ΣΧΟΛΗ ΜΗΧΑΝΙΚΩΝ

ΤΜΗΜΑ ΜΗΧΑΝΙΚΩΝ ΠΛΗΡΟΦΟΡΙΚΗΣ
ΚΑΙ ΗΛΕΚΤΡΟΝΙΚΩΝ ΣΥΣΤΗΜΑΤΩΝ

ΔΙΠΛΩΜΑΤΙΚΗ ΕΡΓΑΣΙΑ

«Κυβερνοασφάλεια ιατρικών συσκευών: Μια έρευνα για τις ευπάθειες και τις επιθέσεις τους»

Του φοιτητή
Μούρτζιου Βασίλειου
Αρ. Μητρώου: 185237

Επιβλέπων
Αμανατιάδης Δημήτριος

Μάιος 2025

Τίτλος Δ.Ε. Κυβερνοασφάλεια ιατρικών συσκευών: Μια έρευνα για τις ευπάθειες και τις επιθέσεις τους

Κωδικός Δ.Ε. 24271

Ονοματεπώνυμο φοιτητή/τών Μούρτζιος Βασίλειος

Ονοματεπώνυμο εισηγητή Αμανατιάδης Δημήτριος

Ημερομηνία ανάληψης Δ.Ε. 23/10/2024

Ημερομηνία περάτωσης Δ.Ε. 20/05/2025

Βεβαιώνω ότι είμαι ο συγγραφέας αυτής της εργασίας και ότι κάθε βοήθεια την οποία είχα για την προετοιμασία της είναι πλήρως αναγνωρισμένη και αναφέρεται στην εργασία. Επίσης, έχω καταγράψει τις όποιες πηγές από τις οποίες έκανα χρήση δεδομένων, ιδεών, εικόνων και κειμένου, είτε αυτές αναφέρονται ακριβώς είτε παραφρασμένες. Επιπλέον, βεβαιώνω ότι αυτή η εργασία προετοιμάστηκε από εμένα προσωπικά, ειδικά ως διπλωματική εργασία, στο Τμήμα Μηχανικών Πληροφορικής και Ηλεκτρονικών Συστημάτων του ΔΙ.ΠΑ.Ε.

«Στην οικογένεια μου»

Πρόλογος

Ο λόγος που επέλεξα το συγκεκριμένο θέμα διπλωματικής εργασίας ήταν επειδή πέρα από τις σπουδές μου στο τμήμα Μηχανικών Πληροφορικής και Ηλεκτρονικών Συστημάτων, έχω αποφοιτήσει κι από το τμήμα Διασωστών του ΕΚΑΒ, οπότε γνωρίζω πόσο σημαντική είναι η υγεία ενός ασθενή και το σημαντικό ρόλο που παίζει το ιατρικό του ιστορικό στη λήψη αποφάσεων για την υγεία και τη ζωή του. Σκοπός μου με το παρόν θέμα διπλωματικής ήταν να συνδυάσω τις γνώσεις που έχω αποκομίσει από τη Σχολή Διασωστών κι από το τμήμα Μηχανικών Πληροφορικής και Ηλεκτρονικών Συστημάτων, προκειμένου να θίξω το θέμα της προστασίας της υγείας του ασθενούς, καθώς με την εξέλιξη της τεχνολογίας έχουν δημιουργηθεί ιατρικές συσκευές οι οποίες διευκολύνουν την παρακολούθηση και την αντιμετώπιση των προβλημάτων υγείας του ασθενούς, αλλά παράλληλα επικείμενες επιθέσεις από κακόβουλους χρήστες στις συσκευές αυτές, θέτουν σε κίνδυνο τα ευαίσθητα ιατρικά δεδομένα του ασθενούς αλλά και την υγεία του.

Περίληψη

Η τεχνολογική εξέλιξη των ιατρικών συσκευών στην πάροδο του χρόνου, έχει ως αποτέλεσμα τη βελτιστοποίηση της διάγνωσης και της θεραπείας της υγείας των ασθενών. Οι ιατροί έχουν πρόσβαση στα ιατρικά δεδομένα των ασθενών τους, που συλλέγονται από εμφυτεύσιμες και φορητές ιατρικές συσκευές, ακόμα κι απομακρυσμένα. Αυτή η εξέλιξη δημιούργησε νέους κινδύνους, όσον αφορά την κυβερνοασφάλεια των ιατρικών συσκευών. Άνθρωποι με κακόβουλες προθέσεις εκμεταλλεύονται ευπάθειες στην ασφάλεια των ιατρικών συσκευών, με αποτέλεσμα να υποκλέπτουν τα ευαίσθητα ιατρικά δεδομένα ασθενών για να ζητήσουν λύτρα, ή και ακόμα να βλάψουν άμεσα την υγεία των ασθενών. Το αντικείμενο αυτής της διπλωματικής είναι να αναλύσει αυτές τις ευπάθειες και τις επιθέσεις που δέχονται οι ιατρικές συσκευές. Επίσης οι κανονισμοί και τα πρότυπα κυβερνοασφάλειας που θα πρέπει να ακολουθούν οι ιατρικές συσκευές πριν κι αφού διατεθούν στην αγορά. Τέλος, προτείνονται τρόποι με τους οποίους μπορεί να ενισχυθεί η ασφάλεια των συσκευών, προκειμένου να περιοριστούν και να αντιμετωπιστούν οι ευπάθειες και οι επιθέσεις.

«Medical device cybersecurity: A survey of vulnerabilities and attacks»

«Mourtzios Vasileios»

Abstract

The technological evolution of medical devices over time has resulted in the optimization of the diagnosis and treatment of patients' health. Physicians have access to their patients' medical data collected by implantable and wearable medical devices, even remotely. This development has created new risks in terms of cybersecurity of medical devices. People with malicious intentions are exploiting vulnerabilities in the security of medical devices, resulting in the interception of patients' sensitive medical data to demand ransom, or even directly harm patients' health. The scope of this thesis is to analyze these vulnerabilities and attacks on medical devices. Also the regulations and cybersecurity standards that medical devices should follow before and after they are placed on the market. Finally, ways in which the security of the devices can be enhanced in order to limit and counter the vulnerabilities and attacks are suggested.

Ευχαριστίες

Θα ήθελα να ευχαριστήσω και να εκφράσω την ευγνωμοσύνη μου σε όλα εκείνα τα άτομα που συνέβαλλαν στην ολοκλήρωση της παρούσας διπλωματικής εργασίας. Πιο συγκεκριμένα, θέλω να ευχαριστήσω τον επιβλέποντα καθηγητή μου, κύριο Δημήτρη Αμανατιάδη, ο οποίος με την καθοδήγηση και τις συμβουλές του, με βοήθησε πραγματικά και με πολύτιμο τρόπο στην εκπόνηση της διπλωματικής μου εργασίας.

Επίσης, θα ήθελα να ευχαριστήσω την οικογένεια και τους φίλους μου, οι οποίοι πίστεψαν σε εμένα και με στήριξαν ο καθένας με το δικό του τρόπο, στηρίζοντας με ψυχολογικά και δίνοντάς μου κίνητρο και ώθηση, ώστε να εκπονήσω τη διπλωματική μου εργασία.

Περιεχόμενα

Κατάλογος Εικόνων

Κατάλογος Πινάκων

Συντομογραφίες

Δ.Ε.	Διπλωματική Εργασία
ΔΙΠΑΕ	Διεθνές Πανεπιστήμιο Ελλάδος
Π.Ε.	Πτυχιακή Εργασία
Π.Ο.Υ.	Παγκόσμιος Οργανισμός Υγείας
FDA	Food and Drug Administration
NIST	National Institute of Standards and Technology
MFA	Multi-Factor Authentication
CIA	Confidentiality Integrity Availability
DoS	Denial of Service
DDoS	Distributed Denial of Service
ARP	Address Resolution Protocol
LAN	Local Area Network
XSS	Cross-Site Scripting
BEC	Business Email Compromise
DNS	Domain Name System
IoT	Internet of Things
AES	Advanced Encryption Standard
SIEM	Security Information and Event Management
IDS	Intrusion Detection System
IPS	Intrusion Prevention System
ΕΕ	Ευρωπαϊκή Ένωση
ΗΠΑ	Ηνωμένες Πολιτείες Αμερικής
MDR	Medical Devices Regulation
MDD	Medical Devices Directive
AIMDD	Active Implantable Medical Devices Directive
GSPR	General Safety and Performance Requirements
MDCG	Medical Device Coordination Group
NIS2	Network and Information Systems Directive
CRA	Cyber Resilience Act
CSA	Cyber Solidarity Act

ECS	European Cyber Shield
SOC	Security Operation Center
CEM	Cyber Emergency Mechanism
GDPR	General Data Protection Regulation
EO	Executive Order
ISO	International Organization for Standardization
IEC	International Electrotechnical Commission
TIR57	Technical Information Report 57
AAMI	Association for the Advancement of Medical Instrumentation
UL	Underwriters Laboratories
NVD	National Vulnerability Database
ITU	International Telecommunications Union
ANSI	American National Standards Institute
DTS	Diabetes Technology Society
IEEE	Institute of Electrical and Electronics Engineers
SBOM	Software Bill of Materials
SPDF	Secure Product Development Framework

Κεφάλαιο 1ο: Εισαγωγή

1.1 Περιγραφή θέματος

Στην εποχή που βρισκόμαστε, η τεχνολογία έχει συμβάλλει δυναμικά στην ανάπτυξη κι εξέλιξη των ιατρικών συσκευών, σε βαθμό όπου πλέον μιλάμε για εμφυτεύσιμες και φορητές ιατρικές συσκευές. Με αυτήν την εξέλιξη, οι ιατρικές συσκευές είναι πλέον ικανές να αντιμετωπίζουν ευπάθειες της υγείας των ασθενών και οι επιστήμονες υγείας έχουν πλέον την ευκολία και τη δυνατότητα να παρακολουθούν την υγεία του ασθενή ακόμα κι απομακρυσμένα.

Με την πάροδο του χρόνου, όλο και περισσότερες τέτοιες ιατρικές συσκευές χρησιμοποιούνται για τη διευκόλυνση και των ασθενών αλλά και των ιατρών. Ένα τέτοιο τεχνολογικό επίτευγμα όμως δεν έρχεται χωρίς κινδύνους. Κακόβουλοι χρήστες εκμεταλλεύονται τα κενά, τις αδυναμίες και τις ελλείψεις στην κυβερνοασφάλεια αυτών των συσκευών διεξάγοντας μια πληθώρα διαφορετικών επιθέσεων. Σκοπός αυτών των επιθέσεων είναι η υποκλοπή ευαίσθητων ιατρικών δεδομένων των ασθενών, προκειμένου οι κακόβουλοι χρήστες να ζητήσουν λύτρα για αυτά ή και ακόμα να τα διαθέσουν σε εξωτερικούς τρίτους παράγοντες. Το πιο σημαντικό όμως είναι ότι βάζουν άμεσα σε κίνδυνο την υγεία του ασθενούς, καθώς πολλές από τις επιθέσεις έχουν ως στόχο τον έλεγχο λειτουργία της ιατρικής συσκευής.

Είναι απαραίτητο οι ιατρικές συσκευές να ακολουθούν συγκεκριμένα πρότυπα ασφαλείας προκειμένου να ενισχύσουν και να βελτιστοποιήσουν τα ενδεχόμενα κενά όπου μπορεί να έχουν στην κυβερνοασφάλειά τους. Ακόμη, είναι σωστή τακτική ο έλεγχος των συσκευών και η αξιολόγηση των κινδύνων τους, πριν και μετά τη διάθεσή τους στην αγορά.

1.2 Οργάνωση κεφαλαίων

Η παρούσα διπλωματική εργασία αποτελείται από εννέα κεφάλαια.

Στο πρώτο κεφάλαιο, γίνεται η περιγραφή του προβλήματος των επιθέσεων και των κενών κυβερνοασφάλειας που έχουν οι ιατρικές συσκευές. Παρουσιάζεται το περιεχόμενο των κεφαλαίων, καθώς και ο στόχος της διπλωματικής εργασίας.

Στο δεύτερο κεφάλαιο, γίνεται μια ιστορική αναφορά στην εξέλιξη των ιατρικών συσκευών, είδη και κατηγορίες ιατρικών συσκευών και παραδείγματα χρήσης τους.

Στο τρίτο κεφάλαιο, γίνεται αναφορά στους όρους ασφάλεια πληροφοριών και κυβερνοασφάλεια, τύπους κυβερνοασφάλειας, τύπους επιθέσεων και τρόπους πρακτικές κυβερνοασφάλειας.

Στο τέταρτο κεφάλαιο, γίνεται μια παρουσίαση στο πως τα διαφορετικά νομικά συστήματα, όπως της Ευρωπαϊκής Ένωσης και των Ηνωμένων Πολιτειών, ρυθμίζουν θέματα κυβερνοασφάλειας στις ιατρικές συσκευές. Ακόμη, γίνεται αναφορά σε ορισμένα πλαίσια που μπορούν να ακολουθούν οι ιατρικές συσκευές.

Στο πέμπτο κεφάλαιο, εξετάζονται τα διάφορα πρότυπα και οι τομείς εστίασης των προτύπων, τα οποία θα πρέπει να ακολουθούν οι ιατρικές συσκευές για την προστασία τους.

Στο έκτο κεφάλαιο, γίνεται εκτενής αναφορά στις ευπάθειες της ασφάλειας των ιατρικών συσκευών και τις κατηγορίες των ευπαθειών.

Στο έβδομο κεφάλαιο, παρουσιάζονται αναλυτικά οι τύποι των επιθέσεων που δέχονται οι ιατρικές συσκευές, πως η κάθε μία επίθεση μπορεί να επηρεάσει τη λειτουργία της συσκευής, καθώς και παραδείγματα επιθέσεων.

Στο όγδοο κεφάλαιο, αναφέρονται ενέργειες που θα πρέπει να ακολουθούνται για την κυβερνοασφάλεια των ιατρικών συσκευών, πριν αλλά και μετά τη διάθεση της συσκευής στην αγορά. Ακόμη, εξετάζονται τρόποι μετρίασης και αντιμετώπισης των επιθέσεων έναντι των ιατρικών συσκευών.

Στο ένατο κεφάλαιο, παρουσιάζονται τα συμπεράσματα και οι μελλοντικές έρευνες.

1.3 Στόχοι έρευνας

Στόχοι της διπλωματικής εργασίας είναι αρχικά η αναλυτική και ακριβής μελέτη και παρουσίαση τόσο των ευπαθειών των ιατρικών συσκευών, όσο και των τύπων επιθέσεων που δέχονται. Η μελέτη προτύπων και πλαισίων που πρέπει να τηρούνται για την κυβερνοασφάλεια είναι επίσης για τις ιατρικές συσκευές ένας στόχος. Ένας επιπλέον στόχος είναι η μελέτη και η παρουσίαση ενδεικτικών τρόπων και προτάσεων ενίσχυσης της κυβερνοασφάλειας των ιατρικών συσκευών και μετρίασης των επιθέσεων ως προς τις συσκευές.

1.4 Επίλογος

Στο πρώτο κεφάλαιο, έγινε αναφορά στο θέμα με το οποίο ασχολείται η παρούσα διπλωματική εργασία. Έπειτα, οργανώθηκε ανά ενότητες η θεματολογία της εργασίας, με αναφορά των περιεχομένων της κάθε ενότητας. Τέλος διασαφηνίστηκαν οι επιθυμητοί στόχοι της παρούσας έρευνας, για την ολοκλήρωση της συγγραφής της διπλωματικής εργασίας.

Κεφάλαιο 2ο: Ιατρικές Συσκευές

2.1 Εισαγωγή

Σε αυτό κεφάλαιο, γίνεται αναφορά στον όρο ιατρικές συσκευές και στην ιστορική εξέλιξη αυτών, καθώς και στην τεχνολογική εξέλιξη των ιατρικών συσκευών, με παραδείγματα από την ημέρα που χρησιμοποιήθηκαν για πρώτη φορά έως και σήμερα. Παρουσιάζονται αναλυτικά τα είδη και η κατηγοριοποίηση των ιατρικών συσκευών. Αναλύεται η αρχιτεκτονική επικοινωνίας των ιατρικών συσκευών, καθώς και τα πρότυπα και τα πρωτόκολλα επικοινωνίας, τα οποία χρησιμοποιούν οι ιατρικές συσκευές για την ανταλλαγή πληροφοριών.

2.2 Ερμηνεία και Ιστορική εξέλιξη

Σύμφωνα με τον Π.Ο.Υ. ιατρική συσκευή είναι: «*κάθε όργανο, συσκευή ή μηχάνημα που χρησιμοποιείται για την πρόληψη, τη διάγνωση ή τη θεραπεία νοσημάτων ή ασθενειών ή για την ανίχνευση, τη μέτρηση, την αποκατάσταση, τη διόρθωση ή την τροποποίηση της δομής ή της λειτουργίας του σώματος για κάποιο υγειονομικό σκοπό*» [1]. Χρησιμοποιούνται μόνες τους ή σε συνδυασμό, για έναν ή περισσότερους από τους παρακάτω ιατρικούς σκοπούς [2]:

- Διάγνωση, παρακολούθηση, θεραπεία, ανακούφιση από τραυματισμό
- Διάγνωση, πρόληψη, παρακολούθηση, θεραπεία ή ανακούφιση από ασθένειες
- Υποστήριξη ή διατήρηση της ζωής
- Διερεύνηση, αντικατάσταση, τροποποίηση ή υποστήριξη της ανατομίας ή μιας φυσιολογικής διαδικασίας
- Έλεγχος της σύλληψης
- Απολύμανση των ιατρικών συσκευών
- Παροχή πληροφοριών μέσω in vitro εξέτασης δειγμάτων, που προέρχονται από το ανθρώπινο σώμα

Μια ιατρική συσκευή μπορεί να βοηθηθεί για τον προβλεπόμενο σκοπό της πάνω στο ανθρώπινο σώμα από φαρμακολογικά, ανοσολογικά ή μεταβολικά μέσα. Αυτό όμως δε σημαίνει ότι τα μέσα αυτά είναι απαραίτητα για την επίτευξη της κύριας λειτουργίας της ιατρικής συσκευής. Με την πάροδο του χρόνου, οι ιατρικές συσκευές εξελίχθηκαν ραγδαία. Μια από τις πιο σημαντικές αλλαγές αφορά το μέγεθός τους το οποίο μειώθηκε αισθητά, κάτι το οποίο τις καθιστά πιο ελαφριές, αλλά πλέον και φορητές, ώστε να μπορούν να χρησιμοποιηθούν για συνεχή και άμεση φροντίδα. [2]

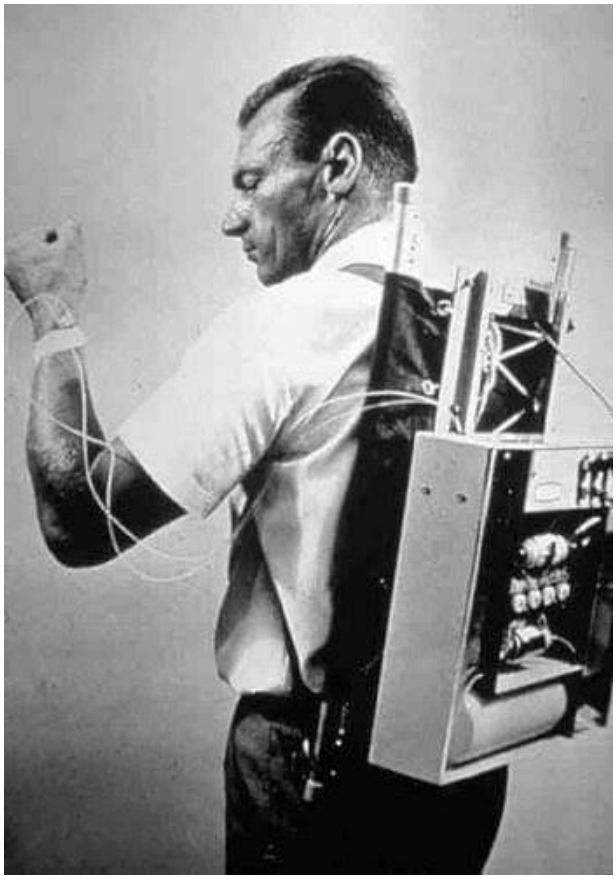
Οι συσκευές αυτές μπορούν πλέον να συνδέονται, τόσο μέσω ενσύρματων όσο και μέσω ασύρματων δικτύων, με άλλα συστήματα και συσκευές. Αυτές οι εξελίξεις ανοίγουν το δρόμο για πιο προσιτή υγειονομική περίθαλψη για όλους, προσφέροντας σημαντικές βελτιώσεις στα αποτελέσματα της υγείας των ασθενών. Η ευκολία της διάγνωσης, της θεραπείας και της παρακολούθησης της υγείας που επιτυγχάνεται μέσω των συνδέσεων αυτών, σε συνδυασμό με τη μείωση του κόστους, αποτελεί ένα σημαντικό βήμα προόδου του τομέα υγείας. [3][4] Παρακάτω ο αναγνώστης μπορεί να δει μια ιστορική αναδρομή σε δύο σημαντικές ιατρικές συσκευές που επηρέασαν τον κόσμο, έτσι ώστε να γίνεται πιο κατανοητή η σημαντικότητα που έχει η εξέλιξή τους στο πέρασμα του χρόνου, στους τομείς που αναφέρθηκαν παραπάνω.

