ΠΑΝΕΠΙΣΤΗΜΙΟ ΑΙΓΑΙΟΥ

ΠΟΛΥΤΕΧΝΙΚΗ ΣΧΟΛΗ

ΤΜΗΜΑ ΜΗΧΑΝΙΚΩΝ ΠΛΗΡΟΦΟΡΙΑΚΩΝ ΚΑΙ ΕΠΙΚΟΙΝΩΝΙΑΚΩΝ ΣΥΣΤΗΜΑΤΩΝ

ΠΡΟΓΡΑΜΜΑ ΜΕΤΑΠΤΥΧΙΑΚΩΝ ΣΠΟΥΔΩΝ

Ασφάλεια Πληροφοριακών και Επικοινωνιακών Συστημάτων

Πόσο ασφαλές είναι το Υπολογιστικό Νέφος

ΔΙΠΛΩΜΑΤΙΚΗ ΕΡΓΑΣΙΑ

των

Δήμητρα Γιαγτζή, Παναγιώτη Λιαρομάτη

Επιβλέπων: Κρητικός Κυριάκος

Μέλη εξεταστικής επιτροπής: Κοκολάκης Σπύρος, Σκούτας Δημήτριος

Σάμος, Αύγουστος, 2023

Η σελίδα αυτή είναι σκόπιμα λευκή.

Πρόλογος και ευχαριστίες

Η παρούσα διπλωματική εργασία πραγματοποιήθηκε στο Πανεπιστήμιο Αιγαίου, στο τμήμα Μηχανικών Πληροφοριακών και Επικοινωνιακών Συστημάτων και συγκεκριμένα στο μεταπτυχιακό πρόγραμμα Ασφάλεια Πληροφοριακών και Επικοινωνιακών συστημάτων, κατά το έτος 2023.
Η ολοκλήρωση της διπλωματικής αυτής εργασίας θα ήταν αδύνατη χωρίς την πολύτιμη υποστήριξη του καθηγητή μας, Αναπλ. Καθηγητή Τμήματος Μηχανικών Πληροφοριακών και Επικοινωνιακών Συστημάτων, Κυριάκου Κρητικού. Του εκφράζουμε ένα βαθύ ευχαριστώ για όλη τη βοήθεια που μας προσέφερε.

Η σελίδα αυτή είναι σκόπιμα λευκή.

Πίνακας περιεχομένων

Λίστα Σχημάτων

Λίστα Πινάκων

Ακρωνύμια

Ακρωνύμιο	**Σημασία (στα Αγγλικά)**	**Σημασία (στα Ελληνικά)**
AES	Advanced Encryption Standard	Προηγμένο πρότυπο κρυπτογράφησης
API	Application Programming Interface	Διεπαφή προγραμματισμού εφαρμογών
CCTV	Closed-Circuit Television	Κλειστό κύκλωμα τηλεόρασης
CPU	Central Processing Unit	Κεντρική μονάδα επεξεργασίας
CSA	Cloud Security Alliance	
CSP	Cloud Service Provider	Πάροχοι υπηρεσιών υπολογιστικού νέφους
DAST	Dynamic Application Security Testing	Δοκιμή δυναμικής ασφάλειας εφαρμογών
DDoS	Distributed Denial-of-Service	Κατανεμημένη άρνηση παροχής υπηρεσιών
DPDP	Dynamic Provable Data Possession	Δυναμική αποδεδειγμένη κατοχή δεδομένων
EC2	Amazon Elastic Compute Cloud	Ελαστικό υπολογιστικό νέφος της Amazon
FaaS	Forensic-as-a-service	Ιατροδικαστική ως υπηρεσία
FbD	Forensic by-design	Ιατροδικαστική από σχεδιασμό
GDPR	General Data Protection Regulation	Γενικός Κανονισμός Προστασίας Δεδομένων
HTTPS	Hypertext Transfer Protocol Secure	Ασφαλές πρωτόκολλο μεταφοράς υπερκειμένου
IAST	Interactive Application Security Testing	Διαδραστική δοκιμή ασφάλειας εφαρμογών
ICMP	Internet Control Message Protocol	Πρωτόκολλο μηνυμάτων ελέγχου Διαδικτύου
IDS	Intrusion Detection System	Σύστημα ανίχνευσης εισβολής
IP	Internet Protocol	Πρωτόκολλο διαδικτύου
IaaS	Infrastructure as-a-service	Υποδομή ως υπηρεσία
JSON	JavaScript Object Notation	Σημειογραφία αντικειμένου JavaScript
LAN	Local Area Network	Τοπικό δίκτυο

MAC	Media Access Control	Έλεγχος πρόσβασης πολυμέσων
NIST	National Institute of Standards and Technology	Εθνικό Ινστιτούτο Προτύπων και Τεχνολογίας
OS / ΛΣ	Operating System	Λειτουργικό Σύστημα
PDP	Provable Data Possession	Ευαπόδεικτη κατοχή δεδομένων
POR	Proof of Retrievability	Απόδειξη δυνατότητας ανάκτησης
PaaS	Platform-as-a-Service	Πλατφόρμα ως υπηρεσία
RDA	Remote Data Audit	Απομακρυσμένος έλεγχος δεδομένων
SAML	Security Assertion Markup Language	Γλώσσα σήμανσης διαβεβαίωσης ασφαλείας
SAST	Static Application Security Testing	Στατική δοκιμή ασφάλειας εφαρμογών
SDN	Software-Defined Networking	Δικτύωση που καθορίζεται από λογισμικό
SLA	Service-Level Agreement	Συμφωνία επιπέδου υπηρεσιών
SLaaS	Security logging-as-a-service	Καταγραφή ασφαλείας ως υπηρεσία
SYN	Synchronize	Συγχρονίζω
SaaS	Software-as-a-Service	Λογισμικό ως υπηρεσία
TCP	Transmission Control Protocol	Πρωτόκολλο Ελέγχου Μετάδοσης
TLS	Transport Layer Security	Ασφάλεια επιπέδου μεταφοράς
UDP	User Datagram Protocol	Πρωτόκολλο Δεδομένων Χρήστη
VM	Virtual Machine	Εικονική μηχανή
VMM	Virtual Machine Manager	Διαχειριστής εικονικής μηχανής
vTPM	virtual Trusted Platform Module	Εικονική μονάδα αξιόπιστης πλατφόρμας
WSDL	Web Service Description Language	Γλώσσα περιγραφής υπηρεσιών Ιστού
XACML	Extensible Access Control Markup Language	Επεκτάσιμη γλώσσα σήμανσης ελέγχου πρόσβασης
XML	Extensible Markup Language	Επεκτάσιμη γλώσσα σήμανσης

Περίληψη

Η παρούσα διπλωματική εργασία επικεντρώνεται στην εξέταση των διαφόρων πτυχών ασφάλειας του υπολογιστικού νέφους, συμπεριλαμβάνοντας απειλές, επιθέσεις, στρατηγικές μετριασμού και μελέτες περιπτώσεων, ενώ παρέχει συγκριτικές αναλύσεις του υπολογιστικού νέφους και των τοπικών περιβαλλόντων καθώς και των παρόχων υπολογιστικού νέφους Amazon AWS, Microsoft Azure και Google Cloud. Οι πρωταρχικοί στόχοι αυτής της έρευνας είναι να παράσχει πληροφορίες σχετικά με τις απειλές και τις επιθέσεις που αντιμετωπίζουν τα συστήματα που βασίζονται στο νέφος, να προσφέρει πρακτικές στρατηγικές για τον μετριασμό των κινδύνων, να παρουσιάσει μελέτες περιπτώσεων από τον πραγματικό κόσμο για να καταδείξει τις συνέπειες των παραβιάσεων ασφάλειας, να πραγματοποιήσει συγκριτικές αναλύσεις μεταξύ συστημάτων που βασίζονται στο νέφος και συστημάτων που φιλοξενούνται από τον ίδιο τον οργανισμό και να αξιολογήσει τις δυνατότητες ασφαλείας των κορυφαίων παρόχων υπηρεσιών νέφους.

Η έρευνα ξεκινά με τον εντοπισμό και την ανάλυση των σημαντικότερων απειλών ασφάλειας και των φορέων επίθεσης που στοχεύουν σε συστήματα που βασίζονται στο υπολογιστικό νέφος. Με την κατανόηση της φύσης και του αντίκτυπου αυτών των απειλών, οι καταναλωτές μπορούν να εφαρμόσουν προληπτικά μέτρα για την προστασία των περιουσιακών τους στοιχείων. Διερευνώνται στρατηγικές μετριασμού και βέλτιστες πρακτικές για την ασφάλεια του υπολογιστικού νέφους, ώστε να παρέχονται αποτελεσματικά αντίμετρα κατά των πιθανών κινδύνων.

Παρουσιάζονται μελέτες περιπτώσεων από τον πραγματικό κόσμο για να καταδειχθούν οι συνέπειες των παραβιάσεων της ασφάλειας σε περιβάλλοντα νέφους. Αυτές οι μελέτες προσφέρουν πολύτιμες πληροφορίες σχετικά με τα τρωτά σημεία που μπορεί να αντιμετωπίσουν οι οργανισμοί και υπογραμμίζουν τη σημασία της εφαρμογής ισχυρών μέτρων ασφαλείας για την προστασία κρίσιμων περιουσιακών στοιχείων.

Για να εκτιμηθούν τα πλεονεκτήματα και οι αδυναμίες ασφάλειας των αρχιτεκτονικών που βασίζονται στο νέφος σε σύγκριση με τα αυτοδιαχειριζόμενα, επιτόπια συστήματα, πραγματοποιείται μια ολοκληρωμένη σύγκριση ασφάλειας. Αναλύοντας τις θεμελιώδεις διαφορές στους μηχανισμούς ασφαλείας και τα μέτρα ελέγχου, οι καταναλωτές μπορούν να λάβουν τεκμηριωμένες αποφάσεις σχετικά με την καταλληλότητα κάθε προσέγγισης για τις συγκεκριμένες απαιτήσεις τους.

Επιπλέον, η διατριβή πραγματοποιεί μια σύγκριση με γνώμονα την ασφάλεια μεταξύ τριών διακεκριμένων παρόχων υπηρεσιών νέφους: Amazon AWS, Microsoft Azure και Google Cloud. Η ανάλυση αυτή εξετάζει τα χαρακτηριστικά ασφαλείας τους, τις πιστοποιήσεις, τα πρότυπα συμμόρφωσης και τις δυνατότητες ασφάλειας που παρέχουν. Με την αξιολόγηση αυτών των παραγόντων, οι καταναλωτές μπορούν να λάβουν τεκμηριωμένες αποφάσεις σχετικά με την επιλογή ενός παρόχου υπηρεσιών υπολογιστικού νέφους που ευθυγραμμίζεται με τις ανάγκες ασφαλείας τους.

Λέξεις Κλειδιά: *ασφάλεια, υπολογιστικό νέφος, ευπάθεια, απειλή, μέτρα ασφαλείας*

Abstract

This thesis focuses on examining the security aspects of cloud computing, including threats, attacks, mitigation strategies, case studies while it supplies a comparative analyses between cloud computing and on-premises environments as well as between three major cloud providers: Amazon AWS, Microsoft azure and Google cloud. The primary objectives of this research are to provide insight into the threats and attacks facing cloud-based systems, offer practical strategies for mitigating risks, present real-world case studies to illustrate the consequences of security breaches, conduct comparative analyses between cloud-based systems and self-hosted systems, and evaluate the security capabilities of the leading cloud service providers.

The research starts with the identification and analysis of the major security threats and attack vectors targeting cloud-based systems. By understanding the nature and impact of these threats, consumers can implement proactive measures to protect their assets. Mitigation strategies and best practices for cloud security are being explored to provide effective countermeasures against potential risks.

Real-world case studies are presented to demonstrate the consequences of security breaches in cloud environments. These studies provide valuable insights into the vulnerabilities that organizations may face and highlight the importance of implementing strong security measures to protect critical assets.

To assess the security strengths and weaknesses of cloud-based architectures compared to self-managed, on-premise systems, a comprehensive security comparison is conducted. By analysing the fundamental differences in security mechanisms and control measures, consumers can make informed decisions about the suitability of each approach for their specific requirements.

In addition, the thesis performs a security comparison between three prominent cloud service providers; Amazon AWS, Microsoft Azure and Google Cloud. This analysis examines their security features, certifications, compliance standards and the security capabilities that they provide. By evaluating these factors, consumers can make informed decisions about choosing a cloud service provider that best aligns with their security needs.

Keywords: *security, cloud computing, vulnerability, threat, security measures*

1. Εισαγωγή

1.1 Το υπολογιστικό νέφος

Στο σημερινό ταχέως εξελισσόμενο τεχνολογικό τοπίο, η υιοθέτηση του υπολογιστικού νέφους έχει γίνει όλο και πιο διαδεδομένη σε διάφορους κλάδους. Το υπολογιστικό νέφος είναι η χρήση υπολογιστικών πόρων (υλικό και λογισμικό) που διαμοιράζονται ως υπηρεσίες μέσω του Διαδικτύου [82] και προσφέρει επεκτασιμότητα, ευελιξία και αποδοτικότητα κόστους, επιτρέποντας στους καταναλωτές να αποθηκεύουν, να επεξεργάζονται και να έχουν πρόσβαση στα δεδομένα και τις εφαρμογές τους με ευκολία. Ωστόσο, μαζί με τα οφέλη του υπολογιστικού νέφους έρχονται και οι εγγενείς προκλήσεις και κίνδυνοι ασφαλείας που πρέπει να αντιμετωπιστούν προσεκτικά για να διασφαλιστεί η εμπιστευτικότητα, η ακεραιότητα και η διαθεσιμότητα των κρίσιμων περιουσιακών στοιχείων. [6]

1.2 Αντικείμενο διπλωματικής

Η παρούσα διπλωματική εργασία έχει ως στόχο να εμβαθύνει στη σφαίρα της ασφάλειας του υπολογιστικού νέφους, διερευνώντας τις διάφορες απειλές και επιθέσεις που ενέχουν σημαντικούς κινδύνους για τα συστήματα που βασίζονται στο υπολογιστικό νέφος και τα μέτρα μετριασμού που μπορούν να χρησιμοποιηθούν για την προστασία από αυτές. Επιπλέον, η παρούσα έρευνα θα παρουσιάσει μελέτες περιπτώσεων που αναδεικνύουν περιστατικά του πραγματικού κόσμου, ώστε να παρέχει πρακτικές γνώσεις σχετικά με τις συνέπειες των παραβιάσεων της ασφάλειας σε περιβάλλοντα νέφους. Η εξέλιξη του υπολογιστικού νέφους έχει φέρει επανάσταση στον τρόπο με τον οποίο οι οργανισμοί διαχειρίζονται τα δεδομένα και τις εφαρμογές τους. Ωστόσο, η χρήση των υπηρεσιών του υπολογιστικού νέφους επιφέρει πολυάριθμες προκλήσεις ασφαλείας που απαιτούν επιμελή προσοχή. Με την ολοκληρωμένη ανάλυση των απειλών, των επιθέσεων, των στρατηγικών μετριασμού, των μελετών περιπτώσεων και τη διενέργεια συγκριτικών αξιολογήσεων ασφαλείας, η παρούσα διπλωματική έχει ως στόχο να μελετήσει το σύνθετο τοπίο της ασφάλειας του υπολογιστικού νέφους και να παράσχει πολύτιμη καθοδήγηση στους οργανισμούς που περιηγούνται σε αυτόν τον δυναμικό και διαρκώς μεταβαλλόμενο τομέα.

Επιπρόσθετα, διεξάγεται μια ολοκληρωμένη σύγκριση ασφάλειας μεταξύ αρχιτεκτονικών που βασίζονται στο νέφος και αυτοδιαχειριζόμενων, επιτόπιων συστημάτων για να αξιολογηθούν τα πλεονεκτήματα και οι αδυναμίες κάθε προσέγγισης από άποψη ασφάλειας. Αναλύοντας τις θεμελιώδεις διαφορές στους μηχανισμούς ασφαλείας και τα μέτρα ελέγχου, μπορούμε να αποκτήσουμε μια βαθύτερη κατανόηση των μοναδικών προκλήσεων και πλεονεκτημάτων που σχετίζονται με την υιοθέτηση του νέφους.

Τέλος, η παρούσα έρευνα πραγματοποιεί μια λεπτομερή σύγκριση ασφάλειας μεταξύ τριών από τους πιο σημαντικούς παρόχους υπηρεσιών υπολογιστικού νέφους: Amazon AWS, Microsoft Azure και Google Cloud. Με την εξέταση των αντίστοιχων χαρακτηριστικών ασφαλείας, των πιστοποιήσεων, των προτύπων συμμόρφωσης και των πλαισίων αντιμετώπισης περιστατικών, η μελέτη αυτή παρέχει μια πολύτιμη αξιολόγηση των δυνατοτήτων ασφαλείας που προσφέρουν αυτοί οι κορυφαίοι πάροχοι

του κλάδου και μπορεί να βοηθήσει τους οργανισμούς να επιλέξουν εκείνο τον πάροχο που ικανοποιεί περισσότερο τις ανάγκες ασφάλειάς τους.
Η παρούσα διπλωματική εργασία αποσκοπεί να συμβάλει στο υπάρχον σώμα γνώσεων γύρω από την ασφάλεια του νέφους και να παράσχει ιδέες και συστάσεις για οργανισμούς που επιδιώκουν να ενισχύσουν την κατάσταση ασφαλείας των αναπτύξεων του νέφους τους.

1.3 Δομή της διπλωματικής

Βασικές έννοιες που έχουν άμεση σύνδεση με το αντικείμενο της διπλωματικής εργασίας παρουσιάζονται στο Κεφάλαιο 2. Το Κεφάλαιο 3 συζητά θέματα που αφορούν κενά ασφαλείας, ρίσκα και επιθέσεις στο υπολογιστικό νέφος. Στο Κεφάλαιο 4 παρουσιάζονται μηχανισμοί ελέγχου και μεθόδοι ασφάλειας που εφαρμόζονται σε περιβάλλοντα του υπολογιστικού νέφους. Στο Κεφάλαιο 5 πραγματοποιείται σύγκριση μεταξύ επιτόπιων περιβαλλόντων και του υπολογιστικού νέφους όπως επίσης και σύγκριση διαφορετικών παρόχων υπολογιστικού νέφους ως προς την ασφάλειά τους. Τέλος, στο Κεφάλαιο 6 παρουσιάζονται συγκεντρωτικά κάποια συμπεράσματα που προκύπτουν από την τρέχουσα διπλωματική εργασία.

2. Υπόβαθρο

2.1 Βασική ορολογία

2.1.1 Τι ειναι ευπάθεια

Σύμφωνα με την ταξινόμηση κινδύνου του Open Group [83], η ευπάθεια είναι η πιθανότητα ένα αγαθό (asset) να είναι ανίκανο να αντισταθεί στις ενέργειες ενός πράκτορα απειλής. Η ευπάθεια υφίσταται όταν υπάρχει διαφορά μεταξύ της δύναμης που ασκείται από τον παράγοντα απειλής και της ικανότητας ενός αντικειμένου να αντισταθεί σε αυτή τη δύναμη.

Έτσι, η ευπάθεια πρέπει πάντα να περιγράφεται με όρους αντίστασης σε συγκεκριμένο τύπο επίθεσης. Για να δώσουμε ένα πραγματικό παράδειγμα, η αδυναμία ενός αυτοκινήτου να προστατεύσει τον οδηγό του από τραυματισμό όταν χτυπηθεί μετωπικά από ένα φορτηγό που οδηγεί με ταχύτητα 60 μίλια την ώρα είναι μια ευπάθεια. Η αντίσταση της κατασκευής σύνθλιψης του αυτοκινήτου είναι απλώς πολύ ασθενής σε σύγκριση με τη δύναμη του φορτηγού. Ενάντια στην «επίθεση» ενός ποδηλάτη ή ακόμα και ενός μικρού αυτοκινήτου που οδηγεί με πιο μέτρια ταχύτητα, η αντοχή αντίστασης του αυτοκινήτου είναι απολύτως επαρκής.

Μπορούμε επίσης να περιγράψουμε την ευπάθεια του υπολογιστή ως την αποδυνάμωση ή αφαίρεση μιας συγκεκριμένης ισχύος αντίστασης. Μια ευπάθεια υπερχείλισης buffer, για παράδειγμα, αποδυναμώνει την αντίσταση του συστήματος στην αυθαίρετη εκτέλεση κώδικα. Το αν οι εισβολείς μπορούν να εκμεταλλευτούν αυτήν την ευπάθεια εξαρτάται από τις δυνατότητές τους.[3]

2.1.5 Τι είναι απειλή

Μια απειλή είναι το ενδεχόμενο παραβίασης της ασφάλειας, το οποίο καθίσταται δυνατό όταν προκύπτει ένα συμβάν που θα μπορούσε να προκαλέσει ρήγμα στην ασφάλεια με πιθανές αρνητικές συνέπειες. Με άλλα λόγια, η απειλή είναι η πιθανότητα εκμετάλλευσης μιας συγκεκριμένης ευπάθειας από μια συγκεκριμένη απειλή με στόχο ένα συγκεκριμένο επιβλαβές αποτέλεσμα. [15]

2.1.2 Τι είναι πράκτορας απειλής

Ένας πράκτορας απειλής είναι μια οντότητα που πραγματοποιεί επίθεση σε ένα σύστημα ή αποτελεί απειλή για αυτό. [15]

2.1.3 Τι είναι επίθεση

Μια επίθεση είναι η προσβολή της ασφάλειας του συστήματος που προκύπτει από μια ευφυή απειλή. Με άλλα λόγια, είναι μια ευφυής ενέργεια που αποτελεί προμελετημένη απόπειρα, ειδικά με την έννοια της μεθόδου ή τεχνικής, με σκοπό την παράκαμψη των υπηρεσιών ασφαλείας και την παραβίαση της πολιτικής ασφάλειας ενός συστήματος. [15]

2.1.4 Τι είναι τα αντίμετρα

Τα αντίμετρα είναι ενέργειες, συσκευές, διαδικασίες ή τεχνικές που μετριάζουν τις απειλές, περιορίζουν τις ευπάθειες ή καταστέλλουν επιθέσεις, εξαλείφωντας ή αποτρέποντάς τις, ελαχιστοποιώντας τη ζημιά που μπορούν να προκαλέσουν αυτές ή ανιχνεύοντας και αναφέροντάς τις έτσι ώστε να ληφθούν κατάλληλα μέτρα αντιμετώπισης. [15]

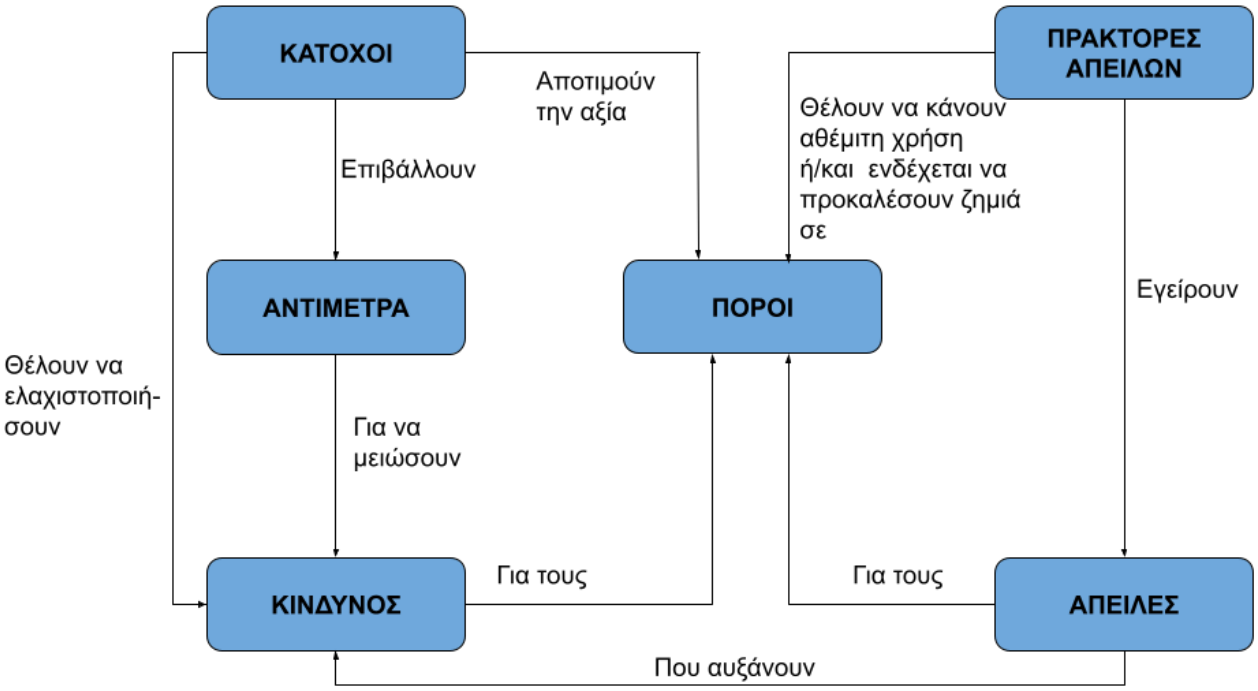
2.1.6 Τι είναι πολιτική ασφάλειας

Μια πολιτική ασφάλειας είναι ένα σύνολο κανόνων και πρακτικών που καθορίζουν ή ρυθμίζουν τον τρόπο με τον οποίο ένα σύστημα ή ένας οργανισμός παρέχει υπηρεσίες ασφαλείας για την προστασία ευαίσθητων και κρίσιμων πόρων του συστήματος. [15]

2.1.7 Τι είναι πόρος συστήματος

Οι πόροι ενός συστήματος μπορεί να είναι δεδομένα που παρέχονται σε ένα πληροφοριακό σύστημα ή μια υπηρεσία που παρέχεται από ένα σύστημα ή μια δυνατότητα του συστήματος, όπως η επεξεργαστική ισχύς ή το εύρος ζώνης της επικοινωνίας, ή ένα στοιχείο του εξοπλισμού του συστήματος (π.χ ένα συστατικό στοιχείο του υλικού ή του υλικό-λογισμικού) ή μία κτιριακή εγκατάσταση που στεγάζει τον εξοπλισμό και τις λειτουργίες του συστήματος. [15]

Οι προαναφερόμενες έννοιες και οι σχέσεις που έχουν μεταξύ τους επιδεικνύονται στο εννοιολογικό μοντέλο της Εικόνας 1.



Εικόνα 1. Έννοιες της ασφάλειας και οι μεταξύ τους σχέσεις [15]

2.2 Υπολογιστικό Νέφος

Το Εθνικό Ινστιτούτο Προτύπων και Τεχνολογίας των ΗΠΑ (NIST) δημοσίευσε έναν ορισμό για το υπολογιστικό νέφος, τον οποίο έχει υποβάλει ως συνεισφορά των ΗΠΑ για ένα διεθνές πρότυπο. Σύμφωνα με το NIST :

Το υπολογιστικό νέφος είναι ένα μοντέλο που επιτρέπει την πανταχού παρούσα, βολική, κατ' απαίτηση δικτυακή πρόσβαση σε μια κοινόχρηστη δεξαμενή διαμορφώσιμων υπολογιστικών πόρων (για παράδειγμα, δίκτυα, διακομιστές, χώρο αποθήκευσης, εφαρμογές και υπηρεσίες) που μπορεί να παρασχεθεί και να διαταχθεί γρήγορα με ελάχιστη προσπάθεια διαχείρισης ή αλληλεπίδραση με τον πάροχο υπηρεσιών[1].[9]

[1] https://nvlpubs.nist.gov/nistpubs/legacy/sp/nistspecialpublication800-145.pdf

2.2.1 Πάροχος Νέφους

Παρέχει πόρους τεχνολογίας πληροφορικής & επικοινωνιών (ΤΠΕ) βασιζόμενους στο υπολογιστικό νέφος. Εκτελεί καθήκοντα διοίκησης και διαχείρισης για την διασφάλιση της συνεχής λειτουργίας της συνολικής υποδομής ΥΝ. Πρέπει να καθιστά τους πόρους και τις υπηρεσίες υπολογιστικού νέφους διαθέσιμες με βάση τις εγγυήσεις των SLA που υπόσχεται. [84]

2.2.2 Καταναλωτής Νέφους

Είναι ιδιώτης ή οργανισμός που έχει επίσημο συμβόλαιο ή διακανονισμό με έναν πάροχο υπολογιστικού νέφους για να χρησιμοποιεί του πόρους που ο δεύτερος παρέχει. Χρησιμοποιεί συνήθως έναν καταναλωτή υπηρεσίας υπολογιστικού νέφους (cloud service consumer) (πρόγραμμα λογισμικού που αλληλεπιδρά με την τεχνική διεπαφή / API μιας υπηρεσίας νέφους) για την πρόσβαση σε μια υπηρεσία υπολογιστικού νέφους η οποία αντιστοιχεί ή περιτυλίγει έναν πόρο. [84]

2.2.3 Ιδιοκτήτης υπηρεσίας Νέφους

Ιδιώτης ή οργανισμός στον οποίο ανήκει νομικά μια υπηρεσία νέφους. Ο ιδιοκτήτης υπηρεσίας νέφους δεν καλείται ιδιοκτήτης πόρου νέφους επειδή ο ρόλος του ιδιοκτήτη υπηρεσίας νέφους εφαρμόζεται μόνο σε υπηρεσίες νέφους. [84]

2.3 Μοντέλα παράδοσης του Νέφους

2.3.1 Ορισμός

Ένα μοντέλο παράδοσης νέφους αντιπροσωπεύει έναν συγκεκριμένο, προσυσκευασμένο συνδυασμό πόρων ΤΠΕ που προσφέρονται από έναν πάροχο.

Το υπολογιστικό νέφος περιλαμβάνει την προσφορά υπολογιστικών πόρων (π.χ. διακομιστές, αποθηκευτικούς χώρους, πλατφόρμες και εφαρμογές) ως υπηρεσίες στους τελικούς χρήστες από παρόχους υπηρεσιών υπολογιστικού νέφους. Οι τελικοί χρήστες έχουν πρόσβαση σε υπηρεσίες του υπολογιστικού νέφους κατά παραγγελία συνήθως μέσω προγραμμάτων περιήγησης ιστού ή και άλλων ειδών διεπαφών, όπως διεπαφή γραμμής εντολών (Command-line Interface - CLI). Οι πάροχοι υπηρεσιών υπολογιστικού νέφους προσφέρουν συγκεκριμένες υπηρεσίες υπολογιστικού νέφους και διασφαλίζουν την ποιότητα των υπηρεσιών αυτών. Βασικά, το υπολογιστικό νέφος περιλαμβάνει τρία επίπεδα: το επίπεδο υποδομής (infrastructure), το επίπεδο πλατφόρμας (platform) και το επίπεδο εφαρμογής (application). [5]

2.3.2 Επίπεδο υποδομής

Το κατώτερο επίπεδο είναι το επίπεδο υποδομής, το οποίο περιλαμβάνει υπολογιστικούς πόρους, όπως διακομιστές, συσκευές δικτύου, μνήμη και αποθήκευση. Είναι γνωστό ως Υποδομή ως Υπηρεσία (Infrastructure as-a-service - IaaS). Ειδικότερα, οι υπολογιστικοί πόροι διατίθενται στους χρήστες ως υπηρεσίες κατ' απαίτηση. Με τη χρήση της τεχνολογίας εικονικοποίησης, το IaaS ουσιαστικά παρέχει εικονικές μηχανές που επιτρέπουν στους πελάτες να δημιουργούν πολύπλοκες δικτυωμένες εικονικές υποδομές. Αυτή η προσέγγιση όχι μονο αφαιρεί την ανάγκη επένδυσης στην κατασκευή υποδομών και την πρόσληψη/απασχόληση προσωπικού διαχείρισης/συντήρησης υποδομών για τις επιχειρήσεις, αλλά επίσης εξομαλύνει το φόρτο της διαχείρισης των πόρων που είναι ήδη στη κατοχή τους. Ένα

παράδειγμα υπηρεσίας IaaS ενός παρόχου υπηρεσιών υπολογιστικού νέφους τι είναι το EC2 της Amazon. Παρέχει ένα εικονικό περιβάλλον υπολογιστών με διεπαφές υπηρεσιών ιστού (web service interfaces). Χρησιμοποιώντας τις διεπαφές, οι χρήστες μπορούν να αναπτύξουν απογυμνωμένα στιγμιότυπα εικονικών μηχανών, στα οποία έπειτα μπορούν να συνδεθούν ώστε να εγκαταστήσουν εκεί την εφαρμογή τους ή μέρος αυτής καθώς και να εκτελέσουν τις δικές τους προσαρμοσμένες εφαρμογές. [5]

2.3.3 Επίπεδο πλατφόρμας

Το μεσαίο επίπεδο είναι αυτό της πλατφόρμας, το οποίο είναι γνωστό ως Πλατφόρμα ως Υπηρεσία (Platform-as-a-Service - PaaS). Έχει σχεδιαστεί για να παρέχει μια πλατφόρμα ανάπτυξης στους χρήστες για να σχεδιάσουν, να αναπτύξουν, να εκτελέσουν και να κλιμακώσουν τις εφαρμογές τους. Αυτό το μοντέλο παράδοσης υπολογιστικού νέφους παρέχει ένα ολοκληρωμένο περιβάλλον για την ανάπτυξη και εκτέλεση εφαρμογών, το οποίο απαρτίζεται από εργαλεία, βιβλιοθήκες, πλαίσια ανάπτυξης και μεσισμικό, επιτρέποντας στους χρήστες να έχουν τον έλεγχο των ρυθμίσεων ανάπτυξης και διαμόρφωσης της εφαρμογής τους. Με το PaaS, οι προγραμματιστές δεν απαιτείται να αγοράζουν και να συντηρούν εργαλεία ανάπτυξης λογισμικού, μειώνοντας, επομένως, το κόστος. Το developers.google.com είναι ένα παράδειγμα PaaS. Είναι μια σουίτα εργαλείων Google που προσφέρεται σε όσους θέλουν να δημιουργήσουν εφαρμογές ή μέρη εφαρμογών, όπως για παράδειγμα τα εργαλεία: Firebase, Android Studio, κτλ. Επιτρέπει στους χρήστες να προσαρμόσουν αυτά τα εργαλεία στις δικές τους ανάγκες. Το Microsoft Azure είναι ένας άλλος πάροχος PaaS. Επιτρέπει στους χρήστες να δημιουργούν εφαρμογές χρησιμοποιώντας διάφορες γλώσσες (πχ Java , Python) ή εργαλεία (πχ Azure Test Plans, Azure DevTest Labs). Κάποιες από αυτές τις εφαρμογές μπορούν να βρίσκονται αποκλειστικά στο νέφος και κάποιες αλλες να χρησιμοποιούν το νέφος ανάλογα με τις ανάγκες τους. Για παράδειγμα, μπορεί ο κώδικας μιας εφαρμογής να βρίσκεται σε τοπικό περιβάλλον αλλά η βάση δεδομένων με την οποία επικοινωνεί να βρίσκεται στο νέφος (Firebase). [5]

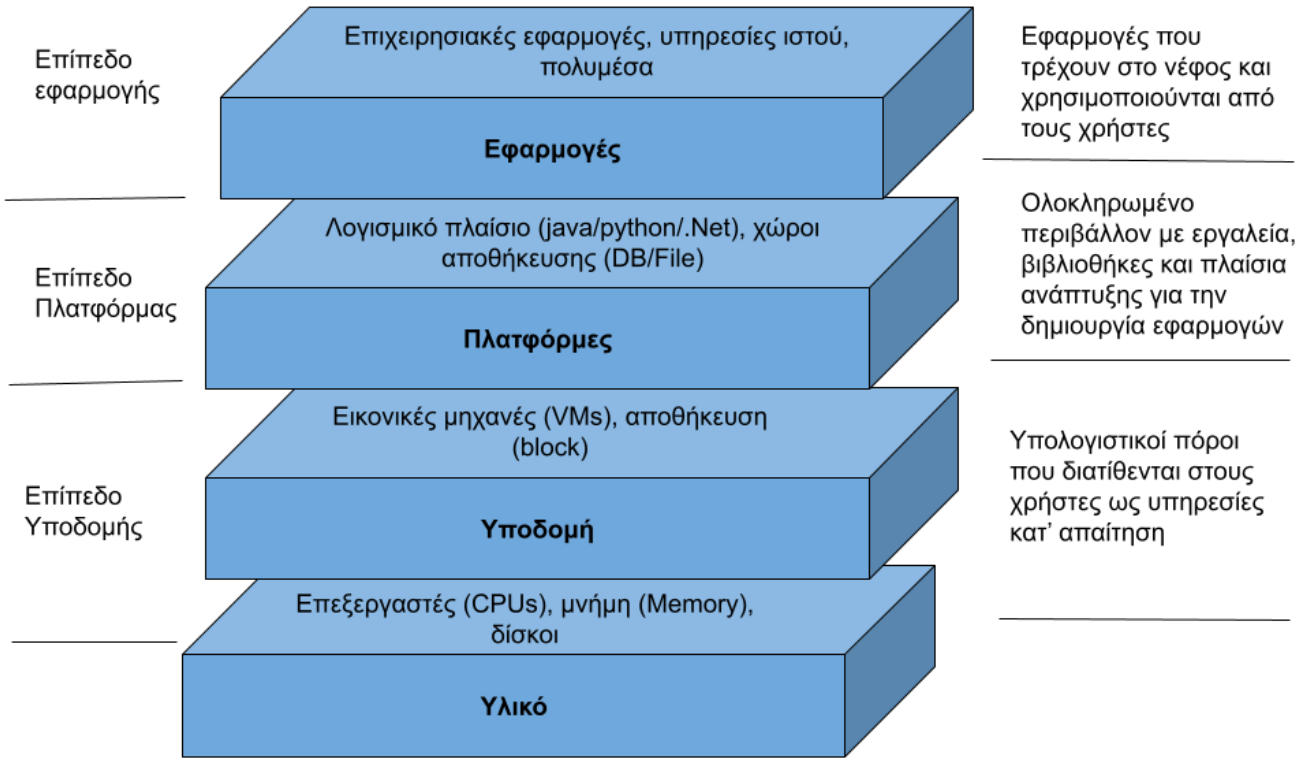
2.3.4 Επίπεδο εφαρμογής

Τέλος, το ανώτερο επίπεδο είναι το επίπεδο εφαρμογής, γνωστό και ως Λογισμικό ως Υπηρεσία (Software-as-a-Service - SaaS). Αυτό το επίπεδο επιτρέπει στους χρήστες να ενοικιάζουν εφαρμογές που τρέχουν στο υπολογιστικό νέφος για να τις χρησιμοποιούν αντί να πληρώνουν για να αγοράσουν αυτές τις εφαρμογές. Οι χρήστες μπορούν, επίσης, να χρησιμοποιούν αυτές τις εφαρμογές ώστε να δημιουργούν νέες και πιο σύνθετες εφαρμογές προστιθέμενης αξίας. Λόγω της ικανότητάς του να μειώνει το κόστος, το SaaS είναι δημοφιλές μεταξύ των νέων εταιρειών που αναπτύσσουν τις επιχειρήσεις τους. Το Dropbox είναι ένα παράδειγμα εταιρείας που προσφέρει υπηρεσίες SaaS. Παρέχει την ομώνυμη υπηρεσία Dropbox, μια ασφαλής υπηρεσία αποθήκευσης αρχείων που βασίζεται στο νέφος, όπου μπορούμε να αποθηκεύσουμε αρχεία και να έχουμε πρόσβαση σε αυτά οπουδήποτε, σε οποιαδήποτε συσκευή. Προσφέρει έναν χώρο εργασίας για κατανεμημένες ομάδες, οι οποίες μπορούν να τον οργανώσουν και να αποκτήσουμε πρόσβαση σε περιεχόμενο σε αυτόν. Άλλες επιχειρήσεις χρησιμοποιούν τις δυνατότητες που παρέχονται από το Dropbox για να συνεργάζονται εσωτερικά και εξωτερικά, να σαρώνουν φωτογραφίες σε έγγραφα, να χρησιμοποιούν λειτουργίες διαχειριστή για να ελέγχουν και να παρακολουθούν τη συμμόρφωση, το απόρρητο και την ασφάλεια. Η Marathon Data Systems είναι ένα άλλο παράδειγμα παρόχου SaaS, ο οποίος προσφέρει πλήρη προϊόντα ή υπηρεσίες SaaS σχετικά με τοπογραφικές δραστηριότητες και γεωγραφικά δεδομένα. Κάποια από τα προσφερόμενα προϊόντα είναι ο Editor για GIS (Σχεδιαστής για Γεωγραφικό Σύστημα

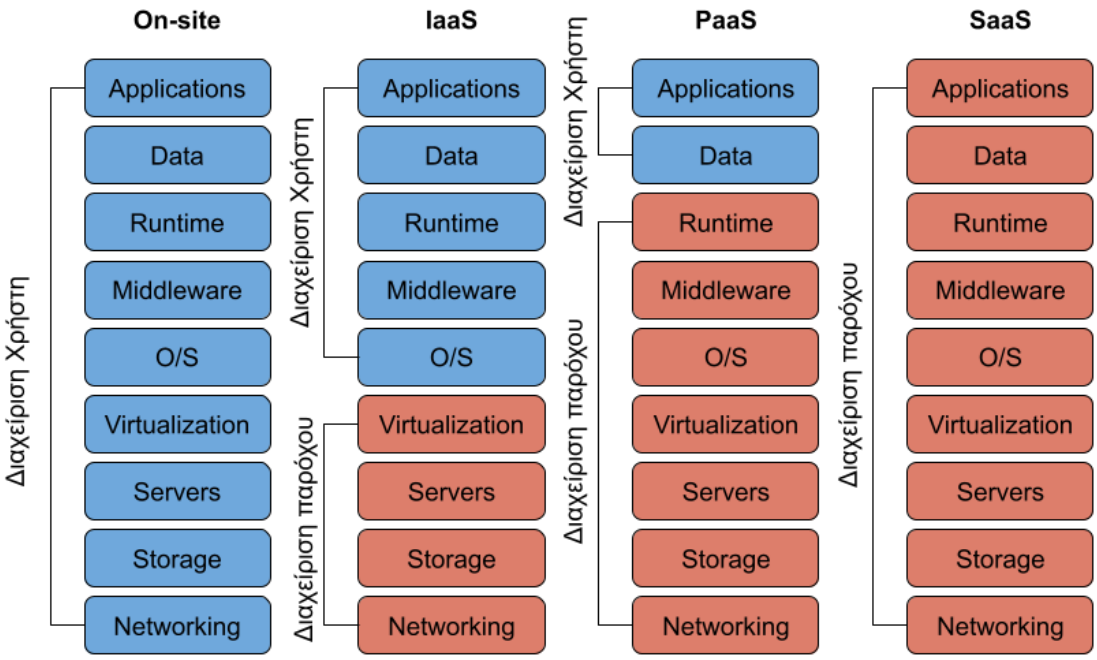
Πληροφοριών), ο Διαχειριστής βάσης δεδομένων για τοπογραφικά δεδομένα (geodata) και ο σχεδιαστής Hybrid Fiber-Coax (Σχεδιαστής για ευρυζωνικά δίκτυα που συνδυάζουν οπτική ίνα και ομοαξονικό καλώδιο) [5]

2.3.5 Διαχείριση ανά επίπεδο

Σε αντίθεση με τον "παραδοσιακό" τρόπο λειτουργίας, όπου όλα διαχειρίζονται από τον τελικό χρήστη, στα διαφορετικά μοντέλα παράδοσης του νέφους έχουμε και διαφορετικό διαχειριστικό φόρτο. Ο φόρτος διαχείρισης μειώνεται καθώς μεταβαίνετε από το IaaS στο PaaS στο SaaS. Το IaaS παρέχει τον μεγαλύτερο έλεγχο και την μεγαλύτερη ευελιξία, αλλά απαιτεί μεγαλύτερη προσπάθεια διαχείρισης από τον πελάτη του νέφους. Από την άλλη πλευρά, το SaaS προσφέρει το μικρότερο διαχειριστικό βάρος, επιτρέποντας στον πελάτη του cloud να επικεντρωθεί στη χρήση της εφαρμογής χωρίς να ανησυχεί για τη διαχείριση της υποκείμενης υποδομής ή της πλατφόρμας. Στην Εικόνα 2 παρουσιάζονται οι πόροι που διαχειρίζεται κάθε επίπεδο υπολογιστικού νέφους και στην Εικόνα 3 παρουσιάζεται το επίπεδο διαχείρισης πόρων που έχει ο πάροχος και ο καταναλωτής ανά μοντέλο παράδοσης υπολογιστικού νέφους. [5]



Εικόνα 2. Πόροι που διαχειρίζεται κάθε επίπεδο Υπολογιστικού Νέφους



Εικόνα 3. Απεικόνιση επιπέδου διαχείρισης πόρων ανά μοντέλο παράδοσης

Στον παρακάτω πίνακα παραθέτουμε μια σειρά από γνωστές υπηρεσίες για το κάθε μοντέλο παράδοσης του νέφους.

