμόρφωση
---	SLA μόνο με επικοινωνία με την εταιρία
ανιχνευτική, προληπτική	ανιχνευτική, προληπτική
διαθεσιμότητα	διαθεσιμότητα
ευαίσθητα δεδομένα	εταιρικά δεδομένα
εσωτερικές απειλές, κακόβουλη δραστηριότητα, διαρροή/απώλεια δεδομένων	διαρροή/απώλεια δεδομένων
οι κανόνες προστασίας είναι διαθέσιμοι μόνο σε Windows	---
10 μέρες δωρεάν	5 μέρες δωρεάν
Web gui	Rest api, Cli
Safetica Technologies	Teramind
Azure	Azure, AWS
3 πακέτα, υποστήριξη 8/5, επικοινωνία με τηλέφωνο, email, tickets, τεκμηρίωση, τεχνικά έγγραφα, βάση γνώσης, τηλεκπαίδευση, κέντρο υποστήριξης	υποστήριξη 24/7, επικοινωνία με email. τηλέφωνο, συχνές ερωτήσεις, βάση γνώσης, εκπαιδευτικο υλικό, τεκμηρίωση

Endpoint Protector	**Active Cypher Cloud Fortress**
SaaS, IaaS	IaaS
δημόσιο	---
DLP, κρυπτογράφηση	DLP, κρυπτογράφηση
πληροφορίες τιμολόγησης μόνο με επικοινωνία με την εταιρία	τιμολόγηση με βάση τον αριθμό χρηστών, χρέωση μηνιαίως
Βασική λειτουργικότητα: -Έλεγχος USB & περιφερειακών θυρών -Σάρωση δεδομένων σε κίνηση -Αυτόματη κρυπτογράφηση USB -Σάρωση δεδομένων σε κατάσταση ηρεμίας -Προστασία Πνευματικής Ιδιοκτησίας -Προσωπικά στοιχεία ταυτοποίησης	**Βασική λειτουργικότητα** -Κρυπτογράφηση από άκρο σε άκρο -Κρυπτογραφική ευέλικτη αρχιτεκτονική -Απλοποίηση και επέκταση της προστασίας **Επιπλέον λειτουργικότητα:**

-Προστασία από εσωτερικές απειλές -Εύκολη ρύθμιση με προκαθορισμένες πολιτικές -Κεντρική διοίκηση **Επιπλέον λειτουργικότητα:** -Συμμόρφωση και Κανονισμοί -Απλοποιημένη διαδικασία ανάπτυξης -Ελαχιστοποίηση ψευδών θετικών στοιχείων και σπατάλης πόρων -Ειδοποίηση και αναφορά σε πραγματικό χρόνο -Αναλυτικά αρχεία καταγραφής -Ενσωμάτωση SIEM	-Ασφάλεια αρχείων Zero-Trust -Συμμόρφωση με GDPR, CCPA, HIPAA
---	---
ανιχνευτική, προληπτική	ανιχνευτική, προληπτική
διαθεσιμότητα, εμπιστευτικότητα	διαθεσιμότητα, εμπιστευτικότητα
δεδομένα, συσκευές usb, πνευματική ιδιοκτησία, προσωπικά στοιχεία ταυτοποίησης	δεδομένα
επιθέσεις από το εσωτερικό ή το εξωτερικό περιβάλλον και απώλεια και κλοπή δεδομένων	κακόβουλο λογισμικό, λυτρισμικό, διαρροή/απώλεια δεδομένων
---	από 10 έως 1 εκατομμύριο χρήστες
30 μέρες δωρεάν	δωρεάν έκδοση χωρίς να αναφέρουν μέρες
Web gui, Cli	Web gui
CoSoSys	Active Cypher
κανένα	Azure
επικοινωνία με τηλέφωνο ,email, tickets, συχνές ερωτήσεις, βάση γνώσης, τεκμηρίωση, ενημερώσεις προϊόντων, εργαλείο testing	επικοινωνία με τηλέφωνο ,email, tickets, συχνές ερωτήσεις

Digital Guardian Data Loss Prevention	**GTB Technologies DLP SaaS**
SaaS	SaaS
δημόσιο	δημόσιο
DLP, κρυπτογράφηση	DLP, κρυπτογράφηση
πληροφορίες τιμολόγησης μόνο με επικοινωνία με την εταιρία	---
Βασική λειτουργικότητα -Ανακάλυψη δεδομένων -Ταξινόμηση Δεδομένων	**Βασική λειτουργικότητα** -Προστασία δεδομένων σε κίνηση -Προηγμένη προστασία τελικού σημείου

-DLP για τελικά σημεία -DLP για δίκτυο -Προστασία δεδομένων Cloud -Αναλύσεις και Αναφορές -Κονσόλα διαχείρισης	-Ανακάλυψη δεδομένων με ταξινόμηση δεδομένων σε πραγματικό χρόνο -Προστασία δεδομένων Cloud -Ορατότητα δεδομένων -Έλεγχος δεδομένων -Προηγμένη προστασία από απειλές **Επιπλέον λειτουργικότητα:** -Έλεγχος εφαρμογών – με Λευκή λίστα εφαρμογών και μαύρη λίστα -Όλα γίνονται στο Endpoint συμπεριλαμβανομένου του εντοπισμού εκτός δικτύου
---	---
ανιχνευτική, προληπτική	ανιχνευτική, προληπτική
διαθεσιμότητα, εμπιστευτικότητα	διαθεσιμότητα, εμπιστευτικότητα
δεδομένα	κρίσιμες πληροφορίες
κακόβουλο λογισμικό, διαρροή/απώλεια δεδομένων	διαρροή/απώλεια δεδομένων
---	---
τίποτα δωρεάν	τίποτα δωρεάν
Web gui, Rest api	Web gui
Helpsystems	GTB Technologies
Azure	κανένα
επικοινωνία με τηλέφωνο ,email, tickets, τεκμηρίωση, εκπαίδευση	4 πακέτα, υποστήριξη 24/7 μέσω τηλεφώνου, επικοινωνία με τηλέφωνο, email, μέσω διαδικτύου, βάση γνώσης, ειδοποιήσεις

Somansa SaaS Endpoint DLP	**Forcepoint DLP**
SaaS	SaaS, IaaS
δημόσιο	δημόσιο
DLP, κρυπτογράφηση	DLP, κρυπτογράφηση
τιμολόγηση με βάση τον αριθμό χρηστών	τιμολόγηση με βάση τον αριθμό χρηστών, 1 χρήστης=1 συσκευή, πληρωμή ανά 12,18,36 μήνες,
Βασική λειτουργικότητα -Πρόληψη απώλειας δεδομένων -Ανακάλυψη δεδομένων **Επιπλέον λειτουργικότητα:** -Συμμόρφωση	**Βασική λειτουργικότητα** -Εντοπισμός, αποκατάσταση και ασφάλεια ευαίσθητων δεδομένων με ανακάλυψη δικτύου, cloud και τελικού σημείου. -Κεντρική διαχείριση πολιτικών σε όλα τα κανάλια, συμπεριλαμβανομένου του cloud, του endpoint, του

	δικτύου, του Web και του email. -Προστασία cloud για την παρακολούθηση και την πρόληψη της απώλειας ευαίσθητων δεδομένων στο διαδίκτυο και την αξιολόγηση του κινδύνου που ενέχουν οι ισότοποι. **Επιπλέον λειτουργικότητα** -Optical Character Recognition (OCR) για αναγνώριση δεδομένων που είναι ενσωματωμένα σε εικόνες. -Προσωπικά αναγνωρίσιμα στοιχεία (PII) για ελέγχους επικύρωσης, ανίχνευση πραγματικού ονόματος και ανάλυση εγγύτητας. -Προσαρμοσμένη αναγνώριση κρυπτογράφησης για την έκθεση κρυφών δεδομένων. -Μηχανική εκμάθηση, η οποία επιτρέπει στους χρήστες να εκπαιδεύουν το σύστημα ώστε να αναγνωρίζει άγνωστα δεδομένα. -Analytics για τον εντοπισμό αλλαγών στη συμπεριφορά των χρηστών.
---	---
ανιχνευτική, προληπτική	ανιχνευτική, προληπτική
διαθεσιμότητα, εμπιστευτικότητα	διαθεσιμότητα, εμπιστευτικότητα
προσωπικά και ευαίσθητα δεδομένα	Προσωπικά αναγνωρίσιμα στοιχεία και προστατευμένες πληροφορίες υγείας, οικονομικά στοιχεία της εταιρείας, εμπορικά μυστικά, δεδομένα πιστωτικών καρτών και άλλα τμήματα ευαίσθητων δεδομένων πελατών
διαρροή/απώλεια δεδομένων	διαρροή/απώλεια δεδομένων
στη "μεγαλύτερη¨ έκδοση έως 300 χρήστες	---
30 μέρες δωρεάν	30 μέρες δωρεάν
Web gui	Web gui, Rest api, Cli
Somansa	Forcepoint
κανένα	κανένα
επικοινωνία με τηλέφωνο, emails, τεκμηρίωση, συχνές ερωτήσεις, βίντεο, έγγραφα, βάση γνώσης	3 πακέτα, υποστήριξη 24/7, επικοινωνία με τηλέφωνο, emails, tickets, forum, βάση γνώσης, τεκμηρίωση, ενημερώσεις, εκπαίδευση

Securetower DLP	**SecurEnvoy DLP**

SaaS, IaaS	IaaS
δημόσιο	---
DLP	DLP
τιμολόγηση με άδεια χρήσης τόσο για μεμονωμένες μονάδες όσο και για συγκεκριμένο αριθμό ελεγχόμενων χρηστών	---
Βασική λειτουργικότητα -Αποκαλύψεις για: διαρροές εμπιστευτικών πληροφοριών, σχέδια απάτης εντός της εταιρείας, εσωτερική δραστηριότητα, αναποτελεσματικοί εργαζόμενοι -Έλεγχος για: ενέργειες στους υπολογιστές των εργαζομένων, αποτελεσματικότητα και πίστη του προσωπικού, επικοινωνίες εργαζομένων, κανάλια δεδομένων -Μπλοκάρισμα σε: κακόβουλες ενέργειες εργαζομένων, πρόσβαση σε πόρους Ιστού, εκκίνηση εφαρμογών , αποθήκευση δεδομένων στο πρόχειρο, σύνδεση συσκευών USB -Ανάλυση σε: περιεχόμενο των μεταφορτωμένων αρχείων (κείμενο, εικόνες, ήχος), αποτελεσματικότητα των εργαζομένων, δραστηριότητα κινδύνου των εργαζομένων, στατιστικούς δείκτες απόδοσης εργαζομένων **Επιπλέον λειτουργικότητα:** -Ερευνά για: περιστατικά ασφάλειας πληροφοριών, αιτίες παραβιάσεων ασφαλείας, λόγους αναποτελεσματικής εργασίας των εργαζομένων, σχέδια απάτης εντός της εταιρείας	**Βασική λειτουργικότητα** -Σάρωση δομημένων & μη δομημένων δεδομένων -Σάρωση αρχείων άγνωστης μορφής -Δακτυλικά αποτυπώματα σε επίπεδο περιεχομένου **Επιπλέον λειτουργικότητα:** -Δυνατότητα οπτικής αναγνώρισης χαρακτήρων -Αυτοματοποιημένη αποκατάσταση δεδομένων -Πλήρες Πλαίσιο Ταξινόμησης
---	99% διαθεσιμότητα, για 95%-99% επιστροφή του κόστους χρήσης για 3 ημέρες, για 90%-95% 5 μέρες, <90% 10 μέρες
ανιχνευτική, προληπτική	ανιχνευτική, προληπτική
διαθεσιμότητα	διαθεσιμότητα
εμπιστευτικές πληροφορίες	δεδομένα
εσωτερικές απειλές, διαρροή/απώλεια δεδομένων	κακόβουλο λογισμικό, εξωτερικές παραβιάσεις, εσωτερικές απειλές και ανθρώπινα λάθη, διαρροή/απώλεια δεδομένων

Τα στοιχεία (components) του SecureTower μπορούν να εγκατασταθούν μόνο στα λειτουργικά συστήματα της οικογένειας Microsoft Windows.	παλιές εκδόσεις προϊόντων δεν υποστηρίζονται
30 μέρες δωρεάν	30 μέρες δωρεάν
Web gui, Rest api, Cli	Rest api, Cli
Falcongaze	SecurEnvoy
κανένα	κανένα
επικοινωνία με τηλέφωνο, emails, τεκμηρίωση, συχνές ερωτήσεις, βάση γνώσης	επικοινωνία με τηλέφωνο, email, έγγραφα, τεκμηρίωσή, blog, ενημερώσεις, πύλη συνεργατων

Zecurion DLP	**MyDLP**
SaaS	IaaS
δημόσιο	---
DLP, κρυπτογράφηση	DLP, κρυπτογράφηση
τιμολόγηση με βάση τον αριθμό χρηστών	τιμολόγηση με βάση τον αριθμό χρηστών, πληρωμή ετησίως
Βασική λειτουργικότητα -Τεχνικές Ανίχνευσης Περιεχομένου -Έλεγχος Συσκευών -Έλεγχος Κυκλοφορίας -Ανακάλυψη Ακατάλληλα Αποθηκευμένων Αρχείων -Ολοκληρωμένος έλεγχος των καναλιών διαρροής δεδομένων -Ευέλικτες πολιτικές και κανόνες -Εξαγωγή περιεχομένων αρχείων -Αρχειοθέτηση αρχείων και μηνυμάτων -Αναφορές **Επιπλέον λειτουργικότητα:** -Ανάλυση συμπεριφοράς χρήστη -Συναισθηματικό προφίλ των χρηστών -Καταγραφή συμβάντων -Ενσωμάτωση Active Directory -Χάρτης συνδέσεων χρήστη	**Βασική λειτουργικότητα** MyDLP Network Protection -Επιβολή πολιτικής DLP σε όλο το οργανωτικό δίκτυο. -Ανάλυση μεγάλων αρχείων σε λίγα δευτερόλεπτα. -Ανακάλυψη δεδομένων από απόσταση/χωρίς πράκτορα. -Δυνατότητα παρακολούθησης / αποκλεισμού email με εξωτερική διεύθυνση BCC MyDLP Endpoint Protection -Έλεγχος αναιρούμενων συσκευών και εκτυπωτών που είναι συνδεδεμένοι σε φορητούς υπολογιστές και σταθμούς εργασίας. -Ανακάλυψη δεδομένων τελικού σημείου. -Κρυπτογράφηση τομέα για αναιρούμενες συσκευές αποθήκευσης. **Επιπλέον λειτουργικότητα:** MyDLP Network Protection -Απρόσκοπτη ενσωμάτωση με οποιαδήποτε λύση φιλτραρίσματος μεσολάβησης ή περιεχομένου που

	υποστηρίζει την ICAP. MyDLP Endpoint Protection -Εύκολη ανάπτυξη με διαθέσιμη υποδομή ανάπτυξης όπως π.χ Microsoft Active Directory ή SCCM -Προστασία εκτός σύνδεσης εκτός του δικτύου του οργανισμού. -Υποστηρίζει όλα τα προγράμματα οδήγησης εκτυπωτή χωρίς εξαίρεση. -Ελάχιστη χρήση πόρων, δεν ενοχλεί τον χρήστη με περιττά μηνύματα και αναδυόμενα παράθυρα.
---	---
ανιχνευτική, προληπτική	ανιχνευτική, προληπτική
διαθεσιμότητα, εμπιστευτικότητα	διαθεσιμότητα, εμπιστευτικότητα
ευαίσθητα και προσωπικά δεδομένα	ευαίσθητες πληροφορίες και ιδιωτικά αρχεία δεδομένων
διαρροή/απώλεια δεδομένων	διαρροή/απώλεια δεδομένων
Αποτρέπεται έως και το 98% των διαρροών δεδομένων, προστατεύονται έως 299.999 υπολογιστές	δεν υποστηρίζονται macOS
τίποτα δωρεάν	30 μέρες δωρεάν
Web gui, Rest api, Cli	Rest api, Cli
Zecurion	Comodo
κανένα	κανένα
υποστήριξη 24/7 επικοινωνία με email, τηλέφωνο	επικοινωνία με τηλέφωνο, email, tickets, forum, βάση γνώσης, έγγραφα, τεκμηρίωση, εκπαιδευτικό υλικό, ιστοσελίδα βοήθειας

Beyond DLP	**Clearswift Adaptive DLP**
SaaS	SaaS
δημόσιο	δημόσιο
DLP	DLP, κρυπτογράφηση
τιμολόγηση με βάση τον αριθμό χρηστών, πληρωμή ετησίως	πληροφορίες τιμολόγησης μόνο με επικοινωνία με την εταιρία
Βασική λειτουργικότητα: -Συλλογή αρχείων καταγραφής πρόσβασης	**Βασική λειτουργικότητα:** -Ευέλικτη ασφάλεια -Μοναδικά προσαρμοστικά χαρακτηριστικά

από όλους τους χώρους αποθήκευσης αρχείων -Εντοπισμός παραβιάσεων δεδομένων και ενημέρωση για το πού και πότε ελήφθησαν δεδομένα, από ποιον και εάν ελήφθησαν άλλα αρχεία -Αποκλεισμός εξωτερικών εισβολέων που στοχεύουν να βλάψουν δεδομένα της εταιρείας (όπως στην περίπτωση του ransomware) σε διαχειριζόμενες και μη διαχειριζόμενες συσκευές -Στόχος να συγκεντρωθούν κρίσιμα δεδομένα στην κεντρική αποθήκευση αρχείων και να μην αφήσουν κρίσιμα δεδομένα στο σύστημα **Επιπλέον λειτουργικότητα:** -Υπολογισμός με μηχανική μάθηση της οπτικοποιησης με χρωματα (heatmap) της πρόσβασης σε δεδομένα με χρώματα -Απόκτηση σκληρών αποδεικτικών στοιχείων εναντίον αδίστακτων εσωτερικών υπαλλήλων που χρησιμοποιούν πράκτορες τεχνητής νοημοσύνης μιας χρήσης -Εκπαίδευση των εργαζομένων να κατεβάζουν μόνο τα απαραίτητα αρχεία -Βοήθεια προς υπαλλήλους ώστε να χρησιμοποιούν κρίσιμα δεδομένα και εφαρμογές με ασφάλεια	-Το Clearswift Endpoint DLP (CED) επεκτείνει το DLP σε τελικά σημεία -ToSECURE Email Gateway (SEG) παρέχει προσαρμοστικές δυνατότητες DLP που επιτρέπουν τη -Σάρωση email SMTP από την έξοδο και την είσοδο στην εταιρεία. -Το SECURE Exchange Gateway (SXG) επιτρέπει τη σάρωση της εσωτερικής αλληλογραφίας **Επιπλέον λειτουργικότητα:** -Ελαχιστοποίηση ψευδώς θετικών -Ο Διακομιστής Διακυβέρνησης Πληροφοριών (IGS) λειτουργεί ως κεντρικό αποθετήριο όπου οι τελικοί χρήστες μπορούν να καταχωρούν ευαίσθητες πληροφορίες -Το SECURE ICAP Gateway (SIG) μπορεί να αυξήσει υπάρχουσες λύσεις φιλτραρίσματος ιστού με ειδικές πολιτικές προσαρμοστικού DLP για πελάτες που διαθέτουν υπάρχουσες λύσεις διακομιστή μεσολάβησης ιστού -Το SECURE Web Gateway (SWG) διαθέτει διακομιστή μεσολάβησης HTTP και μηχανή φιλτραρίσματος περιεχομένου που εκτελεί ταξινόμηση διευθύνσεων URL
Χαμηλή αναλογία ψευδώς θετικών: 2 περιπτώσεις την εβδομάδα κάθε 500 χρήστες με επίπεδο κινδύνου >1	---
ανιχνευτική, προληπτική	ανιχνευτική, προληπτική
διαθεσιμότητα	διαθεσιμότητα, εμπιστευτικότητα
εταιρικά δεδομένα, ευαίσθητα δεδομένα	δεδομένα, κρίσιμες πληροφορίες
λυτρισμικό, διαρροή/απώλεια δεδομένων, εσωτερικές και εξωτερικές απειλές	διαρροή/απώλεια δεδομένων
---	---
δωρεάν δοκιμαστική έκδοση χωρίς να αναφέρονται μέρες	τίποτα δωρεάν
Web gui, Rest api	Web gui
ITsMine	Helpsystems

