Πανεπιστήμιο Πειραιώς

Σχολή Τεχνολογιών Πληροφορικής και Τηλεπικοινωνιών

Τμήμα Ψηφιακών Συστημάτων

Μεταπτυχιακό Πρόγραμμα Σπουδών

«Διοίκηση Ταυτοτήτων και Πρόσβασης σε περιβάλλοντα Νέφους»

Επιβλέπων Καθηγητής: Σ. Γκρίτζαλης

Ονοματεπώνυμο	E-mail	A.M.
Ανδρικόπουλος Αριστείδης	arisandrikop@gmail.com	mte2202

Περιεχόμενα

Περίληψη

Το περιβάλλον cloud computing, συνήθως χωρίζεται σε τρία κύρια μοντέλα υπηρεσιών cloud, όπως Software-as-a-Service (SaaS), Platform-as-a-a-Service (PaaS) και Infrastructure-as-a-Service (IaaS). Το Cloud βασίζεται σε μια αρχιτεκτονική προσανατολισμένη στην υπηρεσία, η οποία έχει τη δυνατότητα να παρέχει Βάση δεδομένων ως υπηρεσία (DbaaS). Το περιβάλλον cloud computing επίσης, παρέχει έναν καλύτερο τρόπο διαχείρισης των διαθέσιμων πόρων τόσο στη βιομηχανία όσο και στον ακαδημαϊκό χώρο.

Η λειτουργία της διαχείρισης ταυτότητας και πρόσβασης (IAM) διαδραματίζει κεντρικό ρόλο στην ασφάλεια των περιβαλλόντων cloud. Η λειτουργία της διαχείρισης ταυτότητας και πρόσβασης περιλαμβάνει τον έλεγχο της πρόσβασης των χρηστών σε πόρους και δεδομένα, διασφαλίζοντας ταυτόχρονα τον έλεγχο ταυτότητας, την εξουσιοδότηση και τη σωστή διαχείριση των χρηστών.

Στόχος του IAM είναι να βοηθήσει τους οργανισμούς να ελέγχουν την πρόσβαση σε εφαρμογές, υπηρεσίες και δεδομένα στο cloud με ολοκληρωμένα πρωτόκολλα ελέγχου ταυτότητας και εξουσιοδότησης. Οι επιχειρήσεις μπορούν να χρησιμοποιήσουν την διαδικασία διαχείρισης ταυτότητας και πρόσβασης σε περιβάλλον Cloud, για να αυξήσουν την ασφάλειά τους, να βελτιώσουν τις διαδρομές πρόσβασης των χρηστών και να διαχειριστούν τις ταυτότητες σε περιβάλλοντα cloud.

Η διαδικασία διαχείρισης ταυτότητας και πρόσβασης σε περιβάλλον Cloud, είναι μια λύση προσαρμοσμένη, ειδικά για λειτουργίες που βασίζονται στο περιβάλλον αυτό με πολλά πλεονεκτήματα, όπως βελτιωμένη διαχείριση ταυτότητας, ολοκληρωμένους μηχανισμούς ασφαλείας και λεπτομερείς ελέγχους πρόσβασης για συγκεκριμένους φόρτους εργασίας. Τέλος, ο έλεγχος ταυτότητας χρήστη, είναι η πρώτη άμυνα στο περιβάλλον Cloud, αφού διασφαλίζει ότι μόνο εξουσιοδοτημένα άτομα μπορούν να έχουν πρόσβαση σε υπηρεσίες και πόρους cloud και προστατεύει ευαίσθητα δεδομένα από πιθανές απειλές.

Εισαγωγή

Αποτελεί γεγονός στις μέρες μας πως ο όρος *cloud computing* αναφέρεται ως ένας συνδυασμός διαφορετικών διαμορφώσιμων υπολογιστικών πόρων όπως τα δίκτυα, οι διακομιστές, οι αποθηκευτικοί χώροι, οι σχετικές υπηρεσίες, οι εφαρμογές που βοηθούν στην παροχή εύκολης και οι κατ' απαίτηση πρόσβαση στους χρήστες του περιβάλλοντος cloud (Marinescu, 2013). Ο όρος cloud computing ωστόσο, αναφέρεται σε μεγάλο βαθμό από τους ανθρώπους και χρησιμοποιείται επί του παρόντος σε πολλούς εμπορικούς τομείς (Mather, Kumaraswamy and Latif, 2009).

Οι πάροχοι υπηρεσιών Cloud (CSP) είναι υπεύθυνοι για την ταυτότητα και άλλα είδη διαχείρισης σε περιβάλλον cloud. Ωστόσο, ένας μεγάλος αριθμός περιστατικών διαρροής δεδομένων, προκαλείται λόγω των τρωτών σημείων στα συστήματα διαχείρισης ταυτότητας (Ghelani, Hua and Koduru, 2022). Ο όρος διαχείριση ταυτότητας και πρόσβασης ή διαφορετικά γνωστός διεθνώς ως Internet and Access Management σε περιβάλλον cloud, είναι ένα σημαντικό στοιχείο για την αποδοχή υπηρεσιών που βασίζονται σε περιβάλλον cloud (Ghelani, 2022).

Επί του παρόντος, ο μηχανισμός διαχείρισης ταυτότητας επικεντρώνεται κυρίως σε παρόχους υπηρεσιών Cloud, το οποίο δύσκολα ικανοποιεί την απαίτηση της ευέλικτης και λεπτομερούς πολιτικής ελέγχου πρόσβασης των χρηστών σε περιβάλλοντα υπολογιστών (Mungoli, 2023a).

Σύμφωνα με τα παραπάνω ωστόσο, θα πρέπει να σημειωθεί πως το περιβάλλον cloud ταξινομείται γενικά ως περιβάλλον Private Cloud, Public Cloud και Hybrid/Federated Cloud. Ένα πλαίσιο λειτουργίας Private Cloud έχει σχεδιαστεί ως προς τις ανάγκες ενός συγκεκριμένου οργανισμού. Σε ένα δημόσιο περιβάλλον cloud (Public Cloud), η υποστήριξη υποδομής σε πολλούς οργανισμούς, διευκολύνεται και διαχειρίζεται από έναν τρίτο πάροχο (Marinescu, 2013)

Επίσης, το μοντέλο ενός δημόσιου υπολογιστικού νέφους είναι γνωστό ως περιβάλλον πολλαπλών λειτουργιών το οποίο μοιράζεται τους πόρους, μεταξύ των οργανισμών με σκοπό να μειώσει το συνολικό κόστος της υπηρεσίας (Comer, 2021) Τέλος, η υβριδική υποδομή cloud, είναι ένας συνδυασμός υπηρεσιών cloud εσωτερικής χρήσης, ιδιωτικών και δημόσιων υπηρεσιών. Μια άλλη έννοια στην υποδομή cloud, είναι τα σύννεφα

πολλαπλών παρόχων, το οποίο είναι ένα περιβάλλον που βασίζεται σε πολλούς παρόχους cloud και διαιρεί τον φόρτο εργασίας μεταξύ ενός περιβάλλοντος cloud. Υπάρχουν, επίσης, διαφορετικά περιβάλλοντα cloud που έχουν σχεδιαστεί ειδικά για να υποστηρίζουν την υπηρεσία, όπως οι υπηρεσίες cloud Internet of Things (IoT), οι οποίες είναι ειδικά σχεδιασμένες για να χειρίζονται και να αναλύουν τα δεδομένα από συσκευές IoT και κινητές υπηρεσίες cloud που χρησιμοποιούν υπολογιστικό νέφος για την παράδοση εφαρμογών σε κινητές συσκευές.

Σύμφωνα με τα παραπάνω, θα πρέπει να σημειωθεί πως το περιβάλλον cloud computing, συνήθως χωρίζεται σε τρία κύρια μοντέλα υπηρεσιών cloud, όπως Software-as-a-Service (SaaS), Platform-as-a-a-Service (PaaS) και Infrastructure-as-a-Service (IaaS). Το Cloud βασίζεται σε μια αρχιτεκτονική, προσανατολισμένη στην υπηρεσία η οποία έχει τη δυνατότητα να παρέχει Βάση δεδομένων ως υπηρεσία (DbaaS) (Comer, 2021).Το περιβάλλον cloud computing επίσης, παρέχει έναν καλύτερο τρόπο διαχείρισης των διαθέσιμων πόρων τόσο στη βιομηχανία όσο και στον ακαδημαϊκό χώρο (Mungoli, 2023a).

Το σύστημα cloud, είναι από τη φύση του ιδιαιτέρως λειτουργικό, λαμβάνοντας υπόψη πολυάριθμους χρήστες, συσκευές, δίκτυα, οργανισμούς και πόρους που συνδέονται και αποσυνδέονται συχνά με το σύστημα. Η καλύτερη επιλογή για το μοντέλο υπηρεσίας cloud που πρέπει να εφαρμοστεί, καθορίζεται από διάφορους παράγοντες. Οι σημαντικοί παράγοντες που πρέπει να ληφθούν υπόψη, είναι η ευελιξία, η επεκτασιμότητα, η διαλειτουργικότητα και ο έλεγχος της υπηρεσίας (Marinescu, 2013).Το περιβάλλον cloud computing απαιτεί εκτεταμένο μηχανισμό ελέγχου ταυτότητας και εξουσιοδότησης για την ασφάλεια των δεδομένων και των πόρων του λόγω της πολυπλοκότητας της χρήσης.

Η έλλειψη αποτελεσματικού μηχανισμού λειτουργίας, δημιουργεί πολλαπλές προκλήσεις στο περιβάλλον cloud, οι οποίες περιλαμβάνουν τη διαχείριση ταυτότητας, τη διαχείριση κινδύνου, τη διαχείριση εμπιστοσύνης, τη συμμόρφωση, την ασφάλεια δεδομένων, την ιδιωτικότητα, τη διαφάνεια και τη διαρροή δεδομένων. Μια άλλη πτυχή των συστημάτων cloud, είναι η πολυπλοκότητα και οι σχετικές προκλήσεις ασφαλείας. Ζητήματα απώλειας ελέγχου και διαφάνειας, δημιουργούνται επίσης κατά την αποθήκευση και επεξεργασία πληροφοριών χρήστη από τους παρόχους υπηρεσιών Cloud (CSP) ή εκτός των οργανωτικών ορίων. Λόγω αυτών των χαρακτηριστικών προκλήσεων ασφαλείας, η υιοθέτηση του περιβάλλοντος cloud είναι αργή ανεξάρτητα από τα ασφαλή και ελκυστικά χαρακτηριστικά του cloud. Παρά τα προαναφερθέντα προβλήματα, ο οργανισμός έχει μια

τάση απροθυμίας να συνεισφέρει τις κρίσιμες πληροφορίες ταυτότητάς του στο περιβάλλον cloud (Mather, Kumaraswamy and Latif, 2009)

Σε ένα σύστημα cloud λοιπόν, η αποθήκευση και η επεξεργασία των δεδομένων, πραγματοποιείται από οργανισμούς ή με τη βοήθεια από μέρους τρίτων προμηθευτών. Ο πάροχος υπηρεσιών ωστόσο, πρέπει να διασφαλίσει ότι τα δεδομένα και οι εφαρμογές που είναι αποθηκευμένα στο cloud, προστατεύονται, καθώς και ότι η υποδομή βρίσκεται σε ασφαλές περιβάλλον.

Επιπλέον, οι χρήστες πρέπει να επαληθεύσουν ότι τα διαπιστευτήριά τους για έλεγχο ταυτότητας, είναι ασφαλή (Ghelani, 2022). Υπάρχουν πολλά ζητήματα ασφάλειας που θέτουν σε κίνδυνο τα δεδομένα στη διαδικασία πρόσβασης και αποθήκευσης δεδομένων στο περιβάλλον cloud, ειδικά στην περίπτωση αποθήκευσης δεδομένων με τη βοήθεια τρίτων προμηθευτών όπου οι ίδιοι μπορεί να είναι κακόβουλοι εισβολείς.

Αν και υπάρχουν διαθέσιμα πρότυπα και βέλτιστες πρακτικές για την αντιμετώπιση τέτοιων προβλημάτων ασφαλείας, οι πάροχοι υπηρεσιών cloud είναι απρόθυμοι να ασφαλίσουν το δίκτυό τους με το ενημερωμένο σύνολο προτύπων ασφαλείας (Ghelani, Hua and Koduru, 2022). Η διαχείριση ταυτότητας και πρόσβασης βέβαια, είναι μία από τις βέλτιστες πρακτικές για μέτρηση στις υπηρεσίες cloud.

Επί του παρόντος, η λειτουργία διαχείρισης ταυτότητας και πρόσβασης (IAM), παρέχει αποτελεσματική ασφάλεια για συστήματα cloud. Τα συστήματα διαχείρισης ταυτότητας και πρόσβασης εκτελούν διαφορετικές λειτουργίες για την παροχή ασφάλειας στο περιβάλλον cloud που περιλαμβάνουν έλεγχο ταυτότητας, εξουσιοδότηση και παροχή αποθήκευσης και επαλήθευσης.

Το σύστημα διαχείρισης ταυτότητας και πρόσβασης, εγγυάται την ασφάλεια των ταυτοτήτων και των χαρακτηριστικών των χρηστών του cloud διασφαλίζοντας ότι τα κατάλληλα άτομα επιτρέπονται στα συστήματα cloud. Τα συστήματα διαχείρισης ταυτότητας και πρόσβασης, βοηθούν επίσης στη διαχείριση των δικαιωμάτων πρόσβασης ελέγχοντας εάν το σωστό άτομο με τα σωστά προνόμια έχει πρόσβαση σε πληροφορίες που είναι αποθηκευμένες σε συστήματα cloud (Marinescu, 2013). Επί του παρόντος, πολλοί οργανισμοί χρησιμοποιούν συστήματα διαχείρισης ταυτότητας και πρόσβασης για να

παρέχουν μεγαλύτερη ασφάλεια για ευαίσθητες πληροφορίες που είναι αποθηκευμένες στο περιβάλλον cloud (Marinescu, 2013).

Κεφάλαιο 1ο – Προστασία Δεδομένων και Ασφάλεια στο Νέφος: Συμμόρφωση και Βέλτιστες Πρακτικές

1.1 Πρότυπα και Νομοθεσία για την Προστασία Δεδομένων στο Νέφος

Το απόρρητο των δεδομένων αποτελεί κρίσιμο ζήτημα στο υπολογιστικό νέφος και είναι σημαντικό να διασφαλιστεί ότι λαμβάνονται τα κατάλληλα μέτρα για την προστασία των ευαίσθητων πληροφοριών. Τα διάφορα πρότυπα και νομοθεσίες που έχουν θεσπιστεί στον τομέα αυτό, όπως τα NIST, ISO, ENISA και GDPR, παρέχουν πολύτιμη καθοδήγηση για την επίτευξη αυτού του στόχου. Κάθε πρότυπο έχει τη δική του σειρά συστάσεων, οι οποίες μπορούν να χρησιμοποιηθούν για την ανάπτυξη κατευθυντήριων γραμμών για την προστασία των προσωπικών δεδομένων στο νέφος. Επιπλέον, τα πρότυπα προτείνουν επίσης διάφορα εργαλεία και τεχνικές που μπορούν να χρησιμοποιηθούν για την αξιολόγηση του κινδύνου παραβίασης των δεδομένων και για τον σχεδιασμό της προστασίας της ιδιωτικότητας στα συστήματα που βασίζονται στο νέφος.

Ένα ευρέως αποδεκτό πρότυπο για τη διαχείριση της ασφάλειας των πληροφοριών είναι το ISO/IEC 27001 (ISO/IEC:27001, 2022). Καθορίζει μια μεθοδική στρατηγική για τη διατήρηση των ευαίσθητων εταιρικών πληροφοριών σε ασφάλεια. Το πρότυπο προσφέρει ένα πλαίσιο για το χειρισμό και τη διασφάλιση ευαίσθητων δεδομένων, συμπεριλαμβανομένων οικονομικών, ατομικών και πληροφοριών πνευματικής ιδιοκτησίας

Μια προσθήκη στο πρότυπο διαχείρισης της ασφάλειας πληροφοριών ISO/IEC 27001 είναι το πρότυπο προστασίας των προσωπικών δεδομένων ISO/IEC 27018:2019 (ISO/IEC 27018, 2019). Για την προστασία των προσωπικών πληροφοριών (PII) σε δημόσια νέφη που χρησιμεύουν ως επεξεργαστές PII, προσφέρει μια σειρά συστάσεων και βέλτιστων πρακτικών.

Στόχος του ISO/IEC 27018:2019 είναι να βοηθήσει τους παρόχους υπηρεσιών νέφους να αποδείξουν ότι συμμορφώνονται με όλους τους ισχύοντες νόμους και κανόνες προστασίας δεδομένων, συμπεριλαμβανομένου του GDPR. Επιπλέον, μπορεί να βοηθήσει τις επιχειρήσεις να διασφαλίσουν την ασφάλεια των δεδομένων τους όταν χρησιμοποιούν υπηρεσίες cloud. Αν και δεν απαιτείται, το πρότυπο θεωρείται συνήθως ως βέλτιστη πρακτική για τη διασφάλιση των προσωπικών δεδομένων στο νέφος. Παρέχει στους πελάτες έναν τρόπο να αξιολογούν τις

πολιτικές προστασίας δεδομένων από τους παρόχους υπηρεσιών νέφους (CSP) και ένα πλαίσιο για τους CSP να υιοθετούν μέτρα προστασίας της ιδιωτικής ζωής. Το πλαίσιο αυτό περιλαμβάνει μια ποικιλία ελέγχων (ISO/IEC 27018, 2019).

1.2 Μέτρα και Πολιτικές Ασφαλείας για την Προστασία Δεδομένων ISO/IEC 27018:2019

Το ISO/IEC 27018:2019 παρέχει ένα σύνολο πολιτικών και μέτρων ασφαλείας για την προστασία των προσωπικών δεδομένων στο περιβάλλον του cloud computing. Οι πάροχοι υπηρεσιών νέφους υποχρεούνται να εφαρμόζουν αυστηρές διαδικασίες για τη διασφάλιση της εμπιστευτικότητας, της διαφάνειας και της συγκατάθεσης των χρηστών, ενώ προστατεύουν τα δεδομένα από μη εξουσιοδοτημένη πρόσβαση ή επεξεργασία. Επιπλέον, το πρότυπο απαιτεί την τήρηση των νομικών και κανονιστικών υποχρεώσεων, την εκπαίδευση του προσωπικού και την εφαρμογή ελέγχων για την ενίσχυση της ασφάλειας σε όλα τα επίπεδα της υπηρεσίας νέφους. (ISO/IEC 27018, 2019) Πιο αναλυτικά :

Πολιτικές ασφάλειας πληροφοριών: Την ελαχιστοποίηση των δεδομένων, τη διαφάνεια, τη συγκατάθεση και τα ατομικά δικαιώματα. Επιπλέον, πρέπει να διασφαλίζουν ότι οι προσωπικές πληροφορίες δεν αποκαλύπτονται, αλλάζουν ή αφαιρούνται χωρίς τη σωστή συγκατάθεση. Ακόμα, πρέπει να εκπαιδεύουν τους πελάτες σχετικά με τις πολιτικές τους για την προστασία των δεδομένων, τα περιστατικά ασφάλειας δεδομένων και τη διαβίβαση δεδομένων σε τρίτους. Η διαφάνεια είναι ένα κρίσιμο στοιχείο. Το πρότυπο ορίζει περαιτέρω ότι όλοι οι υπό επεξεργαστές που απασχολούνται από τους CSP πρέπει να τηρούν τις 3 προδιαγραφές του. Οι CSP υποχρεούνται επίσης να σέβονται τα δικαιώματα προστασίας των προσωπικών δεδομένων των υποκειμένων των δεδομένων. Αυτό περιλαμβάνει την παροχή πρόσβασης και δυνατότητας επεξεργασίας και διαγραφής των προσωπικών τους δεδομένων. Επεξεργαζόμενοι τα δεδομένα προσωπικού χαρακτήρα αποκλειστικά σύμφωνα με τους ισχύοντες νόμους και κανονισμούς, κάθε εμπλεκόμενο μέρος πρέπει να τηρεί το πρότυπο και να αποφεύγει να προβαίνει σε μη εξουσιοδοτημένες ή παράνομες δραστηριότητες επεξεργασίας. Οι CSP πρέπει να διασφαλίζουν ότι τα δεδομένα των πελατών δεν χρησιμοποιούνται για σκοπούς μάρκετινγκ ή διαφήμισης χωρίς τη συγκατάθεση του πελάτη. Τέλος, θα πρέπει να οριστούν διάφορα μέτρα ασφαλείας, συμπεριλαμβανομένων των περιορισμών πρόσβασης, της διαχείρισης περιστατικών, της επιχειρησιακής συνέχειας και της ανάκαμψης από καταστροφές.

Διαχείριση περιουσιακών στοιχείων πληροφοριών - IAM: Το ISO/IEC 27018:2019 απαιτεί την ασφάλεια IAM για έναν CSP να συμμορφώνεται με τις απαιτήσεις του. Ωστόσο, για να γίνει αυτό μπορεί να βρεθεί η πληροφορία στο ISO/IEC 27001, επειδή το IAM δεν είναι ένα θέμα ιδιωτικότητας που βασίζεται στο cloud. Απαιτείται ένας αριθμός βημάτων για τη διασφάλιση της ασφάλειας IAM. Καθιέρωση πολιτικών, διαδικασιών και στόχων για την ασφάλεια των πληροφοριών. Προσδιορισμός και αξιολόγηση των περιουσιακών στοιχείων, συμπεριλαμβανομένης της αξίας, της ευαισθησίας και της κρισιμότητάς τους, και καθορισμός των κατάλληλων μέτρων προστασίας. Εφαρμογή και διατήρηση μιας διαδικασίας διαχείρισης κινδύνων για τον εντοπισμό, την ανάλυση, την αξιολόγηση και την αντιμετώπιση των κινδύνων ασφάλειας. Επιλογή και εφαρμογή κατάλληλων ελέγχων ασφαλείας, συμπεριλαμβανομένων φυσικών, τεχνικών και διοικητικών μέτρων, για την προστασία. Διεξαγωγή τακτικής παρακολούθησης, ανασκόπησης και αξιολόγησης της αποτελεσματικότητας του ΣΔΠΔ και λήψη διορθωτικών μέτρων, εφόσον απαιτείται. Αυτές είναι μόνο μερικές από τις μεθόδους που προτείνει το ISO/IEC 27001 όπως επίσης και το 27018.

Ασφάλεια ανθρώπινου δυναμικού: Οι οργανισμοί πρέπει να διενεργούν ελέγχους ιστορικού για τους εργαζόμενους, τους εργολάβους και το προσωπικό, ώστε να διασφαλίζουν ότι είναι αξιόπιστοι και ότι δεν αποτελούν κίνδυνο για την ασφάλεια. Πρέπει, επίσης, να γνωστοποιούν με σαφήνεια τους όρους και τις προϋποθέσεις απασχόλησης που σχετίζονται με την ασφάλεια των πληροφοριών, συμπεριλαμβανομένης της εμπιστευτικότητας, της επιτρεπόμενης χρήσης των προσωπικών δεδομένων και των κυρώσεων για παραβιάσεις της πολιτικής. Όλα τα μέλη του προσωπικού πρέπει να λαμβάνουν εκπαίδευση για την ασφάλεια των πληροφοριών και να γνωρίζουν τις πολιτικές και τις διαδικασίες. Ο οργανισμός πρέπει να καθιερώσει μια διαδικασία για την αντιμετώπιση των παραβιάσεων της πολιτικής και την επιβολή της πειθαρχίας, ώστε να αποθαρρύνονται οι πιθανοί παραβάτες. Όταν ένας υπάλληλος αποχωρεί ή αλλάζει ρόλο, ο οργανισμός πρέπει να διαθέτει πολιτικές για την ανάκληση της πρόσβασής του σε περιουσιακά στοιχεία πληροφοριών.

Έλεγχος πρόσβασης: Για να διασφαλιστεί η ασφάλεια του ελέγχου πρόσβασης, οι CSP θα πρέπει να διαθέτουν τεκμηριωμένη πολιτική που περιγράφει τις διαδικασίες και τις κατευθυντήριες γραμμές για τη χορήγηση και ανάκληση πρόσβασης σε περιουσιακά στοιχεία. Οι CSP’s θα πρέπει να διαχειρίζονται την πρόσβαση αυτή σύμφωνα με αυτή την

πολιτική, η οποία περιλαμβάνει τη δημιουργία, την ενημέρωση και τη διαγραφή λογαριασμών χρηστών, καθώς και τη χορήγηση δικαιωμάτων πρόσβασης. Οι CSP's πρέπει να θέτουν σε εφαρμογή ελέγχους πρόσβασης σε συστήματα και εφαρμογές, περιορισμούς κωδικών πρόσβασης και διαχείριση προσβάσεων για την αποτροπή μη εξουσιοδοτημένης πρόσβασης σε συστήματα πληροφοριών. Για την τηλεργασία και την κινητή πληροφορική, οι CSP's, πρέπει να διασφαλίζουν ότι τα εργαλεία απομακρυσμένης πρόσβασης και οι κινητές συσκευές είναι ασφαλή και διαθέτουν τα κατάλληλα μέτρα ασφαλείας για τη διασφάλιση των προσωπικών δεδομένων στα οποία παρέχεται πρόσβαση εκτός του οργανισμού. Οι CSP's πρέπει επίσης να παρακολουθούν ποιος έχει πρόσβαση σε συστήματα πληροφοριών για να εντοπίζουν κάθε ύποπτη ή μη εξουσιοδοτημένη δραστηριότητα και να λαμβάνουν τα κατάλληλα μέτρα. Επιπλέον, θα πρέπει να διαθέτουν κατάλληλη διαδικασία διαχείρισης περιστατικών για να χειρίζονται θέματα ασφάλειας που αφορούν τον έλεγχο πρόσβασης. Εάν διαταραχθούν οι μέθοδοι ελέγχου πρόσβασης, οι CSP's πρέπει να εφαρμόσουν τις απαραίτητες διασφαλίσεις για να διατηρήσουν τη διαθεσιμότητα των συστημάτων.

Κρυπτογραφία: Για την προστασία των προσωπικών πληροφοριών θα πρέπει να εφαρμόζονται κρυπτογραφικά μέτρα με βάση τις πολιτικές ασφαλείας του οργανισμού και την ανάλυση κινδύνου. Τα κρυπτογραφικά κλειδιά πρέπει να διατηρούνται ασφαλή και να προστατεύονται από μη εξουσιοδοτημένη χρήση, αποκάλυψη, διαγραφή ή αλλοίωση. Πρέπει να αναπτυχθούν και να εφαρμοστούν διαδικασίες για τη διαχείριση του κύκλου ζωής των κρυπτογραφικών κλειδιών, συμπεριλαμβανομένης της παραγωγής, διανομής, αποθήκευσης, αντικατάστασης και καταστροφής των κλειδιών. Για να εξασφαλιστεί η ασφάλεια των προσωπικών δεδομένων, τα κρυπτογραφικά πρωτόκολλα πρέπει να σχεδιάζονται και να αναπτύσσονται σωστά. Επίσης η εγκυρότητα της προέλευσης των δεδομένων και η ακεραιότητα των δεδομένων, μπορεί να επιτευχθεί με κρυπτογραφικές διαδικασίες. Κατά τη διαβίβαση ευαίσθητων δεδομένων μέσω δημόσιων δικτύων, πρέπει να χρησιμοποιείται ισχυρή κρυπτογράφηση. Οι οργανισμοί θα πρέπει να γνωρίζουν τις πιθανές επιπτώσεις της κβαντικής πληροφορικής στις κρυπτογραφικές διασφαλίσεις και να λαμβάνουν τις απαραίτητες προφυλάξεις για την ελαχιστοποίηση του κινδύνου. Θα πρέπει να απαγορεύεται η χρήση μη εξουσιοδοτημένων κρυπτογραφικών αλγορίθμων ή τρόπων λειτουργίας.

Φυσική και περιβαλλοντική ασφάλεια: Ο εκάστοτε CSP πρέπει να διασφαλίζει ότι τα δεδομένα χειρίζονται και αποθηκεύονται σε ασφαλείς χώρους, στους οποίους έχει πρόσβαση μόνο εξουσιοδοτημένο προσωπικό. Ο πάροχος θα πρέπει να καθιερώσει πολιτικές και διαδικασίες για να διασφαλίσει της ασφάλειας του εξοπλισμού που χρησιμοποιείται για την

επεξεργασία ή την αποθήκευση πληροφοριών, εφαρμόζοντας φυσικές και τεχνικές μεθόδους ασφάλειας για την αποτροπή μη εξουσιοδοτημένης πρόσβασης, κλοπής, ζημίας ή διακοπής. Επίσης, θα πρέπει να παρακολουθεί τη φυσική ασφάλεια για να εντοπίζει και να ανταποκρίνεται σε τυχόν προβλήματα, όπως κλοπή ή μη εξουσιοδοτημένη είσοδος.

Χρειάζεται να υπάρχουν μέτρα που να διασφαλίζουν ότι το περιβάλλον στο οποίο υποβάλλονται σε επεξεργασία ή αποθηκεύονται τα δεδομένα να είναι επαρκές και σταθερό, συμπεριλαμβανομένων των σωστών επιπέδων υγρασίας, θερμοκρασίας και άλλων παραγόντων. Επιπρόσθετα, να φροντίζει ότι εξασφαλίζεται σταθερή και αξιόπιστη παροχή ρεύματος για την αποφυγή διακοπών ή απώλειας δεδομένων. Οφείλουν να θεσπιστούν κατευθυντήριες γραμμές και πρακτικές για την καταστροφή του υλικού και των μέσων που περιέχουν δεδομένα, συμπεριλαμβανομένης της ασφαλούς διαγραφής ή καταστροφής των δεδομένων για την αποτροπή ανεπιθύμητης πρόσβασης ή αποκάλυψης. Θα πρέπει να εφαρμόζονται έλεγχοι πρόσβασης, ώστε να διασφαλίζεται ότι μόνο εξουσιοδοτημένα άτομα μπορούν να έχουν πρόσβαση σε προστατευόμενες περιοχές ή σε εξοπλισμό που περιέχει πληροφορίες. Τέλος, είναι σημαντικό να καθιερωθούν πρωτόκολλα για την αντιμετώπιση καταστάσεων που αφορούν τη φυσική ασφάλεια ή κρίσεις, όπως πυρκαγιές ή φυσικές καταστροφές, ώστε να αποτρέπεται η ζημία ή η απώλεια προσωπικών δεδομένων.

Διαχείριση περιστατικών: Για τον εντοπισμό, την ειδοποίηση, τη διερεύνηση και την επίλυση συμβάντων ασφαλείας που αφορούν προσωπικά δεδομένα, ο πάροχος υπηρεσιών νέφους θα πρέπει να έχει καθιερώσει πολιτικές και διαδικασίες διαχείρισης συμβάντων. Οι πολιτικές και η ανάλυση κινδύνου του οργανισμού θα πρέπει να χρησιμεύουν ως βάση για τις διαδικασίες. Ο CSP θα καλείται να συγκροτήσει μια ομάδα με σαφώς καθορισμένα καθήκοντα για τη διαχείριση περιστατικών. Ο CSP θα πρέπει να διαθέτει τεχνολογίες παρακολούθησης, καταγραφής και ανίχνευσης εισβολών για τον εντοπισμό και την αναφορά περιστατικών ασφαλείας. Όταν ανακαλύπτεται ένα περιστατικό ασφαλείας, ο πάροχος υπηρεσιών cloud θα πρέπει να κινείται γρήγορα για την αντιμετώπισή του και την ελαχιστοποίηση των επιπτώσεών του.

Ο πάροχος πρέπει να είναι σε ετοιμότητα να εντοπίσει την υποκείμενη αιτία του συμβάντος και να εφαρμόσει διορθωτικά μέτρα για να μην ξανά συμβεί. Οι πελάτες ή άλλα μέρη που έχουν επηρεαστεί από το πρόβλημα θα πρέπει να ενημερώνονται σχετικά με αυτό, τις επιπτώσεις του και τα μέτρα που λαμβάνει ο CSP για την αποκατάστασή του. Σύμφωνα με τους σχετικούς κανόνες και κανονισμούς, ο πάροχος υπηρεσιών νέφους, πρέπει επίσης να

αναφέρει τα περιστατικά στις αρμόδιες και ρυθμιστικές αρχές. Οφείλει επιπρόσθετα να δοκιμάζει και να εφαρμόζει περιοδικά τις πολιτικές και τις διαδικασίες διαχείρισης συμβάντων για να αξιολογεί την αποτελεσματικότητά τους. Το πρόγραμμα διαχείρισης συμβάντων θα πρέπει να βελτιώνεται χρησιμοποιώντας τα ευρήματα από τις δοκιμές και τις ασκήσεις.

