Τμήμα Διοικητικής Επιστήμης και Τεχνολογίας

Πρόγραμμα Μεταπτυχιακών Σπουδών

«ΨΗΦΙΑΚΗ ΚΑΙΝΟΤΟΜΙΑ ΚΑΙ ΔΙΟΙΚΗΣΗ»

Διπλωματική Εργασία

«Επιθέσεις στα Πληροφοριακά Συστήματα Υγείας και τεχνικές εντοπισμού και αντιμετώπισής τους»

Μπομπογιάννη Βασιλεία

ΠΑΤΡΑ 2022

Επιτροπή Επίβλεψης Διπλωματικής Εργασίας

Επιβλέπων Καθηγητής

Σταματίου Ιωάννης

Α΄ Συν-Επιβλέπων

Αντωνοπούλου Ήρα

Β΄ Συν-Επιβλέπων

Παπαδόπουλος Δημήτριος

ΕΥΧΑΡΙΣΤΙΕΣ

Θα ήθελα να ευχαριστήσω θερμά τον επιβλέποντα καθηγητή της παρούσας Διπλωματικής Εργασίας κ. Σταματίου Ιωάννη, για τις χρήσιμες συμβουλές, την καθοδήγησή του και κυρίως για την στήριξή του σε όλες τις δυσκολίες που αντιμετώπισα κατά της διάρκεια της συγγραφής της.

Επίσης κρίνω σκόπιμο να εκφράσω τις ευχαριστίες μου προς τα έτερα μέλοι της επιτροπής, κα Ήρα Αντωνοπούλου Πρόεδρο του Τμήματος και κ. Παπαδόπουλο Δημήτριο Καθηγητή του Τμήματος, για την τιμή που μου έκαναν να μετέχουν στην επιτροπή της Διπλωματικής μου εργασίας.

Τέλος, θα ήθελα να ευχαριστήσω ιδιαίτερα τον σύζυγό μου Βασίλη και τα δυο μου παιδιά Ιωάννα και Δημήτρη, που παρ' όλες τις πρωτόγνωρες δυσκολίες της περιόδου της πανδημίας, όντας εργαζόμενοι εγώ και ο σύζυγός μου στο χώρο της υγείας, στάθηκαν αρωγοί δίπλα μου. Η στήριξή τους ήταν μεγάλη και τους ευχαριστώ θερμά για την αμέριστη συμπαράστασή τους και την υπομονής τους.

Περίληψη

Η ασφάλεια στον κυβερνοχώρο γίνεται όλο και περισσότερο μια μεγάλη ανησυχία μεταξύ των παρόχων υγειονομικής περίθαλψης, στην υιοθέτηση ψηφιακών τεχνολογιών για τη βελτίωση της ποιότητας της φροντίδας που παρέχεται στους ασθενείς. Αναφορές για κυβερνοεπιθέσεις, όπως *ransomware* και *WannaCry*, εμφάνισαν τον καταστροφικό χαρακτήρα τέτοιων επιθέσεων στην υγειονομική περίθαλψη. Τέτοιου είδους επιθέσεις κατηγοριοποιούνται ως επιθέσεις κοινωνικής μηχανικής. Μετά την αύξηση της συχνότητας και της εφευρετικότητας των επιθέσεων που εκτοξεύονται εναντίον νοσοκομειακών περιβαλλόντων, με σκοπό να προκαλέσουν διακοπή των υπηρεσιών, υπάρχει έντονη ανάγκη να μελετηθεί το επίπεδο των προγραμμάτων ευαισθητοποίησης και των δραστηριοτήτων κατάρτισης που προσφέρονται στο προσωπικό από οργανισμούς υγειονομικής περίθαλψης.

Ο στόχος αυτής της διπλωματικής είναι να εντοπιστούν οι συνήθεις παράγοντες που επηρεάζουν τις θέσεις κυβερνοασφάλειας ενός οργανισμού υγειονομικής περίθαλψης, που προκύπτουν από την άγνοια της απειλής στον κυβερνοχώρο για την υγειονομική περίθαλψη. Η βιβλιογραφική ανασκόπηση στοχεύει να εδραιώσει την τρέχουσα βιβλιογραφία που αναφέρεται για την ανθρώπινη συμπεριφορά με αποτέλεσμα να δημιουργούνται κενά ασφαλείας που μετριάζουν τη στρατηγική για την κυβερνοάμυνα που υιοθετούν οι οργανισμοί υγειονομικής περίθαλψης. Επιπλέον, η εργασία εξετάζει επίσης τη μεθοδολογία της οργανωτικής αξιολόγησης κινδύνων που εφαρμόζεται και τις πολιτικές που υιοθετούνται για την ενίσχυση της ασφάλειας στον κυβερνοχώρο.

Το θέμα της κυβερνοασφάλειας στο πλαίσιο της υγειονομικής περίθαλψης και του κλινικού περιβάλλοντος έχει προσελκύσει το ενδιαφέρον αρκετών ερευνητών, με αποτέλεσμα να έχουμε ένα ευρύ φάσμα βιβλιογραφίας. Χρησιμοποιήθηκαν λέξεις-κλειδιά που σχετίζονται με την ευαισθητοποίηση στον κυβερνοχώρο, την κατάρτιση, τις μεθοδολογίες εκτίμησης κινδύνου του οργανισμού, τις πολιτικές και τις συστάσεις που υιοθετήθηκαν ως αντίμετρα στη φροντίδα της υγείας. Η έρευνα περιορίστηκε στα τελευταία περίπου 10 χρόνια. Αρκετά από τα άρθρα που επιλέχθηκαν για τη μελέτη αυτή, έχουν σας στόχο την αντιμετώπιση της πολυπλοκότητας των μέτρων κυβερνοασφάλειας που υιοθετήθηκαν στο πλαίσιο της υγειονομικής περίθαλψης και των κλινικών περιβαλλόντων. Τονίζουν την εξελισσόμενη φύση των απειλών στον κυβερνοχώρο,

που προέρχονται από την εκμετάλλευση υποδομών πληροφορικής σε πιο προηγμένες επιθέσεις, που ξεκίνησαν με σκοπό την εκμετάλλευση της ανθρώπινης ευπάθειας. Η σταθερή αύξηση της βιβλιογραφίας σχετικά με την απειλή επιθέσεων ηλεκτρονικού "ψαρέματος" αποδεικνύει την αυξανόμενη απειλή των επιθέσεων κοινωνικής μηχανικής.

Ως αντίμετρο, εντοπίστηκαν άρθρα που παρέχουν μεθοδολογίες που προκύπτουν από μελέτες περιπτώσεων για την προώθηση της ευαισθητοποίησης στον κυβερνοχώρο μεταξύ των ενδιαφερομένων. Τα άρθρα που περιλαμβάνονται υπογραμμίζουν την ανάγκη υιοθέτησης πρακτικών στον τομέα της υγιεινής στον κυβερνοχώρο μεταξύ των επαγγελματιών υγειονομικής περίθαλψης, ενώ έχουν πρόσβαση σε πλατφόρμες κοινωνικών μέσων, η οποία αποτελεί ένα ιδανικό πεδίο δοκιμής για τους επιτιθέμενους με στόχο να αποκτήσουν εικόνα για τη ζωή των επαγγελματιών υγείας. Επιπλέον, περιλαμβάνονται επίσης άρθρα που παρουσιάζουν στρατηγικές που υιοθετήθηκαν από οργανισμούς υγειονομικής περίθαλψης για την αντιμετώπιση των επιπτώσεων των επιθέσεων κοινωνικής μηχανικής.

Η αξιολόγηση της εκτίμησης κινδύνου κυβερνοασφάλειας ενός οργανισμού είναι ένας άλλος βασικός τομέας μελέτης που αναφέρεται στη βιβλιογραφία και συνιστά την οργάνωση ευρωπαϊκών και διεθνών προτύπων για την αντιμετώπιση επιθέσεων κοινωνικής μηχανικής.

Λέξεις κλειδιά: *κυβερνοασφάλεια, κυνερνοεπιθέσεις, εκτίμηση κινδύνου στον κυβερνοχώρο, κυβερνοεπίθεση στον τομέα της υγείας*

Abstract

Cyber security is increasingly becoming a concern among healthcare providers in the adoption of digital technologies to improve the quality of care provided to patients. Reports of cyber-attacks, such as ransomware and WannaCry, have highlighted the devastating nature of such attacks on healthcare. Such attacks are categorized as social engineering attacks. As the frequency and ingenuity of attacks on hospitals and clinical settings increase in order to disrupt services, there is a strong need to study the level of awareness-raising programs and training activities offered to staff by healthcare organizations.

The aim of this dissertation is to identify the common factors that affect the health care positions of a healthcare organization, resulting from ignorance of the cyber threat to healthcare. The literature review aims to consolidate the current literature on human behavior, thus creating security gaps that mitigate the cyber defense strategy adopted by health care organizations. In addition, the paper also examines the methodology of organizational risk assessment applied, and the policies adopted to enhance cyber security. The topic of cybersecurity in the context of healthcare and the clinical environment has attracted the interest of several researchers, resulting in a wide range of literature. Keywords related to cyber awareness, training, risk assessment methodologies of the organization, policies and recommendations adopted as countermeasures in health care were used. Research has been limited to the last 10 years or so.

Many of the articles were selected for inclusion, with the aim of addressing the complexity of cybersecurity measures adopted in the context of healthcare and clinical environments. The articles included, highlight the evolving nature of cyber-threats posed by the exploitation of IT infrastructure in more advanced attacks launched to exploit human vulnerability. The steady increase in the literature on the threat of cyber-attacks attacks demonstrates the growing threat of social engineering attacks. As a countermeasure, articles were identified that provide methodologies derived from case studies to promote cyber awareness among stakeholders. The articles included highlight the need to adopt cybersecurity practices among healthcare professionals, while accessing social media platforms, which is an ideal testing ground for attackers to gain insight into the lives of healthcare professionals.

In addition, articles presenting strategies adopted by healthcare organizations to address the effects of social engineering attacks are also included. Assessing an organization's cybersecurity risk assessment is another key area of study referred to in the literature and recommends the organization of European and international standards for dealing with social engineering attacks.

Key Words : *cybersecurity, cyberattack, cyber risk assessment, cyberattack in healthcare*

ΑΚΡΩΝΥΜΙΑ

API	Application Programming Interface
DDoS	Distributed Denial of Service
DNS	Domain Name System
EMR	Electronic Medical Records
ENISA	European Network and Information Security Agency
GDPR	General Data Protection Regulation
HIPAA	Health Insurance Portability and Accountability Act
HIS	Hospital Information System
HTTP	Hypertext Transfer Protocol
IP address	Διεύθυνση Διαδικτυακού πρωτοκόλλου
LIS	Laboratory Information Systems
NIST	National Institute of Standards and Technology
PACS	Picture Archiving and Communication System
RIS	Radiology Information Systems
VPN	VPN Virtual Private Network

Περιεχόμενα

1. Εισαγωγή 1

1.1. Γενικά 1

1.2. Διάρθρωση Διπλωματικής Εργασίας 3

2. Γενικές Έννοιες..... 4

2.1 Κυβερνοασφάλεια 4

2.2 Το μεταβαλλόμενο τοπίο απειλών στον κυβερνοχώρο..... 6

2.3 Τομείς κυβερνοαπειλών 6

2.4 Τύποι κυβερνοεπιθέσεων 9

2.5 Κυβερνοεπιθέσεις στον τομέα της υγειονομικής περίθαλψης 14

2.6 Πίνακες και ιστογράμματα κυβερνοεπιθέσεων εν μέσω πανδημίας Covid – 19..... 16

3. Δεδομένα Υγείας , Πληροφοριακά Συστήματα & Τεχνολογίες Διαχείρισης Πληροφοριών 20

3.1 Ιατρικά δεδομένα και κατηγοριοποίηση 20

3.1.1. Μεγάλα Δεδομένα (Big Data) & Διαδίκτυο των Πραγμάτων (IoT) 22

3.1.2. Ο ρόλος των μεγάλων δεδομένων στην ιατρική εκπαίδευση 24

3.2 GDPR και άλλα πρωτόκολλα δεδομένων στην ιατρική..... 24

3.3 Τεχνολογία Blockchain 25

3.4.1 Πληροφοριακά συστήματα υγείας Blockchain 26

4. Κυβερνοασφάλεια και κυβερνοεπιθέσεις στην υγεία 28

4.1 Τομέας Υγείας 28

4.2 Κυβερνοασφάλεια στην υγειονομική περίθαλψη και διαχείριση κινδύνων 30

5. Ολοκληρωμένο πληροφοριακό σύστημα υγείας/νοσοκομείου 40

5.1 Εξέλιξη των πληροφοριακών συστημάτων νοσοκομείου 40

5.2 Σύγχρονα πληροφοριακά συστήματα υγείας (HIS) 42

5.2.1 Βάση δεδομένων στο HIS 43

5.2.2 Συστατικά του HIS 43

5.3. Βασικές έννοιες ασφάλειας σύγχρονων πληροφοριακών συστημάτων υγείας ... 48

5.3.1. Ένα σύγχρονο πληροφοριακό σύστημα υγείας κρίνεται ασφαλές, ότι διακατέχεται από τις ακόλουθες αρχές: 48

5.3.2. Υπηρεσίες ασφαλείας & οι στόχοι τους 49

5.4 Παραδείγματα επιθέσεων σε σύγχρονα πληροφοριακά συστήματα υγείας 50

6. Επίθεση σε συστήματα packs σε απομονωμένο δίκτυο LAN 52

6.1. Σενάριο επίθεσης 52

6.2. Συμπεράσματα επιθέσεων 57

7. Άμυνα/επίθεση/πρόληψη κυβερνοεπιθέσεων 61

7.1 Άμυνες/πρόληψη σε επιθέσεις 61

7.2 Στρατηγικές άμυνας στον κυβερνοχώρο 62

7.2.1. Τοίχος προστασίας (firewall) 65

7.3. Τύποι Επίθεσης 66

7.4 Τεχνικές εντοπισμού 68

7.5 Εκπαίδευση προσωπικού σχετικά με τις κυβερνοεπιθέσεις 72

8. Σημερινή κατάσταση στον τομέα της κυβερνοασφάλειας στην υγεία 75

8.1 Υγεία και Internet of Things 75

8.2 Συνοπτική έκθεση κυβερνοασφάλειας ενός ιδιωτικού χώρου υγείας 78

Μεθοδολογία 83

Συμπεράσματα/μελλοντικές εξελίξεις/προτάσεις 86

Βιβλιογραφία 90

Πρόλογος

Τα τελευταία χρόνια, ο τομέας της υγειονομικής περίθαλψης γνώρισε μια μυριάδα εξελίξεων όσον αφορά τις νέες τεχνολογίες και μεθόδους θεραπείας. Τα σύγχρονα συστήματα υγειονομικής περίθαλψης έχουν αλλάξει τη ζωή των ασθενών και των ιατρών. Σήμερα, διαφορετικές εφαρμογές υγειονομικής περίθαλψης έχουν ενσωματωθεί σε συσκευές καταναλωτών από απόσταση, με στόχο να συλλέγουν πληροφορίες για έναν ασθενή και παρέχουν αυτόματη θεραπεία. Επιπλέον, η ανάπτυξη φορητών βιοαισθητήρων χαμηλής ισχύος, εμφυτεύσιμες ιατρικές συσκευές (*IMD*), δίκτυα περιοχής σώματος εξαιρετικά χαμηλής ισχύος, τεχνολογίες *Internet of Things* (*IoT*) και πολυάριθμα ελαφριά πρωτόκολλα επικοινωνίας βοήθησαν στην ανάπτυξη συσκευών μικρής κλίμακας υγειονομικής περίθαλψης που μπορούν να συλλέξουν και να στείλουν διαφορετικές φυσιολογικές τιμές (π.χ. αρτηριακή πίεση, καρδιακό ρυθμό κ.λπ.) από έναν ασθενή στους ιατρικούς επαγγελματίες εξ αποστάσεως και άμεσα για να παρέχουν καλύτερες θεραπείες.

Πράγματι, η αυξανόμενη δημοτικότητα και οι ποικίλες χρησιμότητες των σύγχρονων συστημάτων υγειονομικής περίθαλψης έχουν κάνει τον κλάδο της υγειονομικής περίθαλψης να αναπτυχθεί με τεράστιο ρυθμό. Η παγκόσμια αγορά ιατρικών συσκευών προβλέπεται να αυξηθεί με σύνθετο ετήσιο ρυθμό ανάπτυξης 4,5% από το 2018 έως 2023 και αναμένεται να φτάσει τα 409,5 δισεκατομμύρια δολάρια μέχρι το 2025. Ωστόσο, αυτά τα πιο έξυπνα και προηγμένα συστήματα υγειονομικής περίθαλψης είναι πιο πολύπλοκα σε λογισμικό και υλικό. Αν και η προσαρμογή των νέων τεχνολογιών στον τομέα της υγειονομικής περίθαλψης είναι σε πρώιμο στάδιο, έχουν ήδη βρεθεί αρκετά ελαττώματα λογισμικού και υλικού, τα οποία μπορεί να οδηγήσουν σε πιθανές κακόβουλες επιθέσεις.

Οι πλατφόρμες ανάπτυξης ανοιχτού κώδικα και η συνεχής συνδεσιμότητα ανοίγουν το δρόμο ώστε οι επιτιθέμενοι να εκμεταλλευτούν την ασφάλεια και την ιδιωτικότητα στα συστήματα υγειονομικής περίθαλψης. Τα τελευταία χρόνια, έχουν αναφερθεί σε αρκετές υπηρεσίες υγείας θέματα ασφάλειας, τόσο στα μέσα ενημέρωσης όσο και στην ακαδημαϊκή κοινότητα. Η έλλειψη τυπικής πρακτικής, η ανάγκη για έγκαιρες επιδιορθώσεις ασφαλείας και η ώθηση από την κυβέρνηση να διατηρεί συσκευές και ασφαλείς εφαρμογές επιδεινώνουν αυτήν την κατάσταση.

Λόγω των καταστροφικών συνεπειών για την υγεία, οποιοδήποτε θέμα ασφάλειας σχετικά με τα συστήματα υγειονομικής περίθαλψης θα πρέπει να αντιμετωπιστεί επιθετικά και προληπτικά. Δυστυχώς δεν υπάρχει ολοκληρωμένη λύση ασφάλειας διαθέσιμη στη βιομηχανία και την ερευνητική κοινότητα για τον μετριασμό των αναδυόμενων κυβερνοεπιθέσεων σε συστήματα υγειονομικής περίθαλψης.

Οι ερευνητές έχουν προτείνει μερικά αντίμετρα (π.χ., προστασία της ιδιωτικής ζωής πρωτόκολλα επικοινωνίας, κρυπτογραφημένες βάσεις δεδομένων κ.λπ.) που δεν μπορούν να αντιμετωπίσουν τη συνολική επιφάνεια επίθεσης στα συστήματα υγειονομικής περίθαλψης. Επομένως, η ασφάλεια και η ιδιωτικότητα στα συστήματα υγειονομικής περίθαλψης απαιτούν άμεση προσοχή της ερευνητικής κοινότητας, και της βιομηχανίας ιατρικών συσκευών και ρυθμιστικών φορέων.

Ο σκοπός αυτής της διπλωματικής είναι να παρέχει μια ολοκληρωμένη επισκόπηση της ασφάλειας και της ιδιωτικής ζωής, τάσεις και αναδυόμενες απειλές για τα συστήματα υγειονομικής περίθαλψης, τη διευκόλυνση της κατανόησης της πιεστικής ασφάλειας και προκλήσεις απορρήτου. Οι συνεισφορές αυτής της εργασίας είναι οι εξής: Αρχικά, παρέχεται μια λεπτομερής επισκόπηση ενός τυπικού συστήματος υγειονομικής περίθαλψης και συζητούνται τα συστατικά του. Δεύτερον, διερευνώνται διαφορετικοί στόχοι ασφάλειας και απορρήτου για τα συστήματα υγειονομικής περίθαλψης και συζητούνται πιθανά μοντέλα αντιπαραθέσεων. Τρίτον, παρουσιάζεται μια λεπτομερής ταξινόμηση των υφιστάμενων επιθέσεων στον τομέα της υγειονομικής περίθαλψης αναλύοντάς τις ως αναφέρονται από την ερευνητική κοινότητα και τη βιομηχανία. Συζητείται επίσης ο αντίκτυπος αυτών των επιθέσεων. Τέταρτον, συνοψίζονται οι υπάρχουσες λύσεις που έχουν προταθεί για τον μετριασμό αυτών των επιθέσεων και προσδιορίζονται οι προκλήσεις που αντιμετωπίζει η ερευνητική κοινότητα για τη διασφάλιση της ασφάλειας και της ιδιωτικής ζωής στα συστήματα υγειονομικής περίθαλψης. Τέλος, διατυπώνονται αρκετές ανοικτές προκλήσεις και μελλοντικές ερευνητικές κατευθύνσεις για την επίλυση της ασφάλειας και ζητημάτων απορρήτου στα συστήματα υγειονομικής περίθαλψης.

Τα τελευταία χρόνια, έχουν διεξαχθεί αρκετές έρευνες για την ανασκόπηση των υφιστάμενων επιθέσεων ασφάλειας και απορρήτου στα συστήματα υγειονομικής περίθαλψης. Ωστόσο, αυτά τα έργα είτε εστιάζουν σε συγκεκριμένες επιθέσεις είτε σε λύσεις ασφαλείας για

συγκεκριμένες συσκευές χωρίς να λαμβάνουν υπόψη συνολικά ζητήματα ασφάλειας και ιδιωτικότητας στα συστήματα υγειονομικής περίθαλψης. Οι υπάρχουσες έρευνες επικεντρώνονται κυρίως σε προβλήματα ασφάλειας και ιδιωτικότητας, τρωτά σημεία, και λύσεις που σχετίζονται με θέματα ιδιωτικότητας και ασφάλειας των *IMD*. Οι ερευνητές ανέλυσαν επίσης τα χαρακτηριστικά ασφάλειας και ιδιωτικότητας του IoT από την άποψη της υγειονομικής περίθαλψης. Οι κύριες διαφορές μεταξύ της παρούσας εργασίας και των υφιστάμενων ερευνών μπορεί να διατυπωθεί ως εξής: Ενώ οι περισσότερες τρέχουσες έρευνες επικεντρώνονται στην ασφάλεια και το απόρρητο των *IMD* και των *IWMD*, η παρούσα έρευνα επικεντρώνεται στο συνολικό σύστημα υγειονομικής περίθαλψης, το οποίο καλύπτει στοιχεία από άκρο σε άκρο, συμπεριλαμβανομένων των ιατρικών συσκευών, αισθητήρων, δικτύων/επικοινωνιών και παρόχων υγειονομικής περίθαλψης. Παρέχεται, επίσης, μια επίσημη αρχιτεκτονική στα συστήματα υγειονομικής περίθαλψης και προσδιορίζονται τα κύρια συστατικά τους για να σκιαγραφήσουν τις ανάγκες ασφάλειας και απορρήτου.

1.Εισαγωγή

1.1. Γενικά

Ο ψηφιακός μετασχηματισμός, είναι ένας όρος που χρησιμοποιείται για να περιγράψει το ολιστικό αποτέλεσμα που δημιουργείται από μια εφαρμογή λογισμικού που μεταμορφώνει θεμελιωδώς έναν συγκεκριμένο τομέα. Στο ιστορικό πλαίσιο, ο ψηφιακός μετασχηματισμός υιοθετήθηκε στον κλάδο της υγειονομικής περίθαλψης με παραδείγματα που περιλαμβάνουν την ενσωμάτωση του συστήματος συστημάτων πληροφοριών υγείας και μέτρα κυβερνοασφάλειας για δικτυωμένες ιατρικές συσκευές. Ωστόσο, με τη συνεχιζόμενη πανδημία COVID-19, το ποσοστό υιοθέτησης τέτοιων τεχνολογιών έχει επιταχυνθεί. Η ευθύνη των επαγγελματιών διαχείρισης τεχνολογίας υγειονομικής περίθαλψης είναι να προσφέρουν συμβουλές από ειδικούς σχετικά με τη χρήση των εγκαταστάσεων υγειονομικής περίθαλψης από το κλινικό προσωπικό και να επιβλέπουν τη συντήρηση και τη λειτουργία των ιατρικών συσκευών καθ 'όλη τη διάρκεια του κύκλου ζωής τους.

Οι τεχνικοί εμπειρογνώμονες ενσωματώνουν τεχνολογίες υγείας, προσφέροντας τη δυνατότητα να αξιοποιήσουν τις ιατρικές τεχνολογίες για να παρέχουν καλύτερη και ασφαλέστερη φροντίδα των ασθενών. Σύμφωνα με την τεχνική σειρά που δημοσιεύτηκε από τον Παγκόσμιο Οργανισμό Υγείας (ΠΟΥ) για την πρωτοβάθμια υγειονομική περίθαλψη, η τεχνολογία πληροφοριών και επικοινωνιών (ΤΠΕ) γίνεται όλο και περισσότερο κοινός τόπος με την εισαγωγή έξυπνων τηλεφώνων, tablet και φορητών υπολογιστών. Από την τεχνολογία που επιτρέπει στους ανθρώπους να διαχειρίζονται την υγεία τους πιο αποτελεσματικά, καλύτερους τρόπους διάγνωσης ασθενειών, μέχρι την παρακολούθηση του αντίκτυπου των πολιτικών στην υγεία του πληθυσμού, οι ψηφιακές τεχνολογίες για την υγεία επηρεάζουν τον τρόπο παροχής και λειτουργίας των υπηρεσιών υγείας.

Ένα από τα μεγαλύτερα εμπόδια στην υιοθέτηση στρατηγικών ψηφιακού μετασχηματισμού είναι το έγκλημα στον κυβερνοχώρο, το οποίο είναι υπεύθυνο για την εκμετάλλευση των τρωτών σημείων των συστημάτων καθώς και την αδυναμία που οφείλεται

στον άνθρωπο. Το έγκλημα στον κυβερνοχώρο εμφανίστηκε στα τέλη της δεκαετίας του 1970. Αυτό που ξεκίνησε ως ανεπιθύμητο περιεχόμενο τελικά μετατράπηκε σε ιούς υπολογιστών και κακόβουλο λογισμικό. Η βιομηχανία υγείας αποτελεί ελκυστικό στόχο για εγκληματίες στον κυβερνοχώρο, καθώς τα έγγραφα υγείας περιέχουν ευαίσθητες προσωπικές και οικονομικές πληροφορίες.

Η άνοδος των περιστατικών επίθεσης στον κυβερνοχώρο αποτελεί μια αυξανόμενη απειλή για τη βιομηχανία υγειονομικής περίθαλψης, γενικά, και για τα νοσοκομεία ειδικότερα. Στη βιομηχανία υγειονομικής περίθαλψης, οι συντονισμένες προσπάθειες για την προστασία των δεδομένων των ενδιαφερομένων έχουν μείνει πίσω και δεν έχουν υγειονομική περίθαλψη σε σύγκριση με άλλους κλάδους. Με τη γρήγορη ψηφιοποίηση των αρχείων υγείας των ασθενών, ο αντίκτυπος των παραβιάσεων δεδομένων στα νοσοκομεία προκαλεί μεγάλες οικονομικές και άυλες ζημίες. Για να αντισταθμίσουν τον αντίκτυπο τέτοιων επιθέσεων στον κυβερνοχώρο, οι οργανισμοί έχουν υιοθετήσει στρατηγικές διακυβέρνησης για την προώθηση των βέλτιστων πρακτικών για την ασφάλεια της ηλεκτρονικής υποδομής των νοσοκομείων και άλλων κλινικών περιβαλλόντων.

Ωστόσο, η επιτυχής υιοθέτηση στρατηγικών ψηφιακού μετασχηματισμού στον κλάδο της υγειονομικής περίθαλψης βασίζεται στην επιτυχή αποδοχή μεταξύ των επαγγελματιών του τομέα της υγειονομικής περίθαλψης για την αντιμετώπιση των κινδύνων που προκύπτουν από απειλές στον κυβερνοχώρο. Ως εκ τούτου, είναι σημαντικό να παρέχονται προγράμματα ευαισθητοποίησης και κατάρτισης για επαγγελματίες υγείας. Ο ρόλος της ανθρώπινης συμπεριφοράς στην αντιμετώπιση των κυβερνοεπιθέσεων και στην ενίσχυση της άμυνας στον κυβερνοχώρο ομαδοποιείται στο θέμα των «ανθρώπινων παραγόντων» στην κυβερνοασφάλεια. Μετά τον αυξανόμενο αριθμό άρθρων που δημοσιεύονται, που αφορούν τον ρόλο των ανθρώπων στον βρόχο για την ενίσχυση της κυβερνοασφάλειας από το 2016 υπάρχει ανάγκη ενοποίησης των ευρημάτων της έρευνας.

Ο κύριος στόχος αυτής της διπλωματικής είναι η ανασκόπηση της βιβλιογραφίας για τη συλλογή στοιχείων από οργανωτικές μελέτες περιπτώσεων, παρατηρήσεις συγγραφέων και επιστημονικές εξελίξεις στην κυβερνοασφάλεια για τον εντοπισμό του ρόλου της ένταξης των ανθρώπων στον κύκλο για την ενίσχυση της κυβερνοάμυνας στον κλάδο της υγειονομικής περίθαλψης. Για να επιτευχθεί αυτός ο στόχος, χρειάστηκε να μελετηθεί ένας εκτενείς αριθμός

άρθρων, που αντιμετωπίζουν την πρόκληση της ασφάλειας στον κυβερνοχώρο κατά την αντίληψη οργανωτικών απειλών και προσωπικών επιθέσεων ιδιωτικών πληροφοριών ενός επαγγελματία υγείας.

Οι συνεισφορές της εργασίας περιλαμβάνουν τις ακόλουθες: Διεξαγωγή εκτεταμένης ανασκόπησης διαφόρων τύπων κυβερνοεπιθέσεων που αντιμετωπίζει η υγειονομική περίθαλψη και τα κλινικά περιβάλλοντα που αναφέρονται στη βιβλιογραφία. Μελέτη των οργανωτικών στρατηγικών άμυνας κατά των απειλών στον κυβερνοχώρο. Ανάλυση της μεθοδολογίας που υιοθετήθηκε από διαφορετικούς οργανισμούς υγειονομικής περίθαλψης για τη διενέργεια εκτίμησης κινδύνου στον κυβερνοχώρο. Αξιολόγηση της επίδρασης και του αντίκτυπου των ανθρώπινων παραγόντων στην ενίσχυση/αποδυνάμωση της κυβερνοάμυνας του οργανισμού υγειονομικής περίθαλψης.

1.2. Διάρθρωση Διπλωματικής Εργασίας

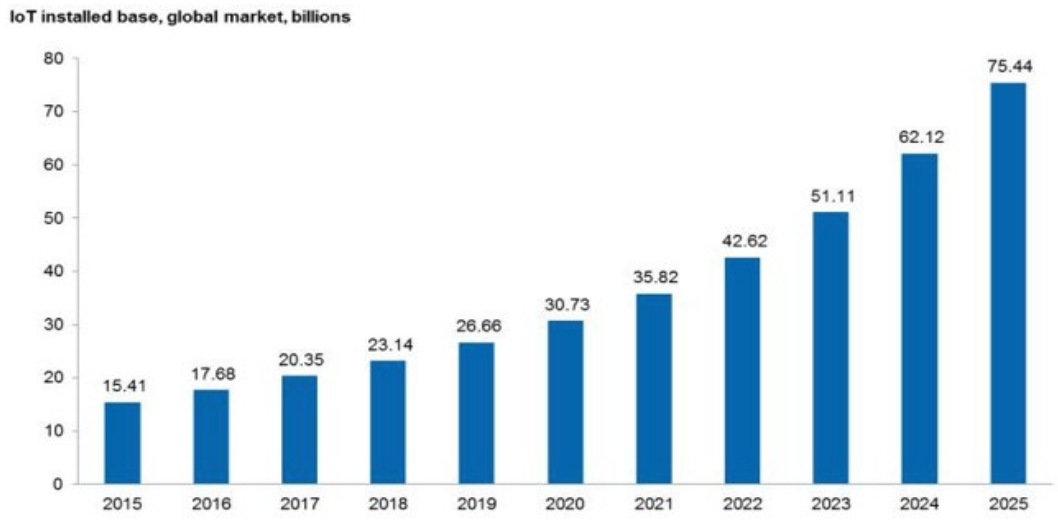
Στο πρώτο κεφάλαιο της εργασίας παρουσιάζονται κάποιες γενικές έννοιες όπως τι είναι οι κυβερνοεπιθέσεις, ποιοι οι τύποι τους, οι τομείς τους και κάποια σχεδιαγράμματα και εικόνες σχετικά. Στο δεύτερο κεφάλαιο παρουσιάζεται μια ανάλυση των δεδομένων στο χώρο της υγείας και πως αυτή κατηγοριοποιείται με έμφαση στα μεγάλα δεδομένα και διάφορα ιατρικά πρωτόκολλα. Στο τρίτο κεφάλαιο παρουσιάζεται η κυβερνοασφάλεια και οι κυβερνοεπιθέσεις στον τομέα της υγείας. Στο τέταρτο κεφάλαιο παρουσιάζεται το ολοκληρωμένο πληροφοριακό σύστημα νοσοκομείου και υγείας, με τα συστατικά του καθώς και μερικά παραδείγματα επιθέσεων. Στο πέμπτο κεφάλαιο παρουσιάζεται ένα σενάριο επίθεσης σε συστήματα packs σε απομονωμένο δίκτυο LAN. Στο έκτο κεφάλαιο παρουσιάζονται τρόποι άμυνας, επίθεσης και πρόληψης στο τομέα της κυβερνοασφάλειας. Στο έβδομο κεφάλαιο παρουσιάζεται μια σημερινή κατάσταση στον τομέα της κυβερνοασφάλειας στην υγεία. Ακολουθεί η βιβλιογραφία στο όγδοο κεφάλαιο και στο ένατο τα συμπεράσματα μαζί με προτάσεις για μελλοντική εξέλιξη.

2. Γενικές έννοιες

2.1 Κυβερνοασφάλεια

Ο σημερινός κόσμος είναι ένα από τα όλο και περισσότερο δικτυωμένα συστήματα από τα οποία εξαρτάται η αλληλεξάρτηση για κοινωνικές συνδέσεις και επιχειρηματικές δραστηριότητες. Αυτά τα γρήγορα κανάλια επικοινωνίας εκτείνονται παγκοσμίως και αυξάνονται εκθετικά με τη πλειοψηφία του πληθυσμού να διεξάγει τώρα αλληλεπιδράσεις και συναλλαγές στον κυβερνοχώρο. Από επιχειρηματικής απόψεως, ο κυβερνοχώρος έχει δημιουργήσει νέες δυνατότητες συμπεριλαμβανομένων εφαρμογών για κινητά, επικύρωση διαπιστευτηρίων συμπεριφοράς ενώ η τεχνητή νοημοσύνη (*AI – Artificial Intelligence*) επιτρέπει στις επιχειρηματικές συναλλαγές να πραγματοποιούνται χωρίς περιορισμούς.

Εν τω μεταξύ, το Διαδίκτυο των Πραγμάτων (*IoT – Internet of Things*) επιτρέπει στα πάντα να ελεγχθούν από απόσταση με την αποστολή ανατροφοδότησης. Ο κυβερνοχώρος μέσα από τη συνδεσιμότητα έχει οδηγήσει σε απίστευτα κέρδη στην εφαρμογή της τεχνολογίας κατά την τελευταία δεκαετία, αλλά οι φορείς απειλής με κακόβουλη πρόθεση έχουν μάθει να χρησιμοποιούν τη συνδεσιμότητα αυτή ως εργαλείο διάπραξης εγκλημάτων. Ενώ η νέα τεχνολογία έχει προσφέρει νέες οδούς επικοινωνίας, έχει επίσης αποκαλύψει εκμεταλλεύσιμα τρωτά σημεία ενσωματωμένα στο υλικό και το λογισμικό που χρησιμοποιείται στη κατασκευή και λειτουργία αυτών των μονοπατιών εκθέτοντας τους ανθρώπους που τα χρησιμοποιούν (Anstee D et al., 2016).



Σχήμα 1: Προβλεπόμενη ανάπτυξη του *IoT*

Πηγή : HIS – Markit, όπως αναφέρθηκε στο Forbes

Αυτά τα τρωτά σημεία ανοίγουν ένα ευρύ φάσμα σημείων εισόδου για κακόβουλους παράγοντες, δημιουργώντας μια πρόκληση για τους επαγγελματίες στον τομέα της ασφάλειας στον κυβερνοχώρο που πρέπει να υπερασπιστούν τους στόχους σε όλο τον κόσμο σε διαφορετικό δίκτυο και γεωγραφική περιοχή. Αυτά τα μονοπάτια μπορούν να γίνουν στόχος απάτης από οποιοδήποτε άτομο. Μπορούν επίσης να στοχεύσουν ευαίσθητα δεδομένα που έχουν στην κατοχή τους καθιστώντας τους έναν άθελο, φιλοξενούμενο συνεργό για επιθέσεις σε πιο πολύτιμους στόχους όπως εταιρικά δίκτυα. Οι επαγγελματίες στον τομέα της ασφάλειας στον κυβερνοχώρο αντιμετωπίζουν μια τρομακτική πρόκληση προκειμένου να εξασφαλίσουν τα δικά τους δίκτυα του οργανισμού κρατώντας τους επιτιθέμενους μακριά από τα πιο πολύτιμα δεδομένα, ενώ ταυτόχρονα να ανταποκρίνονται σε φορείς απειλής που μπορεί να έχουν εισέλθει στην περίμετρο ελέγχου τους. Οι αντίπαλοι στον κυβερνοχώρο είναι αποφασισμένοι. Εργάζονται πολλές ώρες για να επιτύχουν τους στόχους τους χρησιμοποιώντας δημιουργικότητα ώστε να δυσκολέψουν τους επαγγελματίες στον κυβερνοχώρο στο χαρακτηρισμό, την ανίχνευση ή το μετριασμό απειλών. Αυτό δημιουργεί μια αυξανόμενα ποικίλη απειλή στο τοπίο του κυβερνοχώρου (Anstee D et al., 2016).

2.2 Το μεταβαλλόμενο τοπίο απειλών στον κυβερνοχώρο

Το τοπίο της απειλής στον κυβερνοχώρο έχει αλλάξει σημαντικά την τελευταία δεκαετία. Η συχνότητα, η ταχύτητα και η αποτελεσματικότητα των κυβερνοεπιθέσεων συνεχίζουν να αυξάνονται κάτι που σημαίνει ότι οι οργανώσεις πρέπει να είναι σωστές όλη την ώρα, ενώ οι κακόβουλοι παράγοντες πρέπει να είναι τυχεροί μόνο μια φορά. Οι απειλητικοί τομείς έχουν εξελιχθεί σε μεγάλο βαθμό σε αποσυνδεδεμένα άτομα χρησιμοποιώντας περιορισμένα σύνολα εργαλείων σε ένα ευρύ δίκτυο ομάδων που χρησιμοποιούν πολύ εξελιγμένα και προσαρμοσμένα σύνολα εργαλείων.

Σήμερα, οι παράγοντες απειλής υπάρχουν και λειτουργούν μέσα σε οργανωμένες επιχειρήσεις -και σε ορισμένες περιπτώσεις κράτη – ενώ εκμεταλλεύονται όλο και περισσότερο τις διαταρακτικές και καταστροφικές τακτικές για να επιτύχουν οικονομικό όφελος. Η εξέλιξη των παραγόντων απειλής σε πιο οργανωμένες και εξελιγμένες επιχειρήσεις έχει αυξήσει την απειλή που αντιμετωπίζει κάθε οργανισμός που συνδέεται με το Διαδίκτυο. Μόνο το 2018, πλήθος παγκόσμιων οργανισμών αντιμετώπισαν καινοτόμες και επιτυχημένες επιθέσεις, που κυμαίνονταν από στοχευμένες εκστρατείες εναντίον εγχώριων και διεθνών συστημάτων πληρωμών, παραβιάσεις τρίτων προμηθευτών, και πρωτοφανής πνευματικής ιδιοκτησίας καθώς και κλοπή ευαίσθητων δεδομένων, σε καταστροφικές επιθέσεις που επηρεάζουν τη σταθερότητα των επιχειρηματικών δραστηριοτήτων. Οι επιθέσεις δεν χρειάζεται να είναι καινοτόμες για να πετύχουν. Μπορούν να είναι απλές επιθέσεις ενάντια σε ασήμαντα εκμεταλλεύσιμα τρωτά σημεία, όπως αδυναμία ελέγχου ταυτότητας και κακή διαχείριση πρόσβασης οι οποίες αρκούν (Armor, 2018).

