ΠΑΝΕΠΙΣΤΗΜΙΟ ΔΥΤΙΚΗΣ ΑΤΤΙΚΗΣ
ΣΧΟΛΗ ΜΗΧΑΝΙΚΩΝ
ΤΜΗΜΑ ΒΙΟΜΗΧΑΝΙΚΗΣ ΣΧΕΔΙΑΣΗΣ ΚΑΙ ΠΑΡΑΓΩΓΗΣ

Διπλωματική Εργασία

Η ασφάλεια των υπολογιστών (Cybersecurity) στον τομέα της ιατρικής επιστήμης

Συγγραφέας

Κωνσταντίνος Μαστρομιχάλης

ΑΜ: 18389313

Επιβλέπων:

Χρήστος Δρόσος

Αθήνα, Ιούλιος 2023

UNIVERSITY OF WEST ATTICA
SCHOOL ENGINEERING
DEPARTMENT INDUSTRIAL DESIGN AND PRODUCTION

Diploma Thesis

Computer security (Cybersecurity) in the field of medical science

Student name and surname:

Konstantinos Mastromichalis

Registration Number: 18389313

Supervisor name and surname

Christos Drosos

Athens, July 2023

ΠΑΝΕΠΙΣΤΗΜΙΟ ΔΥΤΙΚΗΣ ΑΤΤΙΚΗΣ

ΣΧΟΛΗ ΜΗΧΑΝΙΚΩΝ

ΤΜΗΜΑ ΒΙΟΜΗΧΑΝΙΚΗΣ ΣΧΕΔΙΑΣΗΣ ΚΑΙ ΠΑΡΑΓΩΓΗΣ

Η ασφάλεια των υπολογιστών (cybersecurity) στον τομέα της ιατρικής επιστήμης

Μέλη Εξεταστικής Επιτροπής συμπεριλαμβανομένου και του Εισηγητή

Η πτυχιακή/διπλωματική εργασία εξετάστηκε επιτυχώς από την κάτωθι Εξεταστική Επιτροπή:

Α/α	ΟΝΟΜΑ ΕΠΩΝΥΜΟ	ΒΑΘΜΙΔΑ/ΙΔΙΟΤΗΤΑ	ΨΗΦΙΑΚΗ ΥΠΟΓΡΑΦΗ
	ΔΡΟΣΟΣ ΧΡΗΣΤΟΣ	ΕΔΙΠ Α	Christos Drosos Digitally signed by Christos Drosos Date: 2023.07.18 00:34:37 +03'00'
	ΛΑΣΚΑΡΗΣ ΝΙΚΟΣ	ΕΠΙΚΟΥΡΟΣ	Nikolaos Laskaris Digitally signed by Nikolaos Laskaris Date: 2023.07.23 11:35:25 +03'00'
	ΣΚΛΑΒΟΥΝΟΥ ΕΛΕΝΗ	ΛΕΚΤΟΡΑΣ ΕΦΑΡΜΟΓΩΝ	Eleni-Orsalia Sklavounou Digitally signed by Eleni-Orsalia Sklavounou Date: 2023.07.22 17:58:40 +03'00'

ΔΗΛΩΣΗ ΣΥΓΓΡΑΦΕΑ ΠΤΥΧΙΑΚΗΣ/ΔΙΠΛΩΜΑΤΙΚΗΣ ΕΡΓΑΣΙΑΣ

Ο κάτωθι υπογεγραμμένος Μαστρομιχάλης Κωνσταντίνος του Δημητρίου, με αριθμό μητρώου 18389313 φοιτητής του Πανεπιστημίου Δυτικής Αττικής της Σχολής Μηχανικών του Τμήματος Μηχανικών Βιομηχανικής Σχεδίασης και Παραγωγής, δηλώνω υπεύθυνα ότι:

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

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

Ο Δηλών

Μαστρομιχάλης Κωνσταντίνος

ΠΕΡΙΕΧΟΜΕΝΑ

Περιεχόμενα

ΕΥΧΑΡΙΣΤΙΕΣ

Μέσα από τα παρακάτω λόγια, νιώθω την ανάγκη να εκφράσω τις ευχαριστίες μου στον επιβλέποντα καθηγητή μου, Καθ. Χρήστο Δρόσο για την βοήθεια που μου προσέφερε με σκοπό την επίτευξη της διπλωματικής μου εργασίας. Θα ήθελα επίσης να ευχαριστήσω τα μέλη της τριμελούς επιτροπής εξέτασης αυτής της εργασίας. Τέλος θα ήθελα να εκφράσω τις θερμές μου ευχαριστίες μέσα από τα βάθη της καρδιάς μου στην οικογένεια μου για την υποστήριξη, και την συμπαράσταση που μου έδειξαν όλα τα χρόνια των φοίτησής μου.

Περίληψη

Με την αυξανόμενη χρήση της τεχνολογίας στον τομέα της ιατρικής επιστήμης, η ασφάλεια των υπολογιστικών συστημάτων και δικτύων αποτελεί μία κρίσιμη ανησυχία που πρέπει να ληφθεί σοβαρά υπόψη. Οι παραβιάσεις της κυβερνοασφάλειας μπορούν να επιφέρουν σοβαρές συνέπειες όπως την παραβίαση των δεδομένων των ασθενών και τη διακοπή κρίσιμων ιατρικών λειτουργιών. Η παρούσα διπλωματική εργασία ερευνά τα προβλήματα και τις βέλτιστες πρακτικές για την ασφάλεια των υπολογιστών και την κυβερνοασφάλεια στον τομέα της ιατρικής επιστήμης. Εξετάζονται οι διάφοροι τύποι κυβερνοαπειλών, οι ευπάθειες των ιατρικών συστημάτων και των δικτύων, καθώς και οι στρατηγικές και οι τεχνολογίες που μπορούν να χρησιμοποιηθούν για την πρόληψη και την αντιμετώπιση των κινδύνων.

Επίσης γίνεται έρευνα πάνω στα νομοθετικά πλαίσια και τα πρότυπα που διέπουν την κυβερνοασφάλεια στον τομέα της ιατρικής επιστήμης, όπως ο νόμος περί Φορητότητας και Λογοδοσίας Ασφάλισης Υγείας (Health Insurance Portability and Accountability Act - HIPAA) και το Πλαίσιο Κυβερνοασφάλειας του Εθνικού Ινστιτούτου Προτύπων και Τεχνολογίας (National Institute of Standards and Technology - NIST).

Abstract

With the increasing use of technology in the field of medical science, the security of computer systems and networks has become a critical concern. Cybersecurity breaches can have serious consequences, including compromised patient data and disrupted medical operations. This thesis explores the challenges and best practices for computer security and cybersecurity in the medical science field. It examines the various types of cyber threats, the vulnerabilities of medical systems and networks, and the strategies and technologies that can be used to prevent and mitigate cybersecurity risks.

The thesis also investigates the regulatory frameworks and industry standards that govern cybersecurity in the medical science field, including the Health Insurance Portability and Accountability Act (HIPAA) and the National Institute of Standards and Technology (NIST) Cybersecurity Framework.

This thesis provides a comprehensive understanding of the current state of computer security and cybersecurity in the medical science field, and offers recommendations for improving security practices and ensuring the confidentiality, integrity, and availability of medical data and systems.

Κεφάλαιο 1. Εισαγωγή

1.1 Εισαγωγή

1.1.1 Εισαγωγή

Ο τομέας της ιατρικής επιστήμης έχει επανασχεδιαστεί λόγω της αυξανόμενης χρήσης της τεχνολογίας τα τελευταία χρόνια. Οι ιατρικές οργανώσεις βασίζονται στα υπολογιστικά συστήματα και στα δίκτυα των υπολογιστών για την διαχείριση και την αποθήκευση των ιατρικών δεδομένων. (David Blumenthal, 2010).

Ιατρικά μέσα όπως η τηλεϊατρική και οι φορητές εφαρμογές εφαρμόζονται όλο και περισσότερο τα τελευταία χρόνια ωστόσο, τα σύγχρονα ιατρικά μέσα που βασίζονται στην πρόοδο της τεχνολογίας μπορούν να επιφέρουν σοβαρούς κινδύνους.

Οι ιατρικές οργανώσεις μπορούν να υποστούν σοβαρές συνέπειες αν παραβιαστεί το επίπεδο κυβερνοασφάλειας που διαθέτουν. Η συνεχής ανάπτυξη της τεχνολογίας απαιτεί την εφαρμογή ισχυρών πρωτοκόλλων ασφαλείας προκειμένου να διασφαλιστεί η προστασία των ιατρικών δεδομένων και συστημάτων. (Emmanouil G. Spanakis, 2020)

1.1.2 Ιστορική Αναδρομή Της Ιατρικής Επιστήμης

Η ιστορία της ιατρικής επιστήμης χρονολογείται χιλιάδες χρόνια πίσω. Κατά τον Μεσαίωνα, η ιατρική γνώση βασιζόταν στις διδασκαλίες των Ελλήνων και των Ρωμαίων γιατρών. Η περίοδος της Αναγέννησης είδε ένα σημαντικό ενδιαφέρον για την επιστήμη και την ανθρώπινη ανατομία, συνεισφέροντας σημαντικά στην κατανόηση του ανθρώπινου σώματος (Castiglioni, 2019).

Ο 19ος και ο 20ός αιώνας γνώρισε αξιοσημείωτη πρόοδο στην ιατρική επιστήμη. Για παράδειγμα, ο κλάδος της ανοσολογίας και η ανακάλυψη της αναισθησίας αποτέλεσαν σημαντικά επιτεύγματα.

Ο 20ός αιώνας γνώρισε ραγδαίες προόδους στην ιατρική τεχνολογία και στην ανάπτυξη των ιατρικών ειδικοτήτων. Η ανακάλυψη των αντιβιοτικών έφερε επανάσταση στη θεραπεία των βακτηριακών λοιμώξεων, ενώ η εισαγωγή στην τεχνολογία των ακτίνων Χ, έφερε επανάσταση στην ιατρική διάγνωση.

Τις τελευταίες δεκαετίες η ιατρική επιστήμη έχει κάνει τεράστια βήματα προόδου σε πολλούς τομείς, όπως την εξατομικευμένη ιατρική και την ιατρική ρομποτική. Η ψηφιακή τεχνολογία υγείας έχει επιφέρει νέες δυνατότητες για τη διάγνωση, τη θεραπεία και τη φροντίδα των ασθενών.

1.1.3 Σκοπός

Ο σκοπός της συγκεκριμένης διπλωματικής εργασίας είναι η διερεύνηση των κυβερνοαπειλών και των βέλτιστων πρακτικών και τεχνολογιών που εφαρμόζονται στον τομέα της ιατρικής επιστήμης. Αναλύεται η ασφάλεια των υπολογιστών και η κυβερνοασφάλεια στον τομέα της ιατρικής επιστήμης, επιτρέποντας στον αναγνώστη να κατανοήσει τους πιθανούς κινδύνους που αντιμετωπίζουν οι ιατρικές οργανώσεις, καθώς και τα μέτρα προστασίας για την ενίσχυση της κυβερνοασφάλειας.

1.2 Ανασκόπηση

1.2.1 Επισκόπηση

Η διασφάλιση της προστασίας των ιατρικών υπολογιστικών συστημάτων και των δικτύων είναι απαραίτητη ,καθώς οι κυβερνοαπειλές γίνονται όλο και πιο διαδεδομένες λόγω της ανάπτυξης της τεχνολογίας. Η κυβερνοασφάλεια στον τομέα της ιατρικής επιστήμης, αναφέρεται στην πρακτική της προστασίας των ηλεκτρονικών πληροφοριών και των ιατρικών συστημάτων.

Οι κυβερνοεπιθέσεις έχουν την δυνατότητα να βλάψουν ιατρικές συσκευές και ιατρικά μηχανήματα. Η ζωή ενός ασθενή μπορεί να βρεθεί άμεσα σε κίνδυνο αν υπάρξει μια επιτυχημένη κυβερνοεπίθεση. Είναι πολύ σημαντικό μια ιατρική οργάνωση να έχει λάβει όλα τα απαραίτητα μέτρα ασφαλείας για την εξάλειψη των κυβερνοεπιθέσεων και των απειλών. (Emmanouil G. Spanakis, 2020)

1.2.2 Κυβερνοαπειλές

Οι κυβερνοαπειλές αποτελούν μια κρίσιμη ανησυχία για τους οργανισμούς υγείας, λόγω του ευαίσθητου και του εμπιστευτικού χαρακτήρα των δεδομένων που διαχειρίζονται. Το κακόβουλο λογισμικό (malware) είναι σχεδιασμένο για να προκαλέσει ζημιά, διαταραχή ή να αποκτήσει μη εξουσιοδοτημένη πρόσβαση σε έναν υπολογιστικό σύστημα. Το ransomware είναι ένα είδος κακόβουλου λογισμικού που κρυπτογραφεί τα δεδομένα του θύματος και απαιτεί πληρωμή για το κλειδί αποκρυπτογράφησης. Το ηλεκτρονικό ψάρεμα (phising) είναι μια μορφή κυβερνοεπίθεσης, όπου οι επιτιθέμενοι επιχειρούν να εξαπατήσουν άτομα με σκοπό την αποκάλυψη ευαίσθητων πληροφοριών παριστάνοντας μια αξιόπιστη οντότητα

Είναι πολύ σημαντικό για τους ιατρικούς οργανισμούς να λάβουν τα απαραίτητα μέτρα ασφαλείας. Αυτό περιλαμβάνει, την εκπαίδευση του προσωπικού σε πρακτικές κυβερνοασφαλείας, την θωράκιση των ιατρικών συστημάτων και συσκευών, και την ανάπτυξη ενός σχεδίου ανταπόκρισης. (Emmanouil G. Spanakis, 2020)

1.2.3 Κενά Ασφαλείας

Τα ιατρικά υπολογιστικά συστήματα και δίκτυα αντιμετωπίζουν ευπάθειες όπου οι επιτιθέμενοι μπορούν να εκμεταλλευτούν. Μία από τις βασικές ευπάθειες είναι το υποβαθμισμένο λογισμικό. Οι ιατρικοί οργανισμοί συχνά βασίζονται σε συστήματα τεχνολογίας που δεν υποστηρίζονται πλέον, καθιστώντας τα ευάλωτα σε κυβερνοεπιθέσεις. Μια μελέτη του Ινστιτούτου Ponemon έδειξε ότι το 67% των ιατρικών οργανισμών είχε υποστεί παραβίαση των δεδομένων λόγω υποβαθμισμένου λογισμικού. **(**Ponemon, 2019)

Μία άλλη ευπάθεια που θεωρείτε συνηθισμένη, είναι οι αδύναμοι κωδικοί πρόσβασης. Στον ιατρικό τομέα, οι εργαζόμενοι συχνά χρησιμοποιούν αδύναμους κωδικούς

πρόσβασης ή επαναχρησιμοποιούν τους ίδιους κωδικούς για πολλούς λογαριασμούς, κάτι που μπορεί να εκμεταλλευτούν οι επιτιθέμενοι για να αποκτήσουν μη εξουσιοδοτημένη πρόσβαση στις πληροφορίες των ασθενών. Σε μια έκθεση της εταιρείας Verizon, διαπιστώθηκε ότι το 77% των παραβιάσεων έγινε λόγω αδύναμων διαπιστευτηρίων. (Langlois, 2020)

Η ανεπαρκής εκπαίδευση των εργαζομένων είναι επίσης μια ευπάθεια που μπορεί να εκμεταλλευτούν οι επιτιθέμενοι. Οι υπάλληλοι μπορεί να επισκεφθούν κακόβουλες ιστοσελίδες και να προβούν σε λήψη κακόβουλου λογισμικού εάν δεν εκπαιδευτούν σωστά για να αναγνωρίζουν και να αντιμετωπίζουν απειλές. Μια έρευνα της IBM έδειξε ότι ο ανθρώπινος παράγοντας συνέβαλε κοντά στο 95% των περιστατικών ασφαλείας. (IBM, 2020)

Οι ιατρικές οργανώσεις πρέπει να δώσουν προτεραιότητα στη διαχείριση των κενών ασφαλείας για να μειώσουν τον κίνδυνο των κυβερνοεπιθέσεων. Αυτό περιλαμβάνει την υλοποίηση των τακτικών ενημερώσεων και των επιδιορθώσεων λογισμικού, την επιβολή ισχυρών κωδικών πρόσβασης, και την παροχή εκπαίδευσης στους εργαζομένους που αφορούν τις βέλτιστες πρακτικές κυβερνοασφάλειας.

1.2.4 Βέλτιστες Πρακτικές

Οι βέλτιστες πρακτικές για την πρόληψη και την αντιμετώπιση των κινδύνων κυβερνοασφάλειας θεωρούνται αναγκαίες για την προστασία των ιατρικών δεδομένων. (Frank Luh, 2020). Ορισμένες από τις σημαντικότερες πρακτικές που μπορούν να υιοθετηθούν από τις ιατρικές οργανώσεις περιλαμβάνουν

• Το τείχος προστασίας (Firewall): Το τείχος προστασίας είναι ένα σύστημα ασφαλείας δικτύου που παρακολουθεί και ελέγχει την εισερχόμενη και εξερχόμενη κίνηση βάσει των προκαθορισμένων κανόνων ασφαλείας. Λειτουργεί ως ένα φράγμα μεταξύ ενός αξιόπιστου και ασφαλούς εσωτερικού δικτύου, και ενός αναξιόπιστου εξωτερικού δικτύου, όπως είναι το διαδίκτυο. Τα τείχη προστασίας εμποδίσουν την μη εξουσιοδοτημένη πρόσβαση στα δίκτυα των ιατρικών οργανώσεων, και συμβάλουν στην προστασία των ιατρικών δεδομένων.

• Κρυπτογράφηση (Encryption): Η κρυπτογράφηση είναι η διαδικασία μετατροπής των δεδομένων σε κώδικα με σκοπό να αποτραπεί η πρόσβαση σε αυτά. Οι ιατρικοί οργανισμοί χρησιμοποιήσουν την κρυπτογράφηση για την προστασία των προσωπικών τους δεδομένων. Η κρυπτογράφηση διασφαλίζει ότι μόνο οι εξουσιοδοτημένοι χρήστες μπορούν να έχουν πρόσβαση στα δεδομένα, ακόμη και αν αυτά παραβιαστούν από κάποιον επιτιθέμενο.

• Έλεγχος ταυτότητας πολλών παραγόντων (Multi-Factor Authentication) : Ο έλεγχος ταυτότητας πολλών παραγόντων είναι ένας μηχανισμός ασφαλείας που απαιτεί από τους χρήστες να παρέχουν περισσότερα από ένα μέσο αναγνώρισης πριν από την χορήγηση πρόσβασης σε ένα σύστημα ή ένα δίκτυο υπολογιστών. Οι ιατρικές οργανώσεις μπορούν να χρησιμοποιήσουν τον έλεγχο ταυτότητας πολλών παραγόντων για να προστατεύσουν τα ιατρικά τους αρχεία από τυχόν παραβιάσεις. Ένας κωδικός πρόσβασης και η αναγνώριση των δακτυλικών αποτυπωμάτων, είναι ένα παράδειγμα ελέγχου ταυτότητας πολλών παραγόντων.

• Ενημερώσεις λογισμικού: Οι ιατρικές οργανώσεις πρέπει να ενημερώνουν συχνά το λογισμικό που διαθέτουν στα πληροφοριακά τους συστήματα. Οι ενημερώσεις λογισμικού συνήθως περιλαμβάνουν διορθώσεις που αφορούν θέματα ασφαλείας.

• Εκπαίδευση προσωπικού: Για την διασφάλιση της αναγνώρισης και της αντιμετώπισης των διάφορων κινδύνων, το προσωπικό που εργάζεται στις ιατρικές οργανώσεις θα πρέπει να έχει εκπαιδευτεί σωστά. Για παράδειγμα, οι διάφοροι τύποι επιθέσεων, και οι βέλτιστες πρακτικές για τη δημιουργία και τη διαχείριση των κωδικών πρόσβασης θα πρέπει να περιλαμβάνονται στην εκπαίδευση των εργαζομένων.

Ορισμένες επιπλέον τεχνολογίες που μπορούν να χρησιμοποιηθούν για την πρόληψη και αντιμετώπιση κινδύνων κυβερνοασφάλειας σε ιατρικούς οργανισμούς περιλαμβάνουν συστήματα ανίχνευσης διείσδυσης (IDS), συστήματα πρόληψης διείσδυσης (IPS) και συστήματα διαχείρισης πληροφοριών ασφαλείας και συμβάντων (SIEM). Αυτές οι τεχνολογίες μπορούν να βοηθήσουν στην αναγνώριση και αντιμετώπιση πιθανών κινδύνων ασφάλειας σε πραγματικό χρόνο.

1.3 Οργάνωση Διπλωματικής Εργασίας

1.3.1 Οργάνωση

Το κεφάλαιο 1 αποτελεί μια εισαγωγή στις κυβερνοαπειλές που αντιμετωπίζουν οι ιατρικές οργανώσεις, καθώς και στις βέλτιστες πρακτικές και τεχνολογίες που εφαρμόζονται, για την έγκυρη πρόληψη και αντιμετώπιση των κυβερνοαπειλών. Στο κεφάλαιο 2 περιγράφονται οι κυβερνοαπειλές που αντιμετωπίζουν οι ιατρικές οργανώσεις. Στο κεφάλαιο 3 περιγράφονται οι βέλτιστες πρακτικές κυβερνοασφάλειας που πρέπει να εφαρμόζονται από τις ιατρικές οργανώσεις, για τον περιορισμό των κυβερνοαπειλών. Στο κεφάλαιο 4 περιγράφονται οι τεχνολογίες που χρησιμοποιούν οι ιατρικές οργανώσεις για την αντιμετώπιση των κυβερνοαπειλών, καθώς και οι προηγμένες τεχνολογίες κυβερνοασφάλειας στον τομέα της ιατρικής επιστήμης.

Κεφάλαιο 2. Κυβερνοαπειλές Στην Ιατρική Επιστήμη

2.1 Κυβερνοαπειλές

2.1.1 Επισκόπηση

Οι κυβερνοαπειλές αποτελούν μια σοβαρή απειλή για τον τομέα της ιατρικής επιστήμης. Οι ιατρικές οργανώσεις διαθέτουν κρίσιμα και εξειδικευμένα δεδομένα και μπορούν να γίνουν στόχοι από κυβερνοεγκληματίες. Μια κυβερνοεπίθεση μπορεί να προκαλέσει οικονομικές ζημιές, παραβιάσεις ιατρικών δεδομένων, και διακοπές κρίσιμων ιατρικών λειτουργιών. (Raul Luna, 2016)

Οι κυβερνοαπειλές αποτελούν οποιαδήποτε κακόβουλη ενέργεια που έχει στόχο την παραβίαση της εμπιστευτικότητας (Confidentiality), ακεραιότητας (Integrity) ή διαθεσιμότητας (Availability). Οι κυβερνοαπειλές που μπορεί να αντιμετωπίσουν οι ιατρικές οργανώσεις είναι οι εξής:

• Κακόβουλο Λογισμικό (Malware): Το κακόβουλο λογισμικό κατασκευάστηκε για να αποκτήσει μη εξουσιοδοτημένη πρόσβαση σε υπολογιστικά συστήματα και να προκαλέσει σοβαρές δυσλειτουργίες και ζημιές.