Συμμόρφωση: Για να εξασφαλιστεί η συμμόρφωση με τις νομικές υποχρεώσεις που αφορούν την επεξεργασία δεδομένων προσωπικού χαρακτήρα, οι CSP πρέπει να διαθέτουν πολιτικές και διαδικασίες. Αυτό συνεπάγεται τη λήψη συγκατάθεσης από τα υποκείμενα των δεδομένων, την ενημέρωσή τους για τη φύση και την έκταση της επεξεργασίας και την τήρηση τυχόν περιφερειακών νόμων που ενδέχεται να ισχύουν για την επεξεργασία δεδομένων προσωπικού χαρακτήρα. Επιπλέον, οι CSP υποχρεούνται να διατηρούν αρχεία των δραστηριοτήτων επεξεργασίας και να παρέχουν στις ρυθμιστικές αρχές πρόσβαση στα έγγραφα αυτά κατόπιν αιτήματος. Οι CSP θα πρέπει να εξετάζουν τακτικά τη συμμόρφωσή τους με τα νομικά και κανονιστικά πρότυπα και να προβαίνουν στις αναγκαίες προσαρμογές για τη διατήρηση της συμμόρφωσης. Πρέπει επίσης να διασφαλίζουν ότι οι τρίτοι πάροχοι υπηρεσιών και οι υπεργολάβοι τους τηρούν όλες τις ισχύουσες νομικές και κανονιστικές υποχρεώσεις.

Τέλος θα πρέπει να είναι διαφανείς και υπόλογοι απέναντι στα υποκείμενα των δεδομένων, συμπεριλαμβανομένης της ειδοποίησής τους για τυχόν παραβιάσεις δεδομένων και της λήψης των απαραίτητων μέτρων για τη μείωση της όποιας ζημίας. Προκειμένου να διατηρήσουν τη συμμόρφωση με το πρότυπο, οι πάροχοι υπηρεσιών νέφους οφείλουν επίσης να υποβάλλονται σε συνεχείς ανεξάρτητες αξιολογήσεις και ελέγχους των διαδικασιών ασφαλείας τους. Οι εταιρείες που χρησιμοποιούν υπηρεσίες νέφους απαιτείται από το πρότυπο ISO/IEC 27018:2019 να επιδεικνύουν τη δέουσα επιμέλεια κατά την επιλογή ενός CSP, διασφαλίζοντας ότι ο πάροχος διαθέτει τα προσόντα για την τήρηση των προτύπων. Επιπλέον, προκειμένου να διασφαλιστεί η συμμόρφωση με το πρότυπο, οι επιχειρήσεις χρειάζεται να βεβαιωθούν ότι διαθέτουν τις κατάλληλες συμβάσεις και συμφωνίες με τους παρόχους υπηρεσιών cloud.

Συνολικά, το ISO/IEC 27018:2019 είναι ένα διεξοδικό πρότυπο που δίνει οδηγίες στις επιχειρήσεις και στους παρόχους υπηρεσιών νέφους σχετικά με τον τρόπο διασφάλισης των δεδομένων των πελατών στο νέφος. Τηρώντας το πρότυπο, οι επιχειρήσεις και οι πάροχοι υπηρεσιών cloud μπορούν να δείξουν την αφοσίωσή τους στην προστασία της ιδιωτικής ζωής

και την ασφάλεια των δεδομένων, κερδίζοντας την εμπιστοσύνη των ενδιαφερόμενων μερών και των πελατών τους.

1.3 Κατευθυντήριες Γραμμές και Μέτρα Ασφαλείας του NIST για την Προστασία Δεδομένων στο Υπολογιστικό Νέφος

Το Εθνικό Ινστιτούτο Προτύπων και Τεχνολογίας (NIST) του Υπουργείου Εμπορίου των Ηνωμένων Πολιτειών είναι ένας μη ρυθμιστικός φορέας. Στόχος του είναι να προάγει την επιστήμη, τα πρότυπα και την τεχνολογία για την προώθηση της καινοτομίας και της οικονομικής ανταγωνιστικότητας. Το NIST προσπαθεί να παρέχει πρότυπα και βέλτιστες πρακτικές για την εγγύηση της ασφάλειας των ευαίσθητων δεδομένων στο νέφος (Nieles. Dempsey and Pillitteri (NIST), 2017).

Η πρώτη σειρά κατευθυντήριων γραμμών του NIST για το υπολογιστικό νέφος, η οποία περιλάμβανε προτάσεις για την ασφάλεια των δεδομένων και την προστασία της ιδιωτικής ζωής, δημοσιεύθηκε το 2011. Επιπλέον, το Εθνικό Ινστιτούτο Προτύπων και Τεχνολογίας (NIST) κυκλοφόρησε την ειδική έκδοση NIST Special Publication 800-53, (NIST:800-53, 2020) "Security and Privacy Controls for Federal Information Systems and Organization’s",η οποία προσφέρει οδηγίες για την ασφάλεια των πληροφοριακών συστημάτων στην ομοσπονδιακή κυβέρνηση των Ηνωμένων Πολιτειών. (NIST:CSF 2.0, 2024).

Κανόνες Ασφαλείας και Προστασίας Ιδιωτικότητας

Οι οργανισμοί πρέπει να υιοθετούν πολιτικές που διασφαλίζουν την προστασία των πληροφοριακών τους συστημάτων. Ακολουθούν βασικοί κανόνες (NIST:800-53, 2020):

1. Έλεγχος Πρόσβασης (AC):
Οι οργανισμοί πρέπει να καθορίζουν ποιοι χρήστες έχουν πρόσβαση στους πόρους του νέφους, παρέχοντας ελάχιστα δικαιώματα που είναι απαραίτητα για κάθε ρόλο. Πρέπει επίσης να ελέγχουν τη χρήση αυτών των πόρων, να εφαρμόζουν πολιτικές ασφαλείας και να παρακολουθούν τη δραστηριότητα των χρηστών. Επιπλέον, η κατανομή καθηκόντων μειώνει τον κίνδυνο ανθρώπινων σφαλμάτων ή εσωτερικών απειλών.

2. Έλεγχος και Λογοδοσία (AE):
Η παρακολούθηση της δραστηριότητας στο περιβάλλον του νέφους διασφαλίζει ότι τα

συμβάντα ασφαλείας καταγράφονται. Οι επιχειρήσεις πρέπει να εφαρμόζουν αρχεία ελέγχου που περιλαμβάνουν χρονοσφραγίδες και να προστατεύουν αυτές τις πληροφορίες από μη εξουσιοδοτημένη πρόσβαση.

3. Ταυτοποίηση και Πιστοποίηση Ταυτότητας (IA):
Η επαλήθευση της ταυτότητας των χρηστών μέσω πολυπαραγοντικού ελέγχου ταυτότητας (MFA) είναι κρίσιμη. Πολιτικές όπως ισχυροί κωδικοί πρόσβασης, αυτόματη αποσύνδεση μετά από αδράνεια και ασφαλείς συνδέσεις συμβάλλουν στη μείωση των κινδύνων παραβίασης.

4. Αντιμετώπιση Περιστατικών (IR):
Ένα καλά σχεδιασμένο πλάνο αντιμετώπισης περιστατικών επιτρέπει την άμεση αντίδραση σε παραβιάσεις ασφαλείας. Οι οργανισμοί πρέπει να εκπαιδεύουν το προσωπικό, να παρακολουθούν δραστηριότητες και να συνεργάζονται με τις αρχές όταν χρειάζεται.

5. Προστασία Μέσων (MP):
Η πρόσβαση σε φυσικά και εικονικά μέσα με ευαίσθητες πληροφορίες πρέπει να περιορίζεται. Οι εταιρείες οφείλουν να αποθηκεύουν και να μεταφέρουν τα δεδομένα με ασφάλεια, καθώς και να καταστρέφουν μη χρησιμοποιούμενα μέσα με μεθόδους όπως η κρυπτογράφηση ή η φυσική καταστροφή.

6. Ασφάλεια Προσωπικού (PS):
Οι οργανισμοί πρέπει να πραγματοποιούν ελέγχους ιστορικού υπαλλήλων και να τους εκπαιδεύουν σε θέματα ασφάλειας. Όταν εργαζόμενοι αλλάζουν ρόλους ή αποχωρούν, η πρόσβασή τους σε δεδομένα πρέπει να ανακαλείται άμεσα.

7. Αξιολόγηση Κινδύνων (AK):
Η συνεχής αξιολόγηση κινδύνων επιτρέπει τον εντοπισμό ευπαθειών και τη βελτίωση της στρατηγικής ασφαλείας. Η χρήση εξωτερικών αξιολογήσεων, όπως δοκιμές διείσδυσης, βοηθά στην πρόληψη παραβιάσεων.

8. Αξιολόγηση Ασφάλειας και Εξουσιοδότηση (SA):
Η παρακολούθηση της απόδοσης των ελέγχων ασφαλείας εξασφαλίζει την αποτελεσματική λειτουργία τους. Οργανισμοί πρέπει να επαναξιολογούν τακτικά τις διαδικασίες και να εφαρμόζουν αλλαγές όταν απαιτείται.

9. Προστασία Συστημάτων και Επικοινωνιών (SC):
Η κρυπτογράφηση και οι ασφαλείς διαδρομές επικοινωνίας είναι απαραίτητες για την προστασία δεδομένων κατά τη μεταφορά. Οι πολιτικές ελέγχου πρόσβασης εξασφαλίζουν ότι μόνο εξουσιοδοτημένα άτομα έχουν πρόσβαση σε ευαίσθητες πληροφορίες.

10. Ακεραιότητα Συστημάτων και Πληροφοριών (SI):
Η εφαρμογή μέτρων προστασίας, όπως προγράμματα ανίχνευσης κακόβουλου λογισμικού, διασφαλίζει ότι οι υποδομές του νέφους είναι ανθεκτικές απέναντι σε απειλές και διατηρούν την ακεραιότητά τους.

Με την υιοθέτηση αυτών των μέτρων, οι οργανισμοί μπορούν να ενισχύσουν την ασφάλεια και την ιδιωτικότητα των δεδομένων στο υπολογιστικό νέφος.

Κεφάλαιο 2^{ο} - Ορισμός και Βασικά Χαρακτηριστικά της Λειτουργίας Διαχείρισης Ταυτότητας και Πρόσβασης Καθώς και Τεχνικές Αντιμετώπισης Διαφόρων Αδυναμιών και Προβλημάτων στα Εν Λόγω Συστήματα

2.1 Βασικά Στοιχεία και Χαρακτηριστικά στη Λειτουργία της Διαχείρισης Ταυτότητας και Πρόσβασης

Αποτελεί γεγονός πως τα τελευταία χρόνια, το cloud computing έχει φέρει μια σημαντική επανάσταση στον τρόπο με τον οποίο οι οργανισμοί αποθηκεύουν, επεξεργάζονται και διαχειρίζονται τα δεδομένα και τις εφαρμογές τους. Η ευελιξία, η επεκτασιμότητα και η οικονομική αποδοτικότητα του cloud, το έχουν καταστήσει δημοφιλή επιλογή για επιχειρήσεις όλων των μεγεθών. Ωστόσο, καθώς περισσότεροι οργανισμοί μεταφέρουν τις δραστηριότητές τους στο cloud, οι ανησυχίες για την ασφάλεια έχουν γίνει ένα εξέχον ζήτημα (Ghelani, 2022)

Η λειτουργία της διαχείρισης ταυτότητας και πρόσβασης (IAM) διαδραματίζει κεντρικό ρόλο στην ασφάλεια των περιβαλλόντων cloud. Η λειτουργία της διαχείρισης ταυτότητας και πρόσβασης περιλαμβάνει τον έλεγχο της πρόσβασης των χρηστών σε πόρους και δεδομένα, διασφαλίζοντας ταυτόχρονα τον έλεγχο ταυτότητας, την εξουσιοδότηση και τη σωστή διαχείριση των χρηστών. Σε παραδοσιακά περιβάλλοντα εσωτερικού χώρου, Η λειτουργία της διαχείρισης ταυτότητας και πρόσβασης, έχει καθιερωθεί και κατανοηθεί επαρκώς. Ωστόσο, το cloud computing εισάγει μοναδικές προκλήσεις που απαιτούν μια επαναξιολόγηση των πρακτικών της διαχείρισης ταυτότητας και πρόσβασης (Ghelani, Hua and Koduru, 2022)

Η λειτουργία της διαχείρισης ταυτότητας και πρόσβασης σε περιβάλλοντα cloud, έχει συγκεντρώσει μια σημαντική προσοχή στην ερευνητική κοινότητα λόγω της αυξανόμενης

υιοθέτησης του υπολογιστικού νέφους (cloud) και των σχετικών προκλήσεων ασφάλειας. Ερευνητές και επαγγελματίες έχουν εξερευνήσει διάφορες πτυχές της λειτουργίας της διαχείρισης ταυτότητας και πρόσβασης για να εντοπίσουν πιθανά τρωτά σημεία και να επινοήσουν αποτελεσματικές λύσεις (Marinescu, 2013)

Με σκοπό τα παραπάνω, αναφέρεται το άρθρο Security challenges in cloud computing: A comprehensive analysis (Ang'udi, 2023). Αυτό το αναλυτικό άρθρο ανασκόπησης, παρέχει μια επισκόπηση των προκλήσεων ασφαλείας στο cloud computing, συμπεριλαμβανομένης της λειτουργίας της διαχείρισης ταυτότητας και πρόσβασης. Η μελέτη εντοπίζει τρωτά σημεία που σχετίζονται με τη λειτουργία της διαχείρισης ταυτότητας και πρόσβασης, όπως αδύναμους μηχανισμούς ελέγχου ταυτότητας, κλιμάκωση προνομίων και εσωτερικές απειλές. Η συγγραφής τονίζει τη σημασία των ισχυρών στρατηγικών IAM και προτείνουν την ενσωμάτωση ελέγχου ταυτότητας πολλαπλών παραγόντων και ελέγχων πρόσβασης που βασίζονται σε ρόλους για τον μετριασμό των κινδύνων.

Το άρθρο με τίτλο *A Survey on Identity and Access Management in Cloud Computing*, (Nida, et al., 2014)παρουσιάζει μια εις βάθος ανάλυση των πρακτικών λειτουργίας της διαχείρισης ταυτότητας και πρόσβασης στο cloud computing. Η μελέτη διερευνά διάφορα μοντέλα της λειτουργίας της διαχείρισης ταυτότητας και πρόσβασης, όπως τον έλεγχο πρόσβασης βάσει χαρακτηριστικών (ABAC) και τον έλεγχο πρόσβασης βάσει ρόλου (RBAC), και αξιολογεί την αποτελεσματικότητά τους σε περιβάλλοντα cloud. Οι συγγραφείς υπογραμμίζουν την ανάγκη για λεπτομερείς ελέγχους πρόσβασης και δυναμικές πολιτικές εξουσιοδότησης για τη βελτίωση της λειτουργίας της διαχείρισης ταυτότητας και πρόσβασης στο cloud.

Στο άρθρο με τίτλο *An Analysis of the Cloud Computing Security Problem* (Almorsy, Grundy and Müller, 2016), εξετάζονται τα ζητήματα ασφάλειας και τις προκλήσεις που αντιμετωπίζονται στο cloud computing, με ιδιαίτερη έμφαση στη λειτουργία της διαχείρισης ταυτότητας και πρόσβασης. Η μελέτη συζητά τον αντίκτυπο της κλοπής ταυτότητας, των αδύναμων κωδικών πρόσβασης και της κατάχρησης προνομίων στην ασφάλεια του cloud. Οι συγγραφείς προτείνουν τη χρήση βιομετρικού ελέγχου ταυτότητας και ανάλυσης συμπεριφοράς για την ενίσχυση της λειτουργίας της διαχείρισης ταυτότητας και πρόσβασης και την καταπολέμηση των απειλών που σχετίζονται με την ταυτότητα.

Διερευνά επίσης τις πρακτικές διαχείρισης ταυτότητας στο cloud computing. Η μελέτη κατηγοριοποιεί τα στοιχεία στη λειτουργία της διαχείρισης ταυτότητας και πρόσβασης σε παροχή ταυτότητας, έλεγχο ταυτότητας και έλεγχο πρόσβασης. Οι συγγραφείς υπογραμμίζουν τη σημασία της ομοσπονδίας ταυτότητας και των μηχανισμών single sign-on (SSO) για την απλοποίηση του IAM και τη βελτίωση της εμπειρίας χρήστη σε περιβάλλοντα πολλαπλών νέφους.

Το άρθρο *Cloud Identity and Access Management – A Model Proposal* (Azhar, 2019) παρέχει μια επισκόπηση των λύσεων cloud ως προς τη λειτουργία της διαχείρισης ταυτότητας και πρόσβασης που προσφέρονται από διάφορους παρόχους υπηρεσιών cloud. Η μελέτη αναλύει διαφορετικά εργαλεία και υπηρεσίες IAM, όπως το AWS IAM και το Azure Active Directory, και συγκρίνει τα χαρακτηριστικά και τις δυνατότητές τους. Ο συγγραφέας συζητά τις προκλήσεις της ενσωμάτωσης πολλαπλών λύσεων IAM σε ένα υβριδικό περιβάλλον cloud και προτείνουν κατευθύνσεις έρευνας για μελλοντικές εξελίξεις στη λειτουργία της διαχείρισης ταυτότητας και πρόσβασης.

Το άρθρο *Cloud identity management security issues & solutions: a taxonomy* (Habiba, et al., 2014) ανασκόπησης παρουσιάζει την τελευταία λέξη της τεχνολογίας στη διαχείριση ταυτότητας cloud. Η μελέτη διερευνά την εξέλιξη των προτύπων και πρωτοκόλλων IAM, όπως η Γλώσσα σήμανσης διαβεβαίωσης ασφαλείας (SAML) και το OpenID Connect. Οι συγγραφείς συζητούν τις προκλήσεις διά λειτουργικότητας και τονίζουν την ανάγκη για τυποποιημένες λύσεις στη λειτουργία της διαχείρισης ταυτότητας και πρόσβασης για την εξασφάλιση απρόσκοπτης ενσωμάτωσης σε διαφορετικές πλατφόρμες cloud.

Τέλος, το άρθρο, Identity and Access Management in Cloud Environments: Security Challenges and Solutions (Moneer, 2013) αυτή η έρευνα παρέχει πληροφορίες για τις εφαρμογές στη λειτουργία της διαχείρισης ταυτότητας και πρόσβασης, τις προκλήσεις και τις λύσεις στο cloud computing. Η μελέτη υπογραμμίζει τη σημασία στη λειτουργία της διαχείρισης ταυτότητας και πρόσβασης για την ασφάλεια δεδομένων και πόρων, ειδικά σε περιβάλλοντα με πολλά νέφη και σε ομοσπονδιακά περιβάλλοντα cloud. Συζητούνται οι πιθανοί κίνδυνοι των εσφαλμένων διαμορφώσεων ως προς τη λειτουργία της διαχείρισης ταυτότητας και πρόσβασης και προτείνονται βέλτιστες πρακτικές για την εφαρμογή και τη διαχείριση στη λειτουργία της διαχείρισης ταυτότητας και πρόσβασης.

Ως συμπέρασμα στα παραπάνω, η σχετική ενότητα υπογραμμίζει το αυξανόμενο ενδιαφέρον για τη λειτουργία της διαχείρισης ταυτότητας και πρόσβασης σε περιβάλλοντα cloud. Οι ερευνητές έχουν εξερευνήσει διάφορα μοντέλα σχετικά, μηχανισμούς ελέγχου ταυτότητας, στρατηγικές ελέγχου πρόσβασης και την ενοποίηση των εργαλείων που προσφέρονται από παρόχους υπηρεσιών cloud. Τα κοινά θέματα στη βιβλιογραφία περιλαμβάνουν τη σημασία των ελέγχων πρόσβασης που βασίζονται σε ρόλους, του ελέγχου ταυτότητας πολλαπλών παραγόντων και της συνεχούς παρακολούθησης για βελτιωμένη ασφάλεια (Marinescu, 2013)

2.2 Ορισμός της Λειτουργίας της Διαχείρισης Ταυτότητας και Πρόσβασης σε Περιβάλλον Cloud

Η λειτουργία της διαχείρισης ταυτότητας και πρόσβασης στο περιβάλλον cloud computing, συνεχίζει να εξελίσσεται μέσα το μεταβαλλόμενο τοπίο του cloud και η συνεχιζόμενη έρευνα επιδιώκει να αντιμετωπίσει τις αναδυόμενες προκλήσεις ασφάλειας και να εντοπίσει νέες λύσεις (Ghelani, 2022)

Οι αναθεωρημένες μελέτες υπογραμμίζουν συλλογικά την ανάγκη για τους οργανισμούς να υιοθετήσουν ισχυρές στρατηγικές λειτουργίας της διαχείρισης ταυτότητας και πρόσβασης προσαρμοσμένες σε περιβάλλοντα cloud για να διασφαλίσουν την εμπιστευτικότητα, την ακεραιότητα και τη διαθεσιμότητα πόρων και δεδομένων cloud. Ωστόσο, οι βασικές αρχές διαχείρισης ταυτότητας και πρόσβασης, αναλύονται σχετικά ως εξής (Ghelani, Hua and Koduru, 2022)

Έννοιες και συνιστώσες - Η Διαχείριση Ταυτότητας και Πρόσβασης (IAM) είναι ένας σημαντικός κλάδος που διασφαλίζει την κατάλληλη πρόσβαση σε πόρους και δεδομένα εντός του υπολογιστικού περιβάλλοντος ενός οργανισμού. Η λειτουργία της διαχείρισης ταυτότητας και πρόσβασης προσαρμοσμένες σε περιβάλλοντα cloud, περιλαμβάνει ένα σύνολο αρχών, εννοιών και στοιχείων που διέπουν συλλογικά τις ταυτότητες των χρηστών, τον έλεγχο ταυτότητας, την εξουσιοδότηση και τη διαχείριση χρηστών. Στο πλαίσιο των περιβαλλόντων cloud, η λειτουργία της διαχείρισης ταυτότητας και πρόσβασης προσαρμοσμένες σε περιβάλλοντα cloud, γίνεται ακόμη πιο κρίσιμο καθώς ασχολείται με δυναμικούς και κατανεμημένους πόρους. Αυτή η ενότητα διερευνά τις βασικές έννοιες και στοιχεία του IAM σε περιβάλλοντα cloud.

Έλεγχος ταυτότητας: Ο έλεγχος ταυτότητας είναι η διαδικασία επαλήθευσης της ταυτότητας χρηστών, συσκευών ή εφαρμογών που προσπαθούν να αποκτήσουν πρόσβαση σε πόρους ή υπηρεσίες. Περιλαμβάνει την επικύρωση των διαπιστευτηρίων που παρέχονται από τους χρήστες, όπως ονόματα χρήστη και κωδικούς πρόσβασης, βιομετρικά στοιχεία, διακριτικά ή πιστοποιητικά. Τα περιβάλλοντα cloud μπορεί να χρησιμοποιούν διάφορους μηχανισμούς ελέγχου ταυτότητας, συμπεριλαμβανομένου του Single Sign-On (SSO), του ελέγχου ταυτότητας πολλαπλών παραγόντων (MFA) και της ομοσπονδιακής ταυτότητας.

Εξουσιοδότηση: Η εξουσιοδότηση καθορίζει ποιες ενέργειες ή λειτουργίες επιτρέπεται να εκτελούν οι πιστοποιημένοι χρήστες σε συγκεκριμένους πόρους. Περιλαμβάνει τον καθορισμό πολιτικών ελέγχου πρόσβασης, όπως δικαιώματα ανάγνωσης, εγγραφής, εκτέλεσης ή διαγραφής. Το Role-Based Access Control (RBAC) και το Attribute-Based Access Control (ABAC) είναι κοινά μοντέλα εξουσιοδότησης που χρησιμοποιούνται σε περιβάλλοντα cloud για τη διαχείριση των λεπτομερών αδειών πρόσβασης.

Διαχείριση χρηστών: Η διαχείριση χρηστών περιλαμβάνει τη δημιουργία, τροποποίηση και διαγραφή λογαριασμών χρηστών και σχετικών χαρακτηριστικών. Σε περιβάλλοντα cloud, η διαχείριση χρηστών επεκτείνεται στη διαχείριση όχι μόνο ανθρώπινων χρηστών αλλά και λογαριασμών υπηρεσιών, συσκευών και ταυτοτήτων εφαρμογών. Οι οργανισμοί πρέπει να εφαρμόζουν ισχυρές πρακτικές διαχείρισης του κύκλου ζωής των χρηστών, συμπεριλαμβανομένων των ελέγχων ενσωμάτωσης, αποβίβασης και περιοδικών αναθεωρήσεων πρόσβασης.

Στοιχεία ταυτότητας: Η ομοσπονδία ταυτότητας επιτρέπει στους χρήστες να έχουν πρόσβαση σε πόρους σε διαφορετικούς τομείς ή παρόχους υπηρεσιών cloud χρησιμοποιώντας την υπάρχουσα ταυτότητά τους. Επιτρέπει απρόσκοπτες εμπειρίες Single Sign-On (SSO), όπου οι χρήστες μπορούν να συνδεθούν μία φορά και να έχουν πρόσβαση σε πολλές υπηρεσίες χωρίς εκ νέου έλεγχο ταυτότητας. Τα ενοποιημένα πρότυπα ταυτότητας, όπως η Γλώσσα σήμανσης διαβεβαίωσης ασφαλείας (SAML) και το OpenID Connect διευκολύνουν την ασφαλή συνένωση ταυτότητας.

Λειτουργία Privileged Access Management (PAM): Η λειτουργία Privileged Access Management ασχολείται με τη διαχείριση και την ασφάλεια προνομιακών λογαριασμών, που συχνά σχετίζονται με διαχειριστές ή πρόσβαση σε επίπεδο συστήματος. Σε περιβάλλοντα cloud, το αποτελεσματικό PAM είναι απαραίτητο για την αποτροπή κατάχρησης προνομίων

και μη εξουσιοδοτημένης πρόσβασης σε κρίσιμους πόρους. Η εφαρμογή της άμεσης πρόσβασης και η εγγραφή συνεδρίας είναι κοινές στρατηγικές PAM.

Διαχείριση κύκλου ζωής ταυτότητας: Η διαχείριση κύκλου ζωής ταυτότητας, περιλαμβάνει ολόκληρο τον κύκλο ζωής των ταυτοτήτων χρηστών, από τη δημιουργία τους έως την κατάργηση της παροχής. Περιλαμβάνει τη διαχείριση χαρακτηριστικών χρηστών, την εκχώρηση ρόλων και δικαιωμάτων και τη διασφάλιση ότι οι χρήστες έχουν πρόσβαση μόνο στους πόρους που χρειάζονται. Στο cloud, η αυτοματοποιημένη διαχείριση κύκλου ζωής ταυτότητας είναι ζωτικής σημασίας για τον χειρισμό της δυναμικής φύσης των πόρων του cloud.

Λειτουργία Single Sign-On (SSO): Η λειτουργία Single Sign-On επιτρέπει στους χρήστες να συνδεθούν μία φορά και να αποκτήσουν πρόσβαση σε πολλές εφαρμογές και υπηρεσίες χωρίς την ανάγκη επαναλαμβανόμενου ελέγχου ταυτότητας. Η λειτουργία SSO βελτιώνει την εμπειρία χρήστη, μειώνει την κόπωση του κωδικού πρόσβασης και απλοποιεί τη διαχείριση ελέγχου πρόσβασης. Οι λύσεις SSO που βασίζονται στο cloud ενσωματώνονται με πολλαπλές εφαρμογές cloud μέσω της ομοσπονδίας ταυτότητας.

Έλεγχος ταυτότητας πολλαπλών παραγόντων (MFA): Ο έλεγχος ταυτότητας πολλαπλών παραγόντων, προσθέτει ένα επιπλέον επίπεδο ασφάλειας απαιτώντας από τους χρήστες να παρέχουν πολλαπλές μορφές ταυτοποίησης κατά τη σύνδεση. Η λειτουργία MFA συνήθως συνδυάζει κάτι που γνωρίζει ο χρήστης (κωδικός πρόσβασης), κάτι που έχει ο χρήστης (smartphone ή διακριτικό υλικού) και κάτι που είναι ο χρήστης (βιομετρικός έλεγχος ταυτότητας). Η λειτουργία MFA είναι ένας αποτελεσματικός μηχανισμός για τον μετριασμό των επιθέσεων που βασίζονται σε διαπιστευτήρια.

Οι έννοιες και τα στοιχεία της λειτουργίας της διαχείρισης ταυτότητας και πρόσβασης προσαρμοσμένες σε περιβάλλοντα cloud διαδραματίζουν κρίσιμο ρόλο στην ασφάλεια των περιβαλλόντων cloud διασφαλίζοντας ότι οι σωστοί χρήστες έχουν την κατάλληλη πρόσβαση σε πόρους και δεδομένα. Η αποτελεσματική εφαρμογή μπορεί να μειώσει σημαντικά τον κίνδυνο μη εξουσιοδοτημένης πρόσβασης, παραβιάσεων δεδομένων και εσωτερικών απειλών, ενισχύοντας τελικά τη συνολική θέση ασφαλείας των συστημάτων που βασίζονται στο cloud (Comer, 2021)

2.3 Η Αρχή Ελάχιστων Προνομίων στη Λειτουργίας της Διαχείρισης Ταυτότητας και Πρόσβασης Προσαρμοσμένες σε Περιβάλλοντα cloud

Η αρχή του ελάχιστου προνομίου είναι μια θεμελιώδης έννοια ασφάλειας στο πλαίσιο της Διαχείρισης Ταυτότητας και Πρόσβασης (IAM) που υποστηρίζει την παραχώρηση στους χρήστες του ελάχιστου επιπέδου πρόσβασης που απαιτείται για την συγκεκριμένες επαγγελματικές ευθύνες ή καθήκοντα. Με άλλα λόγια, στους χρήστες θα πρέπει να παραχωρούνται μόνο τα απαραίτητα προνόμια και άδειες για την εκτέλεση της εργασίας τους και όχι περισσότερα. Αυτή η αρχή είναι ο ακρογωνιαίος λίθος των πρακτικών ασφαλούς ελέγχου πρόσβασης και συμβάλλει στον περιορισμό της πιθανής ζημίας που θα μπορούσε να προκληθεί από παραβιασμένους λογαριασμούς ή εσωτερικές απειλές (Ghelani, Hua and Koduru, 2022)

Η αρχή του ελάχιστου προνομίου είναι ιδιαίτερα σημαντική σε περιβάλλοντα cloud, όπου οι πόροι παρέχονται δυναμικά και οι χρήστες ενδέχεται να έχουν πρόσβαση σε διάφορες υπηρεσίες cloud, εφαρμογές και δεδομένα. Με την τήρηση αυτής της αρχής, οι οργανισμοί μπορούν να μετριάσουν τον κίνδυνο μη εξουσιοδοτημένης πρόσβασης, παραβιάσεις δεδομένων και πιθανή κατάχρηση προνομίων. Οι βασικές πτυχές της αρχής του ελάχιστου προνομίου σε περιβάλλοντα cloud, περιλαμβάνουν (Ghelani, 2022):

Λεπτομερής έλεγχος πρόσβασης: Το περιβάλλον Cloud της λειτουργίας της διαχείρισης ταυτότητας και πρόσβασης προσαρμοσμένες σε περιβάλλοντα cloud θα πρέπει να έχει σχεδιαστεί για να παρέχει λεπτομερή στοιχεία ελέγχου πρόσβασης, επιτρέποντας στους διαχειριστές να καθορίζουν ακριβή δικαιώματα για κάθε χρήστη ή ρόλο. Αυτό αποτρέπει τους υπερ προνομιούχους χρήστες από την πρόσβαση σε ευαίσθητα δεδομένα ή την εκτέλεση ενεργειών πέρα από τις απαιτούμενες ευθύνες τους.

Τακτικές αναθεωρήσεις πρόσβασης: Οι οργανισμοί θα πρέπει να διενεργούν τακτικές επιθεωρήσεις πρόσβασης για να διασφαλίζουν ότι τα προνόμια των χρηστών είναι ενημερωμένα και ευθυγραμμισμένα με τους τρέχοντες ρόλους εργασίας τους. Αυτό το στοιχείο περιλαμβάνει τον έλεγχο και την επικύρωση των δικαιωμάτων πρόσβασης των χρηστών για τη διατήρηση της αρχής του ελάχιστου προνομίου.

Έλεγχος πρόσβασης βάσει ρόλων (RBAC): Η εφαρμογή του RBAC απλοποιεί τη διαχείριση πρόσβασης ομαδοποιώντας τους χρήστες με βάση τις λειτουργίες εργασίας τους και

εκχωρώντας κατάλληλα δικαιώματα σε ρόλους. Στη συνέχεια, οι χρήστες ανατίθενται σε συγκεκριμένους ρόλους, μειώνοντας τον κίνδυνο παραχώρησης υπερβολικών προνομίων σε μεμονωμένους λογαριασμούς.

Πρόσβαση Just-in-Time (JIT): Η πρόσβαση JIT περιλαμβάνει την παροχή προσωρινής πρόσβασης σε πόρους ανάλογα με τις ανάγκες. Οι χρήστες λαμβάνουν αυξημένα δικαιώματα μόνο όταν απαιτείται για περιορισμένο χρονικό διάστημα. Αφού ολοκληρωθεί η εργασία, η πρόσβαση ανακαλείται αυτόματα, μειώνοντας την επιφάνεια επίθεσης και το παράθυρο έκθεσης.

Προνομιακή διαχείριση πρόσβασης (PAM): Για προνομιούχους χρήστες που απαιτούν αυξημένη πρόσβαση σε κρίσιμους πόρους, οι λύσεις PAM συμβάλλουν στην επιβολή της αρχής των ελάχιστων προνομίων ελέγχοντας και παρακολουθώντας αυστηρά τις δραστηριότητες των προνομιακών λογαριασμών.

