ΠΑΝΕΠΙΣΤΗΜΙΟ ΔΥΤΙΚΗΣ ΑΤΤΙΚΗΣ

ΣΧΟΛΗ ΜΗΧΑΝΙΚΩΝ

ΤΜΗΜΑ ΜΗΧΑΝΙΚΩΝ ΠΛΗΡΟΦΟΡΙΚΗΣ ΚΑΙ ΥΠΟΛΟΓΙΣΤΩΝ

ΔΙΠΛΩΜΑΤΙΚΗ ΕΡΓΑΣΙΑ

«Αρχιτεκτονική Δικτύων Μηδενικής Εμπιστοσύνης»

ΑΘΑΝΑΣΙΟΣ ΓΑΤΣΙΑΣ
Α.Μ. CSCYB 22028

Εισηγητής: Παναγιώτης Γιαννακόπουλος

ΜΑΡΤΙΟΣ 2024

(Κενό φύλλο)

ΔΙΠΛΩΜΑΤΙΚΗ ΕΡΓΑΣΙΑ

ΑΡΧΙΤΕΚΤΟΝΙΚΗ ΔΙΚΤΥΩΝ ΜΗΔΕΝΙΚΗΣ ΕΜΠΙΣΤΟΣΥΝΗΣ

Αθανάσιος Γάτσιας
CSCYB 22028

Εισηγητής:

Παναγιώτης Γιαννακόπουλος, Καθηγητής

Panagiotis Giannakopoulos
Digitally signed by Panagiotis Giannakopoulos
Date: 2024.04.26 22:33:33 +03'00'

Εξεταστική Επιτροπή:

Κωνσταντίνος Μαυρομάτης, Λέκτορας

Konstantinos Mavrommatis
Digitally signed by Konstantinos Mavrommatis
Date: 2024.04.29 09:54:56 +03'00'

Δημήτριος Κόγιας

Dimitrios Kogias
Digitally signed by Dimitrios Kogias
Date: 2024.04.26 22:24:18 +03'00'

Ημερομηνία εξέτασης 08/03/2024

(Κενό φύλλο)

ΔΗΛΩΣΗ ΣΥΓΓΡΑΦΕΑ ΜΕΤΑΠΤΥΧΙΑΚΗΣ ΕΡΓΑΣΙΑΣ

Ο κάτωθι υπογεγραμμένος Αθανάσιος Γάτσιας του Δημητρίου, με αριθμό μητρώου CSCYB 22028 φοιτητής του Τμήματος Μηχανικών Πληροφορικής και Υπολογιστών της Σχολής Μηχανικών του Πανεπιστημίου Δυτικής Αττικής, δηλώνω ότι:

«Βεβαιώνω ότι είμαι συγγραφέας της παρούσας διπλωματικής εργασίας και ότι έχω αναφέρει ή παραπέμψει σε αυτή, ρητά και συγκεκριμένα, όλες τις πηγές από τις οποίες έκανα χρήση δεδομένων, ιδεών, προτάσεων ή λέξεων, είτε αυτές μεταφέρονται επακριβώς (στο πρωτότυπο ή μεταφρασμένες) είτε παραφρασμένες. Επίσης βεβαιώνω ότι αυτή η εργασία προετοιμάστηκε από εμένα προσωπικά ειδικά για την συγκεκριμένη διπλωματική εργασία».

Ο Δηλών,

(Κενό φύλλο)

ΕΥΧΑΡΙΣΤΙΕΣ

Η παρούσα διπλωματική εργασία ολοκληρώθηκε μετά από επίμονες προσπάθειες, σε ένα ενδιαφέρον γνωστικό αντικείμενο, όπως αυτό της Αρχιτεκτονικής Δικτύων Μηδενικής Εμπιστοσύνης.

Για την προσπάθειά μου αυτή θα ήθελα να ευχαριστήσω την αγαπημένη μου σύζυγο Γεωργία, η οποία στάθηκε από την πρώτη στιγμή αρωγός στο εγχείρημά μου. Κλήθηκε να επωμιστεί το μεγαλύτερο βάρος διαχείρισης της οικογένειάς μου και ανατροφής των τριών παιδιών μου, παρέχοντάς μου αγόγγυστα πολύτιμο χρόνο και συμπαράσταση για να ολοκληρώσω τις σπουδές μου.

Επίσης θα ήθελα να ευχαριστήσω τον κ. Αθανάσιο Καλοφύρη, Διοικητή του τμήματος Πληροφορικής του Γενικού Επιτελείου Εθνικής Άμυνας, ο οποίος καθ' όλη την διάρκεια της επαγγελματικής συνεργασίας μας, αποτέλεσε για εμένα πρότυπο ανθρώπου, επαγγελματία και μέντορα. Το παράδειγμα του αποτέλεσε για εμένα κίνητρο ώστε να ασχοληθώ με τον ευρύτερο τομέα της ασφάλειας δικτύων πληροφορικής και την Αρχιτεκτονική Δικτύων Μηδενικής Εμπιστοσύνης.

(Κενό φύλλο)

ΑΦΙΕΡΩΣΗ

Στα παιδιά μου

Δημήτρη, Όλγα, Μαρία.

ΠΕΡΙΛΗΨΗ

Η εξέλιξη της τεχνολογίας και η ανεξέλεγκτη αύξηση του διαδικτύου σε συνδυασμό με την ταχεία εξάπλωση των κυβερνοαπειλών και των επιθέσεων στον κυβερνοχώρο, καθιστά επιτακτική την ανάγκη για σύγχρονες πρακτικές ασφαλείας και εμπιστοσύνης. Σε αυτό το πλαίσιο, η Μηδενική Εμπιστοσύνη αναδύεται ως κρίσιμη έννοια, προσφέροντας μια πρωτοποριακή προσέγγιση στην αρχιτεκτονική δικτύων, προσφέροντας νέες προοπτικές στην σχεδίαση και την υλοποίηση αυτών.

Στο πλαίσιο αυτό, η παρούσα διπλωματική αναλύει τις βασικές αρχές της Μηδενικής Εμπιστοσύνης και διερευνά μέσω πρακτικών εφαρμογών προηγμένες τεχνικές για την εφαρμογή της σε αρχιτεκτονικές δικτύων. Με στόχο τη δημιουργία συστημάτων που ανταποκρίνονται στις σύγχρονες προκλήσεις της ψηφιακής εποχής, η εργασία εξετάζει μεθόδους που ενισχύουν την ασφάλεια, ενώ παράλληλα διατηρούν την ευελιξία και την αποδοτικότητα των δικτύων.

ΕΠΙΣΤΗΜΟΝΙΚΗ ΠΕΡΙΟΧΗ: Ασφάλεια Δικτύων ΗΥ

ΛΕΞΕΙΣ ΚΛΕΙΔΙΑ: Μηδενική Εμπιστοσύνη, Αρχιτεκτονική, Δίκτυα

ABSTRACT

The relentless advancement of technology and the escalating ubiquity of the internet, accompanied by the swift proliferation of cyber threats and attacks in cyberspace, underscore the critical necessity for contemporary security and trust practices. In response to these challenges, Zero Trust emerges as a pivotal concept, presenting an innovative approach to network architecture and introducing fresh perspectives to their design and implementation.

The examination conducted in this thesis, delving into the foundational principles of Zero Trust. Through practical applications, the research explores advanced techniques for implementing Zero Trust in network architectures. The overarching objective is to develop systems that effectively address the modern challenges of the digital era by enhancing security, all the while preserving the flexibility and efficiency of networks.

ΣΥΝΤΟΜΟΓΡΑΦΙΕΣ

ZT	Zero Trust
ZTN	Zero Trust Networks
ZTA	Zero Trust Architecture
ZTNA	Zero Trust Networks Architecture
PKE	Public Key Encryption
LAN	Local Area Network
IPS	Intrusion Prevention System
IDS	Intrusion Detection System
SIEM	Security Information and Event Management
NGFW	Next Generation Firewall
MTTR	Mean Time To Respond
MTTD	Mean Time To Detect
VPN	Virtual Private Network
RBAC	Role Based Access Control
ABAC	Attribute Based Access Control
PAM	Privileged Access Management
IDSA	Identity Defined Security Alliance
IAM	Identity Access Management
VM	Virtual Machine
API	Application Programming Interfaces
DLP	Data Loss Prevention
PE	Policy Engine
PA	Policy Administrator
PDP	Policy Decision Point
PEP	Policy Enforcement Point
CDM	Continuous Diagnostics and Mitigation
ICS	Industry Compliance System
SDP	Software – Defined Perimeter
CASB	Cloud Access Security Broker
MFA	Multi-Factor Authentication
EDR	Endpoint Detection and Response

NAC	Network Access Control
UEBA	User and Entity Behavior Analytics
MDM	Mobile Device Management
SOAR	Security Orchestration, Automation and Response

Περιεχόμενα

Πίνακας Εικόνων

Zero Trust Networks Architecture

Εισαγωγή στον όρο "Zero Trust" και τη σημασία του στη σύγχρονη κυβερνοασφάλεια.

Το Zero Trust (ZT) αποτελεί μια στρατηγική προστασίας των πιο κρίσιμων περιουσιακών στοιχείων ενός οργανισμού. Η στρατηγική αυτή εστιάζει στην αποτροπή παραβιάσεων κυβερνοασφάλειας εξαλείφοντας το μεγαλύτερο τυφλό σημείο της ασφάλειας των δικτύων υπολογιστών, αυτό της εμπιστοσύνης. Από αυτό πηγάζει και η φράση που χαρακτηρίζει την στρατηγική αυτή «**Never Trust, Always Verify**». Αξίζει να επισημανθεί ότι ο όρος «Εμπιστοσύνη» αναφέρεται στις σχέσεις εμπιστοσύνης κατά την ανταλλαγή πακέτων δεδομένων μεταξύ υπολογιστικών συστημάτων και όχι στην εμπιστοσύνη μεταξύ ανθρώπων.

Το βασικό μήνυμα πίσω από τη στρατηγική ZT είναι η αντίληψη ότι η παραδοσιακή προσέγγιση της κυβερνοασφάλειας, που βασιζόταν στην εμπιστοσύνη προς το εσωτερικό δίκτυο, δεν ήταν αρκετή για την αντιμετώπιση των σύγχρονων κυβερνοαπειλών. Αντίθετα, προτείνεται μια προσέγγιση όπου η εμπιστοσύνη δεν παραχωρείται εκ των προτέρων, αλλά καθορίζεται και επιβεβαιώνεται συνεχώς. Μέσω της στρατηγικής ZT παρέχεται μια συλλογή από έννοιες και ιδέες που σχεδιάστηκαν για να ελαχιστοποιήσουν την αβεβαιότητα στη λήψη αποφάσεων σχετικών με παροχή δικαιωμάτων πρόσβασης, όσο το δυνατόν πιο περιορισμένα, σε πληροφοριακά συστήματα και υπηρεσίες ενός δικτύου που θεωρείται δυνητικά παραβιασμένο.

Η Αρχιτεκτονική Zero Trust (ZTA) είναι το σχέδιο κυβερνοασφάλειας μιας επιχείρησης που χρησιμοποιεί έννοιες του ZT και περιλαμβάνει τις σχέσεις των στοιχείων, το σχεδιασμό ροής εργασιών και τους κανόνες πρόσβασης. Συνεπώς, το Zero Trust Enterprise (ZTE) είναι η υποδομή δικτύου (φυσική και εικονική) και οι λειτουργικές πολιτικές που υπάρχουν για μια επιχείρηση, ως αποτέλεσμα ενός σχεδιασμού αρχιτεκτονικής μηδενικής εμπιστοσύνης[23].

Η έννοια του "Zero Trust" αναδύθηκε αρχικά από τον Τζον Κίντερβαγκ (John Kindervag), ο οποίος ήταν αναλυτής ασφάλειας στην Forrester Research. Ο Kindervag παρουσίασε για πρώτη φορά το μοντέλο Zero Trust στο έγγραφό του με τίτλο "No More Chewy Centers: Introducing The Zero Trust Model Of Information Security" [1] τον Αύγουστο του 2010. Από τότε, το μοντέλο Zero Trust έχει κερδίσει διεθνή αναγνώριση και έχει ενσωματωθεί στις πρακτικές κυβερνοασφάλειας πολλών επιχειρήσεων και οργανισμών. Εταιρίες όπως η Google με το BeyondCorp και η Microsoft με το Zero Trust Security in Microsoft 365 έχουν υιοθετήσει την προσέγγιση Zero Trust στην ασφάλεια των συστημάτων τους.

Η συνεχώς εξελισσόμενη κυβερνοασφάλεια και οι αυξανόμενες απειλές έχουν ενθαρρύνει ολοένα και περισσότερες εταιρίες και οργανισμούς να εξετάζουν και να υιοθετούν το μοντέλο Zero Trust για την προστασία των δικτύων και των δεδομένων τους. Χαρακτηριστική είναι η αναφορά του 2020 της εταιρείας Okta [2] η οποία δείχνει ότι περίπου το 60% των οργανισμών της Β. Αμερικής και περίπου το 40% παγκοσμίως εργάζονταν και συνεχίζουν να εργάζονται πάνω στο μοντέλο «Zero Trust».

Σκοπός και στόχοι της διπλωματικής εργασίας.

Ο σκοπός της διπλωματικής εργασίας είναι η διερεύνηση και η ανάλυση της στρατηγικής «Zero Trust» και η σημασία της στη σύγχρονη κυβερνοασφάλεια.

Μέσα από την διπλωματική εργασία επιδιώκονται:

α. Η κατανόηση του μοντέλου «Zero Trust» και πως διαφοροποιείται από τις παραδοσιακές προσεγγίσεις στην κυβερνοασφάλεια.
β. Ιστορική αναδρομή και εξέλιξη του «Zero Trust».
γ. Παρουσίαση της μεθοδολογίας του John Kindervag για την υλοποίηση του «Zero Trust» .
δ. Παρουσίαση και ανάλυση των αρχών σχεδίασης του μοντέλου «Zero Trust».
ε. Πλεονεκτήματα και προκλήσεις κατά την υλοποίηση του.
στ. Υλοποίηση σε επιχειρήσεις.
ζ. Προκλήσεις στην υιοθέτηση του μοντέλου Zero Trust.

Κεφάλαιο 1: Βάσεις Τεχνολογίας

1.1 Ιστορική εξέλιξη της ασφάλειας δικτύου.

Η έννοια της ασφάλειας δικτύων υπολογιστών αποτελεί πολυεπίπεδη και ουσιώδη πτυχή του χώρου της κυβερνοασφάλειας. Αναφέρεται στη συνολική προστασία των δικτύων υπολογιστών από πιθανούς κινδύνους, επιθέσεις, και απειλές που μπορούν να επηρεάσουν την ακεραιότητα, τη διαθεσιμότητα, και την εμπιστευτικότητα των δεδομένων.

α. Εμπιστευτικότητα (Confidentiality): Προστασία των δεδομένων από μη εξουσιοδοτημένη πρόσβαση. Αυτό επιτυγχάνεται μέσω κρυπτογραφικών μεθόδων και πολιτικών πρόσβασης.

β. Ακεραιότητα (Integrity): Εξασφάλιση ότι τα δεδομένα δεν έχουν τροποποιηθεί με μη εξουσιοδοτημένο τρόπο. Περιλαμβάνει τον έλεγχο των αλλαγών στα δεδομένα κατά τη μετάδοση ή την αποθήκευση τους.

γ. Διαθεσιμότητα (Availability): Προστασία από επιθέσεις που μπορεί να καταρρίψουν τη λειτουργικότητα. Βεβαιώνει ότι οι πόροι του δικτύου είναι διαθέσιμοι και προσβάσιμοι όταν χρειάζονται.

δ. Αυθεντικότητα (Authenticity): Βεβαιώνει την αξιοπιστία των διακριτικών οντοτήτων και των πληροφοριών. Πρόκειται για τη διασφάλιση ότι οι χρήστες ή τα συστήματα είναι αυτό που υποστηρίζουν ότι είναι.

ε. Ευθύνη (Accountability): Καταγραφή δραστηριοτήτων και αναγνώριση ατόμων ή συστημάτων που έχουν πραγματοποιήσει ενέργειες.

Η επίτευξη ασφάλειας στον τομέα αυτό απαιτεί τη συνδυαστική χρήση τεχνικών, διαδικασιών και πολιτικών ασφαλείας. Επιπλέον, η δυναμική φύση των απειλών και η συνεχής εξέλιξη της τεχνολογίας απαιτούν συνεχή ενημέρωση και προσαρμογή των πρακτικών ασφαλείας.

Η ιστορική εξέλιξη της ασφάλειας δικτύων καλύπτει πολλές δεκαετίες και είναι άρρηκτα συνδεδεμένη με τις αλλαγές της τεχνολογίας και την εξέλιξη των απειλών.

Ως αρχή της ασφάλειας δικτύων κρίνεται σκόπιμο να θεωρηθεί η δεκαετία του 50’, όπου αύτη την περίοδο η έννοια της ασφάλειας ΗΥ αρκούνταν στον περιορισμό ενός δυσαρεστημένου υπαλλήλου από το να προκαλέσει καταστροφές καθώς και στον περιορισμό των ανταγωνιστών από το να αποκτήσουν πρόσβαση στον ΗΥ της επιχείρησης. Δεν υπήρχε η έννοια του δικτύου ΗΥ και η ασφάλεια περιοριζόταν στην φυσική ασφάλεια διότι οι ΗΥ ήταν αποκομμένοι από τον έξω κόσμο.

Επόμενο ορόσημο αποτελεί η δεκαετία του 70’, όπου άρχισαν να εμφανίζονται τα πρώτα δίκτυα (ARPANET, 1969 - 1989)[3]. Κατά την περίοδο αυτή, καθόσον αυξάνονταν οι χρήστες που χρησιμοποιούσαν το δίκτυο, ενισχύθηκε και η ανάγκη για ανάπτυξη μηχανισμών και μέτρων ασφαλείας. Το 1969, η Defense Advanced Research Projects Agency (DARPA) προέβη στην έναρξη ενός ερευνητικού έργου με στόχο τη μελέτη των δικτύων δρομολόγησης πακέτων. Σε αυτό το πλαίσιο, προτάθηκε ένα σύστημα όπου μικρά μηνύματα μπορούσαν να μεταδίδονται μεταξύ δύο τερματικών συστημάτων, δρομολογούμενα μέσω ενδιάμεσων συστημάτων με ένα χαλαρά ιεραρχικό τρόπο. Αυτή η προσέγγιση επέτρεπε σε οποιονδήποτε χρήστη βρισκόταν στο δίκτυο να επικοινωνεί με άλλους, ανοίγοντας νέες διαστάσεις στην

επικοινωνία. Οι προσπάθειες αυτές έφεραν καρπούς στα τέλη της δεκαετίας του '70. Κατά το 1975, η IBM ανέπτυξε τον αλγόριθμο Data Encryption Standard (DES), προσφέροντας μια εξελιγμένη μέθοδο κρυπτογράφησης για τις ανάγκες της κυβέρνησης των Ηνωμένων Πολιτειών. Παράλληλα, οι Whitfield Diffie και Martin Hellman εισήγαγαν την έννοια της κωδικοποίησης δημόσιου κλειδιού (Public Key Encryption, PKE) που αποτέλεσε σημαντική εξέλιξη, λύνοντας το πρόβλημα της ασφαλούς ανταλλαγής κλειδιού. Το 1977, οι Rivest, Shamir και Adelman παρουσίασαν τον αλγόριθμο κρυπτογράφησης RSA, βασισμένο στην PKE, καθιερώνοντας τα θεμέλια για τη σύγχρονη ασφάλεια των δικτύων. Αυτές οι καινοτομίες διαμόρφωσαν το τοπίο της κυβερνοασφάλειας και αποτέλεσαν βασικό βήμα προς τη δημιουργία εξελιγμένων συστημάτων ασφαλείας στον κυβερνοχώρο.

Η αυγή της δεκαετίας του 80’ την βρίσκει επηρεασμένη από τον έγκλημα του Kevin Mitnick, ο οποίος κατάφερε να αποσπάσει πηγαίο κώδικα αξίας 80 εκατομμυρίων δολαρίων από διάφορες εταιρίες[4]. Η εισαγωγή και διάδοση των Local Area Networks (LANs) σηματοδότησε μια νέα εποχή στην κοινωνία της πληροφορικής. Με τη δημιουργία αυτών των τοπικών δικτύων, οι επιχειρήσεις και οργανισμοί αντιλήφθηκαν την ανάγκη για ενισχυμένη ασφάλεια, καθώς η πρόσβαση σε κοινόχρηστους πόρους έγινε πιο εύκολη και η επικοινωνία μεταξύ υπολογιστών αυξήθηκε σημαντικά. Μια από τις κύριες προκλήσεις που προέκυψαν ήταν η ανάγκη για προηγμένες μεθόδους ασφάλειας που θα προστάτευαν τα LANs από πιθανές απειλές. Σε αυτό το πλαίσιο, εμφανίστηκαν τα πρώτα λογισμικά antivirus. Τα λογισμικά antivirus κάλυψαν την ανάγκη για προστασία από κακόβουλο λογισμικό. Τα προγράμματα αυτά σάρωναν τους υπολογιστές για ενδείξεις κακόβουλου λογισμικού, προσπαθώντας να ανιχνεύσουν και να εξουδετερώσουν ενδεχόμενες απειλές. Συγκεκριμένα, τα πρώτα λογισμικά antivirus είχαν τη δυνατότητα να πραγματοποιούν σαρώσεις αρχείων για τυχόν ίχνη κακόβουλου κώδικα, αναγνώριση και ταυτοποίηση ιών βάση γνωστών υπογραφών και ενημέρωση της βάσης δεδομένων τους για αντιμετώπιση νέων ιών. Με την παρουσίαση αυτών των λογισμικών, η δεκαετία του '80 σηματοδότησε την έναρξη μιας πορείας προς την ενίσχυση της ασφάλειας των δικτύων, ανταποκρινόμενη στις νέες προκλήσεις που παρουσιάζονταν με την επέκταση των LANs.

Κατά τη δεκαετία του '90, παρατηρήθηκε μια σημαντική μετασχηματιστική περίοδος στον τομέα της κυβερνοασφάλειας. Η δεκαετία αυτή αντιπροσωπεύει μια εποχή εντατικής εξέλιξης, καθώς η τεχνολογία αντιμετωπίζει νέες προκλήσεις και απειλές. Την δεκαετία αυτή οι επιχειρήσεις αύξησαν τη χρήση του Διαδικτύου για επαγγελματικούς σκοπούς. Αυτή η διασύνδεση διέστειλε την επιθετική επιφάνεια και δημιούργησε νέες προκλήσεις για την ασφάλεια. Με την επέκταση του διαδικτύου, οι επιθέσεις από απομακρυσμένους επιτιθέμενους εντατικοποιήθηκαν, γεγονός που συνετέλεσε στην ανάπτυξη προηγμένων συστημάτων ανίχνευσης και λογισμικών πρόληψης εισβολών (IPS) για αντιμετώπιση των εξελιγμένων απειλών. Η ανάγκη για ενοποιημένες στρατηγικές ασφάλειας κατέστη εμφανής. Τα πρώτα λογισμικά διαχείρισης πληροφοριών και συμβάντων ασφαλείας (Security Information and Event Management, SIEM [5]) εμφανίστηκαν για να προσφέρουν ολοκληρωμένη διαχείριση των γεγονότων ασφαλείας και να διασφαλίσουν την καλύτερη προστασία των συστημάτων.

Η δεκαετία του 2000 αποτελεί περίοδο συνεχούς βελτιστοποίησης των τεχνολογιών και των ενοποιημένων λύσεων στον χώρο της κυβερνοασφάλειας. Χαρακτηριστική είναι η εξέλιξη των SIEM ως εργαλεία συλλογής, ανάλυσης και

αντίδρασης σε περιστατικά κυβερνοασφάλειας. Για την επίτευξη αυτού αναπτύχθηκαν εξελιγμένα firewalls με δυνατότητα λεπτομερούς ελέγχου των δεδομένων που αποστέλλονται μέσω ενός δικτύου Η/Υ (Deep Packet Inspection). Τα firewall είχαν τη δυνατότητα να ειδοποιούν, να καταγράφουν, να αποκλείουν και να δρομολογούν εκ νέου τα ελεγμένα πακέτα δεδομένων. Την δεκαετία αυτή κάνουν την εμφάνισή τους οι επιθέσεις Zero – Day οι οποίες εκμεταλλεύονταν λάθη ή παραλείψεις στον πηγαίο κώδικα των λογισμικών με σκοπό να υποκλέψουν πληροφορίες ή και να αποκτήσουν πρόσβαση σε υπολογιστικά συστήματα. Το γεγονός αυτό οδήγησε στην εξέλιξη των IDS/IPS για την αντιμετώπιση αυτών των επιθέσεων. Την ίδια εποχή παρατηρείται από τις μεγάλες εταιρείες και οργανισμούς η υιοθέτηση προγραμμάτων εκπαίδευσης και ευαισθητοποίησης των εργαζομένων τους σε θέματα ασφάλειας πληροφορικής.

Κατά τη δεκαετία του 2010, παρατηρήθηκαν σημαντικές εξελίξεις στον τομέα της κυβερνοασφάλειας. Η δεκαετία αυτή χαρακτηρίζεται από την ανάπτυξη αντιμετώπισης προηγμένων απειλών, την εισαγωγή νέων προσεγγίσεων ασφάλειας, και την αναγκαία προσαρμογή των οργανισμών στον εξελισσόμενο κυβερνοασφαλειακό τοπίο. Η δεκαετία αυτή χαρακτηρίζεται από την ραγδαία αύξηση των επιθέσεων ransomware. Αυτές οι επιθέσεις στοχεύουν στο να κλειδώσουν τα δεδομένα του θύματος και να απαιτήσουν λύτρα για την αποκατάσταση τους. Χαρακτηριστικό παράδειγμα η επίθεση WannaCry το 2017 η οποία έπληξε δεκάδες χιλιάδες επιχειρήσεις. Οι επιθέσεις αυτές οδήγησαν τις επιχειρήσεις και τους οργανισμούς να αναθεωρήσουν τις στρατηγικές τους για την προστασία των δεδομένων και των συστημάτων τους.

Η εξέλιξη των απειλών οδηγεί στην εμφάνιση της έννοιας του Zero Trust, η οποία αναδείχθηκε ως κρίσιμη για την κυβερνοασφάλεια. Σε αντίθεση με την παραδοσιακή προσέγγιση που βασίζεται στην εμπιστοσύνη προς το εσωτερικό δίκτυο, το Zero Trust υιοθετεί την αρχή της "μηδενικής εμπιστοσύνης" προς όλες τις συσκευές και τους χρήστες, ανεξάρτητα από την τοποθεσία τους. Παράλληλα εμφανίζονται προηγμένες προσεγγίσεις προστασίας που συνδυάζουν τεχνολογίες όπως το Machine Learning και η Τεχνητή Νοημοσύνη για ανίχνευση και αντιμετώπιση επιθέσεων.

Σήμερα, η κυβερνοασφάλεια εξελίσσεται σε ένα δυναμικό πεδίο που αντιμετωπίζει προηγμένες απειλές και προοπτικές. Οι κυβερνοεπιθέσεις εξελίσσονται σε πιο εξειδικευμένες και εκτεταμένες. Επιθέσεις όπως οι στοχεύσεις phishing, επιθέσεις με ransomware και εκμετάλλευση των ανθρώπινων ευαισθησιών είναι καθημερινές.

Η εκπαίδευση των χρηστών και η ευαισθητοποίησή τους παίζει καίριο ρόλο στην ασφάλεια. Οι οργανώσεις πλέον επικεντρώνονται στην ανάπτυξη κυβερνοασφαλών συμπεριφορών διότι μέσα από τη φιλοσοφία του Zero Trust καθίσταται σαφές ότι ο χρήστης είναι η πιο κρίσιμη επιφάνεια προστασίας καθόσον αποτελεί βέβαιο και πρωταρχικό στόχο των επιτιθέμενων.

Επίσης, καθώς οι επιχειρήσεις μετακινούν τα δεδομένα τους σε cloud υποδομές, η ασφάλεια στον τομέα αυτόν γίνεται προτεραιότητα. Στις υποδομές αυτές προστίθεται και ένα εκτεταμένο δίκτυο συσκευών IoT οι οποίες πλέον αποτελούν αναπόσπαστο μέρος της καθημερινότητας. Για την προστασία των υποδομών αυτών εφαρμόζονται προηγμένες λύσεις κρυπτογράφησης και διαχείρισης πρόσβασης. Τεχνολογίες όπως η Τεχνητή Νοημοσύνη και η Μηχανική Μάθηση χρησιμοποιούνται

για τον αυτόματο εντοπισμό και την αντιμετώπιση απειλών με γρήγορο και ακριβή τρόπο.

Η προσέγγιση της κυβερνοασφάλειας είναι πλέον παγκόσμια. Οι οργανισμοί συνεργάζονται για την αντιμετώπιση κοινών απειλών και για την άμεση αντίδρασή τους με σκοπό την μείωση του χρόνου ανίχνευσης και αντίδρασης (MTTR).

1.2 Βασικές Αρχές του μοντέλου Zero Trust

1.2.1 Κάστρο και Τάφρος

Προκειμένου να επιτευχθεί ευκολότερη κατανόηση της στρατηγικής υλοποίησης του Zero Trust, είναι σκόπιμο να προβληθεί σύγκριση με την προγενέστερη προσέγγιση ασφαλείας δικτύων, γνωστή ως "Κάστρο και Τάφρος" (Castle and Moat)[7], [8], [9], [56]. Το "Κάστρο και Τάφρος" δεν είναι απαραίτητα μια επιλογή στρατηγικής, αλλά ο όρος είναι συχνά χρησιμοποιούμενος για να αντιπαραβάλλει την παραδοσιακή αρχιτεκτονική δικτύου με την αρχιτεκτονική του Zero Trust.

Το μοντέλο ασφάλειας δικτύου "Κάστρο και Τάφρος" βασίζεται στην αδυναμία πρόσβασης οποιουδήποτε εκτός του δικτύου στα δεδομένα εντός του δικτύου, ενώ οι εσωτερικοί χρήστες έχουν ελεύθερη πρόσβαση. Σε αυτήν την αναπαράσταση, το δίκτυο μιας οργάνωσης παρομοιάζεται με ένα κάστρο, και η περίμετρος του δικτύου παρομοιάζεται με μια τάφρο. Μόλις ανοίξει η κρεμαστή γέφυρα και κάποιος τη διασχίσει, αποκτά ελεύθερη πρόσβαση στην έκταση του κάστρου. Αντίστοιχα, όταν ένας χρήστης συνδέεται σε ένα τέτοιο δίκτυο, μπορεί να ανακτήσει πρόσβαση σε όλες τις εφαρμογές και τα δεδομένα εντός αυτού.

Εικόνα 1: Μοντέλο Castle and Moat. ΠΗΓΗ: Cloudflare [11]

Οι οργανισμοί που χρησιμοποιούν αυτό το μοντέλο επενδύουν σημαντικούς πόρους στην προστασία της περιμέτρου του δικτύου, παραπλήσια με το πώς ένα κάστρο θα επέλεγε να τοποθετήσει τους περισσότερους φρουρούς κοντά στη γέφυρα.

Εφαρμόζουν προληπτικά μέτρα, όπως συστήματα ανίχνευσης παραβίασης (IDS), συστήματα πρόληψης παραβίασης (IPS) και άλλα προϊόντα ασφαλείας που εμποδίζουν τις περισσότερες εξωτερικές επιθέσεις. Ωστόσο, δεν είναι τόσο αποτελεσματικά στον περιορισμό εσωτερικών επιθέσεων, απειλών από εσωτερικούς παράγοντες και διαρροών δεδομένων.

Σήμερα, η προσέγγιση "Κάστρο και Τάφρος" θεωρείται παρωχημένη. Για τις περισσότερες εταιρείες, τα δεδομένα βρίσκονται σε πολλούς προμηθευτές υπηρεσιών στο cloud, αντί να παραμένουν πίσω από μια περίμετρο εταιρικού δικτύου. Για να επεκτείνουμε την αναλογία: δεν είναι λογικό να επικεντρώνουμε όλους τους πόρους μας στην άμυνα του κάστρου, αν η βασίλισσα και η αυλή της είναι διασκορπισμένες σε όλη την ύπαιθρο.

Ορισμένες εταιρείες συνεχίζουν να διατηρούν τα δεδομένα τους στις εγκαταστάσεις τους, ενώ άλλες καθοδηγούν όλη την κυκλοφορία που κατευθύνεται προς το Διαδίκτυο μέσω του κεντρικού εταιρικού δικτύου για να ελέγξουν την πρόσβαση των προμηθευτών υπηρεσιών στο cloud. Παρ' όλα αυτά, αυτές οι χρήσεις του μοντέλου "Κάστρο και Τάφρος" εξακολουθούν να παρουσιάζουν κενά ασφαλείας.

Εικόνα 2: Απεικόνιση σύγχρονης ανάγκης εκχώρησης πρόσβασης σε απομακρυσμένους χρήστες. Πηγή: NIST [10]

Το μεγαλύτερο πρόβλημα στην ασφάλεια είναι ότι αν ένας επιτιθέμενος καταφέρει να κερδίσει πρόσβαση στο δίκτυο — να διασχίσει τη "τάφρο" — τότε μπορεί επίσης να έχει πρόσβαση σε οποιαδήποτε δεδομένα και συστήματα μέσα σε αυτό. Μπορεί να παραβιάσει το δίκτυο κλέβοντας διαπιστευτήρια χρήστη, να εκμεταλλευτεί ευπάθειες στην ασφάλεια, να εισάγει κακόβουλο λογισμικό ή να εκτελέσει επιθέσεις κοινωνικής μηχανικής, ανάμεσα σε άλλες μεθόδους. Τα τείχη ασφαλείας (Firewalls) και άλλα εργαλεία πρόληψης εισβολών μπορεί να αποτρέψουν ορισμένες από αυτές τις επιθέσεις, αλλά αν κάποια περάσει, το κόστος είναι υψηλό.

Προκειμένου να μετριαστεί πρόβλημα αυτό, και με δεδομένο ότι λόγω της πανδημίας Covid-19 προέκυψαν πολλαπλάσιες ανάγκες απομακρυσμένης εργασίας, οι εταιρείες υιοθέτησαν την προσέγγιση ελέγχου πρόσβασης μέσω ιδιωτικών εικονικών δικτύων (Virtual Private Networks, VPN). Τα VPN προσέφεραν μια κρυπτογραφημένη σύνδεση μεταξύ των απομακρυσμένα συνδεδεμένων χρηστών και ενός VPN Server, και κατ' επέκταση με τα δεδομένα που απαιτούνταν για την εργασία τους. Για να καλυφθούν οι ανάγκες πρόσβασης με διαφορετικά δικαιώματα προσπέλασης για την κάθε κατηγορία χρήστη, οι εταιρείες δημιουργούσαν διαφορετικές συνδέσεις VPN. Παρόλο που επιτεύχθηκε ο έλεγχος πρόσβασης, υπήρξαν και τα εξής μειονεκτήματα [7]:

α. Ευπάθεια σε επιθέσεις: Καθόσον το VPN αποτελούσε μοναδικό σημείο αποτυχίας (Single Point of Failure), αρκεί ένας παραβιασμένος λογαριασμός ή συσκευή ώστε ο επιτιθέμενος να αποκτήσει πρόσβαση στα προστατευμένα δεδομένα.

β. Χαμηλή απόδοση: Η λειτουργία των VPN ορίζει πως όλη η δικτυακή κίνηση κρυπτογραφείται και διέρχεται μέσω ενός VPN Server. Το γεγονός αυτό απαιτεί πρόσθετη επεξεργαστική ισχύ και χρόνο περάτωσης με αποτέλεσμα να επιβραδύνει την κυκλοφορία δεδομένων στο δίκτυο.

γ. Επεκτασιμότητα: Αν η χρήση του VPN υπερβεί την ικανότητα του διακομιστή VPN να διαχειριστεί την κυκλοφορία, ο διακομιστής πρέπει να αναβαθμιστεί, διαδικασία που απαιτεί κόστος και εργατοώρες.

δ. Συντήρηση: Τα VPN απαιτούν πολύ χρόνο και πόρους για να διατηρηθούν. Οι ομάδες πληροφορικής πρέπει να εγκαταστήσουν τον κατάλληλο VPN client σε κάθε υπολογιστή του απομακρυσμένου εργαζομένου, να εξασφαλίσουν ότι οι υπάλληλοι διατηρούν αυτό το λογισμικό ενημερωμένο, και να αναβαθμίζουν ή να αντικαθιστούν τον VPN client τακτικά.

Ωστόσο, σχεδόν όλα τα περιστατικά κυβερνοασφαλείας και οι παραβιάσεις των εταιρικών δεδομένων πηγάζουν από την εκμετάλλευση των σχέσεων εμπιστοσύνης του μοντέλου αυτού. Αναπόφευκτα η άμυνα εις βάθος του μοντέλου Castle and Moat καταλήγει να είναι κόστος εις βάθος καθόσον μετά από κάθε επιτυχημένη παραβίαση, η περίμετρος θεωρούνταν ανασφαλής και αποδεσμεύονταν επιπλέον οικονομικοί πόροι για την ενίσχυσή της. Το μοντέλο αυτό εστιάζει στον καθορισμό της επιφάνειας δυνητικής επίθεσης ενός οργανισμού (attacking surface) αλλά η εξέλιξη της τεχνολογίας και κατά συνέπεια η εξέλιξη των μεθόδων επίθεσης καθιστά ασφαλής την υπόθεση ότι πλέον όλος ο ψηφιακός κόσμος αποτελεί δυνητική απειλή για τον οργανισμό. Οποιοδήποτε πρόσωπό η συσκευή στον κόσμο μπορεί να χρησιμοποιηθεί εκούσια ή ακούσια ως μέσω επίθεσης στον οργανισμό.

Λύση στα προβλήματα που παρουσιάζονται στο μοντέλο «Κάστρου και Τάφρου» έρχεται να δώσει το μοντέλο «Zero Trust». Το μοντέλο ZT έρχεται να καλύψει αυτή την αδυναμία αίροντας την πηγαία, κατά το μοντέλο, αιτία του προβλήματος, την έννοια της εμπιστοσύνης, όσον αφορά τα ψηφιακά συστήματα. Στο μοντέλο αυτό η φιλοσοφία η οποία ακολουθείται βασίζεται στην υπόθεση ότι υπάρχουν επιτιθέμενοι και δυνητικές απειλές τόσο εντός όσο και εκτός του ιδιωτικού δικτύου του οργανισμού. Κατά συνέπεια δεν μπορεί να υπάρχει οντότητα εντός του δικτύου η οποία να θεωρείται εν γένει έμπιστη. Για οποιαδήποτε απόκτηση πρόσβασης σε πόρους του δικτύου είναι απαραίτητο να έχει προηγηθεί αυθεντικοποίηση του χρήστη ή της υπηρεσίας που ζητάει την πρόσβαση αυτή. Προκειμένου να το πετύχει αυτό, το μοντέλο εστιάζει σε επιφάνειες μικρότερες αυτής

του κάστρου, τις οποίες μπορεί να ελέγξει. Οι επιφάνειες αυτές αναφέρονται στο μοντέλο ως επιφάνειες προστασίας (Protect Surfaces)[6].

Η υλοποίηση του μοντέλου είναι μοναδική για κάθε οργανισμό λόγω των ιδιαιτεροτήτων που παρουσιάζει ο κάθε οργανισμός. Ωστόσο, οι θεμελιώδεις αρχές σχεδιασμού του μοντέλου αποτελούν τη βάση πάνω στην οποία προσαρμόζεται η υλοποίηση σε κάθε οργανισμό. Οι θεμελιώδεις αυτές αρχές σύμφωνα με τον John Kindervag είναι[1]:

α. Η αρχή του Ελάχιστου Προνομίου (Least Privilege)

β. Η αρχή της μηδενικής εμπιστοσύνης (Zero Trust)

γ. Η αρχή του ελέγχου – επαλήθευσης ταυτότητας (Identity Verification)

δ. Η αρχή της επιτήρησης και ανίχνευσης (Monitoring and Detection)

ε. Η αρχή της Μικροτμηματοποίησης (Micro-Segmentation)

1.2.2 Η αρχή του Ελάχιστου Προνομίου (Least Privilege)

Η περιέργεια αποτελεί αναπόσπαστο κομμάτι της ανθρώπινης φύσης. Παρέχοντας εκτενή προνόμια πρόσβασης στους χρήστες, τους δίνεται η δυνατότητα εξερεύνησης των δεδομένων που δεν είναι απαραίτητα για την διεκπεραίωση της εργασίας τους. Με αυτόν τον τρόπο μετατρέπονται ακούσια (ή και εκούσια κάποιες φορές) στο μέσο παραβίασης που θα αξιοποιήσει ο επιτιθέμενος για να αποκτήσει πρόσβαση στα δεδομένα του οργανισμού. Για τον λόγο αυτό αποτελεί θεμελιώδη αρχή του μοντέλου Zero Trust ότι κάθε χρήστης ή συσκευή πρέπει να έχει μόνο τα απαραίτητα προνόμια (δικαιώματα) που απαιτούνται για την εκτέλεση συγκεκριμένων εργασιών.