• Λογισμικό Κρυπτογράφησης (Ransomware): Το ransomware αποτελεί μια κατηγορία κακόβουλου λογισμικού που κρυπτογραφεί τα αρχεία ενός χρήστη. Το ransomware

ζητάει από τον χρήστη να πληρώσει προκειμένου να του δοθεί το ειδικό κλειδί αποκρυπτογράφησης για την ανάκτηση των αρχείων. Μία επίθεση ransomware μπορεί να προκαλέσει σοβαρή ζημιά σε μια ιατρική οργάνωση λόγο της κρυπτογράφησης των ιατρικών αρχείων. (Qian Chen, 2017)

• Ηλεκτρονικό Ψάρεμα (Phishing): Η αποστολή πλαστών ηλεκτρονικών μηνυμάτων σε χρήστες με σκοπό την εξαπάτηση και την αποκάλυψη πληροφοριών ονομάζεται ηλεκτρονικό ψάρεμα. Οι ιατρικές οργανώσεις μπορεί να θεωρηθούν ευάλωτες στις επιθέσεις ηλεκτρονικού ψαρέματος διότι διαθέτουν ιατρικά και προσωπικά δεδομένα ασθενών. (Ramzan, 2010)

• Κατανεμημένη επίθεση άρνησης υπηρεσίας (Distributed Denial Of Service – DDos): Μια επίθεση DDoS έχει σκοπό στο να υπερφορτώσει μια ιστοσελίδα ή ένα δίκτυο υπολογιστών, κάνοντας το μη προσβάσιμο στους χρήστες. Οι επιθέσεις DDoS έχουν την δυνατότητα να προκαλέσουν διακοπές σε ιατρικές λειτουργίες, με αποτέλεσμα οι ασθενείς να περιορίζονται ή και να μην έχουν καθόλου πρόσβαση σε ιατρικές υπηρεσίες. (Khatkar, Kumar, & Kumar, 2020)

Μια κυβερνοεπίθεση μπορεί να προκαλέσει τα παρακάτω:

• Παραβίαση Δεδομένων: Μια κυβερνοεπίθεση μπορεί να οδηγήσει στην απώλεια των ιατρικών δεδομένων.

• Διακοπή Ιατρικής Υπηρεσίας: Μια ιατρική υπηρεσία μπορεί να διακοπεί εξαιτίας μιας κυβερνοεπίθεσης, προκαλώντας σοβαρούς περιορισμούς στην περίθαλψη των ασθενών.

• Νομικές Συνέπειες: Οι ιατρικοί οργανισμοί έχουν ηθικές και νομικές υποχρεώσεις στο να προστατεύουν τα δεδομένα των ασθενών. Μια κυβερνοεπίθεση μπορεί να έχει σοβαρές επιπτώσεις στα νομικά πλαίσια και τους κανονισμούς, επιφέροντας κυρώσεις και πρόστιμα.

Συνοψίζοντας, οι κυβερνοαπειλές αποτελούν έναν κρίσιμο κίνδυνο για τις ιατρικές οργανώσεις, και είναι απαραίτητο να ληφθούν τα κατάλληλα μέτρα προστασίας. Αυτό περιλαμβάνει την εφαρμογή αξιόπιστων μέτρων κυβερνοασφάλειας, την εκπαίδευση των εργαζομένων σε πρακτικές κυβερνοασφάλειας, και έχοντας ένα διαθέσιμο πλάνο ανταπόκρισης σε περίπτωση που διαπιστωθεί οποιαδήποτε μορφή κυβερνοεπίθεσης.

2.1.2 Κακόβουλο Λογισμικό

Ο όρος κακόβουλο λογισμικό (malicious software ή malware) αναφέρεται σε κάθε πρόγραμμα που έχει σχεδιαστεί για να προκαλέσει ζημιά σε ένα υπολογιστικό σύστημα, δίκτυο ή συσκευή. Στην ιατρική επιστήμη, το malware αποτελεί κρίσιμη απειλή για την εμπιστευτικότητα, την ακεραιότητα και την διαθεσιμότητα των προσωπικών δεδομένων των ασθενών, καθώς και για την ασφάλεια και την αποτελεσματικότητα των ιατρικών συστημάτων και συσκευών.

2.1.2.1 Ιοί

Οι ιοί (viruses) είναι ένα είδος κακόβουλου λογισμικού. Οι ιοί έχουν την δυνατότητα να μολύνουν ένα υπολογιστικό σύστημα, να αναπαράγουν τον εαυτό τους, και να εξαπλώνονται σε άλλα υπολογιστικά συστήματα. Οι ιοί μπορούν να προκαλέσουν την απώλεια των ιατρικών δεδομένων και να επιφέρουν διακοπές στις λειτουργίες των υπολογιστικών συστημάτων. Οι ιατρικοί οργανισμοί θεωρούνται αρκετά ευάλωτοι στους ιούς, καθώς βασίζονται σε ένα μεγάλο βαθμό στην πληροφορική για τη διαχείριση των δεδομένων των ασθενών. (Aycock, 2006)

Υπάρχουν αρκετοί διαφορετικοί τύποι ιών όπως τα μολυσμένα αρχεία (file infectors), ιοί τομέα εκκίνησης (boot sector viruses), μακροϊοί (macro viruses) και ιοί σεναρίων (script viruses). Τα file infectors μπορούν να ενσωματωθούν σε εκτελέσιμα αρχεία και να εξαπλωθούν όταν αυτά τα αρχεία ανοίγονται ή εκτελούνται. Οι ιοί τομέα εκκίνησης εισβάλλουν στον τομέα εκκίνησης ενός σκληρού δίσκου, ο οποίος είναι υπεύθυνος για την εκκίνηση του λειτουργικού συστήματος του υπολογιστή. Οι μακροϊοί προσαρτώνται σε έγγραφα και ενεργοποιούνται όταν το έγγραφο ανοίγει, ενώ οι ιοί σεναρίου μολύνουν ιστοσελίδες και άλλους διαδικτυακούς πόρους.

Όταν ένας ιός μολύνει ένα υπολογιστικό σύστημα μπορεί να προκαλέσει διάφορες κακόβουλες ενέργειες όπως την κλοπή των δεδομένων, την καταστροφή αρχείων, και την απενεργοποίηση των μέτρων ασφαλείας. Οι ιοί μπορούν επίσης να εξαπλωθούν αρκετά γρήγορα σε ένα δίκτυο, μολύνοντας πολλά συστήματα και προκαλώντας εκτεταμένες ζημιές. (Aycock, 2006)

Οι ιατρικές οργανώσεις, για να προστατευτούν από τους ιούς θα πρέπει να διαθέτουν το κατάλληλο antivirus και να το ενημερώνουν συχνά. Οι υπάλληλοι σε μια ιατρική οργάνωση θα πρέπει να έχουν εκπαιδευτεί σχετικά με το πώς να αναγνωρίζουν και να αποφεύγουν κινδύνους όπως, τα ύποπτα συνημμένα αρχεία ηλεκτρονικού ταχυδρομείου ή τις μη εξουσιοδοτημένες λήψεις λογισμικού. Η τακτική δημιουργία αντιγράφων ασφαλείας συστημάτων (backups) μπορεί να βοηθήσει στην αντιμετώπιση μιας επίθεσης από έναν ιό, διότι οι ιατρικές οργανώσεις θα έχουν την δυνατότητα να επαναφέρουν τα δεδομένα τους.

Ένας ιός μπορεί να έχει σοβαρές επιπτώσεις στον ιατρικό τομέα με πολλούς τρόπους. Μια από τις πιο σημαντικές επιπτώσεις είναι η ασφάλεια των δεδομένων των ασθενών. Όταν ένα σύστημα μολυνθεί από έναν ιό, τα ιατρικά δεδομένα των ασθενών μπορούν να παραβιαστούν και να χρησιμοποιηθούν για διάφορες κακόβουλες ενέργειες.

Ένας ιός μπορεί επίσης να διαταράσσει συστήματα και διαδικασίες. Για παράδειγμα, αν ένας ιός μολύνει το ηλεκτρονικό σύστημα ιατρικών αρχείων ενός νοσοκομείου, μπορεί να επιφέρει προβλήματα στις διαδικασίες περίθαλψης των ασθενών. Επιπλέον, αν κάποιος ιός μολύνει μια ιατρική συσκευή, ο ασθενής μπορεί να βρεθεί σε άμεσα σε κίνδυνο.

Ένας ιός μπορεί να έχει σημαντική επίδραση στην ιατρική επιστήμη, με συνέπειες που κυμαίνονται από την ασφάλεια των πληροφοριών των ασθενών και την ασφάλεια τους έως την αποτελεσματικότητα των ιατρικών υπηρεσιών που παρέχονται. Επομένως είναι σημαντικό για ιατρικούς οργανισμούς να λαμβάνουν προληπτικά μέτρα για την πρόληψη, την ανίχνευση και την αντιμετώπιση των ιών. (Lauren E Branch, 2019)

2.1.2.2 Worms

Τα worms είναι ένα είδος κακόβουλου λογισμικού που μπορούν να μολύνουν υπολογιστικά συστήματα και δίκτυα. Σε αντίθεση με τους ιούς τα worms δεν απαιτούν κάποιο πρόγραμμα για να προσκολληθούν. Έχουν την δυνατότητα να εξαπλώνονται ανεξάρτητα μέσω του δικτύου και να αναπαράγονται, προκαλώντας σοβαρές ζημιές στα συστήματα που μολύνουν.

Τα worms θεωρούνται αρκετά επικίνδυνα για τους ιατρικούς οργανισμούς, καθώς μπορούν εύκολα να διαδοθούν μέσω των διασυνδεδεμένων ιατρικών συσκευών,

καταστρέφοντας την ακεραιότητα και την εμπιστευτικότητα των προσωπικών δεδομένων των ασθενών. Τα worms μπορούν να προκαλέσουν διακοπές στις ιατρικές λειτουργίες, καθώς και να υπερφορτώσουν και να καταρρεύσουν ιατρικά υπολογιστικά συστήματα που ευθύνονται για την περίθαλψη των ασθενών. (Fosnock, n.d.)

Ένα από τα πιο γνωστά παραδείγματα επίθεσης τύπου worm στην ιατρική επιστήμη συνέβη το 2017, όταν ένα worm με το όνομα WannaCry μόλυνε υπολογιστές σε νοσοκομεία και ιατρικές εγκαταστάσεις σε όλο τον κόσμο. Αυτή η επίθεση προκάλεσε σημαντικές διαταραχές. Πολλά ιατρικά ιδρύματα και νοσοκομεία αναγκάστηκαν να ακυρώσουν σημαντικά ραντεβού που είχαν προγραμματίσει, λόγω της κατάρρευσης των ηλεκτρονικών συστημάτων και της παραβίασης των ιατρικών δεδομένων. (Hsiao & Kao, 2018)

Οι ιατρικές οργανώσεις για να προστατεύονται από τα worms θα πρέπει να εφαρμόζουν μέτρα ασφαλείας όπως είναι, οι συχνές ενημερώσεις λογισμικού, ο διαχωρισμός του δικτύου, και η εκπαίδευση των χρηστών. Επιπλέον, οι ιατρικές οργανώσεις θα πρέπει να διαθέτουν ένα σχέδιο αντιμετώπισης, που σκοπό θα έχει την μείωση της ζημιάς των υπολογιστικών ιατρικών συστημάτων, και την ανάκτηση των ιατρικών λειτουργιών από μια επίθεση τύπου worm.

Συνοψίζοντας, τα worms αποτελούν μια σοβαρή απειλή για την κυβερνοασφάλεια των ιατρικών οργανισμών, καθώς μπορούν να εξαπλωθούν εύκολα μέσω διασυνδεδεμένων συστημάτων και να προκαλέσουν ζημιές στα δεδομένα των ασθενών.

2.1.2.3 Trojans

Ο δούρειος ίππος (Trojan ή Trojan Horse) είναι ένα είδος κακόβουλου λογισμικού που παρουσιάζεται ως ένα ασφαλές και νόμιμο λογισμικό. Ο σκοπός του δούρειου ίππου είναι να εξαπατήσει τους χρήστες και να τους πείσει να το εγκαταστήσουν στα υπολογιστικά τους συστήματα. Τα trojans μπορούν να προκαλέσουν την κλοπή των προσωπικών πληροφοριών και την καταστροφή των αρχείων. Στον τομέα της ιατρικής επιστήμης, οι επιθέσεις trojans μπορούν να οδηγήσουν στην παραβίαση των ιατρικών

δεδομένων, στην απώλεια προσωπικών πληροφοριών, και στη διακοπή κρίσιμων υπηρεσιών υγείας. (Mishra, 2010)

Τα trojans συνήθως μεταδίδονται μέσω συνημμένων αρχείων ηλεκτρονικού ταχυδρομείου, λήψης αρχείων, ή ενημερώσεων λογισμικού. Τα trojans μπορούν να εκτελέσουν διάφορες κακόβουλες ενέργειες, όπως τη δημιουργία κρυφών εισόδων σε έναν χάκερ για τη πρόσβαση σε ένα σύστημα, την κλοπή κωδικών πρόσβασης, ή την τροποποίηση ιατρικών αρχείων.

Για να αποτραπούν οι επιθέσεις trojans, οι ιατρικές οργανώσεις πρέπει να εφαρμόζουν τα κατάλληλα μέτρα ασφαλείας. Η χρήση ενός προγράμματος κατά των κακόβουλων λογισμικών και η σωστή εκπαίδευση του προσωπικού σε θέματα αναγνώρισης και αποφυγής ηλεκτρονικής απάτης, αποτρέπουν την εγκατάσταση δούρειων ίππων στα ιατρικά υπολογιστικά συστήματα.

2.1.3 Ransomware

Το ransomware είναι ένα είδος κακόβουλου λογισμικού που κρυπτογραφεί τα αρχεία του χρήστη και του ζητάει να πληρώσει ένα χρηματικό ποσό για να λάβει το κλειδί αποκρυπτογράφησης για την ανάκτηση των αρχείων. Το ransomware μπορεί να διαδοθεί με διάφορους τρόπους. Οι απάτες ηλεκτρονικού ταχυδρομείου και οι λήψεις προγραμμάτων από μολυσμένες ιστοσελίδες, είναι ορισμένοι από τους τρόπους μετάδοσης του λογισμικού ransomware. Μόλις ένας υπολογιστής μολυνθεί από το ransomware, τότε εμφανίζεται ένα μήνυμα στον χρήστη που του ζητάει να πληρώσει ένα χρηματικό ποσό για να λάβει το κλειδί αποκρυπτογράφησης.

Το ransomware συχνά ορίζει ένα χρονικό διάστημα στο χρήστη για την καταβολή του ποσού. Αν ο χρήστης βρεθεί εκτός του χρονικού διαστήματος που έχει ορίσει το ransomware, τότε ενδέχεται να υπάρξουν συνέπειες, όπως για παράδειγμα ο διπλασιασμός του αρχικού ποσού πληρωμής, ή και η πλήρη διαγραφή των αρχείων. Το ransomware συνήθως ζητάει από τον χρήστη να πληρώσει σε κρυπτονομίσματα, καθώς αυτή η μέθοδος πληρωμής καλύπτει την ανωνυμία του επιτιθέμενου. (Brewer, 2016)

Οι ιατρικοί οργανισμοί είναι ιδιαίτερα ευάλωτοι στις επιθέσεις ransomware καθώς βασίζονται στα δεδομένα των ασθενών για την παροχή των υπηρεσιών υγείας. Μια

επίθεση ransomware μπορεί επίσης να κρυπτογραφήσει ιατρικά ηλεκτρονικά συστήματα. Για παράδειγμα, εάν ένα σύστημα ηλεκτρονικών ιατρικών αρχείων ή μια ηλεκτρονική ιατρική συσκευή υποστεί μια επίθεση τύπου ransomware, τότε θα διαταραχθούν οι υπηρεσίες υγείας που προσφέρει μια ιατρική οργάνωση.

Τον Μάιο του 2017, το κακόβουλο λογισμικό WannaCry που χαρακτηρίζεται ως ένα ransomware crypto worm, επιτέθηκε στην Εθνική Υπηρεσία Υγείας (National Health Service ή NHS) στο Ηνωμένο Βασίλειο, προκαλώντας εκτεταμένη αναστάτωση στη φροντίδα των ασθενών. Η επίθεση αυτή, επηρέασε πάνω από 80 οργανισμούς του Εθνικού Συστήματος Υγείας (NHS) όπως νοσοκομεία και κλινικές, και προκάλεσε ακυρώσεις προγραμματισμένων ραντεβού αλλά και χειρουργείων. (Collier, 2017)

Για την προστασία από τις επιθέσεις τύπου ransomware, οι ιατρικοί οργανισμοί θα πρέπει να εφαρμόσουν μια πολυεπίπεδη προσέγγιση στην κυβερνοασφάλεια η οποία θα περιλαμβάνει τακτικά αντίγραφα ασφαλείας, εκπαίδευση των εργαζομένων σε μορφές κοινωνικής μηχανικής, και τη χρήση προγράμματος κατά των κακόβουλων λογισμικών καθώς και τοίχοι προστασίας.

2.1.4 Phising

Η επίθεση phishing είναι μια κατηγορία κυβερνοαπειλής που μπορεί να θέσει σημαντικούς κινδύνους για τους ιατρικούς οργανισμούς. Το phising περιλαμβάνει τη χρήση μηνυμάτων ηλεκτρονικού ταχυδρομείου ή και άλλων μέσων επικοινωνίας με σκοπό την απόσπαση προσωπικών δεδομένων από τους χρήστες. Οι επιθέσεις phising μπορούν να λάβουν διάφορες μορφές, συμπεριλαμβανομένων των μηνυμάτων ηλεκτρονικού ταχυδρομείου που φαίνεται να προέρχονται από έγκυρες πηγές, όπως τράπεζες, κυβερνητικές υπηρεσίες ή και άλλες οργανώσεις. Οι επιθέσεις phishing μπορούν να χρησιμοποιηθούν και για την εγκατάσταση κακόβουλων λογισμικών στο δίκτυο μιας ιατρικής οργάνωσης. (Ramzan, 2010)

Οι ιατρικές οργανώσεις για να προστατευτούν από τις επιθέσεις phising, θα πρέπει να εφαρμόζουν τα κατάλληλα πρωτόκολλα ασφαλείας και να παρέχουν την ανάλογη εκπαίδευση στους εργαζόμενους, σχετικά με το πως να αναγνωρίζουν και να αντιδρούν στις πιθανές επιθέσεις phising. Η εκπαίδευση των εργαζομένων θα πρέπει να

περιλαμβάνει την αναγνώριση των ύποπτων μηνυμάτων ηλεκτρονικού ταχυδρομείου και τον έλεγχο της αυθεντικότητας οποιασδήποτε μορφής επικοινωνίας.

Υπάρχουν επίσης διάφορα τεχνικά μέτρα που μπορούν να εφαρμόσουν οι ιατρικές οργανώσεις για να προστατευτούν από τις επιθέσεις phising. Η χρήση λογισμικού anti-phising, και η εφαρμογή ελέγχου ταυτότητας πολλαπλών παραγόντων και ελέγχων πρόσβασης, θεωρούνται απαραίτητα μέτρα για την αποφυγή των επιθέσεων phising.

Οι ιατρικές οργανώσεις οφείλουν να συμμορφώνονται με τις κανονιστικές απαιτήσεις που σχετίζονται με το απόρρητο και την ασφάλεια των δεδομένων, όπως ο HIPAA και το NIST Cybersecurity Framework. Οι οργανώσεις χρειάζεται να εφαρμόζουν συγκεκριμένα μέτρα ασφαλείας και πρωτόκολλα για την προστασία από επιθέσεις phising. (Gurinder Pal Singh, 2021)

Οι επιθέσεις phising αποτελούν έναν σοβαρό κίνδυνο για τις ιατρικές οργανώσεις, και είναι απαραίτητο να ληφθούν προληπτικά μέτρα προστασίας. Με την εφαρμογή των πρωτοκόλλων ασφαλείας, την παροχή εκπαίδευσης στους εργαζομένους και τη χρήση προηγμένων τεχνολογιών ασφαλείας, οι ιατρικές οργανώσεις μπορούν να προστατευθούν από τις επιθέσεις phising και να διασφαλίζουν τα δεδομένα τους.

2.1.5 Social Engineering

Οι επιθέσεις κοινωνικής μηχανικής είναι μια κατηγορία κυβερνοεπίθεσης που περιλαμβάνει την εκμετάλλευση της ανθρώπινης ψυχολογίας για την απόκτηση της μη εξουσιοδοτημένης πρόσβαση σε προσωπικές πληροφορίες ή συστήματα. Στην ιατρική επιστήμη οι επιθέσεις κοινωνικής μηχανικής αποδεικνύονται ιδιαίτερα αποτελεσματικές, λόγω του ευαίσθητου και εμπιστευτικού χαρακτήρα των πληροφοριών των ασθενών. Οι επιτιθέμενοι μπορούν να χρησιμοποιήσουν διάφορες τεχνικές για την εξαπάτηση των εργαζομένων σε μια ιατρική οργάνωση, όπως το ηλεκτρονικό ψάρεμα. (Francois Mouton, 2016)

Ένας τύπος επίθεσης κοινωνικής μηχανικής ονομάζεται pretexting. Το pretexting περιλαμβάνει την δημιουργία ενός ψεύτικου σεναρίου, που σκοπό έχει να εξαπατήσει τον χρήστη. Ο χρήστης αν δεν είναι κατάλληλα προετοιμασμένος, μπορεί να πιστέψει το ψεύτικο σενάριο που περιλαμβάνεται στην επίθεση, και να αποκαλύψει προσωπικές πληροφορίες στον επιτιθέμενο. Ο επιτιθέμενος εκτός από τα προσωπικά δεδομένα που

μπορεί να αποσπάσει, μπορεί επίσης να χειραγώγηση τον χρήστη. (Zuoguang Wang, 2020)

Ένας άλλος τύπος επίθεσης κοινωνικής μηχανικής είναι το baiting. Το baiting αφορά συνήθως την προσφορά μιας συσκευής όπως για παράδειγμα έναν εξωτερικό σκληρό δίσκο, με σκοπό την απόσπαση προσωπικών δεδομένων. Για παράδειγμα, ένας επιτιθέμενος θα μπορούσε να αφήσει ένα usb flash drive με ετικέτα "πληροφορίες ασθενών" σε ένα κοινό σημείο, με την ελπίδα ότι κάποιος υπάλληλος θα το συνδέσει στον υπολογιστή του. Από τη στιγμή που ο υπάλληλος συνδέσει το usb στον υπολογιστή, μπορεί να εγκαταστήσει κάποιο κακόβουλο λογισμικό χωρίς να το γνωρίζει, η να αποκαλύψει προσωπικά δεδομένα στον επιτιθέμενο. (Lohani, 2019)

Το phishing είναι επίσης ένας τύπος επίθεσης κοινωνικής μηχανικής, ο οποίος περιλαμβάνει την αποστολή ηλεκτρονικών μηνυμάτων που φαίνονται να προέρχονται από νόμιμες και ασφαλής πηγές. Τα μηνύματα αυτά έχουν σχεδιαστεί για να εξαπατήσουν τον παραλήπτη και να τον κάνουν να αποκαλύψει προσωπικές πληροφορίες. Για παράδειγμα, ο επιτιθέμενος μπορεί να προσποιηθεί κάποιον συνάδελφο που εργάζεται σε μια ιατρική οργάνωση, και να στείλει ένα email σε ορισμένους εργαζόμενους που πιστεύει ότι δεν θα τον αναγνωρίσουν. Το email αυτό μπορεί να οδηγεί σε κάποια πλαστή ιστοσελίδα κατασκευασμένη από τον επιτιθέμενο. Η ιστοσελίδα αυτή μπορεί να ζητάει τα διαπιστευτήρια του χρήστη με σκοπό να πραγματοποιηθεί κάποια λειτουργία. Ο χρήστης εκτός από ότι θα αποκαλύψει τα προσωπικά του δεδομένα, ενδέχεται να κάνει και λήψη κάποιου κακόβουλο λογισμικού που μπορεί να βλάψει όλο το δίκτυο.

