ΠΑΝΕΠΙΣΤΗΜΙΟ ΔΥΤΙΚΗΣ ΑΤΤΙΚΗΣ
ΣΧΟΛΗ ΜΗΧΑΝΙΚΩΝ
ΤΜΗΜΑ ΜΗΧΑΝΙΚΩΝ ΠΛΗΡΟΦΟΡΙΚΗΣ ΚΑΙ ΥΠΟΛΟΓΙΣΤΩΝ
ΠΡΟΓΡΑΜΜΑ ΜΕΤΑΠΤΥΧΙΑΚΩΝ ΣΠΟΥΔΩΝ: ΚΥΒΕΡΝΟΑΣΦΑΛΕΙΑ

Διπλωματική Εργασία

Κυβερνοασφάλεια στον χώρο της Υγείας

Φοιτητής: Αργιανάς Δημήτριος
ΑΜ: Cscyb22004

Επιβλέπων Καθηγητής:

Δρ. Γιαννακόπουλος Παναγιώτης

.

ΑΘΗΝΑ-ΑΙΓΑΛΕΩ, Φεβρουάριος 2024

ΠΑΝΕΠΙΣΤΗΜΙΟ ΔΥΤΙΚΗΣ ΑΤΤΙΚΗΣ
ΣΧΟΛΗ ΜΗΧΑΝΙΚΩΝ
ΤΜΗΜΑ ΜΗΧΑΝΙΚΩΝ ΠΛΗΡΟΦΟΡΙΚΗΣ ΚΑΙ ΥΠΟΛΟΓΙΣΤΩΝ
ΠΡΟΓΡΑΜΜΑ ΜΕΤΑΠΤΥΧΙΑΚΩΝ ΣΠΟΥΔΩΝ: ΚΥΒΕΡΝΟΑΣΦΑΛΕΙΑ

Κυβερνοασφάλεια στον χώρο της Υγείας

Μέλη Εξεταστικής Επιτροπής συμπεριλαμβανομένου και του Εισηγητή

Η μεταπτυχιακή διπλωματική εργασία εξετάστηκε επιτυχώς από την κάτωθι Εξεταστική Επιτροπή:

Α/Α	ΟΝΟΜΑ- ΕΠΩΝΥΜΟ	ΥΠΟΓΡΑΦΗ
1	**Δρ. Παναγιώτης Γιαννακόπουλος**	Panagiotis Giannakopoulos Digitally signed by Panagiotis Giannakopoulos Date: 2024.04.21 10:49:57 +03'00'
2	**Δρ. Στέφανος Γκρίτζαλης**	STEFANOS GKRITZALIS 22/04/2024 12:17
3	**Δρ. Κωνσταντίνος Μαυρομμάτης**	Konstantinos Mavrommatis Digitally signed by Konstantinos Mavrommatis Date: 2024.04.22 14:56:29 +03'00'

ΔΗΛΩΣΗ ΣΥΓΓΡΑΦΕΑ ΔΙΠΛΩΜΑΤΙΚΗΣ ΕΡΓΑΣΙΑΣ

Ο κάτωθι υπογεγραμμένος **Αργιανάς Δημήτριος** του **Μιχαήλ** με αριθμό μητρώου **Cscyb22004,** φοιτητής του Προγράμματος Μεταπτυχιακών Σπουδών της Κυβερνοασφάλειας του **ΠΑΝΕΠΙΣΤΗΜΙΟΥ ΔΥΤΙΚΗΣ ΑΤΤΙΚΗΣ** της Σχολής ΜΗΧΑΝΙΚΩΝ του Τμήματος **ΜΗΧΑΝΙΚΩΝ ΠΛΗΡΟΦΟΡΙΚΗΣ ΚΑΙ ΥΠΟΛΟΓΙΣΤΩΝ,**

Δηλώνω υπεύθυνα ότι:

«Είμαι συγγραφέας αυτής της διπλωματικής εργασίας και ότι κάθε βοήθεια την οποία είχα για την προετοιμασία της είναι πλήρως αναγνωρισμένη και αναφέρεται στην εργασία. Επίσης, οι όποιες πηγές από τις οποίες έκανα χρήση δεδομένων, ιδεών ή λέξεων, είτε ακριβώς είτε παραφρασμένες, αναφέρονται στο σύνολό τους, με πλήρη αναφορά στους συγγραφείς, τον εκδοτικό οίκο ή το περιοδικό, συμπεριλαμβανομένων και των πηγών που ενδεχομένως χρησιμοποιήθηκαν από το διαδίκτυο. Επίσης, βεβαιώνω ότι αυτή η εργασία έχει συγγραφεί από εμένα αποκλειστικά και αποτελεί προϊόν πνευματικής ιδιοκτησίας τόσο του Ιδρύματος όσο και δικής μου.

Παράβαση της ανωτέρω ακαδημαϊκής μου ευθύνης αποτελεί ουσιώδη λόγο για την ανάκληση του διπλώματός μου.»

Ο Δηλών:

Αργιανάς Δημήτριος του **Μιχαήλ**

(Υπογραφή φοιτητή)

ΕΥΧΑΡΙΣΤΙΕΣ

Η παρούσα διπλωματική εργασία ολοκληρώθηκε στο πλαίσιο των μεταπτυχιακών μου σπουδών με τίτλο «Κυβερνοασφάλεια» του τμήματος Μηχανικών Πληροφορικής και Υπολογιστών του Πανεπιστημίου Δυτικής Αττικής.

Θα ήθελα να ευχαριστήσω θερμά τον επιβλέποντα καθηγητή μου και Διευθυντή του Προγράμματος Μεταπτυχιακών Σπουδών Δρ. Παναγιώτη Γιαννακόπουλο. Πρωτίστως, ως επιβλέποντα καθηγητή για την εμπιστοσύνη που μου επέδειξε αναθέτοντάς μου το συγκεκριμένο θέμα, εν συνεχεία, για την συνεχή του επιστημονική καθοδήγηση, και υποστήριξη καθ' όλη την διάρκεια της συγγραφής της διπλωματικής μου εργασίας. Επιπλέον, ως Διευθυντή του ΠΜΣ για την ομαλή διεξαγωγή του προγράμματος καθώς και για την επίλυση των όποιων ζητημάτων προέκυψαν κατά την διάρκεια του κύκλου σπουδών.

Τέλος, θα ήθελα να ευχαριστήσω και το άρτια καταρτισμένο επιστημονικά λοιπό εκπαιδευτικό προσωπικό, για την εκπαίδευση, την καθοδήγηση και την βοήθεια που προσέφεραν.

Αιγάλεω 2024,

Αργιανάς Δημήτριος

ΠΕΡΙΛΗΨΗ

Η Υγειονομική Περίθαλψη εκτός του ότι είναι ένας τομέας που ανήκει στις κρίσιμες υποδομές ενός κράτους, στην σύγχρονη εποχή είναι πλέον και ένας τομέας που είναι εξαρτώμενος από την τεχνολογία. Η τεχνολογία χρησιμοποιείται σχεδόν σε κάθε επίπεδο του τομέα δημιουργώντας πολλαπλές προκλήσεις κυβερνοασφάλειας. Το μεγάλο μέγεθος επίθεσης ενός φορέα υγείας μπορεί οδηγήσει σε διακοπή λειτουργιών στον οργανισμό, ενώ η ύπαρξη μεγάλου όγκου προσωπικών, αλλά και δεδομένων ειδικών κατηγοριών καθιστά τον οργανισμό ως στόχο υψηλής αξίας με σκοπό τη διαρροή αυτών των δεδομένων.

Ο σκοπός της παρούσης διπλωματικής εργασίας είναι η ανάδειξη του πολυδιάστατου του τομέα της υγείας με την αποτύπωση των διαφόρων περιουσιακών στοιχείων αυτού, των κύριων κυβερνοαπειλών και ευπαθειών που δύναται να τον επηρεάσουν, την ομαλή και απρόσκοπτη λειτουργία του οργανισμού. Επίσης θα εξετάσουμε τους ενδεδειγμένους τρόπους αντιμετώπισης και μετριασμού των κινδύνων. Λύσεις πρόληψης και αντιμετώπισης μπορούν να δοθούν μέσω στρατηγικών, προτύπων και κανονισμών, οργανωτικών και τεχνικών μέτρων, ενώ πλαίσια ασφαλείας μπορούν επίσης να βρουν εφαρμογή σε αυτή την προσπάθεια. Τέλος η εμφάνιση νέων τεχνολογιών μπορεί να προσφέρει επίσης αποτελεσματικά στην αντιμετώπιση αυτών των προκλήσεων.

Λέξεις κλειδιά: Κυβερνοασφάλεια στην Υγεία, Περιουσιακά στοιχεία στην Υγεία, Κυβερνοαπειλές στην Υγεία, Κυβερνοεπιθέσεις στην Υγεία, Πλαίσιο ασφάλειας υγειονομικής περίθαλψης, ασφάλεια σε βάθος, μηδενική εμπιστοσύνη.

ABSTRACT

Health Care, apart from being a sector that belongs to the critical infrastructure of a state, in the modern era is now also a sector that is dependent on technology. Technology is used at almost every level of the sector creating multiple cybersecurity challenges. The large scale of an attack on a healthcare organization can lead to disruption of operations in the organization, while the existence of a large volume of personal and classified data makes the organization a high-value target for the purpose of data breach.

The purpose of this thesis is to highlight the multidimensionality of the health sector by capturing its various assets, the main cyberthreats and vulnerabilities that may affect the smooth and uninterrupted operation of the organization. We will also examine the appropriate ways of dealing with and mitigating the risks. Prevention and response solutions can be provided through strategies, standards and regulations, organizational and technical measures, while security frameworks can also apply in this effort. Finally, the emergence of new technologies can also provide effective solutions to these challenges.

Keywords: Cybersecurity Healthcare, Healthcare assets, Healthcare cyber threats, Healthcare Cyber Attacks, Healthcare security framework, defense in depth, zero trust.

ΠΙΝΑΚΑΣ ΑΚΡΩΝΥΜΙΩΝ

ACLs	Access Control Lists
AI	Artificial Intelligence
ANN	Artificial Neural Network
BDR	Blood Donor Registry
BMS	Building Management Systems
BYOD	Bring your own device
CC	Cloud Computing
CC	Cognitive Computing
CCTV	Closed-circuit television
CISA	Cybersecurity and Infrastructure Security Agency
CISO	Chief Information Security Officer
COBIT	Control Objectives for Information Technologies
CR	Computer Room
dApps	Decentralized Applications
DBF	Database Firewall
DDoS	Distributed Denial-of-Service
DID	Defense-in-Depth
DLP	Data Loss Prevention
DMZ	Demilitarized Zone
DoS	Denial-of-Service
DPIA	Data Protection Impact Assessments
DT	Decision Tree
EDR	Endpoint Detection and Response
EHR	Electronic Health Records
EMR	Electronic Medical Record
ENISA	European Union Agency for Cybersecurity
FBI	Federal Bureau of Investigation
FG	Fog Computing
FHE	Fully Homomorphic Encryption
GDPR	General Data Protection Regulation
HIS	Health Information System
HR	Human Resources
ICS	Industrial Control Systems
ICT	Information and Communication Technologies
IDS	Intrusion Detection System
IIoT	Industrial Internet of Things
IoMT	Internet of Medical Things
IoT	Internet of Things
IP	Internet Protocol
IPS	Intrusion Prevention System
ISA	Interconnection Security Agreement
ISACA	Information Systems Audit and Control Association

ISMS	Information Security Management System
ISO	International Organization for Standardization
IT	Information Technology
ITSMS	Information Technology Services Management System
KNN	k-Nearest Neighbor
LIS	Laboratory Information System
LR	Logistic Regression
MAM	Mobile Application Management
MDM	Mobile Device Management
MDR	Managed Detection and Response
MFA	Multi-Factor Authentication
MiTM	Man-in-the-Middle
ML	Machine Learning
MOA	Memorandum of Agreement
MOU	Memorandum of Understanding
MTD	Moving Target Defense
NB	Naïve Bayes
NCSC	National Cyber Security Centre
NGFW	Next Generation Firewall
NIST	National Institute of Standards and Technology
NOC	Network Operations Center
NSA	National Security Agency
PACS	Picture Archiving and Communication System
PHE	Partial Homomorphic Encryption
PHR	Patient Health Records
PKI	Public Key Infrastructure
QoS	Quality of service
RBAC	Role-Based Access Control
RF	Random Forest
RIS	Radiology Information System
SAML	Security Assertion Markup Language
SAST	Static Application Security Testing
SDN	Software Defined Networking
SHS	Smart Health System
SIEM	Security Information and Event Management
SLA	Service-Level Agreement
SOC	Security Operations Center
SQL	Structured Query Language
SSL	Secure Sockets Layer
SWHE	Somewhat Homomorphic Encryption
TLS	Transport Layer Security
TPM	Trusted Platform Module
VoIP	Voice over Internet Protocol
VPN	Virtual private network

WAF	Web Application Firewall
XDR	Extended Detection and Response
XGB	XGBoost
ZT	Zero Trust
ZTA	Zero Trust Architecture
Ε.Ε.	Ευρωπαϊκή Ένωση
ΗΚΓ	Ηλεκτροκαρδιογράφημα
ΚΕΜ	Καρδιολογική Εντατική Μονάδα
ΜΕΘ	Μονάδα Εντατικής Θεραπείας
Π.Ο.Υ.	Παγκόσμιος Οργανισμός Υγείας
ΤΕΙ	Τακτικά Εξωτερικά Ιατρεία
ΤΕΠ	Τμήμα Επειγόντων Περιστατικών

Περιεχόμενα

Κατάλογος Σχημάτων

Κεφάλαιο 1 – Εισαγωγή και Μεθοδολογία

1.1 Εισαγωγή

Ο τομέας της Υγείας, λόγω του μεγάλου όγκου πολύ ευαίσθητων πληροφοριών – προσωπικών δεδομένων που διαχειρίζεται και κατέχει είναι από τους πιο ελκυστικούς στόχους.[1] Η Βιομηχανία της Υγείας αν και σχετικά νέα με εκκίνηση της από το επίπεδο 1.0 το 1970 σήμερα με την έλευση κυρίως των τεχνολογιών Internet of Things (IoT) και Cloud Computing έχει εξελιχθεί στο επίπεδο 4.0 βασιζόμενη στην ανάπτυξη έξυπνων συσκευών και τη χρήση τους.[61] Ταυτόχρονα λόγω της μεγάλης επιφάνειας επίθεσης (πολλές βάσεις δεδομένων - εφαρμογές και πληροφοριακά συστήματα, ασύρματα δίκτυα, cloud services, email, περιφερειακές συσκευές, συσκευές IoMT και IoT, πολλοί χρήστες με διαφορετικές δεξιότητες, εξωτερικοί συνεργάτες κλπ) είναι ένας από τους πιο ευάλωτους στόχους για κυβερνοεπιθέσεις στον κόσμο.[1],[27],[29] Σε ένα οργανόγραμμα τυπικού μεσαίου Νοσοκομείου όπως π.χ. το Σισμανόγλειο μπορούμε να αντιληφθούμε το πολυδιάστατο ενός οργανισμού παροχής υπηρεσιών υγείας και το μεγάλο μέγεθος της επιφάνειας επίθεσης που προκύπτει.[5] Παγκόσμια ο τομέας της υγείας είναι από τους τομείς ζωτικής σημασίας, τόσο από πλευράς ύπαρξης ευαίσθητων προσωπικών δεδομένων, όσο και από πλευράς απρόσκοπτης συνέχισης παροχής υπηρεσιών με αποτέλεσμα η ασφάλεια αυτού να είναι από τις προτεραιότητες, κάτι που αναφέρεται στην στρατηγική κυβερνοασφάλειας της ΕΕ για την ψηφιακή δεκαετία και στην Εθνική Στρατηγική Κυβερνοασφάλειας 2020 – 2025.[6],[7] Ακόμη επισημαίνεται ότι η πανδημία Covid-19 επιτάχυνε την ψηφιακή μετεξέλιξη του συστήματος υγείας (π.χ. στροφή στην τεχνολογία για την παροχή βασικών υπηρεσιών υγείας, μεγαλύτερη εφαρμογή τηλεργασίας) οδηγώντας σε μεγαλύτερη επιφάνεια για επιθέσεις πυροδοτώντας αύξηση αυτών ακόμα και 220%[15],[17] κάνοντας ακόμα πιο επιτακτικό το θέμα της ασφάλειας[2],[16],[17].

1.2 Μεθοδολογία

Η μεθοδολογία της παρούσας διπλωματικής εργασίας πραγματοποιήθηκε αρχικά με αναζήτηση κυρίως από Google Scholar επιστημονικών άρθρων, αλλά και διαφόρων άρθρων σε web browsing προς αποτύπωση μιας γενικής εικόνας για την κυβερνοασφάλεια στην υγεία με λέξεις κλειδιά cybersecurity in healthcare. Εν συνεχεία αναζητήθηκαν οι προτεραιότητες της Εθνικής Στρατηγικής[6], αλλά και της Στρατηγικής κυβερνοασφάλειας της Ε.Ε.[7] Ακόμη αναζητήθηκε οργανόγραμμα ενός φορέα υγείας ελληνικού νοσοκομείου[5] για κατανόηση της διαφορετικότητας των αντικειμένων και του εύρους των κυβερνοαπειλών που αυτό αντιμετωπίζει και κατ’ επέκταση ο χώρος της υγείας. Από web browsing για την τελευταία 5ετία κυρίως αναζητήθηκαν στατιστικοί δείκτες για τον τομέα της υγείας όσον αφορά κυβερνοεπιθέσεις και κυβερνοαπειλές. Από τον ENISA[8],[9],[10],[11],[12] έγινε αναζήτηση της βιβλιογραφίας του για τον τομέα της υγείας από την οποία έγινε μια μελέτη για τα assets, τις απειλές, τις ευπάθειες, αλλά και μια πρώτη ματιά σε αντίμετρα. Μέσω Google Scholar και web browsing πραγματοποιήθηκε αναζήτηση για τις βασικότερες απειλές του τομέα της υγείας. Αναλυτικότερη μελέτη για αντίμετρα πραγματοποιήθηκε από την βιβλιογραφία των προτύπων της οικογένειας ISO 27000 με πιο κύρια τα ISO 27002[24], ISO 27005[25], ISO 27799, αλλά και του ISO 29100. Αντίμετρα αναζητήθηκαν και από την βιβλιογραφία του NIST (NIST.SP.800-66[21], NIST.SP.800-53[22] και NIST.IR.8228[33]), ενώ από τον GDPR[13] για την προστασία ευαίσθητων δεδομένων. Τέλος από Google Scholar έγινε αναζήτηση επιστημονικών άρθρων για την τελευταία 5ετία που αφορούν κυβερνοεπιθέσεις, κυβερνοαπειλές, αντίμετρα και νέες τάσεις τεχνολογίας. Από την πληθώρα των επιστημονικών άρθρων έγινε αξιολόγηση και τελική επιλογή

αυτών που παρείχαν την καλύτερη βοήθεια στην παρούσα διπλωματική εργασία. Λέξεις κλειδιά που χρησιμοποιήθηκαν καθ' όλη την διαδικασία ήταν: cybersecurity healthcare, Cyber Hospital, healthcare assets, healthcare cyber threats, cybersecurity vulnerabilities, ransomware healthcare, data breach healthcare, IoMT, medical device cyber, Healthcare cyber COVID-19, healthcare privacy, Healthcare Information Technology, healthcare security framework, Healthcare Cloud, defense in depth, zero trust, artificial intelligence healthcare security, blockchain cyber healthcare, homomorphic healthcare, fog computing healthcare.

Κεφάλαιο 2 – Assets φορέων υγείας

Το Νοσοκομείο είναι ένα οικοσύστημα που αποτελείται από πολλά στοιχεία και η ασφάλεια στον κυβερνοχώρο θα πρέπει να αποτελεί προτεραιότητα για όλα αυτά τα διαφορετικά στοιχεία.

Η Εμπιστευτικότητα (Confidentiality) των πληροφοριών και των ευαίσθητων προσωπικών δεδομένων, η Ακεραιότητα (Integrity) αυτών, καθώς η Διαθεσιμότητα (Availability) συστημάτων, υπηρεσιών και πληροφοριών είναι καίρια για την ομαλή λειτουργία ενός Νοσοκομείου.[11],[12]

Στο παρακάτω σχήμα βλέπουμε μια κατηγοριοποίηση των assets ενός οργανισμού παροχής υπηρεσιών υγείας:

Σχήμα 1: Assets taxonomy Νοσοκομείου.[10]

Τα διάφορα assets ενός φορέα υγεία αναλυτικότερα μπορούν να κατηγοριοποιηθούν όπως στις επόμενες ενότητες. [8],[9],[10],[12]

2.1 Κλινικά πληροφοριακά συστήματα

Είναι κάθε είδος λογισμικού προσανατολισμένο στην ιατρική περίθαλψη όπως:

- Πληροφοριακά Συστήματα Νοσοκομείου (Health Information System - HIS) (διαχείριση εισιτηρίων – εξιτηρίων, διακομιδών, κλινών, εφημεριών, ΤΕΠ, ΤΕΙ, φαρμάκων, διατροφής, χειρουργείων κλπ)
- Ηλεκτρονικός Ιατρικός Φάκελος (Electronic Medical Record - EMR) και Ηλεκτρονικός Φάκελος Υγείας (Electronic Health Records - EHR)
- Πληροφοριακά Συστήματα Εργαστηρίων (Laboratory Information System - LIS)

- Ακτινολογικό Πληροφοριακό Σύστημα (Radiology Information System - RIS)
- Σύστημα Αρχειοθέτησης και Επικοινωνίας Εικόνων (Picture Archiving and Communication System - PACS)

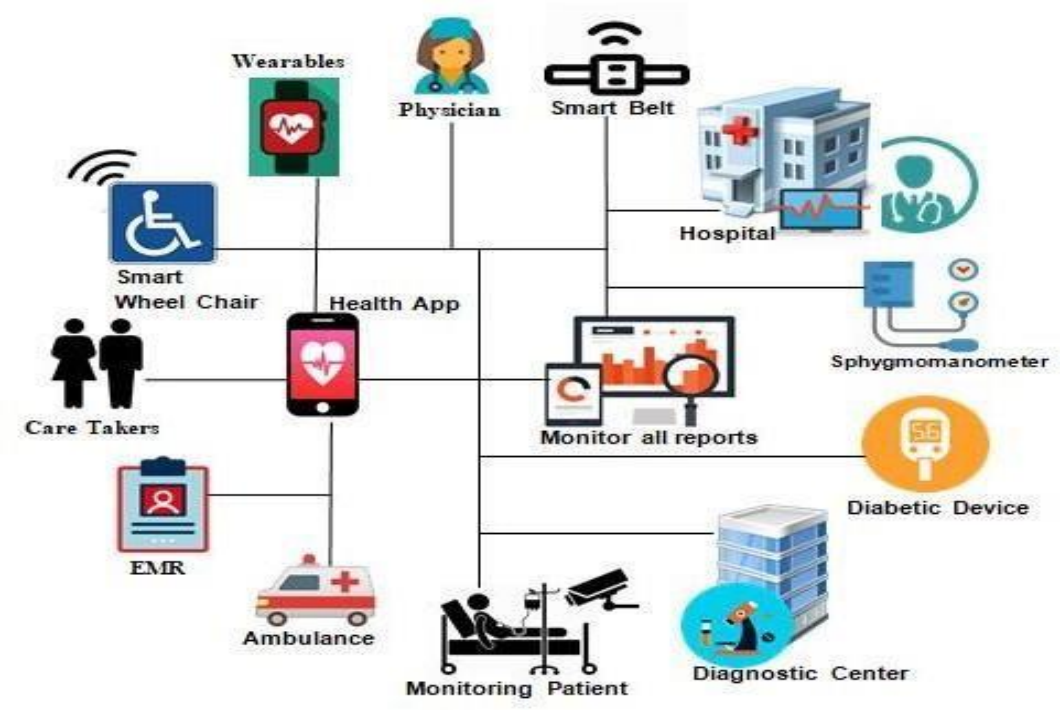
Σε αυτήν την κατηγόρια περιλαμβάνονται και οι αντίστοιχες βάσεις δεδομένων των ως άνω συστημάτων που είναι εγκατεστημένες σε κάποιο Computer Room (CR) του οργανισμού. Καθώς επίσης και τα αντίστοιχα backup που πρέπει να λαμβάνονται τακτικά και να φυλάσσονται σε άλλο φυσικό χώρο από τον χώρο λειτουργίας των βάσεων δεδομένων.

2.2 Ιατροτεχνολογικές συσκευές και συσκευές IoMT

Είναι ο εξοπλισμός που αφορά την θεραπεία, τον έλεγχο ή τη διάγνωση ασθενειών όπως:

- Ακτινολογικός εξοπλισμός (Μαγνητικοί, αξονικοί τομογράφοι, υπέρηχοι κλπ)
- Εξοπλισμός ακτινοθεραπείας
- Εξοπλισμός πυρηνικής ιατρικής
- Εξοπλισμός χειρουργείων, ΜΕΘ, ΚΕΜ
- Ρομπότ χειρουργικών επεμβάσεων (λαπαροσκοπικών)
- Εξοπλισμός ενδοσκόπησης
- Συσκευών σπιρομέτρησης
- Συσκευών λιπομέτρησης
- Τεστ κοπώσεως
- Λοιπού ιατροτεχνολογικού εξοπλισμού

Σε αυτή την κατηγορία εντάσσονται και οι συσκευές IoMT δεδομένου ότι επικοινωνούν με τα πληροφοριακά συστήματα του νοσοκομείου. Τέτοιες συσκευές μπορεί να είναι είτε εμφυτεύσιμες για τον ασθενή (holters, βηματοδότες, αντλίες ινσουλίνης, κοχλιακά εμφυτεύματα, διεγέρτες εγκεφάλου, καρδιακοί απινιδωτές, γαστρικοί διεγέρτες κλπ) ή φορητές συσκευές (εξωτερικά ΗΚΓ ή μετρητές πίεσης και καρδιακών παλμών, οξύμετρα, μετρητές γλυκόζης κλπ).[36],[44]



Σχήμα 2: Internet of Medical Things (IoMT).[44]

2.3 Πληροφοριακός εξοπλισμός

Είναι ο εξοπλισμός του πυρήνα ενός νοσοκομείου, ήτοι των servers του CR. Επίσης οι υπολογιστές των χρηστών και ο λοιπός πληροφοριακός εξοπλισμός.

2.4 Λοιπά πληροφοριακά συστήματα

Είναι κάθε είδος λογισμικού προσανατολισμένο στην Διοικητική λειτουργία και σε λοιπές διαδικασίες όπως:

- Εφαρμογής Προσωπικού (HR) διαχείρισης ανθρωπίνων πόρων
- Εφαρμογής Ηλεκτρονικού Πρωτοκόλλου
- Εφαρμογής Ηλεκτρονικής Διακίνησης Εγγράφων
- Λογισμικού Κεντρικής Διαχείρισης Antivirus

2.5 Δικτυακός εξοπλισμός

Είναι ο εξοπλισμός δικτύωσης του οργανισμού και περιλαμβάνει τις γραμμές του δικτύου, gateways, routers, switches, firewalls, VPNs, IPS/IDS, ασύρματα δίκτυα, IP τηλεφωνία (VoIP) κλπ.