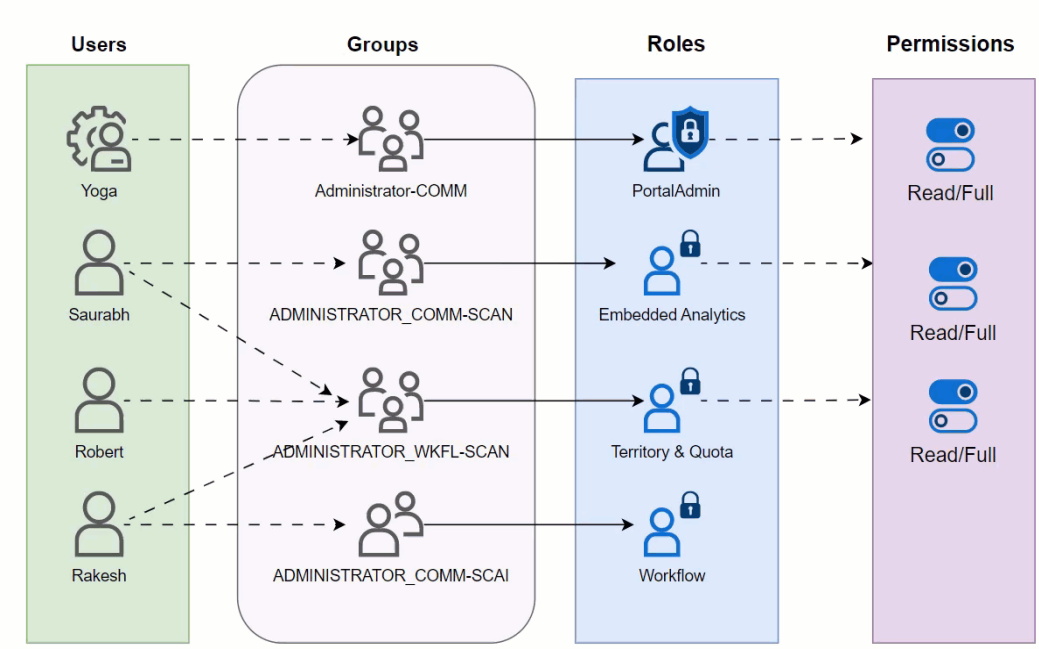
Σε πρακτικούς όρους, το προνόμιο, σε αυτό το πλαίσιο, αφορά στην εξουσιοδότηση που επιτρέπει σε έναν χρήστη ή διαδικασία να παρακάμψει συγκεκριμένους περιορισμούς ασφαλείας. Όταν αυτή η αρχή εφαρμόζεται σε άτομα, υποχρεώνει στην επιβολή του ελάχιστου δυνατού επιπέδου δικαιωμάτων χρήστη που είναι απαραίτητο για την ομαλή εκτέλεση των καθορισμένων ρόλων τους. Η λογική είναι να αποτρέπεται κάθε περιττή αναβάθμιση δικαιωμάτων που θα μπορούσε να οδηγήσει σε αθέμιτη ή επιδιωκόμενη επίθεση στην ασφάλεια.

Άξιο ενδιαφέροντος αποτελεί το γεγονός ότι το πεδίο εφαρμογής της αρχής του ελάχιστου προνομίου υπερβαίνει τον τομέα των ανθρώπινων αλληλεπιδράσεων για να περιλάβει διαδικασίες υπολογιστικών στοιχείων, εφαρμογές, συστήματα και εκτείνεται ακόμη και σε συσκευές εντός του οικοσυστήματος του Διαδικτύου των Πραγμάτων (IoT). Κάθε μία από αυτές τις οντότητες πρέπει να διαθέτει μόνο τα απολύτως απαραίτητα δικαιώματα και προνόμια για την εκτέλεση εξουσιοδοτημένων δραστηριοτήτων. Ο κύριος στόχος είναι να διασφαλιστεί ότι η πρόσβαση προσαρμόζεται ακριβώς στις λειτουργικές ανάγκες, αποφεύγοντας κάθε περιττή άδεια που θα μπορούσε να ανοίξει διόδους για κενά ασφαλείας.

Η επιβολή της προσέγγισης του ελάχιστου προνομίου αποτελεί σημαντική πρακτική στον τομέα της κυβερνοασφάλειας, λειτουργώντας ως προληπτικός μηχανισμός για τη μείωση των κινδύνων ασφαλείας και τη μείωση των πιθανών δυσλειτουργιών της επιχείρησης που προκαλούνται από σφάλματα ή κακόβουλες

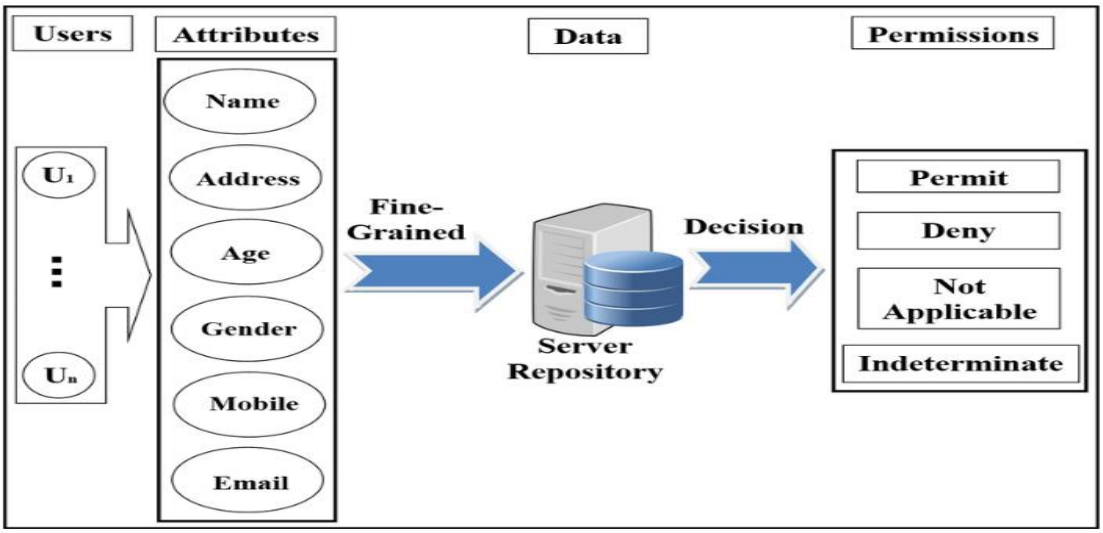
δραστηριότητες. Ουσιαστικά, λειτουργεί ως προληπτικός μηχανισμός ελέγχου που περιορίζει σημαντικά την επιφάνεια επίθεσης και μειώνει τις δυνατότητες επιπτώσεων από περιστατικά ασφαλείας.

Για την επίτευξή της αξιοποιούνται συστήματα ελέγχου πρόσβασης ανάλογα με το ρόλο (καθήκοντα) του κάθε χρήστη (Role – Based Access Control, RBAC)[13], [57]. Στα συστήματα αυτά κάθε χρήστης αντιστοιχίζεται σε έναν ή περισσότερους ρόλους ανάλογα με τη φύση και τις απαιτήσεις της εργασίας του και στη συνέχεια η δυνατότητα προσπέλασης αντιστοιχίζεται στον εκάστοτε ρόλο.



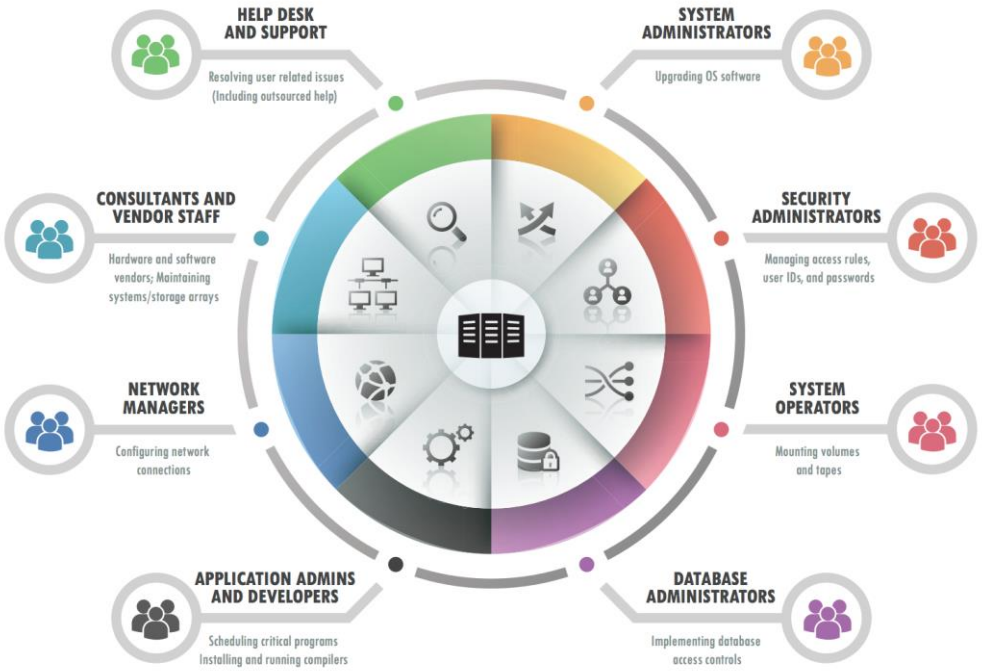
Εικόνα 3: Μοντέλο RBAC[14]

Πέραν των RBAC συστημάτων, υπάρχουν και τα συστήματα πρόσβασης με βάση τα χαρακτηριστικά του χρήστη, τους πόρους, τις ενέργειες και το περιβάλλον (χρόνος, τοποθεσία, συσκευή, πρωτόκολλο επικοινωνίας και ισχύς κρυπτογράφησης) που εμπλέκονται σε ένα αίτημα πρόσβασης (Attribute-Based Access Control, ABAC)[13] . Τα ABAC αντλούν τις πληροφορίες αυτές από λίστες ανθρώπινου δυναμικού και στη συνέχεια τις συγκρίνουν με διαμορφωμένες πολιτικές πρόσβασης για να εγκρίνουν ή να απορρίψουν την πρόσβαση.



Εικόνα 4: Μοντέλο ABAC [15] ΠΗΓΗ: ResearchGate

Επιπλέον στο μοντέλο Zero Trust χρησιμοποιούνται, ως λύση ελέγχου πρόσβασης, τα συστήματα διαχείρισης προνομιακής ταυτότητας (Privileged Access Management, PAM)[14], [58], τα οποία δίνουν τη δυνατότητα στους διαχειριστές να ελέγχουν, να διαχειρίζονται και να παρακολουθούν τα δικαιώματα πρόσβασης που έχουν οι χρήστες του οργανισμού σε κρίσιμους πόρους. Ως κρίσιμοι πόροι μπορούν να θεωρηθούν σημαντικά αρχεία, πληροφορίες και λογαριασμοί χρηστών, πηγαίος κώδικας και στοιχεία υποδομής.



Εικόνα 5: Privileged Access Management [17] ΠΗΓΗ: FORTRA

Η αναγκαιότητα της αρχής του ελάχιστου προνομίου έχει τονιστεί τα τελευταία χρόνια, ιδίως με το εξελισσόμενο τοπίο της κυβερνοασφάλειας που χαρακτηρίζεται από την άνοδο των σεναρίων απομακρυσμένης εργασίας, την επιταχυμένη μετάβαση στον χώρο του cloud και την εμφάνιση ενός περιβάλλοντος χωρίς περιμέτρους. Ακόμη και όταν οι υλοποιήσεις ασφαλείας εξελίσσονται προς μοντέλα μηδενικής εμπιστοσύνης και μοντέλα με κέντρο βάρους την έννοια της ταυτότητας (Identity – Centric), η εφαρμογή του ελάχιστου προνομίου παραμένει βασική, αποτελώντας αναπόσπαστο μέρος μιας ισχυρής αρχιτεκτονικής μηδενικής εμπιστοσύνης (ZTA) και στρατηγικής ασφαλείας ταυτότητας.

Ενώ το έργο της αρχής του ελάχιστου προνομίου φαίνεται απλό στη θεωρία, η αποτελεσματική του εφαρμογή μπορεί να είναι περίπλοκη και πολύπλευρη. Αυτή η πολυπλοκότητα πηγάζει από μια πληθώρα μεταβλητών, συμπεριλαμβανομένης της ποικιλίας των λειτουργικών συστημάτων (Windows, macOS, Unix, Linux), της εξάπλωσης των υπολογιστικών νεφών (cloud computing), της ανάπτυξης εφαρμογών και υπηρεσιών, και της πολυπλοκότητας των δικτύων και των συσκευών. Συνεπώς, η επιτυχής εφαρμογή απαιτεί τη συνεργασία των διαφόρων ενδιαφερόμενων μερών σε μια οργάνωση, συμπεριλαμβανομένων των διαχειριστών συστημάτων, των αναλυτών ασφαλείας, των προγραμματιστών εφαρμογών και των χρηστών.

Υπάρχουν αρκετά γνωστά περιστατικά κυβερνοεπιθέσεων που οφείλονται σε κατάχρηση δικαιωμάτων πρόσβασης από τους χρήστες, τα οποία υπογραμμίζουν τη σημασία της σωστής εφαρμογής της αρχής ελάχιστης πρόσβασης όπως παρακάτω[18]:

α. SolarWinds: Η SolarWinds έπεσε θύμα nation - state κυβερνοεπίθεσης, κατά την οποία επιτιθέμενοι (hackers) εισήλθαν στα συστήματα της εταιρείας και εισήγαγαν malware στον πηγαίο κώδικα της εφαρμογής Orion. Αυτό οδήγησε στην επίθεση των πελατών της SolarWinds όταν εφάρμοζαν αυτόματες ενημερώσεις, χρησιμοποιώντας την εφαρμογή Orion ως backdoor. Η ευπάθεια προήλθε επειδή η εφαρμογή Orion απαιτούσε πλήρη πρόσβαση, συγκεκριμένα, πλήρη κοινόχρηστη διαχειριστική πρόσβαση, για να λειτουργήσει. Το βασικό πρόβλημα είναι ότι οι διαχειριστικοί λογαριασμοί, με όλα τα προνόμια τους, συχνά απαιτούνται για να λειτουργούν σωστά παλαιότερες εφαρμογές όπως το Orion, καθιστώντας δύσκολο το να τηρηθεί η έννοια της διαχείρισης εφαρμογών με ελάχιστα προνομιακά δικαιώματα. Έτσι, οι επιτιθέμενοι είχαν πλήρη και ανεξέλεγκτη πρόσβαση για να λειτουργήσουν, δημιουργώντας μια πολύ μεγάλη επιφάνεια επίθεσης. Καθώς η εφαρμογή Orion ήταν ήδη επηρεασμένη, οι επιτιθέμενοι αξιοποίησαν την απεριόριστη πρόσβαση κατ' επέκταση σε όλα τα περιβάλλοντα των θυμάτων.

Για να αποτραπούν ή να αναχαιτιστούν αυτά τα περιστατικά προνομιακών δικαιωμάτων στις εφαρμογές, οι οργανισμοί πρέπει πρώτα να εντοπίσουν όλες τις εφαρμογές στο περιβάλλον τους που έχουν υψηλά επίπεδα προνομιακών δικαιωμάτων. Όπου είναι δυνατό, οι επιχειρήσεις πρέπει να εφαρμόσουν διαχείριση εφαρμογών με ελάχιστα προνομιακά δικαιώματα, αφαιρώντας όλα τα πλεονάζοντα. Ωστόσο, αυτό μπορεί να αποδειχθεί αδύνατο με πολλές παλαιότερες εφαρμογές. Σε ορισμένες περιπτώσεις, η καλύτερη στρατηγική αντιμετώπισης είναι η κατάργηση της εφαρμογής και η επιλογή νέου προμηθευτή/εφαρμογής για την κάλυψη των επιχειρηματικών αναγκών.

β. Verkada: Το 2020, η διαρροή της Verkada αποκάλυψε τις ζωντανές μεταδόσεις (live feeds) των 150.000 καμερών ασφαλείας που χρησιμοποιούνταν από

διάφορους πελάτες, συμπεριλαμβανομένων φυλακών, νοσοκομείων, κλινικών γυναικολογίας, ψυχιατρικών ιδρυμάτων, αστυνομικών τμημάτων, μεγάλων τεχνολογικών εταιρειών και άλλων. Η διαρροή της Verkada προήλθε από τα δικαιώματα του υπερ-διαχειριστή που ενσωματώθηκαν σε έναν κώδικα python που ήταν προσβάσιμος απομακρυσμένα. Οι επιτιθέμενοι απέκτησαν πρόσβαση διαχειριστή στις κάμερες της Verkada, επαυξάνοντας τα προνόμια τους σε "Υπερ-Διαχειριστή". Αυτός ο λογαριασμός υπερ-διαχειριστή/root επέτρεπε την πρόσβαση σε όλα τα feeds καμερών των πελατών της Verkada, επηρεάζοντας την ασφάλεια και την ιδιωτικότητα σε όλα τα περιβάλλοντα των πελατών.

Η εφαρμογή ελάχιστων προνομίων (αφαίρεση δικαιωμάτων διαχειριστή κλπ.) θα μπορούσε να βοηθήσει στην πρόληψη ή την αναχαίτιση αυτής της διαρροής, όπως και η επιβολή του διαχωρισμού των προνομιακών δικαιωμάτων και των καθηκόντων. Κανένας λογαριασμός δεν θα έπρεπε να κατέχει έλεγχο επί τόσων διαφορετικών λογαριασμών πελατών και να έχει τόσο υψηλά προνομιακά δικαιώματα σε τόσα πολλά συστήματα.

γ. NSA / Διαρροή Edward Snowden: Ως τεχνολογικός εργολάβος για την NSA, ο Edward Snowden είχε δικαιώματα διαχειριστή, ουσιαστικά για να εκτελεί δραστηριότητες όπως η δημιουργία αντιγράφων ασφαλείας και η μεταφορά δεδομένων σε τοπικούς διακομιστές. Ωστόσο, με τη κατάχρηση των δικαιωμάτων διαχειριστή και χρησιμοποιώντας κάποια απλά και ευρέως διαθέσιμα εργαλεία λογισμικού, συμπεριλαμβανομένου ενός αυτοματοποιημένου Web crawler, ο Snowden παραβίασε, αντέγραψε και διέρρευσε περίπου 1,7 εκατομμύρια αρχεία της NSA. Σε απάντηση στη διαρροή του Snowden, η NSA ανακοίνωσε την ανάληψη της πρωτοβουλίας να εξαλείψει το 90% των διαχειριστών συστημάτων, προκειμένου να περιορίσει την πρόσβαση και να βελτιώσει τη θέση της ως προς την αρχή της ελάχιστης προνομιακής πρόσβασης.

δ. Η Διαρροή στην Target: Η διαρροή στην Target του 2013 επηρέασε περίπου 70 εκατομμύρια πελάτες. Οι επιτιθέμενοι απέκτησαν μη εξουσιοδοτημένη πρόσβαση στα συστήματα της Target μέσω κλεμμένων διαπιστευτηρίων από έναν ανάδοχο θέρμανσης και κλιματισμού. Ο ανάδοχος είχε πρόσβαση στο δίκτυο της Target, συμπεριλαμβανομένων των δικαιωμάτων να μεταφορτώνει εκτελέσιμα αρχεία. Αυτά τα προνόμια ήταν πολύ περισσότερα από ό,τι απαιτούνταν για τη συντήρηση των συστημάτων. Με τον περιορισμό των δικαιωμάτων πρόσβασης στα ελάχιστα που απαιτούνται πραγματικά για την εταιρία θέρμανσης, η Target πιθανότατα θα είχε αποφύγει τη διαρροή και τις μετέπειτα επιπτώσεις. Η επιβολή της αρχής της ελάχιστης προνομιακής πρόσβασης για την πρόσβαση προμηθευτών αποτελεί κρίσιμη, αλλά συχνά παραμελημένη και ανεπαρκώς υλοποιημένη, πρακτική ασφαλείας.

Τέλος, είναι σημαντικό να σημειωθεί ότι η αρχή του ελάχιστου προνομίου δεν πρέπει να αντιμετωπίζεται ως ολοκληρωτικός περιορισμός, αλλά ως ένα κομμάτι του ευρύτερου παζλ της ασφάλειας πληροφορικής. Σε συνδυασμό με άλλα μέτρα ασφαλείας, όπως η παρακολούθηση της ασφάλειας, ο έλεγχος ταυτότητας, η κρυπτογράφηση και η επιτήρηση, συμβάλλει στην ενίσχυση του γενικού επιπέδου ασφαλείας ενός συστήματος πληροφορικής.

1.2.3 Η Αρχή της Μηδενικής Εμπιστοσύνης

Η Αρχή της Μηδενικής Εμπιστοσύνης αποτελεί καίρια πτυχή του μοντέλου ασφαλείας ZT και ορίζει μια φιλοσοφία όπου η εμπιστοσύνη δεν προκαθορίζεται για κανέναν χρήστη, συσκευή ή περιοχή του δικτύου. Κάθε αίτηση πρόσβασης θεωρείται ύποπτη μέχρις ότου επαληθευθεί η ταυτότητα του αιτούντος, χρησιμοποιώντας πολλαπλά στοιχεία επαλήθευσης καθώς και επιθεώρηση της συσκευής ή του χρήστη.

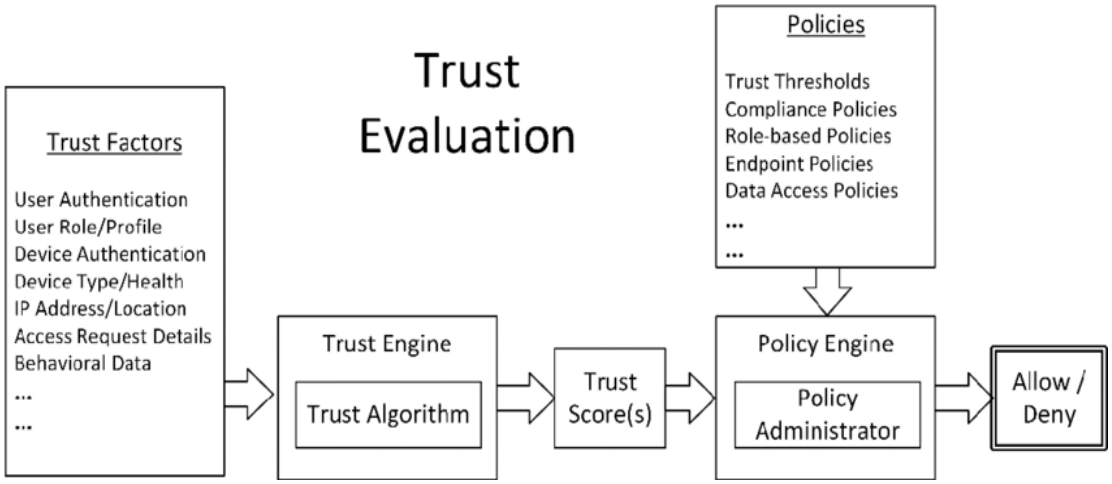
Η εφαρμογή της αρχής αυτής σημαίνει ότι κανένας χρήστης ή συσκευή δεν έχει αυτομάτως πρόσβαση σε ευαίσθητα δεδομένα ή πόρους. Κάθε προσπάθεια πρόσβασης αξιολογείται και επαληθεύεται με βάση πολλαπλούς παράγοντες, όπως η ταυτότητα, η συμπεριφορά χρήστη και η κατάσταση της συσκευής.

Ο στόχος είναι να δημιουργηθεί ένα περιβάλλον όπου η εμπιστοσύνη κερδίζεται με βάση τη συγκεκριμένη κατάσταση και τα δεδομένα, ανεξάρτητα από τον τόπο ή τη συσκευή του χρήστη. Αυτό εξασφαλίζει ότι ακόμη και αν κάποιος εξωτερικός παράγοντας αποκτήσει πρόσβαση σε ένα μέρος του δικτύου, δεν μπορεί αυτομάτως να εκμεταλλευτεί τα υπόλοιπα, προσφέροντας έτσι ένα επίπεδο προστασίας πέραν των παραδοσιακών μοντέλων ασφαλείας.

1.2.4 Η Αρχή του ελέγχου ταυτότητας

Η Αρχή του Ελέγχου ταυτότητας (Identity Verification) στο πλαίσιο του μοντέλου ZT αντιπροσωπεύει το πλέον κρίσιμο στοιχείο που στοχεύει στη διασφάλιση της αξιοπιστίας των χρηστών και των συσκευών που επιχειρούν να αλληλοεπιδράσουν με ένα σύστημα. Εξασφαλίζει ότι μόνο έγκυροι και αξιόπιστοι χρήστες και συσκευές έχουν πρόσβαση σε ευαίσθητα δίκτυα και πληροφορίες.

Παρότι το μοντέλο ZT αφορά ως επί το πλείστων υπολογιστικά συστήματα, η κύρια ιδέα του περιστρέφεται γύρω από την έννοια της ταυτότητας και την διαρκή αμφισβήτηση της εμπιστοσύνης προς αυτή. Παρότι αρκετές φορές συναντάται η λανθασμένη άποψη ότι ο ανθρώπινος παράγοντας αποτελεί τον πιο αδύναμο κρίκο στην ασφάλεια των πληροφοριακών συστημάτων, στην πραγματικότητα είναι αυτός που δέχεται τις περισσότερες επιθέσεις με σκοπό την υποκλοπή της ταυτότητάς του. Συνεπώς, η αμφισβήτηση της ταυτότητας στο μοντέλο Zero Trust δεν αφορά την αμφισβήτηση της ανθρώπινης οντότητας η οποία είναι απαραίτητο να χαίρει εμπιστοσύνης στον οργανισμό προκειμένου να είναι παραγωγική, αλλά την αμφισβήτηση του ψηφιακού αποτυπώματος της οντότητας κατά την αλληλεπίδρασή του με τα πληροφοριακά συστήματα.



Εικόνα 6: Διαδικασία αξιολόγησης εμπιστοσύνης. ΠΗΓΗ: RESEARCHGATE [12]

Η ταυτότητα είναι ο σχεσιακός παράγοντας μεταξύ των εργαζομένων, των πελατών και του οργανισμού. Θεωρείται η κορωνίδα των περιουσιακών στοιχείων του οργανισμού και κατά συνέπεια αποτελεί την πλέον πολύτιμη επιφάνεια προστασίας. Προκειμένου να διαχειριστεί ένας οργανισμός την έννοια της ταυτότητας, απαιτείται μια ολοκληρωτική κατανόηση του τρόπου με τον οποίο επηρεάζει τα πληροφοριακά συστήματα και την γενικότερη λειτουργία του οργανισμού. Δεδομένου ότι η ταυτότητα εμπεριέχει την έννοια της πιστοποίησης μιας οντότητας και των προσωπικών δεδομένων που συνδέονται με αυτή, καθίσταται σαφές ότι η διαδικασία διερεύνησης της έννοιας της ταυτότητας και του αντίκτυπου αυτής στον οργανισμό πρέπει να προηγείται οποιασδήποτε τεχνολογίας εφαρμοστεί για τον έλεγχο αυτής. Για τον λόγο αυτό υφίσταται η επιβεβλημένη υποχρέωση των οργανισμών να συμβαδίζουν με τις διατάξεις του Γενικού Κανονισμού Προστασίας Δεδομένων (GDPR) και των λοιπών νομοθετημάτων επι αυτού.

Στην κατεύθυνση αυτή, η Identity Defined Security Alliance (IDSA), παρέχει ένα πλαίσιο οδηγιών για την ασφάλεια της ταυτότητας και ποιά ψηφιακά συστήματα αλληλοεπιδρούν με αυτή [25]. Ο τρόπος αλληλεπίδρασης των συστημάτων καθορίζει και τον τρόπο με τον οποίο θα εφαρμοστεί η στρατηγική ZT. Συγκεκριμένα, για όλες τις επιφάνειες προστασίας, η πλήρης διαδικασία ταυτοποίησης από άκρο σε άκρο θα πρέπει να αναλυθεί στο στάδιο χαρτογράφησης της ροής δεδομένων της μεθοδολογίας εφαρμογής του μοντέλου ZT. Η διαδικασία αυτή αποσκοπεί αφενός, στη διασφάλιση ότι όλα τα στοιχεία της ταυτότητας που είναι διαθέσιμα, αξιοποιούνται κατά τη δημιουργία πολιτικών Μηδενικής Εμπιστοσύνης σε κάθε επιφάνεια προστασίας, αφετέρου, για κάθε ροή να προσδιοριστούν σημεία για επανέλεγχο της ταυτότητας που θα επηρεάζουν όσο το δυνατόν λιγότερο τον χρήστη.

Η σύνθεση του πλαισίου αποτελείται από τα κάτωθι 7 δομικά στοιχεία:

α. Ταυτότητα (Identity)

β. Συσκευή (Device)

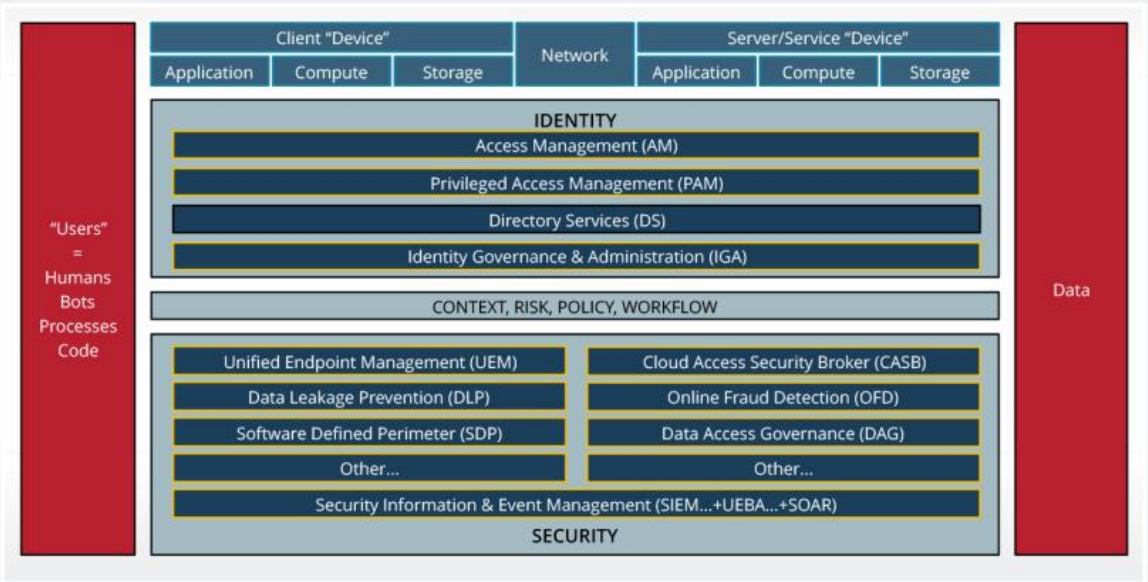
γ. Δίκτυο (Network)

δ. Επεξεργασία δεδομένων (Compute)

ε. Αποθηκευτικός χώρος (Storage)

στ. Εφαρμογή (Application)

ζ. Δεδομένα (Data)



Εικόνα 7: IDSA Framework[25]

Αυτά τα δομικά στοιχεία περιγράφουν το σύνολο των αλληλεπιδράσεων που μεταξύ του χρήστη και των πληροφοριακών συστημάτων σε ένα δίκτυο οργανισμού, και αποτελούν περιοχές όπου θα πρέπει να επαληθεύεται η ταυτότητα. Η σχέση και η αλληλεπίδραση μεταξύ των στοιχείων αυτών αποφέρει τη λογική πάνω στην οποία δημιουργούνται οι πολιτικές ασφαλείας.

Για την ανάπτυξη ενός αξιόπιστου μηχανισμού πιστοποίησης, προτείνεται η υιοθέτηση ενός Identity and Access Management (IAM) framework το οποίο περιλαμβάνει πολιτικές και τεχνολογίες για την διαχείριση των ψηφιακών ταυτοτήτων των χρηστών και των συστημάτων. Τα συστήματα που χρησιμοποιούνται για το IAM περιλαμβάνουν πολυπαραγοντικές μεθόδους επαλήθευσης ταυτότητας, χρησιμοποιώντας για παράδειγμα κωδικούς πρόσβασης, βιομετρική αναγνώριση, πιστοποιητικά καθώς και συστήματα διαχείρισης προνομιούχας πρόσβασης χρηστών, συστημάτων και διαδικασιών[27]. Η σωστή εφαρμογή αυτής της αρχής συμβάλλει στη δημιουργία ενός ασφαλούς περιβάλλοντος, εμποδίζοντας ανεπιθύμητη πρόσβαση και διασφαλίζοντας ότι μόνο εξουσιοδοτημένα άτομα και συσκευές έχουν πρόσβαση σε ευαίσθητα δεδομένα. Η χρήση πολυπαραγοντικών μεθόδων ενισχύει την ασφάλεια, δίνοντας περισσότερες δυνατότητες ελέγχου και παρέχοντας στους διαχειριστές τη δυνατότητα να εφαρμόζουν προσαρμοσμένες και αποτελεσματικές λύσεις ασφαλείας.

1.2.5 Επιτήρηση και Ανίχνευση (Monitoring and Detection)

Στο μοντέλο Zero Trust η επιτήρηση και η ανίχνευση του δικτύου θεωρούνται επιβεβλημένες. Μέσω της συνεχούς επιτήρησης της κίνησης του δικτύου καθίσταται δυνατή η ανίχνευση ανωμαλιών στη συνήθη ψηφιακή συμπεριφορά των χρηστών και ύποπτες δραστηριότητες (πχ κατέβασμα μεγάλου όγκου δεδομένων χωρίς προφανή αιτία). Για την επίτευξη αυτού, συστήματα παρακολούθησης και ανίχνευσης εφαρμόζονται σε όλα τα επίπεδα του δικτύου. Τα συστήματα αυτά παρέχουν, στους

αρμόδιους για την ασφάλεια του δικτύου, την διορατικότητα των γεγονότων που συμβαίνουν στο δίκτυό τους.

Παράλληλα η χρήση των μέσων αυτών δρα και ως αποτρεπτικό μέσο στους επίδοξους κακόβουλους χρήστες. Μέσω των συστημάτων αυτών καθίσταται δυνατή η επιτήρηση του δικτύου και η τήρηση αρχείων καταγραφής συμβάντων (inspection and logging). Η επιτήρηση εφαρμόζεται τόσο στο εσωτερικό δίκτυο όσο και εκτός του δικτύου ανεξάρτητα από την τοποθεσία ή τον τρόπο με τον οποίο συνδέεται ο χρήστης. Με τον τρόπο αυτό προστίθενται η έννοια και η δυνατότητα της επιτήρησης του κακόβουλου χρήστη στο εσωτερικό δίκτυο, έννοιες οι οποίες δεν είχαν υπόσταση σε προηγούμενα μοντέλα ασφαλείας.

1.2.6 Μικροτμηματοποίηση (Micro-Segmentation)

Η αρχή της Μικροτμηματοποίησης αποτελεί θεμέλιο λίθο στο πλαίσιο του μοντέλου ZT, συμβάλλοντας αποτελεσματικά στην προστασία των πληροφοριών και των πόρων μιας οργάνωσης. Αυτή η αρχή επικεντρώνεται στην εφαρμογή της ασφάλειας σε επίπεδο εφαρμογών, υποδεικνύοντας την ανάγκη για ακριβή και ευέλικτη προστασία.

Η Μικροτμηματοποίηση, ως στρατηγική κυβερνοασφάλειας, προσφέρει μια εξειδικευμένη προσέγγιση για την προστασία ενός Data Center. Αφορά μια λεπτομερή και λογική διαίρεση της συνολικής υποδομής σε διακριτικά τμήματα ασφαλείας, που φτάνει μέχρι το επίπεδο των διεργασιών κάθε εφαρμογής. Η Μικροτμηματοποίηση έρχεται σε αντίθεση προς την παραδοσιακή τμηματοποίηση δικτύου, η οποία συνήθως δημιουργεί υποδίκτυα εντός του συνολικού δικτύου.

Το βασικό χαρακτηριστικό της μικροτμηματοποίησης είναι ο λεπτομερής έλεγχος λειτουργίας στο επίπεδο των εφαρμογών (Εικονικών Μηχανών (VMs)) και των μεμονωμένων διεργασιών. Αυτό το επίπεδο λεπτομέρειας επιτρέπει στις εταιρείες να ορίζουν και να επιβάλλουν πολιτικές ασφαλείας με υψηλότερο βαθμό ακρίβειας. Σε αντίθεση με την τμηματοποίηση δικτύου, όπου η κύρια ιδέα έγκειται στη δημιουργία φραγμών εντός του δικτύου για τον περιορισμό της οριζόντιας δικτυακής κίνησης, η μικροτμηματοποίηση πηγαίνει ένα βήμα παραπέρα ασφαλίζοντας ανεξάρτητα κάθε εφαρμογή.

Στην πράξη, αυτό σημαίνει ότι κάθε εφαρμογή λειτουργεί εντός του δικού της τμήματος ασφαλείας, απομονωμένη από άλλες, διότι οι πολιτικές ασφαλείας προσαρμόζονται στις μοναδικές απαιτήσεις και ευαισθησίες κάθε εφαρμογής. Αυτό έχει ως αποτέλεσμα την ελαχιστοποίηση της επιφάνειας επίθεσης και τον περιορισμό της μη εξουσιοδοτημένης πρόσβασης. Είναι ένα προληπτικό μέτρο άμυνας που υπερβαίνει τις παραδοσιακές άμυνες που βασίζονται στο δίκτυο. Μέσω του ελέγχου της κίνησης της κάθε εφαρμογής, καθίσταται δυνατή η ελαχιστοποίηση του κινδύνου των απειλών για την ασφάλεια και η δημιουργία ενός μοντέλου ασφάλειας μηδενικής εμπιστοσύνης.

Για την υλοποίηση της απαιτείται κεντρική διαχείριση και μπορεί να εφαρμοστεί σε μεμονωμένες εφαρμογές παρέχοντας ένα πιο ασφαλές περιβάλλον χωρίς την πρόσθετη επιβάρυνση της συγκεκριμένης διαμόρφωσης του κεντρικού υπολογιστή. Εάν δεν υπάρχει η κεντρική διαχείριση, θα είναι δύσκολη η παρακολούθηση των

πολιτικών ασφαλείας σε διάφορες εφαρμογές ή κεντρικούς υπολογιστές. Μερικά από τα βασικά οφέλη που μπορούν να επιτευχθούν μέσω της μικροτμηματοποίησης είναι:

α. Καλύτερη παρακολούθηση της δικτυακής κίνησης καθόσον γίνονται διακριτά τα δεδομένα που μετακινούνται κατά την επικοινωνία μεταξύ των εφαρμογών.

β. Επιβολή πολιτικής ασφάλειας μέχρι το Επίπεδο Εφαρμογής (Layer 7), γεγονός που εξυπηρετεί την αυτοματοποίηση της διαδικασίας επιβολής πολιτικών και ανάπτυξης αντιμέτρων.

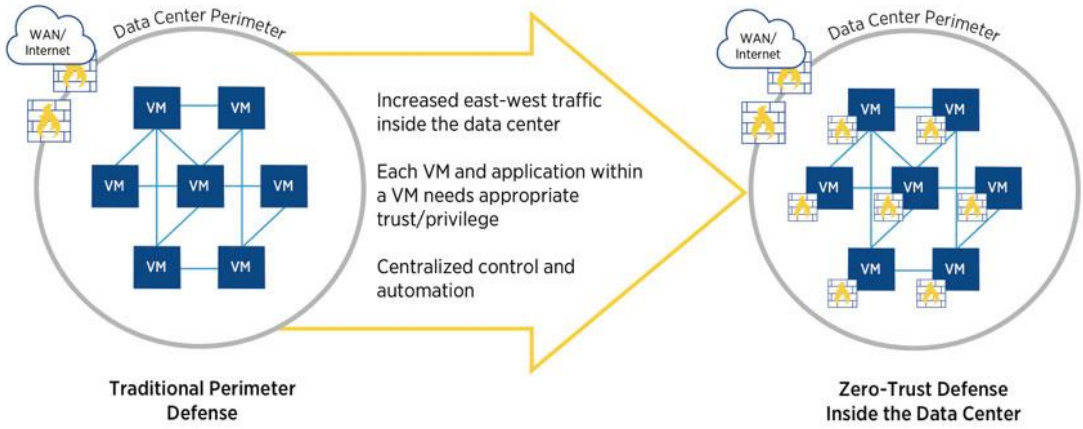
γ. Διατήρηση της ασφάλειας των κρίσιμων εφαρμογών, ακόμη και σε περίπτωση παραβίασης στην περίμετρο (Blast Radius) διότι περιορίζεται η οριζόντια κίνηση μεταξύ των εφαρμογών.

Από την άλλη πλευρά, η τμηματοποίηση δικτύου προσφέρει τα παρακάτω οφέλη:

α. Επιβολή ασφάλειας στην περίμετρο για προστασία από την είσοδο επιθέσεων.

β. Πιο απλή εφαρμογή σε σύγκριση με την μικροτμηματοποίηση.

Αξιοσημείωτο είναι ότι η μικροτμηματοποίηση απαιτεί υψηλή εξειδίκευση τεχνικού προσωπικού το οποίο μπορεί να κατανοήσει τις διεργασίες που εκτελεί μια εφαρμογή, σε αντίθεση με την τμηματοποίηση η οποία απαιτεί μέτρια εξειδίκευση.



Εικόνα 8: MIcro-Segmentation ΠΗΓΗ: NETRONOME[28]

Η έννοια του micro-segmentation δεν αναιρεί την έννοια της περιμέτρου. Αντιθέτως στοχεύει στην καθιέρωση της επιτήρησης, τον μετριασμό των κινδύνων και κατά συνέπεια την παροχή συνεχούς υποστήριξης στον σύγχρονο ψηφιακό κόσμο. Επιπλέον, αποσκοπεί στον μετριασμό της εξάπλωσης της επίθεσης διότι η προσβολή ενός τμήματος θα περιορίσει τις συνέπειες της επίθεσης εντός του τμήματος αυτού (Blast Radius), εμποδίζοντας την εξάπλωσή του στα υπόλοιπα τμήματα και την κυριαρχία του επιτιθέμενου σε όλο το περιβάλλον του δικτύου.

1.3 Εξέταση της σημασίας του Encryption και του Authentication στην επίτευξη του Zero Trust.

Η εξέταση της σημασίας του Encryption και του Authentication στο πλαίσιο της Μηδενικής Εμπιστοσύνης αναδεικνύει την αναγκαιότητα της χρήσης προηγμένων μεθόδων προστασίας στον ψηφιακό χώρο. Το μοντέλο Μηδενικής Εμπιστοσύνης αντιμετωπίζει κάθε συσκευή και εφαρμογή ως αναξιόπιστη, απαιτώντας επιβεβαίωση και πιστοποίηση κατά τη διάρκεια κάθε διαδρομής.