Για να αποτραπούν οι επιθέσεις κοινωνικής μηχανικής, οι ιατρική οργανισμοί πρέπει να παρέχουν την κατάλληλη εκπαίδευση στους υπαλλήλους, για το πώς να εντοπίζουν και να ανταποκρίνονται τύπους επιθέσεων κοινωνικής μηχανικής. (Ramzan, 2010)

2.1.6 Εσωτερικές Απειλές

Οι εργαζόμενοι ευθύνονται για το επίπεδο κυβερνοασφάλειας μιας ιατρικής οργάνωσης. Οι απειλές που προέρχονται από τους εργαζόμενους χωρίζονται σε δύο κύριες μορφές: τα ακούσια λάθη και οι σκόπιμες κακόβουλες ενέργειες.

Τα ακούσια λάθη περιλαμβάνουν ενέργειες όπως, τις απάτες phishing, την χρήση αδύναμων κωδικών πρόσβασης ή την μη ενημέρωση του λογισμικού. Τα ακούσια λάθη μπορούν να οδηγήσουν στις κυβερνοεπιθέσεις, στις κλοπές προσωπικών δεδομένων, ή στην εγκατάσταση κακόβουλων λογισμικών. (Ramzan, 2010)

Οι σκόπιμες κακόβουλες ενέργειες αποτελούν ένα σοβαρό πρόβλημα για τις ιατρικές οργανώσεις, καθώς οι εργαζόμενοι μπορεί να κλέψουν προσωπικές πληροφορίες της οργάνωσης και να τις πουλήσουν σε πιθανούς ανταγωνιστές ή να τις χρησιμοποιήσουν για προσωπικό τους όφελος. Αυτό ονομάζεται εσωτερική απειλή και θεωρείται δύσκολο να ανιχνευθεί καθώς οι εργαζόμενοι έχουν εξουσιοδοτημένη πρόσβαση στις πληροφορίες που προσπαθούν να αποσπάσουν.

Σύμφωνα με μια έρευνα που διεξήγαγε το ινστιτούτο Ponemon, το 64% των οργανισμών υγείας έχουν υποστεί παραβίαση δεδομένων λόγω αμέλειας ή κακόβουλου σκοπού από τους εργαζομένους (Ponemon Institute, 2019). Αυτό επισημαίνει την ανάγκη για τους οργανισμούς να διαθέτουν τα κατάλληλα προγράμματα εκπαίδευσης και τις ανάλογες πολιτικές κυβερνοασφάλειας, για την μείωση των κακόβουλων πράξεων στο τομέα της κυβερνοασφάλειας από τους εργαζόμενους. (Ponemon, 2019)

Οι ιατρικοί οργανισμοί μπορούν να λάβουν διάφορα μέτρα ώστε να μειώσουν τον κίνδυνο των κυβερνοαπειλών που σχετίζονται με τους εργαζόμενους. Αυτό μπορεί να περιλαμβάνει την εφαρμογή ελέγχων πρόσβασης και συστημάτων παρακολούθησης προκειμένου να διασφαλιστεί ότι οι εργαζόμενοι έχουν πρόσβαση μόνο στα δεδομένα και στα συστήματα που χρειάζονται για να εκτελέσουν τα καθήκοντά τους, την τακτική ενημέρωση και επιδιόρθωση λογισμικών και συστημάτων, και την παροχή πλήρους εκπαίδευσης στον τομέα της κυβερνοασφάλειας σε όλους τους εργαζομένους.

Επιπλέον, οι οργανισμοί έχουν την δυνατότητα να καθιερώσουν σαφείς πολιτικές για το πώς να χειρίζονται τις προσωπικές πληροφορίες, συμπεριλαμβανομένων συγκεκριμένων

οδηγιών για τον τρόπο αποθήκευσης, κοινή χρήσης και απόρριψης. Πρέπει να παρέχεται συνεχής ενημέρωση πάνω στις πολιτικές σε όλους τους εργαζομένους.

Οι ιατρικοί οργανισμοί μπορούν να λάβουν τα κατάλληλα προληπτικά μέτρα για να μειώσουν τον κίνδυνο των περιστατικών κυβερνοασφάλειας που σχετίζονται με τους εργαζόμενους και να προστατεύσουν τα προσωπικά δεδομένα από κυβερνοεγκληματίες.

2.2 Κενά Ασφαλείας

2.2.1 Επισκόπηση

Η ιατρική επιστήμη τα τελευταία χρόνια βασίζεται όλο και περισσότερο σε υπολογιστικά συστήματα και δίκτυα για τη διαχείριση των δεδομένων των ασθενών, την ανταλλαγή πληροφοριών και την παροχή ιατρικών υπηρεσιών. Η πρόοδος της τεχνολογίας έχει επιφέρει πολλά οφέλη στον τομέα της ιατρικής επιστήμης, ωστόσο μπορεί να δημιουργηθούν σημαντικά κενά ασφαλείας που θα πρέπει να αντιμετωπιστούν. Αν οι ιατρικές οργανώσεις δεν εντοπίσουν τα κενά ασφαλείας έγκαιρα, τότε τα ιατρικά υπολογιστικά συστήματα μπορούν να γίνουν ευάλωτα σε κυβερνοεπιθέσεις. (Patricia AH Williams, 2022)

Οι ιατρικές οργανώσεις θεωρούνται ευάλωτες σε κυβερνοεπιθέσεις, διότι συλλέγουν, αποθηκεύουν, και επεξεργάζονται ευαίσθητα και προσωπικά δεδομένα ασθενών. Εκτός από τα προσωπικά δεδομένα των ασθενών, περιλαμβάνονται οι εξετάσεις των ασθενών, τα ιστορικά ασθενειών, και άλλες εμπιστευτικές πληροφορίες. Οι κυβερνοεγκληματίες γνωρίζουν την αξία αυτών των πληροφοριών, και κάνουν ό,τι είναι απαραίτητο για την απόσπαση αυτών των πληροφοριών από τις ιατρικές οργανώσεις.

Ένα άλλο πρόβλημα που αντιμετωπίζουν οι ιατρικές οργανώσεις είναι πως χρησιμοποιούν παλαιά υπολογιστικά συστήματα και μη ενημερωμένα λογισμικά. Όταν μια ιατρική οργάνωση δεν έχει ενημερώσει το λειτουργικό της σύστημα ή χρησιμοποιεί

ένα μη ενημερωμένο λογισμικό για την διεκπεραίωση μιας ιατρικής λειτουργίας, αυτό την καθιστά ευάλωτη σε κυβερνοαπειλές, διότι το λογισμικό δεν θα περιλαμβάνει τα βέλτιστα μέτρα ασφαλείας.

Επιπλέον, αρκετές ιατρικές οργανώσεις διαθέτουν σύνθετα συστήματα πληροφορικής με αποτέλεσμα να υπάρχει δυσκολία στην διαχείριση και στην ασφάλιση των συστημάτων. Εκτός από τα εσωτερικά συστήματα και δίκτυα που χρησιμοποιούνται από μια ιατρική οργάνωση, εφαρμόζονται συστήματα και υπηρεσίες τρίτων, που χρησιμοποιούνται για τη διαχείριση των δεδομένων των ασθενών και την παροχή ιατρικών υπηρεσιών. Αυτή η πολυπλοκότητα καθιστά δύσκολο τον εντοπισμό και την αντιμετώπιση των πιθανών κινδύνων ασφαλείας, αφήνοντας τις ιατρικές οργανώσεις ευάλωτες σε κυβερνοαπειλές. (Patricia AH Williams, 2022)

Μια ιατρική οργάνωση μπορεί επίσης να υποστεί ζημιά και από τους εργαζόμενους. Για παράδειγμα, η λήψη κακόβουλου λογισμικού ή απάτη phishing, μπορεί να διακινδυνεύσει την ασφάλεια των συστημάτων και των δικτύων της ιατρικής οργάνωσης. Σε ορισμένες περιπτώσεις, μπορεί να υφίσταται και κάποια εσωτερική απειλή στην ιατρική οργάνωση και να μην πρόκειται για ανθρώπινο λάθος.

2.2.2 Μη Ενημερωμένο Λογισμικό

Οι ιατρικές οργανώσεις που χρησιμοποιούν ένα μη ενημερωμένο λογισμικό, θέτουν σε κίνδυνο τα ιατρικά υπολογιστικά συστήματα και τα δεδομένα των ασθενών. Οποιοδήποτε λογισμικό που δεν λαμβάνει τακτικά ενημερώσεις ασφαλείας θεωρείται ευάλωτο σε κυβερνοεπιθέσεις, καθώς ο κώδικας του προγράμματος δεν τροποποιείται και δεν ενημερώνεται σε θέματα που αφορούν την ασφάλεια του λογισμικού.

Ένα παράδειγμα που αποδεικνύει πώς ένα μη ενημερωμένο λογισμικό μπορεί να αποτελέσει απειλή για την ασφάλεια ιατρικών οργανισμών, είναι η επίθεση ransomware WannaCry που συνέβη το 2017. Η συγκεκριμένη επίθεση κατάφερε να εκμεταλλευτεί ορισμένα κενά ασφαλείας σε παλαιότερες εκδόσεις των Windows που δεν είχαν ενημερωθεί με τις πιο πρόσφατες ενημερώσεις ασφαλείας. Η επίθεση αυτή κατάφερε να προκαλέσει ζημιά στα ιατρικά υπολογιστικά συστήματα και έθεσε σε κίνδυνο την υγεία των ασθενών. (Savita Mohurle, 2017)

Εκτός από τον κίνδυνο των κυβερνοεπιθέσεων, ένα μη ενημερωμένο λογισμικό μπορεί να προκαλέσει αστάθεια στα ιατρικά συστήματα και διακοπές στις ιατρικές υπηρεσίες, καθώς και τη μη συμμόρφωση με τα κανονιστικά πρότυπα, όπως ο νόμος HIPAA, που απαιτεί από τις οργανώσεις να εφαρμόζουν τα απαραίτητα μέτρα για την προστασία των δεδομένων των ασθενών. (Gurinder Pal Singh, 2021)

Οι ιατρικές οργανώσεις θα πρέπει να ενημερώνουν και να επιδιορθώνουν το λογισμικό στα υπολογιστικά τους συστήματα για την αποφυγή κυβερνοαπειλών. Πρέπει να εφαρμόζεται σε τακτικά χρονικά διαστήματα ο απαραίτητος έλεγχος των ιατρικών συστημάτων, για να διασφαλιστεί πως το λογισμικό είναι ενημερωμένο και πως έχουν γίνει όλες οι απαραίτητες επιδιορθώσεις.

2.2.3 Αδύναμοι Κωδικοί Πρόσβασης

Οι αδύναμοι κωδικοί πρόσβασης αποτελούν μια ευπάθεια για πολλούς ιατρικούς οργανισμούς. Οι εύκολοι κωδικοί πρόσβασης μπορεί να παρέχουν στους κυβερνοεγκληματίες πρόσβαση σε προσωπικά δεδομένα, ιατρικά αρχεία και άλλες εμπιστευτικές πληροφορίες. Για αυτόν τον λόγο πρέπει να διασφαλιστεί, πως οι υπάλληλοι μιας ιατρικής οργάνωσης χρησιμοποιούν ισχυρούς κωδικούς πρόσβασης στους λογαριασμούς τους. Για παράδειγμα ορισμένοι κωδικοί πρόσβασης όπως, “admin” ή “12345” θεωρούνται αδύναμοι κωδικοί πρόσβασης. (Sören Preibusch, 2010)

Ένας κίνδυνος που διατρέχουν οι αδύναμοι κωδικοί πρόσβασης είναι η πιθανότητα επίθεσης brute force. Στην επίθεση αυτήν, ένας hacker χρησιμοποιεί ένα αυτοματοποιημένο λογισμικό για να δοκιμάσει κάθε δυνατό συνδυασμό χαρακτήρων, μέχρι να μαντέψει τον σωστό κωδικό πρόσβασης. Η επίθεση brute force μπορεί να επιτύχει εναντίον αδύναμων κωδικών πρόσβασης που βασίζονται σε κοινές λέξεις ή μοτίβα. Όταν ο κωδικός πρόσβασης αποκρυπτογραφηθεί ο hacker μπορεί να αποκτήσει πρόσβαση στο λογαριασμό που έχει στοχεύσει καθώς και στα απόρρητα δεδομένα που ενδέχεται να υπάρχουν. (Dave, 2013)

Ένας άλλος κίνδυνος που αφορά τους αδύναμους κωδικούς πρόσβασης είναι η δυνατότητα επαναχρησιμοποίησής τους. Αν οι εργαζόμενοι μιας ιατρικής οργάνωσης χρησιμοποιούν τον ίδιο κωδικό πρόσβασης για όλους τους λογαριασμούς που διαθέτουν, τότε η ιατρική οργάνωση και οι λογαριασμοί των υπαλλήλων διατρέχουν σοβαρό κίνδυνο ασφαλείας. Σε περίπτωση που ένας hacker αποκτήσει πρόσβαση σε έναν

λογαριασμό αυτομάτως έχει και την δυνατότητα να έχει πρόσβαση και στους υπόλοιπους λογαριασμούς με τον ίδιο κωδικό. (Sören Preibusch, 2010)

Για την αντιμετώπιση των κινδύνων που προέρχονται από τους αδύναμους κωδικούς πρόσβασης, οι ιατρικές οργανώσεις μπορούν να θέσουν μια πολιτική κωδικού πρόσβασης. Η πολιτική κωδικού πρόσβασης απαιτεί να πληρούνται ορισμένες απαιτήσεις πολυπλοκότητας για τους κωδικούς πρόσβασης. Για παράδειγμα οι κωδικοί πρόσβασης να υποχρεούνται να έχουν ένα συγκεκριμένο μήκος, να περιλαμβάνον έναν συνδυασμό από γράμματα, αριθμούς, σύμβολα, και να μην βασίζονται σε γνωστές λέξεις. (Sören Preibusch, 2010)

Οι κίνδυνοι που διατρέχουν οι ιατρικές οργανώσεις λόγω των αδύναμων κωδικών πρόσβασης είναι σημαντικοί, και μπορούν να οδηγήσουν σε κρίσιμες παραβιάσεις ασφαλείας. Με την εφαρμογή της κατάλληλης πολιτικής κωδικού πρόσβασης καθώς και με την παροχή εκπαίδευσης στους εργαζόμενους, οι ιατρικές οργανώσεις αυξάνουν τον βαθμό προστασίας στα δεδομένα και στους λογαριασμούς που διαθέτουν.

2.2.4 Ανεπαρκής Εκπαίδευση Εργαζομένων

Η ανεπαρκής εκπαίδευση των εργαζομένων στον ιατρικό τομέα αποτελεί ένα σοβαρό πρόβλημα. Όταν οι εργαζόμενοι μιας ιατρικής οργάνωσης δεν έχουν εκπαιδευτεί σωστά πάνω σε θέματα κυβερνοασφάλειας μπορούν να θέσουν σε κίνδυνο τα ιατρικά υπολογιστικά συστήματα και δίκτυα μιας ιατρικής οργάνωσης. (Sokratis Nifakos, 2021)

Η ανεπαρκής εκπαίδευση των εργαζομένων μπορεί να οδηγήσει σε απάτες ηλεκτρονικού ψαρέματος. Στην ιατρική επιστήμη, οι επιθέσεις phishing συχνά στοχεύον το προσωπικό που έχει πρόσβαση σε απόρρητα δεδομένα, όπως ιατροί και διοικητικό προσωπικό. (Ramzan, 2010)

Η ελλιπής εκπαίδευση των εργαζομένων μπορεί επίσης να οδηγήσει σε αδύναμους κωδικούς πρόσβασης. Όταν σε μια ιατρική οργάνωση χρησιμοποιούνται αδύναμοι κωδικοί πρόσβασης τα δεδομένα των ασθενών καθώς και οι λογαριασμοί των υπαλλήλων βρίσκονται σε άμεσο κίνδυνο. Ένας αδύναμος κωδικός πρόσβασης είναι πολύ πιο εύκολο να αποκρυπτογραφηθεί από έναν hacker που χρησιμοποιεί τεχνικές

αποκρυπτογράφησης κωδικών πρόσβασης όπως για παράδειγμα, ή επίθεση brute force. (Dave, 2013)

Οι ιατρικές οργανώσεις μπορούν να μειώσουν τον κίνδυνο των κυβερνοαπειλών παρέχοντας τακτική εκπαίδευση κυβερνοασφάλειας στους υπαλλήλους. Η εκπαίδευση αυτή θα πρέπει να καλύπτει τις βασικές αρχές της κυβερνοασφάλειας, όπως για παράδειγμα την αναγνώριση των επιθέσεων phishing, την δημιουργία ισχυρών κωδικών πρόσβασης και τη χρήση ασφαλών καναλιών επικοινωνίας. Με την κατάλληλη παροχή εκπαίδευσης, ενισχύεται η προστασία των δεδομένων και των ιατρικών υπολογιστικών συστημάτων. (Sokratis Nifakos, 2021)

Η ανεπαρκής εκπαίδευση των εργαζομένων αποτελεί έναν σημαντικό παράγοντα κινδύνου για τις ιατρικές οργανώσεις. Οι ιατρικές οργανώσεις θα πρέπει να εφαρμόζουν τακτικά προγράμματα εκπαίδευσης για τον τομέα της κυβερνοασφάλειας, ώστε οι εργαζόμενοί να αποκτήσουν τις απαραίτητες γνώσεις και δεξιότητες για την αναγνώριση και την αντιμετώπιση των πιθανών κυβερνοαπειλών. Αυτό θα βοηθήσει στη διασφάλιση των δεδομένων των ασθενών και στην προστασία των ιατρικών οργανώσεων από τις επιπτώσεις των κυβερνοεπιθέσεων.

2.3 Μελέτη Περίπτωσης: WannaCry Ransomware

2.3.1 Επισκόπηση

Τον Μάιο του 2017 μια τεράστια παγκόσμια επίθεση ransomware με όνομα: WannaCry κατάφερε και μόλυνε πάνω από 200.000 υπολογιστές σε 150 χώρες. Ο τομέας της ιατρικής επιστήμης υπέστη ένα τεράστιο πλήγμα καθώς τα ιατρικά υπολογιστικά συστήματα των ιατρικών οργανώσεων είχαν καταρρεύσει. Η επίθεση στόχευε υπολογιστές που χρησιμοποιούσαν τα λειτουργικά συστήματα Microsoft Windows. Η επίθεση εκμεταλλεύτηκε την ευπάθεια EternalBlue η οποία φέρεται να αναπτύχθηκε από την Εθνική Υπηρεσία Ασφάλειας των Ηνωμένων Πολιτειών (National Security Agency - NSA). (Qian Chen, 2017)

Η επίθεση WannaCry κρυπτογραφούσε τα ιατρικά δεδομένα και στην συνέχεια ζητούσε από τον χρήστη να πληρώσει ένα χρηματικό ποσό, συνήθως σε κρυπτονομίσματα για

την απόκτηση του κλειδιού αποκρυπτογράφησης. Η υγειονομική υποδομή των ιατρικών οργανώσεων όπως για παράδειγμα, οι μαγνητικοί τομογράφοι, τα συστήματα παρακολούθησης ασθενών, καθώς και άλλες ιατρικές συσκευές είχαν επηρεαστεί από αυτήν την επίθεση. Επικράτησε μια μεγάλη αναστάτωση στις ιατρικές εγκαταστάσεις σε όλο τον κόσμο όπως ακυρωμένα ραντεβού, και καθυστερήσεις στις επεμβάσεις. (Savita Mohurle, 2017)

Η επίθεση αυτή είχε σημαντικό αντίκτυπο στον τομέα της ιατρικής επιστήμης αποκαλύπτοντας αδυναμίες και κενά ασφαλείας πολλών ιατρικών οργανώσεων. Η ευρεία χρήση παλαιών λειτουργικών συστημάτων και η ανεπαρκής ενημέρωση των υπολογιστικών συστημάτων, οδήγησαν στον να υπάρξουν επιτυχημένες επιθέσεις ransomware. Επιπλέον, η έλλειψη εκπαίδευσης των εργαζομένων στον τομέας της κυβερνοασφάλειας συνέλαβε στο να υπάρξουν περισσότερες κυβερνοεπιθέσεις. (Savita Mohurle, 2017)

Η επίθεση WannaCry τονίζει την σημασία των μέτρων της κυβερνοασφάλειας που πρέπει να λάβουν οι ιατρικές οργανώσεις. Επιπλέον η επίθεση αυτή καθιστά εμφανές, την ανάγκη εκπαίδευσης των εργαζομένων σε θέματα κυβερνοασφάλειας και τη σημασία της έγκαιρης ενημέρωσης των λειτουργικών συστημάτων.

Η επίθεση WannaCry είχε σημαντικό αντίκτυπο στον τομέα της ιατρικής επιστήμης και τα διδάγματά της συνεχίζουν να εξετάζονται και να αναλύονται προκειμένου να βελτιωθεί η κυβερνοασφάλεια των ιατρικών οργανώσεων.

2.3.2 Επιπτώσεις Στον Τομέα Της Υγείας

Η επίθεση WannaCry ransomware είχε σημαντικό αντίκτυπο στον τομέα της ιατρικής επιστήμης, με συνέπειες που κυμάνθηκαν σε νοσοκομεία, κλινικές και ιατρικές οργανώσεις σε όλο τον κόσμο. Μία από τις πιο σημαντικές συνέπειες ήταν η διακοπή της φροντίδας των ασθενών, καθώς πολλά νοσοκομεία και κλινικές αναγκάστηκαν να ακυρώσουν ραντεβού και να καθυστερήσουν επεμβάσεις. Η επίθεση επηρέασε επίσης τη διαθεσιμότητα του ιατρικού εξοπλισμού και των συσκευών, με πολλά μηχανήματα και συστήματα παρακολούθησης να παρουσιάζουν προβλήματα στις λειτουργίες τους εξαιτίας της επίθεσης. (Noor Thamer, 2021)

Η επίθεση WannaCry ransomware παραβίασε την ιδιωτικότητα και την ασφάλεια των δεδομένων των ασθενών. Η επίθεση κρυπτογράφησε τα δεδομένα των ασθενών καθιστώντας τα μη προσβάσιμα, και απείλησε να τα δημοσιεύσει δημόσια αν δεν πληρωθεί ένα χρηματικό ποσό.

Οι συνέπειες της επίθεσης WannaCry στους παρόχους υγείας και στις ιατρικές οργανώσεις ήταν σημαντικές. Η επίθεση προκάλεσε σημαντικές οικονομικές απώλειες, καθώς οι οργανισμοί έπρεπε να επενδύσουν σε προσπάθειες ανάκτησης των δεδομένων, να πληρώσουν αποζημιώσεις και να αντισταθμίσουν τις απώλειες εσόδων λόγω των ακυρωμένων ραντεβού και θεραπειών. (Noor Thamer, 2021). Η επίθεση υπονόμευσε επίσης την εμπιστοσύνη και τη φήμη των παρόχων υγειονομικής περίθαλψης, καθώς οι ασθενείς και οι ενδιαφερόμενοι αμφισβήτησαν την ικανότητά τους να προστατεύουν προσωπικές πληροφορίες και να διατηρούν αξιόπιστη φροντίδα.