2.6 Υπηρεσίες Cloud

Είναι οποιοδήποτε (Clinical Information System – CIS) ή άλλο σύστημα πληροφοριών που δεν βρίσκεται στον οργανισμό ή σε ένα Computer Room υπό τον πλήρη έλεγχο του τμήματος πληροφορικής του Νοσοκομείου. Τέτοια συστήματα είναι:

- Η ηλεκτρονική συνταγογράφηση (ePrescription service)
- Πληροφοριακά Συστήματα στο cloud: e-health
- Το αρχείο υγείας ασθενών (Patient Health Records - PHR)
- Η εφαρμογή του Εθνικού Μητρώου Αιμοδοτών (BDR)

Ακόμα και κάποιο από τα Κλινικά πληροφοριακά συστήματα ή λοιπά πληροφοριακά συστήματα δύναται να λειτουργεί ως υπηρεσία cloud.

2.7 Building Management Systems (BMS) και Industrial Control Systems (ICS)

Είναι συστήματα λογισμικού που ελέγχουν όλες τις φυσικές πτυχές ενός Νοσοκομείου, όπως συστήματα ρύθμισης ισχύος, access control, CCTV, κλιματισμού - θέρμανσης, ιατρικών αερίων, συναγερμού, νερού, γεννητριών, ανελκυστήρων, πυρανίχνευσης - πυρόσβεσης κλπ.

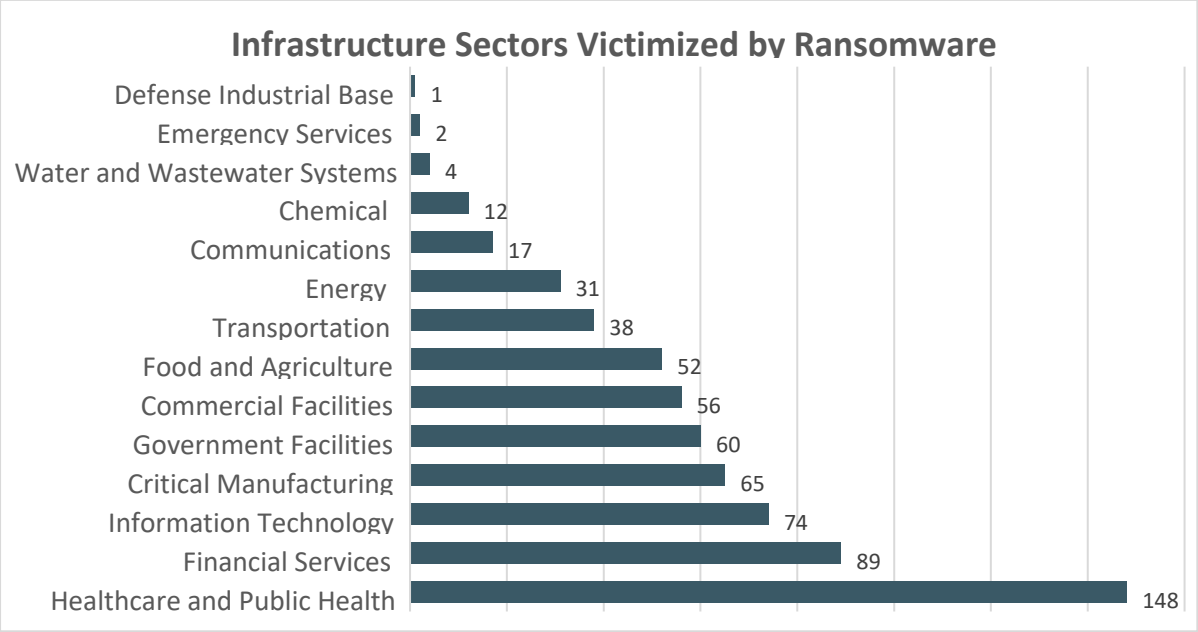
Κεφάλαιο 3 – Κυριότερες απειλές και ευπάθειες ασφάλειας για τον τομέα της Υγείας

Ο τομέας της υγείας λόγω και της μεγάλης επιφάνειας επίθεσης, όπως κατανοήθηκε στην προηγούμενη ενότητα με την ανάλυση των assets, είναι ευάλωτος σε πολλά είδη απειλών, ενώ αρκετές είναι και οι ευπάθειες λόγω του μεγέθους του. Οι κυριότερες εκ των οποίων αποτυπώνονται παρακάτω:[8],[9],[10],[28]

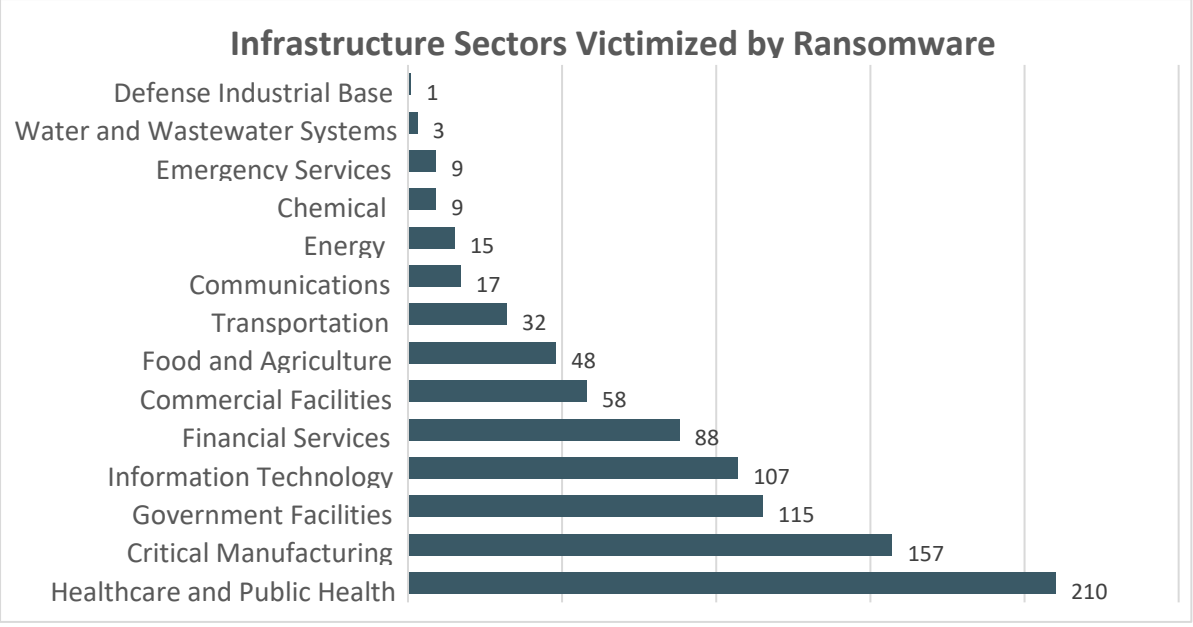
- Κακόβουλο λογισμικό (virus, malware, worms, trojans, rootkits, ransomware[32], spyware, botnets)

  Σε αυτή την κατηγορία ειδικότερα ο ransomware διαχρονικά επηρεάζει τον τομέα της υγείας περισσότερο από τις λοιπές κρίσιμες υποδομές[18],[19]. Ο ransomware WannaCry που το 2017 επηρέασε το Εθνικό Σύστημα Υγείας στο Ηνωμένο Βασίλειο επί πολλές ημέρες[2],[26],[27], η επίθεση με ransomware στο νοσοκομείο Hollywood Presbyterian Medical Center το 2016 που προκάλεσε καθυστέρηση στα χειρουργεία και έπρεπε οι ασθενείς να μεταφερθούν σε κοντινά νοσοκομεία[26], οι επιθέσεις ομοίως με ransomware τον Σεπτέμβριο του 2020 στο

Πανεπιστημιακό Νοσοκομείο του Ντίσελντορφ στη Γερμανία έχοντας ως συνέπεια την αδυναμία πρόσβασης στα συστήματα ανάγκασε το νοσοκομείο στην μεταφορά ασθενών σε άλλη δομή υγείας 30 χλμ. μακριά κάτι που προκάλεσε έμμεσο θάνατο ασθενούς εξαιτίας καθυστέρησης στην μεταφορά[38] και στο Πανεπιστημιακό Νοσοκομείο του Μπρνο στην Τσεχική Δημοκρατία το 2020 κατά την διάρκεια της πανδημίας COVID-19 που είχε ως αποτέλεσμα να αναβληθούν οι χειρουργικές επεμβάσεις[14],[16] είναι ελάχιστα παραδείγματα που καταδεικνύουν την σοβαρότητα αυτού του είδους των απειλών. Στα παρακάτω σχήματα βλέπουμε τα στατιστικά των δύο τελευταίων ετών για τις Η.Π.Α που αφορούν επιθέσεις ransomware και διαπιστώνουμε ότι ο τομέας της υγείας δέχεται τις περισσότερες επιθέσεις από όλες τις υπόλοιπες κρίσιμες υποδομές.

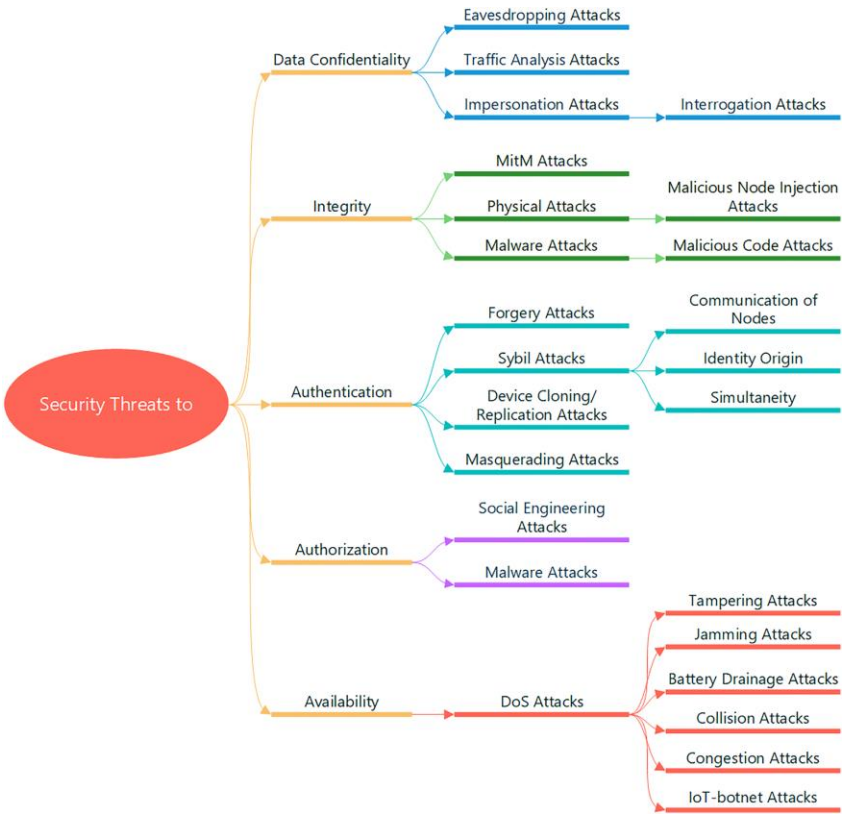


Σχήμα 3: FBI Report 2021 - Infrastructure Sectors Victimized by Ransomware.[18]



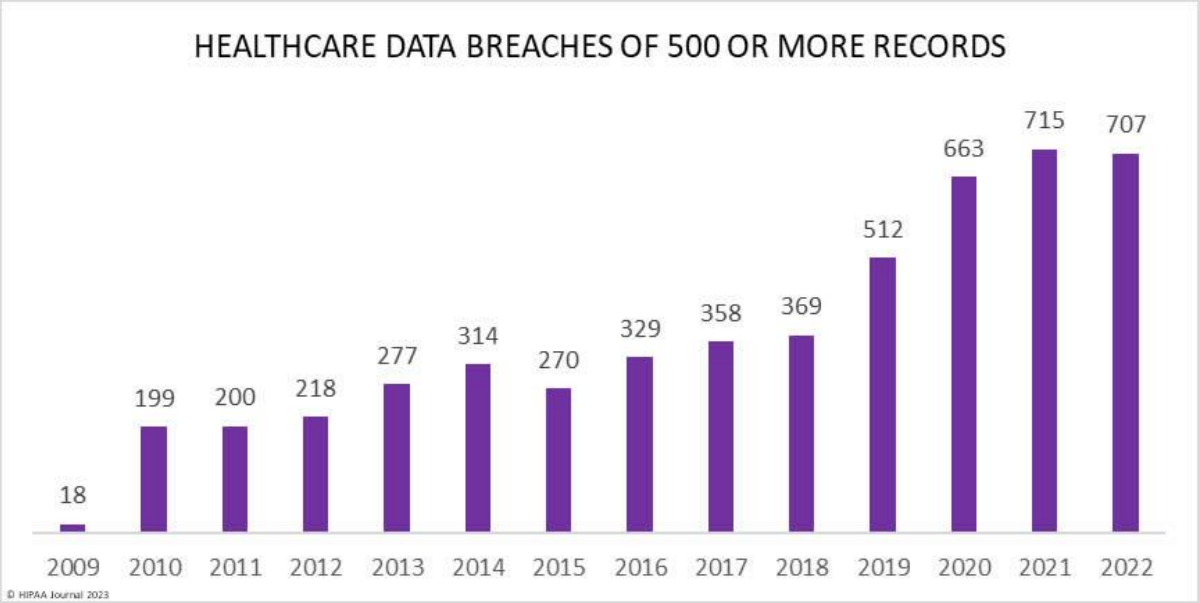
Σχήμα 4: FBI Report 2022 - Infrastructure Sectors Victimized by Ransomware.[19]

- Phishing & Social engineer: Είναι επιθέσεις που σκοπό έχουν την παραπλάνηση των χρηστών για την αποκάλυψη εμπιστευτικών πληροφοριών.[4] Κατά την διάρκεια της πανδημίας Covid-19 η επίθεση phishing κατά του Π.Ο.Υ. ήταν ένα χαρακτηριστικό παράδειγμα.[14],[16]
- Email spamming: Αυτές οι επιθέσεις πραγματοποιούν την αποστολή ανεπιθύμητης αλληλογραφίας σε χρήστες και μπορούν αυτά τα email να μετεξελιχθούν σε απειλή phishing ανάλογα με το επίπεδο εγρήγορσης και εκπαίδευσης των χρηστών.
- Επιθέσεις Web based: Η χρήση υπηρεσιών και εφαρμογών μέσω web χωρίς χρήση https πρωτοκόλλου, η καθυστέρηση στην εφαρμογή ενημερώσεων, διατήρησης της διαμόρφωσης του συστήματος χωρίς αλλαγές για σκοπούς διαλειτουργικότητας και μείωσης του χρόνου session timeout κατά το δυνατόν, διευκολύνει την εκμετάλλευση γνωστών τρωτών σημείων. Το malware injection attack είναι χαρακτηριστικό παράδειγμα τέτοιας εκμετάλλευσης αυτών των ευπαθειών.
- Επιθέσεις Web application: Είναι υποκατηγορία των web based επιθέσεων και έχουν στόχο διαδικτυακές εφαρμογές. Κυρίως το SQL injection αντιπροσωπεύει πολύ μεγάλο ποσοστό επιθέσεων για τον τομέα της υγείας.[4]
- Επιθέσεις man-in-the-middle (MiTM): Είναι επιθέσεις που μπορεί να συμβούν κατά την μετάδοση δεδομένων π.χ. σε εφαρμογές cloud, ασύρματων δικτύων, συσκευών IoMT κλπ και μπορεί να οδηγήσουν σε διαρροή δεδομένων ή και χειραγώγηση αυτών.[4]
- Επιθέσεις κατά συνδεδεμένων ιατρικών συσκευών (Internet of Medical Things - IoMT): Οι συσκευές IoMT που είναι ένα κρίσιμο κομμάτι του ψηφιακού μετασχηματισμού της υγειονομικής περίθαλψης έχουν χαμηλή ασφάλεια, παρέχοντας την δυνατότητα στους εισβολείς ευκολότερης πρόσβασης σε ευαίσθητα δεδομένα καθώς και στα δίκτυα ενός οργανισμού υγείας. Είναι ευάλωτες σε ένα μεγάλο εύρος επιθέσεων όπως μπορούμε να δούμε στο παρακάτω σχήμα:[34]



Σχήμα 5: Είδη επιθέσεων κατά συσκευών IoMT.[34]

- Απώλεια ή κλοπή εξοπλισμού: Η απώλεια ή κλοπή εξοπλισμού είναι από τις κυριότερες αιτίες που οδηγεί σε διαρροή δεδομένων.
- Διαρροή δεδομένων (Data Breach): Είναι από τις πιο επικίνδυνες επιθέσεις που μπορεί να αντιμετωπίσει ο τομέας της υγείας που οδηγεί σε πολλές επιπτώσεις. Πρωτίστως στον πληθυσμό που διέρρευσαν τα ευαίσθητα προσωπικά δεδομένα του, ενώ επιφέρει μεγάλο οικονομικό κόστος σε όλους τους εμπλεκόμενους και έχει αρνητική επίδραση στην φήμη του φορέα που δέχτηκε την επιτυχή επίθεση κλπ.

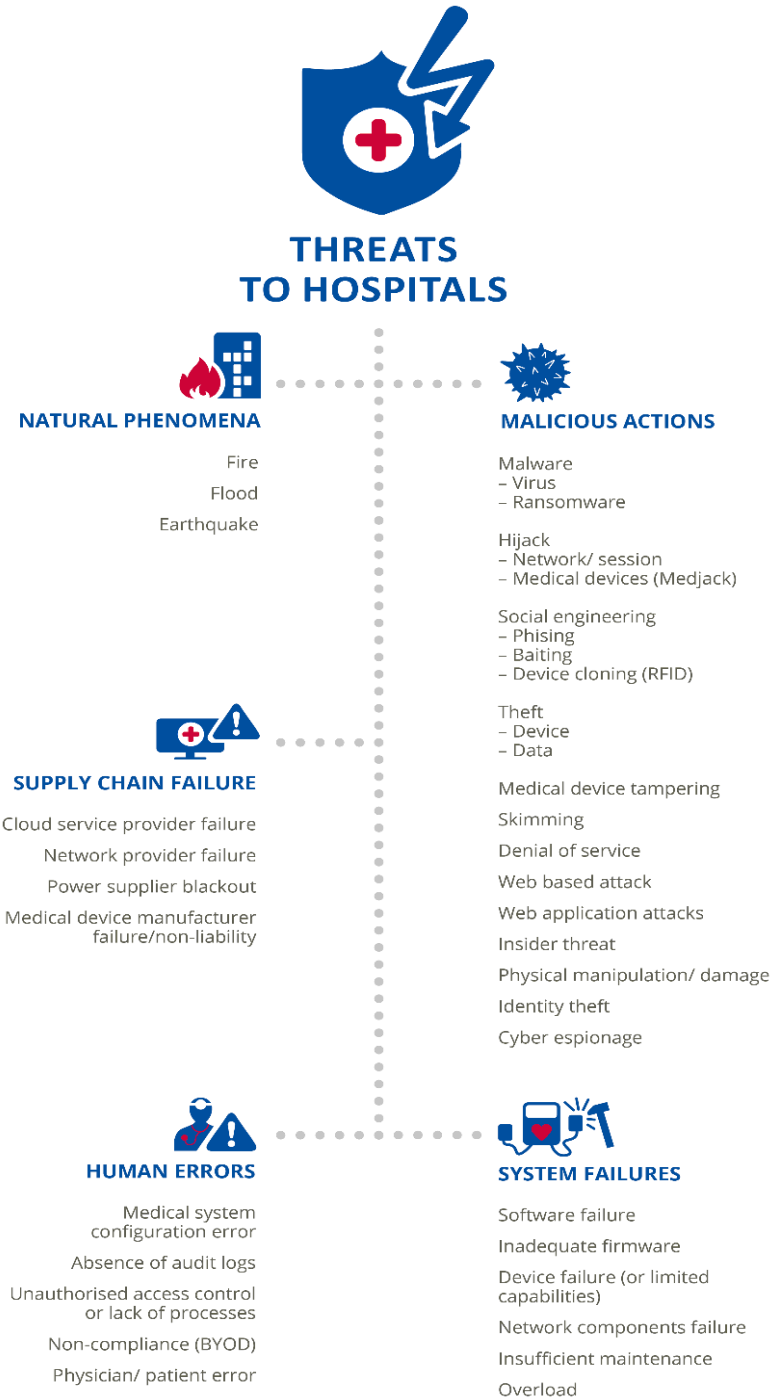


Σχήμα 6: Αναφερόμενες διαρροές δεδομένων στο Υπουργείο Υγείας των Η.Π.Α.[20]

- Επιθέσεις άρνησης υπηρεσίας (DDoS attacks): Οι επιθέσεις DDoS χρησιμοποιώντας ένα δίκτυο παραβιασμένων συστημάτων βομβαρδίζουν έναν στόχο με περισσότερη κίνηση από αυτή που μπορεί να διαχειριστεί με αποτέλεσμα να προκληθεί διακοπή των υπηρεσιών υγείας. Όπως μια επίθεση ransomware, μια επίθεση DDoS μπορεί να ζητήσει λύτρα για να επαναφέρει τις λειτουργίες ενός οργανισμού και των υπηρεσιών του.[4],[16]
- Εσωτερικές απειλές (Insider Threat): Είναι απειλές που μπορεί να προέρχονται από τον οιοδήποτε έχει πρόσβαση εσωτερικά σε έναν οργανισμό υγείας ή γνωρίζει σημαντικές παραμέτρους για την ασφάλεια αυτού. Συγκεκριμένα μπορεί να είναι είτε εργαζόμενοι νυν ή πρώην του οργανισμού ή και κάποιος εξωτερικός συνεργάτης.
- Ανθρώπινα λάθη: Οφείλονται σε ακούσιες ανθρώπινες ενέργειες, με αποτέλεσμα να βλάψουν με ποικίλους τρόπους τα συστήματα υγειονομικής περίθαλψης. Ο ανθρώπινος παράγοντας είναι ο πιο ευάλωτος κρίκος στην αλυσίδα της ασφάλειας ενός οργανισμού υγείας και η πλειοψηφία των περιστατικών ασφαλείας σχετίζονται με ανθρώπινα λάθη.
- Βλάβες συστήματος: Μπορεί να έχουν διαφορετικές αιτίες, οι πιο συνηθισμένες είναι βλάβες λογισμικού ή υλικολογισμικού, αστοχία συσκευής, αστοχία δικτύου, ανεπαρκής συντήρηση, υπερφόρτωση.
- Αστοχία εφοδιαστικής αλυσίδας: Αυτή η απειλή μπορεί να προκληθεί από τον πάροχο cloud, τον πάροχο δικτύου, τον πάροχο τροφοδοσίας ρεύματος ή από τον κατασκευαστή ιατρικών

συσκευών, ο οποίος δεν δίνει επαρκή φροντίδα στην ακεραιότητα της εφοδιαστικής αλυσίδας του.

- Φυσικά φαινόμενα: Περιλαμβάνουν πυρκαγιές, πλημμύρες, σεισμούς και άλλες φυσικές καταστροφές που μπορεί να προκαλέσουν διακοπή των υπηρεσιών υγείας.