1.3.1 Ο Ρόλος της κρυπτογράφησης (Encryption)[19]

Η κρυπτογράφηση είναι θεμελιώδης για τη διασφάλιση του απόρρητου και της ακεραιότητας των δεδομένων. Στο πλαίσιο της Μηδενικής Εμπιστοσύνης, καθίσταται εμφανές ότι η κρυπτογράφηση κατέχει ζωτικό ρόλο στο να καθιστά τα δεδομένα αδύνατα στην κατανόηση και την παρέμβαση από μη εξουσιοδοτημένα πρόσωπα. Η κρυπτογράφηση αποτελεί καίριο στοιχείο της ασφάλειας δεδομένων, όντας ο απλούστερος και πιο ουσιαστικός τρόπος προστασίας των πληροφοριών ενός συστήματος υπολογιστή από κλοπή ή μη εξουσιοδοτημένη ανάγνωση από χρήστες με κακόβουλους σκοπούς.

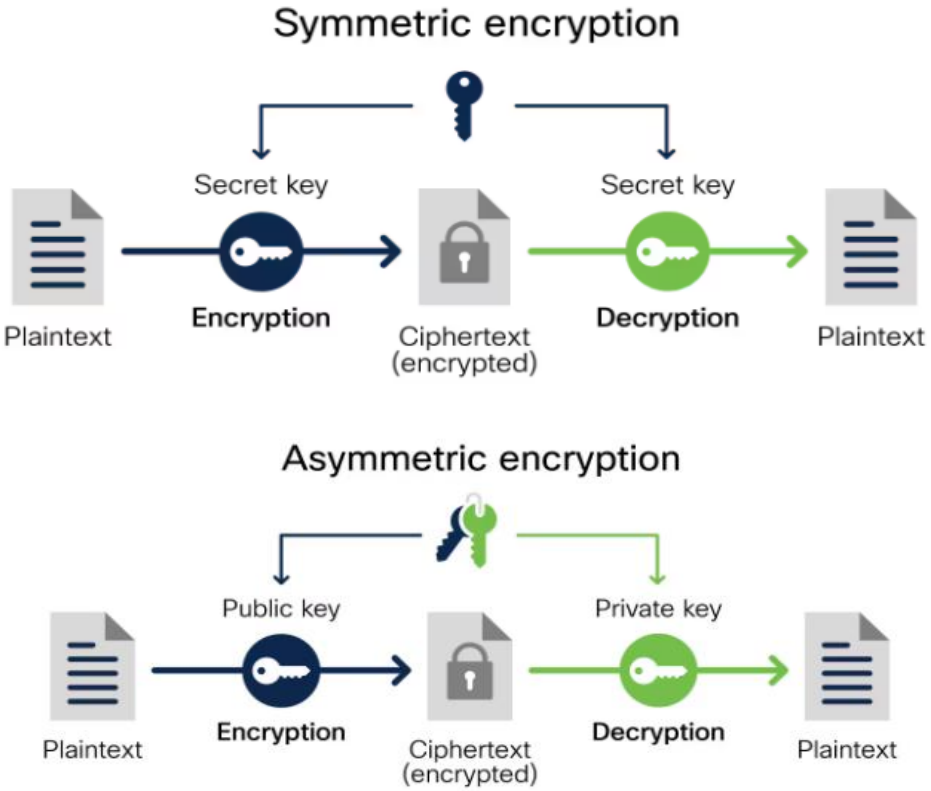
Η κρυπτογράφηση δεδομένων εφαρμόζεται ευρέως, τόσο από μεμονωμένους χρήστες όσο και από μεγάλες εταιρείες, προκειμένου να προστατεύσουν τις πληροφορίες χρήστη που μεταβιβάζονται μεταξύ ενός προγράμματος περιήγησης και ενός διακομιστή. Αυτές οι πληροφορίες μπορεί να αφορούν διάφορα, από δεδομένα πληρωμής μέχρι προσωπικά στοιχεία. Το λογισμικό κρυπτογράφησης δεδομένων, γνωστό και ως αλγόριθμος κρυπτογράφησης, χρησιμοποιείται για την κατασκευή σχημάτων κρυπτογράφησης που θεωρητικά δεν μπορούν να αποκρυπτογραφηθούν παρά μόνο με μεγάλη υπολογιστική ισχύ.

Η διαδικασία κρυπτογράφησης περιλαμβάνει τη μετατροπή του αναγνώσιμου κειμένου από τον άνθρωπο σε ακατανόητο κείμενο, γνωστό ως κρυπτογραφημένο κείμενο. Η κρυπτογράφηση επιτυγχάνεται με τη χρήση ενός κρυπτογραφικού κλειδιού, ενός συνόλου μαθηματικών τιμών που συμφωνούν τόσο ο αποστολέας όσο και ο παραλήπτης. Ο παραλήπτης χρησιμοποιεί το κλειδί για να αποκρυπτογραφήσει τα δεδομένα, επαναφέροντάς τα σε ευανάγνωστο απλό κείμενο. Η πολυπλοκότητα του κρυπτογραφικού κλειδιού καθορίζει την ασφάλεια της κρυπτογράφησης. Όσο πιο περίπλοκο είναι το κλειδί, τόσο η κρυπτογράφηση είναι πιο ασφαλής, καθώς είναι λιγότερο πιθανό να αποκρυπτογραφηθεί δοκιμάζοντας τυχαίους συνδυασμούς. Η κρυπτογράφηση χρησιμοποιείται επίσης για την προστασία των κωδικών πρόσβασης προκειμένου να διασφαλιστούν ότι δεν είναι αναγνώσιμοι από κακόβουλους χρήστες.

Εικόνα 9: Data Encryption ΠΗΓΗ: EGNYTE [20]

Οι δύο βασικές μέθοδοι κρυπτογράφησης είναι η συμμετρική και η ασύμμετρη κρυπτογράφηση. Η συμμετρική κρυπτογράφηση χρησιμοποιεί το ίδιο κλειδί για κωδικοποίηση και αποκωδικοποίηση, ενώ η ασύμμετρη χρησιμοποιεί δύο διαφορετικά κλειδιά, ένα δημόσιο και ένα ιδιωτικό, που συνδέονται μαθηματικά. Αυτές οι μέθοδοι κρυπτογράφησης παίζουν κρίσιμο ρόλο στη διασφάλιση των επικοινωνιών και των δεδομένων σε διάφορα περιβάλλοντα και εφαρμογές.

Ορισμένοι εκ των πιο γνωστών και χρησιμοποιούμενων αλγορίθμων κρυπτογράφησης περιλαμβάνουν τον αλγόριθμο κρυπτογράφησης DES (Data Encryption Standard). Το DES αναφέρεται στο "Πρότυπο Κρυπτογράφησης Δεδομένων" και αποτελεί έναν παρωχημένο αλγόριθμο συμμετρικής κρυπτογράφησης που δεν θεωρείται πλέον κατάλληλος για τις σύγχρονες ανάγκες. Λόγω αυτού, άλλοι προηγμένοι αλγόριθμοι κρυπτογράφησης έχουν αντικαταστήσει το DES.



Εικόνα 10: Συμμετρική και Ασύμμετρη μέθοδος κρυπτογράφησης. ΠΗΓΗ: CISCO [21]

Ένας από αυτούς είναι ο αλγόριθμος κρυπτογράφησης 3DES, που σημαίνει "Triple Data Encryption Standard". Πρόκειται για έναν συμμετρικό αλγόριθμο κλειδιού, με τη λέξη "τριπλό" να χρησιμοποιείται διότι τα δεδομένα υποβάλλονται σε τρεις επαναλήψεις του αλγορίθμου DES κατά τη διαδικασία κρυπτογράφησης. Παρά την σταδιακή απόσυρσή του, ο 3DES διατηρείται για εφαρμογές όπως οι χρηματοοικονομικές υπηρεσίες λόγω της αξιοπιστίας του ως λύσης κρυπτογράφησης υλικού.

Ο αλγόριθμος κρυπτογράφησης AES (Advanced Encryption Standard) αναπτύχθηκε για να αντικαταστήσει τον αρχικό αλγόριθμο DES και έχει ενσωματωθεί

ευρέως σε εφαρμογές ανταλλαγής μηνυμάτων, όπως το Signal και το WhatsApp, καθώς και σε προγράμματα συμπίεσης όπως το WinZip.

Ο αλγόριθμος ασύμμετρης κρυπτογράφησης RSA (Rivest, Shamir, Adleman) ήταν ο πρώτος ευρέως διαθέσιμος αλγόριθμος ασύμμετρης κρυπτογράφησης. Η δημοφιλία του οφείλεται στο μήκος των κλειδιών του και τη χρήση ενός ζεύγους κλειδιών.

Το Twofish, ένας αλγόριθμος κρυπτογράφησης που δεν κατοχυρώνεται με δίπλωμα ευρεσιτεχνίας, θεωρείται ένας από τους ταχύτερους στον τομέα του. Η ανοικτή του διαθεσιμότητα τον καθιστά ευρέως χρησιμοποιούμενο σε προγράμματα κρυπτογράφησης όπως το GPG και το TrueCrypt.

Ο αλγόριθμος κρυπτογράφησης RC4 χρησιμοποιείται σε πρωτόκολλα κρυπτογράφησης WEP και WPA, τα οποία είναι συνήθως χρησιμοποιούμενα σε ασύρματους δρομολογητές.

Η χρήση της κρυπτογράφησης κατά την μεταφορά δεδομένων προστατεύει την εμπιστευτικότητα των επικοινωνιών. Τα πρότυπα όπως το SSL/TLS αντιπροσωπεύουν την προηγμένη χρήση της τεχνολογίας κρυπτογράφησης για την εξασφάλιση ασφαλών συναλλαγών και επικοινωνιών.

1.3.2 Η Σημασία της Αυθεντικοποίησης (Authentication)

Η αυθεντικοποίηση[19] είναι ακόμα ένας πυλώνας πάνω στον οποίο στηρίζεται το μοντέλο Μηδενικής Εμπιστοσύνης. Στον χώρο της κυβερνοασφάλειας, η διαδικασία της αυθεντικοποίησης αφορά τον έλεγχο της ταυτότητας ενός ατόμου ή ενός στοιχείου. Η αυθεντικοποίηση συνήθως πραγματοποιείται μέσω ελέγχου ενός κωδικού πρόσβασης, ενός υλικού (token), ή άλλης πληροφορίας που αποδεικνύει την ταυτότητα. Όπως ένας υπάλληλος σε μια τράπεζα ελέγχει τα έγγραφα ενός πελάτη προτού του παραχωρήσει πρόσβαση στον λογαριασμό του, τα υπολογιστικά συστήματα πρέπει να διασφαλίζουν ότι ένα άτομο ή ένα στοιχείο είναι πράγματι αυτό που δηλώνει.

Η διαδικασία της αυθεντικοποίησης δεν εφαρμόζεται μόνο στους ανθρώπινους χρήστες. Τα υπολογιστικά συστήματα πρέπει επίσης να ελέγχουν τους διακομιστές, το λογισμικό, τις διεπαφές προγραμματισμού εφαρμογών (Application Programming Interfaces, API) και άλλους υπολογιστές για να διασφαλίσουν ότι είναι πράγματι αυτά που υποτίθεται ότι είναι. Σε μια εταιρεία παροχής υπηρεσιών ηλεκτρονικού εμπορίου, για παράδειγμα, η ταυτοποίηση εξασφαλίζει ότι μόνο εγκεκριμένοι εμπορικοί συνεργάτες έχουν πρόσβαση σε ευαίσθητα δεδομένα πελατών.

Η διαδικασία της αυθεντικοποίησης αποτελεί ζωτικό τμήμα της διαχείρισης ταυτότητας και πρόσβασης (Identity and Access Management, IAM), η οποία καθορίζει ποιος έχει πρόσβαση σε δεδομένα και τι είναι σε θέση να πράξει με αυτά. Εκτός από την εφαρμογή σε αυτόν τον τομέα, η ταυτοποίηση εφαρμόζεται και σε πολλούς άλλους τομείς της ασφάλειας όπως παρακάτω:

α. TLS (Ασφάλεια Μεταφοράς Επιπέδου): Η Ασφάλεια Μεταφοράς Επιπέδου (TLS) διαδραματίζει κρίσιμο ρόλο στην ασφάλεια των επικοινωνιών μεταξύ των διακομιστών ιστοσελίδων και των συσκευών χρηστών. Εξασφαλίζει την εμπιστευτικότητα και την ακεραιότητα των δεδομένων κατά τη μετάδοσή τους. Μια

από τις κρίσιμες του λειτουργίες είναι η αυθεντικοποίηση. Όταν ένας χρήστης αποκτά πρόσβαση σε μια ιστοσελίδα, το TLS εξασφαλίζει την ταυτότητα του διακομιστή για να διασφαλίσει ότι ο χρήστης αλληλοεπιδρά με την πραγματική ιστοσελίδα και όχι με κάποια παραπλανητική. Για παράδειγμα, ας υποθέσουμε ότι πραγματοποιείται μια σύνδεση στο διαδικτυακό τραπεζικό λογαριασμό ενός χρήστη. Η πιστοποίηση TLS εξασφαλίζει ότι η σύνδεση γίνεται με τον πραγματικό διακομιστή της τράπεζας, εμποδίζοντας τους κακόβουλους χρήστες από το να παρακολουθούν τα στοιχεία σύνδεσής του χρήστη παριστάνοντας την τράπεζα.

β. APIs (Διεπαφές Προγραμματισμού Εφαρμογών): Στο πλαίσιο των διαδικτυακών εφαρμογών, οι Διεπαφές Προγραμματισμού Εφαρμογών (APIs) είναι ουσιώδεις για τη δυνατότητα επικοινωνίας και ανταλλαγής δεδομένων μεταξύ διάφορων συστημάτων λογισμικού. Η σωστή ασφάλεια των APIs περιλαμβάνει μηχανισμούς αυθεντικοποίησης και για τις δύο άκρες της ενσωμάτωσης του API για να αποτραπούν μη εξουσιοδοτημένες προσβάσεις και δυνητικές επιθέσεις προς τα APIs. Έστω ότι ένας χρήστης χρησιμοποιεί μια τραπεζική εφαρμογή για smartphones που βασίζεται σε APIs για τη λήψη του υπολοίπου του λογαριασμού του. Τα APIs πιστοποιούν τόσο την εφαρμογή όσο και τον διακομιστή της τράπεζας. Αυτό εξασφαλίζει ότι μόνο η εξουσιοδοτημένη εφαρμογή μπορεί να αποκτήσει πρόσβαση στα στοιχεία του λογαριασμού του με ασφάλεια, προστατεύοντας τα χρηματοοικονομικά του δεδομένα από μη εξουσιοδοτημένη πρόσβαση.

γ. Πιστοποίηση Email: Τα e-email είναι ένα σύγχρονο και αναπόσπαστο μέσο επικοινωνίας στην καθημερινότητα και η πιστοποίησή τους είναι κρίσιμη για την πρόληψη του phishing και τη διασφάλιση της ακεραιότητας των μηνυμάτων. Το Domain Key Identified Mail (DKIM) είναι ένα ευρέως χρησιμοποιούμενο μέσο πιστοποίησης email. Προσθέτει μια ψηφιακή υπογραφή στα εξερχόμενα email, επαληθεύοντας ότι προέρχονται από έναν εξουσιοδοτημένο διακομιστή που συνδέεται με τον δηλωμένο τομέα (π.χ. @cloudflare.com, @google.com κλπ.). Τα μη επαληθευμένα email συνήθως καταλήγουν στους φακέλους ανεπιθύμητης αλληλογραφίας. Για παράδειγμα ας υποθέσουμε ότι ο χρήστης λαμβάνει ένα email που ισχυρίζεται ότι προέρχεται από την πλατφόρμα online αγορών του. Η πιστοποίηση DKIM διαβεβαιώνει ότι το email προήλθε πράγματι από τους επίσημους διακομιστές της πλατφόρμας, μειώνοντας τον κίνδυνο να πέσει ο χρήστης θύμα phishing που προσπαθεί να μιμηθεί την εμφάνιση της νόμιμης υπηρεσίας.

δ. Το παράδειγμα του Windows Hello στη Microsoft: Η τεχνολογία Windows Hello είναι μια τεχνολογία αυθεντικοποίησης που εισήχθη από τη Microsoft ως εναλλακτική μέθοδος εισόδου στα Windows 10 και 11. Η βασική ιδέα είναι να προσφέρει πιο ασφαλείς και βολικές μεθόδους για την είσοδο στον υπολογιστή, αντί του παραδοσιακού κωδικού πρόσβασης. Τα βασικά χαρακτηριστικά του Windows Hello περιλαμβάνουν δυνατότητες αναγνώρισης προσώπου, αναγνώρισης δαχτυλικών αποτυπωμάτων και πιστοποίηση μέσω PIN. Μέσα από το Windows Hello η Microsoft υπογραμμίζει πώς η χρήση προηγμένων τεχνικών Authentication συμβάλλει στην αποτροπή μη εξουσιοδοτημένης πρόσβασης.

Το Windows Hello αποτελεί ένα μηχανισμό αυθεντικοποίησης όπου στα πλαίσια βελτιστοποίησης της εμπειρίας του χρήστη, παρέχει τη δυνατότητα πρόσβασης σε πολλαπλά συστήματα με μια μεμονωμένη αυθεντικοποίηση (Single Sign On), μειώνοντας έτσι τον αριθμό των κωδικών πρόσβασης που θα πρέπει να θυμάται ο χρήστης. Εκ πρώτης όψεως οι μηχανισμοί SSO φαίνεται να λειτουργούν

ενάντια στη φιλοσοφία της αρχιτεκτονικής Zero Trust. Στην πραγματικότητα όμως οι μηχανισμοί SSO παρέχουν τα εξής οφέλη:

α. Δεδομένου ότι παρέχεται η ευκολία στο χρήστη να θυμάται ένα μόνο κωδικό ή να χρησιμοποιεί κάποιο βιομετρικό μέσο αυθεντικοποίησης, μειώνονται οι επιλογές του επιτιθέμενου στο να υποκλέψει τον κωδικό αυτό και παράλληλα βοηθάει τον χρήστη στο να επιλέγει μεγαλύτερους και πιο σύνθετους κωδικούς πρόσβασης.

β. Παρά την χρήση ενός μόνο κωδικού πρόσβασης το μοντέλο Zero Trust συνεχώς παρακολουθεί και επικυρώνει τις δραστηριότητες του χρήστη, της συσκευής του και των δικαιωμάτων πρόσβασής του. Επίσης, αξιοποιώντας τις δυνατότητες των εργαλείων που απαρτίζουν το μοντέλο Zero Trust (συστήματα IDS-IPS), δύναται να εντοπιστούν ανωμαλίες στην συνήθη συμπεριφορά του χρήστη και της συσκευής και με βάση αυτές να αποκλειστεί η πρόσβαση.

Συνολικά, η Κρυπτογράφηση και η Αυθεντικοποίηση αποτελούν κρίσιμα στοιχεία στον τομέα της ασφάλειας πληροφορικής και αναδύονται ως ουσιαστικά εργαλεία για την προστασία των ψηφιακών περιουσιών. Εντοπίζονται στον πυρήνα της ασφάλειας των συστημάτων πληροφορικής, καθιστώντας τα εκ των σημαντικότερων στοιχείων για τη διασφάλιση της ακεραιότητας, της εμπιστευτικότητας, και της διαθεσιμότητας των δεδομένων.

Στο πλαίσιο της Μηδενικής Εμπιστοσύνης, η Κρυπτογράφηση και η Αυθεντικοποίηση αναδεικνύονται ως ουσιώδεις παράγοντες, διαμορφώνοντας ένα ασφαλές περιβάλλον βασισμένο στην αρχή της αμφιβολίας και της αυστηρής επαλήθευσης της ταυτότητας. Η ενοποιημένη εφαρμογή αυτών των αρχών επιτυγχάνει μια ισχυρή άμυνα ενάντια σε εξωτερικές απειλές, δημιουργώντας ένα ανθεκτικό σύστημα που αντιμετωπίζει αποτελεσματικά τις προκλήσεις του σύγχρονου κυβερνοχώρου.

Με τη συνδυαστική εφαρμογή Κρυπτογράφησης και Αυθεντικοποίησης, επιτυγχάνεται η δημιουργία ενός περιβάλλοντος που προάγει την ασφαλή λειτουργία ψηφιακών πλατφορμών. Η αρχή της Μηδενικής Εμπιστοσύνης αντικατοπτρίζεται στην ουσιαστική ανάγκη για συνεχή αναθεώρηση και ενίσχυση των πρακτικών ασφαλείας, προκειμένου να αντιμετωπιστούν εξελισσόμενες κυβερνοαπειλές και να διασφαλιστεί η αντοχή του συστήματος απέναντι σε πιθανές επιθέσεις.

Κεφάλαιο 2: Στρατηγική Υλοποίησης του Zero Trust

Το Zero Trust δεν είναι ένα συγκεκριμένο ψηφιακό εργαλείο αλλά η ενοποίηση μιας πληθώρας διαφορετικών εργαλείων σε ένα ενιαίο σύστημα. Επίσης, τα εργαλεία αυτά καθώς και η παραμετροποίησή τους, δεν είναι τυποποιημένη διότι κάθε οργανισμός παρουσιάζει μοναδικά χαρακτηριστικά οργάνωσης και λειτουργίας.

Προκειμένου, λοιπόν, να υλοποιηθεί το μοντέλο, η αρχιτεκτονική του εστιάζει σε τέσσερις αρχές σχεδίασης όπως παρακάτω[6]:

α. Εστίαση στα επιχειρηματικά αποτελέσματα. Η αρχή αυτή αφορά στην κατανόηση του τρόπου με τον οποίο ο οργανισμός παράγει κέρδος. Συνεπώς, είναι απαραίτητος ο εναρμονισμός των πολιτικών ασφαλείας στο ευρύτερο πλαίσιο επιχειρηματικής στρατηγικής που οδηγεί στην παραγωγή κέρδους. Το μοντέλο Zero Trust καλείται να προστατέψει όλα εκείνα τα μέσα τα οποία συμμετέχουν στην επιχειρηματική στρατηγική.

β. Σχεδίαση από μέσα προς τα έξω. Η αρχή αυτή αφορά στον σαφή καθορισμό των στοιχείων που χρήζουν προστασίας και αποτελεί την διαφορά προσέγγισης στην υλοποίηση της ασφάλειας μεταξύ του μοντέλου Zero Trust και του μοντέλου Κάστρου – Τάφρου. Με βάση την αρχή αυτή, πρώτα πρέπει να σχεδιάζεται η ασφάλεια σε κάθε στοιχείο μεμονωμένα και στη συνέχεια να επεκτείνεται προς την περίμετρο του συνόλου των στοιχείων.

γ. Καθορισμός του ποιος / τι χρειάζεται πρόσβαση. Η αρχή αυτή αφορά στην υιοθέτηση της αρχής του ελάχιστου προνομίου και την εκχώρηση των πλέον αναγκαίων δικαιωμάτων πρόσβασης στα στοιχεία για την ορθή και εύρυθμη λειτουργία τους. Χαρακτηριστικό παράδειγμα αυτής της αρχής είναι η λανθασμένη εκχώρηση αναβαθμισμένων δικαιωμάτων πρόσβασης σε μέλη της διοίκησης ενός οργανισμού για λόγους γοήτρου και όχι λόγω αναγκαιότητας της εργασίας τους.

δ. Επιθεώρηση και καταγραφή όλης της δικτυακής κίνησης. Η αρχή αυτή αφορά στην προσπάθεια εντοπισμού κακόβουλης ή αδικαιολόγητης δικτυακής κίνησης, για παράδειγμα πολλαπλές συνδέσεις εκτός του εταιρικού δικτύου ή αυξημένου όγκου αντιγραφής αρχείων. Η αρχή αυτή δεν αφορά στην παρακολούθηση της επικοινωνίας των χρηστών, γεγονός που συνιστά παραβίαση προσωπικών δεδομένων. Εστιάζει αποκλειστικά, στον έλεγχο και στην καταγραφή της ροής των δεδομένων στο δίκτυο.

Για την εφαρμογή των προαναφερθέντων αρχών υπάρχουν πέντε γενικά στάδια υλοποίησης τα οποία προσαρμόζονται στον εκάστοτε οργανισμό όπως παρακάτω:

α. Καθορισμός της επιφάνειας προστασίας.

β. Καταγραφή της δικτυακής κίνησης μεταξύ των συστημάτων.

γ. Σχεδίαση ενός περιβάλλοντος Zero Trust.

δ. Δημιουργία πολιτικών ασφαλείας με βάση το μοντέλο Zero Trust.

ε. Παρακολούθηση και συντήρηση του μοντέλου.

2.1 Καθορισμός της επιφάνειας προστασίας

Συνήθως, το περιβάλλον ενός οργανισμού αποτελείται από μια τεράστια έκταση αλληλένδετων στοιχείων, τα οποία συντελούν στην επίτευξη της επιχειρηματικής στρατηγικής. Προκειμένου να υλοποιηθεί το μοντέλο Zero Trust, το περιβάλλον αυτό πρέπει να κατατμηθεί σε μικρότερα τμήματα τα οποία στη συνέχεια, θα κατηγοριοποιηθούν ανάλογα με το βαθμό αντικτύπου τους στον οργανισμό. Αυτά τα μικρότερα τμήματα αποτελούν τις επιφάνειες προστασίας (Protect Surfaces) στις οποίες εστιάζει το μοντέλο Zero Trust.

Ένα δίκτυο Zero Trust καθορίζει μια επιφάνεια προστασίας με βάση τουλάχιστον ένα από τα τέσσερα ακόλουθα στοιχεία, τα οποία αποτυπώνονται από το ακρωνύμιο DAAS[22]:

α. Δεδομένα (Data): Ποια δεδομένα απαιτούν προστασία.

β. Εφαρμογές (Applications): Ποιες εφαρμογές εμπεριέχουν και επεξεργάζονται ευαίσθητες πληροφορίες.

γ. Περιουσιακά Στοιχεία (Assets): Ποια περιουσιακά στοιχεία είναι ευαίσθητα.

δ. Υπηρεσίες (Services): Ποιες υπηρεσίες, όπως DNS, DHCP και Active Directory, μπορούν να πέσουν θύματα επίθεσης.

Το χαρακτηριστικό της επιφάνειας προστασίας είναι ότι όχι μόνο είναι τάξεις μεγέθους μικρότερη από τη συνολική επιφάνεια επίθεσης, αλλά είναι πάντα γνωστή ή εύκολα διακριτή. Για να γίνει εύκολα κατανοητή η έννοια της επιφάνειας προστασίας, μπορεί να χρησιμοποιηθεί ως παράδειγμα η φυσική ασφάλεια ενός οργανισμού. Μέσα στο κτίριο του οργανισμού υπάρχουν διάφοροι χώροι οι οποίοι έχουν διαφορετική βαρύτητα από άποψη ασφάλειας, όπως για παράδειγμα ο χώρος των γραφείων των υπαλλήλων, ο χώρος διαλλείματος, το data center και ο χώρος των έντυπων αρχείων και των αντιγραφικών μηχανημάτων. Γίνεται εύκολα αντιληπτό ότι αφενός, ο οργανισμός δεν μπορεί να αρκείται στον έλεγχο εισόδου στην κεντρική είσοδο του οργανισμού και στη συνέχεια να επιτρέπει στο σύνολο των εργαζομένων να έχουν πλήρη φυσική πρόσβαση σε όλους τους χώρους, και αφετέρου ότι δεν απαιτούνται ίδιας βαρύτητας μέτρα ελέγχου εισόδου στο Data Center και στο χώρο διαλείμματος. Ωστόσο, οι περισσότεροι οργανισμοί δεν μπορούν πραγματικά να καθορίσουν την επιφάνεια επίθεσης, γι' αυτό, οι ειδικοί σε δοκιμές διείσδυσης καθώς και οι επιτιθέμενοι, σχεδόν πάντα καταφέρνουν να εισέλθουν στην περίμετρο ασφαλείας και κατ’ επέκταση στο εσωτερικό δίκτυο του οργανισμού. Αυτός είναι και ο λόγος που η ιδέα μιας προσέγγισης ασφάλειας βασισμένης σε μεγάλες περιμέτρους έχει αποδειχθεί ανεπιτυχής. Στο παλιό μοντέλο, οι έλεγχοι όπως τα firewalls και οι τεχνολογίες πρόληψης διείσδυσης (IDS -IPS) εφαρμόζονται στην εξωτερική περίμετρο, που συνήθως απέχει πολύ από την επιφάνεια προστασίας.

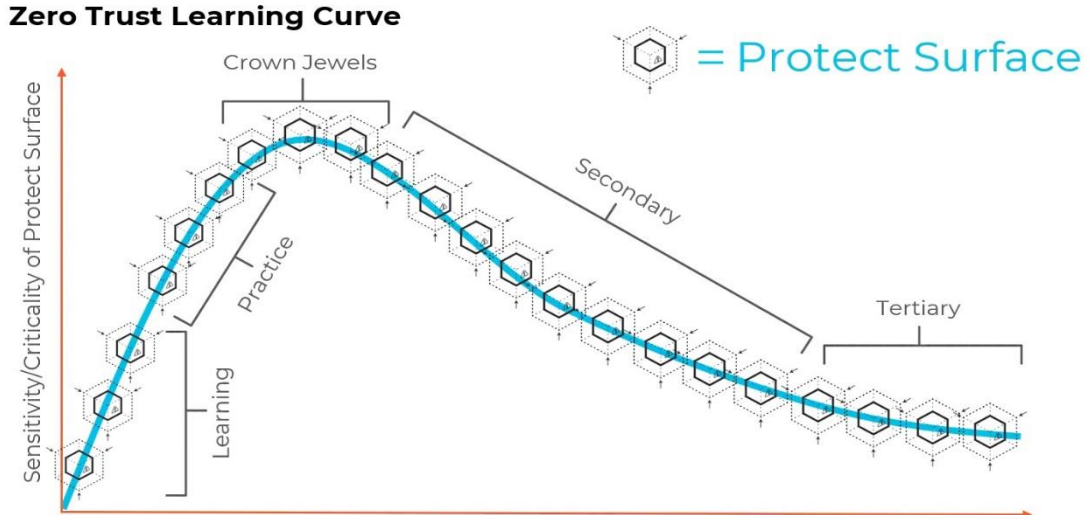
Στη Μηδενική Εμπιστοσύνη, καθορίζοντας μια επιφάνεια προστασίας, μπορούμε να μετακινήσουμε τους ελέγχους όσο το δυνατόν πιο κοντά σε αυτή και να ορίσουμε μια μικροπερίμετρο. Εφαρμόζοντας τεχνολογίες ελέγχου εισόδου – εξόδου (gateways), δίνεται η δυνατότητα λογικού διαχωρισμού των δικτύων (micro-segmentation) και λεπτομερούς καθορισμού και ελέγχου της δικτυακής κίνησης εντός και εκτός της μικροπεριμέτρου. Υπάρχει πολύ περιορισμένος αριθμός χρηστών ή πόρων που πραγματικά χρειάζονται πρόσβαση σε ευαίσθητα δεδομένα ή

περιουσιακά στοιχεία σε ένα περιβάλλον. Με τη δημιουργία πολιτικών που είναι περιορισμένες, ακριβείς και κατανοητές, αποσκοπούμε σε πρώτη φάση να απαγορεύσουμε την δυνατότητα στον επιτιθέμενο να αποκτήσει πρόσβαση σε κρίσιμα υπολογιστικά συστήματα του οργανισμού. Σε δεύτερη φάση να περιορίσουμε τη δυνατότητα του επιτιθέμενου να επεκταθεί και σε άλλα υπολογιστικά συστήματα καθώς και να μειώσουμε τον χρόνο στον οποίο παραμένει συνδεδεμένος στο σύστημα χωρίς να γίνει αντιληπτός (dwell time).

Για να ξεκινήσει ένας οργανισμός την εφαρμογή ή την μετάπτωση σε αρχιτεκτονική Zero Trust πρέπει πρώτα να λάβει υπόψη δυο κύριους άξονες. Ο πρώτος αφορά στο πόσο ευαίσθητη ή κρίσιμη είναι η επιφάνεια προστασίας ενώ ο δεύτερος άξονας αφορά τον χρόνο που θα αφιερωθεί στην αρχιτεκτονική Zero Trust. Ιδανικά ο άξονας αυτός θα πρέπει να ταυτίζεται με τον χρόνο ζωής του οργανισμού.

Είναι σαφές ότι οι εφαρμογές που αποτελούν επιφάνειες προστασίας δεν έχουν όλες την ίδια βαρύτητα στην λειτουργία του δικτύου. Υπάρχουν εφαρμογές οι οποίες είναι ζωτικής σημασίας για τον οργανισμό, όπως για παράδειγμα μια εφαρμογή διαχείρισης προσωπικού και υπάρχουν εφαρμογές επικουρικής φύσεως, όπως για παράδειγμα μια εφαρμογή ατζέντας ή μια εφαρμογή εταιρικής συνομιλίας με γραπτά μηνύματα (chat). Στο στάδιο αυτό είναι απαραίτητο να γίνει ο καθορισμός βαρύτητας της κάθε εφαρμογής και στη συνέχεια η μετάπτωση στην αρχιτεκτονική Zero Trust να ξεκινήσει από τις εφαρμογές με το μικρότερο αντίκτυπο. Αυτό θα έχει ως αποτέλεσμα, το προσωπικό, που θα υλοποιήσει την μετάπτωση, να εκπαιδευτεί και να προσαρμοστεί στις ιδιαιτερότητες του οργανισμού καθώς επίσης, και να διορθώσει τυχόν λάθη και αστοχίες χωρίς αυτό να παρουσιάσει αντίκτυπο στην εύρυθμη λειτουργία του οργανισμού. Στη συνέχεια, και αφότου υπάρξει εξοικείωση με τις επιφάνειες προστασίας που θα χρησιμοποιηθούν για την εκμάθηση και την προσαρμογή, το προσωπικό συνεχίζει με τις επιφάνειες «πρακτικής εφαρμογής», οι οποίες έχουν μεγαλύτερη βαρύτητα από τις επιφάνειες εκμάθησης αλλά τυχόν αστοχίες αυτών δεν θα επηρεάσουν την ομαλή λειτουργία του οργανισμού.

Με την απόκτηση πλήρους εξοικείωσης, συνέχεια έχουν οι επιφάνειες προστασίας οι οποίες εμπεριέχουν τις πλέον κρίσιμες και ζωτικές εφαρμογές του οργανισμού, όπως εφαρμογές διαχείρισης προσωπικού, Active Directories, File Services κλπ. Οι επιφάνειες αυτές αποτελούν την κορυφή της καμπύλης μάθησης του Zero Trust. Στη συνέχεια, και αφότου προστατευθούν οι κρίσιμες επιφάνειες, η πορεία



Εικόνα 11: Καμπύλη εκμάθησης Zero Trust ΠΗΓΗ:NIST[23]

είναι φθίνουσα ομαλή προς τα εμπρός καθόσον ακολουθούν όλο και λιγότερης κρισιμότητας επιφάνειες.

2.2 Καταγραφή της δικτυακής κίνησης μεταξύ των συστημάτων.

Η καταγραφή της δικτυακής κίνησης αποτελεί το δεύτερο στάδιο για την υλοποίηση του μοντέλου Zero Trust. Η διαδικασία καταγραφής αποσκοπεί στην αποσαφήνιση της αναγκαίας δικτυακής κίνησης που δημιουργεί κάθε στοιχείο του δικτύου και κατ' επέκταση στη δημιουργία εξειδικευμένων κανόνων στο Firewall, ώστε να επιτρέπει αποκλειστικά και μόνο την κίνηση αυτή. Αυτό γίνεται με τον ορισμό στους κανόνες των αναγκαίων πρωτοκόλλων και πορτών επικοινωνίας.

Συνήθως, τα κρίσιμα στοιχεία του δικτύου, για παράδειγμα ο Domain Controller, συνοδεύεται από σχετική τεκμηρίωση του κατασκευαστή για το ποια πρωτόκολλα χρησιμοποιούνται προκειμένου να επικοινωνήσει στο δίκτυο. Υφίσταται ωστόσο και το ενδεχόμενο να φιλοξενούνται σε server εφαρμογές με ελλιπή ή καθόλου τεκμηρίωση, γεγονός που καθιστά δύσκολη την διάκριση των αναγκαίων πρωτοκόλλων επικοινωνίας. Το πρόβλημα εντείνεται σε περιπτώσεις όπου το δίκτυο είναι ήδη παραγωγικό και επιδιώκεται η μετάπτωση του στην αρχιτεκτονική Zero Trust, χωρίς να διαταραχθεί η λειτουργία του. Σε κάθε περίπτωση, το προσωπικό που υλοποιεί την μετάπτωση σε αρχιτεκτονική Zero Trust θα πρέπει να έχει ως στόχο την υλοποίηση μικροπεριμέτρου γύρω από αυτή την επιφάνεια εργασίας. Σκοπός είναι ο περιορισμός της επέκτασης σε περίπτωση εισβολής στην επιφάνεια αυτή και όχι η αποξένωσή της από το υπόλοιπο δίκτυο.

Για τον εντοπισμό και την καταγραφή της δικτυακής κίνησης μιας εφαρμογής, δύναται να χρησιμοποιηθούν εξειδικευμένα λογισμικά τα οποία μπορούν να αναλύσουν τα πακέτα επικοινωνίας από και προς την εφαρμογή. Αξιοποιώντας τα λογισμικά αυτά καθίσταται πιο εύκολο στον χειριστή να εντοπίσει το μοτίβο επικοινωνίας μιας εφαρμογής, ποια πρωτόκολλα χρησιμοποιεί και προς τα που εδραιώνει επικοινωνία. Πραγματοποιώντας την ανάλυση αυτή είναι εξαιρετικά πιθανό να διαπιστωθεί ότι το firewall το οποίο προστατεύει την εφαρμογή αυτή δεν είναι παραμετροποιημένο, με αποτέλεσμα να επιτρέπει περισσότερες συνδέσεις από τις αναγκαίες, ιδίως από την μεριά της εφαρμογής προς το δίκτυο. Αυτό συμβαίνει κυρίως, σε ήδη παραγωγικά δίκτυα βασισμένα στο προηγούμενο μοντέλο ασφαλείας, αυτό του Κάστρου – Τάφρου καθόσον βασική αρχή του μοντέλου είναι ότι οτιδήποτε βρίσκεται εντός της περιμέτρου είναι ασφαλές. Στο μοντέλο Zero Trust, αντιθέτως, στο οποίο τίποτα δεν θεωρείται ασφαλές και έμπιστο, οποιαδήποτε επικοινωνία η οποία δεν είναι σαφώς καθορισμένη να επιτρέπεται, εμποδίζεται από το firewall ανεξάρτητα από την πηγή προέλευσής της.

2.3 Σχεδίαση ενός περιβάλλοντος Zero Trust.

Το στάδιο σχεδιασμού ενός περιβάλλοντος Zero Trust αποτελεί μια κρίσιμη φάση που ακολουθεί την αναγνώριση των επιφανειών προστασίας και επικεντρώνεται στην ανάπτυξη μέτρων και εργαλείων προστασίας εντός του παραγωγικού δικτύου. Σε αυτό το στάδιο, καταγράφονται όλα τα μέσα και τα εργαλεία προστασίας που υφίστανται στο δίκτυο, μαζί με τους ρόλους τους σε σχέση με τις επιφάνειες προστασίας.

Μετά την αναγνώριση αυτών των μέτρων προστασίας, η επόμενη ενέργεια είναι ο σχεδιασμός ενός περιβάλλοντος που αξιοποιεί βέλτιστα αυτά τα εργαλεία. Ο σχεδιασμός πρέπει να ευθυγραμμίζεται με τις αρχές του μοντέλου Zero Trust, το οποίο υποστηρίζει ότι κανένα στοιχείο δεν πρέπει να θεωρείται αυτόματα αξιόπιστο. Κατά τη διαδικασία αυτή, επισημαίνεται η ανάγκη για πλήρη εκμετάλλευση των υπαρχόντων μέσων προστασίας και προσδιορίζονται τυχόν κενά που ενδέχεται να υπάρχουν.

Η επίτευξη βέλτιστης αξιοποίησης περιλαμβάνει την υπογράμμιση των δυνατών σημείων των υφιστάμενων μέσων προστασίας και την ευέλικτη προσαρμογή τους, σύμφωνα με τις απαιτήσεις του μοντέλου Zero Trust. Αυτό περιλαμβάνει την προσαρμογή των ρόλων, των δικαιωμάτων πρόσβασης, και των πολιτικών ασφαλείας ώστε να ανταποκρίνονται στις ανάγκες της ασφάλειας με βάση την αρχή της μηδενικής εμπιστοσύνης.

Τέλος, το στάδιο σχεδιασμού προβλέπει την εξέταση της ανάγκης για τυχόν νέα μέσα προστασίας. Κατά την πορεία αυτή, ενδεχομένως να αποκαλυφθεί η ανάγκη για την αντικατάσταση κάποιων εργαλείων με πιο εξελιγμένα ή ενσωμάτωση νέων που να συνάδουν με τις αρχές του Zero Trust. Ο στόχος είναι να διασφαλιστεί ότι το περιβάλλον ανταποκρίνεται δυναμικά στις εξελίξεις της κυβερνοασφάλειας και παραμένει ανθεκτικό έναντι νέων απειλών.

2.4 Δημιουργία πολιτικών ασφαλείας με βάση το μοντέλο Zero Trust.

Το στάδιο αυτό αφορά την δημιουργία των πολιτικών ασφαλείας βασισμένες στο μοντέλο Zero Trust. Ο Kindervag προτείνει την μέθοδο Kipling ώστε να εντοπιστούν τα στοιχεία αυτά του δικτύου που θα πρέπει να έχουν πρόσβαση σε άλλα στοιχεία.

Η πολιτική του Zero Trust, γνωστή και ως η Μέθοδος του Κίπλινγκ[24], αποτίει φόρο τιμής στον Ρούντιαρντ Κίπλινγκ, τον ποιητή που παρουσίασε τις κρίσιμες έννοιες του Ποιος, Τι, Πότε, Πού, Γιατί και Πώς σε ένα ποίημα το 1902. Αυτή η μέθοδος έχει εξελιχθεί σε μια παγκοσμίως αναγνωρισμένη προσέγγιση που ξεπερνά γλωσσικά και πολιτιστικά εμπόδια, διευκολύνοντας τη δημιουργία δηλώσεων πολιτικής Zero Trust που είναι όχι μόνο εύκολες στον σχεδιασμό αλλά και κατανοητές καθώς και ευέλικτες στην εφαρμογή τους σε διάφορες τεχνολογίες.