Πίνακας 1. Παραδείγματα παρόχων υπηρεσιών υπολογιστικού νέφους που ειδικεύονται σε συγκεκριμένα μοντέλα παράδοσης υπολογιστικού νέφους και κάποιες γνωστές υπηρεσίες τους

Μοντέλο Παράδοσης Υπολογιστικού Νέφους	**Πάροχοι Υπηρεσιών Υπολογιστικού Νέφους**
SaaS	• Cloud9 Analytics[2] (Καταγραφή κλήσεων, παρακολούθηση ποιότητας, ανάλυση ομιλίας και διαχείριση εργατικού δυναμικού) • CVM Solutions[3] (πάροχος παγκόσμιων δεδομένων προμηθευτών και λύσεων διαφοροποίησης προμηθευτών) • Exoprise Systems[4] (λύση παρακολούθησης ψηφιακής εμπειρίας

[2] https://www.cloud9ba.com/call-recording-analytics-wfo/
[3] https://supplier.io/
[4] https://www.exoprise.com/

	(DEM) για Microsoft 365, Office 365, Salesforce και άλλες εφαρμογές cloud — παρέχει ορατότητα πληροφορικής και ενισχύει την παραγωγικότητα των εργαζομένων) • Knowledge Tree[5] (συστήματα διαχείρισης εγγράφων ανοιχτού κώδικα) • Oracle Taleo[6] (πλήρες σύνολο εργαλείων για εύρεση, πρόσληψη, στρατολόγηση και ενσωμάτωση των καλύτερων υποψηφίων) • Google Apps[7] (λύση λογισμικού ως υπηρεσία (SaaS) της Google για επιχειρήσεις όλων των μεγεθών, συμπεριλαμβανομένων των μεγάλων επιχειρήσεων. Η λύση αυτή διευκολύνει την παροχή εφαρμογών Google και εργαλείων διαχείρισης χρηστών/επιχειρήσεων, όπως το Gmail, το Google Talk, το Ημερολόγιο Google, τα Έγγραφα Google, τα Βίντεο Google και το Google Cloud Connect) • Microsoft 365[8] (πλατφόρμα παραγωγικότητας που υποστηρίζεται απο το Υπολογιστικό Νέφος. Με μια συνδρομή στο Microsoft 365 προσφέρεται προσβαση στις πιο πρόσφατες εφαρμογές παραγωγικότητας, όπως Microsoft Teams, Word, Excel, PowerPoint, Outlook, OneDrive κτλ) • Salesforce.com[9] (λογισμικό διαχείρισης πελατειακών σχέσεων και εφαρμογών που επικεντρώνονται στις πωλήσεις, την εξυπηρέτηση πελατών, την αυτοματοποίηση μάρκετινγκ, την ανάλυση και την ανάπτυξη εφαρμογών)

[5] https://www.knowledgetree.com/
[6] https://www.oracle.com/human-capital-management/taleo/
[7] https://workspace.google.com/
[8] https://www.office.com/
[9] https://www.salesforce.com/eu/?ir=1

	• IBM[10] (έχει ένα χαρτοφυλάκιο με περισσότερες από 100 εφαρμογές SaaS που λύνουν κρίσιμες επιχειρηματικές ανάγκες για τους πελάτες, πχ. IBM Watson Knowledge Catalog και IBM Cloud Container Registry)
PaaS	• Google App Engine[11] (υποστηρίζει δημοφιλείς γλώσσες ανάπτυξης με μια σειρά εργαλείων προγραμματιστών), Google Cloud Run (δημιουργία και ανάπτυξη επεκτάσιμων εφαρμογών σε κοντέινερ (containerized apps) γραμμένες σε οποιαδήποτε γλώσσα) • Heroku[12] (πχ. Application Metrics που βοηθάει στην αναγνώριση και διάγνωση προβλημάτων εφαρμογής, Heroku Logging καταγραφή ροών συμβάντων σε ένα μόνο κανάλι κάνοντας εύκολη την περιεκτική καταγραφή (comprehensive logging), Heroku OpEx παρακολούθηση της υγείας των εφαρμογών, Heroku Dynos απομονωμένα, εικονικοποιημένα κοντέινερ Linux που έχουν σχεδιαστεί για να εκτελούν κώδικα με βάση μια εντολή που καθορίζεται από τον χρήστη) • IBM (πχ. IBM Analytics Engine παρέχει στα περιβάλλοντα Apache Spark μια υπηρεσία που αποσυνδέει τις βαθμίδες υπολογισμού και αποθήκευσης για τον έλεγχο του κόστους και την επίτευξη αναλυτικών στοιχείων σε κλίμακα, Event Streams πλατφόρμα ροής συμβάντων που βοηθά στην δημιουργία έξυπνων εφαρμογών που μπορούν να αντιδρούν στα γεγονότα καθώς συμβαίνουν) • Dokku[13] (ανοικτού κώδικα πλατφόρμα για την ανάπτυξη εφαρμογών)

[10] https://www.ibm.com/us-en
[11] https://cloud.google.com/appengine
[12] https://www.heroku.com/
[13] https://dokku.com/

	• WorkXpress[14] (πλατφόρμα για ανάπτυξη και ενσωμάτωση εφαρμογών ιστού και κινητών συσκευών με παροχή εργαλείων)
IaaS	• IBM (πχ. IBM Cloud Virtual Server for VPC και Bare metal and virtual servers) • Microsoft Azure[15] (πχ. VMware Solution για εγχώρια εκτέλεση εργασιών natively στο Azure, VM Scale Sets για την διαχείριση και κλιμάκωση σε Linux και Windows εικονικές μηχανές) • Amazon EC2[16] (προσφέρει επεκτάσιμη υποδομή για εταιρείες που θέλουν να φιλοξενήσουν εφαρμογές που βασίζονται σε υπολογιστικό νέφος) • Google Compute Engine[17] (προσαρμόσιμη υπηρεσία που επιτρέπει τη δημιουργία και εκτέλεση εικονικών μηχανων στην υποδομή της Google), Google Cloud Storage (υπηρεσία για την αποθήκευση μη δομημένων δεδομένων)

Πίνακας 2. Πλεονεκτήματα μοντέλων παράδοσης

IaaS	**PaaS**	**SaaS**
Μοντέλο pay as you use, μειωμένο κόστος κτήσης	Μικρότερο κόστος κτήσης εργαλείων ανάπτυξης	Μείωση εξόδων λόγω των ευέλικτων μοντέλων χρέωσης utility based ή pay as you go, μη ανάγκη διατήρησης

[14] https://www.citizendeveloper.com/
[15] https://azure.microsoft.com/en-us
[16] https://aws.amazon.com/ec2/
[17] https://cloud.google.com/compute

Καλύτερη χρήση των πόρων για τον πάροχο, χαμηλή καθυστέρηση, βελτιωμένη απόδοση	Ευκολία χρήσης (λόγω πληθώρας οικείων εργαλείων), λιγότερη διαχείριση (φυσικών υποδομών)	Καμία εγκατάσταση στην πλευρά του πελάτη, ευκολία πρόσβασης από οποιαδήποτε συσκευή αρκεί η σύνδεση στο διαδίκτυο
Ολοκληρωμένη ασφάλεια ανάλογα με το επιλεγμένο μοντέλο ανάπτυξης	Υποστήριξη ευκίνητης/ευέλικτης (agile) ανάπτυξης εφαρμογών, πιο γρήγορη κυκλοφορία εφαρμογών στην αγορά	Εύκολη & δυναμική κλιμάκωση εφαρμογών

Πίνακας 3. Ευθύνη παρόχου/καταναλωτή και παραδείγματα σεναρίων χρήσης μοντέλων παράδοσης

Μοντέλο	**Ευθύνη παρόχου**	**Ευθύνη καταναλωτή**	**Σενάρια χρήσης**
IaaS	Φυσική υποδομή, Hypervisor	Δεδομένα, μεσισμικό, Λειτουργικό σύστημα, Εφαρμογή	Αποκατάσταση καταστροφών (disaster recovery), διαδίκτυο των πραγμάτων (IoT)
PaaS	Φυσική υποδομή, Hypervisor, Λειτουργικό σύστημα, Μεσισμικό	Δεδομένα, Εφαρμογή	Ανάπτυξη και διαχείριση μεσισμικού, DevOps, ανάπτυξη εγγενών εφαρμογών cloud, ανάπτυξη μικροϋπηρεσιών (microservices)
SaaS	Φυσική υποδομή, Hypervisor, Λειτουργικό σύστημα, Μεσισμικό, Εφαρμογή	Δεδομένα	Νεοφυής επιχειρηματικότητα (startups), ανάπτυξη εφαρμογών προστιθέμενης αξίας, ηλεκτρονικό εμπόριο

2.4 Μοντέλα ανάπτυξης του Νέφους

2.4.1 Ορισμός

Ένα μοντέλο ανάπτυξης νέφους αναπαριστά ένα συγκεκριμένο τύπο περιβάλλοντος νέφους, ο οποίος εξαρτάται από το πού βρίσκεται η υποδομή για την ανάπτυξη και ποιος έχει τον έλεγχο αυτής της υποδομής [80]. Ο NIST ορίζει τέσσερα μοντέλα ανάπτυξης νέφους.

2.4.2 Δημόσιο Νέφος

Ένα δημόσιο νέφος είναι ένας τύπος υπολογιστικού νέφους στον οποίο ένας πάροχος υπηρεσιών δημιουργεί υπολογιστικούς πόρους και τους διαθέτει στους χρήστες μέσω του Διαδικτύου. Οι υπολογιστικοί πόροι μπορεί να περιλαμβάνουν οτιδήποτε από εφαρμογές λογισμικού έτοιμες προς χρήση, μεμονωμένες εικονικές μηχανές (VM), έως και πλατφόρμες. Αυτοί οι πόροι μπορεί να είναι προσβάσιμοι δωρεάν ή η πρόσβαση μπορεί να χρεώνεται σύμφωνα με μοντέλα τιμολόγησης βάσει συνδρομής ή χρήσης. Ο πάροχος δημόσιου νέφους κατέχει και διαχειρίζεται τα κέντρα δεδομένων όπου εκτελούνται οι εργασίες των πελατών, με ορισμένες εξαιρέσεις όπου η διαχείριση ανατίθεται σε τρίτους οργανισμούς. Οι πάροχοι δημόσιου νέφους αναλαμβάνουν την ευθύνη για όλη τη συντήρηση του υλικού και της υποδομής και παρέχουν συνδεσιμότητα δικτύου υψηλού εύρους ζώνης για να εξασφαλίσουν γρήγορη πρόσβαση σε εφαρμογές και δεδομένα ανάλογα το μοντέλο κοστολόγησης. Η αρχιτεκτονική του δημόσιου νέφους αντιστοιχεί σε ένα περιβάλλον πολλαπλών ενοικιαστών (multi-tenant environment), σε ένα τέτοιο περιβάλλον, κατανέμονται εικονικοί πόρου σε χρήστες (μεμονωμένους ενοικιαστές) που μπορεί να εκτελούνται πάνω από διαμοιραζόμενους φυσικούς πόρους. Οι εικονικοί πόροι παρέχονται αυτόματα και εκχωρούνται σε αυτούς μέσω μιας διεπαφής αυτοεξυπηρέτησης. Αυτό σημαίνει ότι οι εργασίες πολλών ενοικιαστών ενδέχεται να εκτελούνται ταυτόχρονα σε κοινόχρηστο φυσικό διακομιστή, ωστόσο τα δεδομένα κάθε ενοικιαστή είναι λογικά απομονωμένα από αυτά των άλλων ενοικιαστών. Επίσης, δίνεται στους ενοικιαστές η δυνατότητα επεκτασιμότητας και ελαστικότητας, άμεσα, ανάλογα με τις ανάγκες τους. Με το δημόσιο νέφος συνήθως μειώνεται το λειτουργικό κόστος μιας επιχείρησης/καταναλωτή νέφους ενώ μηδενίζεται το κόστος κτήσης πόρων της. Επιπλέον, οι ενοικιαστές μπορούν να έχουν (σχεδόν) απεριόριστη πρόσβαση σε πόρους που διατίθενται από τον πάροχο.[84]

2.4.3 Ιδιωτικό Νέφος

Το ιδιωτικό νέφος είναι ένα περιβάλλον υπολογιστικού νέφους αφιερωμένο σε έναν μόνο πελάτη. Είναι, δηλαδή, ένα περιβάλλον απομονωμένης πρόσβασης (isolated access) ενός μόνο ενοικιαστή, που σημαίνει ότι όλοι οι πόροι είναι προσβάσιμοι από μόνο έναν πελάτη. Συνδυάζει πολλά από τα πλεονεκτήματα του υπολογιστικού νέφους, συμπεριλαμβανομένης της ελαστικότητας, της επεκτασιμότητας και της ευκολίας παροχής υπηρεσιών με τον έλεγχο πρόσβασης, την ασφάλεια και την προσαρμογή πόρων της εσωτερικής υποδομής. Τα ιδιωτικά νέφη φιλοξενούνται συνήθως στις εγκαταστάσεις στο κέντρο δεδομένων του πελάτη κάτι που σημαίνει ότι ο ίδιος ο πελάτης είναι και ο πάροχος του νέφους.

Οι πελάτες ιδιωτικού νέφους είναι ελεύθεροι να αγοράσουν το υλικό και το λογισμικό που προτιμούν, έναντι του υλικού και του λογισμικού που προσφέρει ο πάροχος δημοσίου νέφους. Επίσης, μπορούν να προσαρμόσουν τους διακομιστές με όποιον τρόπο θέλουν καθώς και το λογισμικό όπως απαιτείται

με πρόσθετα (add-ons) ή μέσω προσαρμοσμένης ανάπτυξης. Επιπρόσθετα, όλες οι εργασίες τρέχουν πίσω από το τείχος προστασίας του πελάτη ενώ εν γένει υπάρχει υψηλό επίπεδο ασφάλειας λόγω του πλήρους ελέγχου και της εφαρμογής κατάλληλων μηχανισμών και αρχιτεκτονικής ασφάλειας. Τέλος υπάρχει πλήρης συμμόρφωση σε κανονιστικές ρυθμίσεις που επιβάλλονται από τρίτα μέρη διότι υπάρχει ο πλήρης έλεγχος του νέφους.[84]

2.4.4 Κοινοτικό

Το κοινοτικό νέφος είναι παρόμοιο με το δημόσιο νέφος αλλά η πρόσβαση σε αυτό περιορίζεται σε μια κοινότητα καταναλωτών νέφους. Μπορεί να ανήκει από κοινού σε μέλη της κοινότητας ή να παρέχεται από ένα τρίτο μέρος. Τα μέλη της κοινότητας συνήθως μοιράζονται την ευθύνη ορισμού και ανάπτυξης του κοινοτικού νέφους. Η συμμετοχή στην κοινότητα δεν εξασφαλίζει την πρόσβαση σε ή τον έλεγχο όλων των πόρων του νέφους. Εκτός από την ευθύνη ορισμού και ανάπτυξης τα μέλη διαμοιράζονται και το κόστος κτήσης, ανάπτυξης, λειτουργίας και συντήρησής του.[84]

2.4.5 Υβριδικό

Το υβριδικό νέφος είναι ένας συνδυασμός διαφορετικών νεφών όπου το κάθε υποκείμενο νέφος είναι ξεχωριστή οντότητα αλλά όλες δεσμεύονται από πρότυπες ή ιδιόκτητες τεχνολογίες που επιτρέπουν την φορητότητα δεδομένων και εφαρμογών. Η συνήθης πρακτική που εφαρμόζεται σε υβριδικά νέφη αφορά την λειτουργία ιδιωτικού νέφους και την άντληση επιπλέον πόρων κατ'απαίτηση από το δημόσιο νέφος. Το αποτέλεσμα είναι ένα ενιαίο, ενοποιημένο και ευέλικτο κατανεμημένο υπολογιστικό περιβάλλον όπου ένας οργανισμός καταναλωτή μπορεί να τρέξει και να κλιμακώσει τις εργασίες του με βάση το πιο κατάλληλο υπολογιστικό μοντέλο. Επιτρέπει δηλαδή να μετακινούνται απρόσκοπτα οι εργασίες μεταξύ των υποκείμενων νεφών, όπως απαιτείται, για βέλτιστη απόδοση, ασφάλεια, συμμόρφωση και οικονομική αποδοτικότητα. Για παράδειγμα, ένας καταναλωτής νέφους αναπτύσσει και ενοποιεί διαφορετικές υπηρεσίες νέφους, όπου οι πρώτες τρέχουν σε ιδιωτικό νέφος διότι διαχειρίζονται προσωπικά δεδομένα ενώ οι δεύτερες τρέχουν σε δημόσιο νέφος διότι διαχειρίζονται μη προσωπικά δεδομένα.[84]

2.4.6 Χαρακτηριστικά μοντέλων ανάπτυξης νέφους

Στον πίνακα 4 παρουσιάζονται και συγκρίνονται τα χαρακτηριστικά των μοντέλων ανάπτυξης του υπολογιστικού νέφους.

Πίνακας 4. Χαρακτηριστικά μοντέλων ανάπτυξης νέφους [84]

Δημόσιο	**Ιδιωτικό**	**Υβριδικό**	**Κοινοτικό**
Προσιτό οικονομικά, λιγότερο δαπανηρό μοντέλο ανάπτυξης	Το πιο κοστοβόρο μοντέλο ανάπτυξης	Υψηλό κόστος & πολυπλοκότητα διαχείρισης (πχ. για την διασύνδεση μεταξύ	Χαμηλό κόστος καθώς το κόστος διαμοιράζεται στα μέλη της κοινότητας

		των διαφορετικών νεφών)	
Λιγότερο ασφαλές σε σχέση με τα άλλα μοντέλα ανάπτυξης	Περισσότερη ασφάλεια και ιδιωτικότητα από τα άλλα μοντέλα, κεντρικός έλεγχος	Εν μέρη ασφαλές λόγω των πολλαπλών νεφών από τα οποία αποτελείται	Μερικώς ασφαλές λόγω (εσωτερικών) επιθέσεων από την κοινότητα
Αρκετά κλιμακώσιμο, Αυστηρά SLAs	Αδύναμα SLAs	Έχει τη συνδυαστική δύναμη των νεφών που συνθέτει	Συνεργατική εργασία στο νέφος, διαμοιρασμός υπευθυνοτήτων

3. Ζητήματα Ασφαλείας

3.1 Απειλές

Στην ασφάλεια υπολογιστών, ως απειλή ορίζεται οτιδήποτε είναι ικανό να προκαλέσει σοβαρή βλάβη σε ένα σύστημα υπολογιστή. Οι απειλές μπορεί να οδηγήσουν σε πιθανές επιθέσεις στο σύστημα υπολογιστή ή την υποδομή δικτύου. Στην μελέτη των Ashish Singh και Kakali Chatterjee που πραγματοποιήθηκε το 2016 με τίτλο "Cloud security issues and challenges: a survey" [6], παρουσιάζονται κάποιες από τις πιο σημαντικές απειλές που σχετίζονται με την αρχιτεκτονική ασφάλειας των υπηρεσιών υπολογιστικού νέφους. Στον Πίνακα 5 παρουσιάζονται οι απειλές που υπάρχουν στο υπολογιστικό νέφος σε συνδυασμό με τους πράκτορες απειλής, τις επιπτώσεις που μπορεί να έχουν, τις υπηρεσίες του υπολογιστικού νέφους που επηρεάζουν καθώς και τις λύσεις που προτείνονται για κάθε απειλή. Ο πίνακας αυτός παρέχει τις προτάσεις της μελέτης "Cloud security issues and challenges: a survey" [6] με πρόσθετη επέκταση την δεύτερη στήλη "Πράκτορες Απειλής (Threat Agents)", η οποία θεωρούμε ότι είναι μια χρήσιμη προσθήκη στην μελέτη.

Πίνακας 5. Απειλές υπολογιστικού νέφους σε συνδυασμό με τους πράκτορες απειλής, τις επιπτώσεις, τις υπηρεσίες που επηρεάζουν και τις πιθανές λύσεις τους [6]

Απειλές (Threats)	**Πράκτορες Απειλής (Threat Agents)**	**Επιπτώσεις (Effects)**	**Υπηρεσίες νέφους που επηρεάζονται (Affected cloud services)**	**Λύσεις (Solutions)**
διαφορετικό μοντέλο	ανώνυμος επιτιθέμενος,	απώλεια ελέγχου στην	PaaS, SaaS, IaaS	ισχυρή κρυπτογράφηση από άκρο σε άκρο, κοινό

παράδοσης/λήψης υπηρεσιών	κακόβουλος πράκτορας υπηρεσίας, εμπιστευμένος χρήστης	υποδομή, πλατφόρμα ή εφαρμογή ανάλογα με το μοντέλο παράδοσης υπολογιστικού νέφους		πρότυπο νόμων ασφαλείας που να εφαρμόζεται από όλους τους παρόχους και σύστημα διαχείρισης εμπιστοσύνης
καταχρηστική χρήση του υπολογιστικού νέφους	κακόβουλος εσωτερικός χρήστης, εμπιστευμένος επιτιθέμενος	απάτη υπηρεσιών, ισχυρότερη επίθεση λόγω μη αναγνωρισμένης εγγραφής (unidentified sign-up)	PaaS, IaaS	Παρακολούθηση κατάστασης του συστήματος, υποστήριξη ισχυρής εγγραφής χρηστών και εφαρμογή πιο εξεζητημένων τεχνικών ελέγχου ταυτότητας
ανασφαλείς διεπαφές και APIs	ανώνυμος επιτιθέμενος, κακόβουλος πράκτορας υπηρεσίας, εμπιστευμένος χρήστης, κακόβουλος εσωτερικός χρήστης, εμπιστευμένος επιτιθέμενος	ακατάλληλος έλεγχος ταυτότητας και εξουσιοδότησης, διείσδυση σε μια υπηρεσία νέφους, μετάδοση λάθος περιεχομένου	PaaS, SaaS, IaaS	Υιοθέτηση κατάλληλου μηχανισμού ελέγχου ταυτότητας και πρόσβασης και ενός μοντέλου ασφαλούς διεπαφής που να περιλαμβάνει μηχανισμούς όπως HTTPS, χρονικά όρια αιτήσεων (request timeouts), τυποποιημένη μετάδοση δεδομένων πχ. σε JSON, σωστός χειρισμός λαθών καθώς και μεσισμικού.
εσωτερικοί χρήστες	εμπιστευμένος επιτιθέμενος, κακόβουλος εσωτερικός χρήστης	διεισδύουν σε πόρους του οργανισμού, βλάπτουν περιουσιακά στοιχεία, απώλεια παραγωγικότητας, επηρεάζουν αρνητικά μια λειτουργία	PaaS, SaaS, IaaS	Χρήση αναφορών και ειδοποιήσεων παραβίασης, διαφανής διαδικασία ασφάλειας και διαχείρισης ασφάλειας, χρήση εξουσιοδοτημένης πρόσβασης σε φυσικούς πόρους

θέματα κοινής τεχνολογίας	εμπιστευμένος επιτιθέμενος, κακόβουλος εσωτερικός χρήστης	παραβίαση hypervisor, έλεγχος εικονικών μηχανών άλλων χρηστών, απώλεια δεδομένων λόγω μη σωστής απομόνωσης πόρων	PaaS, SaaS, IaaS	Σκλήρυνση εικονικών μηχανών, ΛΣ & hypervisor, καλύτερο επίπεδο απομόνωσης εικονικών μηχανών, διασφάλιση ακεραιότητας κώδικα hypervisor, patching, έλεγχοι για ιούς, διαγραφή (περιττών) εικόνων (εικονικών μηχανών) & σημείων ελέγχου
απώλεια, κλείδωμα, διαφυγή και διαρροή δεδομένων	κακόβουλος εσωτερικός χρήστης, εμπιστευμένος επιτιθέμενος, ανώνυμος επιτιθέμενος, πάροχος (για κλείδωμα δεδομένων)	προσωπικά/ευαίσθητα δεδομένα μπορούν να διαρρεύσουν, διαγραφούν, καταστραφούν, τροποποιηθούν ή κλειδωθούν.	PaaS, SaaS, IaaS	Παροχή μηχανισμών ασφαλούς αποθήκευσης δεδομένων και δημιουργίας αντιγράφων ασφαλείας, έλεγχος πρόσβασης, εξεζητημένη ταυτοποίηση χρηστών (πολλαπλών παραγόντων), κρυπτογράφηση δεδομένων κατά την μεταφορά και την αποθήκευση, ασφαλής/ολοκληρωμένη διαγραφή δεδομένων, τμηματοποίηση δεδομένων (για μη αποκάλυψη συσχετίσεων), SLAs
κλοπή υπηρεσίας/ταυτότητας	ανώνυμος επιτιθέμενος, κακόβουλος εσωτερικός χρήστης, εμπιστευμένος επιτιθέμενος, κακόβουλος πράκτορας υπηρεσίας	Κλεμμένα διαπιστευτήρια λογαριασμού χρήστη, πρόσβαση σε κρίσιμες διαδικασίες του υπολογιστικού νέφους επιτρέποντας στον εισβολέα να θέσει σε	PaaS, SaaS, IaaS	Υιοθέτηση ισχυρών μηχανισμών πιστοποίησης ταυτότητας, πολιτικές ασφάλειας και ασφαλές κανάλι επικοινωνίας, ασφαλείς σύνοδοι και ασφαλής προγραμματισμός υπηρεσιών/διεπαφών υπηρεσιών, ισχυροί μηχανισμοί ελέγχου πρόσβασης

		κίνδυνο την ασφάλεια των υπηρεσιών, κλοπή συναλλαγών, παραποίηση πληροφοριών, παράνομες ανακατευθύνσεις, κλοπή ευαίσθητων / προσωπικών δεδομένων		

3.1.1 Διαφορετικό μοντέλο παράδοσης/λήψης υπηρεσιών

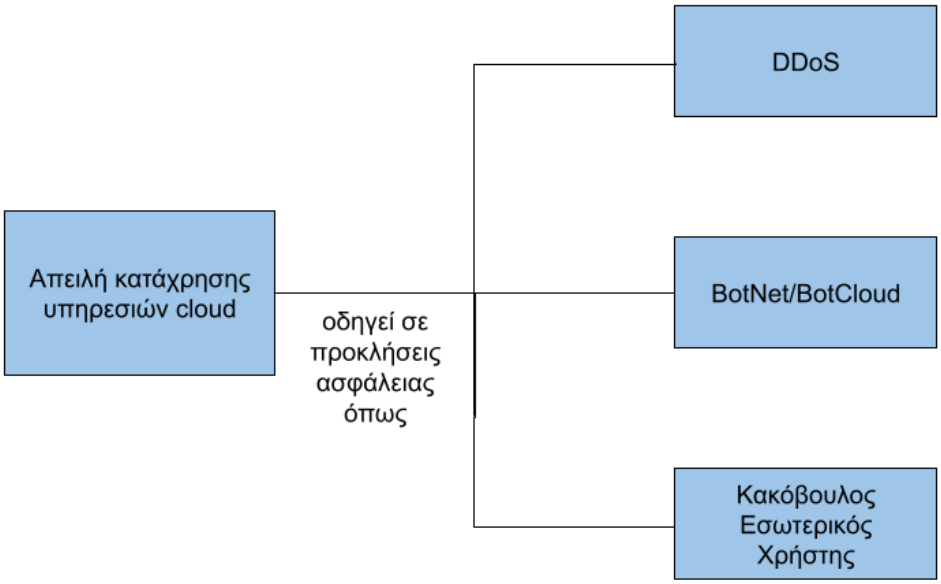
Το υπολογιστικό νέφος χρησιμοποιεί διαφορετικούς τρόπους παροχής υπηρεσιών σε σχέση με το επιχειρησιακό μοντέλο. Τα δεδομένα του υπολογιστικού νέφους μεταφέρονται από μια τοποθεσία σε μια άλλη όπου οι δύο αυτές τοποθεσίες μπορεί να χρησιμοποιούν διαφορετικές πολιτικές ασφαλείας. Όλες οι υπηρεσίες και οι εφαρμογές εκτελούνται απομακρυσμένα σε εικονικές μηχανές του υπολογιστικού νέφους, οι οποίες προσφέρονται από τον πάροχο υπηρεσιών υπολογιστικού νέφους. Επομένως, πρέπει να εξετάζονται όλοι οι κίνδυνοι που σχετίζονται με την απώλεια ελέγχου στο υπολογιστικό νέφος (διαρροή δεδομένων, ανασφαλείς εικονικές μηχανές). Για την αφαίρεση τέτοιων απειλών που σχετίζονται με την απώλεια ελέγχου στην υποδομή του υπολογιστικού νέφους απαιτείται ισχυρή κρυπτογράφηση από άκρο σε άκρο για τη μεταφορά δεδομένων, κοινό πρότυπο πολιτικών ασφαλείας που να εφαρμόζεται από όλους τους παρόχους και σύστημα διαχείρισης εμπιστοσύνης. [6] Τα SLAs υπόσχονται τη διασφάλιση της ποιότητας των υπηρεσιών. Μπορούν, όμως, να βοηθήσουν στην μετρίαση των κινδύνων καθώς μπορούν να προσδιορίζουν κανονισμούς, πιστοποιήσεις ασφαλείας ή πρωτόκολλα που πρέπει να χρησιμοποιεί ο πάροχος για τις υπηρεσίες που προσφέρει.

3.1.2 Καταχρηστική χρήση του υπολογιστικού νέφους

Ο όρος καταχρηστική χρήση του υπολογιστικού νέφους αναφέρεται στο γεγονός της εκμετάλλευσης των υπηρεσιών νέφους για την εκτέλεση ανήθικων ή κακόβουλων δραστηριοτήτων από τους χρήστες του νέφους με σκοπό την απόκτηση διαφόρων ειδών οφελών (πχ. οικονομικού). Στην Εικόνα 4 φαίνονται οι βασικές προκλήσεις από την κατάχρηση υπηρεσιών νέφους.

Το απεριόριστο εύρος ζώνης και η χωρητικότητα αποθήκευσης είναι σημαντικά χαρακτηριστικά που παρέχονται από παρόχους IaaS. Κακόβουλοι εμπιστευμένοι χρήστες μπορούν να χρησιμοποιήσουν τους διαθέσιμους πόρους του υπολογιστικού νέφους για να πραγματοποιήσουν μια επίθεση. Τέτοιες επιθέσεις μπορεί να είναι η αποθήκευση ενός κακόβουλου λογισμικού σε μια εικονική μηχανή στο υπολογιστικό νέφος. Υπάρχουν περιστατικά όπου κακόβουλοι χρήστες έχουν κατορθώσει, χρησιμοποιώντας τους πόρους του νέφους, να επιτεθούν σε άλλες εταιρείες ή κοινωνικά δίκτυα. Πιο συγκεκριμένα, ένα τέτοιο παράδειγμα επίθεσης είναι η περίπτωση όπου κακόβουλοι χρήστες χρησιμοποίησαν τους πόρους που παρέχει η Amazon EC2 και δημιούργησαν ένα botnet με το οποίο

στην συνέχεια επιτέθηκαν στο LinkedIn, επιτυγχάνοντας να εξάγουν και να αντιγράψουν δεδομένα από πολλές σελίδες προφίλ μελών. Για την προστασία του υπολογιστικού νέφους από αυτού του είδους τις απειλές, η αρχική διαδικασία εγγραφής θα πρέπει περιλαμβάνει σωστή επικύρωση και επαλήθευση στοιχείων ώστε να ελέγχεται εάν η ταυτότητα του χρήστη που εγγράφεται είναι πραγματική. Επίσης, για να παρεμποδιστεί ένας κακόβουλος χρήστης που έχει κλέψει τα διαπιστευτήρια ενός νόμιμου χρήστη να εισβάλει στο σύστημα ως ένας νόμιμος χρήστης, πρέπει να γίνεται χρήση ισχυρών IDS/IPS. Επίσης, προτείνονται τα εξής για την εν γένει αντιμετώπιση αυτής της απειλής: χρήση τείχους προστασίας που μπορεί να επιθεωρεί την εισερχόμενη και την εξερχόμενη κίνηση, καταχωρήσεις ενεργειών χρηστών ώστε έπειτα να αναλύονται για τον εντοπισμό καταχρήσεων, κατάλληλη καθώς και εξεζητημένη ABAC εξουσιοδότηση με κατάλληλους κανόνες πρόσβασης.[6]



Εικόνα 4. Σημαντικές προκλήσεις από την απειλή κατάχρησης της υπηρεσίας Νέφους [81]

Πίνακας 6. Προκλήσεις ασφαλείας και πιθανές επιπτώσεις τους [81]

Προκλήσεις Ασφαλείας	**Πιθανές επιπτώσεις που μπορεί να προκύψουν από τις προκλήσεις ασφάλειας**				
DDoS	Διακοπή υπηρεσίας / μη διαθεσιμότητα υπηρεσίας, επιβράδυνση της κυκλοφορίας (traffic slowdown)	Χρηματοοικονομικός αντίκτυπος (financial impact)			Απώλεια δεδομένων, κλοπή, παραβιάσεις, διαρροές, μη εξουσιοδοτημένη

BotNet/BotCloud	επιχειρηματική ασυνέχεια (business discontinuity), υπέρμετρη κατανάλωση εύρους ζώνης, επεξεργαστικής ισχύς, αποθήκευσης, μνήμης		Παραβιάσεις συμμόρφωσης και νομικές προεκτάσεις (compliance violations and legal ramifications)		πρόσβαση
Κακόβουλος Εσωτερικός Χρήστης				Παραβίαση ιδιωτικότητας , σάρωση δεδομένων (data scavenging)	
Ευπάθειες από κοινόχρηστη τεχνολογία					

3.1.3 Ανασφαλίες διεπαφές και APIs

Ο πάροχος υπολογιστικού νέφους παρέχει ένα σύνολο διεπαφών ιστού και APIs στους χρήστες του για επικοινωνία με τις υπηρεσίες υπολογιστικού νέφους που αυτός προσφέρει. Αυτές οι διεπαφές παρέχουν όλες τις λειτουργίες παροχής, διαχείρισης και παρακολούθησης στον πελάτη τους. Έτσι, η ασφάλεια και η διαθεσιμότητα του υπολογιστικού νέφους βασίζεται σε μεγάλο βαθμό στην ασφάλεια αυτών των διεπαφών & API. Ωστόσο, μερικές φορές, τόσο τυχαίες όσο και κακόβουλες προσπάθειες επίθεσης μπορούν να παραβιάζουν την ασφάλεια των APIs αυτών . Για τον λόγο αυτό, τα APIs θα πρέπει να ελέγχονται για και να διορθώνονται ως προς τις πιθανές τους τρωτότητες. Επίσης, θα πρέπει να σχεδιάζονται και υλοποιούνται με γνώμονα την ασφάλεια καθώς και να δοκιμάζονται εκτενώς ώστε να αυξηθεί το επίπεδο αξιοπιστίας τους. Χρειάζεται δηλαδή ένας κύκλος ανάπτυξης ασφαλών εφαρμογών και λογισμικού (και άρα διεπαφών & APIs). Αυτός ο τύπος απειλών μπορεί να επηρεάσει τα μοντέλα υπηρεσιών PaaS, IaaS και SaaS. Όλες αυτές οι απειλές μπορούν να αποτραπούν με την υιοθέτηση του κατάλληλου μηχανισμού ελέγχου ταυτότητας και πρόσβασης και ενός μοντέλου ασφαλούς διεπαφής με χρήση του πρωτοκόλλου HTTPS, χρονικών ορίων αιτήσεων, τυποποιημένης μετάδοσης δεδομένων, όπως για παράδειγμα JSON, κατάλληλου χειρισμού λαθών καθώς και μεσισμικού που να οργανώνει σωστά τα αιτήματα και τα δεδομένα. [6]

3.1.4 Κακόβουλοι εσωτερικοί χρήστες

Μία από τις πιο σημαντικές απειλές στο υπολογιστικό νέφος είναι οι κακόβουλοι εσωτερικοί χρήστες, καθώς έχουν την δυνατότητα να διεισδύουν σε πόρους του οργανισμού, βλάπτουν περιουσιακά στοιχεία ή επηρεάζουν μια λειτουργία προκαλώντας απώλεια παραγωγικότητας. Αυτή η απειλή εκτελείται κυρίως λόγω της έλλειψης διαφάνειας των υπηρεσιών ΤΠΕ και των χρηστών που εργάζονται σε έναν ενιαίο τομέα διαχείρισης. Όταν, με κάποιο τρόπο, ένας εργαζόμενος αποκτά υψηλότερο επίπεδο πρόσβασης, είτε λόγω κενού κανόνων πρόσβασης είτε λόγω κενών ασφαλείας που επιτρέπουν το escalation (κλιμάκωση), μπορεί να διεισδύει στο απόρρητο των δεδομένων και των υπηρεσιών ή εν γένει σε πόρους ενός οργανισμού (του παρόχου ή των πελατών του) με σκοπό να βλάψει τα περιουσιακά στοιχεία του. Αυτό μπορεί να συμβεί από έναν εισβολέα εκ των έσω που μπορεί εύκολα να εισέλθει στο σύστημα μέσω του τείχους προστασίας ή του συστήματος ανίχνευσης εισβολών, εφόσον το σύστημα ασφαλείας αυτό το θεωρήσει ως νόμιμη δραστηριότητα. Πολιτικές ασφαλείας σε θέματα φυσικής και μη ασφάλειας μπορούν να βοηθήσουν στο να αντιμετωπιστούν οι κακόβουλοι εσωτερικοί χρήστες. Επίσης, η τμηματοποίηση δικτύου για καλύτερη διαχείριση και έλεγχο και ο πολυπαραγοντικός έλεγχος ταυτότητας (multi factor authentication) σε ευαίσθητες διαδικασίες αντιμετωπίζουν τις περιπτώσεις που ο κακόβουλος εσωτερικός χρήστης προσπαθεί να αποκτήσει υψηλότερο επίπεδο πρόσβασης από εκείνο που πρέπει να κατέχει (escalation). [6]

3.1.5 Θέματα κοινής τεχνολογίας σε περιβάλλον πολλαπλών μισθώσεων

Οι υπηρεσίες που παρέχονται από προμηθευτές IaaS σε περιβάλλον πολλαπλών μισθωτών υποστηρίζονται από την χρήση εικονικοποίησης. Η εικονικοποίηση παρέχει τη δυνατότητα κοινής χρήσης του ίδιου (φυσικού) πόρου μεταξύ πολλών χρηστών. Ο υπερεπόπτης (hypervisor) σε ένα περιβάλλον πολλαπλών ενοικιαστών μπορεί, λόγω κάποιων τρωτοτήτων που υπάρχουν στο περιβάλλον του, να επιτρέψει σε έναν κακόβουλο χρήστη να αποκτήσει μη εξουσιοδοτημένη πρόσβαση σε δεδομένα άλλων χρηστών. Αυτό οδηγεί σε μεγάλη απειλή, καθώς η υποδομή δεν είναι (πάντοτε) σχεδιασμένη για να προσφέρει ισχυρή απομόνωση σε περιβάλλον πολλών ενοικιαστών. Επομένως, η έννοια της κοινής χρήσης μπορεί να επηρεάσει την συνολική υποδομή ενός υπολογιστικού νέφους. Ο ισχυρός έλεγχος ταυτότητας, η σκλήρυνση εικονικών μηχανών, ΛΣ και υπερεπόπτη, το καλύτερο επίπεδο απομόνωσης εικονικών μηχανών, η διασφάλιση ακεραιότητας κώδικα υπερεπόπτη, το patching (επιδιορθώσεις κώδικα), οι έλεγχοι για ιούς, η διαγραφή εικόνων (εικονικών μηχανών) και σημείων ελέγχου είναι ορισμένοι μηχανισμοί για την αποφυγή αυτού του ζητήματος. [6]

3.1.6 Απώλεια, κλείδωμα (data lock-in), διαφυγή (date remanence) και διαρροή δεδομένων

Το ζήτημα της απώλειας δεδομένων αναφέρεται στη διαγραφή, στην αλλαγή και στην κλοπή δεδομένων χωρίς αντίγραφο ασφαλείας του αρχικού περιεχομένου. Η απώλεια ενός κλειδιού κρυπτογράφησης μπορεί επίσης να προκαλέσει διαρροή δεδομένων, λόγω της παραγωγικής και διαμοιραστικής φύσης του υπολογιστικού νέφους. Ο κύριος λόγος απώλειας δεδομένων και διαρροής είναι η έλλειψη ελέγχου ταυτότητας, εξουσιοδότησης και ελέγχου πρόσβασης, οι αδύναμοι αλγόριθμοι κρυπτογράφησης, τα αδύναμα κλειδιά, ο κίνδυνος συσχέτισης, η έλλειψη ανάκτησης από καταστροφή και η μη κατάλληλη διαγραφή των δεδομένων (που απλώς μαρκάρονται προς διαγραφή χωρίς

ουσιαστικά να διαγράφονται). Αυτές οι απειλές μπορούν να επηρεάσουν τα μοντέλα υπηρεσιών IaaS, PaaS και SaaS. Τα ασφαλή APIs, η ασφαλής αποθήκευση, η χρήση ισχυρών κλειδιών και αλγορίθμων κρυπτογράφησης, η δημιουργία αντιγράφων ασφαλείας δεδομένων, ο έλεγχος πρόσβασης, η εξεζητημένη ταυτοποίηση χρηστών (πολλαπλών παραγόντων), η κρυπτογράφηση δεδομένων κατά την μεταφορά και την αποθήκευση, η ασφαλής/ολοκληρωμένη διαγραφή δεδομένων και η τμηματοποίηση δεδομένων (για την συσχέτιση) είναι μερικές μέθοδοι πρόληψης. [6]

Το πρόβλημα κλειδώματος παρόχου (vendor lock in) στο υπολογιστικό νέφος είναι η κατάσταση όπου οι πελάτες εξαρτώνται αποκλειστικά από τις ιδιόκτητες τεχνολογίες ενός παρόχου και δεν μπορούν εύκολα να μετακινηθούν σε διαφορετικό πάροχο χωρίς σημαντικό κόστος, νομικούς περιορισμούς ή τεχνικές ασυμβατότητες. Το πρόβλημα αυτό επηρεάζει και τα δεδομένα (data lock in) των πελατών. Λύσεις για το πρόβλημα αυτό είναι η τυποποίηση τεχνολογιών που χρησιμοποιούνται από όλους τους παρόχους καθώς και η λήψη σωστών αποφάσεων για επιλογή παρόχου με γνώμονα μελλοντικές αλλαγές.