Σχήμα 7: Γενική αποτύπωση απειλών για τον τομέα της υγείας.[10]

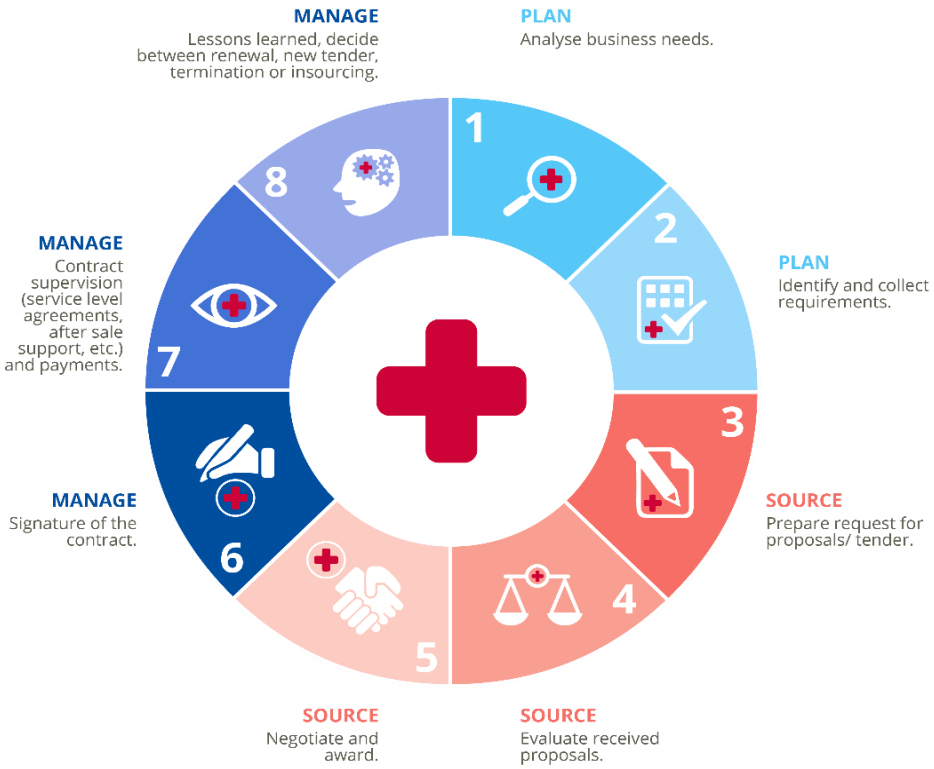
Κεφάλαιο 4 – Οργάνωση - Διαδικασίες - Μέτρα ασφαλείας

Για την αντιμετώπιση των διαφόρων απειλών και ευπαθειών μπορούν να εφαρμοστούν ορισμένες καλές πρακτικές για την προστασία των assets ενός οργανισμού παροχής υπηρεσιών υγείας. Τόσο οι φορείς υγείας όσο και οι προμηθευτές αυτών θα πρέπει να εφαρμόζουν μέτρα ασφαλείας ως καλές πρακτικές. Αυτές οι καλές πρακτικές είναι κυρίως σε δύο κατευθύνσεις. Σε οργανωτικά μέτρα που περιλαμβάνουν πολιτικές, διαδικασίες, διοικητικά εργαλεία και μεθόδους, καθώς και μέτρα για τη δημιουργία και τη διατήρηση της ευαισθητοποίησης που συνήθως εφαρμόζονται με μη αυτόματο τρόπο. Οι πολιτικές και οι διαδικασίες περιγράφουν αποδεκτές και μη αποδεκτές συμπεριφορές των εργαζομένων στο χώρο εργασίας και λειτουργούν ως εσωτερικοί οργανωτικοί κανονισμοί. Παραδείγματα διοικητικών εργαλείων και μεθόδων είναι τα προληπτικά μέσα, όπως η ταξινόμηση των περιουσιακών στοιχείων, η διαχείριση κινδύνων (Risk Management), οι έλεγχοι (audits) κλπ. Στον αντίποδα τα τεχνικά μέτρα είναι ενεργητικά μέσα. Παραδείγματα τεχνικών μέτρων είναι η χρήση τεχνολογιών όπως firewalls, network segmentation, VPNs, συστήματα IPS/IDS, χρήση κρυπτογραφίας, ενημερωμένα συστήματα, antivirus κλπ.[8],[9],10],[11]

4.1 Οργανωτικά μέτρα [8],[9],[10],[11],[16],[21],[22],[26]

- Security by design: Η ασφάλεια ολόκληρου του συστήματος ενός φορέα υγείας θα πρέπει να σχεδιάζεται και να εφαρμόζεται εξ αρχής.
- Privacy by design: Η εφαρμογή πολιτικής Privacy by design βασιζόμενη σε κανονισμούς όπως π.χ. ο GDPR της Ε.Ε.[13] ή και άλλων εθνικών κανονισμών πρέπει να είναι προϋπόθεση για την προστασία των ευαίσθητων προσωπικών δεδομένων που διαχειρίζεται κατά βάση ο τομέας της υγείας. Ακόμη η διεξαγωγή αξιολογήσεων επιπτώσεων (Data Protection Impact Assessments - DPIA) για την προστασία δεδομένων είναι επιβεβλημένη.
- Εφαρμογή προτύπων: Η εφαρμογή προτύπων[55] π.χ. της οικογένειας ISO 27000 (Information Security Management System - ISMS), ISO 20000 (Information Technology Services Management System - ITSMS), εκδόσεων του NIST (800-53 Rev.5 και 800-66 Rev.2)[21],[22] κλπ είναι εκτός από απαραίτητη και επιβαλλόμενη[29]. Ενώ και ο οιοσδήποτε εξοπλισμός που διασυνδέεται θα πρέπει να διαθέτει πιστοποιήσεις ασφαλείας.
- Ποιοτικό τμήμα Πληροφορικής στους φορείς υγείας: Για να έχει ένας οργανισμός υγείας ισχυρή κυβερνοασφάλεια, απαιτεί την ύπαρξη ποιοτικού τμήματος IT. Αν και αυτό είναι ιδιαίτερα δύσκολο να επιτευχθεί σε χώρους υγειονομικής περίθαλψης λόγω έλλειψης σε ανθρώπινους πόρους, περιορισμούς στον προϋπολογισμό και της πολυπλοκότητας των εφαρμογών ωστόσο θεωρείται κρίσιμο.
- Ανάθεση ρόλων και υπευθύνων ασφαλείας: Κάθε φορέας υγείας πρέπει να πληροί καθορισμένες απαιτήσεις ασφαλείας. Ένας CISO (Chief Information Security Officer) δύναται να αναλάβει αυτό τον ηγετικό ρόλο σε αυτή την οργανωτική ιεράρχηση.
- Δημιουργία πολιτικών και διαδικασιών ασφαλείας: Αυτές θα ορίζουν κανόνες, πρωτόκολλα, διαδικασίες και συμπεριφορές εργαζομένων με σκοπό την αποδεκτή χρήση των διαφόρων συστημάτων, τεχνολογιών και εφαρμογών. Ενώ θα πρέπει να επικαιροποιούνται τακτικά. Τέτοιες πολιτικές και διαδικασίες για παράδειγμα είναι: καθαρού γραφείου, καθαρής οθόνης, Bring your own device (BYOD)[31] κλπ.

- Δημιουργία πολιτικών προς τρίτα μέρη: Απαραίτητη είναι η δημιουργία και η εφαρμογή πολιτικών προς τρίτα μέρη, όπως για παράδειγμα της ασφάλειας ανάπτυξης εφαρμογών, των κανόνων παροχής υπηρεσιών cloud, της επεξεργασίας δεδομένων κλπ.
- Συμμετοχή του τμήματος πληροφορικής στις προμήθειες: Οι προμήθειες είναι μια βασική διαδικασία που διαμορφώνει το περιβάλλον ICT (Information and Communication Technologies) των σύγχρονων νοσοκομείων και, ως εκ τούτου, θα πρέπει να βρίσκεται στην πρώτη γραμμή όσον αφορά την επίτευξη των στόχων της κυβερνοασφάλειας.

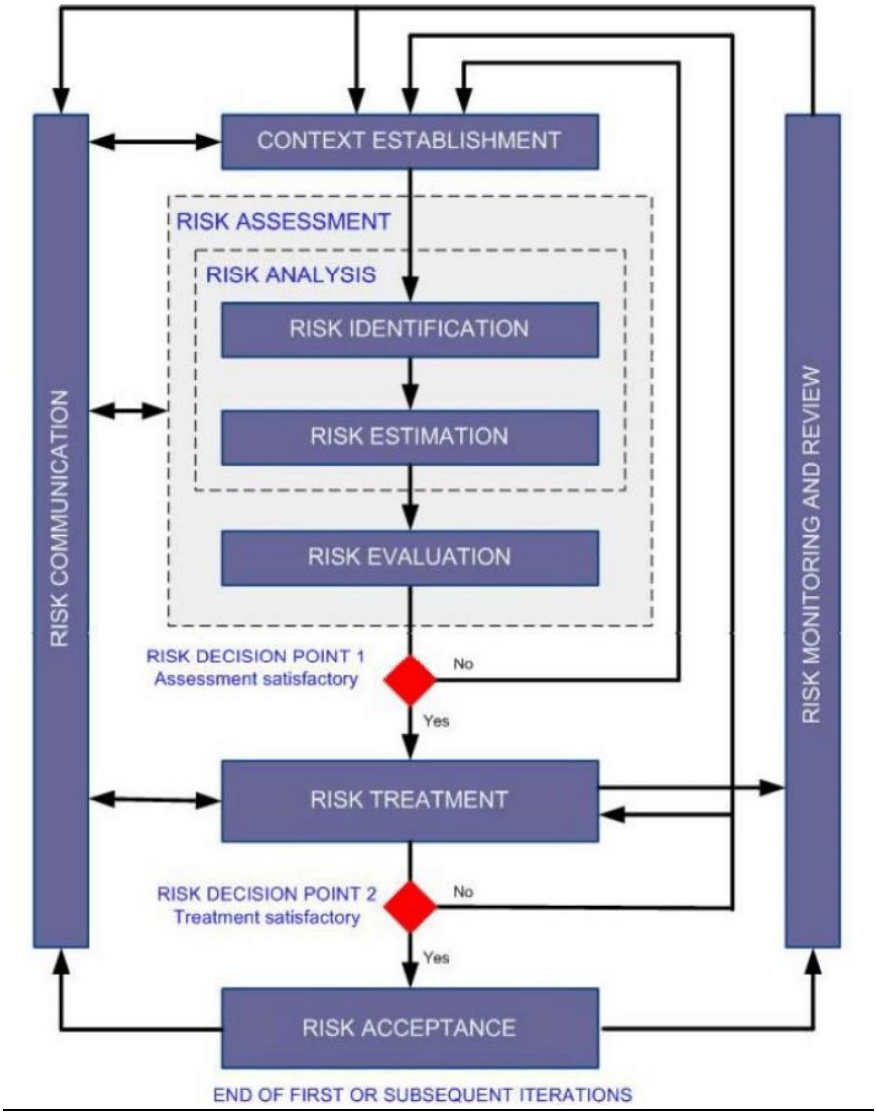


Σχήμα 8: Κύκλος ζωής της διαδικασίας προμηθειών για Νοσοκομεία.[10]

Καθ' όλη τη διάρκεια των διαφόρων φάσεων του κύκλου ζωής των προμηθειών, το νοσοκομείο θα πρέπει να διασφαλίζει ότι η κυβερνοασφάλεια θεωρείται απαίτηση για την προμήθεια εξοπλισμού, εφαρμογών ή μιας υπηρεσίας και θα πρέπει να δίνεται προτεραιότητα στην προμήθεια assets που είναι πιστοποιημένα σύμφωνα με πρότυπα κυβερνοασφάλειας.

- Έλεγχος κύκλου ζωής εξοπλισμού, εφαρμογών και υπηρεσιών: Η δημιουργία και εφαρμογή στρατηγικής κύκλου ζωής για κάθε σύστημα ενός οργανισμού υγείας είναι απαραίτητη.
- Διαλειτουργικότητα συστημάτων: Πρέπει να λαμβάνεται υπ' όψιν η διαλειτουργικότητα, διότι είναι ένας από τους μεγαλύτερους κινδύνους για την ασφάλεια στον κυβερνοχώρο του τομέα υγείας. Το οικοσύστημα πληροφορικής ενός νοσοκομείου αποτελείται από διαφορετικά συστήματα, εφαρμογές, εξοπλισμό κλπ. Ορισμένα από αυτά τα στοιχεία υπάρχουν ήδη σε έναν οργανισμό υγείας και η σύνδεση με νέα στοιχεία ενδέχεται να οδηγήσει σε κενά ασφαλείας.
- Πραγματοποίηση τακτικά Risk Assessment: Είναι πολύ σημαντική διαδικασία για τον προσδιορισμό των κινδύνων, των assets, των απειλών, των ευπαθειών και των επιπτώσεων που μπορεί να υπάρξουν για τους φορείς υγείας, έτσι ώστε να ληφθούν έγκαιρα τα

κατάλληλα αντίμετρα. Ιδιαίτερη προσοχή πρέπει να δοθεί στον εντοπισμό νέων απειλών, στον εντοπισμό αλλαγών στα τρωτά σημεία και στην γρήγορη και αποτελεσματική λήψη αντιμέτρων.



Σχήμα 9: Διάγραμμα διαδικασίας Risk Management.[25]

- Διενέργεια penetration tests: Είναι πολύ σημαντική διαδικασία που πρέπει να πραγματοποιείται τακτικά για την διαπίστωση ευπαθειών και τρωτών σημείων.
- Καθιέρωση σχεδίων επιχειρηματικής συνέχειας (Business Continuity) και επαναφοράς από καταστροφή (Disaster Recovery): Η συνεχής παροχή υπηρεσιών υγείας στους ασθενείς αποτελεί μείζον μέλημα. Η ανάπτυξη ενός σχεδίου έκτακτης ανάγκης είναι πολύ σημαντική, έτσι ώστε να διασφαλίζεται η διαθεσιμότητα των συστημάτων και η ανάκαμψη από περιστατικά. Το σχέδιο έκτακτης ανάγκης θα πρέπει να προσδιορίζει τις βασικές λειτουργίες του νοσοκομείου και τις σχετικές απαιτήσεις έκτακτης ανάγκης. Θα πρέπει επίσης να καθορίζει ρόλους έκτακτης ανάγκης και ευθύνες που θα είναι ανατεθειμένα σε άτομα με στοιχεία επικοινωνίας, καθώς και την αποκατάσταση συστημάτων και την εφαρμογή εναλλακτικών διαδικασιών όταν τα συστήματα διακυβεύονται. Βασική προϋπόθεση

προκειμένου να επιτευχθεί η επιχειρηματική συνέχεια είναι η τακτική διαδικασία δημιουργίας αντιγράφων ασφαλείας δεδομένων, λογισμικού, configuration files εξοπλισμού τα οποία θα πρέπει να φυλάσσονται σε ασφαλές μέρος. Αυτό θα επιτρέψει τη γρήγορη ανάκτηση της υποδομής σε περίπτωση καταστροφής.

- Εφαρμογή καταγραφής (Logging): Η διατήρηση ασφαλών αρχείων καταγραφής από κάθε εφαρμογή και σύστημα είναι ένα από τα πιο σημαντικά καθήκοντα ασφάλειας, αν και η απουσία τους δεν θέτει σε κίνδυνο την ήδη εφαρμοσμένη ασφάλεια. Είναι όμως πολύ σημαντικά για την αντιμετώπιση προβλημάτων και τον εντοπισμό του τρόπου παραβίασης εφ' όσον έχει επιτευχθεί. Θα πρέπει να τηρούνται και αντίγραφα των αρχείων καταγραφής σε ασφαλή τοποθεσία.
- Διενέργεια ελέγχων (Auditing): Προετοιμασία και διενέργεια συχνά έλεγχων ασφαλείας εσωτερικά, αλλά και από ανεξάρτητους συμβούλους. Συνήθως οι έλεγχοι από εξωτερική οπτική γωνία αποδεικνύουν τη συμμόρφωση με ένα πρότυπο, κανονισμό ή μια οδηγία.
- Εκπαίδευση και ευαισθητοποίηση: Καθώς οι άνθρωποι είναι ο πιο αδύναμος κρίκος στην κυβερνοασφάλεια, η ανάγκη για τακτική εκπαίδευση και η ευαισθητοποίηση όλων των χρηστών, ανάλογα με την διαβάθμιση τους, ενός οργανισμού υγείας, αλλά και τρίτων μερών για θέματα ασφαλείας, ορθής χρήσης, καλών πρακτικών κλπ είναι πολύ σημαντική.
- Καθιέρωση διαδικασιών για τη διαχείριση περιστατικών ασφαλείας: Είναι βασική η ανάπτυξη σχεδίου απόκρισης και εφαρμογής διαδικασιών σε περίπτωση περιστατικού κυβερνοασφάλειας, στο οποίο θα καθορίζονται ρόλοι και ευθύνες στο προσωπικό του οργανισμού υγείας.
- Συμμετοχή στην ανταλλαγή πληροφοριών: Η συμμετοχή ενός οργανισμού υγείας σε μία ένωση οργανισμών παροχής υπηρεσιών υγείας και η κοινή χρήση πληροφοριών για την ασφάλεια στον κυβερνοχώρο μεταξύ αυτών των οργανισμών είναι πολύ σημαντικό. Η έγκαιρη γνώση για νέες ευπάθειες και απειλές οδηγούν σε λήψη μέτρων πιο άμεσα.
- Χρήση δοκιμασμένων λύσεων: Είναι καλή πρακτική η χρήση εφαρμοσμένων λύσεων, όπως ανθεκτικών αλγορίθμων κρυπτογράφησης, πρωτοκόλλων επικοινωνίας κλπ.

4.2 Τεχνικά μέτρα [8],[9],[11],[16],[21],[22],[26]

Παρακάτω αναφέρονται βασικά τεχνικά μέτρα ασφάλειας που πρέπει να εφαρμόζονται:

- Έλεγχος πρόσβασης σε συστήματα και εφαρμογές (Authentication and Identification):
  - Χρήση δικαιωμάτων administrator με διαδικασία multi-factor authentication (MFA), ισχυρών κριτηρίων πρόσβασης και όχι χρήσης του σε διαδικασίες ρουτίνας.
  - Δημιουργία protected groups για τους λογαριασμούς χρηστών με αυξημένα δικαιώματα.
  - Χρήση τοπικών λογαριασμών administrator όταν απαιτείται και αποφυγή χρήσης enterprise ή domain admin.
  - Η πιστοποίηση και η πρόσβαση χρηστών να διασφαλίζεται μέσω διαδικασίας MFA.

- Φυσική ασφάλεια:
  - Είσοδος μόνο πιστοποιημένου προσωπικού στα CR και μέσω συστημάτων Access Control.
  - Παρακολούθηση περιβαλλοντικών δεικτών (υγρασία, τάση, θερμοκρασία κλπ.).

- Εγκατάσταση αυτόματου συστήματος πυρανίχνευσης – πυρασφάλειας.
- Εγκατάσταση συστημάτων αδιάλειπτης παροχής ισχύος σε κρίσιμες υποδομές (CR, κατανεμητές δικτύωσης).
- Κλείδωμα και μη εύκολη πρόσβαση σε κατανεμητές δικτύωσης πέραν του εξουσιοδοτημένου προσωπικού.
- Ενεργοποίηση μόνο των χρησιμοποιούμενων θυρών στους κατανεμητές δικτύωσης.
- Εφαρμογή μέτρων προστασίας στην καλωδίωση από υποκλοπές, παρεμβολές ή ζημιές.
- Παρακολούθηση σύνδεσης εξωτερικών συσκευών αποθήκευσης.

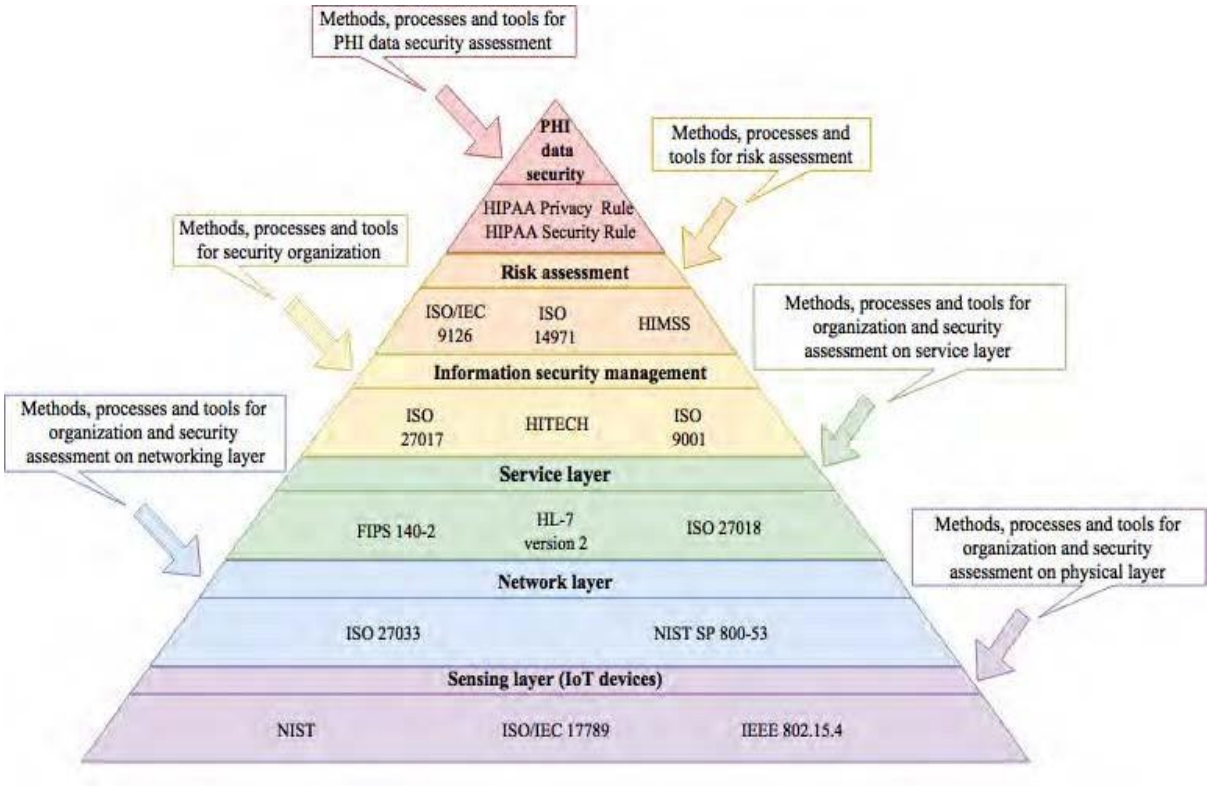
- <u>Συντήρηση συστημάτων και ενημερώσεων:</u>
  - Εφαρμογή ενημερώσεων στα λειτουργικά συστήματα, στις διάφορες εφαρμογές, στο υλικολογισμικό εξοπλισμού και στο λογισμικό προστασίας από ιούς.
  - Τακτική συντήρηση εξοπλισμού και έλεγχος ορθής λειτουργίας του.

- <u>Ασφάλεια δεδομένων:</u>
  - Τα δεδομένα στον πάροχο υπηρεσιών Cloud θα πρέπει να είναι κρυπτογραφημένα καθ' όλη τη διάρκεια του κύκλου ζωής αυτών (δημιουργία, αποθήκευση, χρήση, κοινή χρήση, μετάδοση, αρχειοθέτηση, διαγραφή).
  - Όλες οι κινητές συσκευές που περιέχουν προσωπικές ιατρικές πληροφορίες και ευαίσθητα προσωπικά δεδομένα θα πρέπει να προστατεύονται με κρυπτογράφηση, ενώ το λογισμικό δεν θα πρέπει να εγκαθίσταται χωρίς προηγούμενη συγκατάθεση.
  - Εφαρμογή κρυπτογράφησης όπου αυτό είναι εφικτό, τόσο κατά την μετάδοση, όσο και κατά την αποθήκευση των δεδομένων του φορέα υγείας (π.χ. σε βάσεις δεδομένων, αποθηκευτικές μονάδες, πιστοποιητικών ασφαλείας κλπ).
  - Λειτουργία λογισμικού Data Loss Prevention (DLP).
  - Δημιουργία σε τακτική βάση και τήρηση κρυπτογραφημένων - πιστοποιημένων αντιγράφων ασφαλείας σε ασφαλή χώρο και διαφορετικής γεωγραφικής θέσεως.
  - Περιοδικός έλεγχος των παραγόμενων αντιγράφων ασφαλείας με προσεκτική παρακολούθηση και καταγραφή των αποτελεσμάτων των ελέγχων.
  - Όλοι οι χρήστες, οι ασθενείς, οι γιατροί και οι υπάλληλοι του νοσοκομείου θα πρέπει να έχουν το ελάχιστο επίπεδο προνομίων που είναι απαραίτητο για να μπορέσουν να εκτελέσουν με απρόσκοπτο τρόπο όλο το εύρος των εργασιακών τους αρμοδιοτήτων.
  - Καθορισμός, με αδιάβλητο τρόπο του χρονικού πλαισίου των πληροφοριακών των συστημάτων.
  - Θέσπιση και εφαρμογή κανόνων για την ασφαλή ανάπτυξη λογισμικού, αλλά και διαδικασιών, ελέγχου πριν και κατά την διάρκεια λειτουργίας τους.

- <u>Ασφάλεια περιμέτρου:</u>
  - Firewall NG με IPS/IDS συστήματα, monitoring κίνησης δικτύου, έλεγχοι geolocation.
  - Εφαρμογή τεχνικών network segmentation.
  - Χρήση DMZ (Demilitarized Zone).
  - Χρήση Honeypot για την ανίχνευση παραβιάσεων.
  - Προστασία Endpoint έναντι ιών (Antivirus/Antimalware).
  - Εφαρμογή Web filtering για προσπέλαση σε ιστοσελίδες και εφαρμογή μόνο μέσω ασφαλών πρωτοκόλλων.

- Η πρόσβαση στα δίκτυα Wi-Fi θα πρέπει να είναι περιορισμένη και αυστηρά ελεγχόμενη. Ο αριθμός των συνδεδεμένων συσκευών θα πρέπει να παρακολουθείται και στην περίπτωση των συσκευών IoMT θα πρέπει να επαληθεύεται και να περιορίζεται (MacAddress filtering). Μη εξουσιοδοτημένη συσκευή δεν πρέπει να έχει πρόσβαση στο Wi-Fi.
- Χρήση Access Control Lists (ACLs).
- Το προσωπικό που εργάζεται μέσω τηλεργασίας θα πρέπει να συνδέεται μόνο μέσω Virtual Private Network (VPN) με υψηλή κρυπτογράφηση και με διαδικασία MFA.

Όσον αφορά τις συσκευές IoMT που έχουν φέρει επανάσταση και στον τομέα της υγειονομικής περίθαλψης, αλλά ταυτόχρονα και πολυποίκιλες προκλήσεις ασφαλείας παρέχεται ένα ανεπτυγμένο κανονιστικό ιεραρχικό μοντέλο από διεθνή πρότυπα κυβερνοασφάλειας.[37],[40] Επίσης συστάσεις για την αντιμετώπιση των προκλήσεων, μετριασμού του κινδύνου για την ασφάλεια στον κυβερνοχώρο και διασφάλισης του απορρήτου για τις συσκευές IoT προσφέρει η έκδοση του NIST IR.8228: Considerations for Managing Internet of Things (IoT) Cybersecurity and Privacy Risks[33]. Τέλος οι συσκευές IoMT πρέπει να δοκιμάζονται πριν από την ανάπτυξη ως προς τη συμμόρφωσή τους με τα πρότυπα ασφαλείας, όπως το ISO/IEC 82304: Health Software, το ISO/IEC 62304: Medical Device Software και άλλα σχετικά πρότυπα προϊόντων υγείας[41].



Σχήμα 10: Ιεραρχικό μοντέλο κυβερνοασφάλειας για συσκευές IoMT.[40]

Κεφάλαιο 5 – Security Defense Models

Στον τομέα της Υγειονομικής Περίθαλψης, ο οποίος είναι ένας από τους τομείς ζωτικής σημασίας και συνεχώς εξελισσόμενος δύο ευρέως διαδεδομένα μοντέλα ασφάλειας μπορούν να βρουν εφαρμογή. Αυτά είναι το μοντέλο Defense-in-Depth (DID) και το μοντέλο Zero Trust (ZT). Τα μοντέλα αυτά παρέχουν μια ολοκληρωμένη προσέγγιση σε θέματα ασφαλείας πληροφοριακών υποδομών και θα αναλυθούν στην συνέχεια. Η χρήση αυτών καθορίζεται από την πολυπλοκότητα του κάθε οργανισμού υγείας, ο οποίος καλείται να επιλέξει για την μεμονωμένη ή συνδυαστική χρήση τους. Η επιλογή του οργανισμού για μεμονωμένη ή συνδυαστική χρήση συμβάλει στην αύξηση της ασφάλειας, αλλά και στην πολυπλοκότητα διαχείρισης των πληροφοριακών υποδομών.