2.3 Τομείς κυβερνοαπειλών

Υπάρχουν πέντε διαφορετικοί τύποι φορέων απειλής - εθνικό κράτος, εγκληματίες, ακτιβιστές, τρομοκράτες και εσωτερικοί - ο καθένας με διαφορετικές μεθόδους και στόχους.

- Οι εθνικοί φορείς διεξάγουν κατασκοπεία για να κλέψουν πνευματική ιδιοκτησία και να συλλέξουν ευφυΐα που θεωρείται ζωτικής σημασίας για την προώθηση των εθνικών συμφερόντων. Είναι δύσκολο να εντοπιστούν και να μετριαστούν αυτοί οι παράγοντες διαθέτουν ωστόσο σημαντικούς πόρους για την ανάπτυξη και τη διατήρηση περίπλοκων δυνατοτήτων.

- Οι οργανωμένοι εγκληματίες επικεντρώνονται σε χρηματικά κέρδη μέσω μεθόδων όπως το ηλεκτρονικό ψάρεμα, η κοινωνική μηχανική, τα αυτοματοποιημένα εργαλεία, *ransomware*/άλλα εργαλεία εκβιασμού, και ενισχυμένες κατανεμημένες επιθέσεις άρνησης υπηρεσίας (*DDoS*)-μερικές φορές αναγκαστικές, εκβιάζοντας την επιλογή μεταξύ καταβολής αξιόποινων πράξεων ή μεγάλου κόστους ανάκτησης. Το χρηματικό κέρδος δεν είναι αποκλειστικό για την κλοπή χρημάτων από λογαριασμούς. Τα προσωπικά δεδομένα αναγνωρίσιμων πληροφοριών (*PII*) επίσης κλέβονται και στη συνέχεια πωλούνται σε αγορές στον σκοτεινό ιστό για περαιτέρω εκμετάλλευση εγκληματικών ομάδων.
- Οι τρομοκράτες και οι ακτιβιστές μοιράζονται ομοιότητες καθώς προωθούν και οι δύο πολιτικές ατζέντες με χρήση διαδικτυακών μέσων. Και οι δύο χρησιμοποιούν το φόβο και τις ενοχλητικές κυβερνοεπιθέσεις, όμως οι κυβερνο -τρομοκράτες είναι πιθανότατα μέρος μιας μεγαλύτερης οργάνωσης που μπορεί επίσης να έχει φυσικό συστατικό. Οι ακτιβιστές έχουν περιορισμένη φυσική παρουσία ή άμεσους δεσμούς με τις υπάρχουσες προσωπικές ομάδες διαμαρτυρίας. Προτιμούν να διαμαρτύρονται για πολλά ελαφρά αντιληπτές ευκαιρίες αναζητώντας στόχους για να επιστήσουν την προσοχή σε έναν σκοπό και να επιτύχουν κακή φήμη. Ιστορικά, οι *hacktivists* ξεκινούν επιθέσεις κατανεμημένης άρνησης παροχής υπηρεσιών (*DDoS*) και πραγματοποιούν παραμορφώσεις ιστότοπων ως μέσο διαμαρτυρίας.
- Οι εσωτερικοί φορείς αποτελούν τη μεγαλύτερη απειλή για έναν οργανισμό από τους περισσότερους εξωτερικούς παράγοντες. Χρησιμοποιούν τοπικά εργαλεία και τις γνώσεις τους για το εσωτερικό δίκτυο για να κλέψουν, να ζημιώσουν ή να διεξάγουν απάτη. Αυτές οι πράξεις είναι δύσκολο να εντοπιστούν ως προθέσεις και οι μέθοδοι είναι ποικίλες, που κυμαίνονται από χρηματικό κέρδος και πρόκληση ζημιάς έως αντιληπτές πράξεις άξιες καταγγελίας.

Η απειλή των κυβερνοεπιθέσεων δεν βελτιώνεται, αλλά χειροτερεύει. Οι επιθέσεις παγκοσμίως αυξάνονται σε μέγεθος, αντοχή και πολυπλοκότητα. Μία έρευνα από το Υπουργείο Ψηφιακών, Πολιτιστικών, Μέσων & Αθλητισμού του Ηνωμένου Βασιλείου απέδειξε οτι τέσσερις στις δέκα επιχειρήσεις του Ηνωμένου Βασιλείου και δύο στις δέκα φιλανθρωπικές οργανώσεις είχαν εμπειρία στις παραβιάσεις ασφαλείας του κυβερνοχώρου από τις αρχές του 2018.

Το εκτιμώμενο κόστος για την παγκόσμια οικονομία από τις απώλειες στον κυβερνοχώρο είναι πάνω από 1,5 τρισεκατομμύρια δολάρια το έτος, συμπεριλαμβανομένων 65 δισεκατομμυρίων δολαρίων σε πληρωμές και λειτουργική διακοπή από κυβερνοεπιθέσεις, 725 δισεκατομμύρια δολάρια σε χαμένα έσοδα από επιχειρήσεις που υποφέρουν από σημαντικό επίπεδο επακόλουθων απωλειών επιχειρήσεων και ζημίες 825 δισεκατομμυρίων δολαρίων που υπέστησαν οι συναλλαγές των επιχειρηματικών εταίρων της επηρεαζόμενης επιχείρησης. (Baker S., 2017) Το μέσο κόστος μιας απλής επιτυχούς κυβερνοεπίθεσης εκτιμάται στα 5 εκατομμύρια δολάρια, 7 κυρίως λόγω των μεγάλων περιόδων του χρόνου διακοπής του συστήματος και της χαμένης παραγωγικότητας που συνήθως ακολουθούν μια επίθεση.

Οι οργανισμοί γνωρίζουν επίσης την απειλή για τη φήμη από τον κίνδυνο στον κυβερνοχώρο. Μία σημαντική απώλεια δεδομένων μπορεί να οδηγήσει σε δραματική αλλαγή στην αποτίμηση της αξίας των μετοχών ή μαζικής φυγής πελατών. Καθώς η διακοπή των επιχειρήσεων επηρεάζει περισσότερους ανθρώπους, τα πρόστιμα και οι ρυθμιστικές επιβαρύνσεις αυξάνονται περισσότερο. Τον Σεπτέμβριο του 2018, μετά από μήνες διεθνούς ελέγχου μετά το σκάνδαλο *Cambridge Analytica*, το *Facebook* γνώρισε παραβίαση που έπληξε περισσότερους από 50 εκατομμύρια χρήστες. Οι χάκερ εκμεταλλεύτηκαν τρία τρωτά σημεία στη λειτουργία «προβολής ως» του Facebook και έκλεψαν μάρκες πρόσβασης που τους επέτρεψαν να πάρουν παράνομα τον έλεγχο των προφίλ χρηστών αποκτώντας πρόσβαση σε εφαρμογές τρίτων όπως το *Pinterest* και το *Spotify*.

Η τιμή της μετοχής του *Facebook* μειώθηκε κατά 3% την ημέρα δημοσιοποίησης της παράβασης, με αποτέλεσμα την πτώση της κεφαλαιοποίησης της αγοράς κατά 13 δισεκατομμύρια δολάρια. Επίσης κατά παράβαση των πρόσφατα θεσπισθέντων κανονισμών προστασίας δεδομένων στην Ευρώπη, οι οποίοι θα μπορούσαν να οδηγήσουν σε πρόστιμο ίσο με το 4% του ετήσιου συνολικού κύκλου εργασιών της εταιρείας, ή 1,63 $ δισεκατομμύρια στην περίπτωση του *Facebook*. (Benner K. et al., 2018) Παρόλο που πολλές εταιρείες έχουν υποστεί κάποιου είδους ζημίες λόγω ενός κυβερνοχώρου, η παγκόσμια οικονομία δεν έχει βιώσει ακόμη ένα πραγματικά καταστροφικό γεγονός που θα κοστίζει στην οικονομία εκατοντάδες δισεκατομμύρια δολάρια. Μία έρευνα για ψηφιοποιημένες επιφάνειες επιθέσεων, ωστόσο, δείχνει ότι επιθέσεις αυτού του μεγέθους είναι πιθανές και ότι αυξάνονται οι δυνατότητες και οι φιλοδοξίες των φορέων απειλής. Μια κυβερνο -καταστροφή θα μπορούσε να αλληλοεπιδράσει

δυνητικά σε πολλαπλές βιομηχανίες και γεωγραφικές περιοχές, ανατρέποντας το status quo της σύγχρονης πολιτικής.

2.4 Τύποι κυβερνοεπιθέσεων

Προσπαθώντας να αποτυπώσουμε το ευρύτερο - πολυδιάστατο αυτό πλαίσιο της Κυβερνοασφάλειας καταλήγουμε στον ακόλουθο ορισμό: Κυβερνασφάλεια είναι μια επιστήμη που καθορίζει τα πρότυπα, τις πολιτικές και τις βέλτιστες πρακτικές για προστασία (πρόληψη, ανίχνευση, διακοπή, ανάκτηση, κατάχρηση) λογισμικού και υλικού (ψηφιακά δεδομένα και φυσική υποδομή). Λειτουργεί σε περιβάλλον κυβερνοχώρου με μη εξουσιοδοτημένη πρόσβαση, η οποία μπορεί να οδηγήσει σε κακόβουλη ενέργεια (διαφθορά, κλοπή, καταστροφή ή χειραγώγηση / τροποποίηση, διακοπή της υπηρεσίας) προκειμένου να διατηρεί τη διαθεσιμότητα δεδομένων, την εμπιστευτικότητα, την ακεραιότητα και την κατοχή καθ 'όλη τη διάρκεια του κύκλου ζωής του (από πηγή στον προορισμό και ενδιάμεσο) από το εσωτερικό και το εξωτερικό του εισβολέα.

Τύποι επιθέσεων στον κυβερνοχώρο:

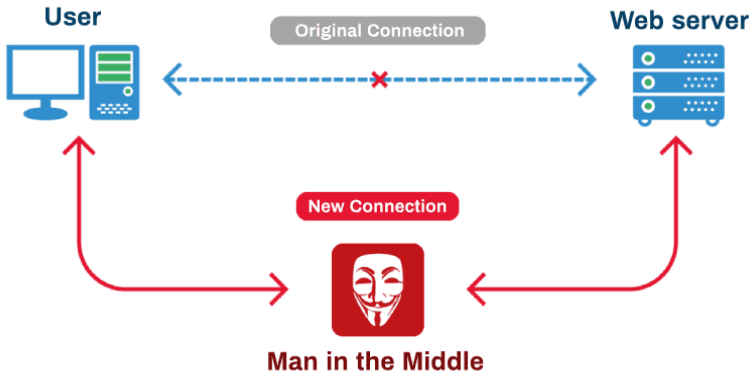
- Κακόβουλο λογισμικό (malicious software) : Λογισμικό το οποίο έχει σχεδιαστεί ειδικά για να προκαλέσει ζημιά ή να αποκτήσει μη εξουσιοδοτημένη πρόσβαση σε ένα σύστημα υπολογιστή. Περιλαμβάνει ιούς (viruses), worms, trojan horses κ.λπ. Σε αυτή την κατηγορία ανήκει και το λογισμικό λύτρων (ransomware), το οποίο όμως εξετάζεται χωριστά λόγω της ιδιαιτερότητάς του.

- Επιθέσεις από το διαδίκτυο (web based attacks): Πρόκειται για απειλές που στοχεύουν απευθείας στο χρήστη μέσω εκμετάλλευσης αδυναμιών στους φυλλομετρητές (browsers), καθώς και στα συστήματα διαχείρισης περιεχομένου (content management systems). Κυριότερα είδη επιθέσεων αυτής της κατηγορίας αποτελούν τα browser exploits, drive-by downloads, watering hole attacks κ.α.

- Phishing : Κακόβουλα μηνύματα ηλεκτρονικού ταχυδρομείου ή τηλεφωνικές συνδιαλλαγές, οι οποίες αποσκοπούν στο να παραπλανήσουν τους χρήστες και να αποκαλύψουν εμπιστευτικές πληροφορίες.

- Επιθέσεις σε διαδικτυακές εφαρμογές (web application attacks): Επιθέσεις που στοχεύουν σε διαδικτυακές εφαρμογές (web applications). Οι εν λόγω εφαρμογές, λόγω της καθολικής χρήσης τους στην προσφορά περιεχομένου, αποτελούν στόχο πολλαπλών ειδών επιθέσεων, με κυριότερες τα cross-site scripting (XSS), SQL injection, path traversal, local file inclusion κ.α.

- Επίθεση man-in-the-middle: Μια man-in-the-middle επίθεση προϋποθέτει την ύπαρξη τριών μερών. Το θύμα, την οντότητα με την οποία προσπαθεί να επικοινωνήσει το θύμα και τον man-in-the-middle, ο οποίος παρακολουθεί και εισβάλλει στις επικοινωνίες του θύματος. Φυσικά, το θύμα δεν γνωρίζει την ύπαρξη του man-in-the-middle.



Εικόνα 1: Επίθεση Man-in-the-middle.

πηγή:https://thehacktoday.com/how-to-make-sure-no-man-in-the-middle-attack-can-harm-you/

Στην επίθεση αυτή ο επιτιθέμενος παρακολουθεί και ουσιαστικά παραβιάζει την ιδιωτικότητα της επικοινωνίας μεταξύ δύο πλευρών. Η επίθεση αυτή πραγματοποιείται με δύο τρόπους. Ο ένας περιλαμβάνει τη φυσική εγγύτητα στο στόχο και ο άλλος την εγκατάσταση κάποιου κακόβουλου λογισμικού. Οι πιο κοινές επιθέσεις man-in-the-middle επιθέσεις είναι:

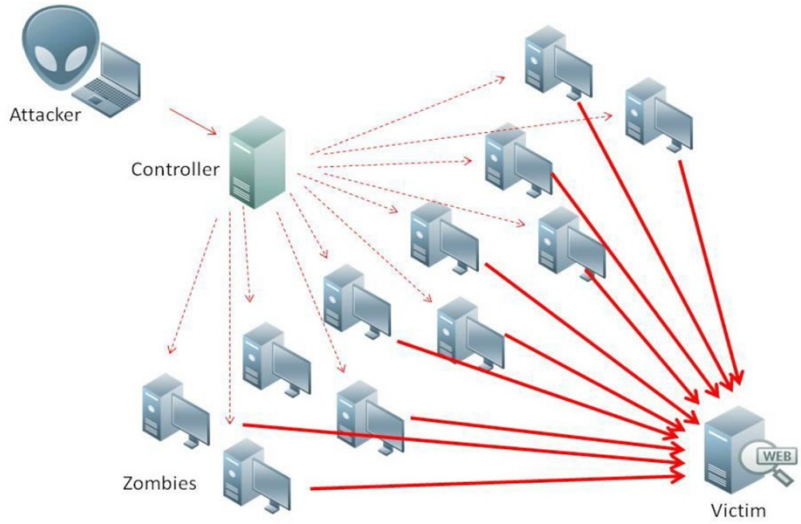
Εικόνα 2: Κοινές Επιθέσεις Man-in-the-middle

https://www.varonis.com/blog/man-in-the-middle-attack/

● Ανεπιθύμητα μηνύματα ηλεκτρονικού ταχυδρομείου: Αναφερόμενες και ως SPAM, αυτές οι επιθέσεις περιλαμβάνουν την αποστολή ανεπιθύμητης αλληλογραφίας σε χρήστες. Η εν λόγω αλληλογραφία χαρακτηρίζεται από το πολύ μικρό κόστος αποστολής των μηνυμάτων, την ενόχληση που προκαλεί στους χρήστες, αλλά και την εν δυνάμει μετεξέλιξη των μηνυμάτων σε απειλή phishing.

● Επιθέσεις άρνησης υπηρεσίας (Denial of Service – DoS attacks): Επιθέσεις κατά τις οποίες μεγάλος όγκος διαδικτυακής κίνησης στοχεύει σε μια υπηρεσία, με σκοπό να καταστεί αδύνατο από τα συστήματα να εξυπηρετήσουν νόμιμα αιτήματα. Ουσιαστικά, εκμεταλλεύονται την πεπερασμένη χωρητικότητα συστημάτων και δικτύων, ώστε να καταστήσουν αδύνατη την παροχή υπηρεσιών (απώλεια διαθεσιμότητας). Η επίθεση άρνησης υπηρεσιών μπορεί να έχει δύο μορφές: α) μετά την επίθεση είναι αναγκαία η επανεκκίνηση της υπηρεσίας ώστε να είναι σε θέση να επαναλειτουργήσει και β) η αποστολή μεγάλου μεγέθους πακέτα ψευδών αιτήσεων, έχει ως αποτέλεσμα την ανικανότητα της υπηρεσίας να εξυπηρετήσει αυτούς που πραγματικά την χρειάζονται. Η

πιο γνωστή και συχνή μορφή αυτού του είδους επίθεσης είναι η Κατανεμημένη Επίθεση Άρνησης Υπηρεσιών – DdoS [Εικόνα 4].



Εικόνα 3: Κατανεμημένη Επίθεση Άρνησης Υπηρεσιών – DdoS

Πηγή:https://privacy.ellak.gr/2017/04/24/ti-ine-mia-epithesi-ddos-mia-isagogi-stis-epithesis-distributed-denial-of-service-ddos/

Η DDoS είναι πιο πολύπλοκη και πιο αποτελεσματική καθώς βασίζεται μέχρι και σε εκατοντάδες χιλιάδες συσκευές, γεγονός που κάνει ακόμα πιο δύσκολο τον εντοπισμό τους. Αρκετά μεγάλες επιθέσεις DDoS, μπορούν να ρίξουν ολόκληρα κέντρα δεδομένων με πολλαπλούς server.

● Κλοπή ταυτότητας χρήστη (identity theft): Ο επιτιθέμενος αποκτά δεδομένα προσωπικού χαρακτήρα του χρήστη (passwords, social security numbers κ.α.), με αποτέλεσμα την ειδιοποίηση της ταυτότητας του χρήστη (impersonation) και με σκοπό το οικονομικό όφελος (αγορές προϊόντων μέσω πιστωτικών καρτών, παράνομη επιστροφή φόρου κ.λπ.) εις βάρος του.

● Παραβιάσεις προσωπικών δεδομένων: Επιθέσεις οι οποίες αποσκοπούν στη διαρροή, αλλοίωση ή μη διαθεσιμότητα προσωπικών δεδομένων. Σύμφωνα με τον Κανονισμό της Ε.Ε. 2016/679, τέτοιου είδους επιθέσεις νοούνται ως παραβιάσεις δεδομένων προσωπικού χαρακτήρα οι οποίες χρήζουν άμεσης αντιμετώπισης.

● Εσωτερικές απειλές (insider threat): Απειλές που προέρχονται από στελέχη Φορέων που εργάζονται ή εργάζονταν σε έναν Οργανισμό, καθώς και εξωτερικών συνεργατών, οι οποίοι κατέχουν εσωτερική πληροφόρηση σχετικά με τις πρακτικές ασφάλειας, τα υπολογιστικά συστήματα και τα δεδομένα του Οργανισμού. Οι εν λόγω απειλές μπορούν να οδηγήσουν σε πλήθος επιθέσεων που περιγράφονται στην παρούσα ενότητα, συνήθως με πολύ μεγάλο αντίκτυπο για το Φορέα και είναι εξαιρετικά δύσκολο να διαγνωσθούν ή/και αντιμετωπιστούν.

● Botnets: Δίκτυα τα οποία αποτελούνται από υπολογιστικές συσκευές ανυποψίαστων χρηστών που έχουν μολυνθεί με κακόβουλο λογισμικό και ελέγχονται κεντρικά από κάποιον επιτιθέμενο, προκειμένου να χρησιμοποιηθούν ομαδικά στην αποστολή μηνυμάτων ανεπιθύμητης αλληλογραφίας, σε επιθέσεις άρνησης υπηρεσίας, σε cryptojacking, κλπ.

● Φυσικές απειλές: Απειλές που στοχεύουν στην καταστροφή ή αλλοίωση ή κλοπή εξοπλισμού, με απώτερο στόχο τη διαρροή ή/και καταστροφή δεδομένων ή την άρνηση υπηρεσίας.

● Διαρροή δεδομένων: Διαρροή δεδομένων σε μη εξουσιοδοτημένους χρήστες. Τα δεδομένα μπορεί να περιλαμβάνουν οικονομικά στοιχεία, πατέντες, δεδομένα με κατοχυρωμένα πνευματικά δικαιώματα, πλάνα στρατηγικής ανάπτυξης κλπ.

● Λογισμικό λύτρων (ransomware): Κακόβουλο λογισμικό (malware) το οποίο κρυπτογραφεί τα δεδομένα του πληροφοριακού συστήματος, για την αποκρυπτογράφηση των οποίων ο επιτιθέμενος απαιτεί λύτρα (συνήθως σε μορφή κρυπτονομίσματος).

● Ηλεκτρονική κατασκοπεία: Κατασκοπεία μέσω του κυβερνοχώρου, η οποία μπορεί να περιλαμβάνει χρήση εξειδικευμένων εργαλείων για την άντληση στοιχείων ή/και χρήση συνδυασμού των προαναφερθέντων απειλών. Συνήθως, αυτή η μορφή επίθεσης αναφέρεται ως «στοχευμένη» (λόγω του ότι οι επιτιθέμενοι έχουν πολύ συγκεκριμένους στόχους), με απώτερο στόχο την υποκλοπή ευαίσθητων, για τον οργανισμό, πληροφοριών.

● Cryptojacking: Τεχνικές που χρησιμοποιούν την υπολογιστική ισχύ του υπολογιστή του χρήστη με σκοπό την άντληση (mining) κρυπτονομισμάτων (bitcoins). Ήδη με βάση τα τελευταία στοιχεία του ENISA (ETL 2020, List of top 15 threats, enisa.europa.eu): – οι επιθέσεις τύπου phishing έχουν ήδη ανέλθει στην 3η θέση, με τα web application attacks να κατεβαίνουν στην 4η , – οι επιθέσεις spam ανέβηκαν στην 5η θέση και οι επιθέσεις DDoS κατέβηκαν στην 6η θέση – οι επιθέσεις identity theft ανέβηκαν από τη 13η στην 7η θέση – η περίπτωση των botnets βρίσκεται πλέον στη 10η θέση – η περίπτωση physical manipulation, damage, theft and loss κατέβηκε στην 11η θέση – ομοίως η περίπτωση information leakage κατέβηκε στη 12η θέση – στη 13η θέση ανήλθαν τα ransomware – στη 14η θέση ανήλθαν οι περιπτώσεις cyberespionage – στη 15η θέση βρίσκονται οι περιπτώσεις cryptojacking.

2.5 Κυβερνοεπιθέσεις στον τομέα της υγειονομικής περίθαλψης

Ο τομέας της υγειονομικής περίθαλψης έχει γίνει γνωστός στόχος για ενοχλητικές κυβερνοεπιθέσεις. Τα νέα για επιθέσεις *ransomware* που έδεσαν νοσοκομεία και συστήματα εμπιστοσύνης δημοσιοποιήθηκαν το 2016, όταν περίπου 20 νοσοκομεία χτυπήθηκαν από διάφορα είδη κακόβουλου λογισμικού σε διάστημα οκτώ μηνών. Το υψηλό ποσοστό πρόσβασης και ευαισθησίας στο χρόνο στην υγειονομική περίθαλψη σημαίνει ότι οι απαιτήσεις για *ransomware* είναι πιο πιθανό να καλυφθούν και η νομισματική απώλεια θεωρείται από πολλά νοσοκομεία ως απαραίτητη απώλεια σε σύγκριση με την αποκατάσταση της πρόσβασης και την ευθύνη περίθαλψης.

Αν και το ποσοστό επιθέσεων εναντίον νοσοκομείων μειώθηκε απότομα μέχρι το 2017, τα περιστατικά αυξήθηκαν ξανά κατά 47% έως το 2018. (Helms K., 2018).

2.5.1. WannaCry

Η κυβερνοεπίθεση *WannaCry* του 2017 ήταν περισσότερο σημαντική για την ευαισθητοποίηση του κοινού για την απειλή στον κυβερνοχώρο στην υγειονομική περίθαλψη. Με την επίθεση *ransomware,* όπου το κακόβουλο λογισμικό μόλυνε υπολογιστές, κρυπτογραφούσε τα δεδομένα του υπολογιστή και δεν επέτρεπε την πρόσβασή τους από τον εκάστοτε χρήστη παρά μόνο εάν έδινε τα απαιτούμενα λύτρα, το NHS επηρεάστηκε άσχημα στο

Ηνωμένο Βασίλειο, φανερώνοντας τόσο τη μολυσματικότητα της επίθεσης όσο και την κακή κατάσταση της ασφάλειας στον κυβερνοχώρο σε μία σημαντική δημόσια υπηρεσία. Υπολογίζεται ότι 1.200 τεμάχια διαγνωστικού εξοπλισμού χτυπήθηκαν από την επίθεση, καθώς και η συντριπτική πλειοψηφία των υπολογιστών και ιατρικών μηχανημάτων που λειτουργούν με ασυμβίβαστα λειτουργικά συστήματα *Microsoft Windows 7*. (Henriksen, 2019)

Σύμφωνα με το Υπουργείο Υγείας και Κοινωνικής, η επίθεση στοίχισε στο *NHS* 92 εκατομμύρια λίρες - 19 εκατομμύρια λίρες από τη χαμένη παραγωγή κατά τη διάρκεια της επίθεσης, 0,5 εκατομμύρια λίρες σε κόστος πληροφορικής κατά τη διάρκεια της επίθεσης και 72 εκατομμύρια λίρες σε κόστος πληροφορικής μετά την επίθεση. (Higgins K., 2018) Νοσοκομεία των ΗΠΑ επηρεάστηκαν επίσης από την επίθεση *WannaCry*, αν και η ζημιά συγκεντρώθηκε στους ενισχυτές εικόνας μαγνητικής τομογραφίας και στις ιατρικές συσκευές *Siemens* και *BD*. (Homeland Security Committee., 2018)

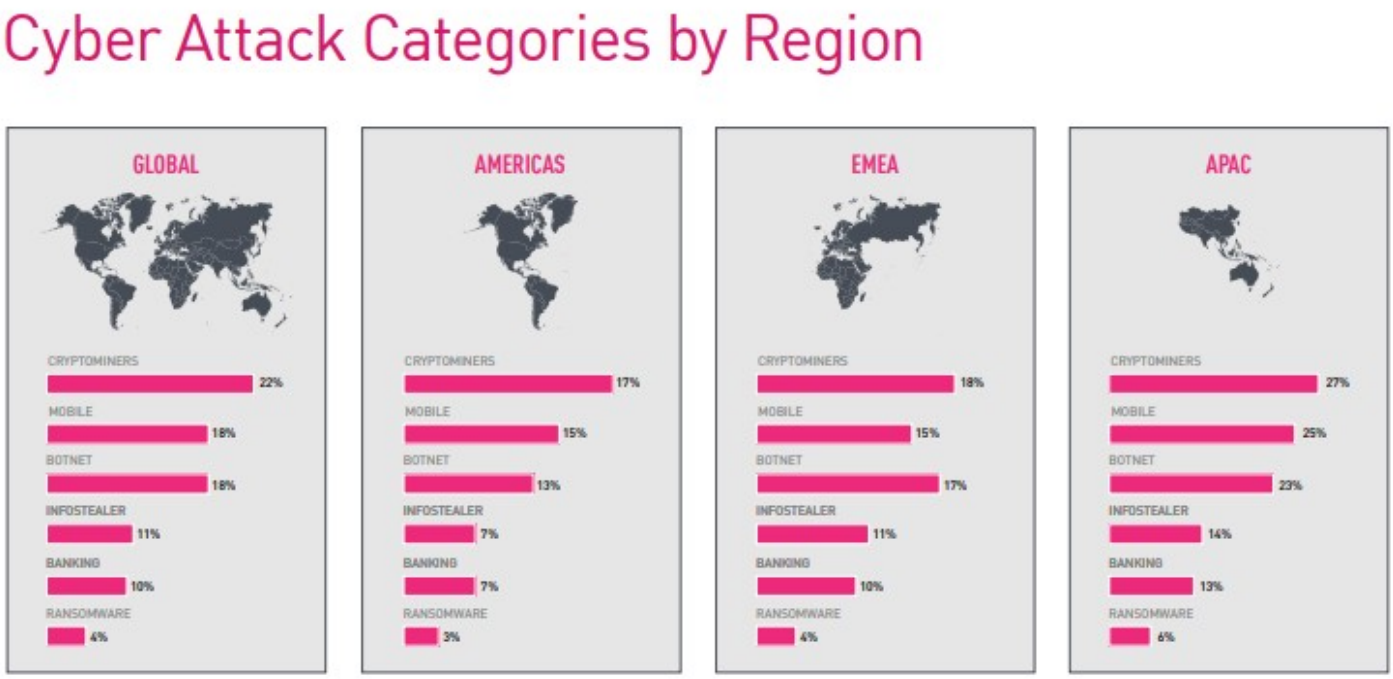
Το *NHS* δέχθηκε κριτική για τη λειτουργία μη ασφαλών, εκτός λειτουργίας, λειτουργικών συστημάτων μετά την επίθεση. Ωστόσο, είναι ζωτικής σημασίας να γίνει αντιληπτό ότι η ενημέρωση της τεχνολογίας της λειτουργίας που χρησιμοποιείται σε νοσοκομεία και ιατρικά περιβάλλοντα φέρει τους δικούς της κινδύνους και κρυφό κόστος. Απαιτούνται επίσης αυστηρές διαδικασίες για την τροποποίηση οποιασδήποτε ιατρικής συσκευής, συμπεριλαμβανομένης της εγκατάστασης επιδιορθώσεων ασφαλείας. Σε πολλές περιπτώσεις στην ιατρική περίθαλψη, συνιστάται στις εγκαταστάσεις να περιορίσουν την αγορά αποθεμάτων τους σε «έναν τύπο συσκευής», προκειμένου να μειωθούν οι περίπλοκοι χρόνοι εκπαίδευσης και να περιοριστεί η σύγχυση των χειριστών.

2.5.2. **Düsseldorf University Hospital**

Αντίστοιχα μία επίθεση ransomware, συνέβει τον Σεπτέμβριο του 2020 στο Düsseldorf University Hospital στη Γερμανία από την οποία είχαμε την πρώτη απώλεια ζωής λόγω κυβερνοεπίθεσης. Η επίθεση είχε ως αποτέλεσμα την απενεργοποίηση των υπολογιστικών συστημάτων του νοσοκομείου και την μεταφορά δεδομένων από φάκελο σε φάκελο με σκοπό την δημιουργία σύγχυσης, δεδομένου ότι τα αρχεία δεν θα ήταν πλέον τα σωστά ανά φάκελο. Η επίθεση αυτή ανάγκασε το νοσοκομείο να απομακρύνει ασθενείς οι οποίοι είχαν προσέλθει στα εξωτερικά ιατρεία ως επείγοντα περιστατικά με αποτέλεσμα, μία γυναίκα η οποία έπρεπε να μεταφερθεί επειγόντως για μία άκρως σημαντική εγχείρηση, πέθανε κατά τη διάρκεια της

μεταφοράς της σε κοντινή πόλη λόγω της καθυστέρησης στη θεραπεία που χρειαζόταν. Οι επιτιθέμενοι εκμεταλλεύτηκαν τρωτά σημεία που υπήρχαν στο VPN λογισμικό του νοσοκομείου. Αυτό το σημείο τρωτότητας ήταν γνωστό αρκετούς μήνες πριν αλλά δεν προστατεύθηκε ούτε διορθώθηκε από την πλευρά του νοσοκομείου.

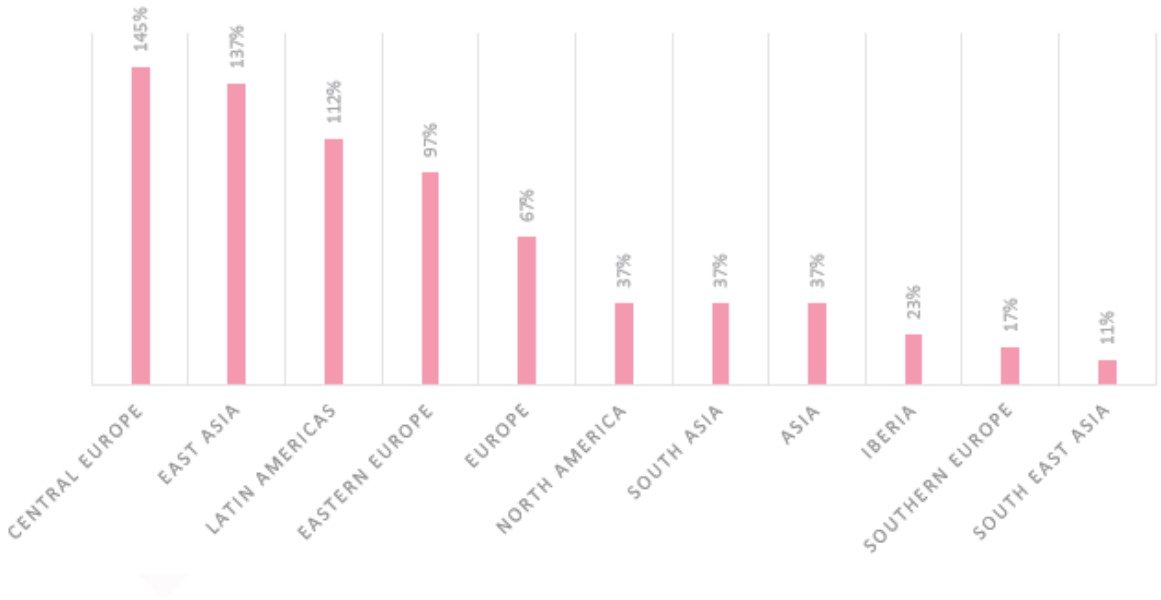
2.6 Πίνακες ιστογράμματα κυβερνο-επιθέσεων εν μέσω πανδημίας Covid – 19 (2020)



Εικόνα 4:Κατηγορίες κυβερνο-επιθέσεων ανά περιοχή

Πηγή: check-point research, cyber attack trends : 2020 mid-year report (CYBER ATTACK TRENDS: 2020 MID-YEAR REPORT - Check Point Research)

Στα τέλη Οκτωβρίου 2020, τα νοσοκομεία και οργανισμοί υγειονομικής περίθαλψης είχαν στοχοποιηθεί από ένα αυξανόμενο κύμα επιθέσεων *ransomware*, με την πλειονότητα των επιθέσεων να χρησιμοποιεί το διαβόητο *ransomware Ryuk*. Αυτό ακολούθησε μια κοινή συμβουλευτική για την κυβερνοασφάλεια που εκδόθηκε από το *CISA*, το *FBI* και το *HHS*, η οποία προειδοποίησε για αυξημένη και επικείμενη απειλή για κυβερνοέγκλημα στα νοσοκομεία και τους παρόχους υγειονομικής περίθαλψης των ΗΠΑ.

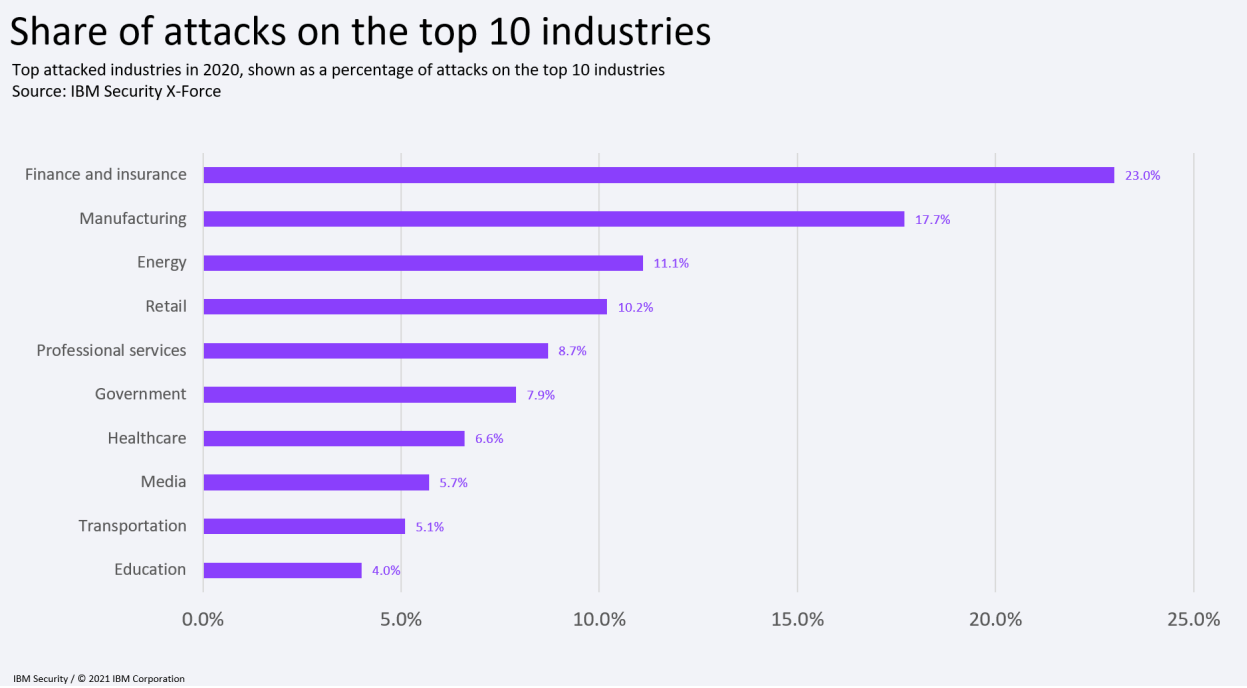


Σχήμα 2 : Αύξηση των επιθέσεων σε υγειονομικούς οργανισμούς ανά περιοχή.

Πηγή: CheckPoint (Attacks targeting healthcare organizations spike globally as COVID-19 cases rise again - Check Point Software)

Η ανάλυση των 10 κορυφαίων βιομηχανιών που στοχεύουν είναι η λιανική, οι επαγγελματικές υπηρεσίες, η κυβέρνηση, η υγειονομική περίθαλψη, τα μέσα ενημέρωσης, οι μεταφορές και εκπαίδευση. Ενώ κατέλαβε την έβδομη θέση το 2020, ο αριθμός των επιθέσεων στην υγειονομική περίθαλψη υπερδιπλασιάστηκε σε σύγκριση με το 2019 και σχεδόν το ένα τρίτο όλων των επιθέσεων στον τομέα της υγειονομικής περίθαλψης ήταν περιπτώσεις *ransomware*.

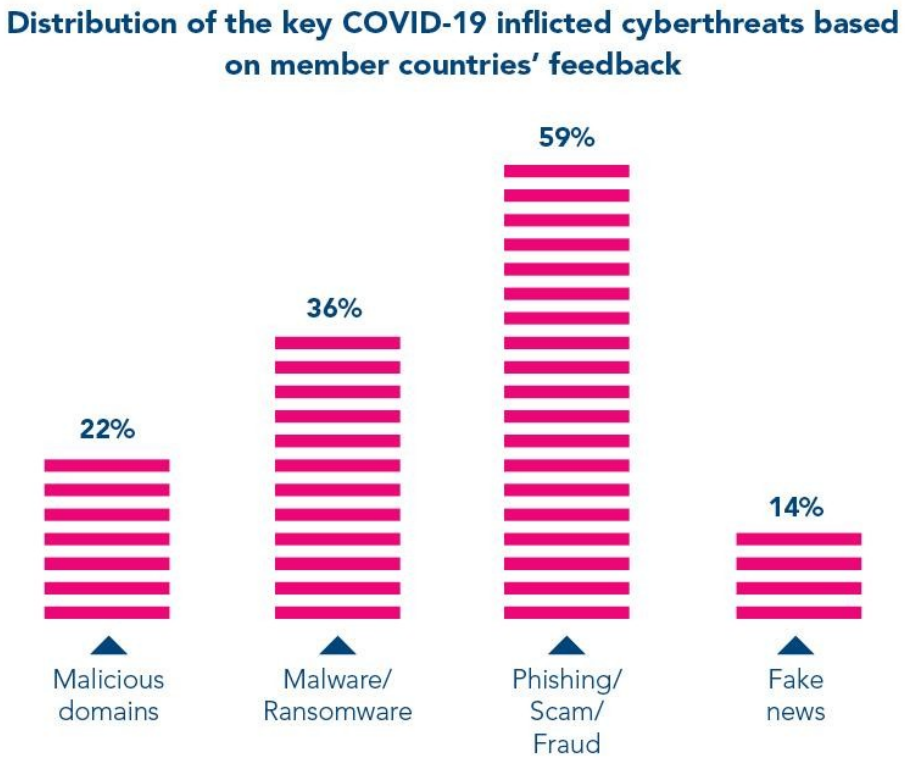
Ο τομέας της υγειονομικής περίθαλψης διανύει εξαιρετικά δύσκολες εποχές, αφού πρέπει να ανταποκριθεί σε μια παγκόσμια πανδημία, ενώ γίνεται όλο και περισσότερο στόχος από εξελιγμένα εγκλήματα στον κυβερνοχώρο και φορείς απειλής εθνικού κράτους για να διαταράξουν και να κλέψουν δεδομένα από οργανισμούς σε αυτόν τον κλάδο.