3.1.7 Κλοπή υπηρεσίας/ταυτότητας

Η πειρατεία υπηρεσίας (service hijacking) είναι μια διαδικασία κατά την οποία ο επιτιθέμενος εισβάλει στην σύνοδο του χρήστη με την υπηρεσία και την υποκλέπτει. Αυτό μπορεί να εκτελεστεί μέσω απάτης, ηλεκτρονικού ψαρέματος (phishing), επίθεσης ενδιάμεσου (man-in-the-middle) (εκμετάλλευση αδύναμης ή μη κρυπτογραφημένης συνόδου) και εκμετάλλευσης των ευπαθειών λογισμικού. Η μη κυκλική ανανέωση των διαπιστευτηρίων και του κωδικού πρόσβασης, η παροχή ευαίσθητης πληροφορίας λόγω επίθεσης ηλ. ψαρέματος, μια επίθεση ενδιάμεσου, μια brute-force επίθεση με σκοπό την κλοπή διαπιστευτηρίων και οι ανασφαλείς σύνοδοι συχνά οδηγούν σε κλοπές υπηρεσίας ή λογαριασμού. Στο υπολογιστικό νέφος, εάν ένας εισβολέας μπορεί να έχει πρόσβαση στα διαπιστευτήρια κάποιου ή στην σύνοδο του, μπορεί να καταγράψει τις δραστηριότητες, τα δεδομένα συναλλαγών, να διενεργήσει νέες συναλλαγές χρεώνοντας το θύμα, να κλέψει ευαίσθητα δεδομένα, να επιστρέψει παραποιημένες πληροφορίες ή να ανακατευθύνει τον πελάτη σε παράνομους ιστότοπους ώστε να δυνητικά να παραβιάσει και άλλους λογαριασμούς του πελάτη σε άλλες υπηρεσίες μέσω κλοπής διαπιστευτηρίων. Η κλοπή ταυτότητας είναι ένα είδος τεχνάσματος κατά το οποίο κάποιος υποδύεται την ταυτότητα ενός νόμιμου χρήστη και επωφελείται από τις πιστώσεις, τους σχετικούς πόρους και άλλα οφέλη υπηρεσιών του. Ως αποτέλεσμα αυτών των απειλών, το θύμα έχει ανεπιθύμητες συνέπειες ενώ μπορεί και να χάσει τα δεδομένα του. Για την αποφυγή τέτοιων απειλών χρειάζεται η υιοθέτηση ισχυρών μηχανισμών πιστοποίησης ταυτότητας & ελέγχου (για μετρίαση του κινδύνου εφόσον κάποιος ελέγχει τον λογαριασμό ενός χρήστη), πολιτικές ασφάλειας και ασφαλές κανάλια επικοινωνίας, ασφαλείς σύνοδοι και ασφαλής προγραμματισμός υπηρεσιών/διεπαφών υπηρεσιών, ισχυροί μηχανισμοί ελέγχου πρόσβασης (για μετρίαση του κινδύνου εφόσον κάποιος ελέγχει τον λογαριασμό ενός χρήστη) [6].

3.2 Επιθέσεις

Οι εταιρείες γνωρίζουν την αξία του υπολογιστικού νέφους σε ένα επιχειρηματικό περιβάλλον. Όμως, μέρα με τη μέρα εμφανίζονται νέες τεχνολογίες που υιοθετούνται από το νέφος, οι οποίες αυξάνουν την επιφάνεια τρωτοτήτων και διαμορφώνουν νέες επιθέσεις προς το υπολογιστικό νέφος. Κάθε

τεχνολογία που εφαρμόζεται από το νέφος αντιστοιχεί σε μια ή περισσότερες επιθέσεις που μπορούν να πραγματοποιηθούν, οι οποίες εκμεταλλεύονται τις τρωτότητες των τεχνολογιών αυτών ή των υλοποιήσεών τους. Στον παρακάτω πίνακα παρουσιάζονται κάποια συγκεκριμένα είδη επιθέσεων στο υπολογιστικό νέφος, οι επιπτώσεις που μπορούν να έχουν στις διάφορες υπηρεσίες του και οι λύσεις αντιμετώπισής τους. [6]

Πίνακας 7. Είδη επιθέσεων που πραγματοποιούνται στο υπολογιστικό νέφος και συσχέτιση με την διαδικασία υλοποίησης τους, τις υπηρεσίες νέφους που επηρεάζονται, τις επιπτώσεις που προκύπτουν και τις πιθανές λύσεις για την αποφυγεί του [6]

Επιθέσεις	**Διαδικασία**	**Υπηρεσίες νέφους που επηρεάζονται**	**Επιπτώσεις**	**Λύσεις**
Zombie επίθεση (DoS/DDoS επίθεση)	Άμεση/έμμεση πλημμύρα πακέτων SYN σε host, επίθεση σε εικονική μηχανή, επίθεση σε hypervisor, επίθεση βάσει δικτύου	SaaS, PaaS, IaaS	Η διαθεσιμότητα της υπηρεσίας μπορεί να επηρεαστεί καθώς και να αντικατασταθεί η νόμιμη υπηρεσία με μια κακόβουλη	Ισχυρή πιστοποίηση και εξουσιοδότηση, προσέγγιση προσωρινής μνήμης SYN, μηχανισμός τείχους προστασίας στο επίπεδο IaaS, ενεργός μηχανισμός παρακολούθησης στο επίπεδο IaaS. Κατάλληλη διαμόρφωση εικονικών μηχανών, διαμόρφωση πόρων δικτύου στο επίπεδο IaaS. Πρόληψη κατά την εγγραφή πηγαίου κώδικα στο επίπεδο SaaS, εκτέλεση του μηχανισμού ελέγχου ορίων πίνακα στο επίπεδο SaaS. Χρήση καλού IDS καθώς και κατάλληλης διαμόρφωσης ασφάλειας για το δίκτυό και τα ΛΣ των δικτυομένων μηχανημάτων για επιθέσεις ping of death
Επίθεση έκχυσης υπηρεσίας (Service injection attack)	Δημιουργία μιας κακόβουλης εικονικής μηχανής ή υπηρεσίας και	SaaS , PaaS, IaaS	Μια κακόβουλη υπηρεσία παρέχεται στους χρήστες αντί για την έγκυρη	Ισχυροί μηχανισμοί απομόνωσης μεταξύ εικονικών μηχανών, σκλήρυνση υπερεπόπτη, χρήση της συνάρτησης

	προσθήκη της στο νέφος με σκοπό την εξαπάτηση του συστήματος ώστε να την θεωρήσει έγκυρη με τελικό σκοπό την ανακατεύθυνση των χρηστών στην κακόβουλη εικονική μηχανή ή υπηρεσία		υπηρεσία	κατακερματισμού για τον έλεγχο της ακεραιότητας της υπηρεσίας, υιοθέτηση ασφαλών προγραμμάτων περιήγησης ιστού και API
Επίθεση στην εικονικοποίηση	Επίθεση σε εικονική μηχανή και στο επίπεδο υπερεπόπτη	IaaS	Πρόσβαση στα διαπιστευτήρια ενός άλλου χρήστη, πλήρης έλεγχος εικονικής μηχανής μέσω hypervisor, υπερφόρτωση φυσικών μηχανών, διαρροή προσωπικών δεδομένων, προσβολή ακεραιότητας δεδομένων & προγραμμάτων	Χρήση αξιόπιστου συντονιστή (trusted coordinator), παρακολούθηση δραστηριοτήτων υπερεπόπτη, σκλήρυνση υπερεπόπτη & του ΛΣ στο οποίο τρέχει, καλύτερη απομόνωση εικονικών μηχανών
User to root επιθέσεις	Υπερχείλιση δεδομένων (buffer overflow). Πρόσβαση σε όλους τους πόρους ενός έγκυρου χρήστη. Επίθεση σε επίπεδο χρήστη	IaaS, PaaS ,SaaS	Επηρεάζεται το απόρρητο των ευαίσθητων πληροφοριών καθώς και η διαθεσιμότητα και ακεραιότητα των υπηρεσιών	Χρήση ισχυρών κωδικών πρόσβασης, καλύτερος μηχανισμός ελέγχου ταυτότητας, ασφαλής επικοινωνία και APIs, κατάλληλος έλεγχος πρόσβασης, απενεργοποίηση ριζικών λογαριασμών, σκλήρυνση του ΛΣ
Επίθεση ενδιάμεσου (Man-	Παρεμβολή ανάμεσα στην	SaaS, PaaS, IaaS	Διείσδυση στο απόρρητο και την	Απαιτείται ασφαλής επικοινωνία μέσω TLS,

in-middle attack)	επικοινωνία πελάτη-υπηρεσίας		ασφάλεια των δεδομένων και/ή αναμετάδοση τροποποιημένων δεδομένων	χρήση υπογραφών για την ακεραιότητα των ανταλλασσόμενων δεδομένων, χρήση συστημάτων ανίχνευσης και πρόληψης εισβολών (IDPS), σωστή διαμόρφωση των τειχών προστασίας και των δρομολογητών, χρήση μηχανισμών παρακολούθησης και ελέγχου
Επίθεση πλαστογράφησης μεταδεδομένων	Τροποποίηση του αρχείου πληροφοριών υπηρεσίας όπως το WSDL. Επίθεση σε επίπεδο υπηρεσίας	SaaS	Αλλαγή της συμπεριφοράς της υπηρεσίας, τροποποίηση περιεχομένου του αρχείου, παροχή δικαιωμάτων πρόσβασης σε επίπεδο διαχειριστή, τροποποίηση ή διαγραφή assertions ασφάλειας ώστε να χρησιμοποιηθούν αδύναμοι αλγόριθμοι κρυπτογράφησης καθώς και να διαρρεύσουν δεδομένα	Χρήση ασφαλούς πρωτοκόλλου μεταφοράς (HTTP + TLS), χρήση ψηφιακής υπογραφής XML που εφαρμόζεται στο WSDL από τον αρχικό υλοποιητή της υπηρεσίας, ισχυρός έλεγχος ταυτότητας για την πρόσβαση σε αυτόν τον τύπο αρχείου
Επίθεση Ηλ. Ψαρέματος (Phishing)	Μπορεί να επιτευχθεί με διάφορους τρόπους (πχ. αποστολή URL μέσω email και πλοήγηση	SaaS, PaaS	Επηρεάζεται το απόρρητο των διαπιστευτηρίων χρήστη που δεν πρέπει να αποκαλυφθούν	Χρήση μαύρων και λευκών λιστών ονομάτων τομέων και ιστοτόπων, χρήση οπτικής ανίχνευσης ομοιότητας, χρήση μηχανικής μάθησης, ευαισθητοποίηση/εκπαίδε

	θύματος στον αντίστοιχο κακόβουλο ιστότοπο του URL)			υση χρηστών, χρήση μηχανισμών παρακολούθησης και ελέγχου, χρήση ελέγχων ακεραιότητας και χρήση μηχανισμών ανίχνευσης βάσει σεναρίου

3.2.1 Zombie επίθεση (DoS/DDoS επίθεση)

Η επίθεση άρνησης υπηρεσίας είναι ένας τύπος επίθεσης στην οποία ένας επιτιθέμενος στέλνει χιλιάδες πακέτα αιτημάτων στο θύμα, μέσω του Διαδικτύου. Ο κύριος στόχος του επιτιθέμενου είναι να κατακλύσει τον στόχο-θύμα με μεγάλο αριθμό αιτημάτων ώστε να εξαντλήσει όλους τους πόρους του, σπαταλώντας την υπολογιστική ισχύ, τον χρόνο απόδοσης και τις κρυπτογραφικές λειτουργίες. Αυτός ο τύπος επίθεσης μπορεί να επηρεάσει την πραγματική συμπεριφορά του υπολογιστικού νέφους και τη διαθεσιμότητα των υπηρεσιών του (ως προς τους νόμιμους χρήστες). [6]

Ο επιτιθέμενος εκμεταλλεύεται αδυναμίες ή τον τρόπο λειτουργίας δικτυακών πρωτοκόλλων, π.χ. του Πρωτοκόλλου Ελέγχου Μεταφοράς (TCP) (Επιθέσεις SYN), του NTP (επίθεση ενίσχυσης), του Πρωτοκόλλου Ελέγχου Μηνυμάτων Διαδικτύου (ICMP) (επίθεση πλημμυρίσματος ICMP), και του Ping (επίθεση ping of death), την μορφή των πακέτων (επίθεση δύσμορφων πακέτων) καθώς επίσης και αδυναμιών ελέγχου εισόδου (επίθεση υπερχείλισης αποταμιευτή). [6]

Ένας εισβολέας με πλαστή διεύθυνση πηγής πλημμυρίζει με πακέτα TCP με τη σημαία SYN το θύμα του. Το θύμα πιστεύει ότι αυτό το αίτημα προέρχεται από έναν αξιόπιστο χρήστη, και δημιουργεί μια σύνδεση TCP με τη βοήθεια του πρωτοκόλλου τριπλής χειραψίας με την πλαστή διεύθυνση πηγής του εισβολέα. Το θύμα καταναλώνει πόρους για την δημιουργία των συνδέσεων και για κάθε σύνδεση κρατάει κάποιες θέσεις στον αποταμιευτή. Αυτή είναι η πιο συχνή επίθεση που είναι γνωστή ως επίθεση πλημμύρας SYN. [6]

Στην περίπτωση της επίθεσης NTP (Network Time Protocol), ο επιτιθέμενος στέλνει μεγάλο αριθμό πακέτων UDP από πολλές διαφορετικές ψευδείς διευθύνσεις σε μια θύρα που δεν ακούει το θύμα. Αφού το θύμα λάβει τα πακέτα, στέλνει το μήνυμα απάντησης ICMP "Host unreachable" σε όλες αυτές τις ψεύτικες διευθύνσεις. Αυτό έχει ως αποτέλεσμα το θύμα να καταναλώνει πολύ χρόνο για να στείλει τα πακέτα απάντησης, μειώνοντας το επίπεδο απόδοσης και διαθεσιμότητάς του ως προς τους νόμιμους χρήστες. [6]

Στην περίπτωση επίθεσης πλημμυρίσματος ICMP, ο επιτιθέμενος στέλνει πολύ μεγάλο αριθμό πακέτων ICMP “Echo request” σε broadcast διευθυνσεις χρησιμοποιώντας ως διεύθυνση αποστολέα την διεύθυνση του εξυπηρετητή-θύμα αντί για αυτή του επιτιθέμενου. Αυτο έχει ως αποτέλεσμα να απαντήσουν όλοι οι υπολογιστές του δικτύου στον εξυπηρετητή-θύμα με μηνύματα “Echo reply”, κατακλύζοντας το θύμα με απαντήσεις. [6]

Στις επιθέσεις τύπου ping of death, στέλνονται μεγάλα πακέτα ping στο θύμα ώστε αυτό να κρασάρει ή να επανεκκινείται συνεχώς. Πολλοί τύποι υπολογιστών και ειδικότερα λειτουργικών συστημάτων δεν μπορούν να χειριστούν πακέτα ping που έχουν μέγεθος μεγαλύτερο από 65,535 bytes οπότε είτε κρασάρουν είτε επανεκκινούνται. Κατά την επίθεση αυτή, λοιπόν, στέλνονται συνεχώς πακέτα ping

άνω των 65,535 bytes ώστε το θύμα να τίθεται συνεχώς εκτός λειτουργίας. Η αποστολή πακέτου ping μεγαλύτερου μεγέθους δεν επιτρέπεται, ωστόσο ο επιτιθέμενος μπορει να σπάσει το πακέτο ping σε δύο τμήματα και να το στείλει ως δυο ξεχωριστα πακέτα IP, με αποτέλεσμα όταν το θύμα τα λάβει, να τα συνθέσει ώστε να δημιουργηθεί το μεγάλο πακέτο και έτσι να προκληθούν τα αντίστοιχα σφάλματα. [16]

Μια άλλη τεχνική επίθεσης είναι αυτή της υπερχείλισης αποταμιευτή (buffer overflow). Σε μια τέτοια επίθεση, ο επιτιθέμενος στέλνει μεγάλα δεδομένα στο θύμα που όχι μόνο προκαλούν υπερχείλιση του αποταμιευτή αλλά μπορούν να εκχύσουν κακόβουλο κώδικα και να κάνουν εκτροπή εκτέλεσης προς αυτόν. Ως αποτέλεσμα, η μηχανή του θύματος θα ελέγχεται έπειτα από τον επιτιθέμενο. Ο επιτιθέμενος θα μπορούσε είτε να βλάψει το μηχάνημα του θύματος είτε να χρησιμοποιήσει το μολυσμένο μηχάνημα για να εκτελέσει μια επίθεση DoS που βασίζεται στο νέφος. [16]

Ένας άλλος τύπος επίθεσης είναι γνωστός ως επίθεση κατανεμημένης άρνησης υπηρεσίας (DDoS). Μια τέτοια επίθεση είναι πολύ πιο περίπλοκη και πιο δύσκολο να εντοπιστεί σε σύγκριση με μια επίθεση DoS. Σε μια επίθεση DDoS, ο επιτιθέμενος καλεί έναν χειριστή, ο οποίος πρώτα σαρώνει ολόκληρο το δίκτυο και απαριθμεί όλους τους κεντρικούς υπολογιστές που έχουν εκμεταλλεύσιμες ευπάθειες και έπειτα εκμεταλλεύεται τις ευπάθειες αυτές ώστε να μετατρέψει τους υπολογιστές αυτούς σε ένα στόλο από ζόμπι. Τέλος, ο χειριστής εξαπολύει την επίθεση στέλνοντας απομακρυσμένες εντολές στο κάθε υπολογιστή-ζόμπι από τον στόλο. [16]

Για την αντιμετώπιση των προαναφερόμενων ειδών επιθέσεων απαιτείται ισχυρή πιστοποίηση και εξουσιοδότηση των χρηστών, προσέγγιση προσωρινής μνήμης SYN ώστε να αποφεύγεται η περιττή επανεπεξεργασία των πακέτων SYN και να μειώνεται ο αριθμός συνδέσεων που πρέπει να παρακολουθεί ο διακομιστής για την βελτίωση της ικανότητας του διακομιστή να χειρίζεται τα αιτήματα σύνδεσης κατα την διάρκεια μιας επίθεσης DoS στο επίπεδο PaaS, μηχανισμός τείχους προστασίας στο επίπεδο IaaS, ενεργός μηχανισμός παρακολούθησης στο επίπεδο IaaS για τις επιθέσεις στο TCP. Επιπλέον, απαιτείται κατάλληλη διαμόρφωση εικονικών μηχανών στο επίπεδο PaaS και κατάλληλη διαμόρφωση πόρων δικτύου στο επίπεδο IaaS για τις επιθέσεις στο ICMP. Επιπρόσθετα, χρειάζεται η εκτέλεση του μηχανισμού ελέγχου ορίων πίνακα στο επίπεδο SaaS για τις επιθέσεις buffer overflow. Τέλος, απαιτείται η χρήση ενός καλού IDS καθώς και η κατάλληλη διαμόρφωση ασφάλειας για το δίκτυό και τα ΛΣ των δικτυωμένων μηχανημάτων για τις επιθέσεις ping of death. [6] [16]

3.2.2 Επίθεση έγχυσης υπηρεσίας (Service injection)

Το σύστημα του υπολογιστικού νέφους παρέχει υπηρεσίες στον χρήστη του. Όταν ένας χρήστης θέλει να αποκτήσει πρόσβαση σε μια υπηρεσία πρώτα στέλνει ένα αίτημα στην υπηρεσία που περιτυλίγει έναν πόρο, η οποία εκτελείται στο υπολογιστικό νέφος, και το σύστημα του υπολογιστικού νέφους είναι υπεύθυνο για την παροχή χρήσης των πόρων της ζητούμενης υπηρεσίας. Όταν ένας επιτιθέμενος πραγματοποιεί επίθεση έγχυσης κακόβουλου λογισμικού, αυτό σημαίνει ότι είτε θα πραγματοποιήσει έγχυση κακόβουλων εικονικών μηχανών στην περίπτωση επίθεσης σε IaaS είτε θα υλοποιήσει μια κακόβουλη υπηρεσία στο νέφος στην περίπτωση επίθεσης σε PaaS ή SaaS [17]. Για να πραγματοποιηθεί η επίθεση, ο επιτιθέμενος αρχικα δημιουργεί την κακόβουλη εικονική μηχανή ή την κακόβουλη υπηρεσία και στην συνέχεια την προσθέτει/εκχύει στο νέφος. Το επόμενο βήμα είναι να εξαπατήσει το σύστημα του υπολογιστικού νέφους ωστε να θεωρήσει αυτους τους κακόβουλους πόρους ως έγκυρους - εάν επιτευχθεί αυτό τότε το σύστημα του υπολογιστικού νέφους ανακατευθύνει τους χρήστες στην κακόβουλη εικονική μηχανή ή υπηρεσία [18].

Ο αρχικός πόρος δεν αντικαθίσταται, απλώς δημιουργείται ένας νέος πόρος, παρεμφερής με τον αρχικό, ο οποίος μπορεί να ξεγελάσει τους χρήστες πως είναι ο αρχικός που προσφέρεται από τον πάροχο. Επομένως, ενδέχεται να γίνει χρήση του νέου πόρου από ανυποψίαστους χρήστες. Σε αυτή την περίπτωση, ο κακόβουλος χρήστης μπορεί να δημιουργήσει έναν πόρο που μοιάζει με τον έγκυρο καθώς και να χρησιμοποιήσει παρόμοιες διεπαφές ή URL για να το πετύχει αυτό (εκτός από το να αντιγράφει τα μεταδεδομένα του αρχικού πόρου ώστε να εμφανίζεται μαζί του στις σχετικές αναζητήσεις των χρηστών). Αυτό μπορεί να επηρεάσει τις πραγματικές λειτουργίες του υπολογιστικού νέφους. Για παράδειγμα, μπορεί να υποκλαπούν ή να τροποποιηθούν δεδομένα και να αποκλειστούν χρήστες ή υπηρεσίες [17].

Για την προστασία από αυτό τον τύπο επίθεσης θα πρέπει να εφαρμοστούν τα εξής: σκλήρυνση υπερεπόπτη, ισχυροί μηχανισμοί απομόνωσης μεταξύ των εικονικών μηχανών, έλεγχοι εικόνων εικονικών μηχανών πριν χρησιμοποιηθούν για την δημιουργία στιγμιότυπων, έλεγχοι δοχείων (containers) τα οποία υλοποιούν υπηρεσίες ή συστατικά τους και έλεγχοι της ακεραιότητας της υπηρεσίας και της ασφάλειας της υπηρεσίας Ιστού. [6]

3.2.3 Επίθεση στην εικονικοποίηση / υπερεπόπτη

Η επίθεση εικονικοποίησης στο νέφος αποτελείται από διάφορους τύπους. Παραδείγματα τέτοιων τύπων επιθέσεων μπορεί να είναι η διαφυγή εικονικών μηχανών (VM escape) και η εγκατάσταση rootkit στον υπερεπόπτη (hypervisor). Ο Υπερεπόπτης στέκεται ως φράγμα που χωρίζει τους πόρους υλικού και τις Εικονικές Μηχανές, προσφέροντας (σχεδόν) πλήρη απομόνωση για την κάθε Εικονική Μηχανή. Η επίθεση διαφυγής εικονικής μηχανής οδηγεί σε μια παραβίαση του περιβάλλοντος εικονικοποίησης από έναν επιτιθέμενο που θα μπορούσε να εκμεταλλευτεί την εικονική μηχανή που τρέχει πάνω από τον υπερεπόπτη. Ως αποτέλεσμα, η εικονική μηχανή δραπετεύει από τη σφαίρα της απομόνωσης. Η επίθεσης αυτή μπορεί να πραγματοποιηθεί όταν ο εισβολέας εκτελεί έναν κώδικα σε μια εικονική μηχανή, επιτρέποντας σε ένα λειτουργικό σύστημα που τρέχει μέσα στον υπερεπόπτη να “σπάσει” και να αλληλεπιδράσει απευθείας μαζί του. Αυτό το είδος επίθεσης μπορεί να επιτρέψει στον εισβολέα να έχει πρόσβαση στο λειτουργικό σύστημα του υπολογιστή φιλοξενίας και σε κάθε εικονική μηχανή που λειτουργεί σε αυτόν τον υπολογιστή [19].

Τα Rootkits είναι ένα είδος κακόβουλου λογισμικού που κρύβεται μέσα σε μολυσμένα συστήματα, χειραγωγώντας με κάποιο τρόπο τα αποτελέσματα της κλήσης συστήματος του λειτουργικού συστήματος. Εστιάζει στην παραβίαση και στον έλεγχο του θύματος από τον επιτιθέμενο. Μόλις εγκατασταθεί, το rootkit και το payload τους καθίστανται αόρατα για το λειτουργικό σύστημα και τις εφαρμογές. Το rootkit επικεντρώνονται στην παροχή κάλυψης για το payload που συνήθως παρέχει απομακρυσμένο έλεγχο (π.χ. backdoors) ή παθητική συλλογή πληροφοριών (π.χ. keyloggers). Ως εκ τούτου, ένα rootkit μπορεί εύκολα να γίνει η βάση για μια επόμενη επίθεση. [20]

Για την αποφυγή αυτών των επιθέσεων απαιτούνται λύσεις ασφαλείας υπερεπόπτη, όπως για παράδειγμα η χρήση αξιόπιστου συντονιστή (trusted coordinator) για τη διαχείριση και την επιβολή πολιτικών ασφαλείας, ελέγχων πρόσβασης και συνολικής ασφάλειας σε ένα περιβάλλον νέφους ώστε να επιτυγχάνεται η διασφάλιση της ακεραιότητας, της εμπιστευτικότητας και της διαθεσιμότητας των πόρων και των δεδομένων που είναι αποθηκευμένα στο νέφος, η παρακολούθηση δραστηριοτήτων υπερεπόπτη, καθώς και καλύτερη απομόνωση των εικονικών μηχανών. [6]

3.2.4 User to root επιθέσεις

Σε αυτή την επίθεση, ο εισβολέας αποκτά πρόσβαση στον νόμιμο λογαριασμό του χρήστη μέσω του κωδικού πρόσβασης, εφόσον τον έχει υποκλέψει. Αυτό τον καθιστά ικανό να εκμεταλλευτεί τις ευπάθειες του συστήματος για να αποκτήσει πρόσβαση σε επίπεδο root στο σύστημα. Για παράδειγμα, οι υπερχειλίσεις αποταμιευτών χρησιμοποιούνται για τη δημιουργία ριζικών κελύφων (root shells) από μια διαδικασία που εκτελείται ως root. Οι μηχανισμοί που χρησιμοποιούνται για την ασφάλεια της διαδικασίας ελέγχου ταυτότητας αποτελούν συχνό στόχο, καθώς δεν υπάρχουν καθολικοί τυπικοί μηχανισμοί ασφαλείας που μπορούν να χρησιμοποιηθούν για την πρόληψη κινδύνων ασφαλείας, όπως η αδύναμη ανάκτηση κωδικού πρόσβασης, επιθέσεις ηλ. ψαρέματος, keylogger κ.λπ. Στην περίπτωση του νέφους, ο εισβολέας αποκτά πρόσβαση σε έγκυρους λογαριασμούς χρήστη που του επιτρέπουν να αποκτήσει πρόσβαση σε επίπεδο ρίζας (root) σε εικονική μηχανή. [21]

Για την αποφυγή τέτοιων επιθέσεων πρέπει να γίνεται έλεγχος δεδομένων και μηνυμάτων που αποστέλλονται από τον χρήστη, εφαρμογή της αρχής των ελαχίστων προνομίων, σύμφωνα με την οποία στους χρήστες χορηγούνται τα ελάχιστα προνόμια που είναι απαραίτητα για την εκτέλεση των καθηκόντων τους, χρήση τείχους προστασίας, κατάλληλος έλεγχος πρόσβασης και μηχανισμοί παρακολούθησης/καταγραφής, σκλήρυνση του λειτουργικού συστήματος, απενεργοποίηση ριζικών λογαριασμών και ανάπτυξη λύσεων host-based IDS που να ανακαλύπτουν ύποπτη συμπεριφορά εντός των εικονικών μηχανών.[6]

3.2.5 Επίθεση Ενδιάμεσου

Η επίθεση ενδιάμεσου (man-in-the-middle) πραγματοποιείται όταν ένας επιτιθέμενος είναι ενεργός ενδιάμεσα σε μια συνδεση και έχει πρόσβαση στα δεδομένα που διαβιβάζονται μεταξύ των δύο μερών της σύνδεσης. Τα δύο αρχικά μέρη εξακολουθούν να φαίνεται πως επικοινωνούν κανονικά μεταξύ τους. Ο αποστολέας του μηνύματος δεν αναγνωρίζει ότι ο παραλήπτης είναι ένας άγνωστος εισβολέας που προσπαθεί να αποκτήσει πρόσβαση (παθητική επίθεση) ή να τροποποιήσει το μήνυμα και να το αναμεταδόσει στον δέκτη (ενεργητική επίθεση). Έτσι, ο εισβολέας ελέγχει ολόκληρη την επικοινωνία[22]. Τα δύο μέρη, επικοινωνούν μεταξύ τους στο υπολογιστικό νέφος, έτσι όταν ένας εισβολέας παρεμβάλλεται μπορεί να έχει πρόσβαση στα ανταλλασσόμενα δεδομένα και να τα τροποποιήσει, εφόσον το κανάλι επικοινωνίας δεν είναι ασφαλές. [6]

Η αποφυγή τέτοιων επιθέσεων μπορεί να γίνει με τη χρήση αμοιβαίου ελέγχου ταυτότητας μεταξύ του χρήστη και του διακομιστή μέσω της χρήσης δημόσιων και ιδιωτικών κλειδίων και σωστής διαμόρφωσης του TLS καθώς και χρήσης της πιο πρόσφατης έκδοσής του, τη χρήση συστημάτων ανίχνευσης και πρόληψης εισβολών (IDPS) ώστε να παρακολουθείται η κυκλοφορία του δικτύου και να εντοπίζονται ανωμαλίες ή ύποπτη συμπεριφορά που υποδηλώνει πως έγινε επίθεση MITM, την υλοποίηση ασφαλούς διαμόρφωσης των τειχών προστασίας και των δρομολογητών ώστε να αποτρέπουν τη μη εξουσιοδοτημένη πρόσβαση και να προστατεύουν από επιθέσεις, καθώς και την εφαρμογή ισχυρών μηχανισμών καταγραφής, παρακολούθησης και ελέγχου για τον εντοπισμό και τη διερεύνηση τυχόν ύποπτων δραστηριοτήτων. [22]

3.2.6 Επίθεση πλαστογράφησης μεταδεδομένων

Η λειτουργικότητα και οι τεχνικές λεπτομέρειες μιας υπηρεσίας (ιστού) αποθηκεύονται στο αρχείο WSDL. Η επίθεση πλαστογράφησης μεταδεδομένων στοχεύει στον κακόβουλο ανασχεδιασμό των

περιγραφών μεταδεδομένων των Υπηρεσιών Ιστού. Για παράδειγμα, ένας επιτιθέμενος μπορεί να τροποποιήσει το WSDL μιας υπηρεσίας έτσι ώστε μια κλήση σε μια λειτουργία deleteUser() να μοιάζει συντακτικά με κλήση σε άλλη λειτουργία, π.χ. setAdminRights(). Έτσι, μόλις δοθεί σε έναν χρήστη ένα τέτοιο τροποποιημένο έγγραφο WSDL, κάθε μία από τις επικλήσεις λειτουργίας του deleteUser() θα έχει ως αποτέλεσμα την αποστολή μηνυμάτων αιτήσεων SOAP που στην πλευρά του διακομιστή μοιάζουν, και επομένως ερμηνεύονται ως επικλήσεις της λειτουργίας setAdminRights(). Εν τέλει, ένας επιτιθέμενος θα μπορούσε να καταφέρει να δημιουργήσει μια δέσμη λογαριασμών χρήστη που θεωρείται ότι διαγράφονται από τη σημασιολογία της εφαρμογής, αλλά στην πραγματικότητα εξακολουθούν να ισχύουν και επιπλέον παρέχουν δικαιώματα πρόσβασης σε επίπεδο διαχειριστή. [23]

Καθώς το ίδιο το σύστημα νέφους έχει κάποιο είδος λειτουργίας αποθετηρίου WSDL (συγκρίσιμο με ένα μητρώο UDDI (Universal Description, Discovery, and Integration)), οι νέοι χρήστες πιθανότατα θα αιτούνται το αρχείο WSDL μιας υπηρεσίας με πιο δυναμικό τρόπο (μέσω ενός τελικού σημείου API ή μια λύση βασισμένη στον ιστό που διευκολύνει την ανάκτηση του αρχείου WSDL). Ο επιτιθέμενος πραγματοποιεί αναγνώριση για να εντοπίσει την υπηρεσία ιστού-στόχο και το σχετικό αρχείο WSDL. Μπορεί να χρησιμοποιήσει διάφορες τεχνικές, όπως σάρωση, παρακολούθηση δικτύου ή εξέταση της δημόσιας τεκμηρίωσης, για να εντοπίσει το αρχείο WSDL. Ο επιτιθέμενος φιλοξενεί το ψεύτικο αρχείο WSDL σε έναν διακομιστή υπό τον έλεγχό του. Μπορεί να χρησιμοποιήσει τεχνικές, όπως δηλητηρίαση DNS, πειρατεία τομέα ή χειραγώγηση URL, για να ανακατευθύνει τους καταναλωτές στον διακομιστή που φιλοξενεί το παραποιημένο WSDL. Όταν ένας νόμιμος καταναλωτής προσπαθεί να αποκτήσει πρόσβαση στην υπηρεσία ιστού, ανακτά το αρχείο WSDL για να κατανοήσει τη δομή και τις διαθέσιμες λειτουργίες της υπηρεσίας. Ωστόσο, λόγω της παραποίησης, ο καταναλωτής καλεί και λαμβάνει εν αγνοία του το ψεύτικο αρχείο WSDL αντί για το γνήσιο. Με τον καταναλωτή να επικοινωνεί εν αγνοία του με τον διακομιστή του επιτιθέμενου, ο επιτιθέμενος μπορεί να εξαπολύσει διάφορους τύπους επιθέσεων. Για παράδειγμα, μπορεί να επιχειρήσει να κλέψει διαπιστευτήρια χρήστη, να εισάγει κακόβουλο κώδικα, να εκτελέσει χειραγώγηση δεδομένων ή να αποκτήσει μη εξουσιοδοτημένη πρόσβαση σε ευαίσθητες πληροφορίες ή λειτουργίες. Έτσι, είναι πιθανή η εξάπλωση του κακόβουλου αρχείου WSDL και επομένως υπάρχει η πιθανότητα για μια επιτυχημένη επίθεση. [23]

Για την λύση αυτής της επίθεσης, οι πληροφορίες σχετικά με τη λειτουργικότητα της υπηρεσίας και άλλες λεπτομέρειες θα πρέπει να μεταφέρονται μέσω ασφαλούς πρωτοκόλλου (HTTP + TLS). Επίσης, ένα άλλο μέτρο που θα μπορούσε να χρησιμοποιηθεί είναι η χρήση ψηφιακής υπογραφής XML που εφαρμόζεται στο WSDL αρχείο από τον αρχικό υλοποιητή της υπηρεσίας ώστε να εξασφαλίζεται η ακεραιότητα του. Τέλος, θα πρέπει να απαιτείται ισχυρός έλεγχος ταυτότητας για την πρόσβαση σε αυτόν τον τύπο αρχείου. [6] [23]

3.2.7 Επίθεση Ηλεκτρονικού Ψαρέματος

Οι επιθέσεις ηλ. ψαρέματος (phishing) στο νέφος αναφέρονται σε κακόβουλες απόπειρες εξαπάτησης των χρηστών και απόκτησης μη εξουσιοδοτημένης πρόσβασης στους λογαριασμούς τους στο νέφος ή σε ευαίσθητες πληροφορίες τους εκμεταλλευόμενοι ανθρώπινες ευπάθειες. Το ηλεκτρονικό ψάρεμα

είναι μια μορφή επίθεσης κοινωνικής μηχανικής[18] όπου οι επιτιθέμενοι υποδύονται αξιόπιστες οντότητες, όπως νόμιμες εταιρείες ή παρόχους υπηρεσιών νέφους, για να εξαπατήσουν τους χρήστες ώστε να αποκαλύψουν τα στοιχεία σύνδεσης, τις οικονομικές πληροφορίες ή άλλα ευαίσθητα δεδομένα τους. [24]

Υπάρχουν διάφορα είδη επιθέσεων ηλεκτρονικού ψαρέματος, όπως το Email Phishing, το Spear Phishing και την Συλλογή διαπιστευτηρίων (Credential Harvesting). Στην περίπτωση του email phishing, οι επιτιθέμενοι αποστέλλουν μηνύματα ηλεκτρονικού ταχυδρομείου που εμφανίζονται να προέρχονται από νόμιμη πηγή, όπως ένας πάροχος υπηρεσιών νέφους, και προτρέπουν τους χρήστες να κάνουν κλικ σε συνδέσμους προς κακόβουλους ιστότοπους ή να εκφορτώσουν μολυσμένα αρχεία. Οι επιθέσεις spear phishing είναι πιο στοχευμένες επιθέσεις ηλ. ψαρέματος . Σε αυτές τις επιθέσεις, οι επιτιθέμενοι προσαρμόζουν τις προσπάθειες ψαρέματος σε συγκεκριμένα άτομα ή οργανισμούς, συλλέγοντας πληροφορίες σχετικά με τον στόχο από διάφορες πηγές για να κάνουν τα emails ή τα μηνύματά τους να φαίνονται πιο νόμιμα. Τέλος, στην περίπτωση των επιθέσεων συλλογής διαπιστευτηρίων (Credential Harvesting), οι επιτιθέμενοι δημιουργούν ψεύτικες φόρμες σύνδεσης ή χρησιμοποιούν παραβιασμένους νόμιμους ιστότοπους για να συλλέγουν τα διαπιστευτήρια σύνδεσης των χρηστών όταν αυτοί τα εισάγουν. [79]

Κάποιες λύσεις για αυτές της επιθέσεις θα μπορούσαν να είναι η χρήση μαύρων και λευκών λιστών ονομάτων τομέων και ιστοτόπων, η χρήση οπτικής ανίχνευσης ομοιότητας διεπαφών κακόβουλων ιστοτόπων και μηνυμάτων, η χρήση μηχανισμών παρακολούθησης και ελέγχου για τον εντοπισμό της ύποπτης συμπεριφοράς του δικτύου, η χρήση ελέγχων ακεραιότητας και μηχανισμών ανίχνευσης βάσει σεναρίου. Σημαντικό είναι να σημειωθεί ότι ένα πολύ χρήσιμο μέτρο κατά του ηλ. ψαρέματος και εν γένει των επιθέσεων κοινωνικής μηχανικής είναι η ενημέρωση, εκπαίδευση και η ευαισθητοποίηση των χρηστών. [25]

[18] Η κοινωνική μηχανική αναφέρεται στη χειραγώγηση της ανθρώπινης ψυχολογίας και συμπεριφοράς για την εξαπάτηση ατόμων ή οργανισμών ώστε να αποκαλύψουν ευαίσθητες πληροφορίες, να εκτελέσουν ορισμένες ενέργειες ή να παραχωρήσουν μη εξουσιοδοτημένη πρόσβαση σε εμπιστευτικά συστήματα ή δεδομένα. Οι επιθέσεις κοινωνικής μηχανικής εκμεταλλεύονται την ανθρώπινη εμπιστοσύνη, περιέργεια, φόβο ή έλλειψη ευαισθητοποίησης για να επιτύχουν τους στόχους τους.