Σε κανένα	Σε κανένα
επικοινωνία με email, τηλέφωνο	2 πακέτα, υποστήριξη 24/7, επικοινωνία με emails, τηλέφωνο, έγγραφα, συχνές ερωτήσεις, εκπαίδευση, κοινότητα, forum, βάση γνώσης, τεκμηρίωση, πυλη υποστηριξης

Πίνακας αποτίμησης 6 – Προϊόντα Κρυπτογράφησης

ΚΡΙΤΗΡΙΑ/ΠΡΟΙΟΝΤΑ	**Fortanix Data Security Manager**
α. τρόπος παράδοσης	SaaS, IaaS
β. μοντέλο διάταξης	δημόσιο, ιδιωτικό
γ. κατηγορία υπηρεσιών στην οποία ανήκει	κρυπτογράφηση
δ. μοντέλο κόστους	τιμολόγηση με βάση τις διαδικασίες (operations) που πραγματοποιούνται, μηνιαία συνδρομή, ελάχιστο συμβόλαιο 1 έτος
ε. μηχανισμοί ασφάλειας που υλοποιούνται	Βασική λειτουργικότητα -Ενσωματωμένη κρυπτογράφηση, διαχείριση κλειδιών και tokenization -Κατανεμημένη πρόσβαση κλειδιού χαμηλής καθυστέρησης -Ενιαίο κλειδί για όλη την επιχείρηση σε σύννεφο και κέντρα δεδομένων -Κεντρική διεπαφή χρήστη που βασίζεται στον ιστό με στοιχεία ελέγχου πρόσβασης σε επίπεδο επιχείρησης και υποστήριξη απλής σύνδεσης Επιπλέον λειτουργικότητα -Υψηλή διαθεσιμότητα, έξυπνη γεωγραφική εξισορρόπηση φορτίου, αντίσταση σε αστοχία τοποθεσίας -επεκτασιμότητα με APIs και standards -Έλεγχοι πρόσβασης σε επίπεδο επιχείρησης και καταγραφή ελέγχων -Πιστοποίηση FIPS 140-2 level 3 -Αρχεία καταγραφής που δεν τροποποιούνται (tamper proof logging) -Ενσωματώνεται με λύσεις SIEM -Ασφάλεια εταιρικού επιπέδου Intel® SGX
στ. μη λειτουργικές εγγυήσεις	99. 95% διαθεσιμότητα

ζ. είδος προσφερόμενης προστασίας	προληπτική
η. ιδιότητες ασφάλειας	εμπιστευτικότητα
θ. αντικείμενα που προστατεύονται	ευαίσθητα δεδομένα
ι. απειλές που αντιμετωπίζονται	μη εξουσιοδοτημένη πρόσβαση
ια. περιορισμοί	---
ιβ. ύπαρξη δωρεάν εκδόσεων	30 ήμερες δωρεάν
ιγ. τρόπος χρήσης προϊόντος	Web gui, Rest api, Cli
ιδ. εταιρεία που προσφέρει το προϊόν	Fortanix
ιε. marketplace(s) όπου προσφέρεται το προϊόν	GCP, AWS, Azure
ιστ. επίπεδο/είδος υποστήριξης για το προϊόν	υποστήριξη 24/7, επικοινωνία με τηλέφωνο, emails, tickets, βάση γνώσης, συχνές ερωτήσεις, τεκμηρίωση, κοινότητα slack, πύλη διαδικτύου

DSaaS_Masking_Tokenization_Encryption_API	**Crypteron Data Security**
SaaS	SaaS
δημόσιο	δημόσιο
κρυπτογράφηση, IAM, DLP	κρυπτογράφηση
---	τιμολόγηση με βάση τα πλάνα/επιλογές του χρήστη (πληροφορίες με επικοινωνία με την εταιρία), πληρωμή μηνιαίως ή ετησίως
Βασική λειτουργικότητα -Υποστήριξη για κάθε τύπο πληροφορίας, από οποιοδήποτε σύστημα ή εφαρμογή και μπορεί να χρησιμοποιηθεί από οποιαδήποτε συσκευή -Μηχανή ανάλυσης για εξόρυξη πεδίου και μετασχηματισμούς -Ενσωματωμένο σύστημα διαχείρισης κλειδιών κρυπτογράφησης (KMS), υποστήριξη για εξωτερικούς διαχειριστές κλειδιών και θησαυροφυλάκια (vaults) -Κρυπτογράφηση & Tokenization - Διατήρηση μορφής, λειτουργίας και μήκους -stateless και vaultless tokenization -Μαζική μετατροπή αρχείων για υπάρχοντα δεδομένα και ειδικές ανάγκες -Επιλογή διακομιστή μεσολάβησης Web app για ενεργοποίηση διαφανούς κρυπτογράφησης	Βασική λειτουργικότητα -Προστασία κρυπτογράφησης και παραποίησης για όλους τους τύπους δεδομένων -Ασφάλεια δομημένων δεδομένων με αντικειμενοστραφή κρυπτογράφηση -Αυτόματη κρυπτογράφηση και αποκρυπτογράφηση με το CipherDB κατά τη χρήση τυπικών API πρόσβασης δεδομένων -Αυτόματη και πλήρως ενσωματωμένη διαχείριση κλειδιών -Περιστρεφόμενα κλειδιά κρυπτογράφησης και μετεγκατάσταση δεδομένων με ένα μόνο κλικ -Πίνακας ελέγχου Επιπλέον λειτουργικότητα -Ασφάλιση γενικών αντικειμένων, συμπεριλαμβανομένου του NoSQL με το CipherObject

χωρίς αλλαγή των εφαρμογών Επιπλέον λειτουργικότητα -Ασφάλεια περιεχομένου -Σάρωση κακόβουλου λογισμικού -Σάρωση DLP -Διαχείριση Πληροφοριακών Δικαιωμάτων (IRM) -Συμμόρφωση -Adaptive Access Control -Ενοποιημένος έλεγχος πολιτικής σε όλες τις εφαρμογές	-Ασφάλεια αρχείων και ροών αρχείων με το CipherStor -Απόκριση σε παραβίαση δεδομένων με ένα μόνο κλικ
---	το ενδιάμεσο λογισμικό (middleware) cipherDB έχει καθυστέρηση < 1ms ανά εγγραφή, 99.95% διαθεσιμότητα, αν η % μηνιαία διαθεσιμότητά της είναι μικρότερη από 99,95%, αυτό το ποσοστό θα χρησιμοποιηθεί για τη χρέωση για τον συγκεκριμένο μήνα.
προληπτική, ανιχνευτική	προληπτική
εμπιστευτικότητα, διαθεσιμότητα	εμπιστευτικότητα
δεδομένα	δεδομένα, αρχεία, ροές αρχείων, γενικά αντικείμενα
μη εξουσιοδοτημένη πρόσβαση, κλοπή διαπιστευτηρίων, πειρατεία λογαριασμών, μη ασφαλή API, κακόβουλοι εσωτερικοί χρήστες ή αναγκαστική αποκάλυψη δεδομένων σε χρήση	μη εξουσιοδοτημένη πρόσβαση, παραβιάσεις δεδομένων
---	---
δωρεάν δοκιμαστική έκδοση χωρίς να αναφέρονται ήμερες	μόνιμη δωρεάν έκδοση με περιορισμένες δυνατότητες και 30 ήμερες δωρεάν για πλήρη έκδοση (enterprise έκδοση)
Web gui, Rest api	Web gui, Rest api
Ciphercloud (συγχώνευση με Lookout)	Crypteron
Azure	Azure
επικοινωνία με τηλέφωνο, emails	επικοινωνία με τηλέφωνο, emails, tickets, τεκμηρίωση, βίντεο, συχνές ερωτήσεις, βάση γνώσης, κοινότητα
Entrust DataControl	**Baffle Data Protection Services**
IaaS	IaaS
δημόσιο, ιδιωτικό	δημόσιο
κρυπτογράφηση, IAM	κρυπτογράφηση, IAM

τιμολόγηση με άδεια χρήσης BYOL	τιμολόγηση με άδεια χρήσης BYOL
Βασική λειτουργικότητα Ισχυρή κρυπτογράφηση Απλοποιημένη διαχείριση κλειδιών Online κρυπτογράφηση και δυναμική επανα-φορά κλειδιού Διαχείριση κρυπτογραφημένων φόρτων εργα-σίας σε μια υποδομή πολλαπλών νέφους Βαθιά προστασία του φόρτου εργασίας Επιπλέον λειτουργικότητα Λογισμικό πολλαπλών ενοικιαστών (multitenant) Επιτάχυνση υλικού σε intel και amd chIPSets Έλεγχος πρόσβασης Αποφυγή διπλότυπων (deduplication support) Φορητό και διαφανές λογισμικό	Βασική λειτουργικότητα -Δυναμική και στατική κάλυψη δεδομένων -Κρυπτογράφηση βάσεων δεδομένων -Tokenization δεδομένων -Κρυπτογράφηση σε επίπεδο πεδίου και εγγραφής -Κρυπτογράφηση αρχείου και αντικειμένου Επιπλέον λειτουργικότητα -Εφαρμογή τεχνολογιών προστασίας δεδομένων (privacy-enhanced computation) και εξαγωγή ανα-λυτικών στοιχείων -Έλεγχος πρόσβασης βάσει ρόλου -Συμμόρφωση -Ασφαλής κοινή χρήση δεδομένων -Αφαίρεση προσωπικών πληροφοριών από δεδο-μένα σε κίνηση
---	---
προληπτική	προληπτική
εμπιστευτικότητα	εμπιστευτικότητα
φόρτο εργασίας (workload)	δεδομένα
μη εξουσιοδοτημένη πρόσβαση	μη εξουσιοδοτημένη πρόσβαση
---	---
τίποτα δωρεάν	τίποτα δωρεάν
Rest api, Cli, Web gui	Rest api
Entrust (Hytrust)	Baffle IO
Azure, AWS	Azure, AWS
επικοινωνία με τηλέφωνο, emails, βάση γνώ-σης, βίντεο, τεκμηρίωση, ενημερώσεις, έγ-γραφα, κέντρο βοηθείας	επικοινωνία με emails

Encrypted ecosystem for truly private data (usecrypt safe)	**D' Amo**
SaaS	IaaS
δημόσιο	---
κρυπτογράφηση	κρυπτογράφηση
2 εκδόσεις για τη μια (pro) τιμολόγηση με βάση τον αριθμό χρηστών, πληρωμή μηνιαίως ή	τιμολόγηση με βάση το φόρτο εργασίας και τα βα-σικά χαρακτηριστικά

εφάπαξ, για την άλλη (custom) πληροφορίες σε επικοινωνία με την εταιρία	
Βασική λειτουργικότητα Διαχείριση υβριδικών εικονικών κλειδιών Κρυπτογράφηση από άκρο σε άκρο Usecrypt's Secure Tunnel (σήραγγα επικοινωνίας βασισμένη σε συμμετρική και ασύμμετρη κρυπτογραφία) Ασφαλείς συνδέσεις (diffie helman) Ισχυρή κρυπτογράφηση (aes 256) Βασίζεται σε επαληθευμένες μεθόδους (rsa, kem) Κλειδιά που δημιουργούνται με ασφάλεια Ανθεκτικό σε hackers	Βασική λειτουργικότητα D'Amo KMS για Cloud (σύστημα διαχείρισης κλειδιών) -Εργαλείο διαχείρισης GUI - Κέντρο ελέγχου D'Amo - KMS SA: πραγματοποιεί κρυπτογράφηση στο περιβάλλον cloud, προϊόντα εικονικού τύπου για ασφαλή διαχείριση και προστασία κλειδιών -Ασφαλές σύστημα διαχείρισης κλειδιών σύμφωνα με εθνικά και διεθνή πρότυπα κρυπτογράφησης -Σύστημα διαχείρισης κλειδιών που αποκτά πιστοποίηση CC με χαρακτηριστικά ασφαλείας και επικυρωμένη ευπάθεια - Δυνατότητες διαχείρισης σε διάφορα εξωτερικά κλειδιά κρυπτογράφησης - Δυνατότητες διαχείρισης στο κλειδί TDE της Oracle Database ή του SQL Server - Λειτουργίες διαχείρισης σε ασύμμετρα κλειδιά που χρησιμοποιούνται στο πιστοποιητικό ή στην κρυπτογράφηση της ενότητας Κρυπτογράφηση D'Amo - Κρυπτογράφηση και αποκρυπτογράφηση - Υποστηρίζει όλα τα περιβάλλοντα DBMS - BA (Business Application) : Κρυπτογράφηση τύπου API που αποφεύγει να επηρεάσει το DBMS πραγματοποιώντας κρυπτογράφηση στην εφαρμογή. - DA (Εφαρμογή DBMS): Κρυπτογράφηση που παρέχει ασφάλεια DB με κρυπτογράφηση, έλεγχο πρόσβασης, έλεγχο και διαχωρισμό εξουσιών μέσω API κρυπτογράφησης και αποκρυπτογράφησης - DP (DBMS Package): Εγκατεστημένο στον διακομιστή DB με τη μορφή πακέτου για προαιρετική κρυπτογράφηση ανά στήλη - DE (DBMS Engine): Συστήματα ασφαλείας οργάνωσης κρυπτογράφησης από εγκαταστάσεις D'Amo στον διακομιστή DB χωρίς περιβαλλοντικές

	τροποποιήσεις. - KE (Kernel): Κρυπτογράφηση βασισμένη σε φακέλους και αρχεία χωρίς τροποποιήσεις πηγής σε επίπεδο πυρήνα Επιπλέον λειτουργικότητα D'Amo KMS για Cloud (σύστημα διαχείρισης κλειδιών) -Διάφορα μέτρα δημιουργίας αντιγράφων ασφαλείας για κλειδιά και αυτόματο συγχρονισμό πολιτικών -Προβολή αρχείων καταγραφής, έλεγχος ακεραιότητας αρχείων καταγραφής και δυνατότητες εναλλαγής αρχείων καταγραφής -Ειδοποίηση για κινδύνους και αστοχίες μέσω αυτοελέγχων και συστήματος αυτόματης αποκατάστασης διαταραχών Κρυπτογράφηση D'Amo -Τμηματοποιημένος έλεγχος πρόσβασης: Παραχωρεί εξουσιοδότηση ανά στήλη/χρήστη και διαχωρίζει την αρχή του διαχειριστή ασφαλείας και του DBA
99.9% διαθεσιμότητα	---
προληπτική	προληπτική
εμπιστευτικότητα	εμπιστευτικότητα
δεδομένα	βάσεις δεδομένων
μη εξουσιοδοτημένη πρόσβαση, απειλές που δημιουργούνται από χακερς	μη εξουσιοδοτημένη πρόσβαση, κακόβουλο κωδικά, απώλεια δεδομένων
στην "pro" έκδοση 1-25 άδειες χρήσης (χρήστες), και στις δυο εκδόσεις σε κάθε χρήστη αντιστοιχούν εως100gb αποθ. χώρου	---
30 ήμερες δωρεάν	τίποτα δωρεάν
Web gui	Web gui
UseCrypt Polska	Penta Security Systems
Azure	Azure
υποστήριξη 24/7, επικοινωνία με τηλέφωνο, email, συχνές ερωτήσεις	επικοινωνία με email, τηλέφωνο

StrongSalt API	**File Vault API**

SaaS	SaaS
δημόσιο	δημόσιο
κρυπτογράφηση	κρυπτογράφηση
τιμολόγηση με βάση τον όγκο δεδομένων και τα βασικά χαρακτηριστικά, 4 πακέτα για όγκο, 3 πακέτα για χαρακτηριστικά	3 πακέτα, τιμολόγηση με βάση τον όγκο δεδομένων, πληρωμή ανά μήνα
Βασική λειτουργικότητα Κρυπτογράφηση δεδομένων με δυνατότητα αναζήτησης Κρυπτογράφηση δεδομένων με δυνατότητα κοινής χρήσης και αναζήτησης Αποκεντρωμένη κρυπτογράφηση δεδομένων με δυνατότητα αναζήτησης Επιπλέον λειτουργικότητα Αποκεντρωμένο κατάστημα αντικειμένων Strongvault - κρυπτογραφημένη εφαρμογή κοινής χρήσης αρχείων και ομαδικών μηνυμάτων Υποστήριξη μεταξύ πλατφορμών	Βασική λειτουργικότητα -Προστασία των ευαίσθητων αρχείων της εφαρμογής χρησιμοποιώντας κρυπτογράφηση AES-256 στην κρυπτογράφηση από την πλευρά του πελάτη και πρόσθετα επίπεδα κρυπτογράφησης από την πλευρά του διακομιστή -Tokenization των ευαίσθητων αρχείων της εφαρμογής Επιπλέον λειτουργικότητα -Κοινή χρήση αρχείων με άλλους με ισχυρούς ελέγχους ασφαλείας -Συμβατό με το PCI Level 1
---	---
προληπτική	προληπτική
εμπιστευτικότητα	εμπιστευτικότητα
δεδομένα	ευαίσθητα αρχεία εφαρμογών
μη εξουσιοδοτημένη πρόσβαση	μη εξουσιοδοτημένη πρόσβαση
---	μέγιστος αποθηκευτικός χώρος ανά μηνά 1TB, μέγιστο μέγεθος ενός αρχείου προς κρυπτογράφηση και αποθήκευση 5GB
τίποτα δωρεάν	δωρεάν μόνιμη έκδοση με 5gb/μηνα αποθηκευτικό χώρο
Web gui, Rest api	Web gui, Rest api
StrongSalt	Enigma security solutions
AWS	AWS
επικοινωνία με emails, τηλέφωνο, τεκμηρίωση	επικοινωνία με τηλέφωνο, email, chat, τεκμηρίωση