Σχήμα 3:Οι 10 περισσότερο επιτιθέμενες βιομηχανίες το 2020 με ποσοστά επιθέσεων.

Πηγή : Security Intelligence (Threat Actors' Most Targeted Industries in 2020: Finance, Manufacturing, and Energy (securityintelligence.com))

Μια εκτίμηση της *INTERPOL* για τον αντίκτυπο του *COVID-19* στο κυβερνοέγκλημα, έδειξε μια σημαντική αλλαγή στόχου από άτομα και μικρές επιχειρήσεις σε μεγάλες εταιρείες, κυβερνήσεις και υποδομές ζωτικής σημασίας. Με τους οργανισμούς και τις επιχειρήσεις να αναπτύσσουν ταχέως απομακρυσμένα συστήματα και δίκτυα για την υποστήριξη του προσωπικού που εργάζεται από το σπίτι, οι εγκληματίες εκμεταλλεύονται επίσης τις αυξημένες ευπάθειες ασφαλείας για να κλέψουν δεδομένα, να δημιουργήσουν κέρδη και να προκαλέσουν αναστάτωση. Σε μία περίοδο τεσσάρων μηνών (Ιανουάριος έως Απρίλιος) περίπου 907.000 μηνύματα ανεπιθύμητης αλληλογραφίας, 737 περιστατικά που σχετίζονται με κακόβουλο λογισμικό και 48.000 κακόβουλα *URL*-όλα σχετικά με τον *COVID-19*-εντοπίστηκαν από έναν από τους συνεργάτες του ιδιωτικού τομέα της *INTERPOL*.



Σχήμα 4: Διανομή των κυριότερων κυβερνο -απειλών που προκλήθηκαν από τον covid 19 με βάση τα σχόλια των κρατών μελών

Πηγή: Interpol (INTERPOL report shows alarming rate of cyberattacks during COVID-19)

3. Δεδομένα Υγείας, Πληροφοριακά Συστήματα & Τεχνολογίες Διαχείρισης Πληροφοριών

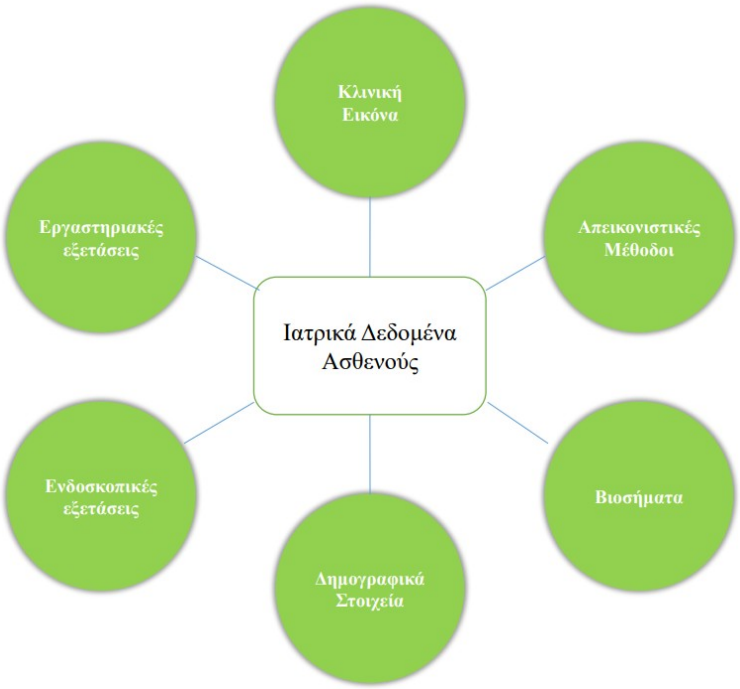
3.1 Ιατρικά δεδομένα και κατηγοριοποίηση

Η πρόοδος της ιατρικής επιστήμης αλλά και η τεχνολογική ανάπτυξη ολοένα και διευρύνει το ήδη ευρύ φάσμα των ιατρικών δεδομένων. Τα βασικότερα ιατρικά δεδομένα που μπορούν καταγραφούν είναι τα εξής:

- Κατά την επίσκεψη του ασθενούς στην μονάδα υγείας καταγράφεται το ιστορικό των συμπτωμάτων και τα συμπεράσματα του ιατρού από την κλινική εξέταση. Η καταγραφή των συμπτωμάτων μπορεί να γίνει συμπληρώνοντας κάποια φόρμα, ενώ τα συμπεράσματα του ιατρού είναι συνήθως ελεύθερο κείμενο το οποίο συντάσσεται με σκοπό να αποδοθεί περιγραφικά η κλινική εικόνα του ασθενούς και να γίνουν τυχούσες διαγνώσεις.
- Συνήθως όταν ένας ασθενής εισάγεται σε δομές πρωτοβάθμιας υγείας, ακολουθούν μια σειρά εργαστηριακών εξετάσεων (π.χ. αιματολογικές, ουρολογικές κ.ο.κ). Τα αποτελέσματα των εξετάσεων αυτών αποτελούν αναπόσπαστο κομμάτι της κλινικής εικόνας του ασθενούς, και επομένως καταγράφονται.
- Άλλες καταγραφές ρουτίνας είναι αυτές που σχετίζονται με τα βιοϊατρικά σήματα. Το πιο χαρακτηριστικό και ευρέως διαδεδομένο είναι το καρδιογράφημα. Πολλά από τα βιοϊατρικά σήματα περιγράφονται με μεγάλη λεπτομέρεια σε αυτό το βιβλίο. Ενδεικτικά αναφέρουμε επίσης το ηλεκτροεγκεφαλογράφημα, ηλεκτρομυογράφημα, αλλά και τα σήματα που συλλέγονται από αισθητήρες κίνησης. Τα σήματα αυτά καταγράφονται ως μια ακολουθία τιμών στη διάρκεια του χρόνου, όπου κάθε τιμή αναπαριστά κάποια στιγμιαία τιμή μιας φυσικής ιδιότητας.

- Εξέχοντα ρόλο κατέχουν επίσης οι καταγραφές εικόνων, οι οποίες προκύπτουν από τις διάφορες απεικονιστικές μεθόδους εξετάσεων. Συγκεκριμένα οι τέσσερις βασικές κατηγορίες απεικονιστικών μεθόδων είναι η ακτινογραφία, ο υπέρηχος, η μέθοδος μαγνητικού συντονισμού (μαγνητική τομογραφία), αλλά και οι πυρηνικές μέθοδοι απεικόνισης, όπως είναι το σπινθηρογράφημα. Όπως γίνεται εύκολα αντιληπτό, τα δεδομένα αυτά καταχωρούνται υπό τη μορφή εικόνας.
- Εκτός από τα σήματα και τις εικόνες πολλές φορές απαιτείται η αποθήκευση βίντεο. Περιπτώσεις βιντεοσκόπησης προκύπτουν κυρίως από ενδοσκοπικές εξετάσεις, όπως για παράδειγμα η γαστροσκόπηση και η κολονοσκόπηση.
- Τέλος εκτός από τα στοιχεία που καταχωρούνται από την παρούσα κατάσταση του ασθενούς μέσω των εξετάσεων και των διαγνωστικών μεθόδων, ο κάθε ασθενής χαρακτηρίζεται και από δεδομένα που πηγάζουν είτε από τον τρόπο ζωής του (π.χ. καπνιστής), είτε από στοιχεία κληρονομικότητας (π.χ. ιστορικό των προγόνων του σε συγκεκριμένες παθογενείς καταστάσεις), είτε και από οποιονδήποτε άλλο παράγοντα μπορεί να θεωρηθεί παράγοντας που επιδρά στη νοσηρότητα.

Το σημείο που αξίζει να τονιστεί είναι η καταχώρηση όλων των δεδομένων με χρονολογική σειρά, γεγονός που επιτρέπει ανά πάσα στιγμή στους ειδικούς να έχουν μια πλήρη εικόνα του ιστορικού του ασθενούς και σχετικά με την ιατρική κατάσταση που αντιμετωπίζουν αλλά και γενικά με την υγεία του ασθενούς. Η εικόνα 4 συνοψίζει τις πηγές από τις οποίες λαμβάνονται τα ιατρικά δεδομένα ενός ασθενούς.



Εικόνα 4: Πηγές από τις οποίες λαμβάνονται τα ιατρικά δεδομένα ενός ασθενούς

Πηγή: https://repository.kallipos.gr/bitstream/11419/2977/1/02_chapter_02.pdf

3.1.1. Μεγάλα Δεδομένα (Big Data) & Διαδίκτυο των Πραγμάτων (IoT)

Σε αυτή τη σύγχρονη τεχνολογική εποχή οι πληροφορίες αυξάνονται εκθετικά. Οι φορητές συσκευές παράγουν συνεχώς ένα τεράστιο όγκο δεδομένων που είναι τελικά γνωστά ως μεγάλα δεδομένα σε λαϊκούς όρους. Τα μεγάλα δεδομένα είναι τα δεδομένα των οποίων η ποικιλία και η κλίμακα πολυπλοκότητας χρειάζονται νέα δομή, αλγόριθμο, τεχνική και αναλύσεις για τη διαχείριση, οπτικοποίηση των νέων ιδεών από τα μεγάλα δεδομένα της υγειονομικής περίθαλψης για περαιτέρω παροχή εύκολης λύσης.

Τα μεγάλα δεδομένα έχουν αποκτήσει μεγάλη σημασία σε πολλούς οργανισμούς, με εφαρμογές υγειονομικής περίθαλψης, τράπεζες, εφαρμογές που βασίζονται στο Διαδίκτυο πραγμάτων (*IoT*), απεικόνιση, έξυπνες πόλεις, έξυπνο σύστημα μεταφορών και πολλά άλλα (Khan N. et al., 2014). Τα δεδομένα αποθηκεύονται με τυποποιημένο τρόπο για εύκολη αποθήκευση, πρόσβαση και ανάκτηση των απαιτούμενων σχετικών πληροφοριών. Έξυπνες

εφαρμογές που βασίζονται στο *IoT* όπως φορητές συσκευές, γεννήτριες ηλεκτρονικών ιατρικών αναφορών (*EMR*), έξυπνα κινητά τηλεφωνικά, συστήματα υγειονομικής περίθαλψης, έχουν μετατρέψει τα συμβατικά συστήματα υγείας στο ψηφιακό σύστημα υγειονομικής περίθαλψης. Ένα τεράστιο ποσοστό δεδομένων παράγεται από αυτές τις συσκευές σε καθημερινή βάση.

Η εκθετική αύξηση των μεγάλων ιατρικών δεδομένων έχει προσελκύσει την ερευνητική κοινότητα για την εξαγωγή και οπτικοποίηση των νέων ιδεών από τα μεγάλα δεδομένα της υγειονομικής περίθαλψης. Πολλές μεγάλες πηγές δεδομένων διατίθεται στην αγορά υγειονομικής περίθαλψης όπως π.χ. στοιχεία εγγραφής, βιομετρικά δεδομένα, ηλεκτρονικά αρχεία υγείας, απεικόνιση, αναφορές ασθενών, δεδομένα στο Διαδίκτυο, δεδομένα βιοδεικτών, κλινικά δεδομένα και διοικητικά στοιχεία (Rumsfeld S.J., Joynt K.E., Maddox M.T., 2016).

Κάποιες από τις σημαντικές προκλήσεις είναι ένα αποτελεσματικό μοντέλο αναγνώρισης που απαιτείται για την επεξεργασία του τεράστιου όγκου δεδομένων υγειονομικής περίθαλψης ενώ για τον προσδιορισμό του χαρακτηριστικού πραγματοποιήθηκε ταξινόμηση για τις αναγνωριστικές ασθένειες, η έλλειψη κινήτρων για την ανταλλαγή δεδομένων και η παράνομη χρήση (εκβιασμού) μεγάλων δεδομένων υγειονομικής περίθαλψης (Wang W., Krishan E., 2014). Για τη συγκέντρωση μεγάλων δεδομένων υγειονομικής περίθαλψης απαιτείται κάποιος δομικός μηχανισμός (Kitchenham B. et al., 2009). Λόγω της εμπλοκής ακριβών εξαρτημάτων υλικού (όργανα), τα μεγάλα δεδομένα για την υγειονομική περίθαλψη είναι πιο ακριβά. Τα δεδομένα αυτά για την υγειονομική περίθαλψη έχουν πολυάριθμες εφαρμογές στον τομέα της δημόσιας υγείας, της επιτήρησης και ασφάλειας ασθενειών, της πρόβλεψης μοντέλων και κλινικών, υποστήριξη αποφάσεων και πολλούς άλλους τομείς έρευνας. Οι ερευνητές αντιμετωπίζουν πολλά εμπόδια στην εξαγωγή των εμπλουτισμένων πληροφοριών από μεγάλα δεδομένα υγειονομικής περίθαλψης και την εφαρμογή τους για σκοπούς αναγνώρισης ασθενειών. Παρόλα αυτά τα μεγάλα δεδομένα έχουν πολλά χαρακτηριστικά που πρέπει να αναλυθούν ειδικά στον τομέα της υγειονομικής περίθαλψης. Μερικοί ερευνητές χρησιμοποίησαν τα χαρακτηριστικά του σακχάρου στο αίμα, το ρυθμό του σφυγμού, τη κλίμακα κώματος της Γλασκόβης και το ρυθμό αναπνοής, ενώ η χρόνια νευρική κλίμακα (ΚΝΣ) μελετάται και αναλύεται (Nazir S. et al., 2019), (Nazir S. et al., 2019). Δεν έχει αναφερθεί εργασία για τον εντοπισμό διαφορετικών τεχνικών για να επιλεχθούν μεγάλες δυνατότητες δεδομένων στην

υγειονομική περίθαλψη. Ένα χαρακτηριστικό μπορεί να είναι τα μοναδικά στοιχεία ταυτότητας τα οποία ως εκ τούτου χρησιμοποιούνται για τον εντοπισμό μιας συγκεκριμένης ασθένειας.

3.1.2. Ο ρόλος των μεγάλων δεδομένων στην ιατρική εκπαίδευση

Οι ερευνητές και οι καθηγητές χρησιμοποίησαν μεγάλα δεδομένα στο πρόγραμμα σπουδών της ιατρικής για το σχεδιασμό, ανάλυση, προγραμματισμό, και την εκτίμηση, διασφαλίζοντας την παράδοση των δραστηριοτήτων των εκπαιδευτικών, ενισχύοντας με αυτό το τρόπο την εκπαίδευση στην υγειονομική περίθαλψη. Τα μεγάλα δεδομένα χρησιμοποιούνται συνήθως στην ιατρική εκπαίδευση για τη βελτίωση της ιατρικής ηλικίας. Το οπτικό *analytic* έχει πολλές εφαρμογές στην ανάλυση των τεχνικών δεδομένων και εκμετάλλευσης, την ανθρώπινη γνωστική δύναμη να αντιλαμβάνεται, την αναπαράσταση πληροφοριών και γνώσεων, καθώς και τον προσδιορισμό οπτικών μοτίβων (Vaittsis C., Nilsson G., Zary N., 2014).

Η δυνατότητα των ιατρικών δεδομένων περικλείει όλες τις βασικές πληροφορίες που απαιτούνται για τη διάγνωση ορισμένων ασθενειών. Τα χαρακτηριστικά είναι οι στατικές έξυπνες τιμές που παρουσιάζονται σε οποιαδήποτε μεγάλα συστήματα δεδομένων. Αυτά τα χαρακτηριστικά δεδομένων είναι σε συνδυασμό μεταξύ τους για συγκεκριμένο σκοπό. Αυτές οι αναλύσεις δεδομένων βοηθούν στον εντοπισμό μιας νόσου για έναν συγκεκριμένο ασθενή με βάση το ιστορικό της υγειονομικής περίθαλψης. Αυτές οι αναλυτικές τιμές δεδομένων τελικά βοηθούν τους γιατρούς και τους επαγγελματίες προτείνοντας το ακριβές φάρμακο για μια συγκεκριμένη ασθένεια για έναν συγκεκριμένο ασθενή.

Η υγειονομική ανάλυση και διαχείριση μεγάλων δεδομένων έχει γίνει ένα δύσκολο έργο για τους ερευνητές. Η έγκαιρη λήψη αποφάσεων στα συστήματα υγειονομικής περίθαλψης απαιτεί τεράστιες δυνατότητες για βελτίωση της ποιότητας της φροντίδας, ελαχιστοποίηση του κόστους περίθαλψης και μείωση του σφάλματος και των αποβλήτων υγειονομική περίθαλψη ανάλυση μεγάλων δεδομένων.

3.2 GDPR και άλλα πρωτόκολλα δεδομένων στην ιατρική

Ο *GDPR* (Γενικός Κανονισμός για την Προστασία Δεδομένων) ονομάζεται «ο κανονισμός του Ευρωπαϊκού Κοινοβουλίου και του συμβούλιο για την προστασία των ατόμων σε σχέση με την επεξεργασία των προσωπικών δεδομένων και την ελεύθερη κυκλοφορία τέτοιων δεδομένων ».

Για παραβιάσεις των βασικών αρχών της επεξεργασίας δεδομένων, δικαιώματα των υποκειμένων δεδομένων ή άλλες μη συμμορφώσεις προς τα άρθρα του *GDPR* επιβάλλονται πρόστιμα έως 20 εκατομμύρια ευρώ ή 4% του ετήσιου κύκλου εργασιών μιας επιχείρησης όποιο είναι υψηλότερο (άρθρο 79 (3α) (E. Union, 2018). Ως εκ τούτου, είναι μια κρίσιμη ανάγκη για κάθε εταιρεία να βρει τρόπους για να επιτύχει και να διατηρήσει τη συμμόρφωση με τον *GDPR*. Ο γενικός κανονισμός απορρήτου δεδομένων (*GDPR*) (E. Union, 2018) είναι 209 σελίδες νομικού εγγράφου. Για τις μικρές επιχειρήσεις, μπορεί να είναι δύσκολο να αντιμετωπιστεί μια τόσο περίπλοκη προδιαγραφή απαιτήσεων. Για να φανεί πώς ο *GDPR* μπορεί να είναι συστηματικά αντιστοιχισμένος σε μια επίσημη προδιαγραφή αρχιτεκτονικής συστήματος, χρησιμοποιούνται καθιερωμένες τεχνικές ασφαλείας και μηχανικής λογισμικού.

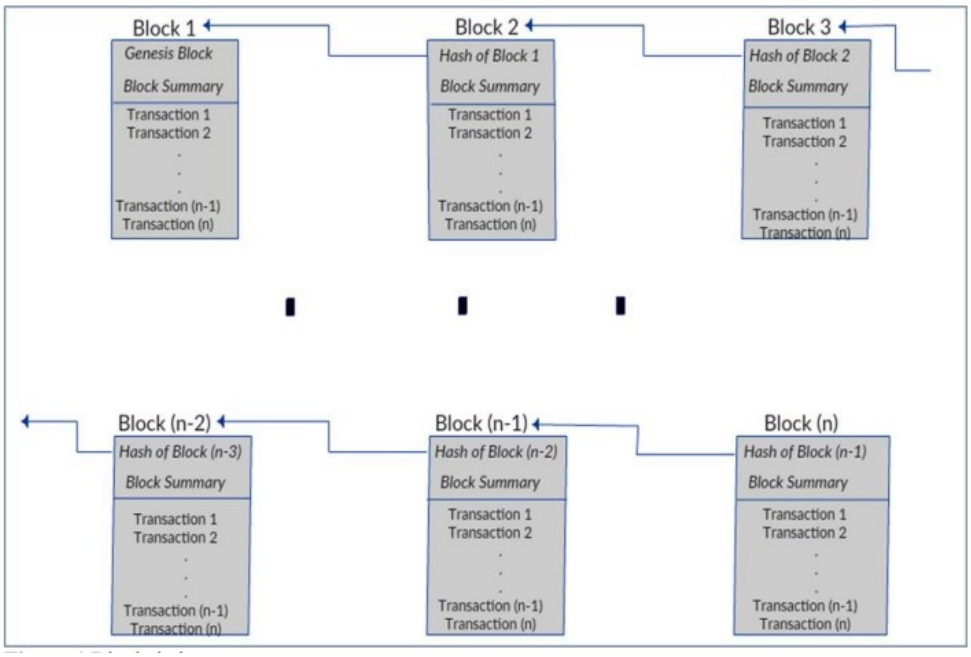
Τεχνικά, προτείνεται ένας συνδυασμός μοντέλων ελέγχου ροής πληροφοριών για την προστασία δεδομένων σε κατανεμημένα συστήματα με σήμανση δεδομένων με ετικέτες ασφαλείας στο ύφος του Αποκεντρωμένου Μοντέλου ετικέτας (*DLM*) (Kammuller F., 2019) και χρησιμοποιείται η ανάπτυξη *Fusion/UML* για ανάλυση και σχεδιασμό συστημάτων λογισμικού. Πιο συγκεκριμένα, χρησιμοποιείται μια εκτεταμένη διαδικασία (Kammuller F., 2019) που καθιερώνει μια σχέση συνέπειας μεταξύ ανάλυσης και σχεδιασμού και παράγει μια επίσημη προδιαγραφή για την εφαρμογή. Σημαντικά σημεία είναι

- Η ανάλυση του νομικού εγγράφου του *GDPR* σε περισσότερο εύπεπτες τεχνικές απαιτήσεις,
- Να δειχθεί πώς μπορεί το Μοντέλο Αποκεντρωμένης Επισήμανσης (*DLM*) να ενσωματωθεί με τις μεθόδους της πραγματιστικής μηχανικής λογισμικού *Fusion/UML* για την παραγωγή μιας τυπικά καθορισμένης Αρχιτεκτονικής του συστήματος,
- Η απεικόνιση της διαδικασίας για την εφαρμογή υγειονομικής περίθαλψης *SUCCESS IoT*. (Kammuller F., 2019)

3.3 Τεχνολογία Blockchain

Η τεχνολογία *Blockchain* είναι ένα διανεμημένο ηλεκτρονικό λογιστικό αρχείο ψηφιακών αρχείων, γεγονότων ή συναλλαγών που είναι κρυπτογραφικά ασφαλές, εξαιρετικά δύσκολο να πλαστογραφηθεί, και μπορεί να ενημερωθεί μέσω ενός πρωτοκόλλου συναίνεσης συμβατό με όλους τους συνδεδεμένους κόμβους. (Laurence T., 2017) Η τεχνολογία χρησιμοποιεί αποκεντρωμένους αλγόριθμους συναίνεσης για έλεγχο συνέπειας της βάσης

δεδομένων. Η βάση δεδομένων είναι καθαρά διανεμημένη στη φύση και μοιράζεται σε όλους τους κόμβους που είναι συνδεδεμένοι στο δίκτυο. Οι συναλλαγές στις βάσεις δεδομένων ομαδοποιούνται για συγκεκριμένο χρονικό διάστημα ώστε να υπάρχει ο απαραίτητος χρόνος για να σχηματιστεί ένα μπλοκ συγκεκριμένου αριθμού συναλλαγών. Αυτά τα μπλοκ είναι συνδεδεμένα κρυπτογραφικά μέσω δεικτών κατακερματισμού για να σχηματίσουν μία αλυσίδα Blockchain (Σχήμα 5) (Laurence T., 2017; Bashir I., 2017).



Σχήμα 5: Η έννοια του *Blockchain*

Πηγή: Research Gate https://www.researchgate.net/publication/330185462

3.4 Πληροφοριακά συστήματα υγείας blockchain

Η υγειονομική περίθαλψη είναι ένας τομέας που απαιτεί πιο αποτελεσματικό και ασφαλές σύστημα διαχείρισης ιατρικών αρχείων, προέγκριση πληρωμών, διακανονισμό ασφαλιστικών απαιτήσεων, και την εκτέλεση και ηχογράφηση πιο πολύπλοκων συναλλαγών. Η τεχνολογία blockchain παρέχει λύσεις σε αυτά τα προβλήματα. Τα αρχεία ηλεκτρονικής ιατρικής τηρούνται σε κέντρα δεδομένων και η πρόσβαση περιορίζεται σε δίκτυα νοσοκομείων και παρόχων φροντίδας. Η συγκέντρωση τέτοιων πληροφοριών το καθιστά ευάλωτο σε παραβίαση της ασφάλειας και μπορεί να είναι δαπανηρό να διατηρηθεί (Grooper A., 2016). Για να το εξαλείψουν τα blockchain το πλήρες ιατρικό ιστορικό για κάθε ασθενή, με πολλαπλές

λεπτομέρειες ελέγχου από τον ασθενή, γιατρούς, ρυθμιστικές αρχές, νοσοκομεία, ασφαλιστές και μεταξύ αυτών άλλα, παρέχουν έναν ασφαλή μηχανισμό καταγραφής και διατηρούν ένα ολοκληρωμένο ιατρικό ιστορικό για τον καθένα. Αυτά εξασφαλίζουν ανθεκτικά σε παραβιάσεις μέσα αποθήκευσης ιατρικού ιστορικού, μειωμένο χρόνο στην ανάλυση των ασφαλιστικών απαιτήσεων, αυξημένη αποτελεσματικότητα σε παροχή ασφαλιστικών εισφορών καθώς και πλήρη ιατρικό ιστορικό του ασθενούς για χρήση από γιατρούς με ακρίβεια συστάσεων για φάρμακα (Grooper A., 2016;Samuel RE., 2016).

Η τεχνολογία Blockchain έχει ήδη εφαρμόσει πολλές διαφορετικές πτυχές στον τομέα της υγειονομικής περίθαλψης για επικύρωση δεδομένων ασθενών, διαχείριση αρχείων ηλεκτρονικής υγείας (EHR), παρακολούθηση μεθόδων έρευνας για την παραγωγή ασφαλέστερων φαρμάκων μεταξύ άλλων. Για παράδειγμα, στη διασφάλιση της σωστής διαλειτουργικότητας, ακεραιότητας και απορρήτου των πληροφοριών των ασθενών, η Guardtime και η εσθονική αρχή ηλεκτρονικής υγείας συνεργάζονται στην εφαρμογή τεχνολογίας blockchain σε εθνικό επίπεδο. Επιπλέον, ο στόχος της εφαρμογής της τεχνολογίας είναι να διασφαλιστεί η διαφάνεια, η δυνατότητα ελέγχου ενώ είναι περισσότερο σημαντική η σωστή διακυβέρνηση και διαχείριση των πληροφοριών του ασθενούς (Randall D, Goel P, Abujamra R. 2017;Kho W., 2018, Engelhardt MA., 2017).

Ωστόσο, η προκρυπτογράφηση στο πλαίσιο της τράπεζας SNS N.V και η Deloitte δημιουργούν ένα σύστημα που διευκολύνει τους ασθενείς να λάβουν συνταγές που αποθηκεύονται με ασφάλεια στο blockchain. Το σύστημα παρέχει στους ασθενείς πλήρη κυριότητα των ιατρικών τους αρχείων, επιτρέποντάς τους να ανακαλέσουν και να χορηγήσουν τον πάροχο πρόσβασης στα προσωπικά τους δεδομένα. (Engelhardt MA. 2017; Benchoufi M, Ravaud P., 2017;, SA Medicalchain 2018; Androulaki E. et al., 2018).

4. Κυβερνοασφάλεια και κυβερνοεπιθέσεις στην υγεία

4.1 Τομέας Υγείας

Ο τομέας της υγειονομικής περίθαλψης, είναι ένας από τους πιο ευάλωτους σε εγκλήματα στον κυβερνοχώρο στον κόσμο. Σύμφωνα με τους Kabir, Ezekekwu, Bhuyan, Mahmood και Dobalian (2020) "Οι οργανώσεις υγειονομικής περίθαλψης είναι ένας κύριος στόχος για κυβερνοεπιθέσεις" (σελ.1). Η κυβερνοασφάλεια είναι ένα εξαιρετικά επίπονο έργο, που απαιτεί πολλή προσπάθεια, πόρους και εστίαση. Το ηλεκτρονικό έγκλημα εμφανίστηκε στα τέλη της δεκαετίας του 1970, όταν ο τομέας της τεχνολογίας της πληροφορίας (ΤΠ) ήταν ακόμη σε εξέλιξη (Kruse, Frederick, Jacobson & Monticone, 2017).

Η κυβερνοασφάλεια είναι μια ολοκληρωμένη έννοια που περιλαμβάνει, μεταξύ άλλων θεμάτων, βέλτιστες πρακτικές, πολιτικές, εγγυήσεις, εκπαίδευση, οδηγίες, διαχείριση κινδύνων, διαχείριση κρίσεων και τεχνολογίες που μπορούν να χρησιμοποιηθούν για την προστασία του τελικού χρήστη, του κυβερνοχώρου και των περιουσιακών στοιχείων του έναν οργανισμό (Alexander, Haseeb & Baranchuk, 2019). Επιπλέον, σύμφωνα με τους Ondiege, Clarke and Mapp (2017), η κυβερνοασφάλεια ορίζεται από την Υπηρεσία Τροφίμων και Φαρμάκων (*FDA*) ως ένα σύνολο πρακτικών για την αποτροπή μη εξουσιοδοτημένης πρόσβασης, τροποποίησης, κακής χρήσης ή άρνησης χρήσης πληροφοριών που αποθηκεύονται, προσπελάζονται ή μεταφέρονται από συσκευή γιατρού σε μη εξουσιοδοτημένο εξωτερικό παραλήπτη.

Σύμφωνα με τους ίδιους συγγραφείς, μια κυβερνοεπίθεση μπορεί να έχει ως στόχο όχι μόνο δεδομένα αλλά και ζωτικές συσκευές που σώζουν ζωές. Ως εκ τούτου, είναι σημαντικό ο τομέας της υγειονομικής περίθαλψης να αντιληφθεί ότι η ευθύνη για την ασφάλεια στον κυβερνοχώρο δεν ανήκει μόνο στους κατασκευαστές ιατρικών συσκευών. Το 2016, οι επιτιθέμενοι στον κυβερνοχώρο ζήτησαν περίπου 3,6 εκατομμύρια δολάρια σε *Bitcoins* για να ξεκλειδώσουν τους υπολογιστές του νοσοκομείου στο Ιατρικό Κέντρο Presbyterian στο Λος Άντζελες της Καλιφόρνια (Abraham, Chatterjee & Sims, 2019).

Το σενάριο πανδημίας *Covid-19* κατέστησε εμφανή την ανάγκη πρόσβασης σε ακριβή δεδομένα υγείας σε πραγματικό χρόνο. Η δράση των επαγγελματιών υγείας εξαρτάται από αξιόπιστα δεδομένα που χρησιμοποιούνται για τη χαρτογράφηση ασθενειών. Ο κλάδος του ιατρικού και νοσοκομειακού εφοδιασμού χρειάζεται δεδομένα για να σχεδιάσει τον κατακερματισμό της αγοράς. Οι κυβερνητικές υπηρεσίες πρέπει να περιορίσουν τις εστίες μόλυνσης βάσει επιδημιολογικών δεδομένων. Τα ινστιτούτα βασίζονται στις έρευνες, τις στατιστικές υγείας και στα αρχεία τους για να καθορίσουν στρατηγικές στην κλινική ανάλυση των δοκιμών εμβολίων (Okereafor & Marcelo, 2020). Ως εκ τούτου, είναι απαραίτητες μελέτες για να αυξηθεί η ευαισθητοποίηση σχετικά με τη σημασία της κυβερνοασφάλειας, να αλλάξουν οι βασικές έννοιες και να δημιουργηθεί αποτελεσματικά μια οργανωτική κουλτούρα προσανατολισμένη στην ασφάλεια στον κυβερνοχώρο. (Natsiavas et al., 2018).

Ο τομέας της υγειονομικής περίθαλψης είναι ένας εξαιρετικά ελκυστικός και ευάλωτος στόχος για τους εγκληματίες στον κυβερνοχώρο λόγω του οικονομικού μεγέθους και της αναποτελεσματικής κυβερνοασφάλειας (Blanke & McGrady, 2016). Έτσι, οι πληροφορίες είναι το νέο καύσιμο της Βιομηχανίας 4.0, με τεράστιο όγκο πληροφοριών που πρέπει να προστατευθούν (Baaziz & Quoniam, 2013). Οι Burns et al. (2011) κατανοούν ότι ο τομέας της υγειονομικής περίθαλψης είναι δομημένος από το σύστημα υγείας, το οποίο περιλαμβάνει την κυβέρνηση, τις εταιρείες, άτομα και ομίλους εταιρειών, ενδιάμεσους χρηματοπιστωτικούς οργανισμούς, που περιλαμβάνουν ασφαλιστικές εταιρείες υγείας, οργανισμούς συντήρησης υγείας (*HMOs*) και διαχείριση φαρμακευτικών παροχών. Επίσης πάροχοι προϊόντων και υπηρεσιών υγείας, που περιλαμβάνουν νοσοκομεία, γιατρούς, ολοκληρωμένα δίκτυα υπηρεσιών υγείας και φαρμακεία, αγοραστές, οι οποίοι περιλαμβάνουν διανομείς προϊόντων υγείας και οργανισμούς αγορών καθώς και κατασκευαστές, οι οποίοι περιλαμβάνουν τη φαρμακοβιομηχανία, κατασκευαστές υγειονομικού εξοπλισμού και κατασκευαστές ιατρικών και χειρουργικών προϊόντων είναι μερικοί ακόμη από τους τομείς της υγειονομικής περίθαλψης.

Σε περιόδους καινοτομίας, οι Burns et al., (2011) θεωρούν πολύτιμο να ενσωματώσουν επίσης τους παρόχους τεχνολογίας πληροφοριών σε σχέση με τους κατασκευαστές. Οι Burns et al. (2011) δικαιολογούν αυτήν την προσθήκη λαμβάνοντας υπόψη το μέγεθος της αγοράς τεχνολογίας πληροφοριών στον τομέα της υγειονομικής περίθαλψης, τη συνάφειά της με τους οργανισμούς υγειονομικής περίθαλψης και τους ασθενείς, καθώς και το γεγονός ότι αυτοί οι

πάροχοι είναι μία από τις πηγές καινοτομίας στην αλυσίδα αξιών. Προηγουμένως, η βιομηχανία υγειονομικής περίθαλψης πιστεύεται ότι ήταν απρόσβλητη από επιθέσεις στον κυβερνοχώρο και τα μέτρα προστασίας δεν είχαν ληφθεί υπόψη με τα χρόνια. Τις τελευταίες δεκαετίες, η βιομηχανία έχει συγκεντρώσει τις προσπάθειές της στην ιατρική περίθαλψη, διαλέγοντας τις συσκευές της για προστασία από κυβερνοεπιθέσεις.

Είναι τεράστια πρόκληση για κάθε οργάνωση στον 21ο αιώνα η προστασία από το έγκλημα στον κυβερνοχώρο. Όπως κάθε καινοτομία είναι μια μεγάλη πρόκληση για τους οργανισμούς. Αν και δεν υπάρχει αλάνθαστη λύση, η βιβλιογραφία δείχνει ότι η αποτελεσματική διαχείριση κινδύνου είναι η καταλληλότερη λύση για την καταπολέμηση της αυξανόμενης δράσης των εγκληματιών στον κυβερνοχώρο (Coronado & Wong, 2014). Σύμφωνα με τον Dionne (2013), το ISO/IEC 27000 (2013) - Τεχνολογία πληροφοριών, δείχνει τεχνικές ασφάλειας και συστήματα διαχείρισης ασφάλειας πληροφοριών. Επιπλέον, στο *ISO 31000* (2018), η διαχείριση κινδύνου ορίζεται ως αυτό. Αυτή η μελέτη προτείνει να απαντήσει στα ακόλουθα ερευνητικά ερωτήματα: ποιες είναι οι ελάχιστες απαιτήσεις και ποιες είναι οι καλύτερες πρακτικές διαχείρισης κινδύνου που εφαρμόζονται για ένα σύστημα κυβερνοασφάλειας στην υγειονομική περίθαλψη;

4.2 Κυβερνοασφάλεια στην υγειονομική περίθαλψη και διαχείριση κινδύνων

Πολλές σύγχρονες ιατρικές συσκευές περιέχουν ενσωματωμένα συστήματα υπολογιστών, τα οποία αλληλοσυνδέονται όλο και περισσότερο μέσω δικτύων. Αυτό περιλαμβάνει συσκευές όπως (αλλά όχι περιοριστικά): μετρητές πίεσης και καρδιακών παλμών, γλυκόμετρα, βηματοδότες και αντλίες ινσουλίνης (Alexander et al., 2019). Υπάρχουν πολλά οφέλη από τη χρήση αυτών των συσκευών, όπως η ταχεία μετάδοση κλινικών πληροφοριών από τους ασθενείς στους γιατρούς και η διαχείριση της θεραπείας σε πραγματικό χρόνο που μπορεί να βελτιώσει τη φροντίδα των ασθενών. Ωστόσο, η ύπαρξη αυτής της συνδεσιμότητας μπορεί να θέσει τους ασθενείς σε κίνδυνο για ευπάθειες στον κυβερνοχώρο που σχετίζονται με την ασφάλεια των πληροφοριών και τη λειτουργία της συσκευής (Alexander et al., 2019). Οι ιατρικές συσκευές που είναι συνδεδεμένες στο δίκτυο χρησιμοποιώντας συσκευές Internet of Things (IoT) ενδέχεται να είναι ευάλωτες σε παραβιάσεις κυβερνοασφάλειας.

Η κυβερνοασφάλεια αντανακλά τους κινδύνους που αντιμετωπίζονται καθώς η διασυνδεσιμότητα μεγαλώνει και διαφοροποιείται και με τους πρόσθετους πόρους και την

ταχύτητα αποθήκευσης, επεξεργασίας και μεταφοράς πληροφοριών να αυξάνεται εκθετικά με κάθε νέα γενιά.

Οι τρέχουσες στρατηγικές για την αντιμετώπιση των κινδύνων στον κυβερνοχώρο επικεντρώνονται κυρίως στην αποκατάσταση ή μέσω ενεργειών από ιδιοκτήτες και καταναλωτές δεδομένων με τη μορφή κρυπτογράφησης δεδομένων, κανονισμών, οργανωτικής υποστήριξης, μέτρων ελέγχου πρόσβασης, εκστρατειών ευαισθητοποίησης, εκτίμησης κινδύνου, αποκλεισμού και παρόμοιων πρακτικών (Berger & Schneck, 2019). Για τους Abraham et al. (2019) ο τομέας της υγειονομικής περίθαλψης, στον οποίο οι κυβερνοεπιθέσεις στον τομέα έχουν αυξηθεί κατά 125% τα τελευταία πέντε χρόνια, αποτελεί ευάλωτο στόχο.