Η ουσία της Μεθόδου του Κίπλινγκ βρίσκεται στον προσδιορισμό της κυκλοφορίας που επιτρέπει να διασχίζει τη μικροπερίμετρο ένα στοιχείο, γεγονός που αποτελεί καίριο παράγοντα για τον περιορισμό της μη εξουσιοδοτημένης πρόσβασης στην επιφάνεια προστασίας και την αποτροπή της παράνομης απόκτησης ευαίσθητων δεδομένων από κακόβουλους χρήστες. Για να επιτευχθεί αυτό, η τεχνολογία επιπέδου εφαρμογής (Layer 7) θεωρείται αναγκαία. Η Μέθοδος του Κίπλινγκ περιγράφει μια στρωματοποιημένη πολιτική Zero Trust στο Layer 7, εξασφαλίζοντας ένα εξαιρετικά λεπτομερές και αποτελεσματικό πλαίσιο ασφαλείας.

Αξιοποιώντας τη Μέθοδο του Κίπλινγκ, η δημιουργία πολιτικών Zero Trust απαιτεί λεπτομερείς εξετάσεις βασικών ερωτήσεων όπως παρακάτω:

α. Ποιος: Αφορά στην αναγνώριση της επικυρωμένης ταυτότητας η οποία επιτρέπεται να έχει πρόσβαση σε ένα πόρο, αντικαθιστώντας αποτελεσματικά την

εξάρτηση από τις source Ips, στους παραδοσιακούς κανόνες του firewall. Ο σχολαστικός ορισμός των ταυτοτήτων των χρηστών προσθέτει ένα επίπεδο βάθους και ανθεκτικότητας στα μέτρα ασφαλείας.

β. Τι: Η δήλωση 'Τι' καθορίζει ακριβώς την εφαρμογή που επιτρέπεται να έχει πρόσβαση σε έναν πόρο. Η επικύρωση στο επίπεδο εφαρμογής αποτελεί καθοριστικό στοιχείο, αποτρέποντας την κακόβουλη εκμετάλλευση στα επίπεδα port και πρωτοκόλλου. Αυτή η προηγμένη προσέγγιση υπερβαίνει τους παραδοσιακούς κανόνες firewall που βασίζονται σε ports και πρωτόκολλα.

γ. Πότε: Η καθοριστική δημιουργία ενός χρονοδιαγράμματος είναι απαραίτητη, ορίζοντας επακριβώς πότε επιτρέπεται στο διαπιστευμένο αναγνωριστικό να έχει πρόσβαση στον πόρο. Ενώ ορισμένοι κανόνες μπορεί να παραμείνουν ενεργοί 24/7, η στρατηγική χρήση περιορισμένων χρονικών κανόνων γίνεται αναγκαία ώστε να αντιμετωπιστούν δυνητικές επιθέσεις κατά τη διάρκεια ανενεργών περιόδων των χρηστών.

δ. Πού: Η δήλωση 'Πού' αποκτά σημασία καθορίζοντας την δυναμική τοποθεσία της Επιφάνειας Προστασίας. Αντίθετα από τους παραδοσιακούς κανόνες firewall που εξαρτώνται από στατικές διευθύνσεις IP προορισμού, αυτή η προσαρμοστική προσέγγιση εναρμονίζεται με την ευέλικτη φύση αποθήκευσης δεδομένων και αναπτύξεων περιουσιακών στοιχείων σε υπολογιστικά νέφη.

ε. Γιατί: Η δήλωση 'Γιατί' αναφέρεται στον λόγο που επιτρέπεται στο διαπιστευμένο αναγνωριστικό να έχει πρόσβαση στον πόρο. Συχνά, συνδέεται με την ευαισθησία των δεδομένων, που καθορίζεται από τη συμμόρφωση ή επιχειρηματικούς παράγοντες. Η δυνατότητα ετικετοποίησης πακέτων για την αναγνώριση ευαίσθητων δεδομένων προσθέτει ένα επίπεδο εξελιγμένης πολυπλοκότητας, δημιουργώντας μεταδεδομένα για την αυτοματοποίηση των δηλώσεων πολιτικής.

στ. Πώς: Η δήλωση 'Πώς' ορίζει λεπτομερώς τα κριτήρια που καθορίζουν πώς η δηλωθείσα κατάσταση 'Ποιος' επιτρέπεται να έχει πρόσβαση σε ένα πόρο. Αυτό περιλαμβάνει μια συνολική εξέταση του τρόπου που θα πρέπει να επεξεργάζεται η κίνηση, καθώς έχει πρόσβαση στον πόρο, αντιμετωπίζοντας πιθανές ευπάθειες και μειώνοντας τους κινδύνους. Προηγμένοι έλεγχοι, συμπεριλαμβανομένων Συστημάτων Πρόληψης Εισβολών (IPS), Συστημάτων Πρόληψης Απώλειας Δεδομένων (DLP), sandboxes, και αποκρυπτογράφησης, αξιοποιούνται σε ένα ενιαίο σύστημα, ενοποιώντας και ενισχύοντας τα μέτρα ασφαλείας, χωρίς την ανάγκη για διαφορετικά προϊόντα.

Who	What	When	Where	Why	How
User ID	Application ID	Time Limitations	Device ID	Classification	Content ID
Auth type			System Object	Data ID	Threat Protection
			Workload		SSL Decryption
			Geolocation		URL Filtering

Εικόνα 12: Μέθοδος Kipling για τον ορισμό κανόνων στο Zero Trust [6]

Στην ουσία, η Μέθοδος Κίπλινγκ αναδύεται ως μια καθοδηγητική φιλοσοφία που όχι μόνο ευνοεί τη δημιουργία πολιτικών Zero Trust, αλλά το κάνει με προσεκτική

και λεπτομερή προσέγγιση. Διασφαλίζει την ανάπτυξη ενός ισχυρού πλαισίου ασφαλείας που ευθυγραμμίζεται άψογα με το εξελισσόμενο τοπίο των κυβερνοαπειλών, προσφέροντας στους οργανισμούς ένα πλήρες και ευπροσάρμοστο παράδειγμα ασφαλείας.

2.5 Παρακολούθηση και συντήρηση του μοντέλου

Η παρακολούθηση και η συντήρηση του μοντέλου αποτελούν ένα θεμελιώδες και συνεχές στάδιο που ενσωματώνεται στις αρχές σχεδιασμού του Zero Trust. Η ουσία αυτού βρίσκεται στον προσεκτικό έλεγχο και την καταγραφή όλης της δικτυακής κίνησης, επεκτείνοντας αυτόν τον έλεγχο μέχρι το Επίπεδο Εφαρμογής (Layer 7).

Αυτή η δέσμευση σε συνεχή παρακολούθηση, αποτελεί μια ισχυρή στρατηγική αμυντικής φύσεως. Τα δεδομένα που παράγονται από τη συνεχή παρακολούθηση δεν είναι απλώς ένα ενεργητικό μέτρο κατά πιθανών παραβιάσεων δεδομένων ή κυβερνοαπειλών, αλλά αντιπροσωπεύει μια γενική προσπάθεια που παράγει πολύτιμες εισηγήσεις για τη βελτίωση της συνολικής ασφάλειας.

Στην πράξη, η εφαρμογή αυτής της αρχής σημαίνει ότι κάθε Επιφάνεια Προστασίας, είτε βρίσκεται στο νέφος, στο δίκτυο ή στο τερματικό, εξελίσσεται σε ένα όλο και περισσότερο ενιαίο και ανθεκτικό σύστημα με την πάροδο του χρόνου. Τα δεδομένα που συλλέγονται μέσω της παρακολούθησης αποτελούν μια πολύτιμη πηγή για ανάλυση. Χρησιμοποιώντας προηγμένες τεχνικές, όπως η ανάλυση συμπεριφοράς, η μηχανική μάθηση και η τεχνητή νοημοσύνη, οι ομάδες ασφαλείας μπορούν όχι μόνο να αποτρέψουν επιθέσεις σε πραγματικό χρόνο, αλλά και να βελτιώσουν στρατηγικά την συνολική ασφάλεια του οργανισμού μακροπρόθεσμα. Συνεχίζοντας την προσεκτική παρακολούθηση και την εκμάθηση από τις δραστηριότητες του δικτύου, οι οργανισμοί μπορούν να προσαρμόζουν δυναμικά τα μέτρα ασφαλείας τους. Οι εισηγήσεις που προκύπτουν από την ανάλυση της τηλεμετρίας επιτρέπουν τον εντοπισμό νέων απειλών, των μοτίβων εχθρικής συμπεριφοράς καθώς και των περιοχών ευπάθειας.

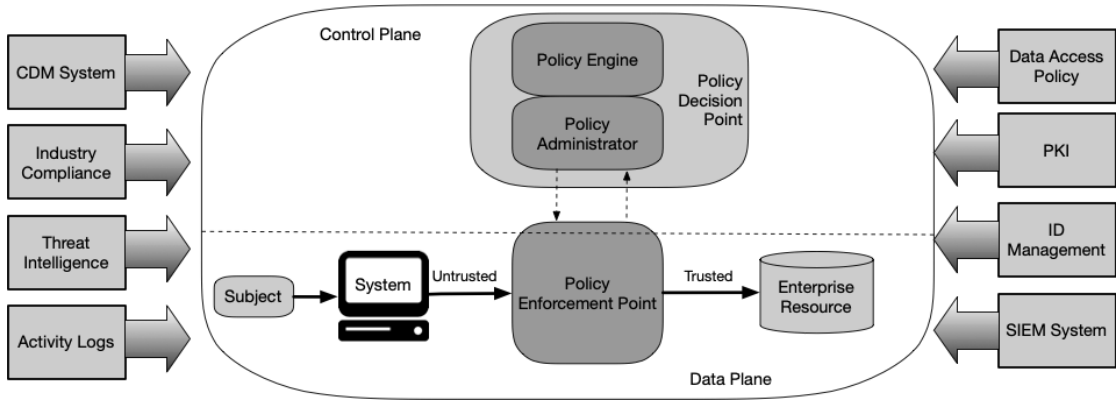
Αυτή η προσέγγιση επιτρέπει στις ομάδες ασφαλείας να υλοποιούν στοχευμένα και αποτελεσματικά μέτρα, ενισχύοντας τελικά τη συνολική αρχιτεκτονική ασφαλείας. Ωστόσο, ο μεγάλος όγκος δεδομένων προς ανάλυση που δημιουργείται, είναι δύσκολα διαχειρίσιμος από αυτές τις ομάδες. Για την αντιμετώπιση αυτής της δυσχέρειας, συστήνεται η χρήση λογισμικού διαχείρισης των δεδομένων αυτών (Security Information and Event Management, SIEM), το οποίο αποτελεί μια λύση που παρέχει τη δυνατότητα στις ομάδες ασφαλείας να αναγνωρίσουν πιθανές απειλές και να τις αντιμετωπίσουν εγκαίρως, πριν αυτές προλάβουν να διαταράξουν τη λειτουργία του οργανισμού. Μέσω των SIEM, οι ομάδες ασφαλείας μπορούν να εντοπίσουν ανωμαλίες στη συνήθη συμπεριφορά των χρηστών και να χρησιμοποιήσουν εργαλεία τεχνητής νοημοσύνης για να αυτοματοποιήσουν τις διαδικασίες αντίδρασης στα περιστατικά αυτά.

2.6 Η αρχιτεκτονική Zero Trust

Πρωταρχικός στόχος της αρχιτεκτονικής ZT είναι να αποτρέψει παραβιάσεις κυβερνοασφαλείας. Από την άποψη του επιχειρείν, η επένδυση ενός οργανισμού σε μέτρα και μεθόδους αποτροπής είναι οικονομικότερη σε σύγκριση με την ανάκαμψη

μετά από μια επιτυχημένη κυβερνοεπίθεση, καθόσον η ανάκαμψη αυτή μπορεί να περιλαμβάνει πληρωμή λύτρων για αποκρυπτογράφηση των εταιρικών δεδομένων, πληρωμή ρητρών λόγω μη παροχής υπηρεσιών ή και αγαθών κατά τη διάρκεια ανάκαμψης, απώλεια πελατών κ.α. .

Το ZT δεν είναι κάποιο συγκεκριμένο ψηφιακό εργαλείο προς αγορά. Ακόμα και αν ο οργανισμός διαθέτει τα πιο σύγχρονα και αποτελεσματικά λογισμικά και συσκευές, συνεχίζει να είναι ευάλωτος σε παραβιάσεις. Το ZT επιτυγχάνεται από τον εναρμονισμό όλων των διαφορετικών ψηφιακών εργαλείων και την ενοποίησή τους σε ένα σύστημα. Εξαιτίας της μοναδικότητας του κάθε οργανισμού, δεν υφίσταται πρότυπη αρχιτεκτονική στην οποία μπορεί να βασιστεί ο εκάστοτε οργανισμός για να το υλοποιήσει. Ωστόσο, ο οργανισμός NIST, με την SP 800-207 κατάτμησε την αρχιτεκτονική σε λογικά τμήματα, στα οποία εφαρμόζοντας τα ψηφιακά εργαλεία, ένας οργανισμός επιτυγχάνει την υιοθέτηση της αρχιτεκτονικής ZT στο δίκτυό του. Τα λογικά τμήματα αναλύονται όπως παρακάτω:



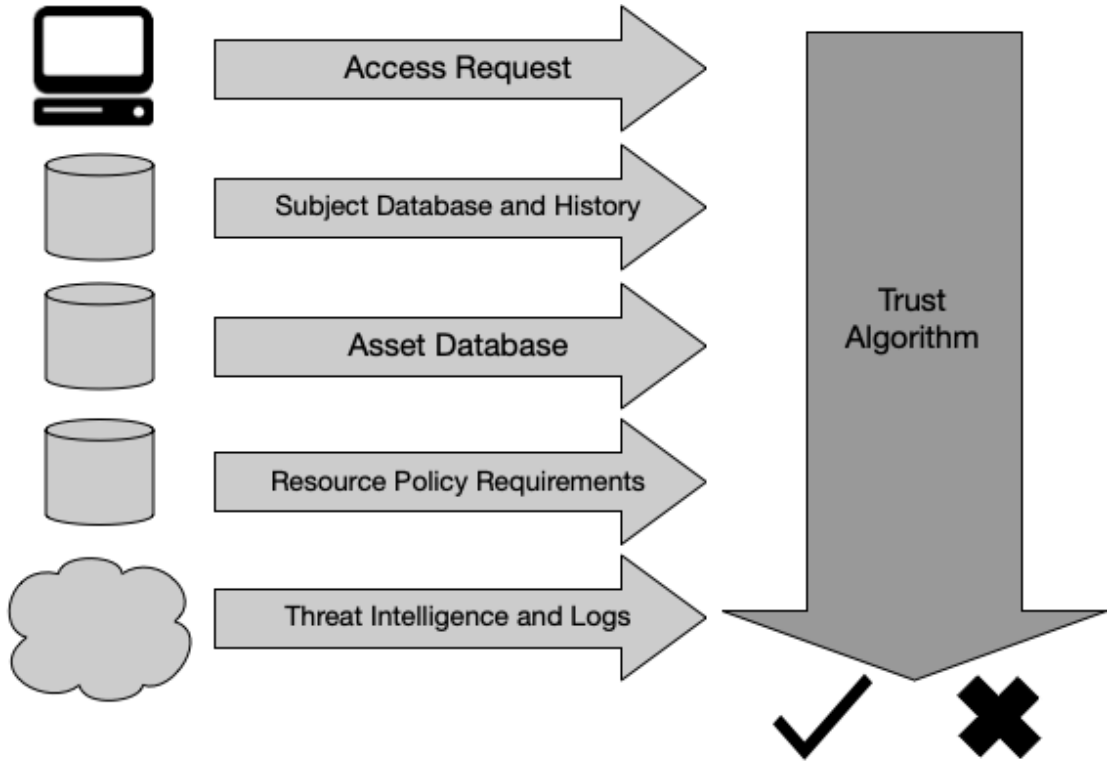
Εικόνα 13: Απεικόνιση δομικών λογικών στοιχείων της αρχιτεκτονικής ZT ΠΗΓΗ: NIST[23]

α. Policy Engine (PE): Αυτό το τμήμα είναι υπεύθυνο για την τελική απόφαση χορήγησης πρόσβασης σε έναν πόρο, βάση συγκεκριμένου αιτήματος. Το PE χρησιμοποιεί την πολιτική ασφαλείας και δικαιωμάτων του οργανισμού, καθώς και άλλες πληροφορίες από εξωτερικές πηγές (πχ συστήματα CDM, πηγές threat intelligence κ.α), ως είσοδο σε έναν αλγόριθμο εμπιστοσύνης (Trust Algorithm) για την χορήγηση, την απόρριψη ή την ανάκληση πρόσβασης στον πόρο. Το PE λειτουργεί συνδυαστικά με το λογικό τμήμα διαχείρισης πολιτικής (Policy Administrator, PA) συνθέτοντας το ευρύτερο λογικό τμήμα που ονομάζεται Σημείο Απόφασης Πολιτικής (Policy Decision Point, PDP). Πρακτικά, το PE λαμβάνει και καταχωρεί την απόφαση ενώ το PA εκτελεί την απόφαση.

β. Policy Administrator (PA): Αυτό το λογικό τμήμα είναι υπεύθυνο για την εφαρμογή της απόφασης του PE. Το PA, αφού λάβει την απόφαση από το PE στη συνέχεια ρυθμίζει κατάλληλα το επόμενο στη σειρά λογικό τμήμα, το οποίο είναι το Σημείο εφαρμογής πολιτικής (Policy Enforcement Point, PEP), ώστε αυτό να επιτρέψει ή να διακόψει τη σύνδεση με τον πόρο του δικτύου.

γ. Policy Enforcement Point (PEP): Το τμήμα αυτό είναι υπεύθυνο για την ενεργοποίηση, παρακολούθηση και διακοπή των συνδέσεων προς τους δικτυακούς πόρους. Το PEP είναι σε συνεχή επικοινωνία με το PA για να λαμβάνει νέα αιτήματα καθώς και για να ενημερώνεται για τυχόν αλλαγές στην πολιτική πρόσβασης.

Πρακτικά αποτελεί τον ενδιάμεσο μεταξύ των χρηστών και των πόρων ενός οργανισμού και συνήθως είναι ένα NG-FW.



Εικόνα 14: Αλγόριθμος Εμπιστοσύνης ΠΗΓΗ:NIST[23]

δ. Continuous Diagnostics and Mitigation System (CDM): Αποτελεί μια εκ των πηγών πληροφοριών του PE. Το CDM είναι υπεύθυνο για την συλλογή πληροφοριών σχετικά με την κατάσταση των πόρων του οργανισμού και εφαρμόζει ενημερώσεις ρυθμίσεων σε αυτούς. Οι πληροφορίες που συλλέγει και στη συνέχεια τροφοδοτεί το PE αφορούν, αιτήματα συνδέσεων των πόρων, έκδοση του λειτουργικού συστήματος του πόρου, τυχόν ευπάθειες που μπορεί να έχει, καθώς επίσης και πληροφορίες σχετικές με την ασφάλεια και την ακεραιότητα των εφαρμογών που λειτουργούν στον πόρο. Επίσης, είναι αρμόδιο για την εφαρμογή τμήματος των πολιτικών ασφαλείας του οργανισμού, σε συσκευές που δεν ανήκουν στο δίκτυο του οργανισμού αλλά συνδέονται με αυτό.

ε. Industry Compliance System: Αυτό το τμήμα εξασφαλίζει ότι ο οργανισμός παραμένει συμμορφωμένος με οποιοδήποτε κανονιστικό καθεστώς μπορεί να υπάγεται (π.χ., FISMA, απαιτήσεις ασφαλείας πληροφοριών στον τομέα της υγείας ή του οικονομικού κλάδου). Αυτό περιλαμβάνει όλους τους κανόνες πολιτικής που αναπτύσσει ο οργανισμός για να εξασφαλίσει τη συμμόρφωση.

στ. Threat Intelligence Feeds: Αφορά την παροχή πληροφοριών σχετικές με απειλές από εξωτερικές ως επί το πλείστων πηγές, που βοηθούν στην λήψη αποφάσεων από το PE. Οι πληροφορίες αυτές αφορούν νέες απειλές και ευπάθειες, σφάλματα σε εφαρμογές και λειτουργικά συστήματα καθώς και πληροφορίες από απειλές που αντιμετωπίστηκαν σε άλλους πόρους του οργανισμού.

ζ. Network and System Activity Logs: Το επιχειρησιακό αυτό σύστημα συγκεντρώνει καταγραφές συμβάντων από τους πόρους του οργανισμού, κίνηση δεδομένων στο δίκτυο, ενέργειες πρόσβασης σε πόρους και άλλα συμβάντα που παρέχουν άμεση ανατροφοδότηση για την ασφάλεια των πληροφοριακών συστημάτων της επιχείρησης.

η. Data Access Policies: Αφορά τις πολιτικές και τους κανόνες πρόσβασης στους πόρους του οργανισμού. Αυτό το σύνολο κανόνων μπορεί να δημιουργηθεί είτε από αρμόδιο χειριστή είτε από ένα PE. Αποτελούν την βάση για την εξουσιοδότηση πρόσβασης σε λογαριασμούς και εφαρμογές του οργανισμού και βασίζονται στους καθορισμένους ρόλους και στις ανάγκες του οργανισμού.

θ. Enterprise Public Key Infrastructure (PKI): Το σύστημα αυτό είναι υπεύθυνο για την δημιουργία και την καταγραφή πιστοποιητικών που εκδίδονται από τον οργανισμό, προς πόρους, υπηρεσίες και εφαρμογές.

ι. ID Management System: Το σύστημα αυτό είναι υπεύθυνο για τη δημιουργία, αποθήκευση και διαχείριση των λογαριασμών των χρηστών του οργανισμού. Σε αυτό περιλαμβάνονται όλες οι απαραίτητες πληροφορίες για τον χρήστη καθώς και ο ρόλος του στην επιχείρηση, οι προσβάσεις του και οι πόροι που χειρίζεται. Αποτελεί ένα από τα κυριότερα στοιχεία που λαμβάνονται υπόψη από το PE για την λήψη απόφασης.

Κεφάλαιο 3: Τεχνολογικά Μέσα για το Zero Trust

Όπως έχει ήδη αναφερθεί, το μοντέλο Zero Trust δεν αποτελείται από ένα ψηφιακό εργαλείο. Απαρτίζεται από ένα σύνολο εργαλείων, αρμονικά συνδυασμένα μεταξύ τους. Είναι προφανές ότι ίδιας κατηγορίας εργαλεία προερχόμενα από διαφορετικούς κατασκευαστές θα παρουσιάζουν διαφορές ως προς την απόδοση και τις δυνατότητες. Ωστόσο, επιδίωξη του μοντέλου είναι ότι μέσω του εναρμονισμού των εργαλείων να υπάρχει αλληλοκάλυψη των αδυναμιών τους, ώστε αφενός, να δημιουργείται μια ομογενοποιημένη περίμετρος ασφαλείας γύρω από κάθε εφαρμογή και αφετέρου, να ελαχιστοποιείται η ανάγκη προμήθειας νέων εργαλείων ίδιας κατηγορίας, προκειμένου να καλυφθούν οι αδυναμίες του ενός εργαλείου με το άλλο.

Λόγω της μοναδικότητας κάθε οργανισμού δεν υπάρχει συγκεκριμένη λίστα εργαλείων. Κάθε αρχιτέκτονας του μοντέλου λαμβάνοντας υπόψη τις ανάγκες του οργανισμού θα πρέπει να συνδυάσει κατηγορίες εργαλείων για να επιτύχει το επιθυμητό αποτέλεσμα. Οι κυριότερες από τις κατηγορίες αυτές είναι οι παρακάτω:

α. Software – Defined Perimeter (SDP).

β. Cloud Access Security Brokers (CASB).

γ. Security Information and Event Management (SIEM).

δ. Jump Servers.

ε. Multi-Factor Authentication (MFA).

στ. Endpoint Protection.

ζ. Identity and Access Management (IAM).

η. Next – Generation Firewalls (NGFW).

θ. Data Loss Prevention.

ι. Virtual Private Networks (VPN).

ια. Endpoint Detection and Response (EDR).

ιβ. Network Access Control (NAC).

ιγ. User and Entity Behavior Analytics (UEBA)

ιδ. Mobile Device Management (MDM).

ιε. Security Orchestration, Automation and Response (SOAR).

3.1 Software – Defined Perimeter (SDP)

Το Software – Defined Perimeter (SDP), είναι μια τεχνική ασφαλείας που ελέγχει την πρόσβαση σε πόρους βασιζόμενη στην ταυτότητα και δημιουργεί ένα εικονικό όριο (περίμετρο) γύρω από τους πόρους που συμμετέχουν στο δίκτυο ή και επικοινωνούν με το διαδίκτυο. Με τον καθορισμό μιας περιμέτρου μέσω λογισμικού αντί μέσω της χρήσης υλικού, μια SDP μπορεί να κρύψει την υποδομή μιας οργάνωσης - ανεξαρτήτως του που βρίσκεται - από οντότητες εκτός της περιμέτρου.

Οι αρχιτεκτονικές SDP μπορούν να συμβάλλουν στη μείωση της επιφάνειας επίθεσης και την αντιμετώπιση εσωτερικών και εξωτερικών επιθέσεων.

Αυτό το πλαίσιο είναι βασισμένο στο μοντέλο "Ανάγκης Γνώσης" (need-to-know) του Υπουργείου Άμυνας των Ηνωμένων Πολιτειών από το 2007, σύμφωνα με το οποίο, όλες οι οντότητες που προσπαθούν να έχουν πρόσβαση σε μια συγκεκριμένη υποδομή πρέπει να ελεγχθούν και να εξουσιοδοτηθούν πριν τους δοθεί η πρόσβαση. Το 2014, η Cloud Security Alliance (CSA) δημοσίευσε κατευθυντήριες οδηγίες, συνδυάζοντας τις αρχές της υπηρεσίας αμυντικών πληροφοριών των ΗΠΑ (Defence Information Systems Agency) με πρότυπα ασφάλειας από τον NIST και άλλους οργανισμούς. Η CSA βελτίωσε περαιτέρω το πλαίσιο της SDP με την έκδοση της έκδοσης 2.0 το 2022 επεκτείνοντας τον ρόλο της SDP στο πλαίσιο της αρχής της μηδενικής εμπιστοσύνης.

3.1.1 Σκοπός του SDP

Οι SDP παρέχουν ασφαλή πρόσβαση σε υπηρεσίες, εφαρμογές και συστήματα που λειτουργούν σε δίκτυο, ανεξάρτητα από το αν αυτά αναπτύσσονται σε δημόσια ή ιδιωτικά cloud ή εταιρικές εγκαταστάσεις. Σκοπός της προσέγγισης SDP είναι να αποκρύπτει τα συστήματα εντός της περιμέτρου, εμποδίζοντας τους εξωτερικούς παρατηρητές να αναλύσουν την εσωτερική αρχιτεκτονική και τις υπηρεσίες του δικτύου.

Το λογισμικό SDP έχει σχεδιαστεί ειδικά για να παρέχει σε μεσαίους και μεγάλους οργανισμούς το μοντέλο περιμετρικής ασφάλειας που απαιτείται για εφαρμογές μηδενικής εμπιστοσύνης και συνδεσιμότητα δικτύου. Πέρα από τη μείωση της επιφάνειας επίθεσης, η εικονική περίμετρος ενός SDP γύρω από το δίκτυο εξαλείφει τυχόν ασυμβατότητες μεταξύ εφαρμογών διαφόρων προμηθευτών, επιτρέποντας την εγκατάσταση σε οποιονδήποτε κεντρικό υπολογιστή χωρίς αναδιαμόρφωση του δικτύου ή επαναδιαμόρφωση της συσκευής. Ένα SDP ενσωματώνει ασφάλεια σε επίπεδο δικτύου και όχι σε επίπεδο εφαρμογής. Αυτό το διαχωρίζει από άλλα στοιχεία ελέγχου που βασίζονται στον περιορισμό των δικαιωμάτων πρόσβασης του χρήστη αλλά επιτρέπουν την ευρεία πρόσβαση στο δίκτυο.

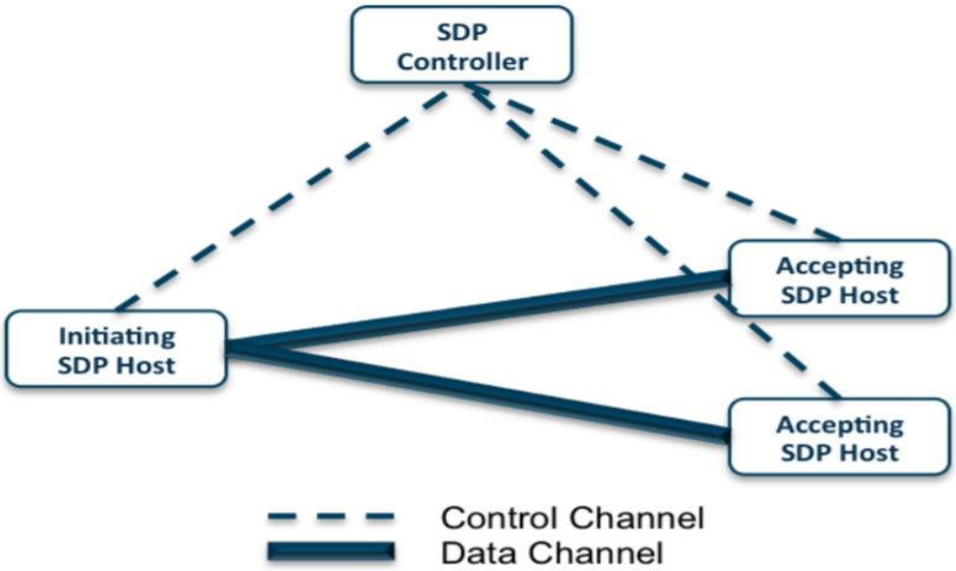
3.1.2 Λειτουργία του SDP

Η προσέγγιση κυβερνοασφάλειας SDP μειώνει τις κοινές επιθέσεις δικτύου, προστατεύοντας όλους τους πόρους ανεξάρτητα από την τοποθεσία τους (cloud, εγκαταστάσεις, data center ή διακομιστής εφαρμογών).

Ένα SDP λειτουργεί ως ενδιάμεσος μεταξύ εσωτερικών εφαρμογών και χρηστών, παρέχοντας πρόσβαση σε υπηρεσίες μόνο εάν ικανοποιούνται τα σωστά κριτήρια ελέγχου ταυτότητας και εξουσιοδότησης. Μόλις γίνει έλεγχος ταυτότητας του χρήστη και της συσκευής, το SDP δημιουργεί μια μεμονωμένη σύνδεση δικτύου μεταξύ αυτής της συσκευής και του διακομιστή στον οποίο προσπαθεί να αποκτήσει πρόσβαση. Ένας πιστοποιημένος χρήστης δεν είναι συνδεδεμένος σε μεγαλύτερο δίκτυο, αλλά του παρέχεται η δική του σύνδεση δικτύου στην οποία κανείς άλλος δεν μπορεί να έχει πρόσβαση και περιλαμβάνει μόνο τις υπηρεσίες στις οποίες ο χρήστης

έχει έγκριση να προσπελάσει. Στο πλαίσιο αναγκαίας γνώσης, ένα SDP παρέχει μόνο τις πληροφορίες που χρειάζεται ένας χρήστης ή μια συσκευή και τίποτα άλλο, μη μοιράζοντας πληροφορίες DNS, εσωτερικές διευθύνσεις IP ή άλλες πληροφορίες για το εσωτερικό δίκτυο.

Οι αρχιτεκτονικές SDP περιλαμβάνουν δύο βασικά στοιχεία: τους ελεγκτές SDP και τους υπολογιστές SDP. Ο "ελεγκτής" SDP είναι το λογικό στοιχείο του SDP που είναι υπεύθυνο για τον καθορισμό των συσκευών και των διακομιστών που θα επιτρέπεται να συνδέονται. Μόλις γίνει έλεγχος ταυτότητας του χρήστη και της συσκευής, ο ελεγκτής μεταβιβάζει την έγκριση του χρήστη και της συσκευής στην πύλη SDP (SPD Gateway). Η πύλη SDP είναι το σημείο όπου η πρόσβαση επιτρέπεται ή απαγορεύεται στην πραγματικότητα. Στην περίπτωση έγκρισης της σύνδεσης η πύλη SPD εγκαθιδρύει μια ασφαλή και κρυπτογραφημένη σύνδεση μεταξύ του χρήστη και των υπηρεσιών που επιτρέπεται να προσπελάσει ο χρήστης. Η σύνδεση αυτή έχει ως μοναδικούς συμμετέχοντες τον χρήστη και τον εξυπηρετητή, απαγορεύοντας σε οποιαδήποτε άλλη οντότητα να χρησιμοποιήσει αυτή την σύνδεση. Αυτές οι συνδέσεις συνήθως αξιοποιούν τεχνολογίες TLS και VPN.



Εικόνα 15: Αρχιτεκτονική SPD ΠΗΓΗ TechTarget[29]

3.1.3 SPD και Zero Trust

Η αρχιτεκτονική SPD αποτελεί ένα μέσο επίτευξης μηδενικής εμπιστοσύνης στο επίπεδο του δικτύου, καθόσον η δομή του βασίζεται στον έλεγχο της ταυτότητας και τον περιορισμό της δικτυακής κίνησης στην απολύτως αναγκαία. Παρότι τόσο το SPD όσο και το Zero Trust στοχεύουν στην ενίσχυση της ασφάλειας ενός δικτύου, το SPD εστιάζει περισσότερο στην τμηματοποίηση του δικτύου και στην δυναμική παροχή υπηρεσιών, ενώ το Zero Trust υιοθετεί μια ευρύτερη προσέγγιση με έμφαση στην συνεχή παρακολούθηση της δικτυακής κίνησης και την ασφάλεια με επίκεντρο τον χρήστη. Η βέλτιστη πρακτική για έναν οργανισμό είναι η υιοθέτηση και των δυο αυτών αρχιτεκτονικών και ο συνδυασμός τους με βάση τις ανάγκες του.

3.2 Cloud Access Security Brokers (CASB)

Στον τομέα του cloud computing, τα δεδομένα αποθηκεύονται απομακρυσμένα και προσπελαύνονται μέσω του Διαδικτύου. Ως αποτέλεσμα, οι εταιρείες που χρησιμοποιούν το cloud έχουν περιορισμένο έλεγχο επί του πού ακριβώς αποθηκεύονται τα δεδομένα και πώς οι χρήστες έχουν πρόσβαση σε αυτά. Οι χρήστες μπορούν να αποκτούν πρόσβαση σε δεδομένα και εφαρμογές cloud από οποιαδήποτε συσκευή συνδεδεμένη στο Διαδίκτυο και από οποιοδήποτε δίκτυο, όχι μόνο από το εσωτερικό δίκτυο που διαχειρίζεται η εταιρεία. Για παράδειγμα, ένας χρήστης μπορεί να συνδεθεί σε μια εφαρμογή SaaS που διαχειρίζεται η εταιρεία από ένα μη ασφαλές δίκτυο στην προσωπική του συσκευή, κάτι που συνήθως δεν θα ήταν εφικτό με εφαρμογές που λειτουργούν εσωτερικά. Η χρήση του cloud δυσχεραίνει επίσης τη διασφάλιση του ιδιωτικού και ασφαλούς χαρακτήρα των δεδομένων, καθώς είναι πιο δύσκολο να αποτραπεί η παρακολούθηση, όπως σε δημόσιους χώρους αντί σε ιδιωτικούς.

Εικόνα 16. Cloud Security Access Broker ΠΗΓΗ: ACL DIGITAL[32]

Για την πλήρη προστασία των δεδομένων στο cloud, οι εταιρείες συνήθως χρησιμοποιούν υπηρεσίες ασφαλείας που βασίζονται επίσης στο cloud. Ωστόσο, αυτή η προσέγγιση δημιουργεί προκλήσεις, καθώς πρέπει να διαπραγματεύονται πολλαπλές συμβάσεις και να διαχειρίζονται την ποικιλομορφία των χαρακτηριστικών διάφορων προμηθευτών. Τα CASB αντιμετωπίζουν αυτές τις προκλήσεις παρέχοντας μια ολοκληρωμένη λύση, εξασφαλίζοντας συνεργασία των τεχνολογιών, απλοποιώντας τη διαχείριση εργαλείων και εξασφαλίζοντας την ενιαία διαχείριση όλων των υπηρεσιών ασφαλείας cloud. Το CASB μπορεί να είναι είτε εργαλείο λογισμικού είτε υπηρεσία που παρέχεται από έναν πάροχο cloud υπηρεσιών και εφαρμόζεται μεταξύ της εσωτερικής υποδομής ενός οργανισμού και της υποδομής που διατηρεί ο οργανισμός σε cloud. Μέσω του CASB, ο οργανισμός αποκτά την δυνατότητα επέκτασης των πολιτικών ασφαλείας του και στην cloud υποδομή του.

3.2.1 Δυνατότητες του CASB

Οι περισσότερες λύσεις CASB παρέχουν ένα ολοκληρωμένο φάσμα τεχνολογιών ασφαλείας, καλύπτοντας τους ακόλουθους τομείς[30]:

α. Επαλήθευση ταυτότητας: Βεβαιώνει την ταυτότητα των χρηστών μέσω ποικίλων παραγόντων, όπως κωδικός πρόσβασης ή φυσικό διακριτικό.

β. Έλεγχος πρόσβασης: Καθορίζει τα δικαιώματα πρόσβασης των χρηστών σε εφαρμογές που ελέγχονται από την εταιρεία.

γ. Ανίχνευση Shadow IT: Εντοπίζει μη εξουσιοδοτημένες χρήσεις συστημάτων και υπηρεσιών από εσωτερικούς χρήστες για επιχειρηματικούς σκοπούς.

δ. Πρόληψη απώλειας δεδομένων (DLP): Αποτρέπει τις διαρροές δεδομένων από πλατφόρμες που ανήκουν στην εταιρεία.

ε. Φιλτράρισμα URL: Αποκλείει ιστότοπους που αξιοποιούνται από εισβολείς για phishing ή κακόβουλο λογισμικό.

στ. Επιθεώρηση πακέτων: Ελέγχει τα δεδομένα που εισέρχονται ή εξέρχονται από το δίκτυο για ενδεχόμενη κακόβουλη δραστηριότητα.

ζ. Sandboxing: Εκτελεί προγράμματα και κώδικα σε απομονωμένο περιβάλλον για την ανίχνευση ενδεχόμενης κακόβουλης συμπεριφοράς.

η. Απομόνωση προγράμματος περιήγησης: Εκτελεί τα προγράμματα περιήγησης σε απομακρυσμένο διακομιστή για επιπλέον προστασία από κακόβουλο κώδικα.

θ. Ανίχνευση κακόβουλου λογισμικού: Εντοπίζει την ύπαρξη κακόβουλου λογισμικού.

Είναι σημαντικό να σημειωθεί ότι οι CASB μπορούν να προσφέρουν και άλλες τεχνολογίες ασφαλείας εκτός από αυτές που παρουσιάζονται παραπάνω. Τα CASB προσαρμόζουν αυτές τις τεχνολογίες ειδικά για το cloud computing. Επιπλέον, μεγάλα CASB μπορεί να ενσωματώσουν προϊόντα ή εταιρείες για να προσφέρουν πλήρεις υπηρεσίες, συνεργαζόμενα και με εξωτερικές εταιρείες για πρόσθετη υποστήριξη.

3.2.2 Προκλήσεις από την υιοθέτηση των CASB

Η υιοθέτηση ενός CASB (Cloud Access Security Broker) μπορεί να αντιμετωπίζει ορισμένες προκλήσεις λόγω της πολυπλοκότητας και των ευαισθησιών των δεδομένων στον κλάδο του cloud. Αυτές οι προκλήσεις αφορούν τα εξής[30][31]:

α. Επεκτασιμότητα: Τα CASB πρέπει να είναι σε θέση να διαχειρίζονται πολυάριθμα δεδομένα και πλατφόρμες, καθώς και πολλές εφαρμογές cloud. Είναι ουσιώδες για τους οργανισμούς να βεβαιώνονται ότι ο πάροχος τους CASB είναι σε θέση να εξελίσσεται συγχρόνως με τις αυξανόμενες ανάγκες τους.

β. Μετριασμός: Δεν παρέχουν όλα τα CASB τη δυνατότητα να αντιμετωπίζουν απειλές ασφαλείας αμέσως μόλις εντοπιστούν. Ανάλογα με την κατάσταση, ένα CASB χωρίς δυνατότητες μετριασμού μπορεί να έχει περιορισμένη χρησιμότητα για έναν οργανισμό.

γ. Ενοποίηση: Οι εταιρείες πρέπει να εξασφαλίζουν ότι το CASB τους ενσωματώνεται σωστά σε όλα τα συστήματα και την υποδομή τους. Χωρίς πλήρη ενοποίηση, το CASB δεν θα διαθέτει πλήρη ορατότητα σε μη εξουσιοδοτημένες ενέργειες και πιθανές απειλές για την ασφάλεια.

δ. Απόρρητο δεδομένων: Ο πάροχος του CASB πρέπει να διατηρεί τα δεδομένα απόρρητα ή να είναι διαφανής σχετικά με το πώς χειρίζεται τα ευαίσθητα δεδομένα. Εάν το CASB μεταφέρει τα δεδομένα των πελατών του στο cloud, είναι κρίσιμο να διασφαλίζεται η ασφάλεια και η ιδιωτικότητα των δεδομένων, ιδίως για οργανισμούς που υπόκεινται σε αυστηρούς κανονισμούς περί απορρήτου δεδομένων.

ε. Συμβατότητα και Ενσωμάτωση: Η ενσωμάτωση ενός CASB σε μια οργάνωση ενδέχεται να απαιτεί προσαρμογές στην υπάρχουσα υποδομή και στις διαδικασίες. Αυτό μπορεί να είναι πολυσύνθετο, ειδικά για μεγάλες επιχειρήσεις με πολύπλοκες αρχιτεκτονικές ήδη σε λειτουργία.