Data Vault API	**Bloombase StoreSafe**
SaaS	IaaS
δημόσιο	δημόσιο
κρυπτογράφηση	κρυπτογράφηση

3 πακέτα, τιμολόγηση με βάση τη χρήση (requests), πληρωμή ανά μήνα	τιμολόγηση με άδεια χρήσης BYOL
Βασική λειτουργικότητα -Διασφάλιση ευαίσθητων δεδομένων χρησιμοποιώντας κρυπτογράφηση AES-256 σε επίπεδο πεδίου και άλλα επίπεδα κρυπτογράφησης χρησιμοποιούνται σε επίπεδο πίνακα -Tokenization ευαίσθητων δεδομένων Επιπλέον λειτουργικότητα -Αναζήτηση ευαίσθητων δεδομένων -Συμβατό με το PCI Level 1	Βασική λειτουργικότητα -Διαφανής κρυπτογράφηση και αποκρυπτογράφηση. -Απρόσκοπτη ενσωμάτωση με τη συσκευή υλικού Bloombase KeyCastle όπου τα κλειδιά κρυπτογράφησης αποθηκεύονται και διαχειρίζονται ξεχωριστά -Οι ρυθμίσεις παραμέτρων του Bloombase StoreSafe παρέχονται εύκολα από την κονσόλα διαχείρισης που βασίζεται στον ιστό. Επιπλέον λειτουργικότητα -Αβίαστη και ακίνδυνη ανάπτυξη και εφαρμογή. -Εύκαμπτος και ασφαλής έλεγχος πρόσβασης. -Υποστήριξη πολλών χρηστών και κοινή χρήση πόρων -Ανεξαρτησία από το υλικό, το λειτουργικό σύστημα, το σύστημα αρχείων και τους χρήστες -Υψηλή διαθεσιμότητα και ομαδοποίηση -Εικονικοποίηση, προστασία μεγάλων δεδομένων και cloud -Ψηφιακή προστασία πνευματικής ιδιοκτησίας -Κρυπτογράφηση αποθετηρίου email -Ασφαλής αναπαραγωγή, ανάκτηση καταστροφών, δημιουργία αντιγράφων ασφαλείας δεδομένων και αρχειοθέτηση
---	---
προληπτική	προληπτική
εμπιστευτικότητα	εμπιστευτικότητα
ευαίσθητα δεδομένα	εταιρικά δεδομένα
μη εξουσιοδοτημένη πρόσβαση	μη εξουσιοδοτημένη πρόσβαση
μέγιστος αριθμός requests/μήνα 400 χιλιάδες	---
δωρεάν μόνιμη έκδοση με 1500 requests/μηνα	τίποτα δωρεάν
Web gui, Rest api	Rest api, Cli, Web gui
Enigma security solutions	Bloombase
AWS	AWS, Azure
επικοινωνία με τηλέφωνο, emails, chat, τεκμηρίωση	2 πακέτα (10/5 και 24/7) επικοινωνία με, emails, πύλη υποστήριξης, βάση γνώσης, κοινότητα, έγγραφα. ενημερώσεις, συχνές ερωτήσεις

Sophos Central Device Encryption	Nordlocker
SaaS	SaaS
δημόσιο	δημόσιο
κρυπτογράφηση	κρυπτογράφηση, BCDR
τιμολόγηση με βάση τον αριθμό χρηστών, ετήσιο ή τριετές συμβόλαιο με αντίστοιχη έκπτωση	2 πακέτα, τιμολόγηση με βάση τον ογκο δεδομένων, μηνιαία χρέωση
Βασική λειτουργικότητα Κρυπτογράφηση ολόκληρου σκληρού δίσκου (bitlocker για windows, filevault για macos) Διαχείριση κρυπτογράφησης παράλληλα με τελικό σημείο, διακομιστή, κινητό, τείχος προστασίας, email και άλλα προϊόντα προστασίας της Sophos Επιπλέον λειτουργικότητα Διασφάλιση κοινής χρήσης εγγράφων Ανάκτηση PIN/κωδικού αυτοεξυπηρέτησης Προτροπή στους χρήστες για τακτικές αλλαγές PIN/κωδικού πρόσβασης Αναφορές συμμόρφωσης	Βασική λειτουργικότητα Κρυπτογραφία δεδομένων που είναι αποθηκευμένα και τοπικά και στο νέφος Κρυπτογράφηση τελευταίας τεχνολογίας Ασφάλεια και συγχρονισμός αρχείων μέσω κρυπτογραφημένου νέφους από άκρο σε άκρο. Επιπλέον λειτουργικότητα Υποστηρίζονται πολλαπλές πλατφόρμες Προστασία αρχείων μέσω του περιηγητή Δημιουργία αντιγράφων ασφαλείας δεδομένων αυτόματα Έλεγχος ταυτότητας πολλαπλών παραγόντων για λογαριασμούς Προστασία από ransomware Σύννεφο αρχιτεκτονικής μηδενικής γνώσης
---	---
προληπτική	προληπτική
εμπιστευτικότητα	εμπιστευτικότητα, διαθεσιμότητα
σκληροί δίσκοι	δεδομένα
μη εξουσιοδοτημένη πρόσβαση	μη εξουσιοδοτημένη πρόσβαση σε αρχεία, λυτρισμικό
---	μέγιστος αποθηκευτικός χώρος 2TB
30 ήμερες δωρεάν	δωρεάν μόνιμη έκδοση με 3gb αποθηκευτικό χώρο
Web gui, Cli	Web gui
Sophos	Tefincom
κανένα	κανένα
επικοινωνία με τηλέφωνο, email, tickets, chat, κοινότητα, τεκμηρίωση, βάση γνώσης, βίντεο, λογαριασμός twitter, έγγραφα, εκπαιδευτικό υλικό	υποστήριξη 24/7 επικοινωνία με emails, συχνές ερωτήσεις, έγγραφα, κέντρο βοηθείας

Datalocker Safecrypt (safeconsole)	**Fabasoft Secomo**
SaaS	SaaS
δημόσιο	δημόσιο
κρυπτογράφηση	κρυπτογράφηση
τιμολόγηση με βάση τον αριθμό εικονικών δίσκων, 1 δίσκος αντιστοιχεί σε 1 άδεια safecrypt + ενα χρηματικό ποσό μια φορά για τη δημιουργία λογαριασμού safeconsole, πληρωμή ανά έτος ή τριετίας	---
Βασική λειτουργικότητα Κρυπτογραφία δεδομένων με AES-256 Κρυπτογραφημένα ονόματα αρχείων, λειτουργία μόνο για ανάγνωση Επιπλέον λειτουργικότητα Περιορισμοί τύπου αρχείου, Προαιρετικός έλεγχος ταυτότητας δύο παραγόντων Άμυνα επίθεσης ωμής δύναμης Σχεδιασμός λογισμικού μηδενικής γνώσης. Συμβατότητα με τοπικά αρχεία, μονάδες δικτύου, εξωτερικά μέσα όπως USB flash και σκληρούς δίσκους και όλους τους μεγάλους παρόχους αποθήκευσης cloud	Βασική λειτουργικότητα Κρυπτογράφηση και υπογραφή πολύτιμων εταιρικών εγγράφων Γνήσια κρυπτογράφηση από άκρο σε άκρο Βιβλιοθήκες κρυπτογραφίας από την IAIK-SIC Επιπλέον λειτουργικότητα Εξαιρετικά επαγγελματική διαχείριση και ολοκληρωμένη παρακολούθηση Μόνο ο πελάτης έχει πρόσβαση στα δεδομένα του Αρχιτεκτονική υψηλής διαθεσιμότητας (cluster δύο διακομιστών) Τεκμηρίωση γνησιότητας μέσω ψηφιακών υπογραφών
99.5% διαθεσιμότητα (safeconsole)	99.9% διαθεσιμότητα
προληπτική	προληπτική
εμπιστευτικότητα, διαθεσιμότητα	εμπιστευτικότητα
δεδομένα	ευαίσθητα και πολύτιμα δεδομένα
μη εξουσιοδοτημένη πρόσβαση, επιθέσεις ωμής βίας	μη εξουσιοδοτημένη πρόσβαση
---	---
30 ήμερες δωρεάν	τίποτα δωρεάν
Cli, Web gui (safeconsole), Rest api (safeconsole)	Web gui
Datalocker	Fabasoft
κανένα	κανένα
επικοινωνία με τηλέφωνο, emails, tickets, βάση γνώσης, συχνές ερωτήσεις, έγγραφα	2 πακέτα 10/5 και 24/7, επικοινωνία με τηλέφωνο, email, tickets, ιστοσελίδα βοηθείας, τεκμηρίωση, έγγραφα

Πίνακας αποτίμησης 7 – Προϊόντα Ασφάλειας Ηλεκτρονικού Ταχυδρομείου

ΚΡΙΤΗΡΙΑ/ΠΡΟΙΟΝΤΑ	**Armorblox Email Protection**
α. τρόπος παράδοσης	SaaS
β. μοντέλο διάταξης	δημόσιο
γ. κατηγορία υπηρεσιών στην οποία ανήκει	ασφάλεια ηλεκτρονικού ταχυδρομείου, DLP
δ. μοντέλο κόστους	τιμολόγηση με βάση τον αριθμό χρηστών, ετήσια συνδρομή
ε. μηχανισμοί ασφάλειας που υλοποιούνται	**Βασική λειτουργικότητα** -Διακοπή στοχευμένων επιθέσεων ηλεκτρονικού ταχυδρομείου -Μείωση του χρόνου έρευνας και απόκρισης αξιοποιώντας εμπλουτισμένους δείκτες απειλών email και μαζική απάντηση με ένα κλικ. -Μείωση των χρόνων απόκρισης με αυτοματοποιημένες και διαμορφώσιμες ενέργειες αποκατάστασης για κάθε κατηγορία απειλών. **Εξτρά λειτουργικότητα** -Μελέτη λεπτομερών δεικτών συμβιβασμού (IOC) που αφορούν συγκεκριμένα email που αντλούν πληροφορίες από τα σήματα ταυτότητας, συμπεριφοράς και γλώσσας. -Μελλοντική προστασία με δυναμικές πολιτικές που μαθαίνουν από μη αυτόματες ενέργειες για προστασία από παρόμοιες μελλοντικές απειλές. -Εντοπισμός απώλειας ευαίσθητων δεδομένων (PII/PCI) σε εφαρμογές email, ανταλλαγής μηνυμάτων (π.χ. Slack) και κοινής χρήσης αρχείων (π.χ. Box) -Κατάργηση των μη αυτόματων εργασιών πολιτικής με προκαθορισμένες κατηγορίες απειλών στις οποίες ταξινομούνται αυτόματα τα ύποπτα email -Σύνδεση του Armorblox με εταιρικό γραμματοκιβώτιο phishing/κατάχρησης για αυτοματοποιημένο εντοπισμό και αποκατάσταση των αναφερόμενων email.

στ. μη λειτουργικες εγγυησεις	99.9% διαθεσιμότητα, για 99.8% - 97% επιστροφή 5% της μηνιαίας συνδρομής, για 96.9% - 93.0% επιστροφή 10%, για 92.9% - 90.0% επιστροφή 20%, για <90% επιστροφή 30%
ζ. ειδος προσφερομενης προστασίας	προληπτική, ανιχνευτική, αντιδραστική
η. ιδιότητες ασφάλειας	διαθεσιμότητα
θ. αντικείμενα που προστατεύονται	ηλεκτρονικό ταχυδρομείο
ι. απειλές που αντιμετωπίζονται	Συμβιβασμός (compromise) προσωπικού και επαγγελματικού email ηλεκτρονικού ψάρεμα, στοχευμένο ηλεκτρονικό ψάρεμα (spearphising), ψάρεμα διαπιστευτηρίων και ανωτέρου προσωπικού (executives) Απάτες πωλητή (vendor) και μισθοδοσίας Εκβιασμοί
ια. περιορισμοί	---
ιβ. ύπαρξη δωρεαν εκδόσεων	90 ημέρες δωρεάν για έως 2000 υπάλληλους
ιγ. τρόπος χρήσης προϊόντος	Web gui, Rest api
ιδ. εταιρεία που προσφέρει το προϊόν	Armorblox
ιε. marketplace(s) όπου προσφέρεται το προϊόν	GCP, Azure
ιστ. επίπεδο/είδος υποστήριξης για το προϊόν	επικοινωνία μέσω emails, βάση γνώσης

Heimdal Email Security	**GreatHorn Cloud Email Security**
SaaS	SaaS
δημόσιο	δημόσιο
ασφάλεια ηλεκτρονικού ταχυδρομείου	ασφάλεια ηλεκτρονικού ταχυδρομείου
---	3 πακέτα, πληροφορίες τιμολόγησης με επικοινωνία με την εταιρία
Βασική λειτουργικότητα -Ασφάλεια email και συμμόρφωση συνδυάζοντας την ευφυΐα απειλών με την ανθρώπινη τεχνογνωσία -Πλήρης προστασία email -Προσέγγιση βαθιάς σάρωσης για διακομιστές email και λογαριασμούς Ολοκληρωμένη ασφάλεια email -Πολλαπλά επίπεδα προστασίας, κάθε email σαρώνεται για πλαστοπροσωπία, κινδύνους διαρροής δεδομένων και πολλά άλλα.	**Βασική λειτουργικότητα** -Δυνατότητα λεπτομερούς αναζήτησης σε ολόκληρο τον φάκελο email -Άμεση αναγνώριση και καραντίνα μεμονωμένων ή μαζικών email σε ολόκληρο το περιβάλλον email. -Ειδοποιήσεις και αναφορές phishing σε πραγματικό χρόνο -Αποκλεισμός κακόβουλων διευθύνσεων URL -Προειδοποιητικές σελίδες για ύποπτους συνδέσμους -Ανίχνευση πλαστογράφησης με χρήση AI, ML και

-Ασφαλείς εκτελέσεις, ο σαρωτής βαθιάς προσάρτησης διασφαλίζει ότι δεν υπάρχει κακόβουλος κώδικας εντός του σταθμού εργασίας **Εξτρά λειτουργικότητα** -Καταγραφή και αναφορές	data Science **Εξτρά λειτουργικότητα** -Analytics -Εφαρμογή αυτοματοποιημένων και προσαρμοσμένων έξυπνων banner, βάσει κινδύνου -Αξιολόγηση σχέσεων, μοτίβων επικοινωνίας και τεχνικών δακτυλικών αποτυπωμάτων -Πρόσβαση σε αναδυόμενες κακόβουλες επιθέσεις, συμπεριλαμβανομένων των zero-days, με ενημερώσεις πολιτικής και προτεινόμενες ενέργειες
---	100% παραμονή δεδομένων στο περιβάλλον του χρήστη. Εξάλειψη του 100% των εξαγορών λογαριασμού Μείωση της αλληλεπίδρασης των χρηστών με ύποπτα email κατά 60%.
προληπτική, ανιχνευτική, αντιδραστικη	προληπτική, ανιχνευτική, αντιδραστική
---	---
ηλεκτρονικό ταχυδρομείο	ηλεκτρονικό ταχυδρομείο
Ηλεκτρονικό ψάρεμα Εκμεταλλεύσεις email & επιθέσεις botnet Ανεπιθύμητο περιεχόμενο Λυτρισμικό Κακόβουλοι σύνδεσμοι και συνημμένα Email που προέρχονται από μολυσμένες IP ή/και τομείς Σύνθετη ανεπιθύμητη αλληλογραφία	Κακόβουλες και ύποπτες διευθύνσεις URL Συμβιβασμός ηλεκτρονικού ταχυδρομείου για επιχειρήσεις Εξαγορές λογαριασμού Πλαστοπροσωπίες Κακόβουλα ωφέλιμα φορτία Κλοπή διαπιστευτηρίων
---	---
30 ημέρες δωρεάν	30 ημέρες δωρεάν για πανω απο 250 χρηστες
Web gui, Cli	Web gui, Rest api
Heimdal Security	Greathorn
Azure	Azure
υποστήριξη 24/7, επικοινωνία με τηλέφωνο , email, tickets, βάση γνώσης, συχνές ερωτήσεις, τεκμηρίωση	επικοινωνία με τηλέφωνο , email, chat, βάση γνώσης πληροφορίες υποστήριξης μόνο με εγγραφή

Libraesva Email Security Gateway	**Clearswift Secure Email Gateway**
IaaS	IaaS
δημόσιο, ιδιωτικό	δημόσιο, ιδιωτικό

ασφάλεια ηλεκτρονικού ταχυδρομείου, κρυπτογράφηση, BCDR	ασφάλεια ηλεκτρονικού ταχυδρομείου,DLP, κρυπτογράφηση
τιμολόγηση με βάση τον αριθμό χρηστών και ελάχιστο 10 χρήστες, ετήσιο συμβόλαιο	BYOL, πληροφορίες μόνο με επικοινωνία με την εταιρία
Βασική λειτουργικότητα Προστασία από πλαστογράφηση Προστασία από κακόβουλα αρχεία Προστασία από κακόβουλες διευθύνσεις URL Προστασία επιθέσεων από παραβιάσεις και πλαστοπροσωπία επαγγελματικών μηνυμάτων ηλεκτρονικού ταχυδρομείου Γρήγορη απόκριση σε απειλές ασφαλείας Αποκατάσταση απειλών **Εξτρά λειτουργικότητα** Πύλη ανάλυσης απειλών Κρυπτογράφηση email Συνέχεια email Εφαρμογή κινητού	**Βασική λειτουργικότητα** Ισχυρή ασφάλεια email με προστασία σε πραγματικό χρόνο Απαράμιλλη επιθεώρηση περιεχομένου σε βάθος Διόρθωση δεδομένων Προστασία εισερχόμενων απειλών Πολυεπίπεδη προστασία από ανεπιθύμητα μηνύματα **Εξτρά λειτουργικότητα** Ευέλικτος και αναλυτικός έλεγχος πολίτικων Εξυγίανση εγγράφων και εικόνας Μήνυμα και δομική εξυγίανση Κρυπτογράφηση Sandboxing για emails Προστασία από την απώλεια δεδομένων εξερχόμενων (outbound) Κανονιστική Συμμόρφωση
Αποκλεισμός πάνω από το 99,9% των επιθέσεων ηλεκτρονικού ψαρέματος και malspam	99,9% ανίχνευση ανεπιθύμητων μηνυμάτων
προληπτική, ανιχνευτική, αντιδραστικη	προληπτική, ανιχνευτική, αντιδραστική
εμπιστευτικότητα, διαθεσιμότητα	εμπιστευτικότητα, διαθεσιμότητα
ηλεκτρονικό ταχυδρομείο	ηλεκτρονικό ταχυδρομείο
Πλαστοπροσωπία (spoofing) Κακόβουλα αρχεία και URL Συμβιβασμός email για επιχειρήσεις Ηλεκτρονικό ψάρεμα Απάτη μέσω email Ανεπιθύμητη αλληλογραφία Ιοί Κακόβουλο λογισμικό	κακόβουλο λογισμικό, ανεπιθύμητη αλληλογραφία, ιοί, προηγμένες μόνιμες απειλές (advanced persistent threats)
ποσοστό ανίχνευσης ανεπιθύμητης αλληλογραφίας έως 99,99%	---
30 ημέρες δωρεάν	τίποτα δωρεάν
Web gui, Rest api	Web gui, Cli
Libraesva	Helpsystems
Azure	AWS