Για παράδειγμα, στην πόλη του Λος Άντζελες των Ηνωμένων Πολιτειών, ένας οργανισμός υγειονομικής περίθαλψης πλήρωσε 17.000 $ σε Bitcoin σε έναν χάκερ που ανέλαβε τον έλεγχο των συστημάτων τους. Επιπλέον, στις Ηνωμένες Πολιτείες, πολλοί ασθενείς λαμβάνουν λογαριασμούς για ιατρικές διαδικασίες που δεν έχουν χρησιμοποιήσει ή για αγορές που δεν έχουν υποβληθεί από τα θύματα. Σύμφωνα με τους συγγραφείς, οι παραβιάσεις της ασφάλειας πληροφοριών στον τομέα της υγειονομικής περίθαλψης έχουν το υψηλότερο κόστος για τις εταιρείες. Στις Ηνωμένες Πολιτείες, ξοδεύονται $ 400 για κάθε χαμένο ή κλεμμένο αρχείο, σε σύγκριση με το κόστος που αντιμετωπίζουν άλλοι τομείς της οικονομίας, όπως ο χρηματοπιστωτικός τομέας, $ 215 ή λιανικά $ 65. Από τις στατιστικές, είναι σαφές ότι ο τομέας της υγειονομικής περίθαλψης έχει γίνει σημαντικός στόχος για τους εγκληματίες στον κυβερνοχώρο. Οι Ondiege et al. (2017) υποδεικνύουν στη μελέτη τους ότι το 90% των οργανώσεων έχουν πρόσφατα στοχοποιηθεί από κυβερνοεγκληματίες.

Για τους εγκληματίες στον κυβερνοχώρο, ο τομέας της υγειονομικής περίθαλψης είναι ένας ελκυστικός στόχος για δύο λόγους: είναι μια πηγή πολύτιμων πληροφοριών και ένας εξαιρετικά ευάλωτος στόχος (Martin, Martin, Hankin, Darzi & Kinross, 2017).

Επομένως, είναι απαραίτητο να προωθηθεί η έρευνα για να διευρυνθεί η αντίληψη σε αυτόν τον τομέα σχετικά με τις μεθόδους διαχείρισης κινδύνου στον κυβερνοχώρο μέσω της συμπερίληψης θεμελιωδών αντιλήψεων, αλλάζοντας τις εταιρικές συνήθειες που αποσκοπούν στην κυβερνοασφάλεια σε όλα τα οργανωτικά επίπεδα των ιδρυμάτων υγειονομικής περίθαλψης (Natsiavas et al., 2018).

Παρόλο που οι κίνδυνοι προέρχονται από την αβεβαιότητα, δεν είναι ακριβώς απρόβλεπτοι, καθώς είναι δυνατόν να προσδιοριστεί η συχνότητα, ο αντίκτυπος και η πιθανότητα, μεταξύ άλλων παραγόντων και, κατά συνέπεια, να προετοιμαστούν για αυτούς σε περίπτωση εμφάνισής τους. Ο μετριασμός, η μεταφορά ή απλώς εξάλειψη βασίζονται σε σχέδια διαχείρισης κινδύνου (PMI, 2017). Επομένως, καθώς οι οργανισμοί εξαρτώνται περισσότερο από διαδικασίες στον κυβερνοχώρο, πρέπει επίσης να διαχειρίζονται τους κινδύνους στους οποίους εκτίθενται μέσα σε αυτή τη νέα πραγματικότητα (World Economic Forum, 2017).

Σύμφωνα με το Project Management Institute (PMI) (2017), οι κίνδυνοι είναι αβεβαιότητες, γεγονότα, συνθήκες ή μελλοντικές συνθήκες που ενδέχεται να έχουν αρνητικό αντίκτυπο στον οργανισμό με ή χωρίς βλάβη φήμης στον οργανισμό. Όσο περισσότερο κάποιος γνωρίζει εκ των προτέρων για τους κινδύνους και τις επιπτώσεις τους, τόσο πιο προετοιμασμένος είναι να τους αντιμετωπίσει εάν συμβούν. Συνεπώς, ο κίνδυνος ορίζεται ως ο συνδυασμός της πιθανότητας εμφάνισης ενός δεδομένου γεγονότος και των αρνητικών επιπτώσεων που προκύπτουν από αυτό, εάν συμβεί ποτέ. Ο κίνδυνος είναι αναπόφευκτος σε κάθε οργανισμό. Ωστόσο, τα μέλη είναι υπεύθυνα για τη διασφάλιση του μετριασμού των κινδύνων στο ελάχιστο δυνατό επίπεδο προκειμένου να επιτευχθούν οι οργανωτικοί στόχοι (Abraham et al., 2019; Coronado & Wong, 2014; Kure et al., 2018).

Το σχέδιο διαχείρισης κινδύνου στον κυβερνοχώρο, στον κλάδο της υγειονομικής περίθαλψης, απαιτεί τη λήψη αποφάσεων καθημερινά. Επί του παρόντος, οι οργανισμοί ανταγωνίζονται για νέες τεχνολογίες, καθώς και για μεγαλύτερη χρήση της ανάλυσης δεδομένων και της επεξεργασίας καινοτομιών και ανάπτυξης σε διασυνδεδεμένα περιβάλλοντα. Επομένως, καθώς οι οργανισμοί εξαρτώνται περισσότερο από διαδικασίες στον κυβερνοχώρο, πρέπει επίσης να διαχειρίζονται τους κινδύνους στους οποίους εκτίθενται μέσα σε αυτή τη νέα πραγματικότητα (World Economic Forum, 2017).

- Έτσι, είναι συχνά απαραίτητο να υποβληθεί αίτηση για την αντιστάθμιση των ελέγχων, χωρίς να διαταραχθεί η κλινική ροή του εξοπλισμού, προκειμένου να καταστεί δυνατή η διαχείριση της κυβερνοασφάλειας στον τομέα της υγειονομικής περίθαλψης και των ιατρικών συσκευών. Οι επαγγελματίες σε αυτόν τον τομέα θα πρέπει να βρουν εναλλακτικές λύσεις όταν δεν υποστηρίζονται χειριστήρια ή / και όταν εμποδίζουν την απαραίτητη απόδοση του εξοπλισμού. Επομένως, η διαχείριση των υπολειπόμενων και ανεξέλεγκτων κινδύνων πρέπει να

είναι μια συνεχής διαδικασία καθ 'όλη τη διάρκεια του κύκλου ζωής των ιατρικών συσκευών (Busdicker & Upendra, 2017).

- Ομοίως, η διαχείριση των κινδύνων για την ασφάλεια στον κυβερνοχώρο πρέπει να θεωρηθεί ως μια πράξη εξισορρόπησης μεταξύ ασφάλειας και ανθεκτικότητας. Κανένας οργανισμός δεν μπορεί να είναι απόλυτα ασφαλής, αλλά μπορεί να αναπτύξει την ικανότητα ελαχιστοποίησης των απειλών και γρήγορης ανάκαμψης από επιθέσεις (Abraham et al., 2019). Είναι σημαντικό να υπάρχει μια επισκόπηση πολλών σημαντικών ζητημάτων πραγματικών απειλών στον κυβερνοχώρο και εκτίμησης κινδύνου για εποπτικό έλεγχο και απόκτηση δεδομένων (*SCADA*) και συστήματα κατανεμημένου ελέγχου (*DCS*) (Abraham et al., 2019; Kure et al., 2018).

- Επιπλέον, η σύγχρονη μέθοδος διαχείρισης κινδύνου περιλαμβάνει υπάρχουσες κανονιστικές απαιτήσεις και τις μετατρέπει σε στόχους ελέγχου οργανισμού. Οι δομές και τα πρότυπα που περιλαμβάνονται σε αυτήν τη μέθοδο διαχείρισης κινδύνου είναι: *National Institute of Standards and Technology* (*NIST*), *ISO 31000* (2018), *ISO/IEC 27001* (2013), *Health Insurance Portability and Accountability Act* (*HIPAA*), *Project Management Body of Knowledge* (*PMBOK*), και πλαίσιο διαχείρισης κινδύνων με αντικειμενικό προσανατολισμό, τα πρότυπα των οποίων παρέχουν κατευθυντήριες γραμμές για δραστηριότητες διαχείρισης κινδύνου (Ondiege et al. 2017).

- Επιπλέον, τα σχέδια διαχείρισης κινδύνου πρέπει να συνδέουν διαφορετικά σενάρια επίθεσης και παραβίασης, ώστε να μπορούν οι οργανισμοί υγειονομικής περίθαλψης να αναλύουν αρνητικές συνέπειες κατά τη στιγμή της παραβίασης για την εκτίμηση των κινδύνων στον κυβερνοχώρο. Μεταξύ αυτών των συνεπειών, εντοπίζεται πληρωμή *ransomware*, αποστολή ασθενών/πελατών σε εναλλακτικές τοποθεσίες για υπηρεσίες βοήθειας, κατεστραμμένη φήμη, κυβερνητικές κυρώσεις, κόστος ανάκτησης δεδομένων και τέλος αντικατάσταση εξοπλισμού και εφαρμογή πρόσθετων μέτρων ασφαλείας (Abraham et al., 2019). Αυτή η εκτίμηση πρέπει να βασίζεται στο κόστος επένδυσης σε διάφορα προληπτικά και ελαφρυντικά μέτρα ανάκτησης (Abraham et al., 2019). Έτσι, το σχέδιο διαχείρισης κινδύνου θα πρέπει να λειτουργεί ως οδηγός και κύρια αναφορά για τους διευθυντές και τους εργαζόμενους. Θα πρέπει να περιγράφει τον τρόπο παρακολούθησης, ελέγχου και εκτέλεσης των κινδύνων ασφαλείας που αντιμετωπίζει ο οργανισμός. Οι κίνδυνοι στον οργανισμό θα πρέπει να

αξιολογούνται με τον ίδιο τρόπο όπως οι οικονομικοί, κλινικοί ή λειτουργικοί κίνδυνοι (Martin et al., 2017).

- Επιπλέον, θα πρέπει να περιλαμβάνει περιγραφές επίθεσης, αναγνώριση ευπάθειας, σύσταση συγκεκριμένων ελέγχων ευπάθειας και εφαρμογή σχεδίου ελέγχου (Blanke & McGrady, 2016). Έτσι, επειδή οι απειλές για την ασφάλεια έχουν αυξηθεί εκθετικά τα τελευταία χρόνια, οι οργανισμοί πρέπει να εφαρμόσουν ολοκληρωμένα συστήματα διαχείρισης κινδύνων στον κυβερνοχώρο για να εντοπίσουν μοναδικές απειλές ή τάσεις. Μια λύση για ένα τέτοιο ζήτημα έγκειται στην πολυεπίπεδη προσέγγιση που χρησιμοποιείται για την εκτίμηση των κινδύνων που βασίζονται στην ασφάλεια προκειμένου να προληφθούν, να μετριαστούν και να ανεχθούν επιθέσεις σε ιατρικές συσκευές και κυβερνοχώρες (Abraham et al., 2019; Kure et al., 2018).

Συνεπώς, η διαχείριση κινδύνου ορίζεται ως μια διαδικασία (ένα ταξίδι) δομημένη σε στάδια. Αυτή η στρατηγική βοηθά στον εντοπισμό του κινδύνου που πρέπει να ελεγχθεί ακολουθώντας διαφορετικές στρατηγικές ελέγχου (Abraham et al., 2019; Blanke & McGrady, 2016; Coronado & Wong, 2014; Kure et al., 2018; PMI, 2017). Οι παραβιάσεις δεδομένων που προκύπτουν από αυτές τις επιθέσεις αποτελούν σημαντική απειλή για τη βιωσιμότητα των οργανισμών υγειονομικής περίθαλψης. Οι ζημίες που προκύπτουν από τέτοιες παραβιάσεις κυμαίνονται από οικονομικές απώλειες έως και παραβίαση της ασφάλειας των ασθενών. Η ασφάλιση στον κυβερνοχώρο έχει γίνει ένα ουσιαστικό εργαλείο για τον περιορισμό των χρηματοοικονομικών υποχρεώσεων που προκύπτουν από παραβιάσεις σε πολλούς οργανισμούς (Kabir et al., 2020; Jalali, Russell, Razak & Gordon, 2019).

Πολλοί επαγγελματίες χρησιμοποιούν την πλατφόρμα εκτίμησης κινδύνου ιατρικής συσκευής για να πραγματοποιήσουν εκτίμηση κινδύνου σε συνδεδεμένες ιατρικές συσκευές (Busdicker & Upendra, 2017). Έτσι, όλοι οι φορείς του οργανισμού πρέπει να βοηθήσουν στον εντοπισμό των κινδύνων στον οργανισμό. Όλοι οι κίνδυνοι πρέπει να καταγράφονται σε ένα μόνο έγγραφο που ονομάζεται πίνακας διαχείρισης κινδύνου (Abraham et al., 2019; Coronado & Wong, 2014; Kure et al., 2018). Σύμφωνα με το *HIPAA*, θα πρέπει να δημιουργηθεί μια λίστα ελέγχου με τις τρέχουσες πρακτικές ασφάλειας και να χρησιμοποιηθεί για τον εντοπισμό κενών σε αυτές τις πρακτικές. Έτσι, ο οργανισμός πρέπει να συγκρίνει πολιτικές που σχετίζονται με

την κυβερνοασφάλεια για να διασφαλίσει τη συμμόρφωση με τους ισχύοντες κανονισμούς και τις βέλτιστες πρακτικές (Blanke & McGrady, 2016).

Σύμφωνα με τους Natsiavas et al. (2018) μια απειλή μπορεί να οριστεί ως ένας λανθάνων κίνδυνος, με άλλα λόγια, οι απειλές είναι καταστάσεις ή ανεξέλεγκτες ενέργειες που μπορεί να σχετίζονται με κακόβουλα άτομα ή παράγοντες εκτός ελέγχου, όπως κακές καιρικές συνθήκες ή φυσικές αποτυχίες, οι οποίες μπορούν να αναλάβουν τον έλεγχο, να βλάψουν ή να καταστρέψουν περιουσιακά στοιχεία εντός οργανισμών. Οι απειλές μπορούν να αναφέρονται σε τεχνικές, λειτουργικές, νομικές, προσωπικές ή πολιτικές πτυχές, αν και δεν περιορίζονται σε αυτές.

Οι τεχνικές απειλές στα συστήματα μπορούν να ταξινομηθούν ως:

- παραχάραξη: πρόσβαση σε ιδιωτικά συστήματα με χρήση ψευδών στοιχείων ταυτοποίησης προκειμένου να τα βλάψουν ή να αποκτήσουν πλεονεκτήματα.
- παραποίηση: αντιγραφή, τροποποίηση αναπαραγωγής ή παραποίηση πληροφοριών, εγγράφων, προϊόντων, εξοπλισμού ή υπηρεσιών χωρίς άδεια
- άρνηση: άρνηση συγκεκριμένων εντολών ή λειτουργιών στα συστήματα, μέσω νόμιμων χρηστών ή μη
- αποκάλυψη πληροφοριών: έκθεση εμπιστευτικών δεδομένων, πληροφοριών ή γνώσεων σχετικά με οργανισμούς
- DoS: Αγγλικό αρκτικόλεξο για την άρνηση υπηρεσίας, που αναφέρεται στη μη διαθεσιμότητα πόρων μιας δεδομένης εφαρμογής, συστήματος ή εξοπλισμού για χρήση. Αυτή η πρακτική καθιστά τις συσκευές άκυρες λόγω υπερφόρτωσης. Συχνά γίνεται με δύο διαφορετικούς τρόπους, συγκεκριμένα, κάνοντας το σύστημα να υπερφορτώνει και να καταναλώνει όλους τους πόρους του για να το σταματήσει να λειτουργεί σωστά ή απενεργοποιώντας την επικοινωνία μεταξύ των συστημάτων για να τα απομονώσει.
- Αύξηση προνομίου: χορήγηση προνομίων σε χρήστες ή επιτιθέμενους εκτός των αδειών που είχαν αρχικά εγκριθεί από το σύστημα, επιτρέποντας στους χρήστες με περιορισμένη πρόσβαση να έχουν απεριόριστη πρόσβαση στο σύστημα ως διαχειριστές.

Η ανάλυση κινδύνου παρέχει ένα πλαίσιο για τους μάνατζερ να γνωρίζουν και να αξιολογούν τα τρωτά σημεία του οργανισμού, καθώς και να αναπτύσσουν σχέδια ασφαλείας πριν πραγματοποιηθεί το γεγονός (Blanke & McGrady, 2016).

Ομοίως, η ποιοτική ανάλυση αναδεικνύει τις υποκειμενικές πτυχές του κάθε μέλους (πώς κάθε μέλος κατανοεί και χαρακτηρίζει τον κίνδυνο). Αυτή η ανάλυση βασίζεται στην εμπειρία των μελών και χρησιμοποιείται για τη διερεύνηση της αντίληψης ή της κατανόησης των μελών σχετικά με τη φύση ενός δεδομένου κινδύνου, με βάση την ερμηνεία τους (Blanke & McGrady, 2016; PMI, 2017). Από την άλλη πλευρά, η ποσοτική ανάλυση αποδίδει αριθμητικές πιθανότητες σε κάθε προσδιορισμένο κίνδυνο καθώς και εξετάζει τις δυνατότητες, τον αντίκτυπο και τις συνέπειές του. Ο κίνδυνος μπορεί να ομαδοποιηθεί σε διαφορετικές κατηγορίες όποτε είναι απαραίτητο. Η ποσοτική ανάλυση επιτρέπει την κατανόηση των κινδύνων στον κυβερνοχώρο βάσει μετρήσιμων και ποσοτικοποιήσιμων δεδομένων, δηλαδή βάσει αριθμών (Blanke & McGrady, 2016; PMI, 2017).

Είναι σημαντικό να τονιστεί ότι η σύνδεση μεταξύ της ασφάλειας των ενεργειακών εφαρμογών και της υποστήριξης της ασφάλειας των υποδομών στις διαδικασίες εκτίμησης κινδύνου παρέχει μια μεθοδολογία ικανή να αξιολογήσει τις πιθανές επιπτώσεις του κινδύνου (Abraham et al., 2019; Kure et al., 2018). Έτσι, τα προτεινόμενα αντίμετρα βασίστηκαν στη μέθοδο του πίνακα κινδύνου με την ταξινόμηση κινδύνου. Οι τιμές που αποδίδονται στους κινδύνους εισήχθησαν στο σύστημα διαχείρισης της ασφάλειας πληροφοριών (*ISMS*) και υποβλήθηκαν σε ποσοτική ανάλυση, η οποία επιτρέπει την λεπτομερή αξιολόγηση των κινδύνων. Η ποσοτική εκτίμηση κινδύνου επέτρεψε την παρατήρηση του κατά πόσον τα προαναφερθέντα αντίμετρα θα μπορούσαν να μειώσουν τους κινδύνους σε κάποιο βαθμό (Abraham et al., 2019; Kure et al., 2018).

Η ανάλυση της σχέσης κόστους-οφέλους που εφαρμόζεται στα προτεινόμενα αντίμετρα είναι μια σημαντική εκτίμηση που πρέπει να πραγματοποιηθεί. Μια αποτελεσματική στρατηγική που επικεντρώνεται στην εκτίμηση του κινδύνου κυβερνοασφάλειας των συστημάτων εποπτείας και απόκτησης δεδομένων (*SCADA*) πρέπει να έχει τουλάχιστον σαφείς στόχους, να κατανοεί τις προτεινόμενες εφαρμογές, να διαιρεί τα στάδια διαχείρισης κινδύνου σε διαχειρίσιμα μέρη, να κατανοεί τις έννοιες διαχείρισης κινδύνων και να μετρά τον αντίκτυπο των κινδύνων και πιθανολογικές πηγές δεδομένων (Abraham et al., 2019; Kure et al., 2018). Έτσι, με βάση τη σχετική βιβλιογραφία, παρά τον σημαντικό αριθμό μεθόδων εκτίμησης κινδύνου που αναπτύχθηκαν για συστήματα όπως το *SCADA*, είναι απαραίτητο να αναπτυχθεί μια

ολοκληρωμένη μέθοδος που θα περιλαμβάνει όλα τα στάδια της διαδικασίας διαχείρισης κινδύνου.

Μια καλή στρατηγική που βρέθηκε στη βιβλιογραφία πρότεινε την αξιολόγηση της ευπάθειας των οργανισμών, σε παραβιάσεις της ασφάλειας πληροφοριών μέσω δεικτών επιπτώσεων απειλών και ευπάθειας στον κυβερνοχώρο βάσει του σχεδιασμού δέντρων ευπάθειας (Kure et al., 2018). Η αξία αυτού του εργαλείου είναι πώς βοηθά τους διαχειριστές να καθορίσουν το τρέχον επίπεδο ασφάλειας στον οργανισμό και να επιλέξουν τους καλύτερους μηχανισμούς ασφαλείας που θα χρησιμοποιηθούν. Αρκετές προσομοιώσεις επιθέσεων - επιπτώσεων - όπως η διαθεσιμότητα του συστήματος και οι επιθέσεις ακεραιότητας - πρέπει να εκτελεστούν στο σύστημα. Αρκετά άρθρα που διατίθενται στη βιβλιογραφία περιορίζουν τις προσπάθειές τους στον εντοπισμό επιθέσεων σε κυβερνο-φυσικά συστήματα (Abraham et al., 2019).

Ωστόσο, για τη συνολική προσέγγιση του κινδύνου κυβερνοασφάλειας, τα άρθρα αξιολόγησης επιτρέπουν το συμπέρασμα ότι είναι σημαντικό να υιοθετηθεί μια ολοκληρωμένη μέθοδος διαχείρισης κινδύνου ικανή να καλύψει όλα τα στάδια της διαδικασίας, από τον εντοπισμό κινδύνου έως την πιθανή απάντηση σε αυτόν τον κίνδυνο. Οι περισσότερες προσεγγίσεις που βρίσκονται στη βιβλιογραφία συχνά δίνουν έμφαση στην εκτίμηση και τα τρωτά σημεία στον εντοπισμό απειλών. Ωστόσο, υπάρχει έλλειψη έμφασης στις διαδικασίες που υιοθετούνται μετά τον προσδιορισμό αυτών των κινδύνων (Kure et al., 2018).

Επομένως, είναι απαραίτητο να αναλυθεί η πιθανή συχνότητα κινδύνων στον κυβερνοχώρο, έτσι ώστε να πραγματοποιηθεί η ανάλυση ή η αριθμητική μέτρηση της πιθανότητας αντιμετώπισης ενός ορισμένου προσδιορισμένου κινδύνου. Αυτή η ανάλυση δίνει τη δυνατότητα στον κλάδο να προσδιορίσει ποιοι κίνδυνοι είναι πιο πιθανό να προκύψουν στη διαχείριση του κυβερνοχώρου σε βάρος άλλων κινδύνων. Με βάση αυτήν την ταξινόμηση, είναι δυνατόν να προσδιοριστούν οι κίνδυνοι που πρέπει να αντιμετωπιστούν με βάση την πιθανότητά τους να συμβούν (Blanke & McGrady, 2016; PMI, 2017). Έτσι, πρέπει κανείς να αναλύσει τον αντίκτυπο, τις συνέπειες και τις επιπτώσεις που μπορούν να έχουν οι καταλογισμένοι κίνδυνοι στον οργανισμό. Θα πρέπει επίσης να τεθούν ερωτήσεις, όπως: εάν ο κίνδυνος αυτός πραγματοποιηθεί, τι αντίκτυπο θα έχει στον οργανισμό;

Στη συνέχεια, θα πρέπει να ταξινομηθούν οι άμεσες και έμμεσες επιπτώσεις ενός τέτοιου κινδύνου (Blanke & McGrady, 2016). Σύμφωνα με τους Abraham et al. (2019) και Kure et al. (2018), είναι απαραίτητο να μετρηθούν οι πληροφορίες με τη μορφή γραφημάτων δέσμευσης και αυξημένων δέντρων ευπάθειας για να προσδιοριστεί ποσοτικά η πιθανότητα επιθέσεων, ο αντίκτυπος αυτών των επιθέσεων και η μείωση του κινδύνου ως απάντηση σε ένα συγκεκριμένο αντίμετρο, προκειμένου να καταστεί δυνατή η λήψη αποφάσεων κάνοντας τις απαραίτητες διαδικασίες. Η προσέγγιση της Δομής Διαίρεσης Κινδύνων (*RBS*) διαδραματίζει βασικό ρόλο στη διαχείριση των κινδύνων του τομέα. Άλλωστε, οι κίνδυνοι που προσδιορίζονται, αξιολογούνται ποσοτικά και ποιοτικά, αναλύεται η πιθανότητα εμφάνισης και ελέγχονται οι επιπτώσεις τους, ενώ είναι απαραίτητο να ταξινομηθεί ο πίνακας κινδύνου με βάση τη σοβαρότητα του κινδύνου (Coronado & Wong, 2014; Kure et al., 2018).

Έτσι, οι κίνδυνοι μπορούν να ταξινομηθούν με βάση διάφορες παραμέτρους ασφάλειας, συγκεκριμένα, λειτουργικούς, μη τεχνικούς, τεχνικούς και διακυβερνητικούς ή κανονιστικούς. Όλοι οι κίνδυνοι ασφαλείας πρέπει να υποβληθούν σε κατάλληλη αξιολόγηση (Abraham et al., 2019; Kure et al., 2018). Ο προγραμματισμός των απαντήσεων στους κινδύνους είναι η διαδικασία σχεδιασμού ενεργειών για την αντιμετώπιση αυτών των κινδύνων, όποτε αυτοί πραγματοποιούνται. Η διαδικασία προγραμματισμού πρέπει επίσης να επιτρέπει στους οργανισμούς να εντοπίζουν και να επιλέγουν υπαλλήλους για την αντιμετώπιση κινδύνου όποτε συμβεί.

Τέσσερις διαφορετικοί τρόποι αντιμετώπισης των κινδύνων βρέθηκαν στη βιβλιογραφία (Blanke & McGrady, 2016; PMI, 2017):

- πρόληψη, η οποία είναι ένα σύνολο αναμενόμενων μέτρων που αποσκοπούν στην πρόληψη των κυβερνοεπιθέσεων.
- μετριασμός, ο οποίος ελαχιστοποιεί τις συνέπειες των κυβερνοεπιθέσεων
- μεταφορά, η οποία μεταφέρει τις συνέπειες των επιθέσεων σε μισθωμένους τρίτους ·
- αποδοχή, η οποία δέχεται τις συνέπειες των επιθέσεων και συχνά εφαρμόζεται όταν δεν υπάρχει βιώσιμη λύση στο πρόβλημα.

Επιπλέον, διεξάγονται διαδικασίες παρακολούθησης και διαχείρισης κινδύνου ταυτόχρονα. Η διαδικασία παρακολούθησης ελέγχει συνεχώς για κινδύνους, ενώ η διαδικασία

διαχείρισης αξιολογεί συνεχώς τους κινδύνους, αναλύει τους υπολειπόμενους κινδύνους και αξιολογεί την αποτελεσματικότητα των σχεδίων διαχείρισης κινδύνων (Blanke & McGrady, 2016; PMI, 2017). Έτσι, όλες αυτές οι διαδικασίες πρέπει να αλληλεπιδρούν μεταξύ τους, δημιουργώντας μια συνέργεια στη διαχείριση ενάντια στους εγκληματίες στον κυβερνοχώρο. Κάθε διαδικασία μπορεί να περιλαμβάνει την προσπάθεια ενός ή περισσότερων ατόμων, ανάλογα με τις ανάγκες που βρέθηκαν. Αν και οι διαδικασίες παρουσιάζονται ως διακριτά στοιχεία με καθορισμένη αλληλουχία, στην πράξη, θα επικαλύπτονται και θα αλληλεπιδρούν μεταξύ τους (Blanke & McGrady, 2016).

5. Ολοκληρωμένο πληροφοριακό σύστημα νοσοκομείου/υγείας

5.1 Εξέλιξη των πληροφοριακών συστημάτων νοσοκομείου

Η διαχείριση πληροφοριών υγείας ορίζεται ως η συλλογή και ανάλυση δεδομένων υγειονομικής περίθαλψης η οποία παρέχει πληροφορίες για αποφάσεις υγειονομικής περίθαλψης που περιλαμβάνουν τη φροντίδα των ασθενών, θεσμική διαχείριση, πολιτικές υγειονομικής περίθαλψης, σχεδιασμό και έρευνα. Οι πρώτες μορφές ιατρικών αρχείων ήταν αφηγήσεις που γράφτηκαν από αρχαίους Έλληνες για να τεκμηριώσουν επιτυχείς θεραπείες, όπου μοιράζονταν παρατηρήσεις σχετικά με τα συμπτώματα και τα αποτελέσματα και δίδασκαν άλλους που παρείχαν ιατρικές συμβουλές μέσω αυτών των μελετών περιπτώσεων. Καθώς η υγειονομική περίθαλψη προχωρούσε, οι γιατροί συνειδητοποίησαν ότι ο καλύτερος τρόπος για να συνεχίσει να βελτιώνεται η διάγνωση και η θεραπεία ασθενειών ήταν να τεκμηριωθούν προσεκτικά οι παρατηρήσεις και οι ενέργειες θεραπείας των ασθενών, και να κοινοποιηθούν αυτές οι πληροφορίες ως τρόπος διδασκαλίας άλλων επαγγελματιών υγείας.

Ήδη από το 1600, οι γιατροί παρείχαν συμβουλές για τον τρόπο παρουσίασης πληροφοριών σε ιατρικό αρχείο, αλλά μόλις το 1928 το Αμερικανικό Κολλέγιο Χειρουργών (*ACOS*) έκανε βήματα τυποποίησης του αυξανόμενου αριθμού ιατρικών αρχείων με την ίδρυση της Αμερικανικής Ένωσης των Αρχείων Βιβλιοθηκονόμων (*AARL*). Ο όρος "βιβλιοθηκονόμοι" ήταν ο όρος που χρησιμοποιήθηκε επειδή τα πρώιμα ιατρικά αρχεία τεκμηριώθηκαν σε χαρτί (Morris F., Collen M.D., 2017). Η τυποποίηση των ιατρικών αρχείων και η αύξηση της πλήρους τήρησης αρχείων συνεχίστηκε από τη δεκαετία του 1920 έως τη δεκαετία του 1960, αλλά τα

αρχεία βασίστηκαν σε χαρτί. Η ανάπτυξη υπολογιστών παρουσίασε την ευκαιρία να διατηρούνται ηλεκτρονικά αρχεία, αλλά το κόστος αγοράς και η διατήρηση ενός *mainframe*, καθώς και το κόστος που σχετίζεται με την αποθήκευση δεδομένων, σήμαινε ότι μόνο οι μεγαλύτεροι οργανισμοί μπορούσαν να χρησιμοποιήσουν τεχνολογία για τη διαχείριση ιατρικών αρχείων.

Η δεκαετία του 1960 επίσης είδε την εισαγωγή του *Medicare* και του *Medicaid*, το οποίο απαιτούσε από τις νοσοκόμες να συλλέγουν δεδομένα χρησιμοποιώντας έγγραφα φροντίδας για επιστροφή χρημάτων. Ενώ οι υπολογιστές χρησιμοποιούνταν όλο και περισσότερο για τη λογιστική και τις λειτουργίες χρέωσης, η χρήση υπολογιστών για τη συλλογή και διαχείριση ιατρικών αρχείων δεν ήταν συνηθισμένη (Liaison, 2017). Στη δεκαετία του 1970, καθώς οι υπολογιστές έγιναν μικρότεροι, το λογισμικό σχεδιάστηκε για να υποστηρίζει κλινικές λειτουργίες για το φαρμακείο, το κλινικό εργαστήριο, την εγγραφή ασθενών και τη χρέωση τους. Το μειονέκτημα αυτών των συστημάτων πληροφοριών υγείας ήταν οι ειδικές λειτουργίες των τμημάτων τους. Δεν ήταν προσβάσιμα από άλλα τμήματα.

Η πρώτη προσπάθεια για ένα συνολικό, ολοκληρωμένο σύστημα αρχείων υγείας υλοποιήθηκε σε μία γυναικολογική μονάδα στο Πανεπιστημιακό Ιατρικό Κέντρο στο Μπέρλινγκτον του Βερμόντ το 1971. Με βάση το προσανατολισμένο σε προβλήματα ιατρικό αρχείο, το σύστημα ήταν προσανατολισμένο στον ασθενή, και όλα τα γνωστικά αντικείμενα περιλαμβάνονταν στις σημειώσεις φροντίδας στο αρχείο για να παραχθεί μια επισκόπηση της φροντίδας με στόχο να φανεί η σχέση μεταξύ συνθηκών, θεραπειών, κόστους και αποτελεσμάτων. Επειδή οι προσωπικοί υπολογιστές και οι διαδεδομένες εφαρμογές λογισμικού που σχετίζονται με την υγεία είχαν αναπτυχθεί σε δημοτικότητα, το προσωπικό της νοσοκομειακής τεχνολογίας πληροφοριών (ΤΠ) είχε την ευθύνη για την ενσωμάτωση πολλαπλών, διαφορετικών συστημάτων. Καθώς αναπτύχθηκαν λύσεις δικτύου, τα τμήματα πληροφορικής ήταν σε θέση να συνδέσουν οικονομικά και κλινικά συστήματα για περιορισμένες λειτουργίες.

Καθώς ο ανταγωνισμός στην υγειονομική περίθαλψη δημιούργησε μια ενοποίηση μεμονωμένων νοσοκομείων για τη διαμόρφωση των συστημάτων υγείας, η ανάγκη ολοκλήρωσης αυξήθηκε. Η τεχνολογική πρόοδος έδωσε στα νοσοκομεία πρόσβαση σε υπολογιστικά συστήματα που θα μπορούσαν να μοιραστούν πληροφορίες σε διαφορετικά

συστήματα για να προετοιμάσουν τη βάση κοινή χρήση δεδομένων (Joshua R., Gamm L.D., 2017). Η σημασία των ολοκληρωμένων ηλεκτρονικών αρχείων υγείας (*EHR*) για να επιτρέπουν στους παρόχους να συντάσσουν καλύτερες αποφάσεις, αυξήθηκαν και περισσότερα νοσοκομεία και γιατροί τα εφάρμοσαν για να μειώσουν το συχνότητα ιατρικού λάθους βελτιώνοντας την ακρίβεια και τη σαφήνεια των ιατρικών αρχείων. Αυξημένη εστίαση στη φροντίδα βάσει αξίας σε αντίθεση με τη φροντίδα βάσει αμοιβών και μια προσπάθεια βελτίωσης των αποτελεσμάτων των ασθενών, ωθούν την αυξανόμενη συσσώρευση δεδομένων για την υποστήριξη κλινικών, καθώς και επιχειρησιακές αποφάσεις στην υγειονομική περίθαλψη.

Ακριβώς όπως οι κλινικοί ιατροί στη δεκαετία του 1920 αντιλήφθηκαν τη σημασία των προηγούμενων αρχείων υγείας ως εργαλεία εκμάθησης που θα βελτιώσουν τα αποτελέσματα, οι επαγγελματίες υγείας αξιοποιούν τα δεδομένα ενίσχυση της φροντίδας σε μεγαλύτερη κλίμακα, χρησιμοποιώντας εργαλεία που αναλύουν δεδομένα υγείας του πληθυσμού.

5.2 Σύγχρονα πληροφοριακά συστήματα υγείας (HIS)

Τα σύγχρονα πληροφοριακά συστήματα υγείας (*HIS*) είναι ολοκληρωμένα και εξειδικευμένα συστήματα πληροφοριών σχεδιασμένα για τη διαχείριση των διοικητικών, οικονομικών και κλινικών πτυχών των νοσοκομείων και τις εγκαταστάσεις υγειονομικής περίθαλψης. Θεωρείται ένα από τα πιο σημαντικά σημεία εστίασης στην παροχή υγειονομικής περίθαλψης εντός νοσοκομείων και διαφορετικών τύπων και εξαρτάται από τα ιατρικά ιδρύματα. Η σημασία αυτών των συστημάτων προκύπτει από τη σημασία του ρόλου που παίζουν στη διατήρηση όλων των τύπων δεδομένων και πληροφοριών των ασθενών, συμπεριλαμβανομένων βασικών δεδομένων σχετικά με τον ασθενή και άλλα ολοκληρωμένα ιατρικά δεδομένα (Balaraman P., Kosalram K., 2013. Ασχολείται επίσης με τη καταγραφή όλων των ιατρικών υπηρεσιών που έχουν παρασχεθεί στον ασθενή όπως π.χ. έρευνες, διαγνώσεις, θεραπείες, εκθέσεις παρακολούθησης και σημαντικές ιατρικές αποφάσεις.

Τα πληροφοριακά συστήματα των νοσοκομείων έχουν τη δυνατότητα να βελτιώσουν την υγεία των ατόμων και των επιδόσεων των παρόχων υγειονομικής περίθαλψης, αποδίδοντας βελτιωμένη ποιότητα, εξοικονόμηση κόστους και μεγαλύτερη συμμετοχή των ασθενών στη δική τους υγειονομική περίθαλψη. Παρά τα στοιχεία για αυτά τα οφέλη, η χρήση του *HIS* και των ηλεκτρονικών αρχείων υγείας από τα νοσοκομεία και τους ιατρούς είναι ακόμα χαμηλή. Η ανταπόκριση των επαγγελματιών υγείας στη χρήση των πληροφοριών των νοσοκομειακών

συστημάτων είναι ένα σημαντικό ερευνητικό θέμα που μπορεί να εξηγήσει την επιτυχία ή την αποτυχία οποιουδήποτε έργου ανάπτυξης και υλοποίησης του *HIS*.

Το σύστημα πληροφοριών του νοσοκομείου (*HIS*) είναι ένα ολοκληρωμένο σύστημα πληροφοριών σχεδιασμένο να διαχειρίζεται όλες τις πτυχές λειτουργίας του νοσοκομείου, όπως ιατρικά, διοικητικά, οικονομικά και νομικά θέματα και την αντίστοιχη επεξεργασία υπηρεσιών. Είναι επίσης γνωστό ως λογισμικό διαχείρισης νοσοκομείων (*HMS*) ή νοσοκομείο σύστημα διαχείρησης (Consultant, 2015).

5.2.1 Βάση δεδομένων στο HIS

Η βάση δεδομένων είναι η καρδιά του συστήματος πληροφοριών του νοσοκομείου. Αποτελείται από ένα κανονικό γραπτό έγγραφο που περιλαμβάνει την ταυτότητα του ασθενούς, το ιστορικό υγείας, ευρήματα φυσικής εξέτασης, εργαστηριακές εκθέσεις, θεραπεία, αναφορές χειρουργικής επέμβασης και νοσοκομειακή πορεία. Όταν ολοκληρωθεί, η εγγραφή θα πρέπει να περιέχει τα δεδομένα για να δικαιολογήσει έρευνες, διάγνωση, θεραπεία και διάρκεια παραμονής, αποτελέσματα φροντίδας και μελλοντική πορεία δράσης. Ένα τέτοιο εργαλείο θα πρέπει (PayamHomayounfar, 2012):

- Να παρέχει ένα μέσο επικοινωνίας μεταξύ των γιατρών, νοσηλευτών και άλλων συναδέλφους επαγγελματίες υγείας
- Να βοηθά στην ιατρική εκπαίδευση και έρευνα για να μπορέσει να παρέχει τη συνέχεια της φροντίδας των ασθενών
- Να παρέχει πληροφορίες για την ποιοτική ανασκόπηση της φροντίδας των ασθενών
- Να προστατεύεται νόμιμα ο γιατρός, ο ασθενής, το νοσοκομείο και οι βοηθοί από τη πληρωμή τρίτων. Η αδυναμία τήρησης ακριβούς, έγκαιρης και πλήρους βάσης δεδομένων χαλάει τη χρησιμότητα του HIS.

5.2.2 Συστατικά του HIS

Τα στοιχεία ενός νοσοκομειακού συστήματος πληροφοριών αποτελούνται από δύο ή περισσότερα από τα ακόλουθα (Scott-clark, 2018):

- Σύστημα κλινικών πληροφοριών (*CIS*).
- Σύστημα χρηματοοικονομικών πληροφοριών (*FIS*).

- Εργαστηριακό Πληροφοριακό Σύστημα (*LIS*).
- Νοσηλευτικά Πληροφοριακά Συστήματα (*NIS*).
- Σύστημα Πληροφοριών Φαρμακείου (*PIS*).
- Σύστημα επικοινωνίας αρχειοθέτησης εικόνων (*PACS*).
- Πληροφοριακό Σύστημα Ακτινολογίας (*RIS*).

Σχήμα 6 : Δομή ΟΠΣΥ (HIS)

Πηγή : %25CE%259F%25CE%25A0%25CE%25A3%25CE%25A5.jpg (400×270) (bp.blogspot.com)

Κλινικό σύστημα πληροφοριών

Το Σύστημα Κλινικών Πληροφοριών (*CIS*) είναι ένα σύστημα που βασίζεται σε υπολογιστή και έχει σχεδιαστεί για τη συλλογή, αποθήκευση, χειρισμό και διάθεση κλινικών πληροφοριών σημαντικών για τη διαδικασία παροχής υγειονομικής περίθαλψης.