Η επίθεση WannaCry επίσης αποκάλυψε, τις συστημικές ευπάθειες στην κυβερνοασφάλεια των ιατρικών οργανώσεων. Πολλοί ιατρικοί οργανισμοί διέθεταν παλαιά λειτουργικά συστήματα και λογισμικό και δεν παρείχαν επαρκή κατάρτιση και εκπαίδευση στους υπαλλήλους. Η επίθεση αυτή, αποκάλυψε αυτά τα αδύναμα σημεία και τόνισε την επείγουσα ανάγκη για την ιατρική επιστήμη, να βελτιώσει τη στάση της στον κυβερνοχώρο και να επενδύσει σε πιο ισχυρά και ολοκληρωμένα μέτρα. (David P, 2018)

Η επίθεση WannaCry είχε ένα βαθύ και ευρύ πεδίο επιδράσεων στον τομέα της υγείας, επηρεάζοντας σημαντικά τους ασθενείς, τους παρόχους υπηρεσιών υγείας και τις ιατρικές οργανώσεις. Οι συνέπειες της επίθεσης αυτής τονίζουν τη σημασία των προληπτικών μέτρων της κυβερνοασφάλειας, συμπεριλαμβανομένων των τακτικών ενημερώσεων λογισμικού, της εκπαίδευσης των εργαζομένων και της υιοθέτησης ισχυρών τεχνολογιών και πρωτοκόλλων ασφαλείας.

2.3.3 Κενά Ασφαλείας

Η επίθεση WannaCry εκμεταλλεύτηκε αρκετές ευπάθειες για την απόκτηση της πρόσβασης στα υπολογιστικά συστήματα. Η πιο σημαντική ευπάθεια που εκμεταλλεύτηκε το κακόβουλο λογισμικό WannaCry ήταν η ευπάθεια EternalBlue, ένα κενό ασφαλείας στο λειτουργικό σύστημα Windows της Microsoft. Η ευπάθεια EternalBlue ανακαλύφθηκε αρχικά από την Υπηρεσία Εθνικής Ασφάλειας των

Ηνωμένων Πολιτειών (NSA) και στη συνέχεια διέρρευσε από μια ομάδα hacker γνωστή ως Shadow Brokers τον Απρίλιο του 2017. (Shou-Ching Hsiao, 2018)

Η ευπάθεια EternalBlue ήταν μια κρίσιμη ευπάθεια διότι επέτρεπε στον κυβερνοεγκληματία να εκτελεί αυθαίρετο κώδικα εξ αποστάσεως χωρίς να υπάρχει κάποιος έλεγχος ταυτοποίησης. Αυτό το κενό ασφαλείας υπήρχε σε πολλές εκδόσεις του λειτουργικού συστήματος Windows, συμπεριλαμβανομένων των Windows XP, Windows 7 και Windows Server 2008. Αυτή η ευπάθεια ήταν ιδιαίτερα επικίνδυνη επειδή πολλές οργανώσεις χρησιμοποιούν παλαιά συστήματα που δεν είχαν ενημερωθεί καταλλήλως. (Houssain Kettani, 2019)

Το WannaCry εκμεταλλεύτηκε επίσης μια άλλη ευπάθεια γνωστή ως DoublePulsar η οποία επίσης διέρρευσε από την ομάδα Shadow Brokers. Η ευπάθεια DoublePulsar επέτρεπε σε έναν εισβολέα να εκτελεί αυθαίρετο κώδικα σε ένα παραβιασμένο σύστημα. (Da-Yu KAO, 2019). Μια άλλη ευπάθεια που εκμεταλλεύτηκε το WannaCry ήταν το πρωτόκολλο Server Message Block (SMB), το οποίο χρησιμοποιούταν για την κοινή χρήση των αρχείων μεταξύ των υπολογιστών. Συγκεκριμένα, το WannaCry εκμεταλλεύτηκε μια ευπάθεια στο SMBv1, μια παλαιότερη έκδοση του πρωτοκόλλου που δεν απαιτούσε πιστοποίηση για να υπάρξει πρόσβαση σε αρχεία σε ένα απομακρυσμένο σύστημα. Αυτή η ευπάθεια υπήρχε σε αρκετές εκδόσεις των Windows, συμπεριλαμβανομένων των Windows 10 και είχε διορθωθεί από τη Microsoft σε μια ενημέρωση ασφαλείας που κυκλοφόρησε τον Μάρτιο του 2017, δύο μήνες πριν από την επίθεση του WannaCry. (Taylor’s University, July)

Η επίθεση WannaCry τόνισε τη σημασία των τακτικών ενημερώσεων ασφαλείας και των επιδιορθώσεων λογισμικού, ιδιαίτερα για τα παλαιά λειτουργικά συστήματα. Οργανισμοί που απέτυχαν να εφαρμόσουν τις διαθέσιμες ενημερώσεις ασφαλείας έμειναν ευάλωτοι στις επιθέσεις του κακόβουλου λογισμικού WannaCry ransomware.

2.3.4 Αντιμετώπιση

Η επίθεση WannaCry έκανε τις ιατρικές οργανώσεις και τις κυβερνήσεις σε ολόκληρο τον κόσμο να συνειδητοποιήσουν την κρίσιμη σημασία της κυβερνοασφάλειας. Μετά

την επίθεση, οι ιατρικές οργανώσεις και οι κυβερνήσεις εφάρμοσαν διάφορα μέτρα για τη μείωση της ζημίας και την πρόληψη παρόμοιων επιθέσεων στο μέλλον.

Ένα από τα κύρια μέτρα αντιμετώπισης ήταν η εφαρμογή ενημερώσεων και διορθώσεων ασφαλείας στα ευπαθή συστήματα. Η Microsoft κυκλοφόρησε μια έκτακτη ενημέρωση ασφαλείας για να αντιμετωπίσει την ευπάθεια EternalBlue, και πολλοί ιατρικοί οργανισμοί και κυβερνήσεις πήραν άμεσα μέτρα για να εφαρμόσουν διορθώσεις στα συστήματά τους. Επιπλέον, οι ιατρικοί οργανισμοί εφάρμοσαν και άλλα μέτρα ασφαλείας όπως τα τοίχοι προστασίας, τα anti-malware λογισμικά, και τα συστήματα ανίχνευσης παραβίασης, για να προστατεύσουν τα δίκτυά και τα συστήματά από μελλοντικές επιθέσεις. (Aljaidi, et al., 2022)

Δημιουργήθηκαν ειδικευμένες ομάδες και υπηρεσίες κυβερνοασφάλειας για τον συντονισμό των απαντήσεων και την ανταλλαγή πληροφοριών από πολλές κυβερνήσεις. Για παράδειγμα, η κυβέρνηση των ΗΠΑ ίδρυσε την Ομάδα Συντονισμού Κυβερνοασφαλείας (Cyber Unified Coordination Group) για την αντιμετώπιση της συγκεκριμένης επίθεσης.

Η συνεργασία και ο διαμοιρασμός πληροφοριών μεταξύ των ιατρικών οργανισμών και των κυβερνήσεων σε παγκόσμιο επίπεδο, θεωρήθηκε ως ένα ισχυρό μέτρο αντιμετώπισης. Οι ιατρικοί οργανισμοί μοιράστηκαν τις εμπειρίες και τις γνώσεις τους για τη πρόληψη και την αντιμετώπιση των κυβερνοεπιθέσεων, ενώ οι κυβερνήσεις μοιράστηκαν πληροφορίες και πρακτικές για τη βελτίωση της κυβερνοασφαλείας.

Οι ιατρικοί οργανισμοί και οι κυβερνήσεις εστίασαν στην εκπαίδευση των εργαζομένων σε σημαντικά θέματα κυβερνοασφάλειας. Πολλές ιατρικές οργανώσεις εφάρμοσαν την υποχρεωτική εκπαίδευση για τους εργαζόμενους, και παρείχαν καθοδήγηση σχετικά με τον τρόπο αναγνώρισης και αντιμετώπισης των κυβερνοαπειλών. (Cheng, 2022)

Συνοψίζοντας, η επίθεση WannaCry ανάγκασε τους ιατρικούς οργανισμούς και τις κυβερνήσεις να λάβουν ολοκληρωμένα μέτρα για τη μείωση των ζημιών και την αποτροπή μελλοντικών επιθέσεων. Αυτά τα μέτρα περιλάμβαναν την εφαρμογή των ενημερώσεων και των διορθώσεων ασφαλείας, την υλοποίηση των μέτρων ασφαλείας, τη δημιουργία ειδικών ομάδων και οργανισμών κυβερνοασφάλειας, τη συνεργασία και την ανταλλαγή πληροφοριών, και την προώθηση της εκπαίδευσης στον τομέα της κυβερνοασφάλειας.

Κεφάλαιο 3. Βέλτιστες Πρακτικές Κυβερνοασφάλειας Στην Ιατρική Επιστήμη

3.1 Βέλτιστες Πρακτικές

3.1.1 Επισκόπηση

Η κυβερνοασφάλεια είναι ένα κρίσιμο ζήτημα που επηρεάζει σημαντικά την ιατρική επιστήμη. Πολλοί οργανισμοί υγείας αντιμετωπίζουν ένα σύνολο προκλήσεων όταν πρόκειται για την ασφάλεια των συστημάτων πληροφορικής και την προστασία των ιατρικών δεδομένων των ασθενών. Τα ιατρικά αρχεία περιέχουν άκρως απόρρητες πληροφορίες. Οι απειλές που αντιμετωπίζουν οι ιατρικοί οργανισμοί μπορούν να θέσουν σε κίνδυνο την ασφάλεια των ασθενών.

Για την αντιμετώπιση αυτών των κινδύνων, οι ιατρικές οργανώσεις χρειάζεται να εφαρμόζουν τις βέλτιστες πρακτικές για την κυβερνοασφάλεια. Οι βέλτιστες πρακτικές αποτελούν τις αναγνωρισμένες προσεγγίσεις και μεθοδολογίες που έχουν δοκιμαστεί και αποδειχθεί αποτελεσματικές, για την ασφάλεια των υπολογιστών και την προστασία των πληροφοριών. Οι πρακτικές αυτές έχουν σκοπό να μειώσουν τον κίνδυνο των κυβερνοαπειλών που μπορούν να επηρεάσουν τη φροντίδα των ασθενών και τη φήμη της ιατρικής οργάνωσης. (Salem T. Argaw, 2020)

Η χρήση παλαιού λογισμικού και υλικού εξακολουθεί να είναι διαδεδομένη στον τομέα της υγείας δημιουργώντας σοβαρές ευπάθειες στα ιατρικά υπολογιστικά συστήματα και δίκτυα. Επιπλέον, οι ιατρικές οργανώσεις συνήθως διαθέτουν σύνθετα δίκτυα υπολογιστών καθιστώντας την ασφάλεια τους πιο περίπλοκη. Επίσης, ο ανθρώπινος

παράγοντας όπως η αμέλεια των εργαζομένων ή μια εσωτερική απειλή, μπορεί να βλάψει την κυβερνοασφάλεια σε μια ιατρική οργάνωση.

Σε αυτό το κεφάλαιο, θα συζητηθούν οι βέλτιστες πρακτικές για την κυβερνοασφάλεια στον τομέα της ιατρικής επιστήμης. Αυτές οι πρακτικές περιλαμβάνουν την εφαρμογή πολιτικών και διαδικασιών κυβερνοασφάλειας, τη διασφάλιση της συνεχούς ενημέρωσης και επιδιόρθωσης των συστημάτων, την ασφάλεια των δεδομένων ασθενών μέσω κρυπτογράφησης και ελέγχων πρόσβασης και την παροχή τακτικής εκπαίδευσης για την ασφάλεια στον κυβερνοχώρο από τους εργαζόμενους.

Ακολουθώντας αυτές τις βέλτιστες πρακτικές, οι οργανισμοί υγειονομικής περίθαλψης μπορούν να προστατεύσουν τα υπολογιστικά συστήματα τους, και να προστατεύσουν το απόρρητο και την ασφάλεια των ασθενών τους.

3.1.2 Έλεγχος Πρόσβασης

Ο έλεγχος πρόσβασης είναι ένα σημαντικό στοιχείο της κυβερνοασφάλειας που χρησιμοποιείται στην ιατρική επιστήμη. Ο έλεγχος πρόσβασης είναι μια πρακτική όπου περιορίζει την πρόσβαση στις προσωπικές πληροφορίες και στα υπολογιστικά συστήματα από το μη εξουσιοδοτημένο προσωπικό. Η εφαρμογή των μέτρων ελέγχου πρόσβασης έχει την δυνατότητα να προστατεύσει τα υπολογιστικά συστήματα μιας ιατρικής οργάνωσης από τη μη εξουσιοδοτημένη πρόσβαση.

Ο έλεγχος πρόσβασης βάσει ρόλου (Role - Based Access Control - RBAC) είναι ένας τύπος ελέγχου πρόσβασης που παρέχει πρόσβαση σε μέσα, με βάση τον ρόλο του χρήστη στον οργανισμό. Οι ιατρικοί οργανισμοί μπορούν να χρησιμοποιήσουν τον έλεγχο πρόσβασης βάσει ρόλου για τον περιορισμό της πρόσβασης στα προσωπικά δεδομένα των ασθενών. Μόνο οι αρμόδιοι υπάλληλοι μπορούν να έχουν πρόσβαση στα προσωπικά δεδομένα των ασθενών για να εκτελέσουν τα εργασιακά τους καθήκοντα. Για παράδειγμα, μια νοσοκόμα μπορεί να έχει πρόσβαση στα ιατρικά αρχεία των ασθενών και στα αποτελέσματα των εξετάσεων, ενώ μια γραμματέας μπορεί να έχει πρόσβαση μόνο στα χρονοδιαγράμματα των ραντεβού και στις πληροφορίες χρέωσης. Ο έλεγχος πρόσβασης βάσει ρόλου μπορεί να βοηθήσει στην πρόληψη των παραβιάσεων των δεδομένων στον κυβερνοχώρο, περιορίζοντας την πρόσβαση στις προσωπικές πληροφορίες και στα ιατρικά πληροφοριακά συστήματα, από τους μη εξουσιοδοτημένους χρήστες. (Sandhu, 1998)

Ο έλεγχος ταυτότητας δύο παραγόντων (Two - Factor Authentication - 2FA) είναι ένα άλλο μέτρο ελέγχου πρόσβασης, που μπορεί να χρησιμοποιηθεί για την ενίσχυση της κυβερνοασφάλειας. Ο έλεγχος ταυτότητας δύο παραγόντων απαιτεί να υπάρχουν δύο μορφές αναγνώρισης από τους χρήστες πριν τους δοθεί η πρόσβαση στα ιατρικά υπολογιστικά συστήματα ή στα δεδομένα. Η εφαρμογή του ελέγχου ταυτότητας δύο παραγόντων μπορεί να περιλαμβάνει για παράδειγμα, έναν κωδικό πρόσβασης και την αναγνώριση του δακτυλικού αποτυπώματος από τον χρήστη. Ο έλεγχος ταυτότητας δύο παραγόντων προσθέτει ένα επιπλέον επίπεδο ασφάλειας στον έλεγχο πρόσβασης, κάνοντας πιο δύσκολη τη πρόσβαση στα προσωπικά δεδομένα και στα ιατρικά υπολογιστικά συστήματα από τους μη εξουσιοδοτημένους χρήστες. Η εφαρμογή του ελέγχου ταυτότητας δύο παραγόντων μπορεί να βοηθήσει στην αποφυγή της παραβίασης των δεδομένων, και στην αποφυγή του ηλεκτρονικού ψαρέματος. (Jessica Colnago, 2018)

Τα μέτρα ελέγχου πρόσβασης περιορίζουν της μη εξουσιοδοτημένη πρόσβασης στα προσωπικά δεδομένα και στα συστήματα στους οργανισμούς υγειονομικής περίθαλψης. Εφαρμόζοντας τα μέτρα ελέγχου πρόσβασης, οι οργανισμοί υγειονομικής περίθαλψης μπορούν να ενισχύσουν σε μεγάλο βαθμό την ικανότητά τους στο να προστατεύουν τα δεδομένα των ασθενών.

3.1.3 Κρυπτογράφηση

Η κρυπτογράφηση είναι ένα κρίσιμο στοιχείο μιας ολοκληρωμένης στρατηγικής κυβερνοασφάλειας στην ιατρική επιστήμη. Η κρυπτογράφηση αποτελεί τη διαδικασία μετατροπής των δεδομένων από μια αναγνώσιμη μορφή σε μια μη αναγνώσιμη μορφή, με σκοπό την προστασία της εμπιστευτικότητας και της ακεραιότητας των δεδομένων. Στην ιατρική επιστήμη, η κρυπτογράφηση μπορεί να χρησιμοποιηθεί για την προστασία των προσωπικών δεδομένων, όπως τα αρχεία υγείας των ασθενών, οι προσωπικές πληροφορίες και οικονομικά δεδομένα.

Η κρυπτογράφηση πλήρους δίσκου είναι ένας τύπος κρυπτογράφησης που χρησιμοποιείται για την προστασία των δεδομένων που αποθηκεύονται στον σκληρό δίσκο ενός υπολογιστή. Με την κρυπτογράφηση πλήρους δίσκου, όλα τα δεδομένα στον σκληρό δίσκο κρυπτογραφούνται, συμπεριλαμβανομένου του λειτουργικού συστήματος και όλων των αρχείων του χρήστη. Σε περίπτωση που χαθεί ή κλαπεί ένα υπολογιστικό σύστημα, η πρόσβαση στα δεδομένα του σκληρού δίσκου δεν θα είναι δυνατή χωρίς το

κλειδί κρυπτογράφησης. Η κρυπτογράφηση πλήρους δίσκου μπορεί να χρησιμοποιηθεί για την προστασία των φορητών υπολογιστών, των επιτραπέζιων υπολογιστών και άλλων συσκευών που αποθηκεύουν ευαίσθητα και προσωπικά δεδομένα. (Min Liang, 2010)

Η κρυπτογράφηση ηλεκτρονικού ταχυδρομείου (Email encryption) είναι επίσης μια συχνή μέθοδος κρυπτογράφησης που χρησιμοποιείται από τους ιατρικούς οργανισμούς. Το ηλεκτρονικό ταχυδρομείο των ιατρικών οργανώσεων περιέχει προσωπικές και ευαίσθητες πληροφορίες των ασθενών. Η κρυπτογράφηση ηλεκτρονικού ταχυδρομείου μπορεί να χρησιμοποιηθεί για την προστασία των πληροφοριών από τη μη εξουσιοδοτημένη πρόσβαση. Με την κρυπτογράφηση του ηλεκτρονικού ταχυδρομείου το περιεχόμενο των ηλεκτρονικών μηνυμάτων κρυπτογραφείται. Μόνο ο προβλεπόμενος παραλήπτης μπορεί να αποκρυπτογραφήσει το ηλεκτρονικό μήνυμα, χρησιμοποιώντας το κλειδί αποκρυπτογράφησης. Ο τρόπος αυτός, διασφαλίζει ότι οι προσωπικές ιατρικές πληροφορίες θα παραμείνουν εμπιστευτικές, και ότι δεν υποκλαπούν από μη εξουσιοδοτημένα άτομα. (Trinabh Gupta, 2017)

Με την εφαρμογή των τεχνικών κρυπτογράφησης όπως είναι η κρυπτογράφηση πλήρους δίσκου και η κρυπτογράφηση ηλεκτρονικού ταχυδρομείου, οι οργανισμοί υγειονομικής περίθαλψης μπορούν να βελτιώσουν τη θέση τους στον κυβερνοχώρο και να προστατεύσουν τα ευαίσθητα δεδομένα από μη εξουσιοδοτημένη πρόσβαση. Η κρυπτογράφηση είναι μια αποδεδειγμένη μέθοδος προστασίας των δεδομένων και αποτελεί ένα ουσιαστικό μέρος μιας ολοκληρωμένης στρατηγικής κυβερνοασφάλειας.

3.1.4 Αντιμετώπιση Περιστατικών Κυβερνοασφάλειας

Η έγκαιρη ανταπόκριση στα περιστατικά κυβερνοασφάλειας είναι ένα κρίσιμο στοιχείο μιας ολοκληρωμένης στρατηγικής κυβερνοασφάλειας που εφαρμόζεται στην ιατρική επιστήμη. Ένα σχέδιο αντιμετώπισης περιστατικών κυβερνοασφάλειας περιγράφει τα στάδια που πρέπει να ακολουθήσει μια ιατρική οργάνωση σε περίπτωση που γίνει στόχος μιας κυβερνοεπίθεσης.

Το πρώτο βήμα για την δημιουργία ενός σχεδίου αντιμετώπισης περιστατικών κυβερνοασφάλειας, είναι ο εντοπισμός των πιθανών απειλών και των κινδύνων.

Περιλαμβάνεται η αξιολόγηση του δικτύου και των συστημάτων για τον προσδιορισμό των κενών ασφαλείας. Αφού εντοπιστούν οι πιθανοί κίνδυνοι, θα πρέπει να αναπτυχθεί ένα σχέδιο αντιμετώπισης των περιστατικών κυβερνοασφάλειας.

Το σχέδιο για την αντιμετώπιση των περιστατικών κυβερνοασφάλειας θα πρέπει να αναφέρει τους ρόλους και τις ευθύνες όλων των μελών της ομάδας αντιμετώπισης περιστατικών κυβερνοασφάλειας, Το σχέδιο αντιμετώπισης περιστατικών κυβερνοασφάλειας θα πρέπει επίσης να προσδιορίζει τα μέσα επικοινωνίας που χρησιμοποιούνται στις περιπτώσεις των περιστατικών κυβερνοασφάλειας, καθώς και την εφαρμογή των απαραίτητων πρωτοκόλλων. (Williams, 2022).

Σε περίπτωση που συμβεί κάποιο περιστατικό κυβερνοασφάλειας θα πρέπει να εφαρμοστεί το σχέδιο αντιμετώπισης, καθώς και να ληφθούν τα απαραίτητα μέτρα για τον περιορισμό του συμβατός και την μείωση της ζημιάς. Αυτό περιλαμβάνει την απομόνωση των επηρεαζόμενων συστημάτων και των συσκευών, τη διατήρηση όλων των αποδεικτικών στοιχείων, και τη διεξαγωγή έρευνας για τον προσδιορισμό της αιτίας του συμβάντος.

Μόλις περιοριστεί το περιστατικό κυβερνοασφάλειας, η ομάδα αντιμετώπισης θα πρέπει να εφαρμόσει τις απαραίτητες ενέργειες για την αποκατάσταση των επηρεαζόμενων συστημάτων και δεδομένων, καθώς και τη λήψη μέτρων αποφυγής παρόμοιων περιστατικών στο μέλλον. Μπορεί να περιλαμβάνεται η επιδιόρθωση των κενών ασφαλείας, η ενημέρωση πολιτικών και διαδικασιών ασφαλείας, και η παροχή προγραμμάτων εκπαίδευσης για τους εργαζόμενους.

Η ύπαρξη ενός σχεδίου αντιμετώπισης περιστατικών κυβερνοασφάλειας θεωρείτε αρκετά σημαντική για τους οργανισμούς υγειονομικής περίθαλψης, καθώς μειώνουν σε μεγάλο βαθμό τις συνέπειες που επιφέρουν τα περιστατικά κυβερνοασφάλειας. Μια προετοιμασμένη ομάδα αντιμετώπισης περιστατικών μπορεί να ανιχνεύσει και να ανταποκριθεί σε περιστατικά κυβερνοασφάλειας γρήγορα και αποτελεσματικά. (Williams, 2022)

Συνοψίζοντας, οι ιατρικοί οργανισμοί θα πρέπει να διαθέτουν ένα ολοκληρωμένο σχέδιο αντιμετώπισης περιστατικών κυβερνοασφάλειας. Το σχέδιο αντιμετώπισης περιστατικών κυβερνοασφάλειας θα πρέπει να περιλαμβάνει τον εντοπισμό πιθανών

κινδύνων, τον καθορισμό ρόλων και ευθυνών, τη δημιουργία καναλιών επικοινωνίας και την λήψη δράσης για τον περιορισμό του περιστατικού και τη μείωση της ζημίας.