2 πακέτα, 10/5 και 24/7, επικοινωνία με τηλέφωνο , email, tickets, κέντρο υποστήριξης, τεκμηρίωση, βάση γνώσης, έγγραφα	2 πακέτα 24/7, επικοινωνία με emails, τηλέφωνο , έγγραφα, συχνές ερωτήσεις, εκπαίδευση, κοινότητα, forum, βάση γνώσης, τεκμηρίωση, πύλη υποστήριξης

Barracuda Email Security Gateway	**Glasswall Rebuild for Email (Glasswall Email Security)**
IaaS	SaaS
δημόσιο	δημόσιο
ασφάλεια ηλεκτρονικού ταχυδρομείου, κρυπτογράφηση	ασφάλεια ηλεκτρονικού ταχυδρομείου
τιμολόγηση με βάση τον αριθμό χρηστών και το φόρτο εργασίας	τιμολόγηση με βάση τον αριθμό χρηστών, μηνιαία χρέωση
Βασική λειτουργικότητα Προηγμένη προστασία από απειλές Προστασία ανεπιθύμητων Προστασία από ιούς Προστασία από επιθέσεις άρνησης υπηρεσίας (DoS). Προφιλτράρισμα ανεπιθύμητων μηνυμάτων και ιών Ασφάλεια εξερχόμενων email Φιλτράρισμα εξερχόμενων Απλοποιημένη διαχείριση email **Εξτρά λειτουργικότητα** Κεντρική διαχείριση με βάση το cloud Τα μηνύματα ηλεκτρονικού ταχυδρομείου μπορούν να παραδοθούν ακόμη και σε περίπτωση αστοχίας διακομιστή email ή απώλειας συνδεσιμότητας Κρυπτογράφηση	**Βασική λειτουργικότητα** Προστασία επιθέσεων Zero day Αφόπλιση κακόβουλου λογισμικού προτού εισέλθει σε έναν οργανισμό Οι χρήστες λαμβάνουν ασφαλή και αξιόπιστα αρχεία Έλεγχοι πολιτικών Ευφυΐα απειλών κακόβουλου λογισμικού **Εξτρά λειτουργικότητα** Επιβολή συμμόρφωσης με δημοσιευμένο πρότυπο για κάθε μορφή αρχείου Οι αναφορές παρέχουν ιατροδικαστικά στοιχεία συνημμένων
Ποσοστό ακρίβειας εντοπισμού ανεπιθύμητης αλληλογραφίας 95 % με επιθέσεις 0,01 % ψευδώς θετικού ποσοστού	99.99% διαθεσιμότητα
προληπτική, ανιχνευτική, αντιδραστική	προληπτική
εμπιστευτικότητα	---
ηλεκτρονικό ταχυδρομείο	ηλεκτρονικό ταχυδρομείο

ανεπιθύμητα μηνύματα, ιοί, κακόβουλο και κατασκοπευτικό λογισμικό, επιθέσεις άρνησης υπηρεσίας, πλαστογράφηση email (spoofing), ηλεκτρονικό ψάρεμα	κακόβουλο λογισμικό, απειλές βασισμένες σε αρχεία, επιθέσεις μηδενικής μέρας
υποστηρίζονται εως 30.000 χρηστες	---
30 ημέρες δωρεάν	30 ημέρες δωρεάν
Web gui	Web gui
Barracuda	Glasswall
AWS, Azure	Azure
3 πακέτα, υποστήριξη 24/7, tickets, email, τηλέφωνο ,chat, πύλη (portal), τεχνικά έγγραφα, forum, ενημέρωση για συνδρομές, κοινότητά, κέντρο γνώσης, τεκμηρίωση, λεξικό	υποστήριξη 24/7, επικοινωνία με τηλέφωνο ,email, tickets , κέντρο βοήθειας

Harmony Email & Collaboration	**Forcepoint Email Security**
SaaS	SaaS, IaaS
δημόσιο	δημόσιο
ασφάλεια ηλεκτρονικού ταχυδρομείου, DLP, κρυπτογράφηση	ασφάλεια ηλεκτρονικού ταχυδρομείου, DLP, κρυπτογράφηση
---	τιμολόγηση με βάση τα βασικά χαρακτηριστικά (modules) και τον αριθμό χρηστών, ετήσιο και διετές συμβόλαιο
Βασική λειτουργικότητα -Αποκλεισμός εξελιγμένων επιθέσεων κοινωνικής μηχανικής -Αποκλεισμός κακόβουλων συνημμένων πριν φτάσουν στους χρηστές, χωρίς να επηρεαστεί η παραγωγικότητα της επιχείρησης -Αποτροπή επιθέσεων εξαγοράς αυξάνοντας τις διαδικασίες ελέγχου ταυτότητας -Παρακολούθηση ενός απλού ταμπλό με χρήσιμες πληροφορίες και αναφορές **Εξτρά λειτουργικότητα** -Προστασία υπηρεσιών κοινής χρήσης αρχείων και εφαρμογών συνεργασιών (πχ slack) -Προστασία ευαίσθητων οικονομικών δεδομένων και διατήρηση της κανονιστικής νομοθεσίας με την προηγμένη πρόληψη διαρροών	**Βασική λειτουργικότητα** Αντιμετώπιση λυτρισμικού και άλλων απειλών Έλεγχος πρόσβασης συσκευής σε συνημμένα email Προστασία από ανεπιθύμητα μηνύματα και phishing Προστασία από απειλές σε πραγματικό χρόνο Προστασία από απειλές μηδενικής ημέρας **Εξτρά λειτουργικότητα** Αντιμετώπιση κλοπής δεδομένων με DLP με επίγνωση του περιεχομένου Προσδιορισμός συμπεριφοράς χρηστών υψηλού κινδύνου Ενσωματωμένη πρόληψη απώλειας δεδομένων Ισχυρή κρυπτογράφηση για πρόσθετη προστασία

δεδομένων (DLP) -Κρυπτογράφηση με βάση τις πολιτικές για ευαίσθητα αρχεία είτε κοινοποιούνται εσωτερικά μέσω email είτε δημόσια	Προσδιορισμός ακατάλληλων εικόνων για επιβολή αποδεκτής χρήσης
-Μείωση του ηλεκτρονικού ψαρέματος που φτάνει στα εισερχόμενα κατά 99,2% -ποσοστό εντοπισμού κακόβολου λογισμικού 99,91% και μπλοκαρίσματος 100%	99.999% διαθεσιμότητα, για περισσότερο από 0,001% μη διαθεσιμότητα οποιουδήποτε ημερολογιακού μήνα, ο πελάτης δικαιούται πίστωση υπηρεσίας ίση με 1 ημέρα για κάθε περίοδο 2 ωρών μη διαθεσιμότητας υπηρεσίας, με μέγιστη πίστωση 5 ημερών ανά 1 μήνα.
προληπτική, ανιχνευτική, αντιδραστική	προληπτική, ανιχνευτική, αντιδραστική
διαθεσιμότητα, εμπιστευτικότητα	διαθεσιμότητα, εμπιστευτικότητα
ηλεκτρονικό ταχυδρομείο, υπηρεσίες κοινής χρήσης αρχείων και εφαρμογές συνεργασίας	ηλεκτρονικό ταχυδρομείο
ηλεκτρονικό ψάρεμα, κακόβουλο λογισμικό, λυτρισμικό, κατάληψη λογαριασμού, διαρροή δεδομένων, επιθέσεις κοινωνικής μηχανικής	εσωτερικές και εξωτερικές απειλές, απειλές μηδενικής μέρας, λυτρισμικό, κλοπή δεδομένων
---	---
δωρεάν δοκιμαστική έκδοση χωρίς να αναφέρονται ημέρες	δωρεάν δοκιμαστική έκδοση χωρίς να αναφέρουν διάρκεια
Web gui, Rest api	Web gui, Cli (IaaS)
Check Point	Forcepoint
Azure	Azure
4 πακέτα(1 πακέτο 9/5 και 3 πακέτα 24/7) επικοινωνία με τηλέφωνο , email, tickets, chat, κέντρο βοήθειας, συχνές ερωτήσεις, βίντεο, ενημερώσεις, τεκμηρίωση, έγγραφα	3 πακέτα, υποστήριξη 24/7, επικοινωνία με τηλέφωνο ,emails, tickets, forum, βάση γνώσης, τεκμηρίωση, ενημερώσεις, εκπαίδευση

Advanced Threat Protection for Email and Collaboration	**FortiMail Secure Email Gateway**
SaaS	IaaS
δημόσιο	δημόσιο
ασφάλεια ηλεκτρονικού ταχυδρομείου	ασφάλεια ηλεκτρονικού ταχυδρομείου, DLP, κρυπτογράφηση
τιμολόγηση με βάση τον αριθμό γραμματοκιβωτίων (mailboxes) που προστατεύονται, μηνιαίο, ετήσιο, διετές, τριετές συμβόλαιο	τιμολόγηση με βάση το φόρτο εργασίας
Βασική λειτουργικότητα -Λήψη του email και εφαρμογή φίλτρων φήμης	**Βασική λειτουργικότητα** Προηγμένη ανίχνευση κακόβουλου λογισμικού

και anti-spam για γρήγορη επισήμανση ενός email ως κακόβουλου. -Αποσυσκευασία του περιεχομένου σε μικρότερες ενότητες (αρχεία και διευθύνσεις URL) με αναδρομικό τρόπο για τον εντοπισμό κρυφών κακόβουλων επιθέσεων. -Μηχανές εντοπισμού phishing -Ευφυία απειλών -Χρησιμοποιούνται μηχανές προστασίας από ιούς που βασίζονται στην υπογραφή για τον εντοπισμό κακόβουλων επιθέσεων. -Πρόληψη επιθέσεων χωρίς ωφέλιμο φορτίο **Εξτρά λειτουργικότητα** -Πλατφόρμα υποβοηθούμενη από υλικό	πολλαπλών επιπέδων Φιλτράρισμα εισερχόμενων και εξερχόμενων Ασφαλής παράδοση μηνυμάτων (TLS και DANE) Παρακολούθηση μηνυμάτων **Εξτρά λειτουργικότητα** Ενοποίηση με το LDAP πελάτη Κρυπτογράφηση βάσει ταυτότητας (IBE) Αναφορές Πρόληψη απώλειας δεδομένων email Ανάλυση για τον εντοπισμό και τη διακοπή απειλών κακόβουλου λογισμικού που ανακαλύπτονται μεταξύ των ενημερώσεων υπογραφής προτού εξαπλωθούν σε έναν οργανισμό.
-100% ποσοστό σάρωσης αρχείων -99.99% διαθεσιμότητα παράδοσης μηνυμάτων ηλεκτρονικού ταχυδρομείου, για <99.99% επιστροφή 20% της μηνιαίας συνδρομής, για <99% επιστροφή 30%, για <98% επιστροφή 40%, για <97% επιστροφή 50%, για <95% επιστροφή 50% και δικαίωμα τερματισμού του συμβολαίου και επιστροφής τυχών προπληρωμένου ποσού -99.99% διαθεσιμότητα προστασίας περιεχομένου για <99.99% επιστροφή 20% της μηνιαίας συνδρομής, για <98% επιστροφή 30%, για <97% επιστροφή 40%, για <95% επιστροφή 50% και δικαίωμα τερματισμού του συμβολαίου και επιστροφής τυχών προπληρωμένου ποσού -99.99% διαθεσιμότητα σάρωσης μηνυμάτων ηλεκτρονικού ταχυδρομείου για κακόβουλο λογισμικό για <99.99% επιστροφή 10% της μηνιαίας συνδρομής, για <98% επιστροφή 20%, για <97% επιστροφή 30% -ποσοστό εντοπισμού ψευδώς θετικών < 0.0001% για 0.0001 ως 0.001 επιστροφή 10% της	99,9% Ανίχνευση κακόβουλων μηνυμάτων ηλεκτρονικού ταχυδρομείου 94% Συνολικό Ποσοστό Ανίχνευσης Απειλής Ποσοστό κάλυψης ανεπιθύμητων μηνυμάτων 99,78%. 100%+ Ποσοστό ανίχνευσης Wildlist

μηνιαίας συνδρομής, για 0.001 ως 0.01 επιστροφή 20%, για 0.01 έως 0.1 επιστροφή 30%, για >0.1 επιστροφή 50%	
προληπτική, ανιχνευτική, αντιδραστικη	προληπτική, ανιχνευτική, αντιδραστική
---	διαθεσιμότητα, εμπιστευτικότητα
ηλεκτρονικό ταχυδρομείο	ηλεκτρονικό ταχυδρομείο
"Επιθέσεις μηδενικής μέρας και N-ημερών Ηλεκτρονικό ψάρεμα Συμβιβασμός επιχειρησιακού email (BEC) Εξαγορά λογαριασμού και πλευρικό ψάρεμα Κακόβουλο λογισμικό Επιθέσεις υπεκφυγής (evasion)"	Ανεπιθύμητη αλληλογραφία Ηλεκτρονικό ψάρεμα, στοχευμένο ηλεκτρονικό ψάρεμα (spearphising) και ηλεκτρονικό ψάρεμα φάλαινας (whaling) Κακόβουλα συνημμένα και διευθύνσεις URL Λυτρισμικό Απειλές μηδενικής ημέρας Μίμηση (impersonation) Συμβιβασμός ηλεκτρονικού ταχυδρομείου για επιχειρήσεις (BEC)
---	---
τίποτα δωρεάν	τίποτα δωρεάν
Web gui	Web gui, Rest api
Perception point	Fortinet
AWS	AWS, Azure
2 πακέτα (1 πακέτο 8/5 και 1 πακέτο 24/7), επικοινωνία με τηλέφωνο , emails, ενημερώσεις, τεκμηρίωση	υποστήριξη 24/7 με τηλέφωνο , tickets, έγγραφα, Φόρουμ, Τεκμηρίωση, βίντεο , Ενημερωτική πύλη ασφαλείας(security portal)

Vircom modusGate Email Security Gateway	**Vircom modusCloud Cloud Email Security**
IaaS	SaaS
δημόσιο	δημόσιο
ασφάλεια ηλεκτρονικού ταχυδρομείου	ασφάλεια ηλεκτρονικού ταχυδρομείου, DLP, κρυπτογράφηση
τιμολόγηση με άδεια χρήσης BYOL στο Azure	---
Βασική λειτουργικότητα Εξαιρετικά λεπτομερής έλεγχος με συγκεκριμένα δικαιώματα και ρυθμίσεις για χρήστες/τομείς. Πολυεπίπεδη διοίκηση Διπλό επίπεδο προστασίας από ιούς που περιλαμβάνει Avira και Bitdefender που	**Βασική λειτουργικότητα** Πρόσβαση SMB/E σε λύσεις σε επίπεδο επιχείρησης Πλήρης έλεγχος διαχειριστή Εύκολη πρόσβαση τελικού χρήστη Απεριόριστη αποθήκευση και διατήρηση email 10

εξασφαλίζουν άμυνα μηδενικής ημέρας έναντι απειλών ηλεκτρονικού ψαρέματος και κακόβουλου λογισμικού. **Εξτρά λειτουργικότητα** Εκχώρηση πλήρους διαχείρισης καραντίνας στους τελικούς χρήστες Αυτόματη διαχείριση όλων των λογαριασμών χρήστη και της διαχείρισης ψευδωνύμων μέσω αναζητήσεων (SMTP, LDAP, MS Active Directory).	ετών Αυτοματοποιημένες Πολιτικές Προστασίας Δεδομένων **Εξτρά λειτουργικότητα** Απόδειξη παραποίησης, Αρχείο ηλεκτρονικού ταχυδρομείου εκτός τοποθεσίας Πρόληψη απώλειας δεδομένων (DLP) Κρυπτογράφηση για χρηματοοικονομική συμμόρφωση και HIPAA Κρυπτογράφηση SMTP μέσω TLS Κρυπτογράφηση εξερχόμενου email Έλεγχος πρόσβασης (granural control)
Ποσοστό κάλυψης ανεπιθύμητων μηνυμάτων 99,93%. 0% ψευδώς θετικό ποσοστό	Ποσοστό κάλυψης ανεπιθύμητων μηνυμάτων 99,93%
προληπτική, ανιχνευτική, αντιδραστική	προληπτική, ανιχνευτική, αντιδραστική
---	διαθεσιμότητα, εμπιστευτικότητα
ηλεκτρονικό ταχυδρομείο	ηλεκτρονικό ταχυδρομείο
Προστασία ανεπιθύμητων μηνυμάτων συμβιβασμού ηλεκτρονικού ταχυδρομείου επιχειρήσεων πλαστογράφησης τομέα και email προστασία URL Άμυνα για κακόβουλα συνημμένα Λυτρισμικό Ηλεκτρονικό ψάρεμα Επιθέσεις μηδενικης μερας Κακόβουλο λογισμικό	Προστασία ανεπιθύμητων μηνυμάτων ηλεκτρονικό ψάρεμα και στοχευμένο ηλεκτρονικό ψάρεμα Προστασία κατά των ιών κακόβουλα συνημμένα και διευθύνσεις URL συμβιβασμός επαγγελματικού email Προστασία από πλαστογράφηση τομέα και email
αποτροπή έως και το 75% του συμβιβασμού των επαγγελματικών email ή επιθέσεων ηλεκτρονικού ψαρέματος που χρησιμοποιούν πλαστογράφηση τομέα και email	αρχειοθέτηση email για εως 10 ετη
30 ημέρες δωρεάν	30 ημέρες δωρεάν
Web gui	Web gui
Vircom	Vircom
Azure	κανένα
υποστήριξη 8.30/5, επικοινωνία με emails, τηλέφωνο , βάση γνώσης, πύλη πελατών, έγγραφα	υποστήριξη 8.30/5 , επικοινωνία με emails, τηλέφωνο , βάση γνώσης, πύλη πελατών, εγγραφα