3.3 Πραγματικές επιθέσεις

3.3.1 Amazon EC2, S3 (2011)

Το 2011, ερευνητές με επικεφαλής τον Δρ. Jorg Schwenk από το Ruhr-University Bochum βρήκαν μια κρυπτογραφική τρύπα στις υπηρεσίες EC2 και S3 της Amazon. Το ελάττωμα εντοπίστηκε στο πρωτόκολλο ασφαλείας των υπηρεσιών ιστού (web) και επέτρεπε στους εισβολείς να ξεγελάσουν τους διακομιστές ώστε να εξουσιοδοτήσουν ψηφιακά υπογεγραμμένα μηνύματα SOAP που είχαν τροποποιηθεί. Οι επιτιθέμενοι θα μπορούσαν με αυτό τον τρόπο να ελέγξουν διεπαφές που χρησιμοποιούνται για τη διαχείριση πόρων υπολογιστικού νέφους, οι οποίες θα τους επέτρεπαν να δημιουργήσουν, να τροποποιήσουν και να διαγράψουν εικόνες μηχανών καθώς και να αλλάξουν κωδικούς πρόσβασης και ρυθμίσεις διαχείρισης. [32] [37]

3.3.2 LastPass (2011)

Τον Μάιο του 2011, η LastPass, μια εταιρεία αποθήκευσης και διαχείρισης κωδικών πρόσβασης που βασίζεται στο νέφος, ανακοίνωσε ένα πιθανό επιτυχημένο χακάρισμα στους διακομιστές της. Δεν υπήρξαν αναφορές για διαρροή δεδομένων, αλλά η εταιρεία επέμεινε ότι οι πελάτες πρέπει να λάβουν ορισμένα μέτρα για να διασφαλίσουν ότι οι πληροφορίες τους είναι ασφαλείς. Οι ειδικοί ασφαλείας ανακάλυψαν ασυνήθιστη συμπεριφορά στους διακομιστές της βάσης δεδομένων που είχαν περισσότερη επισκεψιμότητα. Ιδιαίτερα παρατηρήθηκαν ανωμαλίες στην εξερχόμενη κίνηση κατά τη διάρκεια μιας ασυνήθιστης ώρας. Η εταιρεία υπέθεσε (διότι ήταν μια δυνητική επίθεση άρα το αντίκτυπο δεν μπορεί να καθοριστεί με σιγουριά) ότι επρόκειτο για δραστηριότητα πειρατείας που σχετίζεται με τη συλλογή αποθηκευμένων διαπιστευτηρίων σύνδεσης και άλλων ευαίσθητων δεδομένων χρήστη. Οι κύριοι κωδικοί πρόσβασης (κωδικοί πρόσβασης που προστατεύουν λίστες κωδικών πρόσβασης για πρόσβαση σε άλλους ιστότοπους και διαδικτυακές υπηρεσίες στο cloud) άλλαξαν αμέσως για να προστατεύσουν τους πελάτες από πιθανή διαρροή δεδομένων. [38]

3.3.5 Google (2012)

Τον Ιούλιο του 2012, η ομάδα χάκερ, UGNazi, εκμεταλλεύτηκε ένα σημαντικό ελάττωμα στη διαδικασία ανάκτησης κωδικού πρόσβασης στο Gmail της Google και στο σύστημα αυτόματου τηλεφωνητή της AT&T, το οποίο με τη σειρά του επέτρεψε στην ομάδα να έχει πρόσβαση στον προσωπικό λογαριασμό Gmail του Διευθύνοντα Συμβούλου του CloudFlare. [41]

3.3.3 Cloudbleed (2017)

Η Cloudflare είναι μια εταιρία που παρέχει μια σειρά από υπηρεσίες υπολογιστικού νέφους που επικεντρώνονται στη βελτίωση των επιδόσεων, της ασφάλειας και της αξιοπιστίας ενός ιστότοπου.Το περιστατικό "Cloudbleed" αναφέρεται σε μια ευπάθεια διαρροής δεδομένων που επηρέασε το Cloudflare. Η ευπάθεια, CloudBleed, ονομάστηκε ως λογοπαίγνιο, συνδυάζοντας το "Cloudflare" και την ευρέως γνωστή ευπάθεια "Heartbleed". Η ευπάθεια Heartbleed επηρεάζει κυρίως τη βιβλιοθήκη κρυπτογραφικού λογισμικού OpenSSL, η οποία χρησιμοποιείται για την ασφαλή επικοινωνία μέσω του διαδικτύου. Οι πάροχοι υπηρεσιών cloud, όπως και η Cloudflare, συχνά βασίζονται στο OpenSSL για την ασφαλή επικοινωνία μεταξύ των υπηρεσιών τους και των καταναλωτών τους,

συμπεριλαμβανομένης της κρυπτογράφησης των δεδομένων κατά τη μεταφορά και της διαχείρισης ασφαλών συνδέσεων.

Το περιστατικό Cloudbleed ανακαλύφθηκε και αποκαλύφθηκε τον Φεβρουάριο του 2017. Η Cloudflare ανακάλυψε ένα σφάλμα λογισμικού στον κώδικά της που προκαλούσε τυχαίες διαρροές δεδομένων από τη μνήμη. Το σφάλμα, το οποίο εισήχθη ως μέρος μιας ενημέρωσης κώδικα τον Σεπτέμβριο του 2016, έγινε ενεργό σε συγκεκριμένους ιστότοπους πελατών στις 13 Φεβρουαρίου 2017. Το σφάλμα προκάλεσε τη διαρροή δυνητικά ευαίσθητων πληροφοριών από ιστότοπους που χρησιμοποιούσαν τις υπηρεσίες της Cloudflare. Τα δεδομένα που διέρρευσαν, τα οποία περιλάμβαναν cookies HTTP, tokens ελέγχου ταυτότητας, κωδικούς πρόσβασης απλού κειμένου και άλλες ευαίσθητες πληροφορίες, αποθηκεύτηκαν ακούσια στην προσωρινή μνήμη από μηχανές αναζήτησης όπως η Google. Η Cloudflare εξυπηρετεί έναν τεράστιο αριθμό ιστότοπων και υπηρεσιών διαδικτύου, οπότε ο αντίκτυπος του σφάλματος ήταν εκτεταμένος. Αν και ο ακριβής αριθμός των επηρεαζόμενων ιστότοπων παραμένει ασαφής, εκτιμάται ότι ενδεχομένως επηρεάστηκαν εκατομμύρια τομείς.

Μόλις η Cloudflare έλαβε γνώση του προβλήματος, η εταιρεία έλαβε άμεσα μέτρα για την αντιμετώπιση της ευπάθειας και τον μετριασμό των επιπτώσεων. Η Cloudflare απενεργοποίησε ορισμένες λειτουργίες, καθάρισε τα δεδομένα που αποθηκεύτηκαν στην προσωρινή μνήμη και συνεργάστηκε με τις μηχανές αναζήτησης για να αφαιρέσει τυχόν διαρρεύσαντα δεδομένα από τα ευρετήριά τους. Η Cloudflare γνωστοποίησε αμέσως το περιστατικό στο κοινό και δημιούργησε έναν ειδικό ιστότοπο για την παροχή ενημερώσεων και πληροφοριών. Η εταιρεία ξεκίνησε επίσης έρευνα για να εκτιμήσει την έκταση της διαρροής δεδομένων και ήρθε σε άμεση επαφή με τους πελάτες που επλήγησαν. Ως απάντηση στο περιστατικό, η Cloudflare συνέστησε στους χρήστες να αλλάξουν τους κωδικούς πρόσβασης για τους ιστότοπους που χρησιμοποιούσαν υπηρεσίες της Cloudflare, ειδικά εάν είχαν συνδεθεί κατά την περίοδο που ήταν ενεργό το σφάλμα. Οι χρήστες ενθαρρύνθηκαν επίσης να ενεργοποιήσουν τον έλεγχο ταυτότητας δύο παραγόντων, όπου είναι διαθέσιμος. Το περιστατικό Cloudbleed ανέδειξε τη σημασία της διαχείρισης της ασφάλειας και των τρωτών σημείων στις διαδικτυακές υπηρεσίες. Η ανταπόκριση της Cloudflare στο περιστατικό, συμπεριλαμβανομένης της διαφάνειας και της συνεργασίας με τα θιγόμενα μέρη, συνέβαλε στην αντιμετώπιση του ζητήματος και στην ελαχιστοποίηση της πιθανής βλάβης των χρηστών. [39]

3.3.4 Capital One Data Breach (2019)

Ένας χάκερ απέκτησε μη εξουσιοδοτημένη πρόσβαση στην υποδομή νέφους του Capital One που φιλοξενείται στις Υπηρεσίες Ιστού της Amazon (AWS). Η παραβίαση δεδομένων της Capital One που συνέβη το 2019, ήταν μία από τις μεγαλύτερες παραβιάσεις δεδομένων που είχαν ως στόχο χρηματοπιστωτικό ίδρυμα εκείνη την εποχή. Τον Ιούλιο του 2019, η Capital One Financial Corporation, μια μεγάλη εταιρεία χαρτοφυλακίου τραπεζών, ανακοίνωσε ότι είχε σημειωθεί παραβίαση δεδομένων, η οποία επηρέασε περίπου 100 εκατομμύρια άτομα στις Ηνωμένες Πολιτείες και περίπου 6 εκατομμύρια άτομα στον Καναδά. Ένας πρώην υπάλληλος της εταιρείας παροχής υπηρεσιών νέφους, ο οποίος είχε προηγουμένως συνεργαστεί με την Capital One, εκμεταλλεύτηκε ένα λανθασμένα ρυθμισμένο τείχος προστασίας εφαρμογών ιστού (WAF) για να αποκτήσει μη

εξουσιοδοτημένη πρόσβαση στα δεδομένα πελατών της Capital One. Το άτομο, που αναγνωρίστηκε ως Paige Thompson, συνελήφθη και κατηγορήθηκε για ομοσπονδιακά εγκλήματα που σχετίζονται με την παραβίαση δεδομένων. Η παραβίαση δεδομένων εξέθεσε σημαντικό αριθμό προσωπικών πληροφοριών, συμπεριλαμβανομένων ονομάτων, διευθύνσεων, ημερομηνιών γέννησης, πιστωτικών βαθμολογιών, δεδομένων αιτήσεων για πιστωτικές κάρτες και αριθμών κοινωνικής ασφάλισης των επηρεαζόμενων ατόμων. Ωστόσο, είναι σημαντικό να σημειωθεί ότι δεν εκτέθηκαν σε κίνδυνο οι αριθμοί κοινωνικής ασφάλισης όλων των πελατών.

Η Capital One ανέλαβε άμεσα δράση για την αντιμετώπιση της παραβίασης, συνεργαζόμενη με τις αρχές επιβολής του νόμου και τους εμπειρογνώμονες κυβερνοασφάλειας για τη διερεύνηση του περιστατικού και τον μετριασμό της πιθανής βλάβης των επηρεαζόμενων πελατών. Η τράπεζα παρείχε, επίσης, βοήθεια και υποστήριξη στα θιγόμενα άτομα, συμπεριλαμβανομένων δωρεάν υπηρεσιών παρακολούθησης της πιστοληπτικής ικανότητας και προστασίας της ταυτότητας Η παραβίαση είχε αξιοσημείωτο αντίκτυπο στην Capital One, οδηγώντας σε οικονομικές απώλειες, ζημία στη φήμη της και ρυθμιστικό έλεγχο. Η Capital One βρέθηκε αντιμέτωπη με έρευνες από διάφορες αρχές, συμπεριλαμβανομένου του Γραφείου του Ελεγκτή Νομίσματος των ΗΠΑ, της Ομοσπονδιακής Τράπεζας και των γενικών εισαγγελέων των πολιτειών. [40]

3.3.6 Microsoft (2019)

Στις 22 Ιανουαρίου 2020, η Microsoft ανακοίνωσε ότι μια από τις βάσεις δεδομένων νέφους της παραβιάστηκε τον Δεκέμβριο του 2019, με αποτέλεσμα την έκθεση 250 εκατομμυρίων καταχωρήσεων, συμπεριλαμβανομένων διευθύνσεων email, διευθύνσεων IP και λεπτομερειών υποθέσεων υποστήριξης.

Σύμφωνα με τον γίγαντα των υπολογιστών, η αιτία αυτής της παραβίασης δεδομένων ήταν η λανθασμένη διαμόρφωση σε διακομιστή δικτύου που φιλοξενούσε τις κρίσιμες πληροφορίες. Αν και αυτή δεν είναι η μεγαλύτερη, ήταν μια από τις πιο συγκλονιστικές επιθέσεις στον κυβερνοχώρο λόγω του υψηλού προφίλ χαρακτήρα του στόχου. [42]

3.3.7 Advanced Info Service (AIS) (2020)

Η παραβίαση δεδομένων της Advanced Info Service (AIS) ανακαλύφθηκε από τον ερευνητή κυβερνοασφάλειας Justin Paine κατά την περιήγηση στο BinaryEdge[19] και στο Shodan[20].

Τον Μάιο του 2020, η Advanced Info Service (AIS), ένας σημαντικός φορέας παροχής υπηρεσιών κινητής τηλεφωνίας στην Ταϊλάνδη, αντιμετώπισε ένα περιστατικό έκθεσης δεδομένων. Το

[19] Η BinaryEdge είναι μια εταιρεία κυβερνοασφάλειας που ειδικεύεται στην παροχή υπηρεσιών σάρωσης του Διαδικτύου και πληροφοριών κυβερνοασφάλειας. Προσφέρει μια ολοκληρωμένη πλατφόρμα που επιτρέπει στους οργανισμούς να ανακαλύπτουν και να παρακολουθούν τα ψηφιακά τους περιουσιακά στοιχεία, να εντοπίζουν τα τρωτά σημεία και να αξιολογούν τους πιθανούς κινδύνους ασφαλείας.

[20] Το Shodan είναι μια μηχανή αναζήτησης ειδικά σχεδιασμένη για την εύρεση συσκευών και υπηρεσιών που είναι συνδεδεμένες στο διαδίκτυο. Ενώ οι παραδοσιακές μηχανές αναζήτησης, όπως η Google, ανιχνεύουν ιστοσελίδες, η Shodan επικεντρώνεται στην ανακάλυψη πληροφοριών σχετικά με συσκευές που είναι συνδεδεμένες στο διαδίκτυο, συμπεριλαμβανομένων διακομιστών, δρομολογητών, webcams, εκτυπωτών, συστημάτων βιομηχανικού ελέγχου και πολλών άλλων τύπων συσκευών.

περιστατικό αυτό αφορούσε λανθασμένη διαμόρφωση ενός εσωτερικού συστήματος, η οποία είχε ως αποτέλεσμα μια βάση δεδομένων που περιείχε προσωπικές πληροφορίες πελατών διαμορφώθηκε λανθασμένα με λανθασμένους ελέγχους πρόσβασης και παρέμεινε δημόσια προσβάσιμη στο διαδίκτυο αντί να περιοριστεί κατάλληλα σε εξουσιοδοτημένους χρήστες ή να προστατευτεί πίσω από κατάλληλα μέτρα ασφαλείας, όπως τείχη προστασίας ή μηχανισμούς ελέγχου ταυτότητας. Είναι σημαντικό να σημειωθεί ότι οι συγκεκριμένες τεχνικές λεπτομέρειες της λανθασμένης διαμόρφωσης δεν έχουν δημοσιοποιηθεί με αναλυτικό τρόπο.

Η βάση δεδομένων περιείχε έναν συνδυασμό αρχείων καταγραφής, ερωτημάτων DNS και αρχείων καταγραφής NetFlow για τους πελάτες της εταιρίας. Χρησιμοποιώντας αυτά τα δεδομένα είναι αρκετά απλό να σχηματιστεί μια εικόνα για το τι κάνει ένα άτομο στο Διαδίκτυο. Σύμφωνα με τον Paine, η βάση δεδομένων που διέρρευσε περιελάμβανε 8,3 δισεκατομμύρια αρχεία καταγραφής ροής δικτύου και αρχεία καταγραφής ερωτημάτων DNS πελατών της εταιρείας τηλεπικοινωνιών AWN που εδρεύει στην Ταϊλάνδη. [43]

3.3.8 Raychat (2021)

Τον Φεβρουάριο του 2021, η Raychat, μια διαδικτυακή εφαρμογή συνομιλίας, επέζησε από μια μεγάλης κλίμακας επίθεση στον κυβερνοχώρο. Μια παραβίαση της κακώς διαμορφωμένης βάσης δεδομένων της στο νέφος έδωσε στους επιτιθέμενους δωρεάν πρόσβαση σε 267 εκατομμύρια ονόματα χρηστών, email, κωδικούς πρόσβασης, μεταδεδομένα και κρυπτογραφημένες συνομιλίες. Λίγο αργότερα, μια στοχευμένη επίθεση bot διέγραψε το σύνολο των δεδομένων της εταιρείας. Σύμφωνα με αναφορές, μια εσφαλμένη διαμόρφωση της MongoDB άφησε τα δεδομένα ανοιχτά / διαθέσιμα. Η επίθεση υποδεικνύει πώς η κακή διαμόρφωση των βάσεων δεδομένων NoSQL μπορεί να τις κάνει εύκολο στόχο για τους φορείς απειλών bot. Επομένως, οι οργανισμοί πρέπει να διασφαλίζουν ότι οι βάσεις δεδομένων είναι ασφαλείς και άρα έχουν διαμορφωθεί με ασφαλή τρόπο. Η επίθεση φαίνεται να έγινε μόνο για να καταστρέψει την βάση δεδομένων. Την επίθεση δεν ακολουθησε κανένα σημείωμα λύτρων ή απειλές, αλλά μόνο η λέξη "meow" μαζί με ένα τυχαίο σύνολο αριθμών. [46]

3.3.9 Σύνοψη

Από τις παραπάνω επιθέσεις παρατηρούμε οτι στις περισσότερες περιπτώσεις η κυριότερη αιτία είναι η λάθος διαμόρφωση συστημάτων, διακομιστών και APIs . Οι ακατάλληλες διαμορφώσεις των υπηρεσιών και των πόρων του νέφους μπορούν να δημιουργήσουν τρωτά σημεία ασφαλείας. Οι λανθασμένες διαμορφώσεις μπορεί να περιλαμβάνουν αδύναμους ελέγχους πρόσβασης, ακατάλληλα ρυθμισμένα δικαιώματα, μη ασφαλή αποθήκευση ή ανεπαρκείς ρυθμίσεις ασφαλείας δικτύου.

Για τον μετριασμό αυτών των κινδύνων, οι οργανισμοί και οι πάροχοι υπηρεσιών νέφους θα πρέπει να ακολουθούν βέλτιστες πρακτικές, όπως η εφαρμογή ισχυρών ελέγχων πρόσβασης, η τακτική επιδιόρθωση και ενημέρωση των συστημάτων, η σύγκριση των διαμορφώσεων με βιομηχανικά πρότυπα, η χρήση μέτρων προστασίας και η διενέργεια τακτικών ελέγχων ασφαλείας .

4. Μηχανισμοί ελέγχου, μέτρα ασφαλείας και συμμόρφωση ασφάλειας

Ο στόχος των μηχανισμών ελέγχου και των μέτρων ασφαλείας του υπολογιστικού νέφους είναι η ελαχιστοποίηση ή η εξάλειψη των ευπαθειών στο περιβάλλον του υπολογιστικού νέφους για τη μείωση της επιφάνειας επίθεσης και την εκπλήρωση των διαφορετικών απαιτήσεων ασφαλείας. Οι ευπάθειες στο περιβάλλον του υπολογιστικού νέφους οφείλονται στις εγγενείς ευπάθειες στις υποκείμενες τεχνολογίες του υπολογιστικού νέφους (όπως, εικονικοποίηση, λειτουργικό σύστημα, πρωτόκολλο επικοινωνίας, API, κ.λπ.), στις ευπάθειες στα αρχιτεκτονικά του στοιχεία (όπως εικονική μηχανή, hypervisor, εικονικό δίκτυο, διεπαφές , πύλες κ.λπ.), στις ευπάθειες που οφείλονται σε εσφαλμένες υλοποιήσεις, σε λανθασμένες διαμορφώσεις, σε λανθασμένη χρήση/διαμόρφωση μηχανισμών και αντιμέτρων ασφάλειας και στις ευπάθειες που προκύπτουν από συγκεκριμένα χαρακτηριστικά του υπολογιστικού νέφους (όπως, κοινή χρήση πόρων, πολλαπλή μίσθωση κ.λπ.). [12]

4.1 Μηχανισμοί ελέγχου

Οι μηχανισμοί ελέγχου ασφάλειας επικεντρώνονται στον σχεδιασμό και την εφαρμογή διαφορετικών μέτρων ασφαλείας για την εξάλειψη ή τη μείωση των ευπαθειών στα αρχιτεκτονικά στοιχεία (του νέφους) ώστε να επιτευχθεί μείωση της επιφάνειας επίθεσης και της πιθανότητας επίθεσης. Παρακάτω παρουσιάζονται διαφορετικές λύσεις ασφαλείας που πρέπει να εφαρμοστούν σε αντίστοιχα αρχιτεκτονικά επίπεδα για την αντιμετώπιση των εγγενών ευπαθειών των περιβαλλόντων νέφους και την ελαχιστοποίηση της πιθανότητας επίθεσης. [12]

Οι λύσεις που εφαρμόζονται δεν είναι στατικής φύσης. Μια λύση θα πρέπει να επανεξετάζεται στο πλαίσιο της τακτικής διακυβέρνησης ως προς τη συνάφειά της και πρέπει να προσαρμοστεί με τις εξελισσόμενες επιφάνειες επίθεσης και το φάσμα απειλών. [12]

4.1.1 Επίπεδο εφαρμογής και διεπαφής

Στο επίπεδο αυτό οι συνιστώμενες λύσεις ασφαλείας είναι:

- Χρήση των πρωτοκόλλων, προτύπων και μηχανισμών ασφαλείας των υπηρεσιών ιστού (web), όπως WS-Security, WS-Trust, WS-Federation, XACML, XML-Encryption, XML-Signature, SAML, κ.λπ.
- Περιορισμός των συνόδων (sessions) και χρήση one-time cookies.
- Εξασφάλιση δοκιμών ασφαλείας, ασφαλής προγραμματισμός (διεπαφών & εφαρμογών), έλεγχος συμπεριφοράς προγραμμάτων, εκτεταμένες δοκιμές εφαρμογών (συμπ. ασφάλειας & καταπόνησης), ασφαλής διαμόρφωση εφαρμογών, έλεγχος δεδομένων, ισχυρή ταυτοποίηση χρηστών/πελατών, κατάλληλος έλεγχος πρόσβασης [12]

4.1.2 Επίπεδο πλατφόρμας

Στο επίπεδο πλατφόρμας οι προτεινόμενες λύσεις ασφαλείας είναι οι ακόλουθες:

- Αυστηρός έλεγχος πρόσβασης στα προσφερόμενα περιβάλλοντα ανάπτυξης, δοκιμής και εκτέλεσης
- Ενίσχυση ασφαλείας (σκλήρυνση) του λειτουργικού συστήματος, παρακολούθηση κατάλληλων αρχείων καταγραφής και επιδιόρθωση ασφαλείας του λειτουργικού συστήματος.
- Μελέτη του κύκλου ζωής ανάπτυξης ασφάλειας και εφαρμογή των βέλτιστων πρακτικών ανάπτυξης ασφάλειας, συμπεριλαμβανομένων των δοκιμών ασφαλείας για περιπτώσεις κατάχρησης και διείσδυσης. [12]
- Εφαρμογή patching στο ΛΣ και στο περιβάλλον ανάπτυξης/εκτέλεσης, έλεγχος τρωτοτήτων και επιδιόρθωσή τους, εφαρμογή αντι-ιικών, εφαρμογή κατάλληλου IDS (πχ. host-based ή application-based), έλεγχος/εξασφάλιση ακεραιότητας κώδικα εφαρμογών & περιβάλλοντος, χρήση ασφαλών & αξιόπιστων συστατικών περιβάλλοντος.

4.1.3 Επίπεδο εικονικοποίησης

Σε αυτό το επίπεδο τα μέτρα ασφαλείας χωρίζονται σε τρεις υποκατηγορίες ανάλογα με τον τομέα που θα δεχθεί επίθεση.

1) Μέτρα για την ασφάλεια του κύκλου ζωής εικονικής μηχανής (VM).
    - Χρήση αξιόπιστων εικονικών πλατφόρμων που υποστηρίζονται από υλικό, όπως το vTPM[21]
    - Έλεγχος πρόσβασης για την διαχείριση κύκλου ζωής εικόνας εικονικής μηχανής, διαγραφή περιττών εικόνων εικονικής μηχανής, σάρωση εικόνων εικονικής μηχανής για τρωτότητες, επιδιόρθωση (patching) και κρυπτογράφηση των εικόνων εικονικής μηχανής
    - Ασφαλής μετεγκατάσταση και επαναφορά της εικονικής μηχανής με χρήση ασφαλών τεχνικών προ-αντιγραφής και ζωντανής μετεγκατάστασης, χρήση αξιόπιστου πλαισίου για μετεγκατάσταση και επαναφορά
2) Μέτρα για την ασφάλεια υπερεπόπτη (hypervisor) / virtual machine manager (VMM).
    - Κατάλληλη απομόνωση εικονικών μηχανών και χρήση της ενδοσκόπησης (introspection)[22] της εικονικής μηχανής
    - Χρήση ασφαλών πρακτικών ανάπτυξης για λογισμικό υπερεπόπτη, σχεδίαση βασισμένη σε λειτουργίες για έναν υπερεπόπτη για μείωση της επιφάνειας επίθεσης καθώς και σκλήρυνση υπερεπόπτη και του ΛΣ στο οποίο εκτελείται (ανάλογα με το είδος εικονικοποίησης που εφαρμόζεται).
    - Διατήρηση της ακεραιότητας κώδικα του υπερεπόπτη με την βοήθεια εργαλείων όπως το HyperSage, κατάλληλη διαμόρφωση και προστασία επικοινωνίας υπερεπόπτη με

[21] Μια εικονική μονάδα αξιόπιστης πλατφόρμας (vTPM) είναι μια αναπαράσταση που βασίζεται σε λογισμικό ενός φυσικού τσιπ Trusted Platform Module 2.0. Παρέχει λειτουργίες που βασίζονται σε υλικό και σχετίζονται με την ασφάλεια, όπως η δημιουργία τυχαίων αριθμών, η επιβεβαίωση, η δημιουργία κλειδιών και άλλα.

[22] Το virtual machine introspection (VMI) είναι μια τεχνική "για την παρακολούθηση της κατάστασης του χρόνου εκτέλεσης μιας εικονικής μηχανής σε επίπεδο συστήματος (VM)"

εικονικές μηχανές, patching υπερεπόπτη για την αντιμετώπιση νέων απειλών και την διόρθωση ενδεχόμενων σφαλμάτων.

3) Μέτρα για την ασφάλεια της επικοινωνίας του εικονικού δικτύου
    - Χρήση αξιόπιστων εικονικών τομέων (domains), ασφαλής δρομολόγηση και χρήση τείχους προστασίας
    - Χρήση επικοινωνίας που βασίζεται σε δικτύωση που καθορίζεται από λογισμικό (Software-Defined Networking - SDN). [12]

4.1.4 Επίπεδο δικτύου

Στο επίπεδο δικτύου τα προτεινόμενα μέτρα ασφαλείας είναι :

- Ανάπτυξη συστημάτων ανίχνευσης, πρόληψης, μετριασμού και απόκρισης εισβολής
- Χρήση τείχους προστασίας, εικονικών LAN, αναλυτών κυκλοφορίας δικτύου, τακτικής σάρωσης και διόρθωσης για τον εντοπισμό ευπαθειών και για την επιδιόρθωση τους.
- Μέτρηση και αξιολόγηση απόδοσης συσκευών δικτύου, όπως δρομολογητές και μεταγωγείς, για τη λήψη προληπτικών μέτρων, όπως εξισορρόπηση φορτίου συσκευής
- Κρυπτογράφηση των δεδομένων καθώς μεταδίδονται και χρήση κρυπτογραφικών πρωτοκόλλων σε όλη την επικοινωνία για την διασφάλιση της ακεραιότητας, της εμπιστευτικότητας και του απορρήτου των δεδομένων χρήστη. [12]

4.1.5 Επίπεδο αποθήκευσης

Στο επίπεδο αυτό οι συνιστώμενες λύσεις ασφαλείας είναι:

- Καθορισμός της ταξινόμησης δεδομένων και του επίπεδου ελέγχου πρόσβασης σύμφωνα με την κρισιμότητα, τον ιδιοκτήτη και των γνωρισμάτων των δεδομένων (Attribute-based access control (ABAC))
- Χρήση τεχνικών εκλεπτισμένης πρόσβασης στα δεδομένα (fine-grained data access) και επιλεκτικής πρόσβασης στα δεδομένα (selective data access)
- Κρυπτογράφηση των δεδομένων, χρησιμοποιώντας κατάλληλες τεχνικές, όπως AES, για την εξασφάλιση της μη αναγνωσιμότητας των δεδομένων καθώς και πραγματική διαγραφή των δεδομένων πριν από την ανακύκλωση (ή αναχρησιμοποίηση) της συσκευής αποθήκευσης (είτε είναι φυσική είτε εικονική).
- Τακτικοί έλεγχοι ακεραιότητας δεδομένων για να επιβεβαιωθεί ότι τα δεδομένα δεν έχουν παραβιαστεί ή τροποποιηθεί. Ο έλεγχος περιλαμβάνει τη σύγκριση της τρέχουσας κατάστασης των δεδομένων με προηγούμενες καταστάσεις ή γνωστά σημεία αναφοράς για τον εντοπισμό τυχόν ασυνεπειών ή μη εξουσιοδοτημένων αλλαγών.
- Συνδυασμός τμηματοποίησης και κρυπτογράφησης των δεδομένων για την αποφυγή της συσχέτισης των δεδομένων.
- Χρήση υπογραφών και ελέγχου ακεραιότητας των δεδομένων.

- Χρήση τεχνικών ενίσχυσης της ιδιωτικότητας των δεδομένων, όπως k-ανωνυμία, ανωνυμία διαφορετικότητας τάξης l (l-diversity), διαφορική ιδιωτικότητα (differential privacy), t-εγγύτητα, προσθήκη θορύβου, ανατομία, και κάλυψη δεδομένων (data masking)
- Εξασφάλιση διαθεσιμότητας δεδομένων μέσω αναπαραγωγής, υποστήριξη για απόδειξη κατοχής δεδομένων (PDP), δυναμική απόδειξη κατοχής δεδομένων (DPDP) και απόδειξη δυνατότητας ανάκτησης (δεδομένων) (POR)
- Διαφάνεια στη θέση αποθήκευσης δεδομένων, δημιουργία αντιγράφων ασφαλείας πολλαπλών τοποθεσιών (για παράδειγμα με την χρήση του κανόνα δημιουργίας αντιγράφων ασφαλείας 3-2-1 για την δημιουργία αντιγράφων ασφαλείας σε πολλές τοποθεσίες - δηλαδή 3 Αντίγραφα Δεδομένων, 2 Διαφορετικοί τύποι μέσων δημιουργίας αντιγράφων ασφαλείας και 1 αντίγραφο ασφαλείας να αποθηκεύεται Off Site), μέθοδοι ανάκτησης και αφαίρεσης αντιγράφων δεδομένων, εσωτερική δημιουργία αντιγράφων ασφαλείας κρίσιμων δεδομένων για την επιχείρηση. [12]

4.1.6 Επίπεδο υλικού

Σε αυτό το επίπεδο οι συνιστώμενες λύσεις ασφαλείας είναι :

- Χρήση υλικού & αρχιτεκτονικών που είναι υψηλής απόδοσης και ανθεκτικά σε σφάλματα. Χρήση της αρχιτεκτονικής υποδομής ασφαλούς υλικού για την ενεργοποίηση βελτιωμένης λύσης ασφάλειας υπολογιστικού νέφους, όπως vTPM και χρήση κρυπτογραφίας βασισμένης σε υλικό. [12]

4.1.7 Επίπεδο εγκατάστασης

Στο επίπεδο αυτό οι συνιστώμενες λύσεις ασφαλείας είναι :

- Εφαρμογή ελέγχων φυσικής ασφάλειας για την αποτροπή μη εξουσιοδοτημένης πρόσβασης σε φυσικά περιουσιακά στοιχεία και συστήματα, π.χ. βιομετρικά, CCTV
- Εφαρμογή ελέγχων ασφαλείας για τη φυσική ασφάλεια της εγκατάστασης και τη διατήρηση της περιβαλλοντικής υγιεινής της εγκατάστασης προς επίτευξη της σωστής λειτουργίας των φιλοξενούμενων συσκευών και εξοπλισμού
- Εξασφάλιση διατήρησης σχεδίων διαχείρισης καταστροφών και επιχειρηματικής συνέχειας [12]

4.2 Μέτρα ασφάλειας (αντίμετρα)

Σύμφωνα με το ISO 27000:2018 ως μέτρο ασφαλείας (ή αντίμετρο) ορίζεται ένα μέτρο διαχείρισης του κινδύνου, όπως για παράδειγμα οι πολιτικές, κανόνες, διαδικασίες, οδηγίες, οργανωσιακές πρακτικές, και οργανωσιακές δομές. Τα μέτρα ασφαλείας αποτελούν την βάση για την ασφάλεια των δεδομένων και τη διασφάλιση του απορρήτου στο περιβάλλον του υπολογιστικού νέφους. Τα μέτρα ασφάλειας που εφαρμόζονται παρακολουθούνται συνεχώς, μετρώνται και αξιολογούνται ως προς την αποτελεσματικότητα και τη συνάφειά τους. Με βάση την παρατήρηση και τα ευρήματα, στην συνέχεια

ξεκινούν οι απαραίτητες προληπτικές, διορθωτικές και βελτιωτικές ενέργειες για τη συνεχή ασφάλεια των δεδομένων και τη διασφάλιση του απορρήτου. [12]

Τα μέτρα ασφάλειας που εφαρμόζονται ή πρέπει να εφαρμόζονται στο υπολογιστικό νέφος αναλύονται στις επόμενες υπο-ενότητες.

4.2.1 SLA, Μέτρα και Διακυβέρνηση

Η SLA (Συμφωνία Επιπέδου Υπηρεσίας) είναι μια νομική σύμβαση μεταξύ του παρόχου υπηρεσιών υπολογιστικού νέφους και του χρήστη με οικονομικές επιπτώσεις. Καθορίζει τους διαφορετικούς όρους και προϋποθέσεις παροχής υπηρεσιών, συμπεριλαμβανομένου του προβλεπόμενου επιπέδου απόδοσης της παραδιδόμενης υπηρεσίας. Η ύπαρξη της SLA μπορεί να θεωρηθεί ως ένα μέτρο ασφάλειας από την άποψη οτι λογικά υποχρεώνει τον πάροχο να παρακολουθεί και να διενεργεί μετρήσεις σχετικά με την απόδοση των υπηρεσιών του ώστε να είναι σε θέση να επαληθεύει την εκπλήρωση των όρων της SLA. Ο έλεγχος (auditing) είναι μια σημαντική δραστηριότητα για την απόδειξη της ύπαρξης ή μη παραβιάσεων SLA. [26]

Ο χρόνος για την κλιμάκωση ή την αποκλιμάκωση των εικονικών μηχανών, η αυτόματη κλιμάκωση, η πληρωμή ανά χρήση (με βάση το χρόνο ή βάσει πόρων, όπως για παράδειγμα τον αριθμό των κλήσεων ή τον όγκο των δεδομένων), ο αριθμός ταυτόχρονων περιόδων σύνδεσης χρήστη, η διαθεσιμότητα πόρων υπηρεσίας, η απώλεια δεδομένων, ο χρόνος απόκρισης πρόσβασης δεδομένων, η συμμόρφωση με κανονισμούς, καθώς και η ανάκτηση δεδομένων και υπηρεσιών, είναι μερικές από τις παραμέτρους που πρέπει να ληφθούν υπόψη κατά τον καθορισμό της SLA για την παράδοση της υπηρεσίας υπολογιστικού νέφους. Το έγγραφο SLA περιέχει τις μετρήσιμες βασικές παραμέτρους απόδοσης, τις μεθόδους μέτρησής τους και το εύρος τιμών για το αναμενόμενο και αποδεκτό επίπεδο απόδοσης της παροχής υπηρεσιών. Συνιστάται η χρήση εργαλείων αυτοματισμού για τη συλλογή δεδομένων, τον υπολογισμό της απόδοσης, την ανάλυση, τη δημιουργία αναφορών και τη διανομή στους ενδιαφερόμενους φορείς. Αυτό θα διευκολύνει τη διαφάνεια, την κοινή κατανόηση και τις γρήγορες ενέργειες για αποκλίσεις και βελτιώσεις. [12]

Επιπλέον, υπάρχει μια δομημένη διακυβέρνηση για τη ρύθμιση των πολιτικών και στρατηγικών ασφάλειας, των προσφορών υπηρεσιών και την αξιολόγηση της παροχής υπηρεσιών και της απόδοσης ασφάλειας έναντι της SLA μαζί με την αποτελεσματικότητα των διαδικασιών ελέγχου αλλαγών και διαχείρισης ενημερώσεων κώδικα. Για αποτελεσματική διακυβέρνηση, το διοικητικό όργανο αποτελείται από εκπροσώπους από όλους τους σχετικούς φορείς του υπολογιστικού νέφους που είναι εξουσιοδοτημένοι να λαμβάνουν αποφάσεις. Η ομάδα διακυβέρνησης διαδραματίζει κεντρικό ρόλο στον καθορισμό και τη βελτίωση της ασφάλειας από άκρο σε άκρο του υπολογιστικού νέφους, αναλύοντας την απόδοση παροχής υπηρεσιών υπολογιστικού νέφους, τις εμπειρίες χρήσης υπηρεσιών των τελικών χρηστών, την έναρξη δραστηριοτήτων συνεχούς βελτίωσης και την γνώση διάφορων γεγονότων ασφαλείας. Η ομάδα διακυβέρνησης θα αξιολογήσει τις εξελισσόμενες τεχνολογίες του υπολογιστικού νέφους και θα υιοθετήσει ορισμένες από αυτές για να παραμείνει ανταγωνιστική. Αυτή η ομάδα, επίσης, θα επανεξετάσει και θα προσαρμόσει τις μεταβαλλόμενες απαιτήσεις για τη νομική συμμόρφωση, τις πιστοποιήσεις και τους ελέγχους. [12] [5]

4.2.2 Καταγραφή, παρακολούθηση και απόκριση σε περιστατικά (Logging, Monitoring, Incident Response)

Η καταγραφή της χρήσης πόρων, των δραστηριοτήτων των χρηστών, της επεξεργασίας δεδομένων και των αλλαγών συστήματος πρέπει να ενεργοποιείται και να παρακολουθείται. Η παρακολούθηση προσδιορίζει την ανεξέλεγκτη και μη εξουσιοδοτημένη χρήση πόρων, τις αλλαγές που μπορεί να προκύψουν στο σύστημα, τις αποκλίσεις από την αναμενόμενη συμπεριφορά χρήστη, την κακόβουλη πρόσβαση και κίνηση δεδομένων κ.α. Αυτές οι αποκλίσεις καταγράφονται ως συμβάντα ασφαλείας και παρακολουθούνται για να ενεργοποιηθεί το σύστημα απόκρισης συμβάντων ασφαλείας όπως ορίζεται από τα κριτήρια που καθορίζονται από την διακυβέρνηση. Ο στόχος της ομάδας απόκρισης συμβάντων ασφαλείας είναι να επαναφέρει το σύστημα στην κανονικότητα και να ξεκινήσει την ανάλυση της βασικής αιτίας του συμβάντος για τη λήψη προληπτικών μέτρων με γνώμονα την αποφυγή τέτοιων περιστατικών στο μέλλον.

