2024

Ασφάλεια πληροφοριών σε Cloud υπηρεσίες

ΘΕΟΔΩΡΟΥ ΧΡΗΣΤΟΣ ICSD17057
ΚΑΡΒΟΥΝΗΣ ΧΡΗΣΤΟΣ ICSD17076

ΕΠΙΒΛΕΠΟΥΣΑ ΚΑΘΗΓΗΤΡΙΑ: ΔΙΑΜΑΝΤΟΠΟΥΛΟΥ ΒΑΣΙΛΙΚΗ

ΠΑΝΕΠΙΣΤΗΜΙΟ ΑΙΓΑΙΟΥ |

Πίνακας Περιεχομένων

Table of Contents

Πίνακας Ακρωνύμιων

- NIST (National Institute of Standards and Technology)
- HIPAA (Health Insurance Portability and Accountability Act)
- GDPR (General Data Protection Regulation)
- MFA(Multi-Factor Authentication)
- IAM(Identity and Access Management)
- PCI DSS (Payment Card Industry Data Security Standard)
- ΓΚΠΔ (Γενικός κανονισμός για την προστασία δεδομένων)
- CSP (Content Security Policy)
- PHI (Protected health information)
- PII (Personal Identifiable Information)
- ISMS (information security management systems)
- OWASP (Open Worldwide Application Security Project)
- AD (Active Directory)
- SaaS(Software as a service)
- PaaS(Platform as a Service)
- IaaS (Infrastructure as a service)
- CSC (Computer Science and Communication)
- MBR (Master Boot Record)
- PKI (Public key infrastructure)
- ECC (Error-Correcting Code)
- IDPS (internally displaced persons)
- S3 (Simple Storage Service)
- GKE (Google Kubernetes Engine)

Περίληψη

Το υπολογιστικό νέφος έχει γίνει αναπόσπαστο μέρος της σύγχρονης τεχνολογικής υποδομής, φέρνοντας επανάσταση στον τρόπο με τον οποίο επιχειρήσεις και ιδιώτες έχουν πρόσβαση, αποθηκεύουν και επεξεργάζονται δεδομένα. Στον πυρήνα της, η υπολογιστική νέφους αναφέρεται στην παροχή υπολογιστικών υπηρεσιών -συμπεριλαμβανομένης της αποθήκευσης, της επεξεργαστικής ισχύος και των εφαρμογών- μέσω του διαδικτύου και όχι μέσω υλικού ή λογισμικού στις εγκαταστάσεις. Αυτή η αλλαγή παραδείγματος επέτρεψε στους οργανισμούς να κλιμακώσουν τις δραστηριότητές τους πιο αποτελεσματικά, να μειώσουν το κόστος και να αποκτήσουν πρόσβαση σε προηγμένες τεχνολογίες χωρίς σημαντικές αρχικές επενδύσεις. Για να κατανοήσουμε το βάθος και τη σημασία του cloud computing, είναι απαραίτητο να διερευνήσουμε τις θεμελιώδεις αρχές, τα βασικά χαρακτηριστικά, τα μοντέλα ανάπτυξης, τα μοντέλα υπηρεσιών, τα οφέλη, τις προκλήσεις και τις μελλοντικές τάσεις.

Abstract

Cloud computing has become an integral part of the modern technological infrastructure, revolutionising the way businesses and individuals access, store and process data. At its core, cloud computing refers to the delivery of computing services - including storage, processing power and applications - over the internet rather than through on-premises hardware or software. This paradigm shift has enabled organisations to scale their operations more efficiently, reduce costs and gain access to advanced technologies without significant upfront investment. To understand the depth and importance of cloud computing, it is necessary to explore the fundamentals, key features, deployment models, service models, benefits, challenges and future trends.

1. Εισαγωγή στο Cloud Computing

Το υπολογιστικό νέφος έχει φέρει επανάσταση στον τρόπο με τον οποίο οι επιχειρήσεις και οι ιδιώτες διαχειρίζονται και χρησιμοποιούν τους ψηφιακούς πόρους. Στον πυρήνα του, το υπολογιστικό νέφος αναφέρεται στην παροχή υπολογιστικών υπηρεσιών - συμπεριλαμβανομένων των διακομιστών, της αποθήκευσης, των βάσεων δεδομένων, της δικτύωσης, του λογισμικού, της ανάλυσης και της νοημοσύνης- μέσω του Διαδικτύου («το νέφος») για να προσφέρει ταχύτερη καινοτομία, ευέλικτους πόρους και οικονομίες κλίμακας. Η έλευση του cloud computing επέτρεψε στους οργανισμούς να αποφύγουν το αρχικό κόστος και την πολυπλοκότητα της ιδιοκτησίας και της συντήρησης της υποδομής πληροφορικής τους. Αντ' αυτού, μπορούν απλώς να πληρώνουν για ό,τι χρησιμοποιούν, όταν το χρησιμοποιούν.

΄Ολα τα νέφη, έχουν διαφορετικά χαρακτηριστικά, όπως χωρητικότητα αποθήκευσης, συστήματα χρέωσης και διαφορετικές μεθόδους παροχής των υπηρεσιών άλλων νέφων. Το βασικό πρόβλημα είναι ότι οι άνθρωποι δεν γνωρίζουν ποιο σύννεφο είναι κατάλληλο σύμφωνα με τις απαιτήσεις τους- δεν μπορούν να επιλέξουν το κατάλληλο σύννεφο για τις υπηρεσίες τους μεταξύ των διαφορετικών σύννεφων που διαχειρίζονται διάφοροι πάροχοι σύννεφων. Έτσι, για να διευκολύνει τέτοιου είδους καταστάσεις, το παρόν έγγραφο βοηθά στον καθορισμό της σύγκρισης ορισμένων από τα πιο δημοφιλή νέφη.

Σκοπός και στόχοι

Ο πρωταρχικός σκοπός της παρούσας εργασίας είναι να εμβαθύνει στις πολυπλοκότητες και τις προκλήσεις που σχετίζονται με το cloud computing, εστιάζοντας ιδιαίτερα στις πτυχές της ασφάλειας. Καθώς η υιοθέτηση του υπολογιστικού νέφους συνεχίζει να αυξάνεται, αυξάνεται και η σημασία των ισχυρών μέτρων κυβερνοασφάλειας για την προστασία των ευαίσθητων δεδομένων και τη διασφάλιση της αξιοπιστίας των υπηρεσιών. Η παρούσα εργασία έχει ως στόχο:

1. Να παρέχει επισκόπηση του υπολογιστικού νέφους καθώς και έναν ολοκληρωμένο ορισμό.
2. Να διερευνήσει τους διαφορετικούς τύπους μοντέλων ανάπτυξης υπολογιστικού νέφους και τα αντίστοιχα οφέλη και προκλήσεις.
3. Να αναδείξει την κρίσιμη σημασία της κυβερνοασφάλειας σε περιβάλλοντα νέφους.

4. Να προσδιορίσει και να αναλύσει τις επικρατούσες προκλήσεις ασφάλειας στο υπολογιστικό νέφος, συμπεριλαμβανομένων των παραβιάσεων δεδομένων, των απειλών εκ των έσω και των ζητημάτων συμμόρφωσης.

5. Να εξετάσει το ρόλο των προτύπων ISO 27017 και ISO 27018 στην ενίσχυση της ασφάλειας και της ιδιωτικότητας στο υπολογιστικό νέφος.

6. Να σκιαγραφίσει τα βασικά στοιχεία που είναι απαραίτητα για τη διασφάλιση της ασφάλειας στο υπολογιστικό νέφος, όπως η διαχείριση ταυτότητας και πρόσβασης (IAM), η κρυπτογράφηση, η ασφάλεια δικτύου, η παρακολούθηση της ασφάλειας και η αντιμετώπιση περιστατικών.

7. Να προσφέρει συγκριτική ανάλυση των κυριότερων παρόχων υπηρεσιών cloud - Amazon Web Services (AWS), Microsoft Azure και Google Cloud Platform (GCP) - για να κατανοήθούν οι μοναδικές προσφορές και δυνατότητες ασφαλείας τους.

Μεθοδολογία

Για την επίτευξη αυτών των στόχων, υιοθετείται μια συστηματική προσέγγιση που περιλάμβανε ενδελεχή επισκόπηση της υπάρχουσας βιβλιογραφίας, των προτύπων και των βέλτιστων πρακτικών που σχετίζονται με την ασφάλεια του νέφους. Η μεθοδολογία περιελάμβανε:

1. **Βιβλιογραφική ανασκόπηση**: Πραγματοποιείται εκτενής έρευνα σε επιστημονικά άρθρα, κλαδικές εκθέσεις και “white papers” για τη συλλογή σχετικών δεδομένων σχετικά με το υπολογιστικό νέφος και τις προκλήσεις της κυβερνοασφάλειας.

2. **Ανάλυση προτύπων**: Πραγματοποιείται λεπτομερής εξέταση των προτύπων ISO 27017 και ISO 27018 (Το ISO 27017 συμβουλεύει την διαχείριση ασφάλειας για υπηρεσίες cloud καθώς και το ISO27018 είναι ένα διεθνές πρότυπο που δημιουργήθηκε ειδικά για το απόρρητο των δεδομένων στο cloud computing) για την κατανόηση των κατευθυντήριων γραμμών και των επιπτώσεών τους για την ασφάλεια του υπολογιστικού νέφους.

3. **Συγκριτική ανάλυση**: Συγκρίνονται τα χαρακτηριστικά ασφαλείας και τα μέτρα συμμόρφωσης των κορυφαίων παρόχων υπηρεσιών cloud (AWS, Azure, GCP) για τον εντοπισμό των δυνατών σημείων και των ελλείψεων.

4. **Μελέτες περιπτώσεων**: Αναλύονται παραδείγματα και μελέτες περιπτώσεων από τον πραγματικό κόσμο για να καταδειχθεί η εφαρμογή των πρακτικών ασφαλείας και ο αντίκτυπος των παραβιάσεων σε περιβάλλοντα νέφους.

Αποτελέσματα

Η μελέτη απέδωσε σημαντικές γνώσεις σχετικά με την πολύπλευρη φύση της ασφάλειας του νέφους. Τα βασικά ευρήματα περιλαμβάνουν:

1. **Παραβιάσεις και διαρροές δεδομένων**: Παραμένουν οι πιο διαδεδομένες και επιζήμιες απειλές ασφάλειας σε περιβάλλοντα νέφους. Οι λανθασμένες ρυθμίσεις και η έλλειψη ισχυρής κρυπτογράφησης αποτελούν πρωταρχικές αιτίες.
2. **Απειλές εκ των έσω**: Οι εσωτερικοί χρήστες, είτε κακόβουλοι είτε αμελείς, αποτελούν σημαντικό κίνδυνο για την ασφάλεια του νέφους. Η αποτελεσματική παρακολούθηση και οι αυστηροί έλεγχοι πρόσβασης είναι ζωτικής σημασίας για τον μετριασμό αυτού του κινδύνου.
3. **Μοντέλο κοινής ευθύνης**: Η οριοθέτηση των ευθυνών ασφάλειας μεταξύ των παρόχων cloud και των πελατών είναι απαραίτητη. Οι παρεξηγήσεις σε αυτό το μοντέλο μπορεί να οδηγήσουν σε παραλείψεις που έχουν αντίκτυπο στην ασφάλεια των πληροφοριών.
4. **Συμμόρφωση και ρυθμιστικά ζητήματα**: Η τήρηση των κανονιστικών απαιτήσεων, όπως ο GDPR, το HIPAA και τα ειδικά βιομηχανικά πρότυπα, είναι ζωτικής σημασίας για τη διατήρηση της ασφάλειας του cloud και την αποφυγή νομικών κυρώσεων.
5. **Συμμόρφωση με πρότυπα ISO**: Τα πρότυπα ISO 27017 και ISO 27018 παρέχουν ολοκληρωμένες κατευθυντήριες γραμμές για την ασφάλεια και την προστασία της ιδιωτικότητας των χρηστών στο cloud, προωθώντας τις βέλτιστες πρακτικές και βοηθώντας τους οργανισμούς να επιτύχουν συμμόρφωση.
6. **Βασικά στοιχεία ασφαλείας**: Η αποτελεσματική ασφάλεια του cloud εξαρτάται από έναν συνδυασμό IAM, κρυπτογράφησης, ασφάλειας δικτύου, συνεχούς παρακολούθησης και ισχυρών στρατηγικών αντιμετώπισης περιστατικών.

Δομή της εργασίας

Η παρούσα εργασία είναι δομημένη έτσι ώστε να παρέχει μια λογική και ολοκληρωμένη διερεύνηση της ασφάλειας του νέφους:

1. **Εισαγωγή στο υπολογιστικό νέφος**: Αυτή η ενότητα θέτει τα θεμέλια με τον ορισμό του υπολογιστικού νέφους και τη συζήτηση των διαφόρων μοντέλων ανάπτυξης νέφους (δημόσιο, ιδιωτικό, υβριδικό και πολλαπλό νέφος). Υπογραμμίζει επίσης την κρίσιμη σημασία της ασφάλειας στον κυβερνοχώρο σε περιβάλλοντα νέφους.

2. **Προκλήσεις ασφάλειας στο υπολογιστικό νέφος**: Αυτή η ενότητα εμβαθύνει στις πρωταρχικές προκλήσεις ασφαλείας που αντιμετωπίζει το υπολογιστικό νέφος. Καλύπτει τις παραβιάσεις και διαρροές δεδομένων, τις εσωτερικές απειλές, το μοντέλο κοινής ευθύνης και τα ζητήματα συμμόρφωσης και κανονιστικών ρυθμίσεων.

3. **Πρότυπα ISO 27017 & 27018**: Στην ενότητα αυτή αρχικά περιγράφονται τα πρότυπα ISO 27017 (ασφάλεια υπολογιστικού νέφους) και ISO 27018 (προστασία της ιδιωτικής ζωής στο υπολογιστικό νέφος). Κατόπιν συζητείται η σημασία αυτών των προτύπων, οι κατευθυντήριες γραμμές τους και τα οφέλη της συμμόρφωσης για την ασφάλεια του νέφους.

4. **Βασικά στοιχεία της ασφάλειας του νέφους**: Στην ενότητα αυτή περιγράφονται τα βασικά στοιχεία της ασφάλειας του νέφους. Καλύπτει τη διαχείριση ταυτότητας και πρόσβασης (IAM), την κρυπτογράφηση και τη διαχείριση κλειδιών, την ασφάλεια δικτύου, την παρακολούθηση και καταγραφή της ασφάλειας, καθώς και την αντιμετώπιση και αποκατάσταση περιστατικών.

5. **Ειδικό τμήμα - Σύγκριση των κυριότερων παρόχων υπηρεσιών νέφους**: Αυτή η ενότητα προσφέρει μια συγκριτική ανάλυση των μέτρων ασφαλείας που εφαρμόζουν οι κυριότεροι πάροχοι υπηρεσιών cloud - Amazon Web Services (AWS), Microsoft Azure και Google Cloud Platform (GCP). Επισημαίνει τα μοναδικά χαρακτηριστικά και τις πρακτικές ασφαλείας τους.

6. **Συμπεράσματα**: Η τελευταία ενότητα συνοψίζει τα βασικά ευρήματα, συζητά τις επιπτώσεις για τους οργανισμούς που χρησιμοποιούν ή εξετάζουν το ενδεχόμενο παροχής υπηρεσιών cloud και προσφέρει συστάσεις για την ενίσχυση της ασφάλειας του cloud.

2. Προκλήσεις ασφάλειας στο υπολογιστικό νέφος

Το υπολογιστικό νέφος (cloud computing) αποτελεί μια καινοτόμο τεχνολογία που έχει επαναπροσδιορίσει τον τρόπο με τον οποίο οι οργανισμοί διαχειρίζονται τις υποδομές πληροφορικής, αποθηκεύουν δεδομένα και προσφέρουν υπηρεσίες μέσω των παρόχων. Βασισμένο σε αρχές όπως η επεκτασιμότητα, η εικονικοποίηση και η αυτοματοποίηση, το υπολογιστικό νέφος επιτρέπει την αποδοτική χρήση των πόρων και την ταχύτερη υλοποίηση εφαρμογών. Ωστόσο, η εξάρτηση από διαδικτυακές πλατφόρμες και η φύση της κατανεμημένης αρχιτεκτονικής του δημιουργούν σημαντικές προκλήσεις ασφάλειας.

Η παρούσα ανάλυση διερευνά τις θεμελιώδεις αρχές και τα χαρακτηριστικά του υπολογιστικού νέφους, ενώ εστιάζει στις προκλήσεις που σχετίζονται με την ασφάλεια δεδομένων, τις παραβιάσεις συστημάτων και την εφαρμογή του μοντέλου κοινής ευθύνης. Ιδιαίτερη έμφαση δίνεται στις μορφές απειλών, όπως οι επιθέσεις εκ των έσω και οι τρωτότητες της υποδομής, καθώς και στις στρατηγικές διαχείρισης που μπορούν να μετριάσουν τους κινδύνους. Τέλος, εξετάζονται ζητήματα συμμόρφωσης με διεθνείς κανονισμούς, όπως ο GDPR και το PCI DSS, τονίζοντας τη σημασία της προσαρμογής στις απαιτήσεις ενός σύνθετου και συνεχώς εξελισσόμενου περιβάλλοντος.

2.1 Ορισμός του cloud computing

Παρά το γεγονός ότι το υπολογιστικό νέφος αποτελεί μια καθιερωμένη τεχνολογία εδώ και πολλά χρόνια, η ανάλυση του ορισμού και των βασικών αρχών του παραμένει απαραίτητη. Αυτό συμβαίνει διότι οι εξελίξεις στις εφαρμογές, τα μοντέλα ανάπτυξης και τις απαιτήσεις ασφάλειας συνεχώς μεταβάλλουν το πεδίο. Η σαφής κατανόηση του τι συνιστά το cloud computing θέτει τα θεμέλια για την αξιολόγηση των πλεονεκτημάτων του, αλλά και των προκλήσεων που αντιμετωπίζουν οι οργανισμοί, ειδικά σε τομείς όπως η ασφάλεια, η συμμόρφωση και η ευελιξία. Επιπλέον, η πολυπλοκότητα των υβριδικών μοντέλων και των εξειδικευμένων υπηρεσιών ενισχύει την ανάγκη για συστηματική αναφορά στον ορισμό, ως βάση για τη μελέτη και τη συζήτηση πιο σύνθετων ζητημάτων.

Θεμελιώδεις αρχές του υπολογιστικού νέφους:

Αυτοεξυπηρέτηση κατά παραγγελία: Το υπολογιστικό νέφος επιτρέπει στους χρήστες να παρέχουν υπολογιστικούς πόρους, όπως αποθήκευση, επεξεργαστική ισχύ και εύρος ζώνης δικτύου, χωρίς ανθρώπινη παρέμβαση από τον πάροχο υπηρεσιών (Patel & Kansara, 2021).

Ευρεία πρόσβαση στο δίκτυο: Οι υπηρεσίες υπολογιστικού νέφους είναι προσβάσιμες μέσω του διαδικτύου από διάφορες συσκευές με τυποποιημένα πρωτόκολλα, προωθώντας την πανταχού παρούσα πρόσβαση και ευελιξία (Marinescu, 2022).

Συγκέντρωση πόρων: Οι πόροι συγκεντρώνονται για την εξυπηρέτηση πολλαπλών χρηστών, επιτρέποντας τη δυναμική κατανομή και την αποτελεσματική χρήση των υπολογιστικών πόρων.

Ταχεία ελαστικότητα: Οι πόροι του νέφους μπορούν να παρέχονται και να αποδεσμεύονται ταχέως για να ανταποκρίνονται στις κυμαινόμενες απαιτήσεις, εξασφαλίζοντας επεκτασιμότητα και βέλτιστη απόδοση (Sadeeq et al., 2021).

Μετρούμενη υπηρεσία: Η χρήση του νέφους παρακολουθείται, ελέγχεται και μετράται, επιτρέποντας στους χρήστες να πληρώνουν μόνο για τους πόρους που καταναλώνουν, παρόμοια με τα μοντέλα χρέωσης υπηρεσιών κοινής ωφέλειας.

Βασικά χαρακτηριστικά του Cloud Computing:

Επεκτασιμότητα: Τα περιβάλλοντα υπολογιστικού νέφους μπορούν να κλιμακώσουν απρόσκοπτα τους πόρους προς τα πάνω ή προς τα κάτω ανάλογα με τη ζήτηση, επιτρέποντας στις επιχειρήσεις να διαχειρίζονται αποτελεσματικά τα φορτία αιχμής χωρίς υπερπρομήθεια υλικού (Gai et al., 2020).

Εικονικοποίηση: Οι τεχνολογίες εικονικοποίησης μπορούν να αφαιρέσουν τους υποκείμενους πόρους υλικού, επιτρέποντας την εκτέλεση πολλαπλών εικονικών μηχανών σε έναν μόνο φυσικό διακομιστή, βελτιστοποιώντας τη χρήση των πόρων.

Ανοχή σφαλμάτων και αξιοπιστία: Οι πάροχοι υπηρεσιών νέφους εφαρμόζουν τεχνικές πλεονάζουσας υποδομής και αντιγραφής δεδομένων για να εξασφαλίζουν υψηλή διαθεσιμότητα και ανθεκτικότητα των δεδομένων (Bello et al., 2021).

Ασφάλεια: Οι πλατφόρμες νέφους εφαρμόζουν ισχυρά μέτρα ασφαλείας, όπως κρυπτογράφηση, ελέγχους πρόσβασης και πιστοποιήσεις συμμόρφωσης, για την προστασία των δεδομένων και των εφαρμογών από μη εξουσιοδοτημένη πρόσβαση και απειλές στον κυβερνοχώρο (Alam, 2020).

Αυτοματοποίηση: Οι υπηρεσίες νέφους αξιοποιούν εργαλεία αυτοματοποίησης και API για τον εξορθολογισμό των εργασιών παροχής, διαμόρφωσης και διαχείρισης, ενισχύοντας τη λειτουργική αποδοτικότητα και μειώνοντας τα σφάλματα που προκύπτουν

από διεργασίες που πραγματοποιούνται με ανθρώπινη παρέμβαση. Η αυτοματοποίηση παίζει καθοριστικό ρόλο στην ενίσχυση της λειτουργικής αποδοτικότητας των υπηρεσιών νέφους. Με την αξιοποίηση εργαλείων αυτοματοποίησης και API, οι πάροχοι υπηρεσιών cloud βελτιώνουν την παροχή, τη διαμόρφωση και τη διαχείριση των πόρων, μειώνοντας σημαντικά τα χειροκίνητα σφάλματα και τις διοικητικές δαπάνες.

Ένα από τα κύρια οφέλη της αυτοματοποίησης σε περιβάλλοντα νέφους είναι η αυτοματοποιημένη παροχή και ανάπτυξη πόρων. Εργαλεία όπως το AWS CloudFormation, το Azure Resource Manager και το Terraform επιτρέπουν την υποδομή ως κώδικα (IaC), επιτρέποντας στους οργανισμούς να ορίζουν και να διαχειρίζονται την υποδομή τους μέσω κώδικα. Αυτή η προσέγγιση εξασφαλίζει τη συνοχή σε όλα τα περιβάλλοντα, διευκολύνει τον έλεγχο εκδόσεων και επιταχύνει τη διαδικασία ανάπτυξης. Αντί να ρυθμίζονται χειροκίνητα οι διακομιστές, η αποθήκευση και τα στοιχεία δικτύωσης, αυτοί οι πόροι μπορούν να παρέχονται και να ρυθμίζονται αυτόματα, εξοικονομώντας πολύτιμο χρόνο και ελαχιστοποιώντας τον κίνδυνο ανθρώπινου λάθους.

Η διαχείριση παραμέτρων είναι ένας άλλος κρίσιμος τομέας όπου η αυτοματοποίηση έχει ουσιαστικό αντίκτυπο. Εργαλεία όπως το Ansible, το Puppet και το Chef αυτοματοποιούν τη διαμόρφωση και τη συντήρηση περιβαλλόντων λογισμικού. Αυτά τα εργαλεία διασφαλίζουν ότι τα συστήματα διαμορφώνονται σύμφωνα με προκαθορισμένα πρότυπα και πολιτικές, ενισχύοντας την ασφάλεια και τη συμμόρφωση. Για παράδειγμα, τα αυτοματοποιημένα σενάρια μπορούν να επιβάλλουν διαμορφώσεις ασφαλείας, να εφαρμόζουν τα απαραίτητα διορθωτικά στοιχεία και να διατηρούν τη συνέπεια του συστήματος σε αναπτύξεις μεγάλης κλίμακας.

Η επιχειρησιακή αποδοτικότητα ενισχύεται περαιτέρω μέσω χαρακτηριστικών όπως η αυτόματη κλιμάκωση και η αυτοματοποιημένη παρακολούθηση. Οι δυνατότητες αυτόματης κλιμάκωσης, που είναι διαθέσιμες σε πλατφόρμες όπως το AWS, το Azure και το Google Cloud, προσαρμόζουν αυτόματα τον αριθμό των υπολογιστικών πόρων ανάλογα με τη ζήτηση. Αυτό εξασφαλίζει βέλτιστη απόδοση κατά τη διάρκεια των περιόδων αιχμής και εξοικονόμηση κόστους κατά τις περιόδους χαμηλής χρήσης. Τα εργαλεία αυτοματοποιημένης παρακολούθησης, όπως το AWS CloudWatch και το Azure Monitor, παρέχουν πληροφορίες σε πραγματικό χρόνο σχετικά με την απόδοση του συστήματος, ενεργοποιώντας ειδοποιήσεις και ακόμη και αυτοματοποιημένες ενέργειες αποκατάστασης για την προληπτική αντιμετώπιση προβλημάτων.

Η εφαρμογή του υπολογιστικού νέφους είναι η διαδικασία δημιουργίας ενός εικονικού υπολογιστικού περιβάλλοντος. Η ανάπτυξη στο νέφος παρέχει στους οργανισμούς ευέλικτους και κλιμακούμενους εικονικούς υπολογιστικούς πόρους. Το μοντέλο ανάπτυξης νέφους είναι ο τύπος αρχιτεκτονικής στον οποίο αναπτύσσεται ένα σύστημα νέφους. Τα μοντέλα αυτά διαφέρουν ως προς τη διαχείριση, την ιδιοκτησία, τον έλεγχο πρόσβασης και τα πρωτόκολλα ασφαλείας (Sandhu, 2021). Τα μοντέλα ανάπτυξης νέφους, που περιλαμβάνουν δημόσια, ιδιωτικά και υβριδικά νέφη, επηρεάζουν σημαντικά τη διαχείριση, την ιδιοκτησία, τον έλεγχο πρόσβασης και τα πρωτόκολλα ασφαλείας του εικονικού υπολογιστικού περιβάλλοντος ενός οργανισμού. Σε ένα δημόσιο νέφος, η διαχείριση των πόρων γίνεται από έναν τρίτο πάροχο, ο οποίος αναλαμβάνει όλη τη συντήρηση, τις αναβαθμίσεις και την ασφάλεια. Αυτό το μοντέλο προσφέρει οικονομικά αποδοτική επεκτασιμότητα, καθώς οι οργανισμοί πληρώνουν μόνο για ό,τι χρησιμοποιούν, ενώ μοιράζονται την υποδομή με άλλους μισθωτές, γεγονός που μπορεί να περιορίσει τον έλεγχο του υποκείμενου υλικού και λογισμικού. Η ιδιοκτησία παραμένει στον πάροχο υπηρεσιών νέφους (CSP), παρέχοντας χαμηλότερο κόστος εισόδου και συντήρησης, αλλά λιγότερη προσαρμογή και έλεγχο για τον οργανισμό (Sandhu, 2021).

Αντίθετα, τα ιδιωτικά νέφη προσφέρουν αποκλειστικούς πόρους των οποίων η διαχείριση πραγματοποιείται είτε εσωτερικά από την ομάδα πληροφορικής ενός οργανισμού είτε από έναν τρίτο πάροχο. Αυτό το μοντέλο παρέχει αυξημένο έλεγχο, προσαρμογή και συμμόρφωση με συγκεκριμένες κανονιστικές απαιτήσεις, αν και με υψηλότερο κόστος λόγω της αποκλειστικής χρήσης της υποδομής. Ο οργανισμός ή ένας αποκλειστικός πάροχος διατηρεί την κυριότητα, επιτρέποντας προσαρμοσμένα πρωτόκολλα ασφαλείας και πρακτικές διαχείρισης που ευθυγραμμίζονται με τις συγκεκριμένες ανάγκες του οργανισμού.

Τα υβριδικά νέφη συγχωνεύουν το δημόσιο και το ιδιωτικό μοντέλο, επιτρέποντας τη μετακίνηση δεδομένων και εφαρμογών μεταξύ τους ανάλογα με τις ανάγκες. Αυτή η ευελιξία επιτρέπει στους οργανισμούς να αξιοποιούν την αποδοτικότητα κόστους και την επεκτασιμότητα των δημόσιων clouds για μη ευαίσθητες λειτουργίες όπως είναι η διαχείριση προσωπικών δεδομένων πελατών, διατηρώντας παράλληλα κρίσιμα φορτία εργασίας σε ένα ιδιωτικό cloud. Οι αρμοδιότητες διαχείρισης σε ένα υβριδικό μοντέλο μοιράζονται μεταξύ του CSP και του οργανισμού, προσφέροντας μια ισορροπημένη προσέγγιση ελέγχου και ευελιξίας. Η ιδιοκτησία είναι επίσης μοιρασμένη, με τον οργανισμό να διατηρεί τον έλεγχο των ιδιωτικών πόρων και τον CSP να διαχειρίζεται τα δημόσια στοιχεία (Sandhu, 2021).