Cyren Inbox Security for Microsoft 365	**Alinto cleanmail**
SaaS	SaaS
δημόσιο	δημόσιο
ασφάλεια ηλεκτρονικού ταχυδρομείου	ασφάλεια ηλεκτρονικού ταχυδρομείου, BCDR
---	---
Βασική λειτουργικότητα -Μόνιμη εκ νέου σάρωση εισερχόμενων, εξερχόμενων και παραδοθέντων email σε όλους τους φακέλους -Η ανάλυση σε πραγματικό χρόνο των συμπεριφορών χρήστη και γραμματοκιβωτίου εντοπίζει ανωμαλίες που δείχνουν μια πιθανή απειλή -Η προσθήκη γραμματοκιβωτίου επιτρέπει στους χρήστες να σαρώνουν και να αναφέρουν ύποπτα μηνύματα ηλεκτρονικού ταχυδρομείου κατά βούληση -Η αυτόματη «ρετρό» σάρωση σε κάθε γραμματοκιβώτιο κατά την επιβίβαση δημιουργεί μια ασφαλή γραμμή βάσης και διασφαλίζει ότι δεν υπάρχουν παρατεταμένες απειλές στο γραμματοκιβώτιο -Ανεξάρτητο από το SEG (Secure Email Gateway) **Εξτρά λειτουργικότητα** -Το πλαίσιο απόκρισης βάσει πολιτικής αυτοματοποιεί τις ενέργειες αποκατάστασης σε μεμονωμένα γραμματοκιβώτια και σε όλα τα γραμματοκιβώτια του οργανισμού -Οι αυτοματοποιημένες ροές εργασιών διαχείρισης συμβάντων και υποθέσεων μειώνουν περαιτέρω τα έξοδα έρευνας και επιταχύνουν την επίλυση απειλών Πλήρως ενσωματωμένο με το Office 365	**Βασική λειτουργικότητα** Προστασία Anti-Spam & Anti-Virus Μαύρη λίστα /Whitelisting Αρχειοθέτηση email Πίνακας Ελέγχου με παρακολούθηση σε πραγματικό χρόνο Εξερχόμενη σάρωση email Εύκολο στη χρήση διεπαφή διαχείρισης **Εξτρά λειτουργικότητα** Webmail έκτακτης ανάγκης Συμβατότητα με όλους τους επαγγελματικούς διακομιστές αλληλογραφίας
αφαίρεση του 97% των επιθέσεων από όλα τα επηρεαζόμενα γραμματοκιβώτια (mailboxes)	Εξάλειψη του 99,9% όλων των ανεπιθύμητων μηνυμάτων και των ιών
προληπτική, ανιχνευτική, αντιδραστική	προληπτική, αντιδραστική
---	διαθεσιμότητα
ηλεκτρονικό ταχυδρομείο	ηλεκτρονικό ταχυδρομείο

Επιθέσεις ηλεκτρονικού ψαρέματος Στοχευμένο ηλεκτρονικό ψάρεμα και πλαστά μηνύματα Συμβιβασμός email για επιχειρήσεις και άλλες στοχευμένες επιθέσεις κοινωνικής μηχανικής Νέες καμπάνιες phishing zero-day Εξαγορές λογαριασμού (κλοπή διαπιστευτηρίων) και παρακολούθηση εσωτερικού email	ανεπιθύμητα μηνύματα, ιοί, ηλεκτρονικό ψάρεμα, πλαστογράφηση, κακόβουλο λογισμικό, λυτρισμικό
---	αρχειοθέτηση email για έως 10 ετη
30 ημέρες δωρεάν	δωρεάν δοκιμαστική έκδοση χωρίς να αναφέρονται ημέρες
Web gui	Web gui
Cyren	Alinto
Azure	κανένα
υποστήριξη 9/5, επικοινωνία με τηλέφωνο , email, chat, βάση γνώσης, τεκμηρίωση, εργαλεία	επικοινωνία με τηλέφωνο , emails

Πίνακας αποτίμησης 8 – Προϊόντα Ασφάλειας Δικτύου

ΚΡΙΤΗΡΙΑ/ΠΡΟΙΟΝΤΑ	**Barracuda CloudGen Firewall**
α. τρόπος παράδοσης	IaaS
β. μοντέλο διάταξης	δημόσιο
γ. κατηγορία υπηρεσιών στην οποία ανήκει	ασφάλεια δικτύου, IAM , IDS, ασφάλεια ιστού
δ. μοντέλο κόστους	τιμολόγηση με βάση το φόρτο εργασίας , ετήσια συνδρομή
ε. μηχανισμοί ασφάλειας που υλοποιούνται	**Βασική λειτουργικότητα** -Έλεγχος Εφαρμογών -Ανίχνευση και Πρόληψη Εισβολών -Προστασία από κακόβουλο λογισμικό -Επιλογή συνδέσμων βάσει εφαρμογών για εκχώρηση εύρους ζώνης -Διαμόρφωση Κυκλοφορίας και Ποιότητα Εξυπηρέτησης -Failover και εξισορρόπηση συνδέσμων -Βελτιστοποίηση WAN

	-Ασφαλής απομακρυσμένη πρόσβαση **Επιπλέον λειτουργικότητα** **-**Ανίχνευση προηγμένων απειλών (προαιρετικό) -Έλεγχος πρόσβασης δικτύου (προαιρετικό) -Σύστημα ελέγχου αναθεώρησης, έλεγχος και αναφορές -Φιλτράρισμα Ιστού -Ανάλυση περιβάλλοντος εφαρμογών σε βάθος -Εξατομικευμένος Έλεγχος Εφαρμογών -Επίγνωση ταυτότητας χρηστών -Αναφορές
στ. μη λειτουργικές εγγυήσεις	---
ζ. είδος προσφερόμενης προστασίας	προληπτική , ανιχνευτική
η. ιδιότητες ασφάλειας	διαθεσιμότητα, εμπιστευτικότητα
θ. αντικείμενα που προστατεύονται	δίκτυο
ι. απειλές που αντιμετωπίζονται	προηγμένες απειλές, απειλές δικτύου, ευπάθειες και εκμεταλλεύσεις, κακόβουλο λογισμικό, dos,DDos, κατασκοπευτικό λογισμικό, botnet
ια. περιορισμοί	---
ιβ. ύπαρξη δωρεάν εκδόσεων	30 μέρες δωρεάν
ιγ. τρόπος χρήσης προϊόντος	Web gui, Rest api, Cli
ιδ. εταιρεία που προσφέρει το προϊόν	Barracuda
ιε. marketplace(s) όπου προσφέρεται το προϊόν	AWS, Azure, GCP
ιστ. επίπεδο/είδος υποστήριξης για το προϊόν	υποστήριξη 24/7 και 3 πακέτα, επικοινωνία με tickets ,emails, τηλέφωνο, chat, πύλη (portal), τεχνικά έγγραφα, forum, ενημέρωση για συνδρομές, κοινότητα, κέντρο γνώσης, τεκμηρίωση, λεξικό

FortiGate Next-Generation Firewall	**CloudGuard Network Security (All-In-One/Autoscaling)**
IaaS	IaaS
δημόσιο	δημόσιο, ιδιωτικό
ασφάλεια δικτύου, IDS, ασφάλεια ηλεκτρονικού ταχυδρομείου, ασφάλεια ιστού	ασφάλεια δικτύου, DLP , IDS, ασφάλεια ιστού
τιμολόγηση με βάση το φόρτο εργασίας	---

Βασική λειτουργικότητα -Υπηρεσία ελέγχου εφαρμογών -Υπηρεσία IPS -Προηγμένη προστασία από κακόβουλο λογισμικό (AMP) — Antivirus, Mobile Malware, Botnet, CDR, Προστασία από ιούς και Sandbox Cloud Service **Επιπλέον λειτουργικότητα** -Υπηρεσία φιλτραρίσματος ιστού και βίντεο -Υπηρεσία Antispam	**Βασική λειτουργικότητα** -Πρόληψη προηγμένων απειλών -Τείχος προστασίας -IPS -Έλεγχος Εφαρμογών -IPSec VPN -Antivirus -Anti-Bot -Επιθεώρηση κυκλοφορίας SSL/TLS με προώθηση κίνησης. -Το Threat Extraction αφαιρεί εκμεταλλεύσιμο περιεχόμενο και παρέχει έγκαιρα απολυμασμένο περιεχόμενο στους χρήστες. -Το Threat Emulation αποτρέπει μολύνσεις από νέο κακόβουλο λογισμικό και στοχευμένες επιθέσεις -Επιθεώρηση κυκλοφορίας SSL/TLS με προώθηση κίνησης και υποστήριξη SNI για προηγμένη πρόληψη απειλών εντός ασφαλούς κυκλοφορίας SSL. **Επιπλέον λειτουργικότητα** -DLP -Ενοποιημένη Διαχείριση Ασφαλείας -Φιλτράρισμα URL
---	Προηγμένη πρόληψη απειλών με 100% ποσοστό αποκλεισμού, 100% πρόληψη κακόβουλου λογισμικού, 100% αντίσταση εκμετάλλευσης και 0% ψευδώς θετικά
προληπτική, ανιχνευτική	προληπτική ,ανιχνευτική
---	διαθεσιμότητα
δίκτυο/οτιδήποτε	δίκτυο/οτιδήποτε
λυτρισμικό, κακόβουλο λογισμικό, επιθέσεις command-and-control	κακόβουλο λογισμικό, λυτρισμικό, ιοί, επιθέσεις μηδενικής μέρας, botnets, κλοπή δεδομένων, επιθέσεις άρνησης υπηρεσίας
---	---
30 μέρες δωρεάν	30 μέρες δωρεάν
Web gui, Rest api, Cli	Cli
Fortinet	Check Point
AWS, Azure, GCP	AWS,GCP

υποστήριξη 24/7 με τηλέφωνο, tickets, έγγραφα, Φόρουμ, Τεκμηρίωση, βίντεο , Ενημερωτική πύλη ασφαλείας(security portal)	4 πακέτα (1 πακέτο 9/5 και 3 πακέτα 24/7), επικοινωνία με τηλέφωνο, email, tickets, chat, κέντρο βοήθειας, συχνές ερωτήσεις, βίντεο, ενημερώσεις, τεκμηρίωση, έγγραφα

vSRX Next Generation Firewall	**Cisco Firepower NGFW Virtual (NGFWv) Firewall**
IaaS	IaaS
δημόσιο, ιδιωτικό	δημόσιο, ιδιωτικό
ασφάλεια δικτύου, IAM , IDS, ασφάλεια ιστού	ασφάλεια δικτύου, IDS, ασφάλεια ιστού
τιμολόγηση με βάση τις ώρες χρήσης, χρέωση ανά ώρα ή ανά έτος	τιμολόγηση με βάση τα βασικά χαρακτηριστικά, το φόρτο εργασίας και τις ώρες χρήσης
Βασική λειτουργικότητα -Προηγμένη Πρόληψη Απειλών -Τείχος προστασίας επόμενης γενιάς -Σύστημα αποτροπής εισβολής (IPS) -Ασφάλεια εφαρμογών -Ασφάλεια περιεχομένου -Προσαρμοστική ασφαλή πρόσβαση SSL-VPN σε εταιρικούς πόρους και πόρους cloud -Προστασία φόρτου εργασίας δημόσιου νέφους -Υποστήριξη SDN και εικονικοποίησης λειτουργιών δικτύου (NFV) **Επιπλέον λειτουργικότητα** -Αναγνωριστικά χρηστών και έλεγχοι πρόσβασης βάσει ρόλων -Καταγραφή και Αναφορές	**Βασική λειτουργικότητα** -Αυτοματοποιημένη κατάταξη κινδύνου και σημαίες επιπτώσεων -Ενοποιημένη διαχείριση και αυτοματοποιημένος συσχετισμός απειλών -Ορατότητα και έλεγχος εφαρμογων -Πληροφορίες Ασφαλείας -Σύστημα αποτροπής εισβολής επόμενης γενιάς -Προηγμένη προστασία από κακόβουλο λογισμικό (AMP) -Πλατφόρμα ανάλυσης πληροφοριών απειλών και κακόβουλου λογισμικού **Επιπλέον λειτουργικότητα** -Υποστήριξη τοπικής διαχείρισης συσκευών -Κεντρική διαχείριση -Φιλτράρισμα URL -Υψηλή διαθεσιμότητα και ομαδοποίηση
---	---
προληπτική ,ανιχνευτική	προληπτική, ανιχνευτική
---	---
δίκτυο/οτιδήποτε	δίκτυο/οτιδήποτε
κατασκοπευτικό λογισμικό, λογισμικό διαφημίσεων, ιοί, keylogger, κακόβουλα url, κακόβουλο λογισμικό, ακούσια ή κακόβουλη μετάδοση αρχείων και κακόβουλο περιεχόμενο στο δίκτυο, προηγμένες	κακόβουλο λογισμικό

επίμονες απειλές, επιθέσεις phishing, εισβολές, α-νεπιθύμητο περιεχόμενο	
λειτουργία με ταχύτητες δικτύου έως και 100 Gbps.	στη μέγιστη έκδοση υποστηρίζονται 15.5gbps ρυθμο-αποδοση, έως 2 εκ. ταυτόχρονες συνδέσεις και 10 χι-λιάδες συνδέσεις vpn (vpn peers)
30 μέρες δωρεάν	30 μέρες δωρεάν
Web gui, Rest api, Cli	Web gui, Rest api, Cli
Jupiter networks	Cisco
AWS, Azure, GCP	AWS, Azure, GCP
υποστήριξη 24/7 , επικοινωνία με τηλέφωνο, emails, tickets, chat, πύλη υποστήριξης, έγγραφα, βάση γνώσης, τεκμηρίωση, κοινότητα	επικοινωνία με τηλέφωνο, email, tickets, chat, τεκμη-ρίωση, ενημερώσεις, έγγραφα, κοινότητα, βοηθητικές παροχές

VT AIR Next Generation Enterprise Firewall	**Heimdal Threat Prevention - Network**
IaaS	IaaS
δημόσιο	δημόσιο
ασφάλεια δικτύου, IDS, ασφάλεια ιστού	ασφάλεια δικτύου, IAM , IDS, ασφάλεια ιστού, DLP
τιμολόγηση με βάση τις ώρες χρήσης, χρέωση ανά ώρα ή ανά έτος	πληροφορίες τιμολόγησης μόνο μέσω επικοινωνίας με την εταιρία
Βασική λειτουργικότητα -Προστασία από προηγμένες απειλές -Έλεγχος Εφαρμογών -Ανίχνευση εισβολής και προστασία -Βαθιά επιθεώρηση πακέτων -XDP/eBPF για μεγαλύτερες ταχύτητες τείχους προστασίας -Μεγάλη διαθεσιμότητα -IPSec-VPN -Ανάλυση και παρακολούθηση της κυκλοφορίας του δικτύου **Επιπλέον λειτουργικότητα** -Έλεγχος ταυτότητας πολλαπλών παραγόντων -Έλεγχος Ιστού/Προστασία Ιστού -Πύλη Κεντρικής Διαχείρισης	**Βασική λειτουργικότητα** -Αποκλεισμός Command&Control callbacks -Προστασία από κακόβουλο λογισμικό που βασίζεται σε δίκτυο και ανίχνευση προηγμένων επίμονων απει-λών -Φιλοξενούμενη υπηρεσία - χωρίς διακομιστές ή λογι-σμικό πελάτη -Υποστηρίζει όλους τους διακομιστές, επιτραπέζιους υπολογιστές και φορητές συσκευές -Προσαρμοσμένη λίστα αποκλεισμού και επιτρεπό-μενων -Λειτουργία IDS **Επιπλέον λειτουργικότητα** -Εντοπισμός και αποκλεισμός απειλών που βασίζο-νται στον ιστό -Έλεγχος Ιστού/Προστασία Ιστού

	-Πύλη Κεντρικής Διαχείρισης -Πρόληψη διαρροής δεδομένων -Προσαρμοσμένη σελίδα αποκλεισμού (προαιρετικό) -Βασικά στατιστικά στοιχεία -Προηγμένα στατιστικά και foresincs, με εσωτερικές διευθύνσεις IP και ονόματα κεντρικών υπολογιστών
---	Ακρίβεια 96% στον εντοπισμό και την πρόβλεψη μελλοντικών επιθέσεων
προληπτική, ανιχνευτική	προληπτική ,ανιχνευτική
---	διαθεσιμότητα
δίκτυο/οτιδήποτε	δίκτυο/οτιδήποτε
προηγμένες επίμονες απειλές, απειλές δικτύου, τρωτά σημεία, εκμεταλλεύσεις και απειλές σε λειτουργικά συστήματα και εφαρμογές.	Προηγμένες επίμονες απειλές, διαρροές δεδομένων, ransomware και κακόβουλο λογισμικό δικτύου, κακόβουλο περιεχόμενο ιστού, διήθηση δεδομένων (data extrafiltration)
---	---
30 μέρες δωρεάν	30 μέρες δωρεάν
Web gui, Rest api, Cli	Web gui, Rest api, Cli
Voleatech	Heimdal security
AWS,Azure	Azure
επικοινωνία με τηλέφωνο, email, τεκμηρίωση, βίντεο, συχνές ερωτήσεις	υποστήριξη 24/7 ,επικοινωνία με τηλέφωνο, email, tickets, βάση γνώσης, συχνές ερωτήσεις, τεκμηρίωση

Deep Learning-Powered Network Malware Protection	**Trend Micro Cloud One – Network Security**
SaaS, IaaS	SaaS, IaaS
δημόσιο	δημόσιο
ασφάλεια δικτύου	ασφάλεια δικτύου, IDS
---	για την έκδοση SaaS τιμολόγηση με βάση τον ογκο δεδομένων, ετήσια συνδρομή
Βασική λειτουργικότητα -Αρχιτεκτονική Βελτιστοποιημένη για Αποδοτικότητα -Δεδομένα απειλών που επεξεργάζονται με AI για	**Βασική λειτουργικότητα** -Επιθεώρηση με ταχύτητα δικτύου -Επιθεώρηση κίνησης εισόδου και εξόδου απευθείας ενσωματωμένη, με δυνατότητες ταχύτητας δικτύου.