Η παρακολούθηση χρήσης πόρων παρέχει πληροφορίες για τα επίπεδα απόδοσης παροχής υπηρεσιών και εντοπίζει τυχόν απόκλιση από το SLA. Για παράδειγμα, η παρατηρούμενη υψηλή χρήση της CPU μπορεί να οδηγήσει σε πιο αργό χρόνο απόκρισης στα αιτήματα των χρηστών οπότε ενδέχεται να προκαλέσει απόκλιση από τις αντίστοιχες εγγυήσεις στην SLA. Τέτοιες αποκλίσεις SLA θα πρέπει να καταγράφονται ώστε να ξεκινούν οι απαραίτητες ενέργειες βελτίωσης. Η παρακολούθηση εντοπίζει επίσης δόλια χρήση πόρων. Οι πάροχοι υπηρεσιών υπολογιστικού νέφους (Cloud Service Providers (CSPs)) χρησιμοποιούν τα κατάλληλα εργαλεία για ολοκληρωμένη καταγραφή, παρακολούθηση, ανάλυση και ειδοποίηση για αποκλίσεις. Η αποτελεσματικότητα τέτοιων εργαλείων έγκειται στην ευαισθησία και την ακρίβεια στη λήψη σχετικών δεδομένων, στην αξιολόγηση των μετρήσεων, στον προσδιορισμό του επιπέδου απόδοσης και απόκλισης, στην ανάλυσή τους για την ανάκτηση πολύτιμων πληροφοριών και στην παρουσίασή τους από διαφορετικές οπτικές γωνίες. [12]

4.2.3 Συντήρηση Εγκαταστάσεων

Τα κέντρα δεδομένων φιλοξενούν τη φυσική υποδομή του υπολογιστικού νέφους και παρέχουν τις υπηρεσίες υπολογιστικού νέφους. Οι πάροχοι υπολογιστικού νέφους οφείλουν να διασφαλίζουν ότι οι εγκαταστάσεις που στεγάζουν αυτά τα κέντρα δεδομένων έχουν κατάλληλα επίπεδα ψύξης, τακτικής ηλεκτρικής συντήρησης και ελέγχους φυσικής ασφάλειας, καλωδίωσης και περιβάλλοντος για την ρύθμιση της θέρμανσης, του εξαερισμού, του κλιματισμού, της πυρασφάλειας και άλλων υποσυστημάτων. Η τακτική προληπτικής συντήρησης της εγκατάστασης, όπως για παράδειγμα οι προγραμματισμένοι έλεγχοι για βλάβες μηχανών και μετρήσεις διαθεσιμότητας των εγκαταστάσεων ανά τακτά χρονικά διαστήματα, μπορεί να περιορίσει τις ζημιές σε φυσικά συστήματα και πόρους δικτύου για να βελτιώσει τη διαθεσιμότητα των πόρων και υπηρεσιών νέφους. [12]

4.2.4 Δοκιμές πριν και μετά την ανάπτυξη

Τις περισσότερες φορές, ο χρόνος για την διάθεση μιας υπηρεσίας στην αγορά έχει προτεραιότητα έναντι των δοκιμών, ειδικά των δοκιμών ασφαλείας. Η έλλειψη απαραίτητων δοκιμών έχει συνεπακόλουθες επιπτώσεις, όπως διακοπή στις προσφερόμενες υπηρεσίες λόγω επιθέσεων στον κυβερνοχώρο που προκαλούνται από μη ελεγμένες ευπάθειες, ποινές για απώλεια του απορρήτου των δεδομένων χρήστη, κ.α. Το παραπάνω ζήτημα μπορεί να αντιμετωπιστεί μέσω αυτοματοποίησης των δραστηριοτήτων δοκιμών που ευθυγραμμίζονται με τον έλεγχο αλλαγών και τη διαχείριση ενημερώσεων κώδικα. Όλες οι εφαρμογές λογισμικού και τα στοιχεία που χρησιμοποιούνται για την

παροχή των υπηρεσιών πρέπει να ελεγχθούν για την εκπλήρωση των απαιτήσεων ασφαλείας. Ειδικές δοκιμές ασφαλείας, συμπεριλαμβανομένων των στατικών δοκιμών ασφάλειας εφαρμογών (SAST), των δυναμικών δοκιμών ασφαλείας εφαρμογών (DAST), των δοκιμών ασφάλειας διαδραστικών εφαρμογών (IAST) και δοκιμών διείσδυσης, θα πρέπει να εκτελούνται στις αντίστοιχες φάσεις της ανάπτυξης, της παράδοσης της εφαρμογής και της λειτουργίας της. [12]

4.2.5 Συνεχής βελτίωση

Τα αποτελέσματα της ανάλυσης της βασικής αιτίας των συμβάντων ασφαλείας, οι παρατηρούμενες αποκλίσεις παρακολούθησης, η ανάλυση τάσεων των μετρήσεων απόδοσης, οι ανασκοπήσεις διακυβέρνησης, κ.α., παρέχουν ευκαιρίες για συνεχή βελτίωση των μέτρων ασφαλείας που εφαρμόζονται από τους παρόχους υπηρεσιών υπολογιστικού νέφους. Οι συνεχείς συνεδρίες ευαισθητοποίησης και εκπαίδευσης για την ασφάλεια των ενδιαφερομένων βοηθά στην βελτίωση της αποτελεσματικότητας των εφαρμοζόμενων μέτρων ασφαλείας. [12]

4.3 Συμμόρφωση ασφάλειας

Η τρίτη διάσταση εστιάζει στη διαφάνεια προς τις νομικές και ρυθμιστικές αρχές συμμόρφωσης και στην δεκτικότητα ως προς τους ελέγχους καθώς και στην τήρηση των συστάσεων ασφαλείας των οργανισμών τυποποίησης. Οι πάροχοι υπηρεσιών υπολογιστικού νέφους πρέπει να μοιράζονται με διαφάνεια τα εφαρμοσμένα μέτρα για την ασφάλεια των δεδομένων και τη διασφάλιση του απορρήτου στους χρήστες τους και στις αρχές συμμόρφωσης. Η νομική συμμόρφωση, ο έλεγχος πιστοποίησης και η εφαρμογή μέτρων ασφαλείας, σύμφωνα με τις συστάσεις των οργανισμών τυποποίησης, αντικατοπτρίζουν το επίπεδο αποτελεσματικότητας και επάρκειας των μέτρων ασφαλείας που εφαρμόζονται. [12]

4.3.1 Νομική και Κανονιστική Συμμόρφωση

Τα μοναδικά χαρακτηριστικά του υπολογιστικού νέφους, όπως η κοινή χρήση πόρων, η πολλαπλή μίσθωση, η εικονικοποίηση, η εξωτερική ανάθεση πολλών τοποθεσιών κ.α., απαιτούν από τους παρόχους υπολογιστικού νέφους να διασφαλίζουν τη νομική και κανονιστική συμμόρφωση με τους ισχύοντες νόμους της χώρας φιλοξενίας της υποδομής του υπολογιστικού νέφους. Η γεωγραφικά κατανεμημένη αποθήκευση δεδομένων σε πολλές τοποθεσίες, για την υποστήριξη του πλεονασμού και της επιχειρησιακής συνέχειας, προκαλεί ασάφεια στη λήψη αποφάσεων σχετικά με τις δικαιοδοσίες για τη συμμόρφωση με το απόρρητο δεδομένων και τη διαχείριση του κύκλου ζωής των δεδομένων. Οι απαιτήσεις ψηφιακής εγκληματολογίας (digital forensics) ενδέχεται να έρχονται σε αντίθεση με τις νομικές απαιτήσεις και τις απαιτήσεις απορρήτου της χώρας φιλοξενίας της υποδομής του υπολογιστικού νέφους. Η παροχή συμμόρφωσης γίνεται πιο περίπλοκη όταν τα δεδομένα χρήστη εμπίπτουν σε διαφορετικές δικαιοδοσίες. Το Digital Forensic as a Service (DFaaS) [30], το security logging-as-a-service (SLaaS) [31] και το forensic by-design (FbD) [29] είναι μερικές από τις προτεινόμενες λύσεις για την παροχή δεδομένων συμμόρφωσης. [12]

Το Digital Forensics as a Service (DFaaS) προσφέρει καινοτόμες και οικονομικά αποδοτικές λύσεις στις επιχειρήσεις για την αντιμετώπιση των αυξανόμενων προκλήσεων της κοινότητας της ψηφιακής εγκληματολογίας. Πολλές φορές, πολλές υπηρεσίες επιβολής του νόμου, ιδιώτες και οι περισσότερες εταιρείες δεν έχουν τα μέσα να δημιουργήσουν έναν ειδικό χώρο για τη διεξαγωγή ιατροδικαστικών αναλύσεων. Εδώ, λοιπόν, είναι που οι υπηρεσίες DFaaS γεφυρώνουν το χάσμα. [30]

Το security logging-as-a-service (SLaaS) είναι μια αποδεδειγμένη προσέγγιση για τη διαχείριση και την παρακολούθηση δεδομένων καταγραφής μεγάλου όγκου σε σύγχρονα δυναμικά περιβάλλοντα. Το SLaaS επιτρέπει στις εταιρείες να διαχειρίζονται δεδομένα καταγραφής ανεξάρτητα από το αν προέρχονται από εφαρμογές, διακομιστές ή συσκευές. Με το SLaaS, οι εταιρείες μπορούν πιο εύκολα να συγκεντρώνουν και να ταξινομούν δεδομένα, να κλιμακώνουν και να διαχειρίζονται τις απαιτήσεις αποθήκευσης, να δημιουργούν ειδοποιήσεις και να αναλύουν δεδομένα και τάσεις. Επιτρέπει, επίσης, στις ομάδες να προσαρμόζουν πίνακες εργαλείων, αναφορές και απεικονίσεις. Το SLaaS παρέχει υπηρεσίες και υποστήριξη που βασίζονται στο νέφος, σε αντίθεση με τα πιο παραδοσιακά μοντέλα, όπως οι συνδρομές. [31]

Το "Forensic-by-design" (FbD) επεκτείνει την προοπτική της Ψηφιακής Εγκληματολογικής Ετοιμότητας (DFR). Παρόμοια με το Security-by-design, αυτό το νέο όραμα υποστηρίζει την ενσωμάτωση των Forensic απαιτήσεων στα στάδια σχεδιασμού και ανάπτυξης ενός συστήματος. [29]

Για κάθε άτομο στην Ευρωπαϊκή Ένωση και τον Ευρωπαϊκό Οικονομικό Χώρο, ο γενικός κανονισμός για την προστασία δεδομένων (GDPR)[23] επιβάλλει την προστασία των δεδομένων και της ιδιωτικής του ζωής. Οι επιχειρήσεις και οι οργανισμοί, συμπεριλαμβανομένων των παρόχων υπηρεσιών υπολογιστικού νέφους, που διαχειρίζονται τα προσωπικά δεδομένα των χρηστών πρέπει να συμμορφώνονται με τον GDPR διαφορετικά θα αντιμετωπίζουν οικονομικές κυρώσεις. [12]

4.3.2 Πρότυπα και Πλαίσια

Τα πρότυπα και τα πλαίσια ασφαλείας (πχ το πρότυπο ETSI GS CLOUD[24] από το ευρωπαϊκό ινστιτούτο τηλεπικοινωνιακών προτύπων (ETSI) και τα πρότυπα από την διεθνή ένωση τηλεπικοινωνιών (ITU)[25]) από τους οργανισμούς τυποποίησης παρέχουν μια δομημένη προσέγγιση για την εκπλήρωση των απαιτήσεων ασφαλείας. Δεν είναι υποχρεωτικό να ακολουθούνται οι συστάσεις των προτύπων και των πλαισίων, ωστόσο, η συμμόρφωση με αυτές τις συστάσεις παρέχει μια κοινή γλώσσα για την κατανόηση των βέλτιστων πρακτικών που ακολουθούνται από έναν πάροχο υπηρεσιών υπολογιστικού νέφους. Η συμμόρφωση ενός παρόχου υπηρεσιών υπολογιστικού νέφους με τέτοια πρότυπα και πλαίσια αυξάνει την εμπιστοσύνη των χρηστών. Χρησιμοποιώντας τις συνιστώμενες οδηγίες, ενισχύει τη διαλειτουργικότητα και τη φορητότητα των προσφορών υπηρεσιών του και επιτρέπει με αυτό τον τρόπο στον πάροχο να υιοθετεί είδη συνεργασίας μεταξύ του δικού του νέφους και των άλλων νεφών (περίπτωση πολλαπλών νεφών (multi cloud)) για τη διεύρυνση των υπηρεσιών του. [12]

4.3.3 Έλεγχος και Πιστοποίηση

Οι πάροχοι υπολογιστικού νέφους αναζητούν ελέγχους και πιστοποίηση από τρίτο μέρος (τον ελεγκτή νέφους - cloud auditor) για να αξιολογήσουν εάν τα απαιτούμενα μέτρα ασφαλείας ισχύουν και λειτουργούν σύμφωνα με την αναμενόμενη συμπεριφορά, όπως επίσης και για να αυξάνουν το επίπεδο εμπιστοσύνης τους από τους δυνητικούς τους πελάτες. Αυτό προσφέρει ορατότητα και διαφάνεια στη δέσμευση του παρόχου υπηρεσιών υπολογιστικού νέφους για την παροχή ασφαλών υπηρεσιών με την

[23] https://gdpr-info.eu/
[24] https://www.etsi.org/deliver/etsi_gs/NFV-EVE/001_099/011/03.01.01_60/gs_nfv-eve011v030101p.pdf
[25] https://www.itu.int/en/ITU-T/focusgroups/cloud/Pages/default.aspx

εφαρμογή των απαραίτητων και επαρκών μέτρων ασφαλείας. Ο ελεγκτής πιστοποίησης εκτελεί συλλογή, επαλήθευση και επικύρωση δεδομένων. Η διαδικασία ελέγχου διασφαλίζει την εμπιστευτικότητα και το απόρρητο των υπό έλεγχο δεδομένων χρηστών.

Είναι επιθυμητό να εκτελούνται πιστοποίηση ασφαλείας και έλεγχοι συνεχώς, με δυνατότητα αυτοματοποίησης, λαμβάνοντας υπόψη τον δυναμισμό στην κατανομή πόρων και τα αιτήματα υπηρεσιών σε περιβάλλον υπολογιστικού νέφους. Ο έλεγχος ακεραιότητας των απομακρυσμένων δεδομένων μπορεί να πραγματοποιηθεί με την τεχνική απομακρυσμένου ελέγχου δεδομένων (RDA - Remote Data Auditing). Στον RDA, ένα μικρό τμήμα δεδομένων από το σύνολο των δεδομένων ελέγχεται επιτόπου για ντετερμινιστική ή πιθανολογική διασφάλιση της ακεραιότητας των δεδομένων. Οι τεχνικές απομακρυσμένου ελέγχου δεδομένων που χρησιμοποιούνται ευρέως είναι βασισμένες σε αναπαραγωγή και κωδικοποίηση δικτύου.

Η ISO/IEC 27001:2022[26], η ISO/IEC 27002:2022[27], η ISO/IEC 27017:2015[28], η ISO/IEC 27018:2019[29], η CSA Security Trust Assurance and risk (STAR)[30], η National Institute of Standards and Technology (NIST) 800-53[31], είναι μερικά από τα αναγνωρισμένα πρότυπα πιστοποιητικών για την ασφάλεια των πληροφοριών και τη διασφάλιση του απορρήτου των δεδομένων. [12]

5. Συγκρίσεις

5.1 Σύγκριση Υπολογιστικού νέφους με τα τοπικά περιβάλλοντα

Η αυτο-φιλοξενούμενη (επιτόπια) υποδομή μπορεί να είναι απαλλαγμένη από κάποιες απειλές που συναντάμε στην υποδομή που φιλοξενείται στο νέφος (ιδιαίτερα στο δημόσιο νέφος), ωστόσο η ικανοποίηση των προσδοκιών ασφάλειας όσων εξαρτώνται από αυτήν μπορεί να είναι απαγορευτικά ακριβή. Η εξασφάλιση μιας υποδομής φιλοξενίας έχει σημαντικό κόστος που καθορίζεται σε σχέση με τον αριθμό των μηχανημάτων που πρέπει να διασφαλιστούν, ιδιαίτερα σε περιπτώσεις όπου η υποδομή χρησιμοποιείται και από εξωτερικούς χρήστες. [27]

Παραδείγματα αυτών των σταθερών δαπανών (για την πλευρά της ασφάλειας) περιλαμβάνουν:

- Ανάπτυξη στρατηγικής ασφάλειας κεντρικών υπολογιστών και δικτύου
- Εκπαίδευση του προσωπικού σε όλο το φάσμα των καθηκόντων που απαιτούνται από τη στρατηγική ασφαλείας
- Πρόσληψη εξειδικευμένου προσωπικού
- Ενημέρωση για νέες απειλές και αντίμετρα
- Ανάπτυξη σχέσης με τις αρχές επιβολής του νόμου

[27]

[26] https://www.iso.org/standard/27001
[27] https://www.iso.org/standard/54533.html
[28] https://www.iso.org/standard/43757.html
[29] https://www.iso.org/standard/76559.html
[30] https://cloudsecurityalliance.org/star/
[31] https://csrc.nist.gov/publications/detail/sp/800-53/rev-5/final

Οι χρήστες που εκμεταλλεύονται την υποδομή του υπολογιστικού νέφους δεν χρειάζεται να εστιάσουν τόσο πολύ στην ασφάλεια εφόσον αυτή καλύπτεται από το ίδιο το νέφος και τους υπαλλήλους του πιο αποτελεσματικά από ό,τι οι οργανισμοί που φιλοξενούν αυτοτελώς την υποδομή τους. Το προσωπικό σε παρόχους φιλοξενίας νέφους είναι πιο εξειδικευμένο από τους εργαζομένους μιας επιχείρησης που διαχειρίζονται υποδομές που αυτο-φιλοξενούνται, επιτρέποντάς τους να αναπτύξουν τεχνογνωσία που αυξάνει την παραγωγικότητα ενώ λαμβάνουν χαμηλότερη εκπαίδευση (ανά εργαζόμενο). [27]
Οι διαχειριζόμενες λύσεις ασφάλειας είναι απομακρυσμένες λύσεις ή προϊόντα λογισμικού που ενδέχεται να εγκαθίστανται σε μια τοπική υποδομή και επιτρέπουν στους ιδιοκτήτες υποδομών που αυτο-φιλοξενούνται να επιτύχουν ορισμένα από αυτά τα οφέλη κλίμακας. Αυτές οι διαχειριζόμενες προσφορές κυμαίνονται από λύσεις σε ένα πακέτο, όπου αυτά τα πακέτα μπορεί να παρέχουν τείχη προστασίας, δημιουργία αντιγράφων ασφαλείας ή φιλτράρισμα ανεπιθύμητων μηνυμάτων, συμβουλευτικές υπηρεσίες ασφάλειας έως και πλήρεις υπηρεσίες ασφαλείας (πχ. Web Security as a Service). Δυστυχώς, οι διαχειριζόμενες λύσεις ασφάλειας μπορεί να εκθέσουν τους πελάτες τους σε πολλές από τις ίδιες απειλές που αντιμετωπίζουν οι ενοικιαστές των παρόχων υπολογιστικού νέφους. Για παράδειγμα, ένα πλαίσιο φιλτραρίσματος ανεπιθύμητων μηνυμάτων θα έχει πρόσβαση στην υποδομή δικτύου του πελάτη και σε όλα τα εισερχόμενα μηνύματα ηλεκτρονικού ταχυδρομείου, και άρα είναι επιρρεπής σε ανεπιθύμητη διαρροή πληροφοριών. [27]
Αφού ο πάροχος υπολογιστικού νέφους πρέπει να είναι αξιόπιστος σχετικά με τις εφαρμογές και τα δεδομένα των ενοικιαστών του, οι ενοικιαστές μπορούν να αποκτούν υπηρεσίες διαχείρισης ασφάλειας χωρίς να επεκτείνουν την βάση του οργανισμού τους και το πλήθος των αξιόπιστων εργαζομένων τους. Για παράδειγμα, μια υποδομή που φιλοξενείται στο νέφος και διαχειρίζεται το δίκτυο του οργανισμού, δεν χρειάζεται πρόσθετα προνόμια για να φιλτράρει την εισερχόμενη κίνηση στις θύρες. Επιπλέον, τα χαρακτηριστικά ασφαλείας που είναι ενσωματωμένα στην υποδομή μπορεί να είναι φθηνότερα να προσαρμοστούν και να χρησιμοποιηθούν σε μια εφαρμογή από ότι εκείνα που απαιτούν την εγκατάσταση νέων στοιχείων ή διαθέτουν API που ενδέχεται να μην είναι προσαρμοσμένα στην υποδομή. Από τη στιγμή που ένας πάροχος υποδομής υπολογιστικού νέφους αναλαμβάνει το κόστος για την ανάπτυξη μιας διαχειριζόμενης λύσης ασφάλειας για έναν πελάτη, το οριακό κόστος για την ανάπτυξη της δυνατότητας αυτής και σε άλλους ενοικιαστές είναι συχνά αμελητέο και μπορεί να αποσβεστεί γρηγορότερα εφόσον κάποια χαρακτηριστικά ασφαλείας είναι επί πληρωμή. [27]
Παραδείγματα χαρακτηριστικών ασφαλείας που μπορούν να ενσωματωθούν στο υπολογιστικό νέφος, μερικά από τα οποία υπάρχουν ήδη σε εργαλεία φιλοξενίας, όπως το CPanel[32], είναι τα εξής:

- Έλεγχος δικτύου και λειτουργικών συστημάτων
- Παρακολούθηση όλων των εγκατεστημένων λογισμικών, εκδοτών, εκδόσεων και επιπέδων ενημέρωσης κώδικα
- Αποθήκευση πιστωτικών καρτών και εντοπισμός απάτης
- Δημιουργία δημόσιου/ιδιωτικού κλειδιού, δημιουργία πιστοποιητικού και αποθήκευσής του
- Αυτόματος έλεγχος ταυτότητας και προστασία των επικοινωνιών εντός του δικτύου ενοικιαστών

[32] https://cpanel.net/

- Ασφαλής καταγραφή συμβάντων συστήματος
- Φιλτράρισμα ανεπιθύμητων μηνυμάτων
- Κατακερματισμός και αποθήκευση κωδικού πρόσβασης
- Δημιουργία και επαλήθευση CAPTCHA
- Γραφικά στοιχεία λογισμικού, όπως μετρητές ισχύος κωδικού πρόσβασης [27]

Πολλά από τα παραπάνω χαρακτηριστικα μπορεί να μην είναι οικονομικά προσιτά αν οι ενοικιαστες πρέπει να καλύψουν το αρχικό κόστος, ωστόσο μπορούν να γίνουν προσιτά εάν οι ενοικιαστές πρέπει να καλύψουν μόνο το μερίδιο τους στο οριακό κόστος. Αυτό οδηγεί σε θετικές εξωτερικές επιδράσεις κάθε φορά που ένας υποψήφιος ενοικιαστής που έχει επίγνωση της ασφάλειας απαιτεί ένα νέο χαρακτηριστικό ασφαλείας. [27]
Ένα πλεονέκτημα όσον αφορά την ασφάλεια στην υποδομή του υπολογιστικού νέφους είναι η ασφάλεια ως υπηρεσία (SECaaS). Η ασφάλεια ως υπηρεσία είναι ένα μοντέλο υπολογιστικού νέφους που παρέχει διάφορες υπηρεσίες ασφάλειας σε οργανισμούς. Περιλαμβάνει την εξωτερική ανάθεση ορισμένων πτυχών της υποδομής και της διαχείρισης της ασφάλειας ενός οργανισμού σε έναν τρίτο πάροχο υπηρεσιών χωρίς να χρειάζονται σημαντικές προκαταρκτικές επενδύσεις σε υλικό, λογισμικό και εξειδικευμένη τεχνογνωσία από τον οργανισμό αυτό. Οι υπηρεσίες που παρέχονται από το μοντέλο παράδοσης SECaaS μπορεί να περιλαμβάνουν ασφάλεια δικτύου, προστασία τελικών σημείων, πρόληψη απώλειας δεδομένων, διαχείριση ταυτότητας και πρόσβασης, διαχείριση πληροφοριών και συμβάντων ασφαλείας (SIEM), αξιολογήσεις ευπάθειας, δοκιμές διείσδυσης και άλλα. Οι πάροχοι SECaaS ειδικεύονται στην ασφάλεια και απασχολούν εξειδικευμένες ομάδες εμπειρογνωμόνων ασφαλείας. Οι οργανισμοί μπορούν να επωφεληθούν από την εμπειρογνωμοσύνη των παρόχων SECaaS, καθώς διαθέτουν βαθιά γνώση και εμπειρία στη διαχείριση και τον μετριασμό των κινδύνων ασφαλείας. Πολλές λύσεις SECaaS ενσωματώνουν προηγμένες δυνατότητες ανίχνευσης και αντιμετώπισης απειλών, όπως παρακολούθηση σε πραγματικό χρόνο, ανάλυση συμπεριφοράς και αλγόριθμους μηχανικής μάθησης. Αυτές οι τεχνολογίες βοηθούν στον άμεσο εντοπισμό και την αντιμετώπιση πιθανών περιστατικών ασφαλείας. Τέλος, οι πάροχοι SECaaS διαθέτουν συχνά εμπειρογνωμοσύνη στις απαιτήσεις συμμόρφωσης και μπορούν να βοηθήσουν τους οργανισμούς να ανταποκριθούν σε κανονισμούς και πρότυπα που αφορούν τον συγκεκριμένο κλάδο, όπως ο GDPR (Γενικός Κανονισμός για την Προστασία Δεδομένων), ο HIPAA (Health Insurance Portability and Accountability Act), το PCI DSS (Payment Card Industry Data Security Standard) και άλλα. [33] [34]

Ένα άλλο πλεονέκτημα της δημιουργίας χαρακτηριστικών ασφαλείας στην υποδομή υπολογιστικού νέφους είναι η αξιοποίηση δεδομένων από πολλούς ενοικιαστές. Για παράδειγμα, όταν τα εργαλεία παρακολούθησης εντοπίζουν μια νέα επίθεση εναντίον ενός ενοικιαστή, η ομάδα και το σύστημα παρακολούθησης θα είναι ενημερωμένα ώστε να εντοπίζουν παρόμοιες επιθέσεις εναντίον άλλων ενοικιαστών. Τέτοια συστήματα πρέπει να είναι σχεδιασμένα ώστε να περιορίζουν τη διαρροή ανεπιθύμητων πληροφοριών από τον έναν ενοικιαστή στον άλλο ώστε να αποφεύγονται πιθανές παραβιάσεις. Ωστόσο, τα συστήματα φήμης (reputation systems) που εντοπίζουν bots, αποστολείς ανεπιθύμητης αλληλογραφίας και άλλες κακόβουλες δραστηριότητες μπορούν να επωφεληθούν από

μια πληθώρα δεδομένων και λίγοι ενοικιαστές θα είχαν λόγο να εξαιρεθούν από την παροχή τους. Οι υπάλληλοι του παρόχου νέφους στους οποίους έχει ανατεθεί η διεξαγωγή εγκληματολογικών εξετάσεων στο παραβιασμένο σύστημα ενός ενοικιαστή μπορεί να αξιοποιήσουν όσα έμαθαν από την επιθεώρηση των συστημάτων άλλων ενοικιαστών χωρίς διαρροή δεδομένων. Ωστόσο θα υπάρχει σημαντική καθυστέρηση εφόσον η ανάλυση θα πραγματοποιείται χειρωνακτικά. [27]

Η παρακολούθηση των απειλών για τη δικαιοδοσία και η τήρηση των υπαρχόντων νόμων και κανονισμών είναι ένα δαπανηρό έργο, αλλά έχει οικονομίες κλίμακας. Εάν η υποδομή εντός του πεδίου αρμοδιοτήτων των παρόχων υπολογιστικού νέφους μπορεί να πιστοποιηθεί ότι παρέχει συμμόρφωση με τους κανονισμούς ασφάλειας ή απορρήτου, οι πάροχοι ενδέχεται να είναι σε θέση να βοηθήσουν στη συμμόρφωση με την νομοθεσία σε κλίμακα νέφους. Οι πάροχοι υπολογιστικού νέφους ενδέχεται, επίσης, να είναι σε θέση να βοηθήσουν στη διάδοση πληροφοριών που επιτρέπουν στους ενοικιαστές να αξιολογούν τους κινδύνους δικαιοδοσίας και να συμβαδίζουν με την τοπική νομοθεσία. [27]

Οι οικονομίες κλίμακας που παρουσιάζουν αυτές οι λύσεις ασφαλείας εξηγούν γιατί οι υπάρχουσες λύσεις διαχειριζόμενης ασφάλειας είναι ένας μεγάλος επιχειρηματικός τομέας, παρά τους περιορισμούς κλίμακας που προκύπτουν από την ύπαρξη πελατών σε κατανεμημένες τοποθεσίες με ετερογενείς υποδομές. Η Gartner[33] εκτιμά ότι η συνολική διαχειριζόμενη αγορά παρόχων υπηρεσιών ασφαλείας είχε έσοδα περίπου 500 εκατομμυρίων δολαρίων το 2009. Μεγάλοι τηλεπικοινωνιακοί φορείς όπως η BT[34] και η Verizon[35] προσφέρουν τώρα αυτό το είδος υπηρεσιών. [27]

Όπως αναφέρθηκε προηγουμένως, οι πάροχοι φιλοξενίας νέφους επωφελούνται από την ευκαιρία να οικοδομήσουν σχέσεις μέσω των επαναλαμβανόμενων αλληλεπιδράσεων τους με τις ρυθμιστικές αρχές και τις αρχές επιβολής του νόμου. Εάν οι φορείς επιβολής του νόμου γνωρίζουν ότι ο πάροχος νέφους μπορεί να τους εγγυηθεί πρόσβαση σε αρχεία καταγραφής ελέγχου και στιγμιότυπα δεδομένων, ακόμη και αν ένας ενοικιαστής αποδειχθεί κακόβουλος, είναι λιγότερο πιθανό να βγάλουν έναν ενοικιαστή, ή ακόμα και ένα ολόκληρο κέντρο δεδομένων, εκτός σύνδεσης για την προστασία μιας έρευνας. Πιο στρατηγικά, οι πάροχοι νέφους μπορούν να αναλάβουν ενεργό ρόλο στη διαμόρφωση της συμμόρφωσης και των νομικών καθεστώτων για να ευνοήσουν τους ενοικιαστές τους. [27]

Επομένως, συνοψίζοντας, η φιλοξενία στο υπολογιστικό νέφος έχει επιθυμητά χαρακτηριστικά, όπως χαμηλό αρχικό κόστος, ελαστικότητα πόρων και εξοικονόμηση κόστους που προκύπτουν από οικονομίες κλίμακας. Η αυτο-φιλοξενούμενη (επιτόπια) υποδομή παρέχει μεγαλύτερο άμεσο έλεγχο στην υποδομή από ό,τι μπορεί να επιτευχθεί κατά τη μίσθωση κοινής υποδομής από το νέφος. Παρόλα αυτα, πρέπει να ληφθεί υπόψη ότι στην αυτο-φιλοξενούμενη υποδομή απαιτείται η ύπαρξη ικανοτήτων και εξειδικευμένου προσωπικού στην ασφάλεια καθώς και η προϋπάρχουσα τοπική υποδομή που να έχει σχεδιαστεί με γνώμονα την ασφάλεια. Η επίτευξη των πλεονεκτημάτων της υποδομής νέφους

[33] Η Gartner, Inc. είναι μια εταιρεία τεχνολογικής έρευνας και συμβούλων με έδρα το Στάμφορντ του Κονέκτικατ που διεξάγει έρευνα για την τεχνολογία και μοιράζεται αυτήν την έρευνα τόσο μέσω ιδιωτικών συμβουλών όσο και μέσω προγραμμάτων εκτελεστικών στελεχών και συνεδρίων

[34] Η BT Counterpane, πρώην Counterpane Internet Security, Inc., είναι μια εταιρεία που πουλάει υπηρεσίες ασφάλειας διαχειριζόμενων δικτύων υπολογιστών

[35] Η Verizon Communications Inc., κοινώς γνωστή ως Verizon, είναι ένας αμερικανικός πολυεθνικός όμιλος τηλεπικοινωνιών

μέσω της μεταφοράς του ελέγχου της υποδομής σε τρίτο μέρος δεν οδηγεί απαραίτητα σε καθαρή απώλεια ασφάλειας διότι η ασφάλεια μπορεί επίσης να επωφεληθεί από οικονομίες κλίμακας. Ειδικότερα, οι πάροχοι νέφους μπορούν να "αντέξουν" οικονομικά μέτρα ασφαλείας με προκαταβολικά κόστη που θα ήταν απρόσιτα σε περιβάλλοντα αυτο-φιλοξενίας, αποσβένοντας αυτά τα κόστη σε σχέση με ένα μεγάλο πλήθος μηχανημάτων. Μια βασική ερευνητική ευκαιρία είναι η ανάπτυξη μέτρων ασφαλείας που μειώνουν το οριακό κόστος, ακόμη και αν συνεπάγονται μεγαλύτερο αρχικό κόστος. Στον πίνακα 8 παρουσιάζονται τα πλεονεκτήματα και τα μειονεκτήματα ως προς τα χαρακτηριστικά ασφαλείας της αυτο-φιλοξενούμενης υποδομής και της ενοικιαζόμενης υποδομής στο νέφος [27]

Πίνακας 8. Σύγκριση πλεονεκτημάτων και μειονεκτημάτων ασφάλειας του υπολογιστικού νέφους και τον τοπικών συστημάτων [27]

Χαρακτηριστικά ασφάλειας	Self Hosting (Αυτο-φιλοξενούμενη Υποδομή)		Cloud Hosting (Ενοικιαζόμενη Υποδομή στο Νέφος)	
	Πλεονεκτήματα	Μειονεκτήματα	Πλεονεκτήματα	Μειονεκτήματα
Επαναχρησιμοποίηση δεδομένων (αποκατάσταση από καταστροφές και αντίγραφα ασφαλείας)	Δίνει φυσικό έλεγχο στο αντίγραφο ασφαλείας.	Απαιτεί επένδυση κεφαλαίου σε υλικό και υποδομή.	Δεν χρειάζεται τοπικό υλικό ή έξοδα κεφαλαίου. Κατάλληλο για μικρότερες εταιρείες που μπορεί να αναπτυχθούν σε σύντομο χρονικό διάστημα με αποτέλεσμα να χρειαστούν επέκταση του αποθηκευτικού χώρου τους.	Το κόστος της ανάκτησης δεδομένων αυξάνεται εφόσον η ανάκτηση είναι συχνή και άμεση. Το κόστος μπορεί να είναι ευνοϊκό μόνο σε περιπτώσεις που δεν χρειάζεται η άμεση και συχνή ανάκτηση.
Έλεγχος απορρήτου δεδομένων	Διατηρεί κρίσιμα δεδομένα εσωτερικά. Κανένα τρίτο μέρος δεν έχει πρόσβαση σε αυτά.	Απαιτεί φυσικό χώρο πχ. δωμάτιο διακομιστή, όπως και την αποκλειστική υποστήριξη IT.	Οι κανόνες απορρήτου καθορίζονται για όλους τους παρόχους και οι πάροχοι είναι αναγκασμένοι να τους εφαρμόζουν.	Ο οργανισμός ή η επιχείρηση δεν μπορούν να επέμβουν και να αλλάξουν τους κανόνες σχετικά με το απόρρητο των δεδομένων.
Προσβασιμότητα	Δεν χρειάζεται σύνδεση Διαδικτύου για πρόσβαση στα δεδομένα.	Μπορεί να είναι πιο ευαίσθητη σε απώλεια δεδομένων κατά τη διάρκεια	Η δημιουργία αντιγράφων ασφαλείας και η επαναφορά μπορούν να ξεκινήσουν από οπουδήποτε,	Εάν η συνδεσιμότητα με το διαδίκτυο διακοπεί στην πλευρά του ενοικιαστή ή στην πλευρά του παρόχου

		καταστροφών λόγω της εσωτερικής του θέσης ιδιαίτερα σε περιπτώσεις που τα δεδομένα δεν αναπαράγονται προς επίτευξη υψηλής διαθεσιμότητας και αξιοπιστίας (το πόσο συχνά μεταφέρονται τα δεδομένα εκτός τοποθεσίας αντικατοπτρίζει πόσα δεδομένα θα χαθούν σε περίπτωση έκτακτης ανάγκης).	χρησιμοποιώντας οποιονδήποτε υπολογιστή, tablet ή smartphone όπως επίσης μπορούν και να αυτοματοποιούνται.	νέφους, δεν θα υπάρχει πρόσβαση σε καμία από τις πληροφορίες και τα δεδομένα.
Εμπειρογνωμοσύνη και πόροι	Η τεχνογνωσία καθορίζεται από τις προδιαγραφές που θέτει ο οργανισμός εσωτερικά.	Απαιτεί εσωτερική εμπειρογνωμοσύνη και πόρους	Βασίζεται στην (υπάρχουσα) εμπειρογνωμοσύνη του παρόχου στον τομέα της ασφάλειας	Ο καταναλωτής δεν γνωρίζει το επίπεδο εμπειρίας του παρόχου ώστε να κάνει την καλύτερη δυνατή επιλογή παρόχου. Ο πάροχος αναλαμβάνει την συχνότητα των ενημερώσεων ασφαλείας.
Επιφάνεια επίθεσης	Μειωμένη επιφάνεια επίθεσης	Λόγω ανεπάρκειας προσωπικού, μπορεί η διαμόρφωση και η	Χρήση κατάλληλων αρχιτεκτονικών ασφάλειας, προτύπων και διαδικασιών και	Μεγάλη επιφάνεια επίθεσης (για το δημόσιο νέφος)

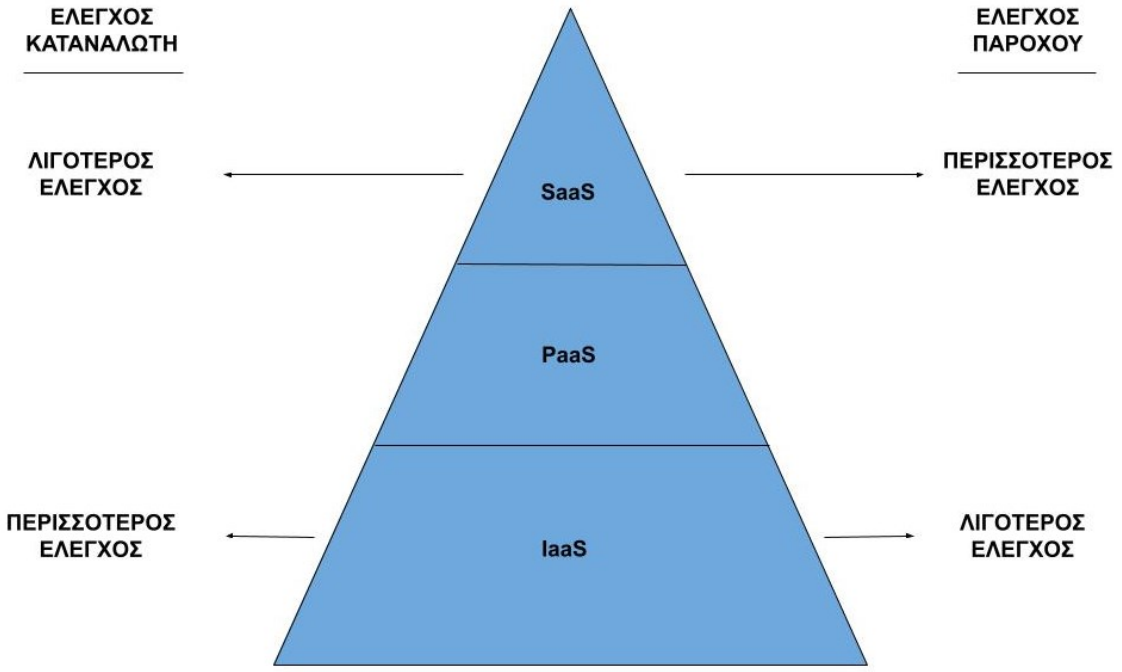
		αρχιτεκτονική ασφάλειας που εφαρμόζεται να μην είναι ικανοποιητική ή ακόμη και ανεπαρκής.	μέτρων ασφάλειας και διαμόρφωση ασφάλειας από έμπειρα και άριστα καταρτισμένο προσωπικό. Αυτό συντελεί σε μείωση των δυνητικών ευπαθειών στο σύστημα και σε ικανότητα μετρίασης και αποφυγής δυνητικών επιθέσεων.	
Κανονιστική συμμόρφωση και πιστοποιήσεις	Λόγω μειωμένης πολυπλοκότητας και μεγέθους, η υλοποίηση της συμμόρφωσης θα είναι πιο εύκολη.	Απαιτεί ανεξάρτητη διασφάλιση της συμμόρφωσης.	Υπάρχει συμμόρφωση με τα πρότυπα και τους κανονισμούς του κλάδου.	Μερικές φορές η συμμόρφωση μπορεί να είναι προβληματική εφόσον υπάρχουν διενέξεις μεταξύ κανόνων ενός κλάδου και της νομοθεσίας στην χώρα φιλοξενίας της υποδομής.
Ασφάλεια υποδομής	Έλεγχος της εφαρμογής των μέτρων ασφαλείας.	Απαιτείται επιπλέον κόστος για την δημιουργία ή την αγορά μέτρων ασφαλείας της υποδομής.	Προηγμένα μέτρα φυσικής, ψηφιακής και δικτυακής ασφάλειας.	Η ασφάλεια εξαρτάται αποκλειστικά από τον πάροχο και ο εκάστοτε οργανισμός δεν μπορεί να επέμβει.

5.2 Συγκρίσεις παρόχων

Οι καταναλωτές του υπολογιστικού νέφους έχουν σημαντικές απώλειες όταν παραβιάζεται μια υπηρεσία νέφους. Η οπτική των 2 βασικών κατηγοριών ενδιαφερομένων, δηλαδή των παρόχων και των χρηστών, δεν πρέπει να παραμελείται όταν μιλάμε για την ασφάλεια του νέφους. Η διακοπή της υπηρεσίας, η απώλεια δεδομένων και η παραβίαση του απορρήτου των χρηστών μπορούν να καταστρέψουν την επιχειρηματική εικόνα του παρόχου με αποτέλεσμα να μειωθεί το πελατολόγιό του και το μερίδιό του στην αγορά. Επομένως, οι πάροχοι υπολογιστικού νέφους πρέπει να επιλέγουν προσεκτικά και να προσαρμόζουν τις επιλογές και λύσεις ασφαλείας για τις υπηρεσίες νέφους τους.