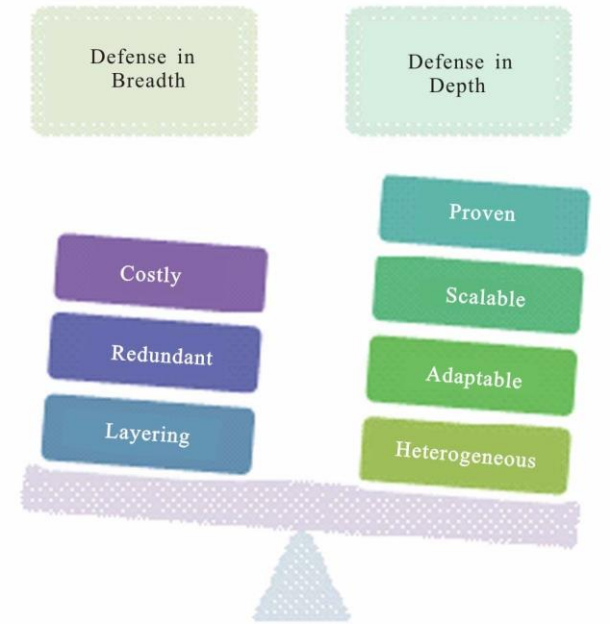
5.1 Defense-in-Depth Model

Το μοντέλο Defense-in-Depth (άμυνα σε βάθος) αρχικά αναπτύχθηκε από την National Security Agency (NSA) και άρχισε να γίνεται δημοφιλές στις αρχές του 2000, έχοντας ως σκοπό την παροχή ενός βαθύτερου επιπέδου προστασίας με βάση την άμυνα των επιπέδων, αυξάνοντας βαθμιαία την ασφάλεια του δικτύου. Η προσέγγιση ασφαλείας αυτού του μοντέλου είναι ολιστική με σκοπό την προστασία όλων των assets, ενώ παράλληλα λαμβάνει υπόψη τις διασυνδέσεις και τις εξαρτήσεις, χρησιμοποιώντας τους διαθέσιμους πόρους ενός οργανισμού για την παροχή αποτελεσματικών επιπέδων παρακολούθησης και προστασίας με βάση την έκθεση της επιχείρησης σε κινδύνους ασφάλειας στον κυβερνοχώρο. Η ανάπτυξη του μοντέλου DID ξεκινά με την χαρτογράφηση της αρχιτεκτονικής των συστημάτων, διότι αυτό εν συνεχεία επιτρέπει στον οργανισμό να λαμβάνει πιο αποτελεσματικά αντίμετρα ασφαλείας, να κατανοεί πιο εύκολα τα συμβάντα ασφαλείας και να διευκολύνει τους διαχειριστές στο να γνωρίζουν τι είναι αυτό που χρήζει προστασίας. Η εφαρμογή των μέτρων πρέπει να είναι στο υψηλότερο δυνατό επίπεδο ασφάλειας, επιτρέποντας παράλληλα την αδιάλειπτη λειτουργικότητα. Δημιουργεί πολυεπίπεδα εμπόδια μεταξύ των εισβολέων και των πληροφοριακών πόρων ενός φορέα, ενώ όσο πιο βαθιά θέλουν να διεισδύσουν οι επιτιθέμενοι στο σύστημα, τόσο μεγαλύτερες δυσκολίες θα αντιμετωπίσουν. Αυτά τα εμπόδια εμποδίζουν τους εισβολείς από το να επιτεθούν σε σημαντικούς πόρους του συστήματος και επίσης αποτρέπουν τους εισβολείς από την αναγνώριση της αρχιτεκτονικής του δικτύου. Η άμυνα σε βάθος είναι το άθροισμα όλων των μέτρων σε κάθε επίπεδο, ενώ και τα στρώματα εμποδίων που εφαρμόζονται είναι επικαλυπτόμενα, έτσι ώστε αυτά να καλύπτουν τις ελλείψεις του ενός στρώματος από το άλλο. Συνήθως η άμυνα σε βάθος είναι μια αποτελεσματική μέθοδος μετριασμού των συνεπειών μιας παραβίασης και πρόληψης αυτόματων επιθέσεων που μπορεί να αντιμετωπίσει ένας οργανισμός. Μια καλά καθορισμένη και καλά εφαρμοσμένη στρατηγική άμυνας σε βάθος μπορεί να αποτρέψει μια μεγάλη ποικιλία επιθέσεων, ενώ δημιουργεί συναγερμούς εισβολής σε πραγματικό χρόνο προς τους διαχειριστές. Κάθε επίπεδο του μοντέλου Defense-in-Depth έχει την δική του υλοποίηση και διαχείριση, έχοντας και τα αντίστοιχα κόστη. Οι οργανισμοί επιβάλλεται να προσαρμόζουν και να βελτιώνουν συνεχώς τα αντίμετρα ασφαλείας για να διασφαλίζουν την προστασία από γνωστές και αναδυόμενες απειλές, ενώ και το ίδιο το μοντέλο βοηθά σε αυτή την κατεύθυνση όντας επεκτάσιμο από την φύση του. Ένα μοντέλο DID δεν θα πρέπει να αποτελείται από τις παραδοσιακά στατικές άμυνες που επικεντρώνονται στην αποτροπή επιθέσεων από την είσοδο σε ένα δίκτυο, ενεργοποιώντας τις δυνατότητες αποκλεισμού πρόσβασης, αλλά και απαιτώντας π.χ. έλεγχο ταυτότητας ή αναλύοντας την κυκλοφορία. Πρέπει να είναι και συμμετρικό επιτρέποντας στο αμυντικό σύστημα δικτύου να αναγνωρίζει εσωτερικές απειλές, ενώ επίσης πρέπει να

ενεργοποιηθούν δυναμικές άμυνες (Moving Target Defense - MTD), οι οποίες αυξάνουν τις επιφάνειες επίθεσης υπερασπίζοντας προληπτικά ένα δίκτυο, αναγκάζοντας τους επιτιθέμενους να ξοδεύουν το μεγαλύτερο μέρος του χρόνου τους στο στάδιο σχεδιασμού της επίθεσης τους, την οποία θα δυσκολεύονται να εκτελέσουν, αφού αντίστοιχα θα μειώνεται το χρονικό διάστημα που θα έχουν για να εκμεταλλευτούν τις όποιες ευπάθειες και τρωτά σημεία.[64],[65],[69],[70],[73],[74]

Το μοντέλο DID έχει ορισμένα χαρακτηριστικά που μπορούν να θεωρηθούν και ως παραλλαγές βασικότερες εκ των οποίων είναι οι:

- Defense-in-Breadth (άμυνα σε πλάτος): Το Defense in Breadth δεν είναι μια πλήρως ανεπτυγμένη μεθοδολογία, αλλά είναι απλώς μια ενημερωμένη έκδοση του μοντέλου DID. Η βασική ιδέα για την δημιουργία της παραλλαγής Defense-in-Breadth είναι η διασφάλιση, ότι οι κοινοί φορείς επιθέσεων που δεν αντιμετωπίζονται από μια τεχνολογία θα αντιμετωπιστούν από μια άλλη μέσω της εφαρμογής ετερογενών τεχνολογιών ασφάλειας. Η άμυνα σε πλάτος έχει προληπτική προσέγγιση αντιμετώπισης κακόβουλων δραστηριοτήτων, καθώς και δημιουργίας ωφέλιμης χρονοκαθυστέρησης στον οργανισμό έναντι σε επιθέσεις. Ορισμένοι αμυντικοί μηχανισμοί που βρίσκουν εφαρμογή σε αυτή την παραλλαγή είναι η εξαπάτηση των εισβολέων (π.χ. με honeypots) και οι κινούμενες άμυνες (Moving Target Defense - MTD) (π.χ. Address Space Randomization). Στο σχήμα 11 μπορούμε να δούμε συμπερασματικά ορισμένα από τα πιο προφανή πλεονεκτήματα και αδυναμίες των μοντέλων άμυνας δικτύου Defense-in-Breadth και Defense-in-Depth. [69],[73],[74]



Σχήμα 11: Πλεονεκτήματα και αδυναμίες των μοντέλων άμυνας δικτύου Defense-in-Breadth και Defense-in-Depth.[69]

- Protection-in-Depth (προστασία σε βάθος): Η προστασία σε βάθος αναφέρεται στην χρήση πολλαπλών διαφορετικών μεμονωμένων στοιχείων, τα οποία έχουν σχεδιαστεί για να ανιχνεύουν, να καθυστερούν και να ανταποκρίνονται σε ενέργειες του επιτιθεμένου συνθέτοντας ένα ειδικό επίπεδο ασφάλειας που χωρίζει δύο διαφορετικές ζώνες ασφαλείας.[70]
- Security-in-Depth (ασφάλεια σε βάθος): Η ασφάλεια σε βάθος αναφέρεται σε μια ολιστική προσέγγιση για την προστασία των assets, όπου με βάση τις απειλές που αποτελούν κίνδυνο

σε έναν οργανισμό εφαρμόζονται διαφορετικά επίπεδα και επίπεδα ελέγχων ασφαλείας, έτσι ώστε να διασφαλιστεί ότι η πρόσβαση σε ένα προστατευμένο περιουσιακό στοιχείο περιορίζεται σε αυτή όπου υπάρχουν νόμιμα δικαιώματα πρόσβασης.[70]

Τα επίπεδα της άμυνας σε βάθος σχηματικά αποτυπώνονται στο σχήμα 12 και κατηγοριοποιούνται ως κάτωθι:

- Πολιτικές και Διαδικασίες Ασφαλείας: Στο πρώτο επίπεδο άμυνας καθορίζονται από τον οργανισμό τα σημεία αναφοράς, ορίζονται οι διαδικασίες, οι πολιτικές, τα πρότυπα, το νομικό πλαίσιο (νόμοι, κανονισμοί, οδηγίες), καθώς και οι βέλτιστες πρακτικές που θα εφαρμοστούν. Σε αυτή την κατηγορία βασικό ρόλο διαδραματίζει η εκπαίδευση και η ευαισθητοποίηση του προσωπικού ενός οργανισμού σε θέματα ασφαλείας. Πρότυπα που μπορούν να εφαρμοστούν είναι κυρίως από τον Διεθνή Οργανισμό Τυποποίησης (ISO) με βασικότερη την σειρά προτύπων 27000 (Information security management systems - ISMS), των εκδόσεων του NIST (National Institute of Standards and Technology) που αφορούν τα framework κυβερνοασφάλειας, όπως π.χ. το SP 800-53, το πλαίσιο COBIT (Control Objectives for Information and Related Technologies) από τον ISACA κλπ. Στο σχήμα 13 βλέπουμε μια αποτύπωση ορισμένων μόνο βασικών πλαισίων που μπορούν να βρουν εφαρμογή. Όσον αφορά την ιδιωτικότητα βρίσκουν εφαρμογή νόμοι-κανονισμοί, όπως π.χ. ο GDPR, καθώς και άλλα διεθνή ή εθνικά νομικά πλαίσια.[64],[67],[68],[75]

- Φυσική Ασφάλεια: Τα μέτρα φυσικής ασφάλειας μειώνουν τον κίνδυνο τυχαίας ή σκόπιμης απώλειας ή ζημιάς στα περιουσιακά στοιχεία ενός οργανισμού, ενώ αυτά δεν αφορούν μόνο την ασφάλιση θυρών περιμετρικά και εσωτερικά του οργανισμού ακόμα και με φυσική παρουσία, αλλά επίσης περιλαμβάνουν την εφαρμογή ποικίλων μέτρων ασφαλείας για τον χώρο του Computer Room, λοιπών υποδομών (π.χ. κατανεμητών δικτύωσης, καλωδίωσης κλπ), λοιπού εξοπλισμού (H/Y, laptops, tablets, συσκευών IoMT κλπ), καθώς επίσης και του ανθρώπινου παράγοντα.[64]

- Ασφάλεια Δικτύου και Περιμέτρου: Η περίμετρος είναι η κύρια διεπαφή ενός οργανισμού με τον έξω κόσμο, ενώ το δίκτυο είναι το επίπεδο που χωρίζει το δίκτυο της επιχείρησης σε θύλακες. Η διαλειτουργικότητα των διαφόρων στοιχείων ενός δικτύου είναι βασικός παράγοντας για την ορθή λειτουργία του συνόλου. Η ασφάλεια του δικτύου ξεκινά με την κάλυψη της αρχιτεκτονικής του έναντι γνωστών και προφανών επιθέσεων.
  Η περιμετρική κυκλοφορία και η ασφάλεια ενός δικτύου πρέπει τουλάχιστον:
  - να φιλτράρεται από τείχη προστασίας (firewalls) και να γίνεται αποκλεισμός επικίνδυνου περιεχόμενου βάσει ενός συνόλου κανόνων.
  - να υπάρχει εφαρμογή τεχνολογιών, όπως Σύστημα Ανίχνευσης Εισβολής (Intrusion Detection System – IDS) και Σύστημα Πρόληψης Εισβολής (Intrusion Prevention System - IPS).
  - να υπάρχουν τεχνολογίες αναγνώρισης και αποκλεισμού κακόβουλου λογισμικού.
  - για απομακρυσμένη πρόσβαση να εφαρμόζονται πρωτόκολλα VPN και αυθεντικοποίηση.
  - να υλοποιούνται τεχνικές network segmentation (Virtual lans, subnetting κλπ)
  - να υπάρχουν αποστρατικοποιημένες ζώνες (Demilitarized Zone – DMZ) στις οποίες θα εκτίθενται οι εξωτερικές υπηρεσίες, όπως π.χ. ηλεκτρονικό ταχυδρομείο, web servers,

honeypots, proxy servers και άλλες δημόσιες συσκευές με σκοπό να κρατούν τους χρήστες/επισκέπτες/κακόβουλους εισβολείς που δεν χρειάζεται να βρίσκονται μέσα στον οργανισμό, έξω από αυτόν.

- να υπάρχει μηχανισμός εξαπάτησης κακόβουλων εισβολέων (Honeypots).
- να υπάρχει σύστημα για αποτροπή απώλειας δεδομένων ή αποτροπή διαρροής δεδομένων (Data Loss Prevention – DLP).

Ακόμη είναι σημαντικό να κατανοήσουμε τι μπορεί να αντιμετωπίσει ένα δίκτυο στην περίμετρο του όσον αφορά τις επιθέσεις και τις απειλές. Τέλος, όταν είναι ορθώς παραμετροποιημένη η ασφάλεια περιμετρικά του δικτύου, τότε μπορεί να υπάρχει προστασία επιτρέποντας μόνο εκείνες τις δραστηριότητες που απαιτούνται για τη λειτουργία του οργανισμού και ταυτόχρονα να αποτρέπει, να καθυστερεί, να απορροφά, να ανιχνεύει επιθέσεις, μειώνοντας έτσι τον κίνδυνο για κρίσιμα συστήματα back-end.[64],[69],[75]

- Παρακολούθηση και Καταγραφή Συμβάντων (Monitoring and Logging): Η αρχιτεκτονική ασφαλείας του μοντέλου DID, εάν δεν υπάρχει κατάλληλο σύστημα παρακολούθησης και καταγραφής, τότε παραμένει ελλιπής. Οι διάφορες λειτουργίες του δικτύου και των συστημάτων πρέπει να παρακολουθούνται συνεχώς για ενδείξεις ενδεχόμενης εισβολής, ενώ δεν θα πρέπει απλώς να γίνεται ανάλυση των αρχείων καταγραφής, αλλά με τη σωστή εφαρμογή της παρακολούθησης των ελέγχων ασφαλείας να δημιουργηθούν αποτελεσματικές ειδοποιήσεις και συναγερμοί. Ακόμη, οι διαχειριστές πρέπει να ελέγχουν τα κρίσιμα αρχεία καταγραφής σε καθημερινή βάση για να ανιχνεύουν προηγμένες εισβολές ή απειλές στο σύστημα. Η λειτουργία σε ένα οργανισμό συστημάτων SIEM (Security Information and Event Management), SOC (Security Operations Center), NOC (Network Operations Center) κρίνεται επιβεβλημένη για αυτοματοποίηση διαδικασιών, ανάλυσης σε πραγματικό χρόνο του μεγάλου όγκου πληροφορίας και υποβοήθησης των διαχειριστών.[64],[75]

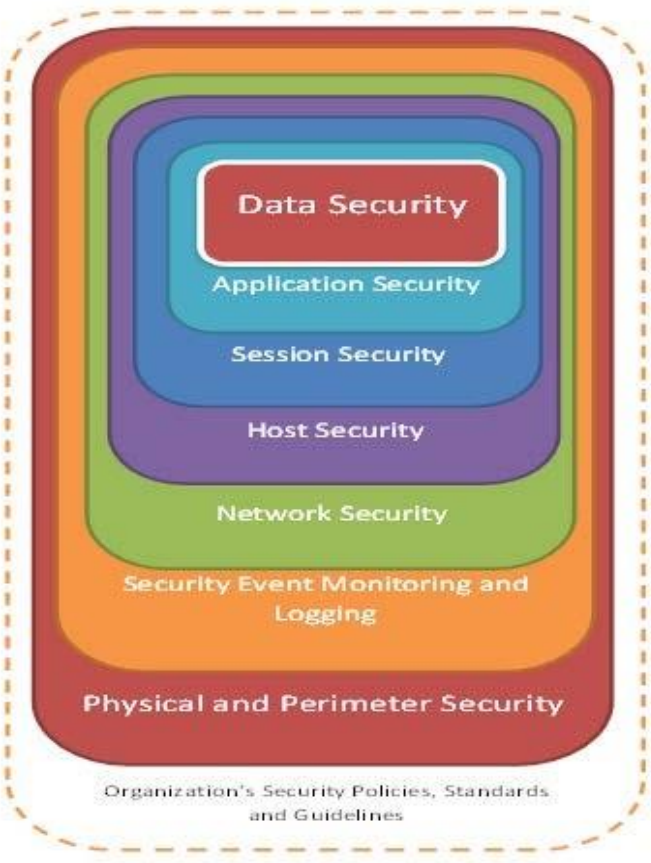
- Ασφάλεια Υπολογιστικών Συστημάτων (Hosts or Endpoint Security): Είναι τα τελικά σημεία (συσκευές - υπολογιστικά συστήματα) που διασυνδέονται με έναν οργανισμό. Η ασφάλεια των υπολογιστικών συστημάτων ενός οργανισμού είναι πολύ σημαντική, όπως είναι και του δικτύου στην αρχιτεκτονική ασφάλειας. Ενημερωμένα συστήματα Antivirus και anti-malware, μηχανισμοί ανίχνευσης και πρόληψης εισβολής υπολογιστικών συστημάτων (IDS/IPS), τείχη προστασίας που βασίζονται σε κεντρικό υπολογιστή και λειτουργούν στα τερματικά, patching και διαχείριση ευπαθειών, σύστημα DLP, virtual machines και σκλήρυνση των λειτουργικών συστημάτων πρέπει να βρίσκουν εφαρμογή τουλάχιστον.[64],[75]

- Ασφάλεια Συνεδρίας (Session): Η ασφάλεια συνεδρίας επιβάλλει περιορισμούς σε έναν χρήστη και είναι κρίσιμο για την ασφάλεια στην χρήση υπηρεσιών και εφαρμογών μέσω web. Αυτή υλοποιείται κυρίως με την χρήση κρυπτογράφησης, κατάλληλων αναγνωριστικών κλειδιού και session ID's.[64]

- Ασφάλεια Εφαρμογών (Application): Ορισμένες λύσεις που υποστηρίζουν την ασφάλεια των εφαρμογών είναι:[64],[75]
  - ο περιορισμός δικαιωμάτων κυρίως στους χρήστες.

- η επικύρωση εισόδου σε συστήματα και εφαρμογές.
- η χρήση κωδικών πρόσβασης και λιστών ελέγχου πρόσβασης (Access Control Lists - ACL).
- ο τακτικός έλεγχος για ευπάθειες (vulnerability assessments) και η εκτέλεση penetration tests.
- η δημιουργία αντιγράφων ασφαλείας, σχεδίου επαναφοράς και η υλοποίηση του εφόσον απαιτηθεί.
- εφαρμογή τείχους προστασίας εφαρμογών Web (Web Application Firewall – WAF).
- εφαρμογή τείχους προστασίας βάσεων δεδομένων (Database Firewall – DBF).
- έλεγχος εκ των προτέρων των όποιων λογισμικών πριν την παραγωγική χρήση τους για την αναζήτηση τρωτών σημείων και ευπαθειών (Static Application Testing - SAST).

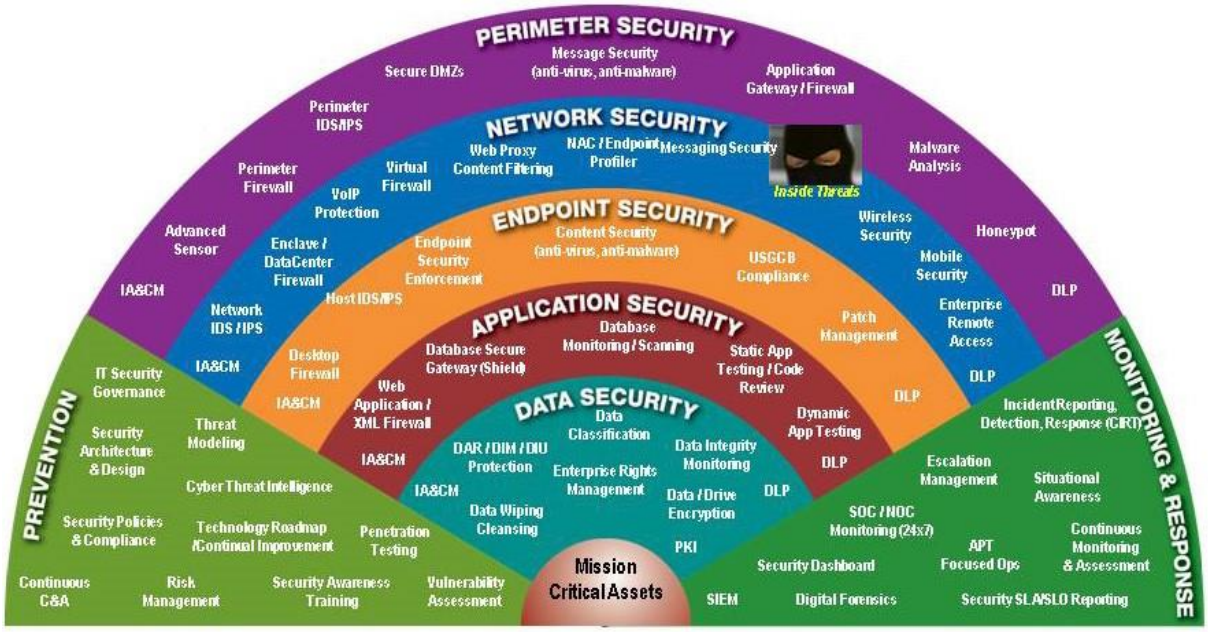
- Ασφάλεια Δεδομένων: Για την ασφάλεια δεδομένων η εφαρμογή σύγχρονων και δοκιμασμένων μοντέλων κρυπτογράφησης επιβάλλεται για την προστασία των δεδομένων του οργανισμού, αλλά και των χρηστών. Αυτή θα πρέπει να εφαρμόζεται σε κάθε επίπεδο όπου διαφαίνονται κίνδυνοι ασφαλείας, όπως π.χ. σε βάσεις δεδομένων, σε αρχεία χρηστών, σε σκληρούς δίσκους, σε φορητές συσκευές, στην αποστολή αρχείων με ηλεκτρονικό ταχυδρομείο, στην χρήση διαδικτύου κλπ. Επίσης πρέπει να γίνεται παρακολούθηση ακεραιότητας δεδομένων, να υφίστανται συστήματα DLP, να υπάρχουν πολιτικές και διαδικασίες όπως π.χ. καταστροφής των δεδομένων κλπ.[64],[75]



Σχήμα 12: Defense-in-Depth Model.[64]

Σχήμα 13: Cybersecurity Compliance Frameworks.[66]

Στο παρακάτω σχήμα μπορούμε συνοπτικά να δούμε, ανά επίπεδο ασφάλειας: μέτρα, πολιτικές, διαδικασίες που βρίσκουν εφαρμογή στο μοντέλο DID.



Σχήμα 14: Λεπτομερής αποτύπωση μέτρων ασφάλειας ανά επίπεδο.[75]

Συνισταμένες που πρέπει να λαμβάνονται υπόψη στο μοντέλο DID είναι:

- Ο ανθρώπινος παράγοντας, τόσο όσον αφορά την πληρότητα γνώσεων των διαχειριστών, όσο και των μελών του τμήματος IT. Επίσης, θα πρέπει να υπάρχει συνεχής εκπαίδευση στη μηχανική ασφάλειας συστημάτων, ενώ θα πρέπει να έχουν αρκετά κίνητρα ώστε να έχουν ενδιαφέρον για μάθηση και εξερεύνηση νέων τάσεων ασφάλειας.[64],[75]
- Η ανθρώπινη πτυχή πρέπει να λαμβάνεται υπόψη και σε οργανισμούς όπου δεν υπάρχει κυλιόμενο ωράριο λειτουργίας. Τότε πρέπει να λαμβάνονται επιπλέον μέτρα για να διασφαλιστεί ότι το σύστημα παραμένει προστατευμένο από επίδοξους εισβολείς.[69]
- Οι προμηθευτές ενός οργανισμού διαδραματίζουν σημαντικό ρόλο στο πλαίσιο ενός ισχυρού μοντέλου DID. Αυτό αφορά τόσο σε προμήθειες προϊόντων, στα οποία θα πρέπει να έχει ενσωματωθεί η ασφάλεια στον κύκλο ζωής τους, όσο και σε υπηρεσίες ή εξωτερική ανάθεση λειτουργιών, όπου θα πρέπει τουλάχιστον να υπάρχουν Συμφωνίες Επιπέδου Υπηρεσιών (Service-Level Agreement - SLA), μνημόνια συμφωνίας (Memorandum of Understanding/Agreement - MOU/MOA) και Συμφωνίες Ασφάλειας Διασύνδεσης (Interconnection Security Agreement - ISA).[72]

Αξιοποίηση υπηρεσιών Cloud στο μοντέλο DID

Η ολοένα και μεγαλύτερη χρήση υπηρεσιών cloud από οργανισμούς υγείας θα πρέπει να παρέχει ένα επίπεδο ενίσχυσης της ασφάλειας ανάλογο με την κρισιμότητα της λειτουργίας που φιλοξενεί. Ειδικότερα, ο οργανισμός θα πρέπει πιο επισταμένα να λαμβάνει υπόψη την ασφάλεια, την ακεραιότητα, την εμπιστευτικότητα και την διαθεσιμότητα των πληροφοριών, διότι παρουσιάζουν μεγαλύτερο κίνδυνο να παραβιαστούν σε ένα σύστημα υπολογιστικού νέφους καθότι είναι υποκείμενες σε μεγαλύτερο εύρος απειλών. Ενδεικτικά θα πρέπει κατ' ελάχιστο να:

- Προστατεύονται τα δεδομένα από μη εξουσιοδοτημένη πρόσβαση, αποκάλυψη, τροποποίηση ή παρακολούθηση με εφαρμογή πολιτικών διαχείρισης ταυτότητας και ελέγχου πρόσβασης για εξουσιοδοτημένους χρήστες που έχουν δικαίωμα πρόσβασης σε υπηρεσίες cloud.
- Αποτρέπεται η μη εξουσιοδοτημένη πρόσβαση σε πόρους υποδομής υπολογιστικού νέφους με υλοποίηση τομέων ασφαλείας που έχουν λογικό διαχωρισμό μεταξύ υπολογιστικών πόρων.
- Αποτρέπονται επιθέσεις σε προγράμματα περιήγησης διαδικτύου που χρησιμοποιούν υπολογιστικό νέφος για τον μετριασμό των τρωτών σημείων ασφαλείας των τελικών χρηστών με εφαρμογή λογισμικού ασφαλείας, προσωπικού τείχους προστασίας και εγκατάσταση ενημερώσεων.
- Εφαρμόζονται λύσεις ελέγχου πρόσβασης, ανίχνευσης και πρόληψης εισβολών (IDS/IPS) σε εφαρμογές υπολογιστικού νέφους.
- Χρησιμοποιείται ισχυρή κρυπτογράφηση κατά τις περιόδους σύνδεσης ιστού και άλλων επικοινωνιών δικτύου (π.χ. πρωτόκολλο SSL/TLS τελευταίας έκδοσης), όποτε μια εφαρμογή αλληλεπιδρά με άλλες εφαρμογές, στις μεταφορές δεδομένων καθώς και στα αποθηκευμένα δεδομένα.
- Είναι καθορισμένα τα όρια εμπιστοσύνης μεταξύ οργανισμού και cloud provider για να διασφαλίζεται ότι οι ευθύνες για την εφαρμογή των μέτρων ασφαλείας προσδιορίζονται σαφώς.