εκπαίδευση -Επιθεώρηση σε πραγματικό χρόνο ωφέλιμου φορτίου και κεφαλίδων με Deep Learning -Ταξινόμηση σε πραγματικό χρόνο -Τα δεδομένα για την ταξινόμηση των απειλών κοινοποιούνται σε όλους τους πελάτες -Αυτοματοποιημένη και Ενορχηστρωμένη Πρόληψη **Επιπλέον λειτουργικότητα** -Ταμπλό	-Ενεργή ασφάλεια -Ανάπτυξη ασφάλειας συστήματος πρόληψης εισβολής (IPS) σε επίπεδο δικτύου -Προστασία πριν από την αποκάλυψη ευπάθειας και απόκτηση προηγμένης ευφυΐας απειλών -Φιλτράρισμα κυκλοφορίας εισόδου και εξόδου -Βαθιά επιθεώρηση πακέτων **Επιπλέον λειτουργικότητα** -Κεντρική ορατότητα και έλεγχος -Προστασία των VPC cloud και ικανοποίηση απαιτήσεων συμμόρφωσης
ανίχνευση απειλών σε λιγότερο από ένα δευτερόλεπτο, με αποτελεσματικότητα μεγαλύτερη από 99,5%.	Στόχος χρόνου αποκατάστασης (RTO) έως 5 ώρες και στόχος σημείου αποκατάστασης (RPO) έως 24 ώρες.
προληπτική, ανιχνευτική	προληπτική, ανιχνευτική
---	---
δίκτυο/οτιδήποτε	δίκτυο/οτιδήποτε
οτιδήποτε/γνωστές και άγνωστες απειλές	επιθέσεις στο επίπεδο δικτύου
---	---
7 μέρες δωρεάν	30 μέρες δωρεάν
Web gui, Rest api	Web gui, Cli
Blue Hexagon	Trend Micro
Azure	AWS, Azure
υποστήριξη 24/7, επικοινωνία με τηλέφωνο, emails, ενημερώσεις	2 πακέτα υποστήριξης, επικοινωνία μεσω τηλέφωνου 24/7 ,email, tickets, chat, κέντρο βοήθειας, συχνές ερωτήσεις, τεκμηρίωση, έγγραφα, ενημερώσεις και αναβαθμίσεις προϊόντων, κοινότητα, forum

SonicWall NSv (Firewall/Security/VPN/Router)	**Netgate pfSense Plus Firewall/VPN/Router**
IaaS	IaaS
δημόσιο, ιδιωτικό, υβριδικο	δημόσιο
ασφάλεια δικτύου, IDS, DLP, ασφάλεια ιστού	ασφάλεια δικτύου, IDS ασφάλεια ιστού
τιμολόγηση με βάση τον αριθμό χρηστών (sso users) , ελάχιστο 25 χρήστες ή τιμολόγηση με βάση τη χρήση και χρέωση ανά ώρα ή ετησίως	δωρεάν λογισμικό

Βασική λειτουργικότητα -Τεχνολογία Deep Memory Inspection (RTDMI) σε πραγματικό χρόνο -Τείχος προστασίας και δικτύωση -Εικονική ιδιωτική δικτύωση (VPN) -Προστασία προηγμένων απειλών -Πρόληψη κρυπτογραφημένων απειλών -Πρόληψη εισβολών -Πρόληψη απειλών -Ευφυΐα και Έλεγχος Εφαρμογών -Φιλτράρισμα περιεχομένου -Antivirus and Anti-Spyware **Επιπλέον λειτουργικότητα** -Διαχείριση και Αναφορές -Content/Context Awareness-DLP	**Βασική λειτουργικότητα** -Αποτροπή επιθέσεων (IDS/IPS) -Τείχος προστασίας -Δρομολογητής -VPN -Φιλτράρισμα διακομιστή μεσολάβησης και περιεχομένου -Υπηρεσίες Δικτύου -Αναφορά/παρακολούθηση συστήματος -Διαχείριση Ασφάλειας Συστήματος -Διαχείριση Αξιοπιστίας/Ανθεκτικότητας
---	---
προληπτική ,ανιχνευτική	ανιχνευτική, προληπτική
διαθεσιμότητα , εμπιστευτικότητα, ακεραιότητα	---
δίκτυο/οτιδήποτε	δίκτυο/οτιδήποτε
απειλές zero-day, άγνωστο κακόβουλο λογισμικό, ιοί, κατασκοπευτικό λογισμικό, bots, προηγμένες επίμονες απειλές, dos, DDos, cross-virtual-machine, side-channel attacks, κοινές εισβολές που βασίζονται σε δίκτυο και ευπάθειες εφαρμογών και πρωτοκόλλων	κακόβουλο λογισμικό, απειλές διαδικτύου
στη μέγιστη έκδοση υποστηρίζονται έως 20 χιλιάδες χρήστες	απόδοση έως 10 Gbps
30 μέρες δωρεάν	δωρεάν λογισμικό
Web gui, Rest api, Cli	Web gui, Cli
SonicWall	Netgate
AWS, Azure	AWS, Azure
επικοινωνία με τηλέφωνο, emails, tickets, πύλη υποστήριξης, βάση γνώσης, τεκμηρίωση, κοινότητα, βίντεο	3 πακέτα, τα δυο είναι 24/7, επικοινωνία με emails, τηλέφωνο, κοινότητα, έγγραφα, τεκμηρίωση, συχνές ερωτήσεις

Hillstone CloudEdge Virtual-Firewall	**Untangle NG Firewall**
IaaS	IaaS
δημόσιο, ιδιωτικό	δημόσιο
ασφάλεια δικτύου, IDS, ασφάλεια ιστού	ασφάλεια δικτύου
5 πακέτα, τιμολόγηση με βάση το φόρτο εργασίας	τιμολόγηση με βάση τον αριθμό συσκευών και τα προσθετά, πληρωμή μηνιαία, ετήσια, τριετής ή τιμολόγηση με βάση τις ώρες χρήσης
Βασική λειτουργικότητα -Υπηρεσίες Δικτύου -Τείχος προστασίας -Πρόληψη εισβολής -Cloud Sandbox -Ενέργειες που βασίζονται σε IP -Αναγνώριση και έλεγχος τελικού σημείου -Εξισορρόπηση φορτίου συνδέσμου -Εξισορρόπηση φορτίου διακομιστή -Έλεγχος Εφαρμογών -VPN -Διαχείριση (administration) -Ταυτότητες χρηστών και συσκευών -Αποκρυπτογράφηση SSL -Antivirus **Επιπλέον λειτουργικότητα** -Μητρώα & Αναφορές -Στατιστική και Παρακολούθηση -Φιλτράρισμα URL	**Βασική λειτουργικότητα** -Προληπτικός αποκλεισμός κακόβουλου λογισμικού, phishing, ανεπιθύμητης αλληλογραφίας, hacking και άλλων εκμεταλλεύσεων από την πρόσβαση σε χρήστες και συσκευές στο δίκτυο. -Φιλτράρισμα κάθε εφαρμογής, κρυπτογραφημένου αιτήματος Ιστού, σημείου διανομής κακόβουλου λογισμικού και ανεπιθύμητων μηνυμάτων. -Διασφάλιση απόδοσης δικτύου, μέγιστου χρόνου λειτουργίας και QoS για αύξηση της παραγωγικότητας. -Διατήρηση της ορατότητας και του ελέγχου των απομακρυσμένων εργαζομένων, των υποκαταστημάτων (branches) και του Wi-Fi επισκεπτών για να διατηρούνται οι χρήστες συνδεδεμένοι και τα δεδομένα ασφαλή. -Δημιουργία πολιτικών ανά χρήστη, ομάδα, συσκευή και χρόνο για τον έλεγχο της πρόσβασης.
---	---
ανιχνευτική, προληπτική	προληπτική
διαθεσιμότητα	---
δίκτυο/οτιδήποτε	δίκτυο/οτιδήποτε
ιοί, command and control, DoS, DDos, Πρωτόκολλο επίλυσης διευθύνσεων (ARP attack)	κακόβουλο λογισμικό, απόπειρες hacking, phishing
στη μέγιστη έκδοση υποστηρίζονται έως και 5 εκατομμύρια ταυτόχρονες συνεδρίες, έως 10000 σήραγγες VPN IPSec και έως 2000 χρήστες SSL VPN	---
30 μέρες δωρεάν	14 μέρες δωρεάν
Web gui, Rest api, Cli	Web gui, Rest api

Hillstone networks	Untangle
AWS,Azure	AWS,Azure
υποστήριξη 8/5, επικοινωνία με τηλέφωνο, email, tickets, βάση γνώσης, ενημερώσεις, έγγραφα, εκπαίδευση	υποστήριξη 12/5, επικοινωνία με τηλέφωνο, emails, κοινότητα, forum, συχνές ερωτήσεις, τεκμηρίωση, έγγραφα

Trend Micro Deep Security	**AhnLab vTrusGuard Next-Generation Firewall**
IaaS	IaaS
δημόσιο	δημόσιο
ασφάλεια δικτύου, IDS, ασφάλεια ιστού	ασφάλεια δικτύου, IDS, DLP, ασφάλεια ιστού
τιμολόγηση με βάση το φόρτο εργασίας μηνιαία ή με άδεια χρήσης BYOL και 1 προϊόν (6.6%)	τιμολόγηση BYOL
Βασική λειτουργικότητα -Αποτροπή εισβολών -Προστασία από κακόβουλο λογισμικό -Τείχος προστασίας -Έλεγχος εφαρμογών για αλλαγές **Επιπλέον λειτουργικότητα** -Φιλτράρισμα περιεχομένου και μαρκάρισμα επικίνδυνων url -Παρακολούθηση ακεραιότητας -Επιθεώρηση αρχείων καταγραφής	**Βασική λειτουργικότητα** -Τείχος προστασίας -IPS -Έλεγχος Εφαρμογών -Μετριασμός DDos -IPSec VPN -SSL VPN -Καταγραφή & Παρακολούθηση -Anti-Virus/Anti-Spam **Επιπλέον λειτουργικότητα** -Φιλτράρισμα Ιστού -Σύνδεση με λύσεις Endpoint
---	---
ανιχνευτική, προληπτική	προληπτική ,ανιχνευτική
---	διαθεσιμότητα
δίκτυο/οτιδήποτε	δίκτυο/οτιδήποτε
κακόβουλο λογισμικό, απειλές διαδικτύου (πχ sql scripting)	ιοί, ανεπιθύμητα μηνύματα, επιθέσεις command and control, DDos
---	---
30 μέρες δωρεάν	τίποτα δωρεάν
Rest api, Cli, Web gui	Cli

Trend micro	Ahnlab
AWS, Azure	AWS
2 πακέτα, επικοινωνία μέσω τηλέφωνου 24/7 ,email, tickets, chat, κέντρο βοήθειας, συχνές ερωτήσεις, τεκμηρίωση, έγγραφα, ενημερώσεις και αναβαθμίσεις προϊόντων, κοινότητα, forum	3 πακέτα και υποστήριξη σε εργάσιμο ωράριο, εργάσιμο και σαββατοκύριακα, 24/7 αντίστοιχα, επικοινωνία μέσω mail, τηλέφωνου, chat, tickets (TAC portal), συχνές ερωτήσεις, κέντρο υποστήριξης

Πίνακας αποτίμησης 9 – Προϊόντα Αποτίμησης Ασφάλειας

ΚΡΙΤΗΡΙΑ/ΠΡΟΙΟΝΤΑ	**Seconize Security Assessment / Derisk Center**
α. τρόπος παράδοσης	SaaS
β. μοντέλο διάταξης	δημόσιο
γ. κατηγορία υπηρεσιών στην οποία ανήκει	assesement
δ. μοντέλο κόστους	---
ε. μηχανισμοί ασφάλειας που υλοποιούνται	**Βασική λειτουργικότητα** -Διαχείριση συμμόρφωσης -Ταμπλό -Αυτόματη αποκατάσταση -Διαχείριση περιουσιακών στοιχείων -Υποσύστημα για κίνδυνους, ευπάθειες και ρυθμίσεις
στ. μη λειτουργικές εγγυήσεις	---
ζ. είδος προσφερόμενης προστασίας	προληπτική, ανιχνευτική
η. ιδιότητες ασφάλειας	---
θ. αντικείμενα που προστατεύονται	οτιδήποτε
ι. απειλές που αντιμετωπίζονται	οτιδήποτε
ια. περιορισμοί	---
ιβ. ύπαρξη δωρεάν εκδόσεων	τίποτα δωρεάν
ιγ. τρόπος χρήσης προϊόντος	Web gui
ιδ. εταιρεία που προσφέρει το προϊόν	Seconize Technologies Private Limited
ιε. marketplace(s) όπου προσφέρεται το προϊόν	Azure
ιστ. επίπεδο/είδος υποστήριξης για το προϊόν	επικοινωνία μέσω email

SecOps Solution Security Platform	**Cymetrics SaaS platform - Cyber Assessment**

SaaS	SaaS
δημόσιο	δημόσιο
assesement	assesement
---	---
Βασική λειτουργικότητα -Έλεγχος & Συμμόρφωση -Μηδενική εγκατάσταση -Αξιολόγηση ευπαθειών **Επιπλέον λειτουργικότητα** -Ασφάλεια εφαρμογών για κινητά -Ασφάλεια εφαρμογών Ιστού -Ασφάλεια νέφους -Ασφάλεια container	**Βασική λειτουργικότητα** -Αξιολόγηση έκθεσης (exposure) -Αξιολόγηση της ευπάθειας -Δοκιμή διείσδυσης
---	---
προληπτική, ανιχνευτική	προληπτική, ανιχνευτική
---	---
εφαρμογές, υποδομές και νεφος	οτιδήποτε
οτιδήποτε	οτιδήποτε
---	---
τίποτα δωρεαν	τίποτα δωρεάν
Web gui	Web gui
SecOps Solution	Cymetrics
Azure	Azure
υποστήριξη 24/7, επικοινωνία μέσω email, έγγραφα, βίντεο, εκπαίδευση	επικοινωνία μέσω email, συχνές ερωτήσεις
ASecureCloud Intelligent CSPM	DisruptOps SaaS
SaaS	SaaS
δημόσιο	δημόσιο
assesement	assesement
2 πακέτα , τιμολόγηση με βάση τον αριθμο λογαριασμών στο AWS	τιμολόγηση με βάση τον αριθμό πόρων (ανά 1000 πόρους (resources)) του AWS
Βασική λειτουργικότητα -Ολοκληρωμένη αξιολόγηση ασφαλείας με 100 κανόνες ασφαλείας με εξατομικευμένες συστάσεις -Υποστήριξη για αξιολογήσεις Οργανισμού AWS	**Βασική λειτουργικότητα** -Αξιολογήσεις πολλών λογαριασμών για τον συνεχή εντοπισμό ζητημάτων ασφάλειας και λειτουργίας με βάση τις βέλτιστες πρακτικές

- Αναφορές συμμόρφωσης με τα πρότυπα του κλάδου -Αυτοματοποιημένες καλά σχεδιασμενες κριτικές AWS -Δημιουργία σύνθετων αρχιτεκτονικών χρησιμοποιώντας τη δυναμική γεννήτρια προτύπων **Επιπλέον λειτουργικότητα** -Πρότυπα αποκατάστασης που δημιουργούνται αυτόματα για την αντιμετώπιση ευρημάτων ασφαλείας -Εβδομαδιαίες περιλήψεις email για να παραμένουν ενημερωμένες για το περιβάλλον AWS και τους τελευταίους κινδύνους	-Διατήρηση του ελέγχου σε κλίμακα με την επιβολή αυτοματοποιημένων μέτρων ασφάλειας και λειτουργίας -Συνεχής αξιολόγηση συμμόρφωσης σε πραγματικό χρόνο με βάση τα πρότυπα του κλάδου και του οργανισμού. -Ανάπτυξη πολιτικών ασφαλείας ειδικά για το περιβάλλον που επιτρέπουν τη συνεχή αξιολόγηση και είτε διαδραστικά είτε αυτόματα την αποκατάσταση ζητημάτων ασφάλειας. **Επιπλέον λειτουργικότητα** -Κεντρική ορατότητα πόρων cloud σε όλους τους λογαριασμούς -Αυτόματη πλατφόρμα αποκατάστασης και απόκρισης για την αντιμετώπιση των κρίσιμων προκλήσεων της ασφάλειας του cloud σε κλίμακα.
---	---
προληπτική, ανιχνευτική	προληπτική, ανιχνευτική
---	---
νεφος AWS	νέφος
οτιδήποτε	οτιδήποτε
---	---
μόνιμη δωρεάν έκδοση με περιορισμένες δυνατότητες	14 μέρες δωρεάν
Web gui, Cli	Web gui
ASecureCloud	DisruptOps
AWS	AWS
επικοινωνία με emails, chat, τεκμηρίωση	επικοινωνία με τηλέφωνο, emails

Nessus	**Qualys Cloud Security Assessment**
IaaS	SaaS
δημόσιο	δημόσιο
assesement	assesement
2 πακέτα, τιμολόγηση με βάση τα χαρακτηριστικά, ετήσια, διετής, τριετής διάρκεια	πληροφορίες τιμολόγησης μόνο με επικοινωνία με την εταιρία

Βασική λειτουργικότητα -Απεριόριστες αξιολογήσεις πληροφορικής -Αξιολόγηση διαμόρφωσης -Αναφορές με δυνατότητα διαμόρφωσης -Σάρωση επιφάνειας εξωτερικής επίθεσης -Δυνατότητα προσθήκης τομέων (domains) -Σάρωση υποδομής Cloud -500 προκατασκευασμένες πολιτικές σάρωσης **Επιπλέον λειτουργικότητα** -Ζωντανά αποτελέσματα	**Βασική λειτουργικότητα** -Συνεχής παρακολούθηση ασφαλείας -Διορατικότητα και ιεράρχηση απειλών -Εκατοντάδες καινοτόμοι έλεγχοι ασφαλείας, καθώς και προσαρμοσμένοι έλεγχοι που χρησιμοποιούνται σε αξιολογήσεις ασφαλείας και αποκατάσταση --Αξιολόγηση της υποδομή ως κώδικα -Πλήρης άποψη της στάσης ασφαλείας του cloud -Συνεχείς έλεγχοι ασφαλείας -Συνεχής Παρακολούθηση Συμμόρφωσης -Αποκατάσταση με ένα μόνο κλικ -Αποτροπή εσφαλμένων διαμορφώσεων στο νέφος **Επιπλέον λειτουργικότητα** -Δυνατότητα δημιουργίας αυτοματοποιημένων ροών εργασίας χωρίς κώδικα
99.95% διαθεσιμότητα, για 95.00% έως 99.94% επιστροφή 10% της μηνιαίας συνδρομής, για 90.00% εως 94.99% επιστροφή 15% για <90% επιστροφή 20%	99.5% διαθεσιμότητα
προληπτική, ανιχνευτική	προληπτική, ανιχνευτική
---	---
οτιδήποτε	νέφος
οτιδήποτε	οτιδήποτε
---	---
7 μέρες δωρεάν	30 μέρες δωρεάν
Rest api, Cli, Web gui	Rest api, Cli,Web gui
Tenable	Qualys
AWS, Azure	κανένα
υποστήριξη 24/7,4 πακέτα, επικοινωνία με τηλέφωνο, emails, tickets, chat, κοινοτητα, τεκμηρίωση, βάση γνώσης, συχνές ερωτήσεις, έγγραφα, βίντεο, ενημερώσεις, εκπαίδευση, blog	υποστήριξη 24/7, επικοινωνία με τηλέφωνο, emails, tickets, chat, κοινότητα, συχνές ερωτήσεις, εκπαίδευση, βίντεο, τεκμηρίωση, ενημερώσεις, έγγραφα, forum, blog