2.2.1 Ιστορική και τεχνολογική εξέλιξη αντλίας ινσουλίνης

Η διάγνωση ενός ανθρώπου με διαβήτη πριν από τη δεκαετία του 1920, αυτόματα σήμαινε μικρότερο προσδόκιμο ζωής και σε ορισμένες περιπτώσεις ακόμα και το θάνατο. Πολλοί ασθενείς έρχονταν αντιμέτωποι με επιπλοκές της ασθένειας. Ο μόνος τρόπος αντιμετώπισης της ασθένειας εκείνη την περίοδο ήταν μια διατροφή χαμηλή σε υδατάνθρακες και σάκχαρα και υψηλή σε πρωτεΐνη και λίπος. Η θεραπεία για το διαβήτη ανακαλύφθηκε το καλοκαίρι του 1921 στο πανεπιστήμιο του Τορόντο, από τους Frederick Banting και Charles Best, οι οποίοι απομόνωσαν επιτυχώς την ινσουλίνη από σκύλους που χρησιμοποιούσαν ως πειραματόζωα, προκαλώντας με αυτόν τον τρόπο συμπτώματα διαβήτη στα ζώα αυτά και στη συνέχεια ξεκίνησαν ένα πρόγραμμα ενέσεων ινσουλίνης, το οποίο επανάφερε τα σκυλιά στην προηγούμενη φυσική τους κατάσταση. Η ανακάλυψη αυτή ανακοινώθηκε επίσημα στον υπόλοιπο κόσμο στις 14 Νοεμβρίου του 1921. [5][6]

Ο πρώτος άνθρωπος που έλαβε ένεση ινσουλίνης ήταν ο Leonard Thompson τον Ιανουάριο του 1922, σε ηλικία μόλις δεκατεσσάρων ετών. Η πρώτη δόση που έλαβε, περιείχε μια ακαθαρσία, η οποία του προκάλεσε αλλεργική αντίδραση. Αναπτύχθηκε όμως ταχύτατα μια νέα διαδικασία για την εξαγωγή ινσουλίνης σε καθαρότερη μορφή, αυτή τη φορά από αγελάδες. Η δεύτερη δόση του χορηγήθηκε επιτυχώς στο τέλος του ίδιου μήνα.[5][6]

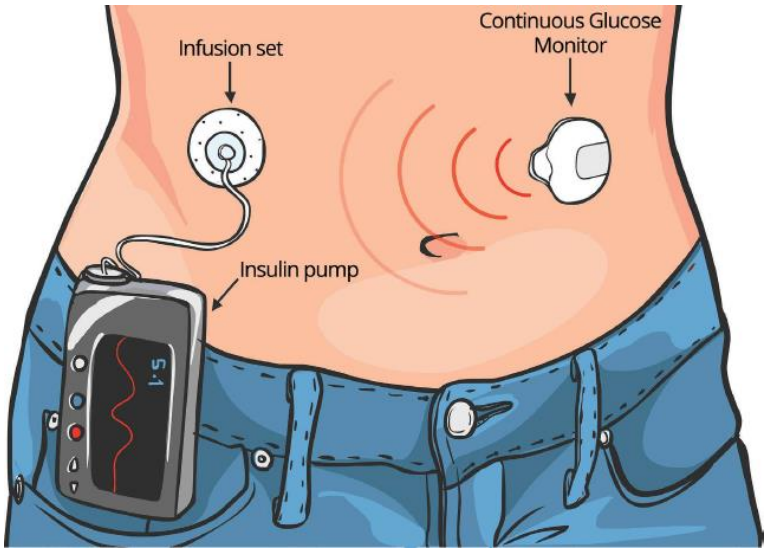
Τη δεκαετία του 1960 εμφανίστηκαν οι πρώτες αντλίες ινσουλίνης. Ωστόσο, το μέγεθος τους αποτελούσε πρόβλημα, καθώς ήταν όσο μεγάλες όσο μια τσάντα πλάτης, κάτι το οποίο δυσκόλευε τη μετακίνηση των ασθενών που τις χρησιμοποιούσαν. [6]



Εικόνα 1 Αντλία ινσουλίνης του 1960

Για πολλά χρόνια χρησιμοποιήθηκε η ινσουλίνη που εξαγόταν από βοοειδή και χοίρους, η οποία ενώ έσωζε εκατομμύρια ζωές, προκαλούσε παράλληλα αλλεργικές αντιδράσεις σε αρκετούς ασθενείς, καθώς δεν ήταν η τέλεια μορφή ινσουλίνης. Η πρώτη συνθετική ινσουλίνη, που ανταποκρινόταν με αυτή που παράγει ο ανθρώπινος οργανισμός, παρήχθη το 1978 χρησιμοποιώντας το βακτήριο Εσερίχια κόλι (E. Coli). [7]

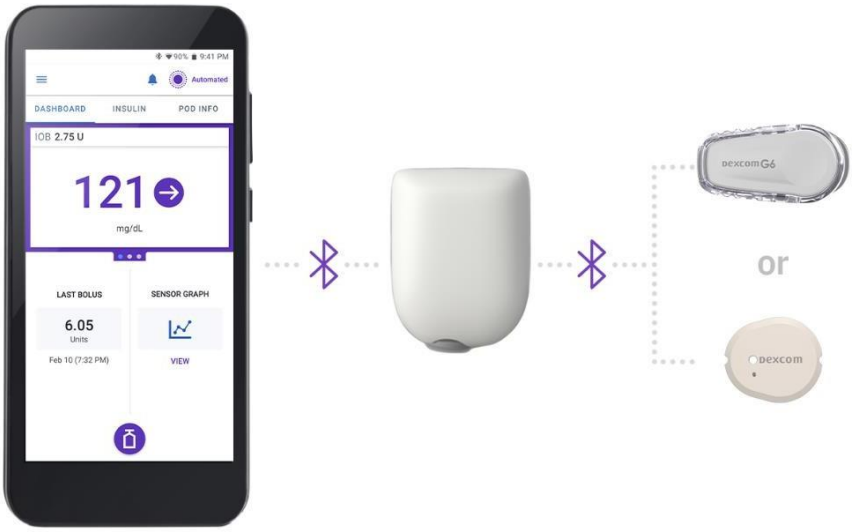
Με την εξέλιξη της τεχνολογίας στην πάροδο των δεκαετιών, άρχισε να μειώνεται και το μέγεθος των αντλιών. Στις 5 Ιουλίου του 1980, έγινε η πρώτη εμφύτευση αντλίας ινσουλίνης στον άνθρωπο. Τα σημερινά νέα συστήματα χορήγησης ινσουλίνης διαθέτουν λογισμικό και δυνατότητες παρακολούθησης και διαχείρισης του επιπέδου της γλυκόζης του ασθενή, διευκολύνοντας έτσι τον ασθενή να διαχειρίζεται και να παρακολουθεί πιο αποτελεσματικά τα επίπεδα σακχάρου στον οργανισμό του. Επίσης, οι ασθενείς έχουν πλέον τη δυνατότητα να μπορούν να διαχειρίζονται τη συσκευή τους, έτσι ώστε να μπορούν να την ελέγχουν για τυχόν δυσλειτουργίες. Αυτή η δυνατότητα είναι εφικτή μέσω ενός μικρού συστήματος που βρίσκεται στη ζώνη του ασθενούς και λειτουργεί με την τεχνολογία Bluetooth 4.0.



Εικόνα 2 Αντλία ινσουλίνης με λειτουργία Bluetooth 4.0

Τον Ιούλιο του 2012, ο Οργανισμός Τροφίμων και Φαρμάκων των Ηνωμένων Πολιτειών (FDA) ενέκρινε τη χρήση αντλιών ινσουλίνης, οι οποίες χρησιμοποιούν τεχνολογία Bluetooth 4.0, κάνοντας έτσι επιτρεπτή την αμφίδρομη ανταλλαγή πληροφοριών για τον ασθενή. Οι αντλίες αυτές λειτουργούν ως εξής: Παρακολουθούν τα επίπεδα γλυκόζης στο αίμα του ασθενούς, το σύστημα ενημερώνει την αντλία σε περίπτωση ανάγκης για χορήγηση, η αντλία ετοιμάζει την ακριβή δόση που χρειάζεται ο ασθενής και τη χορηγεί αυτόματα στον οργανισμό του ασθενή. [7]

Το 2022, μια νέα τεχνολογία εγκρίθηκε από τον Οργανισμό Τροφίμων και Φαρμάκων των Ηνωμένων Πολιτειών. Το προϊόν με την ονομασία Omnipod 5 είναι ένα υβριδικό σύστημα κλειστού βρόγχου χορήγησης ινσουλίνης το οποίο σημαίνει ότι η αντλία ινσουλίνης επικοινωνεί απευθείας με τη συσκευή/αισθητήρα παρακολούθησης γλυκόζης του ασθενή. Για να καθορίσει την ποσότητα ινσουλίνης που πρέπει να χορηγήσει με ασφαλή τρόπο, λειτουργεί έτσι σχεδόν ως ένα τεχνητό πάγκρεας.

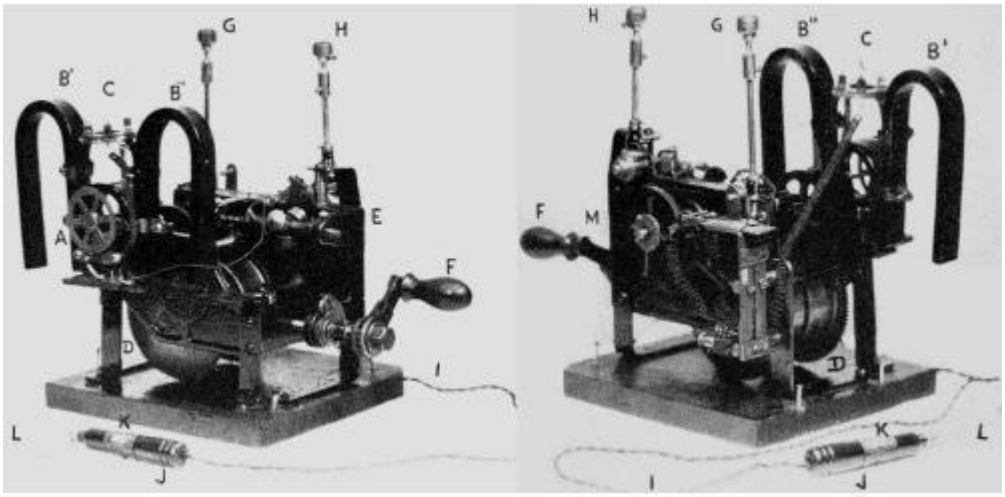


Εικόνα 3 Το σύστημα Omnipod 5

Το Omnipod 5 είναι το πρώτο σύστημα στην αγορά χωρίς σωληνάκια και το οποίο ελέγχεται πλήρως μέσω εφαρμογής στο κινητό του ασθενή, καταργώντας έτσι την ανάγκη μεταφοράς μιας ολόκληρης ξεχωριστής συσκευής. Είναι μικρό και φοριέται κατευθείαν στο δέρμα του ασθενή. Ο ασθενής γεμίζει χειροκίνητα την κάψουλα με ινσουλίνη, την κολλάει στο δέρμα του και την αντικαθιστά ανά 3 ημέρες με εύκολο τρόπο. [8]

2.2.2 Ιστορική και τεχνολογική εξέλιξη βηματοδότη

Η αρρυθμία είναι η διαταραχή του φυσιολογικού ρυθμού της καρδιάς, δηλαδή της ηλεκτρικής δραστηριότητας που ελέγχει τους χτύπους της καρδιάς. Μπορεί να οδηγήσει σε σοβαρές επιπλοκές, όπως υποξία και εγκεφαλικό επεισόδιο, αλλά ακόμη και τον αιφνίδιο καρδιακό θάνατο. Το 1932, ο Albert Hyman άρχισε να εστιάζει στην αναζωογόνηση της «σταματημένης καρδιάς» μέσω μιας μεθόδου που ονόμασε ενδοκαρδιακή θεραπεία. Η θεραπεία αρχικά βασιζόταν στην ενδοκαρδιακή έγχυση διεγερτικών φαρμάκων όπως η επινεφρίνη. Σύντομα διαπιστώθηκε ότι η επανεκκίνηση της καρδιάς δεν οφειλόταν στη χρήση του φαρμάκου, αλλά στη βελόνα η οποία προκαλούσε ένα ρεύμα δράσης τραυματισμού καθώς διαπερνούσε το καρδιακό τοίχωμα. Ο Albert Hyman το 1932 εφηύρε τον πρώτο τεχνητό βηματοδότη. Η συσκευή τροφοδοτούνταν από ένα χειροκίνητο στρόφαλο με ελατήριο. Παρά τη δημιουργία της δεν ήταν όμως αποδεκτή ως μέσο επανεκκίνησης μιας σταματημένης καρδιάς. Ο Hyman δεν αναγνώρισε το γεγονός πως η εφεύρεσή του θα μπορούσε να χρησιμοποιηθεί για άτομα με καρδιακή ανακοπή. [7]



Εικόνα 4 Ο πρώτος τεχνητός βηματοδότης

Το 1949 στο Τορόντο του Καναδά, οι Wifred Bigelow και John Callaghan άρχισαν να χρησιμοποιούν την υποθερμία για να μειώσουν το μεταβολισμό προκαλώντας έτσι βραδυκαρδία και ασυστολία, με στόχο να καταστεί δυνατή η καρδιοχειρουργική επέμβαση. Ωστόσο, η επαναθέρμανση δεν επανέφερε αρκετά γρήγορα την καρδιακή συστολή, οδηγώντας έτσι τους χειρούργους να αρχίσουν να πειραματίζονται με τη διέγερση του φλεβοκομβικού κόμβου. Το 1949 κατά τη διάρκεια μιας πειραματικής επέμβασης σε έναν σκύλο, η καρδιά του σταμάτησε ξαφνικά. Εκεί, ο Wilfred Bigelow, σε κατάσταση απελπισίας, έδωσε στην αριστερή κοιλία της καρδιάς ένα δυνατό χτύπημα με έναν καθετήρα που κρατούσε. Συνέπεια αυτού του χτυπήματος, ήταν να ανταποκριθούν και οι τέσσερις θάλαμοι της καρδιάς. Με περαιτέρω χτυπήματα, η καρδιά άρχισε να χτυπά κανονικά και με καλή αρτηριακή πίεση. Ως άμεσο αποτέλεσμα των πειραμάτων υποθερμίας, δημιουργήθηκε ο ηλεκτρικός βηματοδότης. [9][10]

Το 1951, ο Paul Zoll καρδιολόγος από τη Βοστώνη, ανέπτυξε έναν εξωτερικό επιτραπέζιο βηματοδότη ο οποίος χρησιμοποιήθηκε με επιτυχία για τη θεραπεία του καρδιακού αποκλεισμού. Η εφεύρεσή του θεωρείται ότι εγκαινίασε τη σύγχρονη εποχή της κλινικής καρδιακής βηματοδότησης. Η συσκευή παρέδιδε ηλεκτρικούς παλμούς, μέσω ενός ζεύγους μεταλλικών ηλεκτροδίων τα οποία ήταν δεμένα στο στήθος του ασθενούς, ακριβώς πάνω από την καρδιά του. Οι αρνητικές επιπτώσεις ήταν ότι τα ηλεκτρόδια προκαλούσαν ερεθισμό του δέρματος του ασθενούς και τα επαναλαμβανόμενα ηλεκτροσόκ ήταν επώδυνα για τους ασθενείς. Η συσκευή ήταν ογκώδης και βαριά, μεταφερόταν σε καρότσι και μπορούσε να φτάσει μέχρι όσο επέτρεπε το καλώδιο προέκτασης.[9][10]

Εικόνα 5 Ο Paul Zoll με τον επιτραπέζιο βηματοδότη

Το 1958, ο μηχανικός Earl Bakken από τη Μινεσότα, κατασκεύασε τον πρώτο φορητό εξωτερικό βηματοδότη. Ο βηματοδότης ήταν υλοποιημένος με τρανζίστορ, στεγαζόταν σε ένα μικρό πλαστικό κουτί και διέθετε χειριστήρια για τη ρύθμιση του καρδιακού ρυθμού και της τάσης εξόδου. Συνδεόταν με καλώδια που περνούσαν μέσα από το δέρμα του ασθενούς και κατέληγαν σε ηλεκτρόδια, τα οποία ήταν προσαρτημένα στην επιφάνεια του μυοκαρδίου της καρδιάς. [9]

Τη δεκαετία του 1960 στο Ηνωμένο Βασίλειο, ζητήθηκε από την Lucas Engineering για λογαριασμό του νοσοκομείου Queen Elizabeth, να αναπτύξει ένα πρωτότυπο τρανζίστορ που θα αντικαθιστούσε τα ηλεκτρομηχανικά προϊόντα. Ο Roger Nolan ήταν ο μηχανικός κι επικεφαλής της ομάδας, που σχεδίασε και δημιούργησε τον πρώτο ταλαντωτή μπλοκαρίσματος και ένα βηματοδότη με τρανζίστορ. Ο βηματοδότης αυτός φοριόταν σε μια ζώνη και τροφοδοτούνταν από μια επαναφορτιζόμενη σφραγισμένη μπαταρία, δίνοντας τη δυνατότητα στους ασθενείς να ζουν μια πιο φυσιολογική ζωή. Ένας από τους πρώτους ασθενείς που έλαβαν το συγκεκριμένο βηματοδότη, σε επέμβαση που πραγματοποιήθηκε το 1964, ήταν μια γυναίκα στην ηλικία των τριάντα.[10]