3.1.5 Εκπαίδευση Εργαζομένων

Οι απειλές στον τομέα της κυβερνοασφάλειας εξελίσσονται συνεχώς και οι ιατρικοί οργανισμοί θα πρέπει να φροντίζουν και να λαμβάνουν όλα τα απαραίτητα προληπτικά μέτρα για την αντιμετώπιση των κινδύνων. Ένα σημαντικό στοιχείο μιας αποτελεσματικής στρατηγικής στον τομέα της κυβερνοασφάλειας είναι η σωστή εκπαίδευση των εργαζομένων. Η εκπαίδευση των εργαζομένων στον τομέα της κυβερνοασφάλειας έχει ως αποτέλεσμα την σωστή κατάρτιση των εργαζομένων σχετικά με τις απειλές στον κυβερνοχώρο και τον τρόπο αποφυγής τους. Παρέχοντας στους εργαζομένους τις απαραίτητες γνώσεις και δεξιότητες για τον εντοπισμό και την αντιμετώπιση των απειλών στον κυβερνοχώρο, οι οργανισμοί μπορούν να περιορίσουν τον κίνδυνο παραβιάσεων δεδομένων, αλλά και άλλων περιστατικών κυβερνοασφάλειας. (Sokratis Nifakos, 2021)

Το πρώτο στάδιο για την εφαρμογή ενός προγράμματος εκπαίδευσης στον κυβερνοχώρο είναι η αναγνώριση των βασικών κινδύνων που αντιμετωπίζει ο οργανισμός. Οι απειλές που περιλαμβάνονται είναι, το ηλεκτρονικό ψάρεμα, το κακόβουλο λογισμικό και οι επιθέσεις κοινωνικής μηχανικής. Μόλις αναγνωριστούν οι κίνδυνοι που διατρέχει ένας ιατρικός οργανισμός, μπορεί να αναπτυχθεί ένα εκπαιδευτικό πρόγραμμα αντιμετώπισης αυτών των κινδύνων.

Η εκπαίδευση των εργαζομένων στον τομέα της κυβερνοασφάλειας θα πρέπει να εφαρμόζεται τακτικά και να παρέχεται σε όλους τους εργαζόμενους, ανεξάρτητα από την αρμοδιότητα τους στον οργανισμό. Η εκπαίδευση θα πρέπει να καλύπτει ένα ευρύ φάσμα θεμάτων, συμπεριλαμβανομένων των βασικών εννοιών της κυβερνοασφάλειας, όπως είναι η σημασία των ισχυρών κωδικών πρόσβασης και το ενημερωμένο λογισμικό. Θα

πρέπει επίσης να καλύπτονται και πιο προχωρημένα θέματα, όπως ο τρόπος αναγνώρισης επιθέσεων ηλεκτρονικού ψαρέματος, καθώς και άλλοι τύποι επιθέσεων κοινωνικής μηχανικής. (Zafar, 2016)

Η εκπαίδευση των εργαζομένων μπορεί να είναι και διαδραστική. Αυτό μπορεί να περιλαμβάνει και τη χρήση προσομοιώσεων, για την καλύτερη διατύπωση των θεμάτων κυβερνοασφάλειας. Η εκπαίδευση των εργαζομένων θα πρέπει να έχει διαμορφωθεί με τέτοιον τρόπο, ώστε να μπορεί να προσαρμοστεί στο κάθε τμήμα μιας ιατρικής οργάνωσης.

Για παράδειγμα, οι υπάλληλοι που έχουν πρόσβαση στα προσωπικά δεδομένα των ασθενών μπορεί να χρειάζονται πιο εξειδικευμένη εκπαίδευση σε ορισμένα θέματα κυβερνοασφάλειας, από τους υπαλλήλους που δεν έχουν την ίδια πρόσβαση.

Οι ιατρικοί οργανισμοί εκτός από την εφαρμογή των προγραμμάτων εκπαίδευσης, θα πρέπει επίσης να θεσπίσουν πολιτικές και διαδικασίες για την ενίσχυση των βέλτιστων πρακτικών για την κυβερνοασφάλεια. Για παράδειγμα, μπορούν να εφαρμοστούν πολιτικές σχετικά με τη χρήση των προσωπικών συσκευών, την απομακρυσμένη πρόσβαση, και τη διαχείριση των κωδικών πρόσβασης. (Zafar, 2016)

Συνοψίζοντας, η εκπαίδευση των εργαζομένων στον τομέα της κυβερνοασφάλειας αποτελεί ένα σημαντικό στοιχείο μιας στρατηγικής για την ασφάλεια στον κυβερνοχώρο. Οι οργανισμοί μπορούν να μειώσουν την πιθανότητα παραβίασης των δεδομένων και άλλων περιστατικών ασφάλειας στον κυβερνοχώρο, εκπαιδεύοντας με σωστό τρόπο τους υπαλλήλους.

3.1.6 Ενημερώσεις και Επιδιορθώσεις Λογισμικού

Οι ιατρικοί οργανισμοί στηρίζονται σε ένα μεγάλο βαθμό στο λογισμικό για τη διαχείριση των αρχείων ασθενών, και τη διευκόλυνση της επικοινωνίας μεταξύ των παρόχων υγειονομικής περίθαλψης. Ωστόσο, το λογισμικό μπορεί να θέσει τις ιατρικές οργανώσεις ευάλωτες σε κυβερνοεπιθέσεις. Οι κυβερνοεγκληματίες συχνά στοχεύον τις ιατρικές οργανώσεις που χρησιμοποιούν ένα μη ενημερωμένο λογισμικό. (Tervonen, 2019)

Οι συχνές ενημερώσεις του λογισμικού είναι απαραίτητες για τις ιατρικές οργανώσεις προκειμένου να διατηρηθεί η ασφάλεια των πληροφοριών. Οι ενημερώσεις λογισμικού

αντιμετωπίζουν κενά ασφαλείας, διορθώνουν σφάλματα και βελτιώνουν τη συνολική απόδοση του συστήματος. Το μη ενημερωμένο λογισμικό μπορεί να οδηγήσει σε παραβιάσεις δεδομένων, σε επιθέσεις ransomware, καθώς και σε άλλα περιστατικά ασφαλείας που θα μπορούσαν να θέσουν σε κίνδυνο την ασφάλεια των ασθενών.

Για να διασφαλιστούν όλες οι απαραίτητες ενημερώσεις λογισμικού, οι ιατρικοί οργανισμοί θα πρέπει να αναπτύξουν μια στρατηγική διαχείρισης ενημερώσεων λογισμικού. Αυτή η στρατηγική περιλαμβάνει τα παρακάτω βήματα:

• Καταγραφή Λογισμικού: Οι ιατρικοί οργανισμοί θα πρέπει να καταγράφουν τις εφαρμογές και τα συστήματα λογισμικού που χρησιμοποιούν, συμπεριλαμβανομένων και εκείνων που δεν υποστηρίζονται.

• Σχέδιο επιδιόρθωσης: Θα πρέπει να αναπτυχθεί ένα σχέδιο επιδιόρθωσης που θα δίνει προτεραιότητα στις ενημερώσεις λογισμικού με βάση το επίπεδο κινδύνου.

• Δοκιμαστικές επιδιορθώσεις: Οι ενημερώσεις λογισμικού πρέπει να δοκιμαστούν σε ένα ασφαλές περιβάλλον πριν χρησιμοποιηθούν ώστε να αποφευχθούν τυχόν προβλήματα.

• Έγκαιρη εγκατάσταση ενημερώσεων: Αφού δοκιμαστούν και εγκριθούν οι ενημερώσεις, θα πρέπει να εγκατασταθούν το συντομότερο δυνατό ώστε να μειωθεί το χρονικό διάστημα κατά το οποίο το σύστημα είναι ευάλωτο.

• Παρακολούθηση για νέες ενημερώσεις: Οι ιατρικές οργανώσεις πρέπει να είναι πάντοτε ενήμερες για τυχόν ενημερώσεις λογισμικού προκειμένου να διατηρηθεί η ασφάλεια των εφαρμογών και των υπολογιστικών τους συστημάτων.

Ακολουθώντας μια στρατηγική διαχείρισης ενημερώσεων λογισμικού, οι ιατρικές οργανώσεις μπορούν να μειώσουν σημαντικά τον κίνδυνο των κυβερνοεπιθέσεων και να προστατεύσουν τα δεδομένα των ασθενών.

3.2 Βιομηχανικά Πρότυπα και Κανονισμοί

3.2.1 Επισκόπηση

Οι ιατρικοί οργανισμοί ευθύνονται για τη διαφύλαξη των προσωπικών δεδομένων των ασθενών. Οι ιατρικές οργανώσεις πρέπει να συμμορφώνονται με τα πρότυπα και τους κανονισμούς του τομέα της κυβερνοασφάλειας, προκειμένου να προστατεύουν τα δεδομένα τους.

• Ο Νόμος Φορητότητας και Λογοδοσίας Ασφάλισης Υγείας (HIPAA): Ο HIPAA είναι ένας ομοσπονδιακός νόμος στις Ηνωμένες Πολιτείες που περιγράφει τα πρότυπα για την προστασία των ευαίσθητων ιατρικών δεδομένων των ασθενών, συμπεριλαμβανομένων των ιατρικών αρχείων και άλλων πληροφοριών υγείας. Απαιτεί από τις ιατρικές οργανώσεις να εφαρμόζουν διοικητικές, φυσικές και τεχνικές διασφαλίσεις για την προστασία των πληροφοριών των ασθενών.

• Το Πρότυπο Ασφάλειας Δεδομένων Βιομηχανίας Πληρωμών (PCI DSS): Εάν μια ιατρική οργάνωση δέχεται πληρωμές με πιστωτικές κάρτες, πρέπει να συμμορφώνεται με το PCI DSS, το οποίο είναι ένα σύνολο προτύπων ασφαλείας σχεδιασμένο για να διασφαλίζει ότι τα δεδομένα των πιστωτικών καρτών προστατεύονται κατά τη διάρκεια των συναλλαγών.

• Ο Γενικός Κανονισμός για την Προστασία των Δεδομένων (GDPR): Ο γενικός κανονισμός προστασίας δεδομένων είναι ένας κανονισμός που ισχύει για όλες τις οργανώσεις που επεξεργάζονται προσωπικά δεδομένα ευρωπαίων πολιτών. Οι ιατρικές οργανώσεις πρέπει να συμμορφώνονται με τον GDPR, αν διαθέτουν ασθενείς που είναι ευρωπαίοι πολίτες.

• Το Εθνικό Ινστιτούτο Προτύπων και Τεχνολογίας (NIST): Το πλαίσιο κυβερνοασφάλειας του NIST είναι ένα πλαίσιο κυβερνοασφάλειας που αναπτύχθηκε

από την κυβέρνηση των ΗΠΑ. Το πλαίσιο αυτό, παρέχει καθοδήγηση σχετικά με τον τρόπο διαχείρισης και μείωσης των κινδύνων για την ασφάλεια στον κυβερνοχώρο. Χρησιμοποιώντας το πλαίσιο κυβερνοασφάλειας του NIST, οι ιατρικοί οργανισμοί μπορούν να αξιολογήσουν τις υπάρχουσες διαδικασίες τους στον κυβερνοχώρο και να εντοπίσουν πιθανούς τομείς για βελτίωση.

• Ο Διεθνής Οργανισμός Τυποποίησης (ISO): Ο Διεθνής οργανισμός τυποποίησης είναι ένας μη κυβερνητικός οργανισμός που αναπτύσσει πρότυπα για διάφορους κλάδους, συμπεριλαμβανομένης και της κυβερνοασφάλειας. Το ISO/IEC 27001 είναι το πρότυπο για συστήματα διαχείρισης ασφάλειας πληροφοριών. Οι ιατρικοί οργανισμοί μπορούν να χρησιμοποιούν το πρότυπο αυτό, για να δημιουργήσουν και να διατηρήσουν ένα αποτελεσματικό σύστημα διαχείρισης ασφάλειας πληροφοριών.

Για να διασφαλιστεί η συμμόρφωση με τα βιομηχανικά πρότυπα και τους κανονισμούς, οι ιατρικές οργανώσεις πρέπει να αξιολογούν τακτικά τις πρακτικές ασφάλειας στον κυβερνοχώρο, να εφαρμόζουν τους κατάλληλους ελέγχους ασφαλείας, και να διενεργούν ελέγχους για τον εντοπισμό και την αντιμετώπιση των αδύναμων σημείων.

3.2.2 Ο Νόμος Περί Φορητότητας και Λογοδοσίας Ασφάλισης Υγείας (HIPAA)

Ο Νόμος φορητότητας και λογοδοσίας Ασφάλισης Υγείας (HIPAA) αποτελεί ένα σύνολο κανονισμών που θεσπίζουν εθνικά πρότυπα για την προστασία της εμπιστευτικότητας, της ακεραιότητας και της διαθεσιμότητας των ηλεκτρονικών προστατευόμενων πληροφοριών υγείας (ePHI). Εφαρμόζοντας διοικητικά, φυσικά, και τεχνικά μέτρα, οι οργανισμοί μπορούν να διατηρούν τις ηλεκτρονικές προστατευόμενες πληροφορίες υγείας ασφαλείς. (I. Glenn Cohen, 2018)

Οι απαιτήσεις για τεχνικά μέτρα ασφαλείας περιλαμβάνουν τους ελέγχους πρόσβασης, τους ελέγχους επιθεώρησης, τους ελέγχους ακεραιότητας, την ασφάλεια της μετάδοσης και την κρυπτογράφηση και την αποκρυπτογράφηση. Ο σκοπός των ελέγχων πρόσβασης είναι ο περιορισμός της πρόσβασης στα ePHI μόνο σε άτομα που έχουν εξουσιοδοτηθεί. Οι έλεγχοι επιθεώρησης είναι μηχανισμοί για την καταγραφή και την εξέταση της δραστηριότητας του συστήματος. Περιλαμβάνουν διαδικασίες για τον τακτικό έλεγχο των αρχείων καταγραφής ελέγχου (audit logs) προκειμένου να ανιχνεύονται και να

διερευνώνται ύποπτες δραστηριότητες. Οι έλεγχοι ακεραιότητας αποτελούν μέτρα που διασφαλίζουν ότι τα ePHI δεν έχουν παραβιαστεί ή καταστραφεί. Η ασφάλεια μετάδοσης αναφέρεται στη χρήση κρυπτογράφησης και αποκρυπτογράφησης για την προστασία των ePHI που προστατεύονται ηλεκτρονικά κατά τη διάρκεια της μετάδοσής τους μέσω ανοικτών δικτύων.

Οι ειδικές απαιτήσεις για τις φυσικές διασφαλίσεις περιλαμβάνουν τους ελέγχους πρόσβασης εγκαταστάσεων, τη χρήση σταθμού εργασίας, την ασφάλεια σταθμού εργασίας και τους ελέγχους συσκευών και πολυμέσων. Οι έλεγχοι πρόσβασης εγκαταστάσεων είναι τα μέτρα για τον περιορισμό της φυσικής πρόσβασης σε εγκαταστάσεις όπου αποθηκεύεται ή υποβάλλεται σε επεξεργασία τα ePHI, και περιλαμβάνουν μηχανισμούς όπως κάρτες πρόσβασης και βιομετρικοί έλεγχοι ταυτότητας. Ο όρος σταθμός εργασίας αναφέρεται στα πρωτόκολλα που έχουν θεσπιστεί για να ορίσουν την κατάλληλη χρήση των σταθμών εργασίας που έχουν πρόσβαση στα ePHI. Περιλαμβάνει την εφαρμογή μέτρων που διασφαλίζουν ότι μόνο οι εξουσιοδοτημένοι χρήστες έχουν πρόσβαση στους σταθμούς εργασίας. Η ασφάλεια του σταθμού εργασίας περιλαμβάνει τόσο τις φυσικές όσο και τις τεχνικές διασφαλίσεις που προορίζονται για την προστασία των σταθμών εργασίας που έχουν πρόσβαση στο ePHI. Οι έλεγχοι συσκευών και μέσων αναφέρονται σε μέτρα για την ασφάλεια των συσκευών που αποθηκεύουν ePHI, όπως υπολογιστές και φορητές συσκευές, καθώς και των μέσων που περιέχουν ePHI. (Greene, 2012)

Οι ειδικές απαιτήσεις για τις διοικητικές διασφαλίσεις περιλαμβάνουν τις διαδικασίες διαχείρισης ασφάλειας, το προσωπικό ασφαλείας, τη διαχείριση πρόσβασης σε πληροφορίες, και την εκπαίδευση και την διαχείριση του εργατικού δυναμικού. Οι διαδικασίες διαχείρισης ασφάλειας περιλαμβάνουν πολιτικές και διαδικασίες για τη διαχείριση και την παρακολούθηση της εφαρμογής των μέτρων ασφαλείας, καθώς και για τον εντοπισμό και την αντιμετώπιση των περιστατικών ασφαλείας. Το προσωπικό ασφαλείας είναι η ομάδα που επιβλέπει και διαχειρίζεται την εφαρμογή των μέτρων ασφαλείας που απαιτούνται από τον κανόνα ασφαλείας (I. Glenn Cohen, 2018). Η διαχείριση πρόσβασης πληροφοριών αναφέρεται στις πολιτικές και στις διαδικασίες για την πρόσβαση στα ePHI και περιλαμβάνει μηχανισμούς όπως τον έλεγχο πρόσβασης και την εκκαθάριση ασφαλείας. Η εκπαίδευση και η διαχείριση του εργατικού δυναμικού

περιλαμβάνει τη δημιουργία κανόνων με σκοπό να διασφαλιστεί ότι όλοι οι εργαζόμενοι είναι κατάλληλα εκπαιδευμένοι στις απαιτήσεις των κανόνων ασφαλείας.

Ο σχεδιασμός έκτακτης ανάγκης αναφέρεται στις πολιτικές και στις διαδικασίες για την αντιμετώπιση των καταστάσεων έκτακτης ανάγκης, όπως είναι οι φυσικές καταστροφές ή βλάβες συστήματος. Περιλαμβάνονται μέτρα όπως η δημιουργία αντιγράφων ασφαλείας δεδομένων.

Συνοψίζοντας, ο νόμος φορητότητας και λογοδοσίας Ασφάλισης Υγείας (HIPAA) απαιτεί από τους οργανισμούς να εφαρμόζουν ένα ολοκληρωμένο πρόγραμμα ασφάλειας που περιλαμβάνει διοικητικές, φυσικές και τεχνικές διασφαλίσεις για την προστασία της εμπιστευτικότητας, της ακεραιότητας και της διαθεσιμότητας των ePHI.

3.2.3 Το Πλαίσιο Κυβερνοασφάλειας Του NIST

Το πλαίσιο κυβερνοασφάλειας του NIST αποτελεί ένα σημαντικό εργαλείο για τον τομέα της ιατρικής επιστήμης, διότι εφαρμόζει πρακτικές κυβερνοασφάλειας που είναι ευέλικτες για τη διαχείριση των κινδύνων. Το πλαίσιο χωρίζεται σε πέντε βασικές λειτουργίες: Αναγνώριση, Προστασία, Εντοπισμός, Ανταπόκριση και Ανάκτηση. (Barbara Krumay, 2018)

Στον τομέα της ιατρικής επιστήμης, το πλαίσιο κυβερνοασφάλειας του NIST εφαρμόζεται ως εξής:

1. Αναγνώριση: Το αρχικό στάδιο του πλαισίου κυβερνοασφάλειας περιλαμβάνει την αναγνώριση των πόρων και των συστημάτων που απαιτούν προστασία. Στον τομέα της ιατρικής επιστήμης περιλαμβάνονται τα δεδομένα ασθενών, τα ιατρικά αρχεία, καθώς και άλλες ιατρικές πληροφορίες.

2. Προστασία: Η λειτουργία προστασίας περιλαμβάνει τα μέτρα ασφαλείας για την πρόληψη ή τον περιορισμό των κυβερνοαπειλών. Στην ιατρική επιστήμη, αυτό μπορεί να περιλαμβάνει την εφαρμογή ελέγχων πρόσβασης για τη προστασία των δεδομένων, τη χρήση κρυπτογράφησης για την προστασία των ευαίσθητων πληροφοριών, και την εφαρμογή των μέτρων ασφαλείας για την προστασία των ιατρικών συσκευών και άλλων συστημάτων.

3.Εντοπισμός: Η λειτουργία εντοπισμού περιλαμβάνει την έγκαιρη ανίχνευση των κυβερνοαπειλών. Στον τομέα της ιατρικής επιστήμης, αυτό μπορεί να περιλαμβάνει την

εφαρμογή συστημάτων ανίχνευσης και πρόληψης επιθέσεων, καθώς και την παρακολούθηση δικτύων και συστημάτων.

4. Ανταπόκριση: Η λειτουργία ανταπόκρισης περιλαμβάνει τη λήψη μέτρων για την αντιμετώπιση περιστατικών ασφάλειας στον κυβερνοχώρο. Στον ιατρικό τομέα, αυτό μπορεί να περιλαμβάνει την ανάπτυξη ενός σχεδίου αντιμετώπισης περιστατικών κυβερνοασφάλειας.

5. Ανάκτηση: Η τελική λειτουργία του πλαισίου κυβερνοασφάλειας, είναι η αποκατάσταση των ιατρικών οργανώσεων από τα περιστατικά κυβερνοασφάλειας. Στον τομέα της ιατρικής, αυτό μπορεί να περιλαμβάνει την εφαρμογή συστημάτων αντιγράφων ασφαλείας και ανάκτησης δεδομένων.

Χρησιμοποιώντας το πλαίσιο κυβερνοασφάλειας του NIST, οι ιατρικοί οργανισμοί διασφαλίζουν την προστασία των δεδομένων και την ασφάλεια των συστημάτων τους με έναν ολοκληρωμένο και μεθοδικό τρόπο.

Κεφάλαιο 4. Τεχνολογίες Κυβερνοασφάλειας Στην Ιατρική Επιστήμη

4.1 Τεχνολογίες και Εργαλεία

4.1.1 Επισκόπηση

Η ψηφιοποίηση και η άνοδος της τεχνολογίας έχει φέρει επανάσταση στον τομέα της ιατρικής επιστήμης. Η διασφάλιση ισχυρών μέτρων κυβερνοασφάλειας αποτελεί σημαντική παράμετρος για τις ιατρικές οργανώσεις. Οι ιατρικές οργανώσεις πρέπει να υιοθετούν αποτελεσματικές τεχνολογίες και εργαλεία για την προστασία των προσωπικών τους δεδομένων, και τη διασφάλιση των υπολογιστικών τους συστημάτων.