Σύστημα χρηματοοικονομικής πληροφόρησης

Τα Χρηματοοικονομικά Συστήματα Πληροφοριών (*FIS*) είναι συστήματα υπολογιστών που διαχειρίζονται την επιχειρηματική πτυχή ενός νοσοκομείου.

Πληροφοριακά συστήματα εργαστηρίου

Ένα εργαστηριακό σύστημα πληροφοριών (*LIS*) είναι ένα πληροφοριακό υπολογιστικό σύστημα που διαχειρίζεται εργαστηριακές πληροφορίες για όλους τους κλάδους του εργαστηρίου όπως η κλινική χημεία, η αιματολογία και η μικροβιολογία.

Πληροφοριακό σύστημα νοσηλευτικής

Τα νοσηλευτικά πληροφοριακά συστήματα (*NIS*) είναι συστήματα υπολογιστών που διαχειρίζονται κλινικά δεδομένα από διάφορα περιβάλλοντα υγειονομικής περίθαλψης και διατίθενται με έγκαιρο και τακτικό τρόπο για να βοηθήσουν τους νοσηλευτές στη βελτίωση της φροντίδας των ασθενών.

Πληροφοριακά συστήματα φαρμακείων

Τα συστήματα πληροφοριών φαρμακείου (*PIS*) είναι πολύπλοκα συστήματα υπολογιστών που έχουν σχεδιαστεί για να καλύψουν τις ανάγκες ενός τμήματος φαρμακείου. Μέσω της χρήσης τέτοιων συστημάτων, οι φαρμακοποιοί μπορούν να επιβλέπουν και να έχουν εισροές για το πώς χρησιμοποιούνται τα φάρμακα σε ένα νοσοκομείο.

Σύστημα επικοινωνίας αρχειοθέτησης εικόνων

Το Σύστημα Επικοινωνίας Αρχειοθέτησης Εικόνων (*PACS*) είναι ένας όρος που περιγράφεται από ένα σύνολο συστημάτων που διευκολύνουν την αρχειοθέτηση, επεξεργασία και προβολή ψηφιακών ακτινολογικών εικόνων και των σχετικών πληροφοριών τους(Scott-clark, 2018).

Ακτινολογικό πληροφοριακό σύστημα

Ένα πληροφοριακό σύστημα ακτινολογίας (*RIS*) είναι ένα δικτυωμένο σύστημα λογισμικού για τη διαχείριση ιατρικών εικόνων και συναφών δεδομένων. Ένα *RIS* είναι ιδιαίτερα χρήσιμο για την παρακολούθηση παραγγελιών απεικόνισης ακτινολογίας και πληροφοριών χρέωσης, και συχνά χρησιμοποιείται σε συνδυασμό με το *PACS* για τη διαχείριση αρχείων εικόνων, τήρησης αρχείων και χρέωσης καθηκόντων των πληροφοριακών συστημάτων του νοσοκομείου (Scott-clark, 2018):

- Αποθήκευση και παρακολούθηση της κατάστασης του ασθενούς:
    - Ακριβή και ηλεκτρονικά αποθηκευμένα ιατρικά αρχεία των παρέχονται σε ασθενείς (π.χ. αλλεργίες στα φάρμακα). Δημιουργούνται συστήματα οπτικής και ακουστικής προειδοποίησης στη περίπτωση μη φυσιολογικών αποτελεσμάτων δοκιμών ή άλλων σημαντικών δεδομένων
- Επεξεργασία και ανάλυση δεδομένων για στατιστικούς σκοπούς και ερευνητικούς σκοπούς

- Διαχείριση και ροή δεδομένων:
  - Υποστήριξη αυτόματων μεταφορών δεδομένων ασθενών μεταξύ τμημάτων και ιδρυμάτων
  - ψηφιακές υπογραφές, προκειμένου να δημιουργηθούν ηλεκτρονικά εσωτερικές παραγγελίες
- Επικοινωνία μέσω Εργαστηριακού Πληροφοριακού Συστήματος
  - Καταχώριση ανθρώπινου δυναμικού και ιδιοτήτων τους
    - Οικονομικές πτυχές: Αποτελεσματική διαχείριση των οικονομικών
    - Χρήση και παρακολούθηση φαρμάκων και διαδικασία παραγγελίας.

Οι αναμενόμενες και πραγματικές δαπάνες θεραπείας παρατίθενται και αναφέρονται με την αυτοματοποιημένη αναπαράσταση των αναγκών του νοσηλευτικού προσωπικού, την ανάλυση κατάστασης της πληρότητας του κρεβατιού και της συνολικής απόδοσης στο πληροφοριακό σύστημα του νοσοκομείου.

Παραδείγματα συστημάτων πληροφοριών υγείας (Nasiripour, A.A. et al., 2014):

- Ηλεκτρονικός ιατρικός φάκελος (*EMR*) και ηλεκτρονικός φάκελος υγείας (*EHR*). Οι ηλεκτρονικοί ιατρικοί φάκελοι αντικαθιστούν τους έντυπους φακέλους ασθενών. Αρκετές εταιρείες παρέχουν τέτοια συστήματα πληροφοριών. Οι ιατρικές πληροφορίες για το καθένα ασθενή πρέπει τώρα να συλλέγονται και να αποθηκεύονται ηλεκτρονικά. Αυτοί οι δίσκοι περιλαμβάνουν πληροφορίες για την υγεία των ασθενών, αποτελέσματα εξετάσεων, επισκέψεις γιατρού και ειδικού, και θεραπείες υγειονομικής περίθαλψης. (NIT Security, 2017)
- Πρακτική Λογισμικό Διαχείρισης. Τέτοια συστήματα πληροφοριών βοηθούν τις εγκαταστάσεις και το προσωπικό υγειονομικής περίθαλψης με τη διαχείριση των καθημερινών λειτουργιών της εγκατάστασης. Αυτό περιλαμβάνει πράγματα όπως προγραμματισμός ασθενών και χρέωση ιατρικών υπηρεσιών.
- Δείκτης κύριου ασθενούς (*MPI*). Το λογισμικό αυτού του πληροφοριακού συστήματος υγείας απευθύνεται στη καταγραφή των ασθενών σε περισσότερες από μία βάσεις δεδομένων. Το *MPI* περιέχει αρχεία για κάθε ασθενή εγγεγραμμένο σε οργανισμό υγειονομικής περίθαλψης. Το *MPI,* όπως το όνομα προτείνει, δημιουργεί ένα ευρετήριο όλων των εγγραφών για αυτόν τον ασθενή. Η πρόθεση του είναι να μειωθούν τα διπλά

αρχεία ασθενών και να αποφύγουν τις ανακριβείς πληροφορίες ασθενών που θα μπορούσαν να οδηγήσουν σε απόρριψη αξιώσεων τους.

- Πύλες ασθενών. Αυτό το σύστημα πληροφοριών επιτρέπει στους ασθενείς να μελετήσουν τα δεδομένα υγείας τους. Αυτοί είναι σε θέση να έχουν πρόσβαση σε πληροφορίες ραντεβού, φάρμακα και τη λήψη των εργαστηριακών τους αποτελεσμάτων μέσω διαδικτύου. Μερικές από αυτές τις πύλες ασθενών διευκολύνουν επίσης τους ασθενείς να έχουν ενεργή επικοινωνία με τους επαγγελματίες της υγειονομικής περίθαλψης, συμπεριλαμβανομένων ιατρών, φαρμακοποιών σχετικά με τα αιτήματα συνταγών ή αναπλήρωσης και προγραμματισμός ραντεβού.
- Απομακρυσμένη παρακολούθηση ασθενούς (*RPM*). Αυτό ονομάζεται επίσης τηλεϊατρική. Το *RPM* παρέχει ιατρικούς αισθητήρες που έχουν τη δυνατότητα να διαβιβάζουν δεδομένα ασθενών σε επαγγελματίες υγείας που μπορεί κάλλιστα να βρίσκονται στα μισά του κόσμου. Το *RPM* μπορεί να παρακολουθεί τα επίπεδα γλυκόζης στο αίμα επίπεδα και την αρτηριακή πίεση. Είναι ιδιαίτερα χρήσιμο για ασθενείς με χρόνιες καταστάσεις όπως ο διαβήτης τύπου 2, η υπέρταση ή η καρδιακή νόσος. Τα δεδομένα που συλλέγονται μπορούν να χρησιμοποιηθούν ως μέρος ενός ερευνητικού έργου ή μιας μελέτης υγείας. Το *RPM* είναι ένα σωτήριο σύστημα για ασθενείς σε απομακρυσμένες περιοχές που δεν έχουν πρόσβαση σε πρόσωπο με πρόσωπο φροντίδα υγείας.
- Υποστήριξη κλινικής απόφασης (*CDS*). Το *CDS* αναλύει δεδομένα από κλινικά και διοικητικά συστήματα. Ο στόχος είναι να βοηθήσει τους παρόχους υγειονομικής περίθαλψης στη λήψη τεκμηριωμένων κλινικών αποφάσεων. Διατίθενται δεδομένα και πληροφορίες για ιατρικά επαγγέλματα που προετοιμάζουν τη διάγνωση ή πρόβλεψη ιατρικών καταστάσεων όπως αλληλεπιδράσεις φαρμάκων και αντιδράσεις. Τα εργαλεία *CDS* φιλτράρουν πληροφορίες για να βοηθήσουν τους επαγγελματίες υγείας να φροντίσουν μεμονωμένους πελάτες.

Πλεονεκτήματα του *HIS* (Khalifa, M., & Alswailem, O., 2015):

- Το Νοσοκομειακό Πληροφοριακό Σύστημα βοηθά στη διατήρηση μιας απόλυτης ασφαλείας βάσης δεδομένων ασθενών και επιχειρηματικών πληροφοριών.

- Βοηθά επιπλέον στη βελτίωση της παροχής υγειονομικής περίθαλψης από τη διάθεση ιατρικού προσωπικού με καλύτερη πρόσβαση στα δεδομένα, ταχύτερα δεδομένα ανάκτησης, υψηλότερη ποιότητα δεδομένων έως και τη μεγαλύτερη ευελιξία στην εμφάνιση δεδομένων.
- Συμβάλλει στη βελτίωση της αποτελεσματικότητας, τόσο στο κόστος όσο και την προοπτική της κλινικής περίθαλψης. Αυτό επιτυγχάνεται με την αποφυγή διπλότυπων εγγραφών, επαναλήψεων, καθυστερήσεων, αν λείπουν δίσκοι και υπάρχουν μπερδέματα.
- Βοηθά στην επιβολή της τάξης και τυποποίηση των αρχείων και διαδικασιών των ασθενών στην κλινική, προσφέροντας ταυτόχρονα αυξανόμενη ακρίβεια και πληρότητα των ιατρικών αρχείων του ασθενούς.
- Βοηθά ως ένα καλό διαχειριστικό εργαλείο για τη παροχή συνολικής, οικονομικά αποδοτικής πρόσβασης στα πλήρη και ακριβέστερα δεδομένα περίθαλψης ασθενών για να προσφέρουν βελτιωμένη απόδοση και βελτιωμένη λειτουργίες.
- Βοηθά στην εκπαίδευση των ασθενών σχετικά με την κατάστασή τους προβάλλοντας ασθένειες και χειρουργικές επεμβάσεις μέσω εικόνων και κινούμενων εικόνων.

5.3. Βασικές έννοιες ασφάλειας σύγχρονων πληροφοριακών συστημάτων υγείας

5.3.1. Ένα σύγχρονο πληροφοριακό σύστημα υγείας κρίνεται ασφαλές, ότι διακατέχεται από τις ακόλουθες αρχές:

- Εμπιστευτικότητα: Είναι η αρχή βάση τις οποίες κρίσιμες και ευαίσθητες πληροφορίες προστατεύονται από μη εξουσιοδοτημένα πρόσωπα. Είναι σημαντικό να διασφαλιστεί η μυστικότητα των μηνυμάτων για την προστασία των δεδομένων και των ανταλλαγών επικοινωνίας (Stankovic, Stanislava, 2009).
- Ακεραιότητα: Είναι η αρχή βάση της οποίας τα δεδομένα υγείας τίθεται σε προστασία και διατηρουνται αναλλοίωτα χωρίς προσθήκες ή αφαιρέσεις από μη εξουσιοδοτημένα πρόσωπα και αντίστοιχα αποτρέπουν την πρόσβαση και χρήση των υπολογιστικών συστημάτων και δικτύων.
- Διαθεσιμότητα: Είναι η αρχή που επιτρέπει την πρόσβαση, των εξουσιοδοτημένων προσώπων, σε υπολογιστές, δίκτυα και δεδομένα.
- Πιστοποίηση και Αυθεντικότητα (authentication): Στην περίπτωση αυτή υπάρχουν δύο βασικοί πυλώνες στους οποίους στηρίζεται η πιστοποίηση: την πιστοποίηση οντοτήτων

(entity authentication ή identification) και την πιστοποίηση δεδομένων (data authentication). Με τον πρώτο πυλώνα εξασφαλίζουμε ότι κάθε οντότητα στο πληροφοριακό-επικοινωνιακό σύστημα είναι αυτή που ισχυρίζεται και δεν υπάρχει κάποια πλαστοπροσωπία. Με το δεύτερο πυλώνα εξασφαλίζουμε την τοποθεσία, τη χρονική στιγμή και το είδος των μηνυμάτων που ανταλλάσσονται σε μία επικοινωνία. Παράδειγμα αυθεντικότητας αποτελεί η κάθε είδους εισβολή και υποκλοπή προσωπικών στοιχείων της πιστωτικής μας κάρτας κατά τη διαδικασία μίας διαδικτυακής αγοράς. Τόσο ο οργανισμός θα πρέπει να κατανοεί ότι η αγορά γίνεται από πιστοποιημένη οντότητα όσο και ο αγοραστής να είναι σε θέση να επιβεβαιώσει ότι η αγορά έγινε από τον ίδιο, σε συγκεκριμένη χρονική στιγμή και σε συγκεκριμένη τοποθεσία.

- Μη αποποίηση (non-repudiation): Κανένας χρήστης, είτε αυτός είναι αποστολέας είτε παραλήπτης, δεν μπορεί να αποποιηθεί τις πράξεις που έκανε στο παρελθόν. Ένας από τους πιο διαδεδομένους αλλά και ταυτόχρονα αποτελεσματικούς τρόπους εφαρμογής της μη αποποίησης είναι η χρήση των ψηφιακών υπογραφών και από τις δύο πλευρές.
- Εγκυρότητα (validity): Αφορά κυρίως εκείνους που χρησιμοποιούν συγκεκριμένες πληροφορίες του συστήματος. Οι εμπλεκόμενες πλευρές ενδιαφέρονται για την πληρότητα και την ακρίβειά αυτών των πληροφοριών, λόγω των αποφάσεων που πρέπει να λάβουν. Θα μπορούσαμε να εκλάβουμε την Εγκυρότητα ώς το άθροισμα της Ακεραιότητας και τη Αυθεντικότητας
- Μοναδικότητα (Uniqueness): Είναι η αδυναμία αντιγραφής και αναπαραγωγής της πληροφορίας χωρίς εξουσιοδότηση.

5.3.2. Υπηρεσίες ασφαλείας & οι στόχοι τους

Σε κάθε σύγχρονο πληροφοριακό σύστημα θα πρέπει να υπάρχουν τμήματα υπηρεσιών ασφαλείας που θα ενεργούν ως ακολούθως:

- Αποτροπή (Prevention): Περιλαμβάνει πληροφορίες ελέγχου προσπελασης και παρεμποδίζει την πρόσβαση στο σύστημα με εξουσιοδοτημένων ατόμων.
- Ανίχνευση (Detection): Μέσω του συστήματος ελέγχου και παρακολούθησης ανιχνεύεται πιθανή επίθεση εισβολέων παρατηρώντας πιθανές ασυνήθιστες δραστηριότητες.

- Αντιμετώπιση και επανάκαμψη (containment and recovery): Η υπηρεσία αυτή στοχεύει στην αντιμετώπιση μιας επίθεσης και την επιδιόρθωση των βλαβών που έχει επιφέρει καθώς στην επανάκαψη του πληροφοριακού συστήματος.
- Διαχείριση ασφάλειας (security administration): Σχεδιάζει, διαχειρίζεται και συντηρεί την πολιτική ασφαλείας του συστήματος.

Όλες οι ανωτέρω υπηρεσίες έχουν ως στόχο την εξασφάλιση της εμπιστευτικότητας των δεδομένων, της ακεραιότητας των δεδομένων, την πιστοποίηση της αυθεντικότητας, το έλεγχο προσπέλασης στο σύστημα ή και στο δίκτυο,την μη αποποίησης ευθύνης κατά την αποστολή όσο και κατά τη παράδοση αρχείου , την επανάκαψη του συστήματος μετά από επίθεση, την διαθεσιμότητα του συστήματος και την αλληλουχία των διενεργειών.

5.4. Παραδείγματα επιθέσεων σε σύγχρονα πληροφοριακά συστήματα υγείας.

Μια λεγόμενη κυβερνο-επίθεση, το 2007, οδήγησε την Εσθονική κυβέρνηση να δημιουργήσει τη στρατηγική της για την ασφάλεια στον κυβερνοχώρο, που έχει ενσωματώσει πολλές πτυχές της ασφάλειας σε νόμος της χώρας. (e-Estonia, 2018) Η Αρχή του Εσθονικού Πληροφοριακού Συστήματος δημοσίευσε μια ετήσια έκθεση στον κυβερνοχώρο, που διαπίστωσε ότι σχεδόν 11000 περιστατικά κυβερνοασφάλειας συνέβησαν το 2018, αν και σε μόνο 122 από όλες αυτές τις περιπτώσεις, δέκα από τις οποίες ήταν στην υγειονομική περίθαλψη, επηρέασαν άμεσα τη λειτουργικότητα των συστημάτων. (e-Estonia, 2018) Για την καταπολέμηση των απειλών ασφάλειας στον κυβερνοχώρο στην υγειονομική περίθαλψη, η Εσθονία εισήγαγε τη *blockchain* τεχνολογία για την ασφαλή διαχείριση των ηλεκτρονικών εγγραφών ασθενών δημιουργώντας μια εγγραφή χρονικού σήματος για οποιονδήποτε έρχονται σε επαφή με αυτό.

Οι ΗΠΑ είχαν μερικές από τις πιο δημοφιλείς κυβερνοεπιθέσεις στην υγειονομική περίθαλψη. Το 2015, οι εγκληματίες έκλεψαν 80 εκατομμύρια δίσκους από το *Anthem*, μια αμερικανική εταιρεία ασφάλισης υγείας. (BMJ, 2017) Οι ομοσπονδιακοί κανονισμοί για την προστασία των ασθενών και των πληροφοριών υγείας καλύπτονται από το Νόμο Υγεία περί ασφάλειας φορητότητας και λογοδοσίας του 1996 και η Τεχνολογία Πληροφορικής για την Οικονομία στην Υγεία και Κλινική Υγεία του 2009. (Jalali MS., Kaiser JP., 2018) Μία ανάπτυξη το 2018, ήταν η εκτόξευση του αμερικανικού Ινστιτούτου Προτύπων και Τεχνολογίας κυβερνοασφάλειας *framework11*, το οποίο αντιπροσωπεύει μια συνεργασία μεταξύ της

αμερικανικής κυβέρνησης και ιδιωτικών οντοτήτων προς βελτίωση των υποδομών στον κυβερνοχώρο σε όλη τη χώρα. Αυτό το πλαίσιο, το οποίο είναι εθελοντικό, χρησιμοποιείται σε πολύ σημαντικό βαθμό και είναι το πιο συχνά χρησιμοποιούμενο για τη βελτίωση της κυβερνοανθεκτικότητας στην υγειονομική περίθαλψη στις ΗΠΑ. (nist.gov, 2018)

Τον Μάιο του 2017, το *WannaCry ransomware* κρυπτογράφησε δεδομένα και αρχεία σε 230 000 υπολογιστές σε 150 χώρες, και εξασθένησε τη λειτουργικότητα της Εθνικής Υπηρεσίας Υγείας (NHS) στην Αγγλία. (Smart W., 2018) Τα βασικά συστήματα αποκλείστηκαν, εμποδίζοντας το προσωπικό να έχει πρόσβαση στα δεδομένα ασθενών και κρίσιμες υπηρεσίες. Ωστόσο, η επίθεση *WannaCry* δεν στοχεύτηκε άμεσα στο *NHS*. Άλλες μεγάλες οργανώσεις που συμπεριλήφθηκαν, ήταν οι *Telefonica, FedEx, Nissan, Russian Railways,* και *the Bank of China*. Ωστόσο, το μεγαλύτερο αποτέλεσμα ήταν αναμφίβολα από το *NHS*. (Chosh A., Ashok I., 2017) Ενώ υπήρχε παγκόσμια παρακολούθηση των συστημάτων υγείας, έγινε φανερό πόσο ευαίσθητη είναι η υγεία και η φροντίδα σε οποιαδήποτε απειλή στον κυβερνοχώρο.

Μία από τις δημοσιευμένες κυβερνο-επιθέσεις στην υγεία, ήταν στη Σιγκαπούρη το 2018, στην οποία έκλεψαν τα δεδομένα υγείας 1-5 εκατομμύρια πολιτών, συμπεριλαμβανομένου και του Πρωθυπουργού της. (Kwang K.,, 2018) Οι συστάσεις της εξεταστικής επιτροπής που διορίστηκε στη συνέχεια, περιλάμβαναν την ανασκόπηση όλων των συστημάτων και δικτύων που χρησιμοποιούνται πλήρως και τακτικά από το Υπουργείο Υγείας της Σιγκαπούρης, την εκπαίδευση όλου του προσωπικού στις πρακτικές κυβερνοασφάλειας, την απαίτηση ενισχυμένων ελέγχων ασφαλείας σε κρίσιμα συστήματα και ρύθμιση των απαντήσεων σε επιθέσεις για την αποφυγή ζημιών. (Kwang K.,, 2018)

6. Επίθεση σε συστήματα *pacs* σε απομονωμένο δίκτυο *LAN*

6.1. Σενάριο επίθεσης

Το σενάριο αυτό επικεντρώνεται σε έναν εισβολέα που βρίσκεται στο νοσοκομειακό χώρο και καταφέρνει να έχει πρόσβαση στην εσωτερική τοπική περιοχή του νοσοκομειακού δικτύου (*LAN*).

Η πρώτη φάση της επίθεσης είναι ο συμβιβασμός του νοσοκομειακού *LAN*. Αυτό μπορεί να συμβεί είτε μέσω πρόσβασης σε μία απροστάτευτη θύρα δικτύου του καλωδιακού δικτύου, ή θέτοντας σε κίνδυνο την κρυπτογράφηση του ασύρματου δικτύου (*WLAN*). Με την πάροδο του χρόνου, έχουν ανακαλυφθεί αδυναμίες σε όλους τους μηχανισμούς προστασίας *WLAN* από το *WEP* («*Wired Equivalent Protected*») στο πρωτόκολλο *WPA2* (*Wi-Fi Protected Access 2*) το οποίο εξακολουθεί να χρησιμοποιείται συνήθως και σήμερα. Για παράδειγμα, μία επιτυχημένη επίθεση κατά του *WPA2* που ονομάζεται "*KRACK*" (Επιθέσεις επανεγκατάστασης κλειδιού) δημοσιεύτηκε από τους Vanhoef et al. το 2017, που δείχνει ότι τα μέτρα που εφαρμόζει ο κλάδος της πληροφορικής είναι μέτρια. , δεδομένου ότι η δημοσίευση της αδυναμίας δεν έλυσε πλήρως το ζήτημα.

Η δεύτερη φάση της επίθεσης είναι η παθητική υποκλοπή ή κίνηση του δικτύου από τον εισβολέα, προκειμένου να μάθει για τη δομή του δικτύου, τα συστήματα στο δίκτυο, τα διαπιστευτήρια των χρηστών και το είδος των πρωτοκόλλων δικτύου που χρησιμοποιούνται. Τόσο το *DICOM* όσο και η στάθμη υγείας επτά (*HL7*) έκδοση 2 από προεπιλεγμένη μετάδοση μηνυμάτων σε απροστάτευτη, καθαρή μορφή κειμένου. Αυτό επιτρέπει σε έναν εισβολέα με πρόσβαση στο δίκτυο να χρησιμοποιήσει το λεγόμενο «πακέτο αναλυτή »για να υποκλέψει και να αναλύσει παθητικά την κίνηση του δικτύου.

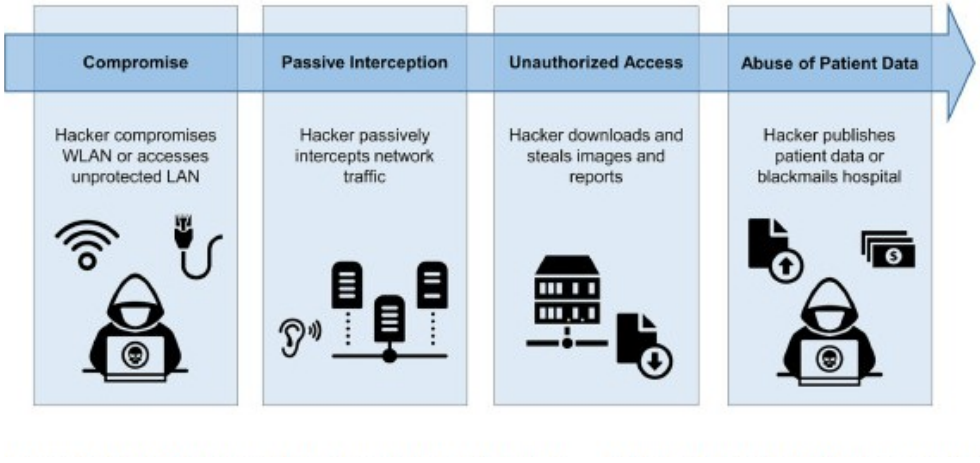
Για παράδειγμα, το *Wireshark* (Wireshark, xx), ένας ευρέως χρησιμοποιούμενος αναλυτής πακέτων, υποστηρίζει ρητά τα πρωτόκολλα δικτύου *HL7* και *DICOM* και είναι ακόμη σε θέση να αποθηκεύσει το περιεχόμενο μιας παθητικά καταγεγραμμένης μετάδοσης εικόνας *DICOM* ως έγκυρο αρχείο *DICOM*. Αυτό σημαίνει ότι ο εισβολέας είναι σε θέση να μάθει τις διευθύνσεις δικτύου και αριθμούς θύρας των συστημάτων *DICOM* και *HL7* στο δίκτυο, καθώς και τη λήψη ονομάτων ασθενών, δημογραφικών δεδομένων και αναγνωριστικών των ασθενών που εισάγονται επί του παρόντος στο νοσοκομείο.

Η τρίτη φάση της επίθεσης είναι η μη εξουσιοδοτημένη πρόσβαση σε συστήματα στο δίκτυο για τη λήψη εικόνων ή αναφορών. Ενώ η παθητική υποκλοπή δικτύου μπορεί να παρέχει σε έναν εισβολέα πληροφορίες για πολλές υπηρεσίες δικτύου γενικής χρήσης που χρησιμοποιούνται εντός του δικτύου (π.χ., e-mail ή Διαπιστευτήρια ιστοτόπου), αυτή η συζήτηση επικεντρώνεται σε συγκεκριμένα ζητήματα που σχετίζονται με την ιατρική απεικόνιση και *PACS*. Το πρωτόκολλο δικτύου *DICOM* ήταν αρχικά σχεδιασμένο στις αρχές της δεκαετίας του 1990, χωρίς μηχανισμούς για δικαιώματα πρόσβασης παρόλο που είχαν προβλεφθεί. Οποιοσδήποτε πελάτης μπορεί να συνδεθεί με επιτυχία στο διακομιστής *PACS* μέσω του δικτύου και μπορεί να εκδώσει ερωτήματα που σχετίζονται με τους ασθενείς, καθώς και μελέτες και εικόνες που είναι αποθηκευμένες σε αυτόν τον διακομιστή.

Η λήψη εικόνων (ή αναφορών σε μορφή *DICOM*) είναι πιο δύσκολες, γιατί το πρωτόκολλο *DICOM C-MOVE* που χρησιμοποιείται συχνότερα για το σκοπό αυτό, απαιτεί από τον διακομιστή *PACS* να ανοίξει ένα ξεχωριστό δίκτυο σύνδεσης με τον πελάτη, με βάση ένα συμβολικό όνομα που ονομάζεται "Μετακίνηση τίτλου οντότητας εφαρμογής". Οι διακομιστές *PACS*, επομένως, διατηρούν στη διαμόρφωση του συστήματος τους μια λίστα γνωστών πελατών με σταθερό δίκτυο. Μόνο τα συστήματα σε αυτήν τη λίστα μπορούν να έχουν λήψη από τον διακομιστή *PACS*. Ωστόσο, ακόμη και χωρίς ικανότητα λήψης εικόνων, ένας χάκερ θα μπορούσε ακόμα να εκδώσει ερωτήματα αποκτώντας έτσι εμπιστευτικές πληροφορίες ασθενών για όλους τους ασθενείς για τους οποίους οι εικόνες δεν αποθηκεύτηκαν ποτέ στο αρχείο.

Επιπλέον, το πρωτόκολλο *DICOM C-GET*, το οποίο υποστηρίζεται από τους περισσότερους σύγχρονους διακομιστές *PACS*, εξαλείφει την ανάγκη για μια προκαθορισμένη

λίστα γνωστών πελατών και επιτρέπει σε κάθε πελάτη που μπορεί να συνδεθεί με το διακομιστή για λήψη επίσης εικόνων. Η τελευταία φάση της επίθεσης θα ήταν η κατάχρηση των παράνομα αποκτηθέντων πληροφοριών «για διασκέδαση και κέρδος (fun and profit)». Οι επιτιθέμενοι θα μπορούσαν απλά να δημοσιεύουν ανώνυμα τα δεδομένα στο Διαδίκτυο, προκαλώντας έτσι νομικά προβλήματα, ποινές και κακή φήμη για το νοσοκομείο (και ενόχληση για τους ασθενείς), ή θα μπορούσαν να προσπαθήσουν να εκβιάσουν το νοσοκομείο με την απειλή δημοσίευσης των δεδομένων.



Σχήμα 7: Φάσεις επίθεσης σε νοσοκομειακό δίκτυο LAN

Πηγή: https://www.researchgate.net/publication/341417986/figure/fig3/AS:891631632924673@1589592955257/Attacker-hacks-into-the-hospital-network-A-phases-of-attack_Q320.jpg

Τα τεχνικά μέτρα που πρέπει να εφαρμοστούν για την πρόληψη αυτού του τύπου επίθεσης, θα πρέπει να αποτελούνται από πολλά επίπεδα για να επιτευχθεί μια «άμυνα σε βάθος»:

Το πρώτο στρώμα προστασίας αποτελείται από φυσικές εγγυήσεις και ασφαλή αρχιτεκτονική δικτύου.

- ➔ Οι θύρες καλωδιακού δικτύου δεν πρέπει να βρίσκονται σε δωμάτια στα οποία μη εξουσιοδοτημένα άτομα ενδέχεται να έχουν πρόσβαση χωρίς επίβλεψη, τα βύσματα του δικτύου πρέπει να είναι φυσικά ασφαλισμένα, έτσι ώστε να μην μπορούν να βγουν και να συνδεθούν σε διαφορετική συσκευή.

- ➔ Σε πολλά δίκτυα οι διακόπτες μπορούν να διαμορφωθούν έτσι ώστε να επιτρέπεται η σύνδεση μόνο σε υπολογιστές με καλά γνωστές διευθύνσεις ελέγχου πρόσβασης πολυμέσων (δηλ. σειριακοί αριθμοί του ελεγκτή διεπαφής δικτύου).
- ➔ Επιπλέον, οι αχρησιμοποίητες θύρες πρέπει να απενεργοποιηθούν μέχρι να χρειαστούν.
- ➔ Τα ασύρματα δίκτυα πρέπει να λειτουργούν σε ασφαλή διαμόρφωση, η οποία είναι σημαντικό να αναθεωρείται και να ενημερώνεται, εάν είναι απαραίτητο, σε τακτικά διαστήματα. Ενώ κανένα από αυτά τα μέτρα από μόνο του δεν θα προσφέρει τέλεια ασφάλεια, θα αυξήσουν την προσπάθεια που απαιτείται ώστε να αποφευχθεί μια επίθεση.
- ➔ Επιπλέον, τα τείχη προστασίας και η τμηματοποίηση δικτύου θα πρέπει να χρησιμοποιούνται για την απομόνωση των ιατρικών συσκευών και των *PACS* από τους υπολογιστές γραφείου που μπορεί να είναι πιο επιρρεπείς σε επιθέσεις. Ο Οργανισμός Ευρωπαϊκής Ένωσης για Ασφάλεια Δικτύων και Πληροφοριών (ENISA, 2016) επισημαίνει ότι «είναι σημαντικό να διαχωριστούν τα κρίσιμα τμήματα του δικτύου από μη κρίσιμα μέρη. Για παράδειγμα, συνίσταται ο διαχωρισμός των ιατρικών συσκευών στο μεγαλύτερο δυνατό από στοιχεία του γραφείου που οφείλονται συνήθως στο χρήση τυποποιημένων εξαρτημάτων ευαίσθητων σε ένα ευρύ φάσμα επιθέσεων. Η *Nippon Telegraph and Telephone Security* εξηγεί ότι η κατάτμηση του δικτύου είναι σημαντική διότι «εάν οι επιτιθέμενοι μπορούν παραβιάζουν διακομιστές *back-end*, μπορεί να μπορούν να μετακινηθούν πλευρικά στην πρόσβαση σε άλλα τμήματα του δικτύου, προκαλώντας περαιτέρω ζημιά, και ενδεχομένως να αποκτήσουν έρεισμα σε πολλαπλά συστήματα »(NIT Security, 2019). Συνιστούν τη χρήση «τείχους προστασίας, δρομολογητών και συσκευών ασφαλείας άλλων δικτύων για την εφαρμογή και την επιβολή του διαχωρισμού δικτύου », δηλαδή, «περιορίζοντας τη ροή της κίνησης δικτύου μεταξύ τμημάτων δικτύου με διαφορετικά προφίλ ασφαλείας »(NIT Security, 2017).

Το δεύτερο επίπεδο προστασίας είναι η χρήση κρυπτογράφησης για μετάδοση δικτύου όχι μόνο μέσω Διαδικτύου, αλλά και εσωτερικά. Ενώ και το *DICOM* και το *HL7* επικοινωνούν από προεπιλογή σε καθαρό κείμενο, όπως περιγράφηκε προηγουμένως, και τα δύο πρωτόκολλα μπορούν να προστατευτούν χρησιμοποιώντας το *Transport Layer Security* (TLS) (Rescorla E., 2018), ένα πρωτόκολλο δικτύου που επιτρέπει στις εφαρμογές να επικοινωνούν μέσω του Διαδικτύου με τρόπο που έχει σχεδιαστεί για να αποτρέπει την υποκλοπή, παραποίηση και παραποίηση μηνυμάτων (Rescorla E., 2018). Το πρότυπο *DICOM* προσφέρει ένα σύνολο

"προφίλ ασφαλούς σύνδεσης μεταφοράς" που περιγράφουν πώς να χρησιμοποιηθεί το *TLS* με συνδέσεις δικτύου *DICOM*.

Ο πρώτος από αυτά προστέθηκε στο πρότυπο *DICOM* το 2000, σχεδόν πριν από 20 χρόνια, και η πρώτη επέκταση εφαρμογής *DICOM* αυτού του ανοιχτού κώδικα δημοσιεύθηκε το ίδιο έτος (Kroll M., Scheutze B., Geibse T., 2003). Για συστήματα που δεν υποστηρίζουν *TLS*, μπορεί να εφαρμοστεί μια πύλη που δέχεται "κανονικές" συνδέσεις δικτύου *DICOM* και προωθώντας τα χρησιμοποιώντας *TLS*. Μια έγκαιρη εφαρμογή μιας τέτοιας πύλης είχε ήδη περιγραφεί από τους Thiel et al. το 1999 (Thiel A., Bernanding J., Jensch P., 2017). Το *DICOM* και το *HL7* προστατεύονται με *TLS*, μια παθητική υποκλοπή της κίνησης του δικτύου δεν θα παρέχει στους επιτιθέμενους καμία εμπιστευτική πληροφορία (τουλάχιστον σχετικά με αυτά τα πρωτόκολλα) ακόμη και εάν καταφέρουν να θέσουν σε κίνδυνο το δίκτυο και να αποκτήσουν πρόσβαση δικτύου. Επιπλέον, εάν το *TLS* χρησιμοποιείται με πιστοποιητικό ανταλλαγής διπλής κατεύθυνσης (μια επιλογή στο πρωτόκολλο *TLS*), στη συνέχεια ένας εισβολέας που αποκτά πρόσβαση στο δίκτυο δεν θα μπορεί να συνδεθεί με κανένα από τα προστατευόμενα συστήματα, αποτρέποντας κάθε απόπειρα λήψης εικόνων ή αναφορών από το διακομιστή *PACS*.

Το τρίτο επίπεδο προστασίας είναι η εφαρμογή της πρόσβασης δικαιωμάτων στο διακομιστή *PACS*. Για το σκοπό αυτό, το πρότυπο *DICOM* τροποποιήθηκε το 2004 (DICOM, 2019) για να καταστεί δυνατή η μετάδοση των πληροφοριών ταυτότητας χρήστη κατά την αρχική φάση μιας *DICOM* σύνδεσης δικτύου. Αυτές οι πληροφορίες μπορούν να χρησιμοποιηθούν από το διακομιστή *PACS* για περιορισμό της πρόσβασης σε εικόνες και αναφορές βάσει πληροφοριών όπως η ανάθεση χρηστών σε τμήματα, ρόλους χρηστών και την τρέχουσα κατάσταση του ασθενούς.

Το πρότυπο *DICOM* δεν διευκρινίζει πώς πρέπει να ορίζονται τέτοια δικαιώματα πρόσβασης και συνδέεται με την ταυτότητα χρήστη, καθώς αυτό θα εξαρτηθεί από τις τοπικές πολιτικές και νόμους. Σε κάθε περίπτωση, τα δικαιώματα εφαρμογής μιας τέτοιας πρόσβασης θα περιορίσουν τον αριθμό των εικόνων και των αναφορών οποιουδήποτε εισβολέα μπορεί να έχει πρόσβαση και λήψη, εάν ο εισβολέας καταφέρει να θέσει σε κίνδυνο το δίκτυο και να δημιουργήσει επιτυχώς μία *TLS* σύνδεση (π.χ. από κλοπή πιστοποιητικού και ιδιωτικού κλειδιού - ένα άλλο σύστημα στο δίκτυο), δεν εμποδίζει, αλλά μετριάζει το αποτέλεσμα μιας επίθεσης.

6.2. Συμπεράσματα επιθέσεων

Πρέπει να επισημανθεί ότι αυτά, δεν είναι μια πλήρης λίστα με τα μέτρα κυβερνοασφάλειας που ισχύουν. Περαιτέρω μέτρα περιλαμβάνουν μία τακτική δημιουργία αντιγράφων ασφαλείας, τη χρήση της παρακολούθησης του δικτύου και της εισβολής συστημάτων ανίχνευσης, την επιτρεπόμενη λίστα των επιτρεπόμενων εφαρμογών, και ολόκληρο το πεδίο των οργανωτικών μέτρων όπως η εκπαίδευση χρηστών, δοκιμές διείσδυσης και διαχείριση περιστατικών. Μια επισκόπηση αυτών των θεμάτων παρέχεται από τον Οργανισμό της Ευρωπαϊκής Ένωσης για την ασφάλεια δικτύων και πληροφοριών (ENISA, 2016). Τα περισσότερα από τα γενικά μέτρα ασφαλείας μπορούν να εφαρμοστούν από την οργάνωση χρηστών (δηλαδή το νοσοκομείο) χωρίς υποστήριξη από προμηθευτές συσκευών, με εξαίρεση τακτικές ενημερώσεις λειτουργικών συστημάτων και λογισμικού εφαρμογών σε όλα τα συστήματα, κάτι που απαιτεί την παροχή ενημερώσεων από τους πωλητές συσκευών, ιδίως στην περίπτωση πιστοποιημένων ιατροτεχνολογικών προϊόντων όπου οποιαδήποτε τροποποίηση πρέπει να υποστεί αυστηρή δοκιμή από τον πωλητή πριν από τη διάθεση στους χρήστες.