Η ζήτηση για υπολογιστικό νέφος έχει οδηγήσει σε διαφορετικούς τύπους μοντέλων ανάπτυξης υπολογιστικού νέφους. Το υπολογιστικό νέφος είναι επίσης γνωστό ως η πέμπτη χρησιμότητα (μαζί με το νερό, το ηλεκτρικό ρεύμα, το φυσικό αέριο και το τηλέφωνο) που είναι διαθέσιμη βάσει της ζήτησης των χρηστών. Το υπολογιστικό νέφος βασίζεται στο μοντέλο πληρωμής ανά χρήση. Σε αυτό, ένα μοντέλο υπολογιστικού νέφους παρέχει μια διαδικτυακή υπολογιστική υπηρεσία κατά παραγγελία, όπως απαιτείται από τον χρήστη. Με όλες τις νέες επιλογές υπολογιστικού νέφους και τη φράση "ως υπηρεσία" που φαίνεται να προστίθεται σε οτιδήποτε μπορεί να φανταστεί κανείς, βοηθάει να κάνουμε ένα βήμα πίσω και να εξετάσουμε τις διαφορές μεταξύ των κύριων τύπων ανάπτυξης υπολογιστικού νέφους και των διαφορετικών τύπων υπηρεσιών. Η ανάπτυξη νέφους περιγράφει τον τρόπο με τον οποίο αναπτύσσεται μια πλατφόρμα νέφους, πώς φιλοξενείται και ποιος έχει πρόσβαση σε αυτήν. Όλα τα μοντέλα ανάπτυξης υπολογιστικού νέφους λειτουργούν με βάση την ίδια αρχή, εικονικοποιώντας την υπολογιστική ισχύ των διακομιστών σε τμηματοποιημένες, καθοδηγούμενες από λογισμικό εφαρμογές που παρέχουν δυνατότητες υπολογισμού και αποθήκευσης (Alouffi et al., 2021).

Εν συντομία, η παρούσα εργασία παρουσιάζει μια ολοκληρωμένη ανάλυση του υπολογιστικού νέφους, εξηγώντας τις υπηρεσίες και τα μοντέλα ανάπτυξής του, προσδιορίζοντας διάφορα χαρακτηριστικά που παρουσιάζουν ενδιαφέρον και συγκρίνοντας τα με διαφορετικά μοντέλα ανάπτυξης (Butt et al., 2020) προκειμένου να κατανοήσουμε εις βάθος τα ζητήματα ασφάλειας πληροφοριών που προκύπτουν σε κάθε υπηρεσία και μοντέλο cloud computing.

2.2 Τύποι μοντέλων ανάπτυξης νέφους

Υπάρχουν έξι τύποι μοντέλων ανάπτυξης νέφους, από τους οποίους οι πέντε είναι οι κυριότεροι: Ιδιωτικό νέφος, δημόσιο νέφος, υβριδικό νέφος, κοινοτικό νέφος, εικονικό ιδιωτικό νέφος. Το Inter-Cloud είναι επίσης ένας τύπος μοντέλων ανάπτυξης και έχει δύο τύπους σύννεφων: Ομαδοποιημένα νέφη, πολλαπλά νέφη.

A. Ιδιωτικό νέφος

Το μοντέλο ανάπτυξης ιδιωτικού νέφους ονομάζεται επίσης εσωτερικό ή εταιρικό μοντέλο. Ένα ιδιωτικό νέφος ανήκει σε έναν συγκεκριμένο οργανισμό. Ο εν λόγω οργανισμός ελέγχει το σύστημα και το διαχειρίζεται κεντρικά, ενώ ένα τρίτο μέρος (για παράδειγμα, ένας πάροχος υπηρεσιών) μπορεί να φιλοξενήσει έναν ιδιωτικό διακομιστή νέφους. Οι περισσότερες εταιρείες επιλέγουν να διατηρούν το υλικό στο τοπικό τους κέντρο δεδομένων.

Από εκεί, μια εσωτερική ομάδα μπορεί να επιβλέπει και να διαχειρίζεται τα πάντα (Ibrahim, 2021).

Β. Δημόσιο υπολογιστικό νέφος

Τα δημόσια νέφη συνιστώνται για την ανάπτυξη λογισμικού και συνεργατικά έργα. Ο πάροχος υπηρεσιών κατέχει και λειτουργεί όλο το υλικό που είναι απαραίτητο για τη λειτουργία ενός δημόσιου νέφους. Οι προμηθευτές διατηρούν τις συσκευές σε τεράστια κέντρα δεδομένων. Το μοντέλο παροχής δημόσιου νέφους παίζει σημαντικό ρόλο στην ανάπτυξη και τις δοκιμές. Οι προγραμματιστές χρησιμοποιούν συχνά υποδομές δημόσιου νέφους για σκοπούς ανάπτυξης και δοκιμών. Το εικονικό του περιβάλλον είναι φθηνό και μπορεί να διαμορφωθεί εύκολα και να αναπτυχθεί γρήγορα, γεγονός που το καθιστά ιδανικό για περιβάλλοντα δοκιμών (Shafiq et al., 2022).

Γ. Υβριδικό νέφος

Τα υβριδικά νέφη συνδυάζουν δημόσια νέφη με ιδιωτικά νέφη. Είναι σχεδιασμένα έτσι ώστε τα δεδομένα και οι εφαρμογές να κινούνται ομαλά μεταξύ τους και οι δύο πλατφόρμες να αλληλεπιδρούν ομαλά. Είναι η ιδανική λύση για μια επιχείρηση ή έναν οργανισμό που χρειάζεται λίγο και από τα δύο, τα οποία γενικά εξαρτώνται από τον κλάδο και το μέγεθος. Στην ουσία, ένα υβριδικό νέφος ξεκινά γενικά ως ιδιωτικό νέφος, το οποίο στη συνέχεια επεκτείνει την ενσωμάτωση ώστε να χρησιμοποιεί μία ή περισσότερες υπηρεσίες δημόσιου νέφους. Αυτό το μοντέλο ανάπτυξης έχει νόημα όταν οι εταιρείες έχουν ευαίσθητα δεδομένα που δεν μπορούν να αποθηκευτούν στο cloud ή κανονιστικές απαιτήσεις που απαιτούν προστασία δεδομένων, αποθήκευση και άλλα (Pallathadka et al., 2022).

Δ. Κοινοτικό νέφος

Το κοινοτικό νέφος είναι μια υπηρεσία νέφους που παρέχει υπηρεσίες σε μια κοινότητα χρηστών ή οργανισμών με κοινά ενδιαφέροντα ή ανησυχίες. Οι οργανισμοί που χρησιμοποιούν αυτή την υπηρεσία νέφους έχουν κοινές αποστολές, διακυβέρνηση, απαιτήσεις ασφαλείας και πολιτικές. Οι υπηρεσίες νέφους μπορούν να φιλοξενούνται στις εγκαταστάσεις του οργανισμού-καταναλωτή, στις εγκαταστάσεις του ομότιμου οργανισμού, σε έναν πάροχο ή σε συνδυασμό αυτών. Αυτός ο όρος του κοινοτικού νέφους χρησιμοποιείται συχνά στο μάρκετινγκ για να εξηγήσει τους καταναλωτές-στόχους της υπηρεσίας, αν και το πραγματικό νέφος θα μπορούσε τεχνικά να είναι ένα μοντέλο εικονικού ιδιωτικού νέφους (Virtual Private Cloud–VPC, ιδιωτικό ή υβριδικό νέφος (Pallathadka et al., 2022)).

Ε. Εικονικό ιδιωτικό νέφος (VPC)

Το εικονικό ιδιωτικό νέφος (VPC) είναι ένα ιδιωτικό περιβάλλον υπολογιστικού νέφους το οποίο βρίσκεται εντός ενός δημόσιου νέφους. Ουσιαστικά, ένα VPC προβλέπει λογικά απομονωμένα τμήματα ενός δημόσιου νέφους για την παροχή ενός εικονικού ιδιωτικού περιβάλλοντος. Όπως όλα τα περιβάλλοντα νέφους, οι πόροι VPC είναι διαθέσιμοι κατά ζήτηση για να κλιμακώνονται ανάλογα με τις ανάγκες και είναι εξαιρετικά διαμορφώσιμοι. Αυτή η υλοποίηση αποτελεί συμβιβασμό μεταξύ ενός δημόσιου και ενός ιδιωτικού μοντέλου όσον αφορά την τιμή και τα χαρακτηριστικά.

Στ. Inter-Clouds

Το inter-cloud είναι ένας όρος που αναφέρεται σε ένα θεωρητικό μοντέλο για υπηρεσίες υπολογιστικού νέφους που βασίζεται στην ιδέα του συνδυασμού πολλών διαφορετικών μεμονωμένων σύννεφων σε μια απρόσκοπτη μάζα όσον αφορά τις λειτουργίες κατά παραγγελία. Το inter-cloud θα εξασφάλιζε απλώς ότι ένα νέφος θα μπορούσε να χρησιμοποιεί πόρους πέραν της εμβέλειάς του, εκμεταλλευόμενο τις προϋπάρχουσες συμβάσεις με άλλους παρόχους νέφους (Pallathadka et al., 2022). Υπάρχουν κυρίως δύο τύποι Inter-cloud, το πολλαπλό (Multi-cloud) και το ομοσπονδιακό:

- Πολλαπλό σύννεφο

Το Πολλαπλό σύννεφο (Multi-cloud) είναι η χρήση δύο ή περισσότερων υπηρεσιών υπολογιστικού νέφους από διάφορους παρόχους υπολογιστικού νέφους. Ένα περιβάλλον πολλαπλού νέφους μπορεί να είναι εντελώς ιδιωτικό, εντελώς δημόσιο ή ένας συνδυασμός και των δύο. Οι επιχειρήσεις χρησιμοποιούν ένα περιβάλλον πολλαπλού νέφους για να κατανέμουν τους υπολογιστικούς πόρους και να μειώνουν τον κίνδυνο διακοπής λειτουργίας και απώλειας δεδομένων. Μπορούν επίσης να αυξήσουν την υπολογιστική ισχύ και τον αποθηκευτικό χώρο που διαθέτουν οι επιχειρήσεις. Οι καινοτομίες του νέφους τα τελευταία χρόνια οδήγησαν σε μια στροφή από τα ιδιωτικά νέφη ενός χρήστη σε δημόσια νέφη πολλαπλών μισθωτών και υβριδικά νέφη (Tabrizchi & Kuchaki, 2020).

- Ομοσπονδιακό σύννεφο

Το ομοσπονδιακό νέφος ονομάζεται επίσης ομοσπονδία νέφους, η οποία διαχειρίζεται πολλαπλές εσωτερικές και εξωτερικές υπηρεσίες υπολογιστικού νέφους για την κάλυψη των επιχειρηματικών αναγκών. Μια ομοσπονδία είναι η ένωση πολλών μικρότερων μερών που εκτελούν μια κοινή δράση (Gai et al., 2020).

2.3 Fog computing, μοντέλα Markov και Honeypots

Με την αύξηση των έξυπνων εφαρμογών και την απαίτηση να μειωθεί η καθυστέρηση μεταξύ του σταδίου παραγωγής και επεξεργασίας δεδομένων, η Cisco δημιούργησε έναν νέο όρο που ονομάζεται υπολογιστική ομίχλη (fog computing). Το fog computing επιτρέπει στις έξυπνες εφαρμογές να εκτελούν την επεξεργασία τους σε συσκευές δικτύου που μπορεί να είναι δρομολογητές, πύλες ή μεταγωγείς αντί να στέλνουν δεδομένα σε κέντρα δεδομένων cloud. Δεν είναι επιθυμητό να εκτελούνται έξυπνες εφαρμογές που είναι ευαίσθητες στην καθυστέρηση (δηλαδή η απόδοσή τους επηρεάζεται από την καθυστέρηση του δικτύου) σε υπολογιστικά κέντρα δεδομένων νέφους για αποτελέσματα σε πραγματικό χρόνο και γρήγορα. Το παράδειγμα της υπολογιστικής ομίχλης προβλέπει τη χρήση αυτών των δικτυακών συσκευών και τη δημιουργία ενός κέντρου δεδομένων για την επεξεργασία έξυπνων εφαρμογών με ευαισθησία στην καθυστέρηση. Σε σύγκριση με την υπολογιστική νέφους, οι συσκευές υπολογιστικής ομίχλης θα παρέχουν μικρότερη καθυστέρηση για την έξυπνη εφαρμογή, ωστόσο δεν είναι δυνατή η απόκτηση υπολογιστικής ισχύος σε σύγκριση με την υπολογιστική νέφους (Sadeeq et al., 2021).

Στην υπολογιστική ομίχλης, για οποιαδήποτε χρονική στιγμή, η ίδια συσκευή άκρου μπορεί να χρησιμοποιηθεί από πολλαπλές έξυπνες εφαρμογές με διαφορετικό σύνολο χρηστών, γεγονός που εγείρει το ζήτημα της ασφάλειας της συσκευής άκρου. Εάν η συσκευή ακραίων σημείων παραβιαστεί, μπορεί να λάβει ψευδή δεδομένα εισόδου και να παράσχει ψευδή δεδομένα εξόδου, να διαμορφώσει κακά αποτελέσματα που μπορεί να επηρεάσουν την απόδοση ολόκληρης της εφαρμογής. Η παραβιασμένη συσκευή μπορεί επίσης να χρησιμοποιηθεί για την ανταλλαγή δεδομένων και αποτελεσμάτων με ανταγωνιστικές εταιρείες ή κακόβουλες ομάδες χρηστών που εμπλέκονται σε ανεπιθύμητες δραστηριότητες. Τα πρωτόκολλα ασφαλείας που χρησιμοποιούνται σήμερα πιστοποιούν την ταυτότητα κάθε συσκευής άκρου με την εφαρμογή πριν από την παροχή δεδομένων ή υπολογισμών προς εκτέλεση. Ωστόσο, εάν η συσκευή που έχει πιστοποιηθεί με τον έλεγχο ταυτότητας παραβιαστεί, τότε η κατάσταση γίνεται ακόμη χειρότερη, επειδή η εν λόγω συσκευή άκρου έχει ορισμένα προνόμια εντός του δικτύου. Έτσι, οι επιθέσεις από συσκευές άκρων στο περιβάλλον υπολογιστών ομίχλης μπορούν να χαρακτηριστούν σε γενικές γραμμές σε δύο κύριες κατηγορίες που είναι: (α) επιθέσεις χωρίς πιστοποίηση και (β) επιθέσεις χωρίς εξουσιοδότηση. Εάν η συσκευή άκρης είναι μη πιστοποιημένη και προσπαθεί να επιτεθεί στο επίπεδο συσκευής ή στο επίπεδο νέφους, τότε αυτή η επίθεση ονομάζεται μη πιστοποιημένη επίθεση ή εξωτερική επίθεση. Αλλά, εάν η συσκευή άκρου που επιτίθεται στο στρώμα

ομίχλης ή στο στρώμα νέφους είναι αυθεντικοποιημένη και βρίσκεται εντός του αξιόπιστου δικτύου της εφαρμογής, τότε ονομάζεται μη εξουσιοδοτημένη ή εσωτερική επίθεση. Οι αυθεντικοποιημένες συσκευές άκρου μπορούν εύκολα να καλύψουν τα ίχνη τους επειδή έχουν ορισμένα προνόμια για να βρίσκονται στο δίκτυο (Marinescu, 2022).

Στο υπολογιστικό νέφος και τη δικτύωση ομίχλης, οι απειλές ασφαλείας κατηγοριοποιούνται με βάση την κατάσταση ελέγχου ταυτότητας της επιτιθέμενης συσκευής. Μια επίθεση χωρίς πιστοποίηση ταυτότητας, γνωστή και ως εξωτερική επίθεση, συμβαίνει όταν μια ακραία συσκευή χωρίς κατάλληλη πιστοποίηση ταυτότητας επιχειρεί να παραβιάσει το επίπεδο συσκευής ή το επίπεδο νέφους. Τέτοιες επιθέσεις εκτελούνται συνήθως από κακόβουλους φορείς εκτός του δικτύου, δημιουργώντας σημαντικούς κινδύνους, καθώς προσπαθούν να εκμεταλλευτούν ευπάθειες για να αποκτήσουν μη εξουσιοδοτημένη πρόσβαση ή να διαταράξουν υπηρεσίες. Αυτές οι επιθέσεις μπορεί να είναι πιο εύκολο να εντοπιστούν και να αμυνθούν εναντίον τους λόγω της έλλειψης νόμιμων διαπιστευτηρίων (Marinescu, 2022).

Αντίθετα, οι εσωτερικές επιθέσεις αφορούν αυθεντικοποιημένες ακραίες συσκευές που αποτελούν μέρος του αξιόπιστου δικτύου. Όταν αυτές οι συσκευές επιτίθενται στο στρώμα ομίχλης ή στο στρώμα νέφους, αξιοποιούν τα νόμιμα προνόμια πρόσβασής τους για τη διεξαγωγή κακόβουλων δραστηριοτήτων. Αυτός ο τύπος επίθεσης είναι πιο ύπουλος και δύσκολο να εντοπιστεί, επειδή ο επιτιθέμενος έχει ήδη εξουσιοδοτημένη πρόσβαση, επιτρέποντάς του να αναμειχθεί με την κανονική κυκλοφορία του δικτύου και να καλύψει αποτελεσματικά τα ίχνη του. Οι εσωτερικές επιθέσεις μπορεί να είναι ιδιαίτερα επιζήμιες, καθώς συχνά παρακάμπτουν τα παραδοσιακά μέτρα ασφαλείας που έχουν σχεδιαστεί για τον αποκλεισμό της μη εξουσιοδοτημένης πρόσβασης (Marinescu, 2022).

Οι αυθεντικοποιημένες ακραίες συσκευές εντός του δικτύου διαθέτουν συγκεκριμένα προνόμια, τα οποία τους επιτρέπουν να εκτελούν ενέργειες που δεν μπορούν να εκτελέσουν μη αυθεντικοποιημένες συσκευές. Αυτή η εγγενής εμπιστοσύνη μπορεί να αξιοποιηθεί, καθιστώντας τις εσωτερικές επιθέσεις ένα κρίσιμο ζήτημα για τα πλαίσια ασφαλείας. Η εφαρμογή αυστηρών μηχανισμών παρακολούθησης και ανίχνευσης ανωμαλιών είναι απαραίτητη για τον εντοπισμό και τον μετριασμό τέτοιων απειλών, διασφαλίζοντας ότι ακόμη και οι αξιόπιστες συσκευές ελέγχονται για ύποπτες δραστηριότητες (Marinescu, 2022).

Η σοβαρότητα της επίθεσης εκ των έσω στο περιβάλλον υπολογιστών ομίχλης είναι επίσης πολύ υψηλή, επειδή οι εφαρμογές που χρησιμοποιούν δεδομένα σε πραγματικό χρόνο έχουν μεγάλη σημασία. Για παράδειγμα, εάν μια εφαρμογή επεξεργάζεται μετεωρολογικά δεδομένα σε πραγματικό χρόνο και προβλέπει πλημμύρες ή άλλες φυσικές καταστροφές, τότε το αποτέλεσμα της τροφοδότησης με ψευδή δεδομένα από επιτιθέμενη συσκευή ακραίων σημείων μπορεί να είναι καταστροφικό. Ως εκ τούτου, υπάρχει άμεση απαίτηση για ένα προληπτικό και προγνωστικό πλαίσιο κυβερνοασφάλειας για την προστασία των υπηρεσιών ομίχλης από κακόβουλες συσκευές ακραίων σημείων. Η προληπτική πρόβλεψη των επιθέσεων κακόβουλων συσκευών άκρου στο σύστημα θα έχει ως αποτέλεσμα την καλύτερη και ασφαλή ανάπτυξη του στρώματος ομίχλης στο περιβάλλον του Διαδικτύου των Πραγμάτων (Patel & Kansara, 2021).

Τα μοντέλα Markov είναι τα στοχαστικά μοντέλα που ικανοποιούν την ιδιότητα Markov, η οποία δηλώνει ότι η πιθανότητα εμφάνισης οποιουδήποτε γεγονότος στο μέλλον εξαρτάται από την παρούσα κατάσταση και όχι από τις παρελθούσες καταστάσεις ενώ, τα κρυφά μοντέλα markov είναι ο τύπος των μοντέλων markov όπου οι ενδιάμεσες καταστάσεις δεν παρατηρούνται ή είναι κρυφές. Τα μοντέλα Markov χρησιμοποιούνται από πολλούς ερευνητές για την ασφάλεια και την αξιολόγηση του δικτύου με βάση τις δραστηριότητες των σημερινών χρηστών. Τα κρυφά μοντέλα markov μπορούν να χρησιμοποιηθούν για την πρόβλεψη της πιθανότητας εμφάνισης κακόβουλης ακραίας συσκευής σε περιβάλλον υπολογιστών ομίχλης με βάση τη δραστηριότητα της συσκευής. Στο πλαίσιο κυβερνοασφάλειας, χρησιμοποιήθηκε μοντέλο κρυμμένου markov δύο σταδίων για την εύρεση της κακόβουλης συσκευής και τη μετατόπισή της στο Virtual Honeypot Cloud (VHD) με βάση τις πρόσφατες δραστηριότητές της. Το Honeypot μπορεί να είναι ένας υπολογιστής, μια εφαρμογή ή δεδομένα που μπορούν να προσομοιώσουν τη συμπεριφορά του πραγματικού συστήματος και να καταγράψουν τη διαδρομή επίθεσης του επιτιθέμενου. Το Honeypot διαφέρει από το σύστημα ανίχνευσης εισβολών (IDS), το σύστημα ανίχνευσης και πρόληψης εισβολών (IDPS) και το τείχος προστασίας υπό την έννοια ότι επιτρέπει στον κακόβουλο χρήστη να επιτεθεί σε μια διαφορετική έκδοση του πραγματικού συστήματος (Sohal et al., 2018).

Η σωστή εγκατάσταση του honeypot μπορεί να οδηγήσει σε πιο αποτελεσματικό και ασφαλές σύστημα, αλλά αν το honeypot είναι στατικό και ο επιτιθέμενος γνωρίζει τη θέση του, τότε η αξία του μειώνεται σε κάποιο βαθμό. Για να γίνει το προτεινόμενο πλαίσιο κυβερνοασφάλειας πιο προσαρμοστικό, έχει προταθεί ένα εικονικό cloud honeypot στο οποίο

η θέση του honeypot αλλάζει δυναμικά, έτσι ώστε η κακόβουλη συσκευή άκρου να μην γνωρίζει ποτέ την ακριβή θέση του. Το VHD θα αποτρέψει την ταυτότητα του honeypot καθώς θα είναι εύκολο να αναπτυχθεί σε σύγκριση με τα παραδοσιακά honeypots. Το VHD θα είναι σαν μια εικόνα εικονικής μηχανής που μπορεί εύκολα να αναπτυχθεί σε οποιοδήποτε διαθέσιμο hypervisor. Με βάση το επίπεδο και τη σοβαρότητα των επιθέσεων, το VHD μπορεί να κλιμακώσει αυτόματα τη χωρητικότητα των πόρων του, γεγονός που το καθιστά πιο προσαρμοστικό σε οποιοδήποτε επίπεδο και αριθμό επιθέσεων από κακόβουλη συσκευή άκρου. Οι επιθέσεις κακόβουλων συσκευών άκρου μπορούν να αποτελέσουν το σημαντικότερο σημείο συμφόρησης σε οποιοδήποτε περιβάλλον υπολογιστών ομίχλης και μπορεί να είναι πιο σοβαρές ανάλογα με τη κρισιμότητα της έξυπνης εφαρμογής (Bello et al., 2021).

Η ασφάλεια του υπολογιστικού νέφους αποτελεί σημαντικό πρόβλημα, παρουσιάζοντας πολλές προκλήσεις που απαιτούν σχολαστική προσοχή. Έρευνες που διεξήγαγε η International Data Corporation (IDC) σε στελέχη πληροφορικής και Chief Information Officers (CIOs) υπογράμμισαν αυτό το ζήτημα, αποκαλύπτοντας ότι η ασφάλεια είναι η πιο συχνά αναφερόμενη πρόκληση στο cloud computing, με το 74% των ερωτηθέντων να την προσδιορίζει ως πρωταρχική ανησυχία. Η έρευνα, η οποία διεξήχθη το 2018, υπογραμμίζει τον κρίσιμο χαρακτήρα της ασφάλειας σε περιβάλλοντα cloud σε σύγκριση με άλλα υπολογιστικά παραδείγματα, όπως το grid computing (Arafat, 2018).

Το Grid computing, γνωστό και ως κατανεμημένος υπολογισμός, περιλαμβάνει ένα δίκτυο υπολογιστών που συνεργάζονται για την εκτέλεση μεγάλων εργασιών, απαιτώντας συχνά ισχυρά και πολύπλοκα μέτρα ασφαλείας. Αντίθετα, η ασφάλεια του υπολογιστικού νέφους θεωρείται απλούστερη αλλά λιγότερο ασφαλής. Αυτή η απλότητα προκύπτει επειδή η ασφάλεια στο υπολογιστικό νέφος τυγχάνει διαχείρισης κυρίως από τον πάροχο υπηρεσιών νέφους (CSP- cloud service provider). Ο CSP είναι υπεύθυνος για την αποθήκευση των δεδομένων και τη διασφάλιση της ασφάλειάς τους, γεγονός που τον επιβαρύνει σημαντικά με την εφαρμογή ισχυρών πρωτοκόλλων ασφαλείας και τη διατήρηση της εμπιστοσύνης με τους πελάτες του.

Η εξάρτηση από τους CSP για την ασφάλεια σημαίνει ότι τυχόν ευπάθειες ή παραβιάσεις στην υποδομή του παρόχου μπορούν να έχουν εκτεταμένες επιπτώσεις. Αυτή η εξάρτηση αναδεικνύει την ανάγκη για αυστηρές πρακτικές ασφάλειας και συνεχή παρακολούθηση για τη διασφάλιση των ευαίσθητων δεδομένων και τη διατήρηση της

ακεραιότητας των υπηρεσιών. Επιπλέον, οι οργανισμοί πρέπει επίσης να υιοθετήσουν ολοκληρωμένες στρατηγικές ασφάλειας, συμπεριλαμβανομένης της κρυπτογράφησης δεδομένων, της διαχείρισης ταυτότητας και πρόσβασης (IAM-identity and access management) και των τακτικών ελέγχων ασφαλείας, για να συμπληρώσουν τα μέτρα που παρέχονται από τους CSP (Arafat, 2018).

2.4 Παραβιάσεις και διαρροές δεδομένων

Το υπολογιστικό νέφος έχει επηρεάσει τον τρόπο με τον οποίο οι οργανισμοί διαχειρίζονται τα δεδομένα και την υποδομή ΤΠ τους. Ωστόσο, με αυτή την ευκολία έρχεται μια πληθώρα προκλήσεων ασφαλείας, και μεταξύ των πιο ανησυχητικών είναι ο κίνδυνος παραβίασης και διαρροής δεδομένων (Arafat, 2018).

Το υπολογιστικό νέφος προσφέρει πολυάριθμα πλεονεκτήματα, όπως επεκτασιμότητα, ευελιξία και οικονομική αποδοτικότητα. Ωστόσο, εισάγει επίσης νέες προκλήσεις ασφαλείας που πρέπει να αντιμετωπίσουν οι οργανισμοί. Οι παραβιάσεις και οι διαρροές δεδομένων αποτελούν σημαντική απειλή για την εμπιστευτικότητα, την ακεραιότητα και τη διαθεσιμότητα των δεδομένων που αποθηκεύονται στο νέφος (Weil, 2018).

Ένας από τους κύριους παράγοντες που συμβάλλουν στις παραβιάσεις δεδομένων στο υπολογιστικό νέφος είναι οι ανεπαρκείς έλεγχοι πρόσβασης. Τα ακατάλληλα διαμορφωμένα δικαιώματα χρήστη και οι αδύναμοι μηχανισμοί ελέγχου ταυτότητας μπορούν να οδηγήσουν σε μη εξουσιοδοτημένη πρόσβαση σε ευαίσθητα δεδομένα. Επιπλέον, η δυναμική φύση των περιβαλλόντων νέφους, όπου οι πόροι παρέχονται και αφαιρούνται κατά παραγγελία, καθιστά δύσκολη τη συνεπή διατήρηση αποτελεσματικών ελέγχων πρόσβασης. Οι εσωτερικές απειλές, είτε σκόπιμες είτε ακούσιες, αποτελούν σημαντικό κίνδυνο για την ασφάλεια του νέφους. Κακόβουλοι εσωτερικοί χρήστες με προνομιακή πρόσβαση μπορούν να κάνουν κατάχρηση των προνομίων τους για να κλέψουν ή να χειραγωγήσουν δεδομένα. Επιπλέον, υπάλληλοι ή τρίτοι πάροχοι υπηρεσιών μπορεί να εκθέσουν ακούσια ευαίσθητες πληροφορίες από αμέλεια ή απροσεξία. Οι απειλές εκ των έσω αναδεικνύουν τη σημασία της εφαρμογής ισχυρών μηχανισμών παρακολούθησης και ελέγχου για τον εντοπισμό ανώμαλης συμπεριφοράς και προσπαθειών μη εξουσιοδοτημένης πρόσβασης (Weil, 2018).

Οι πάροχοι υπολογιστικού νέφους διαχειρίζονται τεράστιες υποδομές που περιλαμβάνουν διακομιστές, δίκτυα και συστήματα αποθήκευσης. Παρά τις προσπάθειές τους για την ασφάλεια αυτών των περιβαλλόντων, τα τρωτά σημεία των υποδομών νέφους

μπορούν να αξιοποιηθούν από επιτιθέμενους για να αποκτήσουν μη εξουσιοδοτημένη πρόσβαση σε δεδομένα. Οι συνήθεις ευπάθειες περιλαμβάνουν λανθασμένες ρυθμίσεις, ελαττώματα λογισμικού και μη ασφαλή API. Οι οργανισμοί πρέπει να επαγρυπνούν και να επιδιορθώνουν ή να μετριάζουν αμέσως τις ευπάθειες για να μειώσουν τον κίνδυνο παραβίασης δεδομένων (Drozdova et al., 2020).

Η ασφάλεια του νέφους λειτουργεί στο πλαίσιο ενός μοντέλου κοινής ευθύνης, όπου τόσο ο πάροχος του νέφους όσο και ο πελάτης είναι υπεύθυνοι για ορισμένες πτυχές της ασφάλειας. Ωστόσο, η οριοθέτηση των αρμοδιοτήτων και η διασφάλιση της συμμόρφωσης με τις βέλτιστες πρακτικές ασφάλειας μπορεί να είναι πολύπλοκη, ιδίως σε περιβάλλοντα πολλαπλών cloud ή υβριδικού cloud. Οι παρεξηγήσεις ή τα κενά στη λογοδοσία μπορούν να οδηγήσουν σε παραλείψεις ασφαλείας και να αυξήσουν την πιθανότητα παραβίασης δεδομένων. Οι παραβιάσεις δεδομένων μπορεί να έχουν σοβαρές συνέπειες για τους οργανισμούς, συμπεριλαμβανομένων οικονομικών απωλειών, ζημιών στη φήμη και νομικών συνεπειών. Η έκθεση ευαίσθητων πληροφοριών πελατών μπορεί να διαβρώσει την εμπιστοσύνη στον οργανισμό, οδηγώντας σε απομάκρυνση πελατών και απώλεια επιχειρηματικών ευκαιριών. Επιπλέον, οι κανονιστικές απαιτήσεις συμμόρφωσης, όπως ο GDPR και ο HIPAA, επιβάλλουν υψηλά πρόστιμα για παραβιάσεις δεδομένων, επιδεινώνοντας περαιτέρω τις οικονομικές επιπτώσεις (Drozdova et al., 2020).