στ. Διαχείριση Πολυπλοκότητας: Τα CASB παρέχουν πολλές λειτουργίες και επιλογές διαμόρφωσης, οι οποίες μπορεί να καταστούν πολύπλοκες για τη διαχείριση. Η επιτυχημένη υιοθέτηση απαιτεί κατάλληλη κατάρτιση και κατανόηση της λειτουργίας του CASB.

3.3 Security Information and Event Management (SIEM)

Το Security Information and Event Management (SIEM)[33],[34] είναι μια προσέγγιση διαχείρισης ασφαλείας που συνδυάζει τις λειτουργίες της Διαχείρισης Πληροφοριών Ασφαλείας (SIM) και της Διαχείρισης Συμβάντων Ασφαλείας (SEM) σε ένα ενιαίο σύστημα διαχείρισης ασφαλείας. Οι βασικές αρχές κάθε συστήματος SIEM περιλαμβάνουν τη συγκέντρωση δεδομένων από διάφορες πηγές, τον εντοπισμό αποκλίσεων από τη συνήθη συμπεριφορά (δικτύου, συστημάτων, χρηστών) και τη λήψη κατάλληλων μέτρων. Για παράδειγμα, κατά τον εντοπισμό ενός πιθανού προβλήματος, ένα σύστημα SIEM μπορεί να καταγράψει επιπλέον πληροφορίες, να δημιουργήσει ειδοποιήσεις και να δώσει εντολή σε άλλους ελεγκτές ασφαλείας να διακόψουν την λειτουργία συγκεκριμένων δραστηριοτήτων.

Αρχικά, η υιοθέτηση του SIEM στις μεγάλες επιχειρήσεις έγινε εξαιτίας της υποχρέωσης συμμόρφωσης με το Πρότυπο Ασφαλείας Δεδομένων της Βιομηχανίας Πληρωμών με Κάρτα. Ωστόσο, οι ανησυχίες για τις εξελισσόμενες απειλές οδήγησαν μικρότερες οργανώσεις να εξετάσουν τα πλεονεκτήματα που μπορούν να προσφέρουν τα εργαλεία SIEM κυριότερο των οποίων είναι η δυνατότητα ανάλυσης όλων των δεδομένων που σχετίζονται με την ασφάλεια από μια ενιαία σκοπιά, γεγονός που διευκολύνει τον εντοπισμό ασυνήθιστων συμπεριφορών. Στην ουσία του, ένα σύστημα SIEM μπορεί να λειτουργεί με μηχανισμούς βασισμένους σε κανόνες ή να χρησιμοποιεί έναν μηχανισμό στατιστικής συσχέτισης για να συσχετίσει εγγραφές στα αρχεία συμβάντων. Τα προηγμένα συστήματα SIEM έχουν εξελιχθεί για να περιλαμβάνουν αναλύσεις συμπεριφοράς χρηστών και οντοτήτων, καθώς και δυνατότητες Security Orchestration, Automation and Response (SOAR).

Τα συστήματα SIEM λειτουργούν με την ανάπτυξη πολλαπλών υπηρεσιών συλλογής δεδομένων (agents) για τη συγκέντρωση συμβάντων που σχετίζονται με την ασφάλεια από συσκευές τελικού χρήστη, διακομιστές, εξοπλισμό δικτύου και

ειδικούς εξοπλισμούς ασφαλείας, όπως firewall, antivirus και τα συστήματα πρόληψης διείσδυσης (IPS). Οι agents μεταβιβάζουν τα συμβάντα σε ένα κεντρικό πίνακα διαχείρισης, όπου οι αναλυτές ασφαλείας αναλύουν τα δεδομένα, συνδέουν τα στοιχεία και δίνουν προτεραιότητα στα συμβάντα ασφαλείας.

Σε ορισμένα συστήματα, η αρχική επεξεργασία μπορεί να πραγματοποιείται στους agents στα άκρα, επιτρέποντας μόνο συγκεκριμένα συμβάντα να προωθούνται σε ένα κεντρικό κόμβο διαχείρισης. Αυτή η προσέγγιση βοηθάει στην ελαχιστοποίηση του όγκου πληροφοριών που μεταδίδονται και αποθηκεύονται. Παρά τη βελτίωση της ικανότητας του συστήματος με την τεχνητή νοημοσύνη για την ακριβή ανίχνευση ανωμαλιών, οι αναλυτές παίζουν σημαντικό ρόλο παρέχοντας επιπρόσθετη αξιολόγηση των συμβάντων, ανατροφοδότηση και συνεχή εκπαίδευση του συστήματος.

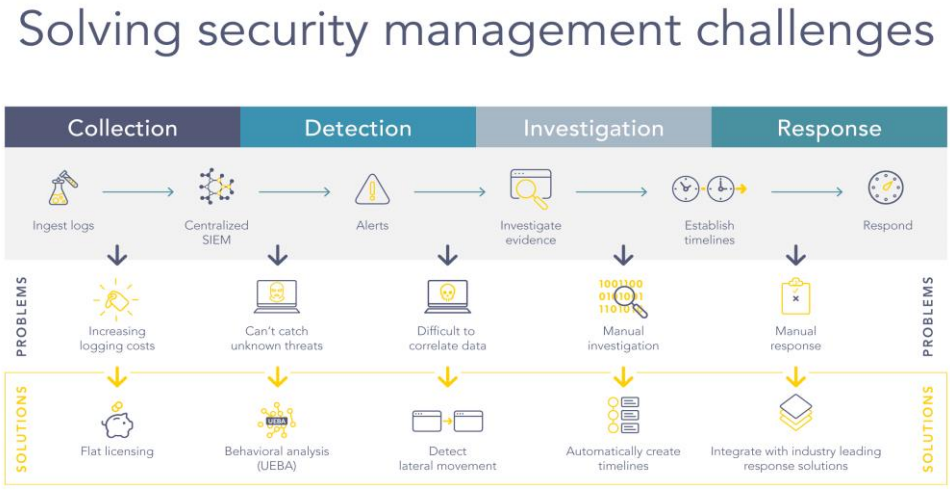
3.3.1 Λειτουργία του SIEM

Τα εργαλεία SIEM συλλέγουν δεδομένα συμβάντων και καταγραφών που δημιουργούνται από τα συστήματα σε όλη τη υποδομή ενός οργανισμού και συγκεντρώνουν αυτά τα δεδομένα σε μια κεντρική πλατφόρμα. Στα συστήματα περιλαμβάνονται εφαρμογές, συσκευές ασφαλείας, antiviruses και firewalls. Τα εργαλεία SIEM κατατάσσουν τα δεδομένα σε ομάδες, όπως για παράδειγμα επιτυχημένες και ανεπιτυχείς συνδέσεις, δραστηριότητα κακόβουλου λογισμικού και άλλες πιθανά κακόβουλες ενέργειες.

Με τον εντοπισμό πιθανών προβλημάτων ασφαλείας, το λογισμικό SIEM δημιουργεί ειδοποιήσεις ασφαλείας, τις οποίες οι οργανισμοί μπορούν να ορίσουν ως χαμηλής ή υψηλής προτεραιότητας χρησιμοποιώντας προκαθορισμένους κανόνες.

3.3.2 Αξία του SIEM

Το SIEM απλοποιεί τη διαχείριση της ασφάλειας για τις επιχειρήσεις φιλτράροντας μεγάλους όγκους δεδομένων καταγραφής και δίνοντας προτεραιότητα στις ειδοποιήσεις ασφαλείας που δημιουργούνται. Το λογισμικό SIEM παρέχει τη δυνατότητα εντοπισμού περιστατικών που ίσως περάσουν απαρατήρητα. Αναλύοντας τις καταχωρήσεις γεγονότων, το λογισμικό εντοπίζει σημάδια κακόβουλης δραστηριότητας, βοηθώντας τις επιχειρήσεις να κατανοήσουν τη φύση και τις επιπτώσεις μιας ενδεχόμενης επίθεσης. Επιπλέον, ένα σύστημα SIEM βοηθά τις επιχειρήσεις να πληρούν τις απαιτήσεις συμμόρφωσης με τη δημιουργία αυτόματων αναφορών που καλύπτουν όλα τα καταγεγραμμένα συμβάντα ασφαλείας από διάφορες πηγές. Χωρίς το λογισμικό SIEM, η συλλογή δεδομένων καταγραφής και η δημιουργία αναφορών θα απαιτούσαν χειροκίνητη εργασία.



Εικόνα 17: Λειτουργία του SIEM ΠΗΓΗ: LOGPOINT[34]

3.3.3 Οφέλη του SIEM

Τα οφέλη του SIEM περιλαμβάνουν:

α. Σημαντική μείωση του χρόνου που απαιτείται για τον εντοπισμό των απειλών και κατά συνέπεια μείωση του αντίκτυπου μιας επιτυχούς επίθεσης.

β. Παροχή ολοκληρωμένης εικόνας του περιβάλλοντος ασφάλειας των πληροφοριών ενός οργανισμού, διευκολύνοντας τη συλλογή και ανάλυση των πληροφοριών ασφαλείας για την ασφάλεια του συστήματος. Όλα τα δεδομένα αποθηκεύονται σε ένα κεντρικό αποθετήριο για εύκολη πρόσβαση.

γ. Υποστήριξη διάφορων περιπτώσεων που σχετίζονται με δεδομένα ή καταγραφές, όπως προγράμματα ασφαλείας, αναφορές ελέγχου και συμμόρφωσης, τμήμα υποστήριξης και αντιμετώπιση προβλημάτων δικτύου.

δ. Χειρισμός μεγάλων όγκων δεδομένων, επιτρέποντας στους οργανισμούς να επεκτείνονται και να προσθέτουν περισσότερα δεδομένα.

ε. Παροχή ανίχνευσης απειλών και ειδοποιήσεων ασφαλείας.

στ. Πραγματοποίηση λεπτομερούς αναλυτικής εξέτασης στην περίπτωση σημαντικών παραβιάσεων της ασφάλειας.

3.3.4 Περιορισμοί του SIEM

Παρά τα οφέλη του, το SIEM έχει κάποιους περιορισμούς[33],[34]:

α. Χρονοβόρα υλοποίηση, που κατά κανόνα απαιτεί 90 ημέρες ή περισσότερο πριν γίνει λειτουργικό.

β. Υψηλό κόστος, συμπεριλαμβανομένων των αρχικών επενδύσεων και των συνεχών εξόδων για προσωπικό, υποστήριξη και λογισμικό.

γ. Εξάρτηση από ειδικούς για ανάλυση, διαμόρφωση και ολοκλήρωση αναφορών.

δ. Εξάρτηση από κανόνες για την ανάλυση των δεδομένων γεγονός που οδηγεί σε αδυναμία διαχείρισης των δεδομένων αυτών, αν οι κανόνες δεν είναι αυστηρά καθορισμένοι.

ε. Πιθανότητα για λανθασμένη ρύθμιση του εργαλείου SIEM, που μπορεί να οδηγήσει στο να χάσει σημαντικά γεγονότα ασφαλείας και να εξασθενίσει την αποτελεσματικότητα της διαχείρισης κινδύνων.

3.4 Jump Box Servers

Οι Jump Box Servers[35] αντιπροσωπεύουν μια προηγμένη προσέγγιση στον τομέα της διαχείρισης ασφαλείας και του ελέγχου πρόσβασης σε εταιρικά δίκτυα. Αυτοί οι διακομιστές λειτουργούν ως ενδιάμεσοι κόμβοι, προσφέροντας ένα ολοκληρωμένο σημείο πρόσβασης για τους διαχειριστές προς τους εσωτερικούς πόρους του δικτύου.

Εικόνα 18: Jump Box Servers ΠΗΓΗ: JAVA Point[35]

3.4.1 Αρχιτεκτονική ενσωμάτωσης στο δίκτυο και λειτουργία

Ο Jump Box Server συνήθως είναι προσβάσιμος από το διαδίκτυο και αξιοποιεί το πρωτόκολλο ασφαλούς σύνδεσης SSH για την εγκαθίδρυση των συνδέσεών του. Συνήθως, εγκαθίσταται ανάμεσα στο εξωτερικό και στο εσωτερικό δίκτυο. Η βέλτιστη πρακτική είναι η τοποθέτηση τους σε μια DMZ του δικτύου για επιπλέον ασφάλεια. Οι διαχειριστές συνδέονται στον Jump Box Server μέσω σύνδεσης SSH και στη συνέχεια, μετά την διαδικασία αυθεντικοποίησης, αποκτούν πρόσβαση στους εσωτερικούς πόρους του δικτύου.

Ο κύριος σκοπός του είναι να λειτουργεί ως πύλη (gateway) της επιφάνειας προστασίας στην οποία συνδέεται με σκοπό την μείωση της ορατής επιφάνειας στους επιτιθέμενους. Η αρχιτεκτονική αυτή δημιουργεί ένα επιπλέον επίπεδο προστασίας, καθόσον οι εξωτερικοί χρήστες δεν έχουν απευθείας πρόσβαση στους εσωτερικούς πόρους. Επιπλέον, αποτελώντας μοναδικό σημείο σύνδεσης με SSH, διευκολύνει την συλλογή των αρχείων καταγραφής (logs) και κατά συνέπεια συνεισφέρει στην αποδοτικότερη λειτουργία των SIEM.

3.4.2 Πλεονεκτήματα των Jump Box Servers

Οι Jump Box Servers συνδυάζουν ασφάλεια, δυνατότητα ελέγχου και καταγραφής καθώς και ευκολία διαχείρισης, καθιστώντας τους αποτελεσματικούς στην προστασία των δικτύων και των συστημάτων από ανεπιθύμητη πρόσβαση και επιθέσεις. Τα πλεονεκτήματά τους είναι:

α. Ενίσχυση Ασφάλειας: Η χρήση ενός Jump Box Server προσφέρει ένα επιπρόσθετο επίπεδο ασφάλειας, καθώς λειτουργεί ως πύλη πρόσβασης. Αυτό δημιουργεί ένα φράγμα μεταξύ του εξωτερικού δικτύου και των εσωτερικών πόρων, περιορίζοντας την επιφάνεια επίθεσης.

β. Ελέγχος Πρόσβασης: Ο Jump Box Server παρέχει έναν ελεγχόμενο τρόπο πρόσβασης σε εσωτερικούς πόρους. Οι διαχειριστές συνδέονται αρχικά, με ασφαλή και κρυπτογραφημένη σύνδεση στο Jump Box Server και από εκεί έχουν πρόσβαση σε άλλους πόρους.

γ. Συγκεντρωμένος Έλεγχος Καταγραφής: Ο Jump Box Server λειτουργεί ως σημείο καταγραφής για όλες τις συνδέσεις, διευκολύνοντας τη διαχείριση καταγραφικών δεδομένων για λογούς ασφαλείας και παρακολούθησης.

δ. Ευκολία Συντήρησης: Ο Jump Box Server μπορεί να χρησιμοποιηθεί για την κεντρική διαχείριση και συντήρηση, καθώς οι ενημερώσεις και οι αλλαγές μπορούν να εφαρμοστούν σε ένα κεντρικό σημείο.

ε. Ελαχιστοποίηση Επιθέσεων: Ο Jump Box Server μειώνει την επιφάνεια επίθεσης, καθώς οι εξωτερικές συσκευές δεν είναι άμεσα προσβάσιμες. Αυτό βοηθά στην αντιμετώπιση δυνητικών κινδύνων ασφαλείας.

στ. Ευελιξία Πρόσβασης: Οι διαχειριστές μπορούν να συνδεθούν από οπουδήποτε στον Jump Box Server, προσφέροντας ευελιξία στην πρόσβαση και τη διαχείριση των συστημάτων.

ζ. Εξοικονόμηση Πόρων: Ο Jump Box Server μπορεί να συμβάλει στην εξοικονόμηση πόρων, καθώς οι διαχειριστές μπορούν να συνδεθούν μόνο στο Jump Box Server αντί να απαιτείται πρόσβαση σε κάθε επιμέρους πόρο ξεχωριστά (Single Sign On).

3.4.3 Μειονεκτήματα των Jump Box Server.

α. Καθυστέρηση Πρόσβασης: Η ανάγκη για επιπλέον στάδια πιστοποίησης μέσω του Jump Box Server μπορεί να προκαλέσει καθυστερήσεις στην

πρόσβαση στους εσωτερικούς πόρους. Αυτή η καθυστέρηση μπορεί να είναι παράγοντας μείωσης απόδοσης για διαχειριστές που απαιτούν γρήγορη πρόσβαση.

β. Διακοπή Υπηρεσιών: Σε περίπτωση που ο Jump Box Server αντιμετωπίσει προβλήματα ή διακοπεί, οι διαχειριστές μπορεί να χάσουν την πρόσβαση σε εσωτερικούς πόρους, προκαλώντας πιθανή διακοπή υπηρεσιών.

γ. Απομακρυσμένη Διαχείριση: Η ανάγκη για σύνδεση μέσω Jump Box Server καθιστά πιο περίπλοκη τη διαχείριση συστημάτων από απομακρυσμένους τόπους, ειδικά σε περιβάλλοντα όπου η σύνδεση στον Jump Box Server απαιτεί πολύπλοκες διαδικασίες πιστοποίησης.

δ. Αυξημένο Κόστος Υποδομής: Η ανάγκη για επιπλέον υποδομή, όπως επιπλέον διακομιστές και ασφαλείς συνδέσεις, μπορεί να αυξήσει το συνολικό κόστος υποδομής.

ε. Πολυπλοκότητα Συντήρησης: Η διαχείριση και η συντήρηση ενός Jump Box Server απαιτεί πρόσθετο χρόνο και πόρους, καθιστώντας την εγκατάσταση και τη συντήρησή του σύνθετες διαδικασίες σε σύγκριση με άλλες λύσεις.

Τα μειονεκτήματα αυτά πρέπει να ληφθούν υπόψη κατά τον σχεδιασμό και την υλοποίηση των Jump Box Servers, προκειμένου να εξασφαλιστεί ότι η επιλογή αυτή είναι συμβατή με τις συγκεκριμένες ανάγκες και απαιτήσεις του οργανισμού.

3.5 Multi-Factor Authentication (MFA)

Η πολυπαραγοντική ταυτοποίηση είναι μια μέθοδος αυθεντικοποίησης χρηστών που απαιτεί τη χρήση δύο ή περισσότερων παραγόντων επιβεβαίωσης πριν από την παροχή πρόσβασης. Αυτοί οι παράγοντες επιβεβαίωσης χωρίζονται συνήθως σε τρεις κατηγορίες: κάτι που γνωρίζει ο χρήστης (π.χ., κωδικός πρόσβασης), κάτι που κατέχει ο χρήστης (π.χ., κάρτα πρόσβασης) και κάτι που είναι ιδιαίτερο για τον χρήστη (π.χ., αναγνώριση δακτυλικών αποτυπωμάτων).

Ο στόχος του MFA είναι να δημιουργήσει μια πολυεπίπεδη άμυνα που καθιστά πιο δύσκολη, για ένα μη εξουσιοδοτημένο άτομο, την πρόσβαση σε έναν στόχο, όπως μια φυσική τοποθεσία, μια υπολογιστική συσκευή, ένα δίκτυο ή μια βάση δεδομένων. Εάν ένας παράγοντας έχει παραβιαστεί ή σπάσει, ο εισβολέας εξακολουθεί να έχει τουλάχιστον ένα ή περισσότερα εμπόδια για να παραβιάσει προτού διαρρήξει επιτυχώς τον στόχο.

3.5.1 Αναγκαιότητα του MFA

Μια από τις πιο συχνές επιθέσεις κυβερνοασφάλειας αποτελεί το phishing, δηλαδή η προσπάθεια παράνομης απόκτησης κωδικών πρόσβασης χρηστών, μέσω παραπλανητικών e-mails. Υπολογίζεται ότι περίπου 3,5 δισεκατομμύρια παραπλανητικά e-mails διακινούνται καθημερινά στο διαδίκτυο[36], τα περισσότερα από τα οποία έχουν ως τελικό αποτέλεσμα την επιτυχή παραβίαση λογαριασμών και υπολογιστικών συστημάτων. Το γεγονός αυτό είναι το πλέον χαρακτηριστικό για να υποδείξει την αναγκαιότητα της χρήσης πολυπαραγοντικών μεθόδων ταυτοποίησης από τους χρήστες, διότι ακόμα και αν αποτελέσουν θύματα phishing, ο επιτιθέμενος

δεν θα μπορέσει εύκολα να αποκτήσει τους υπόλοιπους παράγοντες ταυτοποίησης για να αποκτήσει πρόσβαση στον λογαριασμό.

3.5.2 Τεχνικές Πιστοποίησης στο MFA

Ένας παράγοντας πιστοποίησης λειτουργεί ως μια κατηγορία διαπιστευτηρίων που χρησιμοποιούνται για τον έλεγχο της ταυτότητας. Στον κόσμο του MFA, κάθε επιπλέον παράγοντας προσπαθεί να ενισχύσει τη βεβαιότητα ότι ένα περιεχόμενο σε κάποια μορφή επικοινωνίας ή μια οντότητα που αιτείται πρόσβαση σε ένα σύστημα, είναι πράγματι αυτό που υποστηρίζει ότι είναι.

Οι τρεις κύριες κατηγορίες ή παράγοντες πιστοποίησης[37] περιγράφονται συχνά ως κάτι που γνωρίζεις (knowledge factor), κάτι που κατέχεις (possession factor) και κάτι που είσαι (inherence factor). Το MFA λειτουργεί συνδυάζοντας δύο ή περισσότερους παράγοντες από αυτές τις κατηγορίες.

3.5.2.1 Παράγοντας Γνώσης (Knowledge Factor)

Η πιστοποίηση βασισμένη στη γνώση συνήθως απαιτεί από τον χρήστη να απαντήσει σε προσωπικές ερωτήσεις ασφαλείας. Οι τεχνολογίες παράγοντα γνώσης περιλαμβάνουν κωδικούς πρόσβασης, τετραψήφιους αριθμούς PIN και απαντήσεις σε ερωτήσεις ασφαλείας. Συνήθη σενάρια χρήσης του παράγοντα γνώσης περιλαμβάνουν:

α. Εισαγωγή PIN μετά από το πέρασμα μιας χρεωστικής κάρτας στο ταμείο ενός καταστήματος.

β. Σύνδεση σε ένα VPN δίκτυο με τη χρήση έγκυρου ψηφιακού πιστοποιητικού.

γ. Παροχή απαντήσεων σε προσωπικές ερωτήσεις ασφαλείας.

3.5.2.2 Παράγοντας Κατοχής (Possession Factor)

Οι χρήστες πρέπει να κατέχουν κάτι συγκεκριμένο για να συνδεθούν, όπως μια κάρτα τεχνολογίας RFC, ένα token key, μια μηχανή παραγωγής κλειδών OTP (key fob) ή μια κάρτα SIM ενός κινητού τηλεφώνου (πιστοποίηση με αποστολή μηνύματος η τηλεφωνικής κλήσης). Στην πιστοποίηση μέσω κινητών, τα smartphones συχνά συμβάλλουν στον παράγοντα κατοχής με την ενσωμάτωση μιας εφαρμογής OTP.

Συνήθη σενάρια παράγοντα κατοχής περιλαμβάνουν:

α. Κινητή πιστοποίηση, όπου οι τελικοί χρήστες λαμβάνουν έναν κωδικό στο smartphone τους για να αποκτήσουν ή να παραχωρήσουν πρόσβαση. Παραλλαγές περιλαμβάνουν μηνύματα κειμένου και τηλεφωνήματα που αποστέλλονται σε ένα χρήστη ως μέθοδο out-of-band, εφαρμογές OTP για smartphones, κάρτες SIM και έξυπνες κάρτες με αποθηκευμένα δεδομένα πιστοποίησης.

β. Σύνδεση ενός USB hardware token σε έναν υπολογιστή που δημιουργεί έναν OTP και χρησιμοποιείται για τη σύνδεση σε έναν VPN client.

3.5.2.3 Παράγοντας Κληρονομιάς (Inherence Factor)

Περιλαμβάνει βιολογικά χαρακτηριστικά τα οποία επαληθεύονται για την απόκτηση πρόσβασης. Οι τεχνολογίες παράγοντα κληρονομιάς περιλαμβάνουν μεθόδους βιομετρικής επαλήθευσης όπως σάρωση ίριδας ματιού, σάρωση αποτυπωμάτων, φωνητική πιστοποίηση, γεωμετρία χεριού, σαρωτές ψηφιακών υπογραφών, αναγνώριση προσώπου και γεωμετρία αυτιού. Σε αυτά υιοθετείται σταδιακά όλο και περισσότερο και η χρήση συστημάτων γεωεντοπισμού για την επαλήθευση της τοποθεσίας του χρήστη. Επιπλέον, κυρίως σε τραπεζικά συστήματα υιοθετείται και η πιστοποίηση βάση του χρόνου (time-stamp), εντοπίζοντας το άτομο σε μια συγκεκριμένη ωρική ζώνη, και παρέχοντάς του πρόσβαση μόνο στα υπολογιστικά συστήματα της συγκεκριμένης τοποθεσίας. Για παράδειγμα, μέσω του time-stamp μπορεί να απαγορευτεί η χρήση μιας πιστωτικής κάρτας αν διαπιστωθεί ότι μέσα σε ελάχιστο χρονικό διάστημα χρησιμοποιήθηκε σε δυο διαφορετικές χώρες διαφορετικής ωρικής ζώνης.

3.5.3 Πλεονεκτήματα του Multi – Factor Authentication

Τα πλεονεκτήματα του Multi- Factor Authentication είναι:

α. Ενίσχυση της ασφάλειας σε επίπεδο υλικού, λογισμικού και προσωπικής ταυτότητας.

β. Χρησιμοποιεί κωδικούς μιας χρήσης που αποστέλλονται στα τηλέφωνα σε πραγματικό χρόνο και είναι δύσκολο για τους επιτιθέμενους να τους αποκτήσουν.

γ. Μπορεί να μειώσει σημαντικά τις παραβιάσεις ασφαλείας κατά έως και 99,9% σε σχέση με τους κωδικούς πρόσβασης μόνο.

δ. Είναι εύκολο στην εγκατάσταση από τους χρήστες.

ε. Επιτρέπει στις επιχειρήσεις να περιορίζουν την πρόσβαση ανάλογα με την ώρα της ημέρας ή την τοποθεσία.

στ. Προσφέρει κλιμακούμενο κόστος και προσιτές επιλογές για μικρές επιχειρήσεις.

ζ. Βελτιώνει τα μέτρα ασφαλείας και την ανταπόκριση των επιχειρήσεων, καθώς μπορούν να δημιουργήσουν ένα σύστημα πολυπαραγοντικής ταυτοποίησης που παράγει ενεργά ειδοποιήσεις όταν ανιχνεύονται αμφιλεγόμενες προσπάθειες.

3.5.4 Μειονεκτήματα του Multi – Factor Authentication

Παρά τα αδιαμφησβήτητα πλεονεκτήματά του Multi – Factor Authentication, υπάρχουν μειονεκτήματα τα οποία δυσχεραίνουν την υιοθέτησή του, όπως παρακάτω:

α. Εξάρτηση από Κινητές Συσκευές: Απαιτείται η χρήση κινητού τηλεφώνου για την λήψη ενός κωδικού μηνύματος κειμένου ή για την χρήση ενός OTP authenticator.

β. Κίνδυνος Απώλειας ή Κλοπής: Υπάρχει ο δυνητικός κίνδυνος απώλειας ή κλοπής των token, καθώς και των κινητών τηλεφώνων.

γ. Ακρίβεια των Βιομετρικών Δεδομένων: Η ακρίβεια των βιομετρικών δεδομένων, όπως οι αποτυπώσεις, που υπολογίζονται από αλγόριθμους MFA για προσωπικά αναγνωριστικά, δεν είναι πάντα εγγυημένα και μπορεί να οδηγήσει σε λανθασμένα θετικά ή αρνητικά αποτελέσματα.

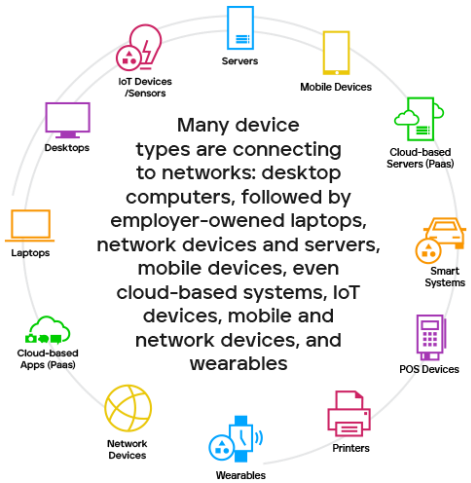
δ. Ευπάθεια σε Διακοπές Δικτύου: Η επαλήθευση MFA μπορεί να αντιμετωπίσει προκλήσεις και να αποτύχει σε περίπτωση διακοπής του δικτύου ή του internet.

ε. Συνεχής ανάγκη αναβάθμισης: Οι τεχνικές MFA πρέπει να αναβαθμίζονται συνεχώς για να προστατεύονται από κυβερνοεπιθέσεις, καθώς οι κυβερνοεγκληματίες εργάζονται αδιακόπως για να τις ανακαλύψουν.

στ. Δυσχέρεια στην χρήση γεωεντοπισμού ως παράγοντα αυθεντικοποίησης, καθόσον σε περίπτωση απόπειρας σύνδεσης ενός χρήστη στο εταιρικό δίκτυο από μη αναμενόμενη τοποθεσία (πχ μέσω χρήσης δημόσιου WIFI) θα προκαλέσει συναγερμό ασφαλείας στο σύστημα.

3.6 Endpoint Security

Το Endpoint security αφορά στην εφαρμογή μέτρων ασφάλειας σε συσκευές τελικού χρήστη όπως desktops, laptops και φορητές συσκευές και αποτελεί μια κρίσιμη πρακτική για την προστασία των οργανισμών από κυβερνοαπειλές. Αυτό περιλαμβάνει την προστασία από κακόβουλους χρήστες που στοχεύουν σε αυτές τις συσκευές διότι αποτελούν σημεία πρόσβασης σε δίκτυα ή στο cloud. Κάθε σημείο που συνδέεται στο εταιρικό δίκτυο αποτελεί μια ευπάθεια, παρέχοντας ένα δυνητικό σημείο εισόδου για κυβερνοεγκληματίες. Συνεπώς, κάθε συσκευή που χρησιμοποιεί ένας εργαζόμενος για σύνδεση σε οποιοδήποτε επιχειρηματικό σύστημα ή πόρο φέρει τον κίνδυνο να γίνει η επιλεγμένη διαδρομή για την εισβολή σε έναν οργανισμό.



Εικόνα 19: Endpoints ΠΗΓΗ: Trellix[39]

Στο σημερινό επιχειρηματικό περιβάλλον, η αύξηση των κυβερνοαπειλών από εξαιρετικά προηγμένους εγκληματίες είναι προφανής, με τους χάκερ να εκτοξεύουν επιθέσεις κάθε 39 δευτερόλεπτα και συνολικά 2.244 επιθέσεις καθημερινά. Τα σημεία πρόσβασης είναι ένα από τα πιο συνήθη θύματα, δεδομένου του μεγάλου αριθμού τους που χρησιμοποιούνται για σύνδεση στα δίκτυα. Σύμφωνα με την έρευνα της Strategy Analytics[38], υπήρχαν ήδη 22 δισεκατομμύρια συνδεδεμένες συσκευές το 2018, έναν αριθμό που προβλέπεται να αυξηθεί σε 38,6 δισεκατομμύρια συσκευές έως το 2025 και 50 δισεκατομμύρια συσκευές έως το 2030.

Ανεξαρτήτως μεγέθους, οι οργανισμοί έρχονται αντιμέτωποι με τους παραπάνω κινδύνους στους οποίους έρχονται να προστεθούν εσωτερικές απειλές από χρήστες οι οποίοι, είτε εκούσια είτε ακούσια, δημιουργούν κενά στην ασφάλεια. Το endpoint security συχνά, θεωρείται η πρώτη γραμμή της κυβερνοασφάλειας και αντιπροσωπεύει έναν από τους πρώτους τομείς που επενδύουν οι οργανισμοί για να ασφαλίσουν τα επιχειρηματικά τους δίκτυα. Καθώς ο όγκος και η πολυπλοκότητα των κυβερνοαπειλών έχουν σταθερά αυξηθεί, έτσι και η ανάγκη για πιο προηγμένες λύσεις endpoint security. Τα σύγχρονα συστήματα προστασίας βασίζονται στο παραδοσιακό λογισμικό Antivirus, ωστόσο ενσωματώνουν και άλλα εξελιγμένα εργαλεία και σχεδιάζονται για να ανιχνεύουν, αναλύουν, αποκλείουν και περιορίζουν γρήγορα εξελιγμένα malware και Zero Day Attacks. Για να το επιτύχουν αυτό, χρειάζονται να συνεργάζονται μεταξύ τους και με άλλες τεχνολογίες ασφαλείας ώστε να παρέχουν στους διαχειριστές ορατότητα σε προηγμένες απειλές, επιταχύνοντας τους χρόνους ανίχνευσης και αντίδρασης στην αντιμετώπιση προβλημάτων.

3.6.1 Δομικά στοιχεία του Endpoint Security

Με την αυξανόμενη δημοτικότητα της πρακτικής "φέρε τη δική σου συσκευή" (BYOD) και την αυξανόμενη χρήση φορητών συσκευών IoT, είναι ζωτικό για τους οργανισμούς να εξετάσουν εάν η λύση ασφαλείας στο τελικό σημείο είναι επαρκώς ολοκληρωμένη για την αντιμετώπιση απειλών σε όλους τους τομείς. Συνεπώς, οι οργανισμοί πρέπει να αναγνωρίσουν τα βασικά στοιχεία μιας λύσης ασφαλείας του τελικού σημείου:

α. Προστασία της συσκευής: Η προστασίας συσκευής αφορά τον εντοπισμό και την έρευνα δραστηριοτήτων που μπορεί να είναι ύποπτες σε συσκευές τελικού σημείου. Περιλαμβάνει εργαλεία Endpoint Detection and Response (EDR), τα οποία παρακολουθούν, καταγράφουν και αναλύουν συμβάντα τελικού σημείου. Αυτό βοηθά τις ομάδες ασφαλείας να ανιχνεύουν αποτελεσματικά και να αντιμετωπίζουν πιθανές απειλές προτού εκδηλωθούν.

Οι λύσεις ασφαλείας τελικού σημείου παρέχουν next-gen antivirus και προστασία από κακόβουλο λογισμικό (malware) για όλα τα είδη συσκευών. Τα next-gen antivirus χρησιμοποιούν δυνατότητες προηγμένης ανάλυσης στοιχείων και μηχανική μάθηση, γεγονός που καθιστά την αντιμετώπιση αναδυόμενων ransomware και προηγμένων επιθέσεων phishing που αποφεύγουν το παραδοσιακό λογισμικό προστασίας από ιούς, πιο εύκολη.

β. Έλεγχος Δικτύου: Ο έλεγχος του δικτύου αφορά την παρακολούθηση και τον έλεγχο της εισερχόμενης δικτυακής κίνησης. Παρέχει λειτουργίες firewall που συντελούν στον εντοπισμό, την αναγνώριση και την αντιμετώπιση πιθανών απειλών που μπορούν να μολύνουν το δίκτυο του οργανισμού.

γ. Έλεγχος Εφαρμογών: Ο έλεγχος των εφαρμογών αφορά στον προσδιορισμό, στην παρακολούθηση και τον περιορισμό της πρόσβασης των τελικών σημείων, στις εφαρμογές του δικτύου του οργανισμού. Επίσης, μέσω αυτού του στοιχείου δύναται να πραγματοποιούνται και οι ενημερώσεις ασφαλείας των εφαρμογών (security patches) που χρησιμοποιούνται στα τελικά σημεία, εξασφαλίζοντας με τον τρόπο αυτό ότι οι συσκευές που διασυνδέονται στο δίκτυο του οργανισμού δεν παρουσιάζουν κενά ασφαλείας, εξαιτίας μη ενημερωμένων εφαρμογών.

δ. Έλεγχος δεδομένων : Αφορά στον τρόπο διαχείρισης των δεδομένων που ταξιδεύουν στο δίκτυο καθώς και στον τρόπο με τον οποίο αυτά αποθηκεύονται. Αποσκοπεί στον περιορισμό της διαρροής δεδομένων, εφαρμόζοντας κρυπτογραφία τόσο κατά την μετάδοση, όσο και κατά την αποθήκευση, έτσι ώστε σε πιθανή διαρροή δεδομένων, αυτά να μην είναι αξιοποιήσιμα στα χέρια του κακόβουλου χρήστη.

ε. Προστασία Περιηγητή Διαδικτύου: Αφορά στην εφαρμογή φίλτρων περιορισμού στους ιστοτόπους που μπορεί να επισκεφθεί ο χρήστης, όσο αυτός είναι συνδεδεμένος στο δίκτυο του οργανισμού. Επιπλέον, περιλαμβάνεται η δυνατότητα αξιολόγησης της ασφάλειας των ιστοτόπων και η προειδοποίηση ή και απαγόρευση την πρόσβασης, σε περίπτωση που ο συγκεκριμένος ιστότοπος έχει χαρακτηριστεί ως κακόβουλος.

3.6.2 Πλεονεκτήματα του Endpoint Security

Το λογισμικό ασφαλείας τελικού σημείου (Endpoint Security Software) είναι μια ολοκληρωμένη λύση που σχεδιάστηκε για να προστατεύει την ακεραιότητα και την ασφάλεια των συσκευών τελικού σημείου εντός ενός δικτύου. Αποτελείται από αρκετά βασικά συστατικά που συνεισφέρουν συλλογικά, σε μια ανθεκτική άμυνα ενάντια σε διάφορες κυβερνοαπειλές. Αυτά τα συστατικά περιλαμβάνουν[39]:

α. Μηχανική Μάθηση: Χρησιμοποιούνται προηγμένοι αλγόριθμοι μηχανικής μάθησης για την αναγνώριση και κατηγοριοποίηση απειλών Zero Day, σε πραγματικό χρόνο, ενισχύοντας έτσι την ικανότητα του λογισμικού να ανιχνεύει και να ανταποκρίνεται σε αναδυόμενα και προηγουμένως αόρατα κακόβουλα προγράμματα.

β. Προστασία Antivirus και Antimalware: Παρέχει προηγμένη προστασία ενάντια σε ευρύ φάσμα κακόβουλου λογισμικού και ιών. Ανιχνεύει, απομονώνει και διορθώνει κακόβουλο λογισμικό, σε διάφορες συσκευές τελικού σημείου και λειτουργικά συστήματα, εξασφαλίζοντας ολοκληρωμένη κάλυψη.

γ. Ασφάλεια Ιστού: Εφαρμόζει μέτρα για την ασφαλή περιήγηση στον ιστό. Ανιχνεύει και αποκλείει προληπτικά δυνητικές απειλές, κατά τη διάρκεια διαδικτυακών δραστηριοτήτων, μειώνοντας τον κίνδυνο μολύνσεων.

δ. Πρόληψη Απώλειας Δεδομένων: Κατηγοριοποιεί τα ευαίσθητα δεδομένα, εφαρμόζοντας μέτρα για τον περιορισμό της μη εξουσιοδοτημένης πρόσβασης, απώλειας ή παραποίησης. Βελτιώνει τη συνολική ασφάλεια των δεδομένων, μέσω της εφαρμογής πολιτικών, για τον έλεγχο της κίνησης ευαίσθητων πληροφοριών.

ε. Ενσωματωμένο Τείχος Προστασίας: Παρακολουθεί και ελέγχει τη ροή δικτυακών δεδομένων βάσει προκαθορισμένων κανόνων ασφαλείας, για την

πρόληψη μη εξουσιοδοτημένης πρόσβασης και κακόβουλων δραστηριοτήτων. Παρακολουθεί και ελέγχει την εισερχόμενη και εξερχόμενη κυκλοφορία δεδομένων για την πρόληψη ανεπιθύμητης πρόσβασης και πιθανών παραβιάσεων ασφάλειας.

στ. Πύλη Email: Προστατεύει ενάντια σε προσπάθειες phishing και επιθέσεις κοινωνικής μηχανικής που στοχεύουν τους υπαλλήλους. Αυτό επιτυγχάνεται μέσω της ανάλυσης των εισερχόμενων emails για κακόβουλο περιεχόμενο, αποτρέποντας τους χρήστες από το να πέσουν θύματα κυβερνοαπειλών μέσω email.

ζ. Ανάλυση Απειλών: Παρέχει στους διαχειριστές λεπτομερείς γνώσεις και εργαλεία ανάλυσης για τη γρήγορη απομόνωση και ανταπόκριση σε περιστατικά ασφάλειας. Δίνει τη δυνατότητα ανάπτυξης προληπτικών μέτρων για τον περιορισμό των επιπτώσεων πιθανών παραβιάσεων ασφάλειας.

η. Προστασία από Εσωτερικές Απειλές: Προστατεύει ενάντια σε ακούσιες και κακόβουλες ενέργειες που προέρχονται από το εσωτερικό του οργανισμού. Παρακολουθεί και ελέγχει τις ενέργειες των χρηστών για την πρόληψη διαρροής δεδομένων που προκαλούνται από εσωτερικές απειλές.

θ. Κεντρική Πλατφόρμα Διαχείρισης Τελικού Σημείου: Βελτιώνει την ορατότητα και τον έλεγχο παρέχοντας μια κεντρική πλατφόρμα για τη διαχείριση της ασφάλειας των συσκευών τελικού σημείου. Καθιστά αποτελεσματική την παρακολούθηση και την ανταπόκριση σε περιστατικά ασφάλειας, απλοποιώντας τις λειτουργίες.

ι. Κρυπτογράφηση: Εφαρμόζει μέτρα κρυπτογράφησης για την πρόληψη μη εξουσιοδοτημένης πρόσβασης σε ευαίσθητα δεδομένα. Διασφαλίζει την ακεραιότητα και την εμπιστευτικότητα κρυπτογραφώντας τα δεδομένα στις συσκευές τελικού σημείου, στα emails και στον αποθηκευτικό χώρο.

Με την ενσωμάτωση αυτών των συστατικών, το λογισμικό ασφαλείας τελικού σημείου παρέχει μια πολυεπίπεδη στρατηγική άμυνας, αντιμετωπίζοντας διάφορες κυβερνοαπειλές και ευπάθειες που μπορεί να στοχεύουν τις συσκευές τελικού σημείου του δικτύου του οργανισμού. Η πολυεπίπεδη αυτή ασφάλεια συνδέεται άρρηκτα με την αρχιτεκτονική Zero Trust καθώς αποτελεί μέτρο προστασίας των συσκευών των χρηστών οι οποίοι αποτελούν την επιφάνεια προστασίας η οποία δέχεται τις περισσότερες επιθέσεις.