Παρακολούθηση και Έλεγχος: Η συνεχής παρακολούθηση και έλεγχος των δραστηριοτήτων των χρηστών είναι ουσιαστικής σημασίας για τον εντοπισμό τυχόν αποκλίσεων από τη συνήθη συμπεριφορά και τον εντοπισμό πιθανής κατάχρησης προνομίων. Τα περιβάλλοντα cloud θα πρέπει να διαθέτουν ισχυρούς μηχανισμούς καταγραφής και ελέγχου για την παρακολούθηση των ενεργειών των χρηστών.

Η τήρηση της Αρχής των Ελάχιστων Προνομίων, ενδέχεται να απαιτεί προσεκτικό σχεδιασμό και συντονισμό μεταξύ των διαχειριστών IT, των ομάδων ασφαλείας και των επιχειρηματικών συμμετοχών. Αν και μπορεί να φαίνεται περιοριστικό στην αρχή, ενισχύει σημαντικά τη στάση ασφαλείας των περιβαλλόντων cloud και μειώνει την επιφάνεια επίθεσης, προστατεύοντας έτσι ευαίσθητα δεδομένα, εφαρμογές και υποδομές από μη εξουσιοδοτημένη πρόσβαση και πιθανή εκμετάλλευση. Παραχωρώντας μόνο τα απαραίτητα προνόμια στους χρήστες, οι οργανισμοί μπορούν να επιτύχουν μια ισορροπία μεταξύ παραγωγικότητας και ασφάλειας στις λειτουργίες τους στο cloud computing (Marinescu, 2013)

Οι αδύναμοι μηχανισμοί ελέγχου ταυτότητας αποτελούν σημαντική πρόκληση ασφαλείας στη Διαχείριση Ταυτότητας και Πρόσβασης (IAM) για περιβάλλοντα cloud. Ο έλεγχος ταυτότητας είναι η διαδικασία επαλήθευσης της ταυτότητας χρηστών ή οντοτήτων που προσπαθούν να αποκτήσουν πρόσβαση σε πόρους cloud και οι αδύναμοι μηχανισμοί

ελέγχου ταυτότητας μπορούν να οδηγήσουν σε μη εξουσιοδοτημένη πρόσβαση, κλοπή ταυτότητας και πιθανές παραβιάσεις δεδομένων. Τα περιβάλλοντα cloud, με τη διαφορετική βάση χρηστών και τους κατανεμημένους πόρους τους, είναι ιδιαίτερα ευάλωτα σε επιθέσεις εάν δεν υπάρχουν ισχυρά μέτρα ελέγχου ταυτότητας.

Έλεγχος ταυτότητας βάσει κωδικού πρόσβασης: Η χρήση αδύναμων κωδικών πρόσβασης είναι ένα κοινό πρόβλημα στο cloud IAM. Οι χρήστες ενδέχεται να επιλέγουν απλούς και εύκολα προβλέψιμους κωδικούς πρόσβασης, να επαναχρησιμοποιούν κωδικούς πρόσβασης σε πολλές υπηρεσίες ή να μην ενημερώνουν τακτικά τους κωδικούς πρόσβασης, καθιστώντας τους λογαριασμούς τους ευάλωτους σε επιθέσεις ωμής βίας και γέμιση διαπιστευτηρίων.

Έλεγχος ταυτότητας ενός παράγοντα (SFA): Το να βασίζεται κανείς αποκλειστικά σε έναν μόνο παράγοντα ελέγχου ταυτότητας, συνήθως έναν κωδικό πρόσβασης, είναι επικίνδυνο. Σε περίπτωση που παραβιαστούν οι κωδικοί πρόσβασης, ένας εισβολέας μπορεί να αποκτήσει μη εξουσιοδοτημένη πρόσβαση χωρίς καμία πρόσθετη επαλήθευση.

Απουσία ελέγχου ταυτότητας πολλαπλών παραγόντων (MFA): Η Λειτουργία MFA προσθέτει ένα επιπλέον επίπεδο ασφάλειας απαιτώντας από τους χρήστες να παρέχουν πολλαπλές μορφές ταυτοποίησης κατά τη σύνδεση. Η έλλειψη MFA αυξάνει την πιθανότητα μη εξουσιοδοτημένης πρόσβασης, ειδικά όταν οι κωδικοί πρόσβασης κλαπούν ή παραβιάζονται.

Μη ασφαλή πρωτόκολλα ελέγχου ταυτότητας: Η χρήση παλαιών ή μη ασφαλών πρωτοκόλλων ελέγχου ταυτότητας, όπως ο Βασικός έλεγχος ταυτότητας HTTP, μπορεί να εκθέσει τα διαπιστευτήρια σε υποκλοπή και υποκλοπή, οδηγώντας σε πιθανές παραβιάσεις της ασφάλειας.

Επιθέσεις ηλεκτρονικού ψαρέματος και κοινωνικής μηχανικής: Οι χρήστες του cloud μπορεί να υποπέσουν θύματα επιθέσεων ηλεκτρονικού *ψαρέματος* ή κοινωνικής μηχανικής, όπου οι εισβολείς εξαπατούν τους χρήστες να αποκαλύψουν τα διαπιστευτήρια σύνδεσής τους, παρακάμπτοντας εντελώς τον έλεγχο ταυτότητας.

Ωστόσο, ως προς την αντιμετώπιση αδύναμων μηχανισμών ελέγχου ταυτότητας, αναφέρονται σχετικά τα εξής στοιχεία (Mather, Kumaraswamy and Latif, 2009). Οι προκλήσεις ασφαλείας που δημιουργούνται από τους αδύναμους μηχανισμούς ελέγχου

ταυτότητας στο cloud IAM, οι οργανισμοί μπορούν να εφαρμόσουν τις ακόλουθες στρατηγικές:

Ισχυρές πολιτικές κωδικών πρόσβασης: Επιβολή ισχυρών πολιτικών κωδικών πρόσβασης που απαιτούν από τους χρήστες να δημιουργούν σύνθετους και μοναδικούς κωδικούς πρόσβασης. Ενθαρρύνετε τη χρήση διαχειριστών κωδικών πρόσβασης για την ασφαλή αποθήκευση και διαχείριση κωδικών πρόσβασης.

Έλεγχος ταυτότητας πολλαπλών παραγόντων (MFA): Εφαρμογή MFA για όλους τους λογαριασμούς χρηστών, ειδικά για όσους έχουν πρόσβαση σε ευαίσθητα δεδομένα ή δυνατότητες διαχείρισης. Το MFA προσθέτει ένα επιπλέον επίπεδο ασφάλειας, καθιστώντας πιο δύσκολο για τους εισβολείς να παραβιάσουν λογαριασμούς.

Βιομετρικός έλεγχος ταυτότητας: Εξετάζεται το ενδεχόμενο εφαρμογής βιομετρικού ελέγχου ταυτότητας, όπως η αναγνώριση δακτυλικών αποτυπωμάτων ή προσώπου, ως μια ασφαλής και βολική μέθοδος ελέγχου ταυτότητας για τους χρήστες cloud.

Υιοθέτηση σε ασφαλή πρωτόκολλα ελέγχου ταυτότητας: Χρησιμοποιείται ασφαλή πρωτόκολλα ελέγχου ταυτότητας, όπως το OAuth ή το OpenID Connect, για την προστασία των διαπιστευτηρίων χρήστη κατά τη διαδικασία ελέγχου ταυτότητας. Αποφύγετε τη χρήση μη ασφαλών πρωτοκόλλων όπως ο βασικός έλεγχος ταυτότητας HTTP.

Εκπαίδευση χρηστών: Εκπαιδεύονται οι χρήστες του cloud σχετικά με τους κινδύνους αδύναμου ελέγχου ταυτότητας και τη σημασία της δημιουργίας ισχυρών κωδικών πρόσβασης και της αναγνώρισης απόπειρες phishing.

Παρακολούθηση ελέγχου ταυτότητας: Εφαρμόζεται συνεχή παρακολούθηση συμβάντων ελέγχου ταυτότητας για τον εντοπισμό ύποπτων προσπαθειών σύνδεσης ή μοτίβων που μπορεί να υποδεικνύουν επιθέσεις ωμής βίας ή παραβιασμούς λογαριασμού.

Adaptive Authentication: Αναπτύσσονται προσαρμοστικές λύσεις ελέγχου ταυτότητας που αναλύουν τη συμπεριφορά των χρηστών και εφαρμόζουν πρόσθετες προκλήσεις ελέγχου ταυτότητας εάν εντοπιστούν μη φυσιολογικές δραστηριότητες.

Με την εφαρμογή ισχυρών μηχανισμών ελέγχου ταυτότητας και την προώθηση βέλτιστων πρακτικών ασφάλειας, οι οργανισμοί μπορούν να ενισχύσουν τη συνολική

ασφάλεια του cloud της διαχείρισης ταυτότητας και πρόσβασης προσαρμοσμένες σε περιβάλλοντα cloud τους και να μετριάσουν τον κίνδυνο μη εξουσιοδοτημένης πρόσβασης και παραβιάσεων δεδομένων. Μια πολύ επίπεδη προσέγγιση που συνδυάζει ισχυρές τεχνολογίες ελέγχου ταυτότητας, εκπαίδευση των χρηστών και συνεχή παρακολούθηση είναι απαραίτητη για τη διαφύλαξη των πόρων cloud και τη διασφάλιση ενός ασφαλούς περιβάλλοντος υπολογιστικού νέφους.

2.4 Αδύναμοι Μηχανισμοί Αυθεντικοποίησης της Λειτουργίας της Διαχείρισης Ταυτότητας και Πρόσβασης Προσαρμοσμένα σε Περιβάλλοντα cloud

Οι αδύναμοι μηχανισμοί ελέγχου ταυτότητας αποτελούν σημαντική πρόκληση ασφαλείας στη Διαχείριση Ταυτότητας και Πρόσβασης (IAM) για περιβάλλοντα cloud. Ο έλεγχος ταυτότητας είναι η διαδικασία επαλήθευσης της ταυτότητας χρηστών ή οντοτήτων που προσπαθούν να αποκτήσουν πρόσβαση σε πόρους cloud και οι αδύναμοι μηχανισμοί ελέγχου ταυτότητας μπορεί να οδηγήσουν σε μη εξουσιοδοτημένη πρόσβαση, κλοπή ταυτότητας και πιθανές παραβιάσεις δεδομένων. Τα περιβάλλοντα cloud, με τη διαφορετική βάση χρηστών και τους κατανεμημένους πόρους τους, είναι ιδιαίτερα ευάλωτα σε επιθέσεις εάν δεν υπάρχουν ισχυρά μέτρα ελέγχου ταυτότητας.

Έλεγχος ταυτότητας βάσει κωδικού πρόσβασης: Η χρήση αδύναμων κωδικών πρόσβασης είναι ένα κοινό πρόβλημα στο cloud λειτουργίας της διαχείρισης ταυτότητας και πρόσβασης προσαρμοσμένες σε περιβάλλοντα cloud. Οι χρήστες ενδέχεται να επιλέγουν απλούς και εύκολα προβλέψιμους κωδικούς πρόσβασης, να επαναχρησιμοποιούν κωδικούς πρόσβασης σε πολλές υπηρεσίες ή να μην ενημερώνουν τακτικά τους κωδικούς πρόσβασης, καθιστώντας τους λογαριασμούς τους ευάλωτους σε επιθέσεις ωμής βίας και γέμιση διαπιστευτηρίων.

Έλεγχος ταυτότητας ενός παράγοντα (SFA): Το να βασίζεται κανείς αποκλειστικά σε έναν μόνο παράγοντα ελέγχου ταυτότητας, συνήθως έναν κωδικό πρόσβασης, είναι επικίνδυνο. Σε περίπτωση που παραβιαστούν οι κωδικοί πρόσβασης, ένας εισβολέας μπορεί να αποκτήσει μη εξουσιοδοτημένη πρόσβαση χωρίς καμία πρόσθετη επαλήθευση.

Απουσία ελέγχου ταυτότητας πολλαπλών παραγόντων (MFA): Η Λειτουργία MFA προσθέτει ένα επιπλέον επίπεδο ασφάλειας απαιτώντας από τους χρήστες να παρέχουν πολλαπλές μορφές ταυτοποίησης κατά τη σύνδεση. Η έλλειψη MFA αυξάνει την πιθανότητα

μη εξουσιοδοτημένης πρόσβασης, ειδικά όταν οι κωδικοί πρόσβασης κλαπούν ή παραβιάζονται.

Μη ασφαλή πρωτόκολλα ελέγχου ταυτότητας: Η χρήση παλαιών ή μη ασφαλών πρωτοκόλλων ελέγχου ταυτότητας, όπως ο Βασικός έλεγχος ταυτότητας HTTP, μπορεί να εκθέσει τα διαπιστευτήρια σε υποκλοπή και υποκλοπή, οδηγώντας σε πιθανές παραβιάσεις της ασφάλειας.

Επιθέσεις ηλεκτρονικού ψαρέματος και κοινωνικής μηχανικής: Οι χρήστες του cloud μπορεί να πέσουν θύματα επιθέσεων ηλεκτρονικού ψαρέματος ή κοινωνικής μηχανικής, όπου οι εισβολείς εξαπατούν τους χρήστες να αποκαλύψουν τα διαπιστευτήρια σύνδεσής τους, παρακάμπτοντας εντελώς τον έλεγχο ταυτότητας.

2.5 Αντιμετώπιση Αδύναμων Μηχανισμών Ελέγχου Ταυτότητας

Για την αντιμετώπιση των προκλήσεων ασφαλείας που δημιουργούνται από τους αδύναμους μηχανισμούς ελέγχου ταυτότητας στο cloud IAM, οι οργανισμοί μπορούν να εφαρμόσουν τις ακόλουθες στρατηγικές (Ghelani, 2022):

Ισχυρές πολιτικές κωδικών πρόσβασης: Επιβολή ισχυρών πολιτικών κωδικών πρόσβασης που απαιτούν από τους χρήστες να δημιουργούν σύνθετους και μοναδικούς κωδικούς πρόσβασης. Ενθαρρύνεται η χρήση διαχειριστών κωδικών πρόσβασης για την ασφαλή αποθήκευση και διαχείριση κωδικών πρόσβασης.

Έλεγχος ταυτότητας πολλαπλών παραγόντων (MFA): Εφαρμογή MFA για όλους τους λογαριασμούς χρηστών, ειδικά για όσους έχουν πρόσβαση σε ευαίσθητα δεδομένα ή δυνατότητες διαχείρισης. Το MFA προσθέτει ένα επιπλέον επίπεδο ασφάλειας, καθιστώντας πιο δύσκολο για τους εισβολείς να παραβιάσουν λογαριασμούς.

Βιομετρικός έλεγχος ταυτότητας: Εξετάζεται το ενδεχόμενο εφαρμογής βιομετρικού ελέγχου ταυτότητας, όπως η αναγνώριση δακτυλικών αποτυπωμάτων ή προσώπου, ως μια ασφαλής και βολική μέθοδος ελέγχου ταυτότητας για τους χρήστες cloud.

Υιοθέτηση σε ασφαλή πρωτόκολλα ελέγχου ταυτότητας: Χρησιμοποιούνται ασφαλή πρωτόκολλα ελέγχου ταυτότητας, όπως το OAuth ή το OpenID Connect, για την προστασία των διαπιστευτηρίων χρήστη κατά τη διαδικασία ελέγχου ταυτότητας.

Εκπαίδευση χρηστών: Εκπαιδεύονται οι χρήστες του cloud σχετικά με τους κινδύνους του αδύναμου ελέγχου ταυτότητας και της σημασίας της δημιουργίας ισχυρών κωδικών πρόσβασης και της αναγνώρισης προσπαθειών phishing. Διεξάγεται μια τακτική εκπαίδευση ευαισθητοποίησης σχετικά με την ασφάλεια.

Παρακολούθηση ελέγχου ταυτότητας: Εφαρμόζεται η συνεχή παρακολούθηση συμβάντων ελέγχου ταυτότητας για τον εντοπισμό ύποπτων προσπαθειών σύνδεσης ή μοτίβων που μπορεί να υποδεικνύουν επιθέσεις ωμής βίας ή παραβιασμούς λογαριασμού.

Adaptive Authentication: Αναπτύσσονται προσαρμοστικές λύσεις ελέγχου ταυτότητας που αναλύουν τη συμπεριφορά των χρηστών και εφαρμόζουν πρόσθετες προκλήσεις ελέγχου ταυτότητας εάν εντοπιστούν μη φυσιολογικές δραστηριότητες.

Με την εφαρμογή ισχυρών μηχανισμών ελέγχου ταυτότητας και την προώθηση βέλτιστων πρακτικών ασφάλειας, οι οργανισμοί μπορούν να ενισχύσουν τη συνολική ασφάλεια του cloud της λειτουργίας της διαχείρισης ταυτότητας και πρόσβασης και να μετριάσουν τον κίνδυνο μη εξουσιοδοτημένης πρόσβασης και παραβιάσεων δεδομένων. Μια πολύ επίπεδη προσέγγιση που συνδυάζει ισχυρές τεχνολογίες ελέγχου ταυτότητας, εκπαίδευση των χρηστών και συνεχή παρακολούθηση είναι απαραίτητη για τη διαφύλαξη των πόρων cloud και τη διασφάλιση ενός ασφαλούς περιβάλλοντος υπολογιστικού νέφους.

2.6 Κλοπή Ταυτότητας και Λογαριασμού Χρήστη

Οι αδύναμοι μηχανισμοί ελέγχου ταυτότητας αποτελούν σημαντική πρόκληση ασφαλείας στη Διαχείριση Ταυτότητας και Πρόσβασης για περιβάλλοντα cloud. Ο έλεγχος ταυτότητας είναι η διαδικασία επαλήθευσης της ταυτότητας χρηστών ή οντοτήτων που προσπαθούν να αποκτήσουν πρόσβαση σε πόρους cloud και οι αδύναμοι μηχανισμοί ελέγχου ταυτότητας μπορούν να οδηγήσουν σε μη εξουσιοδοτημένη πρόσβαση, κλοπή ταυτότητας και πιθανές παραβιάσεις δεδομένων. Τα περιβάλλοντα cloud, με τη διαφορετική βάση χρηστών και τους κατανεμημένους πόρους τους, είναι ιδιαίτερα ευάλωτα σε επιθέσεις εάν δεν υπάρχουν ισχυρά μέτρα ελέγχου ταυτότητας (Mungoli, 2023b) .

Έλεγχος ταυτότητας βάσει κωδικού πρόσβασης: Η χρήση αδύναμων κωδικών πρόσβασης είναι ένα κοινό πρόβλημα στο cloud της λειτουργίας της διαχείρισης ταυτότητας και πρόσβασης. Οι χρήστες ενδέχεται να επιλέγουν απλούς και εύκολα προβλέψιμους κωδικούς πρόσβασης, να επαναχρησιμοποιούν κωδικούς πρόσβασης σε πολλές υπηρεσίες ή να μην

ενημερώνουν τακτικά τους κωδικούς πρόσβασης, καθιστώντας τους λογαριασμούς τους ευάλωτους σε επιθέσεις ωμής βίας και γέμιση διαπιστευτηρίων.

Έλεγχος ταυτότητας ενός παράγοντα (SFA): Το να βασίζεται κανείς αποκλειστικά σε έναν μόνο παράγοντα ελέγχου ταυτότητας, συνήθως έναν κωδικό πρόσβασης, είναι επικίνδυνο. Σε περίπτωση που παραβιαστούν οι κωδικοί πρόσβασης, ένας εισβολέας μπορεί να αποκτήσει μη εξουσιοδοτημένη πρόσβαση χωρίς καμία πρόσθετη επαλήθευση.

Απουσία ελέγχου ταυτότητας πολλαπλών παραγόντων (MFA): Η λειτουργία MFA προσθέτει ένα επιπλέον επίπεδο ασφάλειας, απαιτώντας από τους χρήστες να παρέχουν πολλαπλές μορφές ταυτοποίησης κατά τη σύνδεση. Η έλλειψη MFA αυξάνει την πιθανότητα μη εξουσιοδοτημένης πρόσβασης, ειδικά όταν οι κωδικοί πρόσβασης κλαπούν ή παραβιάζονται.

Μη ασφαλή πρωτόκολλα ελέγχου ταυτότητας: Η χρήση παλαιών ή μη ασφαλών πρωτοκόλλων ελέγχου ταυτότητας, όπως ο Βασικός έλεγχος ταυτότητας HTTP, μπορεί να εκθέσει τα διαπιστευτήρια σε υποκλοπή και υποκλοπή, οδηγώντας σε πιθανές παραβιάσεις της ασφάλειας.

Επιθέσεις ηλεκτρονικού ψαρέματος και κοινωνικής μηχανικής: Οι χρήστες του cloud μπορεί να πέσουν θύματα επιθέσεων ηλεκτρονικού ψαρέματος ή κοινωνικής μηχανικής, όπου οι εισβολείς εξαπατούν τους χρήστες να αποκαλύψουν τα διαπιστευτήρια σύνδεσής τους, παρακάμπτοντας εντελώς τον έλεγχο ταυτότητας.

Για την αντιμετώπιση των προκλήσεων ασφαλείας που δημιουργούνται από τους αδύναμους μηχανισμούς ελέγχου ταυτότητας στο cloud της λειτουργίας της διαχείρισης ταυτότητας και πρόσβασης, οι οργανισμοί μπορούν να εφαρμόσουν τις ακόλουθες στρατηγικές (Marinescu, 2013):

Ισχυρές πολιτικές κωδικών πρόσβασης: Επιβολή ισχυρών πολιτικών κωδικών πρόσβασης που απαιτούν από τους χρήστες να δημιουργούν σύνθετους και μοναδικούς κωδικούς πρόσβασης. Ενθαρρύνετε τη χρήση διαχειριστών κωδικών πρόσβασης για την ασφαλή αποθήκευση και διαχείριση κωδικών πρόσβασης.

Έλεγχος ταυτότητας πολλαπλών παραγόντων (MFA): Εφαρμογή MFA για όλους τους λογαριασμούς χρηστών, ειδικά για όσους έχουν πρόσβαση σε ευαίσθητα δεδομένα ή

δυνατότητες διαχείρισης. Το MFA προσθέτει ένα επιπλέον επίπεδο ασφάλειας, καθιστώντας πιο δύσκολο για τους εισβολείς να παραβιάσουν λογαριασμούς.

Βιομετρικός έλεγχος ταυτότητας: Εξετάστε το ενδεχόμενο εφαρμογής βιομετρικού ελέγχου ταυτότητας, όπως η αναγνώριση δακτυλικών αποτυπωμάτων ή προσώπου, ως μια ασφαλής και βολική μέθοδος ελέγχου ταυτότητας για τους χρήστες cloud.

Υιοθέτηση σε ασφαλή πρωτόκολλα ελέγχου ταυτότητας: Χρησιμοποιήστε ασφαλή πρωτόκολλα ελέγχου ταυτότητας, όπως το OAuth ή το OpenID Connect, για την προστασία των διαπιστευτηρίων χρήστη κατά τη διαδικασία ελέγχου ταυτότητας. Αποφύγετε τη χρήση μη ασφαλών πρωτοκόλλων όπως ο βασικός έλεγχος ταυτότητας HTTP.

Εκπαίδευση χρηστών: Εκπαίδευση στους χρήστες του cloud σχετικά με τους κινδύνους αδύναμου ελέγχου ταυτότητας και τη σημασία της δημιουργίας ισχυρών κωδικών πρόσβασης και της αναγνώρισης απόπειρες phishing. Διεξάγετε τακτικά εκπαίδευση ευαισθητοποίησης σχετικά με την ασφάλεια.

Παρακολούθηση ελέγχου ταυτότητας: Εφαρμογή σε συνεχή παρακολούθηση συμβάντων ελέγχου ταυτότητας για τον εντοπισμό ύποπτων προσπαθειών σύνδεσης ή μοτίβων που μπορεί να υποδεικνύουν επιθέσεις ωμής βίας ή παραβιασμούς λογαριασμού.

Adaptive Authentication: Αναπτύσσονται προσαρμοστικές λύσεις ελέγχου ταυτότητας που αναλύουν τη συμπεριφορά των χρηστών και εφαρμόζουν πρόσθετες προκλήσεις ελέγχου ταυτότητας εάν εντοπιστούν μη φυσιολογικές δραστηριότητες.

Με την εφαρμογή ισχυρών μηχανισμών ελέγχου ταυτότητας και την προώθηση βέλτιστων πρακτικών ασφάλειας, οι οργανισμοί μπορούν να ενισχύσουν τη συνολική ασφάλεια του cloud της λειτουργίας της διαχείρισης ταυτότητας και πρόσβασης τους και να μετριάσουν τον κίνδυνο μη εξουσιοδοτημένης πρόσβασης και παραβιάσεων δεδομένων. Μια πολύ επίπεδη προσέγγιση που συνδυάζει ισχυρές τεχνολογίες ελέγχου ταυτότητας, εκπαίδευση των χρηστών και συνεχή παρακολούθηση είναι απαραίτητη για τη διαφύλαξη των πόρων cloud και τη διασφάλιση ενός ασφαλούς περιβάλλοντος υπολογιστικού νέφους.

Συμπερασματικά, η Διαχείριση Ταυτότητας και Πρόσβασης διαδραματίζει κρίσιμο ρόλο στην ασφάλεια των περιβαλλόντων cloud διασφαλίζοντας ότι οι σωστοί χρήστες έχουν την κατάλληλη πρόσβαση σε πόρους και δεδομένα. Ωστόσο, η λειτουργία της διαχείρισης

ταυτότητας και πρόσβασης στο cloud computing συνοδεύεται από μοναδικές προκλήσεις και ζητήματα ασφάλειας.

Η παραπάνω ενότητα λοιπόν, διερεύνησε διάφορες προκλήσεις ασφαλείας της λειτουργίας της διαχείρισης ταυτότητας και πρόσβασης για περιβάλλοντα cloud, συμπεριλαμβανομένων των απειλών από εσωτερικές πληροφορίες και της κλιμάκωσης των προνομίων, των αδύναμων μηχανισμών ελέγχου ταυτότητας και της πολυπλοκότητας της διαχείρισης της πρόσβασης σε κατανεμημένους και δυναμικούς πόρους cloud. Αυτές οι προκλήσεις μπορεί να οδηγήσουν σε μη εξουσιοδοτημένη πρόσβαση, παραβιάσεις δεδομένων και άλλα συμβάντα ασφάλειας που μπορεί να έχουν σοβαρές συνέπειες για τους οργανισμούς.

Για να αντιμετωπίσουν αποτελεσματικά αυτές τις προκλήσεις, οι οργανισμοί πρέπει να υιοθετήσουν μια ολοκληρωμένη και προορατική προσέγγιση της λειτουργίας της διαχείρισης ταυτότητας και πρόσβασης. Η εφαρμογή της αρχής του ελάχιστου προνομίου είναι ζωτικής σημασίας για τον περιορισμό της πρόσβασης των χρηστών μόνο σε ό,τι είναι απαραίτητο για τις εργασιακές τους ευθύνες, μειώνοντας την επιφάνεια επίθεσης και τους πιθανούς κινδύνους εσωτερικών απειλών. Ισχυροί μηχανισμοί ελέγχου ταυτότητας, όπως ο έλεγχος ταυτότητας πολλαπλών παραγόντων (MFA) και ο βιομετρικός έλεγχος ταυτότητας, προσθέτουν ένα επιπλέον επίπεδο ασφάλειας για προστασία από μη εξουσιοδοτημένη πρόσβαση και κλοπή ταυτότητας (Ghelani, Hua and Koduru, 2022).

Η τακτική εκπαίδευση των χρηστών και εκπαίδευση ευαισθητοποίησης σχετικά με την ασφάλεια είναι ουσιαστικής σημασίας για την ενδυνάμωση των χρηστών να αναγνωρίζουν και να μετριάζουν τους κινδύνους, όπως το phishing και τις επιθέσεις κοινωνικής μηχανικής. Επιπλέον, οι οργανισμοί θα πρέπει να αξιοποιούν τη συνεχή παρακολούθηση και την ανάλυση συμπεριφοράς για τον εντοπισμό ανώμαλων δραστηριοτήτων και πιθανών παραβιάσεων της ασφάλειας σε πραγματικό χρόνο.

Οι λύσεις της λειτουργίας της διαχείρισης ταυτότητας και πρόσβασης από παρόχους υπηρεσιών cloud προσφέρουν μια σειρά από εργαλεία και υπηρεσίες για τη βελτίωση της ασφάλειας στο cloud, αλλά οι οργανισμοί πρέπει να αξιολογούν προσεκτικά και να ενσωματώνουν αυτές τις λύσεις στη στρατηγική τους. Θα πρέπει επίσης να επανεξετάζουν τακτικά τους ελέγχους πρόσβασης και τις άδειες, να διενεργούν ελέγχους ασφαλείας και να

διατηρούν ένα σχέδιο αντιμετώπισης περιστατικών για την έγκαιρη αντιμετώπιση και τον μετριασμό των περιστατικών ασφαλείας (Marinescu, 2013)

Καθώς το cloud computing εξελίσσεται και επεκτείνεται, η λειτουργία της διαχείρισης ταυτότητας και πρόσβασης θα συνεχίσει να είναι ένας κρίσιμος τομέας εστίασης για οργανισμούς που επιδιώκουν να προστατεύσουν τους πόρους, τις εφαρμογές και τα δεδομένα τους στο cloud. Εφαρμόζοντας ισχυρές πρακτικές της λειτουργίας της διαχείρισης ταυτότητας και πρόσβασης και παραμένοντας ενήμεροι για τις αναδυόμενες τάσεις ασφάλειας, οι οργανισμοί μπορούν να οικοδομήσουν μια ισχυρή άμυνα έναντι των απειλών στον κυβερνοχώρο, να προστατεύσουν ευαίσθητες πληροφορίες και να διατηρήσουν την εμπιστοσύνη των χρηστών και των πελατών τους (Comer, 2021)

Συμπερασματικά, οι οργανισμοί πρέπει να αναγνωρίσουν ότι η λειτουργία της διαχείρισης ταυτότητας και πρόσβασης δεν είναι μια εφάπαξ εφαρμογή, αλλά μια συνεχής διαδικασία που απαιτεί συνεχή βελτίωση και προσαρμογή για να ανταποκριθεί στη δυναμική φύση των περιβαλλόντων cloud. Αγκαλιάζοντας μια νοοτροπία που προέχει την ασφάλεια και καλλιεργώντας μια κουλτούρα επαγρύπνησης και υπευθυνότητα, οι οργανισμοί μπορούν να ενισχύσουν τη στάση τους για την ασφάλεια στο cloud και να αξιοποιήσουν με σιγουριά τα οφέλη του cloud computing προστατεύοντας παράλληλα τα ψηφιακά τους στοιχεία.

Κεφάλαιο 3ο – Η Βασική Λειτουργία της Διαχείρισης Ταυτότητας και Πρόσβασης σε Συνάρτηση με τους Παράγοντες που Επηρεάζουν την Ορθή Εφαρμογή και Αξιοποίησή της

3.1 Βασικά Στοιχεία και Χαρακτηριστικά στη Λειτουργία της Διαχείρισης Ταυτότητας και Πρόσβασης

Όπως σημειώθηκε και παραπάνω, το σύστημα της λειτουργίας της διαχείρισης ταυτότητας και πρόσβασης, είναι ικανό να εκτελεί λειτουργίες όπως η διαχείριση, συντήρηση, επιβολή πολιτικής, διαχείριση, ανταλλαγή πληροφοριών και έλεγχος ταυτότητας. Η συγκεκριμένη λειτουργία μπορεί να επικυρώνει ότι η ίδια ταυτότητα χρήστη, χρησιμοποιείται και διαχειρίζεται για όλες τις εφαρμογές και ταυτόχρονα διασφαλίζει την ασφάλεια (Marinescu, 2013).

Χρησιμοποιείται επίσης για τον έλεγχο της ταυτότητας χρηστών, συσκευών ή υπηρεσιών και για την παραχώρηση ή άρνηση δικαιωμάτων πρόσβασης σε δεδομένα και άλλους πόρους του συστήματος. Σε περίπτωση πρόσβασης σε οποιαδήποτε εφαρμογή, το σύστημα ή η υπηρεσία δεν απαιτεί τη δική του αποθήκευση ταυτότητας ή μηχανισμό ελέγχου ταυτότητας για τον έλεγχο ταυτότητας. Αντίθετα, η διαδικασία επαλήθευσης ταυτότητας μπορεί να διαμορφωθεί με τον αξιόπιστο πάροχο ταυτότητας, γεγονός που πράγματι μειώνει τον φόρτο εργασίας της εφαρμογής (Ghelani, Hua and Koduru, 2022).

Η λειτουργία της διαχείρισης ταυτότητας και πρόσβασης, απλοποιεί τη διαχείριση κατανεμημένων συστημάτων μεγάλης κλίμακας. Η διαχείριση ταυτότητας και πρόσβασης χρησιμοποιούνται μέσα σε μια επιχείρηση ή έξω από μια επιχείρηση σε μια σχέση επιχείρησης με επιχείρηση ή ακόμα και μεταξύ μιας ιδιωτικής επιχείρησης και ενός παρόχου cloud (Marinescu, 2013). Η λειτουργία της διαχείρισης ταυτότητας και πρόσβασης έχει μια εκτεταμένη οργανωτική περιοχή που ασχολείται με τον εντοπισμό αντικειμένων cloud, οντοτήτων και τον έλεγχο της πρόσβασης σε πόρους με βάση προκαθορισμένες πολιτικές (Mather, Kumaraswamy and Latif, 2009).