Ο πρώτος εμφυτεύσιμος βηματοδότης σχεδιάστηκε από τον εφευρέτη Rune Elmqvist και τον χειρουργό Ake Senning, συνδέθηκε με ηλεκτρόδια που τοποθετήθηκαν στο μυοκάρδιο μέσω τομής του θώρακος. Οι δύο αυτοί επιστήμονες συνειδητοποίησαν ότι το βασικό πρόβλημα με τους εξωτερικούς βηματοδότες, ήταν ο αυξημένος κίνδυνος μόλυνσης μέσω του ανοιχτού καναλιού που δημιουργούσε το καλώδιο, κάτι το οποίο αποτέλεσε καταλύτης για το σχεδιασμό ενός πλήρως εμφυτεύσιμου συστήματος. [9][10]

Η πρώτη τοποθέτηση ενός εμφυτεύσιμου βηματοδότη, πραγματοποιήθηκε τον Οκτώβριο του 1958, στο Ινστιτούτο Karolinska της Σουηδίας. Ο ασθενής Arne Larsson υπέφερε από συχνές κρίσεις Stokes-Adams, οι οποίες απαιτούσαν καθημερινή αναζωογόνηση πολλές φορές. Η κατάστασή του θεωρούνταν απελπιστική και η εμφύτευση του βηματοδότη χρησιμοποιήθηκε ως τελευταία λύση για την παροχή βοήθειας στην υγεία του ασθενούς. Η πρώτη συσκευή που εμφυτεύθηκε απέτυχε μετά από τρεις ώρες, ενώ η δεύτερη συσκευή η οποία εμφυτεύθηκε αμέσως μετά, διήρκησε δύο ημέρες. Ο Arne έλαβε

συνολικά στη ζωή του εικοσιέξι διαφορετικούς βηματοδότες και έζησε μέχρι τα ογδονταέξι του, ξεπερνώντας σε ζωή και τους δύο επιστήμονες που δημιούργησαν τον εμφυτεύσιμο βηματοδότη. [9][10]

Τα επόμενα χρόνια, οι βηματοδότες εξελίχθηκαν με την εξέλιξη της τεχνολογίας των μπαταριών. Η επόμενη σημαντική εξέλιξη των εμφυτεύσιμων βηματοδοτών ήταν η ασύρματη σύνδεση. Το 2009, δοκιμάστηκαν οι πρώτοι βηματοδότες, οι οποίοι ενσωμάτωναν τεχνολογία Wi-Fi στο σχεδιασμό τους. Το σημαντικότερο πλεονέκτημα τους είναι η δυνατότητα απομακρυσμένης παρακολούθησης της συσκευής. Επιτρέπεται έτσι η ρύθμιση και η αποστολή ειδοποιήσεων τόσο στους ασθενείς όσο και στους ιατρούς. Σε περίπτωση δυσλειτουργίας, γίνεται αποστολή δεδομένων στους ιατρούς για την παρακολούθηση της κατάστασης του ασθενούς. Η πρόοδος της τεχνολογίας οδήγησε στην ανάπτυξη ασύρματων βηματοδοτών χωρίς ηλεκτρόδια. Πλεονεκτήματά τους είναι:

- Το μικρό τους μέγεθος
- Το χαμηλό βάρος τους
- Η απουσία μηχανισμών σύνδεσης μεταξύ της γεννήτριας και των ηλεκτροδίων, διότι συνυπάρχουν σε μια ενιαία μονάδα
- Η αντικατάσταση της εγχείρησης με τη διαδικασία της διακαθετηριακής εμφύτευσης
- Χαμηλότερος κίνδυνος λοιμώξεων, όπως ενδοκαρδίτιδα ή φλεβική απόφραξη

Η διάρκεια της μπαταρίας τους είναι επτά με δέκα χρόνια. Πρωτοπόρες εταιρείες στην κατασκευή τέτοιων βηματοδοτών είναι η Micra και η Nanostim. [7][11][12]

Εικόνα 6 Σύγκριση ενός κλασσικού εμφυτεύσιμου βηματοδότη κι ενός βηματοδότη της Micra

2.3 Κατηγορίες ιατρικών συσκευών

Οι ιατρικές συσκευές διακρίνονται στις παρακάτω κατηγορίες [13]:

- Σταθερές
- Φορητές
- Εξωτερικές
- Εμφυτεύσιμες

2.3.1 Σταθερές ιατρικές συσκευές

Οι σταθερές ιατρικές συσκευές είναι αυτές οι οποίες βρίσκονται σταθερά εγκατεστημένες σε ένα χώρο, όπως αυτός ενός νοσοκομείου ή μιας κλινικής και χρησιμοποιούνται για διαγνωστικούς, υποστηρικτικούς ή θεραπευτικούς σκοπούς. Είναι συνήθως μεγάλης κλίμακας κι απαιτούν εξειδικευμένη εγκατάσταση. Μερικές από τις συσκευές που ανήκουν σε αυτή την κατηγορία είναι οι εξής [15]:

- Μαγνητικός τομογράφος (MRI): Είναι μια συσκευή απεικόνισης που χρησιμοποιεί μαγνητικά πεδία και ραδιοκύματα για τη δημιουργία λεπτομερών εικόνων του εσωτερικού του σώματος. Χρησιμοποιείται για τη διάγνωση και την παρακολούθηση παθήσεων που αφορούν τη σπονδυλική στήλη, τις αρθρώσεις, τον εγκέφαλο και τα διάφορα εσωτερικά όργανα και ιστούς.
- Αξονικός τομογράφος (CT): Είναι μια συσκευή που χρησιμοποιεί ακτίνες Χ σε συνεργασία με ένα πολύ εξελιγμένο υπολογιστικό σύστημα, για να δημιουργήσει τρισδιάστατες εικόνες του ανθρώπινου σώματος. Παρέχει πληροφορίες για τη διάγνωση παθήσεων, οι οποίες επηρεάζουν αγγεία, οστά, εσωτερικά όργανα και μαλακούς ιστούς.
- Σύστημα ακτινοθεραπείας: Είναι συσκευή που χρησιμοποιείται για τη θεραπεία του καρκίνου και διαφόρων άλλων παθήσεων, μέσω ελεγχόμενης χορήγησης ιονίζουσας ακτινοβολίας. Στόχος της είναι η συρρίκνωση ή καταστροφή καρκινικών κυττάρων, διατηρώντας παράλληλα την υγεία των γειτονικών φυσιολογικών ιστών.
- Συσκευή διαγνωστικής υπερηχογραφίας: Είναι μια συσκευή που χρησιμοποιεί υπερήχους για την απεικόνιση των εσωτερικών δομών του σώματος. Είναι ασφαλής και διαδεδομένη στον ιατρικό κλάδο για τη διάγνωση, την καθοδήγηση επεμβάσεων και την παρακολούθηση ασθενειών.

2.3.2 Φορητές ιατρικές συσκευές

Οι φορητές συσκευές είναι ειδικά σχεδιασμένες για να μεταφέρονται εύκολα και να φοριούνται, σε αντίθεση με τις εξωτερικές συσκευές οι οποίες τοποθετούνται ή εφαρμόζονται στο εξωτερικό του σώματος, χωρίς αυτές να είναι απαραίτητα φορητές. Εξοπλισμένες με αισθητήρες, οι φορητές συσκευές παρακολουθούν την κατάσταση της υγείας και τις επιλογές του τρόπου ζωής του ασθενούς, βελτιώνοντας παράλληλα την αυτοπαρακολούθηση και δίνοντας έτσι την ευκολία να έχουν οι ασθενείς πρόσβαση σε πληροφορίες για την υγεία τους, χωρίς να χρειάζεται απαραίτητα η επίσκεψη στον ιατρό.[13] Μερικά παραδείγματα αποτελούν οι ακόλουθες συσκευές [15]:

- Smartwatch: Τα smartwatches πλέον διαθέτουν ένα πλήθος αισθητήρων για τη μέτρηση πολλών ζωτικών λειτουργιών όπως η παρακολούθηση του καρδιακού ρυθμού, ανιχνεύοντας έτσι τυχόν ταχυκαρδίες ή βραδυκαρδίες, η μέτρηση του κορεσμού του οξυγόνου στο αίμα, η οποία είναι χρήσιμη για άτομα με αναπνευστικά προβλήματα, και η παρακολούθηση του ύπνου, καταγράφοντας έτσι διαταραχές που μπορεί να συμβούν κατά τη διάρκεια του ύπνου, όπως αϋπνία ή άπνοια.
- Ανιχνευτής δραστηριότητας εγκεφάλου: Μετρά την εγκεφαλική δραστηριότητα και χρησιμοποιείται για τη νευρολογική παρακολούθηση και τη διαχείριση του άγχους.
- Αισθητήρες πτώσης και εντοπισμού: Είναι συσκευές που φοριούνται στο λαιμό ή στον καρπό του ασθενούς και ανιχνεύουν περιπτώσεις πτώσεις του ασθενούς, έτσι ώστε να σταλεί ειδοποίηση στο φροντιστή ή την κλινική που νοσηλεύεται ο ασθενής.
- Φορητά συστήματα παρακολούθησης εγκυμοσύνης: Αισθητήρες οι οποίοι φοριούνται στη μέση της εγκύου για την παρακολούθηση του καρδιακού ρυθμού του εμβρύου και των συσπάσεων.

Οι φορητές ιατρικές συσκευές και οι εξωτερικές ιατρικές συσκευές δεν είναι απόλυτα ταυτόσημες.

2.3.3 Εξωτερικές ιατρικές συσκευές

Οι εξωτερικές ιατρικές συσκευές εφαρμόζονται στο εξωτερικό του σώματος και χρησιμοποιούνται είτε για διαγνωστικούς, είτε για θεραπευτικούς, είτε για υποστηρικτικούς σκοπούς. Μερικές συσκευές αυτής της κατηγορίας είναι οι ακόλουθες [15]:

- Συσκευή μέτρησης αρτηριακής πίεσης: Ανήκει στην κατηγορία διαγνωστικού σκοπού. Είναι ψηφιακό πιεσόμετρο που χρησιμοποιείται για τη μέτρηση της αρτηριακής πίεσης.
- Οξύμετρο: Ανήκει στην κατηγορία διαγνωστικού σκοπού. Είναι συσκευή που μετρά τον κορεσμό του οξυγόνου στο αίμα και τους καρδιακούς παλμούς.
- Συσκευή συνεχούς θετικής πίεσης αεραγωγών (CPAP): Ανήκει στην κατηγορία θεραπευτικού σκοπού. Παρέχει συνεχή ροή αέρα υπό θετική πίεση μέσω μιας μάσκας, η οποία τοποθετείται στη μύτη ή στο στόμα. Χρησιμοποιείται για διαταραχές της αναπνοής, καθώς και για τη θεραπεία της αποφρακτικής υπνικής άπνοιας.
- Αυτόματος εξωτερικός απινιδωτής (AED): Ανήκει στην κατηγορία θεραπευτικού σκοπού. Αποτελεί συσκευή επείγουσας ιατρικής, καθώς παρέχει ηλεκτροσόκ για την αποκατάσταση της καρδιακής λειτουργίας σε περίπτωση καρδιακής ανακοπής.

2.3.4 Εμφυτεύσιμες ιατρικές συσκευές

Ως εμφυτεύσιμη χαρακτηρίζεται μια ιατρική συσκευή η οποία μόνιμα ή ημιμόνιμα εμφυτεύεται σε έναν ασθενή, με σκοπό τη βελτίωση της λειτουργίας κάποιου μέρους του σώματός του ή τη θεραπεία μιας πάθησης. Μια τέτοια συσκευή εμφυτεύεται με εγχείρηση και συνδέεται με το όργανο που χρειάζεται τη θεραπεία ή την παρακολούθηση. Παραδείγματα τέτοιων ιατρικών συσκευών αποτελούν τα παρακάτω [13][14]:

- Καρδιακές εμφυτευμένες συσκευές: Περιλαμβάνουν συσκευές όπως ο εμφυτεύσιμος απινιδωτής και ο βηματοδότης. Οι συσκευές αυτές σχεδιάστηκαν για τη θεραπεία καρδιακών παθήσεων, παρακολουθώντας τη δραστηριότητα των ηλεκτρικών παλμών της καρδιάς και εφαρμόζοντας ηλεκτρικούς παλμούς στην κατάλληλη ένταση, έτσι ώστε να διατηρήσουν τον καρδιακό ρυθμό σε επιθυμητά επίπεδα. Μερικά πρόσφατα μοντέλα διαθέτουν και αισθητήρες πίεσης, οι οποίοι παρακολουθούν ενεργά τις αλλαγές που ενδέχεται να οδηγήσουν σε καρδιακή ανεπάρκεια, ειδοποιώντας έτσι τον ασθενή ή τον ιατρό σε περίπτωση αύξησης της πίεσης στην κοιλία, κάτι το οποίο αποτελεί ένδειξη κινδύνου. Μπορούν επίσης να εξοπλιστούν και με επιταχυνσιόμετρα για τη μέτρηση του επιπέδου σωματικής δραστηριότητας του ασθενούς, πληροφορία που μπορεί να χρησιμοποιηθεί ως παράμετρος στον ελεγκτή της συσκευής έτσι ώστε να προσαρμοστεί κατάλληλα η συχνότητα της καρδιακής διέγερσης για να ανταποκρίνεται σε πραγματικό χρόνο στις ανάγκες του ασθενούς.
- Νευροδιεγέρτες: Οι συσκευές αυτές μεταδίδουν ηλεκτρικά σήματα χαμηλού πλάτους, μέσω ηλεκτροδίων, τα οποία τοποθετούνται σε διαφορετικές περιοχές του εγκεφάλου, ανάλογα με την πάθηση του ασθενούς. Τα ηλεκτρόδια εμφυτεύονται με ακρίβεια στα συγκεκριμένα σημεία, μέσω μιας διαδικασίας που είναι γνωστή ως Βαθιά Εγκεφαλική Διέγερση (Deep Brain Stimulation – DBS). Η διαδικασία αυτή χρησιμοποιείται για τη θεραπεία διαφόρων παθήσεων, όπως το Πάρκινσον, η επιληψία και σε ορισμένες περιπτώσεις και η κατάθλιψη.
- Συστήματα Χορήγησης Φαρμάκων (Drug Delivery System – DDS): Ένα σύστημα χορήγησης φαρμάκων αποτελείται από μια αντλία κι έναν καθετήρα, οι οποίοι εμφυτεύονται χειρουργικά κάτω από το δέρμα. Η κύρια λειτουργία του συστήματος είναι η ελεγχόμενη, εντοπισμένη και παρατεταμένη χορήγηση φαρμάκων. Το φάρμακο διοχετεύεται κατευθείαν στην περιοχή-στόχο κι έτσι το σύστημα επιτρέπει τη χρήση χαμηλότερων δόσεων σε σύγκριση με τη χορήγηση από το στόμα, μειώνοντας έτσι τυχόν παρενέργειες. Τέτοιες εμφυτεύσιμες συσκευές αποτελούν οι αντλίες ινσουλίνης, οι αντλίες χημειοθεραπείας, οι αντλίες χορήγησης φαρμάκων κι εμφυτεύσιμα συστήματα διαχείρισης καρδιαγγειακών παθήσεων. Οι αντλίες χημειοθεραπείας χορηγούν τοπικά αντικαρκινικά φάρμακα. Οι αντλίες χορήγησης φαρμάκων παρέχουν αναλγητικά κι άλλα φάρμακα απευθείας στο εγκεφαλονωτιαίο υγρό, για την ανακούφιση του

χρόνιου πόνου. Τα εμφυτεύσιμα συστήματα διαχείρισης καρδιαγγειακών παθήσεων χορηγούν θρομβολυτικά ή φάρμακα για τη διαχείριση των στεφανιαίων νόσων.

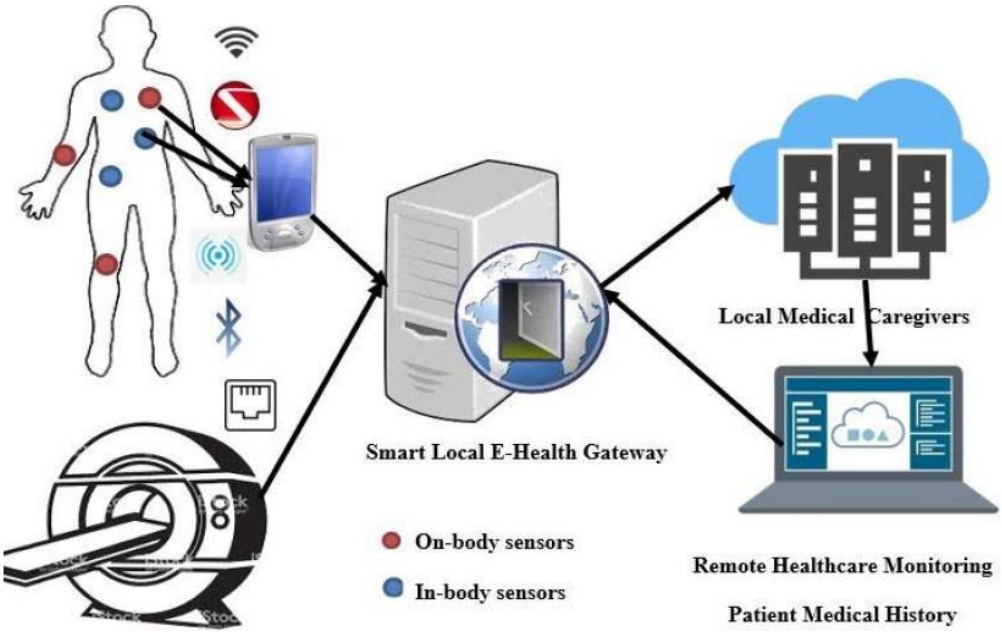
- Βιοαισθητήρες: Τέτοιου τύπου εμφυτεύματα περιλαμβάνουν έναν ή περισσότερους αισθητήρες που τοποθετούνται μέσα στο ανθρώπινο σώμα, με στόχο την παρακολούθηση συγκεκριμένων λειτουργιών ή τμημάτων του οργανισμού. Οι αισθητήρες μετρούν διάφορες φυσιολογικές παραμέτρους και βάσει αυτών των δεδομένων, κρίνεται η λήψη αποφάσεων σχετικά με την υγεία του ασθενούς. Ένα τέτοιο σύστημα περιλαμβάνει και μια συσκευή που λειτουργεί ως κόμβος ελέγχου. Ο κόμβος αυτός επικοινωνεί με τους αισθητήρες, αλλά ακόμα και με εξωτερικές συσκευές, όπως ένας υπολογιστής ή μια άλλη ιατρική συσκευή. Ο συνδυασμός των αισθητήρων και του κόμβου ελέγχου θεωρείται ως ένα ασύρματο δίκτυο βιοαισθητήρων, προσφέροντας δυνατότητες παρακολούθησης και διαχείρισης της υγείας του ασθενούς.