3.7 Next – Generation Firewalls (NGFW)

Το Firewall είναι ένα εργαλείο ασφαλείας το οποίο παρακολουθεί και φιλτράρει την εισερχόμενη και εξερχόμενη κίνηση στο δίκτυο, με βάση τις προκαθορισμένες πολιτικές ασφαλείας μιας οργάνωσης. Στην πιο βασική του μορφή, ένα Firewall είναι ουσιαστικά ο φράχτης που διαχωρίζει το εσωτερικό δίκτυο ενός οργανισμού από το διαδίκτυο. Ο κύριος σκοπός του είναι να αποτρέπει την είσοδο κακόβουλης δικτυακής κίνησης στο εσωτερικό δίκτυο του οργανισμού. Αποτελεί δε, τον ακρογωνιαίο λίθο στην αρχιτεκτονική Zero Trust[40].

Τα Firewall εμφανίστηκαν για πρώτη φορά την δεκαετία του 1980. Οι δυνατότητές τους περιορίζονταν στο φιλτράρισμα των πακέτων του δικτύου. Η δυνατότητα αυτή συμπεριλαμβάνεται ακόμα και σήμερα αλλά τα Firewall έχουν

εξελίξει κατά πολύ τις δυνατότητές τους, απόρροια της εξέλιξης της τεχνολογίας και κατ' επέκταση και των επιθέσεων που καλούνται να μετριάσουν[41].

3.7.1 Δυνατότητες των NGFW

Τα σύγχρονα Firewall ονομάζονται Next – Generation Firewalls και μπορούν να εφαρμοστούν είτε σε συσκευή είτε ως λογισμικό. Διαθέτουν την ικανότητα ανίχνευσης και αντιμετώπισης εξελιγμένων επιθέσεων σε επίπεδο εφαρμογής, πρωτοκόλλου και port. Πέραν αυτού περιλαμβάνουν λειτουργίες όπως:

α. Αναγνώριση και ταξινόμηση εφαρμογών στο δίκτυο (Application Awareness).

β. Ενσωματωμένο σύστημα αναγνώρισης και αντιμετώπισης εισβολής (IDS/IPS).

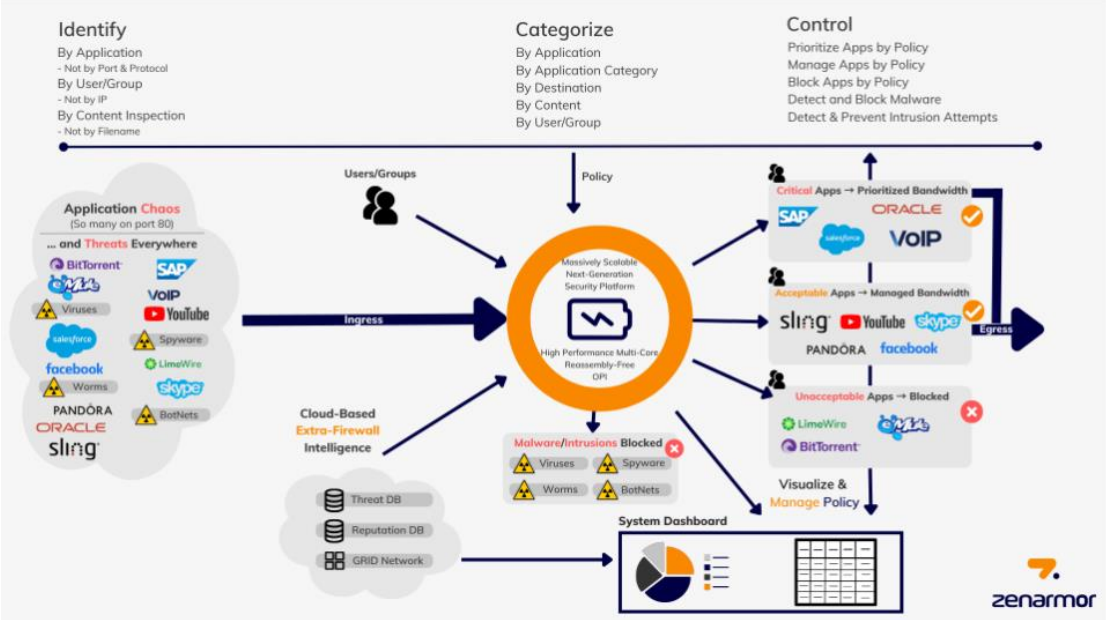
γ. Αναγνώριση ταυτότητας (Ως Certificate Authority).

δ. Λειτουργίες δρομολόγησης.

ε. Χρήση εξωτερικών πηγών πληροφοριών.

στ. Δυνατότητες Network/Port Address Translation (NAT/PAT).

ζ. Δυνατότητες VPN.



Εικόνα 19: NGFW ΠΗΓΗ: Zenarmor[42]

3.7.2 Οφέλη ενός NGFW

Τα NGFW προσφέρουν πολλά πλεονεκτήματα για όλους τους τύπους και μεγέθη δικτύων. Τα οφέλη ενός NGFW είναι[42]:

α. Αυξημένη Παραγωγικότητα: Το κύριο πλεονέκτημα ενός NGFW είναι η ασφαλής χρήση εφαρμογών Διαδικτύου, επιτρέποντας στους χρήστες να είναι πιο παραγωγικοί, ενώ αποκλείονται μη επιθυμητές εφαρμογές. Τα τείχη προστασίας επόμενης γενιάς το επιτυγχάνουν χρησιμοποιώντας τη δυνατότητα deep packet inspection για τον εντοπισμό και τον έλεγχο εφαρμογών ανεξάρτητα από την IP port τους.

β. Ενοποιημένα συστήματα: Τα τείχη προστασίας επόμενης γενιάς περιλαμβάνουν πέραν όλων των λειτουργιών των παραδοσιακών τειχών προστασίας, ολοκληρωμένα συστήματα ανίχνευσης εισβολής (IDS) και συστήματα προστασίας από εισβολή (IPS) που ανιχνεύουν επιθέσεις βάσει ανάλυσης συμπεριφοράς δικτύου (NBA), υπογραφές απειλών ή ανώμαλη δραστηριότητα. Αυτή η λειτουργία βοηθά στη διεξαγωγή αναλυτικότερης επιτήρησης της κυκλοφορίας του δικτύου και στη βελτίωση του φιλτραρίσματος του περιεχομένου των πακέτων μέχρι το επίπεδο εφαρμογής.

γ. Ορατότητα και Δυνατότητα Διαχείρισης: Τα NGFW παρέχουν μεγαλύτερη ορατότητα στις εφαρμογές και στο δίκτυο, επιτρέποντας στους διαχειριστές να δουν τι συμβαίνει από το εσωτερικό δίκτυο στο εξωτερικό δίκτυο ή το αντίστροφο. Επίσης, μπορούν να αναγνωρίσουν τους χρήστες που επισκέπτονται κακόβουλους ιστότοπους ή κάνουν λήψη κακόβουλου κώδικα, καθώς και ποιο είναι το όνομα του κώδικα και από ποια χώρα. Αυτό αντιμετωπίζεται με την ενοποίηση των NGFW με καταλόγους χρηστών τρίτων κατασκευαστών, όπως το Microsoft Active Directory. Η δυναμική πολιτική που βασίζεται στην ταυτότητα παρέχει πιο λεπτομερή ορατότητα και έλεγχο στους χρήστες και τις ομάδες από ό,τι η πολιτική που βασίζεται σε στατική IP και είναι πιο εύκολη στη διαχείριση. Όταν τα τείχη προστασίας δικτύου ανιχνεύουν μια νέα σύνδεση, η διεύθυνση IP αντιστοιχίζεται στο χρήστη και στην ομάδα. Η δυναμική αντιστοίχιση χρήστη σε IP, απαλλάσσει τους διαχειριστές από την ανάγκη συνεχούς ενημέρωσης της πολιτικής ασφαλείας.

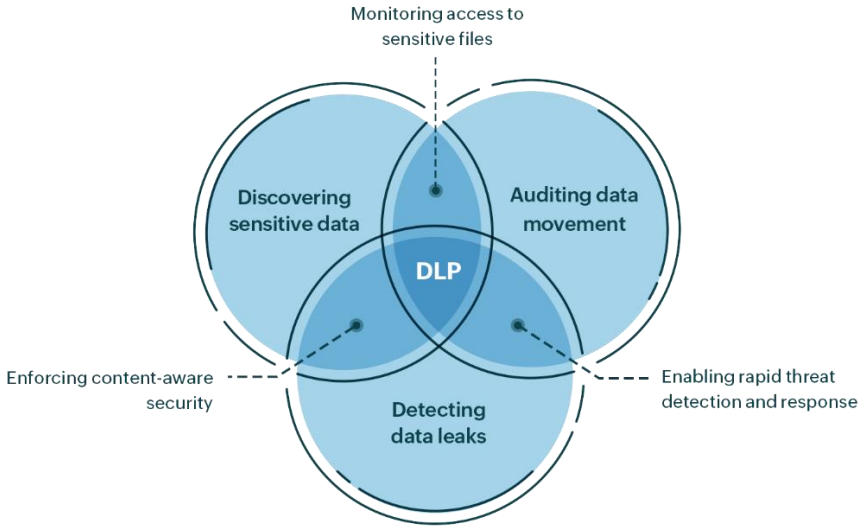
δ. Φιλτράρισμα Περιεχομένου: Ένα άλλο πλεονέκτημα του NGFW είναι το φιλτράρισμα περιεχομένου, το οποίο είναι πολύ χρήσιμο για την αποτροπή διαρροής δεδομένων και τον τερματισμό των απειλών στον κυβερνοχώρο, με λεπτομερή και σε πραγματικό χρόνο επιθεώρηση πακέτων. Οι δυνατότητες φιλτραρίσματος περιεχομένου περιλαμβάνουν φιλτράρισμα URL, δεδομένων και πρόληψη απειλών.

ε. Πρόληψη και Μετριασμός Απειλών: Τα τείχη προστασίας επόμενης γενιάς (NGFW) περιλαμβάνουν προστασία από ιούς και κακόβουλο λογισμικό που ενημερώνεται αυτόματα κάθε φορά που διαπιστώνονται νέες απειλές. Η συσκευή NGFW μειώνει επίσης, την επιφάνεια επίθεσης περιορίζοντας τις εφαρμογές που εκτελούνται σε αυτήν. Ελέγχει όλες τις αποδεκτές εφαρμογές για τυχόν κρυφά ελαττώματα ασφαλείας ή παραβιάσεις εμπιστευτικών δεδομένων, καθώς και κινδύνους που ενέχουν άγνωστες εφαρμογές, γεγονός που στοχεύει στην ελαχιστοποίηση της χρήσης εύρους ζώνης από περιττή κίνηση.

στ. Χαμηλό κόστος: Επειδή μπορούν να συνδυάσουν τις δυνατότητες τείχους προστασίας, προστασίας από ιούς, φίλτρων ιστού και άλλων εφαρμογών ασφαλείας σε μια ενιαία λύση, τα NGFW αποτελούν μια επιλογή χαμηλού κόστους για επιχειρήσεις που προσπαθούν να βελτιώσουν την ασφάλεια της υποδομής τους.

3.8 Data Loss Prevention (DLP)

Η πρόληψη απώλειας δεδομένων αποτελεί τμήμα της στρατηγικής ασφαλείας ενός οργανισμού, και αποσκοπεί στον εντοπισμό και την πρόληψη της απώλειας, διαρροής ή κακής χρήσης των ευαίσθητων ή προσωπικών δεδομένων (PII) του οργανισμού, εξαιτίας παραβιάσεων ασφάλειας, κλοπής δεδομένων και μη εξουσιοδοτημένης χρήσης. Αποτελεί προϊόν συνδυασμού ανθρωπίνων πόρων, διαδικασιών και τεχνολογικών μέσων, όπως λογισμικά Antivirus, τεχνητή νοημοσύνη και Μηχανική μάθηση. Τα συστήματα DLP χρησιμοποιούνται από τους οργανισμούς τόσο για επαύξηση της ασφάλειας στο εσωτερικό τους δίκτυο, όσο και στα πλαίσια συμμόρφωσης με τη νομοθεσία και τους κανονισμούς, όπως ο Γενικός Κανονισμός Προστασίας Δεδομένων της ΕΕ (GDPR) και ο Νόμος Φορητότητας και Υπευθυνότητας Ασφάλισης Υγείας (HIPAA).



Εικόνα 21: Data Loss Prevention ΠΗΓΗ: ManageEngine[45]

Με την υιοθέτηση του DLP οι οργανισμοί αποκτούν τις εξής δυνατότητες[43]:

α. Προσδιορισμό ευαίσθητων πληροφοριών στο εσωτερικό δίκτυο και στο cloud.

β. Αποτροπή μη επιθυμητής/μη εγκεκριμένης κοινής χρήσης δεδομένων.

γ. Παρακολούθηση και προστασία δεδομένων.

δ. Συμμόρφωση των χρηστών στην ισχύουσα πολιτική ασφαλείας σχετικά με τα δεδομένα του οργανισμού.

3.8.1 Βέλτιστες πρακτικές εφαρμογής DLP

Η εφαρμογή μιας κεντρικής πολιτικής DLP σε έναν οργανισμό εάν γίνει βίαια και άναρχα, δύναται να διαταράξει την λειτουργία του οργανισμού και να τον θέσει προσωρινά εκτός επιχειρηματικών στόχων. Είναι απαραίτητο λοιπόν, να ακολουθηθούν οργανωμένες διαδικασίες ενσωμάτωσης, προκειμένου ο οργανισμός

να συνεχίσει να λειτουργεί επαυξάνοντας ταυτόχρονα, την ασφάλειά του σε θέματα δεδομένων. Συνήθεις βέλτιστες πρακτικές ενσωμάτωσης αποτελούν οι κάτωθι[44]:

α. Εφαρμογή ενός ολοκληρωμένου κεντρικού προγράμματος DLP: Πολλοί οργανισμοί χρησιμοποιούν ad hoc πρακτικές και τεχνολογίες DLP, οι οποίες εφαρμόζονται αυτόνομα από διάφορα τμήματα και μονάδες. Η έλλειψη κεντρικού ελέγχου και εφαρμογής οδηγεί σε ανεπαρκή ασφάλεια δεδομένων. Επιπλέον, οι εργαζόμενοι τείνουν να αγνοούν τα προγράμματα DLP τμημάτων που δεν υποστηρίζονται από τον υπόλοιπο οργανισμό.

β. Αξιολόγηση εσωτερικών πόρων: Για την υλοποίηση ενός προγράμματος DLP, οι οργανισμοί χρειάζονται εξειδικευμένο προσωπικό στον τομέα του DLP, συμπεριλαμβανομένων των ειδικών ανάλυσης κινδύνου DLP, απόκρισης και αναφοράς παραβίασης δεδομένων, γνώσης της νομοθεσίας περί προστασίας δεδομένων, εκπαίδευσης και ευαισθητοποίησης στο DLP. Ορισμένοι κυβερνητικοί κανονισμοί απαιτούν από τους οργανισμούς να απασχολούν εσωτερικό προσωπικό ή εξωτερικούς συμβούλους με γνώσεις προστασίας δεδομένων. Για παράδειγμα, ο GDPR περιλαμβάνει διατάξεις που επηρεάζουν οργανισμούς που πωλούν αγαθά ή υπηρεσίες σε καταναλωτές της ΕΕ ή παρακολουθούν τη συμπεριφορά τους.

γ. Διεξαγωγή απογραφής και αξιολόγησης: Η αξιολόγηση των τύπων δεδομένων και της αξίας τους για τον οργανισμό αποτελεί πρώιμο βήμα για την εφαρμογή ενός προγράμματος DLP. Αυτό περιλαμβάνει τον προσδιορισμό των σχετικών δεδομένων, της τοποθεσίας αποθήκευσής τους και της ευαισθησίας τους, όπως πνευματική ιδιοκτησία, εμπιστευτικές πληροφορίες ή δεδομένα που καλύπτονται από κανονισμούς. Ορισμένα προϊόντα DLP έχουν τη δυνατότητα να αναγνωρίζουν στοιχεία για τα δεδομένα αυτά, σαρώνοντας τα μεταδεδομένα αρχείων και καταγράφοντας τα αποτελέσματα. Στη συνέχεια, αξιολογείται ο κίνδυνος που σχετίζεται με κάθε τύπο δεδομένων, εάν διαρρεύσουν. Παράγοντες, όπως τα σημεία εξόδου δεδομένων και το πιθανό κόστος για τον οργανισμό σε περίπτωση απώλειας δεδομένων, λαμβάνονται υπόψη. Για παράδειγμα, η απώλεια πληροφοριών σχετικά με προγράμματα παροχής υπηρεσιών ενέχει διαφορετικό επίπεδο κινδύνου από την απώλεια ιατρικών αρχείων ασθενών ή αριθμών τραπεζικών λογαριασμών και κωδικών πρόσβασης.

δ. Εφαρμογή σε φάσεις: Το DLP αποτελεί μια μακροπρόθεσμη διαδικασία που εφαρμόζεται καλύτερα σταδιακά. Η πιο αποτελεσματική προσέγγιση είναι η ιεράρχιση των τύπων δεδομένων και των καναλιών επικοινωνίας. Επιπλέον, η εφαρμογή τμημάτων λογισμικού DLP όπου απαιτείται, πρέπει να γίνει σταδιακά βάσει των προτεραιοτήτων του οργανισμού και όχι ταυτόχρονα. Η ανάλυση κινδύνου και η απογραφή δεδομένων βοηθούν στον καθορισμό αυτών των προτεραιοτήτων.

ε. Δημιουργία συστήματος ταξινόμησης: Για τη δημιουργία και την εφαρμογή πολιτικών DLP, ένας οργανισμός χρειάζεται ένα πλαίσιο ταξινόμησης δεδομένων. Οι κατηγορίες ασφάλειας δεδομένων μπορεί να περιλαμβάνουν εμπιστευτικά, εσωτερικά, δημόσια, προσωπικής ταυτοποίησης (PII), οικονομικά και ρυθμιζόμενα δεδομένα, πνευματική ιδιοκτησία και άλλα. Τα προϊόντα DLP μπορούν να σαρώνουν δεδομένα χρησιμοποιώντας το σύστημα ταξινόμησης ώστε να εντοπίζουν και να προσδιορίζουν τα ευαίσθητα σύμφωνα με την ταξινόμηση δεδομένα.

στ. Παρακολούθηση και εφαρμογή πολιτικών: Οι πολιτικές DLP πρέπει να παρακολουθούνται και να εφαρμόζονται συνεχώς. Ορισμένα προϊόντα DLP

προσφέρουν δυνατότητες παρακολούθησης και αναφοράς σε πραγματικό χρόνο ώστε να παρέχουν ολοκληρωμένη ορατότητα στις δραστηριότητες που αφορούν τα δεδομένα. Η έννοια της παρακολούθησης περιλαμβάνει την παρακολούθηση του περιβάλλοντος αποθήκευσης δεδομένων, της κίνησης του δικτύου και των ενεργειών των χρηστών.

ζ. Ευαισθητοποίηση και εκπαίδευση: Η επιτυχής υλοποίηση του DLP απαιτεί ευαισθητοποίηση και εκπαίδευση των εργαζομένων. Οι χρήστες πρέπει να γνωρίζουν τις πολιτικές, τους κανόνες και τις συνέπειες που συνδέονται με τη διαχείριση ευαίσθητων δεδομένων. Αυτό επιτυγχάνεται μέσω της εκπαίδευσης των χρηστών για τους κινδύνους της διαρροής δεδομένων και τους τρόπους πρόληψής τους.

η. Αντιμετώπιση των παραβάσεων: Αφορά την οργάνωση ενός σχεδίου αντιμετώπισης παραβάσεων για τη γρήγορη και αποτελεσματική ανταπόκριση σε ενδεχόμενες παραβιάσεις. Αυτό περιλαμβάνει την απομόνωση της παραβίασης, την ανάλυση των αιτιών, την αποκατάσταση της ασφάλειας, και την αναφορά στις αρμόδιες αρχές.

θ. Συνεχής βελτίωση: Η ασφάλεια των δεδομένων είναι ένα δυναμικό πεδίο. Είναι απαραίτητη η συνεχής ενημέρωση των πολιτικών και των τεχνολογιών DLP για την αντιμετώπιση νέων απειλών και την εξασφάλιση της συμμόρφωσης με νέες νομοθεσίες.

Συνεπώς, η επιτυχημένη υλοποίηση ενός προγράμματος DLP απαιτεί προσέγγιση πολλαπλών επιπέδων που συνδυάζει τόσο την τεχνολογία όσο και τις διαδικασίες, ενισχύοντας την ασφάλεια των ευαίσθητων δεδομένων σε όλο το φάσμα της οργάνωσης.

3.8.2 DLP και Zero Trust

Οι αρχές Zero Trust συμπληρώνουν το DLP προσθέτοντας ένα επιπλέον επίπεδο ασφάλειας. Η εφαρμογή της αρχής Zero Trust σημαίνει ότι ακόμη και αν κάποιος έχει πρόσβαση σε ένα δίκτυο ή σε δεδομένα, ο ίδιος πρέπει να περνάει από συνεχείς ελέγχους για να αποδεικνύει την ταυτότητά του και τον λόγο της πρόσβασής του.

Το DLP, σε συνδυασμό με την αρχή Zero Trust, δίνει τη δυνατότητα για πιο εξελιγμένη προστασία. Ακόμη και εάν ένας κακόβουλος χρήστης καταφέρει να αποκτήσει πρόσβαση, τα DLP μέτρα μπορούν να προστατεύσουν τα ευαίσθητα δεδομένα από ανεπιθύμητη χρήση ή διαρροή. Συνεπώς, η συνδυασμένη χρήση του DLP και της αρχής Zero Trust αποτελεί έναν ισχυρό συνδυασμό για την εξασφάλιση της ασφάλειας των δεδομένων σε μια οργάνωση.

3.9 Identity and Access Management (IAM)

Η διαχείριση ταυτότητας και πρόσβασης (Identity and Access Management) αφορά μια σειρά από διαδικασίες, τεχνολογίες και πρακτικές που εφαρμόζονται σε αυτές, που αποσκοπούν στον έλεγχο και τη διαχείριση των δικαιωμάτων πρόσβασης των χρηστών και διαφόρων οντοτήτων, σε ένα πληροφοριακό σύστημα στο δίκτυο του

οργανισμού. Το IAM εξασφαλίζει αφενός ότι μόνο εξουσιοδοτημένοι χρήστες έχουν πρόσβαση σε πόρους, εφαρμογές και πληροφορίες του οργανισμού και αφετέρου ότι η πρόσβαση αυτή είναι η πλέον απαραίτητη για την εκτέλεση των καθηκόντων τους (Αρχή Ελάχιστης Γνώσης).

3.9.1 Λειτουργία του IAM

Η ασφαλής παροχή πρόσβασης σε πόρους μιας οργάνωσης περιλαμβάνει δύο βασικά στοιχεία, τη διαχείριση της ταυτότητας και τη διαχείριση της πρόσβασης.

Στη διαχείριση της ταυτότητας, οι προσπάθειες σύνδεσης επαληθεύονται έναντι μιας συνεχούς ενημερωμένης βάσης δεδομένων ταυτότητας, που περιλαμβάνει πληροφορίες για τα άτομα που έχουν δικαίωμα πρόσβασης. Αυτή η βάση πρέπει να ενημερώνεται συνεχώς καθώς εργαζόμενοι δύναται να ενταχθούν ή αποχωρήσουν από τον οργανισμό, να αλλάξουν ρόλους ή αρμοδιότητες, καθώς επίσης και να τροποποιηθεί το πεδίο που δραστηριοποιείται ο οργανισμός. Οι πληροφορίες που αποθηκεύονται στη βάση περιλαμβάνουν ονόματα υπαλλήλων, τίτλους εργασίας, αριθμούς κινητών τηλεφώνων και προσωπικές διευθύνσεις ηλεκτρονικού ταχυδρομείου. Η επαλήθευση, δηλαδή η αντιστοίχιση των πληροφοριών σύνδεσης, όπως το όνομα χρήστη και ο κωδικός με την ταυτότητά τους στη βάση δεδομένων, αποτελεί κρίσιμο στοιχείο της διαχείρισης της ταυτότητας.

Για επιπλέον ασφάλεια, πολλοί οργανισμοί απαιτούν από τους χρήστες να επαληθεύουν την ταυτότητά τους με πολυπαραγοντική επαλήθευση (MFA). Η MFA είναι πιο ασφαλής από τη χρήση μόνο ονόματος χρήστη και κωδικού πρόσβασης καθώς προσθέτει ένα επιπλέον βήμα στη διαδικασία σύνδεσης, όπου ο χρήστης πρέπει να επαληθεύσει την ταυτότητά του με ένα εναλλακτικό μέσο επαλήθευσης.

Η διαχείριση της πρόσβασης αποτελεί το δεύτερο στοιχείο του IAM. Αφού το σύστημα IAM έχει επαληθεύσει ότι το πρόσωπο ή το αντικείμενο που επιχειρεί να έχει πρόσβαση αντιστοιχεί στην ταυτότητά του, η διαχείριση της πρόσβασης παρακολουθεί τους πόρους στους οποίους το πρόσωπο ή το αντικείμενο έχει άδεια πρόσβασης. Οι περισσότεροι οργανισμοί παρέχουν διάφορα επίπεδα πρόσβασης σε πόρους και δεδομένα, τα οποία καθορίζονται από παράγοντες όπως ο τίτλος εργασίας, ο χρόνος υπηρεσίας, το επίπεδο ασφάλειας και το έργο. Η χορήγηση του σωστού επιπέδου πρόσβασης μετά την επαλήθευση της ταυτότητας του χρήστη ονομάζεται εξουσιοδότηση. Τα συστήματα IAM έχουν ως στόχο να διασφαλίσουν ότι η επαλήθευση και η εξουσιοδότηση λαμβάνουν χώρα σωστά και με ασφάλεια σε κάθε προσπάθεια πρόσβασης.

3.9.2 Πλεονεκτήματα του IAM

Οι τεχνολογίες IAM μπορούν να χρησιμοποιηθούν για την καταγραφή και τη διαχείριση ταυτοτήτων χρηστών και των σχετικών δικαιωμάτων πρόσβασής τους, αυτοματοποιημένα. Ένας οργανισμός αποκομίζει τα εξής οφέλη από το IAM:

α. Τα προνόμια πρόσβασης χορηγούνται σύμφωνα με πολιτικές, εξασφαλίζοντας την κατάλληλη πιστοποίηση, εξουσιοδότηση και έλεγχο όλων των ατόμων και υπηρεσιών. Η αποτελεσματική διαχείριση ταυτοτήτων ενισχύει τον έλεγχο

της πρόσβασης των χρηστών, μειώνοντας έτσι τον κίνδυνο εσωτερικών και εξωτερικών διαρροών δεδομένων.

β. Η αυτοματοποίηση των συστημάτων IAM συντελεί στην αύξηση της λειτουργικότητας, μειώνοντας την προσπάθεια, τον χρόνο και τα έξοδα που θα απαιτούνταν διαφορετικά, για τη χειροκίνητη διαχείριση της πρόσβασης στα δίκτυα ενός οργανισμού.

γ. Από την άποψη της ασφάλειας, το IAM ευνοεί την επιβολή πολιτικών που αφορούν την πιστοποίηση, την επικύρωση και τα προνόμια των χρηστών, αντιμετωπίζοντας προβλήματα όπως η ανεξέλεγκτη αύξηση προνομίων.

δ. Τα συστήματα IAM συμβάλλουν στη συμμόρφωση των επιχειρήσεων με τους κανονισμούς της κυβέρνησης, επιτρέποντάς τους να δείξουν ότι οι εταιρικές πληροφορίες δεν καταχράζονται. Οι εταιρείες μπορούν επίσης, να επιδείξουν ότι οποιαδήποτε δεδομένα που απαιτούνται για επιθεώρηση είναι διαθέσιμα, κατόπιν αιτήματος.

ε. Οι εταιρείες μπορούν να κερδίσουν ανταγωνιστικά πλεονεκτήματα με την εφαρμογή εργαλείων IAM και την εφαρμογή σχετικών βέλτιστων πρακτικών. Για παράδειγμα, οι τεχνολογίες IAM επιτρέπουν στην επιχείρηση να παραχωρήσει σε χρήστες εκτός του οργανισμού - όπως πελάτες, συνεργάτες, εργολάβοι και προμηθευτές - πρόσβαση στο δίκτυό της μέσω κινητών εφαρμογών, εφαρμογών εγκατεστημένων στις εταιρικές εγκαταστάσεις και υπηρεσιών SaaS, χωρίς να θέτουν σε κίνδυνο την ασφάλεια. Αυτό ενισχύει τη συνεργασία, την αποτελεσματικότητα, την αποδοτικότητα και μειώνει τα λειτουργικά κόστη.

3.9.3 Δυνατότητες του IAM

Οι τεχνολογίες IAM στοχεύουν στον επαναπροσδιορισμό των διαδικασιών παροχής χρηστών και εγκατάστασης λογαριασμών. Αυτά τα συστήματα σχεδιάζονται για την επιτάχυνση των διαδικασιών μέσω μιας ελεγχόμενης ροής εργασίας, μείωσης σφαλμάτων και πιθανής κατάχρησης, ενώ επιτρέπουν την αυτοματοποιημένη ολοκλήρωση λογαριασμών χρηστών.

Αυτά τα συστήματα στοχεύουν στο να επιτυγχάνουν ισορροπία μεταξύ της ταχύτητας και της αυτοματοποίησης των διαδικασιών και του ελέγχου που απαιτείται για την παρακολούθηση και την τροποποίηση των δικαιωμάτων πρόσβασης. Για να διαχειριστεί τα αιτήματα πρόσβασης, πρέπει να περιλαμβάνεται ένα σύστημα δικαιωμάτων πρόσβασης που αντιστοιχεί αυτόματα τους τίτλους εργασίας των υπαλλήλων, τα αναγνωριστικά τμημάτων επιχείρησης και τις τοποθεσίες τους, στα σχετικά επίπεδα προνομίων. Ροές εργασίας, με βάση τα δικαιώματα, χρησιμοποιούνται για να πραγματοποιηθεί έλεγχος των ατομικών αιτημάτων για παροχή δικαιωμάτων. Αυτό απλοποιεί την δημιουργία κατάλληλων διαδικασιών ελέγχου για εκχώρηση πρόσβασης υψηλότερου επιπέδου και διευκολύνει τις επανεξετάσεις υπαρκτών δικαιωμάτων για την πρόληψη του φαινομένου "privilege creep", δηλαδή της σταδιακής αύξησης των δικαιωμάτων πρόσβασης πέρα από αυτά που χρειάζονται οι χρήστες για τις εργασίες τους.

Τα συστήματα IAM θα πρέπει να χρησιμοποιούνται για να παρέχουν ευελιξία στην καθιέρωση ομάδων με συγκεκριμένα προνόμια για συγκεκριμένους ρόλους,

ώστε τα δικαιώματα πρόσβασης με βάση τις λειτουργίες των υπαλλήλων να μπορούν να κατανέμονται ομοιόμορφα. Επιπλέον, το σύστημα θα πρέπει να διευκολύνει διαδικασίες αιτήσεων και έγκρισης για τροποποιήσεις προνομίων, διότι χρήστες με τον ίδιο τίτλο και την ίδια τοποθεσία εργασίας μπορεί να χρειάζονται προσαρμοσμένη ή ελαφρώς διαφορετική πρόσβαση.

3.9.4 Τύποι ψηφιακής πιστοποίησης

Μέσα από το IAM, οι επιχειρήσεις μπορούν να υιοθετήσουν διάφορες μεθόδους ψηφιακής πιστοποίησης για να επιβεβαιώσουν την ψηφιακή ταυτότητα και να εξουσιοδοτήσουν την πρόσβαση σε εταιρικούς πόρους όπως παρακάτω:

α. Μοναδικοί Κωδικοί Πρόσβασης: Η πιο κοινή μορφή ψηφιακής πιστοποίησης ενεργοποιείται μέσω μοναδικών κωδικών πρόσβασης. Ορισμένες φορές, οργανισμοί απαιτούν μακρύτερους ή πιο περίπλοκους κωδικούς που απαιτούν συνδυασμό γραμμάτων, συμβόλων και αριθμών για να ενισχύσουν την ασφάλεια.

β. Προκαθορισμένο Κλειδί (PSK): Το PSK είναι μια άλλη μορφή ψηφιακής πιστοποίησης όπου ο κωδικός πρόσβασης κοινοποιείται ανάμεσα σε χρήστες που έχουν εξουσιοδοτηθεί για πρόσβαση στους ίδιους πόρους. Ωστόσο, αυτή η μορφή πιστοποίησης είναι λιγότερο ασφαλής από τους ατομικούς κωδικούς πρόσβασης.

γ. Συμπεριφορική Πιστοποίηση: Για εξαιρετικά ευαίσθητες πληροφορίες, οι οργανισμοί μπορούν να χρησιμοποιούν συμπεριφορική πιστοποίηση, αναλύοντας τη δυναμική των πλήκτρων ή τα χαρακτηριστικά χρήσης του ποντικιού. Η τεχνητή νοημοσύνη μπορεί να αναγνωρίσει γρήγορα ανωμαλίες στη συμπεριφορά του χρήστη ή της μηχανής και να ασφαλίσει αυτόματα τα συστήματα.

δ. Βιομετρικά: Τα σύγχρονα συστήματα IAM αξιοποιούν τη βιομετρία για ακριβή πιστοποίηση, συμπεριλαμβανομένων δαχτυλικών αποτυπωμάτων, ιρίδων, προσώπων, παλαμών, βημάτων, φωνών, σχήματος αυτιού και σε ορισμένες περιπτώσεις, DNA. Η βιομετρία και η ανάλυση βάσει συμπεριφοράς συχνά είναι πιο αποτελεσματικές από τους παραδοσιακούς κωδικούς πρόσβασης.

Παρόλο που η βιομετρία προσφέρει ενισχυμένη ασφάλεια, πρέπει να λαμβάνονται υπόψη ηθικά θέματα σχετικά με την ασφάλεια δεδομένων, τη διαφάνεια και το απόρρητο των βιομετρικών δεδομένων. Προκλήσεις περιλαμβάνουν τον κίνδυνο διαρροής δεδομένων και το κόστος εφαρμογής, συμπεριλαμβανομένων των εξόδων λογισμικού, υλικού και εκπαίδευσης. Είναι ζωτικής σημασίας να ζυγιστούν προσεκτικά τα πλεονεκτήματα και τα μειονεκτήματα πριν από την πλήρη υιοθέτηση της αυθεντικοποίησης IAM χωρίς κωδικούς, με τη χρήση βιομετρικών στοιχείων.

3.9.5 Σχέση IAM και Zero Trust Architecture

Η σχέση μεταξύ της Διαχείρισης Ταυτότητας και Πρόσβασης (IAM) και της Αρχιτεκτονικής Zero Trust είναι στενή και συμπληρωματική, με τους δύο όρους να αποτελούν κρίσιμα στοιχεία για την ενίσχυση της κυβερνοασφάλειας σε επιχειρηματικό επίπεδο.

α. Εξασφάλιση Ταυτότητας (Identity Assurance): Το IAM είναι υπεύθυνο για τον έλεγχο και τη διασφάλιση της ταυτότητας. Σε μια αρχιτεκτονική Zero Trust, αυτό είναι ζωτικής σημασίας για τη συνεχή επαλήθευση των χρηστών και των συσκευών.

β. Διαχείριση Πρόσβασης (Access Management): Το IAM ρυθμίζει τα δικαιώματα πρόσβασης. Σε ένα πλαίσιο Zero Trust, η πρόσβαση πρέπει να επαληθεύεται συνεχώς, ακόμα και μετά την αρχική αυθεντικοποίηση.

γ. Συνεργασία για Ενισχυμένη Ασφάλεια: Η συνδυασμένη χρήση IAM και Zero Trust αυξάνει την ασφάλεια, αποτρέποντας την ανεξουσιοδοτημένη πρόσβαση και παρέχοντας συνεχή προστασία.

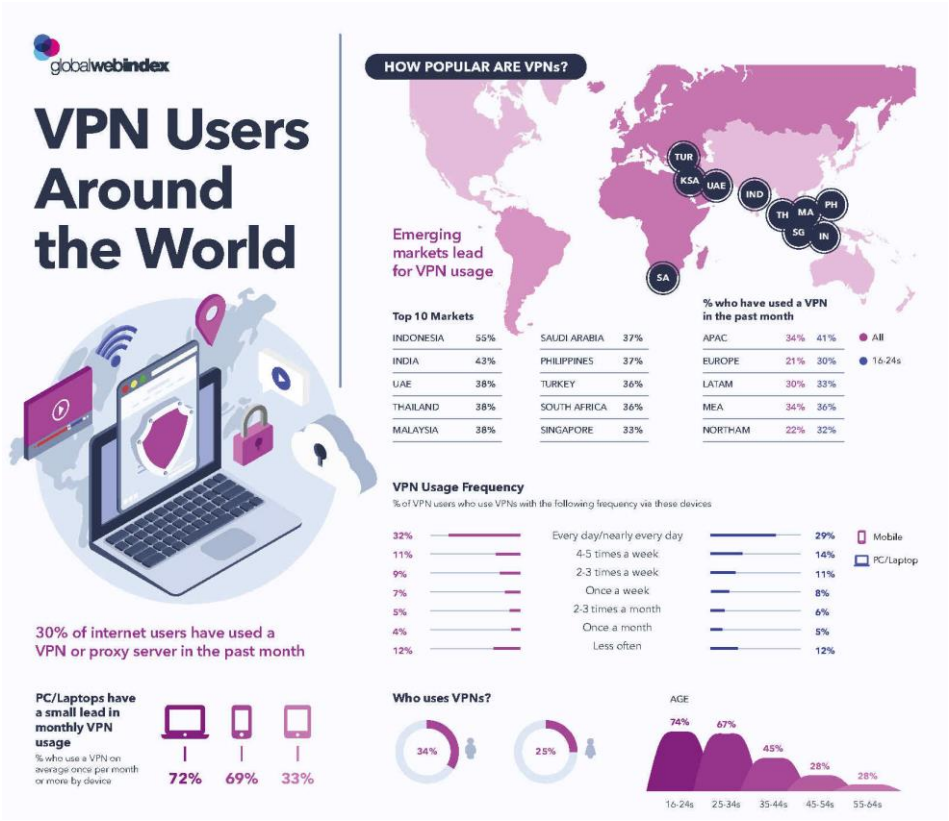
Σε γενικές γραμμές, το IAM λειτουργεί ως εργαλείο εφαρμογής πολιτικών ασφαλείας και προστασίας ταυτότητας, υλοποιώντας την φιλοσοφία της αρχιτεκτονικής Zero Trust ότι καμία πρόσβαση δεν πρέπει να θεωρείται έμπιστη, ανεξαρτήτως της τοποθεσίας ή του χρόνου.

3.10 Virtual Private Networks (VPN)

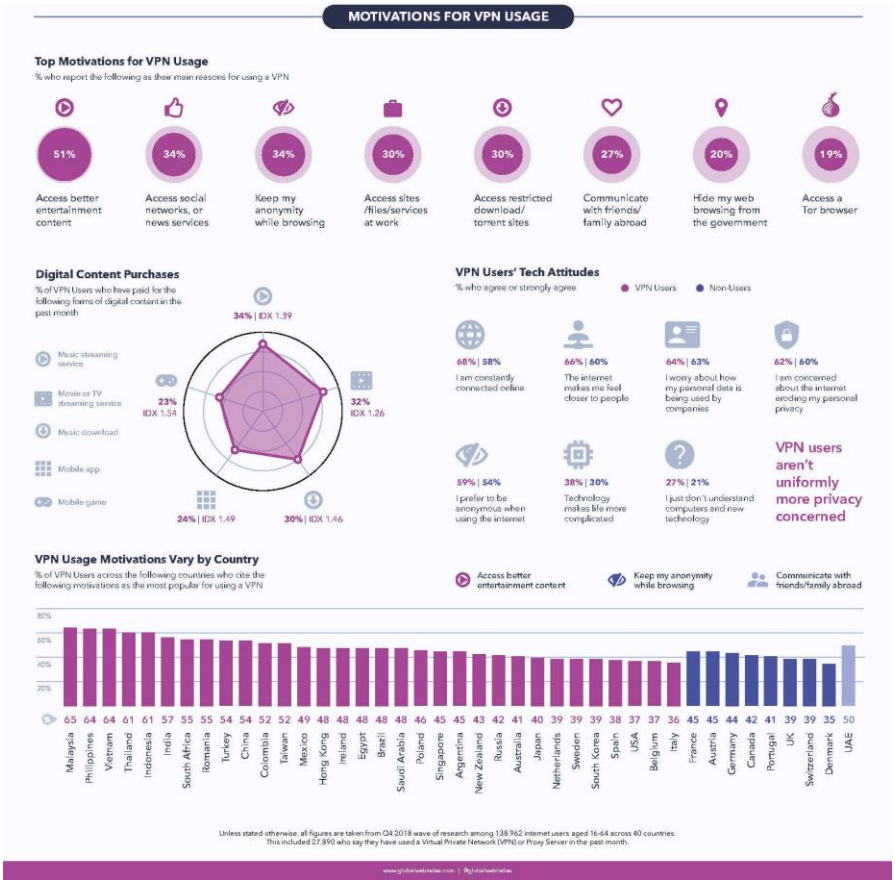
Ο όρος VPN σημαίνει «Ιδιωτικό Εικονικό Δίκτυο» και αφορά στη δυνατότητα δημιουργίας μιας ιδιωτικής κρυπτογραφημένης σύνδεσης στο διαδίκτυο. Η ιδιωτική αυτή σύνδεση δίνει τη δυνατότητα απόκρυψης της ηλεκτρονικής ταυτότητας του χρήστη, γεγονός που καθιστά δύσκολο για τρίτους ενδιαφερόμενους να παρακολουθούν τη δραστηριότητα του χρήστη στο διαδίκτυο και να υποκλέπτουν τα δεδομένα του. Τα πλεονεκτήματα αυτά, έχουν οδηγήσει τους οργανισμούς στην κατά κόρον υιοθέτηση της συγκεκριμένης τεχνολογίας με σκοπό την παροχή δυνατότητας απομακρυσμένης εργασίας στους εργαζόμενούς τους.