Υπάρχει ένας αριθμός επιχειρησιακών περιοχών που σχετίζονται με τη διαχείριση ταυτότητας και πρόσβασης. Οι επιχειρησιακές περιοχές περιλαμβάνουν τη διαχείριση και παροχή ταυτότητας, τη διαχείριση πιστοποίησης ταυτότητας, τη διαχείριση ομοσπονδιακής ταυτότητας, τη διαχείριση εξουσιοδοτήσεων και τη διαχείριση συμμόρφωσης. Αυτές οι περιοχές λειτουργίας διασφαλίζουν ότι οι εξουσιοδοτημένοι χρήστες ενσωματώνονται με ασφάλεια και αποτελεσματικότητα στο cloud. Η Γλώσσα σήμανσης παροχής υπηρεσιών (SPML) είναι ένα πλαίσιο που βασίζεται σε XML και χρησιμοποιείται για τη διαχείριση ταυτότητας. Ανταλλάσσει πληροφορίες πόρων, χρηστών και παροχής υπηρεσιών μεταξύ οργανισμών. Ένα από τα μειονεκτήματα του SPML είναι ότι χρησιμοποιεί πολλαπλά ιδιόκτητα πρωτόκολλα από διάφορους προμηθευτές, γεγονός που οδηγεί σε μια δέσμη διαφορετικών περιφερειακών διεπαφών εφαρμογών (API) (Mungoli, 2023b).

Καθώς τα API δεν είναι του ίδιου προμηθευτή, είναι δύσκολο να αλληλοεπιδράσουν μεταξύ τους. Ο δεύτερος επιχειρησιακός τομέας της λειτουργίας της διαχείρισης ταυτότητας και πρόσβασης, είναι η διαχείριση ταυτότητας. Αυτό διασφαλίζει την ασφαλή διαχείριση διαπιστευτηρίων, όπως κωδικών πρόσβασης και ψηφιακών πιστοποιητικών (Marinescu, 2013). Η τρίτη επιχειρησιακή περιοχή της λειτουργίας της διαχείρισης ταυτότητας και πρόσβασης, είναι η Ομοσπονδιακή Διαχείριση Ταυτότητας. Αυτή η διαχείριση ταυτότητας ελέγχει την ταυτότητα των υπηρεσιών cloud χρησιμοποιώντας τον επιλεγμένο πάροχο ταυτότητας του οργανισμού.

Η σχετική διαχείριση ταυτότητας διασφαλίζει το απόρρητο, την ακεραιότητα και τη μη άρνηση. Αυτό διασφαλίζει επίσης την εμπιστοσύνη μεταξύ μιας διαδικτυακής εφαρμογής και του παρόχου ταυτότητας ανταλλάσσοντας δημόσια κλειδιά πιστοποιημένα από την Υποδομή Δημοσίου Κλειδιού (PKI). Ο τέταρτος επιχειρησιακός τομέας είναι η διαχείριση αδειών. Η διοίκηση καθορίζει εάν η πιστοποιημένη οντότητα επιτρέπεται να εκτελεί οποιαδήποτε λειτουργία σε μια δεδομένη εφαρμογή.

Ο τελευταίος επιχειρησιακός τομέας διαχείρισης ταυτότητας και πρόσβασης είναι η διαχείριση συμμόρφωσης. Αυτό διασφαλίζει ότι οι πόροι ενός οργανισμού είναι ασφαλείς και έχουν πρόσβαση σύμφωνα με τις υπάρχουσες πολιτικές και κανονισμούς (Mungoli, 2023a). Η διαχείριση ταυτότητας διαδραματίζει σημαντικό ρόλο στον τομέα των θεμάτων ασφάλειας cloud. Το απόρρητο και η δια λειτουργικότητα είναι τα κύρια ζητήματα στις υπάρχουσες προσεγγίσεις διαχείρισης ταυτότητας, ειδικά σε περιβάλλοντα δημόσιου cloud (Mungoli, 2023a).

Επί του παρόντος, τα συστήματα της λειτουργίας της διαχείρισης ταυτότητας και πρόσβασης, είναι οι αποτελεσματικοί μηχανισμοί για τη μείωση των κινδύνων που σχετίζονται με το περιβάλλον cloud. Πολλοί οργανισμοί παρέχουν σύστημα IAM για την ασφάλεια των πληροφοριών ελέγχοντας την άδεια πρόσβασης κάθε χρήστη . Οι δημοφιλείς πάροχοι συστημάτων IAM είναι οι SailPoint, IBM, Oracle, RSA και Core Security. Η λύση διαχείρισης ταυτότητας της SailPoint έχει δυνατότητες στους τομείς της διαχείρισης κωδικών πρόσβασης, του ελέγχου συμμόρφωσης, της διαχείρισης πρόσβασης δεδομένων, του αιτήματος πρόσβασης, της αυτοματοποιημένης παροχής και της Single Sign-On (Comer, 2021).

Η σουίτα προϊόντων διαχείρισης ταυτότητας και πρόσβασης της IBM παρέχει λύσεις σε αιτήματα πρόσβασης στον ιστό, παροχή χρήστη, έλεγχο ταυτότητας πολλαπλών παραγόντων, ενιαία σύνδεση της επιχείρησης, προνομιακό έλεγχο ταυτότητας και πρόσβασης και συμμόρφωση με τη δραστηριότητα χρήστη (Mather, Kumaraswamy and Latif, 2009). Το προϊόν Oracle Identity and Access Management παρέχει τέσσερις (4) κύριες λύσεις για την ασφάλεια στο cloud.

Τα προϊόντα της αξιοποιούν την πρώτη της λύση μέσω των διαφόρων δυνατοτήτων διαχείρισης ταυτότητας, όπως αίτημα λογαριασμού αυτοεξυπηρέτησης, διαχείριση κύκλου ζωής ταυτότητας, διαχείριση κωδικών πρόσβασης και διαχείριση εταιρικού ρόλου. Το σύστημα Oracle IAM παρέχει τη δεύτερη λύση για υπηρεσίες ελέγχου ταυτότητας και διαχείρισης εμπιστοσύνης, όπως η ομοσπονδία ταυτότητας, η απλή σύνδεση και το απόρρητο.

Παρέχει επίσης τη τρίτη λύση στον έλεγχο πρόσβασης, όπως τα ακριβή δικαιώματα, η εξουσιοδότηση βάσει κινδύνου και η ασφάλεια των υπηρεσιών Web. Το σύστημα Oracle της λειτουργίας της διαχείρισης ταυτότητας και πρόσβασης, παρέχει την τέταρτη λύση του σε διακυβέρνηση ταυτότητας και πρόσβασης όπως, διαχωρισμός καθηκόντων, αναφορά ελέγχου και συμμόρφωσης, διαχείριση επίλυσης συγκρούσεων, εξόρυξη ρόλων και μηχανική, βεβαίωση, ανάλυση ταυτότητας και πρόληψη απάτης και υπηρεσίες καταλόγου (εικονικοποίηση ταυτότητας, επίμονη αποθήκευση, ασφάλεια χρήστη βάσης δεδομένων και συγχρονισμός) (Marinescu, 2013).

Το πεδίο RSA SecurID Suite προσφέρει ένα ολοκληρωμένο σύνολο δυνατοτήτων, όπως έλεγχο ταυτότητας, διαχείριση πρόσβασης, διακυβέρνηση ταυτότητας, ανάλυση

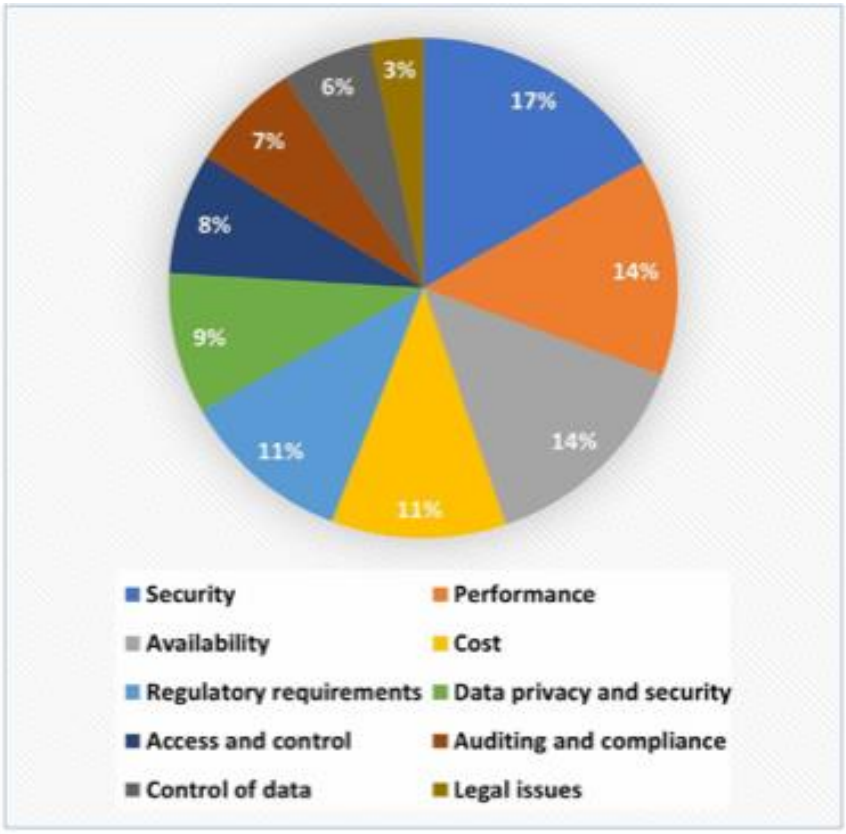
κινδύνου και διαχείριση κύκλου ζωής. Η Core Security παρέχει μια ολοκληρωμένη σειρά λύσεων διαχείρισης ταυτότητας και διακυβέρνησης πρόσβασης στους τομείς της συμμόρφωσης, των προνομιακών υπηρεσιών, της διαχείρισης κωδικών πρόσβασης και της διαχείρισης πρόσβασης και ταυτότητας.

Το Privileged Identity Management (PIM) καθορίζει τους τρόπους διαχείρισης των λογαριασμών υπερ χρήστη και τα δικαιώματα κατόχου λογαριασμού. Η PIM καθιερώνει εργαλεία και διαδικασίες, όπως εργαλεία παροχής ή εξειδικευμένα προϊόντα PIM για διαχείριση ταυτότητας. Οι δημοφιλείς πάροχοι συστημάτων PIM είναι τα IBM PIM, CyberArk και Oracle PAM (Comer, 2021).

3.2 Απειλές για την Ασφάλεια της Λειτουργίας της Διαχείρισης Ταυτότητας και Πρόσβασης σε Περιβάλλον cloud

Το cloud computing είναι μια αναδυόμενη τεχνολογία που επί του παρόντος αποτελεί το πιο αξιόπιστο σύστημα αποθήκευσης και ασφάλειας πληροφοριών. Παρόλο που το σύστημα που βασίζεται στο cloud έχει πολλά πλεονεκτήματα, έχει ορισμένα ζητήματα που σχετίζονται με την ασφάλεια των αποθηκευμένων δεδομένων. Το αρχικό βήμα για την εξάλειψη των κινδύνων είναι ο εντοπισμός των σημαντικότερων κινδύνων σε ένα περιβάλλον cloud (Marinescu, 2013).

Η κοινόχρηστη και η κατ' απαίτηση πρόσβαση κυριαρχούν παράγοντες για τα ζητήματα ασφάλειας που εντοπίστηκαν πρόσφατα στο cloud. Η ένταση της ανάπτυξης του cloud computing αυξάνει τις απειλές ασφαλείας σε πολλαπλές διαστάσεις. Τα εντοπιζόμενα ζητήματα ασφάλειας είναι παραβιάσεις δεδομένων, προστασία διαπιστευτηρίων, πειρατεία λογαριασμών, παραβιασμένες διεπαφές και API, κακόβουλοι μυστικοί χρήστες, επιθέσεις DoS και θέματα κοινής τεχνολογίας. Οι διάφοροι τομείς των απειλών στο περιβάλλον του cloud και το μερίδιό τους στην παρούσα εποχή φαίνονται στο σχήμα No.1.



Εικόνα No.1 – Ανάλυση Διαφόρων θεμάτων που Εμπεριέχονται σε Περιβάλλον Cloud

3.3 Απειλές στην Υποδομή του Περιβάλλοντος Cloud

3.3.1 Ασφάλεια Δεδομένων

Η προστασία των δεδομένων είναι απαραίτητη στο περιβάλλον cloud, όσον αφορά τη διαθεσιμότητα, την ακεραιότητα και την εμπιστευτικότητα. Ένας από τους πιθανούς μηχανισμούς ασφάλειας δεδομένων είναι η κρυπτογραφία. Οι κρυπτογραφικοί μηχανισμοί εφαρμόζουν μέτρα ασφαλείας απευθείας στα δεδομένα. Η παραγοντοποίηση των πρώτων αριθμών, η δυσκολία του διακριτού λογάριθμου, οι γενιές τυχαίων αριθμών είναι μερικές μαθηματικές μέθοδοι για την παραγωγή αριθμητικών δεδομένων για κρυπτογραφία (Ghelani, Hua and Koduru, 2022).

Δύο διακριτοί παράγοντες που συνέβαλαν, είναι η εξελισσόμενη τεχνολογία και οι μέθοδοι διάρρηξης κωδικού πρόσβασης. Καθώς η ικανότητα επεξεργασίας των σύγχρονων υπολογιστικών συσκευών έχει αυξηθεί σημαντικά, η πολυπλοκότητα του χρόνου αναζήτησης και οι τεράστιοι συνδυαστικοί χώροι κλειδιών εκτελούνται εύκολα και γρήγορα. Το πιο ευάλωτο αποτέλεσμα επίθεσης στην κρυπτογραφία είναι η επίθεση ωμής βίας.

Τα θέματα ασφάλειας δεδομένων κατηγοριοποιούνται ως απαιτήσεις ασφαλείας για δεδομένα σε κίνηση και απαιτήσεις ασφαλείας για δεδομένα σε κατάσταση ηρεμίας. Τα ζητήματα ασφαλείας για τα δεδομένα σε κατάσταση ηρεμίας προκύπτουν όταν ένας κακόβουλος χρήστης χρησιμοποιεί κατάχρηση ή χειραγωγεί τις πληροφορίες πρόσβασης του χρήστη μέσω των δικαιωμάτων πρόσβασής του στη βάση δεδομένων της εφαρμογής ή παρέχει δικαιώματα μη εξουσιοδοτημένης πρόσβασης σε τρίτο μέρος για μια συγκεκριμένη εφαρμογή (Mungoli, 2023b)

Τα ευαίσθητα δεδομένα περιέχουν τα στοιχεία των χρηστών και τα προνομιακά τους στοιχεία, τα οποία πρέπει να προστατεύονται μέσω της κατάλληλης κρυπτογραφικής σουίτας. Σε ορισμένα σενάρια ευαίσθητα δεδομένα πρέπει να μεταφερθούν σε μεγάλη ποσότητα από τον διακομιστή στην υπηρεσία που ζητά την εφαρμογή-στόχο. Σε τέτοιες περιπτώσεις, τα δεδομένα θα πρέπει να προστατεύονται με τη βοήθεια πιστοποιητικών SSL.

3.3.2 Ιός ή Κακόβουλο Λογισμικό

Το κακόβουλο λογισμικό αναφέρεται ως κακόβουλο λογισμικό που έχει προγραμματιστεί να διακόπτει τις κανονικές λειτουργίες του υπολογιστή. Χρησιμοποιείται για τη συλλογή ευαίσθητων πληροφοριών ή για την απόκτηση πρόσβασης σε απομονωμένα συστήματα υπολογιστών (Ghelani, 2022). Το κακόβουλο λογισμικό έχει τρομερή πρόθεση να ενεργήσει ενάντια στις απαιτήσεις των χρηστών και να προκαλέσει σοβαρές ζημιές στην απόδοση των συστημάτων που βασίζονται στο cloud. Οι παραβάτες του κυβερνοχώρου μοιράζονται ως επί το πλείστων κακόβουλα προϊόντα και επιμένουν στους χρήστες να εγκαταστήσουν το κοινόχρηστο λογισμικό στους υπολογιστές ή τις φορητές συσκευές τους δίνοντας ψεύτικες υποσχέσεις.

Ο απώτερος στόχος αυτών των εγκληματιών, είναι να αποκτήσουν τον έλεγχο του συγκεκριμένου υπολογιστή ή κινητής συσκευής. Μόλις εγκατασταθεί τέτοιο κακόβουλο λογισμικό, οι εισβολείς δυνητικά αποκτούν τον απόλυτο έλεγχο του υπολογιστή ή των φορητών συσκευών. Ενώ το σύστημα που δέχεται επίθεση προσπαθεί να συνδεθεί με τον διακομιστή cloud για τη χρήση υπηρεσιών cloud, το κακόβουλο λογισμικό εξαπλώνεται στις εικονικές μηχανές του περιβάλλοντος cloud, το οποίο αργότερα εξαπλώνεται σε κάθε χρήστη που έχει πρόσβαση στο cloud. Συμβάντα ή επιθέσεις κακόβουλου λογισμικού συμβαίνουν συχνά σε οργανισμούς που στοχεύουν στην παραβίαση της υποδομής ασφάλειας του (Mather, Kumaraswamy and Latif, 2009).

3.3.3 Διαθεσιμότητα Πόρων

Η διαθεσιμότητα πόρων αναφέρεται στα συστήματα και τις υπηρεσίες που είναι προσβάσιμα από μια οντότητα που έχει πιστοποιηθεί μέσω κατάλληλης εξουσιοδότησης. Η διαθεσιμότητα του cloud σημαίνει το σύνολο των πόρων που είναι προσβάσιμοι ανά πάσα στιγμή από εξουσιοδοτημένες οντότητες (Marinescu, 2013). Η διαθεσιμότητα θεωρείται μια από τις βασικές απαιτήσεις ασφαλείας στο cloud computing καθώς διασφαλίζει τη χρήση των πόρων ανά πάσα στιγμή και σε οποιοδήποτε μέρος από τους χρήστες του cloud.

Σε ορισμένες περιπτώσεις, οι πόροι είναι διαθέσιμοι με διαφορετικό τρόπο, ο οποίος πρέπει να παρέχονται στους χρήστες cloud χωρίς διακοπές κατά την πρόσβαση στην υπηρεσία cloud. Σε περίπτωση παραβίασης της ασφάλειας ή καταστροφής, η δυνατότητα συνέχισης της επιχείρησης ως συνήθως είναι ο πρωταρχικός στόχος της διαθεσιμότητας. Γενικά, οι υπηρεσίες cloud εκτελούνται σε πολλαπλές εικονικές μηχανές. Το Hypervisor ελέγχει τις εικονικές μηχανές επιτρέποντας σε πολλά λειτουργικά συστήματα να μοιράζονται έναν ενιαίο κεντρικό υπολογιστή υλικού. Όποτε ένας hypervisor δεν λειτουργεί κανονικά, επηρεάζει σημαντικά τη διαθεσιμότητα της υπηρεσίας cloud (Marinescu, 2013)

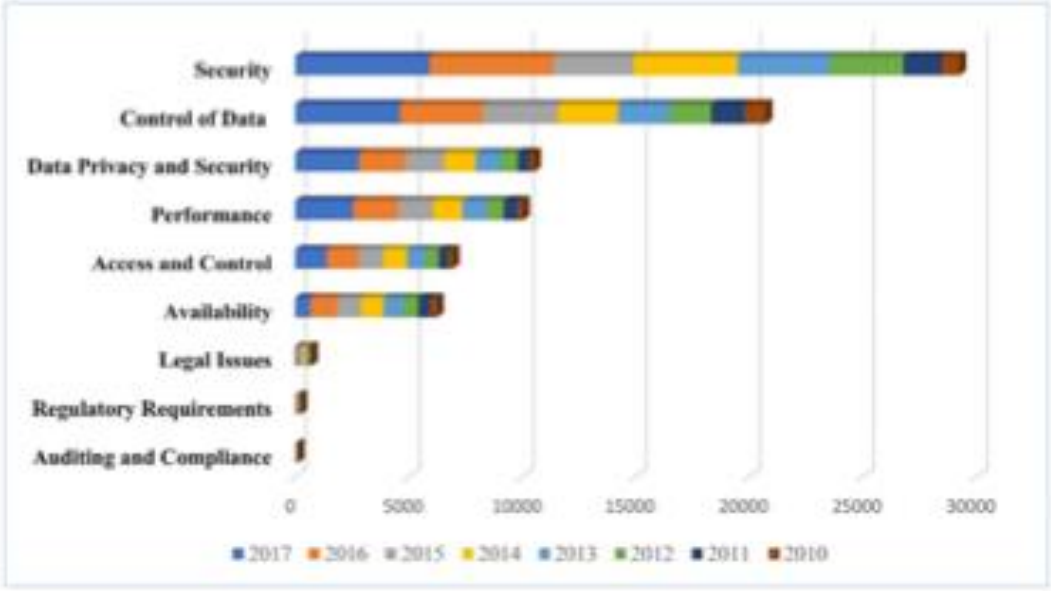
3.3.4 Εικονική Μηχανή και Πολυμίσθωση

Η πολυμίσθωση είναι ένα πλαίσιο λειτουργίας, στο οποίο πολλοί πελάτες χρησιμοποιούν ταυτόχρονα ένα μόνο παράδειγμα μιας εφαρμογής λογισμικού. Ο πελάτης cloud που έχει τη δυνατότητα πρόσβασης σε εφαρμογές στο περιβάλλον cloud ονομάζεται μισθωτής. Η πολυμίσθωση αντιπροσωπεύει ότι περισσότεροι από ένας ενοικιαστές μοιράζονται οποιαδήποτε συγκεκριμένη εφαρμογή, συμπεριλαμβανομένων των υπολογιστικών υπηρεσιών, των πόρων και της αποθήκευσης (Erl, Puttini and Zaigham, 2013).

Στην πολυμίσθωση, οι πόροι μοιράζονται στο δίκτυο cloud. Απαιτείται για να διασφαλιστεί ότι ο πάροχος cloud λαμβάνει τα κατάλληλα μέτρα για τη διασφάλιση της απομόνωσης της κυκλοφορίας δικτύου, των παρουσιών εφαρμογών και των εικονικών μηχανών (VM). Η διαχείριση της χρήσης πόρων γίνεται με διαμερισμό μιας εικονικής, κοινόχρηστης υποδομής μεταξύ διαφόρων πελατών (Erl, Puttini and Zaigham, 2013).

Προκειμένου να επιτευχθεί η επιδιωκόμενη ευελιξία παροχής αξιόπιστων υπηρεσιών, τα δίκτυα cloud χρειάζονται υψηλούς βαθμούς πολυμίσθωσης σε διαφορετικές πλατφόρμες

λειτουργίας. Στο cloud computing, η πολυμίσθωση και η εικονικοποίηση είναι τα τεράστια ζητήματα. Ο οργανισμός πρέπει να διασφαλίσει ότι όλες οι υπηρεσίες ενοικιαστών απομονώνονται με ακρίβεια η μία από την άλλη και επίσης διασφαλίζει ότι υπάρχουν δεν υπάρχουν δυνατότητες διαρροών δεδομένων και συναλλαγών από το περιβάλλον cloud κοινόχρηστων πόρων (Marinescu, 2013)



Εικόνα No.2 – Ερευνητικές Μελέτες σε Κάθε Κατηγορία σε Περιβάλλον Cloud

3.3.5 Τύπος Κακόβουλης Επίθεσης

Η κακόβουλη επίθεση Advanced Persistent Threat (APT) είναι ένα είδος επίθεσης κατά την οποία ένας εισβολέας ή ένα μη εξουσιοδοτημένο άτομο αποκτά πρόσβαση σε ένα περιβάλλον cloud και παραμένει στο δίκτυο για μεγάλο χρονικό διάστημα χωρίς να εντοπιστεί. Η επίθεση APT στοχεύει στην κλοπή των δεδομένων αντί να προκαλέσει ζημιές στο δίκτυο ή τον οργανισμό. Οι οργανισμοί-στόχοι των επιθέσεων APT βρίσκονται σε περιοχές με πολύ ευαίσθητες πληροφορίες, όπως η βιομηχανία, η εθνική άμυνα και η χρηματοπιστωτική βιομηχανία (Dotson, 2019).

Οι πληροφορίες από εταιρείες, κυβερνήσεις και ιδιώτες στοχεύουν να επιτρέψουν τον έλεγχο, την τροποποίηση και τη μελλοντική χρήση των δεδομένων για τη διακοπή της απόδοσης στα συστήματα cloud. Ένα μοντέλο επίθεσης APT αποτελείται από τη φάση συλλογής πληροφοριών κατά την οποία ένας εισβολέας εκτελεί πιο τολμηρές σαρώσεις αναγνώρισης για να χαρτογραφήσει το δίκτυο στόχο. Στη φάση της μοντελοποίησης απειλών,

ο εισβολέας προσδιορίζει το δίκτυο ή τον διακομιστή στόχο και την καλύτερη τεχνική για την εκτέλεση της επίθεσης. Τέλος, ο εισβολέας εκμεταλλεύεται τις πιθανές ευπάθειες και εκτελεί την επίθεση (Dotson, 2019) .

3.3.6 Απειλές στις Υπηρεσίες cloud

Το περιβάλλον cloud όχι μόνο περιέχει υλικό για τα δεδομένα που πρόκειται να αποθηκευτούν και να υποβληθούν σε επεξεργασία, αλλά περιέχει επίσης διαδρομή για τη μετάδοση δεδομένων. Η υποδομή Cloud χρησιμοποιεί διαφορετικά πρότυπα και πρωτόκολλα που υποστηρίζουν πολλαπλούς τομείς για σκοπούς δια λειτουργικότητας και μετάδοσης δεδομένων (Marinescu, 2013).

Το βασικό μοντέλο επικοινωνίας στο Διαδίκτυο είναι το μοντέλο TCP/IP και οι στοίβες του περιλαμβάνουν διαφορετικά πρωτόκολλα και πρότυπα. Τα πρότυπα και τα πρωτόκολλα του cloud που σχετίζονται με τις υπηρεσίες cloud χρειάζονται διεθνή πρότυπα που πρέπει να διατηρηθούν για λειτουργίες πολλαπλών πλατφορμών (Dotson, 2019). Οι απαιτήσεις για τον πάροχο υπηρεσιών cloud είναι να σχεδιάζει, να καθιερώνει, να λειτουργεί, να εφαρμόζει, να αναθεωρεί, να παρακολουθεί, να βελτιώνει και να διατηρεί όπως καθορίζεται από το σύστημα διαχείρισης υπηρεσιών. Η αναγκαιότητα για την εκπλήρωση των απαιτήσεων υπηρεσιών περιλαμβάνει, σχεδιασμό, παράδοση, μετάβαση και βελτίωση των υπηρεσιών. Οι υπηρεσίες cloud σχετίζονται σε μεγάλο βαθμό με το σύστημα διαχείρισης πληροφορικής καθώς οι παρεχόμενες υπηρεσίες βασίζονται σε IT (Dotson, 2019).

3.3.7 Υπηρεσίες Web Cloud

Το περιβάλλον cloud χρησιμοποιεί διαφορετικούς τύπους υπηρεσιών για την ενσωμάτωση διαδικτυακών εφαρμογών. Οι υπηρεσίες Ιστού είναι ένας από τους τυποποιημένους τρόπους ενσωμάτωσης διαδικτυακών εφαρμογών. Οι υπηρεσίες Ιστού χρησιμοποιούν διαφορετικά πρωτόκολλα για διαφορετικές λειτουργίες και αυτά συλλογικά εκτελούν τις υπηρεσίες αποτελεσματικά. Σε περίπτωση προσθήκης ετικετών δεδομένων, οι υπηρεσίες Ιστού χρησιμοποιούν επεκτάσιμη γλώσσα σήμανσης (XML) και για τη μεταφορά δεδομένων, το πρωτόκολλο πρόσβασης απλού αντικειμένου (SOAP) (Erl, Puttini and Zaigham, 2013) .

Οι διαθέσιμες υπηρεσίες Ιστού εμφανίζονται με τη χρήση της Γλώσσας Περιγραφής Υπηρεσιών Ιστού (WSDL) και η λίστα των διαθέσιμων πόρων γίνεται από την Universal

Description Discovery and Integration (UDDI). Η τεχνολογία των υπηρεσιών Ιστού επιτρέπει στους οργανισμούς να χρησιμοποιούν πλήρως το Λογισμικό ως Υπηρεσία (SaaS). Οι τυπικές τεχνολογίες Διαδικτύου αναπτύσσουν κυρίως υπηρεσίες Ιστού. Η διαθεσιμότητα και η προσβασιμότητα των υπηρεσιών Ιστού σε περιβάλλον cloud διατηρούνται από μια ειδική ομάδα που απασχολείται από τους προμηθευτές (Erl, Puttini and Zaigham, 2013).

Κυρίως, ο έλεγχος των αδειών πρόσβασης που επηρεάζουν την ασφάλεια των υπηρεσιών γίνεται από αυτήν την αποκλειστική ομάδα. Προκειμένου να περιοριστούν αυτά τα προβλήματα, είναι απαραίτητοι οι οργανισμοί να εφαρμόζουν καλά οργανωμένους μηχανισμούς ελέγχου πρόσβασης υπηρεσιών Web.

3.3.8 Τεχνολογίες Ιστού

Η τεχνολογία Ιστού είναι ένας εξελιγμένος μηχανισμός που επιτρέπει τη διεπαφή μεταξύ διακομιστή Ιστού και θεμάτων για επικοινωνία μέσω του δικτύου. Αυτή η τεχνολογία επιτρέπει τη γρήγορη, υψηλής ταχύτητας και εύκολη μετάδοση πληροφοριών σε έναν αριθμό συστημάτων και συσκευών (Mungoli, 2023b). Η τεχνολογία Ιστού περιέχει διαφορετικές μεθόδους επικοινωνίας για την αύξηση της αποτελεσματικότητας των λειτουργιών. Οι διαδικασίες που εμπλέκονται στην τεχνολογία Ιστού είναι πολύπλοκες και ποικίλες. Τα συστήματα υπολογιστών επηρεάζονται από επιθέσεις μέσω δικτύων. Η επίθεση κακόβουλου λογισμικού εκμεταλλεύεται τις αδυναμίες ενός δικτύου για να μολύνει διάφορα συστήματα δικτύου.

Οι κακόβουλοι ιστότοποι λειτουργούν σαν γνήσιοι ιστότοποι κρύβοντας την κακόβουλη φύση τους. Τέτοιοι ιστότοποι παράγουν τρωτά σημεία στις εφαρμογές που παρέχονται από τεχνολογίες ιστού. Προκειμένου να μειωθούν αυτές οι κρυφές επιθέσεις, η ασφάλεια του δικτύου είναι απαραίτητη κατά τη χρήση της τεχνολογίας Ιστού. Το κύριο μειονέκτημα της τεχνολογίας Web είναι ότι δεν είναι φιλική προς το χρήστη. Ως εκ τούτου, είναι πολύπλοκο για τους χρήστες που έχουν λιγότερη εμπειρία να παρακολουθούν προβλήματα δικτύου. Απαιτείται ένα καλά εκπαιδευμένο άτομο με συγκεκριμένες δεξιότητες για την επίλυση αυτών των προβλημάτων δικτύου.

3.3.9 Διαθεσιμότητα Υπηρεσιών

Τα κέντρα δεδομένων παρέχουν τεράστιο αριθμό υπηρεσιών που φιλοξενούνται σε πολλούς διακομιστές. Για να υποστηριχθούν αυτές οι υπηρεσίες ή ένας τεράστιος όγκος

μεταφοράς δεδομένων, απαιτούνται κατάλληλες συνδέσεις δικτύου με υψηλό εύρος ζώνης. Υπάρχουν διάφοροι τύποι επιθέσεων ασφαλείας που επηρεάζουν τη διαθεσιμότητα μιας υπηρεσίας που βασίζεται στο cloud, όπως DoS, DDoS, επιθέσεις πλημμύρας, ανάκλαση DNS και επίθεση ενίσχυσης (Dotson, 2019).

Βασικά, το Denial of Service ή αλλιώς οι επιθέσεις πάγου (DoS) ταξινομούνται σε δύο κατηγορίες ως άμεσες και έμμεσες επιθέσεις. Στην άμεση επίθεση, ένα μεμονωμένο κακόβουλο αίτημα δημιουργεί υπερφόρτωση του διακομιστή εκμεταλλευόμενη μια ευπάθεια ή επεξεργαζόμενη πολλά αιτήματα. Στην έμμεση επίθεση, η ροή των πακέτων διαποτίζει πλήρως τις συνδέσεις δικτύου ή τους ενδιάμεσους δρομολογητές με ψεύτικες αιτήσεις που τερματίζουν τις ειλικρινείς συνδέσεις ενώ φτάνει τη χωρητικότητα εύρους ζώνης. Προκειμένου να ξεπεραστεί ο αντίκτυπος των επιθέσεων DoS, απαιτείται η ρύθμιση ενός περιβάλλοντος υψηλής διαθεσιμότητας (HA) που εξαπλώνεται σε πολλά κέντρα δεδομένων και απαιτεί επίσης ένα κατάλληλο σχέδιο αποκατάστασης από καταστροφές (DR) (Ghelani, Hua and Koduru, 2022).