2.4 Αρχιτεκτονική, πρότυπα και πρωτόκολλα επικοινωνίας ιατρικών συσκευών

Τη τελευταία δεκαετία, πολλαπλές δυνατότητες επικοινωνίας και δικτύωσης ενσωματώνονται συνεχώς στις ιατρικές συσκευές. Εξοπλισμένες με ένα ραδιοπομπό, οι ιατρικές συσκευές και κυρίως οι εμφυτεύσιμες, μπορούν να επικοινωνούν με μια εξωτερική συσκευή, η οποία χαρακτηρίζεται ως «*αναγνώστης*» και να της στέλνει δεδομένα, όπως για παράδειγμα δεδομένα από ένα βηματοδότη ή έναν απινιδωτή, τα οποία μπορεί με τη σειρά του ο ιατρός να χρησιμοποιήσει για τον εντοπισμό μιας παθολογικής κατάστασης του ασθενούς. Ο «*αναγνώστης*» μπορεί επίσης να δώσει εντολή στην ιατρική συσκευή ώστε να ρυθμίσει μια θεραπεία ή να εκτελέσει ενημερώσεις λογισμικού. [14]

2.4.1 Αρχιτεκτονική επικοινωνίας

Παρατηρώντας την Εικόνα 7, αναλύεται η αρχιτεκτονική της επικοινωνίας των ιατρικών συσκευών. Ένα σύνολο έξυπνων και μικρών ασύρματων αισθητήρων τοποθετούνται τόσο στην επιφάνεια όσο και στο εσωτερικό του ανθρώπινου σώματος. Οι αισθητήρες είναι ικανοί να συλλέξουν, να επεξεργαστούν και να παρακολουθούν τις φυσιολογικές παραμέτρους του ασθενούς, οι οποίες είναι αναγκαίες για τη διάγνωση και τη διαχείριση της υγείας του ασθενούς. Παράλληλα, σταθερές ιατρικές συσκευές όπως εξοπλισμός Μονάδας Εντατικής Θεραπείας (ΜΕΘ), ακτινολογικός εξοπλισμός κ.λπ. περιέχουν επίσης αισθητήρες και συνδέονται στο διαδίκτυο για την παροχή ορθής θεραπείας. Οι αισθητήρες μοιράζονται τα δεδομένα που συλλέγουν μέσω ενός smartphone ή ενός PDA. Τα δεδομένα αυτά μεταδίδονται μέσω ενσύρματων ή ασύρματων πρωτοκόλλων επικοινωνίας, από το κινητό ή τον ιατρικό εξοπλισμό, σε μια έξυπνη τοπική πύλη. Οι πάροχοι υπηρεσιών υγείας έχουν πρόσβαση μέσω της πύλης στις πληροφορίες των ασθενών. Έπειτα χρησιμοποιείται ένα υπολογιστικό νέφος για την αποθήκευση και την ανάλυση των δεδομένων που συλλέγονται από τους αισθητήρες. Παρέχεται επίσης μια γραφική διεπαφή για την τελική οπτικοποίηση των δεδομένων. Οι πάροχοι υπηρεσιών και οι επαγγελματίες φροντίδας μπορούν να αξιοποιήσουν αυτή την υποδομή νέφους για να έχουν πρόσβαση σε δεδομένα όπως το ιατρικό ιστορικό, οι τάσεις ασθενειών και η απομακρυσμένη παρακολούθηση της υγείας. [14][15]



Εικόνα 7 Αρχιτεκτονική επικοινωνίας ιατρικών συσκευών

2.4.2 Τεχνολογία και πρωτόκολλα επικοινωνίας

Οι ιατρικές συσκευές χρησιμοποιούν τόσο ενσύρματα όσο και ασύρματα πρωτόκολλα και πρότυπα επικοινωνίας, για να εκτελέσουν τις αντίστοιχες διεργασίες τους. Τα πρωτόκολλα και οι τεχνολογίες αυτές διακρίνονται ως εξής [14][15]:

- ZigBee: Είναι τεχνολογία που χρησιμοποιείται σε συσκευές με ενσωματωμένους αισθητήρες. Χαρακτηρίζεται από την αποδοτικότητά της και την ευρεία εφαρμογή της σε περιβάλλοντα χαμηλής κατανάλωσης ενέργειας. Απευθύνεται σε εφαρμογές που χρησιμοποιούν ραδιοσυχνότητες και προσφέρουν μεγάλη διάρκεια ζωής της μπαταρίας, χαμηλή κατανάλωση ισχύος, ασφαλή δικτύωση και χαμηλό ρυθμό μετάδοσης δεδομένων. Οι αισθητήρες με τεχνολογία ZigBee έχουν μεγάλη διάρκεια μπαταρίας, λόγω της δυνατότητας αναστολής της λειτουργίας, καθιστώντας τες έτσι λειτουργικές για πολλά χρόνια προτού εξαντληθεί η μπαταρία τους. Η τυπική εμβέλεια επικοινωνίας του ZigBee κυμαίνεται από 10 έως 100 μέτρα, ανάλογα με τις περιβαλλοντικές συνθήκες και την ισχύ εξόδου.
- Bluetooth: Έχει σχεδιαστεί για μικρής εμβέλειας ασύρματη επικοινωνία. Σχηματίζει ένα δίκτυο στο οποίο μια συσκευή ενεργεί ως master και οι άλλες ως slaves. Ένα σημαντικό χαρακτηριστικό του Bluetooth είναι η δυνατότητα σύνδεσης κι επικοινωνίας με μια σειρά συσκευών από όλο τον κόσμο. Ένα ακόμη βασικό χαρακτηριστικό είναι η ικανότητα των συσκευών αυτών να επικοινωνούν χωρίς την ανάγκη ακριβούς τοποθέτησης. Για αυτό το λόγο, χρησιμοποιούνται ευρέως για τη σύνδεση προσωπικών συσκευών. Η τυπική εμβέλεια του Bluetooth κυμαίνεται από 10 έως 30 μέτρα, ανάλογα με την ισχύ μετάδοσης και την κάλυψή τους.
- Bluetooth Low Energy (BLE): Το BLE είναι μια παραλλαγή του πρωτοκόλλου Bluetooth κι αποτελεί την ιδανική λύση για αισθητήρες σε ιατρικές συσκευές λόγω της χαμηλής κατανάλωσης ενέργειας. Σχεδιάστηκε ειδικά για τη σύνδεση μικρών αισθητήρων με φορητούς σταθμούς. Το πρότυπο αυτό μπορεί να προσφέρει ταχύτητα μετάδοσης δεδομένων έως και 1 Mbps κι ο συγχρονισμός των συσκευών διαρκεί μόνο μερικά χιλιοστά του δευτερολέπτου, καθώς χρησιμοποιεί λίγα κανάλια για τη σύζευξη των συσκευών. Έτσι το BLE καθίσταται σημαντικό στην παρακολούθηση της υγείας και ιδανικό για συσκευές αισθητήρων που απαιτούν μικρή καθυστέρηση.

- IEEE 802.11: Είναι ένα σύνολο προτύπων σχεδιασμένο για ασύρματα τοπικά δίκτυα. Έχει κάλυψη σχεδόν 100 μέτρα. Είναι συνήθως κατάλληλο για εφαρμογές που απαιτούν υψηλή ταχύτητα μεταφοράς δεδομένων, εξασφαλίζοντας γρήγορη ασύρματη συνδεσιμότητα. Το βασικότερο πλεονέκτημα αυτού του προτύπου είναι η ενσωμάτωσή του σε ένα πλήθος συσκευών, όπως φορητοί υπολογιστές και smartphones, ωστόσο η αυξημένη κατανάλωση ενέργειας αποτελεί έναν σημαντικό περιορισμό του.
- IEEE 802.3: Το Ethernet είναι από τα πιο διαδεδομένα πρότυπα που θεσπίστηκαν για την ενσύρματη συνδεσιμότητα. Αποτελείται από δυο διαφορετικά στοιχεία, μεταξύ των οποίων (1) τα μέσα διασύνδεσης και (2) τους κόμβους δικτύου. Μέσα διασύνδεσης είναι τα υλικά και τα τεχνολογικά μέσα, μέσω των οποίων διαδίδονται σήματα σε ένα δίκτυο επικοινωνίας. Κύριος σκοπός τους είναι ο καθορισμός του ρυθμού μεταφοράς δεδομένων. Παραδείγματα τέτοιων μέσων αποτελούν τα ομοαξονικά καλώδια, τα καλώδια συνεστραμμένου ζεύγους και οι οπτικές ίνες. Κόμβοι δικτύου είναι τα σημεία όπου πραγματοποιείται η επικοινωνία σε ένα δίκτυο. Περιλαμβάνουν τον Εξοπλισμό Τερματικού Δεδομένων (Data Terminal Equipment, DTE) και τον Εξοπλισμό Επικοινωνίας Δεδομένων (Data Communications Equipment, DCE). Οι κόμβοι είναι τα συνδετικά σημεία για τη μετάδοση και τη λήψη πληροφοριών μεταξύ συσκευών.

2.4.3 Πλεονεκτήματα ενσύρματης κι ασύρματης επικοινωνίας

Η ενίσχυση των ιατρικών συσκευών με δυνατότητες ενσύρματης κι ασύρματης επικοινωνίας και δικτύωσης, φέρει σημαντικά πλεονεκτήματα [14]:

- Συνεχής παρακολούθηση: Παρέχει συνεχή έλεγχο των φυσιολογικών παραμέτρων του ασθενούς κι άλλων καταστάσεων της υγείας του, που καταγράφονται από τη συσκευή, μειώνοντας έτσι την ανάγκη για τακτικές επισκέψεις παρακολούθησης στον ιατρό και ελαχιστοποιώντας τις παρεμβολές στην καθημερινή ζωή του.
- Βελτιωμένη διαχείριση: Ενισχύει την εποπτεία και τη διαχείριση της λειτουργίας της ιατρικής συσκευής, επιτρέποντας την άμεση αντιμετώπιση τυχόν προβλημάτων μέσω έγκαιρων διορθωτικών ενεργειών.
- Κόστος: Οι δυο παραπάνω παράγοντες, συμβάλλουν παράλληλα στη μείωση του συνολικού κόστους που σχετίζεται με την παρακολούθηση του ασθενούς και τη διαχείριση της ιατρικής συσκευής.

2.5 Επίλογος

Σε αυτό κεφάλαιο αναφέρθηκε ο ορισμός της ιατρικής συσκευής καθώς και στην ιστορική και τεχνολογική εξέλιξη των ιατρικών συσκευών. Καταγράφηκε η κατηγοριοποίηση των ιατρικών συσκευών, παραθέτοντας παραδείγματα για κάθε κατηγορία. Αναλύθηκαν η αρχιτεκτονική επικοινωνίας, οι τεχνολογίες και πρωτόκολλα επικοινωνίας που εφαρμόζονται στις ιατρικές συσκευές, καθώς και τα πλεονεκτήματα που φέρουν οι δυνατότητες ενσύρματης κι ασύρματης επικοινωνίας των ιατρικών συσκευών.

Κεφάλαιο 3ο: Κυβερνοασφάλεια

3.1 Εισαγωγή

Στο κεφάλαιο αυτό, γίνεται αναφορά στους όρους ασφάλεια πληροφοριών, κυβερνοασφάλεια και στην εξέλιξη από την ασφάλεια πληροφοριών στην κυβερνοασφάλεια. Αναφέρεται ο όρος ιός και πως αυτός εξελίχθηκε σε ransomware. Παρουσιάζονται οι ευπάθειες και ο έλεγχος ευπαθειών. Αναλύονται ακόμη οι τύποι κυβερνοεπιθέσεων και οι άμυνες που λαμβάνει η κυβερνοασφάλεια έναντι κυβερνοεπιθέσεων.

3.2 Ασφάλεια πληροφοριών και κυβερνοασφάλεια

Σύμφωνα με το Εθνικό Ινστιτούτο Προτύπων και Τεχνολογίας (NIST), ασφάλεια πληροφοριών είναι: «*η προστασία των πληροφοριών και των πληροφοριακών συστημάτων από μη εξουσιοδοτημένη πρόσβαση, χρήση, αποκάλυψη, διατάραξη, τροποποίηση ή καταστροφή προκειμένου να παρέχεται εμπιστευτικότητα, ακεραιότητα και διαθεσιμότητα*» [16]. Οι πληροφορίες που προστατεύονται ποικίλουν σε μορφή και μπορούν να είναι ψηφιακά αρχεία, έντυπα έγγραφα, φυσικά μέσα ή ακόμη και ανθρώπινος λόγος. [17]

Μια παραβίαση δεδομένων κοστίζει στο θύμα της με ποικίλους τρόπους. Ο αιφνίδιος χρόνος διακοπής λειτουργίας προκαλεί απώλεια επιχειρηματικών δραστηριοτήτων κι εσόδων. Η έκθεση ευαίσθητων πληροφοριών πελατών μπορεί να οδηγήσει σε απώλεια εμπιστοσύνης, απομάκρυνση πελατών και ανεπανόρθωτη δυσφήμιση στην εταιρεία. Η κλοπή πνευματικής ιδιοκτησίας ενδέχεται να πλήξει την οικονομική απόδοση της εταιρείας και να μειώσει το ανταγωνιστικό της πλεονέκτημα. Η ασφάλεια πληροφοριών περιλαμβάνει ένα σύνολο εργαλείων, τεχνολογιών και διαδικασιών με τα οποία εξασφαλίζει την προστασία των επιχειρησιακών δεδομένων σε κάθε συσκευή και τοποθεσία. Στόχος είναι η θωράκιση απέναντι σε κυβερνοεπιθέσεις και περιστατικά που θα προκαλούσαν διαταραχές. Τα εργαλεία αυτά περιλαμβάνουν: [18]

- Ασφάλεια εφαρμογών: Περιλαμβάνει διαδικασίες, εργαλεία, πολιτικές και βέλτιστες πρακτικές που θεσπίζονται για την προστασία εφαρμογών και των δεδομένων τους.
- Ασφάλεια νέφους: Πρόκειται για διαδικασίες, εργαλεία, πολιτικές και βέλτιστες πρακτικές που θεσπίζονται για την προστασία όλων των πτυχών του νέφους, συμπεριλαμβανομένων των συστημάτων, των εφαρμογών, των δεδομένων και της υποδομής.
- Κρυπτογράφηση: Είναι μια μέθοδος προστασίας της επικοινωνίας η οποία χρησιμοποιεί αλγορίθμους για την κωδικοποίηση δεδομένων, ώστε να διασφαλίσει ότι μόνο εξουσιοδοτημένοι παραλήπτες μπορούν να έχουν πρόσβαση σε ένα περιεχόμενο και να το αποκρυπτογραφήσουν.
- Αποκατάσταση από καταστροφές: Αποτελεί μια διαδικασία που στοχεύει στην επαναφορά της λειτουργικότητας των τεχνολογικών συστημάτων μετά από φυσικές καταστροφές, κυβερνοεπιθέσεις ή άλλες διαταραχές, διασφαλίζοντας τη συνέχεια και την αποφυγή παρατεταμένων διακοπών.
- Αντιμετώπιση περιστατικών: Περιλαμβάνει τη στρατηγική και το πλάνο ενός οργανισμού για την ταχεία και αποτελεσματική διαχείριση περιστατικών όπως παραβιάσεις δεδομένων, κυβερνοεπιθέσεις ή άλλα αποδιοργανωτικά συμβάντα, με στόχο την αποκατάσταση της λειτουργίας και τον περιορισμό των συνεπειών.
- Ασφάλεια υποδομών: Πρόκειται για την προστασία της συνολικής τεχνολογικής υποδομής ενός οργανισμού, η οποία περιλαμβάνει το λογισμικό, το υλικό, τα δίκτυα, τα δεδομένα και τις φυσικές εγκαταστάσεις, με στόχο την εξασφάλιση της ακεραιότητας, της διαθεσιμότητας και της εμπιστευτικότητάς τους.
- Διαχείριση τρωτότητας: Αναφέρεται στην οργανωμένη διαδικασία που εφαρμόζει ένας οργανισμός για τον εντοπισμό, την αξιολόγηση και την αποκατάσταση ευπαθειών στα τελικά

σημεία, το λογισμικό και τα συστήματά του. Στόχος είναι η μείωση των κινδύνων ασφαλείας μέσω της προληπτικής αναγνώρισης αδυναμιών, της αξιολόγησης του αντίκτυπού τους και της υλοποίησης μέτρων αποκατάστασης.

Οι πρακτικές ασφάλειας των πληροφοριών στηρίζονται σε θεμελιώδεις αρχές που έχουν αναπτυχθεί και εξελιχθεί μέσα από χρόνια εμπειρίας και καινοτομίας. Οι τρεις βασικοί πυλώνες της ασφάλειας των πληροφοριών, γνωστοί κι ως τριάδα εμπιστευτικότητα, ακεραιότητα, διαθεσιμότητα (Confidentiality, Integrity, Availability, CIA), είναι οι εξής: [17][18]

- Εμπιστευτικότητα: Το απόρρητο αποτελεί θεμελιώδες στοιχείο της ασφάλειας πληροφοριών, διασφαλίζοντας ότι μόνο εξουσιοδοτημένοι χρήστες μπορούν να έχουν πρόσβαση σε ευαίσθητες πληροφορίες. Οι οργανισμοί μπορούν να εφαρμόσουν μέτρα όπως κρυπτογράφηση δεδομένων, έλεγχο ταυτότητας πολλαπλών παραγόντων και συστήματα πρόληψης απώλειας δεδομένων για να προστατεύσουν την εμπιστευτικότητα. Η έννοια της εμπιστευτικότητας περιλαμβάνει την αποτροπή μη εξουσιοδοτημένης πρόσβασης σε δεδομένα, εξασφαλίζοντας ότι οι πληροφορίες παραμένουν προσβάσιμες μόνο από τα κατάλληλα άτομα. Εάν ένα μη εξουσιοδοτημένο άτομο αποκτήσει κωδικό πρόσβασης σε προστατευμένα δεδομένα, θα πρόκειται για παραβίαση της εμπιστευτικότητας.
- Ακεραιότητα: Αναφέρεται στη διασφάλιση ότι οι πληροφορίες στις βάσεις δεδομένων μιας εταιρείας είναι πλήρεις κι ακριβείς. Οι ενέργειες που στοχεύουν στην ακεραιότητα έχουν σκοπό να εμποδίσουν την αλλοίωση των δεδομένων όπως μη εξουσιοδοτημένες προσθήκες, τροποποιήσεις ή διαγραφές. Η ακεραιότητα των δεδομένων αφορά την πρόληψη κάθε απόπειρας να αλλοιωθούν τα δεδομένα, είτε από κακόβουλους χρήστες που το κάνουν σκόπιμα, είτε από χρήστες που χωρίς πρόθεση αλλοιώνουν τα δεδομένα χωρίς την απαιτούμενη εξουσιοδότηση. Εργαλεία όπως τα δικαιώματα αρχείων, η διαχείριση ταυτότητας και οι έλεγχοι πρόσβασης χρηστών συμβάλλουν στην καλύτερη διασφάλιση της ακεραιότητας των δεδομένων.
- Διαθεσιμότητα: Οι χρήστες διασφαλίζουν ότι έχουν τη δυνατότητα να προσπελάσουν τις πληροφορίες στις οποίες έχουν εξουσιοδότηση όταν τις χρειάζονται. Η διαθεσιμότητα απαιτεί από τα μέτρα και τις πολιτικές ασφαλείας να μην εμποδίζουν την εξουσιοδοτημένη πρόσβαση στα δεδομένα. Χαρακτηριστικό της διαθεσιμότητας είναι η εύρυθμη λειτουργία τόσο του υλικού όσο και του λογισμικού, κάνοντας συντήρηση του φυσικού εξοπλισμού και τακτική ενημέρωση του συστήματος, ώστε να αποφεύγονται προβλήματα, όπως και η διασφάλιση εφεδρικών συστημάτων σε περίπτωση αποτυχίας του κύριου συστήματος.