Για να μετριάσουν τον κίνδυνο παραβίασης και διαρροής δεδομένων στο cloud computing, οι οργανισμοί θα πρέπει να υιοθετήσουν μια πολυεπίπεδη προσέγγιση για την ασφάλεια. Αυτό περιλαμβάνει την εφαρμογή ισχυρών ελέγχων πρόσβασης, την κρυπτογράφηση ευαίσθητων δεδομένων τόσο κατά τη μεταφορά όσο και κατά την ηρεμία, την τακτική παρακολούθηση και τον έλεγχο των περιβαλλόντων νέφους για ύποπτες δραστηριότητες και τη διενέργεια ολοκληρωμένων αξιολογήσεων κινδύνου. Επιπλέον, οι οργανισμοί θα πρέπει να επενδύουν σε προγράμματα εκπαίδευσης και ευαισθητοποίησης των εργαζομένων για την εκπαίδευση των χρηστών σχετικά με τις βέλτιστες πρακτικές ασφάλειας και τη σημασία της προστασίας των δεδομένων. Οι παραβιάσεις και οι διαρροές δεδομένων αποτελούν σημαντικές προκλήσεις για την ασφάλεια στο υπολογιστικό νέφος, οι οποίες πηγάζουν από παράγοντες όπως οι ανεπαρκείς έλεγχοι πρόσβασης, οι απειλές εκ των έσω, τα τρωτά σημεία της υποδομής του υπολογιστικού νέφους και η πολυπλοκότητα των μοντέλων κοινής ευθύνης. Αυτές οι απειλές ασφαλείας μπορεί να έχουν σημαντικές επιπτώσεις για τους οργανισμούς, συμπεριλαμβανομένων οικονομικών απωλειών, ζημίας στη φήμη και νομικών συνεπειών. Ωστόσο, με την εφαρμογή προληπτικών μέτρων ασφαλείας και την υιοθέτηση

μιας ολοκληρωμένης προσέγγισης διαχείρισης κινδύνων, οι οργανισμοί μπορούν να μετριάσουν αυτούς τους κινδύνους και να διασφαλίσουν τα δεδομένα τους στο νέφος (Tissir et al., 2021).

2.5Απειλές εκ των έσω

Οι απειλές εκ των έσω αποτελούν σημαντικό κίνδυνο για την ασφάλεια των περιβαλλόντων υπολογιστικού νέφους, όπου άτομα με προνομιακή πρόσβαση μπορούν να κάνουν κατάχρηση της εξουσίας τους για να κλέψουν, να χειραγωγήσουν ή να εκθέσουν ευαίσθητα δεδομένα. Η παρούσα ανάλυση διερευνά τις διάφορες διαστάσεις των εσωτερικών απειλών στο υπολογιστικό νέφος, συμπεριλαμβανομένων των κινήτρων τους, των μεθόδων επίθεσης και των πιθανών επιπτώσεων στους οργανισμούς. Συζητά κοινά σενάρια απειλών εκ των έσω, όπως κακόβουλους εσωτερικούς υπαλλήλους και αμελείς υπαλλήλους, και υπογραμμίζει τις προκλήσεις που συνεπάγεται η ανίχνευση και ο μετριασμός αυτών των κινδύνων σε περιβάλλοντα υπολογιστικού νέφους. Επιπλέον, η ανάλυση παρέχει συστάσεις προς τους οργανισμούς για την ενίσχυση της άμυνάς τους έναντι των εσωτερικών απειλών, τονίζοντας τη σημασία των ισχυρών ελέγχων πρόσβασης, της συνεχούς παρακολούθησης και των προγραμμάτων ευαισθητοποίησης των εργαζομένων (Tissir et al., 2021).

Το υπολογιστικό νέφος έχει μεταμορφώσει τον τρόπο με τον οποίο οι οργανισμοί αποθηκεύουν, επεξεργάζονται και διαχειρίζονται δεδομένα, προσφέροντας επεκτασιμότητα, ευελιξία και οικονομική αποδοτικότητα. Ωστόσο, αυτός ο ψηφιακός μετασχηματισμός έχει επίσης εισάγει νέες προκλήσεις για την ασφάλεια, συμπεριλαμβανομένων των εσωτερικών απειλών. Οι απειλές εκ των έσω συμβαίνουν όταν άτομα με προνομιακή πρόσβαση στα συστήματα και τα δεδομένα ενός οργανισμού κάνουν κατάχρηση της εξουσίας τους για κακόβουλους σκοπούς. Σε περιβάλλοντα υπολογιστικού νέφους, οι απειλές εκ των έσω μπορεί να έχουν καταστροφικές συνέπειες, οδηγώντας σε παραβιάσεις δεδομένων, οικονομικές απώλειες και βλάβη της φήμης. Η παρούσα ανάλυση εμβαθύνει στην πολυπλοκότητα των εσωτερικών απειλών στο cloud computing, διερευνώντας τα κίνητρα, τις μεθόδους, τις επιπτώσεις και τις στρατηγικές μετριασμού τους (Alouffi et al., 2021).

1. Κίνητρα πίσω από τις απειλές εκ των έσω:

Οι απειλές εκ των έσω στο cloud computing μπορεί να προέρχονται από διάφορα κίνητρα, όπως οικονομικό κέρδος, εκδίκηση, κατασκοπεία και ιδεολογικές πεποιθήσεις. Οι κακόβουλοι εσωτερικοί χρήστες μπορεί να επιδιώκουν να εκμεταλλευτούν την πρόσβασή τους σε ευαίσθητα δεδομένα για προσωπικό κέρδος ή για να βλάψουν τη φήμη του

οργανισμού. Επιπλέον, δυσαρεστημένοι εργαζόμενοι ή πρώην εργαζόμενοι μπορεί να εκδικηθούν τον εργοδότη τους με τη διαρροή εμπιστευτικών πληροφοριών ή τη διατάραξη των λειτουργιών. Επιπλέον, εθνικοί κρατικοί φορείς και εγκληματίες του κυβερνοχώρου μπορεί να στρατολογήσουν εσωτερικούς υπαλλήλους για να διευκολύνουν την κατασκοπεία ή τις κυβερνοεπιθέσεις εναντίον οργανισμών, εκμεταλλευόμενοι τις εσωτερικές γνώσεις και τα προνόμια πρόσβασης που διαθέτουν (Alouffi et al., 2021).

2. Τύποι απειλών εκ των έσω:

Οι απειλές εκ των έσω στο υπολογιστικό νέφος εκδηλώνονται με διάφορες μορφές, που κυμαίνονται από σκόπιμες κακόβουλες δραστηριότητες έως ακούσια λάθη ή αμέλεια. Οι συνήθεις τύποι εσωτερικών απειλών περιλαμβάνουν:

- Κακόβουλοι εσωτερικοί χρήστες: Τα άτομα αυτά κάνουν εσκεμμένα κατάχρηση της προνομιακής τους πρόσβασης για να υποκλέψουν, να χειραγωγήσουν ή να εκθέσουν ευαίσθητα δεδομένα. Μπορεί να συμμετέχουν σε διαρροή δεδομένων, απάτη, δολιοφθορά ή κατασκοπεία για να επιτύχουν τους κακόβουλους στόχους τους.

- Απρόσεκτοι υπάλληλοι: Η αμέλεια ή η απροσεξία των υπαλλήλων, των εργολάβων ή των τρίτων παρόχων υπηρεσιών μπορεί να εκθέσει ακούσια ευαίσθητα δεδομένα σε μη εξουσιοδοτημένη πρόσβαση ή σε παραβίαση. Τα παραδείγματα περιλαμβάνουν τυχαίες διαρροές δεδομένων, λανθασμένες ρυθμίσεις και μη τήρηση των πολιτικών και διαδικασιών ασφαλείας (Alouffi et al., 2021).

- Υπονομευμένοι λογαριασμοί: Οι εσωτερικές απειλές μπορεί επίσης να προέρχονται από παραβιασμένους λογαριασμούς χρηστών, όπου κακόβουλοι παράγοντες εκμεταλλεύονται κλεμμένα διαπιστευτήρια ή παραβιασμένους λογαριασμούς για να αποκτήσουν μη εξουσιοδοτημένη πρόσβαση σε πόρους του cloud. Αυτό μπορεί να συμβεί μέσω επιθέσεων phishing, κοινωνικής μηχανικής ή μολύνσεων από κακόβουλο λογισμικό (Butt et al., 2020).

3. Προκλήσεις της ανίχνευσης απειλών εκ των έσω σε περιβάλλοντα νέφους:

Η ανίχνευση εσωτερικών απειλών σε περιβάλλοντα υπολογιστικού νέφους παρουσιάζει σημαντικές προκλήσεις λόγω διαφόρων παραγόντων:

- Πολυπλοκότητα της υποδομής νέφους: Τα περιβάλλοντα υπολογιστικού νέφους είναι δυναμικά και πολύπλοκα, αποτελούμενα από πολλαπλά επίπεδα υποδομών και υπηρεσιών. Η παρακολούθηση και ο εντοπισμός ανώμαλης συμπεριφοράς σε αυτά τα ποικίλα περιβάλλοντα απαιτούν προηγμένη ανάλυση και ορατότητα ασφαλείας (Butt et al., 2020).

- Ανησυχίες κρυπτογράφησης και απορρήτου: Η κρυπτογράφηση από άκρο σε άκρο και η προστασία της ιδιωτικότητας των χρηστών που εφαρμόζονται σε περιβάλλοντα νέφους μπορεί να εμποδίσουν την ορατότητα των δραστηριοτήτων των χρηστών και των προτύπων πρόσβασης στα δεδομένα, καθιστώντας δύσκολη την ανίχνευση εσωτερικών απειλών χωρίς να διακυβεύεται η ιδιωτικότητα των χρηστών (Butt et al., 2020).

- Γνώση εσωτερικών προσώπων και τακτικές αποφυγής: Οι εσωτερικοί χρήστες συχνά διαθέτουν βαθιά γνώση των συστημάτων και των ελέγχων ασφαλείας του οργανισμού, γεγονός που τους επιτρέπει να αποφεύγουν την ανίχνευση και να καλύπτουν τα ίχνη τους πιο αποτελεσματικά. Ενδέχεται να χρησιμοποιούν εξελιγμένες τεχνικές αποφυγής, όπως η μεταμφίεση των δραστηριοτήτων τους ως νόμιμων επιχειρήσεων ή η εκμετάλλευση τυφλών σημείων στα συστήματα παρακολούθησης (Parast et al., 2022).

4. Επιπτώσεις των εσωτερικών απειλών:

Οι απειλές εκ των έσω μπορεί να έχουν σοβαρές επιπτώσεις στους οργανισμούς, μεταξύ άλλων:

- Παραβιάσεις δεδομένων: Οι απειλές εκ των έσω μπορεί να οδηγήσουν σε μη εξουσιοδοτημένη πρόσβαση, κλοπή ή έκθεση ευαίσθητων δεδομένων, με αποτέλεσμα παραβιάσεις δεδομένων και παραβιάσεις της κανονιστικής συμμόρφωσης. Η έκθεση εμπιστευτικών πληροφοριών μπορεί να βλάψει την εμπιστοσύνη των πελατών και να αμαυρώσει τη φήμη του οργανισμού (Parast et al., 2022).

- Οικονομικές απώλειες: Ο οικονομικός αντίκτυπος των απειλών εκ των έσω περιλαμβάνει άμεσες δαπάνες που σχετίζονται με παραβιάσεις δεδομένων, όπως ρυθμιστικά πρόστιμα, νομικά έξοδα και δαπάνες αποκατάστασης, καθώς και έμμεσες δαπάνες που σχετίζονται με τη διακοπή της επιχείρησης, την απώλεια εσόδων και τη μειωμένη αγοραία αξία.

- Ζημία φήμης: Τα περιστατικά εκ των έσω μπορούν να διαβρώσουν την εμπιστοσύνη και την αξιοπιστία του οργανισμού, οδηγώντας σε αρνητική δημοσιότητα, φθορά πελατών και ζημία στη φήμη της εταιρίας. Η αποκατάσταση της εμπιστοσύνης και η αποκατάσταση της φήμης μπορεί να είναι μια μακρά και δαπανηρή διαδικασία για τους επηρεαζόμενους οργανισμούς (Parast et al., 2022).

5. Στρατηγικές μετριασμού:

Για τον μετριασμό των εσωτερικών απειλών στο υπολογιστικό νέφος, οι οργανισμοί θα πρέπει να υιοθετήσουν μια πολύπλευρη προσέγγιση που συνδυάζει τεχνικούς ελέγχους, εκπαίδευση των χρηστών και προληπτική παρακολούθηση:

- Εφαρμογή ισχυρών ελέγχων πρόσβασης: Επιβολή των αρχών των ελάχιστων προνομίων και εφαρμογή ισχυρών μηχανισμών ελέγχου ταυτότητας, όπως ο έλεγχος ταυτότητας πολλαπλών παραγόντων (MFA), για τον περιορισμό της πρόσβασης σε ευαίσθητα δεδομένα και πόρους. Επανεξέταση και επικαιροποίηση των δικαιωμάτων των χρηστών σε τακτά χρονικά διαστήματα, ώστε να ευθυγραμμίζονται με τους ρόλους και τις αρμοδιότητες της θέσης εργασίας (Sun, 2020).

- Παρακολούθηση και ανάλυση των δραστηριοτήτων των χρηστών: Εφαρμογή ισχυρών δυνατοτήτων παρακολούθησης και καταγραφής για την παρακολούθηση των δραστηριοτήτων των χρηστών, της πρόσβασης σε πόρους και της μεταφοράς δεδομένων σε πραγματικό χρόνο. Αξιοποίηση συστημάτων διαχείρισης πληροφοριών και συμβάντων ασφαλείας (SIEM), ανίχνευσης ανωμαλιών και ανάλυσης συμπεριφοράς για τον εντοπισμό ύποπτης συμπεριφοράς που υποδηλώνει εσωτερικές απειλές (Sun, 2020).

- Ευαισθητοποίηση των εργαζομένων σχετικά με τους κινδύνους των εσωτερικών απειλών και εκπαίδευσή τους σε βέλτιστες πρακτικές ασφαλείας, όπως η διασφάλιση των διαπιστευτηρίων, η αναγνώριση των προσπαθειών ηλεκτρονικού "ψαρέματος" και η αναφορά ύποπτων δραστηριοτήτων. Πραγματοποίηση τακτικών εκπαιδευτικών συνεδριών ευαισθητοποίησης σε θέματα ασφάλειας και ενίσχυση της σημασίας της συμμόρφωσης με τις πολιτικές και τις διαδικασίες ασφάλειας (Sun, 2020).

- Διεξαγωγή τακτικών επιθεώρησης και αξιολογήσεις: Εκτέλεση τακτικών ελέγχων και αξιολογήσεων ασφαλείας των περιβαλλόντων νέφους για τον εντοπισμό ευπαθειών, λανθασμένων ρυθμίσεων και αδυναμιών ελέγχου πρόσβασης. Διεξαγωγή δοκιμών διείσδυσης και σάρωσης ευπαθειών για τον προληπτικό εντοπισμό και την αποκατάσταση των κενών ασφαλείας προτού αυτά γίνουν αντικείμενο εκμετάλλευσης από εσωτερικούς ή εξωτερικούς επιτιθέμενους (Tabrizchi & Kuchaki, 2020).

Οι απειλές εκ των έσω αποτελούν σημαντικό κίνδυνο για την ασφάλεια των περιβαλλόντων υπολογιστικού νέφους, όπου άτομα με προνομιακή πρόσβαση μπορούν να εκμεταλλευτούν την εξουσία τους για να κλέψουν, να χειραγωγήσουν ή να εκθέσουν ευαίσθητα δεδομένα. Αυτές οι απειλές μπορεί να πηγάζουν από διάφορα κίνητρα, όπως οικονομικό κέρδος, εκδίκηση, κατασκοπεία και ιδεολογικές πεποιθήσεις, και εκδηλώνονται

με διάφορες μορφές, από κακόβουλους εσωτερικούς χρήστες έως αμελείς υπαλλήλους και παραβιασμένους λογαριασμούς. Η ανίχνευση και ο μετριασμός των απειλών εκ των έσω σε περιβάλλοντα νέφους παρουσιάζουν σημαντικές προκλήσεις λόγω της πολυπλοκότητας της υποδομής νέφους, της κρυπτογράφησης και των ανησυχιών για την προστασία της ιδιωτικής ζωής, καθώς και των γνώσεων και των τακτικών αποφυγής εκ των έσω. Ωστόσο, με την εφαρμογή ισχυρών ελέγχων πρόσβασης, τη συνεχή παρακολούθηση, την εκπαίδευση των εργαζομένων και τα προληπτικά μέτρα ασφαλείας, οι οργανισμοί μπορούν να ενισχύσουν τις άμυνές τους έναντι των απειλών εκ των έσω και να διασφαλίσουν τα δεδομένα τους στο νέφος (Tabrizchi & Kuchaki, 2020).

2.6 Μοντέλο κοινής ευθύνης

Η παρούσα ανάλυση διερευνά τις ιδιαιτερότητες του μοντέλου κοινής ευθύνης, περιγράφοντας τους αντίστοιχους ρόλους και τις υποχρεώσεις των παρόχων και των πελατών του υπολογιστικού νέφους για την ασφάλεια των περιβαλλόντων νέφους. Συζητά τις προκλήσεις που συνδέονται με το μοντέλο κοινής ευθύνης, όπως η ασάφεια στη λογοδοσία και τη συμμόρφωση, και παρέχει βέλτιστες πρακτικές για την αποτελεσματική εφαρμογή και διαχείριση της ασφάλειας στο νέφος (Sinchana & Savithramma, 2020).

Το υπολογιστικό νέφος έχει καταστεί αναπόσπαστο μέρος των σύγχρονων επιχειρηματικών λειτουργιών, επιτρέποντας στους οργανισμούς να αξιοποιούν κλιμακούμενους και κατά παραγγελία υπολογιστικούς πόρους. Ωστόσο, καθώς οι οργανισμοί μεταφέρουν τις εργασίες τους στο νέφος, πρέπει να περιηγηθούν στο πολύπλοκο τοπίο της ασφάλειας του νέφους. Το μοντέλο κοινής ευθύνης είναι μια θεμελιώδης έννοια στο cloud computing που ορίζει τις ευθύνες των παρόχων cloud και των πελατών για την ασφάλεια των περιβαλλόντων cloud. Η παρούσα ανάλυση παρέχει μια εις βάθος εξέταση του μοντέλου κοινής ευθύνης, υπογραμμίζοντας τη σημασία, τις προκλήσεις και τις βέλτιστες πρακτικές του (Sinchana & Savithramma, 2020).

Το μοντέλο κοινής ευθύνης καθορίζει μια σαφή οριοθέτηση των ευθυνών ασφάλειας μεταξύ των παρόχων και των πελατών του υπολογιστικού νέφους. Ενώ οι πάροχοι υπολογιστικού νέφους είναι υπεύθυνοι για την ασφάλεια της υποκείμενης υποδομής και των υπηρεσιών, οι πελάτες είναι υπεύθυνοι για την ασφάλεια των δεδομένων, των εφαρμογών, των ταυτοτήτων και των ρυθμίσεων. Ο καταμερισμός των ευθυνών ποικίλλει ανάλογα με τον τύπο του μοντέλου υπηρεσιών νέφους:

- Υποδομή ως υπηρεσία (IaaS): Σε περιβάλλοντα IaaS, οι πάροχοι υπηρεσιών νέφους διαχειρίζονται την υποκείμενη υποδομή, συμπεριλαμβανομένων των διακομιστών, της αποθήκευσης και των στοιχείων δικτύωσης, ενώ οι πελάτες είναι υπεύθυνοι για την εξασφάλιση των λειτουργικών συστημάτων, των εφαρμογών και των δεδομένων που αναπτύσσονται πάνω στην υποδομή (Sinchana & Savithramma, 2020).

- Πλατφόρμα ως υπηρεσία (PaaS): Σε περιβάλλοντα PaaS, οι πάροχοι νέφους προσφέρουν μια πλατφόρμα για την ανάπτυξη και τη διαχείριση εφαρμογών, ενώ οι πελάτες είναι υπεύθυνοι για την εξασφάλιση των εφαρμογών, των δεδομένων και των παραμετροποιήσεων που δημιουργούνται στην πλατφόρμα.

- Λογισμικό ως υπηρεσία (SaaS): Σε περιβάλλοντα SaaS, οι πάροχοι cloud παρέχουν εφαρμογές λογισμικού μέσω του διαδικτύου, χειριζόμενοι όλες τις πτυχές της υποδομής, της πλατφόρμας και της διαχείρισης των εφαρμογών, ενώ οι πελάτες είναι υπεύθυνοι για τη διαμόρφωση των ελέγχων πρόσβασης, τη διαχείριση των ταυτοτήτων των χρηστών και την προστασία των δεδομένων τους εντός της εφαρμογής (Arafat, 2018).

Ρόλοι και αρμοδιότητες:

Οι πάροχοι cloud και οι πελάτες έχουν διακριτούς ρόλους και ευθύνες στο πλαίσιο του μοντέλου κοινής ευθύνης:

Αρμοδιότητες του παρόχου νέφους:

- Ασφάλιση της υποκείμενης υποδομής, συμπεριλαμβανομένων των φυσικών εγκαταστάσεων, της υποδομής δικτύωσης και των hypervisors.
- Διασφάλιση της διαθεσιμότητας, της επεκτασιμότητας και της απόδοσης των υπηρεσιών νέφους.
- Εφαρμογή ελέγχων ασφαλείας σε επίπεδο υποδομής, όπως τείχη προστασίας, συστήματα ανίχνευσης εισβολών και προστασία DDoS.
- Συμμόρφωση με τους κανονισμούς και τις πιστοποιήσεις του κλάδου, όπως SOC 2, ISO 27001 και GDPR (Arafat, 2018).

Αρμοδιότητες του πελάτη:

- Διασφάλιση της πρόσβασης σε πόρους cloud μέσω ισχυρών μηχανισμών ελέγχου ταυτότητας, όπως ο έλεγχος ταυτότητας πολλαπλών παραγόντων (MFA).

- Διαμόρφωση ελέγχων ασφαλείας δικτύου, όπως εικονικά ιδιωτικά δίκτυα (VPN) και ομάδες ασφαλείας δικτύου (NSG), για τον περιορισμό της πρόσβασης σε πόρους.
- Κρυπτογράφηση δεδομένων σε κατάσταση ηρεμίας και κατά τη μεταφορά για την προστασία της εμπιστευτικότητας και της ακεραιότητας.
- Εφαρμογή ελέγχων διαχείρισης ταυτότητας και πρόσβασης (IAM) για τη διαχείριση ταυτοτήτων, δικαιωμάτων και ρόλων χρηστών (Arafat, 2018).
- Παρακολούθηση και έλεγχος των περιβαλλόντων cloud για περιστατικά ασφαλείας, παραβιάσεις συμμόρφωσης και μη εξουσιοδοτημένες δραστηριότητες.

Προκλήσεις του μοντέλου κοινής ευθύνης:

Ενώ το μοντέλο κοινής ευθύνης παρέχει σαφήνεια όσον αφορά τις ευθύνες ασφάλειας, θέτει επίσης αρκετές προκλήσεις για τους οργανισμούς:

- Ασάφεια όσον αφορά την υπευθυνότητα: Ο καταμερισμός των ευθυνών μεταξύ παρόχων cloud και πελατών μπορεί να είναι διφορούμενος, οδηγώντας σε παρανοήσεις ή κενά στην κάλυψη της ασφάλειας. Οι οργανισμοί πρέπει να καθορίζουν και να τεκμηριώνουν με σαφήνεια τις αντίστοιχες ευθύνες τους, ώστε να αποφεύγεται η σύγχυση και να διασφαλίζεται η συμμόρφωση με τις απαιτήσεις ασφαλείας (Weil, 2018).
- Συμμόρφωση και κανονιστικές ανησυχίες: Η συμμόρφωση με τους κανονισμούς, όπως GDPR, HIPAA και τα πρότυπα του κλάδου όπως PCI DSS, απαιτεί συνεργασία μεταξύ των παρόχων cloud και των πελατών για να διασφαλιστεί η ευθυγράμμιση των ελέγχων και των πρακτικών ασφαλείας. Ωστόσο, η επίτευξη της συμμόρφωσης σε περιβάλλοντα πολλαπλού cloud ή υβριδικού cloud μπορεί να είναι πολύπλοκη και δύσκολη.
- Έλλειψη ορατότητας και ελέγχου: Οι οργανισμοί ενδέχεται να έχουν περιορισμένη ορατότητα και έλεγχο των ελέγχων ασφαλείας που εφαρμόζουν οι πάροχοι cloud, ιδίως σε περιβάλλοντα SaaS, όπου οι πάροχοι διαχειρίζονται ολόκληρη την υπηρεσία. Αυτή η έλλειψη ορατότητας μπορεί να παρεμποδίσει την ικανότητα των οργανισμών να αξιολογούν την κατάσταση ασφαλείας και να ανταποκρίνονται αποτελεσματικά σε περιστατικά ασφαλείας (Drozdova et al., 2020).

Ωστόσο, η διαχείριση του μοντέλου κοινής ευθύνης παρουσιάζει προκλήσεις, όπως ασάφεια στη λογοδοσία, προβλήματα συμμόρφωσης και έλλειψη ορατότητας και ελέγχου. Για την αντιμετώπιση αυτών των προκλήσεων και τον μετριασμό των κινδύνων ασφαλείας στο υπολογιστικό νέφος, οι οργανισμοί θα πρέπει να υιοθετήσουν βέλτιστες πρακτικές, όπως η κατανόηση και η τεκμηρίωση των αρμοδιοτήτων, η εφαρμογή ελέγχων ασφαλείας, η διενέργεια τακτικών αξιολογήσεων κινδύνου, η παροχή εκπαίδευσης και ευαισθητοποίησης των εργαζομένων, καθώς και η παρακολούθηση και η αντιμετώπιση περιστατικών ασφαλείας. Τηρώντας αυτές τις βέλτιστες πρακτικές, οι οργανισμοί μπορούν να διαχειριστούν αποτελεσματικά το μοντέλο κοινής ευθύνης και να ενισχύσουν την ασφάλεια των περιβαλλόντων νέφους τους (Drozdova et al., 2020).

2.7 Συμμόρφωση και κανονιστικά ζητήματα

Καθώς οι οργανισμοί αξιοποιούν όλο και περισσότερο τις υπηρεσίες υπολογιστικού νέφους, τα ζητήματα συμμόρφωσης και κανονιστικών ρυθμίσεων έχουν καταστεί πρωταρχικής σημασίας. Η ικανοποίηση των απαιτήσεων διαφόρων κανονισμών, όπως ο GDPR, ο HIPAA και ο PCI DSS, ενώ χρησιμοποιούνται πόροι cloud, παρουσιάζει μοναδικές προκλήσεις. Η παρούσα ανάλυση διερευνά το τοπίο της συμμόρφωσης και των κανονιστικών ρυθμίσεων στο cloud computing, επισημαίνοντας τους βασικούς κανονισμούς, τις προκλήσεις και τις στρατηγικές για την επίτευξη και τη διατήρηση της συμμόρφωσης. Συζητά το μοντέλο κοινής ευθύνης, τις απαιτήσεις κρυπτογράφησης και τη σημασία του ελέγχου και της παρακολούθησης. Με την κατανόηση αυτών των ζητημάτων και την εφαρμογή κατάλληλων στρατηγικών, οι οργανισμοί μπορούν να περιηγηθούν αποτελεσματικά στην πολυπλοκότητα της συμμόρφωσης στο νέφος (Tissir et al., 2021).

Διάφοροι κανονισμοί και βιομηχανικά πρότυπα διέπουν τη χρήση των υπηρεσιών υπολογιστικού νέφους, διασφαλίζοντας την προστασία των δεδομένων, την ιδιωτικότητα και την ασφάλεια σε διάφορους τομείς και γεωγραφικές περιοχές:

- Γενικός κανονισμός για την προστασία δεδομένων (ΓΚΠΔ): Αυτό σημαίνει ότι οι εταιρίες πρέπει να επεξεργάζονται και να αποθηκεύουν δεδομένα εντός των συνόρων της ΕΕ ή όταν έχουν διασφαλιστεί κατάλληλα και επαρκή μέτρα προστασίας .Οι οργανισμοί πρέπει να λαμβάνουν ρητή συγκατάθεση από τα άτομα για την επεξεργασία δεδομένων, να εφαρμόζουν αυστηρά μέτρα προστασίας δεδομένων και να αναφέρουν αμέσως τις παραβιάσεις δεδομένων. Για το υπολογιστικό νέφος, αυτό σημαίνει ότι οι πάροχοι υπηρεσιών

νέφους (CSP) και οι εταιρίες πρέπει να διασφαλίζουν ότι τα δεδομένα αποθηκεύονται και υποβάλλονται σε επεξεργασία σύμφωνα με τις απαιτήσεις του ΓΚΠΔ, γεγονός που συχνά απαιτεί εντοπισμό δεδομένων και ισχυρά μέτρα κρυπτογράφησης.

- Νομοθεσία περί φορητότητας και λογοδοσίας των ασφαλιστικών φορέων υγείας (HIPAA): Στις Ηνωμένες Πολιτείες, ο HIPAA απαιτεί από τις καλυπτόμενες οντότητες και τους επιχειρηματικούς συνεργάτες, συμπεριλαμβανομένων των CSP που χειρίζονται προστατευόμενες πληροφορίες υγείας (PHI), να εφαρμόζουν διασφαλίσεις για την προστασία των PHI. Αυτό περιλαμβάνει κρυπτογράφηση, ελέγχους πρόσβασης και διαδρομές ελέγχου για τη διασφάλιση της εμπιστευτικότητας, της ακεραιότητας και της διαθεσιμότητας των PHI. Οι πάροχοι υπολογιστικού νέφους πρέπει να προσφέρουν υπηρεσίες συμβατές με το HIPAA, διασφαλίζοντας ότι όλα τα δεδομένα υγείας που αποθηκεύονται ή υποβάλλονται σε επεξεργασία στο υπολογιστικό νέφος πληρούν αυτά τα αυστηρά πρότυπα ασφαλείας (Alouffi et al., 2021).