3.4 Ανάλυση Ασφάλειας σε Περιβάλλον Cloud

3.4.1 Επιθέσεις Man-in-the-Middle (MITM)

Στα συστήματα cloud, ο εισβολέας παρεμποδίζει την επικοινωνία μεταξύ των συστημάτων και χειρίζεται δεδομένα χωρίς τη γνώση του παρόχου και του εξαρτημένου μέρους. Ο εισβολέας μιμείται την επικοινωνία μεταξύ του παρόχου και του εξαρτώμενου μέρους που προσποιείται ότι ενεργεί όπως αυτοί ονομάζεται επίθεση man-in-the-middle. Η επίθεση MITM στοχεύει να κλέψει προσωπικά στοιχεία αναγνώρισης, όπως διαπιστευτήρια, πληροφορίες λογαριασμού και οικονομικά δεδομένα, συμπεριλαμβανομένων αριθμών πιστωτικών καρτών και τραπεζικών στοιχείων.

Οι κλεμμένες πληροφορίες μπορούν να χρησιμοποιηθούν σε κλοπή ταυτότητας, παράνομες αλλαγές κωδικού πρόσβασης και μη εγκεκριμένες μεταφορές χρημάτων. Η χρήση μεθόδων κρυπτογράφησης θα μπορούσε να βοηθήσει στην αποφυγή των παρεμβολών στην επικοινωνία. Η κατάλληλη διαμόρφωση SSL (secure socket layer) μπορεί να μειώσει τον κίνδυνο επιθέσεων MITM. Τα διακριτικά μιας φοράς πρόσβασης και τα κρυπτογραφημένα διακριτικά για την επαλήθευση της ταυτότητας μπορούν να μειώσουν την ευπάθεια MITM (Dotson, 2019).

3.4.2 Επιθέσεις εκ των Έσω

Οι επιθέσεις εκ των έσω εξαπολύονται από κάποιον που βρίσκεται εντός της περιφέρειας ασφαλείας και θέτει σε κίνδυνο την ασφάλεια. Ο κακόβουλος ιός είναι είτε επιχειρηματικός συνεργάτης/ανάδοχος ενός οργανισμού είτε πρώην/νυν υπάλληλος αυτού του οργανισμού. Αυτοί οι εμπιστευτικοί χρήστες κάνουν κατάχρηση των προνομίων τους για να έχουν πρόσβαση στους ευαίσθητους πόρους του οργανισμού που μπορεί να επηρεάσουν την ακεραιότητα, την εμπιστευτικότητα ή τη διαθεσιμότητα αυτού του οργανισμού.

Στα δίκτυα cloud, οι εμπιστευτικοί μπορεί να είναι τρίτοι προμηθευτές ή διαχειριστές cloud που χρησιμοποιούν τους πόρους του cloud για να πραγματοποιήσουν επιθέσεις κατά της οργανωτικής υποδομής. Απαιτείται η χρήση ισχυρού μηχανισμού ελέγχου ταυτότητας και εξουσιοδότησης. Οι πολιτικές διακυβέρνησης πρόσβασης των οργανισμών θα πρέπει να καθοριστούν κατάλληλα, γεγονός που θα μπορούσε να μειώσει σημαντικά τις απειλές από εσωτερικές επιθέσεις.

3.4.3 Επανάληψη Επιθέσεων

Στις υπηρεσίες cloud, ο εισβολέας δημιουργεί ένα αίτημα ελέγχου ταυτότητας από το μήνυμα ελέγχου ταυτότητας που ανταλλάσσονταν προηγουμένως μεταξύ ενός εξουσιοδοτημένου χρήστη και του συστήματος στόχου. Στην επίθεση επανάληψης ή αναπαραγωγής, ο εισβολέας συλλαμβάνει το αίτημα ελέγχου ταυτότητας μέσω hacking και το μιμείται σκόπιμα με ή χωρίς τροποποίηση για να αποκτήσει πρόσβαση στους πόρους του cloud. Μετριασμός: Μια ισχυρή μέθοδος κρυπτογράφησης μπορεί να βοηθήσει στην αποφυγή των παρεμβολών στην επικοινωνία. Οι οργανισμοί μπορούν να αποφύγουν επιθέσεις επανάληψης στο περιβάλλον cloud τους ορίζοντας τη λήξη και τα OTP για τα μηνύματα ελέγχου ταυτότητας (Mather, Kumaraswamy and Latif, 2009).

3.4.4 Παραβίαση Συνεδρίας / Cookie

Η παραβίαση περιόδου λειτουργίας συμβαίνει όταν το αναγνωριστικό περιόδου λειτουργίας για τον έλεγχο ταυτότητας των χρηστών δεν είναι καλά προστατευμένο. Συνήθως, η περίοδος σύνδεσης/cookie αποθηκεύει τα στοιχεία των χρηστών και τα στοιχεία διαπιστευτηρίων του (Dotson, 2019). Μόλις παραβιαστεί μια έγκυρη περίοδος σύνδεσης, ο εισβολέας μπορεί να χρησιμοποιήσει το παραβιασμένο αναγνωριστικό περιόδου λειτουργίας για πλαστογράφηση επίθεσης. Τα εργαλεία ανίχνευσης πακέτων χρησιμοποιούνται για να

αποκτήσουν πρόσβαση στο κλειδί συνεδρίας των χρηστών μέσω της καταγραφής της ακολουθίας σύνδεσης (Mather, Kumaraswamy and Latif, 2009)

Κατά την πειρατεία cookie, το cookie του προγράμματος περιήγησης κλέβεται για έλεγχο ταυτότητας σε άλλο ιστότοπο χωρίς τη γνώση του κατόχου. Η παραβίαση συνεδρίας/cookie συμβαίνει λόγω κακόβουλου λογισμικού, ευπάθειας στο σύστημα, επίθεσης phishing και εργαλείων sniffing. Η χρήση ασφαλούς περιόδου λειτουργίας μπορεί να βοηθήσει στην αποτροπή επιθέσεων παραβίασης συνεδρίας από ιστότοπους πελατών. Συνιστάται επίσης να χρησιμοποιείται αποτελεσματικό λογισμικό προστασίας από ιούς, λογισμικό κατά του κακόβουλου λογισμικού και το λογισμικό θα πρέπει να διατηρείται ενημερωμένο. Η επίθεση πειρατείας συνεδρίας μπορεί να αποτραπεί κρυπτογραφώντας ολόκληρη την επικοινωνία μέσω καναλιών (Dotson, 2019).

3.4.5 Προβλεπόμενες Επιθέσεις

Κατά την εικασία επιθέσεων, ο εισβολέας αναγεννά τους κωδικούς πρόσβασης των χρηστών που χρησιμοποιούν τους κωδικούς πρόσβασης ως απλά μοτίβα ή τους κάνουν να τους θυμούνται εύκολα. Οι εισβολείς συλλέγουν ορισμένες ζωτικής σημασίας πληροφορίες για τους έγκυρους χρήστες και προσπαθούν να προβλέψουν τον κωδικό πρόσβασής τους και επιχειρεί να συνδεθεί μέχρι να αποκτήσει πρόσβαση. Σε περιπτώσεις εκτός σύνδεσης, υπάρχει μεγάλη πιθανότητα να λάβετε τον σωστό κωδικό πρόσβασης μαντεύοντάς τον, καθώς δεν υπάρχει περιορισμός στον αριθμό των προσπαθειών (Brute Force). Μετριασμός: Η χρήση ισχυρών κωδικών πρόσβασης και ο αποκλεισμός του χρήστη μετά από έναν ορισμένο αριθμό προσπαθειών σύνδεσης μπορεί να αποτρέψει το σύστημα από διαφορετικούς τύπους επιθέσεων εικασίας (Ghelani, Hua and Koduru, 2022)

3.4.6 Επιθέσεις Denial-of-Service (DoS/DDoS)

Στην επίθεση Denial of Service (DoS), ο διακομιστής-στόχος υπερφορτώνεται με πλαστά αιτήματα υπηρεσίας που τελικά εμποδίζει το σύστημα να ανταποκρίνεται στα γνήσια αιτήματα. Μόλις ο διακομιστής στόχος δεν είναι σε θέση να χειριστεί μόνος του τα αιτήματα συνεχούς υπηρεσίας, μεταβιβάζει τα αιτήματα σε παρόμοιο παράδειγμα διακομιστή στο σύστημα εξισορρόπησης φορτίου που τελικά οδηγεί σε επιθέσεις πλημμύρας.

Οι επιθέσεις Distributed Denial of Service (DDoS) ξεκινούν από bots ή κακόβουλο λογισμικό από χιλιάδες μολυσμένους κεντρικούς υπολογιστές. Οι διακομιστές σε περιβάλλον

cloud είναι ευάλωτοι σε επιθέσεις DoS/DDoS καθώς υποστηρίζουν μοντέλα IaaS, SaaS. Μετριασμός: Η χρήση τείχους προστασίας για να επιτρέπεται ή να απαγορεύεται η πρόσβαση σε θύρες, πρωτόκολλα ή διευθύνσεις IP. Ο αντίκτυπος λόγω επιθέσεων DoS στις υπηρεσίες cloud μπορεί να ελαχιστοποιηθεί μέσω προγραμματισμού περιορισμού και ρύθμισης (Προϊόντα όπως, DataPower Gateway για περιορισμό της κατανομής του εύρους ζώνης δικτύου) των επισκέψεων από κάθε κανάλι οργανισμού που ζητά (Dotson, 2019).

3.5 Συστάσεις και Βέλτιστες Πρακτικές της Λειτουργίας της Διαχείρισης Ταυτότητας και Πρόσβασης

Τα διαφορετικά μοντέλα ταυτότητας και ελέγχου πρόσβασης συγκρίνονται και οι πτυχές ασφαλείας κάθε μοντέλου αναλύονται σε βάθος για να παρέχουν ολοκληρωμένη επισκόπηση των συστημάτων της λειτουργίας της διαχείρισης ταυτότητας και πρόσβασης για ακαδημαϊκούς και προσωπικό του κλάδου. Οι ακόλουθες συστάσεις προτείνονται για τα μοντέλα ελέγχου ταυτότητας και εξουσιοδότησης για διαφορετικά σενάρια (Mather, Kumaraswamy and Latif, 2009).

- ✓ Ως βέλτιστη πρακτική, πρέπει να χρησιμοποιείται οποιοσδήποτε από τους μηχανισμούς ελέγχου ταυτότητας πολλαπλών παραγόντων σε συνδυασμό με τον παραδοσιακό έλεγχο ταυτότητας που βασίζεται σε διαπιστευτήρια και τον έλεγχο ταυτότητας βάσει κλειδιού SSH. Η εφαρμογή ενός άλλου επιπέδου ασφάλειας πάνω από τον κανονικό έλεγχο ταυτότητας που βασίζεται σε διαπιστευτήρια βοηθά τους οργανισμούς να αποφύγουν τις εσωτερικές απειλές. Για τον ίδιο σκοπό συνιστάται επίσης η χρήση συνδυασμού τσιπ και καρφίτσας πάνω από τους παραδοσιακούς μηχανισμούς τσιπ/μαγνητικών ταινιών.
- ✓ Το πλαίσιο OpenID Connect που προσφέρει κρυπτογραφημένη επικοινωνία μεταξύ των εξαρτώμενων μερών συνιστάται για τη συνένωση μιας εγγενούς εφαρμογής από κινητό ή υπολογιστή.
- ✓ Σε σενάρια SSO που βασίζονται στον ιστό, συνιστάται ανεπιφύλακτα η κρυπτογραφημένη και υπογεγραμμένη επικοινωνία SAML για την αποφυγή τρωτών σημείων όπως ο άνθρωπος σε μεσαίες επιθέσεις και οι επιθέσεις επανάληψης.
- ✓ Ο έλεγχος πρόσβασης βάσει ρόλων συνιστάται ως μηχανισμός εξουσιοδότησης για οργανισμούς. Το μοντέλο RBAC εξασφαλίζει γρήγορη ενσωμάτωση των εργαζομένων/αναδόχων στην οργανωτική δομή που εξοικονομεί κόστος και χρόνο επιβίβασης.

- ✓ Ο μηχανισμός εξουσιοδότησης μοντέλου ABAC συνιστάται για κοινή χρήση υποδομής cloud, καθώς προσφέρει ευέλικτες και δυναμικές λειτουργίες.
- ✓ Ως βέλτιστη πρακτική του κλάδου, οι συστάσεις διακυβέρνησης πρόσβασης, όπως η πιστοποίηση ταυτότητας και λογαριασμού, η διαχείριση του κύκλου ζωής και ο διαχωρισμός καθηκόντων, πρέπει να ακολουθούνται για τη διασφάλιση ασφαλών υπηρεσιών cloud.

Η υπηρεσία cloud είναι ένα σημαντικό παράδειγμα για ψηφιακές λύσεις, καθώς μειώνει τις κεφαλαιουχικές δαπάνες και τις λειτουργικές δαπάνες ενός οργανισμού. Οι κίνδυνοι και τα τρωτά σημεία ασφαλείας αποτελούν το κύριο μέλημα αυτής της τεχνολογίας λόγω της φύσης της πολλαπλής μίσθωσης και της ανάθεσης τρίτων για τη συντήρηση του περιβάλλοντος cloud. Η έρευνα των διαφορετικών μηχανισμών διαχείρισης ταυτότητας και πρόσβασης μαζί με τις διαφορετικές υπηρεσίες που προσφέρει η τεχνολογία cloud υπογραμμίζει την αναγκαιότητα βελτίωσης των υφιστάμενων πλαισίων διαχείρισης ταυτότητας και πρόσβασης, γεγονός που δείχνει πράγματι την κατεύθυνση για μελλοντική έρευνα και ανάπτυξη κατάλληλων μεθοδολογιών.

Κεφάλαιο 4ο – Η Συμβολή του Πεδίου Cloud ως προς την Διαχείριση και Πρόσβαση Ταυτότητας σε «Ευαίσθητα» Δεδομένα των Επιχειρήσεων και ως προς την Προστασία των Δεδομένων Αυτών σε Τεχνολογικό και Νομικό Επίπεδο (Κανονισμός GDPR)

4.1 Η Συμβολή του Πεδίου Cloud ως προς την Διαχείριση και Πρόσβαση Ταυτότητας σε «Ευαίσθητα» Δεδομένα των Επιχειρήσεων

Αποτελεί γεγονός πως τα τελευταία δύο (2) χρόνια ο όρος cloud computing έχει αναπτυχθεί ιδιαίτερα γρήγορα από εφαρμογές ηλεκτρονικού ταχυδρομείου που βασίζονται στον ιστό όπως το Hotmail, σε σουίτες λογισμικού όπως η σουίτα CRM Salesforce.com και η σουίτα γραφείου Microsoft Office 365 (Hotmail, 1996) (Salesforce.com, 1999) (Microsoft Office 365, 2011). Σύμφωνα με έρευνα των Chung και Hermans, η άποψη της πλειοψηφίας των υπευθύνων λήψης αποφάσεων εντός των οργανισμών τεχνολογίας, αναφέρεται στο πεδίο του cloud computing ως ένα σημαντικό μελλοντικό μοντέλο στο πεδίο της πληροφορικής (Chung and Ermans, 2010)

Σύμφωνα με τους Birman, Chockler και van Renesse, το πεδίο του cloud computing θέτει ιδιαίτερα ενδιαφέροντα ερευνητικά ερωτήματα και ευκαιρίες (Birman, Chockler and van Renesse, 2009). Εκτός αυτού του γεγονότος, σύμφωνα με τους Boroujerdi και Nazem «το Cloud Computing μειώνει το κόστος συντήρησης λογισμικού και υλικού στις επιχειρήσεις». (Boroujerdi and Nazem, 2009). Οι οργανισμοί που χρησιμοποιούν την λειτουργία του cloud computing, μπορούν να μειώσουν τις επιχειρησιακές δαπάνες. Το κόστος του υλικού, του λογισμικού και των υπηρεσιών χρεώνεται με βάση ένα βοηθητικό πρόγραμμα ή βάση συνδρομής.

Παρόλο που το cloud computing προσφέρει μεγάλη ευκολία στους χρήστες απαλλάσσοντας αυτούς από την ανάγκη κατανόησης των λεπτομερειών επεξεργασίας του συστήματος, τους αναγκάζει να εμπιστεύονται τον πάροχο υπηρεσιών cloud (CSP), κάτι που τους ανησυχεί αρκετά, δηλαδή την ασφάλεια. (Okuhara, Shiozaki and Suzuki, 2010). Η ασφάλεια είναι το κύριο εμπόδιο για πολλούς οργανισμούς στη μετακίνησή τους την λειτουργία του cloud computing (Okuhara, Shiozaki and Suzuki, 2010)

Εξετάζοντας προηγούμενες έρευνες, διευκρινίζεται ότι η λειτουργία του cloud computing είναι ένα αυξανόμενο φαινόμενο που παρέχει ενδιαφέρουσες ευκαιρίες για οργανισμούς καθώς και για ερευνητικούς σκοπούς. Εκτός αυτού, η ασφάλεια και ο παράγοντας εμπιστοσύνης στην λειτουργία του cloud computing, είναι σημαντικά εμπόδια για τους οργανισμούς στη χρήση του. Η ισχυρή διαχείριση ταυτότητας και πρόσβασης (IAM) είναι μία από τις απαιτήσεις για την ελαχιστοποίηση των ανησυχιών για την ασφάλεια στην λειτουργία του cloud computing (Gopalakrishnan, 2009).

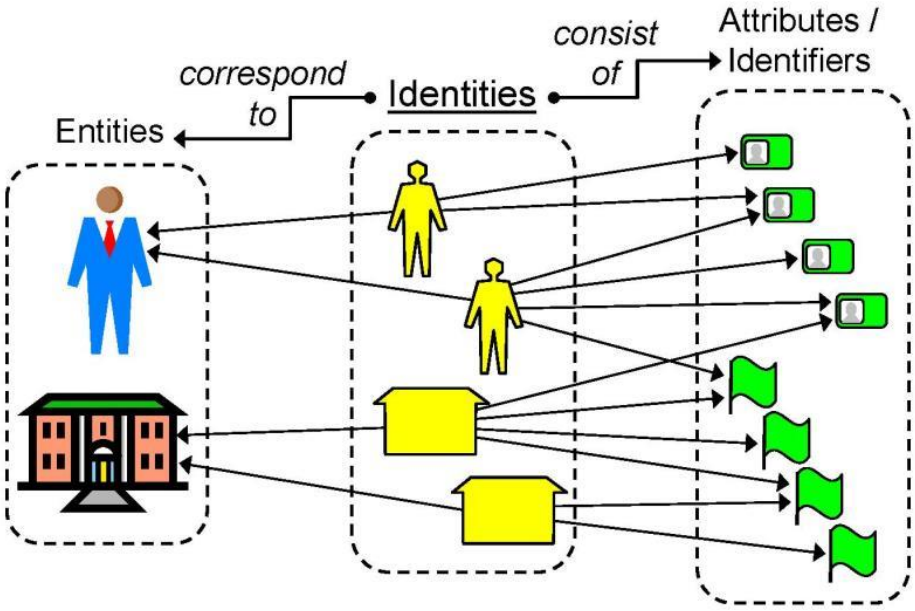
Με τον αυξανόμενο όγκο δεδομένων, των διαφόρων χρηστών και των ρόλων σε σύγχρονους οργανισμούς, ο έλεγχος της πρόσβασης στα δεδομένα, γίνεται όλο και πιο σημαντικός. Εκτός αυτού, οι κανόνες και οι κανονισμοί για την αποθήκευση δεδομένων των οργανισμών, έχουν γίνει αυστηρότεροι τα τελευταία χρόνια (Harauz, Kaufman and Potter, 2009). Αυτό το μέρος της διαχείρισης ασφάλειας εντός των επιχειρήσεων, είναι σχετικό με την λειτουργία του cloud computing.

Η αυξανόμενη δημοτικότητα της όποιας εξωτερικής επεξεργασίας και αποθήκευσης δεδομένων, εγείρει πολυάριθμες προκλήσεις για τους οργανισμούς που θέλουν να επεκτείνουν τις πολιτικές διακυβέρνησης πρόσβασης πέρα από τα τείχη προστασίας του οργανισμού τους στο cloud, ειδικά για τη διαχείριση δεδομένων και τις υπηρεσίες εξωτερικής ανάθεσης (Ponemon Institute, 2010)

Όταν χρησιμοποιεί κανείς την λειτουργία του cloud computing, μέρος των δεδομένων του οργανισμού, δεν αποθηκεύεται πλέον σε συσκευές που διαχειρίζεται. Αυτό το γεγονός αυξάνει τους κινδύνους μη εξουσιοδοτημένης πρόσβασης και αλλάζει τον τρόπο με τον οποίο μπορεί να εκτελεστεί η διαχείριση από μέρους των χρηστών. Η λειτουργία του cloud computing έχει μια σειρά από νέες διαστάσεις που η τρέχουσα κατάσταση της λειτουργίας Identity and Access Management δεν πληροί (Gopalakrishnan, 2009). Αυτές οι πρόσφατες

εξελίξεις καθιστούν τον συνδυασμό της λειτουργίας αυτής για το cloud computing, ένα ενδιαφέρον αντικείμενο έρευνας.

Η λειτουργία Identity and Access Management σχετίζεται, όπως αναφέρθηκε, με τη διαχείριση της πρόσβασης των ταυτοτήτων σε δεδομένα. Σύμφωνα με τους Jøsang και Pope, η ταυτότητα είναι μια αναπαράσταση μιας οντότητας σε έναν συγκεκριμένο τομέα εφαρμογής (Jøsang and Pope, 2005).Οι ταυτότητες συνδέονται με ένα σύνολο χαρακτηριστικών που τις καθορίζουν εντός του συγκεκριμένου τομέα εφαρμογής. Παραδείγματα χαρακτηριστικών, που ονομάζονται επίσης αναγνωριστικά στοιχεία, είναι το όνομα, η ημερομηνία γέννησης ή το αναγνωριστικό λογαριασμού (Harauz, Kaufman and Potter, 2009). Μια οντότητα μπορεί να έχει μία ή πολλές ταυτότητες σε έναν συγκεκριμένο τομέα εφαρμογής και κάθε ταυτότητα μπορεί να έχει πολλαπλά αναγνωριστικά και πρέπει να έχει τουλάχιστον ένα μοναδικό αναγνωριστικό εντός του συγκεκριμένου τομέα εφαρμογής (Jøsang and Pope, 2005). Αυτό το μοναδικό αναγνωριστικό επιτρέπει την αναγνώριση μιας ταυτότητας (Εικόνα No.3).



Εικόνα No.3: Αντιστοιχία μεταξύ οντοτήτων, ταυτοτήτων και αναγνωριστικών στοιχείων στη λειτουργία του Cloud Περιβάλλοντος(Jøsang & Pope, 2005).

Η λειτουργία του Identity and Access Management είναι η διαδικασία διαχείρισης σχετικά με το ποιος έχει πρόσβαση σε ποιες πληροφορίες και για πόσο χρονικό διάστημα (Jøsang and Pope, 2005). Η λειτουργία του Identity and Access Management είναι το σύστημα διαχείρισης, διεργασιών και υποστήριξης που διαχειρίζεται ποιοι χρήστες (άτομα,

εφαρμογές και συστήματα) έχουν πρόσβαση σε πληροφορίες, πόρους πληροφορικής και φυσικούς πόρους και τι είναι εξουσιοδοτημένος να κάνει κάθε χρήστης με αυτούς τους πόρους (Gopalakrishnan, 2009).

4.2 Οι Ανάγκες των Επιχειρήσεων να Ανταποκριθούν στην Προστασία των Δεδομένων τους Καθώς και στην Λειτουργία Αυτών στο Πεδίο του Cloud

Με σκοπό λοιπόν να ανταποκριθούν στις ανάγκες τους καθημερινά οι επιχειρήσεις, η λειτουργία στο cloud computing γίνεται πιο απαραίτητη για αυτές. Η τρέχουσα δημοτικότητα των υπηρεσιών στην λειτουργία στο cloud computing, οφείλεται στην προσβασιμότητα και την αποδοτικότητά τους. Αυτό το γεγονός επιτυγχάνεται μέσω μιας ποικιλίας προσαρμόσιμων μοντέλων υπηρεσιών όπως τα IaaS, SaaS, PaaS και multi-tenancy. Οι κίνδυνοι που συνδέονται με αυτά τα μοντέλα υπηρεσιών, όσον αφορά το απόρρητο και την ασφάλεια, είναι σημαντικοί (Comer, 2021)

Για να μειώσουν τους κινδύνους που σχετίζονται με τις υπηρεσίες στο πεδίο Web cloud, οι επιχειρήσεις χρειάζονται μια αξιόπιστη λύση διαχείρισης ταυτότητας και πρόσβασης (IAM) που να είναι ισχυρή, προσαρμόσιμη, επεκτάσιμη και υπεύθυνη για τους χρήστες. Η ενοποίηση του ελέγχου ταυτότητας και του ελέγχου πρόσβασης βάσει χαρακτηριστικών, βελτιώνει την απόδοση της εφαρμογής στο πεδίο του Web cloud, αποτρέποντας τη μη εξουσιοδοτημένη πρόσβαση (Dotson, 2019).

Καθώς η ψηφιακή τεχνολογία συνεχίζει να αναπτύσσεται με ρυθμό χωρίς προηγούμενο και το Διαδίκτυο των Πραγμάτων (IoT) αναμένεται να συνδέσει περισσότερες από 200 δισεκατομμύρια συσκευές έως το 2025, οι εταιρείες αντιμετωπίζουν ένα ταχέως μεταβαλλόμενο τεχνολογικό σενάριο που έχει επηρεάσει σημαντικά τα συμβατικά πλαίσια λειτουργίας των επιχειρήσεων. Η ολοένα και μεγαλύτερη υιοθέτηση και ο αυξανόμενος αριθμός ψηφιακών ταυτοτήτων, διαφορετικών φορητών συσκευών, αλλάζουν τα επιχειρηματικά μοντέλα, τα κοινωνικά πρότυπα, τους νόμους και το τοπίο πολιτικής σε κάθε εταιρεία και κοινωνία.

Καθώς οι επιχειρήσεις προσαρμόζονται σε αυτές τις τεχνολογικές εξελίξεις, πολλές επιθυμούν να έχουν σχετικά πλεονεκτήματα στο πεδίο του cloud, όπως συντήρηση zero+, την απλότητα πρόσβασης στις εφαρμογές και την ελευθερία επιλογής και χρήσης των λειτουργιών που ταιριάζουν στις λειτουργίες τους. Από την άλλη πλευρά, τα ετερογενή τοπία

που περιλαμβάνουν συστήματα εσωτερικής εγκατάστασης, το cloud και μια ποικιλία συσκευών, εγείρουν αρκετές ανησυχίες για την ασφάλεια, ειδικά όταν πρόκειται για διαχείριση ταυτότητας και πρόσβασης σε συστήματα (Dotson, 2019).

Επιπλέον, οι νέοι και εξελισσόμενοι νόμοι περί απορρήτου, συχνά χρειάζονται αναθεώρηση των τρεχουσών διαδικασιών για να διασφαλιστεί ότι παραμένουν οι επιχειρήσεις παραμένουν συμμορφούμενες με εκείνους. Οι εταιρείες χρειάζονται μια ολοκληρωμένη, συνεπή και κεντρική στρατηγική για τη διαχείριση ταυτότητας και τον έλεγχο πρόσβασης για την επίλυση αυτών των ζητημάτων (Gopalakrishnan, 2009).

Πολλές επιχειρήσεις έχουν εφαρμόσει συστήματα διαχείρισης ταυτότητας και πρόσβασης (IAM) για να επωφεληθούν από τα πολλά πλεονεκτήματα του υπολογιστικού νέφους, ενώ παράλληλα μετριάζουν τους κινδύνους που σχετίζονται με ζητήματα απορρήτου και ασφάλειας. Η διαχείριση ταυτότητας και πρόσβασης (IAM) είναι η κατάσταση πειθαρχίας που διασφαλίζει ότι τα κατάλληλα άτομα έχουν πρόσβαση στους κατάλληλους πόρους την κατάλληλη στιγμή και για τους κατάλληλους λόγους (Habiba, et al., 2014). Εκτός από αυτό το γεγονός, τα συστήματα IAM προσφέρουν ασφάλεια για ευαίσθητες πληροφορίες που διατηρούνται στο πεδίο του cloud, επιτρέποντας την αξιοπιστία και τη χρηστικότητα του ελέγχου πρόσβασης πελατών, κάτι που είναι απαραίτητο για τον ιστότοπο οποιουδήποτε οργανισμού.

Η λειτουργία του IAM, από την άλλη πλευρά, δεν είναι πανάκεια, ούτε αμβλύνει όλες τις ανησυχίες για το απόρρητο και την ασφάλεια που σχετίζονται με το πεδίο του cloud. Επιπλέον, διαφορετικές ταυτότητες (ή διπλότυπες ταυτότητες) ενδέχεται να απαιτούνται από διάφορες εταιρείες εντός του πεδίου εφαρμογής του IAM. Στο πλαίσιο αυτό, πολλές έρευνες προσπαθούν να αξιολογήσουν ορθά την ύπαρξης της σχέσης μεταξύ λύσεων στο πεδίο του cloud και των συστημάτων διαχείρισης ταυτότητας. Παρά τα πολλά πλεονεκτήματα της ανταλλαγής πληροφοριών και σχετικών πόρων από μέρους των επιχειρήσεων, η συνεργασία μεταξύ διαφορετικών οργανισμών, αποτελεί πρόκληση λόγω της περίπλοκης συμμετοχής πολλών στοιχείων (Dotson, 2019).

Ένας σημαντικός παράγοντας αναφέρεται στις ανησυχίες για το απόρρητο και την ασφάλεια, που μπορεί να εμποδίσουν τις επιχειρήσεις να μοιράζονται τα δεδομένα τους, παρόλο που η χρήση και η πρόσβαση στους απαραίτητους πόρους, ωφελούν όλες τις ερευνητικές εγκαταστάσεις. Στις πιο σοβαρές περιπτώσεις, ο ενδιαφερόμενος μπορεί να

κλέψει την τεχνολογία, να εγκαταλείψει τη συνεργασία και να θέσει σε κίνδυνο τη ζωή του άλλου ενδιαφερόμενου που μοιράζεται την τεχνολογία μαζί του.

Η συνεργασία είναι απαραίτητη και συχνά απαραίτητη παρά τους κινδύνους που εμπεριέχονται, καθώς τα κοινά δεδομένα μπορεί να προσφέρουν τις απαραίτητες βασικές γνώσεις για το θέμα και μπορούν να βοηθήσουν στη διατύπωση των καταλληλότερων ερευνητικών ερωτημάτων προς όφελος ολόκληρης της κοινότητας. Επιπλέον, μπορεί να οδηγήσει στην έγκαιρη και προσανατολισμένη στον προϋπολογισμό υλοποίηση μεγάλων έργων τα οποία θα μπορούσαν να επηρεάσουν την επιστήμη, τη δημιουργικότητα, την κοινωνικοοικονομική και την απασχόληση (Harauz, Kaufman and Potter, 2009).

4.3 Ο Σύνθετος Ρόλος της Λειτουργία Διαχείρισης Ταυτότητας και Πρόσβασης Δεδομένων σε Επιχειρήσεις

Η λειτουργία διαχείρισης ταυτότητας και πρόσβασης δεδομένων σε επιχειρήσεις, περιγράφεται ως η διαδικασία ελέγχου του ποιος έχει πρόσβαση σε κρίσιμες πληροφορίες (Dotson, 2019). Οι πληροφορίες που χαρακτηρίζονται ως "ιδιωτικές ή προστατευμένες" μπορεί να περιλαμβάνουν μεταξύ άλλων, από προσωπικά στοιχεία υγείας έως πληροφορίες για πιστωτικές και χρεωστικές κάρτες. Όλες οι πληροφορίες πρέπει να προστατεύονται από παραβιάσεις της κυβερνοασφάλειας, οι οποίες περιλαμβάνουν παράνομη πρόσβαση σε συστήματα.

Είναι σημαντικό να ελέγχεται ποιος έχει πρόσβαση σε προστατευμένα δεδομένα για τη διατήρηση κατάλληλων πρακτικών ασφάλειας στον κυβερνοχώρο, ακόμη και αν οι πληροφορίες διατηρούνται στο cloud. Η διαχείριση μεμονωμένων χρηστών (IAM) ασχολείται με τη διαχείριση των ρόλων, των εξουσιοδοτήσεων πρόσβασης και των αναγκών μεμονωμένων χρηστών σε ένα εταιρικό σύστημα πληροφορικής. Η πιο σημαντική δουλειά είναι η δημιουργία μιας ψηφιακής ταυτότητας για κάθε άτομο (Dotson, 2019). Είναι απαραίτητο να διατηρείται, να ενημερώνεται και να παρακολουθείται η ταυτότητα ενός χρήστη καθ' όλη τη διάρκεια της ζωής του μετά την καθιέρωσή της.