Η κυβερνοασφάλεια θεωρείται κλάδος της ασφάλειας πληροφοριών και είναι [19]: «*η πρακτική της προστασίας συστημάτων, δικτύων και προγραμμάτων από ψηφιακές επιθέσεις, με στόχο τη διασφάλιση της εμπιστευτικότητας, της ακεραιότητας και της διαθεσιμότητας των πληροφοριών*». Σε αντίθεση με την ασφάλεια πληροφοριών, η κυβερνοασφάλεια επικεντρώνεται αποκλειστικά στην προστασία των ψηφιακών δεδομένων και των συστημάτων που τα διαχειρίζονται, από απειλές που πηγάζουν από τον κυβερνοχώρο, όπως επιθέσεις hacking, κακόβουλο λογισμικό κι άλλες επιβλαβείς ενέργειες. Η μετάβαση από ασφάλεια πληροφοριών σε κυβερνοασφάλεια αποδίδεται στη διαρκώς αυξανόμενη εξάρτηση από τα ψηφιακά συστήματα και το διαδίκτυο, γεγονός που δημιούργησε την εμφάνιση νέων κινδύνων και προκλήσεων [20].

3.3 Έννοια και ιστορική εξέλιξη των ιών υπολογιστή

Σύμφωνα με το NIST, ιός ενός υπολογιστικού συστήματος είναι: «*ένα πρόγραμμα που μπορεί να αντιγράψει τον εαυτό του και να μολύνει έναν υπολογιστή χωρίς την άδεια ή τη γνώση του χρήστη*» [21]. Ένας ιός μπορεί να καταστρέψει ή να διαγράψει δεδομένα σε έναν υπολογιστή, να χρησιμοποιήσει προγράμματα ηλεκτρονικού ταχυδρομείου για να εξαπλωθεί σε άλλους υπολογιστές ή ακόμη και να διαγράψει τα πάντα σε έναν σκληρό δίσκο.

Η έννοια του ιού παρουσιάστηκε για πρώτη φορά σε μια σειρά διαλέξεων του μαθηματικού John von Neumann στα τέλη της δεκαετίας του 1940 και αναπτύχθηκε περαιτέρω σε μια εργασία του που δημοσίευσε το 1966 με τίτλο *Theory of Self-Reproducing Automata*. Η εργασία αυτή ήταν ουσιαστικά ένα πείραμα σκέψης που πρότεινε ότι θα μπορούσε να είναι εφικτό για έναν μηχανικό οργανισμό, όπως ένα κομμάτι κώδικα υπολογιστή, να καταστρέφει συστήματα, να αναπαράγει τον εαυτό του και να μολύνει νέους ξενιστές, μιμούμενος τη λειτουργία ενός βιολογικού ιού. Ένας βιολογικός ιός εισβάλλει σε ζωντανά κύτταρα, συνδέεται στην επιφάνεια ενός κυττάρου και εισέρχεται σε αυτό. Απελευθερώνει το DNA του μέσα στο κύτταρο, έτσι ώστε να παραχθούν νέα σωματίδια του ιού τα οποία θα απελευθερωθούν στη συνέχεια από το κύτταρο και θα εξαπλωθούν σε νέα κύτταρα [22].

Ο πρώτος ιός δημιουργήθηκε το 1971 από τον Bob Thomas, με τη χαρακτηριστική ονομασία Creeper. Σχεδιάστηκε αρχικά ως ένα πείραμα ασφαλείας για να ελεγχθεί αν είναι εφικτή η δημιουργία ενός αυτοαναπαραγόμενου προγράμματος, κάτι το οποίο αποδείχθηκε κατά κάποιο τρόπο. Το πρόγραμμα σχεδιάστηκε να κινείται μεταξύ διαφορετικών υπολογιστών στο ARPANET, που είναι πρόδρομος του σύγχρονου Διαδικτύου. Ο Ray Tomlinson, που είναι συνάδελφος του Bob Thomas, τροποποίησε το πρόγραμμα Creeper ώστε όχι μόνο να κινείται μεταξύ υπολογιστών, αλλά και να αντιγράφει τον εαυτό του από τον έναν υπολογιστή στον άλλον. Κάθε φορά που το Creeper μόλυνε ένα νέο σκληρό δίσκο, επιχειρούσε να διαγράψει την παρουσία του από τον προηγούμενο δίσκο. Το Creeper δεν είχε απολύτως καμία κακόβουλη πρόθεση και το μόνο που έκανε ήταν να εμφανίζει το μήνυμα της Εικόνας 8: [22][23][24].

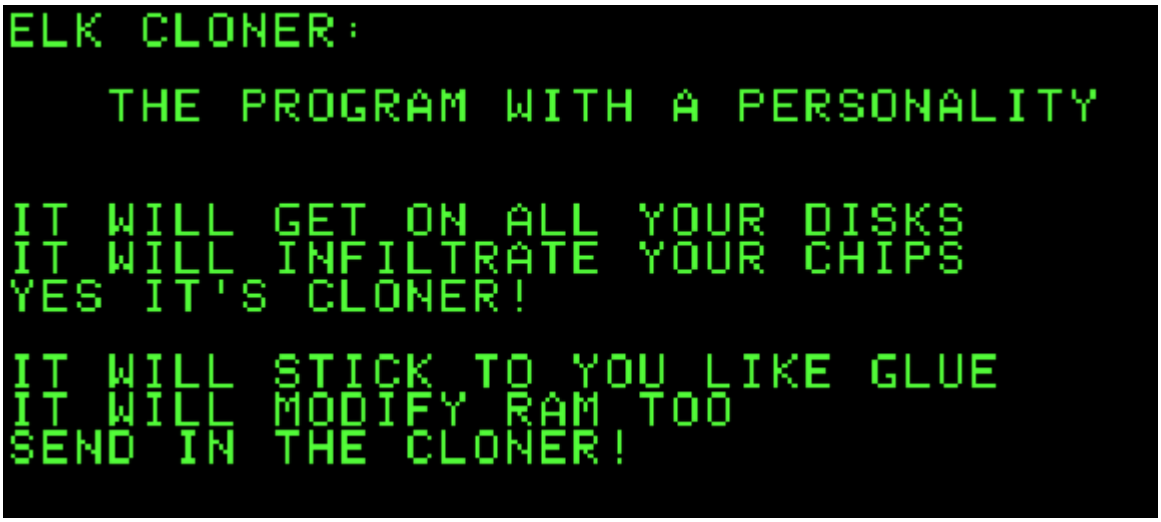
Εικόνα 8 Μήνυμα του ιού Creeper

Το 1974 αναπτύχθηκε ο ιός Rabbit (Λαγός), ο οποίος είχε κακόβουλη πρόθεση και μπορούσε να αναπαράγει τον εαυτό του. Εισερχόταν σε έναν υπολογιστή και δημιουργούσε ασταμάτητα πολλαπλά αντίγραφα του εαυτού του, επιβαρύνοντας σοβαρά την απόδοση του συστήματος και οδηγώντας το στην κατάρρευσή του. Η ονομασία του ιού προέκυψε από την ταχύτητα με την οποία αναπαραγόταν [22].

Το Trojan είναι κακόβουλο πρόγραμμα που παρουσιάζεται ως χρήσιμη ή αβλαβή εφαρμογή ή ενσωματώνεται σε νόμιμο λογισμικό , με σκοπό να εξαπατήσουν τους χρήστες ώστε να τα εγκαταστήσουν. Μόλις γίνει η εγκατάσταση, μπορούν να επιτρέψουν στους επιτιθέμενους να αποκτήσουν μη εξουσιοδοτημένη πρόσβαση στο σύστημα, ώστε να κλέψουν δεδομένα ή να

προκαλέσουν βλάβες στο σύστημα. Το πρώτο Trojan, γνωστό ως Animal, αναπτύχθηκε το 1975 από τον προγραμματιστή John Walker. Την εποχή εκείνη, ήταν δημοφιλή τα {προγράμματα ζώων} τα οποία προσπαθούσαν να μαντέψουν το ζώο που σκεφτόταν ο χρήστης μέσω ενός παιχνιδιού 20 ερωτήσεων. Η έκδοση που είχε δημιουργήσει ο Walker είχε μεγάλη ζήτηση, αλλά απαιτούσε τη δημιουργία και την διανομή μαγνητικών ταινιών. Για να απλοποιήσει τη διαδικασία, ο Walker ανέπτυξε το Pervade, το οποίο εγκαθίστατο αυτόματα μαζί με το Animal. Καθώς ο χρήστης έπαιζε το παιχνίδι, το Pervade σάρωνε όλους τους διαθέσιμους καταλόγους του υπολογιστή και δημιουργούσε ένα αντίγραφου του Animal όπου αυτό δεν υπήρχε ήδη. Το Animal και το Pervade πληρούσαν τον ορισμό του Trojan, χωρίς να έχουν κακόβουλη πρόθεση. Μέσα στο Animal ήταν κρυμμένο ένα άλλο πρόγραμμα που εκτελούσε ενέργειες χωρίς τη συγκατάθεση του χρήστη [22].

Το πρόγραμμα Elk Cloner, που σχεδιάστηκε αρχικά ως μια αθώα φάρσα, δημιουργήθηκε το 1982 από τον Rich Skrenta σε ηλικία μόλις δεκαπέντε ετών,. Ο Skrenta ήταν ενεργό μέλος της λέσχης υπολογιστών του λυκείου του κι είχε αποκτήσει τη φήμη ότι τροποποιούσε παιχνίδια κι άλλο λογισμικό που κυκλοφορούσαν μεταξύ των μελών της ομάδας. Η συνήθεια του να προσθέτει αλλαγές οι οποίες ήταν απρόβλεπτες, έκανε πολλούς να αποφεύγουν να δέχονται δισκέτες από τον Skrenta, καθώς ανησυχούσαν για το τι έκπληξη μπορεί να τους περιμένει. Σε μια προσπάθεια να αλλάξει το λογισμικό των δίσκων στους οποίους δε μπορούσε να έχει άμεση πρόσβαση, ο Skrenta δημιούργησε τον πρώτο γνωστό ιό για Apple υπολογιστές, τον οποίο σήμερα ονομάζουμε ιό του τομέα εκκίνησης (boot sector virus). Ο Elk Cloner εξαπλώθηκε μολύνοντας το λειτουργικό σύστημα Apple DOS 3.3 και μόλις μεταφερόταν από μια μολυσμένη δισκέτα, αντιγραφόταν στη μνήμη του υπολογιστή. Όταν αργότερα μια υγιής δισκέτα τοποθετούνταν στον υπολογιστή, ο Elk Cloner αντιγραφόταν σε αυτή τη δισκέτα και εξαπλώθηκε γρήγορα στους περισσότερους φίλους του Skrenta. Αν και σκόπιμα κακόβουλο, ο Elk Cloner μπορούσε να γράψει κατά λάθος πάνω και να διαγράψει κάποιες δισκέτες. Περιείχε επίσης ένα μήνυμα το οποίο ανάγραφε το μήνυμα της Εικόνας 9: [23]



Εικόνα 9 Μήνυμα του ιού Elk Cloner

Ο Brain θεωρείται ο πρώτος ιός για τους προσωπικούς υπολογιστές IBM και συμβατούς και αναπτύχθηκε το 1986. Οι Amjad και Basit Farooq Alvi, αδέλφια από το Πακιστάν, με στόχο να αποτρέψουν την παραβίαση πνευματικών δικαιωμάτων επειδή ήταν διανομείς ιατρικού εξοπλισμού, δημιούργησαν τον Brain. Σκοπός του ιού ήταν να εμποδίσει τους χρήστες να χρησιμοποιούν αντιγραμμένες εκδόσεις του λογισμικού των δύο αδελφών. Όταν εγκαθίστατο, ο Brain εμφάνιζε ένα μήνυμα που προέτρεπε τους {πειρατές} να καλέσουν τους αδελφούς για να λάβουν τη {θεραπεία} για

τον ιό, χωρίς όμως να αλλοιώνει τα δεδομένα του υπολογιστή του κάθε χρήστη. Υποτιμώντας το πόσο διαδεδομένο ήταν το πρόβλημα της πειρατείας, τα αδέλφια δέχθηκαν το πρώτο τους τηλεφώνημα από τις Ηνωμένες Πολιτείες της Αμερικής, ακολουθούμενο από πολλά ακόμα σε όλο τον κόσμο. [22][23]

Το σκουλήκι είναι κακόβουλο πρόγραμμα που μπορεί να εξαπλωθεί αυτόνομα χωρίς την ανάγκη ανθρώπινης παρέμβασης. Διεισδύει σε συστήματα υπολογιστών και μετακινείται από συσκευή σε συσκευή μέσω δικτύων, εκμεταλλευόμενο ευπάθειες ασφαλείας, ώστε να κλέψει δεδομένα, να εγκαταστήσει κακόβουλο λογισμικό ή να υπερφορτώσει ένα δίκτυο. Το σκουλήκι Morris δημιουργήθηκε το 1988 όχι με κακόβουλη πρόθεση αλλά ως απόδειξη της ιδέας. Δυστυχώς για τον δημιουργό του, τον φοιτητή του MIT Robert Morris, το σκουλήκι αποδείχθηκε πολύ πιο αποτελεσματικό από αυτό που περίμενε. Την εποχή εκείνη μόνο περίπου εξήντα χιλιάδες υπολογιστές είχαν πρόσβαση στο διαδίκτυο, κυρίως στα πανεπιστήμια και στον στρατό. Σχεδιασμένο να εκμεταλλεύεται ένα «παραθυράκι» στα συστήματα Unix και ταυτόχρονα να παραμένει κρυφό, το σκουλήκι γρήγορα εξαπλώθηκε αντιγράφοντας τον εαυτό του συνεχώς και μολύνοντας το 10% όλων των υπολογιστών που ήταν συνδεδεμένοι στο δίκτυο. Το σκουλήκι αντιγραφόταν όχι μόνο σε άλλους υπολογιστές, αλλά και επανειλημμένα στους μολυσμένους υπολογιστές, καταναλώνοντας έτσι μεγάλα ποσοστά της μνήμης. Θεωρείται η πρώτη εκτεταμένη διαδικτυακή κυβερνοεπίθεση στον κόσμο και προκάλεσε ζημιές που μερικές εκτιμήσεις λένε πως ανέρχονται σε εκατομμύρια. Για τη συμμετοχή του σε αυτό, ο Robert Morris ήταν ο πρώτος κυβερνοεγκληματίας που καταδικάστηκε για κυβερνοαπάτη στις Ηνωμένες Πολιτείες. [23]

Το Μάιο του 2000 ο Φιλιππινέζος Onel de Guzman δεν είχε τη δυνατότητα να πληρώσει την υπηρεσία dial-up internet κι έτσι κατασκεύασε έναν σκουλήκι ιό με μακροεντολές, ο οποίος έκλεβε τους κωδικούς πρόσβασης άλλων ανθρώπων. Ο ιός με κωδική ονομασία ILOVEYOU αποτέλεσε το πρώτο σημαντικό κομμάτι κακόβουλου λογισμικού. Ο Guzman αξιοποίησε την ανθρώπινη ψυχολογία, εκμεταλλευόμενος την περιέργεια και τις συναισθηματικές ανάγκες των ανθρώπων για να τους παρασύρει να κατεβάσουν κακόβουλα συνημμένα αρχεία ηλεκτρονικού ταχυδρομείου που εμφανίζονταν ως ερωτικές επιστολές. Το ILOVEYOU ακολούθησε το πρότυπο των προηγούμενων ιών ηλεκτρονικού ταχυδρομείου, αλλά σε αντίθεση με τους συνηθισμένους ιούς οι οποίοι ήταν ενσωματωμένοι σε αρχεία Word, το ILOVEYOU έφτανε ως αρχείο VBS (Visual Basic Script) το οποίο είναι ένας τύπος αρχείου για την αυτοματοποίηση εργασιών στα Windows, όπως διαχείριση αρχείων και δεν προκαλούσε με αυτόν τον τρόπο υποψίες. Με απλό τρόπο εκμεταλλεύτηκε την αδυναμία των χρηστών της εποχής να αναγνωρίσουν ανεπιθύμητα μηνύματα. Το θέμα του μηνύματος ήταν «*I Love You*» και ήταν συνοδευόμενο από ένα συνημμένο αρχείο με την ονομασία «*LOVE-LETTER-FOR-YOU-TXT.vbs*». Ο Guzman σχεδίασε τον ιό ώστε να αντικαθιστά αρχεία των θυμάτων με αντίγραφά του. Η εξάπλωση έγινε μέσω της αποστολής του σε όλες τις επαφές ηλεκτρονικού ταχυδρομείου τους, καθώς τα προγράμματα που διαχειρίζονταν το ηλεκτρονικό ταχυδρομείο είχαν αποθηκευμένες τις επαφές, για να μπορεί ο χρήστης να ανταλλάσσει μηνύματα μαζί τους. Η χρήση του ονόματος ενός γνωστού προσώπου ως αποστολέα ενίσχυε την πιθανότητα τα θύματα να ανοίξουν το μήνυμα, αναδεικνύοντας την αποτελεσματικότητα της κοινωνικής μηχανικής. Ο ιός αυτός προκάλεσε ζημιές εκατομμυρίων και κατάφερε να θέσει εκτός λειτουργίας ακόμη και το υπολογιστικό σύστημα του Κοινοβουλίου του Ηνωμένου Βασιλείου για σύντομο χρονικό διάστημα. Παρόλο που ο Guzman συνελήφθη το 2000 στις Φιλιππίνες , όλες οι κατηγορίες αποσύρθηκαν καθώς στην πραγματικότητα δεν είχε παραβιάσει κανέναν τοπικό νόμο. [22][23]

Το σκουλήκι Mydoom, το οποίο δημιουργήθηκε το 2004, λειτουργούσε παρόμοια με το ILOVEYOU κι αξιοποίησε το ηλεκτρονικό ταχυδρομείο για να εξαπλωθεί και να μολύνει συστήματα σε παγκόσμια κλίμακα. Αφού εγκαθιστόταν σε έναν υπολογιστή, έθετε το σύστημα του θύματος υπό τον έλεγχό του

στέλνοντας περισσότερα αντίγραφα του εαυτού του μέσω email. Υπήρξε περίοδος όπου το spam του Mydoom αντιστοιχούσε στο 25% όλων των email που αποστέλλονταν παγκοσμίως, σημειώνοντας ένα αξεπέραστο ρεκόρ και δείχνοντας την αποτελεσματικότητά του. Το Mydoom αξιοποίησε τους μολυσμένους υπολογιστές για να δημιουργήσει ένα botnet, το οποίο είναι δίκτυο υπολογιστών που έχουν μολυνθεί από κακόβουλο λογισμικό και ελέγχονται από τον επιτιθέμενο, που χρησιμοποιήθηκε για την εκτέλεση κατανεμημένων επιθέσεων άρνησης παροχής υπηρεσιών (Distributed Denial of Service, DDoS), οι οποίες θα αναλυθούν σε επόμενη ενότητα. Οι ζημιές που προκάλεσε ανήλθαν στα τριανταπέντε δισεκατομμύρια δολάρια των Ηνωμένων Πολιτειών, καθιστώντας το ακόμη και προσαρμοσμένο στον πληθωρισμό, το πιο δαπανηρό κακόβουλο λογισμικό που δημιουργήθηκε ποτέ. Παρά τον τεράστιο αντίκτυπο του, οι δημιουργοί του Mydoom δεν έχουν ταυτοποιηθεί ή συλληφθεί ποτέ. [23]