Qualys Security Configuration Assessment	**Securecad Enterprise**
SaaS	IaaS

δημόσιο	δημόσιο
assesement	assesement
πληροφορίες τιμολόγησης μόνο με επικοινωνία με την εταιρία	---
Βασική λειτουργικότητα -Ολοκληρωμένη διαχείριση ευπάθειας και συνεχής αξιολόγηση διαμόρφωσης -Κεντρική διαχείριση με ελάχιστο κόστος ανάπτυξης -Τα στοιχεία ελέγχου Qualys SCA είναι βελτιστοποιημένα για απόδοση, επεκτασιμότητα και ακρίβεια. -Διεξαγωγή απομακρυσμένης σάρωσης και αυτόματης ανακάλυψης περιουσιακών στοιχείων -Γρήγορη και ολοκληρωμένη εκτέλεση αξιολογήσεων διαμόρφωσης **Επιπλέον λειτουργικότητα** -Αυτόματος προγραμματισμός αξιολογήσεων και δημιουργία αναφορών	**Βασική λειτουργικότητα** -Αξιολόγηση κινδύνου -Εύρεση τρωτών δομικών σημείων στην αρχιτεκτονική πληροφορικής -Εύρεση κρίσιμων διαδρομών από έναν πιθανό εισβολέα σε ένα περιουσιακό στοιχείο υψηλής αξίας -Εύρεση βασικών στοιχείων στην αρχιτεκτονική που εκμεταλλεύεται ο εισβολέας για να φτάσει σε όλα τα στοιχεία υψηλής αξίας -Προτεινόμενος μετριασμός της έκθεση σε κίνδυνο -Δημιουργία και εξαγωγή αναφορών **Επιπλέον λειτουργικότητα** -Εργαλείο μοντελοποίησης για αυτόματη δημιουργία τμημάτων ή ολοκληρωμένου μοντέλου της αρχιτεκτονικής -Προσομοιώσεις επίθεσης που δεν επηρεάζουν ή συνδέονται με οποιονδήποτε τρόπο με πραγματικά συστήματα κατά τη διάρκεια της προσομοίωσης
99.5% διαθεσιμότητα, 99.99966% ακρίβεια εντοπισμού ευπαθειών	---
προληπτική, ανιχνευτική	προληπτική, ανιχνευτική
---	---
οτιδήποτε	οτιδήποτε
οτιδήποτε	οτιδήποτε
---	---
30 μέρες δωρεάν	τίποτα δωρεάν
Rest api, Cli, Web gui	Rest api, Web gui
Qualys	Foreseeti
κανένα	κανένα
υποστήριξη 24/7, επικοινωνία με τηλέφωνο, emails, tickets, chat, κοινότητα, συχνές ερωτήσεις,	επικοινωνία με τηλέφωνο, emails, τεκμηρίωση, συχνές ερωτήσεις, ενημερώσεις

εκπαίδευση, βίντεο, τεκμηρίωση, ενημερώσεις, έγγραφα, forum, blog	

S4E Shelter - Automated Assessment	**Defendify Assessments & Testing**
SaaS	SaaS
δημόσιο	δημόσιο
assesement	assesement
2 πακέτα, τιμολόγηση με βάση τα χαρακτηριστικά, πληρωμή μηνιαία ή ετήσια	τιμολόγηση με βάση τα υποσυστήματα (modules). Η χρέωση για το υποσύστημα των επιθεωρήσεων και δοκιμών (assessment and testing) είναι 300$/μήνα, πληρωμή μηνιαία ή ετήσια
Βασική λειτουργικότητα -Εργαλεία αυτοματοποιημένης σάρωσης ευπάθειας -Προσδιορισμός και αποκατάσταση κινδύνων κυβερνοασφάλειας -Το αυτοματοποιημένο εργαλείο σάρωσης ευπάθειας χρησιμοποιεί τεχνικές τεχνητής νοημοσύνης και μηχανικής εκμάθησης -Βίντεο και λεπτομερείς αναφορές PDF για κάθε αυτοματοποιημένη σάρωση ασφαλείας -Αυτοματοποιημένη εύρεση και κατηγοριοποίηση τρωτών σημείων **Επιπλέον λειτουργικότητα** -Το αυτοματοποιημένο εργαλείο σάρωσης ευπάθειας χρησιμοποιεί τεχνικές τεχνητής νοημοσύνης και μηχανικής εκμάθησης -Πρόγραμμα ανίχνευσης εφαρμογών ιστού με προσανατολισμό την ασφάλεια για να βρεθεί κάθε πιθανό σημάδι επίθεσης -Ιστορική κατάσταση τρωτών σημείων που βοηθά στη διερεύνηση και τον εντοπισμό ανεπιθύμητων αλλαγών	**Βασική λειτουργικότητα** -Αξιολογήσεις κυβερνοασφάλειας -Δοκιμές διείσδυσης -Σαρώσεις ευπάθειας **Επιπλέον λειτουργικότητα** -Σαρώσεις παραβιασμένων κωδικών πρόσβασης -Σαρώσεις ιστοσελίδων
---	---
προληπτική, ανιχνευτική	προληπτική, ανιχνευτική
---	---
οτιδήποτε	οτιδήποτε

οτιδήποτε	οτιδήποτε
---	---
μόνιμη δωρεάν έκδοση με περιορισμένες δυνατότητες	τίποτα δωρεάν
Web gui	Web gui
Security For Everyone	Defendify
κανένα	κανένα
επικοινωνία με emails, κέντρο βοήθειας, συχνές ερωτήσεις, βάση γνώσης	επικοινωνία με emails

QS solutions Cyber Security Assessment Tool (CSAT)	**ValuRisQ CCPA Automated Compliance for Small and Medium Businesses**
IaaS	SaaS
δημόσιο	δημόσιο
assesement	assesement
τιμολόγηση BYOL	4 πακέτα, τιμολόγηση με βάση τον αριθμό συστημάτων και προμηθευτών που αξιολογούνται
Βασική λειτουργικότητα -Απόκτηση πληροφορίων για την κατάσταση ασφαλείας μέσω αυτοματοποιημένων σαρώσεων και αναλύσεων. -Το CSAT δείχνει ποια τεχνολογικά και διαδικαστικά μέτρα μπορούν να ληφθούν για τη βελτίωση της ασφάλειας -Η CSAT θα εντοπίσει την περιοχή που απαιτεί προσοχή και θα προτείνει τη λήψη μέτρων	**Βασική λειτουργικότητα** -Αυτοματοποίηση Συμμόρφωσης -Ανάλυση Αξιολόγησης Ασφαλείας -Ποσοτικοποίηση κινδύνου -Διαχείριση Κινδύνων Τρίτων -Αξιολόγηση κινδύνου σε πλαίσια όπως NIST CSF, ISO 27001, CIS Top 20, PCI CCPA, NIST, ISO, CIS Top 20, PCI
---	---
προληπτική, ανιχνευτική	προληπτική, ανιχνευτική
---	---
οτιδήποτε	οτιδήποτε
οτιδήποτε	οτιδήποτε
---	στη μέγιστη έκδοση αξιολογούνται έως 200 συστήματα

τίποτα δωρεάν	τίποτα δωρεάν
---	Web gui
QS solutions	RiskQ
Azure	AWS
επικοινωνία με τηλέφωνο, email	επικοινωνία με τηλέφωνο, email

Cyber360	**Accountable**
SaaS	SaaS
δημόσιο	δημόσιο
assesement	assesement
---	2 πακέτα, τιμολόγηση με βάση τα χαρακτηριστικά
Βασική λειτουργικότητα -Αξιολογήσεις κινδύνου κυβερνοασφάλειας -Χρήση κοινών πλαισίων ελέγχου για τη διασφάλιση της συμμόρφωσης με τα πρότυπα βέλτιστων πρακτικών του κλάδου -Προκατασκευασμένα πρότυπα αξιολόγησης και επαναλαμβανόμενα χρονοδιαγράμματα αξιολόγησης για τον εξορθολογισμό της διαδικασίας αξιολόγησης κινδύνου. -Αποτελεσματική Διαχείριση Κινδύνων Κυβερνοασφάλειας και Αποκατάσταση -Πίνακες ελέγχου και αναφορές	**Βασική λειτουργικότητα** -Αξιολογήσεις Κινδύνων και Αξιολογήσεις Επιπτώσεων Προστασίας Δεδομένων -Διαχείριση κινδύνου με τον εντοπισμό και τον μετριασμό των τρωτών σημείων ασφαλείας -Συμμόρφωση με τους παγκόσμιους νόμους περί απορρήτου -Διαχείριση κινδύνων προμηθευτών -Ευαισθητοποίηση για την ασφάλεια και εκπαίδευση HIPAA για τους υπαλλήλους -Αναφορές συμμόρφωσης, ασφάλειας και απορρήτου -Διαχείριση πολιτικών και διαδικασιών χρησιμοποιώντας πρότυπα πολιτικών **Επιπλέον λειτουργικότητα** -Ευαισθητοποίηση για την ασφάλεια και εκπαίδευση HIPAA για τους υπαλλήλους
---	---
προληπτική, ανιχνευτική	προληπτική, ανιχνευτική
---	---
οτιδήποτε	οτιδήποτε
οτιδήποτε	οτιδήποτε
---	στη μέγιστη έκδοση έως 500 αιτήματα πρόσβασης στα δεδομένα (data requests) ανά έτος

τίποτα δωρεάν	μόνιμη δωρεάν έκδοση με περιορισμένες δυνατότητες
Web gui	Web gui
Centrl	Accountable
κανένα	κανένα
επικοινωνία με τηλέφωνο, email ,έγγραφα, τεκμηρίωση, ενημερώσεις, κέντρο βοήθειας, συχνές ερωτήσεις	επικοινωνία με τηλέφωνο, email, chat

Πίνακας αποτίμησης 10 – Προϊόντα Ασφάλειας Ιστού

ΚΡΙΤΗΡΙΑ/ΠΡΟΙΟΝΤΑ	**Reblaze**
α. τρόπος παράδοσης	SaaS, IaaS
β. μοντέλο διάταξης	δημόσιο
γ. κατηγορία υπηρεσιών στην οποία ανήκει	ασφάλεια ιστού
δ. μοντέλο κόστους	τιμολόγηση με βάση τις ώρες χρήσης και το φόρτο εργασίας (IaaS) ή (SaaS) 2 πακέτα και τιμολόγηση με βάση τη μηνιαία κίνηση, αριθμό αιτημάτων και ιστοσελίδων/εφαρμογών, συμβόλαιο μηνιαίο, ετήσιο, διετές, τριετές
ε. μηχανισμοί ασφάλειας που υλοποιούνται	**Βασική λειτουργικότητα** -Τείχος προστασίας εφαρμογών Ιστού επόμενης γενιάς -Ασφάλεια API -Προηγμένη διαχείριση bot -Αυτοματοποιημένη κλιμάκωση πόρων **Επιπλέον λειτουργικότητα** -Ενσωμάτωση με SIEM -Ανάλυση Ανθρώπινης Συμπεριφοράς -Συμμόρφωση -Ενσωμάτωση CDN (Content Distribution Network) -Εξισορρόπηση φορτίου -Αναλύσεις σε πραγματικό χρόνο

στ. μη λειτουργικές εγγυήσεις	καθυστέρησή κίνησης του δικτύου < 1.5ms και καθυστέρηση επεξεργασίας ~0.5ms
ζ. είδος προσφερόμενης προστασίας	προληπτική, ανιχνευτική
η. ιδιότητες ασφάλειας	διαθεσιμότητα
θ. αντικείμενα που προστατεύονται	ιστοσελίδες και διαδικτυακές εφαρμογές
ι. απειλές που αντιμετωπίζονται	DDos και DoS προσπάθειες παραβίασης έγχυση κώδικα και SQL δέσμες ενεργειών μεταξύ τοποθεσιών (cross site scripting) εκμεταλλεύσεις πρωτοκόλλου φόρμας δηλητηρίαση περιόδων σύνδεσης κακόβουλο ωφέλιμο φορτίο κλοπή δεδομένων κλοπή και διάλυση δεδομένων γέμισμα διαπιστευτηρίων (credential stuffing) επιθέσεις λεξικών σαρωτές ευπάθειας κατάληψη λογαριασμού
ια. περιορισμοί	---
ιβ. ύπαρξη δωρεαν εκδόσεων	14 μέρες δωρεάν
ιγ. τρόπος χρήσης προϊόντος	Reblaze technologies
ιδ. εταιρεία που προσφέρει το προϊόν	Web gui, Rest api, Cli
ιε. marketplace(s) όπου προσφέρεται το προϊόν	AWS, GCP, Azure
ιστ. επίπεδο/είδος υποστήριξης για το προϊόν	επικοινωνία με τηλέφωνο, emails, συχνές ερωτήσεις, blog, τεκμηρίωση

Barracuda CloudGen WAF as a service	**Barracuda CloudGen WAF**
SaaS	IaaS
δημόσιο	δημόσιο
ασφάλεια ιστού	ασφάλεια ιστού, ασφάλεια δικτύου, IAM
τιμολόγηση με βάση τον αριθμό εφαρμογών που προστατεύονται, το εύρος ζώνης που χρησιμοποιείται από όλες τις διαμορφωμένες εφαρμογές και τον αριθμό αρχείων που σαρώνονται	τιμολόγηση με βάση το φόρτο εργασίας και τις ώρες χρήσης

Βασική λειτουργικότητα -Ασφάλεια διαδικτυακών εφαρμογών -Ασφάλεια JSON και XML -Ανακάλυψη API -Προστασία από την πλευρά του πελάτη -Προστασία μεταφόρτωσης αρχείων -Προηγμένη προστασία Bot με μηχανική εκμάθηση που βασίζεται σε σύννεφο **Επιπλέον λειτουργικότητα** -Υποστήριξη CAPTCHA -Εικονική διόρθωση (virtual patching) -Έξυπνες υπογραφές -Βασική επιβολή πολιτικής μέχρι το επίπεδο παραμέτρων -Παραμετροποιησιμα σύνολα κανόνων -Μηχανή αυτόματης διαμόρφωσης	**Βασική λειτουργικότητα** -Έλεγχος απόκρισης -Προηγμένη προστασία από απειλές -Έλεγχος μεταφόρτωσης αρχείων -Antivirus για μεταφόρτωση αρχείων -Δρομολόγηση περιεχομένου **Επιπλέον λειτουργικότητα** -Εκφόρτωση SSL -Έλεγχος ταυτότητας και εξουσιοδότηση -Ενοποίηση σαρωτή ευπάθειας -Τείχος προστασίας δικτύου -Προσωρινή αποθήκευση και συμπίεση -Εξισορρόπηση φορτίου -Προσαρμοστικό προφίλ -Κρυπτογράφηση URL
διαθεσιμότητά ροής της κίνησης (traffic flow) 99.999% Για <99.999% έως 99.9% επιστροφή 10% της μηνιαίας συνδρομής, για < 99.9% έως 98% επιστροφή 20% , για <98% έως 97% επιστροφή 30% για <97% έως 96% επιστροφή 40%, για <96% έως επιστροφή 50% διαθεσιμότητά πρόσβασης (Web access) 99.9% για <99.9% έως 98% επιστροφή 10%, για <98% έως 97% επιστροφή 20% για <97% έως 96% επιστροφή 30%, για <96% έως επιστροφή 40%	---
προληπτική, ανιχνευτική	προληπτική, ανιχνευτική
διαθεσιμότητά, ακεραιότητα, εμπιστευτικότητα	διαθεσιμότητά, ακεραιότητα, εμπιστευτικότητα
διαδικτυακές εφαρμογές	διαδικτυακές εφαρμογές, APIs
OWASP Top 10, DDos, επιθέσεις μηδενικής μέρας Έγχυση SQL, XSS, μεταφορτώσεις κακόβουλου λογισμικού Προηγμένα Bots Επιθέσεις ωμής βίας Παραβίαση παραμέτρων	Προστασία από επιθέσεις OWASP & μηδενικής ημέρας Προηγμένη προστασία Bot Προστασία επιθέσεων API Κακόβουλο λογισμικό DDos

Χειρισμός cookie/φόρμας Παραβίαση εφαρμογών Απόκρυψη ιστοσελίδων Πρόληψη απόξεσης Ιστού Προστασία από γέμιση και ψεκασμό διαπιστευτηρίων (credental stuffing and spraying) κατάληψη λογαριασμών Επιθέσεις API για XML και JSON API	Έγχυση SQL, δέσμες ενεργειών μεταξύ τοποθεσιών, παραβίαση cookie ή φορμών Απόκρυψη ιστότοπου και διακομιστή (cloaking) Προστασία από απόξεση ιστού (Web scrapping) Προστασία από κλοπή εξερχόμενων δεδομένων Επιθέσεις API για XML και JSON API
---	στη μέγιστη έκδοση ρυθμοαποδοση έως 750mpbs και έως 14.000 συνδέσεις/αιτήματα http ανά δευτερόλεπτο
30 μέρες δωρεάν	30 μέρες δωρεάν
Barracuda	Barracuda
Web gui, Rest api	Web gui, Rest api, Cli
AWS, Azure	AWS, GCP, Azure
υποστήριξη 24/7 και 3 πακέτα, επικοινωνία με tickets, emails, τηλέφωνο, chat, πύλη (portal), τεχνικά έγγραφα, forum, ενημέρωση για συνδρομές, κοινότητα, κέντρο γνώσης, τεκμηρίωση, λεξικό	υποστήριξη 24/7 και 3 πακέτα, επικοινωνία με tickets, emails, τηλέφωνο, chat, πύλη (portal), τεχνικά έγγραφα, forum, ενημέρωση για συνδρομές, κοινότητα, κέντρο γνώσης, τεκμηρίωση, λεξικό

Qualys Virtual Firewall Appliance	**Fastly next-gen WAF and RASP**
IaaS	SaaS, IaaS
δημόσιο	δημόσιο
ασφάλεια ιστού	ασφάλεια ιστού
τιμολόγηση με με βάση τον αριθμό των διαδικτυακών εφαρμογών και των εικονικών συσκευών.	3 πακέτα και τιμολόγηση με βάση τον αριθμό workspaces (σύνολο κανόνων και ρυθμίσεων που καθορίζεται από το χρήστη για εφαρμογές και διακομιστές προέλευσης) και τον μέσο όρο αιτημάτων ανά δευτερόλεπτο (RPS) που επεξεργάζεται το Next-Gen WAF
Βασική λειτουργικότητα -Ενσωματωμένη ασφάλεια εφαρμογών ιστού -Πλήρης ορατότητα σε λειτουργία τείχους προστασίας -Ισχυροί κανόνες, ευέλικτος έλεγχος -Πρόληψη παραβιάσεων με αποκλεισμό επιθέσεων	**Βασική λειτουργικότητα** -Επόμενης Γενιάς Web Application Firewall -Κρυπτογράφηση TLS -Κανόνες προστασίας για προστασία API και κατάληψη λογαριασμού (ATO) -Περιορισμός κίνησης δικτύου