Από την άλλη πλευρά, τα περισσότερα PACS/ιατρικής απεικόνισης απαιτούν ειδικά μέτρα ασφαλείας και υποστήριξη από πωλητές συσκευών. Ενώ ένα νοσοκομείο θα πρέπει να μπορεί να αναπτύξει μία σταθερή εγκατάσταση ενός προγράμματος προβολής DICOM για εισαγωγή πολυμέσων, η μετακίνηση από μη κρυπτογραφημένη επικοινωνία στο δίκτυο σε κρυπτογραφημένη επικοινωνία, απαιτεί την υποστήριξη συσκευής ή εναλλακτικά την ανάπτυξη υπολογιστών πύλης, που μπορεί είναι μια επιχειρηματική ευκαιρία για τις νεοφυείς εταιρείες στην περίπτωση κρυπτογραφημένης επικοινωνίας και ψηφιακών υπογραφών, που έχουν τυποποιηθεί στο DICOM εδώ και περίπου 20 χρόνια. Το προφανές ερώτημα είναι: γιατί δεν έχουν αυτά τα μέτρα (ή σπάνια) είχαν αναπτυχθεί στο παρελθόν.

Σύμφωνα με την γενικότερη βιβλιογραφία, υπάρχουν δύο βασικοί λόγοι: ένας λόγος είναι ότι η αναγκαιότητα για εφαρμογή τέτοιων μέτρων εντός του νοσοκομειακού δικτύου και όχι μόνο στο τείχος προστασίας που προστατεύει το «έμπιστο» LAN από το μη αξιόπιστο Διαδίκτυο, έγινε εμφανής μόλις πρόσφατα. Δεδομένου ότι υπήρχε πολύ μικρή ζήτηση από τους χρήστες στο παρελθόν, οι πωλητές δεν έχουν εφαρμόσει χαρακτηριστικά ασφαλείας και θα χρειαστεί σημαντική προσπάθεια από την κοινότητα των χρηστών να αλλάξει αυτό τώρα. Ο

δεύτερος λόγος είναι ότι η εφαρμογή των μέτρων ασφάλειας μπορεί να είναι πιο ακριβά (από την άποψη της απαιτούμενης προσπάθειας). Για παράδειγμα, τόσο η χρήση κρυπτογραφημένης

επικοινωνίας όσο και οι ψηφιακές υπογραφές, απαιτούν από τα νοσοκομεία να αναπτύξουν ένα δημόσιο κλειδί υποδομής καθώς κάθε σύστημα πρέπει να εφοδιάζεται με ένα ατομικό ιδιωτικό κλειδί και υπογεγραμμένο πιστοποιητικό. Όλα αυτά πρέπει να ανανεώνονται τακτικά καθώς τα πιστοποιητικά έχουν πεπερασμένη διάρκεια ζωής (συνήθως μεταξύ τριών μηνών και τριών ετών). Αυτά τα ζητήματα είναι πιο γρήγορα από τους προμηθευτές PACS και modality. Η εφαρμογή των δικαιωμάτων πρόσβασης στο PACS απαιτεί μία υποστήριξη χειρός και στους δύο διακομιστές PACS, η οποία πρέπει να επιβάλει τα δικαιώματα πρόσβασης και στους σταθμούς εργασίας, οι οποίοι πρέπει να πιστοποιηθούν από τον χρήστη και να μεταδώσουν την ταυτότητά του στον διακομιστή.

Από την άλλη, απαιτεί και εργασία από το νοσοκομείο, το οποίο πρέπει να ορίσει κατάλληλους κανόνες για τα δικαιώματα πρόσβασης και να παρέχει διασυνδέσεις με τα συστήματα που διατηρούν τις απαιτούμενες πληροφορίες, π.χ., ποιος ασθενής έχει τοποθετηθεί σε ποιο τμήμα, θάλαμο ή ποιος γιατρός. Αυτές οι πληροφορίες είναι συνήθως διαθέσιμες στο Πληροφοριακό Σύστημα Νοσοκομείων αλλά όχι στο PACS. Τα συστήματα που απολυμαίνουν τα προοίμια των αρχείων *DICOM*, χρησιμοποιούν *bitstream* επικυρωτές και διεργασίες *sandbox* κατά την ενθυλακωμένη επεξεργασία εγγράφων και συμπιεσμένων εικόνων, ενώ χρησιμοποιούν την εφαρμογή με τη λογική να "πιάσει" πιθανώς κακόβουλα μηνύματα *HL7* που μπορεί να παρέχονται μόνο από τους προμηθευτές του συστήματος.

Τέλος, οι ψηφιακές υπογραφές απαιτούν επίσης υποστήριξη του προμηθευτή: Ενώ είναι δυνατή η προσθήκη υπογραφής δημιουργίας λειτουργικότητας σε συστήματα παλαιού τύπου μέσω πύλης υπολογιστών, η προστασία της ακεραιότητας που προσφέρουν οι ψηφιακές υπογραφές είναι άχρηστη εκτός εάν οι θεατές επαληθεύσουν τις υπογραφές κατά την ανάγνωση ενός *DICOM* εγγράφου ή εικόνας, και προειδοποιήσουν τον χρήστη εάν μια υπογραφή δεν είναι έγκυρη ή λείπει. Ένα άλλο σημείο είναι η προστασία που είναι δυνατή ακόμη και από περίπλοκες επιθέσεις κυβερνοασφάλειας, και ότι τα περισσότερα από τα απαιτούμενα μέτρα απαιτούν κοινή γνώση ή ακόμα και τυποποιημένη για μεγάλο χρονικό διάστημα. Στα

νοσοκομεία με εκατοντάδες ή χιλιάδες συστήματα αυτό απαιτεί αυτοματοποίηση, καθώς η χειροκίνητη εγκατάσταση πιστοποιητικών και κλειδιών σε κάθε σύστημα δεν είναι βιώσιμη.

Η αποτυχία ανανέωσης του πιστοποιητικού θα προκαλέσει αυτόματα μια διασύνδεση ολοκλήρωσης αποτυχίας μόλις λήξει το πιστοποιητικό. Επιπλέον, οι κρυπτογραφικοί αλγόριθμοι που χρησιμοποιούνται για την κρυπτογραφημένη επικοινωνία και οι ψηφιακές υπογραφές, θα πρέπει να εξελίσσονται με την πάροδο του χρόνου από τους αλγόριθμους και τα βασικά μήκη που θεωρούνται ασφαλή σήμερα ή που μπορεί να γίνουν ανασφαλείς στο μέλλον. Αυτό πρέπει να συντονιστεί σε όλα τα συστήματα που χρησιμοποιούν αυτούς τους αλγόριθμους, επειδή μια ενημέρωση ενός συστήματος που καταργεί την υποστήριξη για έναν απαρχαιωμένο αλγόριθμο μπορεί να καθιστά μια διεπαφή μη λειτουργική, εάν οι νεότεροι αλγόριθμοι δεν υποστηρίζονται από όλες τις άλλες συσκευές που υποτίθεται ότι επικοινωνούν με αυτό το σύστημα.

Τέλος, το ερώτημα παραμένει ποια μέτρα ασφαλείας πρέπει να λαμβάνονται από τους ακτινολόγους. Σε γενικές γραμμές, θα έπρεπε να υπάρχει μια ομάδα επαγγελματιών πληροφορικής με την ευθύνη του προγραμματισμού και διατήρησης της υπό εξέταση υποδομής πληροφορικής ιατρικής, επιχειρησιακής, οικονομικής, ασφάλειας και παραγόντων ασφαλείας. Μέρος αυτής της εργασίας θα πρέπει να είναι η ανάπτυξη ενός συνόλου τοπικών κατευθυντήριων γραμμών ασφαλείας, μαζί με την ευαισθητοποίηση των χρηστών και μέτρα κατάρτισης για ιατρικούς χρήστες. Αυτές οι κατευθυντήριες γραμμές θα πρέπει να καθοδηγούν τους χρήστες πώς να αντιδρούν όταν ένας ανιχνευτής ιών προειδοποιεί, πώς να χειρίζονται τα μέσα αποθήκευσης που φέρνουν οι ασθενείς, πώς να αναφέρουν ανωμαλίες που μπορεί να είναι ή όχι σχετικές για την ασφάλεια στον κυβερνοχώρο και πώς να διαχειρίζονται περιστατικά κυβερνοασφάλειας.

Εάν δεν υπάρχουν ακόμη τέτοιες κατευθυντήριες οδηγίες, οι ακτινολόγοι θα πρέπει να επιμείνουν στην ανάπτυξη και να συνεργαστούν με επαγγελματίες πληροφορικής για να βεβαιωθούν ότι θα ισχύουν οι κανόνες που καθορίζονται και δεν επηρεάζουν αρνητικά την ιατρική πρακτική. Μόλις υπάρχει η διάθεση κατευθυντηρίων γραμμών, οι ακτινολόγοι θα πρέπει να διασφαλίζουν ότι τηρούνται. Επιπλέον, είναι ζωτικής σημασίας οι επαγγελματίες υγείας, που συχνά θα είναι οι πρώτοι που θα το παρατηρήσουν, να μην αγνοήσουν σχετικές ανωμαλίες αλλά

να τις αναφέρουν αμέσως, αφού ο χρόνος μέχρι την έναρξη της διαχείρισης συμβάντων μπορεί να είναι κρίσιμος περιορίζοντας τη ζημιά που έχει προκληθεί.

7. Άμυνα/Επίθεση/Πρόληψη Κυβερνοεπιθέσεων

7.1 Άμυνες/πρόληψη σε επιθέσεις

Ο σύγχρονος κόσμος εξαρτάται περισσότερο από ποτέ από την τεχνολογία. Ένας τεράστιος όγκος δεδομένων δημιουργείται και συλλέγεται με τη μεγάλη εφαρμογή ακμάζουσας τεχνολογίας όπως το Διαδίκτυο των Πραγμάτων (*IoT*) (Li S., Li Da X., Zhao S., 2015) και το *cloud computing* (Velte T., Velte A., Eslenpeter R., 2009). Αν και τα δεδομένα μπορούν να χρησιμοποιηθούν για την καλύτερη εξυπηρέτηση των αντίστοιχων επιχειρηματικών και ιατρικών αναγκών, οι κυβερνοεπιθέσεις συχνά δημιουργούν μεγάλες προκλήσεις.

Η εκμετάλλευση ή οι απειλές από τα μέσα είναι συνηθισμένες στις μέρες μας (Sarker IH et al., 2020). Αυτοί οι τύποι συμβάντων ασφαλείας ή εγκλήματος στον κυβερνοχώρο μπορούν να προσβάλλουν οργανισμούς υγείας αλλά και άτομα, προκαλούν διαταραχές καθώς και καταστροφικές οικονομικές ζημίες. Για παράδειγμα, σύμφωνα με έκθεση της *IBM*, μια παράβαση δεδομένων κοστίζει 8,19 εκατομμύρια δολάρια για τις Ηνωμένες Πολιτείες (IBM,, 2020), και το εκτιμώμενο ετήσιο κόστος για τη παγκόσμια οικονομία από εγκλήματα στον κυβερνοχώρο ανέρχεται σε 400 δισεκατομμύρια αμερικανικά δολάρια (Fisher EA., 2020). Τα εγκλήματα στον κυβερνοχώρο αυξάνονται με εκθετικό ρυθμό που φέρνει ένα ανησυχητικό μήνυμα για τους επαγγελματίες και ερευνητές της κυβερνοασφάλειας (Sarker IH et al.,, 2020).

Επομένως η αποτελεσματική και έξυπνη προστασία ενός πληροφοριακού συστήματος υγείας, ιδίως συστημάτων που συνδέονται με το Διαδίκτυο από διάφορες απειλές στον κυβερνοχώρο, επιθέσεις, ζημιές, ή μη εξουσιοδοτημένη πρόσβαση, είναι ένα βασικό ζήτημα που πρέπει να λυθεί επειγόντως. Στον πραγματικό κόσμο, η συνολική ασφάλεια του οργανισμού υγείας, της κυβέρνησης, των οργανώσεων και των μεμονωμένων πολιτών της σε μια χώρα εξαρτάται από τα εργαλεία διαχείρισης της ασφάλειας που διαθέτουν την ικανότητα ανίχνευσης και πρόληψης της ασφάλειας των περιστατικών με έγκαιρο και έξυπνο τρόπο.

Η κυβερνοασφάλεια αναφέρεται συνήθως σε μια συλλογή από τεχνολογίες, διαδικασίες και πρακτικές που έχουν σχεδιαστεί για την προστασία δικτύων, υπολογιστών, προγραμμάτων και δεδομένων από επίθεση, διακοπή ή μη εξουσιοδοτημένη πρόσβαση. Είναι επίσης γνωστή ως «ασφάλεια τεχνολογίας πληροφοριών» ή «ασφάλεια ηλεκτρονικών πληροφοριών". Σύμφωνα με

τις πολυάριθμες ανάγκες του σήμερα, οι συμβατικά γνωστές λύσεις ασφαλείας όπως *antivirus*, *firewalls*, ο έλεγχος ταυτότητας χρήστη, η κρυπτογράφηση κλπ. μπορεί να μην είναι αποτελεσματικές (Tavallaee M., Stakhonova N., Ghorbami AA., 2010).

Από την άλλη πλευρά, η Τεχνητή νοημοσύνη (AI), η οποία είναι γνωστή ως η βασική τεχνολογία της Τέταρτης Βιομηχανικής Επανάστασης (Industry 4.0), μπορεί να παίξει σημαντικό ρόλο για έξυπνες υπηρεσίες και διαχείριση κυβερνοασφάλειας στην υγεία, σύμφωνα με την υπολογιστική ισχύ και τις δυνατότητές τους.

7.2 Στρατηγικές άμυνας στον κυβερνοχώρο

Οι στρατηγικές άμυνας στον κυβερνοχώρο στον τομέα της υγείας, είναι συνήθως για την προστασία συστημάτων και δικτύων υπολογιστών από τη βλάβη του σχετικού υλικού, λογισμικού ή δεδομένων, καθώς και ως τη διακοπή των υπηρεσιών που παρέχουν. Πιο συγκεκριμένα, είναι υπεύθυνες για την πρόληψη παραβιάσεων δεδομένων ή συμβάντων ασφαλείας που μπορούν να οριστούν ως κάθε είδους κακόβουλες ή μη εξουσιοδοτημένες δραστηριότητες για την προστασία των συστημάτων (Khraisat A. et al.,, 2019).

Επιλογή κατάλληλων κωδικών πρόσβασης (passwords) : Ο έλεγχος πρόσβασης, μέσω του κωδικού password (κωδικοποιημένες λέξεις που έχουν αμοιβαία συμφωνηθεί και θεωρούνται γνωστά μόνο στο χρήστη και στο σύστημα), είναι ένας μηχανισμός ασφαλείας που ρυθμίζει τυπικά την πρόσβαση ή τη χρήση των πόρων, π.χ. δίκτυα υπολογιστών, αρχεία συστήματος ή δεδομένα, σε υπολογιστικό περιβάλλον. Για παράδειγμα, με βάση τις ευθύνες μεμονωμένων χρηστών, μπορεί να χρησιμοποιηθεί ένα χαρακτηριστικό ή ένα σύστημα ελέγχου πρόσβασης βάσει ρόλου για τον περιορισμό της πρόσβασης στο δίκτυο, μειώνοντας τον κίνδυνο για την εταιρεία ή την οντότητα.

Firewall : Το τείχος προστασίας είναι ένα πλαίσιο ασφαλείας για το δίκτυο που παρακολουθεί και ρυθμίζει την εισερχόμενη και εξερχόμενη κίνηση ενός δικτύου. Τα τείχη προστασίας καθορίζονται ως δίκτυο ή σύστημα βασισμένο σε κεντρικό υπολογιστή που βασίζεται σε ένα σύνολο κανόνων ασφαλείας που επιτρέπουν ή αποκλείουν την κίνηση. Είναι

επίσης ικανό να διώξει μεταφορά από μη ασφαλείς ή ύποπτες πηγές προς αποφυγή επιθέσεων, όπως κακόβουλο λογισμικό.(Yin J., 2016)

Anti-malware : Επίσης γνωστό ως λογισμικό προστασίας από ιούς, είναι ένα πρόγραμμα υπολογιστή που χρησιμοποιείται συνήθως για την πρόληψη, ανίχνευση και αφαίρεση ιών ή κακόβουλου λογισμικού. Το λογισμικό προστασίας από ιούς μπορεί να προστατεύσει τους χρήστες από διάφορες κακόβουλες επιθέσεις όπως *ransomware*, *backdoors*, *trojan horses*, *worms*, *spyware* κ.λπ.(Xue Y. et al., 2017)

Το *Sandbox :* (Hunt T. et al., 2018) είναι ένας μηχανισμός ασφαλείας που χρησιμοποιείται για τον μετριασμό των βλαβών του συστήματος ή των ευπάθειων λογισμικού που εξαπλώνεται μέσω του διαχωρισμού των τρεχόντων προγραμμάτων. Χρησιμοποιείται συχνά για την εκτέλεση μη αξιόπιστων προγραμμάτων ή κώδικα, ενδεχομένως από μη επαληθευμένους προμηθευτές, χρήστες, ιστότοπους ή μη αξιόπιστα τρίτα μέρη.

Πληροφορίες ασφαλείας και διαχείριση συμβάντων (SIEM) (Irfan M. et al., 2016) είναι ένας συνδυασμός διαχείρισης πληροφοριών ασφαλείας (*SIM*) και διαχείριση συμβάντων ασφαλείας (*SEM*) που παρέχουν ανάλυση σε πραγματικό χρόνο του υλικού της συσκευής και των ειδοποιήσεων του δικτύου ασφαλείας.

Η κρυπτογραφία : (Abood OG. Guirguis SK., 2018) είναι μια δημοφιλής μέθοδος που χρησιμοποιείται για την προστασία δεδομένων ή πληροφοριών που χρησιμοποιεί τα μυστικά κλειδιά, π.χ. μυστικό κλειδί, δημόσιο κλειδί και λειτουργία κατακερματισμού, για κρυπτογράφηση και αποκρυπτογράφηση δεδομένων για επικοινωνία. Αν και οι παραδοσιακές γνωστές προσεγγίσεις ασφαλείας έχουν τα δικά τους πλεονεκτήματα για διαφορετικούς σκοπούς, μπορεί να μην είναι αποτελεσματικές σύμφωνα με τις σημερινές ποικίλες ανάγκες στον κυβερνοχώρο λόγω της έλλειψης ευφυΐας και δυναμισμού.

Το σύστημα ανίχνευσης εισβολής (IDS) που γίνεται όλο και περισσότερο δημοφιλές και τυπικά ορίζεται ως «συσκευή ή εφαρμογή λογισμικού που παρακολουθεί ένα δίκτυο ή συστήματα υπολογιστών για κακόβουλη δραστηριότητα ή παραβιάσεις πολιτικής »(Johnson L., 2013). Το *IDS* είναι συνήθως ικανό να εντοπίσει τις διάφορες κυβερνοαπειλές και επιθέσεις, ακόμη και την άγνωστη επίθεση και είναι ικανό να απαντήσει μέσα σε πραγματικό χρόνο με

βάση τις απαιτήσεις του χρήστη. Το *IDS* συγκεντρώνει δεδομένα από διαφορετικές πηγές σε δίκτυο υπολογιστών ή συσκευές. Σκοπός είναι ο εντοπισμός των παραβιάσεων των πολιτικών ασφαλείας που μπορεί να χρησιμοποιηθούν για τον εντοπισμό εσωτερικών και εξωτερικών επιθέσεων (Brahmi I., Brahmi H., Yahia SB., 2015).

Το *IDS* μπορεί να είναι διάφοροι τύποι με βάση τον τύπο περιβάλλοντος και τις προσεγγίσεις ανίχνευσης. Για παράδειγμα, με βάση το εύρος από τους απλούς υπολογιστές έως τα μεγάλα δίκτυα, οι πιο συνηθισμένοι τύποι των I*DS* είναι:

- Το *IDS* (*HIDS*) που βασίζεται σε κεντρικό υπολογιστή εκτελείται σε έναν κεντρικό υπολογιστή και αναλύει τη κίνηση και ανίχνευση κακόβουλης ή ύποπτης δραστηριότητας. Έτσι, μπορεί να παρέχει ορατότητα σε πραγματικό χρόνο για το τι συμβαίνει στα κρίσιμα συστήματα ασφαλείας, και το οποίο προσθέτει επιπλέον ασφάλεια (Sarker IH et al.,, 2020).
- *IDS* βάσει δικτύου (*NIDS*). Από την άλλη πλευρά, το *NIDS* αναλύει και παρακολουθεί τις συνδέσεις δικτύου για τον εντοπισμό κακόβουλης δραστηριότητας ή παραβιάσεων πολιτικής σε ένα δίκτυο (Sarker IH et al.,, 2020). Ομοίως, το *IDS* μπορεί να είναι πολλών τύπων, ανάλογα με τη μέθοδο ανίχνευσης, όπου οι πιο γνωστές εκδόσεις είναι το *IDS* βάσει υπογραφής και *IDS* που βασίζονται σε ανωμαλίες (Khraisat A. et al.,, 2019).

    - *IDS* (*SIDS*) βάσει υπογραφής : Αναζητά μοναδικά μοτίβα, όπως ακολουθίες *byte* κίνησης δικτύου ή αναγνωρισμένες κακόβουλες ακολουθίες που χρησιμοποιεί το κακόβουλο λογισμικό ως υπογραφές. Θεωρείται επίσης ως κακή χρήση ή ανίχνευση βάσει γνώσης που λειτουργεί καλά για τις γνωστές επιθέσεις (Liao H-J et al., 2013). Μπορεί, ωστόσο, να αντιμετωπίσει τη μεγαλύτερη πρόκληση στον εντοπισμό άγνωστων ή νέων επιθέσεων.

    - *IDS* που βασίζονται σε ανωμαλίες (*AIDS*) : Από την άλλη πλευρά, λόγω της ταχείας ανάπτυξης κακόβουλου λογισμικού τις τελευταίες ημέρες, το *AIDS* κυρίως χρησιμοποιείται κυρίως για τον εντοπισμό άγνωστων επιθέσεων. Για τον εντοπισμό ανωμαλιών όπως οι άγνωστες ή μη επιθετικές ημέρες, οι τεχνικές μηχανικής εκμάθησης μπορούν επίσης να χρησιμοποιηθούν για τη δημιουργία του μοντέλου προστασίας (Ammar A., et al., 2012).

- *Hybrid IDS* : Το υβριδικό *IDS* λαμβάνεται με συνδυασμό *IDS* που βασίζεται σε ανωμαλίες με το *IDS* που βασίζεται σε κακή χρήση και μπορεί να χρησιμοποιηθεί για τον αποτελεσματικό εντοπισμό του κακόβουλου λογισμικού σε πολλές περιπτώσεις (Viegas E. et al., 2016).

Stateful Protocol Analysis (SPA) : Το *SPA* είναι ένας άλλος τύπος μεθόδου που προσδιορίζει τις αποκλίσεις της κατάστασης πρωτοκόλλου. Αυτή η προσέγγιση είναι παρόμοια με την μέθοδο ανωμαλιών, ωστόσο, χρησιμοποιεί προκαθορισμένα καθολικά προφίλ της καλοήθους δραστηριότητας πρωτοκόλλου (Liao H-J et al., 2013). Μόλις εντοπιστούν οι κακόβουλες δραστηριότητες, το σύστημα πρόληψης εισαγωγής (*IPS*) μπορεί να χρησιμοποιηθεί για αποφυγή και αποκλεισμό τους. Αυτό μπορεί να γίνει με πολλούς τρόπους, όπως χειροκίνητα, αποστολή ειδοποίησης ή αυτοματοποιημένη λειτουργία (Ragsdale DJ.. et al., 2000). Αναμεταξύ αυτών των μέθοδοι, μπορεί να υπάρχει ένα πιο αποτελεσματικό σύστημα αυτόματης απόκρισης (*ARS*), επειδή δεν περιλαμβάνει ανθρώπινη διεπαφή μεταξύ των συστημάτων ανίχνευσης και απόκρισης.

7.2.1. Τοίχος προστασίας (Firewall)

Το τείχος προστασίας είναι ένα σύστημα που επιβάλλει μία πολιτική ελέγχου πρόσβασης μεταξύ δύο δικτύων — όπως το ιδιωτικό *LAN* και το μη ασφαλές, δημόσιο Διαδίκτυο. Το τείχος προστασίας καθορίζει ποιες εσωτερικές υπηρεσίες μπορεί να έχουν πρόσβαση από έξω, και αντίστροφα. Τα πραγματικά μέσα με τα οποία αυτό επιτυγχάνεται ποικίλλουν ευρέως, αλλά κατ'αρχήν, το τείχος προστασίας μπορεί να θεωρηθεί ως ένα ζευγάρι μηχανισμών: ένα για να αποκλείσει την κυκλοφορία και ένα προς την άδεια κυκλοφορίας. Ένα τείχος προστασίας είναι κάτι περισσότερο από μια κλειδωμένη μπροστινή πόρτα στο δίκτυο. Είναι φύλακας. Τα τείχη προστασίας είναι επίσης σημαντικά επειδή παρέχουν ένα μόνο "σημείο πνιγμού" όπου μπορεί να υπάρχει ασφάλεια και επιβάλλονται έλεγχοι. Μπορεί να παρέχει δίκτυο διαχειριστή με δεδομένα σχετικά με το είδος και τη ποσότητα επισκεψιμότητας που πέρασαν από αυτό, πόσες προσπάθειες έγιναν για να το σπάσουν και ούτω καθεξής (3Com, 2000).

Όπως ένα κλειστό κύκλωμα τηλεοπτικού συστήματος ασφαλείας, το τείχος προστασίας όχι μόνο εμποδίζει την πρόσβαση, αλλά και παρακολουθεί ποιος ήταν ψάχνει γύρω και βοηθά στον

εντοπισμό όσων προσπαθούν να παραβιάσουν την ασφάλειά. Βασικός σκοπός του είναι να κάνει τρία πράγματα για την προστασία του δικτύου ειδικά σε συστήματα υγειονομικής περίθαλψης:

- Αποκλείει τα εισερχόμενα δεδομένα που μπορεί περιέχουν επίθεση χάκερ.
- Κρύβει πληροφορίες σχετικά με το δίκτυο κάνοντάς το να φαίνεται ότι όλη η εξερχόμενη κίνηση προέρχεται από το τείχος προστασίας παρά το δίκτυο. Αυτό ονομάζεται Μετάφραση Διεύθυνσης δικτύου (*NAT*).
- Ελέγχει την εξερχόμενη κίνηση για περιορισμό της χρήσης διαδικτύου ή/και τη πρόσβαση σε απομακρυσμένες τοποθεσίες.

Επίπεδα προβολής

Ένα τείχος προστασίας μπορεί να ελέγξει και την εισερχόμενη και την εξερχόμενη κίνηση. Επειδή η εισερχόμενη κίνηση αποτελεί μεγαλύτερη απειλή για το δίκτυο, συνήθως προβάλλεται περισσότερο στενά από την εξερχόμενη κίνηση. Υπάρχουν τρεις τύποι προβολής που εκτελούν τα τείχη προστασίας(3Com, 2000):

- Προβολή που αποκλείει όποια εισερχόμενα δεδομένα δεν διατάσσονται συγκεκριμένα από τον χρήστη στο δίκτυο
- Προβολή από τη διεύθυνση του αποστολέα
- Προβολή με βάση το περιεχόμενο της επικοινωνίας

Τα επίπεδα ελέγχου λειτουργούν ως μία διαδικασία εξάλειψης. Το τείχος προστασίας πρώτα καθορίζει αν η εισερχόμενη μετάδοση είναι κάτι που ζητείται από έναν χρήστη στο δίκτυο, απορρίπτοντας οτιδήποτε άλλο. Ότι επιτρέπεται μέσα εξετάζεται στη συνέχεια περισσότερο από κοντά. Το τείχος προστασίας ελέγχει τη διεύθυνση του υπολογιστή του αποστολέα για να διασφαλιστεί ότι είναι ένας αξιόπιστος ιστότοπος. Επίσης ελέγχει το περιεχόμενο της μετάδοσης.

7.3. Τύποι Επίθεσης

Πριν καθοριστεί ο ακριβής τύπος του τείχους προστασίας που είναι απαραίτητος, πρέπει πρώτα να κατανοηθεί η φύση των απειλών ασφάλειας που υπάρχουν. Το Διαδίκτυο είναι μία μεγάλη κοινότητα, και όπως σε κάθε κοινότητα υπάρχουν και καλά και κακά στοιχεία. Τα κακά

στοιχεία κυμαίνονται από ανίκανους ξένους που κάνουν ζημιά ακούσια, στους έμπειρους, κακόβουλους χάκερ που εισέρχονται σκόπιμα με επιθέσεις σε εταιρείες που χρησιμοποιούν το Διαδίκτυο, με όπλο επιλογής τους. Γενικά υπάρχουν τρεις τύποι επιθέσεων που θα μπορούσε ενδεχομένως να επηρεάσει την επιχείρηση ή οργανισμό(3Com, 2000):

- Κλοπή πληροφοριών: Κλοπή εμπιστευτικών πληροφοριών, όπως π.χ. αρχεία εργαζομένων, αρχεία πελατών, ή πνευματική ιδιοκτησία της εταιρείας.
- Σαμποτάζ πληροφοριών: Αλλαγή πληροφοριών σε μια προσπάθεια βλάβης της φήμης ενός ατόμου ή μιας εταιρείας, όπως η αλλαγή υπαλληλικών ιατρικών ή εκπαιδευτικών αρχείων ή μεταφόρτωση υποτιμητικού περιεχομένου στην ιστοσελίδα τους.
- Άρνηση υπηρεσίας (*DoS*): Οι νόμιμοι χρήστες δε μπορούν να έχουν πρόσβαση σε υπηρεσίες, ή στις κανονικές λειτουργίες όπως πχ εμποδίζεται η παραγωγή προσπάθειας για απόκτηση πρόσβασης. Ένας χάκερ μπορεί να επιχειρήσει να αποκτήσει πρόσβαση για ευχαρίστηση ή απληστία. Μια προσπάθεια να κερδηθεί η πρόσβαση συνήθως ξεκινά με τη συγκέντρωση πληροφοριών για το δίκτυο. Αργότερα οι επιθέσεις χρησιμοποιούν αυτές τις πληροφορίες για να επιτύχουν τον πραγματικό τους σκοπό - να κλέψουν ή να καταστρέψουν δεδομένα. Ένας χάκερ μπορεί να χρησιμοποιήσει σαρωτή θύρας, ένα λογισμικό που μπορεί να χαρτογραφήσει ένα δίκτυο. Τότε είναι δυνατό να μάθει πώς είναι δομημένο το δίκτυο και τι λογισμικό τρέχει σε αυτό. Μόλις ο χάκερ έχει μια εικόνα του δικτύου, μπορεί να εκμεταλλευτεί γνωστές αδυναμίες του λογισμικού και χρησιμοποιώντας εργαλεία hacking να προκαλέσει όλεθρο. Είναι ακόμη δυνατό να μπεί στα αρχεία του διαχειριστή και να σβήσει τους δίσκους, αν και συνήθως ένας καλός κωδικός πρόσβασης ματαιώνει αυτήν την προσπάθεια.

Επιθέσεις άρνησης υπηρεσίας

Οι επιθέσεις *DoS* είναι καθαρά κακόβουλες. Δεν έχουν κανένα κέρδος για τους χάκερ εκτός από τη «χαρά» της απόδοσης του δικτύου ή τμημάτων αυτού, μη διαθέσιμα για νόμιμη χρήση. Οι επιθέσεις αυτές υπερφορτώνουν ένα σύστημα έτσι ώστε αυτό να μην είναι διαθέσιμο και αρνούνται την ικανότητα χρήσης των υπηρεσιών του δικτύου. Για την υπερφόρτωση του συστήματος, στέλνει συνεχόμενα ο χάκερ πολύ μεγάλα πακέτα δεδομένων ή προγραμμάτων που απαιτούν απόκριση του συστήματος με τη χρήση ψεύτικης εντολής. Για να ξεκινήσει μια

επίθεση *DoS*, ένας χάκερ πρέπει γνωρίζει τη διεύθυνση *IP* της μηχανής στόχου. Ένα καλό τείχος προστασίας δεν θα αποκαλύψει τη δική του διεύθυνση *IP* ή τις *IP* διευθύνσεις στο *LAN*. Ο χάκερ μπορεί να νομίζει ότι έχει έρθει σε επαφή με το δίκτυο όταν έχει επικοινωνήσει μόνο με το τείχος προστασίας - και δεν μπορεί να κλειδώσει το δίκτυο από εκεί. Επί πλέον, όταν ένας χάκερ εξαπολύσει επίθεση, ορισμένα τείχη προστασίας μπορούν να προσδιορίσουν τα εισερχόμενα δεδομένα ως επίθεση, να απορρίψουν τα δεδομένα, να ειδοποιήσουν τον διαχειριστή του συστήματος και να παρακολουθήσουν τα δεδομένα πίσω στον αποστολέα, ο οποίος μπορεί στη συνέχεια να συλληφθεί (3Com, 2000).

7.4 Τεχνικές εντοπισμού

Τεχνικές ανίχνευσης *Ransomware*

Μηχανική μάθηση

Η μηχανική μάθηση (*ML*) περιλαμβάνει την εκμάθηση των προτύπων δεδομένων για τη δημιουργία ενός μοντέλου. Αυτό το μοντέλο μπορεί στη συνέχεια να προβλέψει το αποτέλεσμα όταν τροφοδοτείται με νέα δεδομένα (Cybersecurity, 2021). Ωστόσο, η δυσκολία στη χρήση του ML είναι στην εύρεση του σωστού αλγορίθμου, να ταιριάζει με τον τύπο δεδομένων και το απαραίτητο αποτέλεσμα.

- Πλεονεκτήματα : Το πλεονέκτημα του *ML* είναι ότι μπορεί να προβλέψει με ακρίβεια το αποτέλεσμα με επαρκή δεδομένα κατάρτισης. Τα δεδομένα εκπαίδευσης πρέπει να ποικίλλουν με ισορροπημένη κατανομή των αποτελεσμάτων που προβλέφθηκαν. Επειδή το *ML* περιλαμβάνει την εκμάθηση του μοτίβου στα δεδομένα, είναι λιγότερο επιρρεπή σε συσκότιση.
- Μειονεκτήματα : Η εύρεση του σωστού αλγορίθμου συχνά δεν είναι απλή και μπορεί να απαιτήσει κάποιες δοκιμές και λάθη. Εξάλλου, μπορεί να προκύψει προκατάληψη και υπερπροσαρμογή εάν δεν έχει ληφθεί επαρκής προσοχή.

Honeypot

Το *Honeypot* περιλαμβάνει τη δημιουργία αρχείων παραπλάνησης για τη *ransomware* επίθεση. Μόλις έχει πρόσβαση σε αυτά τα αρχεία, το *ransomware* μπορεί να αναγνωριστεί.

- Πλεονεκτήματα : Οι παγίδες ή τα αρχεία *honeypot* μπορούν να ρυθμιστούν και, στη συνέχεια, απλά υπάρχει η αναμονή της επίθεσης. Επομένως, η ισχύουσα τεχνική δεν απαιτεί μεγάλη ισχύ συντήρησης ή επεξεργασίας από το σύστημα.
- Μειονεκτήματα : Δεν υπάρχει καμία εγγύηση ότι τα αρχεία *honeypot* θα δεχθούν επίθεση από *ransomware*. Ως εκ τούτου, είναι σημαντικό να γνωρίζουν τα χαρακτηριστικά των αρχείων που θα κάνει τη *ransomware* επίθεση.

Στατιστική

Τα στατιστικά μπορούν να χρησιμοποιηθούν για την καλύτερη ανάλυση των *ransomwares* και την κατανόηση των σημαντικών χαρακτηριστικών τους.

Τεχνητή Νοημοσύνη και ανίχνευση εισβολέων

Η τεχνητή νοημοσύνη (που ονομάζεται επίσης μηχανική νοημοσύνη) εμφανίστηκε ως ερευνητικός κλάδος στο *Summer Research Project of Dartmouth College* τον Ιούλιο του 1956. Η τεχνητή νοημοσύνη μπορεί να περιγραφεί με δύο τρόπους: ως επιστήμη που στοχεύει στην ανακάλυψη της ουσίας της ευφυΐας και στην ανάπτυξη ευφυών μηχανών ή ως επιστήμη εύρεσης μεθόδων για την επίλυση σύνθετων προβλημάτων που δεν μπορούν να λυθούν χωρίς εφαρμογή κάποιας ευφυΐας (π.χ. λήψη σωστών αποφάσεων με βάση μεγάλο όγκο δεδομένων). Στην εφαρμογή της τεχνητής νοημοσύνης στην κυβερνοάμυνα, περισσότερο ενδιαφέρον παρουσιάζει ο δεύτερος ορισμός. Το ερευνητικό ενδιαφέρον για την τεχνητή νοημοσύνη περιλαμβάνει τρόπους για τη προσομοίωση μηχανών (υπολογιστές), συμπεριφορά ευφυών ανθρώπων όπως σκέψη, μάθηση, συλλογισμός, προγραμματισμός κ.λπ. (Tyugu E., 2011).

Το γενικό πρόβλημα της προσομοίωσης της νοημοσύνης έχει απλοποιηθεί σε συγκεκριμένα επιμέρους προβλήματα που έχουν ορισμένα χαρακτηριστικά ή δυνατότητες που πρέπει να επιδεικνύει ένα ευφυές σύστημα. Τα ακόλουθα χαρακτηριστικά έχουν λάβει τη μεγαλύτερη προσοχή (Russel J.S., Norvig P., 2003):

- Αφαίρεση, συλλογισμός, επίλυση προβλημάτων (ενσωματωμένοι παράγοντες, νευρωνικά δίκτυα, στατιστικά προσεγγίσεις στην τεχνητή νοημοσύνη).

- Αναπαράσταση γνώσεων (οντολογίες).
- Προγραμματισμός (προγραμματισμός και συνεργασία πολλών πρακτόρων).
- Μάθηση (μηχανική μάθηση).
- Επεξεργασία φυσικής γλώσσας (ανάκτηση πληροφοριών - εξόρυξη κειμένου, αυτόματη μετάφραση).
- Κίνηση και χειρισμός (πλοήγηση, εντοπισμός, χαρτογράφηση, σχεδιασμός κίνησης).
- Αντίληψη (αναγνώριση ομιλίας, προσώπου, αναγνώριση, αναγνώριση αντικειμένου) ·
- Κοινωνική Νοημοσύνη (προσομοίωση ενσυναίσθησης).
- Δημιουργικότητα (τεχνητή διαίσθηση, τεχνητή φαντασία). και
- Γενική Νοημοσύνη (Ισχυρή Τεχνητή Νοημοσύνη).

Οι κλασικές προσεγγίσεις της τεχνητής νοημοσύνης επικεντρώνονται στην ατομική ανθρώπινη συμπεριφορά, στην αναπαράσταση της γνώσης και μεθόδους συμπεράσματος. Η Διανεμημένη Τεχνητή Νοημοσύνη (*DAI*), από την άλλη πλευρά, επικεντρώνεται στην κοινωνική συμπεριφορά, δηλαδή συνεργασία, αλληλεπίδραση και ανταλλαγή γνώσεων μεταξύ διαφορετικών μονάδων (παραγόντων). Η διαδικασία εξεύρεσης λύσης σε κατανεμημένα προβλήματα επίλυσης βασίζεται στην ανταλλαγή γνώσεων το πρόβλημα και τη συνεργασία μεταξύ των πρακτόρων. Ένας πράκτορας είναι μια αυτόνομη γνωστική οντότητα που καταλαβαίνει το περιβάλλον του, δηλαδή μπορεί να λειτουργήσει από μόνο του και έχει ένα εσωτερικό σύστημα λήψης αποφάσεων που δρα παγκοσμίως σε άλλους πράκτορες.