Η λειτουργία διαχείρισης ταυτότητας και πρόσβασης δεδομένων σε επιχειρήσεις, είναι ένα από τα πιο σημαντικά στοιχεία για τη διατήρηση της ασφάλειας δεδομένων στο

cloud. Η πρακτική της αποθήκευσης δεδομένων στο cloud γίνεται πιο κοινή. Τα συστήματα που βασίζονται στο πεδίο αυτό, είναι εύκολα στη χρήση και παρέχουν αρκετό χώρο αποθήκευσης, αλλά μπορεί επίσης να είναι επιρρεπή σε επιθέσεις λόγω της ανοιχτής φύσης τους. Οι χάκερς αποκτούν πρόσβαση στα δεδομένα με διάφορους τρόπους, μεταξύ άλλων μέσω του cloud (Mather, Kumaraswamy and Latif, 2009) . Είναι επίσης πιθανό η πλατφόρμα να καταστήσει πιο δύσκολο για τις επιχειρήσεις τον έλεγχο της πρόσβασης στο δίκτυο.

Σύμφωνα με τα παραπάνω, το cloud computing επιτρέπει στις επιχειρήσεις να εξισορροπούν την ποσότητα χωρητικότητας που χρειάζονται ενώ πληρώνουν για τις υπηρεσίες που χρησιμοποιούν κάθε μήνα (Marinescu, 2013). Όταν πρόκειται για υπηρεσίες ηλεκτρονικών υπολογιστών, το cloud computing είναι ένα παράδειγμα που επιτρέπει την πανταχού παρούσα, πρακτική, κατ' απαίτηση πρόσβαση στο δίκτυο σε μια κοινόχρηστη δεξαμενή προσαρμόσιμων υπολογιστικών πόρων που μπορούν να παρασχεθούν εύκολα και ακόμη και να απελευθερωθούν με μικρή διαχείριση ή συμμετοχή από παρόχους υπηρεσιών. Τέσσερις τύποι ανάπτυξης και τρία μοντέλα υπηρεσιών περιλαμβάνουν το μοντέλο υπολογιστικού νέφους, το οποίο αποτελείται από πέντε κύρια χαρακτηριστικά και πέντε υπό χαρακτηριστικά (Mather, Kumaraswamy and Latif, 2009).

Το cloud computing στοχεύει στην επίτευξη της εικονικοποίησης των πόρων ενώ ταυτόχρονα αυξάνει τη συνολική ικανότητα επεξεργασίας ενός συστήματος. Με την εισαγωγή του cloud computing, έχει καθιερωθεί ένα ολοκαίνουργιο πρότυπο που επιτρέπει στους χρήστες να αποθηκεύουν ή να δημιουργούν δυναμικά προγράμματα ενώ έχουν πρόσβαση σε αυτά από οπουδήποτε και ανά πάσα στιγμή μέσω της χρήσης μιας σύνδεσης δικτύου. Ως αποτέλεσμα της ικανότητάς του να παρέχει υπηρεσίες σε συστήματα υπολογιστών, αποθήκευσης και λογισμικού, το cloud computing έχει αποκτήσει ευρεία δημοτικότητα τόσο μεταξύ των επιχειρήσεων όσο και των ανθρώπων.

Το cloud computing βοηθά στην άμβλυνση του περιορισμού της υποδομής που αντιμετωπίζουν οι πελάτες παρέχοντας εφαρμογές πληρωμής ανά χρήση που είναι διαθέσιμες κατ' απαίτηση (Mather, Kumaraswamy and Latif, 2009). Στο cloud computing, οι πάροχοι υπηρεσιών cloud, αναλαμβάνουν την ευθύνη και εκτελούν τις απαραίτητες λειτουργίες για τη λειτουργία λογισμικού και υλικού για μεγιστοποίηση της απόδοσης. Η εμπορευματοποίηση του υπολογιστικού νέφους έχει οδηγήσει σε έναν ριζικό τύπο κατακόρυφης αποσύνθεσης, στην οποία η φυσική υποδομή αποσυνδέεται από το επίπεδο της πλατφόρμας και παρέχεται ως υπηρεσία.

Οι χρήστες μπορούν να προστεθούν, να τροποποιηθούν ή να αφαιρεθούν από ένα περιβάλλον υπολογιστικού νέφους (cloud) με τον ίδιο τρόπο που θα έκαναν σε ένα συμβατικό σύστημα πληροφορικής, εκτός από ορισμένες μικρές διαφορές. Για να είναι δυνατή η πρόσβαση στους επιτρεπόμενους πόρους ενός συστήματος, πρέπει να προστεθούν, να ενημερωθούν ή να διαγραφούν χρήστες από το σύστημα. Στη συμβατική προσέγγιση, η λειτουργία διαχείρισης ταυτότητας και πρόσβασης δεδομένων σε επιχειρήσεις, διαχειρίζεται, ελέγχεται και ρυθμίζεται από τις εγκαταστάσεις της εταιρείας (Comer, 2021).

Οι χρήστες μπορούν να έχουν πρόσβαση σε τοπικές υπηρεσίες, όπως δεδομένα και εφαρμογές, πραγματοποιώντας σύνδεση με το όνομα χρήστη και τον κωδικό πρόσβασής τους. Η εταιρεία που κάνει χρήση των υπηρεσιών cloud συχνά δεν είναι υπεύθυνη για τη διαδικασία διαχείρισης ελέγχου ταυτότητας. Ο μεγάλος όγκος του ελέγχου ταυτότητας πραγματοποιείται στο cloud, κάτι που είναι βολικό. Οι περισσότεροι πάροχοι υπηρεσιών cloud χρησιμοποιούν τη μέθοδο ελέγχου ταυτότητας για να επιτρέπουν στους πελάτες να έχουν πρόσβαση στις υπηρεσίες τους που βασίζονται σε σύννεφο.

Σε ένα περιβάλλον υπολογιστικού νέφους, οι πόροι στους οποίους μπορούν να έχουν πρόσβαση οι χρήστες καθορίζονται από την επιχείρηση που χρησιμοποιεί τις υπηρεσίες υπολογιστικού νέφους. Όταν ένας οργανισμός κάνει χρήση υπηρεσιών cloud, τόσο οι πάροχοι υπηρεσιών cloud όσο και οι εταιρείες που κάνουν χρήση των υπηρεσιών cloud έχουν εννέα (9) μοντέλα εξουσιοδότησης που διαφέρουν μεταξύ τους (Comer, 2021). Επιπλέον, δεδομένου ότι οι πάροχοι υπηρεσιών cloud ελέγχουν την πρόσβαση στις υπηρεσίες τους, ο οργανισμός που χρησιμοποιεί το cloud s Η υπηρεσία δεν έχει την εξουσία να επιβάλλει τους κανόνες ασφαλείας της έναντι των υπηρεσιών των παρόχων υπηρεσιών cloud.

Η λειτουργία διαχείρισης ταυτότητας και πρόσβασης δεδομένων σε επιχειρήσεις, καθοδηγείται κυρίως από την ανάγκη βελτίωσης της εμπειρίας χρήστη και προστασίας των προσωπικών πληροφοριών. Η διαδικασία διαχείρισης των χρηστών, θα απλοποιηθεί χάρη στην ομόσπονδη διαχείριση ταυτότητας. Οι χρήστες από έναν τομέα μπορούν να έχουν πρόσβαση με ασφάλεια σε πόρους από έναν άλλο τομέα μέσω της χρήσης του παραδείγματος της ομοσπονδίας, το οποίο εξαλείφει την ανάγκη για πολλαπλές διαδικασίες σύνδεσης.

Στο σημερινό περιβάλλον, οι άνθρωποι πρέπει να λαμβάνουν μέτρα για να προστατεύουν τις ευαίσθητες και ιδιωτικές τους πληροφορίες από ανεπιθύμητη πρόσβαση. Οι λίστες ελέγχου πρόσβασης, η κρυπτογράφηση τόμου και αρχείων, καθώς και τα

δικαιώματα αρχείων Unix είναι μερικές μόνο από τις τεχνικές που χρησιμοποιούνται συχνά για τη διατήρηση ιδιωτικών πληροφοριών. Η ακεραιότητα, από την άλλη πλευρά, έχει σχεδιαστεί για να αποτρέπει τη διαγραφή ή την αλλαγή δεδομένων χωρίς άδεια.

Η ικανότητα αντιστροφής της βλάβης όταν ένα εξουσιοδοτημένο άτομο κάνει μια τροποποίηση που δεν θα έπρεπε να έχει γίνει, αναφέρεται ως "ακέραια". Ακόμα κι αν ο στόχος της διαθεσιμότητας είναι η προστασία των πληροφοριών και η διάθεση τους όταν είναι απαραίτητο, είναι επίσης απαραίτητο οι διαδικασίες ελέγχου ταυτότητας, τα δίκτυα πρόσβασης και τα συστήματα να λειτουργούν όπως προβλέπεται. Η εμπιστευτικότητα ενισχύεται στο παράδειγμα της ομοσπονδιακής ταυτότητας με τους ακόλουθους τρόπους: τρίτα μέρη δεν έχουν πρόσβαση σε απλό κείμενο σε διαπιστευτήρια ή χαρακτηριστικά χρήστη και δεν θα μπορέσουν ποτέ να αποκτήσουν κλειδιά αποκρυπτογράφησης (Mather, Kumaraswamy and Latif, 2009).

Μια εχθρική επίθεση man-in-the-middle δεν θα έθετε σε κίνδυνο τα δεδομένα ενός πιστοποιημένου χρήστη και θα ήταν αδύνατο να αποκτηθεί μη εξουσιοδοτημένη πρόσβαση σε δεδομένα συναλλαγών σε ένα τέτοιο σενάριο. Η ακεραιότητα, από την άλλη πλευρά, ενισχύεται με τους εξής τρόπους: το εμπιστευόμενο μέρος έχει την πεποίθηση ότι τα δεδομένα δεν έχουν αλλάξει από τον κόμβο ή από κακόβουλο τρίτο μέρος. και Όταν χρησιμοποιείτε παρόχους υπηρεσιών διαπιστευτηρίων, το στηριζόμενο μέρος μπορεί να είναι σίγουρο ότι τα δεδομένα παρέχονται από γνήσιο πάροχο υπηρεσιών διαπιστευτηρίων και ότι ένα εχθρικό τρίτο μέρος δεν θα υποδυθεί έναν νόμιμο χρήστη και δεν θα επαναλάβει προηγουμένως έγκυρες αξιώσεις.

4.4 Υιοθέτηση του Cloud Computing και του Ψηφιακού Μετασχηματισμού στις Επιχειρήσεις

Με την αυξανόμενη χρήση των υπηρεσιών του cloud, τη συνεχή ανάγκη να παρακολουθούμε την καινοτομία και την ανάγκη κάθε επιχείρησης να δημιουργεί εφαρμογές, η τεχνολογία των πληροφοριών έρχεται αντιμέτωπη με μια σειρά από νέα και δύσκολα ζητήματα. Στόχος των σημερινών ομάδων πληροφορικής είναι να ενισχύουν συνεχώς την

αποτελεσματικότητα και την ασφάλεια τόσο για τις εσωτερικές τους λειτουργίες όσο και για τους τελικούς χρήστες, οι οποίοι είναι πελάτες της εταιρείας (Comer, 2021).

Οποιοσδήποτε διευθυντής πληροφορικής που έχει επιφορτιστεί με τον εκσυγχρονισμό της εταιρείας του, έχει να διαχειριστεί πολλές προκλήσεις, συμπεριλαμβανομένης της ενσωμάτωσης νέων εργαζομένων, της διαχείρισης των πολλών διαφορετικών κύκλων ζωής ταυτότητας και της επίβλεψης μιας χρονοβόρας διαδικασίας offboard που μπορεί να εκθέσει τον οργανισμό σε σημαντικές απειλές για την ασφάλεια.

Η εφαρμογή ενός προγράμματος διαχείρισης ταυτότητας και πρόσβασης δεδομένων σε επιχειρήσεις, έχει πολλά οφέλη, αλλά συνοδεύεται από κινδύνους και δυσκολίες, που πρέπει να ληφθούν υπόψη. Ένας από τους σημαντικότερους κινδύνους είναι η χρήση λογισμικού ελέγχου ταυτότητας και πρόσβασης για την αποτροπή μη εξουσιοδοτημένης χρήσης του συστήματος, το οποίο είναι ένα από τα πιο κοινά σενάρια. Αυτό είναι το πιο πιεστικό ζήτημα για πολλές μεγάλες και μικρές επιχειρήσεις. Εάν τα στοιχεία ελέγχου πρόσβασης είναι κατεστραμμένα, οι χάκερ μπορεί να μπορούν να περιφέρονται ελεύθερα στο δίκτυο χωρίς να εντοπιστούν (Harauz, Kaufman and Potter, 2009).

Αυτό μπορεί να περιλαμβάνει την απόκτηση πρόσβασης σε εμπιστευτικές ή προστατευμένες πληροφορίες (PPI). Αυτό ισχύει ιδιαίτερα με το cloud computing, όπου ο κίνδυνος είναι μεγαλύτερος. Εάν υπάρχουν περισσότερα σημεία πρόσβασης, μπορεί να είναι ευκολότερο για τους χάκερ να διεισδύσουν στο σύστημα εάν οι διαδικασίες ελέγχου ταυτότητας δεν είναι αποτελεσματικές και αποτελεσματικές. Πολλές εταιρείες αντιμετωπίζουν ένα δύσκολο έργο όταν προσπαθούν να δημιουργήσουν ένα πρόγραμμα διαχείρισης ταυτότητας και πρόσβασης δεδομένων σε επιχειρήσεις,.

Οι επαγγελματίες στον τομέα της κυβερνοασφάλειας μπορούν να βοηθήσουν τις εταιρείες στην εφαρμογή ενός προγράμματος διαχείρισης ταυτότητας και πρόσβασης. Με αυτόν τον τρόπο, το προσωπικό πληροφορικής θα μπορεί να συνεχίσει να παρακολουθεί τις τρέχουσες διαδικασίες. Παρά τους κινδύνους και τις δυσκολίες, τα πλεονεκτήματα της εφαρμογής ενός προγράμματος IAM υπερβαίνουν κάθε πιθανό μειονέκτημα.

Αρκετές επιχειρήσεις στις Ηνωμένες Πολιτείες για παράδειγμα, επανεξετάζουν τις συμβατικές μεθόδους τους για τη διατήρηση της ψηφιακής τους ταυτότητας, ως αποτέλεσμα της συνεχούς ανάπτυξης υπηρεσιών που βασίζονται σε cloud. Καθώς οι επιχειρήσεις

μεταφέρουν τις επιχειρηματικές τους δραστηριότητες στο cloud, οι οργανισμοί πρέπει να ελέγχουν την πρόσβαση στα δίκτυα των παρόχων υπηρεσιών cloud και εντός αυτών. Οι τοποθεσίες φιλοξενίας υπηρεσιών ταυτότητας γίνονται λιγότερο σημαντικές καθώς περισσότερες εταιρείες χρησιμοποιούν την έννοια της ασφάλειας Zero Trust, όπως η επαλήθευση ταυτότητας και οι περιορισμοί περιβάλλοντος δικτύου, ως μέρος της συνολικής στρατηγικής ασφαλείας τους.

Οι υπηρεσίες διαχείρισης ταυτότητας παρέχονται από εταιρείες υποδομής cloud, όπως το Amazon Web Services (AWS), το Microsoft Azure και το Google Cloud, αναγκαστικά (Dotson, 2019). Οι εφαρμογές με εξωτερική όψη που λειτουργούν σε υποδομές cloud που φιλοξενούν χρειάζονται την πλήρη υποστήριξη της αρχιτεκτονικής OpenID Connect (OIDC) από τον πάροχο υποδομής cloud για την υποστήριξη υπηρεσιών cloud με πλούσια διεπαφή χρήστη. Οι υπηρεσίες εσωτερικής και εξωτερικής ταυτότητας, είναι δύο από τις πιο βασικές πτυχές των υπηρεσιών ταυτότητας cloud (Mather, Kumaraswamy and Latif, 2009). Η ταυτότητα ως υπηρεσία προσφέρει τον καλύτερο δρόμο μπροστά για την πλειονότητα των επιχειρήσεων που επιδιώκουν να τοποθετηθούν για μακροπρόθεσμη επιτυχία.

Η συνεχής ανάπτυξη της οικονομίας του διαδικτύου, εξαρτάται από τη σωστή διαχείριση των διαδικτυακών πληροφοριών ταυτοποίησης. Όταν πρόκειται για τη διαχείριση ταυτότητας, είναι απαραίτητη μια ποικιλία ρυθμίσεων, συμπεριλαμβανομένων των επιχειρήσεων, του ηλεκτρονικού εμπορίου και της κυβέρνησης, καθώς στηρίζει τις εταιρικές λειτουργίες και υπηρεσίες, καθώς και επιτρέπει ψηφιακές αλληλεπιδράσεις και συναλλαγές από την οπτική γωνία του καταναλωτή. Οι επιχειρήσεις και οι πελάτες του δικτύου τους επωφελούνται από την ομοσπονδία ταυτότητας δεδομένου ότι παρέχει τόσο οικονομικά όσο και πλεονεκτήματα ευκολίας (Erl, Puttini and Zaigham, 2013).

Για παράδειγμα, πολλές εταιρείες μπορεί να συγκεντρώσουν τους πόρους τους για να χρησιμοποιήσουν μια ενιαία εφαρμογή, οδηγώντας σε εξοικονόμηση κόστους και ενοποίηση πόρων. Οι οργανισμοί που συνεργάζονται σε ένα έργο μπορούν να δημιουργήσουν μια ομοσπονδία ταυτότητας για να διευκολύνουν όλους τους χρήστες του να έχουν πρόσβαση και να μοιράζονται πόρους σε ολόκληρο τον οργανισμό.

Ως αποτέλεσμα, οι χρήστες χρειάζεται να συνδεθούν μόνο μία φορά για να μοιράζονται πληροφορίες σε όλους τους τομείς, αλλά οι διαχειριστές σε κάθε οργανισμό ενδέχεται να εξακολουθούν να διαχειρίζονται τον βαθμό πρόσβασης σε πόρους εντός των

αντίστοιχων τομέων τους. Αυτή η στρατηγική έχει τη δυνατότητα εξοικονόμησης χρημάτων, ενώ ταυτόχρονα ενοποιεί τους πόρους της επιχείρησης.

4.5 Προστασία Προσωπικών Δεδομένων από τις Επιχειρήσεις σε Νομικό Επίπεδο με το Νέο Κανονισμό GDPR

4.5.1 Η Επιρροή του GDPR στην Προστασία Προσωπικών Δεδομένων: Δικαιώματα, Συμμόρφωση και Μέτρα Ασφάλειας

Προσωπικά δεδομένα, γνωστά και ως προσωπικά στοιχεία ταυτοποίησης (ΠΣΤ) είναι οποιαδήποτε πληροφορία σχετίζεται με ένα αναγνωρίσιμο πρόσωπο. Η συντομογραφία ΠΣΤ, είναι ευρέως αποδεκτή στις Ηνωμένες Πολιτείες, αλλά οι σχετικές βασίζονται σε προσωπικές ή προσωπικές και αναγνωρίσιμες ή ταυτοποιήσιμες (Mather, Kumaraswamy and Latif, 2009). Σύμφωνα με τα ευρωπαϊκά και άλλα καθεστώτα προστασίας δεδομένων, τα οποία επικεντρώνονται κυρίως στον Γενικό Κανονισμό για την Προστασία Δεδομένων (GDPR), ο όρος "προσωπικά δεδομένα" είναι σημαντικά ευρύτερος και καθορίζει το πεδίο εφαρμογής του ρυθμιστικού καθεστώτος (Kosta, 2013)

Το Εθνικό Ινστιτούτο Προτύπων και Τεχνολογίας, ορίζει τις πληροφορίες προσωπικής ταυτοποίησης ως «οποιεσδήποτε πληροφορίες σχετικά με ένα άτομο που διατηρείται από μια υπηρεσία, συμπεριλαμβανομένων (1) οποιασδήποτε πληροφορίας που μπορεί να χρησιμοποιηθεί για τη διάκριση ή τον εντοπισμό της ταυτότητας ενός ατόμου, όπως π.χ. όνομα, αριθμός κοινωνικής ασφάλισης, ημερομηνία και τόπος γέννησης, πατρικό όνομα της μητέρας ή βιομετρικά αρχεία και (2) κάθε άλλη πληροφορία που συνδέεται ή συνδέεται με ένα άτομο, όπως ιατρικές, εκπαιδευτικές, οικονομικές και εργασιακές πληροφορίες». Για παράδειγμα, η διεύθυνση IP ενός χρήστη δεν ταξινομείται ως ΠΣΤ από μόνη της, αλλά ταξινομείται ως συνδεδεμένο ΠΣΤ (Lynskey, 2015)

Τα προσωπικά δεδομένα ορίζονται σύμφωνα με τον GDPR ως "κάθε πληροφορία που σχετίζεται με ταυτοποιημένο ή ταυτοποιήσιμο φυσικό πρόσωπο". Η διεύθυνση IP ενός συνδρομητή στο Διαδίκτυο μπορεί να ταξινομηθεί ως προσωπικά δεδομένα. Η έννοια των ΠΣΤ έχει γίνει διαδεδομένη καθώς η τεχνολογία πληροφοριών και το Διαδίκτυο έχουν διευκολύνει τη συλλογή ΠΣΤ, οδηγώντας σε μια κερδοφόρα αγορά στη συλλογή και μεταπώληση ΠΣΤ. Ως απάντηση σε αυτές τις απειλές, πολλές πολιτικές απορρήτου

ιστοτόπων αντιμετωπίζουν συγκεκριμένα τη συγκέντρωση ΠΣΤ και νομοθέτες όπως το Ευρωπαϊκό Κοινοβούλιο έχουν θεσπίσει μια σειρά νομοθετημάτων όπως ο Γενικός Κανονισμός για την Προστασία Δεδομένων (GDPR) για τον περιορισμό της διανομής και της προσβασιμότητας των ΠΣΤ ((Kosta, 2013).

Ο κύριος στόχος του Νέου Κανονισμού GDPR – General Data Protection Regulation, είναι να προστατεύσει τους πολίτες της Ε.Ε. από οργανισμούς που χρησιμοποιούν παράνομα προσωπικά αναγνωρίσιμα στοιχεία (PII). Οι κυρώσεις για παραβιάσεις δεδομένων, έχουν επίσης αυξηθεί και οι επιχειρήσεις έχουν νέες απαιτήσεις για ειδοποιήσεις παραβίασης δεδομένων. Οι επιχειρήσεις που δεν συμμορφώνονται με το Νέο Κανονισμό GDPR, θα αντιμετωπίσουν κυρώσεις ύψους 20 εκατ. ευρώ ή 4% του συνολικού ετήσιου κύκλου εργασιών τους.

Οι νέοι κανόνες του GDPR, πρέπει επίσης να βοηθήσουν τους επιχειρησιακούς οργανισμούς να προετοιμάσουν τις σωστές πολιτικές και διαδικασίες για την αντιμετώπιση περιστατικών ασφάλειας στον κυβερνοχώρο. Επιπλέον, η εφαρμογή του Νέου Κανονισμού GDPR, θα αλλάξει τον τρόπο με τον οποίο οι οργανισμοί επεξεργάζονται και αποθηκεύουν προσωπικές αναγνωρίσιμες πληροφορίες. Τα δικαιώματα των πολιτών της Ε.Ε., πρόκειται να επεκταθούν και το GDPR ισχύει για όλους τους οργανισμούς που επεξεργάζονται τα προσωπικά αναγνωρίσιμα στοιχεία των κατοίκων της Ε.Ε. (Γενικός κανονισμός της ΕΕ για την προστασία των δεδομένων (GDPR), (Lynskey, 2015).

Επίσης η εφαρμογή του Νέου Κανονισμού GDPR, τυποποιεί την προστασία των προσωπικών αναγνωρίσιμων πληροφοριών σε κάθε ευρωπαϊκή χώρα. Οι οργανισμοί πρέπει να εξετάσουν το τι ακριβώς τα προσωπικά αναγνωρίσιμα στοιχεία, επεξεργάζονται και πώς πρέπει να το προστατεύσουν. Με την εφαρμογή του Νέου Κανονισμού GDPR, υπάρχουν διαφορετικοί ρόλοι για κάθε οργανισμό που είναι υπεύθυνος επεξεργασίας δεδομένων των ατόμων και πελατών του. Ο κάθε ελεγκτής πρέπει να καθορίσει τον τρόπο και τον λόγο για τον οποίο επεξεργάζεται τα προσωπικά αναγνωρίσιμα στοιχεία και επεξεργάζεται τον επεξεργαστή.

Ακόμη και οι επιχειρησιακές οργανώσεις εκτός της Ευρωπαϊκής Ένωσης που δραστηριοποιούνται στην επικράτεια αυτής, πρέπει να εφαρμόζουν τις απαιτήσεις του κανονισμού. Μετά την ημερομηνία λήξης του χρονικού περιθωρίου για την εφαρμογή του Νέου Κανονισμού GDPR, κάθε οργανισμός πρέπει να χειρίζεται τα προσωπικά δεδομένα

νόμιμα και με διαφάνεια. Επιπλέον, η επεξεργασία στα προσωπικά αναγνωρίσιμα στοιχεία, πρέπει να έχει πραγματικό σκοπό. Όταν οι προσωπικές αναγνωρίσιμες πληροφορίες δεν απαιτούνται πλέον, οι οργανισμοί θα πρέπει να τις καταργήσουν και ουσιαστικά να τις αποσύρουν από τα αρχεία τους (Pormeister, 2017)

Ένα πρόσωπο έχει το δικαίωμα πρόσβασης στις προσωπικές του πληροφορίες (PII), γεγονός που σημαίνει ότι ο υπεύθυνος του μητρώου μιας ιστοσελίδας που δραστηριοποιείται στο διαδικτυακό εμπόριο, πρέπει να ειδοποιήσει το φυσικό πρόσωπο σε περίπτωση επεξεργασίας οποιουδήποτε προσωπικά αναγνωρίσιμου στοιχείου και στη συνέχεια να παραδώσει ένα αντίγραφο των προαναφερθέντων δεδομένων (Lynskey, 2015)

Το Δικαίωμα Διόρθωσης Προσωπικών Πληροφοριών

Ο νέος κανονισμός GDPR παρέχει στα φυσικά πρόσωπα το δικαίωμα να απαιτούν διόρθωση για λανθασμένες πληροφορίες στα συστήματα του ιδιοκτήτη του μητρώου μιας ιστοσελίδας που δραστηριοποιείται στο διαδικτυακό εμπόριο (Pormeister, 2017).

Το Δικαίωμα Αφαίρεσης Προσωπικών Στοιχείων

Ένα πρόσωπο έχει το δικαίωμα να ζητήσει από τους κατόχους μητρώων μιας ιστοσελίδας που δραστηριοποιείται στο διαδικτυακό εμπόριο, να αφαιρέσουν τις προσωπικές πληροφορίες που έληξαν.

Επιπλέον, ένα άτομο έχει το δικαίωμα να ακυρώσει τη συγκατάθεσή του για την επεξεργασία δεδομένων. Επιπλέον, ένα άτομο έχει το δικαίωμα να ζητήσει τη διαγραφή των προσωπικών στοιχείων του, από τα συστήματα του ιδιοκτήτη του μητρώου. Στη συνέχεια τα δεδομένα, πρέπει να διαγραφούν εάν δεν υπάρχει κάποιος νόμιμος σκοπός για την αποθήκευση πια. Ο κανονισμός δεν προβλέπει απαιτήσεις από τεχνική άποψη για τη διαγραφή δεδομένων. Τουλάχιστον τα δεδομένα μπορούν να διαγραφούν, για παράδειγμα, αντικαθιστώντας το έτσι ώστε να μην μπορούν πλέον να αναγνωριστούν φυσικά πρόσωπα από τα δεδομένα.

Επίσης, τα δεδομένα μπορούν να επισημανθούν ως διαγραμμένα και στη συνέχεια να οριστούν περιορισμοί για τη χρήση τους σε συστήματα πληροφοριών. Ωστόσο, με αυτόν τον τρόπο τα δεδομένα εξακολουθούν να υπάρχουν, για παράδειγμα σε μια βάση δεδομένων. Παρ 'όλα αυτά, η καταστροφή των φυσικών συσκευών που θα αποθηκεύουν τα προσωπικά

αναγνωρίσιμα στοιχεία, μπορεί είναι υπερβολική, επειδή μπορεί να είναι δύσκολο να εντοπιστούν οι θέσεις των δεδομένων, π.χ. από τα συστήματα τεχνολογίας i-cloud. (Rumbold and Pierscionek, 2017)

Το Δικαίωμα Μεταφοράς Δεδομένων για τα Φυσικά Πρόσωπα

Το δικαίωμα στη φορητότητα δεδομένων, είναι επίσης μια νέα απαίτηση του νέου κανονισμού GDPR. Ένα άτομο έχει δικαιώματα να συγκεντρώνει όλες τις προσωπικές του πληροφορίες (PII) με κοινή δομημένη μορφή και στη συνέχεια να μεταφέρει αυτά τα δεδομένα σε άλλα συστήματα ελεγκτή καταχωρητών. Μια πτυχή αυτής της φορητότητας δεδομένων, είναι ότι ένα άτομο έχει δικαιώματα να μεταφέρει τα δεδομένα απευθείας από έναν ελεγκτή σε έναν άλλο, εάν αυτό είναι τεχνικά εφικτό.

Το δικαίωμα στη φορητότητα δεδομένων δεν σημαίνει ότι οι υπεύθυνοι επεξεργασίας ή επεξεργαστές πρέπει να σχεδιάζουν και να εφαρμόζουν συμβατά συστήματα. Όταν τα συστήματα είναι διαφορετικά, τα στοιχεία PII μπορεί να μεταφερθούν, χρησιμοποιώντας εξωτερική μνήμη αποθήκευσης και στη συνέχεια φόρτωσης σε άλλο σύστημα ελεγκτή καταχώρησης (Spindler and Schmechel, 2016)

Το Δικαίωμα Ενημέρωσης για Παραβιάσεις Δεδομένων

Μία ευθύνη για τους ελεγκτές καταχώρησης στοιχείων στο διαδίκτυο, είναι να ενημερώνουν τα εγγεγραμμένα πρόσωπα για παραβιάσεις δεδομένων, τα δεδομένα των οποίων έχουν διαρρεύσει. Το δικαίωμα ισχύει εάν η παραβίαση προκαλεί μεγάλους κινδύνους για τα προσωπικά στοιχεία και την ελευθερία ενός ατόμου. Οι προαναφερόμενοι κίνδυνοι είναι για παράδειγμα κλοπές ταυτότητας, απάτες πιστωτικών καρτών ή άλλες παράνομες δραστηριότητες.

Η ειδοποίηση δεν είναι υποχρεωτική, εάν οι πληροφορίες διαρροής προσωπικών στοιχείων ήταν κρυπτογραφημένες και τα κλειδιά κρυπτογράφησης δεν διαρρεύσαν. Ένας οργανισμός μπορεί να χρησιμοποιήσει τα κοινωνικά μέσα ενημέρωσης για την ενημέρωση σχετικά με την παραβίαση δεδομένων, εάν διαφορετικά μπορεί να προκαλέσει πάρα πολύ μεγάλο φόρτο εργασίας (Rumbold and Pierscionek, 2017)

Ο οργανισμός πρέπει να δώσει τα ακόλουθα στοιχεία σχετικά με τις παραβιάσεις δεδομένων στα υποκείμενα των οποίων τα δεδομένα έχουν διαρρεύσει (Spindler and Schmechel, 2016):

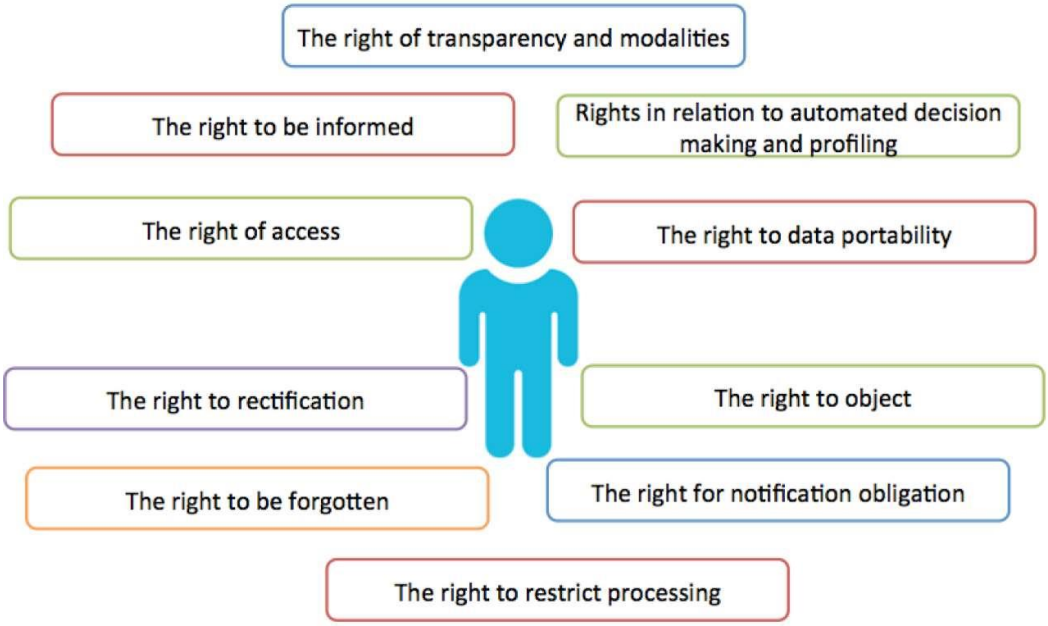
Σαφής και απλή περιγραφή της παραβίασης των δεδομένων

Στοιχεία επικοινωνίας για περισσότερες λεπτομέρειες

Μια περιγραφή των επιπτώσεων μιας παραβίασης δεδομένων μπορεί να προκαλέσει το δικαίωμα ενός ατόμου.