4.1.2 Τείχος Προστασίας

Για την διασφάλιση της προστασίας του δικτύου μιας ιατρικής οργάνωσης, η εφαρμογή των τειχών προστασίας είναι απαραίτητη. Το τείχος προστασίας λειτουργεί σαν ένα προστατευτικό φράγμα μεταξύ του εσωτερικού δικτύου μιας ιατρικής οργάνωσης και των εξωτερικών δικτύων, όπως είναι το διαδίκτυο. Η κύρια λειτουργία του τείχους

προστασίας είναι η παρακολούθηση και ο έλεγχος της εισερχόμενης και εξερχόμενης κίνησης δικτύου, με βάση τους κανόνες ασφαλείας. Τα τείχη προστασίας συμβάλλουν στην αποτροπή της μη εξουσιοδοτημένης πρόσβασης, των κακόβουλων επιθέσεων, και γενικά της εξάπλωσης του κακόβουλου λογισμικού. (Raja Waseem Anwar, 2021)

Τα τείχη προστασίας εξετάζουν κάθε πακέτο δεδομένων που διέρχεται. Οι ιδιότητες των πακέτων αναλύονται από τα τείχη προστασίας, όπως για παράδειγμα οι διευθύνσεις IP προέλευσης και προορισμού, για να καθορίσουν εάν το πακέτο πρέπει να επιτραπεί ή να αποκλειστεί με βάση τις διαμορφωμένες πολιτικές ασφαλείας. Στο πλαίσιο των ιατρικών δικτύων, τα τείχη προστασίας διαδραματίζουν ένα κρίσιμο στοιχείο για τη διαφύλαξη των πληροφοριών υγείας.

Με τη κατάλληλη διαμόρφωση του τοίχου προστασίας, οι ιατρικές οργανώσεις μπορούν να ελέγχουν ποια συστήματα και ποιες συσκευές επιτρέπεται να επικοινωνούν με το δίκτυό τους, μειώνοντας τον κίνδυνο της μη εξουσιοδοτημένης πρόσβασης και των παραβιάσεων των δεδομένων. (Raja Waseem Anwar, 2021)

Για την αποτελεσματική προστασία των ιατρικών υπολογιστικών δικτύων, τα τείχη προστασίας θα πρέπει να ρυθμιστούν με τέτοιο τρόπο ώστε να επιτρέπουν μόνο την απαραίτητη διαδικτυακή κίνηση, αποκλείοντας παράλληλα τις επιβλαβείς ή τις ύποπτες ενέργειες. Αυτό μπορεί να περιλαμβάνει τον περιορισμό της πρόσβασης σε συγκεκριμένες υπηρεσίες, την εφαρμογή συστημάτων πρόληψης και ανίχνευσης επιθέσεων, καθώς και τη χρήση προηγμένων τεχνολογιών ασφαλείας, όπως είναι η βαθιά επιθεώρηση των πακέτων δεδομένων.

Η συχνή παρακολούθηση και συντήρηση των ρυθμίσεων του τείχους προστασίας θεωρείται αρκετά σημαντική. Για την αποφυγή κυβερνοεπιθέσεων αλλά και για τον εντοπισμό των κενών ασφαλείας, είναι σημαντικό οι ιατρικές οργανώσεις να έχουν εγκαταστήσει τις πιο πρόσφατες ενημερώσεις ασφαλείας στα τείχη προστασίας που χρησιμοποιούν.

Συνοψίζοντας, τα τείχη προστασίας αποτελούν ένα σημαντικό στοιχείο για την προστασία των ιατρικών δικτύων. Εφαρμόζοντας και ρυθμίζοντας κατάλληλα τα τείχη προστασίας, οι ιατρικοί οργανισμοί μπορούν να βελτιώσουν την ασφάλεια των δικτύων τους και να προστατεύσουν τα δεδομένα τους.

4.1.3 Συστήματα Ανίχνευσης και Πρόληψης Εισβολών

Ένα σύστημα ανίχνευσης και πρόληψης εισβολών (Intrusion Detection and Prevention System – IDPS) είναι ένα εργαλείο ασφαλείας, σχεδιασμένο για την παρακολούθηση της κυκλοφορίας του δικτύου και για τον εντοπισμό των κυβερνοαπειλών μέσα σε ένα δίκτυο υπολογιστών. Λειτουργεί ως ένα σύστημα επιτήρησης που αναλύει πακέτα δικτύου, αρχεία καταγραφής, και άλλα δεδομένα δικτύου για να εντοπίσει κακόβουλη ή ύποπτη δραστηριότητα. Ο κύριος σκοπός ενός IDPS είναι να ανιχνεύει και να ανταποκρίνεται σε περιστατικά ασφαλείας σε πραγματικό χρόνο. Με αυτόν τον τρόπο οι ιατρικοί οργανισμοί μπορούν να προστατέψουν τα δίκτυα τους, τα ιατρικά υπολογιστικά συστήματα, και τα δεδομένα τους από κυβερνοεπιθέσεις. (Nureni Ayofe Azeez, 2019)

Τα συστήματα ανίχνευσης και πρόληψης εισβολών (IDPS) αποτελούν σημαντικά εργαλεία για τον εντοπισμό και την πρόληψη των κυβερνοεπιθέσεων σε ένα δίκτυο. Τα συστήματα αυτά παρακολουθούν την κυκλοφορία του δικτύου, εντοπίζουν τις πιθανές απειλές, και λαμβάνουν τις κατάλληλες ενέργειες για την μείωση των απειλών. Ένα IDPS μπορεί να χρησιμοποιήσει δύο κύριες μεθόδους ανίχνευσης: Την ανίχνευση βάσει υπογραφών και την ανίχνευση βάσει συμπεριφορών.

• Ανίχνευση με βάση την υπογραφή (Signature Based Detection): Αυτή η μέθοδος περιλαμβάνει τη σύγκριση ορισμένων μοτίβων και συμπεριφορών κυκλοφορίας δικτύου με μια βάση δεδομένων γνωστών υπογραφών επίθεσης. Η βάση δεδομένων περιέχει προκαθορισμένα μοτίβα και χαρακτηριστικά επιθέσεων που έχουν εντοπιστεί στο παρελθόν. Σε περίπτωση που το IDPS εντοπίσει κάποια σχέση μεταξύ της κίνησης δικτύου και μιας υπογραφής στη βάση δεδομένων, ενεργοποιεί μια ειδοποίηση ή λαμβάνει άμεσα μέτρα για την αποτροπή της επίθεσης. Η ανίχνευση βάσει των υπογραφών είναι αποτελεσματική για τον εντοπισμό των γνωστών απειλών και των επιθέσεων που έχουν καθιερωμένα πρότυπα.

• Ανίχνευση με βάσει την συμπεριφορά (Anomaly Based Detection): Η ανίχνευση με βάση την συμπεριφορά, εστιάζει στον στην συμπεριφορά του δικτύου. Το IDPS καθορίζει μια βασική γραμμή κανονικής δραστηριότητας παρακολουθώντας την κυκλοφορία του δικτύου για μια χρονική περίοδο και δημιουργώντας ένα προφίλ για το τι θεωρείται κανονική συμπεριφορά. Οποιαδήποτε δραστηριότητα αποκλίνει σημαντικά από την βασική γραμμή κανονικής δραστηριότητας, επισημαίνεται ως ύποπτη και ενεργοποιείτε μια ειδοποίηση. Η ανίχνευση με βάσει την συμπεριφορά είναι αποτελεσματική για τον εντοπισμό νέων ή άγνωστων επιθέσεων που δεν ταιριάζουν με γνωστές υπογραφές επίθεσης.

Τα συστήματα IDPS μπορούν να λειτουργήσουν με 2 τρόπους, με την λειτουργία του εντοπισμού και της πρόληψης. Στη λειτουργία του εντοπισμού, το σύστημα παρακολουθεί και αναλύει την κυκλοφορία του δικτύου, δημιουργώντας ειδοποιήσεις στην ομάδα ασφαλείας όταν εντοπιστεί πιθανή απειλή. Στη λειτουργία πρόληψης, το IDPS αναλαμβάνει την άμεση δράση για τον αποκλεισμό ή την εξουδετέρωση των απειλών που έχουν εντοπιστεί. (Nureni Ayofe Azeez, 2019)

Με την εφαρμογή των IDPS, οι ιατρικοί οργανισμοί μπορούν να βελτιώσουν τη θέση τους στον κυβερνοχώρο χρησιμοποιώντας τις παρακάτω λειτουργίες:

• Ανίχνευση απειλών σε πραγματικό χρόνο: Το IDPS παρακολουθεί συνεχώς την κυκλοφορία του δικτύου, εντοπίζοντας και ειδοποιώντας για πιθανές επιθέσεις στον κυβερνοχώρο σε πραγματικό χρόνο. Αυτό επιτρέπει στους ιατρικούς οργανισμούς να ανταποκρίνονται άμεσα και να ελαχιστοποιούν τον αντίκτυπο της επίθεσης.

• Πρόληψη επιθέσεων: Όταν το IDPS βρίσκεται σε λειτουργία πρόληψης, οι ιατρικοί οργανισμοί μπορούν να μπλοκάρουν ή να σταματήσουν αυτόματα τις επιθέσεις σε πραγματικό χρόνο, αποτρέποντάς την πρόκληση βλάβης ή της μη εξουσιοδοτημένης πρόσβασης σε προσωπικά ιατρικά δεδομένα.

3. Αντιμετώπιση περιστατικού: Το IDPS παράγει λεπτομερείς ειδοποιήσεις και αρχεία καταγραφής. Παρέχει σημαντικές πληροφορίες για τις ομάδες αντιμετώπισης περιστατικών, για τη διερεύνηση και τη λήψη των κατάλληλων μέτρων αντιμετώπισης.

4. Συμμόρφωση και κανονιστικές απαιτήσεις: Διάφορα κανονιστικά πλαίσια και βιομηχανικά πρότυπα, όπως ο νόμος HIPAA, απαιτούν την εφαρμογή μέτρων

ανίχνευσης και πρόληψης εισβολών. Εφαρμόζοντας ένα IDPS, οι ιατρικοί οργανισμοί μπορούν να διασφαλίσουν ότι συμμορφώνονται με τις κανονιστικές απαιτήσεις.

Συνοψίζοντας, το IDPS αποτελεί μια σημαντική τεχνολογία για τον εντοπισμό και την πρόληψη κυβερνοεπιθέσεων στους ιατρικούς οργανισμούς.

4.1.4 Συστήματα Διαχείρισης Πληροφοριών και Συμβάντων Ασφαλείας

Τα συστήματα διαχείρισης πληροφοριών και συμβάντων ασφαλείας (Security Information and Event Management - SIEM) αποτελούν εργαλεία που ενισχύουν σημαντικά την κυβερνοασφάλεια στην ιατρική επιστήμη. Σκοπό έχουν τη συγκέντρωση και τη συσχέτιση πληροφοριών συμβάντων ασφαλείας από διάφορες πηγές, εντός της υποδομής ενός δικτύου μιας ιατρικής οργάνωσης. Τα συστήματα SIEM συλλέγουν και αναλύουν αρχεία καταγραφής και άλλα δεδομένα, που σχετίζονται με την ασφάλεια από διαφορετικές πηγές όπως τα τείχη προστασίας, τα συστήματα ανίχνευσης εισβολής, τα λογισμικά προστασίας από τους ιούς, τους διακομιστές και τις συσκευές δικτύου. (Gustavo González-Granadillo, 2021)

• Συγκέντρωση Συμβάντων Ασφαλείας και Δεδομένων Καταγραφής: Τα συστήματα SIEM έχουν σχεδιαστεί για να συγκεντρώνουν και να συλλέγουν δεδομένα από διαφορετικές πηγές στην υποδομή ενός δικτύου μιας ιατρικής οργάνωσης. Αυτό περιλαμβάνει τη συλλογή αρχείων καταγραφής και συμβάντων που δημιουργούνται από τα τείχη προστασίας, τις συσκευές δικτύου, τους διακομιστές, τα τερματικά σημεία και τις συσκευές ασφαλείας. Με τη συγκέντρωση αυτών των πληροφοριών, τα συστήματα SIEM παρέχουν μια συνολική εικόνα ασφάλειας.

• Κανονικοποίηση και Ανάλυση: Μόλις συλλεχθούν τα δεδομένα, τα συστήματα SIEM εφαρμόζουν τεχνικές κανονικοποίησης και ανάλυσης για να τυποποιήσουν τη μορφή και τη δομή των δεδομένων. Αυτή η διαδικασία επιτρέπει την τακτική ανάλυση και συσχέτιση των συμβάντων ασφαλείας και των δεδομένων καταγραφής. Η κανονικοποίηση περιλαμβάνει τη μετατροπή των συλλεγόμενων δεδομένων σε μια κοινή μορφή, ενώ η ανάλυση περιλαμβάνει τη διάσπαση των δεδομένων σε πεδία για περαιτέρω ανάλυση.

• Συσχέτιση και Ανάλυση: Τα συστήματα SIEM υπερέχουν στον συσχετισμό και στην ανάλυση των συμβάντων ασφαλείας και των δεδομένων καταγραφής, για τον εντοπισμό των πιθανών συμβάντων ασφαλείας και απειλών. (Gustavo González-Granadillo, 2021) Με την εφαρμογή των κανόνων συσχέτισης, της στατιστικής ανάλυσης, και των αλγορίθμων μηχανικής μάθησης, τα συστήματα SIEM μπορούν να ανιχνεύουν μοτίβα και δραστηριότητες που μπορεί να υποδηλώνουν παραβίαση της ασφάλειας. Η συσχέτιση περιλαμβάνει την αντιστοίχιση και τη συσχέτιση γεγονότων μεταξύ διαφορετικών πηγών δεδομένων, για τη δημιουργία μιας ολοκληρωμένης εικόνας του τοπίου ασφαλείας.

• Δημιουργία ειδοποιήσεων και Απόκριση συμβάντων: Όταν το σύστημα SIEM εντοπίζει ένα συμβάν ή ένα μοτίβο που υπερβαίνει τα προκαθορισμένα όρια ή ταιριάζει με συγκεκριμένους κανόνες, οι διαχειριστές ασφαλείας ειδοποιούνται από το σύστημα. Οι ειδοποιήσεις παρέχουν σημαντικές πληροφορίες που αφορούν τα πιθανά περιστατικά ασφαλείας, και επιτρέπουν την έγκαιρη αντιμετώπιση των περιστατικών αυτών. Τα συστήματα SIEM μπορούν επίσης να αυτοματοποιήσουν ενέργειες απόκρισης συμβάντων, όπως τον αποκλεισμό των κακόβουλων διευθύνσεων IP, την απομόνωση των επηρεαζόμενων συστημάτων, ή την ενεργοποίηση πρόσθετων μέτρων ασφαλείας.

• Αναφορά και Συμμόρφωση: Τα συστήματα SIEM προσφέρουν ισχυρές δυνατότητες αναφοράς, επιτρέποντας στους οργανισμούς να δημιουργούν λεπτομερείς αναφορές για τα συμβάντα ασφαλείας και τη τήρηση της συμμόρφωσης. Αυτές οι αναφορές παρέχουν πληροφορίες σχετικά με τη θέση ασφαλείας του οργανισμού, τις πιθανές ευπάθειες και την κατάσταση συμμόρφωσης. Οι απαιτήσεις συμμόρφωσης που καθορίζονται από τους κανονισμούς μπορούν να αντιστοιχισθούν στο σύστημα SIEM για να διασφαλιστεί η συνεχής τήρηση και να διευκολυνθούν οι διαδικασίες ελέγχου.

• Ενσωμάτωση με Εργαλεία Ασφαλείας: Τα συστήματα SIEM μπορούν να ενσωματωθούν με διάφορα εργαλεία και τεχνολογίες ασφαλείας, όπως οι σαρωτές ευπάθειας και τα συστήματα διαχείρισης πρόσβασης. Αυτή η ενσωμάτωση ενισχύει τη συνολική αποτελεσματικότητα της υποδομής ασφάλειας.

Συνοψίζοντας, τα συστήματα SIEM θεωρούνται σημαντικά για τη συγκέντρωση, την ανάλυση και τη συσχέτιση συμβάντων ασφαλείας και δεδομένων καταγραφής από διάφορες πηγές.

4.1.5 Εικονικά Ιδιωτικά Δίκτυα (VPN)

Τα εικονικά ιδιωτικά δίκτυα (Virtual Private Networks - VPN) αποτελούν μια σημαντική τεχνολογία για την εξασφάλιση της απομακρυσμένης πρόσβασης σε ιατρικά δίκτυα. Ένα VPN παρέχει μια ασφαλή και κρυπτογραφημένη σύνδεση μεταξύ της συσκευής ενός χρήστη και του ιατρικού δικτύου, ακόμη και όταν χρησιμοποιούνται μη αξιόπιστα δίκτυα. Αυτό επιτρέπει στους επαγγελματίες υγείας και στους ασθενείς να έχουν μια ασφαλή πρόσβαση και μετάδοση των ιατρικών δεδομένων, διασφαλίζοντας την εμπιστευτικότητα, την ακεραιότητα και την ιδιωτικότητα. (Harmening, 2017)

Ένα από τα κύρια οφέλη του VPN που αφορά την απομακρυσμένη πρόσβαση, είναι η δημιουργία ενός ασφαλούς τούνελ μεταξύ της συσκευής του χρήστη και του ιατρικού δικτύου (Vasiliki Liagkou, 2019). Το τούνελ που δημιουργείται κρυπτογραφεί όλα τα δεδομένα που μεταδίδονται μεταξύ των δύο τελικών σημείων, καθιστώντας εξαιρετικά δύσκολο για τα μη εξουσιοδοτημένα άτομα να υποκλέψουν ή να έχουν πρόσβαση στα δεδομένα. Με την κρυπτογράφηση των δεδομένων, τα VPN προστατεύουν τα ιατρικά αρχεία και τις προσωπικές πληροφορίες των ασθενών.

Οι υπηρεσίες τηλεϊατρικής βασίζονται σε ένα μεγάλο βαθμό στα VPN για την ύπαρξη των ασφαλών συνδέσεων μεταξύ των παρόχων υπηρεσιών υγείας και των ασθενών. Χρησιμοποιώντας ένα VPN, οι επαγγελματίες υγείας μπορούν να αποκτήσουν μια ασφαλή πρόσβαση στο ιατρικό δίκτυο από τα από μια απομακρυσμένη τοποθεσία, επιτρέποντάς τους να έχουν πρόσβαση στα αρχεία των ασθενών. Οι ασθενείς θα μπορούν να μοιράζονται πληροφορίες υγείας, να συμμετέχουν σε εικονικά ραντεβού και να λαμβάνουν ιατρικές συμβουλές εξ αποστάσεως με την ίδια ασφάλεια.

Τα VPN παρέχουν επίσης μηχανισμούς ελέγχου ταυτότητας και ελέγχου πρόσβασης. Οι χρήστες θα πρέπει να ταυτοποιηθούν χρησιμοποιώντας διαπιστευτήρια πριν δημιουργήσουν μια σύνδεση VPN. Αυτό διασφαλίζει ότι μόνο εξουσιοδοτημένα άτομα μπορούν να έχουν πρόσβαση στο ιατρικό δίκτυο, μειώνοντας τον κίνδυνο της μη εξουσιοδοτημένης πρόσβασης και των πιθανών παραβιάσεων των ιατρικών δεδομένων.

Τα VPN παρέχουν μια ισχυρή ασφάλεια που αφορά την απομακρυσμένη πρόσβαση στα ιατρικά δίκτυα ωστόσο, η σωστή διαμόρφωση και η συντήρηση έχουν καθοριστικό ρόλο για τη διασφάλιση της αποτελεσματικότητάς των VPN. Οι ιατρικοί οργανισμοί θα πρέπει να εφαρμόζουν ασφαλή πρωτόκολλα, αλγόριθμους κρυπτογράφησης, να ενημερώνουν το λογισμικό VPN, καθώς και να εφαρμόζουν ισχυρούς μηχανισμούς ελέγχου ταυτότητας. (Harmening, 2017)

Συνοψίζοντας, τα VPN αποτελούν ένα σημαντικό εργαλείο για την εξασφάλιση της απομακρυσμένης πρόσβασης στα ιατρικά δίκτυα, ιδιαίτερα για τις υπηρεσίες της τηλεϊατρικής. Δημιουργούν ασφαλείς και κρυπτογραφημένες συνδέσεις, προστατεύοντας τα προσωπικά δεδομένα από τις μη εξουσιοδοτημένες προσβάσεις και διασφαλίζοντας την εμπιστευτικότητα και την ακεραιότητα των πληροφοριών των ασθενών. Με την εφαρμογή των VPN, οι ιατρικοί οργανισμοί μπορούν να παρέχουν με ασφάλεια τις απομακρυσμένες παροχές υγειονομικής περίθαλψης, και να βελτιώνουν το επίπεδο κυβερνοασφάλειας στις υποδομές που αφορούν την τηλεϊατρική.

4.1.6 Ασφάλεια Τελικού Σημείου

Τα μέτρα ασφαλείας τελικού σημείου συμβάλουν σημαντικά στην προστασία των μεμονωμένων συσκευών από κυβερνοαπειλές στον τομέα της ιατρικής επιστήμης. Το λογισμικό προστασίας από τους ιούς, τα συστήματα ανίχνευσης εισβολής που βασίζονται σε κεντρικούς υπολογιστές (Host-based Intrusion Detection System - HIDS), και η διαχείριση των φορητών συσκευών (Mobile Device Management - MDM), διασφαλίζουν την ακεραιότητα, την εμπιστευτικότητα και τη διαθεσιμότητα των δεδομένων. (Slate, 2018)

Το antivirus είναι ένα θεμελιώδες στοιχείο της ασφάλειας τελικού σημείου. Εντοπίζει, αποτρέπει και αφαιρεί διάφορους τύπους κακόβουλου λογισμικού που μπορούν να θέσουν σε κίνδυνο την ασφάλεια μιας συσκευής. Το antivirus σαρώνει αρχεία, προγράμματα και εισερχόμενα δεδομένα, με σκοπό να αναγνωρίσει κακόβουλα μοτίβα. Η συχνή ενημέρωση του antivirus είναι πολύ σημαντική για τη διασφάλιση της προστασίας του συστήματος από τις πιο πρόσφατες απειλές.

Τα συστήματα ανίχνευσης εισβολής (HIDS) που βασίζονται σε έναν κεντρικό υπολογιστή είναι ένα άλλο σημαντικό επίπεδο ασφάλειας τελικού σημείου. Το σύστημα

ανίχνευσης εισβολής παρακολουθεί τις δραστηριότητες και τα συμβάντα που συμβαίνουν σε μια μεμονωμένη συσκευή, όπως τις απόπειρες μη εξουσιοδοτημένης πρόσβασης, τις αλλαγές συστήματος αρχείων και τις ύποπτες συνδέσεις δικτύου. Τα συμβάντα αυτά συγκρίνονται με γνωστές υπογραφές επίθεσης η προκαθορισμένους κανόνες για τον εντοπισμό των πιθανών παραβιάσεων ασφάλειας. Το HIDS μπορεί επίσης να δημιουργήσει ειδοποιήσεις ή να προβεί σε αυτοματοποιημένες ενέργειες, όπως τον αποκλεισμό της κυκλοφορίας του δικτύου ή τον περιορισμό των ύποπτων αρχείων για την μείωση των πιθανών απειλών. (Ming Liu, 2018)

Οι λύσεις της διαχείριση των φορητών συσκευών (MDM) έχουν σχεδιαστεί ειδικά για την ασφάλεια και τη διαχείριση των κινητών συσκευών, όπως τα smartphones και τα tablets στο περιβάλλον της υγειονομικής περίθαλψης. Η διαχείριση των φορητών συσκευών παρέχει κεντρικό έλεγχο και επίβλεψη, επιτρέποντας στους διαχειριστές να επιβάλλουν πολιτικές ασφαλείας, να διαμορφώνουν τις ρυθμίσεις συσκευών και να διαχειρίζονται και να παρακολουθούν εξ αποστάσεως συσκευές. Οι λύσεις του MDM μπορούν να επιβάλουν την κρυπτογράφηση της συσκευής, την εφαρμογή ισχυρών απαιτήσεων κωδικών πρόσβασης, την ενεργοποίηση της απομακρυσμένης διαγραφής δεδομένων σε περίπτωση απώλειας ή κλοπής, και τον περιορισμό της πρόσβασης σε μη εξουσιοδοτημένες εφαρμογές ή πόρους. (Keunwoo Rhee, 2012)

Η συχνή ενημέρωση του λογισμικού και οι επιδιορθώσεις, έχουν καθοριστικό ρόλο για τη διατήρηση της ασφάλειας των συσκευών τελικού σημείου. Η διαχείριση των ενημερώσεων κώδικα διασφαλίζει ότι τα λειτουργικά συστήματα, οι εφαρμογές, και το firmware, έχουν λάβει τις πιο πρόσφατες ενημερώσεις κώδικα ασφαλείας.