- Λαμβάνονται υπόψη οι πρακτικές και τα σχέδια ασφάλειας των φυσικών εγκαταστάσεων σε τοποθεσίες παρόχων υπολογιστικού νέφους ως μέρος των συνολικών εκτιμήσεων κινδύνου κατά την επιλογή ενός παρόχου.

Επίσης λειτουργικές λεπτομέρειες που σχετίζονται με την ανάκτηση, τη διαχείριση συμβάντων και άλλες λειτουργικές ακολουθίες απαιτούν ειδική υποστήριξη από τον πάροχο υπηρεσιών φιλοξενίας cloud.[72],[76],[77],[78]

Η χρήση, όμως, υπηρεσιών cloud παρέχει και πλεονεκτήματα στο μοντέλο DID της ασφάλειας. Επί παραδείγματι το υπολογιστικό νέφος λειτουργώντας ως δυναμική άμυνα, μπορεί να χρησιμοποιηθεί για την αποτροπή της αποτελεσματικότητας των τυπικών επιθέσεων άρνησης υπηρεσίας (DoS).[73]

Το μοντέλο DID πλην του τομέα της υγείας μπορεί να έχει εφαρμογή σε μια μεγάλη ποικιλία τομέων ασφαλείας και οργανισμών. Επί παραδείγματι μπορεί να έχει σημαντική εφαρμογή σε Συστήματα Βιομηχανικού Ελέγχου (Industrial Control Systems - ICS), σε περιβάλλοντα της 4ης Βιομηχανικής Επανάστασης όπου συμπλέκονται συστήματα OT (Operational Technology) με συσκευές IIoT (Industrial Internet of Things) και IT (Information Technology), σε αρχιτεκτονικές εφαρμογών υπολογιστικού νέφους, σε οργανισμούς με βάσεις ευαίσθητων δεδομένων όπου οι χρήστες πρέπει να είναι περιορισμένοι στην πρόσβαση τους κλπ. Βασικά χαρακτηριστικά της ασφάλειας του μοντέλου DID είναι το βάθος της άμυνας, το πλάτος της άμυνας, η αντοχή σε επιθέσεις, η ευελιξία του και η επεκτασιμότητα του.[71],[79]

5.2 Zero Trust Security Model

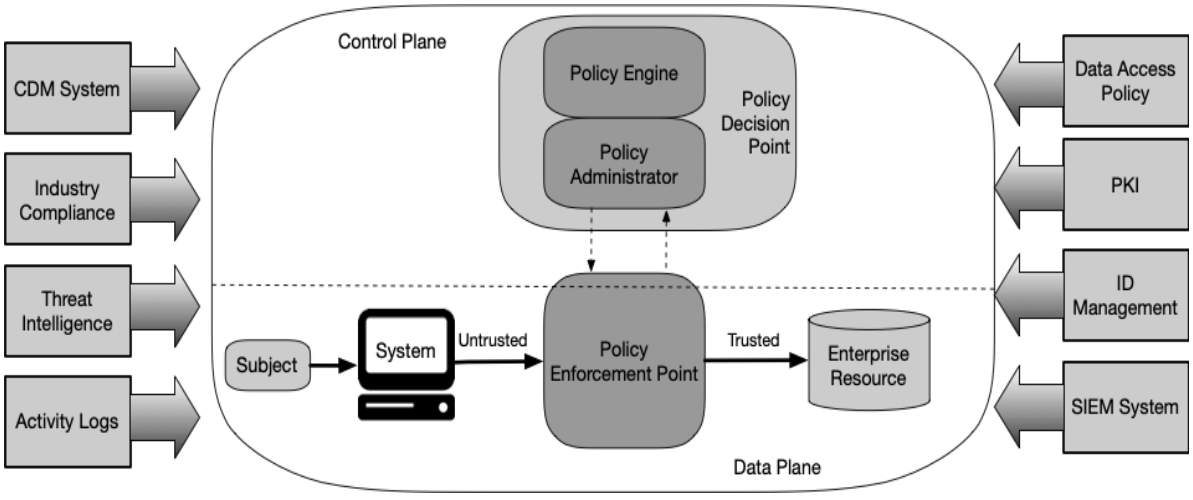
Το Zero Trust Security Model ή εναλλακτικά Zero Trust Architecture-ZTA (Αρχιτεκτονική Μηδενικής Εμπιστοσύνης) που πρωτοεμφανίστηκε ως έννοια στον τομέα της κυβερνοασφάλειας από τον John Kindervag το 2010 είναι ένα είδος μοντέλου ασφάλειας δικτύου, το οποίο βασίζεται στην έννοια της μηδενικής εμπιστοσύνης (never trust and always verify). Είτε η ανάγκη πρόσβασης είναι από το εσωτερικό δίκτυο ή είτε εξωτερικά αυτού, θα πρέπει αυτή πάντοτε να πιστοποιείται για την πρόσβαση σε πόρους (assets, υπηρεσίες, ροές εργασίας, λογαριασμοί δικτύου, κ.λπ.). Η μηδενική εμπιστοσύνη εστιάζει στην προστασία των πόρων και όχι σε τμήματα δικτύου, καθώς η τοποθεσία του δικτύου δεν θεωρείται πλέον ως το κύριο στοιχείο για την ασφάλεια των πόρων.[80],[81],[84]

Το Zero Trust Architecture έχει διάφορες προσεγγίσεις από διάφορους οργανισμούς με πιο σημαντικές αυτές των NIST, National Cyber Security Centre UK (NCSC), Forrester.[80],[82],[84],[85],[89],[90]

Σύμφωνα με το NIST το Zero Trust Architecture σχεδιάζεται και αναπτύσσεται συμμορφούμενο με τις ακόλουθες επτά βασικές αρχές μηδενικής εμπιστοσύνης:[80],[83]

1. Όλες οι πηγές δεδομένων και οι υπηρεσίες λογίζονται ως πόροι (π.χ. υπολογιστές, συσκευές IoT, εφαρμογές και μέσω cloud, προσωπικές συσκευές κλπ).
2. Ολόκληρη η επικοινωνία ελέγχεται ως προς την ασφάλεια της ανεξάρτητα από πού προέρχεται στο δίκτυο. Οποιοδήποτε σημείο στο δίκτυο δεν συνεπάγεται αυτόματα και εμπιστοσύνη. Συνεπώς, όλη η επικοινωνία θα πρέπει να γίνεται με τον πιο ασφαλή διαθέσιμο τρόπο, έτσι ώστε να προστατεύει το απόρρητο, την ακεραιότητα και να παρέχει έλεγχο ταυτότητας.

3. Η πρόσβαση σε μεμονωμένους πόρους ενός οργανισμού παρέχεται ανά συνεδρία και με τα λιγότερα προνόμια που απαιτούνται για την ολοκλήρωση της εργασίας. Ενώ, ο έλεγχος ταυτότητας (authentication) και η εξουσιοδότηση (authorization) σε έναν πόρο δεν θα εκχωρούν αυτόματα πρόσβαση σε διαφορετικό πόρο.
4. Η πρόσβαση στους πόρους καθορίζεται από δυναμική πολιτική (συμπεριλαμβανομένης της παρατηρήσιμης κατάστασης της ταυτότητας του αιτούντος την πρόσβαση, της όποιας εφαρμογής ή υπηρεσίας και του asset για το οποίο ζητείται η πρόσβαση). Ενώ μπορεί να περιλαμβάνει επιπλέον χαρακτηριστικά συμπεριφοράς και περιβάλλοντος. Επίσης, εφαρμόζονται οι αρχές ελάχιστων προνομίων με σκοπό τον περιορισμό τόσο της ορατότητας (visibility) όσο και της προσβασιμότητας (accessibility).
5. Ο οργανισμός παρακολουθεί και μετρά την ακεραιότητα, καθώς και την ασφάλεια όλων των assets (ιδιόκτητων και διασυνδεδεμένων). Αυτό διότι κανένα asset δεν θεωρείται αξιόπιστο από προεπιλογή. Η παρακολούθηση και η αξιολόγηση πρέπει να είναι μια συνεχής διαδικασία, κάτι το οποίο, απαιτεί ένα ισχυρό σύστημα παρακολούθησης και αναφοράς για την παροχή αξιόπιστων δεδομένων σε πραγματικό χρόνο όλων των πόρων ενός οργανισμού.
6. Ο έλεγχος ταυτότητας και η εξουσιοδότηση πρόσβασης σε πόρους είναι μια δυναμική διαδικασία που επιβάλλεται αυστηρά πριν επιτραπεί αυτή. Ενώ είναι ένας συνεχής κύκλος απόκτησης πρόσβασης, σάρωσης και αξιολόγησης απειλών, προσαρμογής και συνεχούς επαναξιολόγησης της εμπιστοσύνης στη συνεχή αλληλεπίδραση.
7. Ένας οργανισμός συλλέγει όσο το δυνατόν περισσότερες πληροφορίες σχετικά με την τρέχουσα κατάσταση των assets, την υποδομή δικτύου και τις επικοινωνίες, με σκοπό να τις χρησιμοποιεί για την βελτίωση του σχεδίου ασφαλείας του σε κάθε παράμετρο.



Σχήμα 15: Στοιχεία Zero Trust σύμφωνα με τον NIST.[80]

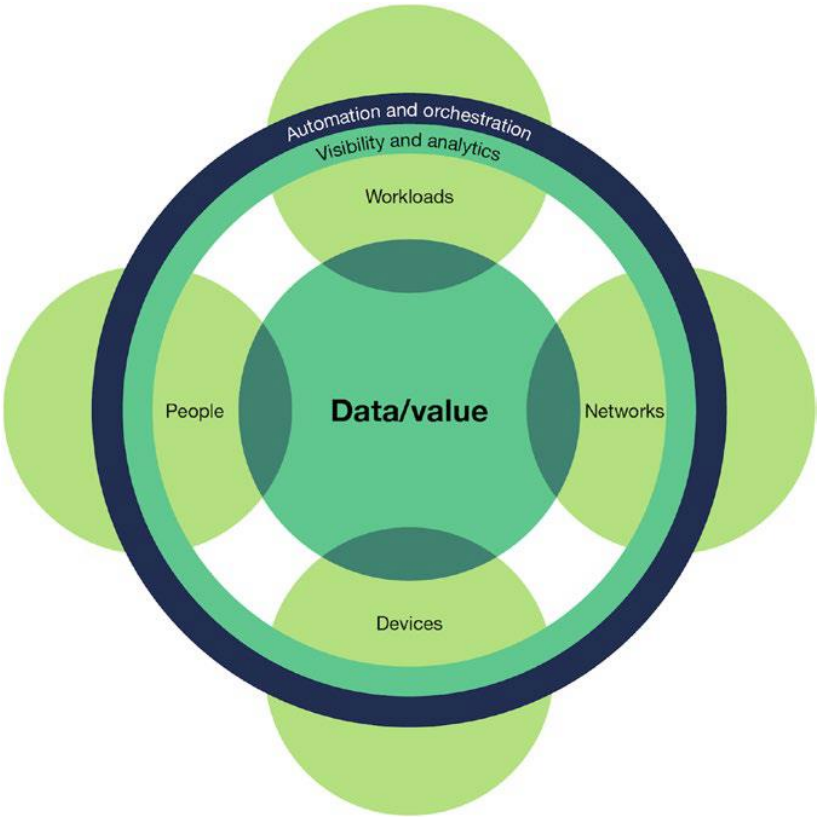
Η προσέγγιση που υιοθετείται από το NCSC, περιλαμβάνει οκτώ βασικές αρχές για την υλοποίηση του μοντέλου ZTA:[82],[90]

1. Ο οργανισμός να είναι γνώστης της αρχιτεκτονικής του, συμπεριλαμβανομένων των χρηστών, των συσκευών, των υπηρεσιών και των δεδομένων αυτού. Και αυτό, για να αξιοποιούνται πλήρως τα πλεονεκτήματα που προσφέρει το μοντέλο ZTA.

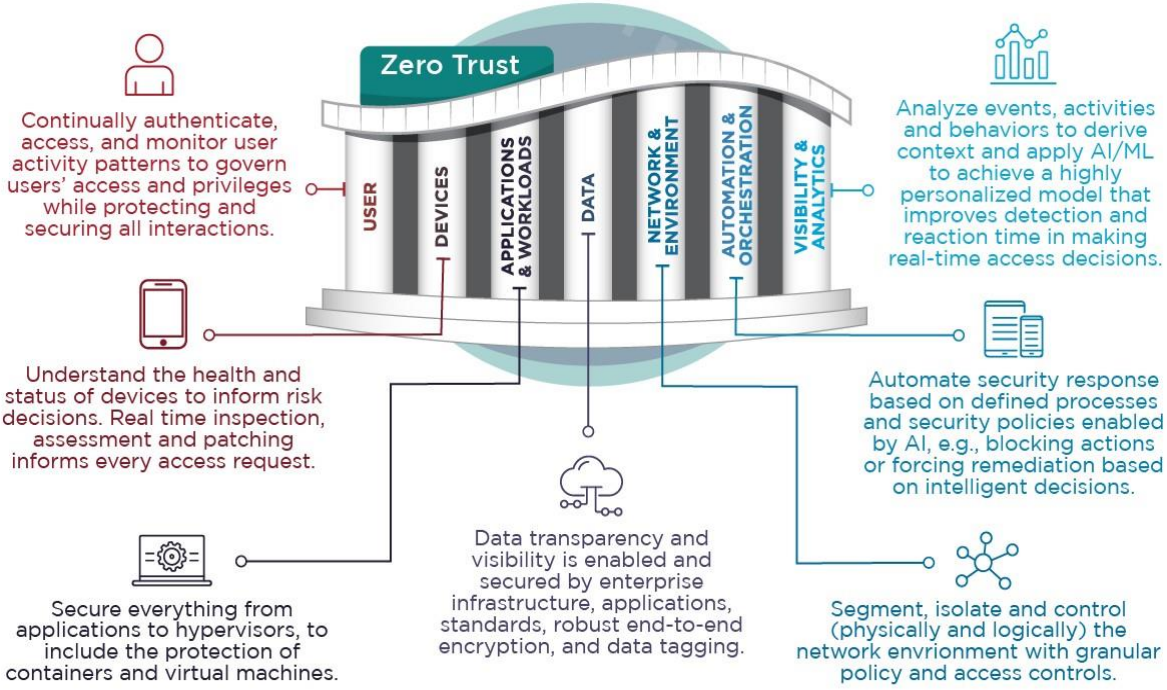
2. Να είναι γνωστές οι ταυτότητες χρηστών, υπηρεσιών και συσκευών. Η ταυτότητα ενός χρήστη, μιας υπηρεσίας και μιας συσκευής, είναι πολύ σημαντικός παράγοντας κατά τη λήψη αποφάσεων πρόσβασης σε ένα δίκτυο Zero Trust.
3. Να αξιολογείται συνεχώς η συμπεριφορά των χρηστών, των υπηρεσιών και η εύρυθμη λειτουργία των συσκευών, όντας σημαντικοί δείκτες στην προσπάθεια επίτευξης εμπιστοσύνης στην ασφάλεια των συστημάτων ενός οργανισμού.
4. Να εφαρμόζονται πολιτικές για την εξουσιοδότηση αιτημάτων πρόσβασης σε δεδομένα και υπηρεσίες. Η ισχύς μιας αρχιτεκτονικής μηδενικής εμπιστοσύνης προέρχεται από τις πολιτικές πρόσβασης που έχουν οριστεί, ενώ μπορούν επίσης να βοηθήσουν στη διευκόλυνση της διαχειριζόμενης κοινής χρήσης δεδομένων ή υπηρεσιών με επισκέπτες χρήστες ή συνεργαζόμενους οργανισμούς.
5. Να πραγματοποιείται έλεγχος ταυτότητας και εξουσιοδότηση σε κάθε αίτημα θεωρώντας το δίκτυο ως εχθρικό περιβάλλον.
6. Να πραγματοποιείται ολοκληρωμένη παρακολούθηση της συμπεριφοράς χρηστών, υπηρεσιών και συσκευών, κάτι το οποίο θα βοηθήσει στην αύξηση της ασφάλειας στον κυβερνοχώρο.
7. Να μην υπάρχει εμπιστοσύνη κανενός δικτύου, συμπεριλαμβανομένου του ίδιου του οργανισμού λογίζοντας το ως εχθρικό. Κάθε φορά πρέπει να δημιουργείται εμπιστοσύνη στους χρήστες, τις συσκευές και τις υπηρεσίες.
8. Να επιλέγονται υπηρεσίες που έχουν σχεδιαστεί για αρχιτεκτονικές δικτύου μηδενικής εμπιστοσύνης. Σε μια αρχιτεκτονική μηδενικής εμπιστοσύνης, δεν υφίσταται εμπιστοσύνη στο δίκτυο, επομένως, πρέπει να επιλέγονται υπηρεσίες που έχουν σχεδιαστεί, έτσι ώστε να προστατεύονται από όλες τις πιθανές πηγές επίθεσης περιλαμβάνοντας και το Διαδίκτυο, στο οποίο στοιχεία του δικτύου θα μπορούσαν να εκτεθούν άμεσα.

Στην προσέγγιση από την εταιρεία έρευνας και παροχής συμβουλών Forrester οι βασικές αρχές ενός μοντέλου ZTA είναι οι κάτωθι τρεις:[84],[85],[89]

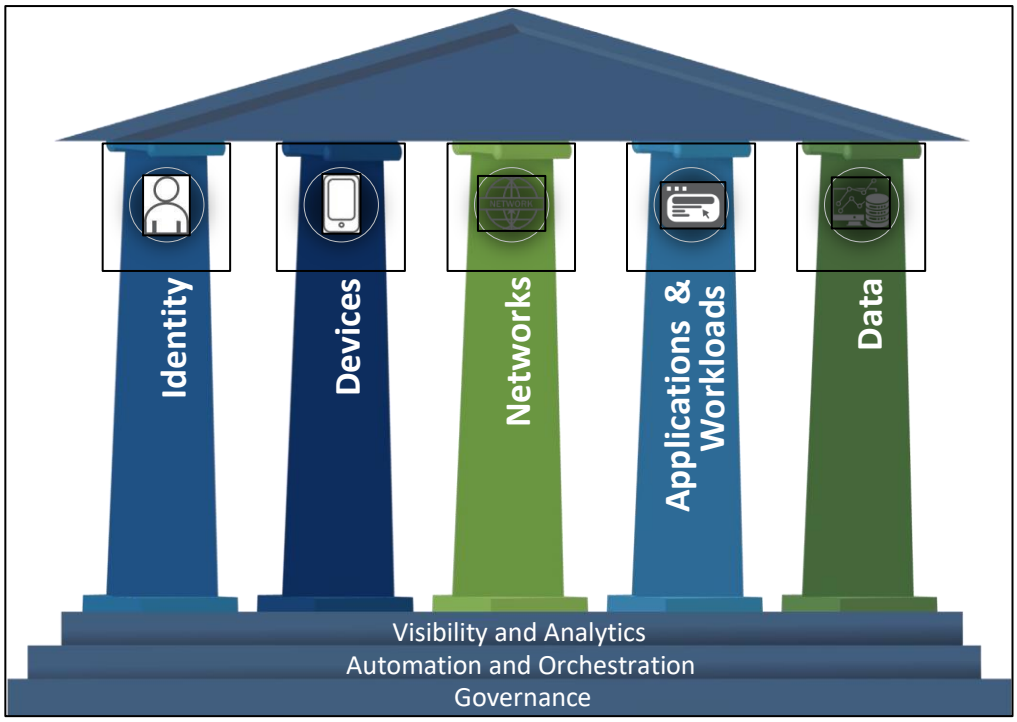
1. Πρέπει από τον οργανισμό να γίνεται επαλήθευση και διασφάλιση όλων των πόρων αυτού. Στο μοντέλο ZTA εξαλείφεται η έννοια της εμπιστοσύνης από το δίκτυο, συνεπώς επιβάλλεται να διασφαλίζεται ότι όλοι οι πόροι είναι προσβάσιμοι με ασφάλεια και αυτό ανεξάρτητα από το ποιος το αιτείται ή από πού προέρχεται.
2. Να επιβάλλονται αυστηρά μέτρα περιορισμού και ελέγχου πρόσβασης. Είναι θεμελιώδης η έννοια των ελάχιστων προνομίων και του αυστηρού ελέγχου πρόσβασης σε πόρους.
3. Να πραγματοποιείται επιθεώρηση και καταγραφή όλης της κίνησης του δικτύου σε πραγματικό χρόνο.



Σχήμα 16: Forrester Zero Trust eXtended Model 2020.[86]



Σχήμα 17: Περιγραφή των επτά πυλώνων του μοντέλου Zero Trust Architecture σύμφωνα με την NSA.[87]



Σχήμα 18: Πυλώνες του μοντέλου Zero Trust Architecture σύμφωνα με τον CISA βασιζόμενες στις επτά βασικές αρχές μηδενικής εμπιστοσύνης του NIST SP 800-207.[88]

Για την υλοποίηση ενός μοντέλου ZTA η εφαρμογή τουλάχιστον των παρακάτω μέτρων και τεχνολογιών θεωρείται απαραίτητη:[82],[86],[87],[88],[95],[97]

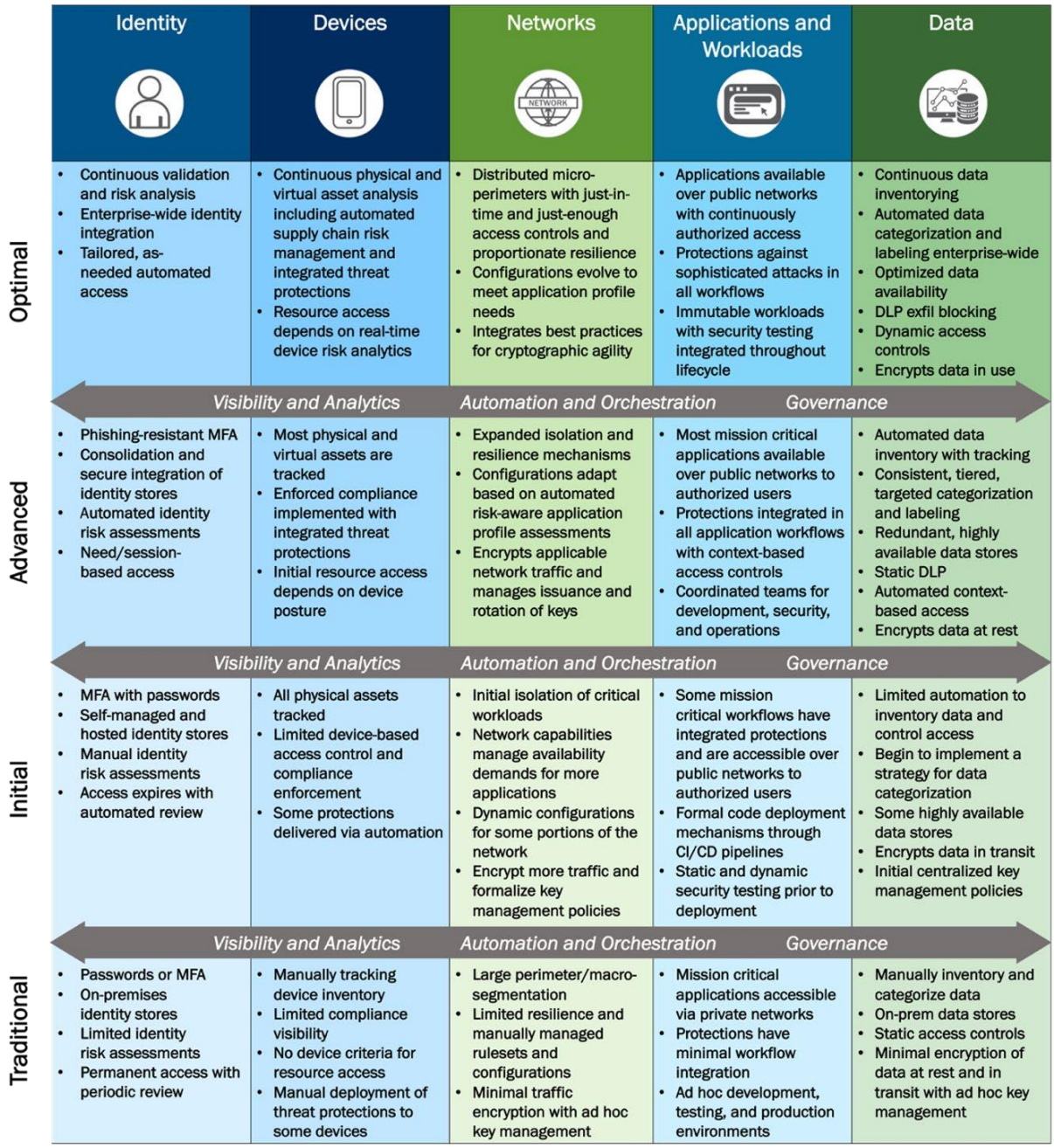
- Διεξαγωγή Risk Assessment στην αρχή υλοποίησης ενός μοντέλου ZTA, αλλά και ανά τακτά χρονικά διαστήματα.
- Χαρτογράφηση του δικτύου με λεπτομερές διάγραμμα των στοιχείων του δικτύου, συμπεριλαμβανομένων όλων των χρηστών, συσκευών και εφαρμογών, ώστε να προσδιορίζεται εύκολα κάθε σημείο πρόσβασης σε αυτό και οι συνδέσεις του.
- Εφαρμογή τμηματοποίησης στο δίκτυο (Network segmentation).
- Χρήση firewall επόμενης γενιάς (Next-Generation Firewall - NGFW).
- Δημιουργία ομάδων (groups) για καλύτερη διαχείριση και εφαρμογή πολιτικών.
- Εφαρμογή πολιτικών για την εξουσιοδότηση πρόσβασης σε δεδομένα ή υπηρεσίες.
- Μοναδική ταυτοποίηση ανά χρήστη, υπηρεσία και συσκευή. Για την ταυτοποίηση χρήστη θα πρέπει να χρησιμοποιείται ένας οριστικός κατάλογος χρηστών, δημιουργώντας λογαριασμούς που θα συνδέονται προσωποποιημένα. Για τις υπηρεσίες ενδείκνυται ο έλεγχος ταυτότητας με μοναδικό πιστοποιητικό (certificate) που μπορεί εν συνεχεία να χρησιμοποιηθεί για τη δημιουργία αμοιβαίων συνδέσεων Transport Layer Security (TLS). Η χρήση τεχνολογίας Trusted Platform Module (TPM) για μοναδική ταυτοποίηση συσκευής θεωρείται η ιδανικότερη.
- Καθορισμός ρόλων με την αρχή του ελάχιστου προνομίου (Principle of least privilege).
- Εφαρμογή ισχυρών access controls για περιορισμό και έλεγχο της πρόσβασης στο δίκτυο καθώς και στους πόρους του οργανισμού. Αυτό μπορεί να επιτευχθεί μέσω ελέγχου πρόσβασης βάσει ρόλου (Role-based access control - RBAC) και ιδανικά μέσω ελέγχου ταυτότητας πολλαπλών παραγόντων (Multi-factor authentication: MFA).
- Εφαρμογή αυθεντικοποίησης μεταξύ αιτημάτων υπηρεσιών π.χ. με χρήση API tokens, frameworks όπως το OAuth 2.0 ή το Public Key Infrastructure (PKI).