Η τεχνολογία VPN άρχισε να υιοθετείται μαζικά στις αρχές της δεκαετίας του 2010, ωστόσο οι πρώτες προσπάθειες ανάπτυξης της τεχνολογίας αυτής ξεκίνησαν το 1993, όπου μια ερευνητική ομάδα του πανεπιστημίου της Columbia σε συνεργασία με την AT&T Bell Labs, πέτυχε την δημιουργία μιας πρώτης εκδοχής του VPN γνωστό ως swipe (Software IP encryption protocol). Επόμενο ορόσημο αποτελεί η ανάπτυξη του πρώτου δικτύου IPsec από τον Wei Xu το έτος 1994, ενώ το έτος 1996 η Gurdeep Singh-Pall δημιούργησε το πρωτόκολλο Peer-to-Peer Tunelling (PPTP), πάνω στο οποίο βασίζεται η τεχνολογία VPN.

Οι πρώτες ολοκληρωμένες λύσεις VPN ξεκίνησαν να υιοθετούνται σε εταιρικό επίπεδο στις αρχές του 2000, προκειμένου να καλύψουν την απαίτηση των εταιριών σε κρυπτογραφημένη πλοήγηση στο διαδίκτυο, ενώ το 2010 η καταναλωτική αγορά για VPN άρχισε να αυξάνεται συμπεριλαμβάνοντας και ιδιώτες. Με βάση την έρευνα της GlobalWebIndex[46] την διετία 2016-2018 η χρήση της τεχνολογίας VPN τετραπλασιάστηκε σε χώρες της Ασίας όπου επιβάλλεται λογοκρισία, ενώ σύμφωνα με την Security.org[47] κατά την περίοδο της πανδημίας Covid-19 η αύξηση στο δυτικό κόσμο ανήλθε σε ποσοστά 124% γεγονός που δικαιολογείται, λόγω της αυξημένης ανάγκης για απομακρυσμένη εργασία.



Εικόνα 22: Έρευνα χρήσης VPN ΠΗΓΗ: GlobalWebIndex[46]



Εικόνα 23: Κίνητρα χρήσης VPN ΠΗΓΗ: GlobalWebIndex[46]

3.10.1 Λειτουργία του VPN

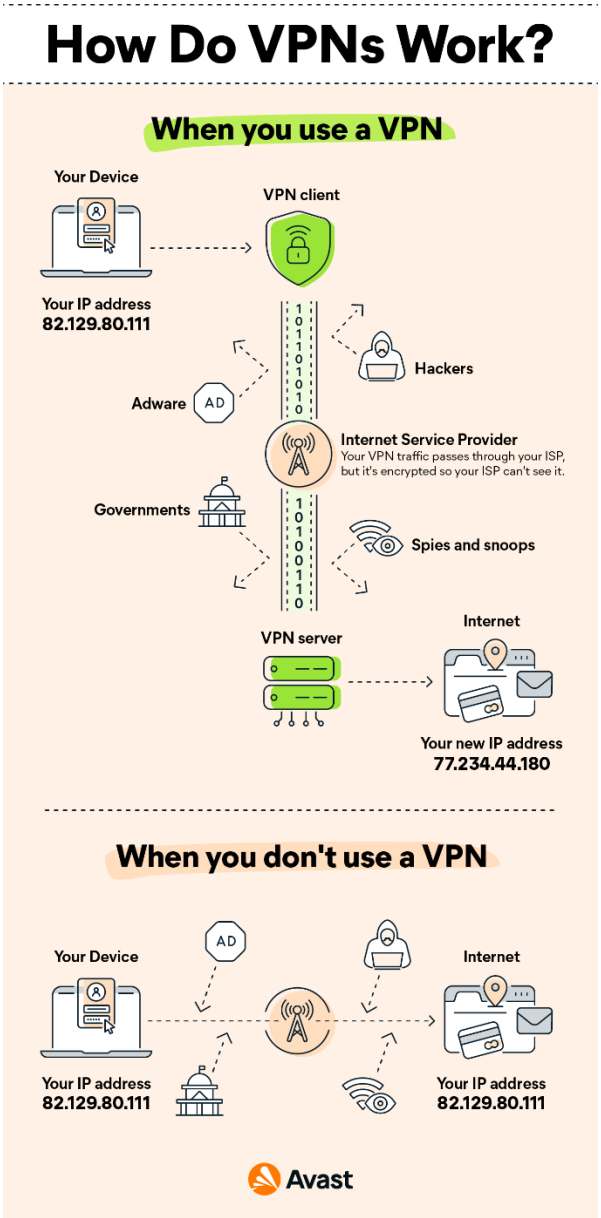
Σε βασικό επίπεδο, το VPN δημιουργεί μια σύνδεση σημείου προς σημείο (Point-to-Point), που δεν μπορεί να προσπελαστεί από μη εξουσιοδοτημένους χρήστες. Για τη δημιουργία του τούνελ, χρησιμοποιείται ένα πρωτόκολλο VPN tunneling πάνω σε ήδη υφιστάμενα δίκτυα. Οι πάροχοι VPN χρησιμοποιούν διάφορα πρωτόκολλα tunneling, όπως το OpenVPN ή το Secure Socket Tunneling Protocol (SSTP). Το πρωτόκολλο tunneling που χρησιμοποιείται εξαρτάται από την πλατφόρμα στην οποία χρησιμοποιείται το VPN, όπως το SSTP που χρησιμοποιείται στο λειτουργικό σύστημα Windows και παρέχει κρυπτογράφηση δεδομένων σε διάφορες δυναμικότητες. Για την εγκαθίδρυση σύνδεσης VPN απαιτείται ο χρήστης να διαθέτει έναν VPN Client εγκατεστημένο στη συσκευή του και ο οποίος θα εκτελείται στο παρασκήνιο χωρίς να γίνεται αντιληπτός από το χρήστη.

Χρησιμοποιώντας τον VPN Client ο οποίος αξιοποιεί ένα πρωτόκολλο VPN Tunneling, η συσκευή ενός χρήστη θα συνεχίσει να συνδέεται στον ISP ωστόσο τα δεδομένα που θα στέλνονται θα είναι κρυπτογραφημένα. Στη συνέχεια ο ISP θα ανακατευθύνει τα δεδομένα στον VPN server που βρίσκεται σε μια απομακρυσμένη τοποθεσία και έχει άλλη διεύθυνση IP, όπου εκεί θα γίνεται η αποκρυπτογράφησή τους και στη συνέχεια θα συνεχίζουν στο διαδίκτυο. Με τον τρόπο αυτό αποκρύπτονται οι προσωπικές πληροφορίες από επιτιθέμενους ή άλλους ενδιαφερόμενους που αποσκοπούν στο να αποκτήσουν πρόσβαση στις δραστηριότητες του χρήστη. Αυτό επιτυγχάνεται διότι τα VPN συσχετίζουν το ιστορικό αναζήτησης ενός χρήστη με τη διεύθυνση IP του διακομιστή VPN. Οι υπηρεσίες VPN έχουν διακομιστές που βρίσκονται σε διάφορες γεωγραφικές περιοχές, έτσι ώστε να φαίνεται ότι ο χρήστης θα μπορούσε να είναι από οποιαδήποτε από αυτές τις τοποθεσίες.

Ορισμένα προϊόντα VPN διαθέτουν ένα επιπρόσθετο χαρακτηριστικό ασφαλείας που ονομάζεται "kill switch". Εάν η σύνδεση VPN διακοπεί, το "kill switch" θα αποσυνδέσει αυτόματα τη συσκευή από το διαδίκτυο για να εξαλείψει τον κίνδυνο αποκάλυψης της διεύθυνσης IP. Υπάρχουν δύο τύποι "kill switches"[49]:

α. Ενεργά πρωτόκολλα "kill switch": Αποτρέπουν τις συσκευές από το να συνδέονται σε ανασφαλή δίκτυα όταν η συσκευή είναι συνδεδεμένη στο VPN. Σταματούν τη λειτουργία τους σε περιπτώσεις που ο VPN server δεν λειτουργεί ή ο χρήστης απενεργοποιήσει τη σύνδεση VPN.

β. Παθητικά πρωτόκολλα "kill switch": Είναι πιο ασφαλή, καθόσον αποτρέπουν τη συσκευή από το να συνδέεται σε μη VPN συνδέσεις ακόμη και όταν είναι αποσυνδεδεμένη από τον διακομιστή VPN.



Εικόνα 24: Λειτουργία του VPN ΠΗΓΗ: AVAST[50]

3.10.2 Είδη VPN

Οι διαχειριστές δικτύου έχουν πολλές επιλογές όσον αφορά την εφαρμογή ενός VPN, περιλαμβάνοντας τις ακόλουθες επιλογές[48][49]:

α. Απομακρυσμένη Πρόσβαση VPN (Remote Access VPN): Οι απομακρυσμένοι χρήστες συνδέονται σε ένα διακομιστή πύλης VPN στο δίκτυο του οργανισμού. Ο διακομιστής απαιτεί από τη συσκευή να επαληθεύσει την ταυτότητά της προτού χορηγήσει πρόσβαση στους εσωτερικούς πόρους του δικτύου. Αυτός ο τύπος συνήθως βασίζεται είτε σε IPsec είτε σε SSL για την ασφάλεια της σύνδεσης.

β. Δίκτυο προς Δίκτυο VPN (Site-to-Site VPN): Ένα VPN δικτύου προς δίκτυο χρησιμοποιεί μια συσκευή πύλης για να συνδέσει ένα ολόκληρο δίκτυο σε μια τοποθεσία, με ένα άλλο σε μια διαφορετική τοποθεσία. Οι συσκευές στην

απομακρυσμένη τοποθεσία δεν χρειάζονται VPN clients καθώς η πύλη χειρίζεται τη σύνδεση. Τα περισσότερα VPN δικτύου προς δίκτυο που συνδέονται μέσω διαδικτύου χρησιμοποιούν IPsec. Συνήθως, χρησιμοποιούν συνδέσεις φορέα MPLS (Multiprotocol Label Switching) αντί για το δημόσιο διαδίκτυο ως μεταφορικό μέσο για τα VPN δικτύου προς δίκτυο. Είναι δυνατή η εγκαθίδρυση σύνδεσης στο Επίπεδο 3 (MPLS IP VPN) ή στο Επίπεδο 2 (Virtual Private Local Area Network Service).

γ. Φορητό VPN (Mobile VPN): Σε ένα φορητό VPN, ο διακομιστής παραμένει στο άκρο του δικτύου του οργανισμού, παρέχοντας δυνατότητα ασφαλούς πρόσβασης σε εξουσιοδοτημένους πελάτες. Τα VPN tunnels του κινητού δεν συνδέονται με φυσικές διευθύνσεις IP. Αντίθετα, κάθε tunnel συσχετίζεται με μια λογική διεύθυνση IP που διατηρείται για την κινητή συσκευή.

δ. Συσκευές VPN (Hardware VPN): Οι συσκευές VPN προσφέρουν σημαντικά πλεονεκτήματα έναντι των VPN βασισμένων σε λογισμικό. Πέρα από την παροχή ενισχυμένης ασφάλειας, οι συσκευές VPN μπορούν να παρέχουν εξισορρόπηση στη δικτυακή κίνηση σε VPN clients που ζητούν μεγάλο bandwidth. Ωστόσο, μια συσκευή VPN είναι πιο ακριβή από ένα αντίστοιχο, βασισμένο σε λογισμικό, για τον λόγο αυτό συνήθως οι λύσεις VPN με χρήση ξεχωριστών συσκευών υιοθετείται από μεγάλους οργανισμούς που μπορούν να διαθέσουν τους οικονομικούς πόρους για την απόκτησή τους. Ενδιάμεση λύση αποτελούν οι δρομολογητές με δυνατότητα VPN.

ε. Δυναμικό Πολλαπλών Σημείων Εικονικό Ιδιωτικό Δίκτυο (Dynamic Multipoint Virtual Private Network - DMVPN): Ένα DMVPN ανταλλάσσει δεδομένα μεταξύ των τοποθεσιών χωρίς την ανάγκη να περνά από τον διακομιστή VPN ή τον κεντρικό δρομολογητή του οργανισμού. Ένα DMVPN δημιουργεί ένα υπηρεσιακό δίκτυο VPN που λειτουργεί σε δρομολογητές VPN και Firewall. Κάθε απομακρυσμένη τοποθεσία έχει έναν δρομολογητή που έχει ρυθμιστεί για να συνδεθεί με τον κεντρικό δρομολογητή του οργανισμού.

3.10.3 Σχέση VPN και Zero Trust Architecture

Η χρήση VPN σε συνδυασμό με την αρχιτεκτονική Zero Trust συμβάλλει στην ενίσχυση της ασφάλειας, προστατεύοντας τις εταιρικές πληροφορίες και εξασφαλίζοντας ότι η πρόσβαση είναι πάντα ελεγχόμενη και επαληθευμένη. Η αξιοποίηση της τεχνολογίας VPN συμβάλλει στην αρχή του ελάχιστου προνομίου, καθόσον κάθε χρήστης ο οποίος συνδέεται στο δίκτυο του οργανισμού έχει προκαθορισμένα δικαιώματα πρόσβασης στους πόρους που απαιτούνται για να εκτελέσει την εργασία του. Επίσης, βάση της τεχνολογίας VPN η σύνδεση είναι κρυπτογραφημένη, γεγονός που εμποδίζει την διαρροή δεδομένων μέσω υποκλοπής της σύνδεσης.

Ωστόσο η τεχνολογία VPN από μόνη της δεν εξασφαλίζει το Zero Trust. Σε περίπτωση που ο επιτιθέμενος καταφέρει να αποκτήσει πρόσβαση στην σύνδεση VPN τότε αυτομάτως αποκτάει πρόσβαση και στους πόρους του οργανισμού. Είναι, λοιπόν, απαραίτητο να συνδυάζεται η τεχνολογία VPN με τις υπόλοιπες αρχές του Zero Trust, έτσι ώστε σε περίπτωση παραβίασης της σύνδεσης, ο επιτιθέμενος να πρέπει να υπόκειται σε διαρκή αυθεντικοποίηση και παράλληλα να είναι περιορισμένος στην επιφάνεια προστασίας που έχει συνδεθεί, χωρίς να έχει τη δυνατότητα να μεταπηδήσει σε άλλες.

3.11 Network Access Control (NAC)

Ο έλεγχος πρόσβασης στο δίκτυο αποτελεί ένα μέσο ενίσχυσης της ασφάλειας, της ορατότητας και της διαχείρισης της πρόσβασης στο ιδιωτικό δίκτυο ενός οργανισμού. Η μέθοδος αυτή, γνωστή και ως έλεγχος αποδοχής δικτύου, αποσκοπεί στον έλεγχο της διαθεσιμότητας των πόρων του δικτύου στους χρήστες, βασιζόμενη σε συγκεκριμένη πολιτική ασφαλείας που έχει καθορίσει ο οργανισμός. Η τεχνολογία NAC περιλαμβάνει πληθώρα εργαλείων όπως Antivirus, Firewall και μεθόδους αυθεντικοποίησης.

Ο έλεγχος πρόσβασης στο δίκτυο περιλαμβάνει δυο προσεγγίσεις[51]:

α. Προσέγγιση Pre-admission, όπου αξιολογείται η προσπάθεια πρόσβασης στο δίκτυο και επιτρέπει την πρόσβαση μόνο σε εξουσιοδοτημένους χρήστες και συσκευές.

β. Προσέγγιση Post-admission, όπου οι χρήστες καλούνται σε αυθεντικοποίηση κάθε φορά που προσπαθούν να εισέλθουν σε διαφορετικό τμήμα του δικτύου. Με τον τρόπο αυτό περιορίζεται η οριζόντια μετακίνηση των χρηστών και η ζημιά από κυβερνοεπιθέσεις (Blast Radius).

3.11.1 Περιπτώσεις εφαρμογής NAC

Τα εργαλεία NAC δρουν προληπτικά και είναι σχεδιασμένα για να αποτρέπουν την μη εξουσιοδοτημένη πρόσβαση πριν συμβεί. Προστατεύουν το δίκτυο ενός οργανισμού, συμπεριλαμβανομένης της φυσικής υποδομής, των συσκευών, του λογισμικού, των εφαρμογών και των περιουσιακών στοιχείων που βρίσκονται στο cloud.

Οι συνήθεις περιπτώσεις χρήσης του NAC από έναν οργανισμό είναι[51]:

α. Φέρε τη Δική Σου Συσκευή (BYOD): Προστατεύει από τις ευπάθειες που δημιουργούνται όταν οι εργαζόμενοι χρησιμοποιούν τις προσωπικές τους συσκευές ή όταν χρησιμοποιούν συσκευές της εταιρείας από απομακρυσμένες τοποθεσίες.

β. Παροχή πρόσβασης στο δίκτυο σε τρίτους (Προμηθευτές ή Συνεργάτες): Το NAC, σε συνδυασμό με VPN, επιτρέπει σε εξωτερικούς συνεργάτες να έχουν ασφαλή πρόσβαση στο εταιρικό δίκτυο ή σε συγκεκριμένα τμήματά του, μέσω μιας ασφαλούς πύλης αυτοεξυπηρέτησης.

γ. Διαδίκτυο των Πραγμάτων (IoT): Το NAC αποτρέπει τις κυβερνοαπειλές, εξασφαλίζοντας προληπτικά τις συσκευές IoT που συνδέονται στο εταιρικό δίκτυο, μια περιοχή που συχνά παραμελείται όσον αφορά την ασφάλεια και την παρακολούθηση.

δ. Έλεγχος συσκευών: Τα εργαλεία NAC αναγνωρίζουν τις μη ενημερωμένες συσκευές και απενεργοποιούν αυτόματα την πρόσβαση προκειμένου να αποτρέψουν την εξάπλωση μιας επίθεσης στο δίκτυο, χωρίς να διακόψουν την υπόλοιπη λειτουργία του δικτύου (Business As Usual, BAU)[52]. Σε ορισμένες περιπτώσεις συνδέουν την συσκευή σε ξεχωριστό δίκτυο έως ότου λάβει όλες τις απαραίτητες ενημερώσεις ασφαλείας και στη συνέχεια την συνδέουν στο τμήμα του δικτύου που πρέπει να έχει πρόσβαση σύμφωνα με την καθορισμένη πολιτική ασφαλείας.

3.11.2 Σχέση NAC και Zero Trust Architecture

Αξιοποιώντας την τεχνολογία NAC σε ένα δίκτυο Zero Trust επιτυγχάνεται αφενός ο έλεγχος ταυτότητας, κάτι που αποτελεί βασική αρχή του Zero Trust και αφετέρου επιτυγχάνεται ο έλεγχος προσπέλασης των χρηστών στους πόρους του οργανισμού, ανεξάρτητα από τη συσκευή που χρησιμοποιούν και την τοποθεσία που βρίσκονται. Επίσης, μέσω του NAC προσεγγίζεται η ασφάλεια των IoT συσκευών, καθόσον θεωρείται κρίσιμη επιφάνεια προστασίας δεδομένου ότι είναι επιρρεπής σε κυβερνοεπιθέσεις.

3.12 User and Entity Behavior Analytics (UEBA)

Το UEBA είναι λογισμικό το παρακολουθεί ενεργά τις δραστηριότητες των χρηστών και των οντοτήτων εντός ενός οργανισμού. Αξιολογεί αυτά τα δεδομένα για να καθορίσει εάν συγκεκριμένες ενέργειες ή συμπεριφορές θα μπορούσαν να αποτελέσουν δυνητική κυβερνοαπειλή. Το UEBA βασίζεται στην ικανότητα να διακρίνει μεταξύ φυσιολογικής και ύποπτης συμπεριφοράς, έτσι ακόμα κι αν ένας επιτιθέμενος καταφέρει να αποκτήσει τα διαπιστευτήρια ενός χρήστη για να συνδεθεί, συνήθως δυσκολεύεται να αντιγράψει τις 'φυσιολογικές' ενέργειες μέσα στο σύστημα, καθιστώντας τις ανωμαλίες συμπεριφοράς αντιληπτές από το UEBA.

Το UEBA μπορεί να αντλήσει και να επεξεργαστεί δεδομένα από διάφορες αποθηκευτικές βάσεις, συμπεριλαμβανομένων γενικών πηγών δεδομένων όπως data lakes ή data warehouses, καθώς επίσης και να ενσωματωθεί με συστήματα SIEM (Διαχείριση Πληροφοριών και Συμβάντων Ασφαλείας) που συγκεντρώνουν δεδομένα από διάφορες πηγές. Αυτή η ενσωμάτωση είναι ζωτικής σημασίας, καθώς το UEBA συνήθως βασίζεται σε δεδομένα ασφαλείας που συλλέγονται και αποθηκεύονται από συστήματα SIEM.

3.12.1 Λειτουργία του UEBA

Η λειτουργία του UEBA βασίζεται στην ικανότητά του να παρακολουθεί τη συμπεριφορά των χρηστών και των συσκευών στο δίκτυο. Με τη διαρκή παρακολούθηση σχηματίζει σταδιακά ένα μοτίβο φυσιολογικής συμπεριφοράς και δραστηριότητας για κάθε οντότητα, αξιοποιώντας τεχνολογία μηχανικής μάθησης, στατιστικά μοντέλα, και γνωστές υπογραφές malware. Το μοτίβο που σχηματίζει περιλαμβάνει στοιχεία, όπως πόσες φορές μπορεί να εισάγει ένας χρήστης λανθασμένο κωδικό πρόσβασης, πόσο γρήγορα πληκτρολογεί και πόσο bandwidth χρησιμοποιεί. Τα δεδομένα που χρησιμοποιεί το UEBA συνήθως βρίσκονται σε Data Lakes ή συνεργάζεται με ένα σύστημα SIEM. Συνεπώς, όταν ανιχνεύσει παρέκκλιση από αυτό το μοτίβο συμπεριφοράς εγείρει συναγερμό ασφαλείας προς τους διαχειριστές για περαιτέρω ανάλυση του περιστατικού.

3.12.2 Πλεονεκτήματα του UEBA

Η ολοένα αυξανόμενη ενσωμάτωση προϊόντων UEBA οφείλεται στο γεγονός ότι πλέον τα παραδοσιακά συστήματα ασφαλείας δεν είναι σε θέση να προστατέψουν

πλήρως έναν οργανισμό, γεγονός που καθιστά την ανίχνευση της παραμικρής ασυνήθιστης συμπεριφοράς άκρως επιτακτική. Τα πλεονεκτήματα που παρουσιάζει ένα UEBA είναι:

α. Αντιμετώπιση ευρύτερου φάσματος κυβερνοεπιθέσεων: Επιθέσεις όπως Brute Force, DDoS, insider threats και παραβιασμένοι λογαριασμοί είναι εύκολο να ανιχνευτούν με τη χρήση ενός UEBA.

β. Ελαχιστοποίηση αναγκαίου προσωπικού: Καθόσον το UEBA αξιοποιεί τεχνολογίες μηχανικής μάθησης και τεχνητής νοημοσύνης, μπορεί να παράγει λεπτομερέστερα και ακριβέστερα αποτελέσματα σε ελάχιστο χρόνο, αντικαθιστώντας το προσωπικό που απαιτούνταν για να παράξει αυτό το αποτέλεσμα.

γ. Μείωση κόστους: Ως απόρροια της μείωσης του προσωπικού και της αποτελεσματικότερης ανίχνευσης απειλών, οι οργανισμοί δύνανται να μειώσουν το κόστος λειτουργίας τους, αφενός διότι απασχολούν λιγότερο προσωπικό και αφετέρου διότι προστατεύονται καλύτερα από κυβερνοεπιθέσεις που έχουν ως αποτέλεσμα την διακοπή της επιχειρηματικής δραστηριότητας ή την αποδέσμευση οικονομικών πόρων για την αντιμετώπιση ransomware.

δ. Μείωση κινδύνου: Αποτελεί το κυριότερο όφελος των UEBA. Λαμβάνοντας υπόψη το γεγονός ότι ένας οργανισμός δύναται να απασχολεί εργαζόμενους είτε στις εγκαταστάσεις του είτε απομακρυσμένα, να διαθέτει πληθώρα και ποικιλομορφία συσκευών IoT και επίσης να είναι αναγκασμένος να φιλοξενεί εξωτερικούς συνεργάτες στο δίκτυό του, είναι όλο και πιο δύσκολο να αντιμετωπίσει τις απειλές σε τόσο μεγάλη επιφάνεια, όσο μεγάλο τμήμα IT και να διαθέτει. Το UEBA, με τις δυνατότητες που προσφέρει, παρέχει την απαραίτητη ορατότητα στους αναλυτές ώστε να αντιδράσουν ταχύτερα σε ενδεχόμενες επιθέσεις και κατά συνέπεια να αυξήσουν την ασφάλεια του οργανισμού.

3.12.3 Σχέση UEBA και Zero Trust Architecture

Οι λύσεις UEBA θεωρούνται σημαντική προσθήκη σε μια αρχιτεκτονική Zero Trust. Το UEBA παρέχει πρόσθετα επίπεδα ασφάλειας με την ανίχνευση ανωμαλιών στη συμπεριφορά, ενώ η Αρχιτεκτονική Zero Trust επιβεβαιώνει ότι η πρόσβαση είναι πάντα βασισμένη σε πραγματική, επαληθευμένη ταυτότητα. Κατά συνέπεια, η συνδυαστική χρήση του UEBA και της Αρχιτεκτονικής Zero Trust αποτελεί ολοκληρωμένη προσέγγιση για την ενίσχυση της προστασίας των πληροφοριών και της δικτυακής ασφάλειας.

3.13 Mobile Device Management (MDM)

Οι φορητές συσκευές αποτελούν πλέον αναπόσπαστο κομμάτι της καθημερινότητας του ανθρώπου. Η χρήση των Smartphones, smart watches, tablet και laptops έχει ενσωματωθεί στην καθημερινότητα όλων, όπου μέσα από αυτά ρυθμίζονται διάφορες πτυχές της, από απλές υπενθυμίσεις μέχρι την παρακολούθηση ζωτικών ενδείξεων του ανθρώπου, την διασκέδασή του και την διεκπεραίωση των επαγγελματικών του υποχρεώσεων. Στο πλαίσιο αυτό, η χρήση τους έχει υιοθετηθεί και από τους οργανισμούς προκειμένου να εκμεταλλευτούν τα πλεονεκτήματα που

προσφέρουν οι συσκευές αυτές για να αυξήσουν την απόδοση και την παραγωγικότητα των εργαζομένων τους. Αυτό βέβαια προϋποθέτει ότι οι συσκευές έχουν πρόσβαση στους πόρους του οργανισμού. Καθίσταται λοιπόν σαφές ότι οι συσκευές αυτές, είτε γιατί έχουν λίγους υπολογιστικούς πόρους όπως για παράδειγμα τα smartwatches, είτε γιατί έχουν την δυνατότητα να εξέρχονται από τον οργανισμό τόσο ως υλικό όσο και λογικά, συνδεόμενες σε διάφορα δίκτυα, δύνανται να αποτελέσουν σημεία παραβίασης της ασφάλειας του οργανισμού. Συνεπαγόμενα, είναι κρίσιμο οι οργανισμοί να έχουν την δυνατότητα να διαχειρίζονται και να ασφαλίζουν τις συσκευές αυτές εντός του περιβάλλοντος του οργανισμού.

3.13.1 Χαρακτηριστικά των MDM

Λύση σε αυτό προσφέρουν οι πλατφόρμες διαχείρισης φορητών συσκευών (MDM). Οι πλατφόρμες MDM παρέχουν τη δυνατότητα διαχείρισης των φορητών συσκευών ενός οργανισμού, ανεξάρτητα από τον τύπο τους και το λειτουργικό τους σύστημα, συμβάλλοντας στην διατήρησης της ασφάλειας των συσκευών, ενώ ταυτόχρονα διατηρούν τα στοιχεία ευελιξίας και παραγωγικότητας.

Οι λύσεις MDM, βασιζόμενες στις πολιτικές και τις διαδικασίες του οργανισμού, χρησιμοποιούν λογισμικό μέσω του οποίου εφαρμόζουν μέτρα ασφαλείας και διαχείρισης στις φορητές συσκευές. Με την εφαρμογή του MDM, οι συσκευές λαμβάνουν πρόσβαση βάσει ενός ρόλου στα δεδομένα του οργανισμού, συνδέονται αποκλειστικά μέσω VPN και εφαρμόζεται σε αυτές παρακολούθηση μέσω γεωεντοπισμού καθώς και προστασία με κωδικό πρόσβασης. Παράλληλα το MDM αξιοποιώντας agents που έχουν εγκατασταθεί στις συσκευές, παρακολουθεί τη συμπεριφορά των συσκευών καθώς και τα κρίσιμα δεδομένα που έχουν αποθηκευτεί τοπικά στις συσκευές. Οι agents παράλληλα, προσφέρουν τη δυνατότητα αξιολόγησης της συσκευής από άποψη ασφάλειας, διαχείρισης των εφαρμογών και των ενημερώσεων ασφαλείας, ελέγχου των ενσωματωμένων μικροσυσκευών όπως μικρόφωνο και κάμερα, κρυπτογράφηση καθώς και πλήρη διαγραφή των δεδομένων σε περίπτωση απώλειας ή κλοπής.

3.13.2 Σχέση MDM και Zero Trust Architecture

Οι λύσεις MDM αποτελούν σημαντικό κομμάτι της Αρχιτεκτονικής Zero Trust, δημιουργώντας ένα ασφαλές και διαχειριζόμενο περιβάλλον για τις φορητές συσκευές. Οι λύσεις MDM διαδραματίζουν κρίσιμο ρόλο στην επιβολή της συμμόρφωσης της συσκευής με τις πολιτικές ασφαλείας του οργανισμού, καθόσον απαιτείται να τηρούν συγκεκριμένες ρυθμίσεις ασφαλείας συνυφασμένες με την αρχιτεκτονική Zero Trust. Επιπρόσθετα, οι λύσεις MDM παρέχουν παρακολούθηση πραγματικού χρόνου παρέχοντας πληροφορίες σχετικές με την κατάσταση και την συμπεριφορά των φορητών συσκευών, συμβάλλοντας στη συνεχή αξιολόγηση της εμπιστοσύνης προς τη φορητή συσκευή. Τέλος, μέσω των λύσεων MDM διασφαλίζεται ότι μόνο οι εξουσιοδοτημένες συσκευές έχουν πρόσβαση σε συγκεκριμένους πόρους του οργανισμού, συμπληρώνοντας τις αρχές του Zero Trust που εστιάζουν σε χρήστες και εφαρμογές.

3.14 Security Orchestration, Automation and Response (SOAR)

Σύμφωνα με την έρευνα του ινστιτούτου Ponemon σε συνεργασία με την IBM[53], το 2023, το μέσο κόστος μιας παραβίασης δεδομένων έφτασε στο ιστορικό υψηλό των 4,45 εκατομμυρίων δολαρίων ΗΠΑ, σημειώνοντας αύξηση 2% σε σύγκριση με το 2022 (4,35 δολάρια ΗΠΑ εκατομμύριο). Οι εταιρείες που εφάρμοσαν μια αρχιτεκτονική μηδενικής εμπιστοσύνης πλήρωσαν κατά μέσο όρο 4,15 εκατομμύρια δολάρια για μια παραβίαση δεδομένων. Όσοι δεν είχαν στρατηγικές μηδενικής εμπιστοσύνης πλήρωσαν 1,76 εκατομμύρια δολάρια περισσότερο, δηλαδή 5,10 εκατομμύρια δολάρια.

Όλες οι κυβερνοεπιθέσεις μελετώνται πάνω σε μια βάση χρονικής ακολουθίας γεγονότων (timeline). Η έναρξη της ακολουθίας γίνεται με την εκδήλωση ενεργειών αναγνώρισης του στόχου από τον επιτιθέμενο (Reckoning). Στην συνέχεια και αφού συγκεντρώσει όλα τα απαραίτητα στοιχεία, πραγματοποιείται η παραβίαση. Το επόμενο τμήμα στην χρονική ακολουθία είναι εκείνο όπου υποδεικνύει τον χρόνο που χρειάζεται ο οργανισμός για να συνειδητοποιήσει την παραβίαση (Mean Time To Detection) και στη συνέχεια ακολουθεί ένα χρονικό διάστημα μέχρι την αντιμετώπιση (Mean Time To Respond). Στην ίδια έρευνα[53], αναφέρεται ότι το 2021, χρειάστηκαν κατά μέσο όρο 212 ημέρες για να εντοπιστεί μια παράβαση και 75 ημέρες για να περιοριστεί. που αντιστοιχεί σε κύκλο ζωής παραβίασης 287 ημερών. Το 2022, ο μέσος χρόνος για τον εντοπισμό μιας παραβίασης είναι 207 ημέρες και ο μέσος χρόνος για τον περιορισμό της είναι 70 ημέρες με συνολικό κύκλο ζωής παραβίασης 277 ημερών υποδεικνύοντας πτώση 10 ημερών σε σύγκριση με τα δεδομένα του 2021. Καθίσταται λοιπόν σαφές ότι το χρονικό διάστημα από την παραβίαση ενός οργανισμού μέχρι την αντιμετώπιση της παραβίασης αυτής αφενός δεν είναι αμελητέο και αφετέρου είναι εξαιρετικά κοστοβόρο. Λύση σε αυτό προσφέρουν οι πλατφόρμες SOAR.

Το SOAR αποτελεί μια πλατφόρμα όπου λογισμικά σχετιζόμενη με την αντιμετώπιση κυβερνοεπιθέσεων, συνδυάζονται με σκοπό την παροχή δυνατότητας στον οργανισμό να αναγνωρίζει την επίθεση, να συλλέγει δεδομένα σχετικά με αυτή και στη συνέχεια να ανταποκρίνεται για την αντιμετώπισή της. Τα SOAR αποτελούνται από τρία δομικά στοιχεία[54], την ενορχήστρωση ασφαλείας, τον αυτοματισμό και την απόκριση σε κυβερνοεπιθέσεις.

3.14.1 Δομικά στοιχεία του SOAR

α. Ενορχήστρωση ασφαλείας: Το στοιχείο αυτό αφορά στην σύνδεση και ενσωμάτωση διαφόρων λογισμικών όπως σαρωτές ευπαθειών, προϊόντα Endpoint Security, λύσεις UEBA, Firewalls, IDS/IPS, πλατφόρμες διαχείρισης πληροφοριών και συμβάντων (SIEM) καθώς και πληροφορίες από τρίτες πηγές. Μέσω της συλλογής δεδομένων από τα λογισμικά αυτά με τη χρήση κατάλληλων API δημιουργείται ένα ενιαίο πλαίσιο (υπόθεση) που αφορά την επίθεση και στη συνέχεια διαμορφώνεται μια αυτοματοποιημένη διαδικασία για την αντιμετώπισή της.

β. Αυτοματισμός Ασφαλείας: Ο Αυτοματισμός ασφαλείας αφορά την ανάλυση και αξιοποίηση των δεδομένων που έχουν συλλεχθεί κατά την ενορχήστρωση και στη συνέχεια τη δημιουργία αυτοματοποιημένων διαδικασιών. Ο αυτοματισμός έρχεται να αντικαταστήσει χειροκίνητες διαδικασίες που εκτελούνταν από αναλυτές μειώνοντας έτσι κατά πολύ τον χρόνο απόκρισης. Αξιοποιώντας λύσεις

Τεχνητής Νοημοσύνης και Μηχανικής Μάθησης η δυνατότητα αυτοματοποίησης του SOAR μπορεί να ιεραρχήσει πολλαπλές απειλές με βάση την κρισιμότητα, να κάνει συστάσεις αντιμετώπισης και να δημιουργήσει playbooks.

γ. Τα Playbooks [55] είναι προκαθορισμένες αυτοματοποιημένες ενέργειες που αφορούν αντιμετώπιση μικρών συμβάντων κυβερνοασφάλειας, για παράδειγμα την αντιμετώπιση ενός phishing mail. Στο συγκεκριμένο παράδειγμα το playbook μπορεί να περιλαμβάνει ενέργειες όπως τον αποκλεισμό του email, την ειδοποίηση του χρήστη και τον αποκλεισμό της διεύθυνσης IP. Μέσω του SOAR, πολλά τέτοια playbooks μπορούν να συνδυαστούν δυναμικά σε ένα εκτενέστερο, βασισμένο στις πληροφορίες που έχουν συλλεχθεί κατά την ενορχήστρωση έτσι ώστε να ταιριάζει στα χαρακτηριστικά της συγκεκριμένης κυβερνοεπίθεσης.

δ. Απόκριση Ασφαλείας: Το στοιχείο αυτό αφορά στην διαδικασία διαμόρφωσης του playbook και την εφαρμογή του για την αντιμετώπιση της επίθεσης. Προσφέρει μια ολοκληρωμένη εικόνα στους αναλυτές σχετικά με τον σχεδιασμό, την παρακολούθηση και την αναφορά των ενεργειών που πραγματοποιήθηκαν. Στο στοιχείο αυτό περιλαμβάνονται επίσης και ενέργειες που έπονται της αντιμετώπισης της κυβερνοεπίθεσης όπως αξιολόγηση των playbooks, δημιουργία νέων και αναφορά.

3.14.2 Οφέλη του SOAR

Με την ενσωμάτωση εργαλείων ασφαλείας και την αυτοματοποίηση εργασιών, οι πλατφόρμες SOAR μπορούν να εξορθολογήσουν κοινές ροές εργασιών ασφάλειας, όπως διαχείριση υποθέσεων, διαχείριση ευπάθειας και απόκριση περιστατικών. Τα οφέλη αυτού του εξορθολογισμού περιλαμβάνουν [54],[55]:

α. Γρηγορότερη Ανίχνευση και Αντίδραση σε Περιστατικά: Ο όγκος και η ταχύτητα των απειλών και των συμβάντων ασφαλείας αυξάνονται διαρκώς. Το βελτιωμένο πλαίσιο δεδομένων του SOAR, σε συνδυασμό με την αυτοματοποίηση, μπορεί να μειώσει τον Μέσο Χρόνο Ανίχνευσης (MTTD) και να επιταχύνει τον Μέσο Χρόνο Απόκρισης (MTTR).

β. Συνδυασμός πληροφοριών: Ενσωματώνοντας περισσότερα δεδομένα από ένα ευρύτερο φάσμα εργαλείων ασφαλείας και συστημάτων καθώς και εξωτερικές πηγές, οι πλατφόρμες SOAR μπορούν να προσφέρουν καλύτερη ανάλυση και ενημερωμένες πληροφορίες απειλών.

γ. Απλοποιημένη Διαχείριση: Οι πλατφόρμες SOAR ενοποιούν τους πίνακες εργαλείων από διάφορα συστήματα ασφαλείας σε μια ενιαία διεπαφή. Αυτό βοηθά τις ομάδες SecOps στη συγκέντρωση των πληροφοριών, απλοποιώντας τη διαχείριση και εξοικονομώντας χρόνο.

δ. Επεκτασιμότητα: Η διαχείριση των συνεχώς αυξανόμενων περιστατικών ασφαλείας χωρίς αυτοματοποίηση οδηγεί στην εξάντληση της ταυτόχρονης δυνατότητας παρακολούθησης από τους αναλυτές λόγω του πεπερασμένου αριθμού τους, με αποτέλεσμα την μείωση της δυνατότητας ανίχνευσης και αντιμετώπισης των περιστατικών. Η ενορχήστρωση, η αυτοματοποίηση και οι ροές εργασίας του SOAR μπορούν να ανταποκριθούν στις απαιτήσεις επεκτασιμότητας πιο εύκολα.

ε. Αύξηση της Παραγωγικότητας των Αναλυτών: Η αυτοματοποίηση της αντιμετώπισης των χαμηλότερου επιπέδου απειλών ενισχύει τις δυνατότητες των ομάδων SecOps και των Κέντρων Επιχειρησιακής Ασφάλειας (SOC), επιτρέποντάς τους να ιεραρχούν τις εργασίες πιο αποδοτικά και να απασχολούνται σε αυτές που χρειάζονται πραγματικά ανθρώπινη παρέμβαση.

στ. Βελτιωμένες Λειτουργίες: Οι τυποποιημένες διαδικασίες και τα playbooks που εκτελούν εργασίες χαμηλότερου επιπέδου επιτρέπουν στις ομάδες SecOps να ανταποκρίνονται σε περισσότερες απειλές ταυτόχρονα. Αυτές οι αυτοματοποιημένες ροές εργασίας εξασφαλίζουν επίσης, ότι οι ίδιες τυποποιημένες προσπάθειες αποκατάστασης εφαρμόζονται σε ολόκληρο τον οργανισμό, σε όλα τα συστήματα.

ζ. Αναφορά και Συνεργασία: Οι αναφορές και η ανάλυση από τις πλατφόρμες SOAR ενοποιούν γρήγορα τις πληροφορίες, επιτρέποντας καλύτερες διαδικασίες διαχείρισης δεδομένων και αποτελεσματικότερες προσπάθειες απόκρισης για την ενημέρωση των υφιστάμενων πολιτικών και προγραμμάτων ασφαλείας, προς όφελος της πιο αποτελεσματικής ασφάλειας. Ο κεντρικός πίνακας εργαλείων μιας πλατφόρμας SOAR μπορεί επίσης να βελτιώσει την ανταλλαγή πληροφοριών μεταξύ διαφορετικών εταιρικών ομάδων, ενισχύοντας την επικοινωνία και τη συνεργασία.

η. Μειωμένο Κόστος: Σε πολλές περιπτώσεις, η ενίσχυση των αναλυτών ασφαλείας με τα εργαλεία SOAR μπορεί να μειώσει το κόστος, αντίθετα με τη μη αυτοματοποιημένη εκτέλεση όλων των προσπαθειών ανάλυσης, εντοπισμού και απόκρισης σε απειλές καθόσον μετά από ένα σημείο συσσώρευσης απειλών απαιτείται η ενίσχυση με επιπλέον αναλυτές προκειμένου να διατηρηθεί το επίπεδο ασφαλείας του οργανισμού.