- Πρότυπο ασφάλειας δεδομένων της βιομηχανίας καρτών πληρωμών (PCI DSS): Αυτό το παγκόσμιο πρότυπο επιβάλλει ελέγχους ασφαλείας σε οργανισμούς που επεξεργάζονται, μεταδίδουν ή αποθηκεύουν δεδομένα καρτών πληρωμών, συμπεριλαμβανομένων εκείνων που χρησιμοποιούν υπηρεσίες cloud. Η συμμόρφωση με το PCI DSS περιλαμβάνει την εφαρμογή ασφάλειας δικτύου, κρυπτογράφησης, ελέγχων πρόσβασης και τακτικών αξιολογήσεων ασφαλείας για τη διασφάλιση των δεδομένων των κατόχων καρτών. Οι οργανισμοί πρέπει να διασφαλίζουν ότι οι CSP τους τηρούν τις απαιτήσεις του PCI DSS, οι οποίες περιλαμβάνουν ασφαλή αρχιτεκτονική cloud και τακτικές επιθεωρήσεις ασφαλείας για την προστασία των πληροφοριών πληρωμής.

-Νόμος Sarbanes-Oxley (SOX): Στις Ηνωμένες Πολιτείες, ο νόμος SOX θεσπίζει απαιτήσεις για τη χρηματοοικονομική πληροφόρηση και τους εσωτερικούς ελέγχους για την πρόληψη της απάτης και τη διασφάλιση της διαφάνειας στις χρηματοοικονομικές λειτουργίες. Οι οργανισμοί πρέπει να εφαρμόζουν ελέγχους για την προστασία των χρηματοοικονομικών δεδομένων, συμπεριλαμβανομένων των ελέγχων πρόσβασης, των διαδρομών ελέγχου και του διαχωρισμού των καθηκόντων. Για το υπολογιστικό νέφος, αυτό σημαίνει ότι τα χρηματοοικονομικά δεδομένα που αποθηκεύονται στο νέφος πρέπει να συμμορφώνονται με τις απαιτήσεις SOX, γεγονός που επιβάλλει στους CSP να προσφέρουν χαρακτηριστικά όπως λεπτομερής καταγραφή, ασφαλής διαχείριση πρόσβασης και ελέγχους ακεραιότητας δεδομένων (Alouffi et al., 2021).

Αυτοί οι κανονισμοί και τα πρότυπα διασφαλίζουν ότι οι υπηρεσίες υπολογιστικού νέφους χρησιμοποιούνται υπεύθυνα και με ασφάλεια, παρέχοντας ένα πλαίσιο για την προστασία προσωπικών και ευαίσθητων δεδομένων σε διάφορους κλάδους και περιοχές.

3. Πρότυπα ISO 27017 & 27018

Το ISO/IEC 27018 (Information technology - Security techniques - Code of practice for protection of personally identifiable information (PII) in public clouds acting as PII processors)δημοσιεύθηκε στα μέσα του 2014.Τόσο το ISO/IEC 27017 (Information technology - Security techniques - Code of practice for information security controls based on ISO/IEC 27002 for cloud services.) όσο και το ISO/EC 29151 (Information technology – Security techniques – Code of practice for personally identifiable information protection), όπως και το ISO/IEC 27018, αποσκοπούν στην παροχή ενός συνόλου ελέγχων και σχετικών οδηγιών εφαρμογής που στοχεύει στη συμπλήρωση εκείνων που δίνονται στο ISO/IEC 27002 για έναν συγκεκριμένο τομέα εφαρμογής.

Κατά μία έννοια, και τα τρία αυτά πρότυπα έχουν ως υποσύνολο την εστίαση του ISO/IEC 27018. Το ISO/IEC 27017, το οποίο πλησιάζει στην ολοκλήρωσή του (στα μέσα του 2015 βρισκόταν στο στάδιο του τελικού σχεδίου διεθνούς προτύπου, το τελευταίο στάδιο πριν από τη δημοσίευση), αποσκοπεί στη βελτίωση του συνόλου των ελέγχων του ISO/IEC 27002 ώστε να καλύπτει όλες τις πτυχές της ασφάλειας και της ιδιωτικότητας της λειτουργίας μιας υπηρεσίας νέφους. Παρέχει κατευθυντήριες γραμμές που υποστηρίζουν την εφαρμογή των ελέγχων ασφάλειας πληροφοριών για τους πελάτες υπηρεσιών νέφους και τους παρόχους υπηρεσιών νέφους. Πολλές από τις κατευθυντήριες γραμμές καθοδηγούν τους παρόχους υπηρεσιών νέφους να βοηθούν τους πελάτες υπηρεσιών νέφους στην εφαρμογή των ελέγχων και καθοδηγούν τους πελάτες υπηρεσιών νέφους στην εφαρμογή των εν λόγω ελέγχων. Η επιλογή των κατάλληλων ελέγχων ασφάλειας πληροφοριών και η εφαρμογή των παρεχόμενων οδηγιών εφαρμογής εξαρτάται από την αξιολόγηση του κινδύνου καθώς και από τυχόν νομικές, συμβατικές, κανονιστικές ή άλλες ειδικές απαιτήσεις ασφάλειας πληροφοριών στον τομέα του νέφους (Butt et al., 2020).

Μια κάπως συμπληρωματική εστίαση ισχύει για την ανάπτυξη του ISO/IEC 29151, το οποίο από τα μέσα του 2015 έχει μόλις φθάσει στο στάδιο του προσχεδίου της επιτροπής. Το ISO/IEC 29151 αποσκοπεί στην τεκμηρίωση των ελέγχων που σχετίζονται με την προστασία των PII, ανεξάρτητα από το πού αποθηκεύονται και ποια οντότητα ενεργεί ως επεξεργαστής ή υπεύθυνος επεξεργασίας των PII. Ο αριθμός των οργανισμών που επεξεργάζονται PII αυξάνεται, όπως και ο όγκος των PII που διαχειρίζονται οι οργανισμοί αυτοί. Ταυτόχρονα, αυξάνονται και οι κοινωνικές προσδοκίες για την προστασία και την ασφάλεια των δεδομένων που αφορούν τα άτομα. Ορισμένες χώρες ενισχύουν τη νομοθεσία

τους για να αντιμετωπίσουν τον αυξημένο αριθμό παραβιάσεων υψηλού προφίλ (Parast et al., 2022).

Καθώς αυξάνεται ο αριθμός των παραβιάσεων των προσωπικών δεδομένων, οι οργανισμοί που ελέγχουν ή επεξεργάζονται προσωπικά δεδομένα, συμπεριλαμβανομένων των μικρότερων νεοεισερχόμενων (π.χ. μικρομεσαίες επιχειρήσεις (ΜΜΕ)), θα χρειάζονται όλο και περισσότερο καθοδήγηση σχετικά με τον τρόπο με τον οποίο θα πρέπει να προστατεύουν τα προσωπικά δεδομένα, προκειμένου να μειώσουν τον κίνδυνο παραβιάσεων της ιδιωτικής ζωής και να μειώσουν τις επιπτώσεις των παραβιάσεων στον οργανισμό και στα ενδιαφερόμενα άτομα.

Επιστρέφοντας στην προστασία της ιδιωτικής ζωής, αξίζει να σημειωθεί ότι ένας από τους ελέγχους του ISO/IEC 27002 έχει τίτλο "Ιδιωτική ζωή και προστασία των πληροφοριών που μπορούν να αναγνωριστούν ως προσωπικά" και διευκρινίζει ότι "η ιδιωτική ζωή και η προστασία των πληροφοριών που μπορούν να αναγνωριστούν ως προσωπικά πρέπει να διασφαλίζονται όπως απαιτείται από τη σχετική νομοθεσία και τους κανονισμούς, όπου εφαρμόζεται". Η σχετική καθοδήγηση εφαρμογής είναι πολύ γενική, ξεκινώντας με τη δήλωση ότι "Η πολιτική δεδομένων ενός οργανισμού για την προστασία της ιδιωτικής ζωής και την προστασία των πληροφοριών που μπορούν να αναγνωριστούν ως προσωπικά πρέπει να αναπτυχθεί και να εφαρμοστεί. Η πολιτική αυτή θα πρέπει να κοινοποιείται σε όλα τα πρόσωπα που εμπλέκονται στην επεξεργασία πληροφοριών που μπορούν να ταυτοποιηθούν ως προσωπικά". Συνεχίζει να συζητά την ανάγκη για μια πολιτική προστασίας της ιδιωτικής ζωής, καθώς και την πιθανή ανάγκη για έναν διορισμένο υπεύθυνο προστασίας δεδομένων σε έναν οργανισμό για τη διαχείριση των θεμάτων προστασίας της ιδιωτικής ζωής. Αυτό οδηγεί φυσικά στη συζήτηση του ISO//IEC 27018 (Parast et al., 2022).

Αυτό το πρότυπο επικεντρώνεται ειδικά στην προστασία των προσωπικών δεδομένων όταν η επεξεργασία τους γίνεται στο νέφος - πιο συγκεκριμένα όταν η επεξεργασία πραγματοποιείται από δημόσιο πάροχο υπηρεσιών νέφους. Παρέχει ένα σύνολο ελέγχων, που συμπληρώνουν το ISO/IEC 27002, με στόχο τους παρόχους υπηρεσιών νέφους που ενεργούν ως επεξεργαστές για λογαριασμό ενός υπεύθυνου επεξεργασίας. Δηλαδή, η κύρια εστίαση του προτύπου δεν είναι οι πάροχοι υπηρεσιών νέφους που ενεργούν ως υπεύθυνοι επεξεργασίας PII, αν και οι έλεγχοι του ISO/IEC 27018 θα εφαρμόζονται σχεδόν σίγουρα σε τέτοιες οντότητες (καθώς και πολλοί άλλοι έλεγχοι, π.χ. όπως δίνονται στα αναδυόμενα πρότυπα ISO/IEC 27017 και ISO/IEC 29151 - βλ. παρακάτω). Η ιδέα πίσω από

το ISO/IEC 27018 είναι ότι ένας πάροχος υπηρεσιών νέφους μπορεί να ελέγξει το ISMS(Information Security Management System) του χρησιμοποιώντας το σύστημα ISO/IEC 27001, όπου ο ελεγκτής θα επαληθεύσει ότι η διαδικασία διαχείρισης κινδύνων και η επακόλουθη εφαρμογή του ISMS έχουν λάβει δεόντως υπόψη το συμπληρωματικό σύνολο ελέγχων του ISO/IEC 27018. Η πιστοποίηση που προκύπτει μπορεί στη συνέχεια να χρησιμοποιηθεί τόσο για την ενημέρωση των υποψήφιων χρηστών σχετικά με τις ιδιότητες της υπηρεσίας νέφους που σέβονται την ιδιωτικότητα των χρηστών, όσο και για να αποτελέσει μέρος των σχετικών συμβατικών ρυθμίσεων όταν χρησιμοποιείται η υπηρεσία νέφους. Πιθανότατα αυτό να απλουστεύσει σημαντικά το έργο του υπεύθυνου επεξεργασίας προσωπικών δεδομένων κατά την επιλογή ενός παρόχου υπηρεσιών νέφους. Το σύνολο των ελέγχων του προτύπου προέρχεται από διάφορες πηγές. Πριν από την εκπόνηση του πρώτου σχεδίου του ISO/IEC 27018, πραγματοποιήθηκε εκτενής ανάλυση της υφιστάμενης νομοθεσίας σχετικά με την επεξεργασία από τρίτους.

Ορισμένα πρότυπα της σειράς επιδιώκουν να επεκτείνουν συγκεκριμένα θέματα που εξετάζονται στο πλαίσιο του ISO/IEC 27001, όπως:

- ISO/IEC 27003: Οδηγίες εφαρμογής, που παρέχουν περισσότερες λεπτομέρειες σχετικά με την εφαρμογή μιάς ΣΔΠΔ (Συνοπτική Πολιτική Προστασίας Προσωπικών Δεδομένων),

- ISO/IEC 27004: Μέτρηση, που καλύπτει μετρήσεις ασφάλειας,

- ISO/IEC 27005: Διαχείριση κινδύνου ασφάλειας πληροφοριών- και

- ISO/IEC 27006: Απαιτήσεις για φορείς που παρέχουν έλεγχο και πιστοποίηση συστημάτων διαχείρισης της ασφάλειας των πληροφοριών, οι οποίες καθορίζουν τον τρόπο με τον οποίο πρέπει να πραγματοποιείται η πιστοποίηση των ISMS(information security management systems) βάσει του ISO/IEC 27001(Sinchana & Savithramma, 2020).

3.1 Επισκόπηση του ISO 27017 (ασφάλεια στο νέφος)

Ο λόγος που δημιουργήθηκε το ISO 27017 είναι οι ανησυχίες ότι τα δεδομένα θα μπορούσαν να καταλήξουν σε λάθος χέρια και το ποσοστό ελέγχου του πελάτη έναντι των απρόσεκτων χειριστών. Υπάρχουν όμως και άλλες ανησυχίες: θέματα όπως η ταυτότητα του πελάτη, ο διαχωρισμός των περιουσιακών στοιχείων σε εικονικούς διακομιστές και το τι συμβαίνει με τα περιουσιακά στοιχεία σε περίπτωση που ένας CSP(Cloud Service Providers) κλείσει τη δραστηριότητά του είναι επίσης θέματα που απασχολούν τους δυνητικούς χρήστες

του cloud.Η σειρά ISO 27001 αντιμετωπίζει ορισμένες από αυτές τις ανησυχίες, αλλά ένα νέο πρότυπο, το ISO/IEC 27017 Informationtechnology - Security techniques, προχωράει παραπέρα και προσφέρει μεγαλύτερη ηρεμία στους δυνητικούς πελάτες του cloud, τυπικά πρότυπα για το νέφος και τεχνικά πρότυπα που αφορούν τους ελέγχους του παρόχου υπηρεσιών νέφους και τις οδηγίες που απευθύνονται στον πάροχο υπηρεσιών νέφους. Αυτό που είναι μοναδικό και εξαιρετικά χρήσιμο στο ISO/IEC 27017 είναι ότι παρέχει καθοδήγηση και συμβουλές τόσο στον CSP όσο και στον πελάτη υπηρεσιών cloud. Εκτός από τη διασφάλιση της ασφάλειας των υπηρεσιών, το ISO/IEC 27017 στοχεύει επίσης στην ενημέρωση των πελατών σχετικά με το τι πρέπει να ζητούν από τον πάροχό τους (Jimmy, 2024).

Το πρότυπο παρέχει καθοδήγηση για 37 απο τους 114 ελέγχους του ISO/IEC 27002, αλλά περιλαμβάνει και επτά νέους ελέγχους.

- CLD(Control Objectives and Controls).6.3.1: Η συμφωνία για τις κοινές ή κατανεμημένες ευθύνες μεταξύ πελάτη και παρόχου σχετικά με τους ρόλους ασφάλειας πληροφοριών που σχετίζονται με τις υπηρεσίες νέφους πρέπει να καθορίζεται, να καταγράφεται και να κοινοποιείται με σαφήνεια.

- CLD.8.1.5: Αντιμετωπίζεται ο τρόπος με τον οποίο τα δεδομένα των πελατών επιστρέφονται ή αφαιρούνται από το νέφος όταν λήγει η σύμβαση/συμφωνία μεταξύ πελάτη και παρόχου (Jimmy, 2024).

- CLD.9.5.1: Ο πάροχος πρέπει να προστατεύει και να διαχωρίζει το εικονικό περιβάλλον του πελάτη από άλλους πελάτες και εξωτερικά μέρη.

- CLD.9.5.2: Ο πελάτης και ο πάροχος πρέπει να διασφαλίζουν ότι οι εικονικές μηχανές έχουν ρυθμιστεί ώστε να ανταποκρίνονται στις ανάγκες του οργανισμού.

- CLD.12.1.5: Ευθύνη του πελάτη να καθορίζει, να τεκμηριώνει και να παρακολουθεί τις διοικητικές λειτουργίες και διαδικασίες που σχετίζονται με το περιβάλλον cloud και απαίτηση του CSP να κοινοποιεί τεκμηρίωση σχετικά με κρίσιμες λειτουργίες και διαδικασίες, όταν και εφόσον το ζητούν οι πελάτες.

- CLD.12.4.5: Πώς οι δυνατότητες που προσφέρει ο πάροχος επιτρέπουν στον πελάτη να παρακολουθεί τη δραστηριότητα εντός του περιβάλλοντος υπολογιστικού νέφους.

- CLD.13.1.4: Πρέπει να γίνονται συνεπείς διαμορφώσεις ώστε το εικονικό περιβάλλον δικτύου να είναι σύμφωνο με την πολιτική ασφάλειας πληροφοριών του φυσικού δικτύου.

Έλεγχοι ασφαλείας: Δεν είναι μόνο ο διαχωρισμός των ευθυνών που το πρότυπο βοηθά στον καθορισμό: Το ISO/IEC 27017 αναλύει επίσης πολύ περισσότερο τον τύπο των ελέγχων ασφαλείας που πρέπει να εφαρμόζουν οι πάροχοι υπηρεσιών, συμβάλλοντας στη μείωση των εμποδίων για την υιοθέτηση του νέφους.Το ISO/IEC 27017 προσφέρει έναν τρόπο για τους παρόχους υπηρεσιών νέφους να δηλώνουν το επίπεδο των ελέγχων που έχουν εφαρμοστεί. Αυτό σημαίνει ότι τεκμηριωμένα αποδεικτικά στοιχεία, υποστηριζόμενα από ανεξάρτητες πηγές, όπως η πιστοποίηση σύμφωνα με ορισμένα πρότυπα, δείχνουν ότι έχουν εφαρμοστεί οι κατάλληλες πολιτικές και, κυρίως, ποιοι τύποι ελέγχων έχουν εισαχθεί. Οι πληροφορίες αυτές θα πρέπει να κοινοποιούνται στον πελάτη του cloud πριν από την υπογραφή οποιασδήποτε σύμβασης, ώστε να συμβάλλουν στην άμβλυνση τυχόν προβλημάτων στο μέλλον.Σε περιπτώσεις όπου οι ανεξάρτητοι έλεγχοι δεν είναι πρακτικοί ή θα αποτελούσαν μεγαλύτερο κίνδυνο για την ασφάλεια των πληροφοριών, το πρότυπο παρέχει στους CSP τη δυνατότητα αυτοαξιολόγησης.Σε αυτή την περίπτωση, ο CSP πρέπει να ενημερώνει τους πελάτες ότι έχει κάνει αυτή την ενέργεια (Jimmy, 2024).

3.2 Επισκόπηση του ISO 27018 (προστασία της ιδιωτικής ζωής στο νέφος)

Η προστασία των προσωπικών πληροφοριών δεν έχει ποτέ αποτελέσει υψηλότερη προτεραιότητα. Πολλοί εθνικοί και διεθνείς οργανισμοί, όπως ο Διεθνής Οργανισμός Τυποποίησης (ISO), η κυβέρνηση των ΗΠΑ και η Ευρωπαϊκή Ένωση, λαμβάνουν μέτρα για την αντιμετώπιση αυτού του ζητήματος. Μια κοινή τους πρωτοβουλία είναι το διεθνές πρότυπο ISO/IEC 27018 (Sun, 2020).

Το ISO/IEC 27018 είναι ένας κώδικας πρακτικής για την προστασία των προσωπικά αναγνωρίσιμων πληροφοριών σε δημόσιες υπηρεσίες νέφους.Είναι δομημένο ως επέκταση του ISO/IEC 27002 για τους ελέγχους ασφάλειας πληροφοριών. Τι ακριβώς προσφέρει λοιπόν το ISO/IEC 27018 στους πελάτες των υπηρεσιών cloud και γιατί είναι σημαντικό; Η πιθανή έκθεση των προσωπικών δεδομένων βρίσκεται στην κορυφή της διεθνούς ατζέντας. Ο συντριπτικός αριθμός παραβιάσεων ασφαλείας μεγάλου ρίσκου έχει εστιάσει την προσοχή των ανθρώπων στο πώς πρέπει να προστατεύονται τα προσωπικά τους στοιχεία. Στον κατάλογο των παραβιάσεων και τον αριθμό των ατόμων που επηρεάστηκαν: από το Γραφείο Διαχείρισης Προσωπικού των ΗΠΑ κλάπηκαν δεδομένα για πάνω από 21 εκατομμύρια κυβερνητικούς υπαλλήλους και η επίθεση στην Carphone Warehouse στο Ηνωμένο Βασίλειο επηρέασε περισσότερους από 2 εκατομμύρια πελάτες της. Αυτά αποτελούν μόνο την κορυφή του παγόβουνου των επιθέσεων σε διάστημα τριών μηνών το 2015 (Sun, 2020).

Το 2015 παραβιάστηκαν περίπου 707,5 εκατομμύρια αρχεία δεδομένων, σύμφωνα με το Breach LevelIndex. Παρά το τεράστιο αυτό νούμερο, οι εταιρείες συνεχίζουν να αυξάνουν τις δαπάνες τους για την ασφάλεια. Σύμφωνα με στοιχεία της IDC, οι παγκόσμιες δαπάνες για την ασφάλεια της πληροφορικής αναμενόταν να φτάσουν τα 101,6 δισεκατομμύρια δολάρια έως το 2020.

Ωστόσο, πέρα από τις εξωτερικές απειλές, ένας από τους πιο ύπουλους κινδύνους είναι αυτός των εσωτερικών παραγόντων, δηλαδή των υπαλλήλων που, είτε σκόπιμα είτε κατά λάθος, αφήνουν μια εταιρεία εκτεθειμένη σε επιθέσεις. Οι εσωτερικές απειλές είναι ιδιαίτερα επικίνδυνες, καθώς συχνά δεν αναφέρονται ή καλύπτονται. Σύμφωνα με έρευνα της PricewaterhouseCoopers, το 75% των οργανισμών που υπέστησαν παραβιάσεις ασφαλείας από υπαλλήλους δεν απευθύνθηκαν στις διωκτικές αρχές ούτε προχώρησαν σε νομικές ενέργειες. Αυτό σημαίνει ότι οι πελάτες αυτών των οργανισμών παραμένουν εκτεθειμένοι, ενώ οι εταιρείες που ενδέχεται να προσλάβουν στο μέλλον αυτά τα άτομα δεν γνωρίζουν το παρελθόν τους, αυξάνοντας έτσι τον κίνδυνο νέων επιθέσεων.

Ένα σημαντικό ποσοστό των παραβιάσεων δεδομένων, συγκεκριμένα το 64% κατά το πρώτο εξάμηνο του 2016, αφορά την κλοπή ταυτότητας. Αυτό έχει προκαλέσει έντονη ανησυχία σχετικά με τον τρόπο προστασίας των προσωπικών δεδομένων, ειδικά όταν αυτά αποθηκεύονται στο υπολογιστικό νέφος (cloud) ή όταν εμπιστεύονται παρόχους υπηρεσιών νέφους (CSP). Για να αντιμετωπίσει αυτές τις προκλήσεις, η Ευρωπαϊκή Ένωση έχει εφαρμόσει τον Γενικό Κανονισμό για την Προστασία Δεδομένων (GDPR), με στόχο την εναρμόνιση της νομικής κατάστασης σε ολόκληρη την Ευρώπη. Παρόλα αυτά, εξακολουθούν να υπάρχουν σημαντικές δυσκολίες για τους παρόχους υπηρεσιών cloud, καθώς κάθε χώρα της Ευρώπης έχει διαφορετικούς νόμους περί προστασίας δεδομένων, καθιστώντας τη λειτουργία τους περίπλοκη ((Breach LevelIndex (Έρευνα 2015), IDC (International Data Corporation, Εκτίμηση 2020), Έρευνα της PricewaterhouseCoopers (Έρευνα 2016)) .

Το υπολογιστικό νέφος διασχίζει τα διεθνή σύνορα, ενώ οι νόμοι που διέπουν την ασφάλεια των δεδομένων είναι κυρίως ανά χώρα.Μέρος του προβλήματος ήταν επίσης ο τρόπος με τον οποίο οι οργανισμοί διατηρούν τα δεδομένα - υπάρχει νομικός διαχωρισμός όσον αφορά τους παρόχους υπηρεσιών νέφους. Εδώ επικεντρώνονται οι φόβοι σχετικά με τους παρόχους υπηρεσιών CSP: όλοι οι πάροχοι υπηρεσιών CSP μιλούν ευχαρίστως για την εμπειρογνωμοσύνη τους στον τομέα της ασφάλειας, το ποσό που δαπανούν για την

προστασία των δεδομένων και τα φυσικά εμπόδια που θέτουν σε εφαρμογή για την αποτροπή παραβιάσεων, αλλά υπάρχει υποβόσκουσα ανησυχία σχετικά με το κατά πόσον οι πάροχοι υπηρεσιών CSP θα αντιμετωπίσουν τα προσωπικά και εμπιστευτικά δεδομένα με τον ίδιο τρόπο που θα το έκαναν οι πελάτες τους. Ενώ η Ευρωπαϊκή Ένωση εισάγει κάποια συνοχή στο πεδίο της προστασίας των δεδομένων, οι ΗΠΑ έχουν να αντιμετωπίσουν μια διαφορετική κατάσταση: στις ΗΠΑ δεν υπάρχει εθνικός νόμος που να ρυθμίζει τον τρόπο χειρισμού των προσωπικών δεδομένων. Οι διαφορετικές πολιτικές των επιμέρους πολιτειών μπορούν να προκαλέσουν σύγχυση. Αυτό επιδεινώνεται από τις διαφορετικές κανονιστικές απαιτήσεις σε διάφορους κλάδους. Όλοι αυτοί οι παράγοντες συνδυάζονται και καθιστούν τη διαμόρφωση μιας συνεκτικής πολιτικής δεδομένων μάλλον δύσκολη. Σε μια προσπάθεια να αρχίσει να αντιμετωπίζεται αυτή η έλλειψη, τον Αύγουστο του 2015, το Εθνικό Ινστιτούτο Τεχνολογίας Προτύπων συμβούλεψε τις ομοσπονδιακές υπηρεσίες να «χρησιμοποιούν τα σχετικά διεθνή πρότυπα για την ασφάλεια στον κυβερνοχώρο, όπου είναι αποτελεσματικά και κατάλληλα, στις δραστηριότητες αποστολής και χάραξης πολιτικής » (Sun, 2020).

3.3 Σημασία της συμμόρφωσης με τα πρότυπα ISO 27017 & 27018 στην ασφάλεια του νέφους

Η χρήση υβριδικών αρχιτεκτονικών νέφους έχει καταστεί κρίσιμη για πολλές επιχειρήσεις, ιδίως όταν πρόκειται για την ασφαλή και αποδοτική διαχείριση δεδομένων. Αυτή η προσέγγιση συνδυάζει υπηρεσίες νέφους, όπως το Azure, με υφιστάμενες υποδομές, και εγείρει προκλήσεις για τη συμμόρφωση και την ασφάλεια. Στο παρακάτω κείμενο περιγράφεται η διαδικασία αξιολόγησης κινδύνων που πραγματοποιήθηκε, βασιζόμενη σε διεθνή πρότυπα και πρακτικές, με σκοπό τη διασφάλιση της ασφάλειας των δεδομένων και τη συμμόρφωση με τις ισχύουσες κανονιστικές απαιτήσεις.

Η αξιολόγηση κινδύνων πραγματοποιήθηκε σύμφωνα με τα δεδομένα της υβριδικής αρχιτεκτονικής νέφους που χρησιμοποιούν εφαρμογές βασισμένες στο Azure (SaaS) και τις διεπαφές των υποδομών κεντρικού υπολογιστικού κέντρου (back-end data center) συστημάτων. Η μεθοδολογία της αξιολόγησης στηρίχθηκε στην κοινή κατανόηση του υφιστάμενου Συστήματος Διαχείρισης Ασφάλειας Πληροφοριών (ISMS) του ISO 27001 και στις νέες εφαρμογές που περιγράφηκαν.

Κατά τη διάρκεια της διαδικασίας, εξετάστηκαν διάφορα πρότυπα, όπως το ISO 27001 (Διαχείριση Ασφάλειας Πληροφοριών), το ISO 27017 (Ασφάλεια στο Νέφος) και το ISO 27018 (Προστασία Προσωπικών Δεδομένων στο Νέφος), καθώς και οι συνέπειες που έχει η

υιοθέτηση των τεχνολογιών cloud του Azure στη διαχείριση και τον οργανισμό (Parast et al., 2022).

Επιπλέον, ο καθορισμός ενός συγκεκριμένου πλαισίου συμμόρφωσης αποτέλεσε βασικό στοιχείο της διαδικασίας αξιολόγησης κινδύνου. Τα διάφορα εμπορικά πλαίσια ελέγχου που εξετάστηκαν περιλαμβάνουν τα πρότυπα ISO 27001/27002, PCI DSS, NIST και NERC CIP. Παράλληλα, λήφθηκαν υπόψη κυβερνητικά πρότυπα συμμόρφωσης όπως τα FISMA, FedRAMP, DFARS, CJIS και HIPAA. Η ενσωμάτωση αυτών των πλαισίων επιτρέπει την εφαρμογή τεχνολογικών και διοικητικών πρακτικών που βελτιώνουν τη συμμόρφωση και μειώνουν τον κίνδυνο ασφαλείας στις υβριδικές αρχιτεκτονικές νέφους(Parast et al., 2022).