Επιπλέον, οι καταναλωτές νέφους πρέπει να έχουν περισσότερες γνώσεις και έλεγχο σχετικά με τον τρόπο με τον οποίο η υπηρεσία υπολογιστικού νέφους τους είναι ασφαλής για να μπορούν να προετοιμάσουν ένα σχέδιο διαχείρισης κινδύνου (για παράδειγμα). Με αυτό τον τρόπο, θα μπορούν να διαμορφώνουν κατάλληλα την ασφάλεια των υπηρεσιών που χρησιμοποιούν (ανάλογα βέβαια με το είδος της υπηρεσίας προς κατανάλωση) ή ακόμη και να την ενισχύουν, εφόσον αυτό είναι εφικτό. Τέλος, πρέπει να υπάρχει κάποιο είδος πιστοποίησης ώστε οι καταναλωτές να έχουν μεγαλύτερη εμπιστοσύνη στον πάροχο υπηρεσιών. [28]

Η Εικόνα 5 δείχνει τα διαφορετικά μοντέλα παράδοσης/υπηρεσιών νέφους και τον βαθμό ελέγχου που έχουν ο καταναλωτής και ο πάροχος υπηρεσιών νέφους για καθένα από αυτά τα μοντέλα. Παρατηρούμε ότι καθώς το μοντέλο παράδοσης αλλάζει από IaaS σε PaaS και σε SaaS, ο έλεγχος των καταναλωτών για την ασφάλεια και το απόρρητο μειώνεται. Ωστόσο, ο έλεγχος του παρόχου αυξάνεται. [28]



Εικόνα 5. Απεικόνιση κατοχής ελέγχου από τους καταναλωτές και τους παρόχους ανά μοντέλο υπηρεσιών

Παρακάτω κατηγοριοποιούμε τα χαρακτηριστικά ασφάλειας και απορρήτου του υπολογιστικού νέφους και εξηγούμε τη σημασία τους. Επισημαίνουμε, επίσης, πτυχές που θα πρέπει να έχουν σημασία για τους καταναλωτές κατά την έρευνα για διαφορετικούς παρόχους (CSPs) για κάθε χαρακτηριστικό. Στην συνέχεια εξηγούμε πώς αυτά τα χαρακτηριστικά μπορούν να χρησιμοποιηθούν για την αξιολόγηση και τη σύγκριση πιθανών υπηρεσιών υπολογιστικού νέφους. Για την σύγκριση χρησιμοποιήσαμε τα δεδομένα από τρεις εξέχοντες εμπορικούς CSPs, συγκεκριμένα, τον Amazon Web Services (AWS), τον Microsoft Azure και τον Google Cloud Platform (GCP). [28]

5.2.1 Δημιουργία Αντιγράφων και Αποκατάσταση από καταστροφές

Οι πάροχοι υπολογιστικού νέφους συνήθως προσφέρουν μια υπηρεσία δημιουργίας αντιγράφων (backup service). Η υπηρεσία αυτή είναι απαραίτητη για την προστασία, ανάκτηση και διαθεσιμότητα δεδομένων καθώς και την ανθεκτικότητα του κέντρου δεδομένων. Οι καταναλωτές πρέπει να έχουν, εκτός από την ικανότητα δημιουργίας αντιγράφων (που είτε είναι εγχώρια είτε παρέχεται από το νέφος), και ένα σχέδιο ανάκαμψης από καταστροφές (disaster recovery plan) για την επιχειρηματική τους συνέχεια. Το Disaster Recovery as a Service, μια διαχειρίσιμη υπηρεσία ασφάλειας, επιτρέπει στον ιδιοκτήτη επιχείρησης να επανέλθει γρήγορα μετά από μια καταστροφή (όσον αφορά την αποκατάσταση των δεδομένων και της λειτουργίας των συστημάτων του που βρίσκονται στο νέφος). Οι πιο σημαντικοί παράγοντες για τους οποίους πρέπει να ενδιαφέρονται οι καταναλωτές κατά την έρευνα διαφορετικών παρόχων για το χαρακτηριστικό αυτό είναι είναι οι εξής:

1. Προσφέρονται αυτοματοποιημένες υπηρεσίες δημιουργίας αντιγράφων ασφαλείας;
2. Είναι δυνατή η ανάκτηση των δεδομένων εάν υπάρχει καταστροφή στην υποδομή cloud;
3. Παρέχεται ανάπτυξη πολλαπλών ζωνών διαθεσιμότητας[36] (Multi-AZ); [28]

Πίνακας 9. Σύγκριση των ικανοτήτων διενέργειας αντιγράφων και επαναφοράς από καταστροφές των παρόχων υπολογιστικού νέφους AWS, Microsoft Azure και του Google Cloud [47] [48] [49] [50]

[36] Μια Ζώνη Διαθεσιμότητας είναι ένα φυσικά ξεχωριστό κέντρο δεδομένων σε μια συγκεκριμένη περιοχή. Το Multi-AZ αναφέρεται στην έννοια της ανάπτυξης πόρων σε πολλαπλές Ζώνες Διαθεσιμότητας (σε μια περιοχή ή κατά μήκος πολλαπλών περιοχών) για τη διασφάλιση πλεονασμού και την ελαχιστοποίηση του χρόνου διακοπής λειτουργίας σε περίπτωση βλαβών.

Ανησυχία Καταναλωτή	Amazon Web Services (AWS)	Microsoft Azure	Google Cloud Platform (GCP)
Προσφέρονται αυτοματοποιημένες υπηρεσίες δημιουργίας αντιγράφων ασφαλείας;	Η AWS προσφέρει το AWS Backup[37] (Back up as a service), το οποίο παρέχει μια συγκεντρωτική και πλήρως διαχειρίσιμη υπηρεσία δημιουργίας αντιγράφων ασφαλείας για τους πόρους του AWS. Υποστηρίζει τη δημιουργία αντιγράφων ασφαλείας και την αποκατάσταση διαφόρων υπηρεσιών AWS, συμπεριλαμβανομένων των Amazon EC2[38] instances (δηλ. στιγμιοτύπων εικονικών μηχανών), των βάσεων δεδομένων Amazon RDS[39], των τόμων Amazon EBS[40] και άλλων, καθώς και προσφέρει αυτοματοποιημένο προγραμματισμό αντιγράφων ασφαλείας, διαχείριση διατήρησης και αυξητικά αντίγραφα ασφαλείας για την ελαχιστοποίηση του κόστους αποθήκευσης. Παρέχει χαρακτηριστικά όπως αντίγραφα ασφαλείας μεταξύ περιοχών και λογαριασμών για πρόσθετη ανθεκτικότητα και προστασία δεδομένων.	Το Azure Backup[42] είναι ένας τρόπος δημιουργίας αντιγράφων ασφαλείας και επαναφοράς δεδομένων στο νέφος. Υποστηρίζει διάφορους φόρτους εργασίας (workloads), όπως εικονικές μηχανές, βάσεις δεδομένων SQL και διακομιστές αρχείων. Το Azure Storage backup [43]είναι μια επιλογή για τη δημιουργία αντιγράφων ασφαλείας των δεδομένων που είναι αποθηκευμένα στο Azure Blob Storage[44]. Παρέχει αυξητικά (incremental) αντίγραφα ασφαλείας και μπορεί να χρησιμοποιηθεί τόσο για βραχυπρόθεσμη όσο και για μακροπρόθεσμη αποθήκευση αντιγράφων ασφαλείας.	Το Google Cloud Platform παρέχει διάφορες επιλογές δημιουργίας αντιγράφων ασφαλείας, όπως το Google Cloud Storage[45] για αντίγραφα ασφαλείας αποθήκευσης αντικειμένων και στιγμιότυπα για αντίγραφα ασφαλείας μόνιμου δίσκου. Το Google Cloud Backup[46] είναι μια διαχειριζόμενη υπηρεσία δημιουργίας αντιγράφων ασφαλείας για πόρους του Google Cloud, όπως εικονικές μηχανές, βάσεις δεδομένων και αποθήκευση αρχείων.

[37] https://aws.amazon.com/backup/
[38] https://aws.amazon.com/ec2/
[39] https://aws.amazon.com/rds/
[40] https://aws.amazon.com/ebs/
[41] https://aws.amazon.com/s3/
[42] https://learn.microsoft.com/en-us/azure/backup/backup-overview
[43] https://learn.microsoft.com/en-us/azure/backup/blob-backup-overview
[44] https://azure.microsoft.com/en-us/products/storage/blobs
[45] https://cloud.google.com/storage
[46] https://cloud.google.com/backup-disaster-recovery/docs/deployment/deployment-plan#overview_of_the_service_architecture

Η Amazon διαθέτει το υπολογιστικό σύννεφο EC2 και το αποθετήριο δεδομένων S3[41]. Από προεπιλογή μπορεί κανείς να δημιουργήσει αντίγραφα ασφαλείας από το EC2 στο S3. Ο καταναλωτής μπορεί είτε να το εκτελέσει χειροκίνητα είτε να χρησιμοποιήσει εργαλεία προγραμματισμού όπως το

	cron.		
Μπορούμε να ανακτήσουμε τα δεδομένα εάν υπάρχει καταστροφή στην υποδομή cloud;	Το AWS προσφέρει πρόσθετες υπηρεσίες ανάκαμψης από καταστροφές, όπως το AWS Disaster Recovery[47], το οποίο επιτρέπει την αντιγραφή και ανάκτηση εφαρμογών σε περίπτωση διακοπής λειτουργίας. Το EC2 παρέχει πολλαπλές επιλογές για την αποκατάσταση καταστροφών. Οι χρήστες μπορούν να αντιγράψουν (replicating) τις περιπτώσεις (instances) (εικονικών μηχανών) EC2 τους σε διαφορετικές ζώνες διαθεσιμότητας (AZ) εντός μιας περιοχής για υψηλή διαθεσιμότητα. Επιπλέον, μπορούν να χρησιμοποιήσουν υπηρεσίες AWS όπως το Amazon Elastic Block Store (EBS) και το Amazon S3 για να δημιουργήσουν αντίγραφα ασφαλείας των δεδομένων τους σε διαφορετικές περιοχές για σκοπούς ανάκαμψης από καταστροφές.	Η Azure Site Recovery[48] (ASR) είναι μια υπηρεσία που επιτρέπει την αποκατάσταση από καταστροφή για Azure εικονικές μηχανές (VMs) και φόρτους εργασίας στις εγκαταστάσεις. Επιτρέπει την αντιγραφή (replicating) VMs σε μια δευτερεύουσα περιοχή Azure ή στο κέντρο δεδομένων του ίδιου του χρήστη, παρέχοντας δυνατότητες failover και failback.	Το Google Cloud Disaster Recovery περιλαμβάνει υπηρεσίες όπως το Google Cloud VMware Engine[49] για την αντιγραφή (replicating) και ανάκτηση φόρτων εργασίας VMware και το Google Cloud Deployment Manager[50] για την ενορχήστρωση της υποδομής κατά τη διάρκεια σεναρίων ανάκαμψης από καταστροφές.
Ανάπτυξη πολλαπλών ζωνών διαθεσιμότητας (Multi-AZ)	Η AWS (Amazon Web Services) παρέχει δυνατότητες (ανάπτυξης φόρτων εργασίας & αντιγραφής δεδομένων) πολλαπλών ζωνών διαθεσιμότητας Multi-AZ (Availability Zone) για ορισμένες υπηρεσίες της όπως	Το Microsoft Azure παρέχει δυνατότητες πολλαπλών ζωνών διαθεσιμότητας (Multi-AZ) σε κάποιες από τις υπηρεσίες του όπως: τις εικονικές μηχανές (VM) Azure, την υπηρεσία βάσεων δεδομένων Azure SQL Database[51] και το Azure Storage[52]	Το Google Cloud Platform (GCP) παρέχει διαμορφώσεις πολλαπλών ζωνών και περιοχών για κάποιες από τις υπηρεσίες του όπως: την Google Compute Engine[53] για την αποθήκευση στιγμιοτύπων (εικονικών μηχανών) σε πολλαπλές ζώνες, την υπηρεσία

[47] https://aws.amazon.com/disaster-recovery/
[48] https://learn.microsoft.com/en-us/azure/site-recovery/site-recovery-overview
[49] https://cloud.google.com/vmware-engine/docs/vmware-ecosystem/howto-disaster-recovery-zerto
[50] https://cloud.google.com/architecture/dr-scenarios-for-applications
[51] https://learn.microsoft.com/en-us/azure/azure-sql/database/database-copy-overview?view=azuresql
[52] https://learn.microsoft.com/en-us/azure/storage/common/storage-introduction
[53] https://cloud.google.com/compute/docs/instances/nested-virtualization/overview

	το Amazon EC2 (Elastic Compute Cloud), την Amazon RDS (Υπηρεσία σχεσιακών βάσεων δεδομένων), και την Amazon S3 (Simple Storage Service)		αποθήκευσης Google Cloud Storage, την υπηρεσία βάσεων δεδομένων Google Cloud SQL[54] και την υπηρεσία Google Kubernetes Engine (GKE)[55] για την διαχείριση δοχειοποιημένων εφαρμογών (container-based applications)

Παρατηρούμε ότι για την δημιουργία αντιγράφων ασφαλείας και οι τρεις πάροχοι προσφέρουν ανταγωνιστικές αυτοματοποιημένες λύσεις όπως αντίστοιχα και για την αποκατάσταση από τις καταστροφές. Παρατηρούμε επίσης ότι και οι τρεις πάροχοι παρέχουν πολλαπλές ζώνες διαθεσιμότητας για κάποιες από τις υπηρεσίες τους. Μπορούμε να πούμε, λοιπόν, ότι δεν υστερεί κάποιος πάροχος ως προς τις συγκεκριμένες ανησυχίες.

5.2.2 Κρυπτογράφηση

Το Dropbox επέτρεψε σε οποιονδήποτε στον κόσμο να έχει πρόσβαση σε οποιοδήποτε από τα 25 εκατομμύρια ντουλάπια αποθήκευσης (storage lockers) των πελατών του, απλά πληκτρολογώντας οποιονδήποτε κωδικό πρόσβασης το 2011. Αυτό εγείρει την ανάγκη κρυπτογράφησης για δεδομένα που αποθηκεύονται στο νέφος και όχι μόνο για δεδομένα που μεταφέρονται από και προς το νέφος έτσι ώστε να μην μπορούν να γίνουν εκμεταλλεύσιμα από έναν εισβολέα. Οι καταναλωτές πρέπει να διασφαλίσουν ότι

1) Τα δεδομένα συναλλαγών τους που μεταφέρονται προς και από την υπηρεσία νέφους κρυπτογραφούνται προκαθορισμένα
2) Τα δεδομένα που βρίσκονται σε διακομιστές νέφους είναι κρυπτογραφημένα από προεπιλογή
3) Ο πάροχος χρησιμοποιεί κατάλληλους αλγόριθμους κρυπτογράφησης
4) Υπάρχει υπηρεσία διαχείρισης κλειδιών [28]

Πίνακας 10. Σύγκριση ικανοτήτων κρυπτογράφησης των παρόχων υπολογιστικού νέφους AWS, Microsoft Azure και Google Cloud. [51] [52] [53]

Ανησυχία Καταναλωτή	Amazon Web Services (AWS)	Microsoft Azure	Google Cloud Platform (GCP)
Τα δεδομένα συναλλαγών που μεταφέρονται προς και από την	Το AWS υποστηρίζει τα πρωτόκολλα κρυπτογράφησης TLS για την ασφάλεια των δεδομένων κατά τη μεταφορά. Κατά τη σύνδεση σε υπηρεσίες	Το Azure υποστηρίζει πρωτόκολλα κρυπτογράφησης TLS για την ασφάλεια των δεδομένων κατά τη μεταφορά και για τη δημιουργία	Το Google Cloud χρησιμοποιεί από προεπιλογή πρωτόκολλα κρυπτογράφησης TLS για δεδομένα που μεταφέρονται μέσω του διαδικτύου. Κατά την

[54] https://cloud.google.com/sql/docs/introduction
[55] https://cloud.google.com/kubernetes-engine/docs/concepts/kubernetes-engine-overview

υπηρεσία νέφους κρυπτογραφούνται προκαθορισμένα	AWS μέσω του διαδικτύου, το TLS μπορεί να χρησιμοποιηθεί για τη δημιουργία ασφαλών και κρυπτογραφημένων συνδέσεων από προεπιλογή.	ασφαλών και κρυπτογραφημένων συνδέσεων.	επικοινωνία με τις υπηρεσίες του Google Cloud, το TLS χρησιμοποιείται για τη δημιουργία ασφαλών και κρυπτογραφημένων συνδέσεων.
Τα δεδομένα που βρίσκονται σε διακομιστές νέφους είναι κρυπτογραφημένα από προεπιλογή	Τα δεδομένα που βρίσκονται σε διακομιστές νέφους στο AWS (Amazon Web Services) δεν κρυπτογραφούνται από προεπιλογή. Ωστόσο παρέχονται ορισμένες βασικές επιλογές κρυπτογράφησης για δεδομένα σε κατάσταση ηρεμίας σε διάφορες υπηρεσίες στο AWS που μπορούν να χρησιμοποιήσουν οι χρήστες όπως: ● το Amazon S3 προσφέρει κρυπτογράφηση από την πλευρά του διακομιστή για την κρυπτογράφηση δεδομένων σε κατάσταση ηρεμίας με διάφορες επιλογές κρυπτογράφησης, όπως SSE-S3[56] (Server-Side Encryption with S3 Managed Keys), SSE-KMS[57] (Server-Side Encryption with AWS Key Management Service) ή SSE-C[58] (Server-Side Encryption with Customer-Provided	Τα δεδομένα που βρίσκονται σε διακομιστές νέφους κρυπτογραφούνται από προεπιλογή για ορισμένες υπηρεσίες του Azure όπως για παράδειγμα: ● Το Azure Storage κρυπτογραφεί αυτόματα τα δεδομένα σε κατάσταση ηρεμίας για υπηρεσίες όπως το Azure Blob storage και το Azure File storage[60] με την χρήση του αλγόριθμου κρυπτογράφησης AES-256. ● Η βάση δεδομένων Azure SQL Database προσφέρει από προεπιλογή διαφανή κρυπτογράφηση δεδομένων (TDE) με την χρήση του αλγόριθμου κρυπτογράφησης AES-256. ● οι Διαχειριζόμενοι δίσκοι Azure (Azure Managed Disks)[61]	Στο Google Cloud, τα δεδομένα που βρίσκονται σε διακομιστές νέφους είναι κρυπτογραφημένα από προεπιλογή σε ορισμένες υπηρεσίες όπως για παράδειγμα: ● Στο Google Cloud Storage η διαδικασία κρυπτογράφησης είναι διαφανής για τον χρήστη και πραγματοποιείται παρασκηνιακά με την χρήση του αλγορίθμου AES-256 ● Η υπηρεσία Google Cloud Bigtable[63] που χρησιμοποιείται για διαχείριση μεγάλων βάσεων δεδομένων κρυπτογραφεί τα δεδομένα με την χρήση του αλγορίθμου AES-256 ● Η υπηρεσία βάσεων δεδομένων Google Cloud SQL[64] κρυπτογραφεί τα δεδομένα με την χρήση του αλγόριθμου AES-

[56] https://docs.aws.amazon.com/AmazonS3/latest/userguide/UsingServerSideEncryption.html
[57] https://docs.aws.amazon.com/AmazonS3/latest/userguide/UsingKMSEncryption.html
[58] https://docs.aws.amazon.com/AmazonS3/latest/userguide/ServerSideEncryptionCustomerKeys.html
[60] https://learn.microsoft.com/en-us/azure/storage/files/storage-files-introduction
[61] https://learn.microsoft.com/en-us/azure/virtual-machines/managed-disks-overview
[63] https://cloud.google.com/bigtable/docs/overview
[64] https://cloud.google.com/sql/docs/introduction

	Keys). Σε όλες τις περιπτώσεις χρησιμοποιείται ο αλγόριθμος AES-256. ● οι τομείς Amazon EBS μπορούν να κρυπτογραφηθούν για την προστασία των δεδομένων που είναι αποθηκευμένα στους εικονικούς δίσκους με χρήση της κρυπτογράφησης AWS KMS[59] (Key Management Service) με την χρήση του αλγορίθμου AES-256. ● η Amazon RDS (Υπηρεσία σχεσιακών βάσεων δεδομένων) παρέχει επιλογές κρυπτογράφησης για δεδομένα σε κατάσταση ηρεμίας για περιπτώσεις βάσεων δεδομένων. Οι χρήστες μπορούν να επιλέξουν να ενεργοποιήσουν την κρυπτογράφηση χρησιμοποιώντας την υπηρεσία AWS KMS και να κρυπτογραφήσουν τα δεδομένα τους με την χρήση του αλγορίθμου AES-256	προσφέρουν κρυπτογράφηση σε κατάσταση ηρεμίας από προεπιλογή. Οι διαχειριζόμενοι δίσκοι χρησιμοποιούν την υπηρεσία κρυπτογράφησης Azure Storage Service Encryption (SSE)[62] με την χρήση του αλγόριθμου κρυπτογράφησης AES-256.	256. ● Το Google Cloud Spanner[65], μια παγκοσμίως κατανεμημένη υπηρεσία σχεσιακών βάσεων δεδομένων, χρησιμοποιεί τον αλγόριθμο κρυπτογράφησης AES-256
Ποιους αλγόριθμους κρυπτογράφησης	Η AWS χρησιμοποιεί ● τον AES-256, έναν συμμετρικό αλγόριθμο κρυπτογράφησης, για	Το Microsoft Azure χρησιμοποιεί διάφορους αλγόριθμους κρυπτογράφησης όπως:	Το Google Cloud χρησιμοποιεί τους παρακάτω αλγόριθμους κρυπτογράφησης :

[59] https://docs.aws.amazon.com/kms/latest/developerguide/overview.html
[62] https://learn.microsoft.com/en-us/azure/storage/common/storage-service-encryption
[65] https://cloud.google.com/spanner/docs#docs

χρησιμοποιεί ο πάροχος;	την κρυπτογράφηση δεδομένων σε κατάσταση ηρεμίας και κατά τη μεταφορά. ● τον αλγόριθμο ασύμμετρης κρυπτογράφησης RSA και τον ECC (κρυπτογραφία ελλειπτικής καμπύλης) για εργασίες όπως η ασφαλής ανταλλαγή κλειδιών και οι ψηφιακές υπογραφές. ● τον HMAC-SHA256 & HMAC-SHA512 (Κώδικας ελέγχου ταυτότητας μηνυμάτων με βάση κατακερματισμό) για σκοπούς ακεραιότητας δεδομένων, ψηφιακών υπογραφών και ελέγχου ταυτότητας.	● τον AES-256 για την κρυπτογράφηση δεδομένων σε κατάσταση ηρεμίας και κατά τη μεταφορά. ● τον αλγόριθμο ασύμμετρης κρυπτογράφησης RSA και τον ECC (κρυπτογραφία ελλειπτικής καμπύλης) για εργασίες όπως η ασφαλής ανταλλαγή κλειδιών, οι ψηφιακές υπογραφές και ο έλεγχος ταυτότητας βάσει πιστοποιητικών ● τις συναρτήσεις κατακερματισμού SHA-256 και SHA-512, για την ακεραιότητα δεδομένων και τις ψηφιακές υπογραφές.	● τον AES-256, έναν συμμετρικό αλγόριθμο κρυπτογράφησης, για την κρυπτογράφηση δεδομένων σε κατάσταση ηρεμίας και κατά τη μεταφορά. ● τον αλγόριθμο ασύμμετρης κρυπτογράφησης RSA και τον ECC (κρυπτογραφία ελλειπτικής καμπύλης) για εργασίες όπως η ασφαλής ανταλλαγή κλειδιών και οι ψηφιακές υπογραφές. ● τον HMAC-SHA256 (Κώδικας ελέγχου ταυτότητας μηνυμάτων με βάση κατακερματισμό) για σκοπούς ακεραιότητας δεδομένων, ψηφιακών υπογραφών και ελέγχου ταυτότητας.
Υπάρχει υπηρεσία διαχείρισης κλειδιών	Το AWS KMS[66] (Key Management Service) είναι μια πλήρως διαχειρίσιμη υπηρεσία που επιτρέπει την δημιουργία και τον έλεγχο των κλειδιών κρυπτογράφησης που χρησιμοποιούνται για την κρυπτογράφηση των δεδομένων των καταναλωτών. Ενσωματώνεται με πολλές άλλες υπηρεσίες του AWS, επιτρέποντάς την κρυπτογράφηση των δεδομένων	Το Azure Key Vault[67] είναι μια υπηρεσία που βασίζεται στο cloud και επιτρέπει την διασφάλιση κρυπτογραφικών κλειδιών και πιστοποιητικών που χρησιμοποιούνται από εφαρμογές και υπηρεσίες cloud. Επιτρέπει την ασφαλή διαχείριση κλειδιών και τον έλεγχο πρόσβασης για την κρυπτογράφηση δεδομένων και τη διαχείριση πιστοποιητικών.	Το Google Cloud KMS[68] είναι μια υπηρεσία διαχείρισης κλειδιών που επιτρέπει την δημιουργία, την χρήση και την καταστροφή κλειδιών κρυπτογράφησης στο νέφος. Ενσωματώνεται με άλλες υπηρεσίες του GCP για να παρέχει δυνατότητες κρυπτογράφησης και αποκρυπτογράφησης για δεδομένα που είναι αποθηκευμένα σε διάφορους

[66] https://docs.aws.amazon.com/kms/latest/developerguide/overview.html
[67] https://learn.microsoft.com/en-us/azure/key-vault/general/overview
[68] https://cloud.google.com/kms/docs#docs

	που είναι αποθηκευμένα σε διάφορους πόρους του AWS, όπως το Amazon S3, τόμους EBS και άλλα.		πόρους του GCP.

Παρατηρούμε ότι οι τρεις πάροχοι χρησιμοποιούν τα ίδια πρωτόκολλα κρυπτογράφησης για τα δεδομένα συναλλαγών που μεταφέρονται προς και από τις υπηρεσίες τους. Παρατηρούμε, επίσης, ότι και οι τρεις πάροχοι προσφέρουν μια ποικιλία από λύσεις κρυπτογράφησης για τα δεδομένα που είναι αποθηκευμένα στους διακομιστές και χρησιμοποιούν συγχρονους και ισχυρούς αλγόριθμους κρυπτογράφησης αλλα και ανταγωνιστικές υπηρεσίες διαχείρισης κλειδιών. Μπορούμε να πούμε, λοιπόν, ότι δεν υστερεί κάποιος πάροχος ως προς την κρυπτογράφηση τόσο των δεδομένων που μεταφέρονται όσο και των δεδομένων που είναι αποθηκευμένα στους διακομιστές. Όμως, τονίζουμε πως μόνο ο Azure φαίνεται να υποστηρίζει την κρυπτογράφηση δεδομένων σε ηρεμία από προ-επιλογή για διάφορες υπηρεσίες & βάσεις δεδομένων του.

5.2.3 Έλεγχος ταυτότητας και έλεγχοι πρόσβασης

Ενώ ο έλεγχος ταυτότητας παρέχει απόδειξη ταυτότητας, δεν περιορίζει τις ενέργειες ή τις λειτουργίες που μπορεί να εκτελέσει ένας νόμιμος χρήστης ενός συστήματος. Επομένως, ο καταναλωτής του υπολογιστικού νέφους πρέπει να αποφασίσει ποιος μπορεί να έχει πρόσβαση σε τι. Ένα σύνολο ερωτήσεων που μπορεί να θέσει ένας καταναλωτής στον πάροχο είναι το εξής:

1) παρέχετε πολιτικές για τον έλεγχο πρόσβασης και αν ναι τι είδους;
2) πόσο ασφαλές είναι το σύστημα ελέγχου ταυτότητας (ποιά είναι τα πρότυπα που χρησιμοποιούνται);
3) ποιοι μηχανισμοί ελέγχου ταυτότητας χρησιμοποιούνται; [28]

Πίνακας 11. Σύγκριση των μεθόδων ελέγχου ταυτότητας και πρόσβασης των παρόχων υπολογιστικού νέφους AWS, Microsoft Azure και Google Cloud [54] [55] [56] [57]

Ανησυχία Καταναλωτή	Amazon Web Services (AWS)	Microsoft Azure	Google Cloud Platform (GCP)
Παρέχονται πολιτικές για τον έλεγχο πρόσβασης και αν ναι τι είδους;	Ο πρωταρχικός μηχανισμός που χρησιμοποιείται για τον έλεγχο πρόσβασης στο AWS είναι το AWS Identity and Access Management (IAM)[69], το οποίο επιτρέπει το ορισμό λεπτομερών πολιτικών πρόσβασης για χρήστες, ομάδες και ρόλους. Οι πολιτικές IAM είναι έγγραφα JSON που καθορίζουν τα δικαιώματα για ενέργειες και πόρους. Επιτρέπει την χορήγηση των λιγότερων απαραίτητων προνομίων για την εκτέλεση συγκεκριμένων ενεργειών, συμβάλλοντας στη διατήρηση της ασφάλειας και της ακεραιότητας του περιβάλλοντός AWS. Η AWS παρέχει την έννοια των ορίων δικαιωμάτων (περιορισμών), η οποία επιτρέπει τον ορισμό μέγιστων δικαιωμάτων που μπορεί να έχει μια οντότητα IAM. Τα όρια δικαιωμάτων μπορούν να βοηθήσουν στην επιβολή αυστηρότερων ελέγχων πρόσβασης και να αποτρέψουν τις οντότητες από το να κλιμακώσουν τα δικά τους δικαιώματα. Παρέχονται δύο είδη πολιτικών, οι πολιτικές που βασίζονται στην ταυτότητα, οι οποίες χορηγούν δικαιώματα σε μια ταυτότητα IAM (χρήστες, ομάδες στις οποίες ανήκουν οι χρήστες ή ρόλους), και οι πολιτικές που βασίζονται στους πόρους και χορηγούν δικαιώματα στον κύριο δικαιούχο (principal) που καθορίζεται στην πολιτική. Οι κύριοι δικαιούχοι μπορεί να βρίσκονται στον ίδιο λογαριασμό	Υπηρεσία ελέγχου πρόσβασης Azure (ACS) βάσει ρόλων (RBAC)[71] που υποστηρίζεται από το Azure Active Directory [72](AD) για τον έλεγχο της πρόσβασης χρηστών σε φιλοξενούμενες εφαρμογές όπως το Windows Live, το Google ή το Facebook. Ενσωματώνεται με το Windows Identity Foundation. Η Azure παρέχει επίσης και την πολιτική Azure (Azure Policy)[73], η οποία αξιολογεί την κατάσταση εξετάζοντας τις ιδιότητες των πόρων που αντιπροσωπεύονται στη διαχείριση πόρων και τις ιδιότητες ορισμένων Παρόχων πόρων. Η Azure Policy διασφαλίζει ότι η κατάσταση των πόρων συμμορφώνεται με τους επιχειρηματικούς κανόνες του καταναλωτή χωρίς να ενδιαφέρεται για το ποιος έκανε την αλλαγή ή ποιος έχει δικαίωμα να κάνει μια αλλαγή. Η Azure Policy μέσω του αποτελέσματος DenyAction μπορεί επίσης να αποκλείσει ορισμένες ενέργειες σε πόρους. Ορισμένοι πόροι της πολιτικής Azure, όπως ορισμοί πολιτικής, ορισμοί πρωτοβουλιών και αναθέσεις, είναι ορατοί σε όλους τους χρήστες. Αυτός ο σχεδιασμός επιτρέπει τη	Το Google Cloud χρησιμοποιεί τον έλεγχο πρόσβασης βάσει ρόλων (RBAC) ως θεμελιώδη μηχανισμό για τον έλεγχο πρόσβασης. Το RBAC στο Google Cloud IAM[75] (Διαχείριση ταυτότητας και πρόσβασης) επιτρέπει τον ορισμό ρόλων και την εκχώρηση συγκεκριμένων δικαιωμάτων σε αυτούς τους ρόλους (χρήστες, ομάδες ή λογαριασμούς υπηρεσιών). Το Google Cloud IAM παρέχει ένα σύνολο προκαθορισμένων ρόλων, όπως ο Ιδιοκτήτης (Owner), ο Συντάκτης (Editor) και ο Θεατής (Viewer), με σαφώς καθορισμένα δικαιώματα. Εκτός από τους προκαθορισμένους ρόλους δίνει την δυνατότητα δημιουργίας προσαρμοσμένων ρόλων που επιτρέπουν τον καθορισμό συγκεκριμένων συνόλων δικαιωμάτων που απαιτούνται για μια συγκεκριμένη περίπτωση χρήσης ή ρόλου/είδος χρηστών. Το Google Cloud υποστηρίζει Έλεγχο πρόσβασης βάσει χαρακτηριστικών (ABAC) μέσω της χρήσης του IAM Conditions[76]. Το ABAC είναι ένα μοντέλο ελέγχου πρόσβασης που χρησιμοποιεί χαρακτηριστικά ή ιδιότητες των υποκειμένων, των αντικειμένων και του περιβάλλοντος για τη λήψη

[69] https://docs.aws.amazon.com/IAM/latest/UserGuide/introduction.html
[71] https://learn.microsoft.com/en-us/azure/role-based-access-control/overview
[72] https://learn.microsoft.com/en-us/azure/active-directory/fundamentals/active-directory-whatis
[73] https://learn.microsoft.com/en-us/azure/governance/policy/overview
[75] https://cloud.google.com/iam/docs/overview
[76] https://cloud.google.com/iam/docs/conditions-overview

	με τον πόρο ή σε άλλους λογαριασμούς. Η AWS υποστηρίζει Έλεγχο πρόσβασης βάσει χαρακτηριστικών (ABAC)[70]. Στο AWS, αυτά τα χαρακτηριστικά ονομάζονται ετικέτες. Ο καταναλωτής μπορεί να επισυνάψει ετικέτες σε πόρους IAM, συμπεριλαμβανομένων των οντοτήτων IAM (χρήστες ή ρόλους) και σε πόρους AWS. Μπορεί να δημιουργήσει μια ενιαία πολιτική ABAC ή ένα μικρό σύνολο πολιτικών για τους εντολείς IAM. Αυτές οι πολιτικές ABAC μπορούν να σχεδιαστούν ώστε να επιτρέπουν λειτουργίες όταν η ετικέτα του ιδιοκτήτη ταιριάζει με την ετικέτα του πόρου.	διαφάνεια σε όλους τους χρήστες και τις υπηρεσίες για το ποιοι κανόνες πολιτικής έχουν οριστεί στο περιβάλλον τους. Το Azure ABAC[74] βασίζεται στο Azure RBAC προσθέτοντας συνθήκες ανάθεσης ρόλων με βάση χαρακτηριστικά στο πλαίσιο συγκεκριμένων ενεργειών. Μια συνθήκη ανάθεσης ρόλου είναι ένας πρόσθετος έλεγχος που μπορεί να προστεθεί προαιρετικά στην ανάθεση ρόλου για να παρέχεται πιο λεπτομερής έλεγχος πρόσβασης. Μια συνθήκη φιλτράρει τα δικαιώματα που χορηγούνται ως μέρος του ορισμού ρόλου και της ανάθεσης ρόλου. Ωστόσο δεν παρέχεται η ρητή άρνηση πρόσβασης σε συγκεκριμένους πόρους χρησιμοποιώντας μόνο συνθήκες.	αποφάσεων ελέγχου πρόσβασης. Με το IAM Conditions στο Google Cloud, δίνεται η δυνατότητα ορισμού προσαρμοσμένων συνθηκών με βάση διάφορα χαρακτηριστικά. Αυτές οι συνθήκες μπορούν να χρησιμοποιηθούν για την αξιολόγηση παραγόντων περιβάλλοντος, όπως ο χρόνος, η διεύθυνση IP, ο τύπος συσκευής, η γεωγραφική θέση κ.α.
Πόσο ασφαλές είναι το σύστημα ελέγχου ταυτότητας (ποιά είναι τα πρότυπα που χρησιμοποιούνται);	Το AWS υποστηρίζει κοινώς χρησιμοποιούμενα πρότυπα ανοιχτής ταυτότητας, όπως το Security Assertion Markup Language 2.0 (SAML 2.0)[77], το Open ID Connect (OIDC)[78], το LDAPS (Lightweight Directory Access Protocol over Secure Sockets Layer (SSL)/Transport Layer Security (TLS))[79], το Mutual TLS[80],το Kerberos v5[81] και το OAuth 2.0[82].	Το Microsoft Azure υποστηρίζει προτυπα ανοιχτής ταυτότητας όπως το Security Assertion Markup Language 2.0 (SAML 2.0), το Open ID Connect (OIDC),το LDAP (Lightweight Directory Access Protocol), το RADIUS (Remote Authentication Dial-In User Service)[83], το Secure Shell (SSH)[84], το Kerberos[85] και το OAuth 2.0.	Το Google AppEngine χρησιμοποιεί το πρότυπο ανοιχτής ταυτότητας Security Assertion Markup Language 2.0 (SAML 2.0), το Open ID Connect (OIDC),το LDAP (Lightweight Directory Access Protocol)[86] και το OAuth 2.0.

[70] https://docs.aws.amazon.com/IAM/latest/UserGuide/introduction_attribute-based-access-control.html
[74] https://learn.microsoft.com/en-us/azure/role-based-access-control/conditions-overview
[77] http://docs.oasis-open.org/security/saml/Post2.0/sstc-saml-tech-overview-2.0.html
[78] https://openid.net/developers/how-connect-works/
[79] https://docs.aws.amazon.com/directoryservice/latest/admin-guide/ms_ad_ldap.html
[80] https://aws.amazon.com/blogs/security/approaches-for-authenticating-external-applications-in-a-machine-to-machine-scenario/
[81] https://datatracker.ietf.org/doc/html/rfc4120
[82] https://oauth.net/2/
[83] https://learn.microsoft.com/en-us/azure/active-directory/fundamentals/auth-radius
[84] https://learn.microsoft.com/en-us/azure/active-directory/fundamentals/auth-ssh
[85] https://learn.microsoft.com/en-us/azure/active-directory/app-proxy/application-proxy-configure-single-sign-on-with-kcd
[86] https://ldap.com/

ποιοι μηχανισμοί ελέγχου ταυτότητας χρησιμοποιούν ται;	Η AWS υποστηρίζει έλεγχο ταυτότητας πολλαπλών παραγόντων (MFA)[87], ο οποίος προσθέτει ένα επιπλέον επίπεδο ασφάλειας στον έλεγχο ταυτότητας του χρήστη, απαιτώντας από τους χρήστες να παρέχουν μια δεύτερη μορφή επαλήθευσης (π.χ. έναν κωδικό πρόσβασης μίας χρήσης από μια εικονική συσκευή MFA). Η AWS παρέχει την υπηρεσία AWS Security Token Service (STS)[88]. Η STS επιτρέπει την έκδοση προσωρινών διαπιστευτηρίων ασφαλείας σε χρήστες ή εφαρμογές. Τα προσωρινά διαπιστευτήρια έχουν περιορισμένη διάρκεια και είναι χρήσιμα σε σενάρια όπου οι χρήστες ή οι εφαρμογές χρειάζονται προσωρινή πρόσβαση σε πόρους του AWS χωρίς να απαιτούν μακροπρόθεσμα κλειδιά πρόσβασης. Η AWS υποστηρίζει την ομοσπονδιοποίηση ταυτότητας ιστού (Web Identity Federation)[89], επιτρέποντας στους χρήστες να πιστοποιούνται χρησιμοποιώντας διαπιστευτήρια από διάφορους παρόχους ταυτότητας, όπως η Google, το Facebook ή η ίδια η Amazon. Αυτό επιτρέπει την χορήγηση πρόσβασης σε πόρους του AWS με βάση εξωτερικά συστήματα ταυτότητας. Η AWS Single Sign-On (SSO)[90] απλοποιεί τη διαχείριση της πρόσβασης των χρηστών σε πολλαπλούς λογαριασμούς AWS και επιχειρηματικές εφαρμογές. Επιτρέπει στους χρήστες να συνδεθούν μία φορά και να έχουν πρόσβαση σε πολλούς λογαριασμούς και εφαρμογές AWS	Η Microsoft Azure υποστηρίζει έλεγχο ταυτότητας πολλαπλών παραγόντων (MFA)[91], ο οποίος προσθέτει ένα επιπλέον επίπεδο ασφάλειας στον έλεγχο ταυτότητας των χρηστών, απαιτώντας από τους χρήστες να παρέχουν μια δεύτερη μορφή επαλήθευσης, όπως μια τηλεφωνική κλήση, ένα μήνυμα κειμένου ή μια ειδοποίηση εφαρμογής για κινητά, εκτός από τα κανονικά διαπιστευτήριά τους. Η Microsoft Azure παρέχει την υπηρεσία Azure Conditional Access[92] που υποστηρίζει την πρόσβαση υπό όρους και επιτρέπει τον ορισμό και την επιβολή ελέγχων πρόσβασης βάσει συγκεκριμένων συνθηκών, όπως η τοποθεσία του χρήστη, η υγεία της συσκευής και το επίπεδο κινδύνου. Η Microsoft Azure υποστηρίζει την υπηρεσία Azure Service Principal[93], η οποία παρέχει έναν συγκεκριμένο τύπο ταυτότητας που χρησιμοποιείται από εφαρμογές και υπηρεσίες για τον έλεγχο ταυτότητας στο Azure. Επιτρέπει σε αυτοματοποιημένες διαδικασίες και εφαρμογές να έχουν ασφαλή πρόσβαση στους πόρους του Azure. Η Microsoft Azure υποστηρίζει της	Το Google Cloud υποστηρίζει έλεγχο ταυτότητας πολλαπλών παραγόντων (MFA)[95], ο οποίος είναι ένα πρόσθετο επίπεδο ασφάλειας που απαιτεί από τους χρήστες να παρέχουν δύο ή περισσότερες μορφές ταυτοποίησης πριν αποκτήσουν πρόσβαση στους λογαριασμούς ή τους πόρους τους, όπως κωδικούς πρόσβασης μίας χρήσης με βάση το χρόνο (TOTP) και ειδοποιήσεις push στις κινητές συσκευές για την έγκριση ή την απόρριψη αιτήματος ελέγχου ταυτότητας. Το Google Cloud υποστηρίζει δυνατότητες Single Sign-On (SSO)[96] το οποίο επιτρέπει στους χρήστες να συνδεθούν μία φορά με τα κύρια διαπιστευτήριά τους και στη συνέχεια να αποκτήσουν πρόσβαση σε πολλαπλές εφαρμογές και υπηρεσίες χωρίς να χρειάζεται να εισάγουν εκ νέου τα διαπιστευτήριά τους για κάθε μία. Το Google Cloud παρέχει την υπηρεσία Service Accounts[97], η οποία παρέχει έναν τρόπο χορήγησης των απαραίτητων δικαιωμάτων σε εφαρμογές χωρίς να απαιτούνται διαπιστευτήρια τελικού χρήστη. Αυτό είναι ιδιαίτερα χρήσιμο σε σενάρια όπου αυτοματοποιημένες διεργασίες ή υπηρεσίες πρέπει να αλληλεπιδρούν με πόρους του GCP προγραμματιστικά. Το Google Cloud προσφέρει την υπηρεσία Identity-Aware

[87] https://docs.aws.amazon.com/IAM/latest/UserGuide/id_credentials_mfa.html
[88] https://docs.aws.amazon.com/STS/latest/APIReference/welcome.html
[89] https://docs.aws.amazon.com/amazondynamodb/latest/developerguide/WIF.html
[90] https://aws.amazon.com/what-is/sso/
[91] https://learn.microsoft.com/en-us/azure/active-directory/authentication/concept-mfa-howitworks
[92] https://learn.microsoft.com/en-us/azure/active-directory/conditional-access/overview
[93] https://learn.microsoft.com/en-us/cli/azure/create-an-azure-service-principal-azure-cli
[95] https://cloud.google.com/identity-platform/docs/web/mfa
[96] https://cloud.google.com/architecture/identity/single-sign-on
[97] https://cloud.google.com/iam/docs/service-account-overview

	χωρίς να χρειάζεται να εισάγουν ξεχωριστά διαπιστευτήρια για τον καθένα.	Διαχειριζόμενες ταυτότητες Azure[94]. Οι Azure Managed Identities είναι αυτόματα διαχειριζόμενες ταυτότητες για πόρους του Azure, όπως εικονικές μηχανές και λειτουργίες του Azure. Επιτρέπουν στις εφαρμογές που εκτελούνται σε αυτούς τους πόρους να πιστοποιούνται με ασφάλεια χωρίς την ανάγκη ρητών διαπιστευτηρίων.	Proxy (IAP)[98], η οποία ελέγχει τα αιτήματα πρόσβασης που αποστέλλονται σε διαδικτυακές εφαρμογές που εκτελούνται στο GCP, πιστοποιεί τον χρήστη που κάνει το αίτημα χρησιμοποιώντας την υπηρεσία Google Identity Service και αφήνει τα αιτήματα να περάσουν μόνο αν προέρχονται από χρήστη που έχει εξουσιοδοτηθεί να έχει πρόσβαση στην εφαρμογή.