3.14.3 Σχέση SOAR και Zero Trust Architecture

Η σχέση μεταξύ των πλατφορμών SOAR (Security Orchestration, Automation, and Response) και της αρχιτεκτονικής ZERO TRUST είναι στενά συνδεδεμένη ως προς τον τρόπο που αντιλαμβάνονται και αντιμετωπίζουν την ασφάλεια των πληροφοριών και των δικτύων. Η συνδυασμένη χρήση πλατφορμών SOAR και αρχιτεκτονικής ZERO TRUST επιτρέπει στους οργανισμούς να επιτυγχάνουν μια ολοκληρωμένη προσέγγιση στην ασφάλεια. Η αυτοματοποίηση και ο συντονισμός που παρέχουν οι πλατφόρμες SOAR συμβάλλουν στην αποτελεσματική αντίδραση σε απειλές, ενώ η αρχή της μη εμπιστοσύνης αποτελεί τη βάση για τον εντοπισμό και τον έλεγχο της ταυτότητας σε κάθε σημείο του δικτύου. Κατ' αυτόν τον τρόπο, επιτυγχάνεται μια σφαιρική προστασία κατά των κυβερνοαπειλών, ενισχύοντας την ασφάλεια και μειώνοντας τον κίνδυνο ανεπιθύμητων προσβάσεων.

Κεφάλαιο 4: Πρακτικές Εφαρμογές

4.1 Ανάλυση πρακτικών εφαρμογών του Zero Trust σε διάφορες επιχειρησιακές περιπτώσεις.

Στο πλαίσιο κατανόησης και περιγραφής του ZT μέχρι τώρα στην παρούσα εργασία, χρησιμοποιήθηκε ως σημείο αναφοράς ένα δίκτυο ενός οργανισμού, ώστε πάνω σε αυτό να ενσωματωθεί η λογική του ZT. Ωστόσο όπως έχει ήδη αναφερθεί, το ZT αποτελεί μια φιλοσοφία η οποία βρίσκει εφαρμογή και πέραν της αρχιτεκτονικής δικτύων.

4.1.1 Zero Trust στην ψηφιακή εγκληματολογία

Στην ψηφιακή εγκληματολογία[59] είναι λογικό ότι ορισμένες πτυχές της έρευνας εξαρτώνται αναπόφευκτα από την εμπιστοσύνη. Ωστόσο, αυτή είθισται να μην εξετάζεται πάντα ρητά ή να αξιολογείται επαρκώς και συχνά να θεωρείται ως δεδομένη. Δεδομένου ότι η έρευνα στην ψηφιακή εγκληματολογία βασίζεται σε μεγάλο βαθμό σε ψηφιακά εργαλεία, η εσφαλμένη αντιμετώπιση των χαρακτηριστικών της έρευνας ως αξιόπιστα, μπορεί να είναι εξαιρετικά επιζήμια για τη συνολική αξιοπιστία των πορισμάτων μιας έρευνας καθώς και για την εμπιστοσύνη που μπορεί να έχουν σε αυτή οι εξωτερικοί ενδιαφερόμενοι. Για παράδειγμα, οι σκηνές ψηφιακών εγκλημάτων μπορούν να παραποιηθούν σε περίπτωση παραβίασης των ψηφιακών εργαλείων που τις συλλέγουν, τις επεξεργάζονται και τις αναλύουν. Επίσης, η ανίχνευση της παραποίησης αυτής είναι εξαιρετικά δύσκολη και σπάνια, κάτι που αφήνει τις ψηφιακές ιατροδικαστικές έρευνες ευάλωτες σε κατηγορίες για ανακρίβεια.

Ως λύση σε αυτό προτείνεται η υιοθέτηση του Zero trust Forensics το οποίο είναι μια στρατηγική που θεωρεί ότι κάθε πτυχή της έρευνας είναι αναξιόπιστη μέχρι να επαληθευτεί. Το ZTF στην προσπάθεια να άρει τις αμφιβολίες περιλαμβάνει μεθόδους επαλήθευσης του ίδιου αποτελέσματος με διαφορετικά εργαλεία από διαφορετικούς επαγγελματίες, δοκιμή και πιστοποίηση της αποτελεσματικότητας των εργαλείων πριν την χρήση τους σε κάποια υπόθεση ψηφιακής εγκληματολογίας καθώς και επαλήθευση της ακεραιότητάς τους.

4.1.2 Zero Trust σε Virtual Power Plants

Τα Virtual Power Plants[60] είναι αρχιτεκτονικές όπου πολλές γεννήτριες από ανανεώσιμες πηγές ενέργειας μπορούν να ενσωματωθούν σε ένα δίκτυο χρησιμοποιώντας “έξυπνες τεχνολογίες”, παροχετεύοντας την παραγόμενη ενέργειά τους στη συνολική παραγωγή ενός σταθμού παραγωγής ενέργειας. Ωστόσο, η ενσωμάτωση αυτή ελλοχεύει διάφορες προκλήσεις όπως προβλήματα ενσωμάτωσης, ατέλειωτο εφοδιασμό ενέργειας χωρίς επαρκείς δυνατότητες αποθήκευσης, ασφάλεια των συσκευών ελέγχου, υπερτάσεις, απώλειες μετασχηματιστών κ.α. Επομένως είναι απαραίτητο τα δίκτυα ηλεκτρικής ενέργειας να προσαρμοστούν σε μια αποκεντρωμένη προσέγγιση για τη μείωση αυτών των επιπλοκών καθώς και για την αντιμετώπιση των προκλήσεων.

Η ψηφιοποίηση των δικτύων ηλεκτρικής ενέργειας έχει αλλάξει τη δυναμική των τελευταίων δεκαετιών. Αυτή η πρόοδος στην τεχνολογία έχει συνεισφέρει σημαντικά

στην καλύτερη κατανόηση της παραγωγής και κατανάλωσης ενέργειας. Αυτό ανοίγει τον δρόμο για την υιοθέτηση της ανάλυσης δεδομένων χρησιμοποιώντας μεγάλης κλίμακας αναλύσεις δεδομένων, που παρέχει τεράστιες ευκαιρίες για την βελτιστοποίηση των δικτύων, τη μείωση των λειτουργικών κοστών, των διακοπών, της κλοπής, της προγραμματισμένης συντήρησης κ.λπ.. Ωστόσο, τα τεράστια δεδομένα που συλλέγονται στα αποθετήρια είναι κατανοητά μόνο με τη χρήση ισχυρών εργαλείων επεξεργασίας δεδομένων. Αυτή η κατακόρυφη αύξηση των δυνατοτήτων αποτελεί παράλληλα και αυξημένη απειλή. Επίσης, η αυτοματοποίηση θέτει ένα άλλο μεγάλο πρόβλημα, καθώς οι συσκευές χρειάζονται σύνδεση στο διαδίκτυο κάτι που τις καθιστά ευάλωτες σε επιθέσεις. Επομένως, είναι απαραίτητο να διασφαλιστεί μια πολύπλευρη προσέγγιση για μια αποτελεσματική ψηφιοποίηση, συμπεριλαμβανομένων των παραδοσιακών εγκαταστάσεων παραγωγής ενέργειας, ώστε να αποτραπούν επιθέσεις κυβερνοασφάλειας. Στο όλο εγχείρημα, μεγαλύτερο κίνδυνο παρουσιάζουν οι ανεξάρτητοι παραγωγοί, καθόσον οι παραδοσιακές εγκαταστάσεις υποστηρίζονται από κυβερνήσεις και μεγάλες εταιρίες και διαθέτουν ώριμα συστήματα ασφαλείας καθώς και πόρους συντήρησης και επέκτασης αυτών.

Είναι απαραίτητο λοιπόν, η μηδενική εμπιστοσύνη να εφαρμοστεί σε κάθε παραγωγό ή καταναλωτή που συνδέεται με τους σταθμούς παραγωγής ενέργειας. Οι συσκευές σύνδεσης πρέπει να παρακολουθούνται και να υπόκεινται σε διαρκή επαλήθευση της ταυτότητάς τους ώστε να διασφαλίζεται η ακεραιότητα λειτουργίας τους και η συμμόρφωσή τους με τα αυστηρά πρότυπα του εκάστοτε σταθμού.

4.2 Μελέτη περιπτώσεων επιχειρήσεων ή οργανισμών που έχουν υλοποιήσει με επιτυχία το Zero Trust.

4.2.1 Εφαρμογή του Zero Trust από την Akamai

Η Akamai πίστευε ότι η δικτυακή προσέγγιση στην ασφάλεια και την πρόσβαση δεν ήταν πλέον επαρκής για την προστασία των περιουσιακών περιουσιών της εταιρείας. Οι παραδοσιακές λύσεις VPN συνοδεύονται από τους ανάλογους κινδύνους ασφαλείας, συμπεριλαμβανομένου του αυξημένου κινδύνου μη εξουσιοδοτημένης απομακρυσμένης πρόσβασης σε ευαίσθητα δεδομένα και πρόσβασης σε όλες τις εφαρμογές στο εταιρικό δίκτυο, από οποιαδήποτε πιστοποιημένη συσκευή. Η προσέγγιση στην απομακρυσμένη πρόσβαση δημιουργεί κινδύνους που δεν είναι αναγκαίοι. Με το VPN, κάθε χρήστης μπορεί γενικά να έχει πρόσβαση στις ίδιες εφαρμογές που μπορεί κάθε άλλος χρήστης.

Η Akamai αποφάσισε να υιοθετήσει μια στρατηγική ασφαλείας Zero Trust[65] που θα εξαλείψει το παραδοσιακό εταιρικό VPN και θα απομακρυνθεί από ένα μοντέλο ασφαλείας βασισμένο σε περίμετρο. Ο στόχος ήταν να προστατευτούν οι εφαρμογές και τα δεδομένα της Akamai και να αποτραπεί η πλευρική κίνηση στο εταιρικό δίκτυο, παρέχοντας παράλληλα βελτιωμένη εμπειρία χρήστη.

Στο πλαίσιο της μετάβασης προς τη μεταστροφή Zero Trust, η Akamai δεσμεύτηκε σε έναν πυρήνα αρχών:

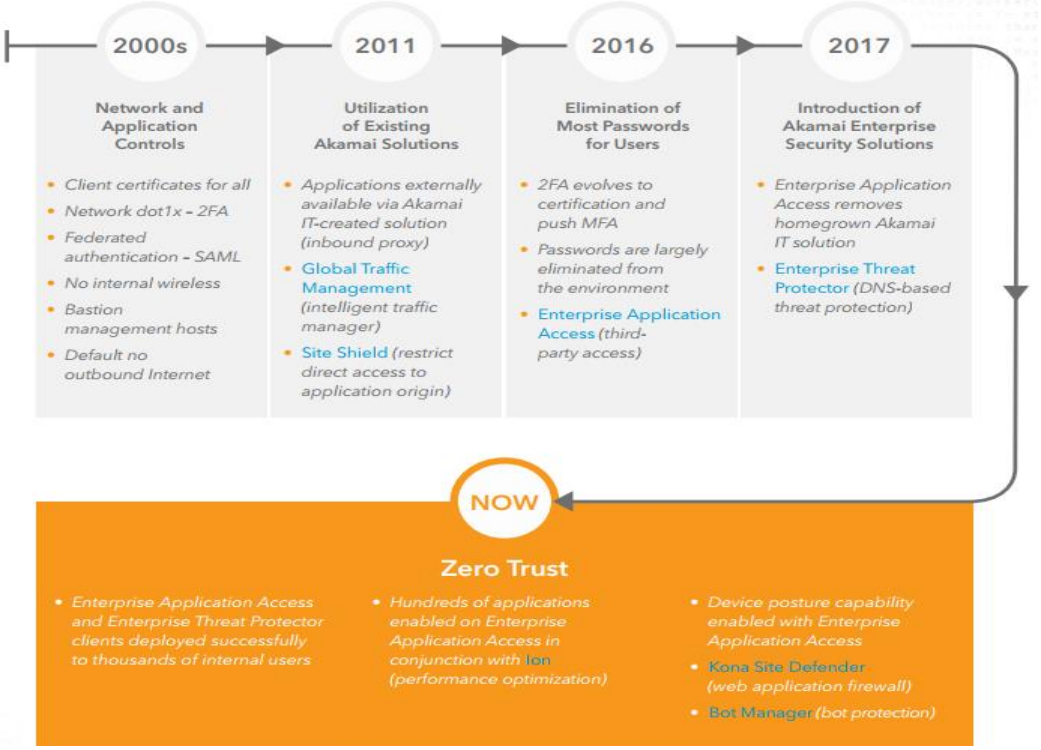
α. Μετάβαση σε ένα περιβάλλον χωρίς περίμετρο όπου το Διαδίκτυο γίνεται το εταιρικό δίκτυο.

β. Κάθε γραφείο πρέπει να γίνει Wi-Fi hotspot.

γ. Η πρόσβαση στις εφαρμογές επιτρέπεται δυναμικά βάσει της ταυτότητας, παραγόντων περιβάλλοντος, όπως η τοποθεσία και η ώρα της ημέρας, και σημάτων συσκευής, όπως πιστοποιητικά πελάτη ή συμμόρφωση της συσκευής προς την εταιρική πολιτική ασφαλείας. Αυτή η προσέγγιση βασίζεται στην αποδοχή του κόστους αποδοτικών τεχνολογιών που υποστηρίζουν την κινητικότητα, την ενισχυμένη ασφάλεια, την ευελιξία πρόσβασης και την εικονικοποίηση, εκμεταλλευόμενες παράλληλα την απλότητα του νέφους.

Το τμήμα IT της Akamai υιοθέτησε το Enterprise Application Access για να μεταβεί από το VPN στη νέα προσέγγιση. Αυτή η λύση πρόσβασης βασίζεται στο νέφος και κλειδώνει το εταιρικό δίκτυο με πρόσβαση μόνο σε εφαρμογές πίσω από το τείχος προστασίας. Με την τεχνολογία της Akamai, η πρόσβαση στις εφαρμογές, ανεξαρτήτως του πού φιλοξενούνται (εντός εγκαταστάσεων, IaaS, SaaS), βασίζεται αποκλειστικά στα δικαιώματα, την ταυτότητα, την πιστοποίηση και την εξουσιοδότηση σε επίπεδο εφαρμογής. Χρησιμοποιώντας το Enterprise Application Access για την προσβασιμότητα και τον έλεγχο κάθε εφαρμογής, η Akamai επιτρέπει ευελιξία, απλότητα και μια καλύτερη εμπειρία χρήστη για ολόκληρο το εργατικό δυναμικό, συμπεριλαμβανομένων των ομάδων IT και ασφαλείας.

Η προσέγγιση της Akamai μείωσε το κόστος και τις πολυπλοκότητες που συνήθως σχετίζονται με την ασφάλεια της πρόσβασης στις εφαρμογές. Αντί να προσπαθεί να ελέγξει ή να περιορίσει συσκευές που αποκτούν απομακρυσμένη πρόσβαση στο εταιρικό δίκτυο, είχε περισσότερο νόημα για την Akamai να υιοθετήσει μια λύση που επιτρέπει στο IT να παρακολουθεί και να ελέγχει την πρόσβαση μόνο σε εκείνες τις εφαρμογές που οι χρήστες πραγματικά χρειάζονται. Η μετάβαση όλων

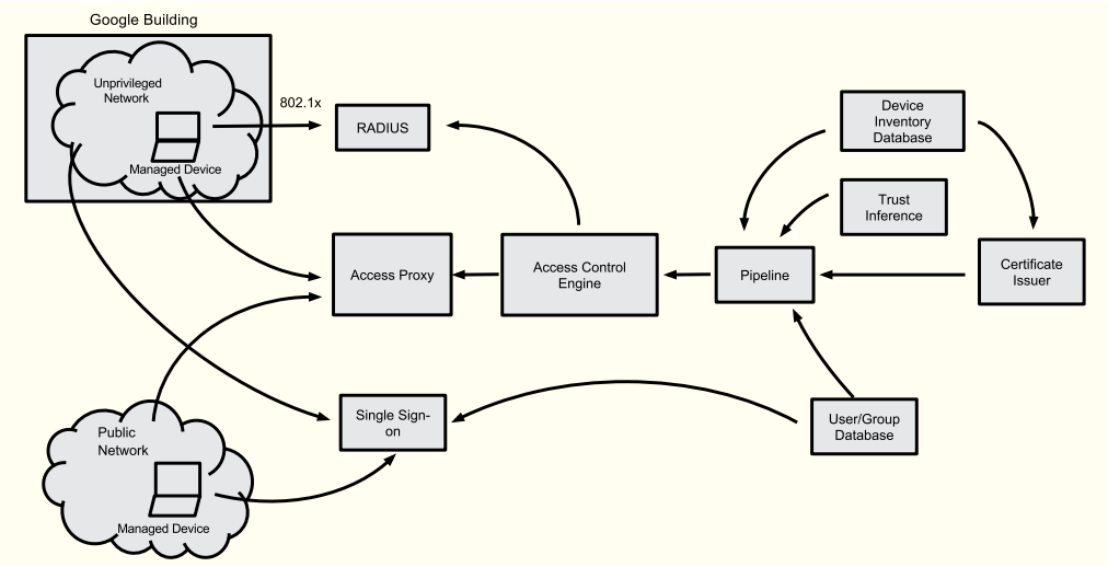


Εικόνα 25: Χρονικό μετάπτωσης της Akamai σε ZT[65]

εκτός του VPN και του εταιρικού δικτύου, και η χρήση μιας προσέγγισης μηδενικής εμπιστοσύνης για να αποκτήσει ορατότητα για όλη την κίνηση (μεταξύ χρηστών, συσκευών, τοποθεσιών και εφαρμογών), όχι μόνο μείωσε σημαντικά τον κίνδυνο, αλλά επίσης εξυπηρέτησε την διαδικασία ανάπτυξης εφαρμογών της εταιρείας. Η εκμετάλλευση της θέσης της συσκευής για δυναμικές αποφάσεις πρόσβασης είναι μια ακόμη κύρια συνιστώσα για την ολοκλήρωση της μετάβασης της Akamai σε ένα μοντέλο μηδενικής εμπιστοσύνης. Η θέση της συσκευής συμπληρώνει και ενισχύει τους υπάρχοντες κανόνες πιστοποίησης, εξουσιοδότησης, ελέγχου πρόσβασης και δυνατοτήτων αναφοράς, παρέχοντας επιπλέον πλαίσιο και σήμα για τη δυναμική πρόσβαση στις εφαρμογές.

4.2.2 Εφαρμογή ZT από την Google με το BeyondCorp Framework.

Το BeyondCorp Framework[61] αποτελεί πρωτοβουλία της Google και εμφανίστηκε για πρώτη φορά στις αρχές τις δεκαετίας του 2000, έπειτα από την επιτυχημένη κυβερνοεπίθεση με όνομα “Operation Aurora”. Με την υιοθέτηση του BeyondCorp Framework,, η Google άλλαξε ριζικά την φιλοσοφία της στο θέμα της κυβερνοασφάλειας στηριζόμενη πλέον στον παράγοντα «ταυτότητα» για την εκχώρηση δικαιωμάτων πρόσβασης στους χρήστες του δικτύου της, ανεξάρτητα από την τοποθεσία τους και χωρίς τη χρήση VPN.



Εικόνα 26: BeyondCorp components and access flow ΠΗΓΗ: BeyondCorp[61]

Το BeyondCorp Framework για να εξασφαλίσει ότι μόνο οι εξουσιοδοτημένες συσκευές και χρήστες έχουν πρόσβαση στις εταιρικές εφαρμογές, ενσωματώνει στοιχεία ελέγχου ταυτότητας συσκευής και χρήστη και σύστημα Single Sign – On, τα οποία τροφοδοτούν μια μηχανή ελέγχου πρόσβασης (κατ’ αντιστοιχία με την PE στο μοντέλο ZT) η οποία αποφασίζει για την εκχώρηση ή την απαγόρευση της πρόσβασης σε εταιρικούς πόρους. Το μοντέλο αυτό βασίζεται κατά κύριο λόγο στον browser της Google (Chrome), αν και είναι συμβατό και με άλλους browsers μεγάλων εταιριών (Edge, Firefox), όπου μέσα από την καταχώρηση του εταιρικού λογαριασμού στον browser γίνεται η ταυτοποίηση του χρήστη και εκχωρούνται οι προσβάσεις σε αυτόν

καθώς και όλα τα στοιχεία ασφαλείας που τον διέπουν (DLP policies, Malware protection κ.α) για την προστασία των εταιρικών πόρων.

Το BeyondCorp βασίζεται στις θεμελιώδεις αρχές της αρχιτεκτονικής ZT με την διαφορά ότι όλοι οι εταιρικοί πόροι βρίσκονται διαθέσιμοι στο υπολογιστικό νέφος της Google και η προσπέλασή τους πραγματοποιείται με την αυθεντικοποίηση μέσω Browser. Με τον τρόπο αυτό δεν απαιτείται η χρήση VPN για την σύνδεση σε κλειστό εταιρικό δίκτυο και το βάρος της ασφάλειας μετατοπίζεται στην αυθεντικοποίηση του χρήστη.

Κεφάλαιο 5: Προκλήσεις και Συμπεράσματα.

5.1 Προκλήσεις

Όπως έχει ήδη αναφερθεί και αναλυθεί στην παρούσα εργασία, το ZT αποτελεί μια νέα προσέγγιση στον τομέα της κυβερνοασφάλειας. Υιοθετώντας ένα μοντέλο ZT οι οργανισμοί επιτυγχάνουν την επαύξηση της ασφάλειας των πόρων τους και την μείωση του αντικτύπου των επιτυχών κυβερνοεπιθέσεων. Ωστόσο, το ZT δεν αποτελεί την θεραπεία στην ολοένα και μεγαλύτερη μάστιγα των κυβερνοεπιθέσεων. Σύμφωνα με την Gartner[62], έως το 2026, περισσότερες από τις μισές επιθέσεις στον κυβερνοχώρο θα στοχεύουν σε τομείς που η μηδενική εμπιστοσύνη δεν καλύπτει και δεν μπορεί να προστατεύσει. Αυτό οφείλεται κυρίως στον αργό ρυθμό υιοθέτησης του ZT από τους οργανισμούς καθώς και την ανάγκη αυτών για διατήρηση παλαιών συστημάτων και εφαρμογών. Χαρακτηριστική είναι η έρευνα του Cybersecurity Insiders[63] σε δείγμα 400 επαγγελματιών πληροφορικής και ασφάλειας στις ΗΠΑ, η οποία αναφέρει ότι μόλις το 19% των οργανισμών έχει εφαρμόσει ZT. Στην ίδια έρευνα αναφέρεται επίσης ότι σε ένα ποσοστό 30% η διαδικασία βρίσκεται σε εξέλιξη ενώ το 38% βρίσκεται στο στάδιο του σχεδιασμού. Παράλληλα, η Gartner στην έρευνά[62] της, εμφανίζει λιγότερο αισιόδοξα αποτελέσματα καθώς εκτιμά ότι λιγότεροι από το 1% των οργανισμών έχουν ένα ώριμο και μετρήσιμο πρόγραμμα μηδενικής εμπιστοσύνης και μόνο το 10% θα έχει ένα μέχρι το 2026.

Ακόμη και όταν έχει αναπτυχθεί μηδενική εμπιστοσύνη, δεν σημαίνει ότι έχουν λυθεί όλα τα ζητήματα ασφάλειας. Το ZT έχει πολλά τυφλά σημεία, όπως συστήματα παλαιού τύπου που δεν σχεδιάστηκαν για μηδενική εμπιστοσύνη, προνομιούχους χρήστες που κάνουν πράγματα που δεν θα έπρεπε, συσκευές IoT χωρίς παρακολούθηση, συστήματα τρίτων και, φυσικά, το συνεχές πρόβλημα της διαχείρισης αλλαγών. Από τις παραπάνω έρευνες προκύπτει ότι οι τομείς όπου το ZT αντιμετωπίζει δυσχέρειες στο να προστατέψει αποτελεσματικά τους οργανισμούς είναι οι κάτωθι:

α. Συστήματα παλαιού τύπου: Οι επαγγελματίες στο χώρο της ασφάλειας γνωρίζουν ότι υπάρχουν συστήματα και εφαρμογές τα οποία λειτουργούν στους οργανισμούς σε ευρεία κλίμακα και δεν έχουν σχεδιαστεί να υποστηρίζουν τις αρχές του ZT. Ωστόσο η αντικατάστασή τους με νεότερα, αφενός θα επηρεάσει σε πολύ μεγάλο βαθμό την λειτουργία του οργανισμού και αφετέρου απαιτεί τεράστιο κόστος (εφαρμογές HR επι παραδείγματι). Λόγω των δυσχερειών αυτών εξαναγκάζονται να εφαρμόσουν ημίμετρα επί των τρεχουσών εφαρμογών και συστημάτων, προκειμένου να πλησιάσουν τα πρότυπα του ZT, ωστόσο αυτό ενέχει τον κίνδυνο δημιουργίας κενών ασφαλείας και “τυφλών σημείων” τα οποία αποτελούν στόχους προς εκμετάλλευση για τους επίδοξους επιτιθέμενους.

β. Συσκευές IoT: Λόγω της αρχιτεκτονικής τους και του τρόπου λειτουργίας τους, οι συσκευές αυτές αποτελούν ένα διαρκές πρόβλημα για την ασφάλεια. Καθόσον οι συσκευές αυτές αφορούν λειτουργίες του οργανισμού, όπως για παράδειγμα συσκευές ελέγχου εισόδου σε πόρτες (Card Readers), θερμοστάτες κεντρικής θέρμανσης κ.α., είναι απαραίτητο να είναι συνδεδεμένες στο δίκτυο ώστε να δεσμεύονται από την πολιτική ασφαλείας του οργανισμού. Είθισται δε, η διαχείρισή τους να ανατίθεται σε εξωτερικούς συνεργάτες, χωρίς βέβαια να είναι απαραίτητη προϋπόθεση για αυτούς να ακολουθούν τις αρχές του ZT. Συνεπώς, καθίσταται σαφές

ότι οι συσκευές IoT αποτελούν ζωτικό παράγοντα λειτουργίας αλλά ταυτόχρονα και εν δυνάμει κενό στην ασφάλεια του οργανισμού.

γ. Προνομιακή Πρόσβαση: Ακόμα και με την εφαρμογή της πιο αυστηρής πολιτικής στη διαχείριση των δικαιωμάτων πρόσβασης, δεν παύουν να αποτελούν ένα εν δυνάμει κενό στην ασφάλεια, καθόσον τα δικαιώματα είναι άρρηκτα συνδεδεμένα με τον ανθρώπινο παράγοντα. Είναι δε στατιστικά βέβαιο ότι σε κάθε οργανισμό υφίστανται χρήστες που η φύση της εργασίας τους απαιτεί πρόσβαση σε εμπιστευτικές πληροφορίες, όπως επίσης υφίστανται και χρήστες οι οποίοι είναι επιρρεπείς σε επιθέσεις κοινωνικής μηχανικής. Συνεπώς, ο χρήστης αποτελεί αστάθμητο παράγοντα στην ασφάλεια καθώς είτε ακούσια είτε εκούσια δύναται να προξενήσει ρήγμα στην ασφάλεια το οποίο θα οδηγήσει σε απώλεια δεδομένων.

δ. Υπηρεσίες Τρίτων Παρόχων: Όλες οι εταιρείες και οι οργανισμοί, ανεξάρτητα από το μέγεθός τους και τις επιχειρηματικές τους δραστηριότητες, προκειμένου να παράξουν τα προϊόντα και τις υπηρεσίες τους εξαρτώνται από υπηρεσίες τρίτων παρόχων. Αυτές οι υπηρεσίες μπορεί να αφορούν από προμήθεια πρώτων υλών, δυνατότητα χρήσης εφαρμογών ως υπηρεσία (Software as a Service) ή ακόμα και ολική διαχείριση δευτερευόντων συστημάτων, όπως για παράδειγμα εταιρίες ασφάλειας ή κλιματισμού. Λόγω της φύσης αυτής της επιχειρηματικής σχέσης, οι τρίτοι πάροχοι έχουν πρόσβαση και πολλές φορές προνομιούχα δικαιώματα στο δίκτυο του οργανισμού ή επικοινωνούν με αυτόν μέσω APIs. Συνεπώς, η μη τήρηση των αρχών ZT από αυτούς αποτελεί εν δυνάμει κίνδυνο για τον οργανισμό, ακόμα και αν ο οργανισμός εφαρμόζει στο έπακρο τις αρχές ZT.

ε. Νέες Τεχνολογίες και Εφαρμογές: Σύμφωνα με έρευνα της Beyond Identity[64] η ενσωμάτωση και ο χειρισμός νέων εφαρμογών αποτελεί την τρίτη μεγαλύτερη πρόκληση στην εφαρμογή του ZT. Οι εταιρίες στο πλαίσιο βελτίωσης των παρεχόμενων υπηρεσιών τους επιδιώκουν την τροποποίηση των υφιστάμενων εφαρμογών τους καθώς και την ενσωμάτωση νέων, που οδηγούν σε νέα και βελτιωμένη εμπειρία για τον χρήστη – καταναλωτή. Το γεγονός αυτό έρχεται σε αντίθεση με την έννοια της εμπιστοσύνης των δεδομένων, η οποία θέτει εμπόδια στην λειτουργία των εφαρμογών αυτών. Πρακτικά, αν το ZT δεν σχεδιαστεί και δεν εφαρμοστεί σωστά, μπορεί να αποτελέσει πλήγμα στην παραγωγικότητα του οργανισμού. Σε αυτό έρχεται να προστεθεί και η ολοένα αυξανόμενη ενσωμάτωση στοιχείων AI στις εταιρικές εφαρμογές. Θεωρώντας δεδομένο ότι όσο περισσότερες πληροφορίες διαθέτει το AI τόσο πιο αποδοτικό είναι, η συγκέντρωση αυτή οδηγεί σε επέκταση της επιφάνειας επίθεσης και κατά συνέπεια στην αύξηση του κινδύνου.

5.2 Συμπεράσματα

Η εξέταση της έννοιας της Αρχιτεκτονικής Δικτύων Μηδενικής Εμπιστοσύνης ανέδειξε τη σημασία της επίτευξης της ασφάλειας και της εμπιστοσύνης στα σύγχρονα δίκτυα, όπου η επικοινωνία και η ανταλλαγή πληροφοριών καταλαμβάνουν κεντρική θέση.

Κατά τη διάρκεια της εργασίας αυτής, έγινε σαφής η ανάγκη για καινοτόμες προσεγγίσεις και προηγμένες τεχνικές, οι οποίες να ενισχύουν την ασφάλεια των δικτύων ώστε να ανταποκρίνονται στις σύγχρονες προκλήσεις της ψηφιακής εποχής. Η Μηδενική Εμπιστοσύνη, ως βασικό στοιχείο της εξέλιξης, αναδεικνύεται ως μία αναγκαία προσέγγιση που προσφέρει προοπτικές ασφαλούς και αξιόπιστης επικοινωνίας. Μέσω της εργασίας παρουσιάστηκε και αναλύθηκε εκτενώς η προσέγγιση της Αρχιτεκτονικής Μηδενικής Εμπιστοσύνης, η σύγκρισή της με παλαιότερες προσεγγίσεις, τα τεχνολογικά εργαλεία που μπορούν να ενσωματωθούν στην αρχιτεκτονική και τέλος παραδείγματα μεγάλων εταιριών που έχουν υιοθετήσει την αρχιτεκτονική αυτή.

Ολοκληρώνοντας, εκτιμώ πως η παρούσα εργασία ανταποκρίνεται στον στόχο της δημιουργίας ενός ενημερωμένου και ενδιαφέροντος πλαισίου για την ανάλυση και την εφαρμογή της Αρχιτεκτονικής Δικτύων Μηδενικής Εμπιστοσύνης. Στόχος μου είναι να ενθαρρύνω την κοινότητα των ερευνητών, των επαγγελματιών και των εκπαιδευτικών να συνεχίσουν τον ενεργό διάλογο και τη συνεργασία προς την κατεύθυνση της επίτευξης περισσότερων εξελίξεων στον τομέα αυτόν. Μέσω συνεχούς έρευνας και καινοτόμων προσεγγίσεων, καθίσταται δυνατή η διαμόρφωση ενός μέλλοντος, όπου η ασφάλεια των δικτύων δεν αποτελεί μόνο προτεραιότητα αλλά και αναπόσπαστο κομμάτι της ψηφιακής επικοινωνίας.

Πηγές και Βιβλιογραφία

[1] No More Chewy Centers: Introducing The Zero Trust Model Of Information Security https://crystaltechnologies.com/wp-content/uploads/2017/12/forrester-zero-trust-model-information-security.pdf

[2] The State of Zero Trust Security in Global Organizations (2020) https://www.okta.com/resources/reports/state-of-zero-trust-security-in-global-organizations/

[3] ARPANET https://www.techtarget.com/searchnetworking/definition/ARPANET#:~:text=The%20U.S.%20Advanced%20Research%20Projects,for%20academic%20and%20research%20purposes.

[4] Kevin Mitnick https://en.wikipedia.org/wiki/Kevin_Mitnick

[5]SIEM https://www.ibm.com/topics/siem#:~:text=Security%20information%20and%20event%20management%2C%20or%20SIEM%2C%20is%20a%20security,chance%20to%20disrupt%20business%20operations.

[6] George Finney – Project Zero Trust (2022)

[7] What is the castle-and-moat network model (Cloudflare) https://www.cloudflare.com/en-gb/learning/access-management/castle-and-moat-network-security/

[8] Why the Castle and Moat Approach to Security Is Obsolete (Emily Omier) https://thenewstack.io/why-the-castle-and-moat-approach-to-security-is-obsolete/

[9] Castle-and-Moat Network Security Model (CyberHoot) https://cyberhoot.com/cybrary/castle-and-moat-network-model/

[10] Zero Trust Cybersecurity: 'Never Trust, Always Verify' (NIST, Alper Kerman) https://www.nist.gov/blogs/taking-measure/zero-trust-cybersecurity-never-trust-always-verify

[11] Zero Trust security | What is a Zero Trust network? https://www.cloudflare.com/en-gb/learning/security/glossary/what-is-zero-trust/

[12] Introducing Zero Trust by Design: Principles and Practice Beyond the Zero Trust https://www.researchgate.net/publication/353324913_Introducing_Zero_Trust_by_Design_Principles_and_Practice_Beyond_the_Zero_Trust_Hype

[13] Role-Based Access Control (RBAC) Atribute – Based Access Control (ABAC), https://www.okta.com/au/identity-101/what-is-role-based-access-control-rbac/

[14]What is Privileged Identity Management (PIM), https://www.fortinet.com/resources/cyberglossary/privileged-identity-management

[15]Implementing Authorization With User Roles (RBAC), https://blogs.sap.com/2022/11/21/sap-commissions-implementing-authorization-with-user-roles-rbac/

[16] ABAC Model – ResearchGate https://www.researchgate.net/figure/Scheme-of-attribute-based-access-control-ABAC-model_fig2_332732675

[17]Privileged Access Management – FORTRA https://www.fortra.com/resources/guides/essentials-privileged-access-management

[18] What Is Least Privilege & Why Do You Need It? (BeyondTrust) https://www.beyondtrust.com/blog/entry/what-is-least-privilege

[19] What is Data Encryption? (Kaspersky) https://www.kaspersky.com/resource-center/definitions/encryption

[20] Data Encryption (EGNYTE) https://www.egnyte.com/guides/governance/data-encryption

[21]Encryption Algorithms (CISCO) https://www.cisco.com/c/en/us/products/security/encryption-explained.html#~encryption-algorithms

[22] Define a Protect Surface to Massively Reduce Your Attack Surface (PaloAlto) https://www.paloaltonetworks.com/blog/2018/09/define-protect-surface-massively-reduce-attack-surface/#:~:text=Typically%2C%20a%20Zero%20Trust%20network,Which%20assets%20are%20most%20sensitive%3F

[23] Zero Trust Architecture (NIST SP 800-207) https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-207.pdf

[24] The Definitive Zero Trust Guide (Cyber Theory) https://cybertheory.io/the-definitive-zero-trust-guide/

[25] The path to Zero Trust starts with Identity (IDSA Whitepaper)

[26] What is identity and access management? Guide to IAM (TechTarget) https://www.techtarget.com/searchsecurity/definition/identity-access-management-IAM-system

[27] Privileged Access Management (PAM) (BeyondTust) https://www.beyondtrust.com/resources/glossary/privileged-access-management-pam

[28] Zero-Trust Security for Cloud Data Centers – How Much Does it Cost? https://www.netronome.com/blog/zero-trust-security-for-cloud-data-centers-how-much-does-it-cost/

[29] Software Defined Perimeter (TechTarget) https://www.techtarget.com/searchcloudcomputing/definition/software-defined-perimeter-SDP

[30] What is a cloud access security broker (CloudFlare)
https://www.cloudflare.com/en-gb/learning/access-management/what-is-a-casb/

[31] Understanding Cloud Access Security Brokers
https://www.strongdm.com/blog/casb

[32] Securely Adopt Cloud Services and Enforce Security Policies
https://www.acldigital.com/offerings/telco-cloud-and-networking/security/cloud-security/cloud-access-security-broker

[33] security information and event management (SIEM) (TechTarget)
https://www.techtarget.com/searchsecurity/definition/security-information-and-event-management-SIEM

[34] SIEM definition – What is SIEM? (LogPoint)
https://www.logpoint.com/en/what-is-siem/

[35] What is a Jump Server (JAVA Point)
https://www.javatpoint.com/what-is-a-jump-server

[36] The Latest 2023 Phishing Statistics (updated October 2023)
https://aag-it.com/the-latest-phishing-statistics/

[37] multifactor authentication (TechTarget)
https://www.techtarget.com/searchsecurity/definition/multifactor-authentication-MFA

[38] Number of connected devices reached 22 billion, where is the revenue? (Strategy Analytics)
Number of connected devices reached 22 billion, where is the revenue? - Help Net Security

[39] What Is Endpoint Security? (Trellix)
https://www.trellix.com/security-awareness/endpoint/what-is-endpoint-security/#:~:text=Endpoint%20security%20is%20the%20practice,the%20cloud%20from%20cybersecurity%20threats.

[40] What is a Next Generation Firewall? (Check Point)
https://www.checkpoint.com/cyber-hub/network-security/what-is-next-generation-firewall-ngfw/

[41] What is a Firewall? (Check Point)
https://www.checkpoint.com/cyber-hub/network-security/what-is-firewall/

[42] What is a Next Generation Firewall (Zenarmor)
https://www.zenarmor.com/docs/network-security-tutorials/next-generation-firewall

[43] What is data loss prevention? (Microsoft)

https://www.microsoft.com/en-us/security/business/security-101/what-is-data-loss-prevention-dlp

[44] What Is DLP and How Does It Work? (Trellix)
https://www.trellix.com/security-awareness/data-protection/how-data-loss-prevention-dlp-technology-works/

[45] Data loss prevention (ManageEngine)
https://www.manageengine.com/data-security/what-is/data-loss-prevention.html

[46] VPN users around the world (GlobalWebIndex)
https://www.gwi.com/reports/vpn-usage-around-the-world

[47] 2023 VPN Usage Statistics (Security.org)
https://www.security.org/vpn/statistics/#:~:text=While%2032%20percent%20of%20mobile,11%20percent%20of%20mobile%20users.

[48] What is VPN? How It Works, Types of VPN (Kaspersky)
https://www.kaspersky.com/resource-center/definitions/what-is-a-vpn

[49] VPN (virtual private network) (TechTarget)
https://www.techtarget.com/searchnetworking/definition/virtual-private-network

[50] What Is a VPN & How Does It Work? (AVAST)
https://www.avast.com/c-what-is-a-vpn

[51] network access control (NAC) (TechTarget)
https://www.techtarget.com/searchnetworking/definition/network-access-control

[52] What Is Network Access Control? Definition, Key Components, and Best Practices (Spiceworks)
https://www.spiceworks.com/it-security/network-security/articles/what-is-network-access-control/

[53] What is the Cost of a Data Breach in 2023?
https://www.upguard.com/blog/cost-of-data-breach

[54] What is SOAR?
https://www.ibm.com/topics/security-orchestration-automation-response

[55] SOAR (security orchestration, automation and response)
https://www.techtarget.com/searchsecurity/definition/SOAR

[56] Egerton H, Hammoudeh M, Unal D, Adebisi B. Applying Zero Trust Security Principles to Defence Mechanisms Against Data Exfiltration Attacks. Security and Privacy in the Internet of Things: Architectures, Techniques, and Applications 2021:57–89.
https://doi.org/10.1002/9781119607755.CH3

[57] A novel zero-trust network access control scheme based on the security profile of devices and users. P. García-Teodoro ∗, J. Camacho, G. Maciá-Fernández, J.A. Gómez-Hernández, V.J. López-Marín, Network Engineering & Security Group, CITIC - University of Granada, Spain

[58] Advancing Zero Trust with Privileged Access Management (PAM) (BeyondTrust Whitepaper)

[59] The case for Zero Trust Digital Forensic, Cristofer Neale, Ian Kennedy, Blaine Price, Yijun Yu, Bashar Nuseibeh

[60] Augmenting Zero Trust Network Architecture to enhance security in virtual power plants. Annamalai Alagappan, Sampath Kumar Venkatachary, Leo John Baptist Andrews

[61] A new Approach to Enterprise security (BeyondCorp)
https://research.google/pubs/beyondcorp-a-new-approach-to-enterprise-security/

[62] Gartner Predicts 10% of Large Enterprises Will Have a Mature and Measurable Zero-Trust Program in Place by 2026.
https://www.gartner.com/en/newsroom/press-releases/2023-01-23-gartner-predicts-10-percent-of-large-enterprises-will-have-a-mature-and-measurable-zero-trust-program-in-place-by-2026

[63] 2023 ZERO TRUST SECURITY report (Fortra)
https://www.cybersecurity-insiders.com/portfolio/2023-zero-trust-security-report-fortra/

[64] Majority of Security Experts Choose Zero Trust [Survey] (Beyond Identity)
https://www.beyondidentity.com/resources/zero-trust-sentiments-cyber-security-professionals

[65] How Akamai implemented a Zero Trust Security Model without a VPN.
https://www.akamai.com/site/en/documents/case-study/how-akamai-implemented-a-zero-trust-security-model-without-a-vpn.pdf