Μια περιγραφή των δραστηριοτήτων που ο ιδιοκτήτης του μητρώου έχει ήδη κάνει ή θα κάνει για τη μείωση των επιπτώσεων μιας παραβίασης των δεδομένων.

Το σχήμα No.1 απεικονίζει τα δικαιώματα των φυσικών προσώπων βάσει του GDPR



Σχήμα No.1 - Δικαιώματα του ατόμου υπό GDPR (Gunathunga, 2017)

Ο Κανονισμός GDPR περιέχει υποχρεώσεις για τους υπευθύνους και τους εκτελούντες την επεξεργασία δεδομένων. Πρώτον, πρέπει να υπακούουν στις ίδιες αρχές που ορίζονται στο άρθρο (Άρθρο 5 (1) (Union Council of the European, 2016)). Ωστόσο, ο υπεύθυνος επεξεργασίας δεδομένων είναι υπεύθυνος για την απόδειξη της συμμόρφωσης με

αυτές τις αρχές (άρθρο 5 παράγραφος 2 GDPR). Εάν δεν μπορεί να αποδείξει τη συμμόρφωση, κινδυνεύουν τα υψηλά πρόστιμα (Άρθρο 83 (5) (Union Council of the European, 2016)). Επιπλέον, σύμφωνα με την αρχή της ακεραιότητας και της εμπιστευτικότητας των δεδομένων, ο Κανονισμός GDPR υποχρεώνει τους υπεύθυνους επεξεργασίας και τους εκτελούντες την επεξεργασία να λαμβάνουν τα κατάλληλα τεχνικά και οργανωτικά μέτρα για να εξασφαλίσουν επαρκή προστασία των προσωπικών δεδομένων (άρθρο 5 (1) (Union Council of the European, 2016)).

Ο Κανονισμός GDPR καθορίζει αυτά τα μέτρα ασφαλείας (άρθρο 32 GDPR). Συνεπώς, τα προσωπικά δεδομένα θα πρέπει να είναι ψευδώνυμα και κρυπτογραφημένα (Άρθρο 32 (1) (Union Council of the European, 2016)). Επιπλέον, οι υπεύθυνοι επεξεργασίας και οι υπεύθυνοι επεξεργασίας πρέπει να διασφαλίζουν την εμπιστευτικότητα, την ακεραιότητα, τη διαθεσιμότητα και την ανθεκτικότητα των συστημάτων και των υπηρεσιών τους σε μόνιμη βάση και απαιτείται να αποκαθιστούν τη διαθεσιμότητα και την πρόσβαση των δεδομένων σε περίπτωση συμβάντος όσο το δυνατόν γρηγορότερα (άρθρο 32 παράγραφος 1) (Union Council of the European, 2016)). Επιπλέον, πρέπει να εφαρμόζουν διαδικασίες για την τακτική επανεξέταση των μέτρων ασφαλείας τους (άρθρο 32 παράγραφος 1 (Union Council of the European, 2016)).

Επιπλέον, όλοι οι υπεύθυνοι επεξεργασίας δεδομένων με τουλάχιστον 250 υπαλλήλους, απαιτείται να διατηρούν αρχείο όλων των δραστηριοτήτων επεξεργασίας δεδομένων τους και να το διαθέτουν στις εποπτικές αρχές κατόπιν αιτήματος (Άρθρο 30 (1, 2, 4) (Union Council of the European, 2016)). Αυτό περιλαμβάνει τους σκοπούς της επεξεργασίας, τις κατηγορίες προσωπικών δεδομένων, τα υποκείμενα των δεδομένων και τους αποδέκτες και τα μέτρα ασφαλείας που λαμβάνονται για την προστασία των δεδομένων (άρθρο 30 παράγραφος 1, (2) (Union Council of the European, 2016)).

Επίσης ο Κανονισμός GDPR παρέχει έναν πολύ πιο ολοκληρωμένο κατάλογο πληροφοριών που ο υπεύθυνος επεξεργασίας δεδομένων πρέπει να παρέχει στο υποκείμενο των δεδομένων (άρθρα 13, 14 (Union Council of the European, 2016)). Κυρίως, ο υπεύθυνος επεξεργασίας πρέπει να παρέχει στο υποκείμενο των δεδομένων τα στοιχεία επικοινωνίας του/της και του υπεύθυνου προστασίας δεδομένων (Άρθρο 13 παράγραφος 1, 14 (1) (Union Council of the European, 2016)). Επιπλέον, ο υπεύθυνος επεξεργασίας πρέπει να είναι σε θέση να παρουσιάσει τη νομική βάση της επεξεργασίας δεδομένων και – εάν συμβαίνει αυτό

– της μεταφοράς των δεδομένων σε τρίτη χώρα (άρθρο 13 παράγραφος 1, 14 (1) (Union Council of the European, 2016)).

Εάν τα δεδομένα συλλέγονται απευθείας από το υποκείμενο των δεδομένων, ο υπεύθυνος επεξεργασίας ενδέχεται επίσης να πρέπει να υποδείξει τα έννομα συμφέροντά του, τα οποία αποτελούν τη βάση για την επεξεργασία (άρθρο 13 παράγραφος 1 (Union Council of the European, 2016)). Εάν τα δεδομένα συλλέγονται από το υποκείμενο των δεδομένων έμμεσα, ο υπεύθυνος επεξεργασίας πρέπει να παρέχει πρόσθετες πληροφορίες σχετικά με τις κατηγορίες δεδομένων που επεξεργάζεται (άρθρο 14 (1) (Union Council of the European, 2016)). Και στα δύο σενάρια, ο υπεύθυνος επεξεργασίας πρέπει να παρέχει περαιτέρω πληροφορίες, σχετικά με τη φύση της επεξεργασίας και τα δικαιώματα του υποκειμένου των δεδομένων, στον βαθμό που είναι απαραίτητος για δίκαιη και διαφανή επεξεργασία δεδομένων (Άρθρο 13 (2), 14 (2) (Union Council of the European, 2016)).

Εάν τα δεδομένα δεν συλλέγονται απευθείας από το υποκείμενο των δεδομένων, ο υπεύθυνος επεξεργασίας πρέπει επίσης να υποδεικνύει την πηγή των δεδομένων (άρθρο 14 παράγραφος 2 (Union Council of the European, 2016)). Επιπλέον, εάν τα δεδομένα αποκτηθούν απευθείας, το υποκείμενο των δεδομένων ενδέχεται να πρέπει να ενημερωθεί γιατί υποχρεούται να παράσχει τα δεδομένα και ποιες θα ήταν οι συνέπειες της μη παροχής (άρθρο 13 (2) (Union Council of the European, 2016)). Ωστόσο, εάν η επεξεργασία δεδομένων βασίζεται σε δεδομένη συγκατάθεση, ο υπεύθυνος επεξεργασίας πρέπει να το διευκρινίσει και να ενημερώσει τον ενδιαφερόμενο ότι έχει το δικαίωμα να ανακαλέσει τη συγκατάθεση (Άρθρο 13 παράγραφος 2, 14 (2) (Union Council of the European, 2016)). Επιπλέον, πρέπει να παρέχονται πληροφορίες εάν ο αρχικός σκοπός της επεξεργασίας αλλάξει από τον υπεύθυνο επεξεργασίας (άρθρο 13 παράγραφος 3, 14 παράγραφος 4 (Union Council of the European, 2016))

Εάν τα δεδομένα προσωπικού χαρακτήρα συλλέγονται έμμεσα από το υποκείμενο των δεδομένων, αυτές οι διατάξεις ενδέχεται να καταργηθούν εάν οι δαπάνες είναι δυσανάλογες, εάν τα δεδομένα είναι εμπιστευτικά ή εάν η νομοθεσία απαιτεί ρητά τη συλλογή των δεδομένων (άρθρο 14 παράγραφος 5 (Union Council of the European, 2016)). Όλες οι παρεχόμενες πληροφορίες πρέπει να είναι διαθέσιμες σε γραπτή μορφή και να κοινοποιούνται σε σαφή και απλή γλώσσα (άρθρο 12 (1) (Union Council of the European, 2016)).

Ένα νέο χαρακτηριστικό του GDPR είναι η υποχρέωση ενημέρωσης του υποκειμένου των δεδομένων και της υπεύθυνης εθνικής νομοθεσίας για παραβιάσεις δεδομένων, οι οποίες θα μπορούσαν να αποτελέσουν απειλή για την ιδιωτική ζωή του ατόμου (Άρθρο 33, 34 (Union Council of the European, 2016)). Η κοινοποίηση στην εποπτική αρχή πρέπει να γίνει σε κάθε περίπτωση εντός 72 ωρών, διαφορετικά η καθυστέρηση πρέπει να αιτιολογείται εύλογα (άρθρο 33 (1) (Union Council of the European, 2016)). Το επηρεαζόμενο υποκείμενο των δεδομένων πρέπει να ενημερώνεται χωρίς αδικαιολόγητη καθυστέρηση, εάν η παραβίαση δεδομένων είναι πιθανό να θέσει σε κίνδυνο τα δικαιώματα του απορρήτου (άρθρο 34 (1) (Union Council of the European, 2016)).

Σε εξαιρετικές περιπτώσεις, δεν απαιτείται αναφορά στην εθνική νομοθεσία, εάν ο υπεύθυνος επεξεργασίας μπορεί να αποδείξει ότι, παρά την παραβίαση δεδομένων, δεν υπάρχει κίνδυνος για τα δικαιώματα και τις ελευθερίες του υποκειμένου των δεδομένων (άρθρο 33 παράγραφος 1 (Union Council of the European, 2016)). Οι πληροφορίες του υποκειμένου των δεδομένων δεν είναι απαραίτητες εάν ο υπεύθυνος επεξεργασίας μπορεί να αποδείξει ότι εφάρμοσε κατάλληλα τεχνικά μέτρα που εγγυώνται την ασφάλεια των προσωπικών δεδομένων (άρθρο 34 (1) (Union Council of the European, 2016)).

Σύμφωνα με όσα αναφέρθηκαν παραπάνω, θα λέγαμε πως η καινοτομία του GDPR είναι η υποχρέωση των υπευθύνων επεξεργασίας δεδομένων να διενεργούν εκτίμηση επιπτώσεων στην προστασία των δεδομένων πριν από την επεξεργασία, εάν είναι πιθανό να θέσει σε υψηλό κίνδυνο τα δικαιώματα και τις ελευθερίες των θιγόμενων ατόμων (άρθρο 35 (Union Council of the European, 2016)).

Μια τέτοια εκτίμηση επιπτώσεων πρέπει να διενεργείται, στην περίπτωση αυτοματοποιημένης επεξεργασίας δεδομένων, συμπεριλαμβανομένου του "προφίλ", εάν πρέπει να υποβληθεί σε επεξεργασία μεγάλης κλίμακας ειδικών κατηγοριών προσωπικών δεδομένων (άρθρο 9 (Union Council of the European, 2016)) ή σε περίπτωση εκτεταμένης βίντεο επιτήρησης δημόσιου χώρου προγραμματίζεται (άρθρο 35 (3) (Union Council of the European, 2016)). Εάν η εκτίμηση επιπτώσεων καταλήξει στο συμπέρασμα ότι η επεξεργασία θα έθετε σε κίνδυνο τα δικαιώματα προστασίας της ιδιωτικής ζωής, ο υπεύθυνος επεξεργασίας πρέπει να συμβουλευτεί την αρμόδια εποπτική αρχή και να λάβει μέτρα για τον μετριασμό του κινδύνου (άρθρο 36 (1) (Union Council of the European, 2016).

Επιπλέον, ο GDPR απαιτεί από τους υπευθύνους επεξεργασίας και τους εκτελούντες την επεξεργασία να ορίσουν έναν εσωτερικό υπεύθυνο προστασίας δεδομένων που παρακολουθεί τη συμμόρφωση με τις υποχρεώσεις προστασίας δεδομένων, συμβουλεύει τους υπευθύνους επεξεργασίας ή τους εκτελούντες την επεξεργασία και επικοινωνεί με την εποπτική αρχή (άρθρο 37, 39 (Union Council of the European, 2016)). Αυτή η υποχρέωση ισχύει ιδίως για δημόσιους φορείς, αλλά και για ορισμένους μη δημόσιους φορείς που ασχολούνται κυρίως με την εκτέλεση πράξεων επεξεργασίας δεδομένων (άρθρο 37 παράγραφος 1 (Union Council of the European, 2016)).

Τέλος, ο GDPR ενθαρρύνει τους υπευθύνους επεξεργασίας δεδομένων και τους εκτελούντες την επεξεργασία να εφαρμόζουν έναν κώδικα δεοντολογίας για τη διαχείριση των προσωπικών δεδομένων σύμφωνα με τον GDPR. Αυτοί οι κανόνες μπορούν να πιστοποιηθούν από τις εποπτικές αρχές ή άλλους ανεξάρτητους διαπιστευμένους φορείς και να θεσπίσουν νομική βάση για την επεξεργασία δεδομένων προσωπικού χαρακτήρα (άρθρα 40, 41, 42, 43 (Union Council of the European, 2016)).

4.5.2 Υποχρεώσεις GDPR Παρόχου Cloud και Επιχειρήσεων

Η προστασία των δεδομένων προσωπικού χαρακτήρα στο νέφος είναι κρίσιμη για την ασφάλεια των πληροφοριών και τη συμμόρφωση με τον Γενικό Κανονισμό Προστασίας Δεδομένων (ΓΚΠΔ). Οι επιχειρήσεις και οι πάροχοι υπηρεσιών νέφους πρέπει να εφαρμόζουν αυστηρές πολιτικές και διαδικασίες για να εξασφαλίσουν την ασφάλεια, την αποτροπή παραβιάσεων και τη σωστή διαχείριση των δεδομένων. Στη συνέχεια, εξετάζουμε τα κύρια μέτρα και διαδικασίες που πρέπει να ακολουθούνται για την προστασία των δεδομένων προσωπικού χαρακτήρα στο νέφος (Union Council of the European, 2016):

Ασφάλεια: Για να διασφαλιστεί η ασφάλεια των δεδομένων προσωπικού χαρακτήρα που υποβάλλονται σε επεξεργασία στο νέφος, τόσο οι οργανισμοί όσο και οι πάροχοι υπηρεσιών νέφους πρέπει να εφαρμόζουν κατάλληλες τεχνικές και οργανωτικές διασφαλίσεις. Σε προηγούμενες ενότητες, συζητήσαμε διάφορους ελέγχους και μέτρα ασφαλείας, όπως η εμπιστευτικότητα, η ακεραιότητα και η διαθεσιμότητα, η κρυπτογράφηση, οι έλεγχοι πρόσβασης, η ανάκαμψη από καταστροφές, οι τακτικές αξιολογήσεις ασφαλείας και η εκπαίδευση των εργαζομένων. Είναι ζωτικής σημασίας να έχετε κατά νου ότι αυτές οι προδιαγραφές δεν είναι πλήρεις και μπορεί να διαφέρουν ανάλογα με τον τύπο των

προσωπικών δεδομένων που διαχειρίζονται στο νέφος και τους κινδύνους που ενέχει. Προκειμένου να διασφαλιστεί η συμμόρφωση με τις υποχρεώσεις ασφάλειας του ΓΚΠΔ , είναι ζωτικής σημασίας, τόσο για τους παρόχους cloud όσο και για τις επιχειρήσεις, να διενεργούν ενδελεχή αξιολόγηση κινδύνου και να θέτουν σε εφαρμογή τις απαραίτητες διασφαλίσεις.

Γνωστοποίηση παραβίασης δεδομένων: Όταν συμβεί παραβίαση δεδομένων, τόσο οι πάροχοι νέφους όσο και οι επιχειρήσεις έχουν αυστηρή προθεσμία για να ενημερώσουν την αρμόδια ρυθμιστική αρχή. Η κοινοποίηση αυτή πρέπει να περιλαμβάνει περιγραφή της φύσης της παραβίασης, του αριθμού και των ομάδων ατόμων που επηρεάζονται, των αναμενόμενων επιπτώσεων και των μέτρων που λαμβάνονται για την αποκατάστασή της. Τα υποκείμενα των δεδομένων που επηρεάζονται από την παραβίαση χρειάζεται να ενημερώνονται χωρίς αδικαιολόγητη καθυστέρηση, στην περίπτωση που η παραβίαση ενέχει σημαντικό κίνδυνο για τα δικαιώματα και τις ελευθερίες τους. Επιπλέον, τόσο οι πάροχοι υπηρεσιών νέφους όσο και οι επιχειρήσεις οφείλουν να τηρούν αρχεία όλων των παραβιάσεων δεδομένων, συμπεριλαμβανομένων των περιστάσεων της παραβίασης, των συνεπειών και των διορθωτικών μέτρων που έχουν ληφθεί.

Διαχείριση υπό επεξεργαστών: Οι πάροχοι υπηρεσιών νέφους πρέπει να διασφαλίζουν ότι όλοι οι υπεργολάβοι που προσλαμβάνουν για να χειρίζονται δεδομένα προσωπικού χαρακτήρα συμμορφώνονται με τις ίδιες υποχρεώσεις προστασίας δεδομένων όπως και ο πάροχος υπηρεσιών νέφους. Οι υποχρεώσεις αυτές πρέπει να τεκμηριώνονται σε σύμβαση ή νομική συμφωνία. Προτού οι επιχειρήσεις προσλάβουν έναν υπό επεξεργαστή για τη διαχείριση δεδομένων προσωπικού χαρακτήρα, είναι αναγκαίο να λάβουν έγκριση από τον πάροχο υπηρεσιών νέφους. Ο πάροχος νέφους και η επιχείρηση πρέπει να επιδεικνύουν τη δέουσα επιμέλεια σε κάθε υπό επεξεργαστή που προσλαμβάνεται για την επεξεργασία δεδομένων προσωπικού χαρακτήρα, ώστε να διασφαλίζεται ότι μπορεί να παρέχει το απαραίτητο επίπεδο προστασίας των δεδομένων. Επιπλέον, και τα δύο μέρη πρέπει να παρακολουθούν τις ενέργειες των 18 υπεργολάβων που προσλαμβάνονται για την επεξεργασία δεδομένων προσωπικού χαρακτήρα, ώστε να διασφαλίζουν ότι τηρούν τα πρότυπα προστασίας δεδομένων του ΓΚΠΔ. Τόσο ο πάροχος νέφους όσο και η επιχείρηση φέρουν την πλήρη ευθύνη για τυχόν παραβιάσεις του ΓΚΠΔ που διαπράττουν οι υπό επεξεργαστές τους.

Τήρηση αρχείων: Για να εξασφαλιστεί η συμμόρφωση με τον ΓΚΠΔ, τόσο οι επιχειρήσεις όσο και οι πάροχοι υπηρεσιών νέφους επιβάλλεται να τηρούν αρχεία των δραστηριοτήτων επεξεργασίας δεδομένων τους, συμπεριλαμβανομένων εκείνων που σχετίζονται με δεδομένα προσωπικού χαρακτήρα που υποβάλλονται σε επεξεργασία στο νέφος. Τα αρχεία αυτά πρέπει να περιλαμβάνουν πληροφορίες σχετικά με τους στόχους της επεξεργασίας, τους τύπους των δεδομένων προσωπικού χαρακτήρα που χρησιμοποιήθηκαν και ποιος έλαβε τα δεδομένα. Επιπλέον, εάν απαιτείται από τον ΓΚΠΔ, χρειάζεται επιπλέον να τηρούν αρχεία των αξιολογήσεων αντικτύπου για την προστασία των δεδομένων τους. Η διάρκεια διατήρησης των αρχείων μπορεί να ποικίλλει ανάλογα με τη φύση της δραστηριότητας επεξεργασίας και τις σχετικές κανονιστικές απαιτήσεις. Σε περίπτωση αιτήματος από τον αρμόδιο εποπτικό φορέα, τόσο οι επιχειρήσεις όσο και οι πάροχοι νέφους πρέπει να καθιστούν προσβάσιμα τα αρχεία των δραστηριοτήτων επεξεργασίας τους.

Υπεύθυνος προστασίας δεδομένων: Σύμφωνα με τον ΓΚΠΔ, οι επιχειρήσεις και οι πάροχοι cloud ενδέχεται να χρειαστεί να διορίσουν έναν υπεύθυνο προστασίας δεδομένων (DPO) ανάλογα με τη φύση και την έκταση των δραστηριοτήτων επεξεργασίας δεδομένων τους. Ο ΥΠΔ είναι υπεύθυνος για τη διασφάλιση της συμμόρφωσης με τους κανονισμούς προστασίας δεδομένων του ΓΚΠΔ και χρησιμεύει ως σύνδεσμος μεταξύ της εταιρείας και των εποπτικών αρχών. Ο DPO πρέπει να έχει τα προσόντα και να έχει προσληφθεί για το ρόλο αυτό. Επιπλέον, ο DPO πρέπει να διαθέτει ανεξαρτησία και να μπορεί να εκτελεί τις αρμοδιότητές του χωρίς να φοβάται αντίποινα ή αντίποινα. Οι οργανισμοί και οι πάροχοι cloud υποχρεούνται να παρέχουν στους DPO τους επαρκείς πόρους, συμπεριλαμβανομένου του προσωπικού, της χρηματοδότησης και των εργαλείων, για την αποτελεσματική εκτέλεση των καθηκόντων τους.

Λογοδοσία: Υπάρχουν διάφορες μέθοδοι για τη διασφάλιση της λογοδοσίας, συμπεριλαμβανομένης της εφαρμογής της προστασίας δεδομένων εκ κατασκευής και εξ ορισμού και της διενέργειας εκτιμήσεων αντικτύπου σχετικά με την προστασία δεδομένων (DPIA), οι οποίες θα εξηγηθούν στα επόμενα κεφάλαια. Επιπλέον, η διατήρηση ορθών πρακτικών τήρησης αρχείων και η ύπαρξη ορισμένου Υπεύθυνου Προστασίας Δεδομένων (DPO), όπως συζητήθηκε προηγουμένως, μπορούν να ενισχύσουν τη λογοδοσία. Τέλος, είναι υψίστης σημασίας τόσο για τις εταιρείες όσο και για τους παρόχους cloud να συνεργάζονται στενά με τις εποπτικές αρχές, όπως η ανταπόκριση σε αιτήματα παροχής πληροφοριών και η

παροχή πρόσβασης σε αρχεία και άλλα σχετικά έγγραφα που σχετίζονται με τις δραστηριότητες επεξεργασίας τους.

Συμφωνία επεξεργασίας δεδομένων - DPA: Για να διασφαλιστεί η συμμόρφωση με τον ΓΚΠΔ, πρέπει να υπάρχει γραπτή συμφωνία επεξεργασίας δεδομένων (ΣΔΠ). Η ΣΔΠ χρειάζεται να περιέχει πληροφορίες σχετικά με τους τύπους των δεδομένων προσωπικού χαρακτήρα που υποβάλλονται σε επεξεργασία, τη φύση, το πεδίο εφαρμογής και τον σκοπό τους, καθώς και τη διάρκεια της επεξεργασίας. Ο εκτελών την επεξεργασία πρέπει να συμμορφώνεται με τις απαιτήσεις του ΓΚΠΔ για την προστασία των δεδομένων, εφαρμόζοντας οργανωτικές και τεχνικές εγγυήσεις για την προστασία των δεδομένων προσωπικού χαρακτήρα, συμπεριλαμβανομένων μέτρων κατά της μη εξουσιοδοτημένης πρόσβασης, αποκάλυψης, τροποποίησης ή καταστροφής. Ο ΥΠΔ πρέπει επίσης να περιγράφει τους όρους χρήσης των υπεργολάβων επεξεργασίας και να διασφαλίζει ότι αυτοί συμμορφώνονται με τα ίδια πρότυπα προστασίας δεδομένων με τον εκτελούντα την επεξεργασία. Ο εκτελών την επεξεργασία οφείλει να συνεργάζεται με τον υπεύθυνο επεξεργασίας για την αντιμετώπιση αιτημάτων των υποκειμένων των δεδομένων για πρόσβαση, διόρθωση, διαγραφή και φορητότητα. Ο ΥΠΔ χρειάζεται να μπορεί να επιτρέπει στον υπεύθυνο επεξεργασίας να ελέγχει την τήρηση των κανόνων προστασίας δεδομένων του ΓΚΠΔ από τον εκτελούντα την επεξεργασία. Σε περίπτωση παραβίασης, η ΑΠΔ θα πρέπει να αναφέρει ότι η σύμβαση μπορεί να καταγγελθεί και να απαιτήσει από τον εκτελούντα την επεξεργασία να επιστρέψει ή να καταστρέψει όλα τα δεδομένα προσωπικού χαρακτήρα που έχει στην κατοχή του.

Δικαιώματα του υποκειμένου των δεδομένων: Σύμφωνα με τον ΓΚΠΔ, τόσο οι εταιρείες όσο και οι πάροχοι cloud είναι υπεύθυνοι να διασφαλίζουν ότι τα άτομα μπορούν να ασκούν τα δικαιώματά τους όσον αφορά τα προσωπικά τους δεδομένα. Τα δικαιώματα αυτά περιλαμβάνουν τη δυνατότητα πρόσβασης στα δεδομένα προσωπικού χαρακτήρα και στις πληροφορίες σχετικά με τον τρόπο επεξεργασίας τους, την αίτηση διόρθωσης ανακριβών ή ελλιπών δεδομένων, την αίτηση διαγραφής δεδομένων προσωπικού χαρακτήρα σε ορισμένες περιπτώσεις, τον περιορισμό της επεξεργασίας των δεδομένων τους σε ορισμένες περιπτώσεις, τη λήψη των δεδομένων τους σε δομημένη και αναγνώσιμη από μηχανήματα μορφή και τη διαβίβασή τους σε άλλον υπεύθυνο επεξεργασίας. Τα άτομα μπορούν επίσης να αντιταχθούν στην επεξεργασία των δεδομένων τους σε ορισμένες περιπτώσεις, όπως για παράδειγμα για απευθείας εμπορική προώθηση. Για να διασφαλιστεί ότι τα άτομα μπορούν

να ασκήσουν τα δικαιώματά τους, οι εταιρείες και οι πάροχοι cloud πρέπει να διαθέτουν διαδικασίες, να απαντούν εντός συγκεκριμένου χρονικού πλαισίου και να μην χρεώνουν τέλη εκτός από ορισμένες περιπτώσεις. Η μη συμμόρφωση με αυτές τις απαιτήσεις μπορεί να οδηγήσει σε σημαντικές κυρώσεις και πρόστιμα.

Ελαχιστοποίηση δεδομένων: Για να συμμορφωθούν με τον ΓΚΠΔ, τόσο οι εταιρείες όσο και οι πάροχοι cloud πρέπει να ακολουθούν την αρχή της ελαχιστοποίησης των δεδομένων, που σημαίνει ότι θα πρέπει να συλλέγουν, να επεξεργάζονται και να διατηρούν μόνο τα δεδομένα προσωπικού χαρακτήρα που είναι απαραίτητα για έναν συγκεκριμένο σκοπό. Αυτό συμβάλλει στην αποτροπή της περιττής συλλογής ή επεξεργασίας δεδομένων προσωπικού χαρακτήρα και στη μείωση του κινδύνου παραβίασης δεδομένων ή μη εξουσιοδοτημένης πρόσβασης. Ο ΓΚΠΔ απαιτεί τα δεδομένα προσωπικού χαρακτήρα να είναι επαρκή, συναφή και περιορισμένα. Αυτό σημαίνει ότι ο όγκος των δεδομένων προσωπικού χαρακτήρα που συλλέγονται πρέπει να είναι επαρκής για την επίτευξη του επιδιωκόμενου σκοπού, να είναι συναφής με τον επιδιωκόμενο σκοπό και να περιορίζεται στα αναγκαία για τον επιδιωκόμενο σκοπό.

Συνοψίζοντας, τόσο οι εταιρείες όσο και οι πάροχοι νέφους πρέπει να αξιολογούν την αναγκαιότητα της συλλογής και επεξεργασίας δεδομένων προσωπικού χαρακτήρα και να εφαρμόζουν μέτρα για να διασφαλίζουν ότι τα δεδομένα προσωπικού χαρακτήρα δεν υποβάλλονται σε επεξεργασία πέραν του αναγκαίου. Παραδείγματα τέτοιων μέτρων περιλαμβάνουν την εφαρμογή πολιτικών διατήρησης δεδομένων, την ανωνυμοποίηση ή ψευδωνυμοποίηση προσωπικών δεδομένων και την ελαχιστοποίηση της συλλογής ευαίσθητων προσωπικών δεδομένων.

4.5.3 Υποχρεώσεις GDPR από Πάροχο Cloud

Η διαφάνεια και η ασφάλεια στην επεξεργασία δεδομένων προσωπικού χαρακτήρα είναι κρίσιμη για την προστασία της ιδιωτικότητας των χρηστών και τη συμμόρφωση με τον Γενικό Κανονισμό Προστασίας Δεδομένων (ΓΚΠΔ). Οι πάροχοι υπηρεσιών νέφους έχουν την ευθύνη να ενημερώνουν πλήρως τους πελάτες τους για τις διαδικασίες επεξεργασίας των δεδομένων και να διασφαλίζουν την αποτελεσματικότητα των μέτρων ασφαλείας τους. Στη συνέχεια, θα εξετάσουμε τις βασικές υποχρεώσεις των παρόχων νέφους, όπως η διαφάνεια στις πολιτικές προστασίας δεδομένων, οι έλεγχοι ασφαλείας, οι μηχανισμοί μεταφοράς

δεδομένων και η διαχείριση περιστατικών ασφαλείας (Union Council of the European, 2016). Πιο αναλυτικά:

Διαφάνεια: Οι πάροχοι cloud πρέπει να διασφαλίζουν ότι οι πελάτες ενημερώνονται πλήρως για την επεξεργασία των προσωπικών τους δεδομένων βάσει του ΓΚΠΔ. Αυτό περιλαμβάνει την παροχή σαφών και συνοπτικών πληροφοριών σχετικά με τους σκοπούς, τους τύπους, τη νομική βάση, την κοινοποίηση σε τρίτους, την περίοδο διατήρησης και τα δικαιώματα των υποκειμένων των δεδομένων που σχετίζονται με την επεξεργασία των δεδομένων προσωπικού χαρακτήρα. Οι πληροφορίες πρέπει να είναι εύκολα προσβάσιμες και να παρέχονται με σαφή και κατανοητό τρόπο, όπως μέσω μιας πολιτικής απορρήτου. Οι πάροχοι υπολογιστικού νέφους οφείλουν επίσης να ενημερώνουν τους πελάτες για τυχόν αλλαγές στις πολιτικές προστασίας προσωπικών δεδομένων ή στις πρακτικές επεξεργασίας δεδομένων και να λαμβάνουν τη συγκατάθεσή τους για τυχόν σημαντικές αλλαγές στην επεξεργασία δεδομένων προσωπικού χαρακτήρα.

Έλεγχοι ασφαλείας: Οι πάροχοι υπολογιστικού νέφους υποχρεούνται να αξιολογούν τακτικά τα μέτρα ασφαλείας τους για να διασφαλίζουν ότι παραμένουν αποτελεσματικά και ενημερωμένα. Οφείλουν να εφαρμόζουν κατάλληλα τεχνικά και οργανωτικά μέτρα για την προστασία των προσωπικών δεδομένων, όπως κρυπτογράφηση, έλεγχο πρόσβασης και τακτική δημιουργία αντιγράφων ασφαλείας. Οι πάροχοι υπολογιστικού νέφους πρέπει να διενεργούν τακτικές αξιολογήσεις κινδύνου για τον εντοπισμό πιθανών απειλών και τρωτών σημείων για την ασφάλεια των δεδομένων προσωπικού χαρακτήρα. Επιπλέον, πρέπει να διαθέτουν πολιτικές και διαδικασίες για την αντιμετώπιση περιστατικών, την κοινοποίηση παραβίασης δεδομένων και την αναφορά περιστατικών ασφαλείας. Οι πάροχοι υπολογιστικού νέφους πρέπει επίσης να συμμορφώνονται με τα σχετικά πρότυπα ασφαλείας και πιστοποιήσεις, όπως το ISO 27001, ώστε να διατηρούν υψηλό επίπεδο ασφάλειας για τα δεδομένα προσωπικού χαρακτήρα. Είναι απαραίτητο να διενεργούνται τακτικοί έλεγχοι ασφαλείας για να διασφαλίζεται η αποτελεσματικότητα των μέτρων ασφαλείας τους.