Παρατηρούμε ότι και οι τρεις πάροχοι χρησιμοποιούν έλεγχο πρόσβασης βάσει ρόλων και βάσει χαρακτηριστικών όπως επίσης προσφέρουν και την δυνατότητα δημιουργίας πολιτικών ελέγχου πρόσβασης ανάλογα με τις ανάγκες του καταναλωτή. Παρατηρούμε, επίσης, ότι χρησιμοποιούν ενημερωμένα και σύγχρονα πρότυπα ελέγχου ταυτότητας. Βέβαια, σε αυτή την περίπτωση, οι πάροχοι AWS & Azure φαίνεται να υπερτερούν λίγο ως προς τον Google Cloud. Οι τρεις πάροχοι παρέχουν έλεγχο ταυτότητας πολλαπλών παραγόντων και άλλους μηχανισμούς ελέγχου ταυτότητας. Κάποιοι από αυτούς τους μηχανισμούς είναι κοινοί ή όμοιοι και κάποιοι διαφορετικοί Επομένως, μπορούμε να πούμε ότι σε γενικές γραμμές δεν υστερεί κάποιος πάροχος ως προς τον έλεγχο ταυτότητας και πρόσβασης.

5.2.4 Ειδικό υλικό και απομόνωση δεδομένων

Η ιδιότητα πολλαπλής μίσθωσης της υπηρεσίας υπολογιστικού νέφους θέτει τα δεδομένα των καταναλωτών σε κίνδυνο μη εξουσιοδοτημένης πρόσβασης.

Στοχεύοντας περισσότερους πελάτες, το νέο νέφος της Amazon προσέφερε αποκλειστικό υλικό το 2011. Ορισμένοι καταναλωτές υπηρεσιών νέφους τείνουν να ζητούν να έχουν τα δεδομένα τους σε ειδικά/φυσικά/αποκλειστικά μηχανήματα επειδή πιστεύουν ότι είναι πιο ασφαλές να απομονώνουν τα δεδομένα τους από τα δεδομένα και τις συναλλαγές άλλων. Επιπλέον ένας άλλος λόγος που προτιμαται η χρήση αποκλειστικών μηχανημάτων είναι αποφυγή παρεμβολών φόρτων εργασίας σε διαφορετικούς καταναλωτές. Εφόσον γίνεται υπερ-προμήθεια (over-provisioning) των πόρων και μη κατάλληλη διανομή των πόρων ενός φυσικού μηχανήματος σε εικονικές μηχανές, τότε πολλές φορές γίνονται παρεμβολές μεταξύ των φόρτων εργασίας σε διαφορετικές εικονικές μηχανές διαφορετικών καταναλωτών με αποτέλεσμα να μην επιδεικνύεται η κατάλληλη απόδοση (& αξιοπιστία). Για αυτό

[94] https://learn.microsoft.com/en-us/azure/active-directory/managed-identities-azure-resources/overview
[98] https://codelabs.developers.google.com/secure-serverless-application-with-identity-aware-proxy#0

τον λόγο, ένα αποκλειστικό μηχάνημα θα έδινε περισσότερο έλεγχο στον καταναλωτή ώστε να εγκαταστήσει εκεί τους σωστούς φόρτους εργασίας χωρίς ιδιαίτερες παρεμβολές, επιτυγχάνοντας σχεδόν σταθερά επίπεδα απόδοσης.

Τα αποκλειστικά μηχανήματα αντιμετωπίζουν τα εξής ζητήματα ασφάλειας. Οι κανονισμοί ορισμένων οργανισμών επιβάλλουν ότι τα δεδομένα πρέπει να βρίσκονται σε ένα απομονωμένο μηχάνημα και για αυτόν τον λόγο απαιτείται από τον πάροχο η κατάλληλη απομόνωση των μηχανημάτων αυτων. Επίσης, το αποκλειστικό φυσικό μηχάνημα επιδεικνύει περισσότερη ασφάλεια για τα δεδομένα και τις συνδέσεις.

Ένας καταναλωτής θα πρέπει να ρωτήσει τον CSP:

1) εάν προσφέρει αποκλειστικά μηχανήματα που χρησιμοποιούνται από έναν μόνο καταναλωτή. [28]

Πίνακας 12. Σύγκριση παροχής απομονωμένου υλικού των πάροχων υπολογιστικού νέφους AWS, Microsoft Azure και Google Cloud. [58] [59] [60]

Ανησυχία Καταναλωτή	Amazon Web Services (AWS)	Microsoft Azure	Google Cloud Platform (GCP)
Προσφέρεται αποκλειστικό υλικό αφιερωμένο σε έναν μόνο καταναλωτή	Το AWS (Amazon Web Services) προσφέρει επιλογές για αποκλειστικό υλικό και απομόνωση δεδομένων όπως: ● Dedicated Instances[99] τα οποία είναι instances (δηλ. στιγμιότυπα εικονικών μηχανών) που λειτουργούν σε αποκλειστικό υλικό και είναι απομονωμένα από τα instances που εκτελούνται σε κοινόχρηστο υλικό. ● Dedicated Hosts[100], οι οποίοι είναι φυσικοί διακομιστές που προορίζονται αποκλειστικά για χρήση από έναν καταναλωτή. Επιτρέπουν τον πλήρη έλεγχο τόσο της	Το Microsoft Azure προσφέρει επιλογές για αποκλειστικό υλικό και απομόνωση δεδομένων όπως: ● Azure Dedicated Hosts[103], οι οποίοι είναι φυσικοί διακομιστές αφιερωμένοι αποκλειστικά στον καταναλωτή και προσφέρουν πλήρη έλεγχο του υλικού και τοποθέτηση των εικονικών μηχανών σε αυτό ώστε να είναι απομονωμένες. ● Azure Private Link[104] επιτρέπει την ασφαλή πρόσβαση στις υπηρεσίες Azure μέσω	Το Google Cloud προσφέρει επιλογές για αποκλειστικό υλικό και απομόνωση δεδομένων όπως: ● Dedicated VM Instances[106], οι οποίες είναι εικονικές μηχανές που εκτελούνται σε αποκλειστικούς φυσικούς κεντρικούς υπολογιστές. Παρέχει αποκλειστική πρόσβαση στο υποκείμενο υλικό, διασφαλίζοντας ότι οι φόρτοι εργασίας είναι απομονωμένοι από τους φόρτους εργασίας άλλων καταναλωτών.

[99] https://aws.amazon.com/ec2/pricing/dedicated-instances/
[100] https://aws.amazon.com/ec2/dedicated-hosts/
[103] https://learn.microsoft.com/en-us/azure/virtual-machines/dedicated-hosts
[104] https://learn.microsoft.com/en-us/azure/private-link/private-link-overview
[106] https://cloud.google.com/compute/docs/nodes/sole-tenant-nodes

	τοποθέτησης των διακομιστών όσο και τον καθορισμό των χαρακτηριστικών τους. ● Virtual Private Cloud[101], το οποίο είναι απομονωμένο εικονικό δίκτυο εντός του νέφους AWS που επιτρέπει την απομόνωση των πόρων με τον έλεγχο της εισερχόμενης και εξερχόμενης κυκλοφορίας του δικτύου. ● AWS PrivateLink[102]: παρέχει την δυνατότητα ιδιωτικής πρόσβασης στις υπηρεσίες του AWS ώστε να μπορεί ο καταναλωτής να συνδέεται με ασφάλεια στις υπηρεσίες AWS χωρίς να διασχίζει το διαδίκτυο.	μιας ιδιωτικής σύνδεσης δικτύου, παρέχοντας απομόνωση δεδομένων από το διαδίκτυο. ● Εικονικά δίκτυα (VNET)[105] που επιτρέπουν την δημιουργία απομονωμένων εικονικών δικτύων εντός του Azure με τον ορισμό εύρους διευθύνσεων IP του VNET, την δημιουργία υποδικτύων και τον έλεγχο της κυκλοφορίας του δικτύου χρησιμοποιώντας ομάδες ασφαλείας δικτύου (NSG) και τερματικά σημεία υπηρεσιών εικονικού δικτύου.	● Google Virtual Private Cloud (VPC)[107], το οποίο επιτρέπει την δημιουργία απομονωμένων εικονικών δικτύων εντός του περιβάλλοντος του Google Cloud. Επιτρέπει τον ορισμό εύρους διευθύνσεων IP του VPC, την δημιουργία υποδικτύων και τον έλεγχο της κυκλοφορίας του δικτύου χρησιμοποιώντας κανόνες τείχους προστασίας και ετικέτες δικτύου. ● Google Private Service Connect[108], το οποίο επιτρέπει την ιδιωτική πρόσβαση στις υπηρεσίες του Google Cloud χρησιμοποιώντας αποκλειστικές συνδέσεις χωρίς να χρειάζεται ο καταναλωτής να διασχίζει το διαδίκτυο.

Παρατηρούμε ότι και οι τρεις πάροχοι παρέχουν ανταγωνιστικές επιλογές για αποκλειστικό υλικό και απομόνωση δεδομένων, ωστόσο υπάρχει μια σημαντική διαφορά καθώς η Amazon AWS προσφέρει αποκλειστικά στιγμιότυπα εικονικών μηχανών και αποκλειστικούς φυσικούς διακομιστές ενώ η Microsoft Azure προσφέρει μόνο αποκλειστικούς φυσικούς διακομιστές και το Google Cloud προσφέρει μόνο αποκλειστικά στιγμιότυπα εικονικών μηχανών.

[101] https://docs.aws.amazon.com/vpc/latest/userguide/what-is-amazon-vpc.html
[102] https://docs.aws.amazon.com/vpc/latest/userguide/endpoint-services-overview.html
[105] https://learn.microsoft.com/en-us/azure/virtual-network/virtual-networks-overview
[107] https://cloud.google.com/vpc/docs/overview
[108] https://cloud.google.com/vpc/docs/private-service-connect

5.2.5 Παρακολούθηση

Είναι απαραίτητο μετά την ανάπτυξη όλων των χαρακτηριστικών ασφαλείας, να υπάρχει ένας μηχανισμός παρακολούθησης ώστε να τραβήξετε τη σκανδάλη μόλις παρατηρήσετε μια ανεπιθύμητη ενέργεια. Οι καταναλωτές μπορεί να θέλουν να μάθουν την τρέχουσα κατάσταση ασφαλείας των συστημάτων τους στο νέφος. Για να αξιολογήσουν αυτό το χαρακτηριστικό, οι καταναλωτές μπορεί να θέλουν να ρωτήσουν τους παρόχους υπηρεσιών τα εξής:

1. Χρησιμοποιούνται εργαλεία παρακολούθησης για τον εντοπισμό κινδύνων και πως λειτουργούν;

[28]

Πίνακας 13. Σύγκριση μεθόδων παρακολούθησης πόρων των παρόχων υπολογιστικού νέφους AWS, Microsoft Azure και Google Cloud [61] [62] [63]

Ανησυχία Καταναλωτή	Amazon Web Services (AWS)	Microsoft Azure	Google Cloud Platform (GCP)
Χρησιμοποιούνται εργαλεία παρακολούθησης για τον εντοπισμό κινδύνων και πως λειτουργούν;	Η AWS (Amazon Web Services) χρησιμοποιεί διάφορα εργαλεία και υπηρεσίες παρακολούθησης για τον εντοπισμό κινδύνων και τη διασφάλιση της ασφάλειας και της συμμόρφωσης της υποδομής και των υπηρεσιών της όπως: ● AWS CloudTrail[109] καταγράφει τη δραστηριότητα και τα συμβάντα API στην υποδομή AWS. Παρέχει λεπτομερή αρχεία καταγραφής των ενεργειών που πραγματοποιούνται από χρήστες, υπηρεσίες και πόρους, επιτρέποντάς την παρακολούθηση και τον έλεγχο του περιβάλλοντος AWS. Τα αρχεία καταγραφής του CloudTrail μπορούν να χρησιμοποιηθούν για τον	Η Microsoft Azure χρησιμοποιεί διάφορα εργαλεία και υπηρεσίες παρακολούθησης για τον εντοπισμό κινδύνων και τη διασφάλιση της ασφάλειας και της συμμόρφωσης της υποδομής και των υπηρεσιών της όπως: ● Azure Security Center[115] παρέχει μια ενοποιημένη προβολή της κατάστασης ασφαλείας των πόρων. Παρακολουθεί συνεχώς τους πόρους και παρέχει συστάσεις για τη βελτίωση της ασφάλειας με βάση τις βέλτιστες πρακτικές ασφάλειας. Αναλύει τα αρχεία καταγραφής ασφαλείας,	Το Google Cloud χρησιμοποιεί διάφορα εργαλεία και υπηρεσίες παρακολούθησης για τον εντοπισμό κινδύνων και τη διασφάλιση της ασφάλειας και της συμμόρφωσης της υποδομής και των υπηρεσιών του όπως: ● Google Cloud Monitoring[120] συλλέγει και παρακολουθεί μετρήσεις, αρχεία καταγραφής και συμβάντα από τους πόρους του Google Cloud. Παρέχει ορατότητα σε πραγματικό χρόνο σχετικά με την απόδοση, την υγεία και τη διαθεσιμότητα των εφαρμογών και

[109] https://docs.aws.amazon.com/awscloudtrail/latest/userguide/cloudtrail-user-guide.html
[115] https://techcommunity.microsoft.com/t5/itops-talk-blog/what-s-the-difference-between-azure-security-center-azure/ba-p/2155188
[120] https://cloud.google.com/monitoring/docs

	εντοπισμό κινδύνων ασφαλείας, την αντιμετώπιση λειτουργικών προβλημάτων και την εκπλήρωση των απαιτήσεων συμμόρφωσης. • AWS Config[110] παρέχει λεπτομερή απογραφή των πόρων AWS και των διαμορφώσεών τους με την πάροδο του χρόνου. Παρακολουθεί τις αλλαγές στις διαμορφώσεις και επιτρέπει την αξιολόγηση της συμμόρφωσης με τις επιθυμητές διαμορφώσεις. Με τη συνεχή παρακολούθηση των διαμορφώσεων των πόρων, το AWS Config βοηθά στον εντοπισμό τυχόν μη εξουσιοδοτημένων αλλαγών ή πιθανών κινδύνων ασφαλείας.\ • AWS CloudWatch[111] είναι μια υπηρεσία παρακολούθησης και παρατηρησιμότητας που συλλέγει και παρακολουθεί μετρήσεις, αρχεία καταγραφής και συμβάντα από πόρους AWS. Δίνει τη δυνατότητα απόκτησης πληροφοριών σχετικά με	πραγματοποιεί ανάλυση πληροφοριών σχετικά με απειλές και εντοπίζει πιθανές ευπάθειες και κινδύνους σε όλο το περιβάλλον Azure • Azure Monitor[116] είναι μια ολοκληρωμένη λύση παρακολούθησης που συλλέγει και αναλύει δεδομένα από διάφορες υπηρεσίες Azure. Δίνει τη δυνατότητα παρακολούθησης της απόδοσης και της διαθεσιμότητας των εφαρμογών, εντοπίζει ανωμαλίες και παρέχει πληροφορίες σχετικά με την υγεία της υποδομής. Μπορεί να ρυθμιστεί ώστε να παράγει ειδοποιήσεις βάσει συγκεκριμένων συνθηκών, βοηθώντας στον εντοπισμό πιθανών κινδύνων ή προβλημάτων. • Azure Sentinel[117] είναι μια cloud-native υπηρεσία διαχείρισης πληροφοριών ασφαλείας και συμβάντων (SIEM).	της υποδομής. Επιτρέπει την ρύθμιση προσαρμοσμένων ειδοποιήσεων και την δημιουργία πινάκων ελέγχου για την παρακολούθηση συγκεκριμένων μετρήσεων και τον εντοπισμό πιθανών κινδύνων ή προβλημάτων. • Google Cloud Logging[121] που επιτρέπει την συγκέντρωση και την ανάλυση αρχείων καταγραφής από διάφορες πηγές, όπως εικονικές μηχανές, δοχεία (containers) και υπηρεσίες Google Cloud, καθώς και τον εντοπισμό συμβάντων ασφαλείας, ανωμαλιών και πιθανών κινδύνων. • Google Cloud Security Command Center[122] παρέχει μια ενιαία προβολή της ασφάλειας και της συμμόρφωσης σε όλους τους πόρους στο Google Cloud. Βοηθά στον εντοπισμό τρωτών σημείων ασφαλείας,

[110] https://docs.aws.amazon.com/config/latest/developerguide/WhatIsConfig.html
[111] https://docs.aws.amazon.com/AmazonCloudWatch/latest/monitoring/WhatIsCloudWatch.html
[116] https://learn.microsoft.com/en-us/azure/azure-monitor/overview
[117] https://learn.microsoft.com/en-us/azure/sentinel/overview
[121] https://cloud.google.com/logging/docs/overview
[122] https://cloud.google.com/security-command-center/docs/concepts-security-command-center-overview

	την απόδοση και τη λειτουργική υγεία των εφαρμογών και της υποδομής. Οι συναγερμοί του CloudWatch μπορούν να ρυθμιστούν ώστε να ειδοποιούν για συγκεκριμένα κατώτατα όρια μετρήσεων, βοηθώντας στον εντοπισμό πιθανών κινδύνων ή προβλημάτων. ● AWS GuardDuty[112] είναι μια υπηρεσία ανίχνευσης απειλών που παρακολουθεί συνεχώς για κακόβουλη δραστηριότητα και μη εξουσιοδοτημένη συμπεριφορά στους λογαριασμούς και τους φόρτους εργασίας στο AWS. Χρησιμοποιεί αλγορίθμους μηχανικής μάθησης και πληροφορίες απειλών για την ανάλυση δεδομένων καταγραφής και κίνησης δικτύου, εντοπίζοντας πιθανές απειλές και κινδύνους για την ασφάλεια. ● Amazon Inspector[113] είναι μια αυτοματοποιημένη υπηρεσία αξιολόγησης της ασφάλειας που βοηθά στον εντοπισμό ευπαθειών ασφαλείας και αποκλίσεων από τις	Παρέχει έξυπνες αναλύσεις ασφαλείας και ανίχνευση απειλών στους πόρους Azure. Συλλέγει δεδομένα ασφαλείας από διάφορες πηγές, όπως το Azure Monitor, το Azure Security Center και εξωτερικά συστήματα, και εφαρμόζει προηγμένες αναλύσεις και μηχανική μάθηση για τον εντοπισμό και την αντιμετώπιση απειλών ασφαλείας. ● Azure Advisor[118] είναι μια υπηρεσία που παρέχει συστάσεις για τη βελτιστοποίηση των πόρων Azure σε σχέση με το κόστος, τις επιδόσεις, την ασφάλεια και την αξιοπιστία. Αναλύει τις διαμορφώσεις των πόρων, τα μοτίβα χρήσης και τις βέλτιστες πρακτικές για την παροχή συμβουλών που μπορούν να αναληφθούν και τον μετριασμό των κινδύνων	λανθασμένων ρυθμίσεων και πιθανών κινδύνων. ● Google Cloud Audit Logging Google Cloud[123] καταγράφει τις διοικητικές δραστηριότητες και τις κλήσεις API που πραγματοποιούνται στους πόρους Google Cloud. Δημιουργεί αρχεία καταγραφής ελέγχου που μπορούν να χρησιμοποιηθούν για ανάλυση ασφάλειας, παρακολούθηση συμμόρφωσης και εγκληματολογικές έρευνες. ● Google Cloud Security Scanner[124] είναι μια υπηρεσία σάρωσης ασφάλειας εφαρμογών ιστού. Σαρώνει αυτόματα τις εφαρμογές ιστού σας για κοινές ευπάθειες και παράγει αναφορές με συστάσεις για την αντιμετώπιση τυχόν εντοπισμένων κινδύνων. ● Google Cloud DLP[125] προσφέρει εργαλεία για τον εντοπισμό, την ταξινόμηση και την

[112] https://docs.aws.amazon.com/guardduty/latest/ug/what-is-guardduty.html
[113] https://docs.aws.amazon.com/inspector/latest/user/what-is-inspector.html
[118] https://learn.microsoft.com/en-us/azure/advisor/advisor-overview
[123] https://cloud.google.com/logging/docs/audit
[124] https://cloud.google.com/security-command-center/docs/concepts-web-security-scanner-overview
[125] https://cloud.google.com/dlp

	βέλτιστες πρακτικές ασφαλείας στους πόρους AWS. Εκτελεί αξιολογήσεις ασφαλείας αναλύοντας τα επίπεδα δικτύου, λειτουργικού συστήματος και εφαρμογών των πόρων, παρέχοντας ευρήματα και συστάσεις για την αντιμετώπιση τυχόν εντοπισμένων κινδύνων.\ ● AWS Trusted Advisor [114]είναι μια υπηρεσία που παρέχει συστάσεις για τη βελτιστοποίηση της υποδομής AWS. Αναλύει το περιβάλλον AWS σε σχέση με τις βέλτιστες πρακτικές ασφάλειας και παρέχει αξιοποιήσιμες συμβουλές για τον μετριασμό των κινδύνων και τη βελτίωση της αποδοτικότητας.	● Azure Log Analytics[119] συλλέγει και αναλύει δεδομένα καταγραφής από διάφορες πηγές, συμπεριλαμβανομένων των υπηρεσιών Azure και των προσαρμοσμένων εφαρμογών. Δίνει τη δυνατότητα συγκέντρωσης και αναζήτησης δεδομένων καταγραφής, εκτέλεσης προηγμένων αναλύσεων και απόκτησης πληροφοριών σχετικά με λειτουργικά ζητήματα και ζητήματα ασφάλειας.	προστασία ευαίσθητων δεδομένων. Βοηθά στον εντοπισμό και στην κατανόηση των τύπων των ευαίσθητων δεδομένων που είναι αποθηκευμένα στο περιβάλλον Google Cloud, όπως πληροφορίες προσωπικής ταυτοποίησης (PII) και παρέχει ανάλυση κινδύνου στους πόρους στο Google Cloud.

Παρατηρούμε ότι και οι τρεις πάροχοι παρέχουν μια μεγάλη ποικιλία από ανταγωνιστικά εργαλεία παρακολούθησης για τον εντοπισμό κινδύνων. Μπορούμε να πούμε ότι δεν υστερεί κάποιος πάροχος ως προς αυτό το χαρακτηριστικό ασφαλείας.

5.2.6 Πρότυπα και Πιστοποιήσεις Ασφαλείας

Τα πρότυπα και οι πιστοποιήσεις ασφαλείας που υποστηρίζει και κατέχει, αντίστοιχα, ο κάθε πάροχος επιβεβαιώνουν τους καταναλωτές πως ο πάροχος αυτός ακολουθεί τα πρότυπα και τις βέλτιστες πρακτικές ασφαλείας. Επομένως, οι καταναλωτές μπορεί να χρειαστεί να ρωτήσουν τους παρόχους υπολογιστικού νέφους εάν η υπηρεσία τους είναι πιστοποιημένη ή όχι ως προς την ασφάλειά της. [28]

[114] https://docs.aws.amazon.com/awssupport/latest/user/trusted-advisor.html
[119] https://learn.microsoft.com/en-us/azure/azure-monitor/logs/log-analytics-overview

Πίνακας 14. Σύγκριση προτύπων και πιστοποιήσεων που διαθέτουν οι πάροχοι υπολογιστικού νέφους AWS, Microsoft Azure, Google Cloud [64] [65] [66]

Ανησυχία Καταναλωτή	Amazon Web Services (AWS)	Microsoft Azure	Google Cloud Platform (GCP)
Είναι πιστοποιημένο το περιβάλλον νέφους που προσφέρεται;	Τα υπολογιστικά περιβάλλοντα AWS ελέγχονται συνεχώς, με πιστοποιήσεις από φορείς διαπίστευσης σε διάφορες γεωγραφικές περιοχές και κλάδους, συμπεριλαμβανομένων των ● SOC 1/SSAE 16/ISAE 3402[126] (πρώην SAS 70), SOC 2[127], SOC 3[128] για την οργάνωση υπηρεσιών και τον έλεγχο προτύπων ασφάλειας. ● ISO 9001 / ISO 27001[129] σχετικά με τα Πρότυπα Διαχείρισης Ασφάλειας Πληροφοριών. ● ISO/IEC 27017[130] σχετικά με τον Κώδικα Πρακτικής για Ελέγχους Ασφάλειας Πληροφοριών ● ISO/IEC 27018[131] σχετικά με τον	Το Microsoft Azure κατέχει τις παρακάτω πιστοποιήσεις ● Βεβαίωση CSA STAR για τον έλεγχο του Cloud Security Alliance της στάσης ασφαλείας ενός παρόχου cloud. ● ISO/IEC 20000-1:2011[140] σχετικά με τη Διαχείριση Υπηρεσιών Πληροφορικής. ● ISO 22301[141]. Πρότυπο διαχείρισης επιχειρησιακής συνέχειας του Διεθνούς Οργανισμού Τυποποίησης (ISO). ● ISO/IEC 27001 σχετικά με τα Πρότυπα Διαχείρισης Ασφάλειας Πληροφοριών. ● ISO/IEC 27017 σχετικά με τον Κώδικα Πρακτικής για Ελέγχους Ασφάλειας Πληροφοριών. ● ISO/IEC 27018 σχετικά με τον κώδικα πρακτικών για την προστασία προσωπικών	Το Google Cloud έχει τις παρακάτω πιστοποιήσεις ● ISO/IEC 27018: εστιάζει στους ελέγχους απορρήτου και ασφάλειας για παρόχους υπηρεσιών δημόσιου cloud που επεξεργάζονται πληροφορίες προσωπικής ταυτοποίησης (PII). ● Το ISO/IEC 27001 παρέχει τις απαιτήσεις για ένα σύστημα διαχείρισης ασφάλειας πληροφοριών (ISMS) ● Το ISO/IEC 27017:2015 παρέχει οδηγίες για ελέγχους ασφάλειας πληροφοριών που ισχύουν για την παροχή και τη χρήση υπηρεσιών cloud. ● CSA STAR Πρόγραμμα Μητρώου Ασφάλειας, Εμπιστοσύνης και

126 https://ssae-16.com/soc-1/
127 https://ssae-16.com/soc-2/
128 https://ssae-16.com/soc-3/
129 https://www.iso.org/standard/27001
130 https://www.iso.org/standard/43757.html
131 https://www.iso.org/standard/76559.html
140 https://www.iso.org/standard/51986.html
141 https://www.iso.org/standard/75106.html

	κώδικα πρακτικών για την προστασία προσωπικών δεδομένων στο νέφος. • DoD[132] σχετικά με τις πολιτικές και διαδικασίες που διέπουν και ρυθμίζουν τις αμυντικές δραστηριότητες. • CSA STAR[133] Πρόγραμμα Μητρώου Ασφάλειας, Εμπιστοσύνης και Διασφάλισης της CSA. • FedRAMP[134]: τυποποιημένη προσέγγιση για την αξιολόγηση της ασφάλειας, την εξουσιοδότηση και τη συνεχή παρακολούθηση για προϊόντα και υπηρεσίες νέφους. • PCI DSS Επίπεδο 1.i[135] σχετικά με την προστασία δεδομένων. • Όλες οι υπηρεσίες AWS μπορούν να χρησιμοποιηθούν σε συμμόρφωση με τον Γενικό κανονισμό προστασίας	δεδομένων στο νέφος. • SOC 1, 2, και 3 για την οργάνωση υπηρεσιών και τον έλεγχο προτύπων ασφάλειας. • WCAG 2.0[142]. - οδηγίες προσβασιμότητας περιεχομένου Ιστού 2.0. • GDPR για την προστασία των προσωπικών δεδομένων των χρηστών	Διασφάλισης της CSA. • SOC 1, 2, και 3 για την οργάνωση υπηρεσιών και τον έλεγχο προτύπων ασφάλειας. • Το ISO/IEC 27018 εστιάζει στους ελέγχους απορρήτου και ασφάλειας για παρόχους υπηρεσιών δημόσιου cloud που επεξεργάζονται πληροφορίες προσωπικής ταυτοποίησης (PII). • PCI DSS είναι ένα σύνολο κατευθυντήριων γραμμών για την ασφάλεια δικτύου και τις βέλτιστες επιχειρηματικές πρακτικές που εγκρίθηκαν από το Συμβούλιο Προτύπων Ασφαλείας PCI για τη θέσπιση ενός «ελάχιστου προτύπου ασφαλείας» για την προστασία των στοιχείων της κάρτας πληρωμής των πελατών. • GDPR για την προστασία των προσωπικών δεδομένων των

[132] https://open.defense.gov/Regulatory-Program/
[133] https://cloudsecurityalliance.org/star/
[134] https://www.fedramp.gov/
[135] https://www.pcisecuritystandards.org/standards/
[142] https://www.w3.org/TR/WCAG20/

	δεδομένων (GDPR)[136]. • FIPS 140-2[137] είναι ένα σύνολο κατευθυντήριων γραμμών το οποίο προσδιορίζει τις απαιτήσεις ασφαλείας που πρέπει να ικανοποιεί μια κρυπτογραφική ενότητα, παρέχοντας τέσσερα αυξανόμενα ποιοτικά επίπεδα που προορίζονται να καλύψουν ένα ευρύ φάσμα πιθανών εφαρμογών και περιβαλλόντων. • NIST 800-171[138] σχετικά με την προστασία ελεγχόμενων μη διαβαθμισμένων πληροφοριών σε μη ομοσπονδιακά συστήματα και οργανισμούς • FISMA [139] ομοσπονδιακός νόμος των Ηνωμένων Πολιτειών που ψηφίστηκε το 2002 και κατέστησε απαίτηση για τις ομοσπονδιακές υπηρεσίες να αναπτύσσουν, να τεκμηριώνουν και να εφαρμόζουν ένα		χρηστών.

[136] https://gdpr-info.eu/
[137] https://csrc.nist.gov/pubs/fips/140-2/upd2/final
[138] https://csrc.nist.gov/pubs/sp/800/171/r2/upd1/final
[139] https://www.cisa.gov/topics/cyber-threats-and-advisories/federal-information-security-modernization-act

	πρόγραμμα ασφάλειας και προστασίας πληροφοριών.		

Παρατηρούμε ότι και οι τρεις πάροχοι διαθέτουν μια μεγάλη ποικιλία προτύπων και πιστοποιήσεων ως προς την ασφάλεια. Πολλά από αυτά τα πρότυπα και πιστοποιήσεις, ιδιαίτερα τα πιο σημαντικά, υποστηρίζονται και από τους τρεις παρόχους. Αλλά υπάρχουν ορισμένες διαφοροποιήσεις. Ειδικότερα, μόνο ο Amazon AWS φαίνεται να υποστηρίζει τα DoD, FIPS 140-2, NIST 800-171, FedRAMP & FISMA. Από την άλλη, μόνο ο Microsoft Azure υποστηρίζει τα ISO/IEC 20000-1, ISO 22301 & WCAG 2.0. Συνεπώς, μπορούμε να πούμε πως οι Amazon AWS και Microsoft Azure φαίνονται πως υποστηρίζουν μια σχετικά μεγαλύτερη γκάμα προτύπων και πιστοποιήσεων σε σχέση με το Google Cloud.

5.2.7 Data Sanitization & Retrieval

Όταν τερματίζεται μια υπηρεσία cloud, τα δεδομένα του καταναλωτή θα πρέπει να διαγράφονται για λόγους ασφαλείας ώστε να μην υπάρχει κίνδυνος διαρροής. Ωστόσο είναι χρήσιμο να υπάρχει ένα διάστημα κατά το οποίο τα δεδομένα παραμένουν αποθηκευμένα ώστε να δίνεται η δυνατότητα ανάκτησής/επαναφοράς τους εφόσον ο χρήστης επιλέξει να μην τερματίσει τελικά την χρήση του λογαριασμού του.
Ο καταναλωτής θα πρέπει να ενδιαφέρεται για:

1) τι συμβαίνει με τα αντίγραφα των δεδομένων εάν τερματιστεί η υπηρεσία;

[28]

Πίνακας 15. Σύγκριση καθαρισμού και επαναφοράς δεδομένων στους παρόχους υπολογιστικού νέφους AWS, Microsoft Azure και Google Cloud [67] [68] [69]

Ανησυχία Καταναλωτή	Amazon Web Services (AWS)	Microsoft Azure	Google Cloud Platform (GCP)
Τι συμβαίνει με τα αντίγραφα των δεδομένων εάν τερματιστεί η υπηρεσία;	Η AWS διατηρεί τα δεδομένα για το λογαριασμό για 90 ημέρες από την ημερομηνία έναρξης ισχύος του κλεισίματος του λογαριασμού του καταναλωτή. Μέσα σε αυτό το διάστημα είναι εφικτό να γίνει επαναφορά του λογαριασμού εφόσον το επιθυμεί ο καταναλωτής ωστόσο ενδέχεται να υπάρχει κόστος για οποιαδήποτε υπηρεσία AWS	Μετά το αίτημα διαγραφής του λογαριασμού, η Microsoft περιμένει 30 - 90 ημέρες πριν διαγράψει οριστικά τα δεδομένα του καταναλωτή σε περίπτωση που χρειαστεί να αποκτήσει πρόσβαση σε αυτά ή αν επιθυμεί να ενεργοποιήσει εκ νέου τη συνδρομή του. Δεν υπάρχουν χρεώσεις για	Μόλις υποβληθεί το αίτημα διαγραφής, τα δεδομένα συνήθως χαρακτηρίζονται προς διαγραφή αμέσως και στόχος είναι να εκτελεστεί αυτό το βήμα εντός μέγιστης περιόδου 24 ωρών. Αφού τα δεδομένα επισημανθούν για

	που δεν τερματίστηκε πριν κλείσει ο λογαριασμός. Για παράδειγμα εάν ανοίξει εκ νέου ο λογαριασμός ενός καταναλωτή AWS 30 ημέρες μετά το κλείσιμο και ο λογαριασμός AWS είχε μόνο ένα ενεργό στιγμιότυπο Amazon EC2, η τιμή είναι $0,01 ανά ώρα. Σε αυτή την περίπτωση, ο καταναλωτής μπορεί να χρεωθεί για 30 ημέρες x 24 ώρες x 0,01 $ ανά ώρα = 7,20 $. Στο τέλος της περιόδου των 90 ημερών, η AWS διαγράφει μόνιμα όλα τα δεδομένα για τον λογαριασμό.	την διατήρηση και επαναφορά των δεδομένων. Τα αποθηκευμένα ή εφεδρικά αντίγραφα θα διαγραφούν εντός 30 ημερών από το τέλος της περιόδου διατήρησης.	διαγραφή, μπορεί να ισχύσει μια εσωτερική περίοδος ανάκτησης έως και 30 ημέρες, ανάλογα με την υπηρεσία ή το αίτημα διαγραφής. Ο χρόνος που απαιτείται για να ολοκληρωθούν οι εσωτερικές εργασίες συλλογής των απορριμμάτων και να επιτευχθεί η λογική διαγραφή από τα ενεργά συστήματα είναι περίπου δύο μήνες. Όσον αφορά τα αντίγραφα ασφαλείας είναι σχεδιασμένα να λήγουν τα διαγραμμένα δεδομένα μέσα στα αντίγραφα ασφαλείας του κέντρου δεδομένων εντός έξι μηνών από το αίτημα διαγραφής.

Παρατηρούμε ότι οι τρεις πάροχοι έχουν κάποιες μικρές διαφορές όσον αφορά το διάστημα που κρατούν τους λογαριασμους και τα δεδομένα τον χρηστών μετά την αίτηση διαγραφής λογαριασμού από τον χρήστη. Ωστόσο η σημαντικότερη διαφορά που παρατηρούμε είναι ότι στην Amazon AWS σε περίπτωση επαναφοράς εντός του προβλεπόμενου διαστήματος υπάρχει κόστος για οποιαδήποτε υπηρεσία AWS που δεν τερματίστηκε πριν κλείσει ο λογαριασμός, κάτι που δεν συμβαίνει στους άλλους δύο παρόχους.

5.2.8 Συμμόρφωση SLA

Η μελέτη που έχει γίνει πάνω στον τομέα δείχνει ότι ο αριθμός των αναφορών για νομικά θέματα και ζητήματα διακυβέρνησης αντιπροσωπεύει το 73% των αναφορών που αφορούν την ασφάλεια. Όλοι οι πάροχοι οφείλουν βάσει κανονισμού να διατυπώνουν και να διατηρούν ένα SLA, το οποίο καθορίζει τα ποσοστα διαθεσιμότητας καθώς και τις αποζημιώσεις σε περίπτωση παραβίασης του SLA. Είναι σημαντικό να αναφερθεί ότι ο πελάτης είναι υπεύθυνος να συλλέγει δεδομένα ώστε να έχει τα

κατάλληλα διαπιστευτήρια σε περίπτωση παραβίασης του SLA, γεγονός που οδηγεί σε σημαντικό κόστος λόγω της ανάγκης δημιουργίας και συντήρησης υποδομής παρακολούθησης. Ο καταναλωτής πρέπει να προχωρήσει στις εξής ερωτήσεις προς έναν CSP:

1. Εφόσον η πραγματική διαθεσιμότητα διαφέρει από την ορισμένη στο SLA, πώς θα αποζημιωθώ;
2. Υπάρχουν πιστώσεις υπηρεσιών στην περίπτωση που δεν τηρηθεί το SLA;
3. Πως αποδεικνύεται η παραβίαση του SLA;

[28]

Πίνακας 16. Σύγκριση SLAs των παρόχων υπολογιστικού νέφους AWS, Microsoft Azure και Google Cloud [70] [71] [72]

Ανησυχία Καταναλωτή	Amazon Web Services (AWS)	Microsoft Azure	Google Cloud Platform (GCP)
Εάν το επίπεδο διαθεσιμότητας δεν είναι αυτό που ορίζεται στο SLA, πώς θα αποζημιωθώ;	Η AWS προσφέρει SLAs για διάφορες υπηρεσίες, όπως EC2 (εικονικοί διακομιστές), S3 (αποθήκευση αντικειμένων) κ.ά. Για το Amazon EC2 αν τα επίπεδα μηνιαίας υπηρεσίας χρόνου σύνδεσης πέφτουν μεταξύ 99.99% εώς 99.0% ο καταναλωτής λαμβάνει πίστωση 10% , αν τα επίπεδα μηνιαίας υπηρεσίας χρόνου σύνδεσης πέφτουν μεταξύ 99.0% εώς 95.0% ο καταναλωτής λαμβάνει πίστωση 30% και αν τα επίπεδα μηνιαίας υπηρεσίας χρόνου σύνδεσης πέφτουν κάτω από 95.0% ο καταναλωτής λαμβάνει πίστωση 100%. Τα ίδια ποσοστά ισχύουν για την υπηρεσία S3.	Η Microsoft Azure προσφέρει SLAs για διάφορες υπηρεσίες, όπως το Azure Virtual Machines (εικονικά μηχανήματα), το Blob Storage (αποθήκευση αντικειμένων) κ.α Για το Azure Virtual Machines αν τα επίπεδα μηνιαίας υπηρεσίας χρόνου σύνδεσης πέφτουν εώς και μεταξύ 99.99% εώς 99.0% καταναλωτής λαμβάνει πίστωση 10%, αν τα επίπεδα μηνιαίας υπηρεσίας χρόνου σύνδεσης πέφτουν μεταξύ 99.0% εώς 95.0% ο καταναλωτής λαμβάνει πίστωση 25% και αν τα επίπεδα μηνιαίας υπηρεσίας χρόνου σύνδεσης πέφτουν κάτω από 95.0% ο καταναλωτής λαμβάνει πίστωση 100%. Για την υπηρεσία Blob Storage αν τα επίπεδα μηνιαίας υπηρεσίας χρόνου σύνδεσης πέφτουν μεταξύ 99.99% εώς 99.0% ο	Η Google Cloud προσφέρει SLAs για διάφορες υπηρεσίες, όπως Compute Engine Service (εικονικά μηχανήματα). Για το Compute Engine Service εάν τα επίπεδα μηνιαίας υπηρεσίας χρόνου σύνδεσης πέφτουν μεταξύ 99,99% έως 99,00% ο καταναλωτής λαμβάνει πίστωση 10% σε μελλοντικό λογαριασμό. Εάν τα επίπεδα μηνιαίας υπηρεσίας χρόνου λειτουργίας σύνδεσης είναι μικρότερα από 99,00 και πάνω από ή ίσα με 95,00% ο καταναλωτής λαμβάνει πίστωση 25% σε μελλοντικό λογαριασμό. Εάν τα επίπεδα μηνιαίας υπηρεσίας χρόνου λειτουργίας σύνδεσης πέσουν κάτω από 95,00%, οι καταναλωτές λαμβάνουν πίστωση 100% σε μελλοντικό λογαριασμό.