- Παρακολούθηση συσκευών, υπηρεσιών και συμπεριφοράς χρηστών. Αυτό μπορεί να επιτευχθεί μέσω τεχνολογιών όπως η ανάλυση ασφαλείας (security analytics), Συστημάτων Ανίχνευσης Εισβολής (IDS) και συστημάτων Διαχείρισης Πληροφοριών Ασφαλείας και Συμβάντων (Security Information and Event Management - SIEM). Για χρήστες ανήκοντες στην κατηγορία Bring Your Own Device (BYOD) μπορεί να υλοποιηθεί με χρήση λύσεων τύπου Mobile Device Management (MDM) και Mobile Application Management (MAM).
- Όλες οι επικοινωνίες για πρόσβαση σε δεδομένα ή υπηρεσίες, θα πρέπει να χρησιμοποιούν ασφαλή μεταφορά όπως π.χ. το πρωτόκολλο TLS.
- Οι υπηρεσίες και τα δεδομένα, στα οποία έχουν πρόσβαση οι χρήστες επιβάλλεται να προστατεύονται με πιστοποιημένα και κρυπτογραφημένα πρωτόκολλα. Η χρήση σύγχρονων πρωτοκόλλων ισχυρής κρυπτογράφησης πρέπει να εφαρμόζεται σε κάθε επίπεδο (encrypt: Data at rest, Data in transit, Data in use), όχι μόνο εξωτερικά του δικτύου ενός οργανισμού, αλλά και εσωτερικά αυτού.
- Χρήση λογισμικού πρόληψης απώλειας δεδομένων (Data Loss Prevention - DLP).
- Χρήση τεχνολογιών που βασίζονται σε πρότυπα για την επίτευξη διαλειτουργικότητας μεταξύ συσκευών και υπηρεσιών. Ο έλεγχος ταυτότητας και η εξουσιοδότηση, μπορούν να επιτευχθούν με κοινά πρότυπα όπως το OpenID Connect, το OAuth 2.0 Authorization Framework ή το SAML (Security Assertion Markup Language) που επιτρέπουν τη διαλειτουργικότητα μεταξύ υπηρεσιών και παρόχων ταυτότητας.
- Να υπάρχει αποτροπή και έλεγχος κίνησης κακόβουλου λογισμικού τελικών σημείων με εγκατεστημένα antivirus/antimalware σε κάθε συσκευή (Endpoint Detection and Response-EDR/Managed Detection and Response-MDR/Extended Detection and Response-XDR).
- Οι εφαρμογές και οι συσκευές πρέπει να έχουν εγκατεστημένες τις τελευταίες ενημερώσεις λογισμικού ασφαλείας (security updates/patches) και υπολογισμικού (firmware).

Σε ένα δίκτυο μοντέλου ZTA ορισμένα από τα πλεονεκτήματα είναι τα κάτωθι:[85]

- Είναι εφαρμόσιμο ανεξάρτητα από πλατφόρμα ή σύστημα (Platform-agnostic).
- Μπορεί να βοηθήσει στην συμμόρφωση σε πρωτοκόλλα και αξιολογήσεις ασφαλείας, καθώς και να μειώσει το κόστος στην συμμόρφωση αυτών.
- Εφαρμόζει ασφάλεια στην εικονικοποίηση (virtualization).
- Δημιουργεί κλιμακωτή ανάπτυξη στον οργανισμό που εφαρμόζεται και ανοίγει νέα πεδία επιχειρηματικής δραστηριότητας σε αυτόν.
- Είναι βασικό θεμέλιο σε περιβάλλοντα χρήσης πολλαπλών μισθώσεων (π.χ. σε περιβάλλοντα cloud).
- Μπορεί εύκολα να κάνει load-balancing στους δικτυακούς πόρους εφαρμόζοντας διαλειτουργικότητα και μειώνοντας το λειτουργικό κόστος.
- Είναι επεκτάσιμο προσφέροντας επιπλέον επιλογές, ενώ μπορεί να εφαρμοστεί και σε υπάρχοντα δίκτυα.

Το μοντέλο ZTA βασίζεται σε τεχνολογίες ελέγχου ταυτότητας, ελέγχου πρόσβασης, και αξιολόγησης εμπιστοσύνης. Είναι μια σύγχρονη προσέγγιση για την ασφάλεια στον κυβερνοχώρο που μπορεί να καλύψει τις απαιτήσεις ασφαλείας των τελευταίων τάσεων και αναγκών ενός πολύπλοκου οικοσυστήματος IT, όπως είναι και ο τομέας της υγείας.[81],[91],[92],[93],[94] Παρόλα αυτά, το μοντέλο ZTA έχει και δυσκολίες υλοποίησης όπως είναι η μετάβαση από παλαιές υποδομές. Μπορεί, όμως, σε τέτοιες περιπτώσεις αυτό το μοντέλο να λειτουργήσει έστω και εν μέρει (υβριδικά) με παλαιοτέρα μοντέλα π.χ. το DID.[96]



Σχήμα 19: Κλιμακωτή εφαρμογή μέτρων του μοντέλου Zero Trust Architecture από τον CISA.[88]

Κεφάλαιο 6 – Εφαρμογή νέων τεχνολογιών

Στην κυβερνοασφάλεια στον τομέα της υγείας μπορούν να συμβάλλουν και ορισμένες νέες τεχνολογίες. Η χρήση τους όμως θα πρέπει να γίνεται με μεγάλη επιμέλεια και επιφύλαξη. Αυτό καθότι δεν πρέπει να διακυβευτεί με οιονδήποτε τρόπο η ασφάλεια και η ιδιωτικότητα του τομέα υγείας.

6.1 Τεχνολογία Blockchain

Η τεχνολογία blockchain παρουσιάστηκε αρχικά το 2008 ως ένα σύστημα ηλεκτρονικών πληρωμών κάνοντας χρήση ενός νέου τότε νομίσματος που ήταν το bitcoin. Αυτό το αρχικό έτος έναρξης (2008) μέχρι και το 2013 ήταν η πρώτη περίοδος του δικτυού blockchain, στο οποίο αναδείχτηκαν και τα πρώτα μειονεκτήματα της τεχνολογίας με κυριότερα τον μεγάλο χρόνο απόκρισης και την απαιτούμενη υπολογιστική ισχύ. Η δεύτερη περίοδος του blockchain (2013-2016) καθορίστηκε με την εμφάνιση του δικτύου Ethereum, με το οποίο δόθηκε η δυνατότατα στους χρήστες του δικτύου η αποθήκευση προγραμμάτων σε αυτό γνωστά ως smart contracts και άρχισαν να παρουσιάζονται οι πρώτες Decentralized Applications (dApps) αναδεικνύοντας περεταίρω τις δυνατότητες της τεχνολογίας πέρα από τις ηλεκτρονικές πληρωμές. Σήμερα διανύουμε την τρίτη περίοδο της τεχνολογίας blockchain αρχής γενομένης από το 2017.[98]

Τα πλεονεκτήματα που έχουν αναδειχθεί από την τεχνολογία blockchain μπορούν να συνοψισθούν στα εξής:[98],[99],[100]

- απουσία κεντρικής αρχής με απευθείας συνδιαλλαγή των χρηστών.
- αποδοτικότητα συστήματος και απουσία αποτυχίας που απορρέει από την αποκεντρωμένη φύση της τεχνολογίας.
- αμεταβλητότητα και ακεραιότητα δεδομένων που διασφαλίζεται με την χρήση κρυπτογραφίας διαδοχικά στα blocks.
- διαφάνεια συναλλαγών.
- αξιοπιστία συστήματος που αυξάνεται ανάλογα και με την αύξηση των χρηστών.
- ταχύτητα ολοκλήρωσης συναλλαγών.
- πλήρης ιχνηλάτηση συναλλαγών απόρροια της διαφάνειας, της ακεραιότητας και της αμεταβλητότητας του συστήματος blockchain.
- ανυπαρξία ύπαρξης διπλών συναλλαγών.
- εμπιστοσύνη από τους χρήστες του δικτύου.
- ανθεκτικότητα σε κυβερνοεπιθέσεις λόγω της υλοποίησης peer-to-peer.

Στα μειονεκτήματα της τεχνολογίας blockchain συγκαταλέγονται:[98],[99],[100]

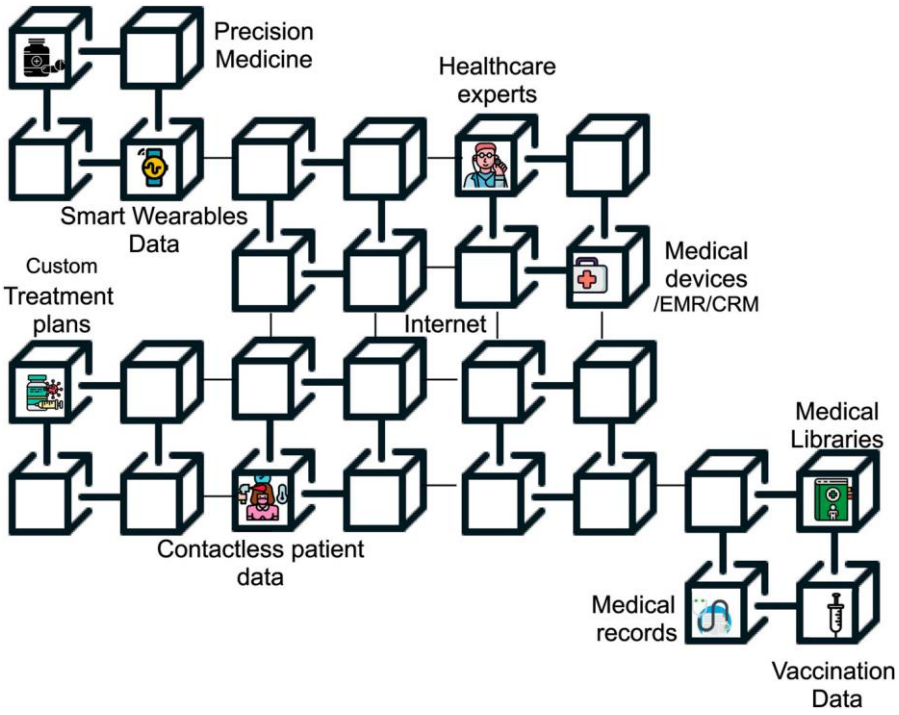
- η επεκτασιμότητα του δικτύου καθότι όσο αυτό αυξάνει τόσο πιο χρονοβόρο γίνεται.
- αμφιβολίες ιδιωτικότητας απόρροια της διαφάνειας που χαρακτηρίζει αυτή την τεχνολογία. Ο Γενικός Κανονισμός Προστασίας Δεδομένων όμως της Ε.Ε. (GDPR) έχει βοηθήσει στην επίλυση τέτοιων ζητημάτων αν και χρειάζεται ιδιαίτερη προσοχή όταν γίνεται χρήση αυτής της τεχνολογίας σε περιβάλλοντα με ευαίσθητα προσωπικά δεδομένα, όπως είναι ο χώρος της Υγειονομικής Περίθαλψης.
- μεγάλο κόστος υλοποίησης από την πληθώρα κόμβων στο δίκτυο και υψηλής κατανάλωσης ενέργειας απόρροια της μεγάλης χρήσης υπολογιστικής ισχύος.

- πιθανότητα εμφάνισης καθυστερήσεων λόγω επεξεργασίας των συναλλαγών από το σύστημα παρόλη την ταχύτατα ολοκλήρωσης τους.
- πολυπλοκότητα της τεχνολογίας κάτι που επιδρά αρνητικά στην αποδοχή της από το ευρύ κοινό.

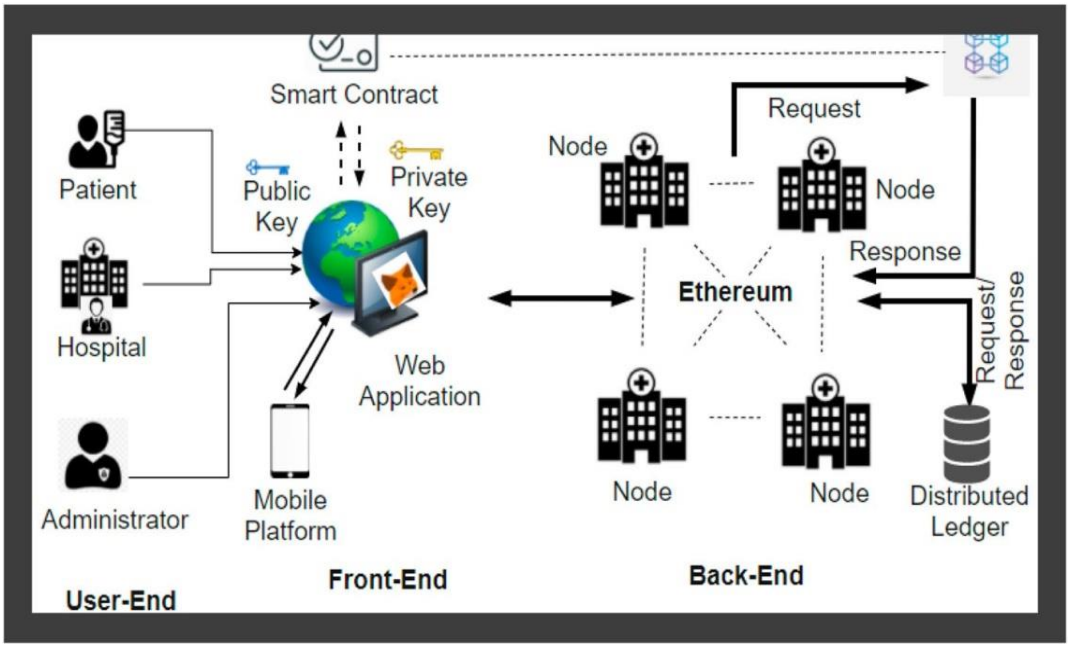
Η εφαρμογή τεχνολογίας Blockchain στον τομέα της Υγειονομικής Περίθαλψης μπορεί να συμβάλει στην ασφάλεια[32], την ακεραιότητα, την αυθεντικότητα, τη διαλειτουργικότητα, την ανταλλαγή δεδομένων, τον πραγματικό χρόνο εφαρμογής και την ιδιωτικότητα των ευαίσθητων προσωπικών δεδομένων τόσο σε εφαρμογές αρχείου ασθενών, λοιπών πληροφοριακών συστημάτων όσο και συσκευών IoMT.[1],[36],[39],[44],[45],[46],[47],[53]

Το Blockchain είναι μια τεχνολογία peer-to-peer για κατανεμημένη κοινή χρήση δεδομένων και υπολογισμό. Το Blockchain επιτρέπει στα άγνωστα μέρη να εκτελούν διαφορετικές συναλλαγές στο δίκτυο, ακόμη και αν δεν εμπιστεύονται το ένα το άλλο. Το Blockchain είναι ένας τύπος δομής δεδομένων που μπορεί να παρακολουθεί και να αποθηκεύει πληροφορίες από τον τεράστιο αριθμό συσκευών και συστημάτων χωρίς κάποιον διαχειριστή π.χ. κεντρικό cloud. Η κρυπτογραφία δημόσιου κλειδιού χρησιμοποιείται σε αυτήν την τεχνολογία για την εκτέλεση συναλλαγών μεταξύ κόμβων. Στη συνέχεια, οι συναλλαγές αποθηκεύονται σε ένα κοινό βιβλίο. Το καθολικό περιέχει την αλυσίδα των μπλοκ που συνδέονται κρυπτογραφικά μεταξύ τους. Το Blockchain είναι ένα ψηφιακό καθολικό που δεν παραβιάζεται και κανείς δεν μπορεί να αλλάξει εγγραφές ή να καταργήσει μπλοκ δεδομένων που έχουν καταγραφεί μόλις στο καθολικό της αλυσίδας μπλοκ, γεγονός που αυξάνει την ακρίβεια των εγγραφών.[44]

Οι ασφαλείς, αποκεντρωμένες και αυτόνομες δυνατότητες του Blockchain το καθιστούν ιδανική λύση για προβλήματα ασφάλειας IoMT, καταγράφοντας τις συναλλαγές της ψηφιακής επικοινωνίας.[35],[44],[45],[46],[53]



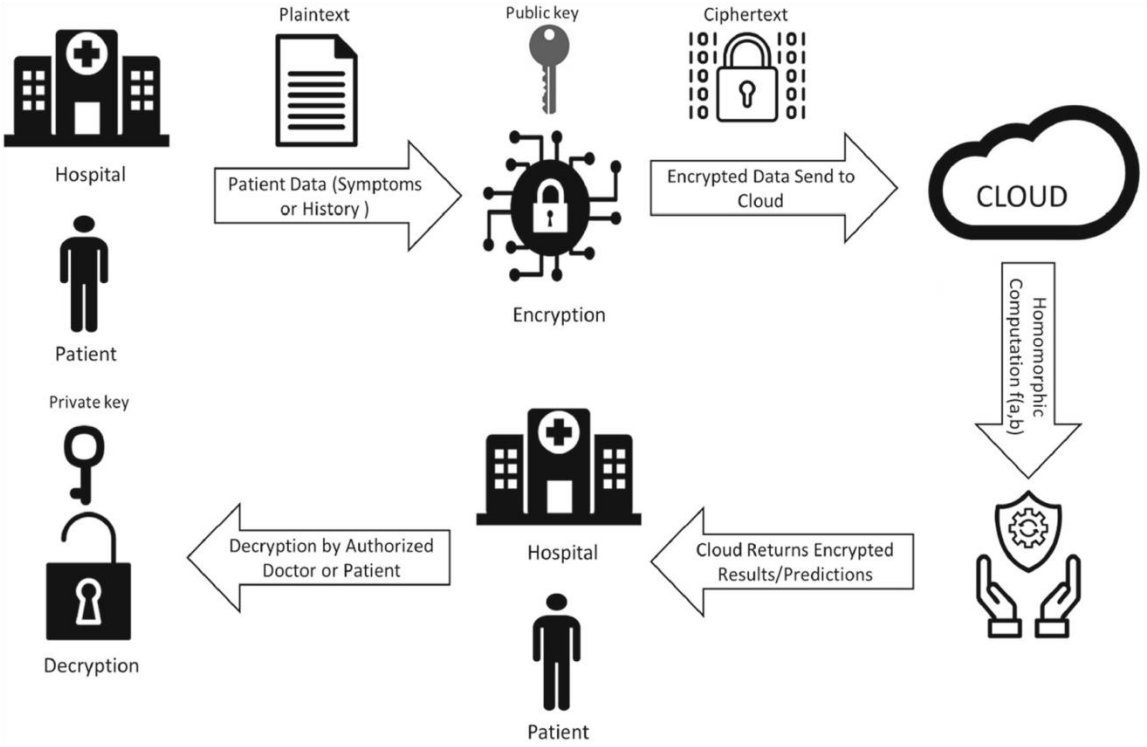
Σχήμα 20: Εφαρμογή τεχνολογίας Blockchain σε IoMTs.[35]



Σχήμα 21: Blockchain framework σε Ηλεκτρονικά Μητρώα Υγείας.[35]

6.2 Ομομορφική κρυπτογραφία

Όταν ένα πληροφοριακό σύστημα λειτουργεί σε cloud, τότε οι κίνδυνοι για τα ευαίσθητα δεδομένα που διακινούνται μέσω διαδικτύου είναι μεγαλύτεροι από ένα παραδοσιακό σύστημα που η βάση δεδομένων είναι σε κάποιο CR εντός του φορέα υγείας. Το ίδιο πρόβλημα προκύπτει και για δεδομένα που μπορεί να διακινούνται από άλλες εφαρμογές ή συσκευές IoMT. Η χρήση ομομορφικής κρυπτογραφίας μπορεί να δώσει λύση σε αυτό το πρόβλημα, αλλά και σε ποικίλες ακόμα εφαρμογές του τομέα της υγείας, όπως είναι η τελεϊατρική, η βοήθεια στο σπίτι, η κοινή χρήση δεδομένων για πιο αποτελεσματική φροντίδα ασθενών ή η διεξαγωγή μελετών-ερευνών κλπ. Η ομομορφική κρυπτογράφηση επιτρέπει τον υπολογισμό σε κρυπτογραφημένα δεδομένα χωρίς να τα αποκρυπτογραφεί και παρέχει κρυπτογραφημένα αποτελέσματα στον χρήστη. Η ομομορφική κρυπτογράφηση συνεπώς όχι μόνο επιτρέπει την επεξεργασία κρυπτογραφημένων δεδομένων, αλλά διατηρεί και το απόρρητο στη διαδικασία. Η τεχνολογία αυτή διακρίνεται σε τρεις κατηγορίες. Την μερική ομομορφική κρυπτογράφηση (Partial Homomorphic Encryption - PHE), η οποία υποστηρίζει μια λειτουργία στα ομομορφικά δεδομένα και είναι η πιο ανίσχυρη. Την κάπως ομομορφική κρυπτογράφηση (Somewhat Homomorphic Encryption - SWHE), η οποία υποστηρίζει περισσότερες λειτουργίες, αλλά μέχρι ενός προκαθορισμένου ορίου. Και την πλήρη ομομορφική κρυπτογράφηση (Fully Homomorphic Encryption - FHE), η οποία υποστηρίζει άπειρους υπολογισμούς, όντας η πιο ισχυρή κατηγορία.[42],[43]



Σχήμα 22: Χρήση ομομορφικής κρυπτογραφίας στον τομέα της υγείας.[42]

6.3 Τεχνητή νοημοσύνη και μηχανική μάθηση

Εφαρμογή τεχνικών και αλγορίθμων τεχνητής νοημοσύνης (Artificial Intelligence – AI) και μηχανικής μάθησης (Machine Learning – ML) για δημιουργία IDS συστημάτων σε ένα έξυπνο σύστημα υγειονομικής περίθαλψης (Smart Health System – SHS) προς αντιμετώπιση επιθέσεων σε συσκευές IoMT, ασφαλής κοινής χρήσης δεδομένων υγειονομικής περίθαλψης συσκευών IoMT στο cloud, σε περιβάλλοντα windows, αλλά και στο γενικότερο οικοσύστημα SHS. Αλγόριθμοι που έχουν χρησιμοποιηθεί στην εφαρμογή τέτοιων IDS συστημάτων είναι οι: Artificial Neural Network (ANN), Decision Tree (DT), Random Forest (RF), k-Nearest Neighbor (KNN), Naïve Bayes (NB), Logistic Regression (LR), Adaptive Boosting (AdaBoost), XGBoost (XGB) κλπ. Για βελτιωμένη λήψη αποφάσεων, οι αλγόριθμοι μηχανικής μάθησης θα πρέπει να βασίζονται και σε δεδομένα συσκευών IoMT που παράγονται και μεταδίδονται από αυτές. Αυτή η λύση προστασίας συσκευών IoMT θα δύναται να προστατεύει το firmware από παραβίαση, να προστατεύει τα αποθηκευμένα δεδομένα από τη συσκευή, να ασφαλίζει την επικοινωνία και να αποτρέπει επιθέσεις στον κυβερνοχώρο.[32],[38],[48],[49],[54],[101]

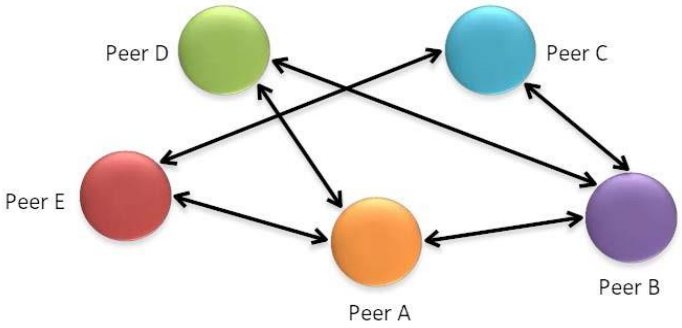
6.4 Τεχνολογία Cognitive Computing

Εφαρμογή τεχνολογίας Cognitive Computing (CC). Η τεχνολογία CC είναι υποσύνολο της AI διαφέροντας στο γεγονός ότι την τελική απόφαση την έχει ο ανθρώπινος παράγοντας αντί αυτή να είναι αυτοματοποιημένη. Η ολοένα και μεγαλύτερη ψηφιοποίηση του τομέα της υγείας έχει σημειώσει μια εκθετική αύξηση της δικτύωσης και της πολυπλοκότητας των συστημάτων, καθώς και του όγκου δεδομένων που πρέπει να διαχειριστούν. Αυτό καθιστά δύσκολο για τα άτομα να παρακολουθούν και να αναλύουν τα αρχεία καταγραφής του δικτύου σε συνεχή βάση αποτρέποντας εν δυνάμει επιθέσεις. Τα CC συστήματα μπορούν να βρουν εφαρμογή στον χειρισμό και την

επεξεργασία αυτού του τεράστιου όγκου δεδομένων και να βοηθήσουν στην αντιμετώπιση των δυναμικά μεταβαλλόμενων προκλήσεων ασφαλείας βελτιώνοντας την λήψη αποφάσεων του ανθρώπινου παράγοντα.[50]