Τα μέτρα ασφαλείας τελικού σημείου θα πρέπει να εφαρμόζονται παράλληλα και με άλλα μέτρα ασφαλείας στον κυβερνοχώρο προκειμένου να διαμορφωθεί μια ολοκληρωμένη στρατηγική άμυνας. Ορισμένα μέτρα από αυτά είναι, τα μέτρα ασφαλείας των δικτύων, η εκπαίδευση των χρηστών, και η εφαρμογή ισχυρών ελέγχων πρόσβασης.

Συνοψίζοντας, τα μέτρα ασφαλείας τελικού σημείου, όπως το λογισμικό προστασίας από τους ιούς, τα συστήματα ανίχνευσης εισβολής (HIDS), και η διαχείριση των φορητών συσκευών (MDM) είναι απαραίτητα για την προστασία των μεμονωμένων συσκευών από τις κυβερνοαπειλές στον τομέα της ιατρικής επιστήμης. Τα μέτρα αυτά βοηθούν

στον εντοπισμό και στην πρόληψη του κακόβουλου λογισμικού, στην παρακολούθηση και στην αντιμετώπιση των ύποπτων ενεργειών, και στην επιβολή πολιτικών ασφαλείας στις συσκευές. Εφαρμόζοντας αυτά τα μέτρα, οι ιατρικοί οργανισμοί μπορούν να ενισχύσουν την ασφάλεια των συσκευών τελικού σημείου και να μειώσουν τον κίνδυνο των κυβερνοεπιθέσεων.

4.1.7 Πρόληψη Απώλειας Δεδομένων

Η πρόληψη απώλειας δεδομένων (Data Loss Prevention - DLP) έχει σκοπό στην πρόληψη της μη εξουσιοδοτημένης αποκάλυψης των προσωπικών ιατρικών δεδομένων, στον τομέα της ιατρικής επιστήμης. Οι λύσεις DLP έχουν σχεδιαστεί για να αναγνωρίζουν, να παρακολουθούν, και να προστατεύουν τα προσωπικά ιατρικά δεδομένα. Αυτές οι λύσεις χρησιμοποιούν διάφορες τεχνικές για τον εντοπισμό και την πρόληψη των παραβιάσεων των δεδομένων, διασφαλίζοντας την προστασία των προσωπικών πληροφοριών.

Οι λύσεις DLP χρησιμοποιούν έναν συνδυασμό επιθεώρησης περιεχομένου, ανάλυσης περιεχομένου, και επιβολής πολιτικών διαδικασιών για τον εντοπισμό και τον έλεγχο των προσωπικών δεδομένων. Η επιθεώρηση περιεχομένου περιλαμβάνει τη σάρωση των δεδομένων σε διαφορετικές μορφές, όπως έγγραφα, μηνύματα ηλεκτρονικού ταχυδρομείου ή καταχωρήσεις βάσης δεδομένων, για τον εντοπισμό των προσωπικών πληροφοριών με βάση τους προκαθορισμένους κανόνες, τα μοτίβα ή τις ταξινομήσεις των δεδομένων. Μπορεί να περιλαμβάνονται τα προσωπικά αναγνωρίσιμα στοιχεία (PII), οι προστατευόμενες υγειονομικές πληροφορίες (PHI), τα οικονομικά δεδομένα ή οποιοδήποτε άλλα είδη προσωπικών πληροφοριών στον ιατρικό τομέα. (Manghui Tu, 2016)

Η ανάλυση περιεχομένου είναι ένα άλλο βασικό στοιχείο των λύσεων DLP. Περιλαμβάνει την ανάλυση του πλαισίου στην οποία γίνεται η πρόσβαση, η χρήση ή μετάδοση των προσωπικών δεδομένων. Αυτό μπορεί να περιλαμβάνει διάφορους παράγοντες, όπως την συμπεριφορά των χρηστών, τα μοτίβα πρόσβασης των δεδομένων, οι τοποθεσίες δικτύου και οι τύποι συσκευών. Λαμβάνοντας υπόψη τους παράγοντες που σχετίζονται με την ανάλυση περιεχομένου, οι λύσεις DLP μπορούν να εντοπίσουν άμεσα τις πιθανές παραβιάσεις των δεδομένων ή τις παραβιάσεις πολιτικών διαδικασιών, ακόμα κι αν τα ίδια τα δεδομένα δεν ταξινομούνται ως προσωπικά η ευαίσθητα.

Οι λύσεις DLP επιβάλλουν επίσης πολιτικές και εφαρμόζουν μέτρα προστασίας για την πρόληψη της μη εξουσιοδοτημένης αποκάλυψης των προσωπικών δεδομένων. Αυτό μπορεί να περιλαμβάνει ενέργειες όπως, την κρυπτογράφηση των δεδομένων, τον αποκλεισμό των δεδομένων, την εφαρμογή ελέγχων πρόσβασης καθώς και την δημιουργία ειδοποιήσεων για περαιτέρω έρευνα. Για παράδειγμα, εάν ένας χρήστης επιχειρήσει να στείλει ένα μήνυμα ηλεκτρονικού ταχυδρομείου που περιέχει προσωπικά ιατρικά δεδομένα σε έναν εξωτερικό παραλήπτη, η λύση DLP μπορεί να αποκλείσει το μήνυμα αυτό, ή να κρυπτογραφήσει το ευαίσθητο περιεχόμενο του πριν υπάρξει μετάδοση. (Manghui Tu, 2016)

Επιπλέον, οι λύσεις DLP μπορούν να παρέχουν δυνατότητες παρακολούθησης και αναφοράς για την επίβλεψη και τον έλεγχο της χρήσης δεδομένων σε έναν ιατρικό οργανισμό. Οι λύσεις DLP έχουν την δυνατότητα να δημιουργούν ειδοποιήσεις σε πραγματικό χρόνο στις περιπτώσεις παραβιάσεων πολιτικής, επιτρέποντας στις ομάδες ασφαλείας να ανταποκρίνονται άμεσα στις πιθανές παραβιάσεις των δεδομένων. Επιπλέον, οι λειτουργίες ολοκληρωμένων αναφορών παρέχουν πληροφορίες για τις ροές των δεδομένων, τις παραβιάσεις πολιτικής, και τη συνολική αποτελεσματικότητα της προστασίας των δεδομένων.

Με την εφαρμογή των λύσεων DLP, οι ιατρικοί οργανισμοί μπορούν να μειώσουν σε ένα μεγάλο βαθμό τον κίνδυνο της μη εξουσιοδοτημένης αποκάλυψης των προσωπικών ιατρικών δεδομένων. Αυτές οι λύσεις συμβάλλουν στην επιβολή των πολιτικών προστασίας δεδομένων, στον εντοπισμό και στην πρόληψη παραβιάσεων δεδομένων, και στην διατήρηση της συμμόρφωσης με τους κανονισμούς και τα πρότυπα του ιατρικού τομέα, όπως είναι ο νόμος περί φορητότητας και λογοδοσίας ασφάλισης υγείας (HIPAA).

Οι λύσεις DLP είναι αποτελεσματικές για την πρόληψη της μη εξουσιοδοτημένης αποκάλυψης των δεδομένων ωστόσο, θα πρέπει να εφαρμόζονται ως ένα μέρος μιας ευρύτερης στρατηγικής για την κυβερνοασφάλεια. Αυτό περιλαμβάνει μέτρα, όπως την εκπαίδευση των χρηστών, τους ελέγχους πρόσβασης, την ασφάλεια δικτύου και τις τακτικές αξιολογήσεις ασφάλειας.

Συνοψίζοντας, οι λύσεις DLP αποτελούν απαραίτητα εργαλεία για την πρόληψη της μη εξουσιοδοτημένης αποκάλυψης των προσωπικών ιατρικών δεδομένων στον τομέα της ιατρικής επιστήμης. Χρησιμοποιώντας τις δυνατότητες επιθεώρησης περιεχομένου, την ανάλυση περιεχομένου, και την επιβολή πολιτικής, οι λύσεις DLP συμβάλλουν στον εντοπισμό και στην προστασία των προσωπικών δεδομένων, διασφαλίζοντας την εμπιστευτικότητα των δεδομένων σύμφωνα με τους κανονισμούς προστασίας.

4.2 Προηγμένες Τεχνολογίες και Τάσεις

4.2.1 Επισκόπηση

Η τεχνητή νοημοσύνη έχει φέρει επανάσταση στον τομέα της κυβερνοασφάλειας πάνω στην ιατρική επιστήμη, επιτρέποντας την προηγμένη ανίχνευση και ανάλυση των απειλών. Τα συστήματα που λειτουργούν με βάση την τεχνητή νοημοσύνη μπορούν να αναλύσουν τεράστιες ποσότητες δεδομένων, συμπεριλαμβανομένης της κυκλοφορίας του δικτύου, της συμπεριφοράς των χρηστών, και των αρχείων καταγραφής του συστήματος, για τον εντοπισμό των πιθανών απειλών και των προτύπων στον κυβερνοχώρο σε πραγματικό χρόνο. Οι αλγόριθμοι μηχανικής μάθησης μπορούν συνεχώς να μαθαίνουν και να προσαρμόζονται σε νέες τεχνικές επίθεσης, ενισχύοντας την αποτελεσματικότητα των συστημάτων ανίχνευσης και πρόληψης των εισβολών. Η τεχνητή νοημοσύνη μπορεί επίσης να αυτοματοποιήσει τις διαδικασίες απόκρισης των περιστατικών, να βελτιώσει τη διαχείριση των ευπαθειών, και να ενισχύσει τη συνολική άμυνα στον κυβερνοχώρο.

Η τεχνολογία Blockchain προσφέρει διάφορες λύσεις για την ενίσχυση της ασφάλειας και της ιδιωτικότητας των ιατρικών δεδομένων. Στην ιατρική επιστήμη, η τεχνολογία blockchain μπορεί να χρησιμοποιηθεί για την ασφαλή αποθήκευση των προσωπικών πληροφοριών των ασθενών, διατηρώντας παράλληλα την ιδιωτικότητα και αποτρέποντας τη μη εξουσιοδοτημένη πρόσβαση. Επιπλέον, τα έξυπνα συμβόλαια (smart contracts) επιτρέπουν την ασφαλή μετάδοση των δεδομένων μεταξύ των διάφορων ιατρικών οργανισμών.

Το διαδίκτυο των ιατρικών πραγμάτων (Internet of Medical Things - IoMT) αναφέρεται στα δίκτυα των ιατρικών συσκευών, των φορητών συσκευών, και των αισθητήρων που συλλέγουν και μεταδίδουν τα δεδομένα των ασθενών. Το IoMT προσφέρει πολλά οφέλη για τη φροντίδα και την παρακολούθηση των ασθενών, ωστόσο εισάγει ζητήματα ασφαλείας στον κυβερνοχώρο. Η προστασία των συνδεδεμένων ιατρικών συσκευών από κυβερνοαπειλές πρέπει να διασφαλίζεται στο μέγιστο βαθμό. Ο ασφαλής έλεγχος της ταυτότητας των συσκευών, η κρυπτογράφηση των δεδομένων, και η τμηματοποίηση του δικτύου, είναι κάποια από τα μέτρα που μπορούν να συμβάλουν στην μείωση των κινδύνων που σχετίζονται με το IoMT.

Το cloud computing χρησιμοποιείτε όλο και περισσότερο στον τομέα της ιατρικής επιστήμης λόγω της επεκτασιμότητας, της ευελιξίας, και της οικονομικής αποδοτικότητας του. Ωστόσο και το cloud computing εισάγει ζητήματα ασφαλείας στον κυβερνοχώρο. Το cloud security εστιάζει στην προστασία των δεδομένων που αποθηκεύονται στο cloud. Με αυτόν τον τρόπο, διασφαλίζεται η ιδιωτικότητα των δεδομένων, ο έλεγχο πρόσβασης, και η ασφαλής μετάδοση των δεδομένων. Οι ισχυροί μηχανισμοί ελέγχου ταυτότητας, η κρυπτογράφηση, οι τακτικοί έλεγχοι και η συμμόρφωση με τους σχετικούς κανονισμούς, είναι απαραίτητοι για τη διατήρηση μιας ασφαλούς υποδομής cloud στον ιατρικό τομέα.

Οι τεχνολογίες αυτές, διαμορφώνουν το μέλλον της κυβερνοασφάλειας στον τομέα της ιατρικής επιστήμης. Η εφαρμογή των ισχυρών μέτρων ασφαλείας βοηθάει τους ιατρικούς οργανισμούς να προστατεύουν τα προσωπικά τους δεδομένα, να αποτρέπουν τυχόν κυβερνοεπιθέσεις, και να διασφαλίζουν την εμπιστοσύνη και την ασφάλεια των ασθενών.

4.2.2 Τεχνητή Νοημοσύνη

Η τεχνητή νοημοσύνη (Artificial Intelligence – AI) επιτρέπει την ενίσχυση της κυβερνοασφάλειας στον τομέα της ιατρικής επιστήμης. Με την αυξανόμενη ψηφιοποίηση των συστημάτων υγείας, και τον αυξανόμενο όγκο των ιατρικών δεδομένων, η εφαρμογή προηγμένων τεχνολογιών κυβερνοασφάλειας είναι σημαντική. Η τεχνητή νοημοσύνη προσφέρει προηγμένες δυνατότητες για την ανίχνευση και την αντιμετώπιση των απειλών, βοηθώντας τις ιατρικές οργανώσεις να προστατεύουν τα δεδομένα τους και να διασφαλίζουν την ιδιωτικότητα των ασθενών. (Kun-Hsing Yu, 2018)

Μια βασική εφαρμογή της τεχνητής νοημοσύνης είναι η χρήση των αλγορίθμων μηχανικής μάθησης. Οι αλγόριθμοι μηχανικής μάθησης μπορούν να αναλύσουν μεγάλους όγκους ιατρικών δεδομένων για να εντοπίσουν τους πιθανούς κινδύνους ασφαλείας. Με την εφαρμογή της τεχνητής νοημοσύνης, οι ιατρικοί οργανισμοί έχουν την δυνατότητα να ανιχνεύουν και να περιορίζουν τις κυβερνοαπειλές σε πραγματικό χρόνο.

Οι αλγόριθμοι μηχανικής μάθησης μαθαίνουν από τα ιστορικά δεδομένων και προσαρμόζονται στις εξελισσόμενες απειλές. Μπορούν να ανιχνεύσουν κακόβουλες ενέργειες, όπως απόπειρες μη εξουσιοδοτημένης πρόσβασης ή ασυνήθιστες μεταφορές δεδομένων, και να ειδοποιούν για περαιτέρω διερεύνηση περιστατικών κυβερνοασφάλειας. Με την αυτοματοποίηση αυτών των διαδικασιών, η τεχνητή νοημοσύνη επιτρέπει τον έγκαιρο εντοπισμό και την ταχεία ανταπόκριση στις κυβερνοεπιθέσεις. (Kun-Hsing Yu, 2018)

Επιπλέον, η τεχνητή νοημοσύνη μπορεί να ενισχύσει την ασφάλεια των ιατρικών συσκευών. Καθώς το διαδίκτυο των ιατρικών πραγμάτων (IoMT) εφαρμόζεται όλο και περισσότερο στον τομέα της ιατρικής επιστήμης, η ασφάλεια των συνδεδεμένων ιατρικών συσκευών θεωρείται σημαντική. Η τεχνητή νοημοσύνη μπορεί να παρακολουθεί τη συμπεριφορά αυτών των συσκευών σε πραγματικό χρόνο, να εντοπίζει ύποπτες δραστηριότητες, και να ενεργοποιεί τα κατάλληλα μέτρα ασφαλείας. Με αυτόν τον τρόπο, διασφαλίζεται η ακεραιότητα και η ασφάλεια των ιατρικών συσκευών.

Τα συστήματα που λειτουργούν με βάση την τεχνητή νοημοσύνη μπορούν επίσης να συμβάλουν στη διαχείριση των ευπαθειών, εντοπίζοντας τις πιθανές αδυναμίες στα ιατρικά δίκτυα, στα συστήματα, ή στις εφαρμογές. Μέσω της αυτοματοποιημένης ανάλυσης, η τεχνητή νοημοσύνη μπορεί να ανιχνεύει ευπάθειες και να προτείνει τις κατάλληλες ενημερώσεις ασφαλείας ή επιδιορθώσεις. Η προσέγγιση αυτή, βοηθά στην πρόληψη της εκμετάλλευσης των αδύναμων σημείων, και ενισχύει τη συνολική θέση της ασφαλείας των ιατρικών οργανισμών. (Kun-Hsing Yu, 2018)

4.2.3 Blockchain

Η τεχνολογία Blockchain αποτελεί μια λύση για την ενίσχυση της ασφάλειας και της ιδιωτικότητας των ιατρικών δεδομένων και των συναλλαγών. Τα ιατρικά δεδομένα αποθηκεύονται σε κεντρικά συστήματα, καθιστώντας τα ευάλωτα σε τυχόν παραβιάσεις. Η τεχνολογία blockchain φέρνει επανάσταση στον τρόπο αποθήκευσης, μετάδοσης και ασφάλειας των ιατρικών δεδομένων. (Peng Zhang, 2018)

Ένα από τα βασικά χαρακτηριστικά της τεχνολογίας blockchain είναι η ικανότητά της να παρέχει αποκεντρωμένη διαχείριση ταυτότητας. Αυτό σημαίνει ότι οι ασθενείς και οι ιατρικοί οργανισμοί μπορούν να έχουν τον έλεγχο της δικής τους ψηφιακής ταυτότητας. Με την αποκεντρωμένη διαχείριση ταυτότητας, οι ασθενείς μπορούν να διαχειρίζονται με ασφάλεια τα προσωπικά τους αρχεία.

Επιπλέον, η τεχνολογία blockchain επιτρέπει τη χρήση των έξυπνων συμβολαίων. Τα έξυπνα συμβόλαια είναι αυτοεκτελούμενες συμφωνίες που αποθηκεύονται στο blockchain και εκτελούν αυτόματα προκαθορισμένες ενέργειες όταν πληρούνται συγκεκριμένες προϋποθέσεις. Στον τομέα της ιατρικής επιστήμης, τα έξυπνα συμβόλαια μπορούν να απλοποιήσουν διάφορες διαδικασίες. Αξιοποιώντας τα έξυπνα συμβόλαια, οι ιατρικοί οργανισμοί μπορούν να διασφαλίζουν την ακρίβεια και την αποτελεσματικότητα στις ιατρικές υπηρεσίες που παρέχουν. (Peng Zhang, 2018)

Η τεχνολογία blockchain παρέχει ένα υψηλό επίπεδο ασφάλειας μέσω των χαρακτηριστικών που διαθέτει. Η τεχνολογία blockchain καθιστά εξαιρετικά δύσκολη την παραβίαση των αποθηκευμένων δεδομένων από κυβερνοεγκληματίες και χάκερς. Κάθε συναλλαγή καταγράφεται σε ένα μπλοκ όπου συνδέεται με ένα προηγούμενο μπλοκ μέσω κρυπτογραφικών κατακερματισμών, σχηματίζοντας μια αμετάβλητη

αλυσίδα. Με αυτόν τον τρόπο, διασφαλίζεται η ακεραιότητα των δεδομένων και η αποτροπή των μη εξουσιοδοτημένων τροποποιήσεων. (Maria Prokofieva, 2019)

Επιπλέον, το blockchain χρησιμοποιεί αλγορίθμους κρυπτογράφησης για την ασφάλεια των δεδομένων και τη διασφάλιση της εμπιστευτικότητας. Οι συμμετέχοντες στο δίκτυο του blockchain διαθέτουν ιδιωτικά κλειδιά που τους επιτρέπουν την ασφαλή πρόσβαση στα δεδομένα. Οι συναλλαγές μπορούν να κρυπτογραφηθούν για την προστασία των προσωπικών πληροφοριών. Επίσης, εφαρμόζονται έλεγχοι πρόσβασης για τη ρύθμιση της κοινής χρήσης των δεδομένων μεταξύ εξουσιοδοτημένων μερών.

Η τεχνολογία blockchain προσφέρει σημαντική ασφάλεια, ωστόσο μπορεί να εισάγει διάφορα ζητήματα. Η επεκτασιμότητα, η διαλειτουργικότητα και η συμμόρφωση προς τους κανονιστικούς κανόνες, είναι μερικές από τις προκλήσεις που πρέπει να αντιμετωπιστούν κατά την εφαρμογή λύσεων αλυσίδας μπλοκ, στον τομέα της ιατρικής επιστήμης. Επιπλέον, πρέπει να δημιουργηθούν τα κατάλληλα πλαίσια διακυβέρνησης για τη διασφάλιση της ακεραιότητας και της αξιοπιστίας ενός δικτύου blockchain.

4.2.4 Το Διαδίκτυο Των Ιατρικών Πραγμάτων (IoMT)

Η αυξανόμενη χρήση των ιατρικών συσκευών έχει επιφέρει πολλά οφέλη στον τομέα της ιατρικής επιστήμης,, όπως την βελτιωμένη παρακολούθηση των ασθενών, και την βελτιωμένη παροχή υγειονομικής περίθαλψης. Ωστόσο, το IoMT εισάγει διάφορα ζητήματα ασφαλείας που πρέπει να αντιμετωπιστούν για την προστασία των προσωπικών ιατρικών δεδομένων.

Ένα ζήτημα ασφαλείας που σχετίζεται με τις συσκευές IoMT είναι η ανάγκη για την ασφάλεια των ιατρικών δεδομένων κατά τη μεταφορά. Οι συσκευές IoMT συχνά συλλέγουν και μεταδίδουν προσωπικές πληροφορίες ασθενών. Αυτά τα δεδομένα συνήθως μεταδίδονται μέσω δικτύων σε ιατρικούς οργανισμούς ή αποθηκεύονται σε κεντρικά συστήματα ή συστήματα που βασίζονται σε περιβάλλον cloud. Η διασφάλιση της εμπιστευτικότητας και της ακεραιότητας αυτών των δεδομένων είναι άκρως σημαντική για την αποτροπή παραβιάσεων. (Vishnu, Ramson, & Jegan, 2020)

Η διασφάλιση των ιατρικών δεδομένων κατά τη μεταφορά απαιτεί την εφαρμογή ισχυρών πρωτοκόλλων κρυπτογράφησης και ασφαλών καναλιών επικοινωνίας. Ορισμένοι τρόποι κρυπτογράφησης, όπως είναι το TLS (Transport Layer Security) ή το πρωτόκολλο SSL (Secure Sockets Layer) μπορούν να χρησιμοποιηθούν για την κρυπτογράφηση των δεδομένων κατά τη μετάδοση, καθιστώντας τα μη αναγνώσιμα σε μη εξουσιοδοτημένα άτομα. Επιπλέον, τα ασφαλή πρωτόκολλα επικοινωνίας όπως τα εικονικά ιδιωτικά δίκτυα (VPN) ή τα ασφαλή δίκτυα Wi-Fi, μπορούν να χρησιμοποιηθούν για τη δημιουργία ασφαλών συνδέσεων μεταξύ των συσκευών IoMT και των συστημάτων υγειονομικής περίθαλψης.