Σε συστήματα πολλαπλών πρακτόρων, μια ομάδα κινητών αυτόνομων παραγόντων συνεργάζεται με συντονισμένο και έξυπνο τρόπο για να λύσουν ένα συγκεκριμένο πρόβλημα ή τάξεις προβλημάτων. Είναι κάπως ικανοί να κατανοήσουν το περιβάλλον τους, να πάρουν αποφάσεις και επικοινωνία με άλλους πράκτορες (Helano J., Nogueira M., 2006). Τα συστήματα ευφυών παραγόντων είναι μόνο ένα μέρος μιας πολύ μεγαλύτερης προσέγγισης *AI* που ονομάζεται Υπολογιστική Νοημοσύνη (*CI*). Η *CI* περιλαμβάνει αρκετές άλλες τεχνικές εμπνευσμένες από τη φύση, όπως νευρωνικά δίκτυα, ασαφή λογική, εξελικτικό υπολογισμός, νοημοσύνη σμήνους, μηχανική μάθηση και τεχνητά ανοσοποιητικά συστήματα. Αυτές οι τεχνικές παρέχουν ευέλικτους μηχανισμούς λήψης αποφάσεων για δυναμικά περιβάλλοντα όπως εφαρμογές ασφάλειας στον κυβερνοχώρο.

Η έννοια «εμπνευσμένη από τη φύση», σημαίνει οτι υπάρχει ένα αυξανόμενο ενδιαφέρον στον τομέα των υπολογιστικών τεχνολογιών για να μιμηθούν βιολογικά συστήματα (όπως το βιολογικό ανοσοποιητικό σύστημα) και τις αξιοσημείωτες ικανότητές τους να μαθαίνουν, να απομνημονεύουν, να αναγνωρίζουν να ταξινομούν και να επεξεργάζονται πληροφορίες. Το τεχνητό ανοσοποιητικό σύστημα (*AIS*) είναι ένα τέτοιο παράδειγμα τεχνολογίας (Dasgupta D., 2006). Παρέχουν ισχυρές, προσαρμοστικές και βέλτιστες λύσεις ακόμη και για πολύπλοκα υπολογιστικά προβλήματα. Μπορούν να χρησιμοποιηθούν για τη δημιουργία κανόνων για την ταξινόμηση των επιθέσεων ασφαλείας και τη δημιουργία συγκεκριμένων κανόνων για διαφορετικές επιθέσεις ασφαλείας σε *IDS* (Alrajeh N.A., Lloret J., 2013).

Έχουν αναπτυχθεί πολλές μέθοδοι για την ασφάλεια δεδομένων μέσω δικτύων και Διαδικτύου (π.χ. λογισμικό προστασίας από ιούς, τείχος προστασίας, κρυπτογράφηση, ασφαλή πρωτόκολλα κ.λπ.). Ωστόσο, οι αντίπαλοι μπορούν πάντα να βρουν νέους τρόπους επίθεσης σε συστήματα δικτύου.

Το σύστημα ανίχνευσης και πρόληψης εισβολών (*IDPS*) είναι ένα λογισμικό ή συσκευή υλικού τοποθετημένη μέσα στο δίκτυο, το οποίο μπορεί να ανιχνεύσει πιθανές εισβολές προσπαθώντας ταυτόχρονα να τις αποτρέψει. Οι *IDPS* παρέχουν τέσσερις ζωτικές λειτουργίες ασφάλειας: παρακολούθηση, ανίχνευση, ανάλυση και ανταπόκριση σε μη εξουσιοδοτημένες δραστηριότητες (Kaliyamurthie K.P., Suresh R.M., 2012)

Επιθυμητά Χαρακτηριστικά ενός *IDPS*

Ένας *IDPS* θα πρέπει να έχει ορισμένα χαρακτηριστικά για να μπορεί να παρέχει αποτελεσματική ασφάλεια έναντι σοβαρών επιθέσεων. Τα χαρακτηριστικά αυτά περιλαμβάνουν τα ακόλουθα (Patel A., 2010):

- Ανίχνευση εισβολής σε πραγματικό χρόνο-ενώ η επίθεση βρίσκεται σε εξέλιξη ή αμέσως μετά.
- Οι ψευδώς θετικοί συναγερμοί πρέπει να ελαχιστοποιηθούν,
- Η ανθρώπινη επίβλεψη πρέπει να μειωθεί στο ελάχιστο και να συνεχιστεί η εξασφαλισμένη λειτουργία

- Ανακτήσιμη από συντριβές συστήματος, είτε τυχαία είτε αυτά που προκύπτουν από επιθέσεις,
- Ικανότητα αυτοπαρακολούθησης προκειμένου να εντοπιστούν οι προσπάθειες των επιτιθέμενων να αλλάξουν το σύστημα,
- Συμμόρφωση με τις πολιτικές ασφαλείας του συστήματος που παρακολουθείται και
- Προσαρμογή στις αλλαγές του συστήματος και τη συμπεριφορά του χρήστη με την πάροδο του χρόνου.

Τα τεχνητά νευρωνικά δίκτυα (*ANN*) αποτελούνται από τεχνητούς νευρώνες που μπορούν να μάθουν και να λύσουν προβλήματα όταν συνδυάζονται μαζί. Νευρωνικά δίκτυα που έχουν ικανότητα μάθησης, επεξεργάζονται κατανεμημένες πληροφορίες, αυτο-οργάνωση και προσαρμογή, εφαρμόζονται στην επίλυση προβλημάτων που απαιτούν εξέταση προϋποθέσεων, ανακρίβεια και ασάφεια ταυτόχρονα. Όταν τα νευρωνικά δίκτυα αποτελούνται από ενα μεγάλο αριθμό τεχνητών νευρώνων, μπορούν να παρέχουν μια λειτουργικότητα μαζικής παράλληλης μάθησης και τη λήψη αποφάσεων με μεγάλη ταχύτητα, γεγονός που τα καθιστά κατάλληλα για μοτίβο εκμάθησης αναγνώρισης, ταξινόμησης και επιλογής απαντήσεων σε επιθέσεις (Wang X.B. et al., 2008).

7.5 Εκπαίδευση προσωπικού σχετικά με τις κυβερνοεπιθέσεις

Καθοριστική για οποιαδήποτε μετριαστική ενέργεια είναι η επένδυση σε σύγχρονες υποδομές πληροφορικής με αποτελεσματική διαχείριση επιδιορθώσεων και προστασία από κακόβουλο λογισμικό στην υγειονομική περίθαλψη (Cybersecurity, 2021). Παράλληλα, τα ιδρύματα θα πρέπει να διασφαλίζουν ότι όλο το προσωπικό γνωρίζει τις συνήθεις κυβερνοεπιθέσεις συμπεριλαμβανομένων

- Την παραπλάνηση των θυμάτων στη λήψη κακόβουλων εφαρμογών,
- ηλεκτρονικά μηνύματα ηλεκτρονικού "ψαρέματος" μεταμφιεσμένα ως επίσημες ενημερώσεις εστίας που αποσπούν κακόβουλο λογισμικό μέσω συνημμένων ή συνδέσμων και
- ενσωματωμένο λογισμικό υποκλοπής spyware ή κακόβουλο λογισμικό σε δημόσια διαθέσιμους διαδραστικούς χάρτες και ιστοσελίδες (Cybersecurity, 2021).

Δεύτερον, η καλή «κυβερνο-υγιεινή» πρέπει να ενσωματωθεί στα καθημερινά πρότυπα εργασίας του προσωπικού. Αυτό περιλαμβάνει;

- ➔ χρήση ισχυρών κωδικών πρόσβασης,
- ➔ αποφυγή ανοίγματος άγνωστων emails και συνδέσμων,
- ➔ ενεργοποίηση της προστασίας από τείχη προστασίας στην εργασία και το σπίτι, και
- ➔ παροχή αποτελεσματικής εκπαίδευσης προσωπικού (Information Security Instiute, 2021).

Τα ιδρύματα υγειονομικής περίθαλψης πρέπει να γνωρίζουν ότι αντιμετωπίζουν πρόσθετους κινδύνους στο πλαίσιο οποιασδήποτε κυβερνοεπίθεσης και να διασφαλίσουν ότι υπάρχει κατάλληλη διαχείριση (Information Security Instiute, 2021). Υποεπενδύσεις στην κυβερνοασφάλεια στα ιδρύματα υγειονομικής περίθαλψης σημαίνει ότι ορισμένα είναι ιδιαίτερα ευάλωτα στις επιθέσεις *ransomware*, ιδιαίτερα κατά τη διάρκεια της πανδημίας *COVID-19*. Οι εγκληματίες στον κυβερνοχώρο μπορούν να κλείσουν συσκευές, διακομιστές ή ολόκληρα δίκτυα και απαιτούν λύτρα για να διορθώσουν την κρυπτογράφηση. Αυτό μπορεί να προκαλέσει παραβίαση των αρχείων ασθενών, απεικονιστικών και χειρουργικών υπηρεσιών, ιατρικών συσκευών και συστημάτων ραντεβού.

Τα ιδρύματα υγειονομικής περίθαλψης πρέπει να θυμούνται ότι οποιαδήποτε παραβίαση της ασφάλειας στον κυβερνοχώρο μπορεί να οδηγήσει σε αποκάλυψη προσωπικών ιατρικών πληροφοριών και μπορεί να διακόψουν σοβαρά τις κλινικές υπηρεσίες, συμπεριλαμβανομένης της περίθαλψης έκτακτης ανάγκης ή της σωτήριας ζωής, που μπορεί ενδεχομένως να οδηγήσει σε απώλεια της ζωής. Τα ιδρύματα θα πρέπει να είναι προετοιμασμένα να χειρίζονται τις βραχυπρόθεσμες και μακροπρόθεσμες επιπτώσεις κάθε επίθεσης, έχοντας υπόψη τις οικονομικές και νομικές επιπτώσεις, και πρέπει να έχουν ισχυρά σχέδια επιχειρηματικής συνέχειας.

Παράλληλα, θα πρέπει να δημιουργήσουν μια «κουλτούρα ασφάλειας» μεταξύ του προσωπικού διασφαλίζοντας εκπαίδευση στον κυβερνοχώρο για όλους τους εργαζόμενους. Μία άριστα εκπαιδευμένη και ανταποκρινόμενη ομάδα ασφάλειας στον κυβερνοχώρο θα πρέπει να είναι άμεσα διαθέσιμη, και οι οργανισμοί πρέπει να διασφαλίζουν σχολαστικό έλεγχο του ποιος έχει πρόσβαση στα συστήματα μητρώου υγείας. Όλες οι κινητές συσκευές που περιέχουν προσωπικές ιατρικές πληροφορίες πρέπει να προστατεύονται με κρυπτογράφηση και το

λογισμικό δεν πρέπει να εγκατασταθεί από το προσωπικό χωρίς προηγούμενη συγκατάθεση. Για το προσωπικό που εργάζεται σε απομακρυσμένες συσκευές θα πρέπει να είναι δυνατή η σύνδεση σε ένα εικονικό ιδιωτικό δίκτυο (VPN) για τη διατήρηση μιας ασφαλούς σύνδεσης χωρίς ασφάλεια υποδομής διαδικτύου (Bhuyan SS. et al., 2020)

8. Σημερινή κατάσταση στον τομέα της κυβερνοασφάλειας στην υγεία

8.1 Υγεία και Internet of Things

Η καινοτομία σε πολυάριθμες τεχνολογίες *IoT* οδήγησε στην αποκέντρωση των μηχανισμών υγειονομικής περίθαλψης από παραδοσιακούς σε ένα συνηθισμένο τοπικό φόρουμ μέσω της βοήθειας των *gadgets* εξουσιοδοτημένων από το *IoT*. Αυτά τα *gadget* βασίζονται στην ιδέα ενός πλαισίου πολλαπλών αισθητήρων για την καταγραφή διαφόρων παραμέτρων. Αυτές περιλαμβάνουν την καταγραφή του σακχάρου στο αίμα, το ΗΚΓ (ηλεκτροκαρδιογράφημα), τον παλμό, τη θερμοκρασία του ασθενούς κ.λ.π.. Αυτή η προσαρμογή υποστηρίζει την έννοια της απομακρυσμένης παρακολούθησης της υγείας, η οποία περιλαμβάνει κυρίως φαρμακευτική αγωγή στο σπίτι, φροντίδα ηλικιωμένων ή οποιοδήποτε πρόγραμμα γυμναστικής (Fazeldehkordi E., Owe O., Noll J., 2019; Singh I., Kumar D., 2019; Lavanya S., Divyabharthi J., 2017).

Η υγειονομική περίθαλψη στο IoT περιλαμβάνει κυρίως τέσσερις βασικές οντότητες, οι οποίες είναι οι φορείς, οι αισθητήρες, τα δίκτυα επικοινωνίας και οι εφαρμογές. Οι τομείς περιλαμβάνουν ασθενείς, κλινικό προσωπικό που περιλαμβάνει γιατρούς, νοσηλευτές, ειδικούς. Οι αισθητήρες χρησιμοποιούνται για να ενημερώνουν τους τομείς με βασικές απαιτήσεις και στη συνέχεια να αποστέλλουν τις πληροφορίες μέσω ενός κατάλληλου δικτύου επικοινωνίας (Bangotra DK. et al., 2020). Υπάρχουν άφθονες συσκευές που κυριαρχούν για την ανάγνωση και την παρακολούθηση ζωτικών δεδομένων ασθενών και άλλων ιατρικών στατιστικών. Αυτές οι συσκευές κυμαίνονται από έξυπνες φορητές όπως έξυπνες ζώνες, ρολόγια, παπούτσια έως έξυπνες βιντεοκάμερες και μετρητές. Οι εφαρμογές βοηθούν με ειδοποιήσεις σε πραγματικό χρόνο, βοηθώντας έτσι σε κάθε υπηρεσία έκτακτης ανάγκης.

Η παρακολούθηση σε πραγματικό χρόνο των δεδομένων που παράγονται από έξυπνες συσκευές και η μετάδοσή τους στο οικοσύστημα είναι πολύ κρίσιμη για την ευφυή λήψη αποφάσεων. Αυτά τα ευφυή συστήματα λειτουργούν αυτόνομα χωρίς ανθρώπινη παρέμβαση και

η απόφαση σχετικά με τον μετριασμό μιας συγκεκριμένης απειλής λαμβάνεται σε πραγματικό χρόνο μετά την προσαρμογή στις περιβαλλοντικές αλλαγές. Οι αισθητήρες χρησιμοποιούνται για την ανάγνωση των δεδομένων του ασθενούς και συνδέονται με τους μικροεπεξεργαστές. Αυτοί οι μικροεπεξεργαστές συνδέονται περαιτέρω με οποιαδήποτε τεχνολογία ασύρματης επικοινωνίας για τη δρομολόγηση και την προώθηση των δεδομένων μέσω της πύλης. Τα δεδομένα αποθηκεύονται στις εικονικές μηχανές που είναι δημοφιλείς ως *clouds* για προεπεξεργασία και ανάλυση. Αυτά τα δεδομένα μπορούν να έχουν πρόσβαση από γιατρούς, ειδικούς, ακόμη και ασθενείς.

Ωστόσο, απαιτείται ένας κατάλληλος μηχανισμός ασφαλείας για την αποφυγή κάθε είδους ζημιάς από τους αντιπάλους. Διάφορες αρχιτεκτονικές *IoT* έχουν προχωρήσει τα τελευταία χρόνια. Δίνονται μερικές από τις εξέχουσες αυτές αρχιτεκτονικές. Για παράδειγμα, το *mHealth* είναι ένα σύστημα πρωτοβάθμιας φροντίδας υγείας με δομή τριών στρωμάτων. Τα επίπεδα περιλαμβάνουν ένα επίπεδο συλλογής δεδομένων ακολουθούμενο από ένα επίπεδο αποθήκευσης δεδομένων, το οποίο προβλέπει την αποθήκευση των δεδομένων στα ράφια στοίβας και ένα επίπεδο επεξεργασίας δεδομένων για σωστή επιθεώρηση και σάρωση τους (Kumar N., 2017). Επιπλέον, το *Lowpan* αποτελείται από πολλά σημεία πρόσβασης με δυνατότητες προώθησης και δρομολόγησης. Οι αναπτυγμένοι κόμβοι αισθητήρων, μαζί με τα σημεία πρόσβασης, οδηγούν στο σχηματισμό συμπλεγμάτων. Η σύνδεση επιτυγχάνεται μέσω της βοήθειας του *IPV6*.

Αυτή η προσέγγιση προτιμάται από άλλες λόγω των χαμηλών ενεργειακών απαιτήσεών της, γεγονός που την καθιστά κατάλληλη για τον αισθητήρα με μπαταρία. Οι Gao et al. (Tokognon et al., 2017) συζήτησαν για ένα δομικό σύστημα παρακολούθησης της υγείας με βάση το *Zigbee*. Η επανάσταση στο *WSN* επιτρέπει σε πολλούς κόμβους αισθητήρων να επικοινωνούν ασύρματα με τον σταθμό βάσης. Για να αυξηθεί η διάρκεια ζωής του δικτύου, είναι απαραίτητο ένα κανάλι επικοινωνίας χαμηλής ενέργειας. Αυτό οδήγησε στο *Zigbee injection* για επικοινωνία στο σύστημα παρακολούθησης της υγείας. Παρά τα πολλά οφέλη, αυτός ο τομέας της τεχνολογίας υποφέρει από διάφορα κενά.

Παρά τα πολυάριθμα οφέλη, όπως καλύτερη διάγνωση, θεραπεία και άλλες εγκαταστάσεις, η έξυπνη και πανταχού παρούσα φύση το εκθέτει σε πολλαπλές κυβερνοαπειλές. Η κυβερνοασφάλεια στον τομέα της υγειονομικής περίθαλψης βρίσκεται σε αρχικό στάδιο και συνεπώς απαιτεί προληπτικές και βελτιωμένες τεχνολογίες για την προστασία της από διάφορες

επιθέσεις. Η κατανόηση των διαφορετικών προκλήσεων ασφαλείας είναι απαραίτητη πριν αντιμετωπιστούν άλλες επιπλοκές της. Υπάρχουν πολλές προκλήσεις και ζητήματα για τις σύγχρονες εφαρμογές υγειονομικής περίθαλψης. Η εκπομπή της επικοινωνίας στην υγειονομική περίθαλψη οδηγεί στην εκμετάλλευση της ιδιωτικής ζωής των ασθενών, δημιουργώντας έτσι πλατφόρμες για σοβαρές απειλές όπως η υποκλοπή. Αυτή η πτυχή, με τη σειρά της, οδηγεί στην εκμετάλλευση του απορρήτου των δεδομένων (Alromaihi S., Elmedany W., Balakrishna C., 2018).

Επιπλέον, οποιαδήποτε αλλαγή στα δεδομένα που λαμβάνονται από τους αισθητήρες μπορεί να είναι απειλητική για τη ζωή στην περίπτωση εφαρμογών υγειονομικής περίθαλψης. Επομένως, η ακεραιότητα και ο έλεγχος ταυτότητας είναι οι δύο κύριες ανησυχίες εδώ. Επιπλέον, ο συγγραφέας στο (Poorejbari S., Mansoon W.,, 2019) απεικονίζει πώς μπορούν να διαταραχθούν και να παραβιαστούν οι υπηρεσίες έκτακτης ανάγκης εξαιτίας της έλλειψης μιας ενιαίας υποδομής που βασίζεται στο *cloud*, όπου θα μπορούν να έχουν πρόσβαση σε όλα τα αρχεία ηλεκτρονικής υγείας. Περαιτέρω παραβιάσεις ασφαλείας στην αποθήκευση *cloud* μπορούν να επιδεινώσουν την κατάσταση.

Για να αντιμετωπιστούν τα προαναφερθέντα ελαττώματα, απαιτούνται καλύτερα και βελτιωμένα πλαίσια ασφαλείας που απαιτούν τη συγχώνευση της μηχανικής μάθησης σε αυτόν τον τομέα. Αυτό το εργαλείο τεχνητής νοημοσύνης μπορεί να λύσει πολλές υποθέσεις και ζητήματα που σχετίζονται με την ασφάλεια ενεργώντας ως ανιχνευτής ανωμαλιών. Οι Newaz et al. (Newaz et al., 2019) πρότειναν την εφαρμογή του υγειονομικού φρουρού: ένα πλαίσιο εφαρμογής ασφάλειας που βασίζεται σε *ML* για συστήματα υγειονομικής περίθαλψης. Αυτό το πλαίσιο αξιοποίησε πολλούς αλγόριθμους *ML* (*KNN, Random Forest, DT, ANN*) για τον εντοπισμό κακόβουλης δραστηριότητας και μπόρεσε να επιτύχει ακρίβεια 91%.

Το πλαίσιο μπορεί να ενσωματώνει και να παρατηρεί συσχετίσεις μεταξύ πολλαπλών λειτουργιών του σώματος και άλλων κρίσιμων σημείων. Η δομή δοκιμάστηκε έναντι απειλών που περιλάμβαναν σφραγισμένες ιατρικές συσκευές, *DOS* και άλλα ψευδή δεδομένα. Για περαιτέρω αύξηση της ασφάλειας, διεξήγθηκε έρευνα για τον συνδυασμό του *ML* με την τεχνολογία *blockchain*. Οι Tanwar et al. (Tanwar S. et al., 2020) πρότειναν τη χρήση του *ML* στο *blockchain* για να αυτοσχεδιάσει την ασφάλεια και την ιδιωτικότητα των δεδομένων. Η αρχιτεκτονική προτάθηκε με την ενσωμάτωση του *blockchain* με το *ML*. Το μαθησιακό

δυναμικό του *ML* σε συνδυασμό με την τεχνολογία *blockchain,* όχι μόνο θα το κάνει πιο έξυπνο αλλά και θα μειώσει πολλά ζητήματα που αφορούν τα δεδομένα στο *IoT* (Gupta R., Reebadiya D., Tanwar S., 2021; Gupta R., Nair A., Tanwae S., Kumar N., 2021; Gupta R. et al., 2019; Gupta R et al., 2020).

Η αποκέντρωση, η διαφάνεια και το αμετάβλητο είναι οι πρωταρχικοί στόχοι της τεχνολογίας *blockchain*, οι οποίοι συμβάλλουν στη βελτίωση της ασφάλειας του συστήματος (Mehta P., Gupta R., Tanwar S., 2020; Gupta R., Kumari A., Tanwar S., 2020). Αυτός ο συνδυασμός θα οδηγήσει σε σωστές προβλέψεις και καλύτερη ασφάλεια. Επιπλέον, οι Nilima et al. (Pardakhe N.V., Deshmukh V.M., 2019) υποστήριξαν περαιτέρω ότι η χρήση του *ML* με *blockchain* θα κάνει το σύστημα πιο έξυπνο ώστε να αντιμετωπίζει θέματα απορρήτου, ακεραιότητας και ελέγχου ταυτότητας.

8.2 Συνοπτική έκθεση κυβερνοασφάλειας ενός ιδιωτικού χώρου υγείας

Οι επαγγελματίες ασφαλείας είναι ομόφωνοι: Ο πιο αδύναμος κρίκος σε οποιοδήποτε σύστημα υπολογιστή είναι ο χρήστης. Οι ερευνητές που μελετούν την ψυχολογία και την κοινωνιολογία των χρηστών της Τεχνολογίας της Πληροφορίας (ΤΠ) έχουν αποδείξει ξανά και ξανά πόσο πολύ δύσκολο είναι να ευαισθητοποιηθούν οι άνθρωποι σχετικά με απειλές και ευπάθειες που μπορεί να θέσουν σε κίνδυνο τις πληροφορίες με τις οποίες εργάζονται καθημερινά. Κανένα από τα μέτρα που παρουσιάζονται δεν μπορεί να είναι αποτελεσματικό εκτός εάν η πρακτική υγειονομικής περίθαλψης είναι πρόθυμη και ικανή να τα εφαρμόσει, να επιβάλει πολιτικές που απαιτούν τη χρήση αυτών των εγγυήσεων και να εκπαιδεύσει αποτελεσματικά και προληπτικά όλους τους χρήστες έτσι ώστε να ευαισθητοποιηθούν στη σημασία της ασφάλειας των πληροφοριών.

Εν ολίγοις, κάθε πρακτική υγειονομικής περίθαλψης πρέπει να ενσταλάζει και να υποστηρίζει μια οργανωτική κουλτούρα με γνώμονα την ασφάλεια. Μία από τις πιο δύσκολες πτυχές της ενστάλαξης της ασφάλειας στους χρήστες είναι η υπέρβαση της αντίληψης ότι "δεν μπορεί να συμβεί σε μένα". Οι άνθρωποι, ανεξάρτητα από το επίπεδο εκπαίδευσης ή την πολυπλοκότητά τους, πιστεύουν ότι «δεν θα υποκύψουν ποτέ σε ατημέλητες πρακτικές ή σε πληροφορίες για τον ασθενή σε κίνδυνο. Αυτό συμβαίνει μόνο σε άλλους ανθρώπους » (Healthit, 2019a).

Ακολουθώντας ένα σύνολο προδιαγεγραμμένων πρακτικών και ελέγχοντάς τα κάθε φορά, μπορεί να αποφευχθούν τουλάχιστον μερικά από τα λάθη που οφείλονται σε υπερβολική εμπιστοσύνη. Οι λίστες ελέγχου από μόνες τους δεν είναι αρκετές. Είναι υποχρέωση οποιουδήποτε οργανισμού όπου διακυβεύονται ζωές να υποστηρίζει την κατάλληλη ασφάλεια πληροφοριών μέσω της καθιέρωσης μιας κουλτούρας ασφάλειας. Κάθε άτομο στον οργανισμό πρέπει να εγγραφεί σε ένα κοινό όραμα για την ασφάλεια των πληροφοριών, έτσι ώστε οι συνήθειες και οι πρακτικές να είναι αυτόματες.

Οι πρακτικές ασφάλειας πρέπει να είναι ενσωματωμένες και όχι αγκιστρωμένες. Καμία λίστα ελέγχου δεν μπορεί να περιγράψει επαρκώς όλα όσα πρέπει να γίνουν για να δημιουργηθεί η κουλτούρα ασφάλειας ενός οργανισμού, αλλά υπάρχουν ορισμένα προφανή βήματα που πρέπει να γίνουν (Healthit, 2019a):

- Η εκπαίδευση και η κατάρτιση πρέπει να είναι συχνές και συνεχείς.
- Αυτοί που διαχειρίζονται και κατευθύνουν το έργο των άλλων πρέπει να δώσουν ένα καλό παράδειγμα και να αντισταθούν στον πειρασμό να επιδοθούν στον εξαιρετισμό.
- Η λογοδοσία και η ανάληψη ευθύνης για την ασφάλεια των πληροφοριών πρέπει να είναι μεταξύ των βασικών αξιών του οργανισμού.

Η προστασία των ασθενών μέσω ορθών πρακτικών για την ασφάλεια των πληροφοριών θα πρέπει να είναι η δεύτερη φύση του οργανισμού υγειονομικής περίθαλψης, όπως οι υγειονομικές πρακτικές.

- Προστασία κινητών συσκευών : Οι φορητές συσκευές - φορητοί υπολογιστές, *smartphone*, φορητά μέσα αποθήκευσης - έχουν ανοίξει έναν κόσμο ευκαιριών για την αποδέσμευση των Ηλεκτρονικών Αρχείων Υγείας (*EHR*) από την επιφάνεια εργασίας. Αλλά αυτές οι ευκαιρίες παρουσιάζουν επίσης απειλές για την ιδιωτικότητα και την ασφάλεια των πληροφοριών. Ορισμένες από αυτές τις απειλές επικαλύπτονται εκείνες του επιτραπέζιου κόσμου, άλλες όμως είναι μοναδικές για φορητές συσκευές (Healthit, 2019a).
- Καλές συνήθειες στη χρήση υπολογιστών : Ο ιατρός είναι εξοικειωμένος με τη σημασία των υγιεινών συνηθειών για τη διατήρηση της καλής υγείας και τη μείωση του κινδύνου μόλυνσης και ασθενειών. Το ίδιο ισχύει για τα συστήματα πληροφορικής, συμπεριλαμβανομένων των συστημάτων *EHR* - πρέπει να συντηρούνται σωστά, ώστε να

συνεχίσουν να λειτουργούν σωστά και αξιόπιστα με τρόπο που να σέβεται τη σημασία και την ευαίσθητη φύση των πληροφοριών που αποθηκεύονται μαζί τους. Όπως συμβαίνει με κάθε θεραπευτικό σχήμα υγείας, τα απλά μέτρα προχωρούν πολύ (Healthit, 2019b).

- Χρήση τείχους προστασίας : Εκτός εάν μια μικρή πρακτική χρησιμοποιεί ένα σύστημα *EHR* που είναι εντελώς αποσυνδεδεμένο από το Διαδίκτυο, θα πρέπει να διαθέτει τείχος προστασίας για προστασία από εισβολές και απειλές από εξωτερικές πηγές. Ενώ το λογισμικό προστασίας από ιούς θα βοηθήσει στην εύρεση και την καταστροφή κακόβουλου λογισμικού που έχει ήδη εισέλθει, η δουλειά ενός τείχους προστασίας είναι να αποτρέψει τους εισβολείς από την είσοδο. Εν ολίγοις, ο αντι-ιός μπορεί να θεωρηθεί ως έλεγχος μόλυνσης ενώ το τείχος προστασίας έχει το ρόλο της πρόληψης των ασθενειών. Ένα τείχος προστασίας μπορεί να λάβει τη μορφή ενός προϊόντος λογισμικού ή μιας συσκευής υλικού. Σε κάθε περίπτωση, η δουλειά του είναι να επιθεωρεί όλα τα μηνύματα που έρχονται στο σύστημα από έξω (είτε από το Διαδίκτυο είτε από το τοπικό δίκτυο) και να αποφασίζει, σύμφωνα με προκαθορισμένα κριτήρια, εάν πρέπει να επιτρέπεται το μήνυμα (Healthit, 2019c).
- Εγκατάσταση και συντήρηση λογισμικού προστασίας από ιούς : Ο πρωταρχικός τρόπος με τον οποίο οι επιτιθέμενοι συμβιβάζουν τους υπολογιστές είναι μέσω ιών και παρόμοιου κώδικα που εκμεταλλεύεται τρωτά σημεία στο μηχάνημα. Αυτά τα τρωτά σημεία είναι πανταχού παρόντα στη φύση του υπολογιστικού περιβάλλοντος. Ακόμη και ένας υπολογιστής που έχει όλες τις τελευταίες ενημερώσεις ασφαλείας και τις εφαρμογές στο λειτουργικό του σύστημα, μπορεί να εξακολουθεί να κινδυνεύει λόγω των ανιχνευθέντων ελαττωμάτων. Επιπλέον, οι υπολογιστές μπορούν να μολυνθούν από φαινομενικά αθώες εξωτερικές πηγές όπως *CD, email*, μονάδες *flash* και λήψεις ιστού. Ως εκ τούτου, είναι σημαντικό να χρησιμοποιείται ένα προϊόν που παρέχει συνεχώς ενημερωμένη προστασία. Το λογισμικό προστασίας από ιούς είναι ευρέως διαθέσιμο, καλά δοκιμασμένο ως αξιόπιστο και κοστίζει σχετικά λίγο (Healthit, 2019d).
- Σχέδιο για το απρόσμενο : Αργά ή γρήγορα, θα συμβεί το απροσδόκητο. Πυρκαγιά, πλημμύρες, τυφώνες, σεισμοί και άλλες φυσικές καταστροφές μπορούν να χτυπήσουν ανά πάσα στιγμή. Σημαντικά αρχεία υγειονομικής περίθαλψης και άλλα ζωτικά περιουσιακά στοιχεία πρέπει να προστατεύονται από απώλεια από αυτά τα γεγονότα.

Υπάρχουν δύο βασικά μέρη αυτής της πρακτικής: η δημιουργία αντιγράφων ασφαλείας και η ύπαρξη ενός υγιούς σχεδίου αποκατάστασης (Healthit, 2019e).

- Έλεγχος πρόσβασης σε προστατευμένες πληροφορίες υγείας : Για να ελαχιστοποιηθεί ο κίνδυνος για τις ηλεκτρονικές πληροφορίες υγείας κατά την αποτελεσματική εγκατάσταση συστημάτων *EHR*, συζητείται η σημασία των κωδικών πρόσβασης. Ο κωδικός πρόσβασης, ωστόσο, είναι μόνο το ήμισυ του συνόλου των διαπιστευτηρίων ενός χρήστη υπολογιστή. Το άλλο μισό είναι η ταυτότητα του χρήστη ή το όνομα χρήστη. Στα περισσότερα συστήματα υπολογιστών, αυτά τα διαπιστευτήρια (όνομα χρήστη και κωδικός πρόσβασης) χρησιμοποιούνται ως μέρος ενός συστήματος ελέγχου πρόσβασης στο οποίο οι χρήστες έχουν ορισμένα δικαιώματα πρόσβασης στα δεδομένα εντός. Αυτό το σύστημα ελέγχου πρόσβασης ενδέχεται να είναι μέρος ενός λειτουργικού συστήματος (π.χ. Windows) ή να είναι ενσωματωμένο σε μια συγκεκριμένη εφαρμογή (π.χ., μονάδα συνταγογράφησης ane). Συχνά ισχύουν και τα δύο. Σε κάθε περίπτωση, διαμορφώνεται η εφαρμογή *EHR* για να παρέχεται πρόσβαση σε ηλεκτρονικές πληροφορίες υγείας μόνο στα απαραίτητα άτομα (Healthit, 2019f).
- Περιορισμός πρόσβασης στο δίκτυο : Η ευκολία χρήσης και η ευελιξία κάνουν τα σύγχρονα εργαλεία δικτύωσης πολύ ελκυστικά. Οι τεχνολογίες *Web 2.0* όπως η κοινή χρήση αρχείων από ομότιμους χρήστες και τα άμεσα μηνύματα είναι δημοφιλείς και χρησιμοποιούνται ευρέως. Η ασύρματη δρομολόγηση είναι ένας γρήγορος και εύκολος τρόπος για τη δημιουργία ευρυζωνικών δυνατοτήτων εντός σπιτιού ή γραφείου. Ωστόσο, λόγω της ευαισθησίας των πληροφοριών περί υγειονομικής περίθαλψης και του γεγονότος ότι προστατεύονται από τον νόμο, εργαλεία που ενδέχεται να επιτρέψουν στους ξένους να αποκτήσουν πρόσβαση σε ιατρική περίθαλψη, το δίκτυο της πρακτικής πρέπει να χρησιμοποιείται με μεγάλη προσοχή (Healthit, 2019g).
- Έλεγχος φυσικής πρόσβασης : Πρέπει να εξασφαλίζονται περιουσιακά στοιχεία όπως αρχεία και πληροφορίες. Οι ίδιες οι συσκευές που απαρτίζουν ένα σύστημα ΕΑΥ πρέπει επίσης να είναι ασφαλείς από μη εξουσιοδοτημένη πρόσβαση. Ο πιο κοινός τρόπος με τον οποίο τίθενται σε κίνδυνο οι ηλεκτρονικές πληροφορίες υγείας είναι μέσω της απώλειας συσκευών, είτε αυτό συμβαίνει τυχαία είτε μέσω κλοπής. Τα περιστατικά που αναφέρθηκαν στο Γραφείο Πολιτικών Δικαιωμάτων δείχνουν ότι περισσότερο από το ήμισυ όλων αυτών των περιπτώσεων απώλειας δεδομένων αποτελούνται από συσκευές

που λείπουν, συμπεριλαμβανομένων φορητών μέσων αποθήκευσης (π.χ. φορητούς υπολογιστές, μονάδες *flash*, *CD* ή *DVD*), φορητούς υπολογιστές, επιτραπέζιους υπολογιστές, ακόμη και σκληρούς δίσκους που έχουν αφαιρεθεί από μηχανές, έχουν χαθεί και κλαπεί εφεδρικές κασέτες και ολόκληροι διακομιστές δικτύου (Healthit, 2019h).

Μεθοδολογία

Η μεθοδολογία που υιοθετήθηκε στην παρούσα μελέτη βασίστηκε σε μια συστηματική βιβλιογραφική ανασκόπηση (Alcântara & Martens, 2018) η οποία ανάμειξε βιβλιομετρική και ανάλυση περιεχομένου. Σύμφωνα με τον Bardin (2011), η ανάλυση περιεχομένου αναφέρεται στην ομαδοποίηση τεχνικών για την αξιολόγηση της ανθρώπινης επικοινωνίας, χρησιμοποιώντας συστηματικές διαδικασίες με στόχο τον καθορισμό του περιεχομένου του μηνύματος, έχοντας ως κύριο στόχο την εξαγωγή γνώσεων που σχετίζονται με την αντίληψη του περιεχομένου ενός δεδομένου μηνύματος. Έτσι, ακόμη και σύμφωνα με τον ίδιο συγγραφέα, είναι δυνατό να εμπλουτιστεί η ερμηνεία των δεδομένων που συλλέγονται μέσω νοήματος που συχνά είναι σαφής ή κρυφή.

Με αυτόν τον τρόπο, αυτή η μελέτη χρησιμοποιεί τις τρεις κλασικές φάσεις του Bardin (2011): προ-ανάλυση, διερεύνηση του υλικού και επεξεργασία των αποτελεσμάτων και ερμηνειών. Η πρώτη φάση που ονομάζεται *Pre-Analysis* υποδιαιρείται σε πέντε στάδια. Το πρώτο στάδιο αναφέρεται στην αναζήτηση στις διαδικτυακές βάσεις έρευνας, στην οποία χρησιμοποιήθηκε ο συνδυασμός των λέξεων -κλειδιών: *Healthcare, Cybersecutity* και *Risk Management*, στον τίτλο του άρθρου, πεδία περίληψης και λέξεων κλειδιών των επτά διαδικτυακών βάσεων δεδομένων που επιλέχθηκαν για να παραχθεί ένα ευρύ φάσμα που σχηματίζει ένα σταθερό και συνεπές θεωρητικό πλαίσιο για ακαδημαϊκές σπουδές.

Το δεύτερο στάδιο αναφέρεται στα κριτήρια επιλογής και αποκλεισμού για πηγές και επικεντρώνεται στην επιλογή εγγράφων που σχετίζονται με το ερευνητικό θέμα. Ως κριτήρια επιλογής, χρησιμοποιήθηκαν μόνο έγγραφα σε μορφή άρθρων και άρθρα κριτικής, συμπεριλήφθηκαν επίσης μόνο άρθρα που δημοσιεύτηκαν σε παγκόσμια περιοδικά από το 2016 έως το 2021, σε ψηφιακή μορφή και στην αγγλική γλώσσα. Κριτήρια εξαίρεσης ήταν έγγραφα συνεδρίων, κεφάλαια βιβλίων, έντυπα άρθρα ή ακαδημαϊκές εργασίες και διατριβές. Το τρίτο στάδιο αναφέρεται στο σκεπτικό του σώματος του έργου. Με την εφαρμογή των κριτηρίων ένταξης / αποκλεισμού, η χρονική περίοδος των δημοσιευμένων άρθρων που θα αναλυθούν και οι επιλεγμένες βάσεις δεδομένων, αποτέλεσαν τα άρθρα που υποστήριξαν το σώμα της εργασίας αυτής της διατριβής.

Το βήμα τέταρτο περιλαμβάνει την κυμαινόμενη ανάγνωση των επιλεγμένων άρθρων από τον τίτλο του άρθρου, τα πεδία περίληψης και εισαγωγής, αυτή η διαδικασία επέτρεψε να βρεθούν επαναλαμβανόμενα άρθρα, καθώς και άρθρα που δεν ήταν σχετικά για τους σκοπούς της τρέχουσας έρευνας. Το βήμα πέντε επέτρεψε τη σύλληψη των προτάσεων και των στόχων αυτής της έρευνας στο οποίο ήταν δυνατό να παρατηρηθεί η σημασία της κυβερνοασφάλειας στον τρέχοντα κλάδο 4.0.

Η ευαισθητοποίηση και ο διαχωρισμός των πέντε κενών που διαπιστώθηκαν:

- Η κυβερνοασφάλεια είναι ένα εξαιρετικά σημαντικό θέμα στον τομέα της υγειονομικής περίθαλψης.
- Η κυβερνοασφάλεια στον τομέα της υγειονομικής περίθαλψης παραμελείται.
- Δεν υπάρχουν σημαντικές επενδύσεις στον τομέα της υγειονομικής περίθαλψης.
- Οι πληροφορίες που παράγονται από τον τομέα της υγειονομικής περίθαλψης είναι πλούσιες σε περιεχόμενο.
- Υπάρχει έλλειψη δράσεων για την προστασία των δεδομένων στον τομέα της υγειονομικής περίθαλψης προσφέροντας έτσι στα ιδρύματα υγειονομικής περίθαλψης παραμέτρους που θα χρησιμοποιηθούν στην καταπολέμηση του εγκλήματος στον κυβερνοχώρο.