6.5 Χρήση peer to peer δικτύων

Οι πληροφορίες ενός οργανισμού, η ανταλλαγή και η ασφαλής μετάδοση τους μπορούν να βοηθήσουν άλλους οργανισμούς να αμυνθούν πιο αποτελεσματικά από επιθέσεις διαδραματίζοντας βασικό ρόλο στην καταπολέμηση του εγκλήματος στον κυβερνοχώρο που αυξάνεται διαρκώς. Η δημιουργία και χρήση peer to peer δικτύων για διαμοιρασμό γνώσης και πληροφοριών μεταξύ φορέων παροχής υπηρεσιών υγείας μπορεί να είναι μια λύση σε αυτή την κατεύθυνση. Με την χρήση τέτοιων δικτύων, οι πληροφορίες μεταδίδονται γρήγορα μεταξύ των διαφορετικών ενδιαφερόμενων οργανισμών. Όμως μια βασική απαίτηση για την ανταλλαγή γνώσεων είναι ο τρόπος με τον οποίο οι φορείς μπορούν να μοιράζονται πληροφορίες χωρίς να τίθεται σε κίνδυνο η δική τους λειτουργία. Συχνά υπάρχει ανάγκη για τους οργανισμούς να μοιράζονται διαβαθμισμένες πληροφορίες ασφαλείας, όπως συμβάντα ασφαλείας ή πληροφορίες σχετικά με τρωτά σημεία στα διάφορα συστήματα τους. Η κοινή χρήση τέτοιων πληροφοριών ενέχει πάντα έναν κίνδυνο και απαιτεί μια εμπιστευτική σχέση μεταξύ των συμμετεχόντων οργανισμών. Κάθε οργανισμός πρέπει να είναι υπεύθυνος για τον καθορισμό του δικού του επιπέδου ασφάλειας ταξινόμησης για τις δικές του πληροφορίες που θα κοινοποιηθούν και ως εκ τούτου τον προσδιορισμό του επιπέδου κινδύνου με βάση τις πληροφορίες που μοιράζονται και τον συνδεδεμένο οργανισμό. Οι οργανισμοί που έχουν το ίδιο ή το πλησιέστερο επίπεδο ταξινόμησης μπορούν να εμπιστεύονται καλύτερα ο ένας τον άλλον. Ένας οργανισμός δεν χρειάζεται να μοιράζεται πληροφορίες με όλους τους άλλους οργανισμούς παρά μόνο σε αυτούς τους οποίους το επίπεδο κινδύνου έχει αξιολογηθεί.[30]

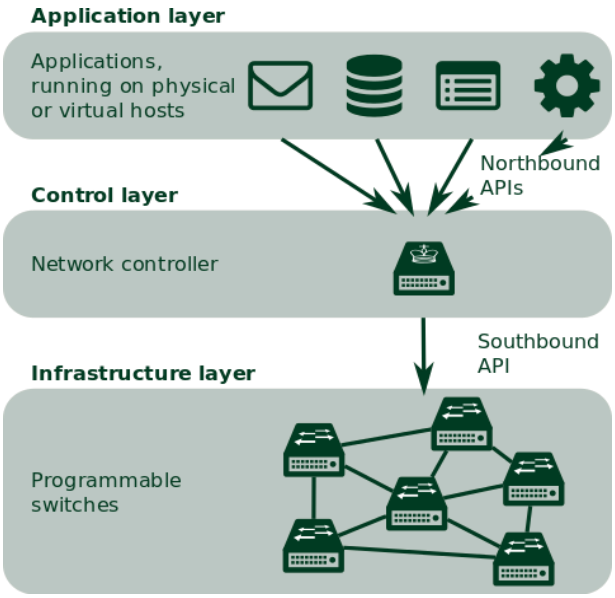


Σχήμα 23: Μοντέλο Peer to Peer.[30]

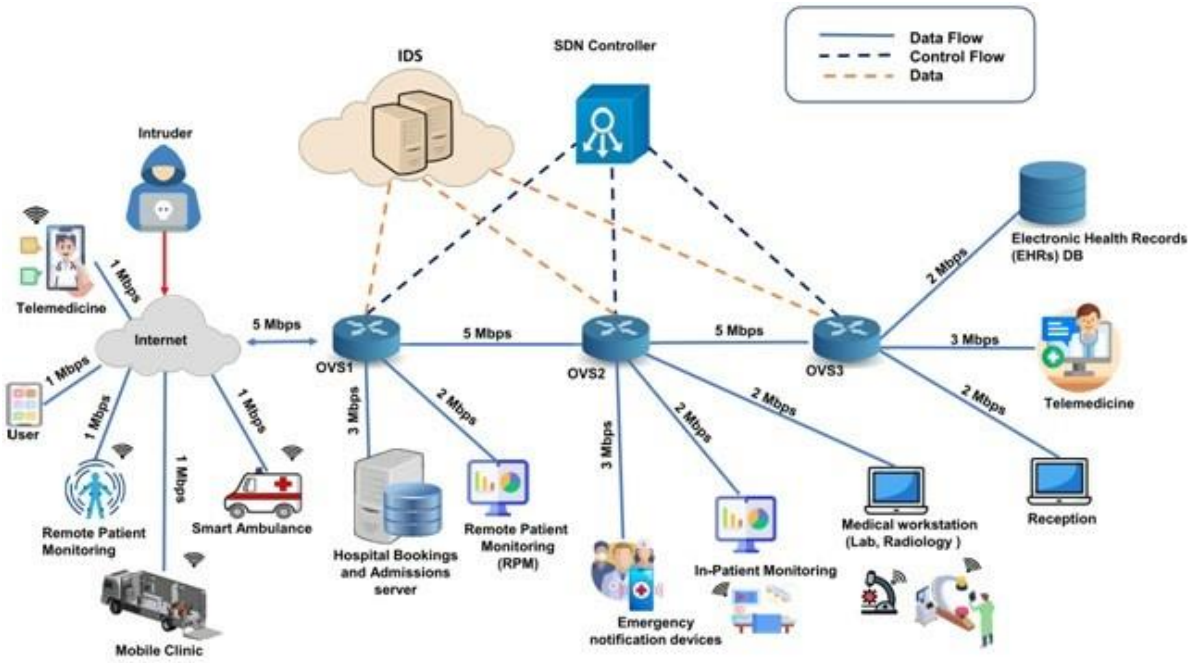
6.6 Τεχνολογία SDN

Η ανομοιογένεια εφαρμογών, συστημάτων, χάσματος τεχνολογίας, ετερογενή εξοπλισμού που είναι συνδεδεμένος στο δίκτυο, συσκευών IoMT είναι ένα βασικό πρόβλημα σε οργανισμούς υγείας που οδηγεί και σε προβλήματα κυβερνοασφάλειας. Η κεντρική διαχείριση του δικτύου μέσω ενός controller με εφαρμογή τεχνολογιών software defined networking (SDN) μπορεί να δώσει λύση σε αυτό το πρόβλημα. Η τεχνολογία SDN επιτρέπει τη δημιουργία σύνδεσης μεταξύ των μεγάλων συνόλων συσκευών, γεφυρώνει ανομοιογένειες και προσφέρει πολλαπλές υπηρεσίες δικτύου, όπως

απλή διαχείριση δικτύου, εντοπισμού συσκευών, προγραμματισμού και διαχείρισης κυκλοφορίας, ασφάλειας, εφαρμογής πολιτικών, ρύθμισης παραμέτρων ελέγχου πρόσβασης κλπ. Το SDN αναπτύχθηκε για τη μείωση της πολυπλοκότητας του δικτύου, την εφαρμογή πολιτικών δικτύου, την προσαρμοστική ευελιξία διαχείρισης κίνησης και τον προγραμματισμό στον έλεγχο του δικτύου. Συνήθως η υπάρχουσα υποδομή που είναι διαθέσιμη σε δίκτυα φορέων υγειονομικής περίθαλψης δεν είναι σε θέση να υποστηρίξει τις δυναμικές απαιτήσεις των χρηστών με αποτέλεσμα πολλοί οργανισμοί να επεκτείνουν και να αναβαθμίζουν την υποδομή του δικτύου τους με νέες τεχνολογίες. Για να γεφυρωθεί το χάσμα που δημιουργείται με την παραδοσιακή αρχιτεκτονική δικτύου, μπορεί να εφαρμοστεί η τεχνολογία SDN για να βοηθήσει το δίκτυο ενός φορέα υγειονομικής περίθαλψης στην μείωση της πολυπλοκότητας του, στην διαλειτουργικότητα του και στην καλύτερη διαχείριση του. Όταν σε ένα δίκτυο εφαρμόζεται τεχνολογία με ελεγκτή SDN και προς αποφυγή επιθέσεων σε αυτόν π.χ. DoS attacks, vulnerability scan, port proves, side-channel, MiTM επιβάλλεται η ύπαρξη συστήματος IDS στην αρχιτεκτονική του.[32],[51],[52],[53],[54]



Σχήμα 24: Αρχιτεκτονική Software Defined Networking (SDN).[53]



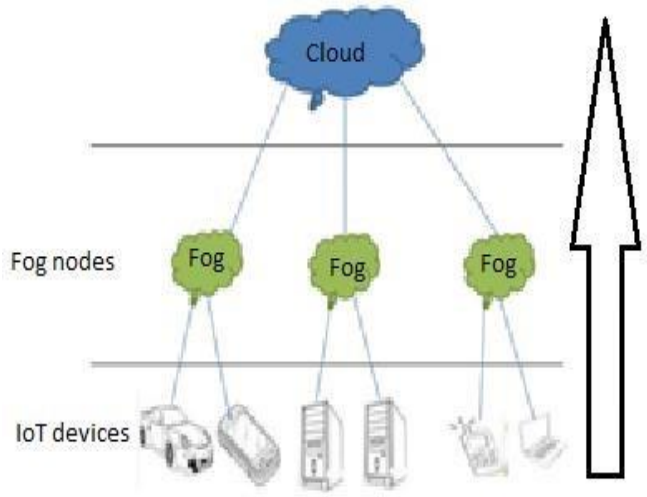
Σχήμα 25: Αρχιτεκτονική SDN οργανισμού υγείας.[54]

6.7 Τεχνολογία Fog Computing

Η τεχνολογία πληροφοριών και επικοινωνιών έχει μετατρέψει τη βιομηχανία 1.0 σε διασυνδεδεμένη βιομηχανία 4.0. Σε αυτή την μετεξέλιξη στην βιομηχανία 4.0 σημαντικό ρόλο έχει διαδραματίσει η ανάπτυξη και η χρήση έξυπνων συσκευών του Internet of Thing (IoT) καθώς και το Cloud Computing (CC). Παρόμοια κατηγοριοποίηση έχει και ο τομέας της υγείας, ο οποίος με την αξιοποίηση συσκευών Internet of Medical Things (IoMT) κατηγοριοποιείται στην γενιά 4.0.[60],[61]

Παρά τα πλεονεκτήματα του cloud (τεράστια χωρητικότητα αποθήκευσης και υψηλές υπολογιστικές υπηρεσίες με υψηλή διαθεσιμότητα, επεκτασιμότητα και προσιτή τιμή), υπάρχουν διάφορα εμπόδια στο περιβάλλον CC που κυμαίνονται από μεγάλους χρόνους απόκρισης έως ζητήματα ασφάλειας. Ως λύση σε θέματα που σχετίζονται με την απόδοση του υπολογιστικού νέφους, π.χ. υψηλός χρόνος απόκρισης και επεξεργασία δεδομένων σε πραγματικό χρόνο, η CISCO εισήγαγε την τεχνολογία Fog Computing (FC) το 2012 με την εφαρμογή πολλαπλών cloud πιο κοντά στον τελικό χρήστη. Η ειδική έκδοση του NIST 500-325 μας παρέχει μια ολοκληρωμένη εννοιολογική ανάλυση του μοντέλου Fog Computing. Το Fog Computing είναι μια τεχνολογία που επεκτείνει το cloud λειτουργώντας ενδιάμεσα μεταξύ αυτού και των τελικών συσκευών. Δεν είναι δηλαδή η πλήρης αντικατάσταση του cloud, αλλά συμπληρώνει τη λειτουργικότητα του και λειτουργεί πιο κοντά στις συσκευές άκρης παρέχοντας υπολογιστικούς πόρους σε αυτές. Ακόμη αυτή η νέα τεχνολογία ξεπερνά τα ζητήματα επεκτασιμότητας και αξιοπιστίας που υπάρχουν στην παραδοσιακή αρχιτεκτονική IoMT-cloud. Αυτή η πολλά υποσχόμενη τεχνολογία FC επιτρέπει στους τελικούς χρήστες (π.χ. Οργανισμούς Υγείας) να χρησιμοποιούν υπολογιστικές και επεξεργαστικές υπηρεσίες στην άκρη του δικτύου, γεγονός που με τη σειρά του μειώνει τον χρόνο απόκρισης και χρήσης ανάλογων υπηρεσιών στο περιβάλλον CC. Οι Fog nodes της τεχνολογίας Fog Computing συνεπώς λειτουργούν στην άκρη του δικτύου ενισχύοντας την ασφάλεια των δεδομένων, την ακρίβεια, τη συνοχή και μειώνουν το ποσοστό καθυστέρησης που είναι σημαντικός παράγοντας για εφαρμογές

όπως τα ιατρικά δεδομένα επιτυγχάνοντας έτσι καλύτερη ποιότητα υπηρεσίας (QoS).[57],[58],[61],[63] Η ανθεκτικότητα (resiliency) θεωρείται ακόμα ένα πλεονέκτημα έναντι της τεχνολογίας Cloud Computing μιας και σε περίπτωση αποτυχίας του δικτύου ή του cloud, το FC επιτρέπει την ασφαλή ανάκτηση εφαρμογών και δεδομένων.[61]



Σχήμα 26: Γενική Αρχιτεκτονική Fog Computing.[57]

Η τεχνολογία FC που είναι επέκταση του μοντέλου CC κληρονομεί τα ίδια ζητήματα ασφάλειας και απορρήτου από το cloud. Η ασφάλεια όμως στο μοντέλο FC ενισχύεται καθώς ελαχιστοποιείται η απόσταση των δεδομένων που αποστέλλονται στο cloud, καθιστώντας αυτά τα υπολογιστικά συστήματα FC πλεονεκτικά. Η τοπική επεξεργασία δεδομένων από την τεχνολογία FC και η ελαχιστοποίηση αυτής της απόστασης ελαχιστοποιεί αντίστοιχα τη μετάδοση ευαίσθητων δεδομένων μέσω του δικτύου στο cloud, μειώνοντας έτσι την ευαισθησία σε υποκλοπές συμβάλλοντας έτσι στην διατήρηση της ιδιωτικής ζωής. Διάφορα ζητήματα ασφάλειας και προστασίας της ιδιωτικής ζωής μπορούν να μετριαστούν με την ενσωμάτωση τεχνολογίας FC στην υποδομή συσκευών IoMT.[58],[62]

Επισημάνεται ότι προκειμένου να γίνει πλήρης εκμετάλλευση και αξιοποίηση των ικανοτήτων συσκευών IoMT, απαιτείται η χρήση γρήγορων και ενεργειακά αποδοτικών υπολογιστών, μεγαλύτερη χωρητικότητα αποθήκευσης, επίγνωση τοποθεσίας, που το παραδοσιακό Cloud Computing δεν μπορεί να αντιμετωπίσει.[59]

Ακόμη η αποθήκευση δεδομένων στο Fog layer συμβάλλει στην καλύτερη προστασία των δεδομένων. Προκειμένου να προστατευθεί το απόρρητο των δεδομένων, τα ευαίσθητα δεδομένα από τους τελικούς χρήστες επιβάλλεται να κρυπτογραφούνται πριν από την προώθηση τους στο Fog node. Για τη διατήρηση του απορρήτου των δεδομένων μεταξύ του Fog Computing και του Cloud Computing μπορούν να εφαρμοστούν διάφορες τεχνικές διατήρησης της ιδιωτικής ζωής όπως π.χ. το διαφορικό απόρρητο (differential privacy) ή η ομομορφική κρυπτογράφηση.[62]

Όσον αφορά στον έλεγχο ταυτότητας (Authentication) το Fog layer έχει τη δυνατότητα να ενεργοποιεί τον έλεγχο ταυτότητας σε συσκευές IoMT ή να εφαρμόζει αλγορίθμους κρυπτογράφησης ελαφριάς μορφής μεταξύ Fog node και συσκευών IoMT για τη βελτίωση αυτού.[62]

Η ανάπτυξη Fog nodes στην άκρη του δικτύου όμως δημιουργεί και προκλήσεις για τη διαχείριση του. Η χρήση τεχνολογίας Software Defined Networking (SDN) μπορεί να δώσει λύση όσον

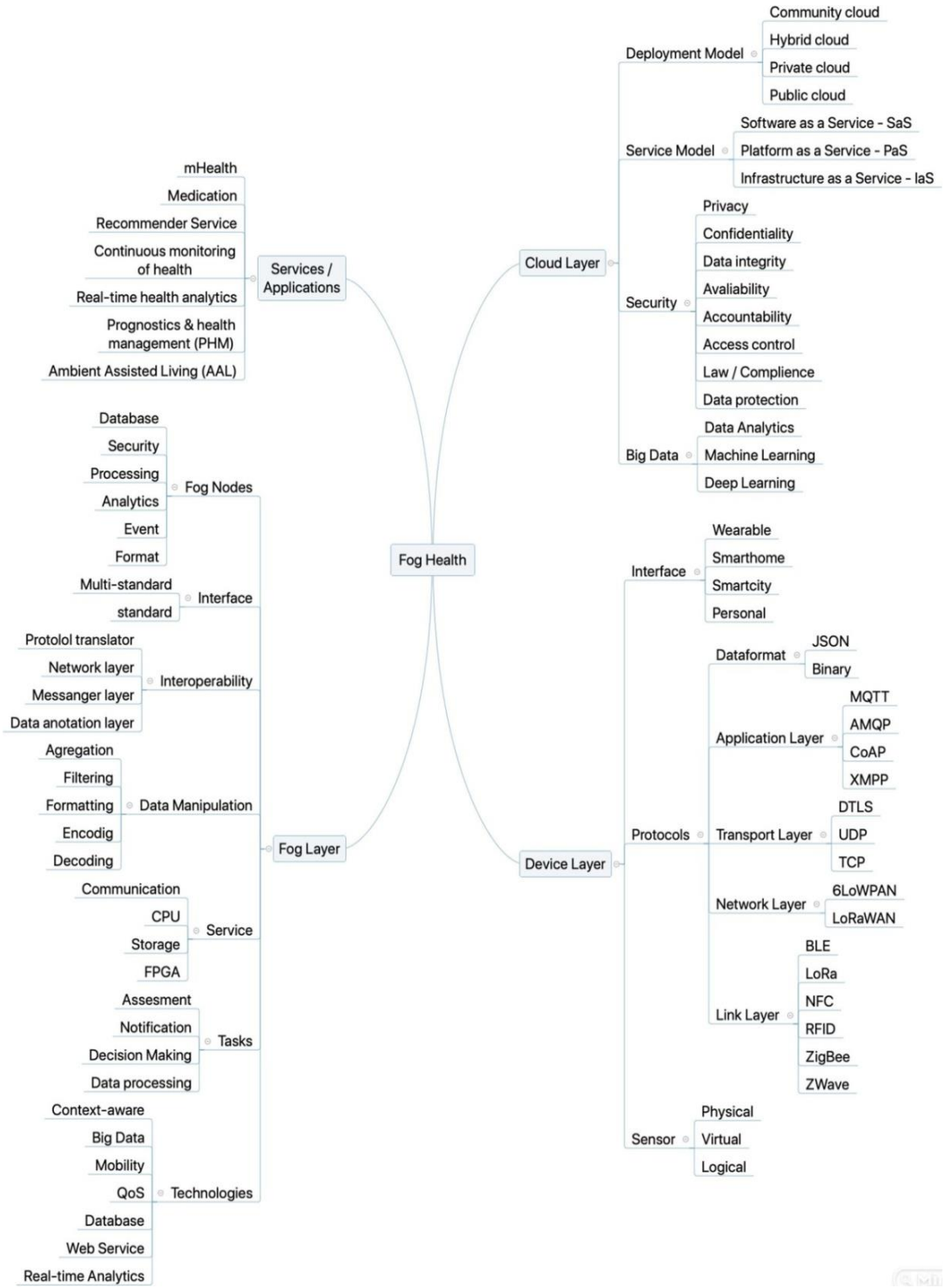
αφορά στην ασφάλεια του δικτύου από την αύξηση αυτής της επεκτασιμότητας λόγω της ανάπτυξης Fog nodes στην άκρη του.[62]

Η τεχνολογία FC επιτρέπει τη βελτιωμένη ανίχνευση ασυνήθιστης συμπεριφοράς ή κακόβουλων επιθέσεων, τόσο σε συσκευές IoMT, όσο και στην πλευρά του Cloud. Η ανίχνευση επίθεσης στην πλευρά του Fog node μπορεί να πραγματοποιηθεί με την παρακολούθηση και την ανάλυση αρχείων καταγραφής, πολιτικών ελέγχου πρόσβασης και δεδομένων σύνδεσης χρήστη. Με αυτόν τον τρόπο, οι Fog nodes είναι σε θέση να εντοπίζουν απειλές ή επιθέσεις γρηγορότερα και να τις μετριάζουν πριν καταφέρουν να περάσουν στο σύστημα. Από την πλευρά του Fog network, είναι εφικτός ο εντοπισμός κακόβουλων επιθέσεων, όπως άρνησης υπηρεσίας (denial-of-service: DoS), port scanning, κλπ.[62]

Για τον έλεγχο πρόσβασης το Fog layer διευκολύνει την υιοθέτηση πολλών τυποποιημένων μοντέλων ελέγχου πρόσβασης, ενώ δημιουργεί ευκαιρίες για το σχεδιασμό νέων μοντέλων ελέγχου πρόσβασης.[62]

Για την ασφάλεια και το απόρρητο, τα διάφορα Fog nodes μπορούν να συνεργαστούν κρυπτογραφώντας τα συλλεχθέντα δεδομένα. Ενώ με την χρήση ομομορφικής κρυπτογράφησης μπορούν να εκτελέσουν συγκεκριμένες λειτουργίες στα κρυπτογραφημένα δεδομένα και στη συνέχεια να τα υποβάλουν συγκεντρωτικά στο cloud.[62]

Η τεχνολογία Fog Computing συμπερασματικά λειτουργεί συμπληρωματικά ως προς το Cloud Computing προσφέροντας σημαντικά οφέλη, όπως είναι η χαμηλή καθυστέρηση, η αλληλεπίδραση σε πραγματικό χρόνο, η γεωγραφική κατανομή, η επεξεργασία ετερογενών δεδομένων, η διαλειτουργικότητα, η αξιοπιστία, η αποδοτικότητα, η επεκτασιμότητα, η πλήρης αξιοποίηση των ικανοτήτων συσκευών IoMT, η ασφάλεια δεδομένων, η ακρίβεια, η συνοχή, το απόρρητο, η ιδιωτικότητα και η ανθεκτικότητα.[57],[58],[59],[61],[62],[63]



Σχήμα 27: Αρχιτεκτονική Fog Computing.[62]

Συμπεράσματα

Ο ραγδαίος ψηφιακός μετασχηματισμός του τομέα της υγειονομικής περίθαλψης που επιταχύνθηκε και λόγω της πανδημίας Covid-19, είναι μια ουσιαστική εξέλιξη καθώς οι κοινωνίες μεταβαίνουν σε μια οικονομία που βασίζεται σε ριζικές καινοτομίες του τομέα των τεχνολογιών της πληροφορίας. Αυτή όμως η υιοθέτηση των πιο πρόσφατων τεχνολογιών και της εφαρμογής τους στον τομέα της υγείας παράλληλα με την ύπαρξη συστημάτων παλαιάς τεχνολογίας δημιουργεί πολύπλοκα προβλήματα και προκλήσεις ασφαλείας στον κυβερνοχώρο που πρέπει να αντιμετωπιστούν αποτελεσματικά για να μην οδηγηθεί ακόμα και σε κατάρρευση. Η κατανόηση τουλάχιστον των βασικών εννοιών για θέματα κυβερνοασφάλειας κυρίως από τους εμπλεκόμενους στον χώρο της υγειονομικής περίθαλψης, όπως και χρηματοδότησης για επένδυση σε τεχνολογία και εξειδικευμένο προσωπικό είναι βασικές παράμετροι που πρέπει να υπάρχουν για την υλοποίηση ενός ανθεκτικού σε κυβερνοεπιθέσεις τομέα υγειονομικής περίθαλψης. Ακόμη η προληπτική εφαρμογή κάθε κατηγορίας μέτρων και πολιτικών (security και privacy by design) που θα πρέπει να είναι με βάση πρότυπα και κανονισμούς, είναι βασικός παράγοντας για την κυβερνοασφάλεια στον τομέα της υγείας, αντί της εφαρμογής αυτών μετά από μια κυβερνοεπίθεση. Ενώ χρειάζεται συνεχής εγρήγορση έναντι νέων επιθέσεων, αλλά και εκπαίδευση του πιο αδύναμου κρίκου στην αλυσίδα που είναι ο ανθρώπινος παράγοντας δημιουργώντας κουλτούρα κυβερνοασφάλειας σε όλους τους εμπλεκόμενους. Το μεγαλύτερο στοίχημα στον κλάδο της υγειονομικής περίθαλψης είναι η εύρεση μιας καλής ισορροπίας μεταξύ της ασφάλειας, του απορρήτου και της χρηστικότητας.[2],[3],[14],[28],[29],[56]

Αναφορές – Βιβλιογραφία

[1] Abu Ali, K., & Alyounis, S. (2021, Ιούλιος 14-15). CyberSecurity in Healthcare Industry. *IEEE The 10th International Conference on Information Technology (ICIT 2021).* https://doi.org/10.1109/ICIT52682.2021.9491669

[2] Ravidas, D., Pattinson, M., & Oliver, P. (2021, Ιούλιος). Cyber Security in Healthcare Organisations. *Human Aspects of Information Security and Assurance (HAISA 2021),* σσ 3-11. https://doi.org/10.1007/978-3-030-81111-2_1

[3] Mohan, D. N., Gowda, S., & Vikyath, S. (2020, Ιανουάριος). Cyber Security in Health Care. *International Journal of Research in Engineering, Science and Management, 3*(1). https://www.ijresm.com/Vol.3_2020/Vol3_Iss1_January20/IJRESM_V3_I1_145.pdf

[4] Dogaru, D. I., & Dumitrache, I. (2017, Ιούνιος 22-24). Cyber security in healthcare networks. *IEEE E-Health and Bioengineering Conference (EHB 2017).* https://doi.org/10.1109/EHB.2017.7995449

[5] Υπ. Απόφαση 121793/2012, Οργανισμός του Γενικού Νοσοκομείου Αττικής «Σισμανόγλειο», Εφημερίς της Κυβερνήσεως της Ελληνικής Δημοκρατίας (ΦΕΚ Β 3475/31.12.2012). https://www.et.gr/api/DownloadFeksApi/?fek_pdf=20120203475

[6] Εθνική Αρχή Κυβερνοασφάλειας (2020, Δεκέμβριος). Εθνική Στρατηγική Κυβερνοασφάλειας 2020-2025. https://mindigital.gr/wp-content/uploads/2020/12/Εθνική-Στρατηγική-Κυβερνοασφάλειας.pdf

[7] Ευρωπαϊκή Επιτροπή (2020, Δεκέμβριος 16). Η στρατηγική κυβερνοασφάλειας της ΕΕ για την ψηφιακή δεκαετία. https://eur-lex.europa.eu/legal-content/EL/TXT/?uri=CELEX%3A52020JC0018