Το Trojan Emotet το οποίο ο Arne Schoenbohm, επικεφαλής του Γερμανικού Γραφείου Ασφάλειας Πληροφοριών, χαρακτήρισε ως «βασιλιά του κακόβουλου λογισμικού», πρωτοεμφανίστηκε το 2014 κι αποτελεί κλασσικό παράδειγμα πολυμορφικού κακόβουλου λογισμικού. Αυτό το είδος κακόβουλου λογισμικού δυσκολεύει τους ειδικούς της ασφάλειας πληροφοριών στο να το εξαλείψουν πλήρως, καθώς τροποποιεί ελαφρώς τον κώδικά του κάθε φορά που αναπαράγεται. Αντί για ακριβή αντίγραφα, δημιουργεί παραλλαγές που είναι εξίσου επικίνδυνες. Αυτή η ιδιότητα καθιστά τα πολυμορφικά κακόβουλα λογισμικά ιδιαίτερα δύσκολο να εντοπιστούν και να αποκλειστούν από προγράμματα αντιμετώπισης κακόβουλου λογισμικού. [23]

Το ransomware (ή λυτρισμικό) «*είναι ένα είδος κακόβουλου λογισμικού που απειλεί να δημοσιοποιήσει τα προσωπικά δεδομένα του θύματος ή να διακόψει την πρόσβαση του θύματος σε αυτά μέχρι να δοθούν λύτρα από το θύμα*» [24]. Τα τελευταία χρόνια το ransomware έχει παρουσιάσει αυξομειώσεις κι αλλαγές στον τρόπο δράσης του. Οι κακόβουλοι χρήστες πλέον επικεντρώνονται σε πιο προβεβλημένους στόχους, προκαλώντας μεγαλύτερες ζημιές. Μια ανησυχητική εξέλιξη είναι η άνοδος του Ransomware-as-a-Service (RaaS), το οποίο διατίθεται σε αγορές του σκοτεινού ιστού και προσφέρει ένα μοντέλο plug-and-play. Επαγγελματίες χάκερ εκτελούν επιθέσεις λυτρισμικού για λογαριασμό πελατών με αντάλλαγμα αμοιβή. Ενώ οι παλαιότερες επιθέσεις απαιτούσαν εξειδικευμένες τεχνικές δεξιότητες, το RaaS επιτρέπει σε οποιονδήποτε με κακή πρόθεση και τα απαραίτητα χρήματα να πραγματοποιεί καταστροφικές επιθέσεις. [23]

3.3.1 Μέρη ενός ιού

Ένας ιός περιέχει τρία μέρη [25]:

- Τον μηχανισμό μόλυνσης, ο οποίος βρίσκει και μολύνει νέα αρχεία
- Το ωφέλιμο φορτίο, το οποίο είναι ο κακόβουλος κώδικας προς εκτέλεση
- Τη σκανδάλη, η οποία καθορίζει πότε θα ενεργοποιηθεί το ωφέλιμο φορτίο

Μηχανισμός μόλυνσης: Είναι ο τρόπος με τον οποίο εξαπλώνεται ο ιός. Ορισμένοι ιοί έχουν μια ρουτίνα αναζήτησης, η οποία εντοπίζει και μολύνει αρχεία στο δίσκο. Υπάρχουν και ιοί οι οποίοι μολύνουν αρχεία καθώς εκτελούνται.

Ωφέλιμο φορτίο: Είναι το σώμα του ιού που εκτελεί την κακόβουλη δραστηριότητα. Οι κακόβουλες δραστηριότητες περιλαμβάνουν την καταστροφή αρχείων, την κλοπή εμπιστευτικών πληροφοριών ή την κατασκοπεία του μολυσμένου συστήματος. Η δραστηριότητα του ωφέλιμου φορτίου είναι αξιοσημείωτη, καθώς μπορεί να προκαλέσει επιβράδυνση ή ακόμα και πάγωμα του συστήματος.

Σκανδάλη: Είναι γνωστή κι ως λογική βόμβα και είναι το τμήμα του ιού που καθορίζει τη συνθήκη για την οποία ενεργοποιείται το ωφέλιμο φορτίο. Η συνθήκη αυτή μπορεί να είναι μια συγκεκριμένη ώρα, ημερομηνία, η παρουσία ενός άλλου προγράμματος, το άνοιγμα ενός συγκεκριμένου αρχείου ή το μέγεθος στο δίσκο που υπερβαίνει ένα όριο.

3.3.2 Φάσεις ενός ιού

Οι φάσεις ενός ιού είναι στην πραγματικότητα ο κύκλος ζωής του. Αυτός ο κύκλος ζωής μπορεί να χωριστεί στις παρακάτω φάσεις [25]:

- Φάση αδράνειας: Ο ιός βρίσκεται σε αδράνεια κατά τη διάρκεια αυτής της φάσης. Ο ιός έχει καταφέρει να αποκτήσει πρόσβαση στον υπολογιστή ή το λογισμικό του χρήστη, αλλά κατά τη διάρκεια αυτής της φάσης, δεν αναλαμβάνει καμία δράση. Ο ιός θα ενεργοποιηθεί από τη σκανδάλη που δηλώνει ποιο γεγονός θα εκτελέσει τον ιό. Δεν έχουν όλοι οι ιοί αυτό το στάδιο.
- Φάση διάδοσης: Στη φάση διάδοσης ο ιός αρχίζει να πολλαπλασιάζεται και να αναπαράγεται. Εισάγει αντίγραφα του εαυτού του σε άλλα προγράμματα ή σε συγκεκριμένα τμήματα του συστήματος, όπως στο δίσκο. Τα αντίγραφα αυτά ενδέχεται να μην είναι εντελώς πανομοιότυπα με την αρχική έκδοση, καθώς πολλοί ιοί τροποποιούνται ή μεταλλάσσονται ώστε να αποφύγουν την ανίχνευση από επαγγελματίες κυβερνοασφάλειας και λογισμικό προστασίας. Κάθε μολυσμένο πρόγραμμα περιέχει πλέον έναν κλώνο του ιού, ο οποίος με τη σειρά του εισέρχεται στη δική του φάση διάδοσης.
- Φάση ενεργοποίησης: Στη φάση ενεργοποίησης, ένας ιός που παραμένει αδρανής εισέρχεται σε λειτουργία και αρχίζει να εκτελεί το σκοπό για τον οποίο δημιουργήθηκε. Η ενεργοποίηση μπορεί να πυροδοτηθεί από διάφορα γεγονότα στο σύστημα, όπως ο αριθμός των φορών που ο ιός έχει δημιουργήσει αντίγραφα του εαυτού του. Η ενεργοποίηση μπορεί επίσης να προγραμματιστεί να συμβεί σε συγκεκριμένες περιστάσεις, όπως η πάροδος ενός προκαθορισμένου χρονικού διαστήματος, ώστε να μειωθούν οι πιθανότητες εντοπισμού.
- Φάση εκτέλεσης: Στη φάση εκτέλεσης ο ιός ολοκληρώνει το σκοπό του, απελευθερώνοντας το ωφέλιμο φορτίο του. Αυτό μπορεί να περιλαμβάνει καταστροφικές ενέργειες, όπως διαγραφή αρχείων, πρόκληση κατάρρευσης του συστήματος ή αλλοίωση δεδομένων. Σε άλλες περιπτώσεις, το ωφέλιμο φορτίο μπορεί να είναι και σχετικά ακίνδυνο, περιοριζόμενο στην εμφάνιση χιουμοριστικών μηνυμάτων στην οθόνη του χρήστη.

3.4 Ευπάθειες και έλεγχος ευπαθειών

Οι ευπάθειες στην κυβερνοασφάλεια αφορούν αδυναμίες σε ένα σύστημα ή στον τρόπο σχεδιασμού του που μπορούν να αξιοποιηθούν από έναν εισβολέα για να εκτελέσει κακόβουλες ενέργειες, να αποκτήσει μη εξουσιοδοτημένη πρόσβαση σε δεδομένα ή να προκαλέσει επιθέσεις άρνησης παροχής υπηρεσιών (DoS), οι οποίες αναλύονται σε επόμενη ενότητα. [26][27]

3.4.1 Κατηγορίες ευπαθειών

Οι ευπάθειες χωρίζονται σε διάφορες κατηγορίες, με τις κυριότερες να αναλύονται παρακάτω [28][29]:

Η κλοπή διαπιστευτηρίων είναι από τις πιο συχνές κι επικίνδυνες επιθέσεις στον κυβερνοχώρο, καθώς επιτρέπει στους εγκληματίες του κυβερνοχώρου να αποκτούν πρόσβαση σε ευαίσθητα δεδομένα και συστήματα, εκμεταλλευόμενοι την εξουσιοδότηση ενός νόμιμου χρήστη. Οι επιτιθέμενοι μπορούν να χρησιμοποιήσουν διάφορες μεθόδους για να κλέψουν διαπιστευτήρια όπως το phishing, το κακόβουλο λογισμικό και οι επιθέσεις πλήρωσης διαπιστευτηρίων. Η χρήση αδύναμων διαπιστευτηρίων αποτελεί επίσης σοβαρό κίνδυνο για την κυβερνοασφάλεια, καθώς επιτρέπει στους εγκληματίες του κυβερνοχώρου να αποκτούν εύκολα πρόσβαση σε προσωπικούς λογαριασμούς και συστήματα.

Όταν ένα λογισμικό έχει **εσφαλμένα διαμορφωμένες ρυθμίσεις**, όπως η απενεργοποίηση ή η κακή ρύθμιση των λειτουργιών ασφαλείας, δημιουργούνται κενά που μπορούν να εκμεταλλευτούν οι εγκληματίες του κυβερνοχώρου. Οι εγκληματίες του κυβερνοχώρου αναζητούν αυτά τα κενά και τις λανθασμένες ρυθμίσεις για να τα εκμεταλλευτούν και να αποκτήσουν μη εξουσιοδοτημένη πρόσβαση. Τα συστήματα που απαιτούν χειροκίνητη διαμόρφωση είναι συνήθως αυτά που μπορεί να έχουν σφάλματα και κενά.

Το **μη ενημερωμένο λογισμικό** αναφέρεται σε εφαρμογές, συστήματα ή εργαλεία που δεν έχουν λάβει τις απαραίτητες ενημερώσεις ή διορθώσεις ασφαλείας. Οι ενημερώσεις αυτές συχνά περιλαμβάνουν επιδιορθώσεις για γνωστά τρωτά σημεία και η μη εφαρμογή τους αφήνει το λογισμικό εκτεθειμένο σε πιθανές επιθέσεις. Οι εγκληματίες του κυβερνοχώρου επικεντρώνονται στην αναζήτηση σφαλμάτων ή ελαττωμάτων στο λογισμικό, τα οποία μπορούν να τους επιτρέψουν να αποκτήσουν μη εξουσιοδοτημένη πρόσβαση σε συστήματα. Τα ελαττώματα αυτά μπορούν να επιτρέψουν την υποκλοπή ευαίσθητων δεδομένων ή την εκτέλεση διαφόρων κακόβουλων ενεργειών. Συνέπειες του μη ενημερωμένου λογισμικού πέρα από τις παραβιάσεις δεδομένων είναι οι οικονομικές ζημιές και η υποβάθμιση της φήμης του οργανισμού.

Η **μη εξουσιΟδοτημένη πρόσβαση** είναι μια από τις πιο κοινές και επικίνδυνες απειλές για την κυβερνοασφάλεια. Όταν οι υπάλληλοι λαμβάνουν περισσότερα δικαιώματα από όσα είναι απαραίτητα για την εκτέλεση των καθηκόντων τους, αποτελεί παράδειγμα αυτής της ευπάθειας. Αυτή η επιπλέον πρόσβαση μπορεί να δημιουργήσει σοβαρούς κινδύνους (α) λόγω ανθρώπινου λάθους, (β) μέσω κακόβουλης δράσης, (γ) λόγω κατάχρησης αυτών των δικαιωμάτων (δ) αν ο λογαριασμός ενός υπαλλήλου παραβιαστεί από κάποιον απειλητικό παράγοντα.

Η **έλλειψη κρυπτογράφησης** αποτελεί σοβαρή απειλή για την ασφάλεια των δεδομένων ενός οργανισμού, καθώς επιτρέπει στους εγκληματίες του κυβερνοχώρου να υποκλέψουν, να αποκτήσουν και να εκμεταλλευτούν τα δεδομένα που μεταδίδονται μέσω του δικτύου. Χωρίς την κατάλληλη κρυπτογράφηση, τα δεδομένα παραμένουν εκτεθειμένα κι εύκολα προσβάσιμα.

Η **κακή εξυγίανση δεδομένων** είναι μια από τις κύριες αιτίες που αφήνουν εφαρμογές ευάλωτες σε επιθέσεις. Πρόκειται για την αποτυχία επαρκούς επικύρωσης ή καθαρισμού των δεδομένων που εισάγονται σε ένα σύστημα πριν αυτά υποβληθούν σε επεξεργασία ή χρήση. Δηλαδή, οι εφαρμογές λαμβάνουν δεδομένα από χρήστες ή εξωτερικά συστήματα, ένας επιτιθέμενος εισάγει δεδομένα που περιέχουν κακόβουλο κώδικα ή ακολουθίες δεδομένων που προκαλούν απρόβλεπτη συμπεριφορά, με την έλλειψη σωστής επικύρωσης ή καθαρισμού, τα κακόβουλα δεδομένα επεξεργάζονται από την εφαρμογή, οδηγώντας σε ανεπιθύμητες ενέργειες. Αίτια της κακής εξυγίανσης δεδομένων αποτελούν η αδυναμία διαχωρισμού δεδομένων από εντολές, η υπερβολική εμπιστοσύνη σε εισροές από χρήστες ή τρίτους και η έλλειψη χρήσης βιβλιοθηκών και εργαλείων ασφαλείας.

Η ευπάθεια **Ημέρα Μηδέν** (Zero Day) που ανακαλύπτεται από εγκληματίες του κυβερνοχώρου και αξιοποιείται πριν υπάρξει διαθέσιμη επιδιόρθωση ή ενημέρωση ασφαλείας από τον προγραμματιστή του συστήματος ή του λογισμικού. Οι ευπάθειες μηδενικής ημέρας είναι ιδιαίτερα επικίνδυνες λόγω του αιφνίδιου χαρακτήρα τους και της σοβαρής ζημιάς που μπορεί να προκαλέσουν. Η απουσία διαθέσιμων μέτρων προστασίας δίνει στους επιτιθέμενους την ευκαιρία να εκμεταλλευτούν το κενό ασφάλειας προτού οι υπεύθυνοι ή οι οργανισμοί προλάβουν να αντιδράσουν. Μπορεί να οδηγήσουν σε απώλεια δεδομένων, παραβίαση συστημάτων ή σημαντικές οικονομικές και λειτουργικές ζημιές.

Οι **εσωτερικές απειλές** προέρχονται από άτομα που έχουν ήδη νόμιμη πρόσβαση στα συστήματα και δεδομένα ενός οργανισμού και είναι δύσκολες να ανιχνευθούν. Αυτά τα άτομα μπορούν να είναι πρώην

ή νυν εργαζόμενοι του οργανισμού, συνεργάτες, εργολάβοι ή προμηθευτές και η απειλή μπορεί να είναι είτε εκούσια, για παράδειγμα κακόβουλες ενέργειες, είτε ακούσια, για παράδειγμα λάθος από αμέλεια. Οι κίνδυνοι ποικίλουν και μπορεί να είναι από κλοπή και αλλοίωση δεδομένων μέχρι επιθέσεις στον ίδιο τον οργανισμό και οικονομικές ζημιές.

3.4.2 Έλεγχος ευπαθειών

Ορισμένες ευπάθειες στην κυβερνοασφάλεια είναι αναπόφευκτες και θα παραμείνουν πάντοτε πρόβλημα για τους οργανισμούς. Οι περισσότερες από αυτές όμως μπορούν να μετριαστούν ή να περιοριστούν, ώστε να μην τις εκμεταλλευτούν οι εγκληματίες του κυβερνοχώρου. Οι οργανισμοί μπορούν να χρησιμοποιήσουν τις εξής τακτικές για να ελέγξουν τις ευπάθειες: [28][29][30]

- Ενημέρωση λογισμικού: Μια από τις πιο κοινές ευπάθειες της κυβερνοασφάλειας είναι το μη ενημερωμένο λογισμικό. Οι εφαρμογές συχνά εκδίδουν ενημερώσεις που διορθώνουν γνωστές αδυναμίες ασφαλείας κι ενσωματώνουν νέες λειτουργίες για την ενίσχυση της προστασίας των συστημάτων. Είναι απαραίτητο οι οργανισμοί να διατηρούν το λογισμικό τους ενημερωμένο, ώστε να αποφεύγεται η εκμετάλλευση των ευπαθειών από τους εγκληματίες του κυβερνοχώρου.
- Εφαρμογή πρακτικών κυβερνοασφάλειας: Ορισμένες ευπάθειες στην κυβερνοασφάλεια προκύπτουν από ανθρώπινα λάθη. Ένας οργανισμός μπορεί να εκπαιδεύσει το προσωπικό του σε πρακτικές κυβερνοασφάλειας, προκειμένου να μειωθεί ο κίνδυνος. Ένα συχνό πρόβλημα που προκαλείται από ανθρώπινο λάθος είναι τα αδύναμα διαπιστευτήρια σύνδεσης. Το προσωπικό θα πρέπει να χρησιμοποιεί ισχυρούς και μοναδικούς κωδικούς πρόσβασης, ώστε να καθιστούν δύσκολη την παραβίασή τους από επιτιθέμενους. Το προσωπικό θα πρέπει επίσης να ενεργοποιεί τον έλεγχο ταυτότητας πολλαπλών παραγόντων (Multi-Factor Authentication, MFA) για να προσθέσουν ένα επιπλέον επίπεδο ασφάλειας στους λογαριασμούς τους. Το MFA απαιτεί από τους χρήστες να παρέχουν επιπλέον στοιχεία πιστοποίησης για την επαλήθευση της ταυτότητάς τους, γεγονός που καθιστά πιο δύσκολη την κατάχρηση των διαπιστευτηρίων τους ακόμη κι αν αυτά διαρρεύσουν. Κρίσιμο είναι επίσης το προσωπικό να εκπαιδευτεί σε επιθέσεις όπως το phishing, οι οποίες προσπαθούν να τους εξαπατήσουν ώστε να παραχωρήσουν τα διαπιστευτήριά τους. Για να αποφύγουν τέτοιες επιθέσεις, θα πρέπει να αποφεύγουν ύποπτα συνημμένα ή συνδέσμους που τους στέλνονται.
- Εφαρμογή της πρόσβασης με ελάχιστα προνόμια: Η αρχή αυτή συμβάλλει στη μείωση των τρωτών σημείων ασφαλείας που προκύπτουν από ανεπαρκή έλεγχο πρόσβασης. Οι χρήστες πρέπει να λαμβάνουν μόνο την απαραίτητη πρόσβαση που απαιτείται για την εκτέλεση των καθηκόντων τους χωρίς περιττά επιπλέον προνόμια. Η εφαρμογή της πρόσβασης με ελάχιστα προνόμια βοηθά τους οργανισμούς να μειώσουν την επιφάνεια επίθεσης, περιορίζοντας τις ευκαιρίες που μπορούν να εκμεταλλευτούν οι εγκληματίες του κυβερνοχώρου. Σε περίπτωση που ένας κακόβουλος παράγοντας αποκτήσει πρόσβαση στο σύστημα, η προσέγγιση αυτή περιορίζει τις ενέργειες που μπορεί να εκτελέσει, ενισχύοντας έτσι την ασφάλεια του οργανισμού.
- Ασφαλή δίκτυα WiFi: Οι εγκληματίες του κυβερνοχώρου συχνά εκμεταλλεύονται αδύναμη ή ανύπαρκτη κρυπτογράφηση και κυρίως σε μη ασφαλή δίκτυα WiFi. Για την προστασία των δεδομένων τους, οι οργανισμοί πρέπει να διασφαλίζουν ότι το δίκτυο WiFi τους είναι σωστά ασφαλισμένο. Αυτό περιλαμβάνει τη χρήση ισχυρού και μοναδικού κωδικού πρόσβασης, την ενημέρωση του λογισμικού του δρομολογητή και την ενεργοποίηση πρωτοκόλλων κρυπτογράφησης. Αυτά τα μέτρα συμβάλλουν στην αποτροπή πιθανών επιθέσεων.
- Δοκιμή διείσδυσης (penetration testing): Είναι μια ελεγχόμενη προσομοίωση κυβερνοεπίθεσης που αξιολογεί την ανθεκτικότητα των συστημάτων ασφαλείας ενός οργανισμού. Μέσω αυτής της διαδικασίας οι ειδικοί εντοπίζουν πιθανές ευπάθειες που θα μπορούσαν να αξιοποιηθούν από κυβερνοεγκληματίες. Οι οργανισμοί ανακαλύπτουν κενά ασφαλείας που προέρχονται από ανθρώπινα λάθη είτε από αδυναμίες λογισμικού. Αυτό επιτρέπει τη βελτίωση των υφιστάμενων μέτρων προστασίας και την αποτροπή μελλοντικών επιθέσεων.