σε ευπάθειες διακομιστή ιστού -Οπτικοποίηση και αναφορές -Βαθιά ενοποίηση μεταξύ του τείχους προστασίας διαδικτυακών εφαρμογών και της σάρωσης εφαρμογών Ιστού **Επιπλέον λειτουργικότητα** Συμμόρφωση	 **Επιπλέον λειτουργικότητα** -Εικονική διόρθωση -Προσαρμοσμένα σήματα
---	Διαθεσιμότητα 99,9%, για <99,9-99,0 επιστροφή 5% της μηνιαίας συνδρομής, για <99,0%-98,5% επιστροφή 10% για <98,5%-98,0% επιστροφή 15%, για <98,0% επιστροφή 20%
προληπτική, ανιχνευτική	προληπτική, ανιχνευτική
διαθεσιμότητά	διαθεσιμότητά, ακεραιότητα, εμπιστευτικότητα
διαδικτυακές εφαρμογές	διαδικτυακές εφαρμογές και APIs
DDos Δέσμες ενεργειών μεταξύ τοποθεσιών (XSS) Έγχυση SQL Απομακρυσμένη εκτέλεση εντολών XXE Clickjacking και άλλες επιθέσεις που βασίζονται σε πρόγραμμα περιήγησης	 OWASP Top 10 Κατάληψη λογαριασμού Επιθέσεις API Bots DDos
---	---
30 μέρες δωρεάν	δωρεάν δοκιμαστική έκδοση χωρίς να αναφέρονται ημέρες
Qualys	Signal Sciences
Rest api, Cli	Web gui, Rest api, Cli
AWS, GCP, Azure	AWS, GCP, Azure
υποστήριξη 24/7, επικοινωνία με τηλέφωνο, emails, tickets, κοινότητα, blog, τεκμηρίωση, έγγραφα, εκπαιδευτικό υλικό, συχνές ερωτήσεις	3 πακέτα, υποστήριξη απο 9/5 εως 24/7, επικοινωνία με τηλέφωνο, emails, chat, τεκμηρίωση, συχνές ερωτήσεις, πύλη υποστήριξης, κοινότητα, βάση γνώσης, κανάλι στο slack, κέντρο βοήθειας, έγγραφα, ενημερώσεις

Penta Security - WAPPLES SA (WAF)	**Akamai Web Application Protector**

IaaS	SaaS
ιδιωτικό, δημόσιο	δημόσιο
ασφάλεια ιστού, DLP	ασφάλεια ιστού
4 πακέτα, τιμολόγηση με βάση το φόρτο εργασίας και τις ώρες χρήσης, χρέωση ανά ώρα ή ανά έτος	3 πακέτα, τιμολόγηση με βάση τον αριθμό των domains και του μηναίου όγκου δεδομένων/κίνησης
Βασική λειτουργικότητα -Ευφυής μηχανή ανάλυσης λογικής για τον αποκλεισμό άγνωστων επιθέσεων -Επεξεργασία επισκεψιμότητας Ιστού -Έλεγχος επικύρωσης XML -Αποτροπή διαρροής ευαίσθητων δεδομένων -Επεξεργασία κρυπτογραφημένης κίνησης HTTP (HTTPS). -Προσαρμόσιμες αναφορές **Επιπλέον λειτουργικότητα** -Ασφαλής διαχείριση κλειδιών SSL -Έλεγχος έκδοσης SSL -Εξισορρόπηση φορτίου -Εικονική ενημέρωση κώδικα και ενημερώσεις ασφαλείας -Προσαρμόσιμο σύνολο κανόνων για ευκολία διαχείρισης -Ισχυρός και βολικός έλεγχος ταυτότητας για πρόσβαση GUI μέσω AD/LDAP και MOTP -Λειτουργία οπτικοποίησης για ταμπλό σε πραγματικό χρόνο -Βελτιωμένη διαχείριση αρχείων καταγραφής -Αυτόματες κρίσιμες ειδοποιήσεις και ειδοποιήσεις μέσω email -Ενοποίηση με λύσεις SIEM	**Βασική λειτουργικότητα** -Τείχος προστασίας εφαρμογών Web με ένα αυτοματοποιημένο σύνολο κανόνων -Προσαρμογή για χαμηλά ψευδώς θετικά αποτελέσματα. **Επιπλέον λειτουργικότητα** -Αυτοματοποιημένες ενημερώσεις -Εικονικές ενημερώσεις κώδικα -Πιστοποιητικό TLS ή SSL -Μετριασμός προβλημάτων δικτύου και βελτίωση της απόδοσης και της διαθεσιμότητας. -Δυνατότητες ενσωματωμένες στο CDN του Akamai, όπως προσωρινή αποθήκευση, προηγμένες δυνατότητες εκφόρτωσης και βελτιστοποίηση TCP
---	διαθεσιμότητα 100%
προληπτική, ανιχνευτική	προληπτική, ανιχνευτική
διαθεσιμότητα, ακεραιότητα, εμπιστευτικότητα	διαθεσιμότητα
διαδικτυακές εφαρμογές, , APIs	διαδικτυακές εφαρμογές και APIs
OWASP Top 10 Έγχυση SQL/NoSQL/LDAP/Xpath Έγχυση από την πλευρά του διακομιστή	Επιθέσεις DDos και διαδικτυακών εφαρμογών SQL injection, XSS, RFI και άλλοι τύποι απειλών επιπέδου εφαρμογής

DDos/DoS Δακτυλική εκτύπωση CAPTCHA και Browser Δέσμες ενεργειών μεταξύ τοποθεσιών (cross site scripting) Cross Site Request Forgery Path Traversal προστασία απόξεσης ιστού (web scrapping) Απομακρυσμένη/Τοπική συμπερίληψη αρχείων Χειρισμός παραμέτρων Δηλητηριασμος Cookies Μεταφόρτωση κακόβουλου αρχείου Παραμόρφωση Ιστοσελίδας Ανίχνευση Bots Προστασία από επιθέσεις μηδενικής ημέρας Επιθέσεις ωμής βίας Αποκλεισμός κόμβων Tor	
στη μέγιστη έκδοση 1gbps ρυθμοαποδοση	---
30 μέρες δωρεάν	30 μέρες δωρεάν
Penta Security	Akamai Technologies
Web gui, Rest api, Cli	Cli, Rest api
Azure, AWS	Azure
επικοινωνία με email, τηλέφωνο	2 πακέτα, υποστήριξη 24/7 επικοινωνία με τηλέφωνο, email, tickets, κανάλι slack, συχνές ερωτήσεις, κοινότητα, κέντρο βοήθειας, βάση γνώσης, τεκμηρίωση, Blog, εκπαίδευση

WebFRONT-KS	**Haltdos WAF**
IaaS	IaaS
ιδιωτικό, δημόσιο	δημόσιο
ασφάλεια ιστού	ασφάλεια ιστού, DLP
4 πακέτα, τιμολόγηση με βάση το φόρτο εργασίας και τις ώρες χρήσης	3 πακέτα, τιμολόγηση με βάση με βάση τα χαρακτηριστικά, το φόρτο εργασίας και τις ώρες χρήσης
Βασική λειτουργικότητα -Επεξεργασία Κυκλοφορίας -Ανίχνευση βάσει συμπεριφοράς χρήστη για διάκριση των κανονικών χρηστών από έναν	**Βασική λειτουργικότητα** -Τείχος προστασίας εφαρμογών Ιστού -Αποκλεισμός φήμης Geo / IP -Παρακολούθηση Κυκλοφορίας

αυξανόμενο αριθμό bots -Εντοπισμός, ανάπτυξη και ενημέρωση των προφίλ συμπεριφοράς των χρηστών. -Έξυπνη ανίχνευση με εύρεση των χαρακτηριστικών παραλλαγής/νέας επίθεσης χωρίς υπογραφή -Γρήγορη ανίχνευση με τον εντοπισμό γνωστών προτύπων επίθεσης **Επιπλέον λειτουργικότητα** -Κατοπτρισμός αποκρυπτογράφησης SSL -Εξισορρόπησης φορτίου -Ανάλυση ασφάλειας και διαχείριση στατιστικών	-Αναφορές **Επιπλέον λειτουργικότητα** -RUM Metrics -Ενσωμάτωση SIEM -Αρχεία καταγραφής -Πρόληψη διαρροών δεδομένων -Εικονική διόρθωση -Εξισορρόπηση φορτίου -Υπογραφές Κοινότητας -Προηγμένες υπογραφές
---	διαθεσιμότητα 99.9%. Το σύστημα ποινών χρησιμοποιεί έναν σύνθετο μαθηματικό τύπο
προληπτική, ανιχνευτική	προληπτική, ανιχνευτική
διαθεσιμότητα, ακεραιότητα, εμπιστευτικότητα	διαθεσιμότητα, ακεραιότητα, εμπιστευτικότητα
διαδικτυακές εφαρμογές και APIs	διαδικτυακές εφαρμογές και APIs
Owasp top 10,DDos, επιθέσεις API, Bots, Απόκρυψη κωδικού σφάλματος, URL, δεδομένων διακομιστή και κώδικα Διαρροή προσωπικών πληροφοριών (εκροή) Γέμισμα διαπιστευτηρίων Πρόληψη παραποίησης Ιστού Υπερχείλιση buffer Shellcode Προστασία cookie Προγράμματα διαδικτυακής επίθεσης Έγχυση SQL Δέσμες ενεργειών μεταξύ τοποθεσιών (XSS) Εισροή προσωπικών πληροφοριών	DDos Επιθέσεις μηδενικής μέρας Προστασία Bot Απόξεση ιστότοπου Επιθέσεις Ωμής βίας Owasp top 10, κακόβουλο λογισμικό, XSS, SQL και άλλες απειλές που βασίζονται στο διαδίκτυο
στη μεγιστη εκδοση 6gbps ρυθμοαποδοση	---
τίποτα δωρεάν	δωρεάν δοκιμαστική έκδοση χωρίς να αναφέρονται ημέρες
Piolink	Halt Dos
Rest api	Rest api, Cli
Azure, AWS	Azure

υποστήριξη 24/7, επικοινωνία με τηλέφωνο, email, κέντρο βοήθειας	υποστήριξη 9/5 έως 24/7, επικοινωνία με τηλέφωνο, email

Big WAF	**Edgenexus Web Application Firewall (WAF)**
SaaS	IaaS
δημόσιο	δημόσιο
ασφάλεια ιστού	ασφάλεια ιστού, DLP
3 πακέτα και τιμολόγηση με βάση τον αριθμό αιτημάτων (defense requests) ανά μήνα, μηνιαία, ετήσια, διετής, τριετής πληρωμή	τιμολόγηση με βάση το φόρτο εργασίας και τις ώρες χρήσης
Βασική λειτουργικότητα -Προστασία από επιθέσεις διαδικτυακών εφαρμογών -Νοημοσύνη απειλών επίθεσης -Προσαρμοσμένη Στρατηγική Προστασίας -Υψηλή αξιοπιστία και υψηλή απόδοση **Επιπλέον λειτουργικότητα** -Ειδοποιήσεις παρακολούθησης επιθέσεων -Οπτικοποίηση δεδομένων προστασίας	**Βασική λειτουργικότητα** -Εξάλειψη ευπαθειών εφαρμογών -Ικανοποιούνται οι απαιτήσεις του τείχους προστασίας εφαρμογών PCI-DSS και OWASP -Μηχανή κανόνων που παρέχει λευκή και μαύρη λίστα -Ολοκληρωμένη καταγραφή και αναφορές **Επιπλέον λειτουργικότητα** -Υποστήριξη πολλαπλών εφαρμογών ή την εφαρμογή αρχιτεκτονικής ασφαλείας πολλαπλών επιπέδων -Χρήση τεχνολογίας κοντέινερ για την απομόνωση κάθε παρουσίας τείχους προστασίας εφαρμογής
---	---
προληπτική, ανιχνευτική	προληπτική, ανιχνευτική
διαθεσιμότητα, ακεραιότητα, εμπιστευτικότητα	διαθεσιμότητα
διαδικτυακές εφαρμογές και APIs	διαδικτυακές εφαρμογές
Επιθέσεις OWASP Έγχυση SQL Δέσμες ενεργειών μεταξύ τοποθεσιών, Μεταφόρτωση Webshell, Ευπάθειες αποσειριοποίησης, Επιθέσεις XXE, Επιθέσεις 0 ημερών,	Δέσμες ενεργειών μεταξύ τοποθεσιών (XSS) Έγχυση SQL Session Hijacking Πρόληψη απώλειας δεδομένων Τοπική συμπερίληψη αρχείων (LFI) Απομακρυσμένη συμπερίληψη αρχείων (RFI) Απομακρυσμένη εκτέλεση κώδικα (RCE) PHP Code Injection

Δούρειοι ίπποι ιστότοπου και άλλες κοινές επιθέσεις εφαρμογών Ιστού.	Παραβιάσεις πρωτοκόλλου HTTP HTTPoxy Shellshock Διόρθωση συνεδρίας Ανίχνευση σαρωτή Διαρροές μεταδεδομένων/Σφάλματος
στη μέγιστη έκδοση έως 300 εκατομμύρια αιτήματα ανά μήνα	---
τίποτα δωρεάν	30 μέρες δωρεάν
Wangsu Science and Technology	Edgenexus
Web gui	Rest api, Web gui
AWS	AWS, Azure
5 πακέτα, (4 24/7 και 1 9.00-24.00) επικοινωνία με τηλέφωνο, mail, tickets, chat ,κέντρο αυτοβοήθειας, τεκμηρίωση	επικοινωνία με τηλέφωνο, emails, τεκμηρίωση, forum, συχνές ερωτήσεις, κέντρο βοήθειας, έγγραφα, blog, βίντεο

MONITORAPP AIWAF-VE for Azure	**UBIKA WAAP Cloud**
IaaS	IaaS
δημόσιο	δημόσιο
ασφάλεια ιστού, DLP	ασφάλεια ιστού
5 πακέτα, τιμολόγηση με βάση το φόρτο εργασίας και τις ώρες χρήσης	τιμολόγηση με βάση το φόρτο εργασίας και τις ώρες χρήσης
Βασική λειτουργικότητα -Παρακολούθηση συστήματος -Διάφορες λειτουργίες διαμόρφωσης δικτύου -Μετάδοση αποκρυπτογραφημένης κίνησης HTTPS με λύση ασφαλείας τρίτου μέρους -Πλατφόρμα πληροφοριών απειλών -Πλήρης υποστήριξη HTTP/2 -Βελτιστοποίηση ασφάλειας -Βελτιστοποίηση κυκλοφορίας -Πολυεπίπεδη άμυνα των επιθέσεων Ιστού **Επιπλέον λειτουργικότητα** -Ενημέρωση σε πραγματικό χρόνο και ειδοποίηση τρωτών σημείων έκτακτης ανάγκης	**Βασική λειτουργικότητα** -Προληπτική προστασία έναντι γνωστών και άγνωστων απειλών -Τυπική ασφάλεια βασισμένη σε γενικά πρότυπα και μηχανισμός βαθμολόγησης που συμπληρώνεται από προηγμένους κινητήρες ασφαλείας για πιο λεπτομερή και ακριβή ανίχνευση -Βαθμολόγηση φήμης χρήστη για την αποτροπή διαδικτυακής απάτης και κλοπής που αποτρέπει τους παράνομους χρήστες -Τείχος προστασίας JSON και ανάλυση και επικύρωση XML -Απρόσκοπτη ενσωμάτωση με σαρωτές αρχείων τρίτων κατασκευαστών

-Μείωση της επισκεψιμοτητας και του χρόνου απόκρισης μέσω της προσωρινής αποθήκευσης ιστού -Μηχανική Μάθηση -Προσαρμοστικό προφίλ -Ανάλυση αρχείων καταγραφής -Ρυθμίσεις πολιτικής	-Γεωγραφικός εντοπισμός IP -Η ισχυρή ανάλυση κορμού επιτρέπει τη διερεύνηση ενός συγκεκριμένου ζητήματος ασφαλείας -Μηχανισμοί ασφαλείας σε πραγματικό χρόνο **Επιπλέον λειτουργικότητα** -Εισαγωγή / Εξαγωγή OpenAPI για ασφάλεια API και DevOps -Επανάληψη καταγραφής για δοκιμές πολιτικής και foresincs -Δυνατότητα υπογραφής, επαλήθευσης υπογραφής, κρυπτογράφησης, αποκρυπτογράφησης, τροποποίησης οποιουδήποτε μέρους ή οντότητας αιτήματος ή απάντησης -Εκμάθηση εφαρμογών για ισχυρότερη προστασία και βελτιωμένη απόδοση κατά τη διάρκεια του κύκλου ανάπτυξης λογισμικού
---	---
προληπτική, ανιχνευτική	προληπτική, ανιχνευτική
διαθεσιμότητα, ακεραιότητα, εμπιστευτικότητα	διαθεσιμότητα, ακεραιότητα, εμπιστευτικότητα
διαδικτυακές εφαρμογές και APIs	διαδικτυακές εφαρμογές και APIs
Ανίχνευση μόλυνσης από κακόβουλο λογισμικό Έγχυση SQL XSS/CSRF Ευάλωτη πρόσβαση στη σελίδα Buffer-Υπερχείλιση Πρόσβαση σε κακόβουλο αρχείο Ανίχνευση Spambot/Scanner/Proxy Κωδικοποίηση- Μεταφόρτωση πρόσβασης σε κακόβουλο αρχείο Έγχυση εντολών Cookies παραποιημένα Ευπάθειες κεφαλίδας Πρόσβαση στο σύστημα αρχείων Ευπάθεια διακομιστή Ιστού/Εφαρμογής Σκουλήκια/Ιοί Πρόσβαση καταλόγου Επιθέσεις DDos, ευπάθειες OWASP 10, ευπάθειες NIS 8	Dos Owasp top 10 Bots

στη μέγιστη έκδοση 2.5gbps ρυθμοαποδοση	υποστηρίζονται εως 100 χιλιάδες συναλλαγές (transactions) ανά δευτερόλεπτο
30 μέρες δωρεάν	τίποτα δωρεάν
Monitorapp	UBIKA
Rest api, Web gui	Rest api
Azure	AWS
επικοινωνία με tickets, email	υποστήριξη 24/7, επικοινωνία με τηλέφωνο, email, tickets, τεκμηρίωση, ενημερώσεις