Η δεύτερη φάση που ονομάζεται εξερεύνηση επιλεγμένων άρθρων είναι η φάση στην οποία γίνεται κάθετη ανάλυση / ανάγνωση των επιλεγμένων άρθρων. Το μόνο βήμα αυτής της φάσης συνίσταται στην εμβάθυνση της κατανόησης και της ανάλυσης των επιλεγμένων κειμένων μέσω της εξερεύνησης και κωδικοποίησης των επιλεγμένων άρθρων, γεγονός που οδήγησε στη συγκρότηση αυτής της διατριβής. Τα άρθρα διαβάστηκαν πλήρως και κατηγοριοποιήθηκαν μέσα από ένα πλαίσιο ανάλυσης της σχέσης με το προτεινόμενο θέμα μελέτης. Σε αυτό το πλαίσιο, οι μονάδες εγγραφής ήταν αποσπάσματα, παραπομπές και σημαντικές ιδέες από τα επιλεγμένα άρθρα.

Έτσι, δημιουργήθηκαν κάποιες κύριες ομάδες περιεχομένου, όπως: κρυπτογραφία, συστήματα στον κυβερνοχώρο, ασφάλεια στον κυβερνοχώρο, κακόβουλο λογισμικό, συστήματα ασφαλούς ελέγχου, ιοί, διαχείριση κρίσεων, διαχείριση σχεδίου, διαχείριση έργου, διαχείριση κινδύνων, 5G, βιομηχανία 4.0, *internet of things*, επεξεργασία δεδομένων και υγειονομικής περίθαλψης, που είχαν σχέση με τον σκοπό αυτής της εργασίας. Η τρίτη φάση, που ονομάζεται

αντιμετώπιση αποτελεσμάτων και ερμηνειών, αποτελεί την ερμηνεία των επιλεγμένων πληροφοριών και ομαδοποιείται σε μια πιο πλούσια κατανόηση και νέες γνώσεις που προτείνονται από αυτήν την εργασία. Μέσα από αυτή τη φάση ήταν δυνατό να γίνουν όλα τα ποσοτικά προσόντα και τα προσόντα που χρησιμοποιήθηκαν κατά τη διάρκεια αυτής της μελέτης, καθώς και η σύνθεση και επιλογή των προτεινόμενων αποτελεσμάτων

Συμπεράσματα/Μελλοντικές εξελίξεις/Προτάσεις

Καθώς αυξάνονται οι κίνδυνοι και οι ανησυχίες για την ασφάλεια των δικτύων υγειονομικής περίθαλψης, οι πάροχοι θα πρέπει να αναλάβουν μια συστηματική, πολυεπίπεδη προσέγγιση για τον σχεδιασμό και την ανάπτυξη μιας εξαιρετικά ασφαλούς υποδομής δικτύου. Αυτή η προσέγγιση θα πρέπει να περιλαμβάνει μια προσεκτική αξιολόγηση κάθε τομέα του δικτύου, προσδιορισμός πιθανών απειλών, ανάπτυξη πρακτικής πολιτικής ασφάλειας και εφαρμογή τεχνολογιών ασφάλειας δικτύου.

Σε αυτό το έγγραφο, παρουσιάστηκε μια επισκόπηση της υπάρχουσας έρευνας ασφάλειας και απορρήτου στα συστήματα υγειονομικής περίθαλψης. Η αύξηση της λειτουργικής πολυπλοκότητας, ο περισσότερος προγραμματισμός λογισμικού και η αύξηση της συνδεσιμότητας ασύρματων δικτύων είναι γενικές τάσεις που παρατηρούνται στις εφαρμογές συσκευών υγειονομικής περίθαλψης. Ωστόσο, υπάρχουν παρενέργειες αυτών των τάσεων, γεγονός που καθιστά τις συσκευές και τις εφαρμογές υγειονομικής περίθαλψης όλο και πιο ευάλωτες σε ζητήματα ασφάλειας και απορρήτου.

Αναλύθηκαν διάφορες πτυχές των απειλών και πώς οι τρέχουσες λύσεις ξεπερνούν αυτές τις απειλές. Με δεδομένα τα κρίσιμα καθήκοντα που εκτελούνται από συσκευές υγειονομικής περίθαλψης, αυτά τα ζητήματα θα πρέπει να αντιμετωπιστούν επιθετικά και προληπτικά από την κοινότητα. Η παρούσα έρευνα τεκμηριώνει επιθέσεις και άμυνες διευκολύνοντας ένα πιο ευαισθητοποιημένο οικοσύστημα για την ασφάλεια και την ιδιωτικότητα στα συστήματα υγειονομικής περίθαλψης. Εστιάστηκε στους πρωταρχικούς στόχους ασφάλειας και απορρήτου για την επόμενη γενιά συσκευών υγειονομικής περίθαλψης και ανέλυσε τους πιο συνηθισμένους και συναφείς μηχανισμούς προστασίας που έχουν προταθεί μέχρι τώρα.

Για την εξασφάλιση ενός συστήματος υγειονομικής περίθαλψης, οι προτάσεις ασφαλείας πρέπει να λαμβάνουν υπόψη τους περιορισμούς ενέργειας, αποθήκευσης και υπολογιστικής ισχύος των συσκευών υγειονομικής περίθαλψης που προσφέρονται. Σε αυτήν την ενότητα, συζητούνται οι συστάσεις και οι πρακτικές ασφάλειας, ώστε οι μελλοντικές ερευνητικές

κατευθύνσεις να μπορούν να προσφέρουν τη διασφάλιση της ασφάλειας και της ιδιωτικής ζωής στα συστήματα υγειονομικής περίθαλψης:

Εξασφάλιση δεδομένων υγειονομικής περίθαλψης: Η βιομηχανία υγειονομικής περίθαλψης παράγει γρήγορα δεδομένα, και αυτά τα δεδομένα υγειονομικής περίθαλψης έχουν κλινική, οικονομική και λειτουργική αξία στην αγορά. Για την αποτελεσματική προστασία αυτών των δεδομένων υγειονομικής περίθαλψης από παραβιάσεις, απαιτούνται μέτρα ασφαλείας, όπως κρυπτογραφικές λύσεις, για την εξασφάλιση ασύρματης επικοινωνίας, καθώς και τις πληροφορίες που είναι αποθηκευμένες στη συσκευή ή στο διακομιστή. Από αυτή την άποψη, κρυπτογραφικά πρωτόκολλα που είναι συμμετρικά και ελαφριά, μπορεί να παρέχουν ένα μέσο για τον έλεγχο της πρόσβασης σε συσκευές υγειονομικής περίθαλψης και την προστασία από πλαστογραφία και αύξηση των επιθέσεων προνομίων.

Ωστόσο, η ενσωμάτωση κρυπτογραφικών μηχανισμών στις υπάρχουσες συσκευές υγειονομικής περίθαλψης συνεπάγεται ότι οι τρέχουσες συσκευές όπως τα *IMD* πρέπει να αντικατασταθούν ή να επανασχεδιαστούν. Σε περίπτωση έκτακτης ανάγκης, μπορεί να χρειαστεί επικοινωνία με μη εξουσιοδοτημένο προσωπικό, η οποία μπορεί να διακοπεί λόγω της εφαρμογής των κρυπτογραφικών σχημάτων. Ως εκ τούτου, οι ερευνητές πρέπει να επικεντρωθούν στην ανάπτυξη ιατρικοκεντρικών κρυπτογραφικών λύσεων για την επίτευξη των μοναδικών στόχων ασφάλειας του συστήματος υγειονομικής περίθαλψης.

Έλλειψη τυπικών πρωτοκόλλων επικοινωνίας: Το πρότυπο επικοινωνίας για συσκευές υγειονομικής περίθαλψης είναι καλή πρακτική, και πολλά διεθνή πρότυπα θεωρούνται ως προαπαιτούμενα για την πιστοποίηση συσκευών υγειονομικής περίθαλψης. Αυτά τα πρότυπα περιορίζονται στη διαδικασία αξιολόγησης των κινδύνων ανάπτυξης και σχεδιασμού, αλλά δεν επικεντρώνονται σχετικά με τις ειδικές απαιτήσεις ασφαλείας εντός της περίπλοκης ανάπτυξης ρύθμισης. Πολλά ελαττώματα ασφαλείας και αντίστοιχα τρωτά σημεία όπως η έγχυση *SQL* και η υπερχείλιση *buffer* είναι συνέπεια του κακού σχεδιασμού του λογισμικού, που μπορεί να σχετίζονται με τα πρότυπα επικοινωνίας που χρησιμοποιούνται σε αυτές τις συσκευές.

Σχεδιασμός ανθεκτικός σε σφάλματα: Η αξιοπιστία είναι η κορυφαία προτεραιότητα στα συστήματα υγειονομικής περίθαλψης που είναι κρίσιμα για τη ζωή. Κατά τη διάρκεια του τυπικού ελέγχου, είναι δυνατόν να εντοπιστεί ένας μεγάλος αριθμός ελαττωμάτων υλικού ή λογισμικού, αλλά ενδέχεται η πλήρης κάλυψη βλαβών να μην είναι δυνατή. Μέσω της

ταυτόχρονης ανίχνευσης, διάγνωσης και διόρθωσης των επιπτώσεων βλάβης, οι σχεδιασμοί ανεκτικοί σε σφάλματα επιτρέπουν σε ένα σύστημα να συνεχίσει να λειτουργεί σε περίπτωση βλάβης των συστατικών του. Επιπλέον, μπορεί να επεκταθεί για να αντιμετωπίσει σφάλματα λογισμικού που προκαλούνται από ανεπάρκειες σχεδιασμού. Αν και ορισμένοι τύποι πλεονασμού όπως ο χρόνος, το υλικό ή οι πληροφορίες απαιτούνται για την ανοχή σε σφάλματα, αυτό ο πλεονασμός κοστίζει συχνά την υποβάθμιση της απόδοσης ή άλλου είδους επιβάρυνση.

Μηχανισμός ανίχνευσης εισβολής για τον εντοπισμό επιθέσεων: Η διασφάλιση της ασφάλειας των ασθενών είναι ο βασικός λόγος για την ανάγκη ασφάλισης συσκευών υγειονομικής περίθαλψης. Συνήθως απαιτείται ένα σύστημα ανίχνευσης εισβολής (*IDS*) για τον εντοπισμό οποιωνδήποτε τύπων επιθέσεων. Μπορεί να δημιουργηθεί μια ειδοποίηση για τους ασθενείς ή το ιατρικό προσωπικό εάν ένας αντίπαλος απειλεί το σύστημα υγείας ή κάποια συσκευή. Ένα *IDS* θα παρακολουθεί την εισερχόμενη κίνηση που προέρχεται από την εξωτερική συσκευή προς τις συσκευές υγειονομικής περίθαλψης που βασίζονται σε ορισμένους προκαθορισμένους κανόνες (π.χ., η καθυστέρηση μεταξύ δύο διαδοχικών αιτημάτων που προέρχονται από μια εξωτερική συσκευή, το μήκος του ωφέλιμου φορτίου μηνύματος κ.λπ.).

Η ερευνητική κοινότητα πρέπει να δώσει μεγαλύτερη έμφαση για την ανάπτυξη ενός τυπικού *IDS* όπου οι προκαθορισμένοι κανόνες μπορούν να αναφέρονται σε διαφορετικά πρωτόκολλα επικοινωνίας σε πρότυπες συσκευές υγειονομικής περίθαλψης.

Λεπτομερής έλεγχος πρόσβασης: Τρέχοντες μηχανισμοί ελέγχου πρόσβασης, όπως πολιτική βάσει χαρακτηριστικών και βάσει κινδύνου, ο έλεγχος πρόσβασης επικεντρώθηκε κυρίως στην πρόληψη μη εξουσιοδοτημένης πρόσβασης σε συσκευές υγειονομικής περίθαλψης. Ωστόσο, αυτά τα δεδομένα υγειονομικής περίθαλψης διαβιβάζονται μέσω διαφορετικών τμημάτων ενός συστήματος υγειονομικής περίθαλψης, όπου η ακεραιότητα και το απόρρητο των δεδομένων δεν είναι εξασφαλισμένα. Ως λύση σε αυτό το πρόβλημα, θα πρέπει να επιβληθεί μια τυπική πολιτική ελέγχου πρόσβασης σε διαφορετικά στοιχεία ενός συστήματος υγειονομικής περίθαλψης για τον εντοπισμό τυχόν παραβίασης της ασφάλειας στα δεδομένα πρόσβασης.

Έλλειψη γενικής πλατφόρμας: Διαφορετικές συσκευές υγειονομικής περίθαλψης χρησιμοποιούν πολυάριθμες προδιαγραφές υλικού, εφαρμογή λογισμικού, πρωτόκολλα επικοινωνίας και λειτουργικά συστήματα. Αυτή η ετερογένεια καθιστά δύσκολη τη μελέτη των ερευνητών ασφάλειας για τις υπάρχουσες απειλές, και παρέχουν μια κοινή λύση ασφάλειας για

αυτές τις συσκευές υγειονομικής περίθαλψης. Ως αποτέλεσμα, οι περισσότερες από τις λύσεις ασφαλείας είναι συγκεκριμένες για την πλατφόρμα και δεν μπορούν να λύσουν το ευρύ φάσμα προβλημάτων ασφαλείας. Ερευνητές, προγραμματιστές και η βιομηχανία θα πρέπει να εργαστούν για την ανάπτυξη ενός κοινού προτύπου για συστήματα υγειονομικής περίθαλψης που θα βοηθήσουν στην ανάπτυξη γενικευμένων λύσεων ασφαλείας.

Σύστημα υγειονομικής περίθαλψης που προστατεύει την ιδιωτικότητα: Υφιστάμενες λύσεις απορρήτου όπως ανωνυμία χρηστών και επικοινωνιών, επικεντρώθηκαν κυρίως στην πρόληψη οποιασδήποτε μη εξουσιοδοτημένης πρόσβασης στα δεδομένα και την επικοινωνία της υγειονομικής περίθαλψη. Ωστόσο, εξακολουθούν να υπάρχουν αρκετά ζητήματα στα συστήματα υγειονομικής περίθαλψης που θα μπορούσαν να επηρεάσουν το απόρρητο των χρηστών και τα δεδομένα υγειονομικής περίθαλψης εάν δεν αντιμετωπιστούν σωστά. Για να διασφαλιστεί το απόρρητο, οι κατασκευαστές θα πρέπει να βρουν έναν ασφαλέστερο τρόπο για να μοιραστούν τις πληροφορίες της συσκευής με τους χρήστες και οι ερευνητές θα πρέπει να εστιάσουν περισσότερο στην επιβολή μιας τυπικής πολιτικής απορρήτου σε διαφορετικά στοιχεία των συστημάτων υγειονομικής περίθαλψης.

Μελέτη έξυπνων ιατρικών συσκευών και υφιστάμενων απειλών: Τα τελευταία χρόνια, η έννοια του *IoT* έχει ενσωματωθεί στον ιατρικό τομέα, καθιστώντας τις σύγχρονες ιατρικές συσκευές ενημερωμένες για το περιβάλλον και έξυπνες. Ωστόσο, υπάρχουν αρκετές επιθέσεις σε συσκευές *IoT* που μπορούν να προσαρμοστούν σε μια έξυπνη ιατρική πλατφόρμα με ελάχιστες τροποποιήσεις. Καθώς οι απαιτήσεις ασφαλείας των συσκευών *IoT* και των συστημάτων υγειονομικής περίθαλψης διαφέρουν πολύ, οι υπάρχουσες λύσεις ασφαλείας συσκευών, συχνά δεν μπορούν να εξασφαλίσουν την απόλυτη ανάγκη ασφάλειας ιατρικών συσκευών.

Ως εκ τούτου, είναι απαραίτητο να μελετηθούν οι έξυπνες πλατφόρμες υγειονομικής περίθαλψης, καθώς και στον τομέα ιατρικού *IoT* για τον εντοπισμό και την ανάπτυξη λύσεων ασφαλείας των υποκείμενων απειλών, συγκεκριμένες για τον τομέα της υγειονομικής περίθαλψης. Η ερευνητική κοινότητα θα πρέπει να εστιάσει περισσότερο στις έξυπνο συσκευές υγειονομικής περίθαλψης για την αντιμετώπιση αυτών των απειλών και οι ειδικοί του κλάδου θα πρέπει να προτείνουν μια τυπική πρακτική για την κατασκευή συσκευών και ανάπτυξη εφαρμογών για την ελαχιστοποίηση αυτών των απειλών.

Βιβλιογραφία

Ξενόγλωσση

1. Abood OG, Guirguis SK. A survey on cryptography algorithms. Int J Sci Res Publ. 2018;8(Wang X.B. et al., 2008):410–5
2. Ahmed, A. A., & Ahmed, W. A. (2019). An Effective Multifactor Authentication Mechanism Based on Combiners of Hash Function over Internet of Things. Sensors, 19 n.17. doi:10.3390/s19173663.
3. Alcantara, D. P., & Martens, M. L. (2018). Technology Roadmapping (TRM): a systematic review of the literature focusing on models. Technological Forecasting and Social Change, pp. 127-138. doi:doi.org/10.1016/j.techfore.2018.08.014.
4. Alexander, B., Haseeb, S., & Baranchuk, A. (2019). Are implanted electronic devices hackable? Trends in Cardiovascular Medicine, pp. 476-480. doi:10.1016/j.tcm.2018.11.011
5. Alromaihi, S.; Elmedany, W.; Balakrishna, C. Cyber Security Challenges of Deploying IoT in Smart Cities for Healthcare Applications. In Proceedings of the 2018 6th International Conference on Future Internet of Things and Cloud Workshops (FiCloudW), Barcelona, Spain, 6–8 August 2018; pp. 140–145.
6. Askar, A. J. (2019). Healthcare management system and cybersecurity. International Journal of Recent Technology and Engineering, 237-248.
7. Androulaki E, Barger A, Bortnikov V, Cachin C, Christidis K, De Caro A, et al. Hyperledger fabric: a distributed operating system for permissioned blockchains. In proceedings of the EuroSys Conference 2018 (p. 30). ACM.
8. Balaraman, P., & Kosalram, K. (2013). E-hospital management & hospital information systems-changing trends. International Journal of Information Engineering and Electronic Business, 5(Smart W., 2018), 50.
9. Bellazzi R., ``Big data and biomedical informatics: A challenging opportunity," IMIA Yearbook Med. Informat., vol. 23, no.1, pp. 8-13, 2014.

10. Benchoufi M, Ravaud P. Blockchain technology for improving clinical research quality. Trials. 2017; 18(Smart W., 2018):335.
11. Berger, K. M., & Schneck, P. A. (2019). National and transnational security implications of asymmetric access to and use of biological data. Frontiers in Bioengineering and Biotechnology, 7. doi:10.3389/fbioe.2019.00021.
12. Bhuyan SS, Kabir U, Escareno JM, et al. Transforming healthcare cybersecurity from reactive to proactive: current status and future recommendations. J Med Syst 2020;44: 10.1007/s10916-019-1507-y
13. Blanke, S. J., & McGrady, E. (2016). When it comes to securing patient health information from breaches, your best medicine is a dose of prevention: A cybersecurity risk assessment checklist. Journal of healthcare risk management, 14-24. doi:10.1002/jhrm.21230.
14. Bissonnette, L., & Bergeron, M. G. (2017). Portable devices and mobile instruments for infectious diseases point-of-care testing. Expert Review of Molecular Diagnostics, 471-494. doi:10.1080/14737159.2017.1310619.
15. Bojanova, I., & Voas, J. (2017). Trusting the Internet of Things. IT Professional, 19 n.5, 16-19. doi:10.1109/MITP.2017.3680956.
16. Braga, A., Dahab, R., Antunes, N., Laranjeiro, N., & Vieira, M. (2019). Understanding How to Use Static Analysis Tools for Detecting Cryptography Misuse in Software. IEEE TRANSACTIONS ON RELIABILITY, 1384-1403. doi: 10.1109/TR.2019.2937214.
17. Brahmi I, Brahmi H, Yahia SB. A multi-agents intrusion detection system using ontology and clustering techniques. In: IFIP international conference on computer science and its applications. Springer; 2015. p. 381–393.
18. Brody, R. G., Chang, H. U., & Schoenberg, E. S. (2018). Malware at its worst: death and destruction. International Journal of Accounting & Information Management. doi:10.1108/ijaim.2011.36619caa.003.
19. Busdicker, M., & Upendra, P. (2017). The role of healthcare technology management in facilitating medical device cybersecurity. Biomedical Instrumentation and Technology, 19-25. doi:10.2345/0899-8205-51.s6.19.

20. Coveney, P. V., Dougherty, E. R., & Highfield, R. R. (2016). Big data need big theory too. Philosophical Transactions Of The Royal Society A-Mathematical Physical And Engineering Sciences, 374. doi:10.1098/rsta.2016.0153.
21. Coventry, L., & Branley, D. (2018). Cybersecurity in healthcare: A narrative review of trends, threats and ways forward. Maturitas, 48-52. doi:10.1016/j.maturitas.2018.04.008.
22. Cleland-Huang, J. (2014). How well do you know your personae non gratae? IEEE Software, 31, 28-31. doi:10.1109/MS.2014.85.
23. Dandage, R., Mantha, S. S., & Rane, S. B. (2018). Ranking the risk categories in international projects using the TOPSIS method. International Journal of Managing Projects in Business, 11, 317-331. doi:10.1108/IJMPB-06-2017-0070.
24. Diggans, J., & Leproust, E. (2019). Next steps for access to safe, secure DNA synthesis. Frontiers in Bioengineering and Biotechnology, 7. doi:10.3389/fbioe.2019.00086.
25. Educational Center of Kermanshah. Adv. Environ. Biol., 8(nist.gov, 2018): 748- 753.
26. e-Estonia. Cyber security report 2018: investing in the security of information systems to secure digital lifestyle. 2018. https://e-estonia.com/cyber-security-report-2018/
27. eHospital System. [Online]. Available: https://www.adroitinfosystems.com/products/ehospital-systems
28. Elizabeth, M. J., Jobin, J., & Dona, J. (2019). A fog based security model for electronic medical records in the cloud database. International Journal of Innovative Technology and Exploring Engineering, 8 n.7, pp. 2552-2560.
29. Fazeldehkordi, E.; Owe, O.; Noll, J. (2019). Security and Privacy in IoT Systems: A Case Study of Healthcare Products. In Proceedings of the 2019 13th International Symposium on Medical Information and Communication Technology (ISMICT), Oslo, Norway, 8–10 May 2019.
30. Foroughi F, Luksch P. Data science methodology for cybersecurity projects. arXiv preprint arXiv: 1803. 04219. 2018.
31. Frontoni, E., Mancini, A., Bald, M., Paolanti, M., Moccia, S., Zingaretti, P., . . . Misericordia, P. (2019). Sharing health data among general practitioners: The Nu.Sa. project. International Journal of Medical Informatics, 129, pp. 267-274. doi:10.1016/j.ijmedinf.2019.05.016.

32. Ghafir, I., Prenosil, V., Hammoudeh, M., Baker, T., Jabbar, S., Khalid, S., & Jaf, S. (2018). BotDet: A System for Real Time Botnet Command and Control Traffic Detection. IEEE Access, 38947-38958. doi:10.1109/ACCESS.2018.2846740.
33. Ghafur, S., Grass, E., Jennings, N., & Darzi, A. (2019). The challenges of cybersecurity in health care: the UK National Health Service as a case study. The Lancet Digital Health, 1 n.1, pp. 10-12. doi:10.1016/S2589-7500(19)30005-6.
34. Ghosh A, Ashok I. WannaCry: list of major companies and networks hit by ransomware around the globe. International Business Times May 16, 2017. https://www.ibtimes.co.uk/wannacry-list-major-companies-networks-hitby-deadly-ransomware-around-globe-1621587
35. Grimes, S., & Wirth, A. (2017). Holding the Line: Events that Shaped Healthcare Cybersecurity. Biomedical instrumentation & technology. doi:10.2345/0899-8205-51.s6.30.
36. Gupta, R.; Reebadiya, D.; Tanwar, S. 6G-enabled Edge Intelligence for Ultra -Reliable Low Latency Applications: Vision and Mission. *Comput. Stand. Interfaces* **2021**, *77*, 103521.
37. Gupta, R.; Nair, A.; Tanwar, S.; Kumar, N. Blockchain-assisted secure UAV communication in 6G environment: Architecture, opportunities, and challenges. *IET Commun.* **2021**, 1–16.
38. Gupta, R.; Kumari, A.; Tanwar, S. A taxonomy of blockchain envisioned edge-as-a-connected autonomous vehicles. *Trans. Emerg. Telecommun. Technol.* **2020**, 1–24.
39. Handler, I. (2018). Data Sharing Defined-Really! Computer, 36-42. doi:10.1109/MC.2018.1451659.
40. Helms, K. (2018). Big-Name Insurers Stepping Up Their Crypto Game. Bitcoin News. https://news.bitcoin.com /insurerscrypto/.
41. Henriksen (2019). The end of the road for the UN GGE process: The future regulation of cyberspace. Journal of Cybersecurity, 22 January 2019, Vol 5, issue 1
42. House of Commons. (2018). Cyber-Attack on the NHS. https://publications. parliament.uk/pa/cm201719/cmselect/cmpubacc/787/787.pdf
43. Jalali MS and Kaiser JP. Cybersecurity in hospitals: a systematic, organizational perspective. J Med Internet Res 2018; 20: e10059.
44. Johnson L. Computer incident response and forensics team management: conducting a successful incident response. 2013.

45. Kabir, U. Y., Ezekekwu, E., Bhuyan, S. S., Mahmood, A., & Dobalian, A. (2020). Trends and best practices in health care cybersecurity insurance policy. Journal of Healthcare Risk Management, pp. 1-5. doi:10.1002/jhrm.21414.
46. Kessler, S. R., Pindek, S., Kleinman, G., Andel, S. A., & Spector, P. E. (2019). Information security climate and the assessment of information security risk among healthcare employees. Health informatics Journal. doi:10.1177/1460458219832048.
47. Khalifa, M., & Alswailem, O. (2015). Hospital information systems (HIS) acceptance and satisfaction: a case study of a tertiary care hospital. Procedia Computer Science, 63, 198-204.
48. Khan N., I. Yaqoob, I. A. T. Hashem, Z. Inayat, W. K. M. Ali, and M. Alam, ``Big data: Survey, technologies, opportunities, and challenges," Sci. World J., vol. 2014, pp. 1-18, Jul. 2014.
49. Khraisat A, Gondal I, Vamplew P, Kamruzzaman J. Survey of intrusion detection systems: techniques, datasets and challenges. Cybersecurity. 2019;2(1):20.
50. King, F., Klonoff, D. C., Kerr, D., Hu, J., Lyles, C., Quinn, C., . . . Gabbay, R. (2018). Digital Diabetes Congress 2018. Journal of Diabetes Science and Technology, 1231-1238. doi:10.1177/1932296818805632.
51. Kinkorová J. and O. Topol£an, ``Biobanks in horizon 2020: Sustainability and attractive perspectives," EPMA J., vol. 9, no. 4, pp. 345-353, Dec. 2018.
52. Kitchenham B., Brereton O. P., Budgen D., Turner M., Bailey J., and Linkman S., ``Systematic literature reviews in software engineering-a systematic literature review," Inf. Softw. Technol., vol. 51, no. 1, pp. 7-15, Jan. 2009.
53. Koppel, R., & Kuziemsky, C. (2019). Healthcare data are remarkably vulnerable to hacking: Connected healthcare delivery increases the risks. Studies in Health Technology and Informatics, 218-222. doi:10.3233/978-1-61499-951-5-218.
54. Kroll M, Sch€utze B, Geisbe T, et al. Embedded systems for signing medical images using the DICOM standard. Int Congr Ser 2003; 1256:849–854. https://doi.org/10.1016/S0531-5131(03)00463-1.
55. Kruse, C. S., Frederick , B., Jacobson , T., & Monticone , K. (2017). Cybersecurity in healthcare: A systematic review of modern threats and trends. Technology and Health Care, 25, 1-10. doi:10.3233/THC-161263.

56. Kuerbis, B., & Badiei, F. (2017). Mapping the cybersecurity institutional landscape. Australian Catholic University, 19, 466-492. doi:10.1108/DPRG-05-2017-0024.

57. Kumari, A.; Gupta, R.; Tanwar, S.; Kumar, N. Blockchain and AI amalgamation for energy cloud management: Challenges, solutions, and future directions. *J. Parallel Distrib. Comput.* **2020**, *143*, 148–166.

58. Kumar, N. (2017). IoT architecture and system design for healthcare systems. In Proceedings of the 2017 International Conference on Smart Technologies for Smart Nation (SmartTechCon), Bengaluru, India, 17–19 August 2017; pp. 1118–1123.

59. Kure, H. I., Islam, S., & Razzaque, M. A. (2018). An integrated cyber security risk management approach for a cyber-physical system. Applied Sciences (Switzerland). doi:10.3390/app8060898.

60. Kwang K. SingHealth cyberattack: Committee of Inquiry appointed, report due end-2018. Channel NewsAsia July 24, 2018. https://www.channelnewsasia.com/news/singapore/singhealth-cyberattack-committee-ofinquiry-appointed-report-due-10557724

61. Laurence T. Blockchain for dummies. John Wiley & Sons; 2017.

62. Lavanya, S.; Divyabharathi, J. (2017). Remote prescription and I-Home healthcare based on IoT. In Proceedings of the 2017 International Conference on Innovations in Green Energy and Healthcare Technologies (IGEHT), Coimbatore, India, 16–18 March 2017; pp. 1–3

63. Liao H-J, Richard Lin C-H, Lin Y-C, Tung K-Y. Intrusion detection system: a comprehensive review. J Netw Comput Appl. 2013;36(1):16–24.

64. Loi, M., Christen, M., Kleine, N., & Weber, K. (2019). Cybersecurity in health – disentangling value tensions. Journal of Information, Communication and Ethics in Society, 229-245. doi:10.1108/JICES-12-2018-0095

65. Martin, G., Martin , P., Hankin , C., Darzi , A., & Kinross , J. (2017). Cybersecurity and healthcare: How safe are we? BMJ (Online). doi:10.1136/bmj.j3179.

66. Mehta, P.; Gupta, R.; Tanwar, S. Blockchain envisioned UAV networks: Challenges, solutions, and comparisons. *Comput. Commun.* **2020**, *151*, 518–538.

67. Natsiavas, P., Rasmussen, J., Voss-Knude, M., Votis, K., Coppolino, L., Cano, I., . . . Nalin, M. (2018). Comprehensive user requirements engineering methodology for secure and

interoperable health data exchange. BMC Medical Informatics and Decision Making, 18 n.1. doi:10.1186/s12911-018-0664-0.

68. Nazir S., Nawaz M., Adnan A., Shahzad S., and Asadi S., ``Big data features, applications, and analytics in cardiology. A systematic literature review," IEEE Access, vol. 7, pp. 143742-143771, 2019.

69. Newaz, A.I.; Sikder, A.K.; Rahman, M.A.; Uluagac, A.S. HealthGuard: A Machine Learning-Based Security Framework for Smart Healthcare Systems. In Proceedings of the 2019 6th International Conference on Social Networks Analysis, Management and Security (SNAMS), Granada, Spain, 22–25 October 2019; pp. 389–396.

70. Ondiege, B., Clarke, M., & Mapp, G. (2017). Exploring a new security framework for remote patient monitoring devices. Computers, 6 n.1. doi:10.3390/computers6010011.

71. Patel A., Q. Qassim, Z. Shukor, J. Nogueira, J. Júnior, C. Wills, (2010) "Autonomic Agent-Based Self-Managed Intrusion Detection and Prevention System," Proceedings of the South African Information Security Multi-Conference (SAISMC 2010), Port Elizabeth, South Africa, May 17-18,2010.

72. Qi H, Di X, Li J. Formal definition and analysis of access control model based on role and attribute. J Inf Secur Appl. 2018;43:53–60.

73. Silva F., J. C., Braga, C. S., & Reboucas, S. M. (2016). Perception of the brazilian manufacturing industry about the main barriers to innovation. International journal of innovation, v. 5 n.1, p. 114-131, 2016. doi 10.5585/iji.v5i1.114.

74. The History of Health Information Management – from then to now. [Online]. Available: https://liaison.opentext.com/blog/2017/05/02/history-heath-information-management-now/

75. Vanhoef M. and F. Piessens, "Release the Kraken: new KRACKs in the 802.11 Standard," Proc. 2018 ACM SIGSAC Conference on Computer and Communications Security, 299-314. https://doi.org/10.1145/3243734.3243807.

76. Wireshark Network Protocol Analyzer. Available at: https://www.wireshark.org/.

77. Xue Y, Meng G, Liu Y, Tan TH, Chen H, Sun J, Zhang J. Auditing anti-malware tools by evolving android malware and dynamic loading technique. IEEE Trans Inf Forensics Secur. 2017;12(Wang X.B. et al., 2008):1529–44.

78. Yin J. Firewall policy management, May 10 2016. US Patent 9,338,134.

79. Zhang, X., Tan, Y.-a., Xue, Y., Zhang, Q., Li, Y., Zhang, C., & Zheng, J. (2017). Cryptographic key protection against FROST for mobile devices. Cluster Comput, 2393-2402. doi:10.1007/s10586-016-0721-3.

Διαδικτυακή

1. Anstee, D. et al (2016).Worldwide Infrastructure Security Report. Arbor Networks Special Report. 11. NETSCOUT http://www.icir.org/vern/cs261n/papers/Arbor-WISR2016.pdf. Τελευταία πρόσβαση 29/09/2021
2. Armor. (2018). The Black Market Report: A Look Inside the Dark Web. https://cdn.armor.com/app/uploads/2018/03/27222933/2018-Q1-Reports-BlackMarket-DIGITAL-min.pdf. Τελευταία πρόσβαση 29/09/2021
3. Baker, S. (2017). Cybersecurity Becoming Big ESG Concern. Pension & Investments. Accessed January 22. https://www.pionline .com/article/20171002/PRINT/171009985/cybersecurity-becoming-big-esg-concern. Τελευταία πρόσβαση 29/09/2021
4. BBC.(2015).Web Attack Knocks BBC Websites Offline. https://www.bbc.co.uk/news/technology-35204915 Τελευταία πρόσβαση 29/09/2021
5. Benner, K., et al. (2018). Saudis Image Makers: A Troll Army and a Twitter Insider. The New York Times. October 20, 2018. https://www.nytimes.com/2018/10/20/us/politics/saudi-image-campaign-twitter.html Τελευταία πρόσβαση 29/09/2021
6. Bilek, A. M., Muscionico, D., & Amiel, C. (2017). A primer on the regulation and development of M-Health products. Regulatory Rapporteur, https://www.scopus.com/record/display.uri?eid=2s2.085032879397&origin=inward&txGid=408ced46814b35c8bd8454243cf24e2d. Τελευταία πρόσβαση 12/10/2021
7. Caresoft. [Online]. Available: https://caresoft.co.in/ Τελευταία πρόσβαση 12/10/2021
8. CHIST-ERA, "Success: Secure accessibility for the internet of things," 2016, http://www.chistera.eu/projects/success. Τελευταία πρόσβαση 14/10/2021

9. 3Com. 2000 White Paper: «Network Security:A Simple Quide to Firewalls». 3Com Corporation www.3com.com Τελευταία πρόσβαση 15/10/2021
10. Cybersecurity: How can it be Improved in Healthcare? Chicago: University of Illinois. https://healthinformatics.uic.edu/blog/cybersecurity-howcan-it-be-improved-in-health-care/ Τελευταία πρόσβαση 14/10/2021
11. DICOM Standards Committee, Working Group 14. Digital imaging and communications in medicine (DICOM) supplement 99: extended negotiation of user identity. Final Text 2004. Available at: ftp://medical.nema.org/medical/dicom/final/sup99_ft.pdf Τελευταία πρόσβαση 15/10/2021
12. Digital Health Project. Information and Communication Technology Agency (ICTA) – Sri Lanka. [Online]. Available: https://www.icta.lk/projects/digital-health/ Τελευταία πρόσβαση 15/10/2021
13. European Union Agency for Network and Information Security (ENISA), Smart hospitals security and resilience for smart health service and infrastructures," 2016. https://doi.org/10.2824/28801. Τελευταία πρόσβαση 29/09/2021
14. European Union, "The eu general data protection regulation (gdpr)," 2018, http://www.eugdpr.org. Τελευταία πρόσβαση 15/10/2021
15. Healthcare Information Security: Best Practices for Healthcare. Information Security Institute. https://resources.infosecinstitute.com/category/healthcare-information-security/is-best-practices-for-healthcare/ Τελευταία πρόσβαση 29/09/2021
16. Healthit 2019a. «Your mobile device and health information privacy and security» http://healthit.gov/providers-professionals/your-mobile-device-and-health-information-privacy-and-security Τελευταία πρόσβαση 14/10/2021
17. Healthit 2019b. «Mobile Device Checklist» http://healthit.gov/sites/default/files/Mobile Device Checklist.pdf Τελευταία πρόσβαση 14/10/2021
18. Healthit 2019c. «Maintanance Checklist» http://healthit.gov/sites/default/files/Maintenance Checklist.pdf Τελευταία πρόσβαση 14/10/2021
19. Healthit 2019e. «Firewall Checklist» http://healthit.gov/sites/default/files/Firewall Checklist.pdf Τελευταία πρόσβαση 14/10/2021
20. Healthit 2019f. «Anti-Virus Checklist» http://healthit.gov/sites/default/files/Anti-Virus Checklist.pdf Τελευταία πρόσβαση 14/10/2021

21. Healthit 2019g http://healthit.gov/safer/guide/sg003 Τελευταία πρόσβαση 14/10/2021
22. Healthit 2019h. «Backup and Recovery Checklist» http://healthit.gov/sites/default/files/Backup and Recovery Checklist.pdf Τελευταία πρόσβαση 14/10/2021
23. Healthit 2019i. «Password Checklist» http://healthit.gov/sites/default/files/Password Checklist.pdf Τελευταία πρόσβαση 14/10/2021
24. Healthit 2019j. «Network Access Checklist» http://healthit.gov/sites/default/files/Network Access Checklist.pdf Τελευταία πρόσβαση 14/10/2021
25. Higgins, K. (2018). Unpatched Vulnerabilities the Source of Most Data Breaches. Dark Reading. https://www.darkreading.com/vulnerabilities---threats/unpatched-vulnerabilities-the-source-of-most-data-breaches/d/did/1331465. Τελευταία πρόσβαση 10/10/2021
26. Ibm security report. https:// www. ibm. com/ secur ity/ data- breach. Τελευταία πρόσβαση 10/10/2021
27. ISO/IEC 27001 (2013) Information technology - Security techniques — Information security management systems — Requirements. [S.l.]. https://www.iso.org/standard/54534.html. Τελευταία πρόσβαση 12/10/2021
28. ISO31000 (2018). Risk management - Principles and guidelines. [S.l.]. https://www.iso.org/standard/65694.html Τελευταία πρόσβαση 12/10/2021
29. Joshua R Vest and Larry D Gamm. Health information exchange: persistent challenges and new strategies. [Online]. Available: https://www.ncbi.nlm.nih.gov/pmc/articles/PMC2995716/ Τελευταία πρόσβαση 29/09/2021
30. National Institute of Standards and Technology. Cybersecurity framework. 2018. https://www.nist.gov/industry-impacts/cybersecurity Τελευταία πρόσβαση 10/10/2021
31. NTT Security, "2019 Global Threat Intelligence Report (GTIR)," Available at: https://www.nttsecurity.com/landing-pages/2019-gtir/. Τελευταία πρόσβαση 13/10/2021
32. OpenMRS. A free, open-source electronic medical record platform. [Online]. Available: https://openmrs.org/ Τελευταία πρόσβαση 13/10/2021
33. Pandemic profiteering: how criminals exploit the COVID-19 crisis. European Union Agency for Law Enforcement Cooperation. https://www.europol.europa.eu/publications-documents/pandemic-profiteering-howcriminals-exploit-covid-19-crisis Τελευταία πρόσβαση 10/10/2021

34. Ponemon Institute. 2012 Cost of Cyber Crime Study: United State. Ponemon Institute; 2012. Available from: http: //static.knowledgevision.com/account/idgenterprise/assets/attachment/ HPESP WP PonemonCostofCyberCrimeStudy2012 US.pdf. Τελευταία πρόσβαση 10/10/2021