Η αξιολόγηση κινδύνων και οι συστάσεις που παρατίθενται κατωτέρω αφορούν τους τομείς ασφάλειας που είναι κατάλληλοι για το γενικό πεδίο εφαρμογής της ασφάλειας SaaS στο περιβάλλον Azure:

1. Διακυβέρνηση ασφάλειας, διαχείριση προμηθευτών και διαχείριση κινδύνων: Ποιες οργανωτικές δομές διακυβέρνησης, διαχείρισης προμηθευτών και διαχείρισης κινδύνων θα πρέπει να υπάρχουν και πώς θα πρέπει να διαμορφωθούν οι υποστηρικτικές διαδικασίες και οι έλεγχοι στο σωστό μέγεθος για τον οργανισμό;

2. Ασφάλεια εφαρμογών: Πώς θα πρέπει μια εταιρεία να προστατεύει τις εφαρμογές της από επιθέσεις στον κυβερνοχώρο (π.χ. OWASP top 10), να διασφαλίζει την ασφάλεια της διεπαφής προγράμματος εφαρμογής (API) και να ενσωματώνει με ασφάλεια τα στοιχεία του συστήματος που βρίσκονται σε τοπικό επίπεδο με τα στοιχεία στο περιβάλλον Microsoft Azure; (Parast et al., 2022).

3. Ασφάλεια δικτύου: Πώς πρέπει να διασυνδέεται το περιβάλλον υβριδικών εφαρμογών νέφους με την παραδοσιακή ασφάλεια δικτύου;

4. Ασφάλεια δεδομένων: Πώς θα πρέπει να προστατεύονται τα δεδομένα των πελατών και οι προσωπικές πληροφορίες(π.χ. κρυπτογράφηση, tokenization, συσκότιση, πρόληψη διαρροής δεδομένων (DLP) κ.λπ.)

5. Διαχείριση ταυτότητας και πρόσβασης: Πώς θα πρέπει να ενσωματωθούν οι τεχνολογίες και οι πρακτικές IAM;

6. Παρακολούθηση της ασφάλειας: Ποιες τεχνολογίες και πρακτικές παρακολούθησης απαιτούνται;

7. Αντιμετώπιση περιστατικών: Ποιες διαδικασίες και πρωτόκολλα επικοινωνίας απαιτούνται για την αντίδραση και ανταπόκριση σε περίπτωση συμβάντος διαρροής δεδομένων ή άλλων περιστατικών;

8. Επιχειρησιακή συνέχεια/αποκατάσταση από καταστροφές: Πώς μπορεί να διασφαλιστεί η διαθεσιμότητα και η ανθεκτικότητα της υπηρεσίας υβριδικού νέφους; (Parast et al., 2022).

3.4 Κατευθυντήριες γραμμές εφαρμογής για το ISO 27017 & 27018

Ο οργανισμός ISO ανακοίνωσε επίσημα το πρότυπο ISO 27017 τον Δεκέμβριο του 2015, ο πελάτης υπηρεσιών νέφους (CSC) και ο πάροχος υπηρεσιών νέφους (CSP) μπορούν να ανατρέξουν στις προδιαγραφές εργασίας, να βελτιστοποιήσουν την ασφάλεια στις υπηρεσίες νέφους με βάση το ISO 27001.

Ειδικότερα, το ISO/IEC 27018 καθορίζει κατευθυντήριες γραμμές με βάση το ISO/IEC 27002, λαμβάνοντας υπόψη τις κανονιστικές απαιτήσεις για την προστασία των προσωπικών δεδομένων που ενδέχεται να ισχύουν στο πλαίσιο του περιβάλλοντος(-ων) κινδύνου ασφάλειας πληροφοριών ενός παρόχου δημόσιων υπηρεσιών νέφους. μια σημαντική αύξηση των χρηστών των υπηρεσιών νέφους τα τελευταία χρόνια, αλλά για την προστασία αυτού του μέρους των δεδομένων νέφους είναι σχετικά ανεπαρκής.

Το ISO/IEC 27018 καθορίζει κοινά αποδεκτούς στόχους ελέγχου, ελέγχους και κατευθυντήριες γραμμές για την εφαρμογή μέτρων προστασίας των προσωπικών πληροφοριών που μπορούν να αναγνωριστούν (PII) σύμφωνα με τις αρχές προστασίας της ιδιωτικής ζωής του ISO/IEC 29100 για το περιβάλλον του δημόσιου υπολογιστικού νέφους.Ειδικότερα, το ISO/IEC 27018 καθορίζει κατευθυντήριες γραμμές με βάση το ISO/IEC 27002, λαμβάνοντας υπόψη τις κανονιστικές απαιτήσεις για την προστασία των PII που ενδέχεται να ισχύουν στο πλαίσιο του(των) περιβάλλοντος(-ων) κινδύνου ασφάλειας πληροφοριών ενός παρόχου υπηρεσιών δημόσιου υπολογιστικού νέφους (Abdulsalam & Hedabou, 2021).

4. Βασικά στοιχεία της ασφάλειας του νέφους

Σε αυτή την ενότητα, η εργασία εστιάζει κυρίως στις διάφορες κατηγορίες θεμάτων ασφάλειας που σχετίζονται με το υπολογιστικό νέφος, καθώς και στις λύσεις που έχουν προταθεί για την αντιμετώπισή τους. Αρχικά, γίνεται μια συνοπτική παρουσίαση του ζητήματος της ασφάλειας στο νέφος, ενώ στη συνέχεια αναλύονται οι προτεινόμενες απαντήσεις.

Ένα ζήτημα ασφάλειας μπορεί να περιλαμβάνει επιθέσεις, λανθασμένες διαμορφώσεις, σφάλματα, ζημιές, παραβιάσεις δεδομένων ή κενά ασφαλείας. Είναι σημαντικό να σημειωθεί ότι τα θέματα ασφάλειας στο νέφος διαφέρουν από τα γενικά θέματα ασφάλειας, λόγω των ιδιαίτερων χαρακτηριστικών της κατανεμημένης πληροφορικής, όπως ορίζονται από το Εθνικό Ινστιτούτο Προτύπων και Τεχνολογίας (NIST). Οι ρυθμίσεις ασφαλείας στο νέφος είναι συχνά πιο περίπλοκες λόγω αυτών των χαρακτηριστικών. Το υπολογιστικό νέφος, ως συνδυασμός τεχνολογίας, διαδικασιών, ανθρώπων και εμπορικών πρακτικών, παρουσιάζει, όπως κάθε άλλη τεχνολογία, ορισμένα τρωτά σημεία.

Η έρευνα κατηγοριοποιεί τα θέματα ασφάλειας σε διάφορες κατηγορίες, όπως:

- Θέματα ασφάλειας αποθήκευσης δεδομένων και υπολογισμού.
- Θέματα ασφάλειας εικονικοποίησης.
- Θέματα ασφάλειας που σχετίζονται με το Διαδίκτυο και τις υπηρεσίες.
- Θέματα ασφάλειας δικτύου.
- Θέματα ελέγχου πρόσβασης.
- Θέματα ασφάλειας λογισμικού.
- Θέματα διαχείρισης εμπιστοσύνης.
- Θέματα συμμόρφωσης και νομικά ζητήματα.

Τα ζητήματα που αφορούν την αποθήκευση δεδομένων, την εικονικοποίηση και τα στάδια υπολογισμού εντάσσονται στα μοντέλα παροχής υπηρεσιών cloud. Επίσης, η μελέτη εξετάζει θέματα που συνδέονται με το Διαδίκτυο και καταλήγει σε ανάλυση θεμάτων εμπιστοσύνης και νομικών ζητημάτων (Ali et al., 2020).

1) Θέματα ασφάλειας αποθήκευσης δεδομένων και υπολογισμού

Τα δεδομένα αποτελούν θεμελιώδες κομμάτι του υπολογιστικού νέφους. Τα δεδομένα που τοποθετούνται στο νέφος είναι απομονωμένα από τους πελάτες. Στην απομακρυσμένη αποθήκευση ή στην αποθήκευση από τρίτους (παρόχους), το θεμελιώδες ζήτημα είναι ότι ο πελάτης δεν αντιλαμβάνεται τι συμβαίνει με τη χωρητικότητα των δεδομένων στο νέφος. Ο ιδιοκτήτης των δεδομένων δεν γνωρίζει την τοποθεσία των δεδομένων, τις διαδικασίες ασφαλείας και τα συστήματα ασφαλείας που χρησιμοποιούνται για την εξασφάλιση των πληροφοριών του. Η διαχείριση αποτελεί κεντρικό ζήτημα στην κατανεμημένη αποθήκευση δεδομένων. Ο πάροχος υπηρεσιών αποθήκευσης στο νέφος χρειάζεται αξιόπιστες και νόμιμες μεθόδους, καθώς και συστήματα που εξασφαλίζουν την αποτελεσματική, σταθερή και ποιοτική αποθήκευση των δεδομένων στο νέφος. Οι πληροφορίες των πελατών αποθηκεύονται σε φάρμες διακομιστών (data farms), οι οποίες συνήθως βρίσκονται υπό τον έλεγχο του παρόχου υπηρεσιών νέφους.

Μεγάλοι οργανισμοί προσφέρουν κατανεμημένη αποθήκευση σε εξαιρετικά χαμηλό κόστος, καθιστώντας την πρόσβαση σε αυτές τις υπηρεσίες ευρέως εφικτή. Τα δεδομένα που αποθηκεύονται στο νέφος είναι συχνά πλεονασματικά (redundant) και διανέμονται σε διαφορετικές γεωγραφικές περιοχές για λόγους ανθεκτικότητας και διαθεσιμότητας. Παράλληλα, η πλεονάζουσα παροχή ενέργειας και τα αποτελεσματικά συστήματα ψύξης στις φάρμες διακομιστών εξασφαλίζουν ότι οι πληροφορίες παραμένουν διαθέσιμες και προστατευμένες ανά πάσα στιγμή.

Τέλος, με τη χρήση προηγμένων μεθόδων κατανομής και διαχείρισης αποθηκευτικού χώρου, ο χώρος αποθήκευσης στο νέφος μπορεί να χρησιμοποιηθεί και να ανακυκλωθεί πιο αποδοτικά, μειώνοντας τα περιττά κόστη και βελτιώνοντας τη συνολική απόδοση των υπηρεσιών (Ali et al., 2020).

Το πλεόνασμα πληροφοριών (data redundancy) αποτελεί βασική μέθοδο για την εξασφάλιση υψηλής διαθεσιμότητας των δεδομένων στο υπολογιστικό νέφος. Μέσω αυτής της διαδικασίας, τα δεδομένα αντιγράφονται και αποθηκεύονται σε έναν εφεδρικό διακομιστή. Έτσι, σε περίπτωση σοβαρού προβλήματος ή αστοχίας στη φάρμα ενός διακομιστή, ο πάροχος υπηρεσιών μπορεί να ανακτήσει τις πληροφορίες από τον εφεδρικό διακομιστή. Αυτή η μέθοδος εξασφαλίζει την απρόσκοπτη πρόσβαση και προστασία των δεδομένων.

Επιπλέον, η κρυπτογράφηση αποτελεί ουσιώδη μηχανισμό για την ασφάλεια του νέφους. Μετατρέπει τα δεδομένα από απλό κείμενο (plaintext) σε κρυπτογραφημένη μορφή (ciphertext), καθιστώντας τα μη αναγνώσιμα χωρίς το κατάλληλο κλειδί αποκρυπτογράφησης. Η ισχύς της ασφάλειας εξαρτάται άμεσα από την αποτελεσματικότητα του αλγορίθμου κρυπτογράφησης και τη διαχείριση του κλειδιού.

Είναι κρίσιμο οι μέθοδοι κρυπτογράφησης να εφαρμόζονται προσεκτικά και με ισχυρά συστήματα, καθώς η συνολική ασφάλεια βασίζεται στη μυστικότητα και την ακεραιότητα του κλειδιού. Χωρίς αυτά τα μέτρα, η προστασία των δεδομένων έναντι πιθανών επιθέσεων ή μη εξουσιοδοτημένης πρόσβασης είναι δύσκολο να διασφαλιστεί (Ali et al., 2020).

2) Ζητήματα ασφάλειας εικονοποίησης

Ο βασικός λόγος για την ευρεία αποδοχή του cloud computing από τις επιχειρήσεις είναι η τεχνολογία εικονικοποίησης (virtualized cloud computing). Για να αξιοποιηθεί πλήρως το επιχειρηματικό δυναμικό του υπολογιστικού νέφους, οι πάροχοι υπηρεσιών απαιτούν υψηλά επίπεδα εμπιστοσύνης στα εικονικά μηχανήματα (Virtual Machines - VM). Στο περιβάλλον του νέφους, η εικονικοποίηση αποτελεί θεμελιώδη προϋπόθεση για τη διαχείριση και την αποτελεσματική λειτουργία των υπηρεσιών.

Η έννοια της πολλαπλής μίσθωσης (multi-tenancy) και η χρήση της εικονικοποίησης προσφέρουν σημαντικά οφέλη, όπως οικονομίες κλίμακας και βελτιστοποίηση πόρων. Ωστόσο, αυτά τα πλεονεκτήματα συνοδεύονται από προκλήσεις, καθώς οι τεχνολογίες αυτές δεν είναι απαλλαγμένες από κινδύνους και απειλές. Πολλοί κακόβουλοι χρήστες επιτίθενται σε κοινόχρηστες περιοχές των διακομιστών με στόχο να αποκτήσουν πρόσβαση σε ευαίσθητα δεδομένα ή να επηρεάσουν τις παρεχόμενες υπηρεσίες.

Για να αντιμετωπιστούν αυτές οι απειλές, οι ερευνητές και οι ειδικοί αναπτύσσουν στρατηγικές που εξασφαλίζουν νομικό, λογικό και εικονικό διαχωρισμό των δεδομένων και των πόρων μεταξύ των χρηστών. Αυτή η διαδικασία είναι απαραίτητη για τη διασφάλιση της εμπιστευτικότητας, της ακεραιότητας και της διαθεσιμότητας στο υπολογιστικό νέφος (Jimmy, 2024).

3) Θέματα ασφάλειας που σχετίζονται με το Διαδίκτυο και τις υπηρεσίες

Η υποδομή νέφους δημιουργείται με πολλές διοικήσεις και περιουσιακά στοιχεία, καθώς και με τον απαιτούμενο μεταφορέα που μεταδίδει τις πληροφορίες μεταξύ αποστολέα και παραλήπτη. Το Διαδίκτυο είναι φορέας διότι μεταδίδει τον σημαντικό αριθμό δεσμών από την πηγή στον στόχο ως προηγμένη πληροφορία. Η πληροφορία περνά από διάφορους κόμβους, οπότε δεν είναι προστατευμένη. Εξαιτίας ενός κεκτημένου ζητήματος με το Web 2.0 αναπτύχθηκαν πολλά νέα είδη κινδύνων. Το Διαδίκτυο καταχράται πολυάριθμα θέματα ασφάλειας, όπως επιθέσεις MitM, IP spoofing, σάρωση θύρας, ενέσεις κακόβουλου λογισμικού και packet sniffing. Η πρόσβαση στις υπηρεσίες cloud και η διαχείρισή τους γίνεται μέσω του διαδικτύου και του προγράμματος περιήγησης στο διαδίκτυο, το οποίο δεν αποτελεί ασφαλή λύση για τους τελικούς χρήστες. Υπάρχουν πολυάριθμες ρυθμίσεις ασφαλείας που είναι προσβάσιμες, αλλά τα άτομα αποδέχονται ότι οι πληροφορίες που ανταλλάσσονται μέσω του Διαδικτύου δεν είναι ασφαλείς (Jimmy, 2024).

4) Θέματα ασφάλειας δικτύου

Το δίκτυο αποτελεί θεμελιώδες στοιχείο του υπολογιστικού νέφους. Ως εκ τούτου, τα ζητήματα ασφάλειας και λειτουργίας δεν περιορίζονται μόνο στο επίπεδο των εικονικών μηχανών (Virtual Machines - VM), της διαχείρισης ή των εφαρμογών, αλλά επεκτείνονται και στο επίπεδο του δικτύου. Τα προβλήματα στο επίπεδο του συστήματος μπορούν να επηρεάσουν άμεσα το πλαίσιο λειτουργίας του νέφους.

Η δυναμική φύση της αρχιτεκτονικής του νέφους καθιστά τα ζητήματα δικτύου εξίσου σημαντικά τόσο για τα εσωτερικά όσο και για τα εξωτερικά συστήματα. Για παράδειγμα, ένας κακόβουλος χρήστης μπορεί να εκτελέσει μια επίθεση άρνησης υπηρεσίας (Denial of Service - DoS) με στόχο να διαταράξει την προσβασιμότητα των υπηρεσιών. Μια τέτοια επίθεση μπορεί επίσης να επηρεάσει αρνητικά τη μετάδοση δεδομένων εντός του συστήματος, οδηγώντας σε αυξημένη συμφόρηση στο δίκτυο.

Η διασφάλιση της απρόσκοπτης λειτουργίας του δικτύου είναι ζωτικής σημασίας για την ομαλή παροχή υπηρεσιών στο υπολογιστικό νέφος, καθιστώντας τις στρατηγικές πρόληψης και ανίχνευσης επιθέσεων απαραίτητες για τη συνολική του ασφάλεια (Jimmy, 2024).

5) Θέματα ελέγχου πρόσβασης

Η ασφάλεια ελέγχου πρόσβασης είναι απαραίτητη για την προστασία των δεδομένων από μη εξουσιοδοτημένη χρήση. Σε περιβάλλοντα cloud με πολλούς χρήστες, όπου η πρόσβαση σε υπηρεσίες γίνεται μέσω διαφόρων διεπαφών (όπως web εφαρμογές ή API), η ανάγκη για ισχυρά μέτρα ασφάλειας είναι ακόμη μεγαλύτερη. Οι παραδοσιακοί μέθοδοι επαλήθευσης ταυτότητας, που συνδυάζουν ένα όνομα χρήστη ή διεύθυνση email με έναν κωδικό πρόσβασης, δεν επαρκούν πλέον.

Για να αντιμετωπιστεί αυτό το πρόβλημα, οι οργανισμοί πρέπει να υιοθετήσουν πιο σύνθετους μηχανισμούς ελέγχου πρόσβασης, όπως η πολυπαραγοντική επαλήθευση ταυτότητας (multi-factor authentication). Επιπλέον, είναι σημαντικός ο λεπτομερής διαχωρισμός των εξουσιοδοτήσεων, ώστε κάθε χρήστης να έχει πρόσβαση μόνο στα απαραίτητα δεδομένα και λειτουργίες. Αυτή η αρχή, γνωστή ως "least privilege principle", συμβάλλει στην ελαχιστοποίηση των επιπτώσεων σε περίπτωση παραβίασης της ασφάλειας.(Sun, 2020).

6) Θέματα ασφάλειας λογισμικού

Η αυξανόμενη πολυπλοκότητα των σύγχρονων λογισμικών συστημάτων, που χαρακτηρίζεται από την ύπαρξη ετερόκλητων γλωσσών προγραμματισμού και εκτεταμένων βάσεων κώδικα, ενισχύει σημαντικά την επιφάνεια επίθεσης και καθιστά την εγγυημένη ασφάλεια ενός συστήματος εξαιρετικά απαιτητική. Παρότι η τήρηση αυστηρών προτύπων και κανόνων κωδικοποίησης αποτελεί βασικό παράγοντα για την ανάπτυξη ασφαλούς λογισμικού, η πιθανότητα εισαγωγής κρυπτών ευπάθειών, ακόμη και από έμπειρους προγραμματιστές, παραμένει υψηλή. Αυτό υποδηλώνει ότι η ασφάλεια του λογισμικού αποτελεί ένα πολυδιάστατο πρόβλημα που απαιτεί συνεχή έρευνα και ανάπτυξη νέων μεθοδολογιών και εργαλείων. (Sun, 2020).

7) Θέματα διαχείρισης εμπιστοσύνης

Η εμπιστοσύνη αποτελεί κρίσιμο παράγοντα για την επιτυχή υλοποίηση υπηρεσιών υπολογιστικού νέφους. Η ανάγκη για διασφάλιση της εμπιστοσύνης μεταξύ παρόχου και καταναλωτή υπηρεσιών νέφους προκύπτει από την ανάθεση ευαίσθητων επιχειρηματικών δεδομένων και πόρων. Η εμπιστοσύνη αυτή συνδέεται άρρηκτα με την αξιοπιστία των υποκείμενων υποδομών και τεχνολογιών, όπως συστήματα αποθήκευσης, δίκτυα, αλγόριθμοι

και μηχανισμοί εικονικοποίησης. Οι παράγοντες που υπονομεύουν την εμπιστοσύνη σε περιβάλλοντα νέφους είναι πολυεπίπεδοι και απαιτούν διεξοδική ανάλυση.

8) Θέματα συμμόρφωσης και νομικής ασφάλειας

Το Service Level Agreement είναι ένα έγγραφο που παίζει σημαντικό ρόλο στο επιχειρηματικό μοντέλο του νέφους. Περιέχει μια συμφωνία μεταξύ των δύο επικοινωνούντων μερών, με όλες τις πληροφορίες που σχετίζονται με την υπηρεσία,καθώς και τους όρους και τις προϋποθέσεις της υπηρεσίας. Η SLA υπογράφεται και από τα δύο μέρη για να δείξει ότι συμφωνούν με τη συμφωνία αυτή (Parast et al., 2022).

Διαχείριση ταυτότητας και πρόσβασης (IAM)

Η διαχείριση ταυτοτήτων και πρόσβασης (IAM) αποτελεί έναν κρίσιμο πυλώνα της ασφάλειας πληροφοριών στις σύγχρονες επιχειρήσεις. Είναι η διαδικασία που αφορά την παροχή, τη διαχείριση και τον έλεγχο της πρόσβασης των χρηστών σε πόρους πληροφοριών, εφαρμογές και συστήματα. Σε έναν κόσμο όπου οι κυβερνοεπιθέσεις γίνονται όλο και πιο συχνές και περίπλοκες, η αποτελεσματική διαχείριση των ταυτοτήτων είναι πιο σημαντική από ποτέ.

Η Ανάγκη για Διαχείριση Ταυτοτήτων και Πρόσβασης

Οι σύγχρονες επιχειρήσεις βασίζονται σε μια ποικιλία τεχνολογιών που απαιτούν διαφορετικά επίπεδα πρόσβασης και εξουσιοδότησης. Η διαχείριση αυτών των πολλαπλών ταυτοτήτων και ρόλων αποτελεί μια σημαντική πρόκληση για τα τμήματα πληροφορικής. Επιπλέον, οι αυξανόμενες απαιτήσεις για συμμόρφωση με κανονισμούς όπως ο GDPR αυξάνουν την ανάγκη για λεπτομερή έλεγχο και καταγραφή των δραστηριοτήτων των χρηστών.

Οι Παραδοσιακές Προσπάθειες για Διαχείριση IAM

Ιστορικά, οι επιχειρήσεις έχουν υιοθετήσει δύο κύριες στρατηγικές για τη διαχείριση των ταυτοτήτων:

A. Σημειακές λύσεις: Αυτές οι λύσεις εστιάζουν σε συγκεκριμένες ανάγκες, όπως η επαναφορά κωδικών πρόσβασης ή η διαχείριση δικαιωμάτων για συγκεκριμένες εφαρμογές. Αν και είναι εύκολες στην υλοποίηση, συχνά οδηγούν σε ένα αποσπασματικό περιβάλλον, όπου οι διαδικασίες και οι πολιτικές δεν είναι ενοποιημένες.

B. Ολοκληρωμένα πλαίσια IAM: Αυτά τα πλαίσια προσφέρουν μια πιο ολιστική προσέγγιση, παρέχοντας μια ενιαία πλατφόρμα για τη διαχείριση όλων των ταυτοτήτων και των σχετικών διαδικασιών. Ωστόσο, η υλοποίηση τους μπορεί να είναι πολύπλοκη και κοστοβόρα.

Οι Προκλήσεις της Διαχείρισης IAM

Παρά τις προσπάθειες που έχουν καταβληθεί, η διαχείριση των ταυτοτήτων εξακολουθεί να αντιμετωπίζει σημαντικές προκλήσεις, όπως:

- Πολυπλοκότητα: Η διαχείριση πολλών συστημάτων και εφαρμογών με διαφορετικές απαιτήσεις πρόσβασης δημιουργεί ένα πολύπλοκο περιβάλλον.
- Ασφάλεια: Η προστασία των ταυτοτήτων από απειλές όπως ο κλοπές κωδικών πρόσβασης και οι επιθέσεις phishing αποτελεί μια συνεχή πρόκληση.
- Συμμόρφωση: Οι αυστηροί κανονισμοί για την προστασία των δεδομένων απαιτούν από τις επιχειρήσεις να διατηρούν λεπτομερή αρχεία για όλες τις δραστηριότητες που σχετίζονται με την πρόσβαση.
- Κόστος: Η υλοποίηση και η διατήρηση ενός αποτελεσματικού συστήματος IAM μπορεί να είναι δαπανηρή (Yang et al., 2020).

Τα βασικά στοιχεία μιας νέας ενοποιημένης και έξυπνης λύσης για το IAM περιλαμβάνουν τα εξής:

- Ενσωμάτωση κάθε ταυτότητας σε μια ενιαία, προϋπάρχουσα ταυτότητα, όποτε αυτό είναι εφικτό.
- Ανάπτυξη ενός ενιαίου συνόλου προτεραιοτήτων, πολιτικών, δραστηριοτήτων και ελέγχου ταυτότητας για εκείνη την ενιαία ταυτότητα, η οποία συχνά διαχειρίζεται ένα πολύ μεγαλύτερο μέρος της επιχείρησης.
- Αντιμετώπιση κρίσιμων ζητημάτων με σημειακές λύσεις που είναι απολύτως συμβατές με τον ενοποιημένο τομέα ταυτότητας. Παραδείγματα περιλαμβάνουν τη χρήση ενιαίας σύνδεσης επιχείρησης με βάση το AD (Active Directory) σε πλατφόρμες που πρέπει να ενσωματωθούν με το AD, συμπεριλαμβανομένων των ειδικών για την πλατφόρμα υπηρεσιών διαχείρισης προνομίων που βασίζονται σε ρόλους και ταυτότητες τοy AD για προσαρμοσμένη ανάθεση προνομίων, μεταξύ άλλων.
- Ενοποίηση των πάντων (ενοποιημένων και μη ενοποιημένων συστημάτων) σε ένα σύστημα που κατανοεί και μετατρέπει όλους τους υφιστάμενους ρόλους,

κανονισμούς, διαδικασίες και βεβαιώσεις σε ένα συγκεκριμένο μοντέλο που επιτυγχάνει τον έλεγχο ταυτότητας χρησιμοποιώντας τους επιχειρηματικούς στόχους και τις τεχνικές δυνατότητες ως κινητήρια δύναμη (Yang et al., 2020).

4.2 Κρυπτογράφηση και διαχείριση κλειδιών

Δεδομένου ότι η κρυπτογράφηση είναι η κύρια μέθοδος που χρησιμοποιείται για τη διασφάλιση της ασφάλειας των δεδομένων, είναι φυσικό να αντιμετοπίσουμε το πρόβλημα της διαχείρισης των κλειδιών. Τα κλειδιά κρυπτογράφησης δεν μπορούν να αποθηκευτούν στο νέφος- ως εκ τούτου, ο πελάτης πρέπει να διαχειρίζεται και να ελέγχει ένα σύστημα διαχείρισης κλειδιών για οποιαδήποτε κρυπτογραφική μέθοδο χρησιμοποιείται. Για τα απλά σχήματα κρυπτογράφησης, μπορεί να μην υπάρχει πρόβλημα, δεδομένου ότι ένα και μόνο κλειδί κρυπτογράφησης και αποκρυπτογράφησης μπορεί να χρησιμοποιηθεί για ολόκληρο το σύστημα. Ωστόσο, σχεδόν κάθε πραγματική βάση δεδομένων απαιτεί ένα πιο σύνθετο σύστημα. Αυτό το απλό σύστημα για τη διαχείριση των κλειδιών θα πρέπει ίσως να έχει τη μορφή μιας μικρής βάσης δεδομένων, η οποία θα πρέπει να είναι μια ασφαλής τοπική βάση δεδομένων, γεγονός που και πάλι μπορεί να αναιρεί τον σκοπό της μεταφοράς της αρχικής βάσης δεδομένων στο νέφος (Yang et al., 2020).

Είναι σαφές ότι η διαχείριση των κλειδιών είναι ένα πραγματικό πρόβλημα για τα συστήματα cloud που χρησιμοποιούν κρυπτογράφηση, και έχει γίνει έρευνα για τη χρήση κρυπτογράφησης δύο επιπέδων που επιτρέπει την αποθήκευση του συστήματος διαχείρισης κλειδιών στο cloud. Αυτό το σύστημα είναι αποτελεσματικό και μπορεί να αποτελέσει τη λύση των προβλημάτων της διαχείρισης κλειδιών που αντιμετωπίζουν τα συστήματα νέφους- ωστόσο, δεν έχει ακόμη εφαρμοστεί ειδικά για στην κρυπτογράφηση βάσεων δεδομένων (Yang et al., 2020).

4.3 Ασφάλεια δικτύου

Οι εφαρμογές που αναπτύσσονται στο υπολογιστικό νέφος είναι πιθανό να αντιμετωπίσουν διάφορες επιθέσεις λόγω της εξάρτησής τους από το μοντέλο πελάτη-εξυπηρετητή. Ιδιαίτερα, οι εφαρμογές τύπου SaaS (Software as a Service) εμφανίζουν ευπάθειες σε κακόβουλο λογισμικό, όπως ιούς, σκουλήκια και δούρειους ίππους (Trojan). Οι ιοί μπορούν να διαδοθούν μέσω συνημμένων ηλεκτρονικού ταχυδρομείου, εγκατάστασης κακόβουλου λογισμικού ή μέσω του MBR (Master Boot Record) του λειτουργικού συστήματος που παρέχεται από το νέφος. Τα σκουλήκια είναι σε θέση να μεταφέρονται αυτόνομα μεταξύ συστημάτων, ενώ οι δούρειοι ίπποι είναι λογισμικό που εκτελείται με

κακόβουλες προθέσεις, διασπώντας τη λειτουργία του σε μέρη όταν φορτώνεται στη μνήμη. Οι SaaS εφαρμογές, βασιζόμενες σε υπηρεσίες και φυλλομετρητές ιστού, επηρεάζονται από προκλήσεις ασφαλείας που συνδέονται με το δίκτυο και τις διαδικτυακές υποδομές, ενώ οι υποδομές IaaS και PaaS, που εξαρτώνται από το υλικό, αντιμετωπίζουν επιπλέον προκλήσεις που απορρέουν από τα χαρακτηριστικά του υπολογιστικού νέφους (Amah et al., 2023).