- Βελτίωση ποιότητας των δεδομένων: Για την ενίσχυση της ποιότητας των δεδομένων, οι ομάδες κυβερνοασφάλειας μπορούν να εφαρμόσουν προηγμένες μεθόδους προεπεξεργασίας. Αυτές περιλαμβάνουν τεχνικές καθαρισμού, κανονικοποίησης και εμπλουτισμού, οι οποίες διασφαλίζουν την ομοιομορφία και τη βελτιωμένη ακρίβεια των δεδομένων πριν από την ενσωμάτωσή τους σε αυτοματοποιημένα συστήματα.

3.5 Τύποι επιθέσεων και άμυνων κυβερνοασφάλειας

Μια επίθεση αποτελείται από μια σειρά ενεργειών που πραγματοποιούνται από μια ή περισσότερες απειλές με σκοπό την παραβίαση της ασφάλειας ή των πολιτικών ασφαλείας ενός συστήματος. Οι απειλές στοχεύουν συστήματα λογισμικού μέσω επιθέσεων και εάν αυτές είναι επιτυχείς, θεωρείται ότι έχει γίνει εκμετάλλευση του συστήματος. Όταν ένα λογισμικό πέσει θύμα εκμετάλλευσης, μπορεί να οδηγήσει σε παραβίαση της ασφάλειας ή των πολιτικών ασφαλείας [27].

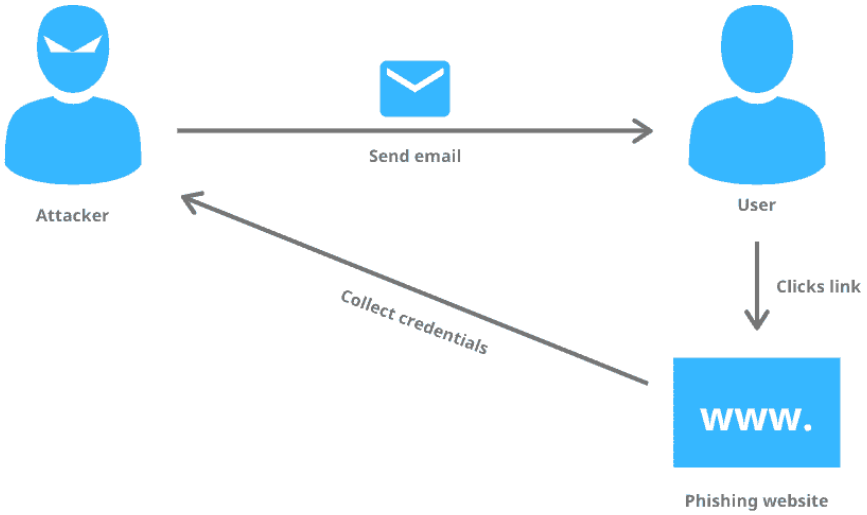
3.5.1 Επιθέσεις κυβερνοασφάλειας

Οι τύποι επιθέσεων ποικίλουν και μπορούν να διαχωριστούν στις ακόλουθες κατηγορίες [31][32]:

Κακόβουλο λογισμικό (malware) είναι οποιοδήποτε πρόγραμμα ή κώδικας σχεδιασμένος με σκοπό να προκαλέσει ζημιά σε έναν υπολογιστή, δίκτυο ή διακομιστή. Αποτελεί τη συνηθέστερη μορφή κυβερνοεπίθεσης καθώς περιλαμβάνει διάφορες κατηγορίες. όπως ransomware, Trojan, spyware, ιούς, σκουλήκια, keyloggers, bots, cryptojacking (έχει γίνει αναφορά σε προηγούμενο υποκεφάλαιο για το Trojan, τους ιούς και τα σκουλήκια).

- Σε μια επίθεση ransomware ο εισβολέας κρυπτογραφεί τα δεδομένα του θύματος και απαιτεί λύτρα σε αντάλλαγμα για το κλειδί αποκρυπτογράφησης. Αφού μολύνει το σύστημα, ο επιτιθέμενος απαιτεί λύτρα για να αποκαταστήσει τα δεδομένα, ωστόσο ακόμη και αν καταβληθούν τα λύτρα, δεν υπάρχει εγγύηση ότι ο κυβερνοεγκληματίας δεν έχει διατηρήσει αντίγραφα των πληροφοριών που έκλεψε. Το ransomware εξαπλώνεται συχνά μέσω ψεύτικων συνημμένων ή συνδέσμων που φαίνονται να είναι από αξιόπιστες πηγές.
- Το spyware είναι ένας τύπος κακόβουλου λογισμικού που μολύνει έναν υπολογιστή ή άλλη συσκευή και παρακολουθεί τις διαδικτυακές δραστηριότητες του χρήστη, συλλέγοντας προσωπικές πληροφορίες χωρίς τη συγκατάθεση ή ενημέρωσή του. Οι επιτιθέμενοι χρησιμοποιούν το spyware για κλοπή προσωπικών πληροφοριών όπως κωδικούς πρόσβασης σε email και τραπεζικούς λογαριασμούς. Μπορεί επίσης να δημιουργήσει αναδυόμενες διαφημίσεις, να αποστέλλει spam και να επιβραδύνει το σύστημα καταναλώνοντας υπολογιστικούς πόρους.
- Τα keyloggers είναι κακόβουλα εργαλεία που καταγράφουν κάθε πληκτρολόγηση που κάνει ο χρήστης σε μια συσκευή. Σε μια επίθεση keylogger, το λογισμικό παρακολουθεί και καταγράφει κάθε πληκτρολόγηση και στέλνει αυτές τις πληροφορίες στον επιτιθέμενο, χωρίς να το γνωρίζει το θύμα.
- Η κρυπτο-πειρατεία ή αλλιώς crypto-jacking είναι μια μορφή κακόβουλου λογισμικού που εκμεταλλεύεται τους υπολογιστικούς πόρους ενός μολυσμένου συστήματος για να εξορύξει κρυπτονομίσματα. Αυτή η επίθεση κλέβει τη δυνατότητα επεξεργασίας του συστήματος, θέτοντάς το υπό συνεχή υψηλό φόρτο με σκοπό την παραγωγή κρυπτονομισμάτων.

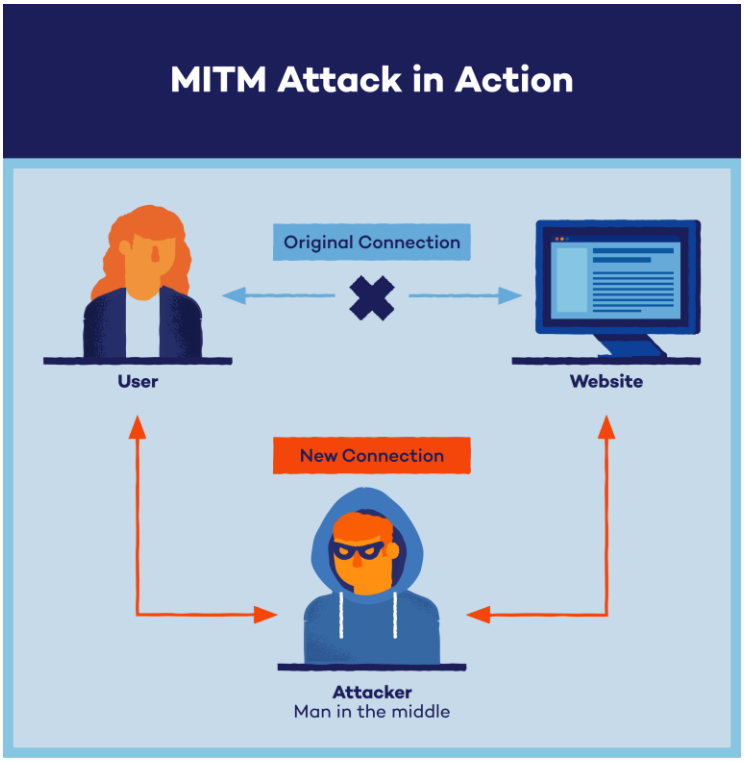
Το **phishing** είναι μια μορφή κυβερνοεπίθεσης που εκμεταλλεύεται το ηλεκτρονικό ταχυδρομείο, τα SMS μηνύματα, τις τηλεφωνικές κλήσεις, τα μέσα κοινωνικής δικτύωσης και άλλες τεχνικές κοινωνικής μηχανικής για να εξαπατήσει τα θύματα. Στόχος είναι να τα πείσει να αποκαλύψουν ευαίσθητες πληροφορίες όπως (α) κωδικούς πρόσβασης, (β) τραπεζικούς λογαριασμούς, (γ) να τα παρασύρει στη λήψη κακόβουλων αρχείων που μπορεί να εγκαταστήσουν ιούς κι άλλα επιβλαβή προγράμματα στις συσκευές τους. Οι συχνές επιθέσεις phishing περιλαμβάνουν το spear phishing, το whaling, το smishing και το vishing.



Εικόνα 10 Επίθεση phishing

- Το spear phishing είναι μια εξειδικευμένη μορφή phishing που στοχεύει συγκεκριμένα άτομα ή οργανισμούς, συνήθως μέσω προσεκτικά σχεδιασμένων κακόβουλων μηνυμάτων ηλεκτρονικού ταχυδρομείου. Ο κύριος στόχος είναι η υποκλοπή ευαίσθητων πληροφοριών, όπως διαπιστευτήρια σύνδεσης, ή η εγκατάσταση κακόβουλου λογισμικού στη συσκευή του θύματος.
- Το whaling είναι μια προηγμένη μορφή phishing που στοχεύει ανώτερα ή ανώτατα στελέχη ενός οργανισμού. Ο στόχος των επιτιθέμενων είναι η κλοπή χρημάτων, η υποκλοπή ευαίσθητων πληροφοριών ή η απόκτηση πρόσβασης στα συστήματα του οργανισμού για την διενέργεια περαιτέρω κυβερνοεπιθέσεων.
- Το smishing είναι ένας τύπος επίθεσης phishing που πραγματοποιείται μέσω SMS ή εφαρμογών ανταλλαγής μηνυμάτων. Οι επιτιθέμενοι στέλνουν απατηλά μηνύματα με σκοπό να εξαπατήσουν τα θύματα ώστε να αποκαλύψουν προσωπικά δεδομένα, όπως κωδικούς πρόσβασης, στοιχεία τραπεζικών λογαριασμών ή αριθμούς πιστωτικών καρτών. Οι κυβερνοεγκληματίες συχνά προσποιούνται ότι είναι αξιόπιστοι οργανισμοί.
- Το vishing ή φωνητικό phishing είναι μια μορφή κοινωνικής μηχανικής όπου οι επιτιθέμενοι χρησιμοποιούν τηλεφωνικές κλήσεις ή ηχογραφημένα μηνύματα για να εξαπατήσουν τα θύματα και να τα πείσουν να αποκαλύψουν ευαίσθητες πληροφορίες. Οι κυβερνοεγκληματίες προσποιούνται ότι είναι εκπρόσωποι τραπεζών ή υπάλληλοι τεχνικής υποστήριξης για να κερδίζουν την εμπιστοσύνη των θυμάτων τους.

Οι **επιθέσεις με βάση την ταυτότητα** εκμεταλλεύονται την κλοπή ή την κατάχρηση διαπιστευτηρίων πρόσβασης, επιτρέποντας στους επιτιθέμενους να εμφανίζονται ως νόμιμοι χρήστες. Οι επιθέσεις αυτού του είδους είναι ιδιαίτερα δύσκολο να ανιχνευθούν, καθώς ο κυβερνοεγκληματίας χρησιμοποιεί έγκυρα διαπιστευτήρια για να αποκτήσει πρόσβαση σε συστήματα και δεδομένα. Κάποιες από τις πιο κοινές επιθέσεις τέτοιου τύπου είναι οι man-in-the-middle, η συλλογή διαπιστευτηρίων, ο ψεκασμός κωδικού πρόσβασης (password spraying) και οι επιθέσεις ωμής βίας (brute force attacks).



Εικόνα 11 Επίθεση man-in-the-middle

- Η επίθεση man-in-the-middle είναι ένας τύπος κυβερνοεπίθεσης κατά την οποία ο επιτιθέμενος παρεμβαίνει στην επικοινωνία μεταξύ δυο μερών (συνήθως ενός χρήστη κι ενός διακομιστή ή υπηρεσίας) χωρίς να γίνεται αντιληπτός. Ο επιτιθέμενος έχει τη δυνατότητα να παρακολουθεί, να τροποποιεί ή να ανακατευθύνει τα δεδομένα που ανταλλάσσονται μεταξύ των δυο πλευρών, χωρίς να τον αντιληφθούν τα θύματα.
- Η συλλογή διαπιστευτηρίων είναι μια σημαντική τεχνική που χρησιμοποιούν οι κυβερνοεγκληματίες για να αποκτήσουν πρόσβαση σε λογαριασμούς, συστήματα ή εφαρμογές με σκοπό την κλοπή δεδομένων, την εκτέλεση κακόβουλων ενεργειών ή την εκμετάλλευση του προσωπικού ή εταιρικού απορρήτου. Οι επιθέσεις με στόχο τη συλλογή διαπιστευτηρίων περιλαμβάνουν την απόκτηση δεδομένων σύνδεσης, όπως ονόματα χρήστη, κωδικούς πρόσβασης, διευθύνσεις email κι άλλες ευαίσθητες πληροφορίες.
- Η επίθεση password spraying είναι μια μέθοδος που χρησιμοποιούν οι κυβερνοεγκληματίες για να παρακάμψουν τους μηχανισμούς ασφαλείας που προστατεύουν τους λογαριασμούς. Οι επιτιθέμενοι με password spraying χρησιμοποιούν έναν κοινό κωδικό πρόσβασης για πολλούς λογαριασμούς ταυτόχρονα. Αυτή η τεχνική μειώνει την πιθανότητα ανίχνευσης καθώς οι επιτιθέμενοι δεν δοκιμάζουν πολλούς κωδικούς σε έναν μόνο λογαριασμό, αλλά διάφορους λογαριασμούς με τον ίδιο κωδικό.
- Η επίθεση ωμής βίας είναι μια από τις πιο απλές αλλά και πιο επιβλαβείς μεθόδους κυβερνοεπίθεσης. Ο επιτιθέμενος χρησιμοποιεί αυτή την τεχνική για να μαντέψει συστηματικά κωδικούς πρόσβασης, ονόματα χρήστη ή κλειδιά κρυπτογράφησης, υποβάλλοντας κάθε δυνατό συνδυασμό μέχρι να βρει τον σωστό.

Το **spoofing** είναι μια μέθοδος εξαπάτησης όπου ένας κυβερνοεγκληματίας προσποιείται ότι είναι μια αξιόπιστη οντότητα για να παραπλανήσει θύματα και να αποκτήσει μη εξουσιοδοτημένη πρόσβαση σε συστήματα ή δεδομένα. Οι επιτιθέμενοι μπορούν να υποκλέψουν πληροφορίες, να διανείμουν κακόβουλο λογισμικό ή να εξαπατήσουν θύματα ώστε να εκτελέσουν ενέργειες προς όφελός τους, όπως η μεταφορά χρημάτων ή η αποκάλυψη διαπιστευτηρίων ασφαλείας. Το spoofing περιλαμβάνει διάφορες μορφές όπως domain spoofing, email spoofing και ARP spoofing (αλλοίωση του πρωτοκόλλου επίλυσης διευθύνσεων) (Address Resolution Protocol).

- Το domain spoofing είναι μια τεχνική εξαπάτησης στην οποία ο κυβερνοεγκληματίας πλαστογραφεί ένα domain name για να μιμηθεί έναν αξιόπιστο οργανισμό. Αυτό μπορεί να γίνει είτε μέσω ενός ψεύτικου ιστότοπου που μοιάζει με τον πραγματικό είτε μέσω παραποιημένων διευθύνσεων email. Οι επιτιθέμενοι εκμεταλλεύονται μικρές διαφορές στο domain name, όπως την αντικατάσταση χαρακτήρων (π.χ. "rn" αντί για "m") ή τη χρήση παρόμοιων επεκτάσεων (.net αντί για .com), για να ξεγελάσουν τα θύματα και να τα πείσουν να αποκαλύψουν ευαίσθητες πληροφορίες ή να κατεβάσουν κακόβουλο λογισμικό.
- Το email spoofing είναι μια τεχνική επίθεσης που χρησιμοποιείται από κυβερνοεγκληματίες για να πλαστογραφήσουν τη διεύθυνση αποστολέα ενός email κάνοντάς το να φαίνεται ότι προέρχεται από μια αξιόπιστη πηγή. Επειδή ο παραλήπτης εμπιστεύεται τον υποτιθέμενο αποστολέα, είναι πολύ πιθανό να ανοίξει το email και να αλληλεπιδράσει με το περιεχόμενό του που μπορεί να είναι ένα συνημμένο αρχείο ή ένας κακόβουλος σύνδεσμος.
- Το ARP spoofing είναι ένας τύπος επίθεσης δικτύου στην οποία ένας επιτιθέμενος στέλνει πλαστά μηνύματα ARP σε μια σε μια τοπική περιοχή δικτύου (Local Area Network, LAN) για να συνδέσει τη δική του διεύθυνση MAC με τη διεύθυνση IP μιας νόμιμης συσκευής. Έτσι η συσκευή εξαπατάται και στέλνει μηνύματα στον κακόβουλο χρήστη αντί για τον προοριζόμενο παραλήπτη. Με αυτόν τον τρόπο ο κακόβουλος χρήστης αποκτά πρόσβαση στις επικοινωνίες μιας συσκευής και στα ευαίσθητα δεδομένα που μπορεί να συμπεριλαμβάνονται.