[8] The European Union Agency for Cybersecurity (2016, Νοέμβριος). Smart Hospitals: Security and Resilience for Smart Health Service and Infrastructures. https://www.enisa.europa.eu/publications/cyber-security-and-resilience-for-smart-hospitals

[9] The European Union Agency for Cybersecurity (2019, Ιανουάριος 31). ICT security certification opportunities in the healthcare sector. https://www.enisa.europa.eu/publications/healthcare-certification

[10] The European Union Agency for Cybersecurity (2020, Φεβρουάριος 24). Procurement Guidelines for Cybersecurity in Hospitals. https://www.enisa.europa.eu/publications/good-practices-for-the-security-of-healthcare-services

[11] The European Union Agency for Cybersecurity (2015, Δεκέμβριος 18). Security and Resilience in eHealth Infrastructures and Services. https://www.enisa.europa.eu/publications/security-and-resilience-in-ehealth-infrastructures-and-services

[12] The European Union Agency for Cybersecurity (2021, Ιανουάριος 18). Cloud Security for Healthcare Services. https://www.enisa.europa.eu/publications/cloud-security-for-healthcare-services

[13] Regulation of the European Parliament and of the Council 2016/679, General Data Protection Regulation. https://eur-lex.europa.eu/eli/reg/2016/679

[14] Muthuppalaniappan, M., & Stevenson, K. (2020, Σεπτέμβριος 27). Healthcare cyber-attacks and the COVID-19 pandemic: an urgent threat to global health. *International Journal For Quality In Health Care, 33*(1). https://doi.org/10.1093/intqhc/mzaa117

[15] Kumar, R., Sharma, S., Vachhani, C., & Yadav, N. (2022, Σεπτέμβριος). What changed in the cyber-security after COVID-19?. *Computers & Security, 120.* https://doi.org/10.1016/j.cose.2022.102821

[16] He, Y., Aliyu, A., Evans, M., & Luo, C. (2021, Απρίλιος 4). Health Care Cybersecurity Challenges and Solutions Under the Climate of COVID-19: Scoping Review. *Journal of Medical Internet Research, 23*(4). https://doi.org/10.2196/21747

[17] Gafni, R., & Pavel, T. (2021, Αύγουστος 9). Cyberattacks against the health-care sectors during the COVID-19 pandemic . *Information and Computer Security, 30*(1), σσ 137-150. https://doi.org/10.1108/ICS-05-2021-0059

[18] United States Department of Justice, Federal Bureau of Investigation (2021). *Internet Crime Report 2021*. https://www.ic3.gov/Media/PDF/AnnualReport/2021_IC3Report.pdf

[19] United States Department of Justice, Federal Bureau of Investigation (2022). *Internet Crime Report 2022*. https://www.ic3.gov/Media/PDF/AnnualReport/2022_IC3Report.pdf

[20] Murray-Watson, R. (2022, Ιανουάριος 24). 2022 Healthcare Data Breach Report. *The HIPAA Journal.* https://www.hipaajournal.com/2022-healthcare-data-breach-report/

[21] Marron, J. A. (2022). Implementing the Health Insurance Portability and Accountability Act (HIPAA) Security Rule: A Cybersecurity Resource Guide. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-66, Rev. 2. https://doi.org/10.6028/NIST.SP.800-66r2.ipd

[22] Joint Task Force (2020). Security and Privacy Controls for Information Systems and Organizations. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-53, Rev. 5. https://doi.org/10.6028/NIST.SP.800-53r5

[23] International Organization for Standardization (2013). Information technology — Security techniques — Information security management systems — Requirements (ISO Standard No. 27001:2013). https://www.iso.org/standard/54534.html

[24] International Organization for Standardization (2022). Information security, cybersecurity and privacy protection — Information security controls (ISO Standard No. 27002:2022) https://www.iso.org/standard/75652.html

[25] International Organization for Standardization (2022). Information security, cybersecurity and privacy protection — Guidance on managing information security risks (ISO Standard No. 27005:2022) https://www.iso.org/standard/80585.html

[26] Argaw, S. T., Troncoso-Pastoriza, J. R., Lacey, D, Florin, M-V, Calcavecchia, F., Anderson, D., Burleson, W., Vogel, J-M., O'Leary, C., Eshaya-Chauvin, B., & Flahault, A. (2020). Cybersecurity of Hospitals: discussing the challenges and working towards mitigating the risks. *BMC Medical Informatics and Decision Makin, 20*(146). https://doi.org/10.1186/s12911-020-01161-7

[27] Ahmed, Y., Naqvi, S., & Josephs, M. (2019, Μάϊος 8-10). Cybersecurity Metrics for Enhanced Protection of Healthcare IT Systems. *IEEE 2019 13th International Symposium on Medical Information and Communication Technology (ISMICT).* https://doi.org/10.1109/ISMICT.2019.8744003

[28] Bhuyan, S. S., Kabir, U. Y., Escareno, J. M., Ector, K., Palakodeti, S., Wyant, D., Kumar, S., Levy, M., Kedia, S., Dasgupta, D., & Dobalian, A. (2020, Απρίλιος 2). Transforming Healthcare Cybersecurity from Reactive to Proactive: Current Status and Future Recommendations. *Journal of Medical Systems, 44*(98). https://doi.org/10.1007/s10916-019-1507-y

[29] Kioskli, K., Fotis, T., & Mouratidis, H. (2021, Αύγουστος 17-20). The landscape of cybersecurity vulnerabilities and challenges in healthcare: Security standards and paradigm shift recommendations. *Conference ARES '21: Proceedings of the 16th International Conference on Availability, Reliability and Security,* (136), σσ 1–9. https://doi.org/10.1145/3465481.3470033

[30] Hautamäki, J., & Kokkonen, T. (2020, Ιούνιος 12-13). Model for Cyber Security Information Sharing in Healthcare Sector. *IEEE 2020 International Conference on Electrical, Communication, and Computer Engineering (ICECCE).* https://doi.org/10.1109/ICECCE49384.2020.9179175

[31] Wani, T. A., Mendoza, A., & Gray, K. (2020, Ιούνιος 18). Hospital Bring-Your-Own-Device Security Challenges and Solutions: Systematic Review of Gray Literature. *JMIR Mhealth Uhealth, 8*(6). https://doi.org/10.2196/18175

[32] Thamer, N., & Alubady, R. (2021, Απρίλιος 28-29). A Survey of Ransomware Attacks for Healthcare Systems: Risks, Challenges, Solutions and Opportunity of Research. *IEEE 2021 1st Babylon International Conference on Information Technology and Science (BICITS).* https://doi.org/10.1109/BICITS51482.2021.9509877

[33] Boeckl, K., Fagan, M., Fisher, W., Lefkovitz, N., Megas, K. N., Nadeau, E., O'Rourke, D. G., Piccarreta, B., & Scarfone, K. (2019). Considerations for Managing Internet of Things (IoT) Cybersecurity and Privacy Risks. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) NIST.IR.8228. https://doi.org/10.6028/NIST.IR.8228

[34] Papaioannou, M., Karageorgou, M., Mantas, G., Sucasas, V., Essop, I., Rodriguez, J., & Lymberopoulos, D. (2020, Ιούλιος 20). A Survey on Security Threats and Countermeasures in Internet of Medical Things (IoMT). *Transactions on Emerging Telecommunications Technologies.* https://doi.org/10.1002/ett.4049

[35] Razdan, S., & Sharma, S. (2022). Internet of Medical Things (IoMT): Overview, Emerging Technologies, and Case Studies. *IETE Technical Review, 39*(4), σσ 775-788. https://doi.org/10.1080/02564602.2021.1927863

[36] Rejeb, A., Rejeb, K., Treiblmaier, H., Appolloni, A., Alghamdi, S., Alhasawi, Y., & Iranmanesh, M. (2023, Ιούλιος). The Internet of Things (IoT) in healthcare: Taking stock and moving forward. *Internet of Things: Engineering Cyber Physical Human Systems,22*(100721). https://doi.org/10.1016/j.iot.2023.100721

[37] Hatzivasilis, G., Soultatos, O., Ioannidis, S., Verikoukis, C., Demetriou, G., & Tsatsoulis, C. I. (2019, Μάϊος 29-31). Review of Security and Privacy for the Internet of Medical Things (IoMT). *IEEE 2019 15th International Conference on Distributed Computing in Sensor Systems (DCOSS)*. https://doi.org/10.1109/DCOSS.2019.00091

[38] Ghourabi, A. (2022, Μάϊος). A Security Model Based on LightGBM and Transformer to Protect Healthcare Systems From Cyberattacks. *IEEE Access, 10*. https://doi.org/10.1109/ACCESS.2022.3172432

[39] Tunc, M. A., Gures, E., & Shayea, I. (2021, Σεπτέμβριος 5). A Survey on IoT Smart Healthcare: Emerging Technologies, Applications, Challenges, and Future Trends. *Journal of Networking and Internet Architecture, arXiv:2109.02042*. https://doi.org/10.48550/arXiv.2109.02042

[40] Strielkina, A., Illiashenko, O., Zhydenko, M., & Uzun, D. (2018, Μάϊος 24-27). Cybersecurity of Healthcare IoT-Based Systems: Regulation and Case-Oriented Assessment. *2018 IEEE 9th International Conference on Dependable Systems, Services and Technologies (DESSERT).* https://doi.org/10.1109/DESSERT.2018.8409101

[41] Marshal, R., Gobinath, K., & Venkateswara Rao, V. (2021, Απρίλιος 21-24). Proactive Measures to Mitigate Cyber Security Challenges in IoT based Smart Healthcare Networks. *2021 IEEE International IOT, Electronics and Mechatronics Conference (IEMTRONICS)* https://doi.org/10.1109/IEMTRONICS52119.2021.9422615

[42] Munjal, K., & Bhatia, R. (2022, Μάϊος 3). A systematic review of homomorphic encryption and its contributions in healthcare industry. *Complex & Intelligent Systems, 9*(4), σσ 3759–3786. https://doi.org/10.1007/s40747-022-00756-z

[43] Lauter, K., Dai, W., & Laine, K. (2021). Protecting Privacy through Homomorphic Encryption. *Springer*. https://doi.org/10.1007/978-3-030-77287-1

[44] Dilawar, N., Rizwan, M., Ahmad, F., & Akram, S. (2019, Ιανουάριος). Blockchain: Securing Internet of Medical Things (IoMT). *International Journal of Advanced Computer Science and Applications (IJACSA), 10*(1). https://dx.doi.org/10.14569/IJACSA.2019.0100110

[45] Haleem, A., Javaid, M., Singh, R. P., Suman, R., & Rab, S. (2021). Blockchain technology applications in healthcare: An overview. *International Journal of Intelligent Networks, 2,* σσ 130-139. https://doi.org/10.1016/j.ijin.2021.09.005

[46] Nwosu, A. U., Goyal, S. B., & Bedi, P. (2021). Blockchain Transforming Cyber-Attacks: Healthcare Industry. *Innovations in Bio-Inspired Computing and Applications. Advances in Intelligent Systems and Computing, Springer, 1372*, σσ 258–266. https://doi.org/10.1007/978-3-030-73603-3_24

[47] Lodha, G., Pillai, M., Solanki, A., Sahasrabudhe, S., & Jarali, A. (2021, Μάϊος 6-8). Healthcare System Using Blockchain. *IEEE 2021 5th International Conference on Intelligent Computing and Control Systems (ICICCS)*. https://doi.org/10.1109/ICICCS51141.2021.9432157

[48] Sundas, A., Badotra, S., Bharany, S., Almogren, A., Tag-ElDin, E. M., & Rehman, A. U. (2022, Σεπτέμβριος). HealthGuard: An Intelligent Healthcare System Security Framework Based on Machine Learning. *Sustainability, 14*(19). https://doi.org/10.3390/su141911934

[49] AlZubi, A.A., Al-Maitah, M. & Alarifi, A. (2021, Ιούνιος 26). Cyber-attack detection in healthcare using cyber-physical system and machine learning techniques. *Soft Computing, 25*, σσ 12319–12332. https://doi.org/10.1007/s00500-021-05926-8

[50] Sreedevi, A. G., Harshitha, T. N., Sugumaran, V., & Shankar, P. (2022, Μάρτιος). Application of cognitive computing in healthcare, cybersecurity, big data and IoT: A literature review. *Information Processing and Management, 59*(102888). https://doi.org/10.1016/j.ipm.2022.102888

[51] Badotra, S., Nagpal, D., Panda, S. N., Tanwar, S., & Bajaj, S. (2020, Ιούνιος 4-5). IoT-Enabled Healthcare Network With SDN. *IEEE 2020 8th International Conference on Reliability, Infocom Technologies and Optimization (Trends and Future Directions) (ICRITO).* https://doi.org/10.1109/ICRITO48877.2020.9197807

[52] Isravel, D.P., Silas, S., & Rajsingh, E.B. (2020). SDN-Based Traffic Management for Personalized Ambient Assisted Living Healthcare System. *Intelligence in Big Data Technologies—Beyond the Hype. Advances in Intelligent Systems and Computing, Springer, 1167,* σσ 379–388. https://doi.org/10.1007/978-981-15-5285-4_38

[53] Barka, E., Dahmane, S., Kerrache, C. A., Khayat, M., & Sallabi, F. (2021, Ιούλιος 26). STHM: A Secured and Trusted Healthcare Monitoring Architecture Using SDN and Blockchain. *Electronics, 10*(15), 1787. https://doi.org/10.3390/electronics10151787

[54] Halman, L. M., & Alenazi, M. J. F. (2023, Απρίλιος 13). MCAD: A Machine Learning Based Cyberattacks Detector in Software-Defined Networking (SDN) for Healthcare Systems. *IEEE Access, 11*, σσ 37052-37067. https://doi.org/10.1109/ACCESS.2023.3266826

[55] Akinsanya, O. O., Papadaki, M., & Sun, L. (2019, Μάρτιος 29-30). Current Cybersecurity Maturity Models: How Effective in Healthcare Cloud?. *5th Collaborative European Research Conference (CERC 2019). Part 4:Smart Healthcare and Safety Systems,* σσ 211-222. https://ceur-ws.org/Vol-2348/paper16.pdf

[56] Garcia-Perez, A., Cegarra-Navarro, J. G., Sallos, M. P., Martinez-Caro, E., & Chinnaswamy, A. (2023, Μάρτιος). Resilience in healthcare systems: Cyber security and digital transformation. *Technovation, 121*(102583). https://doi.org/10.1016/j.technovation.2022.102583

[57] Winnie, Y., Umamaheswari, E., & Ajay, D. M. (2018, Σεπτέμβριος 10-11). Enhancing Data Security in IoT Healthcare Services Using Fog Computing. *IEEE 2018 International Conference on Recent Trends in Advance Computing (ICRTAC).* https://doi.org/10.1109/ICRTAC.2018.8679404

[58] Alazeb, A., Panda, B., Almakdi, S., & Alshehri, M. (2021, Μάϊος 30). Data Integrity Preservation Schemes in Smart Healthcare Systems That Use Fog Computing Distribution. *Electronics, 10*(11), 1314. https://doi.org/10.3390/electronics10111314

[59] Hartmann, M., Hashmi, U. S., & Imran, A. (2022, Μάρτιος). Edge computing in smart health care systems: Review, challenges, and research directions. *Transactions on Emerging Telecommunications Technologies, 33*(3), e3710. https://doi.org/10.1002/ett.3710

[60] Anand, D., & Khemchandani, V. (2020, Αύγουστος 26). Data Security and Privacy Functions in Fog Computing for Healthcare 4.0. *Fog Data Analytics for IoT Applications, Studies in Big Data, Spring*er, *76,* σσ 387–420. https://doi.org/10.1007/978-981-15-6044-6_16

[61] Kumari, A., Tanwar, S., Tyagi, S., & Kumar, N. (2018, Νοέμβριος). Fog computing for Healthcare 4.0 environment: Opportunities and challenges. *Computers & Electrical Engineering, 72*, σσ 1–13. https://doi.org/10.1016/j.compeleceng.2018.08.015

[62] de Moura Costa, H. J., da Costa, C. A., da Rosa Righi, R., & Antunes, R. S. (2020, Μάϊος 31). Fog computing in health: A systematic literature review. *Health and Technology, 10*, σσ 1025–1044. https://doi.org/10.1007/s12553-020-00431-8

[63] Iorga, M., Feldman, L., Barton, R., Martin, M. J., Goren, N., & Mahmoudi, C. (2018, Μάρτιος). Fog Computing Conceptual Model. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 500-325. https://doi.org/10.6028/NIST.SP.500-325

[64] Shamim, A., Fayyaz, B., & Balakrishnan, V. (2014, Σεπτέμβριος 19-20). Layered Defense in Depth Model for IT Organizations. *2nd International Conference on Innovations in Engineering and Technology (ICCET'2014).* http://iieng.org/images/proceedings_pdf/8285E0914047.pdf

[65] Zhou, X., Xu, Z., Wang, L., Chen, K., Chen, C., & Zhang, W. (2018). Construction and Evaluation of Defense-in Depth architecture in SCADA System. *2018 International Conference on Smart Materials, Intelligent Manufacturing and Automation (SMIMA 2018). MATEC Web of Conferences 173,*(01012). https://doi.org/10.1051/matecconf/201817301012

[66] Mindmajix. (2023, Απρίλιος 03). Cyber Security Frameworks. Ανακτήθηκε από https://mindmajix.com/cyber-security-frameworks

[67] Barrett, M. (2018, Απρίλιος 18). Framework for Improving Critical Infrastructure Cybersecurity Version 1.1. *National Institute of Standards and Technology.* https://doi.org/10.6028/NIST.CSWP.04162018

[68] Donaldson, S. E., Siegel, S. G., Williams, C. K., & Aslam, A. (2015, Μάϊος). Cybersecurity Frameworks. *Enterprise Cybersecurity,* σσ 297–309. Apress, Berkeley, CA. https://doi.org/10.1007/978-1-4302-6083-7_17

[69] Cleghorn, L. (2013, Ιούλιος). Network Defense Methodology: A Comparison of Defense in Depth and Defense in Breadth. *Journal of Information Security, 4*(3), σσ 144–149. http://dx.doi.org/10.4236/jis.2013.43017

[70] Coole, M., Corkill, J., & Woodward, A. (2012, Δεκέμβριος 3-5). Defence in Depth, Protection in Depth and Security in Depth: A Comparative Analysis Towards a Common Usage Language. *5th Australian Security and Intelligence Conference.* https://doi.org/10.4225/75/57a034ccac5cd

[71] Mell, P., Shook, J., & Harang, R. (2016, Δεκέμβριος). Measuring and Improving the Effectiveness of Defense-in-Depth Posture s. *Proceedings of the 2nd Annual Industrial Control System Security Workshop (ICSS '16),* σσ 15–22. https://doi.org/10.1145/3018981.3018986

[72] Cybersecurity and Infrastructure Security Agency (2016, Σεπτέμβριος). *Recommended Practice: Improving Industrial Control System Cybersecurity with Defense-in-Depth Strategies.* U.S. Department of Homeland Security.

https://www.cisa.gov/sites/default/files/recommended_practices/NCCIC_ICS-CERT_Defense_in_Depth_2016_S508C.pdf
[73] Groat, S., Tront, J., & Marchany, R. (2012, Ιούλιος 16-19). Advancing the defense in depth model. *2012 7th International Conference on System of Systems Engineering (SoSE).* https://doi.org/10.1109/SYSoSE.2012.6384127
[74] Cho, J-H., & Ben-Asher, N. (2018). Cyber defense in breadth: Modeling and analysis of integrated defense systems. *The Journal of Defense Modeling and Simulation, 15*(2), σσ 147–160. https://doi.org/10.1177/1548512917699725
[75] McCallam, D. H. (2012). *An Analysis of Cyber Reference Architectures.* NATO 2012 Workshop with Industry on Cybersecurity Capabilities, The Hague, Netherlands. https://www.sto.nato.int/publications/STO%20Educational%20Notes/STO-EN-IST-170/EN-IST-170-09.pdf
[76] Sokol, A. W., & Hogan, M. D. (2013, Ιούλιος 22). NIST Cloud Computing Standards Roadmap. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 500–291, Rev. 2. http://dx.doi.org/10.6028/NIST.SP.500-291r2
[77] Badger, M. L., Grance, T., Patt-Corner, R., & Voas, J. (2012, Μάϊος). Cloud Computing Synopsis and Recommendations. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800–146. https://doi.org/10.6028/NIST.SP.800-146
[78] Mavroeidakos, T., Michalas, A., & Vergados, D. D. (2016, Απρίλιος 10-14). Security Architecture based on Defense in Depth for Cloud Computing Environment. *2016 IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS).* https://doi.org/10.1109/INFCOMW.2016.7562097
[79] Mosteiro-Sanchez, A., Barcelo, M., Astorga, J., & Urbieta, A. (2020, Οκτώβριος). Securing IIoT using Defence-in-Depth: Towards an End-to-End secure Industry 4.0. *Journal of Manufacturing Systems, 57,* σσ 367–378. https://doi.org/10.1016/j.jmsy.2020.10.011
[80] Rose, S., Borchert, O., Mitchell, S., & Connelly S. (2020, Αύγουστος). Zero Trust Architecture. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-207. https://doi.org/10.6028/NIST.SP.800-207
[81] He, Y., Huang, D., Chen, L., Ni, Y., & Ma, X. (2022, Ιούνιος 15). A Survey on Zero Trust Architecture: Challenges and Future Trends. *Wireless Communications and Mobile Computing, 2022*(6476274). https://doi.org/10.1155/2022/6476274
[82] UK National Cyber Security Centre (2021, Ιούλιος 23). *Zero trust architecture design principles.* U.K. Government Communications Headquarters. https://www.ncsc.gov.uk/collection/zero-trust-architecture
[83] Shore, M., Zeadally, S., & Keshariya, A. (2021, Νοέμβριος). Zero Trust: The What, How, Why, and When. *IEEE Computer, 54*(11), σσ 26–35. https://doi.org/10.1109/MC.2021.3090018
[84] Kindervag, J., Balaouras, S., & Coit., L. (2010, Σεπτέμβριος 17). No More Chewy Centers: Introducing The Zero Trust Model Of Information Security. *Forrester Research Inc, 3.* https://media.paloaltonetworks.com/documents/Forrester-No-More-Chewy-Centers.pdf
[85] Kindervag, J., Balaouras, S., & Coit., L. (2010, Νοέμβριος 5). Build Security Into Your Network's DNA: The Zero Trust Network Architecture. *Forrester Research Inc, 27.* https://www.actiac.org/system/files/Forrester_zero_trust_DNA.pdf
[86] Garbis, J., & Chapman, J. W. (2021, Φεβρουάριος 26). *Zero Trust Security: An Enterprise Guide.* Apress, Berkeley, CA. https://doi.org/10.1007/978-1-4842-6702-8
[87] National Security Agency (2023, Απρίλιος). *Advancing Zero Trust Maturity Throughout the User Pillar.* U.S. Department of Defense. https://media.defense.gov/2023/Mar/14/2003178390/-1/-1/0/CSI_Zero_Trust_User_Pillar_v1.1.PDF
[88] Cybersecurity and Infrastructure Security Agency (2023, Απρίλιος). *Zero Trust Maturity Model.* U.S. Department of Homeland Security. https://www.cisa.gov/sites/default/files/2023-04/zero_trust_maturity_model_v2_508.pdf

[89] Kindervag, J., Balaouras, S., Mak, K., & Blackborow, J. (2016, Μάρτιος 23). No More Chewy Centers: The Zero Trust Model Of Information Security. *Forrester Research, Inc.* https://crystaltechnologies.com/wp-content/uploads/2017/12/forrester-zero-trust-model-information-security.pdf
[90] Wylde, A. (2021, Ιούνιος 14-18). Zero trust: Never trust, always verify. *2021 International Conference on Cyber Situational Awareness, Data Analytics and Assessment (CyberSA).* https://doi.org/10.1109/CyberSA52016.2021.9478244
[91] Sarkar, S., Choudhary, G., Shandilya, S. K., Hussain, A., & Kim, H. (2022, Σεπτέμβριος 7). Security of Zero Trust Networks in Cloud Computing: A Comparative Review. *Sustainability, 14*(18). https://doi.org/10.3390/su141811213
[92] Mehraj, S., & Banday, M. T. (2020, Ιανουάριος 22-24). Establishing a Zero Trust Strategy in Cloud Computing Environment. *2020 International Conference on Computer Communication and Informatics (ICCCI)*. https://doi.org/10.1109/ICCCI48352.2020.9104214
[93] Li, S., Iqbal, M., & Saxena, N. (2022, Μάρτιος 10). Future Industry Internet of Things with Zero-trust Security. *Information Systems Frontiers*. https://doi.org/10.1007/s10796-021-10199-5
[94] Yan, X., & Wang, H. (2020, Σεπτέμβριος 13). Survey on Zero-Trust Network Security. *Artificial Intelligence and Security. ICAIS 2020. Communications in Computer and Information Science, 1252*, σσ 50–60. https://doi.org/10.1007/978-981-15-8083-3_5
[95] GeeksforGeeks (2023, Μάρτιος 18). *Zero Security Model.* Ανακτήθηκε από https://www.geeksforgeeks.org/zero-security-model/
[96] Bertino, E. (2021, Σεπτέμβριος 3). Zero Trust Architecture: Does It Help? *IEEE Security & Privacy, 19*(5), σσ 95–96. https://doi.org/10.1109/MSEC.2021.3091195
[97] National Security Agency (2023, Οκτώβριος). *Advancing Zero Trust Maturity Throughout the Device Pillar.* U.S. Department of Defense. https://media.defense.gov/2023/Oct/19/2003323562/-1/-1/1/CSI-DEVICE-PILLAR-ZERO-TRUST.PDF
[98] Πατρικάκης, Ζ. Χ., Λελίγκου, Αικ.-Ε., & Κόγιας, Γ. Δ. (2022). *Αλυσίδες συστοιχιών (Blockchain) – Εισαγωγή στις τεχνολογίες και παραδείγματα* [Μεταπτυχιακό εγχειρίδιο]. Κάλλιπος, Ανοικτές Ακαδημαϊκές Εκδόσεις. http://dx.doi.org/10.57713/kallipos-171
[99] Golosova, J., & Romanovs, A. (2018, Νοέμβριος 8-10). The Advantages and Disadvantages of the Blockchain Technology. *2018 IEEE 6th Workshop on Advances in Information, Electronic and Electrical Engineering (AIEEE)*. https://doi.org/10.1109/AIEEE.2018.8592253
[100] Sarmah, S. S. (2018). Understanding Blockchain Technology. *Computer Science and Engineering, 8*(2), σσ 23–29. doi: 10.5923/j.computer.20180802.02
[101] Silvestri, S., Islam, S., Papastergiou, S., Tzagkarakis, C., & Ciampi, M. (2023, Ιανουάριος 6) A Machine Learning Approach for the NLP-Based Analysis of Cyber Threats and Vulnerabilities of the Healthcare Ecosystem. *Sensors, 23*(2). https://doi.org/10.3390/s23020651