Για την αντιμετώπιση αυτών των ζητημάτων ασφαλείας, η υποδομή δημόσιου κλειδιού (PKI) προτείνεται ως μία από τις πλέον κατάλληλες λύσεις. Η κρυπτογραφία ελλειπτικής καμπύλης (ECC), ως μία εκδοχή της κρυπτογραφίας δημόσιου κλειδιού, ξεχωρίζει για την αποτελεσματικότητά της. Η ECC μπορεί να διαδραματίσει κρίσιμο ρόλο στη βελτίωση της ασφάλειας και στη μείωση της κατανάλωσης ενέργειας, ιδιαίτερα στις επικοινωνίες των κινητών τηλεφώνων με τους παρόχους υπηρεσιών νέφους (CSPs). Η εφαρμογή της ECC υποδεικνύεται ως ένα πολλά υποσχόμενο αντικείμενο μελέτης για τη βελτιστοποίηση της ασφάλειας και της απόδοσης σε περιβάλλοντα υπολογιστικού νέφους (Amah et al., 2023).

4.4 Παρακολούθηση και καταγραφή ασφάλειας

Η ασφάλεια του υπολογιστικού νέφους είναι ένας πολύπλευρος τομέας που αποσκοπεί στην προστασία των δεδομένων, των εφαρμογών και των υποδομών που εμπλέκονται στο υπολογιστικό νέφος. Η παρακολούθηση και η καταγραφή της ασφάλειας αποτελούν κρίσιμα στοιχεία της ασφάλειας του υπολογιστικού νέφους, διασφαλίζοντας την ακεραιότητα, την εμπιστευτικότητα και τη διαθεσιμότητα των πόρων. Ακολουθούν τα βασικά στοιχεία που σχετίζονται με την παρακολούθηση και την καταγραφή της ασφάλειας στην ασφάλεια του νέφους:

1. Συνεχής παρακολούθηση

Η συνεχής παρακολούθηση περιλαμβάνει την παρακολούθηση σε πραγματικό χρόνο των περιβαλλόντων νέφους για τον εντοπισμό πιθανών απειλών και ανωμαλιών ασφαλείας. Οι βασικές πτυχές περιλαμβάνουν (Amah et al., 2023):

- Καταγραφή συμβάντων: Καταγραφή αρχείων καταγραφής συμβάντων, όπως οι δραστηριότητες των χρηστών, οι αλλαγές στο σύστημα και η κυκλοφορία του δικτύου.
- Συστήματα ανίχνευσης και πρόληψης εισβολών (IDPS): Εντοπισμός και αντιμετώπιση πιθανών παραβιάσεων ασφαλείας.

- Ανίχνευση ανωμαλιών: Χρήση μηχανικής μάθησης και στατιστικών μεθόδων για τον εντοπισμό ασυνήθιστης συμπεριφοράς.
- Παρακολούθηση συμμόρφωσης: Διασφάλιση της τήρησης των πολιτικών ασφαλείας και των κανονιστικών απαιτήσεων (Amah et al., 2023).

2. Καταγραφή και διαχείριση αρχείων καταγραφής

Η αποτελεσματική καταγραφή και διαχείριση αρχείων καταγραφής είναι κρίσιμες για την παρακολούθηση και την κατανόηση περιστατικών ασφαλείας. Τα σημαντικά στοιχεία περιλαμβάνουν:

- Ολοκληρωμένη καταγραφή: Καταγραφή λεπτομερών αρχείων καταγραφής των ενεργειών των χρηστών, των μοτίβων πρόσβασης και των αλλαγών στο σύστημα.
- Κεντρική διαχείριση αρχείων καταγραφής: Συγκέντρωση των αρχείων καταγραφής από διάφορες πηγές σε ένα κεντρικό σύστημα για ευκολότερη ανάλυση.
- Εργαλεία ανάλυσης αρχείων καταγραφής: Χρήση εργαλείων για την ανάλυση, το φιλτράρισμα και την ανάλυση δεδομένων καταγραφής για τον εντοπισμό ζητημάτων ασφαλείας.
- Πολιτικές διατήρησης: Καθιέρωση πολιτικών για το χρονικό διάστημα αποθήκευσης των αρχείων καταγραφής, που συχνά καθορίζεται από κανονιστικές απαιτήσεις.

3. Αναγνώριση απειλών

Η ενσωμάτωση πληροφοριών απειλών βοηθά στην πρόβλεψη και τον μετριασμό των απειλών ασφαλείας. Αυτό περιλαμβάνει:

- Τροφοδοτήσεις απειλών: Συνδρομή σε εξωτερικές τροφοδοσίες πληροφοριών απειλών για να παραμένετε ενημερωμένοι σχετικά με τις αναδυόμενες απειλές.
- Αυτοματοποιημένη ανίχνευση απειλών: Αξιοποίηση αυτοματοποιημένων εργαλείων για την ενσωμάτωση πληροφοριών απειλών στα συστήματα παρακολούθησης.
- Σχέδια αντιμετώπισης περιστατικών: Ανάπτυξη και τελειοποίηση σχεδίων αντιμετώπισης με βάση τις γνώσεις των πληροφοριών απειλών.

4. Διαχείριση πληροφοριών ασφαλείας και συμβάντων (SIEM)

Τα συστήματα SIEM διαδραματίζουν κεντρικό ρόλο στην παρακολούθηση της ασφάλειας του cloud, παρέχοντας ολοκληρωμένη διαχείριση των δεδομένων ασφαλείας. Οι βασικές λειτουργίες περιλαμβάνουν:

- Συγκέντρωση δεδομένων: Συλλογή και συσχέτιση δεδομένων από διαφορετικές πηγές.
- Ανάλυση σε πραγματικό χρόνο: Περιλαμβάνει την παροχή πληροφοριών και ειδοποιήσεων σε άμεσο χρόνο, βασισμένων σε δεδομένα που υποβάλλονται σε συνεχή ανάλυση και επεξεργασία, επιτρέποντας την άμεση λήψη αποφάσεων και την έγκαιρη αντίδραση σε δυναμικές συνθήκες.
- Διαχείριση συμβάντων: Διευκόλυνση του εντοπισμού, της ιεράρχησης και της αντιμετώπισης περιστατικών ασφαλείας.
- Πίνακες ελέγχου και αναφορές: Παροχή οπτικοποιήσεων και αναφορών για τη λήψη αποφάσεων και τη συμμόρφωση (Amah et al., 2023).

5. Έλεγχος και υποβολή εκθέσεων

Ο τακτικός έλεγχος και η λεπτομερής υποβολή εκθέσεων είναι απαραίτητα για τη διατήρηση της κατάστασης ασφαλείας και της συμμόρφωσης. Οι βασικές δραστηριότητες περιλαμβάνουν:

- Τακτικοί έλεγχοι: Διενέργεια περιοδικών ελέγχων για την επανεξέταση των ελέγχων και των πρακτικών ασφαλείας (Jiang et al., 2021).
- Αναφορές συμμόρφωσης: Δημιουργία αναφορών για την απόδειξη της συμμόρφωσης με τους σχετικούς νόμους και πρότυπα.
- Αναφορά περιστατικών: Τεκμηρίωση και αναφορά περιστατικών ασφαλείας, όπως απαιτείται από τους ρυθμιστικούς φορείς.

6. Διαχείριση πρόσβασης και ταυτότητας (IAM)

Η παρακολούθηση και η καταγραφή της πρόσβασης στους πόρους του cloud είναι ζωτικής σημασίας για τη διατήρηση της ασφάλειας. Τα βασικά στοιχεία περιλαμβάνουν:

- Παρακολούθηση της δραστηριότητας των χρηστών: Παρακολούθηση των ενεργειών των χρηστών και των μοτίβων πρόσβασης.

- Έλεγχος πρόσβασης βάσει ρόλων (RBAC): Διασφάλιση ότι οι χρήστες έχουν τα κατάλληλα επίπεδα πρόσβασης με βάση τους ρόλους τους.
- Αυθεντικοποίηση πολλαπλών παραγόντων (MFA): Προσθήκη επιπέδων ασφάλειας για την επαλήθευση των ταυτοτήτων των χρηστών (Jiang et al., 2021).

7. Αυτοματοποίηση και ενορχήστρωση

Η αυτοματοποίηση ενισχύει την αποδοτικότητα και την αποτελεσματικότητα της παρακολούθησης και της απόκρισης της ασφάλειας. Τα βασικά συστατικά στοιχεία περιλαμβάνουν:

- Αυτοματοποιημένες απαντήσεις: Εφαρμογή αυτόματων ενεργειών για την αντίδραση σε εντοπισμένες απειλές (π.χ. απομόνωση των επηρεαζόμενων συστημάτων).
- Εργαλεία ενορχήστρωσης: Συντονισμός και αυτοματοποίηση ροών εργασίας σε διαφορετικά εργαλεία και συστήματα ασφαλείας.

8. Παρακολούθηση κρυπτογράφησης και ακεραιότητας δεδομένων

Διασφάλιση της προστασίας και της ακεραιότητας των δεδομένων τόσο σε κατάσταση ηρεμίας όσο και κατά τη μεταφορά. Οι βασικές πρακτικές περιλαμβάνουν:

- Κρυπτογράφηση: Χρήση ισχυρών πρωτοκόλλων κρυπτογράφησης για την προστασία των δεδομένων
- Έλεγχοι ακεραιότητας: Παρακολούθηση των δεδομένων για μη εξουσιοδοτημένες αλλαγές ή διαφθορά (Jiang et al., 2021).

9. Αντιμετώπιση περιστατικών και εγκληματολογία

Ανάπτυξη ενός ισχυρού σχεδίου αντιμετώπισης συμβάντων και διεξαγωγή εγκληματολογικής ανάλυσης όταν συμβαίνουν παραβιάσεις. Τα βασικά στοιχεία περιλαμβάνουν:

- Ομάδες αντιμετώπισης περιστατικών: Δημιουργία ειδικών ομάδων για τον χειρισμό περιστατικών ασφαλείας.
- Εργαλεία εγκληματολογικής ανάλυσης: Χρήση εργαλείων και τεχνικών για τη διερεύνηση και κατανόηση των παραβιάσεων ασφαλείας.

10. Εκπαίδευση και κατάρτιση χρηστών

Εκπαίδευση των χρηστών σχετικά με τις βέλτιστες πρακτικές ασφάλειας και τη σημασία της παρακολούθησης της ασφάλειας. Αυτό περιλαμβάνει:

- Προγράμματα ευαισθητοποίησης σε θέματα ασφάλειας: Διεξαγωγή τακτικών εκπαιδευτικών συνεδριών για τους χρήστες.
- Προσομοιώσεις phishing: Έλεγχος της ευαισθητοποίησης και της ετοιμότητας των χρηστών μέσω προσομοιώσεων επιθέσεων.

Με την ενσωμάτωση αυτών των στοιχείων σε μια ολοκληρωμένη στρατηγική ασφάλειας cloud, οι οργανισμοί μπορούν να βελτιώσουν σημαντικά την ικανότητά τους να παρακολουθούν, να ανιχνεύουν και να ανταποκρίνονται στις απειλές ασφαλείας, εξασφαλίζοντας την προστασία των περιβαλλόντων cloud τους (Jiang et al., 2021).

4.5 Αντιμετώπιση και αποκατάσταση περιστατικών

1. Προετοιμασία

Η αποτελεσματική αντιμετώπιση περιστατικών αρχίζει με την ενδελεχή προετοιμασία. Αυτή περιλαμβάνει:

- Σχέδιο αντιμετώπισης περιστατικών (IRP): Ανάπτυξη και τακτική ενημέρωση ενός ολοκληρωμένου IRP που περιγράφει τους ρόλους, τις αρμοδιότητες και τις διαδικασίες.
- Ομάδα αντιμετώπισης περιστατικών (IRT): Συγκρότηση μιας εξειδικευμένης και εξουσιοδοτημένης ομάδας αφιερωμένης στην αντιμετώπιση περιστατικών
- Εκπαίδευση και ασκήσεις: Διεξαγωγή τακτικών εκπαιδευτικών συνεδριών και ασκήσεων προσομοίωσης αντιμετώπισης συμβάντων για να διασφαλιστεί η ετοιμότητα.

2. Ανίχνευση και αναγνώριση (Jiang et al., 2021).

Η ανίχνευση και ο ακριβής εντοπισμός περιστατικών είναι ζωτικής σημασίας. Οι βασικές δραστηριότητες περιλαμβάνουν:

- Συστήματα παρακολούθησης
- Μηχανισμοί ειδοποίησης
- Αρχική αξιολόγηση

3. Περιορισμός

Ο άμεσος περιορισμός της απειλής για την αποτροπή περαιτέρω ζημιών είναι απαραίτητος. Αυτό μπορεί να διαχωριστεί σε:

- Βραχυπρόθεσμο περιορισμό: Γρήγορη απομόνωση των επηρεαζόμενων συστημάτων ή δικτύων για να σταματήσει η εξάπλωση της απειλής, όπως η αποσύνδεση των συστημάτων που έχουν παραβιαστεί ή ο αποκλεισμός των κακόβουλων διευθύνσεων IP.
- Μακροπρόθεσμος περιορισμός: Εφαρμογή ολοκληρωμένων μέτρων για τη σταθεροποίηση του περιβάλλοντος, όπως η εφαρμογή επιδιορθώσεων ή η αναδιαμόρφωση τμημάτων δικτύου (Alouffi et al., 2021).

4. Εξάλειψη

Η εξάλειψη της αιτίας του συμβάντος περιλαμβάνει:

- Ανάλυση της αιτίας του συμβάντος: Διερεύνηση για τον εντοπισμό της υποκείμενης αιτίας.
- Αφαίρεση κακόβουλου λογισμικού: Εξάλειψη κάθε κακόβουλου λογισμικού ή κώδικα.
- Διόρθωση τρωτών σημείων: Αντιμετώπιση των ευπαθειών που έχουν γίνει αντικείμενο εκμετάλλευσης, όπως εφαρμογή διορθώσεων ή επαναδιαμόρφωση των ρυθμίσεων ασφαλείας (Alouffi et al., 2021).

5. Ανάκτηση

Η αποκατάσταση της κανονικής λειτουργίας των συστημάτων και των υπηρεσιών περιλαμβάνει:

- Αποκατάσταση του συστήματος: Επαναφορά συστημάτων από καθαρά αντίγραφα ασφαλείας ή αναδημιουργία τους, εάν είναι απαραίτητο.
- Επαλήθευση: Διασφάλιση της σωστής και ασφαλούς λειτουργίας των συστημάτων.
- Παρακολούθηση: Εντατική παρακολούθηση των συστημάτων για τυχόν ενδείξεις επαναλαμβανόμενων προβλημάτων ή νέων επιθέσεων κατά τη διάρκεια της περιόδου αποκατάστασης (Alouffi et al., 2021).

6. Ανάλυση και υποβολή εκθέσεων μετά το συμβάν

Η ανάλυση του συμβάντος και η εκμάθηση από την εμπειρία είναι ζωτικής σημασίας για τη μελλοντική πρόληψη. Η φάση αυτή περιλαμβάνει:

- Τεκμηρίωση του συμβάντος: Τεκμηρίωση των λεπτομερειών του συμβάντος, συμπεριλαμβανομένου του χρονοδιαγράμματος, των ενεργειών που έγιναν και των αποτελεσμάτων (Alouffi et al., 2021).
- Ανάλυση μετά το συμβάν: Επανεξέταση του περιστατικού για να γίνει κατανοητό το τι συνέβη και πώς αντιμετωπίστηκε.
- Εκμάθηση διδαγμάτων: Εντοπισμός τομέων για βελτίωση της διαδικασίας αντιμετώπισης περιστατικών.

7. Αποκατάσταση και βελτίωση

Η βελτίωση της στάσης ασφαλείας και η πρόληψη μελλοντικών περιστατικών περιλαμβάνει:

- Ενημερώσεις πολιτικών: Επικαιροποίηση των πολιτικών και των διαδικασιών ασφαλείας με βάση τις γνώσεις από το συμβάν (Balani & Varol, 2020).
- Βελτιώσεις της ασφάλειας: Εφαρμογή πρόσθετων ελέγχων ασφαλείας ή τεχνολογιών για την αντιμετώπιση εντοπισμένων κενών.
- Συνεχής βελτίωση: Τακτική επανεξέταση και βελτίωση του σχεδίου αντιμετώπισης περιστατικών και των μέτρων ασφαλείας.

Βασικές βέλτιστες πρακτικές για την αντιμετώπιση περιστατικών

- Επικοινωνία: Καθιέρωση σαφών διαύλων επικοινωνίας εντός της IRT και με εξωτερικούς ενδιαφερόμενους.
- Τεκμηρίωση: Τηρείτε λεπτομερή αρχεία όλων των ενεργειών που αναλαμβάνονται κατά τη διάρκεια ενός συμβάντος για λογοδοσία και ανάλυση.
- Συντονισμός: Συντονισμός με τις ομάδες νομικών, συμμόρφωσης και δημοσίων σχέσεων, ιδίως για παραβιάσεις δεδομένων ή κανονιστικά ζητήματα.
- Συνεργασία με τρίτους (Balani & Varol, 2020).

- Συμμόρφωση: Διασφάλιση της συμμόρφωσης όλων των ενεργειών με τους σχετικούς νόμους, κανονισμούς και συμβατικές υποχρεώσεις.

Ακολουθώντας αυτές τις δομημένες φάσεις και τις βέλτιστες πρακτικές, οι οργανισμοί μπορούν να αντιμετωπίσουν και να αποκαταστήσουν αποτελεσματικά τα περιστατικά ασφαλείας, ελαχιστοποιώντας τις επιπτώσεις και ενισχύοντας τη συνολική κατάσταση ασφαλείας (Balani & Varol, 2020).

5. Ειδικό Μέρος - Σύγκριση των κυριότερων παρόχων υπηρεσιών cloud

Στόχος της έρευνας

Ο πρωταρχικός στόχος της παρούσας έρευνας είναι να συγκρίνει τους κύριους παρόχους υπηρεσιών νέφους, εστιάζοντας στα χαρακτηριστικά ασφαλείας, τις επιδόσεις, την τιμολόγηση, τις προσφορές υπηρεσιών και την υποστήριξη πελατών. Η σύγκριση αποσκοπεί στην παροχή μιας ολοκληρωμένης κατανόησης των δυνατών και αδύνατων σημείων κάθε παρόχου.

Σχεδιασμός της έρευνας

Η παρούσα μελέτη χρησιμοποιεί συγκριτικό ερευνητικό σχεδιασμό, χρησιμοποιώντας τόσο ποιοτικά όσο και ποσοτικά δεδομένα για την αξιολόγηση και τη σύγκριση των κυριότερων παρόχων υπηρεσιών νέφους. Η έρευνα θα είναι περιγραφική και αναλυτική, παρέχοντας λεπτομερείς συγκρίσεις και γνώσεις.

Δείγμα

Το δείγμα για την παρούσα μελέτη περιλαμβάνει τους τρεις κύριους παρόχους υπηρεσιών νέφους:

- Amazon Web Services (AWS)
- Microsoft Azure
- Google Cloud Platform (GCP)

Οι εν λόγω πάροχοι επιλέχθηκαν λόγω της κυριαρχίας τους στην αγορά, των ολοκληρωμένων προσφορών υπηρεσιών και της ευρείας υιοθέτησής τους σε διάφορους κλάδους.

5.1 Amazon Web Services (AWS)

Ανάλυση των υπηρεσιών Amazon Web Services (AWS)

Η Amazon Web Services (AWS) είναι μια ολοκληρωμένη και ευρέως αποδεκτή πλατφόρμα cloud, η οποία προσφέρει πάνω από 200 πλήρως εξοπλισμένες υπηρεσίες από κέντρα δεδομένων σε όλο τον κόσμο. Ξεκίνησε το 2006, η AWS παρέχει κλιμακούμενη, αξιόπιστη και χαμηλού κόστους υποδομή cloud, εξυπηρετώντας εκατομμύρια πελάτες, συμπεριλαμβανομένων νεοφυών επιχειρήσεων, επιχειρήσεων και κυβερνητικών οργανισμών (Kewate et al., 2022).

Χαρακτηριστικά ασφαλείας

Η ασφάλεια αποτελεί ύψιστη προτεραιότητα για την AWS. Η πλατφόρμα ενσωματώνει πολυάριθμα χαρακτηριστικά ασφαλείας για την προστασία των δεδομένων, των εφαρμογών και της υποδομής. Οι βασικές πτυχές ασφάλειας περιλαμβάνουν:

- Κρυπτογράφηση δεδομένων: Η AWS προσφέρει εκτεταμένες επιλογές κρυπτογράφησης, συμπεριλαμβανομένης της κρυπτογράφησης από την πλευρά του διακομιστή (SSE) για το S3 (Simple Storage Service) και της κρυπτογράφησης από την πλευρά του πελάτη. Η κρυπτογράφηση κατά τη μεταφορά διασφαλίζεται με τη χρήση πρωτοκόλλων TLS (Kewate et al., 2022).
- Διαχείριση ταυτότητας και πρόσβασης (IAM): Το AWS IAM επιτρέπει τον λεπτομερή έλεγχο της πρόσβασης και των δικαιωμάτων των χρηστών. Ο έλεγχος ταυτότητας πολλαπλών παραγόντων (MFA) προσθέτει ένα πρόσθετο επίπεδο ασφάλειας.
- Συμμόρφωση: Το AWS πληροί ένα ευρύ φάσμα προτύπων συμμόρφωσης, όπως ISO 27001, SOC 1/2/3, GDPR, HIPAA και FedRAMP, καθιστώντας το κατάλληλο για ρυθμιζόμενες βιομηχανίες.
- Παρακολούθηση ασφάλειας: Η AWS παρέχει υπηρεσίες όπως το AWS CloudTrail για την καταγραφή και την παρακολούθηση της δραστηριότητας λογαριασμού, το Amazon GuardDuty για την ανίχνευση απειλών και το AWS Config για τη συμμόρφωση με τη διαμόρφωση των πόρων (Kewate et al., 2022).

Απόδοση

Η AWS είναι γνωστή για τις ισχυρές επιδόσεις της, οι οποίες υποστηρίζονται από ένα παγκόσμιο δίκτυο κέντρων δεδομένων. Τα βασικά χαρακτηριστικά επιδόσεων περιλαμβάνουν:

- Χρόνος διαθεσιμότητας της υπηρεσίας: Η AWS προσφέρει υψηλό επίπεδο διαθεσιμότητας υπηρεσιών, το οποίο υποστηρίζεται από SLA για διάφορες υπηρεσίες. Για παράδειγμα, το Amazon EC2 εγγυάται SLA διαθεσιμότητας 99,99% (Kewate et al., 2022).
- Παγκόσμια εμβέλεια: Η AWS λειτουργεί σε 99 ζώνες διαθεσιμότητας σε 31 γεωγραφικές περιοχές, παρέχοντας παγκόσμια κάλυψη και πρόσβαση με χαμηλή καθυστέρηση.
- Επεκτασιμότητα: Η AWS επιτρέπει την ελαστική κλιμάκωση των πόρων με υπηρεσίες όπως η αυτόματη κλιμάκωση και η ελαστική εξισορρόπηση φορτίου, επιτρέποντας την αυτόματη προσαρμογή της χωρητικότητας ανάλογα με τη ζήτηση.
- Βελτιστοποιημένη απόδοση: Υπηρεσίες όπως το Amazon CloudFront (CDN) και ο AWS Global Accelerator ενισχύουν την απόδοση μειώνοντας την καθυστέρηση και βελτιώνοντας την ταχύτητα παράδοσης περιεχομένου (Kewate et al., 2022).

Τιμολόγηση

Η τιμολόγηση της AWS έχει σχεδιαστεί ώστε να είναι ευέλικτη και οικονομικά αποδοτική, προσφέροντας διάφορα μοντέλα τιμολόγησης:

- Pay-As-You-Go: Χρεώσεις βάσει της πραγματικής χρήσης χωρίς προκαταβολικά έξοδα, καθιστώντας το οικονομικά αποδοτικό για μεταβλητούς φόρτους εργασίας.
- Reserved Instances: Προσφέρει σημαντικές εκπτώσεις (έως και 75%) σε σύγκριση με την τιμολόγηση κατά παραγγελία με αντάλλαγμα τη δέσμευση χρήσης του AWS για περίοδο 1 ή 3 ετών.
- Spot Instances: Επιτρέπει την υποβολή προσφορών για την ελεύθερη υπολογιστική χωρητικότητα, προσφέροντας έως και 90% εξοικονόμηση σε σύγκριση με τις τιμές on-demand (Kewate et al., 2022).
- Σχέδια εξοικονόμησης: Παρέχει ευέλικτη τιμολόγηση για τη χρήση του AWS, προσφέροντας χαμηλότερες τιμές για ένα δεσμευμένο ποσό χρήσης για περίοδο 1 ή 3 ετών.

Η AWS παρέχει επίσης έναν υπολογιστή κόστους και εργαλεία προϋπολογισμού για την αποτελεσματική διαχείριση και βελτιστοποίηση του κόστους (Saraswat & Tripathi, 2020).

Προσφορές υπηρεσιών

Η AWS προσφέρει ένα ευρύ φάσμα υπηρεσιών σε διάφορες κατηγορίες, καθιστώντας την μια ευέλικτη πλατφόρμα για διαφορετικές περιπτώσεις χρήσης:

- Υπολογισμός: Υπηρεσίες όπως το Amazon EC2, το AWS Lambda και το Amazon ECS παρέχουν ευέλικτες επιλογές υπολογισμού για διαφορετικές απαιτήσεις φόρτου εργασίας.
- Αποθήκευση: Η AWS προσφέρει κλιμακούμενες λύσεις αποθήκευσης όπως το Amazon S3, το Amazon EBS και το Amazon Glacier για διάφορες ανάγκες αποθήκευσης δεδομένων.
- Βάση δεδομένων: Η AWS παρέχει διαχειριζόμενες υπηρεσίες βάσεων δεδομένων, συμπεριλαμβανομένων των Amazon RDS, Amazon DynamoDB και Amazon Aurora, καλύπτοντας διαφορετικές απαιτήσεις βάσεων δεδομένων.
- Μηχανική μάθηση: Η AWS προσφέρει υπηρεσίες μηχανικής μάθησης, όπως το Amazon SageMaker, το οποίο επιτρέπει στους προγραμματιστές να δημιουργούν, να εκπαιδεύουν και να αναπτύσσουν μοντέλα ML σε κλίμακα (Saraswat & Tripathi, 2020).
- Ανάλυση: Οι υπηρεσίες ανάλυσης AWS, όπως το Amazon Redshift και το Amazon Athena, επιτρέπουν στις επιχειρήσεις να αναλύουν αποτελεσματικά μεγάλα σύνολα δεδομένων.
- Δικτύωση: Υπηρεσίες όπως το Amazon VPC, το AWS Direct Connect και το AWS Transit Gateway παρέχουν ισχυρές λύσεις δικτύωσης για ασφαλή και κλιμακούμενη συνδεσιμότητα (Saraswat & Tripathi, 2020).

Υποστήριξη πελατών

Η AWS παρέχει διάφορα πακέτα υποστήριξης για την κάλυψη των διαφορετικών αναγκών των πελατών:

- Βασική υποστήριξη: Δωρεάν βαθμίδα που περιλαμβάνει 24ωρη πρόσβαση στην εξυπηρέτηση πελατών, τεκμηρίωση, λευκά έντυπα και βασικούς ελέγχους του AWS Trusted Advisor.
- Υποστήριξη για προγραμματιστές: Περιλαμβάνει όλες τις βασικές λειτουργίες καθώς και πρόσβαση μέσω ηλεκτρονικού ταχυδρομείου σε εργάσιμες ώρες σε συνεργάτες υποστήριξης Cloud.

- Υποστήριξη για επιχειρήσεις: Παρέχει 24ωρη πρόσβαση μέσω τηλεφώνου, ηλεκτρονικού ταχυδρομείου και συνομιλίας σε Μηχανικούς Υποστήριξης Cloud, καθώς και πρόσβαση στο πλήρες σύνολο ελέγχων του AWS Trusted Advisor.
- Υποστήριξη για επιχειρήσεις: Προσφέρει έναν αποκλειστικό Τεχνικό Διαχειριστή Λογαριασμού (TAM), προληπτική καθοδήγηση και πρόσβαση 24/7 σε ανώτερους μηχανικούς υποστήριξης cloud (Saraswat & Tripathi, 2020).

5.2 Microsoft Azure

Το Microsoft Azure, που ξεκίνησε το 2010, είναι μια κορυφαία υπηρεσία υπολογιστικού νέφους που δημιουργήθηκε από τη Microsoft για τη δημιουργία, δοκιμή, ανάπτυξη και διαχείριση εφαρμογών και υπηρεσιών μέσω κέντρων δεδομένων που διαχειρίζεται η Microsoft. Το Azure παρέχει μια ευρεία γκάμα υπηρεσιών, συμπεριλαμβανομένων εκείνων για υπολογισμούς, αναλύσεις, αποθήκευση και δικτύωση (Gupta et al., 2021).

Χαρακτηριστικά ασφαλείας

Το Azure δίνει προτεραιότητα στην ασφάλεια και προσφέρει διάφορα χαρακτηριστικά για να διασφαλίσει την προστασία των δεδομένων και των εφαρμογών:

- Κρυπτογράφηση: Τα δεδομένα σε κατάσταση ηρεμίας κρυπτογραφούνται χρησιμοποιώντας την υπηρεσία κρυπτογράφησης αποθήκευσης Azure Storage Service Encryption (SSE) και την κρυπτογράφηση δίσκων Azure Disk Encryption. Τα δεδομένα κατά τη μεταφορά προστατεύονται με τη χρήση πρωτοκόλλων SSL/TLS.
- Διαχείριση ταυτότητας και πρόσβασης (IAM): Το Azure Active Directory (AD) είναι μια ολοκληρωμένη υπηρεσία διαχείρισης ταυτότητας και πρόσβασης που υποστηρίζει ενιαία σύνδεση (SSO), έλεγχο ταυτότητας πολλαπλών παραγόντων (MFA) και πρόσβαση υπό όρους (Gupta et al., 2021).
- Συμμόρφωση: Το Azure πληροί πολυάριθμα πρότυπα συμμόρφωσης, συμπεριλαμβανομένων των ISO 27001, SOC 1/2/3, GDPR, HIPAA και FedRAMP. Αυτό το καθιστά κατάλληλο για κλάδους με υψηλές κανονιστικές ρυθμίσεις.
- Παρακολούθηση ασφάλειας: Το Azure Security Center παρέχει ενοποιημένη διαχείριση ασφάλειας και προηγμένη προστασία από απειλές σε υβριδικούς

φόρτους εργασίας cloud. Περιλαμβάνει πληροφορίες σχετικά με απειλές και αξιολογήσεις ευπάθειας.