		καταναλωτής λαμβάνει πίστωση 10% και αν τα τα επίπεδα μηνιαίας υπηρεσίας χρόνου σύνδεσης πέφτουν κάτω από 99.0% ο καταναλωτής λαμβάνει πίστωση 25%	
Υπάρχουν πιστώσεις υπηρεσιών στην περίπτωση που δεν τηρηθει το SLA ;	Παρέχονται πιστώσεις υπηρεσιών. Οι πιστώσεις υπηρεσιών υπολογίζονται με βάση τη διάρκεια της μη διαθεσιμότητας της υπηρεσίας και το ποσό εφαρμόζεται στον λογαριασμό AWS του πελάτη.	Παρέχονται πιστώσεις υπηρεσιών. Το ποσό των πιστώσεων υπηρεσιών βασίζεται στη διάρκεια της διακοπής της υπηρεσίας και εφαρμόζεται στη συνδρομή Azure του πελάτη.	Παρέχονται πιστώσεις υπηρεσιών. Οι πιστώσεις υπηρεσιών γίνονται με βάση τη διάρκεια της μη διαθεσιμότητας της υπηρεσίας Google Cloud, οι οποίες μπορούν να εφαρμοστούν στη χρέωση του πελάτη στο GCP.
Πως αποδεικνύεται η παραβίαση του SLA ;	Ο πελάτης πρέπει να παραδωσει τα διαπιστευτήρια στην Amazon και στην συνέχεια το υπεύθυνο τμήμα τα εξετάζει και αποφασίζει εάν υπάρχει όντως παραβίαση του SLA.	Ο πελάτης πρέπει να παραδωσει τα διαπιστευτήρια στην Microsoft και στην συνέχεια το υπεύθυνο τμήμα τα εξετάζει και αποφασίζει εάν υπάρχει όντως παραβίαση του SLA.	Ο πελάτης πρέπει να παραδωσει τα διαπιστευτήρια στην Google και στην συνέχεια το υπεύθυνο τμήμα τα εξετάζει και αποφασίζει εάν υπάρχει όντως παραβίαση του SLA.

Παρατηρούμε ότι οι τρεις πάροχοι έχουν κάποιες μικρές διαφορές όσον αφορά τα ποσοστά πίστωσης των καταναλωτών, όπως για παράδειγμα στην περίπτωση των υπηρεσιών εικονικών μηχανημάτων στην κατηγορία διαθεσιμότητας 99.0% εώς 95.0% όπου η Amazon προσφέρει πίστωση 30% ενώ οι άλλοι δύο πάροχοι προσφέρουν 25%. Ωστόσο, παρατηρούμε ότι οι τρεις πάροχοι ακολουθούν την ίδια πολιτική ως προς την απόδειξη παραβίασης του SLA, η οποία είναι ευθύνη του καταναλωτή.

5.2.9 Ασφάλεια Υπερεπόπτη (Hypervisor Security)

Το χαρακτηριστικό πολλαπλών μισθώσεων του υπολογιστικού νέφους δημιούργησε την ανάγκη της ενίσχυσης της ασφάλειας του υπερεπόπτη. Οι υπερεπόπτες επιτρέπουν την δημιουργία πολλαπλών εικονικών μηχανών με δυνητικά διαφορετικά λειτουργικά συστήματα ταυτόχρονα πάνω από ένα μόνο φυσικό μηχάνημα. Εάν κλονιστεί η ασφάλεια του υπερεπόπτη τότε ως αποτέλεσμα θα επηρεαστεί και η ασφάλεια των εικονικών μηχανημάτων που διαχειρίζεται. Επομένως, είναι σημαντικό να λαμβάνονται μέτρα προστασίας σε επίπεδο υπερεπόπτη ώστε να ενισχύεται και η ασφάλεια των εικονικών μηχανημάτων. Οι καταναλωτές θα πρέπει να ενδιαφέρονται για τα εξής:

1. Παρέχεται Απομόνωση Hypervisor;

2. Γίνονται τακτικές ενημερώσεις ασφαλείας στους υπερεπόπτες του παρόχου;
3. Υπάρχει φυσική ασφάλεια στα μηχανήματα όπου εκτελούνται οι υπερεπόπτες του παρόχου; [28]

Πίνακας 17. Σύγκριση ασφάλειας σε επίπεδο υπερεπόπτη στους παρόχους υπολογιστικού νέφους AWS, Microsoft Azure και Google Cloud [73] [74] [75]

Ανησυχία Καταναλωτή	Amazon Web Services (AWS)	Microsoft Azure	Google Cloud Platform (GCP)
Παρέχεται Απομόνωση Hypervisor;	• Η AWS χρησιμοποιεί μια προσαρμοσμένη και προστατευμένη έκδοση του hypervisor Xen. Ο Xen είναι ένας ευρέως χρησιμοποιούμενος hypervisor ανοικτού κώδικα που παρέχει δυνατότητες εικονικοποίησης. Η AWS έχει εφαρμόσει εκτεταμένες βελτιώσεις και τροποποιήσεις ασφαλείας στον Xen για να ικανοποιήσει τις συγκεκριμένες απαιτήσεις ασφαλείας της. • Το AWS Nitro System είναι μια τεχνολογία εικονικοποίησης επόμενης γενιάς που αναθέτει καθήκοντα διαχείρισης του υπερεπόπτη σε συγκεκριμένο υλικό και λογισμικό. Αυτό επιτρέπει στο AWS Nitro System να αφιερώνει όλους τους υπολογιστικούς πόρους σε συγκεκριμένους φόρτους εργασίας στο AWS. Παρακολουθεί συνεχώς τους εικονικοποιημένους πόρους και αποτρέπει την ακούσια πρόσβαση.Το AWS Nitro System προσφέρει κάποια πλεονεκτήματα ασφαλείας όπως την άμεση πρόσβαση στο υλικό, μειώνοντας τους κινδύνους που σχετίζονται με πολλαπλές μισθώσεις, την επιβολή της εκκινησης από αξιόπιστη πηγή, αποτρέποντας μη εξουσιοδοτημένες τροποποιήσεις, την επιβολή αυστηρών ορίων μεταξύ hypervisor	Το Azure χρησιμοποιεί τον hypervisor Hyper-V ως την υποκείμενη τεχνολογία εικονικοποίησης. Το Hyper-V παρέχει ισχυρές δυνατότητες απομόνωσης, επιτρέποντας την εκτέλεση πολλαπλών εικονικών μηχανών (VM) σε έναν μόνο φυσικό διακομιστή, διατηρώντας παράλληλα αυστηρό διαχωρισμό μεταξύ τους.	Το Google Cloud χρησιμοποιεί έναν ειδικά κατασκευασμένο hypervisor (KVM hypervisor) που έχει σχεδιαστεί ειδικά για να παρέχει ισχυρή απομόνωση και ασφάλεια για των εικονικών μηχανών. Ο hypervisor ενσωματώνει χαρακτηριστικά ασφαλείας για την επιβολή ορίων απομόνωσης.

	και υλικού, αποτρέποντας μη εξουσιοδοτημένη πρόσβαση και την υποστήριξη κρυπτογράφησης μνήμης για ένα πρόσθετο επίπεδο προστασίας δεδομένων		
Γίνονται τακτικές ενημερώσεις ασφαλείας;	Η Amazon ενημερώνει και επιδιορθώνει τακτικά τον υπερεπόπτη για την αντιμετώπιση των τρωτών σημείων ασφαλείας και τη διατήρηση της ασφάλειας των στιγμιοτύπων (εικονικών μηχανών) των πελατών.	Η Microsoft εφαρμόζει τακτικά ενημερώσεις ασφαλείας και επιδιορθώσεις για τον υπερεπόπτη για την αντιμετώπιση ευπαθειών και τη διασφάλιση της ασφάλειας των των στιγμιοτύπων (εικονικών μηχανών) των πελατών.	Η Google συντηρεί και ενημερώνει τακτικά τον υποκείμενο υπερεπόπτη με επιδιορθώσεις και ενημερώσεις ασφαλείας για την αντιμετώπιση ευπαθειών και τη διασφάλιση ενός ασφαλούς περιβάλλοντος.
Υπάρχει φυσική ασφάλεια στους υπερεπόπτες του παρόχου;	Τα κέντρα δεδομένων της AWS, όπου βρίσκονται οι υπερεπόπτες, διαθέτουν αυστηρά μέτρα φυσικής ασφάλειας, συμπεριλαμβανομένων ελέγχων πρόσβασης, βιντεοεπιτήρησης και περιβαλλοντικών ελέγχων και συστημάτων πλεονασμού, για την προστασία της υποκείμενης υποδομής.	Τα κέντρα δεδομένων Azure διατηρούν αυστηρά μέτρα φυσικής ασφάλειας για την προστασία της υποκείμενης υποδομής. Τα μέτρα αυτά περιλαμβάνουν ελέγχους πρόσβασης, βιντεοεπιτήρηση, περιβαλλοντικούς ελέγχους και συστήματα πλεονασμού (redundancy systems) για τη διασφάλιση της διαθεσιμότητας και της ασφάλειας της υποδομής hypervisor.	Τα κέντρα δεδομένων του Google Cloud είναι εξοπλισμένα με αυστηρά μέτρα φυσικής ασφάλειας, συμπεριλαμβανομένων ελέγχων πρόσβασης, βιντεοεπιτήρησης, περιβαλλοντικής παρακολούθησης, συστημάτων πλεονασμού και άλλων συστημάτων ασφαλείας. Αυτά τα μέτρα συμβάλλουν στην προστασία της υποδομής hypervisor από μη εξουσιοδοτημένη

			πρόσβαση και φυσικές απειλές.

Παρατηρούμε ότι και οι τρεις πάροχοι διαθέτουν τους δικούς τους υπερεπόπτες, οι οποίοι είναι σχεδιασμένοι έτσι ώστε να παρέχουν ισχυρή ασφάλεια. Επιπλέον, οι τρεις πάροχοι πραγματοποιούν τακτικές ενημερώσεις στους υπερεπόπτες τους αλλά και διαθέτουν κατάλληλα φυσικά μέτρα ασφαλείας στα κέντρα δεδομένων τους. Επομένως, μπορούμε να πούμε ότι δεν υστερεί κάποιος πάροχος ως προς την ασφάλεια υπερεπόπτη.

5.2.10 Ένθετες υπηρεσίες

Η περίπτωση μιας ένθετης/σύνθετης υπηρεσίας αναφέρεται σε μια υπηρεσία που αποτελείται από πολλαπλές υποκείμενες υπηρεσίες ή πόρους, συχνά από διαφορετικούς παρόχους υπολογιστικού νέφους. Για παράδειγμα, ένας δημόσιος πάροχος SaaS θα μπορούσε να βασίσει τις υπηρεσίες του σε εκείνες ενός PaaS ή IaaS. Φυσικά, αυτό θα μετατοπίσει εν μέρει την ευθύνη ασφάλειας στον πάροχο υπηρεσιών SaaS, εφόσον υπάρχει αντίστοιχο SLA, αλλά η ασφάλεια και η διαθεσιμότητα του SaaS θα εξαρτώνται και από την υποδομή. Για να μπορέσει να ξεπεράσει παρόμοια προβλήματα, ένας καταναλωτής πρέπει να γνωρίζει αυτές τις καταστάσεις και να βεβαιωθεί ότι η συμφωνία SLA καλύπτει όλες τις πτυχές της ασφάλειας όταν υπάρχει τρίτος που παρέχει άλλες υπηρεσίες προς την υπηρεσία που καταναλώνεται. Στην περίπτωση που ο καταναλωτής συνθέτει ο ίδιος υπηρεσίες από διαφορετικούς παρόχους υπηρεσιών νέφους για τη δημιουργία μιας λύσης, οι συμφωνίες επιπέδου υπηρεσιών κάθε παρόχου ισχύουν ανεξάρτητα. Αυτό σημαίνει ότι οι SLAs για τις υπηρεσίες που συντίθενται δεν συνδυάζονται σε μια ενιαία ενοποιημένη SLA για όλους τους παρόχους. Κάθε πάροχος νέφους είναι υπεύθυνος για τη διασφάλιση των δεσμεύσεων SLA για τις αντίστοιχες υπηρεσίες του. [28]

Πινακας 18. Σύγκριση αντιμετώπισης προβλημάτων από ένθετες υπηρεσίες από τα SLAs των παρόχων υπολογιστικού νέφους AWS, Microsoft Azure, Google Cloud [76] [77] [78]

Ανησυχία Καταναλωτή	Amazon Web Services (AWS)	Microsoft Azure	Google Cloud Platform (GCP)
Η SLA καλύπτει όλες τις πτυχές της ασφάλειας όταν υπάρχει τρίτο μέρος που παρέχει άλλες υπηρεσίες προς την	Το Amazon EC2 SLA αποκλείει από την σφαίρα ευθύνης της τη μη διαθεσιμότητα, την αναστολή ή τον τερματισμό του Amazon EC2 που προκύπτουν από ενέργειες ή αδράνειες από τον πελάτη ή οποιοδήποτε τρίτο που προκύπτουν από καταναλωτικό	Το Microsoft Azure SLA αποκλείει οποιοδήποτε πρόβλημα απόδοσης ή διαθεσιμότητας προκύπτει από υλικό ή λογισμικό τρίτων μερών. Η υπηρεσία τρίτου μέρους θα διέπεται από την ισχύουσα δήλωση	Το Google Cloud SLA δεν καλύπτει τυχόν σφάλματα που προκαλούνται από παράγοντες εκτός του εύλογου ελέγχου της Google που προέκυψαν από λογισμικό ή υλικό τρίτων που είναι

προσφερόμενη (του SLA);	εξοπλισμό, λογισμικό ή άλλη τεχνολογία ή/και εξοπλισμό τρίτου ή/και πελατη (εκτός από εξοπλισμό τρίτων που υπάγεται στον άμεσο έλεγχο της εταιρείας).	απορρήτου και τις πολιτικές του τρίτου μέρους.	αποτέλεσμα καταχρήσεων ή άλλων συμπεριφορών που παραβιάζουν τη συμφωνία.

Παρατηρούμε ότι οι τρεις πάροχοι παρουσιάζουν διαφορές για προβλήματα που προέρχονται από ένθετες/σύνθετες υπηρεσίες με βάση τα SLAs που αυτοί προσφέρουν. Στην περίπτωση της Amazon παρατηρούμε ότι η εταιρεία αναλαμβάνει την ευθύνη σε περίπτωση προβληματικού εξοπλισμού/υπηρεσίας που προσφέρεται από τρίτο μέρος και χρησιμοποιείται από τον πάροχο ενώ οι άλλοι δύο πάροχοι δεν προσφέρουν κάποια κάλυψη. Ωστόσο μπορούμε να πούμε ότι σε αυτή την περίπτωση, όλοι οι πάροχοι υστερούν διότι δεν παρέχουν κάλυψη προβλημάτων που οφείλονται σε υπηρεσίες τρίτων. Είναι σημαντικό για τον καταναλωτή, ο πάροχος του υπολογιστικού νέφους που χρησιμοποιεί, να διασφαλίζει μέσω ενός σύνθετου SLA πως η συμπεριφορά των συστατικών τρίτων μερών είναι η κατάλληλη. Η Amazon φαίνεται να καλύπτει εν μέρει το πρόβλημα αυτό ωστόσο δεν το καλύπτει επαρκώς.

5.2.11 Σύνοψη

Οι τρείς παραπάνω πάροχοι υπολογιστικού νέφους είναι οι κορυφαίοι πάροχοι στην αγορά αυτή την στιγμή με το μεγαλύτερο μερίδιο. Με βάση την σύγκριση που έγινε στο Κεφάλαιο 5.2 (Ενότητες 5.2.1 έως 5.2.10) δεν φαίνεται εν γένει να υπερτερεί ή να μειονεκτεί κάποιος. Ωστόσο υπάρχουν κάποιες διαφορές μεταξύ των παρόχων σε ορισμένες περιπτώσεις (ειδικό υλικό και απομόνωση, SLAs, πρότυπα & πιστοποιήσεις ασφάλειας, πρότυπα ελέγχου πρόσβασης, προκαθορισμένη κρυπτογράφηση δεδομένων και ανάκτηση λογαριασμού μετά από αίτηση διαγραφής) που θα μπορούσαν να αποτελέσουν τον καθοριστικό παράγοντα επιλογής για έναν καταναλωτή. Τα χαρακτηριστικά που παρέχουν είναι ως επί το πλείστον ανταγωνιστικά και όμοια μεταξύ τους. Επομένως, Ο προσδιορισμός της επιλογής του κατάλληλου πάροχου υπολογιστικού νέφους γίνεται μόνο συνυπολογίζοντας τις συγκεκριμένες ανάγκες, τον προϋπολογισμό, τις επιθυμητές υπηρεσίες, την εξοικείωση και εμπειρία με παρόμοια συστήματα και την επιθυμητή υποστήριξη που χρειάζεται ο καταναλωτής.

6. Συμπεράσματα

Η ταχεία υιοθέτηση του υπολογιστικού νέφους έχει επιφέρει σημαντικά οφέλη στους οργανισμούς, όπως η επεκτασιμότητα, η ευελιξία και η αποδοτικότητα του κόστους. Ωστόσο, δεν μπορούν να αγνοηθούν οι προκλήσεις ασφαλείας που υπάρχουν στα περιβάλλοντα νέφους. Η παρούσα διπλωματική εργασία διερεύνησε διάφορες πτυχές της ασφάλειας του νέφους, συμπεριλαμβανομένων των απειλών, των επιθέσεων, των στρατηγικών μετριασμού και των μελετών περιπτώσεων πραγματικών επιθέσεων ενώ παρείχε συγκριτικές αναλύσεις με γνώμονα την ασφάλεια μεταξύ του

νέφους και των επιτόπιων περιβαλλόντων και μεταξύ των μεγαλύτερων παρόχων δημόσιου νέφους, ώστε να παρέχει μια ολοκληρωμένη κατανόηση του θέματος.

Εντοπίζοντας και αναλύοντας τις σημαντικότερες απειλές ασφαλείας και τους φορείς επιθέσεων, οι καταναλωτές μπορούν να αποκτήσουν μια πολύ καλή εικόνα των πιθανών κινδύνων που αντιμετωπίζουν στο νέφος. Η κατανόηση αυτή επιτρέπει την εφαρμογή αποτελεσματικών στρατηγικών μετριασμού και βέλτιστων πρακτικών για τη διασφάλιση κρίσιμων περιουσιακών στοιχείων. Μέσω προληπτικών μέτρων, οι οργανισμοί μπορούν να μετριάσουν τον αντίκτυπο των παραβιάσεων ασφάλειας και να διατηρήσουν την εμπιστευτικότητα, την ακεραιότητα και τη διαθεσιμότητα των δεδομένων και των εφαρμογών τους.

Η συμπερίληψη μελετών περιπτώσεων από τον πραγματικό κόσμο παρείχε πρακτικές γνώσεις σχετικά με τις συνέπειες των παραβιάσεων της ασφάλειας σε περιβάλλοντα νέφους. Με την εξέταση αυτών των περιστατικών, οι καταναλωτές μπορούν να κατανοήσουν καλύτερα τις ευπάθειες που μπορεί να υπάρχουν και τη σημασία της εφαρμογής ισχυρών μέτρων ασφαλείας. Τα διδάγματα που αντλήθηκαν από αυτές τις μελέτες περιπτώσεων μπορούν να χρησιμεύσουν ως καθοδήγηση για τους καταναλωτές που επιδιώκουν να ενισχύσουν τη στάση ασφαλείας τους στο νέφος.

Η συγκριτική ανάλυση μεταξύ των αρχιτεκτονικών που βασίζονται στο νέφος και των αυτοδιαχειριζόμενων (επιτόπιων) συστημάτων έριξε φως στα πλεονεκτήματα και τις αδυναμίες της ασφάλειας της κάθε προσέγγισης. Επομένως, οι οργανισμοί πρέπει να εξετάζουν προσεκτικά τις συγκεκριμένες απαιτήσεις και προτιμήσεις τους, τις ικανότητες ασφάλειας που οι ίδιοι έχουν, τον διαθέσιμο προϋπολογισμό τους καθώς και την ανοχή τους σε κινδύνους όταν επιλέγουν μεταξύ των περιβαλλόντων νέφους και των επιτόπιων περιβαλλόντων. Σημαντική βάση σε αυτή την προσπάθεια προς την λήψη τεκμηριωμένων αποφάσεων επιλογής κατάλληλου τύπου περιβάλλοντος είναι ιδιαίτερα η κατανόηση των διαφορών στους μηχανισμούς ασφαλείας και στα μέτρα ελέγχου που υπάρχουν μεταξύ των δύο αυτών διαφορετικών τύπων περιβαλλόντων.

Επιπλέον, η σύγκριση της ασφάλειας μεταξύ των κορυφαίων παρόχων υπηρεσιών νέφους, δηλαδή των Amazon AWS, Microsoft Azure και Google Cloud, παρείχε πολύτιμες πληροφορίες σχετικά με τις αντίστοιχες δυνατότητες ασφαλείας τους. Οι καταναλωτές μπορούν να αξιολογήσουν παράγοντες όπως τα χαρακτηριστικά/ικανότητες ασφαλείας (δημιουργία αντιγράφων ασφαλείας και αποκατάσταση από καταστροφές, κρυπτογράφηση, μέθοδοι ελέγχου ταυτότητας και πρόσβασης, ειδικό υλικό και απομόνωση, μέθοδοι παρακολούθησης, μέθοδοι ασφάλειας υπερεπόπτη), τις πιστοποιήσεις και τα υποστηριζόμενα πρότυπα συμμόρφωσης για να επιλέξουν έναν πάροχο νέφους που να ανταποκρίνεται στις απαιτήσεις ασφαλείας τους και τον προϋπολογισμό τους.

Καθώς το νέφος συνεχίζει να εξελίσσεται, το τοπίο της ασφάλειας (σε αυτό) θα αλλάζει συνεχώς. Οι καταναλωτές πρέπει να παραμένουν σε εγρήγορση και να προσαρμόζουν ανάλογα τις στρατηγικές ασφαλείας τους. Παραμένοντας ενημερωμένοι σχετικά με τις αναδυόμενες απειλές, αξιοποιώντας τις βέλτιστες πρακτικές και λαμβάνοντας υπόψη τα μοναδικά χαρακτηριστικά των αναπτύξεων νέφους, οι καταναλωτές μπορούν να περιηγηθούν αποτελεσματικά στις πολυπλοκότητες της ασφάλειας νέφους και να διασφαλίσουν την ανθεκτικότητα της ψηφιακής υποδομής τους σε έναν ολοένα και πιο διασυνδεδεμένο κόσμο.

Βιβλιογραφία

1. Modi, C., Patel, D., Borisaniya, B., Patel, A., & Rajarajan, M. (2012). A survey on security issues and solutions at different layers of Cloud computing. *The Journal of Supercomputing*, *63*(2), 561–592. https://doi.org/10.1007/s11227-012-0831-5
2. Latif, R., Abbas, H., Assar, S., Ali, Q. (2014). Cloud Computing Risk Assessment: A Systematic Literature Review. *In: Park, J., Stojmenovic, I., Choi, M., Xhafa, F. (eds) Future Information Technology. Lecture Notes in Electrical Engineering, vol 276. Springer, Berlin, Heidelberg*. http://dx.doi.org/10.1007/978-3-642-40861-8_42
3. Grobauer, B., Walloschek, T., & Stocker, E. (2011). Understanding cloud computing vulnerabilities. *IEEE Security & Privacy Magazine*, *9*(2), 50–57. https://doi.org/10.1109/msp.2010.115
4. Aasarmya, A., & Agarwal, S. (2019). Improving Security for Data Migration in Cloud Computing using Randomized Encryption Technique. *International Journal of Computer Sciences and Engineering*, *7*(8), 39–43. https://doi.org/10.26438/ijcse/v7i8.3943

5. Chou, T. S. (2013). Security threats on cloud computing vulnerabilities. *International Journal of Computer Science & Information Technology*, *5*(3), 79-88. https://doi.org/10.5121/ijcsit.2013.5306
6. Singh, A., & Chatterjee, K. (2017). Cloud security issues and challenges: A survey. *Journal of Network and Computer Applications*, *79*, 88-115 https://doi.org/10.5121/ijcsit.2013.5306
7. Basu, S., Bardhan, A., Gupta, K., Saha, P., Pal, M., Bose, M., Basu, K., Chaudhury, S., & Sarkar, P. (2018, January). Cloud computing security challenges & solutions-A survey. *IEEE 8th Annual Computing and Communication Workshop and Conference (CCWC), Las Vegas, NV, USA*. http://dx.doi.org/10.1109/ccwc.2018.8301700
8. Behl, A. (2011, December). Emerging security challenges in cloud computing: An insight to cloud security challenges and their mitigation. In *2011 World Congress on Information and Communication Technologies, Mumbai, India* (pp.217-222). IEEE. http://dx.doi.org/10.1109/wict.2011.6141247
9. Mell, P. (2012). What's special about cloud security? *IT Professional*, *14*(4), 6–8. https://doi.org/10.1109/mitp.2012.84
10. Behl, A., & Behl, K. (2012, October). An analysis of cloud computing security issues. *World Congress on Information and Communication Technologies, Trivandrum, India*. http://dx.doi.org/10.1109/wict.2012.6409059
11. Sridhar, S., & Smys, S. (2017, January). Intelligent security framework for iot devices cryptography based end-to-end security architecture. *International Conference on Inventive Systems and Control (ICISC), Coimbatore, India*. http://dx.doi.org/10.1109/icisc.2017.8068718
12. Kumar, R., & Goyal, R. (2021). Top threats to cloud: A Three-Dimensional model of cloud security assurance. In *Computer Networks and Inventive Communication Technologies* (pp. 683–705). Springer Nature Singapore. http://dx.doi.org/10.1007/978-981-15-9647-6_53
13. Al Nafea, R., & Almaiah, M. A. (2021, July). Cyber security threats in cloud: Literature review. *International Conference on Information Technology (ICIT), Amman, Jordan,* (pp. 779-786). IEEE. http://dx.doi.org/10.1109/icit52682.2021.9491638
14. Sasubilli, M. K., & Venkateswarlu, R. (2021, January). Cloud computing security challenges, threats and vulnerabilities. *6th international conference on inventive computation technologies (ICICT), Coimbatore, India,* (pp. 476-480). IEEE. http://dx.doi.org/10.1109/icict50816.2021.9358709
15. Stallings, W., & Brown, L. (2015). *Computer security: Principles and practice* (3rd ed.). Prentice Hall.
16. Darwish, M., Ouda, A., & Capretz, L. F. (2013, June). Cloud-based DDoS attacks and defenses. In *International Conference on Information Society (i-Society 2013), Toronto, ON, Canada* (pp. 67-71). IEEE. https://doi.org/10.1016/j.jisa.2014.12.001
17. Shaikh, A. A. (2016, October). Attacks on cloud computing and its countermeasures. *International Conference on Signal Processing, Communication, Power and Embedded System (SCOPES), Paralakhemundi, India,* (pp. 748-752). IEEE. http://dx.doi.org/10.1109/scopes.2016.7955539

18. Smita Sharma, R.P. Singh, (2019). A Critical Survey on: Cloud Security and privacy issues and its associated solutions. *International Journal of Computer Sciences and Engineering*, 7(8), 288-296. https://doi.org/10.26438/ijcse/v7i8.288296
19. Abusaimeh, H. (2020). Virtual machine escape in cloud computing services. *International Journal of Advanced Computer Science and Applications*, *11*(7). https://doi.org/10.14569/ijacsa.2020.0110743
20. Hwang, T., Shin, Y., Son, K., & Park, H. (2013, December). Design of a hypervisor-based rootkit detection method for virtualized systems in cloud computing environments. In *AASRI Winter International Conference on Engineering and Technology (AASRI-WIET 2013), Saipan, USA,* (pp. 27-32). Atlantis Press. http://dx.doi.org/10.2991/wiet-13.2013.7
21. Mehmood, Y., Shibli, M. A., Habiba, U., & Masood, R. (2013, December). Intrusion detection system in cloud computing: Challenges and opportunities. *2nd National Conference on Information Assurance (NCIA), Rawalpindi, Pakistan,* (pp. 59-66). IEEE. http://dx.doi.org/10.1109/ncia.2013.6725325
22. Chouhan, P., & Singh, R. (2016). Security attacks on cloud computing with possible solution. *International Journal of Advanced Research in Computer Science and Software Engineering*, *6*(1).
23. Jensen, M., Schwenk, J., Gruschka, N., & Iacono, L. L. (2009, September). On technical security issues in cloud computing. *International Conference on Cloud Computing, Bangalore, India,* (pp. 109-116). IEEE. http://dx.doi.org/10.1109/cloud.2009.60
24. Singh, J. (2014). Cyber-attacks in cloud computing: A case study. *International Journal of Electronics and Information Engineering*, *1*(2), 78-87. https://doi.org/10.17781/p001294
25. Alabdan, R. (2020). Phishing attacks survey: Types, vectors, and technical approaches. *Future internet*, *12*(10), 168. https://doi.org/10.3390/fi12100168
26. De Carvalho, C. A. B., de Castro Andrade, R. M., de Castro, M. F., Coutinho, E. F., & Agoulmine, N. (2017). State of the art and challenges of security SLA for cloud computing. *Computers & Electrical Engineering*, *59*, 141-152. https://doi.org/10.1016/j.compeleceng.2016.12.030
27. Molnar, D., & Schechter, S. E. (2010, June). Self Hosting vs. Cloud Hosting: Accounting for the Security Impact of Hosting in the Cloud. In *WEIS* (Vol. 2010, pp. 1-18).
28. Abuhussein, A., Bedi, H., & Shiva, S. (2012, December). Evaluating security and privacy in cloud computing services: A Stakeholder's perspective. In *2012 international conference for internet technology and secured transactions, London, UK,* (pp. 388-395). IEEE.
29. Akilal, A., & Kechadi, M. T. (2022). An improved forensic-by-design framework for cloud computing with systems engineering standard compliance. *Forensic Science International: Digital Investigation*, *40*, 301315. https://doi.org/10.1016/j.fsidi.2021.301315
30. van Beek, H. M., Van Eijk, E. J., van Baar, R. B., Ugen, M., Bodde, J. N. C., & Siemelink, A. J. (2015). Digital forensics as a service: Game on. *Digital Investigation*, *15*, 20-38. https://doi.org/10.1016/j.diin.2015.07.004

31. Ganesh, N. G., Venkatesh, N. M., & Prasad, D. V. V. (2022). A systematic literature review on forensics in cloud, IoT, AI & blockchain. *Illumination of Artificial Intelligence in Cybersecurity and Forensics*, 197-229. http://dx.doi.org/10.1007/978-3-030-93453-8_9
32. Barron, C., Yu, H., & Zhan, J. (2013, July). Cloud computing security case studies and research. In *Proceedings of the world congress on engineering* (Vol. 2, No. 2, pp. 1-6).
33. Varadharajan, V., & Tupakula, U. (2014). Security as a service model for cloud environment. *IEEE Transactions on network and Service management*, *11*(1), 60-75. https://doi.org/10.1109/tnsm.2014.041614.120394
34. Hussain, M., & Abdulsalam, H. (2011, April). SECaaS: security as a service for cloud-based applications. In *Proceedings of the Second Kuwait Conference on e-Services and e-Systems, Kuwait City,* (pp. 1-4). http://dx.doi.org/10.1145/2107556.2107564
35. Kamal, M. A., Raza, H. W., Alam, M. M., & Mohd, M. (2020). Highlight the features of AWS, GCP and Microsoft Azure that have an impact when choosing a cloud service provider. *Int. J. Recent Technol. Eng*, *8*(5), 4124-4232. https://doi.org/10.35940/ijrte.d8573.018520
36. Attaran, M., & Woods, J. (2019). Cloud computing technology: improving small business performance using the Internet. *Journal of Small Business & Entrepreneurship*, *31*(6), 495-519. https://doi.org/10.1080/08276331.2018.1466850
37. Somorovsky, J., Heiderich, M., Jensen, M., Schwenk, J., Gruschka, N., & Lo Iacono, L. (2011, October). All your clouds are belong to us: security analysis of cloud management interfaces. In *Proceedings of the 3rd ACM workshop on Cloud computing security workshop, Chicago, Illinois, USA,* (pp. 3-14). http://dx.doi.org/10.1145/2046660.2046664
38. Tucker, G., & Li, C. (2012). Cloud Computing Risks. In *Proceedings on the International Conference on Internet Computing (ICOMP), Las Vegas, Nevada, USA,* (p. 1). The Steering Committee of The World Congress in Computer Science, Computer Engineering and Applied Computing (WorldComp).
39. Abel, S., Xiao, L., & Wang, H. (2018, December). Causal Modeling for Cybersecurity. In *2018 International Symposium on Security and Privacy in Social Networks and Big Data (SocialSec), Santa Clara, CA, USA,* (pp. 209-212). IEEE. http://dx.doi.org/10.1109/socialsec.2018.8760379
40. Novaes Neto, N., Madnick, S., de Paula, M. G., & Malara Borges, N. (2020). A case study of the capital one data breach. *Stuart E. and Moraes G. de Paula, Anchises and Malara Borges, Natasha, A Case Study of the Capital One Data Breach (January 1, 2020)*. https://doi.org/10.2139/ssrn.3542567
41. Padma, P., & Srinivasan, S. (2016, August). A survey on biometric based authentication in cloud computing. In *2016 International Conference on Inventive Computation Technologies (ICICT), Coimbatore, India,* (Vol. 1, pp. 1-5). IEEE. http://dx.doi.org/10.1109/inventive.2016.7823273
42. Nwosu, J. N. (2022). Evolving Cybercrimes and How to Contain them. Idosr Journal Of Computer And Applied Science, 7(1), 1-8.

43. Kumar, S. U. B. O. D. H., Athavale, V. A., & Kartikey, D. I. V. Y. E. (2021). Security issues in cloud computing: A holistic view. *International Journal of Internet of Things and Web Services*, *6*, 18-29.
44. *IBM Cloud*. (n.d.). IBM. Retrieved July 24, 2023, from https://www.ibm.com/cloud
45. *Topics*. (n.d.). IBM. Retrieved July 24, 2023, from https://www.ibm.com/topics
46. Devalla, V., Raghavan, S. S., Maste, S., Kotian, J. D., & Annapurna, D. (2022). murli: A tool for detection of malicious urls and injection attacks. *Procedia Computer Science*, *215*, 662-676. https://doi.org/10.1016/j.procs.2022.12.068
47. *Backup and recovery using AWS Backup*. (n.d.). AWS Prescriptive Guidance. Retrieved July 24, 2023, from https://docs.aws.amazon.com/prescriptive-guidance/latest/backup-recovery/aws-backup.html
48. AbhishekMallick-MS. (n.d.). *What is Azure Backup? - Azure Backup*. Microsoft Learn. https://learn.microsoft.com/en-us/azure/backup/backup-overview
49. dennispadia. (n.d.). *Disaster Recovery overview and infrastructure guidelines for SAP workload*. Microsoft Learn. Retrieved July 24, 2023, from https://learn.microsoft.com/en-us/azure/sap/workloads/disaster-recovery-overview-guide
50. Set up and plan a Backup and DR Service deployment. (n.d.). *Google Cloud*. Retrieved July 24, 2023, from https://cloud.google.com/backup-disaster-recovery/docs/configuration/deployment-plan#overview_of_the_service_architecture
51. *Data encryption*. (n.d.). Introduction to AWS Security. Retrieved July 24, 2023, from https://docs.aws.amazon.com/whitepapers/latest/introduction-aws-security/data-encryption.html
52. *Azure encryption overview*. Microsoft Learn. Retrieved July 24, 2023, from https://learn.microsoft.com/en-us/azure/security/fundamentals/encryption-overview
53. Default encryption at rest. (n.d.). *Google Cloud*. Retrieved July 24, 2023, from https://cloud.google.com/docs/security/encryption/default-encryption
54. *Identity and access control*. (n.d.). Introduction to AWS Security. Retrieved July 24, 2023, from https://docs.aws.amazon.com/whitepapers/latest/introduction-aws-security/identity-and-access-control.html
55. TerryLanfear. (n.d.). *Azure security features that help with identity management*. Microsoft Learn. Retrieved July 24, 2023, from https://learn.microsoft.com/en-us/azure/security/fundamentals/identity-management-overview
56. IAM overview. (n.d.). *Google Cloud*. Retrieved July 24, 2023, from https://cloud.google.com/iam/docs/overview
57. Overview of IAM conditions. (n.d.). *Google Cloud*. https://cloud.google.com/iam/docs/conditions-overview
58. *Configure instance tenancy with a launch configuration*. (n.d.). Amazon EC2 Auto Scaling. Retrieved July 24, 2023, from https://docs.aws.amazon.com/autoscaling/ec2/userguide/auto-scaling-dedicated-instances.html

59. *Isolation in the azure public cloud*. Microsoft Learn. Retrieved July 24, 2023, from https://learn.microsoft.com/en-us/azure/security/fundamentals/isolation-choices
60. Sole-tenancy overview. (n.d.). *Google Cloud*. Retrieved July 24, 2023, from https://cloud.google.com/compute/docs/nodes/sole-tenant-nodes
61. *Monitoring and logging*. (n.d.). Introduction to AWS Security. Retrieved July 24, 2023, from https://docs.aws.amazon.com/whitepapers/latest/introduction-aws-security/monitoring-and-logging.html
62. *Azure Monitor overview - Azure Monitor*. Microsoft Learn. Retrieved July 24, 2023, from https://learn.microsoft.com/en-us/azure/azure-monitor/overview
63. *Operations: Cloud monitoring & logging*. (n.d.). Google Cloud. Retrieved July 24, 2023, from https://cloud.google.com/products/operations
64. *Compliance programs - Amazon Web Services (AWS)*. (n.d.). Amazon Web Services, Inc. Retrieved July 24, 2023, from https://aws.amazon.com/compliance/programs/
65. *Azure and other Microsoft cloud services compliance offerings - Azure Compliance*. Microsoft Learn. Retrieved July 24, 2023, from https://learn.microsoft.com/en-us/azure/compliance/offerings/
66. *Cloud Compliance - Regulations & Certifications*. (n.d.). Google Cloud. Retrieved July 24, 2023, from https://cloud.google.com/security/compliance/offerings#/regions=Global
67. *Closing an account*. (n.d.). AWS Billing. Retrieved July 24, 2023, from https://docs.aws.amazon.com/awsaccountbilling/latest/aboutv2/close-account.html
68. *Cancel your Azure subscription - Microsoft Cost Management*. Microsoft Learn. Retrieved July 24, 2023, from https://learn.microsoft.com/en-us/azure/cost-management-billing/manage/cancel-azure-subscription
69. Data deletion on Google Cloud. (n.d.). *Google Cloud*. Retrieved July 24, 2023, from https://cloud.google.com/docs/security/deletion#deletion_timeline
70. *AWS service level agreements*. (n.d.). Amazon Web Services, Inc. Retrieved July 24, 2023, from https://aws.amazon.com/legal/service-level-agreements/?aws-sla-cards.sort-by=item.additionalFields.serviceNameLower&aws-sla-cards.sort-order=asc&awsf.tech-category-filter=*all&aws-sla-cards.q=ec2&aws-sla-cards.q_operator=AND
71. *Licensing documents*. (n.d.). Retrieved July 24, 2023, from https://www.microsoft.com/licensing/docs/view/Service-Level-Agreements-SLA-for-Online-Services?lang=1
72. *Cloud Functions Service Level Agreement (SLA)*. (n.d.). Google Cloud. Retrieved July 24, 2023, from https://cloud.google.com/functions/sla
73. *What is a Hypervisor? - Hypervisor Explained - AWS*. (n.d.). Amazon Web Services, Inc. Retrieved July 24, 2023, from https://aws.amazon.com/what-is/hypervisor/
74. *Hypervisor security on the Azure fleet - Azure Security*. Microsoft Learn. Retrieved July 24, 2023, from https://learn.microsoft.com/en-us/azure/security/fundamentals/hypervisor

75. Honig, A., & Porter, N. (2017, January 26). 7 ways we harden our KVM hypervisor at Google Cloud: Security in plaintext. *Google Cloud*. https://cloud.google.com/blog/products/gcp/7-ways-we-harden-our-kvm-hypervisor-at-google-cloud-security-in-plaintext
76. *Amazon compute service level agreement*. (n.d.). Amazon Web Services, Inc. Retrieved July 24, 2023, from https://aws.amazon.com/compute/sla/?did=sla_card&trk=sla_card
77. *Licensing documents*. (n.d.). Retrieved July 24, 2023, from https://www.microsoft.com/licensing/docs/view/Service-Level-Agreements-SLA-for-Online-Services?lang=1
78. *Cloud Functions Service Level Agreement (SLA)*. (n.d.). Google Cloud. Retrieved July 24, 2023, from https://cloud.google.com/functions/sla
79. Gonzalez, H., Nance, K., & Nazario, J. (2011, October). Phishing by form: The abuse of form sites. In *2011 6th International Conference on Malicious and Unwanted Software, Fajardo, PR, USA,* (pp. 95-101). IEEE. http://dx.doi.org/10.1109/malware.2011.6112332
80. Rountree, D., & Castrillo, I. (2014). Chapter 3-cloud deployment models. *The Basics of Cloud Computing*, 35-47. http://dx.doi.org/10.1016/b978-0-12-405932-0.00003-7
81. Ahmad, I., & Bakht, H. (2019). Security challenges from abuse of cloud service threat. *International Journal of Computing and Digital Systems*, *8*(01), 19-31. https://doi.org/10.12785/ijcds/080103
82. Khalid, A. (2013). Cloud computing technology: services and opportunities. *Pakistan Journal of Science*, *65*(3).
83. *O-RT 3.0.1*. (n.d.). Retrieved July 24, 2023, from https://pubs.opengroup.org/security/o-rt/
84. Κρητικός Κυριάκος. Διαφάνειες Μαθήματος 321-11001-Τεχνολογίες Νέφους, *2η Διάλεξη – Θεμελιώδης Αρχές & Μοντέλα*. Πανεπιστήμιο Αιγαίου, Τμήμα Μηχανικών Πληροφοριακών & Επικοινωνιακών Συστημάτων, Σάμος, Ελλάδα.