Η διασφάλιση των ιατρικών δεδομένων περιλαμβάνει την εφαρμογή ισχυρών ελέγχων πρόσβασης καθώς και την εφαρμογή μηχανισμών κρυπτογράφησης. Τα στοιχεία ελέγχου πρόσβασης μπορούν να περιορίσουν τα μη εξουσιοδοτημένα άτομα, στο να αποκτήσουν πρόσβαση στα προσωπικά ιατρικά δεδομένα που αποθηκεύονται στις βάσεις δεδομένων, στους διακομιστές ή στις πλατφόρμες cloud. Ο έλεγχος ταυτότητας χρήστη, ο έλεγχος πρόσβασης βάσει ρόλου, και ο έλεγχος ταυτότητας πολλαπλών παραγόντων είναι μερικές από τις τεχνικές που μπορούν να χρησιμοποιηθούν για την διασφάλιση των δεδομένων.

Η κρυπτογράφηση αποτελεί μια σημαντική τεχνική για την ασφάλεια των ιατρικών δεδομένων. Η κρυπτογράφηση των δεδομένων μπορεί να εφαρμοστεί σε επίπεδο συσκευής, διασφαλίζοντας την κρυπτογράφηση των δεδομένων πριν αυτά αποθηκευτούν. Μόνο τα εξουσιοδοτημένα άτομα που διαθέτουν τα κατάλληλα κλειδιά αποκρυπτογράφησης θα μπορούν να έχουν πρόσβαση στα αποθηκευμένα δεδομένα. Οι ισχυροί αλγόριθμοι κρυπτογράφησης, όπως ο αλγόριθμος Advanced Encryption Standard (AES), μπορούν να χρησιμοποιηθούν για την προστασία της εμπιστευτικότητας και της ακεραιότητας των δεδομένων.

Επιπλέον, οι μηχανισμοί παρακολούθησης και ανίχνευσης απειλών είναι απαραίτητοι για τον εντοπισμό των πιθανών παραβιάσεων. Τα συστήματα ανίχνευσης και πρόληψης εισβολών (IDPS) παρακολουθούν την κυκλοφορία του δικτύου, και ειδοποιούν έγκαιρα τους παρόχους υγειονομικής περίθαλψης όταν διαπιστώνεται κάποια ύποπτη ενέργεια. Επιπλέον, τα συστήματα διαχείρισης πληροφοριών και συμβάντων ασφαλείας (SIEM) μπορούν να χρησιμοποιηθούν για τη συγκέντρωση και την ανάλυση των συμβάντων ασφαλείας και των αρχείων καταγραφής από διάφορες συσκευές και συστήματα IoMT,

παρέχοντας μια ολοκληρωμένη εικόνα του τοπίου ασφαλείας και επιτρέποντας την έγκαιρη αντιμετώπιση πιθανών απειλών.

Η ασφάλεια των συσκευών IoMT και των ιατρικών δεδομένων απαιτεί μια πολυεπίπεδη προσέγγιση, η οποία περιλαμβάνει οργανωτικές πολιτικές και την εκπαίδευση των χρηστών. Η διαχείριση των ενημερώσεων κώδικα και οι συχνές αξιολογήσεις ασφαλείας, είναι απαραίτητες για τη διασφάλιση της προστασία των συσκευών IoMT. Οι ιατρικοί οργανισμοί θα πρέπει επίσης να έχουν θεσπίσει πολιτικές ασφαλείας για να βελτιώσουν την συνολική προστασία τους.

4.2.5 Cloud Security

Η διασφάλιση των ιατρικών δεδομένων στο cloud απαιτεί την εξέταση διαφόρων παραγόντων που διασφαλίζουν την εμπιστευτικότητα, την ακεραιότητα και την διαθεσιμότητα των προσωπικών πληροφοριών των ασθενών. Το υπολογιστικό νέφος (Cloud Computing) προσφέρει πολυάριθμα οφέλη για τις ιατρικές οργανώσεις, όπως την επεκτασιμότητα, την οικονομική αποδοτικότητα, και την προσβασιμότητα. Ωστόσο, εισάγει ζητήματα ασφάλειας που πρέπει να αντιμετωπιστούν για την αποτελεσματική προστασία των ιατρικών δεδομένων.

Η διασφάλιση της ιδιωτικότητας των ιατρικών δεδομένων στο cloud είναι ένα ζήτημα ασφαλείας που πρέπει να αντιμετωπιστεί. Οι ιατρικοί οργανισμοί πρέπει να διασφαλίζουν την ιδιωτικότητα και την προσβασιμότητα των πληροφοριών υγείας μόνο σε εξουσιοδοτημένα άτομα. Η κρυπτογράφηση είναι μια σημαντική μέθοδος για την επίτευξη της ιδιωτικότητας των δεδομένων. Τα πρωτόκολλα TLS ή SSL μπορούν να χρησιμοποιηθούν για την κρυπτογράφηση των δεδομένων κατά τη μετάδοση, ενώ οι προηγμένοι αλγόριθμοι κρυπτογράφησης, όπως ο αλγόριθμος AES, μπορούν να προστατεύσουν τα δεδομένα που αποθηκεύονται στο cloud. (Igor Muttik, 2009)

Ένα άλλο ζήτημα ασφαλείας είναι η διατήρηση της ακεραιότητας των δεδομένων. Οι ιατρικοί οργανισμοί πρέπει να διασφαλίζουν ότι τα ιατρικά δεδομένα που διαχειρίζονται παραμένουν αμετάβλητα. Οι ψηφιακές υπογραφές καθώς και άλλοι μηχανισμοί ασφαλείας, μπορούν να βοηθήσουν στην ανίχνευση των παραβιάσεων των δεδομένων.

Η διαθεσιμότητα των ιατρικών δεδομένων είναι επίσης ένα άλλο σημαντικό ζήτημα που πρέπει να ληφθεί υπόψη. Οι ιατρικοί οργανισμοί βασίζονται στην τακτική πρόσβαση των πληροφοριών των ασθενών για την παροχή των υπηρεσιών υγείας. Οι πάροχοι υπηρεσιών cloud θα πρέπει να διαθέτουν μια ισχυρή υποδομή, προκειμένου να μπορούν να διασφαλίζουν την υψηλή διαθεσιμότητα των ιατρικών δεδομένων.

Ο έλεγχος πρόσβασης είναι ένα απαραίτητο στοιχείο για την ασφάλεια των ιατρικών δεδομένων στο cloud. Οι ιατρικοί οργανισμοί θα πρέπει να εφαρμόζουν ισχυρούς μηχανισμούς ελέγχου ταυτότητας, προκειμένου να επαληθεύουν την ταυτότητα των χρηστών που έχουν πρόσβαση στο cloud. Ο έλεγχος πρόσβασης βάσει ρόλων μπορεί να χρησιμοποιηθεί για τη χορήγηση των κατάλληλων προνομίων πρόσβασης με βάση τους ρόλους και τις ευθύνες εργασίας. (Yazan Al-Issa, 2019)

Ο διαχωρισμός και η απομόνωση των δεδομένων είναι ένα σημαντικό στοιχείο που πρέπει να εφαρμόζεται σε ένα περιβάλλον cloud. Οι ιατρικοί οργανισμοί θα πρέπει να έχουν διασφαλίσει ότι τα δεδομένα τους διαχωρίζονται σωστά, προκειμένου να μπορούν να αποτρέψουν τη μη εξουσιοδοτημένη πρόσβαση των δεδομένων. Η εφαρμογή τεχνικών τμηματοποίησης και κρυπτογράφησης δεδομένων μπορεί να βοηθήσει στην επιβολή της απομόνωσης των δεδομένων.

Οι τακτικές αξιολογήσεις και οι έλεγχοι ασφαλείας θεωρούνται απαραίτητοι για την διασφάλιση της προστασίας των ιατρικών δεδομένων στο cloud. Οι δοκιμές διείσδυσης, η σάρωση ευπάθειας, και η παρακολούθηση των συμβάντων ασφαλείας, θα πρέπει να εκτελούνται τακτικά για τον εντοπισμό και την αντιμετώπιση των πιθανών αδυναμιών ασφαλείας. Η συμμόρφωση με τους κανονισμούς και τα βιομηχανικά πρότυπα πρέπει να ληφθεί σοβαρά υπόψη κατά την επιλογή ενός παρόχου cloud. (Igor Muttik, 2009)

Για την μείωση των κινδύνων που σχετίζονται με την ασφάλεια των ιατρικών δεδομένων στο cloud, οι ιατρικοί οργανισμοί θα πρέπει να θεσπίσουν σαφείς πολιτικές και διαδικασίες ασφαλείας, καθώς και να παρέχουν τακτική εκπαίδευση στο προσωπικό σχετικά με τις βέλτιστες πρακτικές ασφάλειας cloud.

Κεφάλαιο 5. Συμπεράσματα

5.1 Συμπεράσματα

Η ραγδαία άνοδο της τεχνολογίας έχει προσφέρει πολλά οφέλη στον τομέα της ιατρικής επιστήμης. Ωστόσο, η εξάρτηση της τεχνολογίας μπορεί να επιφέρει σοβαρές συνέπειες για τις ιατρικές οργανώσεις. Στη παρούσα διπλωματική εργασία, διερευνήθηκαν οι κυβερνοαπειλές που αντιμετωπίζουν οι ιατρικοί οργανισμοί, όπως είναι οι επιθέσεις ransomware και οι επιθέσεις ηλεκτρονικού ψαρέματος. Επίσης, έχει γίνει εμβάθυνση στις βέλτιστες πρακτικές που περιορίζουν τις κυβερνοαπειλές στον τομέα της ιατρικής επιστήμης, με έμφαση στα προληπτικά μέτρα, στην εκπαίδευση των εργαζομένων, και στην εφαρμογή ισχυρών ελέγχων πρόσβασης. Επιπλέον, διερευνήθηκαν διάφορες τεχνολογίες και εργαλεία που αξιοποιούν οι ιατρικοί οργανισμοί για την ενίσχυση της κυβερνοασφάλειας, όπως τα εικονικά ιδιωτικά δίκτυα (VPN) και το διαδίκτυο των ιατρικών πραγμάτων (IoMT).

Βιβλιογραφία

Aljaidi, M., Alsarhan, A., Samara, G., Alazaidah, R., Almatarneh, S., Khalid, M., & Al-Gumaei, Y. A. (2022 , November 29). NWannaCry Ransomware Attack: Technical Explanation of The Vulnerability, Exploitation, and Countermeasures. IEEE Xplore: https://ieeexplore.ieee.org/abstract/document/10050485

Aycock, J. (2006). Computer Viruses and Malware. https://books.google.gr/books?hl=el&lr=&id=xnW-qvk1gzkC&oi=fnd&pg=PA1&dq=Computer+viruses&ots=utpipbIk5u&sig=Ht2ElLkEt638pF3TU4jc8pstTbk&redir_esc=y#v=onepage&q=Computer%20viruses&f=false

Barbara Krumay, E. W. (2018, November 02). Evaluation of Cybersecurity Management Controls and Metrics of Critical Infrastructures: A Literature Review Considering the NIST Cybersecurity Framework. SPRINGER LINK: https://link.springer.com/chapter/10.1007/978-3-030-03638-6_23

Brewer, R. (2016, September). Ransomware attacks: detection, prevention and cure. ScienceDirect: https://www.sciencedirect.com/science/article/abs/pii/S1353485816300861

Castiglioni, A. (2019, January). A History of Medicine. https://books.google.gr/books?hl=el&lr=&id=06l-DwAAQBAJ&oi=fnd&pg=PT32&dq=History+of+Medical+Science&ots=_HY2Jg_tux&sig=3xcnmQz3ddn-MciUH_saZHpvTl8&redir_esc=y#v=onepage&q=History%20of%20Medical%20Science&f=false

Cheng, J. (2022, June 22). The Human Consequences of Ransomware Attacks. ISACA: https://www.isaca.org/resources/isaca-journal/issues/2022/volume-3/the-human-consequences-of-ransomware-attacks

Collier, R. (2017, June 5). NHS ransomware attack spreads worldwide. CMAJ: https://www.cmaj.ca/content/189/22/E786.short

Dave, K. T. (2013, June). Brute-force Attack “Seeking but Distressing”. https://citeseerx.ist.psu.edu/document?repid=rep1&type=pdf&doi=02449b7b97662ef7cd48b880a701f416084d8c31

David Blumenthal, M. T. (2010, August 5). The “Meaningful Use” Regulation for Electronic Health Records. The New England Journal of Medicine: https://www.nejm.org/doi/full/10.1056/NEJMp1006114

David P, N. S. (2018, May 11). Healthcare Facilities: Another Target for Ransomware Attacks. Marshall Digital Scholar : https://mds.marshall.edu/mgmt_faculty/194/

Da-Yu KAO, S.-C. H. (2019, Feb 20). Analyzing WannaCry Ransomware Considering the Weapons and Exploits. IEEE Xplore: https://ieeexplore.ieee.org/abstract/document/8702049

Douglas A. Perednia, A. A. (1995, February 8). Telemedicine Technology and Clinical Applications. Jama Network: https://jamanetwork.com/journals/jama/article-abstract/386892

Emmanouil G. Spanakis, S. B. (2020, July). Cyber-attacks and threats for healthcare – a multi-layer thread analysis. IEEE Xplore: https://ieeexplore.ieee.org/abstract/document/9176698/authors#authors

Fosnock, C. (χ.χ.). Computer Worms: Past, Present, and Future. https://ivanlef0u.fr/repo/madchat/vxdevl/avtech/Computer%20Worms_%20Past,%20Present,%20and%20Future.pdf

Francois Mouton, L. L. (2016, June). Social engineering attack examples, templates and scenarios. ScienceDirect: https://www.sciencedirect.com/science/article/abs/pii/S0167404816300268

Frank Luh, Y. Y. (2020, August). Cybersecurity in Science and Medicine: Threats and Challenges. Science Direct: https://www.sciencedirect.com/science/article/abs/pii/S0167779920300548

Greene, A. H. (2012, April). HIPAA Compliance for Clinician Texting. AHIMA.

Gurinder Pal Singh, V. B. (2021, January). A Review on NIST, ISO 27001, HIPAA and. https://www.researchgate.net/profile/Gurinder-Singh-32/publication/371313513_A_Review_on_NIST_ISO_27001_HIPAA_and_MITRE_ATTCK_Cybersecurity_Frameworks/links/647eb5ed2cad460a1bf8a8b4/A-Review-on-NIST-ISO-27001-HIPAA-and-MITRE-ATT-CK-Cybersecurity-Framework

Gustavo González-Granadillo, S. G.-Z. (2021, July 12). Security Information and Event Management (SIEM): Analysis, Trends, and Usage in Critical Infrastructures. https://www.mdpi.com/1424-8220/21/14/4759: https://www.mdpi.com/1424-8220/21/14/4759

Harmening, J. T. (2017). Chapter 58 - Virtual Private Networks. ScienceDirect: https://www.sciencedirect.com/science/article/abs/pii/B9780128038437000582

Houssain Kettani, P. W. (2019, March 17). On the Top Threats to Cyber Systems. IEEE Xplore: https://ieeexplore.ieee.org/xpl/conhome/8703750/proceeding

Hsiao, S.-C., & Kao, D.-Y. (2018, February). The static analysis of WannaCry ransomware. IEEE XPLORE: https://ieeexplore.ieee.org/abstract/document/8323680

I. Glenn Cohen, M. M. (2018, July 17). HIPAA and Protecting Health Information in the 21st Century. JAMA Network: https://jamanetwork.com/journals/jama/article-abstract/2682916

IBM. (2020). Cost of a Data Breach Report. https://www.ibm.com/security/digital-assets/cost-data-breach-report/1Cost%20of%20a%20Data%20Breach%20Report%202020.pdf

Igor Muttik, C. B. (2009, February). Cloud security technologies. ScienceDirect: https://www.sciencedirect.com/science/article/abs/pii/S1363412709000028

Jessica Colnago, S. D. (2018, April). “It's not actually that horrible”: Exploring Adoption of Two-Factor Authentication at a University. ACM DIGITAL LIBRARY: https://dl.acm.org/doi/abs/10.1145/3173574.3174030

Keunwoo Rhee, W. J. (2012, April). Security Requirements of a Mobile Device Management System. https://www.researchgate.net/profile/Dongho-Won-2/publication/267227402_Security_Requirements_of_a_Mobile_Device_Management_System/links/55ca889508aeca747d69ea6e/Security-Requirements-of-a-Mobile-Device-Management-System.pdf

Kun-Hsing Yu, A. L. (2018, October 10). Artificial intelligence in healthcare. nature biomedical engineering : https://www.nature.com/articles/s41551-018-0305-z

Khatkar, M., Kumar, K., & Kumar, B. (2020, February 21). An overview of distributed denial of service and internet of things in healthcare devices. Xplore: https://ieeexplore.ieee.org/abstract/document/9392171

LA WRENCE J TRAUTMAN, P. C. (χ.χ.). WANNACRY, RANSOMWARE, AND THE EMERGING THREAT TO CORPORATIONS . HEINONLINE: https://heinonline.org/HOL/LandingPage?handle=hein.journals/tenn86&div=16&id=&page=

Langlois, P. (2020). 2020 Data Breach. https://www.cisecurity.org/wp-content/uploads/2020/07/The-2020-Verizon-Data-Breach-Investigations-Report-DBIR.pdf

Lauren E Branch, W. S. (2019, Feb). Trends in Malware Attacks against United States Healthcare Organizations, 2016-2017. Global Biosecurity: https://jglobalbiosecurity.com/articles/10.31646/gbio.7

Lohani, S. (2019, Feb 6). Social Engineering: Hacking into Humans. SSRN: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3329391

Manghui Tu, K. S.-H. (2016, 26 July). Data Loss Prevention Management and Control: Inside Activity Incident Monitoring, Identification, and Tracking in Healthcare Enterprise Environments. The journal of digital forensics security and law: https://commons.erau.edu/jdfsl/vol10/iss1/3/

Maria Prokofieva, S. J. (2019, 07 15). Blockchain in healthcare. AUSTRALASIAN JOURNAL OF INFORMATION SYSTEMS: https://journal.acs.org.au/index.php/ajis/article/view/2203

Min Liang, C.-w. C. (2010, July 09-11). Research and design of full disk encryption based on virtual machine. IEEE XPLORE: https://ieeexplore.ieee.org/abstract/document/5565144

Ming Liu, Z. X. (2018, November 19). Host-Based Intrusion Detection System with System Calls: Review and Future Trends. ACM DIGITAL LIBRARY : https://dl.acm.org/doi/abs/10.1145/3214304

Mishra, U. (2010, August 25). An Introduction to Computer Viruses. SSRN: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=1916631

Noor Thamer, R. A. (2021, August 12). A Survey of Ransomware Attacks for Healthcare Systems: Risks, Challenges, Solutions and Opportunity of Research. IEEE Xplore : https://ieeexplore.ieee.org/abstract/document/9509877

Nureni Ayofe Azeez, T. M. (2019, October 25). Intrusion Detection and Prevention Systems: An Updated Review. SPRINGER LINK: https://link.springer.com/chapter/10.1007/978-981-32-9949-8_48

Patricia AH Williams, A. J. (2022, Dec 21). Cybersecurity vulnerabilities in medical devices: a complex environment and multifaceted problem. Taylor & Francis Online: https://www.tandfonline.com/doi/full/10.2147/MDER.S50048

Peng Zhang, D. C. (2018). Chapter One - Blockchain Technology Use Cases in Healthcare. ScienceDirect: https://www.sciencedirect.com/science/article/abs/pii/S0065245818300196

Ponemon. (2019). Cost of a Data Breach Report. https://www.ibm.com/downloads/cas/RDEQK07R

Qian Chen, R. A. (2017, December 18). Automated Behavioral Analysis of Malware: A Case Study of WannaCry Ransomware. IEEE Xplore: https://ieeexplore.ieee.org/abstract/document/8260673

Raja Waseem Anwar, T. A. (2021, October 02). Firewall Best Practices for Securing Smart Healthcare Environment: A Review. MDPI: https://www.mdpi.com/2076-3417/11/19/9183

Ramzan, Z. (2010). Phishing Attacks and Countermeasures. SPRINGER LINK: https://link.springer.com/chapter/10.1007/978-3-642-04117-4_23

Raul Luna, E. R. (2016). Cyber threats to health information systems: A systematic review. PubMed: https://pubmed.ncbi.nlm.nih.gov/26578272/

Salem T. Argaw, J. R.-P.-V.-M.-C. (2020, July 3). Cybersecurity of Hospitals: discussing the challenges and working towards mitigating the risks. SPRINGER LINK: https://link.springer.com/article/10.1186/s12911-020-01161-7

Sandhu, R. S. (1998). Role-based Access Control. ScienceDirect: https://www.sciencedirect.com/science/article/abs/pii/S0065245808602065

Savita Mohurle, M. P. (2017, May-June). A brief study of Wannacry Threat: Ransomware Attack 2017. https://sbgsmedia.in/2018/05/10/2261f190e292ad93d6887198d7050dec.pdf

Shou-Ching Hsiao, D.-Y. K. (2018, Feb 14). The static analysis of WannaCry ransomware. IEEE Xplore: https://ieeexplore.ieee.org/abstract/document/8323680

Slate, S. (2018, May 7). Endpoint Security: An Overview and a Look into the Future. https://www.cs.tufts.edu/comp/116/archive/spring2018/sslate.pdf

Sokratis Nifakos, K. C. (2021, June 29). Influence of Human Factors on Cyber Security within Healthcare Organisations: A Systematic Review. MDPI: https://www.mdpi.com/1424-8220/21/15/5119

Sören Preibusch, J. B. (2010). The Password Game: Negative Externalities from Weak Password Practices. SPRINGER LINK: https://link.springer.com/chapter/10.1007/978-3-642-17197-0_13

Taylor's University. (July, 2018 24). A REVIEW OF LATEST WANNACRY. Journal of Engineering Science and Technology: https://jestec.taylors.edu.my/Special%20Issue%20ICCSIT%202018/ICCSIT18_03.pdf

Tervonen, L. (2019, Dec 16). Efficient Distribution of Software Updates - A Case Study in Healthcare. Aalto University: https://aaltodoc.aalto.fi/handle/123456789/41688

Trinabh Gupta, H. F. (2017, August 07). Pretzel: Email encryption and provider-supplied functions are compatible. ACM DIGITAL LIBRARY: https://dl.acm.org/doi/abs/10.1145/3098822.3098835

Vasiliki Liagkou, V. K. (2019, May 5). Attack Detection for Healthcare Monitoring Systems Using Mechanical Learning in Virtual Private Networks over Optical Transport Layer Architecture. MDPI: https://www.mdpi.com/2079-3197/7/2/24

Vishnu, S., Ramson, S. J., & Jegan, R. (2020, April 23). Internet of Medical Things (IoMT) - An overview. IEEE Xplore: https://ieeexplore.ieee.org/abstract/document/9075733

Williams, P. A. (2022, Dec 21). Cybersecurity vulnerabilities in medical devices: a complex environment and multifaceted problem. Taylor & Francis Online : https://www.tandfonline.com/doi/full/10.2147/MDER.S50048

Yazan Al-Issa, M. A. (2019, Sept 03). eHealth Cloud Security Challenges: A Survey. Journal of Healthcare Engineering: https://www.hindawi.com/journals/jhe/2019/7516035/

Zafar, H. (2016). Cybersecurity: Role of Behavioral Training in. https://core.ac.uk/download/pdf/301368936.pdf

Zuoguang Wang, L. S. (2020, May 6). Defining Social Engineering in Cybersecurity. Xplore: https://ieeexplore.ieee.org/abstract/document/9087851