Απόδοση

Το Azure προσφέρει ισχυρές επιδόσεις με μια παγκόσμια υποδομή και πολυάριθμα εργαλεία για τη βελτιστοποίηση της ταχύτητας και της αξιοπιστίας:

- Διαρκής χρόνος λειτουργίας των υπηρεσιών: Το Azure παρέχει SLA διαθεσιμότητας 99,95% για τις περισσότερες από τις υπηρεσίες του, εξασφαλίζοντας υψηλή αξιοπιστία.
- Παγκόσμια εμβέλεια: Το Azure λειτουργεί σε περισσότερες από 60 περιοχές παγκοσμίως, περισσότερες από οποιονδήποτε άλλο πάροχο cloud, εξασφαλίζοντας πρόσβαση με χαμηλή καθυστέρηση και πλεονασμό (Gupta et al., 2021).
- Επεκτασιμότητα: Οι υπηρεσίες Azure, όπως τα Virtual Machine Scale Sets και η υπηρεσία Azure Kubernetes Service (AKS), επιτρέπουν την αυτόματη κλιμάκωση των εφαρμογών ανάλογα με τη ζήτηση.
- Βελτιστοποίηση επιδόσεων: Το Azure Traffic Manager και το Δίκτυο Παράδοσης Περιεχομένου (CDN) βελτιώνουν την απόδοση και τη διαθεσιμότητα των εφαρμογών, κατευθύνοντας την κυκλοφορία των χρηστών στο πλησιέστερο κέντρο δεδομένων και αποθηκεύοντας το περιεχόμενο στην προσωρινή μνήμη (Gupta et al., 2021).

Τιμολόγηση

Το Azure προσφέρει ευέλικτες επιλογές τιμολόγησης για την κάλυψη διαφόρων επιχειρηματικών αναγκών:

- Pay-As-You-Go: Χρεώσεις βάσει της πραγματικής χρήσης, επιτρέποντας ευελιξία και έλεγχο του κόστους.
- Reserved Instances: Σημαντικές εκπτώσεις (έως και 72%) για τη δέσμευση χρήσης των υπηρεσιών Azure για περίοδο 1 ή 3 ετών.
- Azure Hybrid Benefit: Παρέχει εξοικονόμηση κόστους επιτρέποντας στους πελάτες να χρησιμοποιούν τις άδειες Windows Server και SQL Server που διαθέτουν στις εγκαταστάσεις τους στο cloud.

- Spot VMs: Προσφέρει αχρησιμοποίητη χωρητικότητα Azure σε χαμηλότερη τιμή, ιδανική για διακοπτόμενους φόρτους εργασίας.

Το Azure παρέχει εργαλεία διαχείρισης κόστους, όπως το εργαλείο διαχείρισης και χρέωσης κόστους Azure, που βοηθούν στην παρακολούθηση και βελτιστοποίηση των δαπανών (Gupta et al., 2021).

Προσφορές υπηρεσιών

Το Azure προσφέρει μια ολοκληρωμένη σουίτα υπηρεσιών σε διάφορες κατηγορίες, καλύπτοντας ένα ευρύ φάσμα περιπτώσεων χρήσης:

- Υπολογισμός: Azure Virtual Machines, Azure Functions και Azure Batch παρέχουν ευέλικτες επιλογές υπολογισμού.
- Αποθήκευση: Το Azure προσφέρει διάφορες λύσεις αποθήκευσης, συμπεριλαμβανομένων των Azure Blob Storage, Azure Disk Storage και Azure Files.
- Βάση δεδομένων: Το Azure παρέχει διαχειριζόμενες υπηρεσίες βάσεων δεδομένων, όπως Azure SQL Database, Azure Cosmos DB και Azure Database for PostgreSQL.
- Τεχνητή νοημοσύνη και μηχανική μάθηση: Οι υπηρεσίες Azure AI και Azure Machine Learning επιτρέπουν τη δημιουργία και την ανάπτυξη μοντέλων τεχνητής νοημοσύνης (Kaushik et al., 2021).
- Ανάλυση: Υπηρεσίες όπως Azure Synapse Analytics, Azure HDInsight και Azure Data Lake Storage υποστηρίζουν φόρτους εργασίας μεγάλων δεδομένων και ανάλυσης.
- Δικτύωση: Το Azure Virtual Network, το Azure ExpressRoute και το Azure Firewall παρέχουν ασφαλείς και κλιμακούμενες επιλογές δικτύωσης.

Υποστήριξη πελατών

Το Azure παρέχει μια σειρά από πακέτα υποστήριξης για την κάλυψη των διαφορετικών αναγκών των πελατών:

- Βασική υποστήριξη: Δωρεάν βαθμίδα που περιλαμβάνει 24ωρη πρόσβαση στην υπηρεσία εξυπηρέτησης πελατών, τεκμηρίωση και συστάσεις του Azure Advisor.

- Υποστήριξη για προγραμματιστές: Πρόσβαση κατά τις εργάσιμες ώρες σε μηχανικούς υποστήριξης και συμβουλευτικές υπηρεσίες (Kaushik et al., 2021).
- Τυπική υποστήριξη: Πρόσβαση 24/7 σε τεχνική υποστήριξη για μεσαίου μεγέθους επιχειρήσεις, συμπεριλαμβανομένων ταχύτερων χρόνων απόκρισης.
- Professional Direct και Premier Support: Προηγμένες επιλογές υποστήριξης που προσφέρουν χειρισμό κατά προτεραιότητα, αρχιτεκτονική καθοδήγηση και έναν αποκλειστικό Διαχειριστή Τεχνικού Λογαριασμού (TAM) (Kaushik et al., 2021).

5.3 Πλατφόρμα νέφους της Google (GCP)

Το Google Cloud Platform (GCP), που ξεκίνησε από την Google το 2008, είναι μια σουίτα υπηρεσιών υπολογιστικού νέφους που λειτουργεί στην ίδια υποδομή που χρησιμοποιεί η Google εσωτερικά για τα προϊόντα της για τελικούς χρήστες, όπως το Google Search, το Gmail και το YouTube. Το GCP προσφέρει ένα ευρύ φάσμα υπηρεσιών νέφους, συμπεριλαμβανομένων των υπολογιστών, της αποθήκευσης, της ανάλυσης δεδομένων και της μηχανικής μάθησης (Kamal et al., 2020).

Χαρακτηριστικά ασφαλείας

Το GCP δίνει μεγάλη έμφαση στην ασφάλεια, προσφέροντας πολλαπλά χαρακτηριστικά για τη διασφάλιση των δεδομένων και των εφαρμογών:

- Κρυπτογράφηση δεδομένων: Η Google Cloud Platform (GCP) εφαρμόζει κρυπτογράφηση τόσο για δεδομένα σε κατάσταση ηρεμίας (εν αποθηκεύσει) όσο και κατά τη μεταφορά, ως προεπιλογή, προκειμένου να εξασφαλίσει την προστασία των δεδομένων των χρηστών. Η διαχείριση των κλειδιών κρυπτογράφησης πραγματοποιείται μέσω της υπηρεσίας Google Cloud Key Management Service (KMS), η οποία επιτρέπει στους χρήστες να δημιουργούν, να ελέγχουν και να διαχειρίζονται κλειδιά κρυπτογράφησης με σκοπό την ασφαλή προστασία των δεδομένων τους σε όλη τη διάρκεια της αποθήκευσης και μεταφοράς τους.
- Διαχείριση ταυτότητας και πρόσβασης (IAM): Το GCP παρέχει λεπτομερή έλεγχο σχετικά με το ποιος μπορεί να κάνει συγκεκριμένες ενέργειες σε πόρους μέσω ρόλων και πολιτικών IAM. Υποστηρίζει επίσης έλεγχο

ταυτότητας πολλαπλών παραγόντων (MFA) και Cloud Identity για ενοποιημένη διαχείριση ταυτότητας (Kamal et al., 2020).

- Συμμόρφωση: Το GCP τηρεί διάφορα πρότυπα συμμόρφωσης, όπως ISO 27001, SOC 1/2/3, GDPR, HIPAA και FedRAMP (Federal Risk and Authorization Management Program), καθιστώντας το κατάλληλο για κλάδους με υψηλές κανονιστικές απαιτήσεις.
- Παρακολούθηση ασφάλειας: Εργαλεία όπως το Google Cloud Security Command Center (SCC) παρέχουν κεντρική ορατότητα σε κινδύνους ασφάλειας και δεδομένων, ενώ τα αρχεία καταγραφής ελέγχου Google Cloud παρακολουθούν όλες τις δραστηριότητες.

Απόδοση

Το GCP είναι γνωστό για την αξιοποίηση της παγκόσμιας υποδομής της Google για την παροχή υψηλών επιδόσεων:

- Διαρκής χρόνος λειτουργίας των υπηρεσιών: GCP προσφέρει SLA διαθεσιμότητας 99,95% για τις περισσότερες υπηρεσίες, εξασφαλίζοντας υψηλή αξιοπιστία (Kamal et al., 2020).
- Παγκόσμια εμβέλεια: Το GCP λειτουργεί σε 37 περιοχές και 112 ζώνες παγκοσμίως, παρέχοντας ευρεία κάλυψη και πρόσβαση με χαμηλή καθυστέρηση.
- Επεκτασιμότητα: Οι υπηρεσίες του GCP, όπως το Google Kubernetes Engine (GKE) και το Compute Engine, προσφέρουν δυνατότητες αυτόματης κλιμάκωσης για την αποτελεσματική διαχείριση διαφορετικών φόρτων εργασίας.
    - Βελτιστοποίηση επιδόσεων: Η Google Cloud Platform (GCP) εκμεταλλεύεται το παγκόσμιο δίκτυο οπτικών ινών της Google, το οποίο αποτελεί μία από τις πιο εξελιγμένες υποδομές στον κόσμο για την εξασφάλιση ταχύτητας και αξιοπιστίας στη μετάδοση δεδομένων. Επιπλέον, χρησιμοποιεί τεχνικές προσωρινής αποθήκευσης στην άκρη (edge caching) για να μειώσει τη καθυστέρηση και να βελτιώσει την απόδοση των υπηρεσιών της. Αυτή η αρχιτεκτονική επιτρέπει την παροχή υπηρεσιών με εξαιρετικά χαμηλή καθυστέρηση και υψηλή απόδοση, ικανοποιώντας τις απαιτήσεις για πραγματικό χρόνο και μεγάλες κλίμακες εφαρμογών.

Τιμολόγηση

Το μοντέλο τιμολόγησης του GCP έχει σχεδιαστεί για να είναι ευέλικτο και διαφανές:

- Pay-As-You-Go: Χρεώσεις βάσει της πραγματικής χρήσης χωρίς προκαταβολικά έξοδα, καθιστώντας το οικονομικά αποδοτικό για μεταβλητούς φόρτους εργασίας.
- Συμβάσεις δεσμευμένης χρήσης: Προσφέρει σημαντικές εκπτώσεις (έως και 57%) για τη δέσμευση χρήσης συγκεκριμένων πόρων για περίοδο 1 ή 3 ετών (Kamal et al., 2020).
- Εκπτώσεις συνεχούς χρήσης: Αυτόματα εφαρμοζόμενες εκπτώσεις που μειώνουν το κόστος καθώς η χρήση αυξάνεται κατά τη διάρκεια του κύκλου χρέωσης.
- Προεπιλεγμένα VM: Παρέχουν μειωμένες τιμές για φόρτους εργασίας που επιδεικνύουν ανεκτικότητα σε διακοπές λειτουργίας, προσφέροντας σημαντική εξοικονόμηση πόρων για συγκεκριμένες κατηγορίες εφαρμογών. (Ucuz, 2020).

Το GCP παρέχει επίσης εργαλεία διαχείρισης του κόστους, όπως ο Υπολογιστής Τιμών Google Cloud και οι αναφορές χρέωσης Google Cloud, που βοηθούν στην παρακολούθηση και τη βελτιστοποίηση των δαπανών.

Προσφορές υπηρεσιών

Το GCP προσφέρει μια ευρεία γκάμα υπηρεσιών για την κάλυψη ποικίλων επιχειρηματικών αναγκών:

- Υπολογισμός: Google Compute Engine, Google Kubernetes Engine (GKE) και Cloud Functions παρέχουν επιλογές κλιμακούμενων υπολογισμών.
- Αποθήκευση: Google Cloud Storage, Persistent Disks και Filestore προσφέρουν ισχυρές και κλιμακούμενες λύσεις αποθήκευσης (Ucuz, 2020).
- Βάση δεδομένων: Οι διαχειριζόμενες υπηρεσίες βάσεων δεδομένων περιλαμβάνουν τις υπηρεσίες Cloud SQL, Cloud Spanner και Bigtable για τις ανάγκες σχεσιακών και NoSQL βάσεων δεδομένων.
- Μηχανική εκμάθηση και τεχνητή νοημοσύνη: Το GCP παρέχει ισχυρά εργαλεία όπως το TensorFlow, το AI Platform και το AutoML για την ανάπτυξη μοντέλων μηχανικής εκμάθησης (Ucuz, 2020).

- Μεγάλα δεδομένα και αναλύσεις: Υπηρεσίες όπως το BigQuery, το Dataflow και το Dataproc επιτρέπουν την επεξεργασία και την ανάλυση μεγάλων συνόλων δεδομένων.
- Δικτύωση: Οι υπηρεσίες VPC, Cloud Load Balancing και Cloud CDN παρέχουν δυνατότητες ασφαλούς και υψηλής απόδοσης δικτύωσης.

Υποστήριξη πελατών

Το GCP προσφέρει διάφορα πακέτα υποστήριξης για την κάλυψη των διαφορετικών αναγκών των πελατών:

- Βασική υποστήριξη: Περιλαμβάνει πρόσβαση στην τεκμηρίωση, την υποστήριξη της κοινότητας και την υποστήριξη χρέωσης (Ucuz, 2020).
- Βασική υποστήριξη: Πρόσβαση 24/7 σε τεχνική υποστήριξη και συμβουλές από ειδικούς του cloud με μηνιαία χρέωση.
- Ενισχυμένη υποστήριξη: Παρέχει ταχύτερους χρόνους απόκρισης και πρόσθετους πόρους υποστήριξης, συμπεριλαμβανομένης της τεχνολογικής υποστήριξης τρίτων.
- Υποστήριξη Premium: Προσφέρει έναν αποκλειστικό Τεχνικό Διαχειριστή Λογαριασμού (ΤΔΛ), προληπτική υποστήριξη και αρχιτεκτονική καθοδήγηση για κρίσιμους φόρτους εργασίας (Saraswat & Tripathi, 2020).

Δυνατά και αδύνατα σημεία:

Δυνατά σημεία:

- Μηχανική μάθηση και AI: Το GCP υπερέχει στην AI (Τεχνητή Νοημοσύνη) και τη μηχανική μάθηση με προηγμένα εργαλεία και υποδομές.
- Αναλύσεις δεδομένων: Ισχυρές δυνατότητες στην επεξεργασία και την ανάλυση μεγάλων δεδομένων, με υπηρεσίες όπως το BigQuery να κατέχουν ηγετική θέση στην αγορά.
- Παγκόσμιο δίκτυο: Χρησιμοποιεί το εκτεταμένο παγκόσμιο δίκτυο οπτικών ινών της Google για χαμηλές καθυστερήσεις και υψηλές επιδόσεις.
- Υποστήριξη ανοικτού κώδικα: Ισχυρή υποστήριξη για τεχνολογίες και ενσωματώσεις ανοικτού κώδικα (Saraswat & Tripathi, 2020).

Αδυναμίες:

- Μερίδιο αγοράς: Το GCP έχει μικρότερο μερίδιο αγοράς σε σύγκριση με το AWS και το Azure, γεγονός που μπορεί να επηρεάσει την προτίμηση των πελατών και τη διαθεσιμότητα ενσωματώσεων τρίτων.
- Πολυπλοκότητα υπηρεσιών: Το εύρος και το βάθος των υπηρεσιών μπορεί να είναι συντριπτικό για τους νέους χρήστες, απαιτώντας σημαντικό χρόνο για την εκμάθηση και τη διαχείριση.

Το Google Cloud Platform ξεχωρίζει για τις προηγμένες δυνατότητες μηχανικής μάθησης και ανάλυσης δεδομένων, αξιοποιώντας την ισχυρή παγκόσμια υποδομή της Google. Αν και το μερίδιο αγοράς του είναι μικρότερο σε σύγκριση με το AWS και το Azure, οι καινοτόμες υπηρεσίες του GCP, τα ισχυρά χαρακτηριστικά ασφαλείας και η δέσμευση στις τεχνολογίες ανοικτού κώδικα το καθιστούν μια ελκυστική επιλογή για τις επιχειρήσεις που αναζητούν ισχυρές λύσεις cloud. Παρά την πολυπλοκότητα και την καμπύλη εκμάθησης, η επεκτασιμότητα, οι επιδόσεις και οι ολοκληρωμένες προσφορές υπηρεσιών του GCP το καθιστούν ισχυρό ανταγωνιστή στην αγορά υπολογιστικού νέφους (Saraswat & Tripathi, 2020).

6 Έρευνα

6.1 Εισαγωγή:

Η αλματώδης ανάπτυξη της τεχνολογίας του υπολογιστικού νέφους έχει επιφέρει σημαντικές αλλαγές στον τρόπο με τον οποίο οι επιχειρήσεις διαχειρίζονται και προστατεύουν τις πληροφορίες τους. Ωστόσο, η αυξημένη χρήση του cloud συνοδεύεται από νέες προκλήσεις και απειλές για την ασφάλεια των πληροφοριών, οι οποίες απαιτούν την προσοχή των οργανισμών και των υπευθύνων ασφάλειας. Η ανάγκη για κατανόηση των τάσεων που επικρατούν στην ασφάλεια του cloud καθιστά επιτακτική τη διεξαγωγή στοχευμένης έρευνας, με σκοπό να αναλυθούν οι πρακτικές και οι απόψεις που κυριαρχούν στις επιχειρήσεις σήμερα.

Στο πλαίσιο αυτό, η παρούσα ερευνητική ενότητα στοχεύει στη δημιουργία ενός εξειδικευμένου ερωτηματολογίου, το οποίο θα συμβάλλει στη συλλογή δεδομένων σχετικά με τις προσεγγίσεις, τις στρατηγικές και τις ανησυχίες των επιχειρήσεων γύρω από την ασφάλεια πληροφοριών σε περιβάλλοντα cloud. Μέσω της ανάλυσης των απαντήσεων που θα συλλεχθούν, επιδιώκεται να αποτυπωθεί μια σαφής εικόνα των σύγχρονων τάσεων και προτεραιοτήτων στον τομέα της ασφάλειας πληροφοριών.

Ο σκοπός της έρευνας είναι να διερευνήσει τις διαφορετικές προσεγγίσεις που εφαρμόζουν οι επιχειρήσεις για την προστασία των δεδομένων τους στο cloud και να εντοπίσει τις κοινές πρακτικές, τα σημαντικότερα εμπόδια και τις ανάγκες βελτίωσης. Η γνώση αυτή θα επιτρέψει τη διαμόρφωση συστάσεων και πρακτικών κατευθύνσεων, ώστε οι οργανισμοί να μπορούν να ενισχύσουν τις πολιτικές ασφάλειας τους, συμβάλλοντας παράλληλα στην αντιμετώπιση των διαρκώς εξελισσόμενων απειλών στον κυβερνοχώρο

6.2 Μεθοδολογία Έρευνας

Στην παρούσα ενότητα περιγράφεται η μεθοδολογία που ακολουθήθηκε για τη συλλογή και ανάλυση των δεδομένων. Για να διερευνηθούν οι απόψεις και οι πρακτικές των επιχειρήσεων σχετικά με την ασφάλεια πληροφοριών σε περιβάλλον cloud, δημιουργήθηκε ένα εξειδικευμένο ερωτηματολόγιο το οποίο απευθύνεται σε στελέχη πληροφορικής και υπεύθυνους ασφάλειας.

Η δομή των ερωτήσεων καθορίστηκε με βάση τις κατευθυντήριες γραμμές και απαιτήσεις που θέτουν τα πρότυπα ISO 27017 και ISO 27018, τα οποία εστιάζουν στην ασφάλεια και προστασία της ιδιωτικής ζωής στο cloud. Επιπλέον, χρησιμοποιήθηκαν κανονιστικά πλαίσια,

όπως ο GDPR, για να εξασφαλιστεί ότι οι ερωτήσεις καλύπτουν κρίσιμα σημεία συμμόρφωσης και βέλτιστων πρακτικών. Οι ερωτήσεις περιλαμβάνουν θέματα, όπως:

- Στρατηγικές για την προστασία των δεδομένων στο cloud,
- Προκλήσεις και ανησυχίες που αντιμετωπίζουν οι επιχειρήσεις στον τομέα της ασφάλειας,
- Συμμόρφωση με πρότυπα ασφαλείας και τήρηση βέλτιστων πρακτικών,
- Αναγκαιότητα συνεχούς εκπαίδευσης και ενημέρωσης του προσωπικού.

Το δείγμα των συμμετεχόντων επιλέχθηκε ώστε να περιλαμβάνει οργανισμούς διαφόρων μεγεθών και τομέων, επιδιώκοντας να αποτυπώσει ένα ευρύ φάσμα προσεγγίσεων και αναγκών στην ασφάλεια του cloud. Η συλλογή των απαντήσεων έγινε μέσω διαδικτυακών φορμών, εξασφαλίζοντας την ανωνυμία και ειλικρίνεια των συμμετεχόντων.

6.3 Αποτελέσματα και Σχολιασμός

Στην παρούσα ενότητα, παρουσιάζονται αναλυτικά τα αποτελέσματα της έρευνας που πραγματοποιήθηκε σχετικά με την ασφάλεια δεδομένων στο cloud. Η ανάλυση καλύπτει ποσοτικά και ποιοτικά ευρήματα που αφορούν τις τρέχουσες πρακτικές, προτεραιότητες και ανησυχίες των οργανισμών γύρω από την ασφάλεια στο cloud. Κάθε υποενότητα περιλαμβάνει τα βασικά ευρήματα, καθώς και τον σχολιασμό τους, με σκοπό να αναδείξει την κατανόηση και τις προσεγγίσεις που υιοθετούν οι οργανισμοί σε θέματα ασφάλειας.

Η ενότητα αυτή επιδιώκει να προσφέρει μια ολοκληρωμένη εικόνα για το πώς οι οργανισμοί αντιλαμβάνονται και διαχειρίζονται την ασφάλεια των δεδομένων τους στο cloud, επισημαίνοντας τα πεδία όπου οι πρακτικές τους ευθυγραμμίζονται με τις βέλτιστες προσεγγίσεις και εκείνα όπου μπορεί να υπάρχουν περιθώρια βελτίωσης. Μέσω της ανάλυσης και του σχολιασμού, προσδιορίζονται επίσης οι βασικές τάσεις, προκλήσεις και ευκαιρίες για ενίσχυση της ασφάλειας, συμβάλλοντας στην καλύτερη κατανόηση του πεδίου και στις μελλοντικές στρατηγικές βελτίωσης.

1. Εξοικείωση με την Κυβερνοασφάλεια Το 46,3% των ερωτηθέντων δηλώνει ότι είναι "Εξοικειωμένος" με την έννοια της κυβερνοασφάλειας, ενώ το 36,6% είναι "Πολύ εξοικειωμένο." Ένα μικρό ποσοστό, 12,2%, είναι "Λίγο εξοικειωμένο," ενώ το 4,9% δεν έχει καθόλου εξοικείωση.

Συμπέρασμα: Η πλειοψηφία (83%) έχει κάποιο επίπεδο εξοικείωσης, με το μεγαλύτερο ποσοστό σε υψηλό επίπεδο. Αυτό δείχνει κατανόηση της σημασίας της κυβερνοασφάλειας, με ένα μικρό τμήμα που χρειάζεται επιπλέον ενημέρωση.

2. Τεχνολογίες Cloud στις Επιχειρήσεις Το 63,4% χρησιμοποιεί "Ιδιωτικό cloud," το 31,7% "Υβριδικό cloud," το 29,3% "Δημόσιο cloud," και το 9,8% "Πολυδιάστατο cloud." **Συμπέρασμα:** Οι επιχειρήσεις δείχνουν προτίμηση σε λύσεις Ιδιωτικού και Υβριδικού cloud, ενώ ένα σημαντικό ποσοστό χρησιμοποιεί Δημόσιο cloud για εφαρμογές με λιγότερες απαιτήσεις ασφάλειας.

3. Κύριες Υπηρεσίες Cloud Η αποθήκευση δεδομένων είναι η πιο διαδεδομένη υπηρεσία (95,1%), ακολουθούμενη από βάσεις δεδομένων (51,2%), υπολογιστική ισχύ (41,5%), και ανάλυση δεδομένων (7,3%).
Συμπέρασμα: Η αποθήκευση αποτελεί βασική ανάγκη, ενώ υπηρεσίες ανάλυσης είναι λιγότερο διαδεδομένες, πιθανώς λόγω εξειδίκευσης ή κόστους.

4. Σημασία Ασφάλειας Δεδομένων Το 82,9% θεωρεί την ασφάλεια στο cloud "Πολύ σημαντική" και το 14,6% "Σημαντική." Ένα 2,5% την αξιολογεί ως λιγότερο σημαντική. **Συμπέρασμα:** Η πλειοψηφία αναγνωρίζει την ασφάλεια ως κρίσιμη για τη χρήση του cloud, γεγονός που τονίζει τη σημασία της εμπιστοσύνης στα συστήματα ασφαλείας.

5. Συχνότητα Ελέγχου Ευπαθειών και Απειλών Το 36,6% πραγματοποιεί εβδομαδιαίους ελέγχους, το 29,3% σπάνια, το 26,8% καθημερινά, και το 7,3% μηνιαία. **Συμπέρασμα:** Η τακτική παρακολούθηση είναι κοινή πρακτική, αν και ένα ποσοστό (29,3%) που ελέγχει σπάνια μπορεί να παραμένει ευάλωτο.

6. Υιοθέτηση Μέτρων Προστασίας Δεδομένων Το 68,3% έχει υιοθετήσει μέτρα, το 14,6% δεν έχει λάβει μέτρα και το 17,1% σκοπεύει να το κάνει. **Συμπέρασμα:** Αν και οι περισσότεροι έχουν λάβει μέτρα, ένα ποσοστό παραμένει ευάλωτο λόγω απουσίας προστασίας.

7. Επίπεδο Πρόσβασης Χρηστών Το 61% έχει κανονικό επίπεδο πρόσβασης, το 29,3% διαχειριστική, και το 9,8% περιορισμένη.
Συμπέρασμα: Η διαχείριση πρόσβασης είναι σημαντική, με έμφαση στην περιορισμένη πρόσβαση για μη εξουσιοδοτημένους χρήστες.

8. Χρήση Υπηρεσιών Ασφαλείας Τρίτων Παρόχων Το 63,4% χρησιμοποιεί τρίτους παρόχους για ορισμένες υπηρεσίες, το 22% εμπιστεύεται τις ενσωματωμένες λειτουργίες και

ένα 7,3% δεν χρησιμοποιεί εξωτερικές υπηρεσίες. **Συμπέρασμα:** Η επιλεκτική χρήση τρίτων παρόχων δείχνει ότι οι οργανισμοί προσαρμόζουν την ασφάλεια στις ανάγκες τους.

9. Πολλαπλή Επαλήθευση Ταυτότητας (MFA) Το 41,5% εφαρμόζει MFA σε όλες τις υπηρεσίες, το 43,9% σε κάποιες και το 14,6% καθόλου. **Συμπέρασμα:** Παρά την ευρεία χρήση του MFA, ένα 14,6% δεν αξιοποιεί καθόλου αυτή τη μέθοδο ασφαλείας.

10. Πολιτικές IAM στο Cloud Το 38,1% έχει εφαρμόσει πλήρως IAM, το 47,6% μερικώς, και το 14,3% δεν έχει εφαρμόσει. **Συμπέρασμα:** Παρότι η πλειονότητα εφαρμόζει πολιτικές IAM, υπάρχει περιθώριο βελτίωσης για μια συνεπή διαχείριση ταυτότητας.

11. Συχνότητα Αξιολογήσεων Ασφαλείας Το 41,5% διενεργεί μηνιαία, το 26,8% ετήσια, το 14,6% τριμηνιαία ή εξαμηνιαία, και το 14,6% δεν πραγματοποιεί καθόλου αξιολογήσεις. **Συμπέρασμα:** Οι αξιολογήσεις είναι τακτικές, αλλά η έλλειψή τους σε ορισμένους οργανισμούς δημιουργεί ευπάθειες.

12. Ενημέρωση Λογισμικού Ασφαλείας Το 61% ενημερώνει τακτικά, το 34,1% όχι σταθερά και το 4,9% καθόλου. **Συμπέρασμα:** Ενώ οι περισσότεροι ενημερώνουν το λογισμικό τους, η έλλειψη συνέπειας σε ορισμένους οργανισμούς μπορεί να δημιουργήσει κενά ασφαλείας.

13. Μέτρα Προστασίας Δεδομένων Το 85,4% χρησιμοποιεί backups, το 70,7% κρυπτογράφηση, το 68,3% πολιτικές πρόσβασης, και το 46,3% ανίχνευση εισβολών. Μόνο το 31,7% διενεργεί τακτικές αξιολογήσεις και το 1,2% εφαρμόζει όλα τα μέτρα. **Συμπέρασμα:** Αν και οι οργανισμοί κατανοούν τη σημασία της ασφάλειας, υπάρχει περιθώριο βελτίωσης, ειδικά για ολοκληρωμένες στρατηγικές ασφάλειας.

14. Καταγραφή Συμβάντων Ασφαλείας Το 59,5% χρησιμοποιεί λογισμικό καταγραφής συμβάντων, το 26,2% χειροκίνητα και το 14,3% δεν διαθέτει διαδικασία καταγραφής. **Συμπέρασμα:** Η καταγραφή είναι σημαντική, αλλά η χρήση χειροκίνητων μεθόδων ή η απουσία διαδικασιών σε κάποιους οργανισμούς αναδεικνύει την ανάγκη για αυτοματοποιημένες λύσεις.