Μηχανισμοί μεταφοράς δεδομένων: Σύμφωνα με τον ΓΚΠΔ, η διαβίβαση δεδομένων από τον ΕΟΧ σε χώρες εκτός ΕΟΧ πρέπει να γίνεται με προσοχή, ώστε να διασφαλίζεται η καλή προστασία των προσωπικών δεδομένων. Ο ΓΚΠΔ προσφέρει διάφορους τρόπους για την προστασία των προσωπικών δεδομένων από τους παρόχους cloud, όπως η μεταφορά δεδομένων σε χώρες που θεωρούνται ότι έχουν επαρκή επίπεδα προστασίας δεδομένων από την Ευρωπαϊκή Επιτροπή. Οι πάροχοι μπορούν επίσης να χρησιμοποιούν τυποποιημένες

συμβατικές ρήτρες (SCC) εγκεκριμένες από την Ευρωπαϊκή Επιτροπή για τη διασφάλιση των δεδομένων που μεταφέρονται εκτός του ΕΟΧ. Εσωτερικές πολιτικές που ονομάζονται δεσμευτικοί εταιρικοί κανόνες (BCR) και έχουν εγκριθεί από τις αρμόδιες αρχές προστασίας δεδομένων μπορούν να χρησιμοποιηθούν για τη διαβίβαση δεδομένων εντός εταιρικών ομίλων. Σε εξαιρετικές περιπτώσεις, μπορούν να χρησιμοποιηθούν παρεκκλίσεις, όπως όταν το υποκείμενο των δεδομένων συναινεί ρητά στη διαβίβαση ή όταν η διαβίβαση είναι απαραίτητη για την εκτέλεση σύμβασης. Οι πάροχοι πρέπει να διασφαλίζουν ότι διαθέτουν κατάλληλους μηχανισμούς μεταφοράς δεδομένων πριν από τη μεταφορά δεδομένων προσωπικού χαρακτήρα εκτός του ΕΟΧ. Επιπλέον, πρέπει να αξιολογούν τους κινδύνους, να τεκμηριώνουν την αξιολόγησή τους και να λαμβάνουν τα απαραίτητα μέτρα για τον μετριασμό τυχόν κινδύνων.

Αντιμετώπιση περιστατικών: Σύμφωνα με τον ΓΚΠΔ, οι πάροχοι υπηρεσιών νέφους πρέπει να διαθέτουν σχέδιο για τον εντοπισμό, τη διερεύνηση και την αντιμετώπιση περιστατικών ασφαλείας που θα μπορούσαν να επηρεάσουν τα δεδομένα προσωπικού χαρακτήρα που επεξεργάζονται. Για να διασφαλιστεί η εμπιστευτικότητα, η ακεραιότητα και η διαθεσιμότητα των δεδομένων προσωπικού χαρακτήρα, οι πάροχοι νέφους πρέπει να λαμβάνουν τα κατάλληλα τεχνικά και οργανωτικά μέτρα, συμπεριλαμβανομένης της προστασίας από μη εξουσιοδοτημένη πρόσβαση και καταστροφή των δεδομένων. Επίσης, καλούνται επίσης να καθιερώσουν διαδικασίες για την τακτική δοκιμή και αξιολόγηση των μέτρων ασφαλείας και των σχεδίων αντιμετώπισης συμβάντων. Σε περίπτωση παραβίασης δεδομένων, οι πάροχοι νέφους πρέπει να ενημερώνουν αμέσως τον υπεύθυνο επεξεργασίας δεδομένων και να παρέχουν πληροφορίες σχετικά με τη φύση της παραβίασης, τον αριθμό των επηρεαζόμενων υποκειμένων των δεδομένων και τις πιθανές συνέπειες. Οφείλουν τέλος να συνεργάζονται με τον υπεύθυνο επεξεργασίας δεδομένων και να τεκμηριώνουν και να αναφέρουν τυχόν περιστατικά μαζί με τις ενέργειες αποκατάστασης που έχουν ληφθεί.

4.5.4 Υποχρεώσεις GDPR από Επιχειρήσεις

Ο Γενικός Κανονισμός Προστασίας Δεδομένων (ΓΚΠΔ) θέτει αυστηρές υποχρεώσεις για τις εταιρείες που χρησιμοποιούν υπηρεσίες νέφους, προκειμένου να διασφαλίσουν την προστασία των προσωπικών δεδομένων και την τήρηση των δικαιωμάτων των υποκειμένων τους. Οι αρμοδιότητες των υπευθύνων επεξεργασίας δεδομένων περιλαμβάνουν τη σωστή διαχείριση των προμηθευτών, τη διασφάλιση της φορητότητας των δεδομένων και τη

διαπραγμάτευση συμφωνιών με τους παρόχους cloud για την συμμόρφωση με τον ΓΚΠΔ. Επιπλέον, απαιτείται η τακτική αξιολόγηση κινδύνων και η λήψη κατάλληλων μέτρων για την προστασία των δεδομένων. Στη συνέχεια, εξετάζουμε αυτές τις υποχρεώσεις, τις πρακτικές που πρέπει να ακολουθήσουν οι εταιρείες και οι πάροχοι υπηρεσιών νέφους, καθώς και τις συνέπειες σε περίπτωση παραβίασης των κανονισμών του ΓΚΠΔ (Union Council of the European, 2016):

Αρμοδιότητες ελεγκτή δεδομένων και διαχείριση προμηθευτών: Οι εταιρείες που χρησιμοποιούν υπηρεσίες νέφους πρέπει να συμμορφώνονται με τις ευθύνες τους ως υπεύθυνοι επεξεργασίας δεδομένων σύμφωνα με τον ΓΚΠΔ. Αυτό περιλαμβάνει τη λήψη συγκατάθεσης από τα υποκείμενα των δεδομένων, την εφαρμογή κατάλληλων μέτρων ασφαλείας και την ανταπόκριση σε αιτήματα των υποκειμένων των δεδομένων. Επιπλέον, οι εταιρείες πρέπει να διασφαλίζουν ότι επιλέγουν έναν πάροχο υπηρεσιών νέφους που συμμορφώνεται με τον ΓΚΠΔ και διαθέτει κατάλληλα τεχνικά και οργανωτικά μέτρα για την προστασία των προσωπικών δεδομένων. Θα πρέπει επίσης να διαχειρίζονται τη σχέση τους με τον πάροχο υπηρεσιών cloud μέσω ενός προγράμματος διαχείρισης προμηθευτών που διασφαλίζει ότι ο πάροχος πληροί τις απαιτήσεις του GDPR. Αυτό περιλαμβάνει την επαλήθευση των μηχανισμών μεταφοράς δεδομένων, των μέτρων ασφαλείας, της δέουσας επιμέλειας του προμηθευτή, της διαχείρισης των υπό επεξεργαστών και της συνεχούς παρακολούθησης της συμμόρφωσης με τις απαιτήσεις του ΓΚΠΔ. Σε περίπτωση που προκύψουν οποιαδήποτε ζητήματα, θα πρέπει να ληφθούν τα κατάλληλα μέτρα.

Φορητότητα δεδομένων: Ο ΓΚΠΔ παρέχει στα άτομα το δικαίωμα στη φορητότητα των δεδομένων, πράγμα που σημαίνει ότι μπορούν να λάβουν τις προσωπικές τους πληροφορίες από έναν υπεύθυνο επεξεργασίας και να τις διαβιβάσουν σε άλλον χωρίς περιορισμούς. Η υποχρέωση αυτή ισχύει και για τις εταιρείες που χρησιμοποιούν υπηρεσίες υπολογιστικού νέφους για την επεξεργασία δεδομένων πελατών. Σύμφωνα με τους κανονισμούς του ΓΚΠΔ, οι επιχειρήσεις πρέπει να παρέχουν τα προσωπικά δεδομένα στα υποκείμενα των δεδομένων σε δομημένη, κοινώς χρησιμοποιούμενη και αναγνώσιμη από μηχανήματα μορφή. Εάν είναι τεχνικά εφικτό, τα δεδομένα πρέπει να διαβιβάζονται απευθείας από έναν υπεύθυνο επεξεργασίας σε άλλον. Επιπλέον, οι πάροχοι υπηρεσιών νέφους πρέπει να βοηθούν τις επιχειρήσεις να συμμορφώνονται με τις απαιτήσεις για φορητότητα των δεδομένων, παρέχοντας εργαλεία και υπηρεσίες που διευκολύνουν τη διαβίβαση δεδομένων προσωπικού χαρακτήρα σε άλλον υπεύθυνο επεξεργασίας. Τα εργαλεία αυτά μπορεί να περιλαμβάνουν API, πρωτόκολλα ασφαλούς μεταφοράς δεδομένων και άλλες μεθόδους που επιτρέπουν στις

επιχειρήσεις να μεταφέρουν τα δεδομένα προσωπικού χαρακτήρα απρόσκοπτα σε άλλον υπεύθυνο επεξεργασίας.

Διαπραγμάτευση συμφωνίας επεξεργασίας δεδομένων: Ο ΓΚΠΔ απαιτεί επίσημη σύμβαση με τους παρόχους υπηρεσιών νέφους για τις επιχειρήσεις που χρησιμοποιούν υπηρεσίες υπολογιστικού νέφους για την επεξεργασία προσωπικών δεδομένων. Σύμφωνα με τον ΓΚΠΔ, η ΣΔΠ πρέπει να περιέχει συγκεκριμένες υποχρεωτικές ρήτρες, όπως: Η ΣΠΔ θα πρέπει επίσης να περιγράφει τα μέτρα που θα λάβει ο πάροχος υπηρεσιών νέφους για να διασφαλίσει τη συμμόρφωση με τον ΓΚΠΔ, καθώς και τις υποχρεώσεις που αφορούν την ασφάλεια και την εμπιστευτικότητα των δεδομένων προσωπικού χαρακτήρα που υποβάλλονται σε επεξεργασία. Οι εταιρείες θα πρέπει να διασφαλίζουν ότι η ΣΠΔ που διαπραγματεύονται με έναν πάροχο υπηρεσιών νέφους περιέχει όλες τις υποχρεωτικές ρήτρες του ΓΚΠΔ. Για να εγγυηθούν ότι οι ιδιαίτερες ανάγκες τους για την επεξεργασία δεδομένων καλύπτονται σωστά, θα πρέπει να διαπραγματευτούν επιπλέον πρόσθετες ρήτρες, εφόσον απαιτείται.

Αξιολογήσεις κινδύνων: Ο ΓΚΠΔ απαιτεί από τις εταιρείες που χρησιμοποιούν υπηρεσίες υπολογιστικού νέφους να αξιολογούν τους κινδύνους για την προστασία των ατομικών δεδομένων και της ιδιωτικής ζωής. Υποχρεώνει να εντοπίζουν τους δυνητικούς κινδύνους και τα τρωτά σημεία που σχετίζονται με τη χρήση υπηρεσιών cloud και να λαμβάνουν μέτρα ασφαλείας για τη μείωση των κινδύνων αυτών. Για να διατηρήσουν την ασφάλεια των προσωπικών δεδομένων στο νέφος, οι επιχειρήσεις θα πρέπει να διενεργούν τακτικές αξιολογήσεις κινδύνου, ιδίως όταν το περιβάλλον νέφους αλλάζει ή όταν εισάγονται νέες υπηρεσίες νέφους. Θα πρέπει επίσης να τεκμηριώνουν τα αποτελέσματα των αξιολογήσεων κινδύνου και να λαμβάνουν τα απαραίτητα τεχνικά και οργανωτικά μέτρα για να διασφαλίζουν τη συνεχή ασφάλεια και προστασία των δεδομένων προσωπικού χαρακτήρα.

Ο ΓΚΠΔ επιβάλλει αυστηρές κυρώσεις για τις παραβιάσεις των κανόνων του. Υπάρχουν δύο βαθμίδες προστίμων ανάλογα με τη σοβαρότητα της παράβασης. Η πρώτη βαθμίδα μπορεί να οδηγήσει σε πρόστιμα ύψους έως και 10 εκατ. ευρώ ή 2% των ετήσιων παγκόσμιων εσόδων της εταιρείας, ανάλογα με το ποιο από τα δύο είναι μεγαλύτερο, για μη συμμόρφωση με τις εκτιμήσεις αντικτύπου προστασίας δεδομένων, τις απαιτήσεις τήρησης αρχείων, τις κοινοποιήσεις παραβίασης δεδομένων ή τις υποχρεώσεις του υπεύθυνου προστασίας δεδομένων. Η δεύτερη βαθμίδα μπορεί να οδηγήσει σε πρόστιμα ύψους έως και 20 εκατομμυρίων ευρώ ή 4% των ετήσιων παγκόσμιων εσόδων της εταιρείας, ανάλογα με το ποιο από τα δύο είναι μεγαλύτερο. Αυτή η βαθμίδα περιλαμβάνει παραβάσεις θεμελιωδών

αρχών προστασίας της ιδιωτικής ζωής, όπως η λήψη συγκατάθεσης, ο σεβασμός των δικαιωμάτων των υποκειμένων των δεδομένων και η διαβίβαση δεδομένων εκτός ΕΕ.Στα πρόστιμα αυτά υπόκεινται, τόσο οι υπεύθυνοι επεξεργασίας όσο και οι εκτελούντες την επεξεργασία δεδομένων, συμπεριλαμβανομένων των παρόχων cloud. Η μη συμμόρφωση μπορεί να έχει ως αποτέλεσμα την αναστολή ή τον περιορισμό των δραστηριοτήτων επεξεργασίας δεδομένων, γεγονός που μπορεί να επηρεάσει σημαντικά τις δραστηριότητες και τη φήμη μιας εταιρείας. Ο ΓΚΠΔ προβλέπει επίσης μη οικονομικές κυρώσεις, όπως προειδοποιήσεις, επιπλήξεις και αναστολή των δραστηριοτήτων επεξεργασίας δεδομένων. Επιπλέον, τα υποκείμενα των δεδομένων έχουν το δικαίωμα να υποβάλουν αγωγές και να ζητήσουν αποζημίωση από τους υπευθύνους επεξεργασίας ή τους εκτελούντες την επεξεργασία που παραβιάζουν τα δικαιώματά τους. Τέλος, οι εποπτικές αρχές μπορούν να απαιτούν από τους υπευθύνους επεξεργασίας και τους εκτελούντες την επεξεργασία να λαμβάνουν συγκεκριμένα μέτρα για τη συμμόρφωση με τον ΓΚΠΔ.

Εν κατακλείδι, ο ΓΚΠΔ ορίζει ένα πλήρες σύνολο κατευθυντήριων γραμμών και προτύπων που έχουν σχεδιαστεί για τη διασφάλιση της εμπιστευτικότητας των προσωπικών δεδομένων στο υπολογιστικό νέφος. Οι εν λόγω κανονισμοί, οι οποίοι καλύπτουν ένα ευρύ φάσμα θεμάτων, όπως τα μέτρα ασφάλειας δεδομένων, η διαχείριση υπό επεξεργαστών, η αντιμετώπιση περιστατικών και οι ευθύνες του υπεύθυνου προστασίας δεδομένων, ισχύουν εξίσου για τους παρόχους υπηρεσιών νέφους και τις επιχειρήσεις που χρησιμοποιούν τις υπηρεσίες τους.

Ο ΓΚΠΔ προσδιορίζει μια σειρά από τύπους δεδομένων, συμπεριλαμβανομένων των ευαίσθητων και των προσωπικών δεδομένων, και επιβάλλει ποικίλες απαιτήσεις ανάλογα με τον τύπο των δεδομένων. Προκειμένου να διασφαλιστεί η ασφαλής και ηθική χρήση των δεδομένων σε περιβάλλοντα υπολογιστικού νέφους, είναι δέουσας σημασίας η συμμόρφωση με τους κανόνες του ΓΚΠΔ, δεδομένου ότι τα δεδομένα εξακολουθούν να αποτελούν πολύτιμο περιουσιακό στοιχείο τόσο για τους οργανισμούς όσο και για τα άτομα. Με την τήρηση των άνωθεν κατευθυντήριων γραμμών, οι επιχειρήσεις και οι πάροχοι cloud μπορούν να οικοδομήσουν την εμπιστοσύνη των χρηστών, να διασφαλίσουν τη φήμη τους και να μείνουν μακριά από προβλήματα νομικά και οικονομικά.

Κεφάλαιο 5ο – Προσωπική Άποψη – Συμπεράσματα Σχετικά με την Λειτουργίας της Διαχείρισης Ταυτότητας και Πρόσβασης σε Cloud Περιβάλλον

Σύμφωνα με όσα αναφέρθηκαν παραπάνω, η λειτουργία Cloud Identity and Access Management (cloud IAM) αναφέρεται ως το κλειδί για τις επιχειρήσεις που πλοηγούνται στην πολυπλοκότητα των συγκεκριμένων λειτουργιών. Η διαδικασία διαχείρισης ταυτότητας και πρόσβασης σε περιβάλλον Cloud, είναι ουσιαστικά τα εργαλεία και οι υπηρεσίες που έχουν σχεδιαστεί για να επιβλέπουν τις ψηφιακές ταυτότητες και να ρυθμίζουν την πρόσβαση των χρηστών σε πόρους που συνδέονται με το περιβάλλον cloud.

Στόχος του είναι να βοηθήσει τους οργανισμούς να ελέγχουν την πρόσβαση σε εφαρμογές, υπηρεσίες και δεδομένα στο cloud με ολοκληρωμένα πρωτόκολλα ελέγχου ταυτότητας και εξουσιοδότησης. Οι επιχειρήσεις μπορούν να χρησιμοποιήσουν την διαδικασία διαχείρισης ταυτότητας και πρόσβασης σε περιβάλλον Cloud, για να αυξήσουν την ασφάλειά τους, να βελτιώσουν τις διαδρομές πρόσβασης των χρηστών και να διαχειριστούν τις ταυτότητες σε περιβάλλοντα cloud.

Η διαδικασία διαχείρισης ταυτότητας και πρόσβασης σε περιβάλλον Cloud, είναι μια λύση προσαρμοσμένη, ειδικά για λειτουργίες που βασίζονται στο περιβάλλον αυτό με πολλά πλεονεκτήματα, όπως βελτιωμένη διαχείριση ταυτότητας, ολοκληρωμένους μηχανισμούς ασφαλείας και λεπτομερείς ελέγχους πρόσβασης για συγκεκριμένους φόρτους εργασίας.

Η διαδικασία διαχείρισης ταυτότητας και πρόσβασης σε περιβάλλον Cloud, διαχειρίζεται τις ταυτότητες των χρηστών στα συστήματα του περιβάλλοντος, επιβλέποντας τον έλεγχο ταυτότητας, την εξουσιοδότηση και τον έλεγχο πρόσβασης. Μπορεί να διαχειριστεί τις ταυτότητες των χρηστών από την παροχή έως την κατάργηση της παροχής, ενώ τηρεί αυστηρά πρότυπα ασφάλειας και συμμόρφωσης. Ο έλεγχος ταυτότητας σημαίνει τη χρήση μηχανισμών όπως ο έλεγχος ταυτότητας πολλαπλών παραγόντων (MFA) και η

απλή σύνδεση (SSO) για την επαλήθευση της ταυτότητας των χρηστών, συσκευών και εφαρμογών που έχουν πρόσβαση σε πόρους cloud.

Μετά τον έλεγχο ταυτότητας, το περιβάλλον cloud χρησιμοποιεί τακτικές εξουσιοδότησης. Αξιοποιώντας λεπτομερείς ελέγχους πρόσβασης και πολιτικές πρόσβασης βάσει ρόλων, το cloud βοηθά τους οργανισμούς να προσαρμόσουν τα δικαιώματα πρόσβασης στις συγκεκριμένες ανάγκες του φόρτου εργασίας τους στο cloud για να βελτιώσουν την ασφάλεια και να διασφαλίσουν ότι οι χρήστες διαθέτουν τα δικαιώματα που απαιτούνται για τους ρόλους τους.

Η διαδικασία διαχείρισης ταυτότητας και πρόσβασης σε περιβάλλον Cloud, είναι διαφορετικές προσεγγίσεις για τη διαχείριση ψηφιακών ταυτοτήτων και τη ρύθμιση της πρόσβασης σε πόρους, καθεμία σχεδιασμένη για διαφορετικά λειτουργικά συστήματα. Σε αντίθεση με τα παραδοσιακά συστήματα διαχείρισης ταυτότητας και πρόσβασης, τα οποία συχνά βασίζονται σε υποδομή εσωτερικής εγκατάστασης και άκαμπτους ελέγχους πρόσβασης, η διαδικασία διαχείρισης ταυτότητας και πρόσβασης σε περιβάλλον Cloud, είναι προσαρμόσιμο σε περιβάλλοντα cloud για απαράμιλλη επεκτασιμότητα, ευελιξία και ασφάλεια.

Το παραδοσιακό περιβάλλον Cloud, μπορεί να χρειάζεται βοήθεια για να συμβαδίσει με τη ζήτηση επεκτασιμότητας των λειτουργιών που βασίζονται στο cloud, οι οποίες συχνά απαιτούν μη αυτόματες παρεμβάσεις και μακροχρόνιες διαδικασίες παροχής. Το περιβάλλον Cloud μπορεί να χρησιμοποιήσει την αρχιτεκτονική και τον αυτοματισμό εγγενούς για να καλύψει τις αλλαγές στους πληθυσμούς των χρηστών, τις απαιτήσεις πόρων και τις απαιτήσεις πρόσβασης. Επιπλέον, τα παραδοσιακά συστήματα της διαδικασίας διαχείρισης ταυτότητας και πρόσβασης σε περιβάλλον Cloud, λειτουργούν συνήθως στο εσωτερικό δίκτυο ενός οργανισμού, ενώ το cloud μπορεί να επεκταθεί πέρα από αυτά τα όρια για κεντρική διαχείριση ταυτότητας σε διαφορετικές πλατφόρμες.

Πολλά βασικά στοιχεία είναι σημαντικά για την προστασία των περιβαλλόντων cloud και τη διαχείριση της πρόσβασης των χρηστών. Αυτά τα στοιχεία είναι θεμελιώδη για τα συστήματα διαχείρισης ταυτότητας και πρόσβασης σε περιβάλλον Cloud και περιλαμβάνουν έλεγχο ταυτότητας χρήστη, εξουσιοδότηση, ρόλους και δικαιώματα και τη διαχείριση ψηφιακών ταυτοτήτων. Οι οργανισμοί μπορούν να βελτιώσουν καλύτερα την ασφάλειά τους, κατανοώντας πώς λειτουργούν και συνεργάζονται αυτά τα στοιχεία.

Ο έλεγχος ταυτότητας χρήστη, είναι η πρώτη *άμυνα* στο περιβάλλον Cloud, αφού διασφαλίζει ότι μόνο εξουσιοδοτημένα άτομα μπορούν να έχουν πρόσβαση σε υπηρεσίες και πόρους cloud και προστατεύει ευαίσθητα δεδομένα από πιθανές απειλές. Το «εργαλείο» MFA είναι μόνο μια μέθοδος για τη βελτίωση του ελέγχου ταυτότητας απαιτώντας από τους χρήστες να παρέχουν πολλαπλές φόρμες επαλήθευσης, όπως κωδικούς πρόσβασης, βιομετρικά δεδομένα ή διακριτικά ασφαλείας.

Το εργαλείο SSO είναι μια άλλη μέθοδος ελέγχου ταυτότητας που επιτρέπει στους χρήστες να έχουν πρόσβαση σε διαφορετικές εφαρμογές και υπηρεσίες με ένα ενιαίο σύνολο διαπιστευτηρίων σύνδεσης, βελτιώνοντας την εμπειρία χρήστη και αυξάνοντας την παραγωγικότητα, απλοποιώντας παράλληλα τη διαχείριση ταυτότητας για τους διαχειριστές. Η βιομετρική επαλήθευση χρησιμοποιείται για την επαλήθευση ταυτοτήτων και μοναδικά βιολογικά χαρακτηριστικά όπως τα δακτυλικά αποτυπώματα και η αναγνώριση προσώπου χρησιμοποιούνται για τον έλεγχο ταυτότητας των χρηστών. Αυτή είναι μια από τις πιο αλάνθαστες μεθόδους, καθώς τα βιομετρικά δεδομένα είναι πολύπλοκο να αναπαραχθούν.

Η εξουσιοδότηση και ο έλεγχος πρόσβασης καθορίζουν τους πόρους στους οποίους έχουν πρόσβαση οι χρήστες και τις ενέργειες που μπορούν να εκτελέσουν σε περιβάλλοντα cloud. Η διαδικασία διαχείρισης ταυτότητας και πρόσβασης σε περιβάλλον Cloud χρησιμοποιεί διάφορες μεθόδους για την επιβολή ελέγχων πρόσβασης, συμπεριλαμβανομένου του ελέγχου πρόσβασης βάσει ρόλων (RBAC), του ελέγχου πρόσβασης βάσει χαρακτηριστικών (ABAC) και της διαχείρισης πρόσβασης βάσει αστυνομικών.

Το «εργαλείο» RBAC εκχωρεί άδεια σε χρήστες με βάση τους ρόλους τους σε έναν οργανισμό. Οι χρήστες ομαδοποιούνται σε προκαθορισμένους ρόλους και τα δικαιώματα παραχωρούνται ανάλογα με το ρόλο, που σημαίνει ότι τα δικαιώματα ευθυγραμμίζονται με τις ευθύνες εργασίας, επομένως οι διοικητικές εργασίες απλοποιούνται. Το «εργαλείο» ABAC εξετάζει πρόσθετα χαρακτηριστικά εκτός από τους ρόλους χρήστη, όπως χαρακτηριστικά χρήστη, χαρακτηριστικά πόρων και περιβαλλοντικά χαρακτηριστικά. Αξιολογεί ένα σύνολο κανόνων για τον καθορισμό των δικαιωμάτων πρόσβασης με βάση το συγκεκριμένο πλαίσιο κάθε αιτήματος πρόσβασης, έτσι ώστε οι οργανισμοί να μπορούν να προσαρμόζουν τους ελέγχους πρόσβασης σε μοναδικά σενάρια και επιχειρηματικές απαιτήσεις. Η διαχείριση πρόσβασης βάσει πολιτικής θεσπίζει κανόνες πρόσβασης και πολιτικές που καθορίζουν την πρόσβαση των χρηστών στους πόρους. Αυτές οι πολιτικές

προσδιορίζουν τους όρους υπό τους οποίους χορηγείται ή απαγορεύεται η πρόσβαση, λαμβάνοντας υπόψη παράγοντες όπως η ταυτότητα χρήστη, άρα ευαισθησία και το πλαίσιο. Το Frictionless Identity and Access Management της Ericom είναι ένα εξαιρετικό εργαλείο για αναγνώριση, έλεγχο ταυτότητας και εξουσιοδότηση με τη δυνατότητα χρήσης ενσωματωμένων λύσεων συμβατών με IAM ή SAML.

Η διαχείριση ταυτότητας διαδραματίζει ζωτικό ρόλο στην ασφάλεια των συστημάτων cloud, καθώς επιβλέπει τον κύκλο ζωής των ψηφιακών ταυτοτήτων και ρυθμίζει την πρόσβαση σε πόρους. Περιλαμβάνει την αναγνώριση των χρηστών, τον έλγχο ταυτότητας της ταυτότητάς τους, την εξουσιοδότηση της πρόσβασής τους σε πόρους και τη διαχείριση των αδειών τους καθ' όλη τη διάρκεια του κύκλου ζωής τους μέσα στο σύστημα πληροφορικής ενός οργανισμού. Η αποτελεσματική διαχείριση ταυτότητας είναι σημαντική για τον έλεγχο πρόσβασης, καθώς επιτρέπει στους οργανισμούς να επιβάλλουν πολιτικές και να μειώνουν τον κίνδυνο μη εξουσιοδοτημένης πρόσβασης.

Η εφαρμογή λύσεων στη διαδικασία διαχείρισης ταυτότητας και πρόσβασης σε περιβάλλον Cloud, περιλαμβάνει μια στρατηγική προσέγγιση για την καλύτερη λειτουργική απόδοση. Η διεξαγωγή τακτικών ελέγχων πρόσβασης είναι μια πρακτική που επιτρέπει στους οργανισμούς να αξιολογούν τα δικαιώματα και τις άδειες πρόσβασης τακτικά και να ανακαλούν τυχόν περιττά προνόμια. Η εφαρμογή της πρόσβασης ελάχιστων προνομίων διασφαλίζει ότι οι χρήστες λαμβάνουν μόνο τα απαραίτητα δικαιώματα για την εκτέλεση των εργασιών τους.

Περιορίζοντας την πρόσβαση στο ελάχιστο που απαιτείται για τις εργασίες, οι οργανισμοί ελαχιστοποιούν τον πιθανό αντίκτυπο των συμβάντων ασφαλείας και των μη εξουσιοδοτημένων δραστηριοτήτων. Η αξιοποίηση προηγμένων χαρακτηριστικών ασφαλείας όπως η τεχνητή νοημοσύνη και η μηχανική εκμάθηση είναι επίσης σημαντική και βοηθά τους οργανισμούς να εντοπίζουν προληπτικά και να ανταποκρίνονται σε ανωμαλίες και απειλές ασφαλείας σε πραγματικό χρόνο. Αυτές οι τεχνολογίες μπορούν να αναλύσουν μοτίβα συμπεριφοράς των χρηστών, να εντοπίσουν ύποπτες δραστηριότητες και να ενεργοποιήσουν αυτοματοποιημένες απαντήσεις ή ειδοποιήσεις για καλύτερη συνολική ανίχνευση απειλών.

Βιβλιογραφία

Almorsy, Grundy and Müller, 2016. *An Analysis of the Cloud Computing Security Problem.*

Ang'udi, 2023. *Security challenges in cloud computing: A comprehensive analysis.*

Azhar, I., 2019. *Cloud Identity and Access Management – A Model Proposal.*

Badger, Grance, Patt-Corner & Voas, 2012. *National Institute of Standards and Technology. Special Publication 800-146: Cloud Computing Synopsis and Recommendations.*

Birman, Chockler and van Renesse, 2009. *Toward a Cloud Computing Research Agenda.*

Boroujerdi and Nazem, 2009. *Cloud Computing: Changing Cogitation about Computing.*

Chung and Ermans, 2010. *From Hype to Future: KPMG's 2010 Cloud Computing Survey.*

Comer, D., 2021. *The Cloud Computing Book: The Future of Computing Explained.*

Dotson, C., 2019. *Practical Cloud Security A Guide for Secure Design and Deployment.*

Erl, Puttini and Zaigham, 2013. *Cloud Computing Concepts, Technology & Architecture.*

Ghelani, Hua and Koduru, 2022. *Cyber Security Threats, Vulnerabilities, and Security Solutions Models in Banking.*

Ghelani, D., 2022. *Cyber Security in Smart Grids, Threats, and Possible Solutions.*

Gopalakrishnan, S., 2009. *Cloud Computing Identity Management.*

Gunathunga, S., 2017. *Individual's rights under GDPR.*

Habiba, U., Masood, R., Shibli, M. A. & Niazi, M. A., 2014. *Cloud identity management security issues & solutions: a taxonomy.*

Harauz, Kaufman and Potter, 2009. *Data Security in the World of Cloud Computing.*

ISO/IEC 27018, 2019. *Information technology — Security techniques — Code of practice for protection of personally identifiable information (PII) in public clouds acting as PII processors.*

ISO/IEC:27001, 2022. *Information security, cybersecurity and privacy protection — Information security management systems.*

Jøsang and Pope, 2005. *User Centric Identity Management. AusCERT Asia Pacific Information Technology Security Conference.*

Kosta, E., 2013. *Consent in European Data Protection Law.*

Lynskey, 2015. *The Foundations of EU Data Protection Law.*

Marinescu, 2013. *Cloud Computing: Theory and Practice.*

Mather, Kumaraswamy and Latif, 2009. *Cloud Security and Privacy: An Enterprise Perspective on Risks and Compliance.*

Moneer, H., 2013. *Identity and Access Management in Cloud Environments: Security Challenges and Solutions.*

Mungoli, N., 2023a. *Adaptive Ensemble Learning: Boosting Model Performance through Intelligent Feature Fusion in Deep Neural Networks.*

Mungoli, N., 2023b. *Deciphering the Blockchain: A Comprehensive Analysis of Bitcoin's Evolution, Adoption, and Future Implications.*

Nida, Pinki, Harsh Dhiman & Shahnawaz Hussain, 2014. *A Survey on Identity and Access Management in Cloud Computing.*

Nieles. Dempsey and Pillitteri (NIST), 2017. *National Institute of Standards and Technology (2001) Special Publication 800-12 Rev. 1: An Introduction to Information Security.*

NIST:800-53, 2020. *National Institute of Standards and Technology Special Publication 800-53 Rev. 5: Security and Privacy Controls for Information Systems and Organizations.*

NIST:CSF 2.0, 2024. *National Institute of Standards and Technology, The NIST Cybersecurity Framework (CSF) 2.0.*

Okuhara, Shiozaki and Suzuki, 2010. *Security Architecture for Cloud Computing.*

Ponemon Institute, 2010. *Security of Cloud Computing Providers Study.*

Pormeister, K., 2017. *Genetic data and the research exemption: is the GDPR going too far?.*

Ralph, Stair and Reynolds, 2008. *Principles of Information Systems.* s.l.:s.n.

Rumbold and Pierscionek, 2017. *The Effect of the General Data Protection Regulation on Medical Research.*

Spindler and Schmechel, 2016. *Personal Data and Encryption in the European General Data Protection Regulation.*

Union Council of the European, 2016. *Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC.*