15. Σχέδιο Ανάκαμψης από Καταστροφές Το 61% διαθέτει τεκμηριωμένο σχέδιο, το 22% δεν έχει και το 17,1% βρίσκεται στη διαδικασία ανάπτυξης.

Συμπέρασμα: Παρά την ύπαρξη σχεδίων ανάκαμψης σε πολλούς οργανισμούς, η έλλειψη σχεδίου σε κάποιους αφήνει ευπάθειες σε απρόβλεπτα γεγονότα.

16. Συχνότητα Ελέγχου Σχεδίου Ανάκαμψης Το 36,6% ελέγχει το σχέδιο ανά εξάμηνο, το 29,3% ετησίως, το 19,5% σε περίπτωση αλλαγών, και το 14,6% δεν το ελέγχει. **Συμπέρασμα:** Οι τακτικοί έλεγχοι είναι καλή πρακτική, αλλά η μη τακτική αναθεώρηση σε κάποιους οργανισμούς μπορεί να μειώσει την αποτελεσματικότητά τους.

17. Συμμόρφωση με το GDPR Το 85,4% δηλώνει συμβατότητα με το GDPR, ενώ το 14,6% δεν συμμορφώνεται.
Συμπέρασμα: Η συμμόρφωση με τον GDPR είναι προτεραιότητα, αν και ορισμένοι οργανισμοί παραμένουν μη συμβατοί.

18. Διαχείριση Περιπτώσεων Μη Συμμόρφωσης Το 61% προχωρά σε άμεση διόρθωση, το 29,3% συστήνει λύσεις στον πάροχο και το 9,8% δεν έχει καθορισμένες διαδικασίες. **Συμπέρασμα:** Παρά τις διαδικασίες που έχουν αναπτυχθεί για διαχείριση μη συμμόρφωσης, η απουσία καθορισμένων διαδικασιών σε μερικούς οργανισμούς ενδέχεται να δημιουργεί κινδύνους.

19. Εσωτερικοί Έλεγχοι Ασφάλειας Πληροφοριών Το 48,8% διενεργεί τακτικούς ελέγχους, το 43,9% όταν προκύπτει ανάγκη και το 7,3% δεν διενεργεί καθόλου. **Συμπέρασμα:** Οι τακτικοί έλεγχοι είναι βασικοί για την ασφάλεια, αν και η έλλειψή τους μπορεί να αφήσει ευπάθειες.

20. Εκπαίδευση Προσωπικού σε Θέματα Ασφάλειας Cloud Το 79,7% θεωρεί την εκπαίδευση "πολύ σημαντική" και το 22% "σημαντική." **Συμπέρασμα:** Υπάρχει υψηλή αναγνώριση της αξίας της εκπαίδευσης, αν και μερικοί οργανισμοί ενδέχεται να υποτιμούν τη σημασία της.

21. Ποσοστό Εκπαίδευσης Προσωπικού Το 70,7% έχει εκπαιδεύσει το προσωπικό του, το 14,6% δεν έχει προβεί σε εκπαίδευση και το 14,6% σκοπεύει να εκπαιδεύσει στο μέλλον. **Συμπέρασμα:** Η εκπαίδευση αναγνωρίζεται ως σημαντική, αν και υπάρχει περιθώριο βελτίωσης για όσους δεν έχουν ακόμα προβεί σε αυτήν.

22. Κύριες Ανησυχίες για Ασφάλεια Δεδομένων στο Cloud Οι μεγαλύτερες ανησυχίες περιλαμβάνουν την παραβίαση (78%), απώλεια δεδομένων (75,6%) και μη εξουσιοδοτημένη πρόσβαση (63,4%).

Συμπέρασμα: Η προστασία από παραβιάσεις και απώλειες είναι προτεραιότητα, αναδεικνύοντας την ανάγκη για ενισχυμένα μέτρα προστασίας.

23. Αξιολόγηση Λύσεων Ασφαλείας στο Cloud Το 80,5% αξιολογεί τις λύσεις ως εξαιρετικές, το 12,2% ως καλές και το 7,3% ως μέτριες, με κανέναν να μην τις θεωρεί κακές. **Συμπέρασμα:** Οι περισσότερες λύσεις ασφαλείας θεωρούνται αποτελεσματικές, παρότι κάποιοι βλέπουν περιθώρια βελτίωσης.

6.4 Σύγκριση Θεωρίας και Αποτελεσμάτων Έρευνας

Σε αυτή την τελευταία ενότητα, θα πραγματοποιήσουμε μια συγκριτική ανάλυση μεταξύ της θεωρίας που εξετάσαμε και των ευρημάτων της παρούσας έρευνας. Σκοπός της σύγκρισης είναι να αναδείξει τις αντιστοιχίες και αποκλίσεις μεταξύ των θεωρητικών προσεγγίσεων στην ασφάλεια δεδομένων στο cloud και της πρακτικής εφαρμογής αυτών των αρχών, όπως αποτυπώνεται στα αποτελέσματα της έρευνάς μας.

Η ανάλυση αυτή είναι σημαντική, καθώς αποκαλύπτει το επίπεδο ευθυγράμμισης των οργανισμών με τις βέλτιστες πρακτικές και κανονιστικές απαιτήσεις που έχουν τεθεί στη θεωρία, ενώ ταυτόχρονα εντοπίζει τις περιοχές στις οποίες μπορεί να υπάρχουν κενά ή αναντιστοιχίες. Μέσα από αυτήν τη σύγκριση, φιλοδοξούμε να επισημάνουμε τις περιοχές όπου οι οργανισμοί μπορούν να βελτιώσουν τη στρατηγική ασφάλειας τους, βασιζόμενοι τόσο στα θεωρητικά πλαίσια όσο και στα αποτελέσματα που προκύπτουν από την τρέχουσα πρακτική.

- Συμμόρφωση με Κανονιστικά Πλαίσια:
    - Θεωρία: Η συμμόρφωση με κανονιστικά πρότυπα όπως GDPR, ISO 27017, και ISO 27018 είναι απαραίτητη για την προστασία των δεδομένων στο cloud.
    - Ευρήματα: Οι περισσότεροι οργανισμοί επιδιώκουν συμμόρφωση, ιδιαίτερα με το GDPR, ενώ τα πρότυπα ISO υιοθετούνται κυρίως σε μεγάλες επιχειρήσεις.
- Ασφάλεια Δεδομένων και Ιδιωτικότητα:
    - Θεωρία: Η προστασία δεδομένων θεωρείται κρίσιμη, με έμφαση στην κρυπτογράφηση και στην προστασία της ιδιωτικότητας.

- Ευρήματα: Οι συμμετέχοντες θεωρούν την κρυπτογράφηση και τις πολιτικές προστασίας ιδιωτικότητας βασικά μέτρα, ωστόσο υπάρχει ανάγκη για επιπλέον εκπαίδευση στο προσωπικό.

- Μηχανισμοί Ελέγχου Πρόσβασης:
  - Θεωρία: Η πολυπαραγοντική αυθεντικοποίηση (MFA) και η διαχείριση προσβάσεων (IAM) είναι καίρια για την αποτροπή μη εξουσιοδοτημένων προσβάσεων.
  - Ευρήματα: Οι οργανισμοί έχουν αγκαλιάσει το MFA και το IAM, όμως τα ποσοστά δείχνουν περιθώρια βελτίωσης στην τήρηση αυτών των πρακτικών.
- Ενίσχυση Συμμόρφωσης και Ασφάλειας:
  - Τα αποτελέσματα δείχνουν ότι, ενώ οι οργανισμοί δίνουν έμφαση στη συμμόρφωση, υπάρχει ανάγκη για διεύρυνση της εφαρμογής προτύπων όπως το ISO 27017 και ISO 27018, ειδικά σε μικρότερες επιχειρήσεις.
- Επένδυση στην Εκπαίδευση Προσωπικού:
  - Παρά τη γενική εφαρμογή πολιτικών ασφαλείας, τα αποτελέσματα του ερωτηματολογίου δείχνουν ότι η εκπαίδευση για την ασφάλεια παραμένει ανεπαρκής.
  - Η καλλιέργεια κουλτούρας ασφάλειας μέσω τακτικής εκπαίδευσης και ενημερώσεων κρίνεται αναγκαία για την αποτελεσματική αντιμετώπιση απειλών.
- Ενίσχυση των Μηχανισμών Ελέγχου Πρόσβασης:
  - Αν και οι περισσότεροι οργανισμοί εφαρμόζουν MFA και IAM, είναι σημαντικό να διασφαλιστεί η τακτική αναθεώρηση και επικαιροποίηση των διαδικασιών πρόσβασης.
  - Η ενίσχυση των τεχνολογιών παρακολούθησης πρόσβασης και ανίχνευσης ανωμαλιών προτείνεται για μεγαλύτερη ασφάλεια.
- Ανάγκη για Προσαρμογή σε Νέες Τεχνολογίες και Απειλές:
  - Η συνεχής εξέλιξη των τεχνολογιών cloud και οι αυξανόμενες απειλές απαιτούν από τους οργανισμούς να παραμείνουν ευέλικτοι και ενημερωμένοι.

- Προτείνεται η υιοθέτηση εργαλείων για την παρακολούθηση νέων απειλών και την προσαρμογή στις απαιτήσεις της κυβερνοασφάλειας.

Συμπεράσματα

Το υπολογιστικό νέφος έχει φέρει επανάσταση στον τρόπο λειτουργίας των οργανισμών, προσφέροντας απαράμιλλη ευελιξία, επεκτασιμότητα και αποδοτικότητα. Με τη μετάβαση από τις παραδοσιακές υποδομές στις εγκαταστάσεις σε λύσεις που βασίζονται στο cloud, οι επιχειρήσεις μπορούν να έχουν πρόσβαση σε ένα ευρύ φάσμα υπηρεσιών και πόρων κατά παραγγελία, μεταμορφώνοντας τις επιχειρησιακές τους δυνατότητες. Οι θεμελιώδεις πτυχές του υπολογιστικού νέφους, συμπεριλαμβανομένου του ορισμού του, των μοντέλων ανάπτυξης και των επιπτώσεων στην ασφάλεια, θέτουν τις βάσεις για την κατανόηση της πολυπλοκότητας και των πλεονεκτημάτων αυτής της τεχνολογίας.

Ορισμός και μοντέλα ανάπτυξης

Το υπολογιστικό νέφος ορίζεται από την ικανότητά του να παρέχει υπολογιστικούς πόρους μέσω του διαδικτύου, επιτρέποντας στους χρήστες να αξιοποιούν υποδομές, πλατφόρμες και λογισμικό ως υπηρεσίες. Αυτή η αλλαγή παραδείγματος οδήγησε στην εμφάνιση διαφόρων μοντέλων ανάπτυξης -δημόσια, ιδιωτικά, υβριδικά και πολλαπλά σύννεφα- που το καθένα προσφέρει ξεχωριστά πλεονεκτήματα και περιπτώσεις χρήσης. Τα δημόσια νέφη παρέχουν οικονομικά αποδοτικές λύσεις με υψηλή επεκτασιμότητα, τα ιδιωτικά νέφη προσφέρουν αυξημένη ασφάλεια και έλεγχο, τα υβριδικά νέφη συνδυάζουν τα καλύτερα και από τους δύο κόσμους και οι στρατηγικές πολλαπλών νέφων εξασφαλίζουν ανθεκτικότητα και ευελιξία.

Σημασία της κυβερνοασφάλειας σε περιβάλλοντα cloud

Καθώς οι οργανισμοί υιοθετούν ολοένα και περισσότερο τεχνολογίες cloud, η σημασία των ισχυρών μέτρων κυβερνοασφάλειας δεν μπορεί να υπερτονιστεί. Το νέφος εισάγει μοναδικές προκλήσεις ασφαλείας, οι οποίες απαιτούν ολοκληρωμένες στρατηγικές για την προστασία ευαίσθητων δεδομένων και τη διατήρηση της κανονιστικής συμμόρφωσης. Η αποτελεσματική ασφάλεια του νέφους περιλαμβάνει μια πολυεπίπεδη προσέγγιση, η οποία αντιμετωπίζει τις πιθανές ευπάθειες σε κάθε επίπεδο της στοίβας του νέφους.

Προκλήσεις ασφάλειας στο υπολογιστικό νέφος

Τα περιβάλλοντα υπολογιστικού νέφους αντιμετωπίζουν πολυάριθμες προκλήσεις ασφαλείας, συμπεριλαμβανομένων των παραβιάσεων δεδομένων, των απειλών εκ των έσω,

της πολυπλοκότητας του μοντέλου κοινής ευθύνης και της συμμόρφωσης με κανονιστικά πλαίσια.

Παραβιάσεις και διαρροές δεδομένων

Οι παραβιάσεις δεδομένων αποτελούν σημαντική ανησυχία, με δυνατότητα σοβαρής οικονομικής ζημίας και ζημίας στη φήμη. Η διασφάλιση της ακεραιότητας και της εμπιστευτικότητας των δεδομένων είναι υψίστης σημασίας, απαιτώντας προηγμένες τεχνικές κρυπτογράφησης, ελέγχους πρόσβασης και συνεχή παρακολούθηση για τον εντοπισμό και τον μετριασμό των απειλών

Απειλές εκ των έσω

Οι απειλές εκ των έσω αποτελούν μοναδική πρόκληση, καθώς αφορούν άτομα εντός του οργανισμού που εκμεταλλεύονται τα προνόμια πρόσβασής τους. Ο μετριασμός αυτών των απειλών περιλαμβάνει αυστηρές πρακτικές διαχείρισης ταυτότητας και πρόσβασης (IAM), εκπαίδευση των εργαζομένων και ολοκληρωμένο έλεγχο.

Μοντέλο κοινής ευθύνης

Το μοντέλο κοινής ευθύνης οριοθετεί τις ευθύνες ασφάλειας μεταξύ των παρόχων υπηρεσιών cloud και των πελατών τους. Η κατανόηση και η αποτελεσματική διαχείριση αυτού του μοντέλου είναι ζωτικής σημασίας για τη διατήρηση ενός ασφαλούς περιβάλλοντος cloud, καθώς αποσαφηνίζει τους ρόλους και τις υποχρεώσεις κάθε μέρους.

Θέματα συμμόρφωσης και κανονιστικά ζητήματα

Η συμμόρφωση με ρυθμιστικά πρότυπα όπως ο GDPR, το HIPAA και το PCI-DSS είναι απαραίτητη για τους οργανισμούς που δραστηριοποιούνται στο νέφος. Η πλοήγηση σε αυτές τις πολύπλοκες απαιτήσεις προϋποθέτει σχολαστικό σχεδιασμό, τεκμηρίωση και εφαρμογή των κατάλληλων ελέγχων ασφαλείας.

Πρότυπα ISO 27017 & 27018

Τα πρότυπα ISO 27017 και ISO 27018 είναι κρίσιμα πρότυπα για τη διασφάλιση της ασφάλειας και της ιδιωτικότητας στο cloud.

ISO 27017

Το ISO 27017 παρέχει κατευθυντήριες γραμμές για τους ελέγχους ασφάλειας πληροφοριών ειδικά προσαρμοσμένους στις υπηρεσίες νέφους, αντιμετωπίζοντας τους

μοναδικούς κινδύνους που σχετίζονται με τα περιβάλλοντα νέφους. Η συμμόρφωση με το ISO 27017 ενισχύει τη στάση ασφαλείας ενός οργανισμού, εξασφαλίζοντας ισχυρή προστασία των περιουσιακών στοιχείων που βασίζονται στο cloud.

ISO 27018

Το ISO 27018 επικεντρώνεται στην προστασία των προσωπικών δεδομένων στο νέφος, παρέχοντας ένα πλαίσιο για τη διασφάλιση της ιδιωτικότητας και της ασφάλειας των δεδομένων. Η τήρηση του ISO 27018 βοηθά τους οργανισμούς να διασφαλίζουν τις ευαίσθητες πληροφορίες και να διατηρούν την εμπιστοσύνη των πελατών.

Βασικά στοιχεία της ασφάλειας του νέφους

Η διασφάλιση της ασφάλειας του cloud περιλαμβάνει διάφορα κρίσιμα στοιχεία:

Διαχείριση ταυτότητας και πρόσβασης (IAM)

Η IAM είναι θεμελιώδης για την ασφάλεια του cloud, επιτρέποντας στους οργανισμούς να ελέγχουν ποιος μπορεί να έχει πρόσβαση σε πόρους και ποιες ενέργειες μπορεί να εκτελέσει. Οι αποτελεσματικές πρακτικές IAM περιλαμβάνουν τη χρήση ελέγχου ταυτότητας πολλαπλών παραγόντων, πρόσβασης με τα λιγότερα προνόμια και τακτικών ελέγχων.

Κρυπτογράφηση και διαχείριση κλειδιών

Η κρυπτογράφηση είναι απαραίτητη για την προστασία των δεδομένων σε κατάσταση ηρεμίας και κατά τη μεταφορά. Οι ισχυρές πρακτικές διαχείρισης κλειδιών διασφαλίζουν ότι τα κλειδιά κρυπτογράφησης αποθηκεύονται και διαχειρίζονται με ασφάλεια, αποτρέποντας τη μη εξουσιοδοτημένη πρόσβαση.

Ασφάλεια δικτύου

Η διασφάλιση του δικτύου νέφους περιλαμβάνει την εφαρμογή τειχών προστασίας, συστημάτων ανίχνευσης και πρόληψης εισβολών και ασφαλών πρωτοκόλλων επικοινωνίας. Τα μέτρα αυτά προστατεύουν από εξωτερικές επιθέσεις και διασφαλίζουν την ακεραιότητα της μετάδοσης δεδομένων.

Παρακολούθηση και καταγραφή της ασφάλειας

Η συνεχής παρακολούθηση και η καταγραφή είναι ζωτικής σημασίας για τον εντοπισμό και την αντιμετώπιση περιστατικών ασφαλείας. Η εφαρμογή ολοκληρωμένης καταγραφής και παρακολούθησης σε πραγματικό χρόνο επιτρέπει στους οργανισμούς να εντοπίζουν και να μετριάζουν άμεσα τις απειλές.

Αντιμετώπιση και αποκατάσταση περιστατικών

Η ύπαρξη ενός καλά καθορισμένου σχεδίου αντιμετώπισης περιστατικών διασφαλίζει ότι οι οργανισμοί μπορούν να ανταποκρίνονται αποτελεσματικά σε περιστατικά ασφαλείας και να ανακάμπτουν από αυτά. Αυτό περιλαμβάνει τακτικές ασκήσεις, σαφή πρωτόκολλα επικοινωνίας και ανάλυση μετά το συμβάν για τη βελτίωση των μελλοντικών προσπαθειών αντιμετώπισης.

Σύγκριση των κυριότερων παρόχων υπηρεσιών cloud

Amazon Web Services (AWS)

Η AWS είναι κυρίαρχος παίκτης στην αγορά του cloud, προσφέροντας ευρύ φάσμα υπηρεσιών και ισχυρά χαρακτηριστικά ασφαλείας. Η εκτεταμένη παγκόσμια υποδομή της, τα ευέλικτα μοντέλα τιμολόγησης και οι ολοκληρωμένες προσφορές υπηρεσιών την καθιστούν προτιμώμενη επιλογή για πολλούς οργανισμούς.

Microsoft Azure

Το Microsoft Azure παρέχει ισχυρή ενοποίηση με τα προϊόντα της Microsoft, καθιστώντας το ιδανική επιλογή για επιχειρήσεις που αξιοποιούν το οικοσύστημα της Microsoft. Η εστίαση του Azure στις δυνατότητες υβριδικού νέφους και στις λύσεις επιχειρηματικού επιπέδου ενισχύει την ελκυστικότητά του σε μεγάλους οργανισμούς με σύνθετες ανάγκες.

Google Cloud Platform (GCP)

Το GCP ξεχωρίζει για τις προηγμένες δυνατότητες μηχανικής μάθησης και ανάλυσης δεδομένων. Αξιοποιώντας την ισχυρή παγκόσμια υποδομή της Google, το GCP προσφέρει λύσεις υψηλής απόδοσης και κλιμάκωσης. Η δέσμευσή της στις τεχνολογίες ανοικτού κώδικα και τα ισχυρά μέτρα ασφαλείας ενισχύουν περαιτέρω τη θέση της στην αγορά του cloud.

Τελικές σκέψεις

Η εξέλιξη του cloud computing συνεχίζει να αναδιαμορφώνει το τεχνολογικό τοπίο, προσφέροντας πρωτοφανείς ευκαιρίες για καινοτομία και αποτελεσματικότητα. Ωστόσο, καθώς οι οργανισμοί μεταναστεύουν στο cloud, πρέπει να παραμένουν σε εγρήγορση όσον αφορά την ασφάλεια. Η κατανόηση των συγκεκριμένων προκλήσεων και η υιοθέτηση βέλτιστων πρακτικών για την ασφάλεια στο cloud είναι ζωτικής σημασίας για την προστασία των ευαίσθητων δεδομένων και τη διατήρηση της συμμόρφωσης με τα κανονιστικά πρότυπα.

Η τήρηση προτύπων όπως το ISO 27017 και το ISO 27018 παρέχει μια σταθερή βάση για την ασφάλεια και την προστασία της ιδιωτικής ζωής στο νέφος. Επιπλέον, η αξιοποίηση των πλεονεκτημάτων κορυφαίων παρόχων υπηρεσιών cloud, όπως οι AWS, Azure και GCP, μπορεί να βοηθήσει τους οργανισμούς να βελτιστοποιήσουν τις στρατηγικές τους για το cloud, εξασφαλίζοντας ισχυρή ασφάλεια, υψηλές επιδόσεις και οικονομική αποδοτικότητα.

Καθώς το τοπίο του cloud computing συνεχίζει να εξελίσσεται, η ενημέρωση σχετικά με τις αναδυόμενες απειλές και τις εξελίξεις στις τεχνολογίες ασφαλείας θα είναι απαραίτητη. Οι οργανισμοί πρέπει να καλλιεργήσουν μια κουλτούρα συνεχούς βελτίωσης και προληπτικής διαχείρισης κινδύνων για να περιηγηθούν επιτυχώς στις πολυπλοκότητες της ασφάλειας του cloud.

Συμπερασματικά, η μετάβαση στο υπολογιστικό νέφος προσφέρει σημαντικά οφέλη, αλλά απαιτεί επίσης μια ολοκληρωμένη και δυναμική προσέγγιση της ασφάλειας στον κυβερνοχώρο. Με την κατανόηση των περιπλοκών των περιβαλλόντων νέφους, την τήρηση των καθιερωμένων προτύπων και την αξιοποίηση των δυνατοτήτων των κορυφαίων παρόχων υπηρεσιών νέφους, οι οργανισμοί μπορούν να αξιοποιήσουν πλήρως τις δυνατότητες του υπολογιστικού νέφους, προστατεύοντας παράλληλα τα πιο πολύτιμα περιουσιακά τους στοιχεία.

Βιβλιογραφία

Abdulsalam, Y. S., & Hedabou, M. (2021). Security and privacy in cloud computing: technical review. *Future Internet*, *14*(1), 11.

AlAhmad, A. S., Kahtan, H., Alzoubi, Y. I., Ali, O., & Jaradat, A. (2021). Mobile cloud computing models security issues: A systematic review. *Journal of Network and Computer Applications*, *190*, 103152.

Alam, T. (2020). Cloud Computing and its role in the Information Technology. *IAIC Transactions on Sustainable Digital Innovation (ITSDI)*, *1*(2), 108-115.

Alouffi, B., Hasnain, M., Alharbi, A., Alosaimi, W., Alyami, H., & Ayaz, M. (2021). A systematic literature review on cloud computing security: threats and mitigation strategies. *IEEE Access*, *9*, 57792-57807.

Alouffi, B., Hasnain, M., Alharbi, A., Alosaimi, W., Alyami, H., & Ayaz, M. (2021). A systematic literature review on cloud computing security: threats and mitigation strategies. *IEEE Access*, *9*, 57792-57807.

Arafat, M. (2018, June). Information security management system challenges within a cloud computing environment. In *Proceedings of the 2nd International Conference on Future Networks and Distributed Systems* (pp. 1-6).

Balani, Z., & Varol, H. (2020, June). Cloud computing security challenges and threats. In *2020 8th International Symposium on Digital Forensics and Security (ISDFS)* (pp. 1-4). IEEE.

Bello, S. A., Oyedele, L. O., Akinade, O. O., Bilal, M., Delgado, J. M. D., Akanbi, L. A., ... & Owolabi, H. A. (2021). Cloud computing in construction industry: Use cases, benefits and challenges. *Automation in Construction*, *122*, 103441.

Butt, U. A., Mehmood, M., Shah, S. B. H., Amin, R., Shaukat, M. W., Raza, S. M., ... & Piran, M. J. (2020). A review of machine learning algorithms for cloud computing security. *Electronics*, *9*(9), 1379.

Drozdova, M., Bridova, I., Uramova, J., & Moravcik, M. (2020, November). Private cloud security architecture. In *2020 18th International Conference on Emerging eLearning Technologies and Applications (ICETA)* (pp. 84-89). IEEE.

Gai, K., Guo, J., Zhu, L., & Yu, S. (2020). Blockchain meets cloud computing: A survey. *IEEE Communications Surveys & Tutorials*, *22*(3), 2009-2030.

Gupta, B., Mittal, P., & Mufti, T. (2021, March). A review on amazon web service (aws), microsoft azure & google cloud platform (gcp) services. In *Proceedings of the 2nd International Conference on ICT for Digital, Smart, and Sustainable Development, ICIDSSD 2020, 27-28 February 2020, Jamia Hamdard, New Delhi, India*.

Ibrahim, I. M. (2021). Task scheduling algorithms in cloud computing: A review. *Turkish Journal of Computer and Mathematics Education (TURCOMAT)*, *12*(4), 1041-1053.

ISO 690

Jiang, P., Wang, Q., Huang, M., Wang, C., Li, Q., Shen, C., & Ren, K. (2021). Building in-the-cloud network functions: Security and privacy challenges. *Proceedings of the IEEE*, *109*(12), 1888-1919.

Jimmy, F. N. U. (2024). Cyber security Vulnerabilities and Remediation Through Cloud Security Tools. *Journal of Artificial Intelligence General science (JAIGS) ISSN: 3006-4023*, *2*(1), 129-171.

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.

Kaushik, P., Rao, A. M., Singh, D. P., Vashisht, S., & Gupta, S. (2021, November). Cloud computing and comparison based on service and performance between Amazon AWS, Microsoft Azure, and Google Cloud. In *2021 International Conference on Technological Advancements and Innovations (ICTAI)* (pp. 268-273). IEEE.

Kumar, S., Karnani, G., Gaur, M. S., & Mishra, A. (2021, April). Cloud security using hybrid cryptography algorithms. In *2021 2nd international conference on intelligent engineering and management (ICIEM)* (pp. 599-604). IEEE.

Marinescu, D. C. (2022). *Cloud computing: theory and practice*. Morgan Kaufmann.

Pallathadka, H., Sajja, G. S., Phasinam, K., Ritonga, M., Naved, M., Bansal, R., & Quiñonez-Choquecota, J. (2022). An investigation of various applications and related challenges in cloud computing. *Materials Today: Proceedings*, *51*, 2245-2248.

Parast, F. K., Sindhav, C., Nikam, S., Yekta, H. I., Kent, K. B., & Hakak, S. (2022). Cloud computing security: A survey of service-based models. *Computers & Security*, *114*, 102580.

Parast, F. K., Sindhav, C., Nikam, S., Yekta, H. I., Kent, K. B., & Hakak, S. (2022). Cloud computing security: A survey of service-based models. *Computers & Security*, *114*, 102580.

Patel, H. B., & Kansara, N. (2021). Cloud Computing Deployment Models: A Comparative Study. *International Journal of Innovative Research in Computer Science & Technology (IJIRCST)*.

Sadeeq, M. M., Abdulkareem, N. M., Zeebaree, S. R., Ahmed, D. M., Sami, A. S., & Zebari, R. R. (2021). IoT and Cloud computing issues, challenges and opportunities: A review. *Qubahan Academic Journal*, *1*(2), 1-7.

Sandhu, A. K. (2021). Big data with cloud computing: Discussions and challenges. *Big Data Mining and Analytics*, *5*(1), 32-40.

Saraswat, M., & Tripathi, R. C. (2020, December). Cloud computing: Comparison and analysis of cloud service providers-AWs, Microsoft and Google. In *2020 9th international conference system modeling and advancement in research trends (SMART)* (pp. 281-285). IEEE.

Shafiq, D. A., Jhanjhi, N. Z., & Abdullah, A. (2022). Load balancing techniques in cloud computing environment: A review. *Journal of King Saud University-Computer and Information Sciences*, *34*(7), 3910-3933.

Sinchana, M. K., & Savithramma, R. M. (2020). Survey on cloud computing security. Innovations in Computer Science and Engineering: *Proceedings of 7th ICICSE*, 1-6.

Sohal, A. S., Sandhu, R., Sood, S. K., & Chang, V. (2018). A cybersecurity framework to identify malicious edge device in fog computing and cloud-of-things environments. *Computers & Security*, *74*, 340-354.

Sun, P. (2020). Security and privacy protection in cloud computing: Discussions and challenges. *Journal of Network and Computer Applications*, *160*, 102642.

Sunyaev, A., & Sunyaev, A. (2020). Cloud computing. *Internet Computing: Principles of Distributed Systems and Emerging Internet-Based Technologies*, 195-236.

Tabrizchi, H., & Kuchaki Rafsanjani, M. (2020). A survey on security challenges in cloud computing: issues, threats, and solutions. *The journal of supercomputing*, *76*(12), 9493-9532.

Tissir, N., El Kafhali, S., & Aboutabit, N. (2021). Cybersecurity management in cloud computing: semantic literature review and conceptual framework proposal. *Journal of Reliable Intelligent Environments*, *7*, 69-84.

Ucuz, D. (2020, June). Comparison of the IoT platform vendors, microsoft Azure, Amazon web services, and Google cloud, from users' perspectives. In *2020 8th international symposium on digital forensics and security (ISDFS)* (pp. 1-4). IEEE.

Weil, T. (2018). Taking compliance to the cloud—Using ISO standards (tools and techniques). *IT Professional*, *20*(6), 20-30.

Yang, P., Xiong, N., & Ren, J. (2020). Data security and privacy protection for cloud storage: A survey. *Ieee Access*, *8*, 131723-131740.