Η **επίθεση άρνησης παροχής υπηρεσιών** (DoS) είναι μια κακόβουλη ενέργεια που έχει στόχο να πλημμυρίσει ένα δίκτυο με ψευδή αιτήματα, διαταράσσοντας τη λειτουργία του διακομιστή. Στην περίπτωση μιας επίθεσης DoS, οι χρήστες αδυνατούν να πραγματοποιήσουν βασικές ενέργειες όπως πρόσβαση σε email, ιστοσελίδες, λογαριασμούς ή άλλους πόρους που εξαρτώνται από έναν υπολογιστή ή δίκτυο που έχει υποστεί παραβίαση. Παρόλο που τέτοιες επιθέσεις δεν προκαλούν συνήθως απώλεια δεδομένων και επιλύονται χωρίς την καταβολή λύτρων, κοστίζουν στον οργανισμό χρόνο, χρήματα και πόρους για την αποκατάσταση των λειτουργιών του. Η βασική διαφορά ανάμεσα στις επιθέσεις DoS και στις επιθέσεις κατανεμημένης άρνησης παροχής υπηρεσιών (DDoS) είναι η προέλευση της επίθεσης. Στην περίπτωση των DoS η επίθεση προέρχεται από ένα μόνο σύστημα, ενώ στις DDoS η επίθεση προέρχεται από πολλά συστήματα ταυτόχρονα. Οι επιθέσεις DDoS είναι πιο γρήγορες και πιο δύσκολο να αποκρουστούν, καθώς απαιτείται εξουδετέρωση πολλαπλών συστημάτων για να σταματήσει η επίθεση

Οι **επιθέσεις έγχυσης κώδικα** είναι μια κατηγορία κυβερνοεπιθέσεων στις οποίες ο επιτιθέμενος εισάγει κακόβουλο κώδικα σε μια εφαρμογή ή σε ένα σύστημα με σκοπό να αλλάξει την κανονική λειτουργία του, συνήθως για να αποκτήσει πρόσβαση σε ευαίσθητα δεδομένα, να εκτελέσει κακόβουλες ενέργειες ή να προκαλέσει άλλες βλάβες στο σύστημα. Υπάρχουν διάφοροι τύποι επιθέσεων όπως η έγχυση SQL (SQL injection) και η διασταυρούμενη έγχυση σεναρίων (Cross-Site Scripting, XSS).

- Η επίθεση SQL Injection είναι μια από τις πιο επικίνδυνες και συχνές επιθέσεις στον τομέα της ασφάλειας των εφαρμογών και των βάσεων δεδομένων που χρησιμοποιούν SQL. Στην επίθεση SQL Injection, ο επιτιθέμενος εκμεταλλεύεται μια ευπάθεια στην εφαρμογή που χειρίζεται δεδομένα και κατασκευάζει κακόβουλες SQL εντολές για να χειραγωγήσει τη βάση δεδομένων. Αυτές οι εντολές μπορούν να αποκαλύψουν ευαίσθητα δεδομένα, να τροποποιήσουν τα περιεχόμενα της βάσης δεδομένων ή να διαγράψουν κρίσιμα δεδομένα.
- Το Cross-Site-Scripting είναι μια επικίνδυνη επίθεση ασφαλείας που εκμεταλλεύεται αδυναμίες σε ιστότοπους που επιτρέπουν στους χρήστες να εισάγουν ή να δημοσιεύουν περιεχόμενο χωρίς επαρκή επικύρωση και φιλτράρισμα. Όταν οι ιστότοποι επιτρέπουν στους χρήστες να εισάγουν δεδομένα όπως σχόλια, φόρμες ή άλλοι τύποι δεδομένων και αυτά τα δεδομένα στη συνέχεια ενσωματώνονται στον ιστότοπο χωρίς σωστό φιλτράρισμα, οι επιτιθέμενοι μπορούν να ενσωματώσουν κακόβουλο κώδικα σε αυτές τις περιοχές εισαγωγής. Όταν άλλοι χρήστες

επισκέπτονται την επηρεασμένη σελίδα, ο κακόβουλος κώδικας εκτελείται στον περιηγητή τους, εκθέτοντας ευαίσθητες πληροφορίες.

Οι **επιθέσεις κοινωνικής** μηχανικής (social engineering) βασίζονται στην εκμετάλλευση της ανθρώπινης ψυχολογίας και της συναισθηματικής αδυναμίας των στόχων για να τους πείσει να εκτελέσουν ενέργειες που δε θα έκαναν συνήθως, όπως η αποκάλυψη ευαίσθητων δεδομένων ή η παραχώρηση πρόσβασης σε συστήματα. Παραδείγματα επιθέσεων κοινωνικής μηχανικής είναι το pretexting, εκστρατείες παραπληροφόρησης, honeytrap και οι επιθέσεις BEC (Business Email Compromise).

- Το pretexting είναι μια επίθεση κοινωνικής μηχανικής όπου ο επιτιθέμενος δημιουργεί μια ψεύτικη ιστορία ή πρόφαση για να κερδίσει την εμπιστοσύνη του θύματος και να αποκτήσει πρόσβαση σε ευαίσθητες πληροφορίες ή συστήματα. Ο επιτιθέμενος χρησιμοποιεί το pretexting για να παραπλανήσει το θύμα και να το κάνει να αποκαλύψει πληροφορίες όπως κωδικούς πρόσβασης, τραπεζικούς λογαριασμούς ή άλλου τύπου ευαίσθητες πληροφορίες.
- Οι εκστρατείες παραπληροφόρησης είναι μια από τις πιο επικίνδυνες μορφές ψηφιακής επιρροής που χρησιμοποιούν στρατηγικές διανομής ψευδών ή παραπλανητικών πληροφοριών με σκοπό την προώθηση συγκεκριμένων κοινωνικών, πολιτικών ή στρατιωτικών συμφερόντων. Αυτές οι εκστρατείες αξιοποιούν κυρίως τα δίκτυα κοινωνικής δικτύωσης και τις πλατφόρμες διαδικτύου για να διαδώσουν ψευδείς αφηγήσεις και να δημιουργήσουν σκόπιμες παρανοήσεις στο κοινό.
- Οι επιθέσεις honeytrap είναι μια επικίνδυνη μορφή κοινωνικής μηχανικής που εκμεταλλεύεται την ανθρώπινη ανάγκη για συναισθηματική σύνδεση κι επικοινωνία, ιδιαίτερα μέσω διαδικτυακών εφαρμογών γνωριμιών. Οι δράστες δημιουργούν ψεύτικα προφίλ με σκοπό να προσελκύσουν άτομα που αναζητούν αγάπη ή φιλία και στη συνέχεια τους εξαπατούν για να αποκτήσουν χρήματα, προσωπικές πληροφορίες ή πρόσβαση σε συστήματα και λογαριασμούς.
- Σε μια επίθεση BEC οι επιτιθέμενοι αναλαμβάνουν την ταυτότητα ενός αξιόπιστου χρήστη ή εκπροσώπου μιας επιχείρησης για να εξαπατήσουν άλλους υπαλλήλους ή πελάτες της εταιρείας με σκοπό την απόκτηση χρημάτων, εμπιστευτικών δεδομένων ή πρόσβασης σε συστήματα.

Το **botnet**, του οποίου ο όρος προέρχεται από τις λέξεις robot και network, αποτελεί ένα δίκτυο υπολογιστών που έχουν μολυνθεί από κακόβουλο λογισμικό και ελέγχονται εξ αποστάσεως από ένα διαχειριστή. Ο διαχειριστής χρησιμοποιεί αυτούς τους μολυσμένους υπολογιστές για να πραγματοποιήσει επιθέσεις, όπως να προκαλέσει υπερφόρτωση σε δίκτυα, να διαδώσει κακόβουλο λογισμικό, να κλέψει διαπιστευτήρια ή να εκτελέσει εργασίες που απαιτούν υψηλή χρήση επεξεργαστικής ισχύος.

Με την εξέλιξη της **τεχνητής νοημοσύνης** και της μηχανικής μάθησης αυξάνονται και οι εφαρμογές τους. Οι κυβερνοεγκληματίες χρησιμοποιούν αυτές τις τεχνολογίες για να παραβιάσουν δίκτυα και να υποκλέψουν ευαίσθητα δεδομένα. Η αξιοποίηση της τεχνητής νοημοσύνης από κυβερνοεγκληματίες μπορεί να οδηγήσει σε πιο εξελιγμένες και δύσκολα ανιχνεύσιμες επιθέσεις. Παραδείγματα αποτελούν η επιθετική τεχνητή νοημοσύνη, η σκοτεινή τεχνητή νοημοσύνη (Dark AI) και το deepfake.

- Οι κυβερνοεγκληματίες χρησιμοποιούν επιθετική τεχνητή νοημοσύνη και μηχανική μάθηση για να αποδυναμώσουν ή να παραπλανήσουν συστήματα τεχνητής νοημοσύνης. Αυτό επιτυγχάνεται με τη χειραγώγηση των δεδομένων εκπαίδευσης, εισάγοντας ανακριβείς ή κακόβουλες πληροφορίες ώστε το σύστημα να κάνει λανθασμένες προβλέψεις ή να παρουσιάζει αδυναμίες που μπορούν να αξιοποιηθούν.
- Το Dark AI αναφέρεται στη χρήση τεχνητής νοημοσύνης και μηχανικής μάθησης από κυβερνοεγκληματίες για την εκμετάλλευση αδυναμιών ασφαλείας. Αυτή η κακόβουλη τεχνολογία δρα κρυφά, διεισδύοντας σε συστήματα χωρίς να εντοπίζεται μέχρι να προκαλέσει ζημιά, όπως την υποκλοπή δεδομένων ή τη διατάραξη κρίσιμων λειτουργιών.

- Τα deepfakes είναι ψεύτικα πολυμέσα που δημιουργούνται με τη βοήθεια τεχνητής νοημοσύνης, αποδίδοντας ρεαλιστικές εικόνες, βίντεο ή ήχο που μπορούν να παραπλανήσουν το κοινό. Αυτές οι τεχνικές πλαστογραφίας μπορούν να χρησιμοποιηθούν για τη χειραγώγηση της κοινής γνώμης, τη δυσφήμιση ατόμων ή την επιρροή σε πολιτικές και κοινωνικές εξελίξεις.

Μια **επίθεση στο Διαδίκτυο των Πραγμάτων** (Internet of Things, IoT) αναφέρεται σε οποιαδήποτε κυβερνοεπίθεση που στοχεύει συσκευές ή δίκτυα IoT. Όταν μια συσκευή παραβιάζεται, ο επιτιθέμενος μπορεί να αναλάβει τον έλεγχό της, να κλέψει δεδομένα ή να την προσθέσει σε ένα δίκτυο μολυσμένων συσκευών, όπως botnets, το οποίο μπορεί να χρησιμοποιηθεί για να εξαπολυθούν επιθέσεις DoS. Πολλές συσκευές IoT δε λαμβάνουν τακτικές ενημερώσεις λογισμικού, κάτι που τις αφήνει ευάλωτες απέναντι στους κυβερνοεγκληματίες ώστε να εκτελέσουν κακόβουλες εντολές ή να εγκαταστήσουν κακόβουλο λογισμικό. Οι τύποι επιθέσεων στις IoT συσκευές ποικίλουν.

- Οι επιτιθέμενοι μπορούν να παρεμβάλλονται στην επικοινωνία μεταξύ δύο IoT συσκευών, υποκλέπτοντας τα δεδομένα που ανταλλάσσονται (γνωστή κι ως επίθεση man-in-the-middle).
- Οι κυβερνοεγκληματίες μπορούν να εισάγουν κακόβουλο κώδικα στο ενσωματωμένο λογισμικό (firmware) μιας IoT συσκευής, δίνοντάς τους τον πλήρη έλεγχο της συσκευής.
- Επιθέσεις σε IoT συστήματα που βασίζονται σε ραδιοσυχνότητες (Radio Frequency Identification, RFID) και κοντινή επικοινωνία (Near Field Communication, NFC) με σκοπό την υποκλοπή δεδομένων πιστωτικών καρτών μέσω ανέπαφων τερματικών πληρωμών.
- Επιθέσεις πλευρικού καναλιού (Side-Channel Attacks) οι οποίες εκμεταλλεύονται πληροφορίες όπως η κατανάλωση ενέργειας και ο χρόνος απόκρισης της IoT συσκευής, με σκοπό την εξαγωγή δεδομένων ή την παράκαμψη μηχανισμών ασφαλείας.

Το **DNS tunneling** είναι μια κυβερνοεπίθεση που εκμεταλλεύεται τα αιτήματα και τις απαντήσεις του συστήματος ονομάτων τομέα (Domain Name System, DNS) για να παρακάμψει τα παραδοσιακά μέτρα ασφαλείας και να μεταφέρει δεδομένα ή κακόβουλο λογισμικό εντός του δικτύου. Μετά τη μόλυνση του συστήματος, ο επιτιθέμενος μπορεί να αποκτήσει πλήρη πρόσβαση για να εκτελεί διοικητικές ενέργειες και να χρησιμοποιεί το DNS tunnel για να διαβιβάσει κακόβουλο λογισμικό ή να αποσπάσει δεδομένα, ευαίσθητες πληροφορίες και IP διευθύνσεις, κωδικοποιώντας τες σε μικρές μονάδες μέσα στις DNS απαντήσεις.

Η **επίθεση στην αλυσίδα εφοδιασμού** στοχεύει το δίκτυο αξιόπιστων προμηθευτών ή συνεργατών μιας επιχείρησης και μπορεί να μολύνει μια επιχείρηση ή έναν οργανισμό μέσω ενός κακόβουλου τρίτου μέρους. Σε αυτές τις επιθέσεις, ο επιτιθέμενος εκμεταλλεύεται την εμπιστοσύνη που υπάρχει ανάμεσα στις εταιρείες και τους προμηθευτές τους για να εισάγει κακόβουλο κώδικα ή κακόβουλες ενέργειες σε λογισμικό ή υλικό που χρησιμοποιούν.

3.5.2 Άμυνες έναντι κυβερνοεπιθέσεων

Κάθε οργανισμός θα πρέπει να είναι έτοιμος να αντιμετωπίσει τις επερχόμενες κυβερνοεπιθέσεις, υιοθετώντας ένα συνδυασμό από τους διάφορους τύπους άμυνας έναντι κυβερνοεπιθέσεων [33][34][35][36]:

- Τείχος προστασίας (Firewall): Είναι μηχανισμός ασφαλείας που επιβλέπει κι ελέγχει τη ροή δεδομένων μέσα κι έξω από ένα δίκτυο. Αναλύει και φιλτράρει την κίνηση σύμφωνα με προκαθορισμένους κανόνες και επιτρέπει ή απορρίπτει τη μεταφορά δεδομένων, προστατεύοντας έτσι το σύστημα από μη εξουσιοδοτημένη πρόσβαση κι απειλές. Μπορεί να αποκλείσει ύποπτες δραστηριότητες που θα μπορούσαν να θέσουν σε κίνδυνο την ασφάλεια του δικτύου.
- Λογισμικό anti-virus: Αναπτύχθηκαν αρχικά για την ανίχνευση και αφαίρεση ιών υπολογιστών, εξ ου και η ονομασία τους. Στις πρώτες δεκαετίες της πληροφορικής, τα anti-virus ήταν συνήθως εμπορικά προϊόντα που απαιτούσαν αγορά άδειας χρήσης. Οι χρήστες πλήρωναν για

την απόκτηση του λογισμικού, το οποίο πρόσφερε βασικές λειτουργίες όπως σάρωση αρχείων, αφαίρεση ανιχνευμένων απειλών και ενημερώσεις. Το λογισμικό προστασίας έναντι ιών αποτελεί βασικό εργαλείο άμυνας κυβερνοασφάλειας, το οποίο πολλοί χρήστες γνωρίζουν και χρησιμοποιούν. Η εγκατάστασή του αποτρέπει τη μόλυνση από κακόβουλο λογισμικό. Δεδομένου ότι οι ιοί εξελίσσονται συνεχώς, είναι σημαντικό οι εταιρείες να ενημερώνονται για τις νεότερες τεχνολογίες προστασίας και να αναβαθμίζουν το λογισμικό τους. Με την πάροδο του χρόνου τα anti-virus εξελίχθηκαν για να παρέχουν προστασία έναντι διαφόρων απειλών, όπως Trojans, σκουλήκια και spyware και παράλληλα με την εξέλιξη της τεχνολογίας και την αύξηση των διαδικτυακών απειλών, τα anti-virus ενσωμάτωσαν πρόσθετες λειτουργίες όπως προστασία σε πραγματικό χρόνο, firewall, και εργαλεία για την προστασία της ιδιωτικότητας. Υπάρχουν πλέον τόσο εμπορικές όσο και δωρεάν εκδόσεις anti-virus, προσφέροντας ποικίλους τρόπους προστασίας.

- Κρυπτογράφηση δεδομένων: Η κρυπτογράφηση δεδομένων είναι μια ευρέως χρησιμοποιούμενη μέθοδος κυβερνοασφάλειας που εξασφαλίζει ότι μόνο όσοι διαθέτουν το κατάλληλο κλειδί αποκρυπτογράφησης μπορούν να έχουν πρόσβαση στις πληροφορίες. Οι κυβερνοεγκληματίες που επιχειρούν να παραβιάσουν κρυπτογραφημένα δεδομένα καταφεύγουν σε επιθέσεις ωμής βίας, δοκιμάζοντας συνεχώς διάφορα κλειδιά μέχρι να βρουν το σωστό, κάτι που κάνει την αποκρυπτογράφηση εξαιρετικά χρονοβόρα και δύσκολη. Ακόμη κι αν ένας κυβερνοεγκληματίας υποκλέψει τα δεδομένα, η ισχυρή κρυπτογράφηση θα τα καταστήσει ακατανόητα ή άχρηστα για κακόβουλη χρήση. Υπάρχουν δύο κύριοι τύποι κρυπτογράφησης, η συμμετρική και η ασύμμετρη. Στη συμμετρική κρυπτογράφηση χρησιμοποιείται το ίδιο κλειδί τόσο για την κρυπτογράφηση όσο και για την αποκρυπτογράφηση των δεδομένων. Ένας από τους πιο διαδεδομένους αλγορίθμους αυτής της κατηγορίας είναι το Προηγμένο Πρότυπο Κρυπτογράφησης (Advanced Encryption Standard, AES), ο οποίος επεξεργάζεται δεδομένα σε μπλοκ των 128 bit, υποστηρίζει κλειδιά μήκους 128, 192 και 256 bit, όπου τα μεγαλύτερα μήκη προσφέρουν και αυξημένη ασφάλεια και παρέχει ισχυρή ασφάλεια και αποδοτικότητα. Στην ασύμμετρη κρυπτογράφηση, που είναι γνωστή και ως κρυπτογράφηση δημοσίου κλειδιού, χρησιμοποιούνται δύο διαφορετικά αλλά μαθηματικά συνδεδεμένα κλειδιά: ένα δημόσιο και ένα ιδιωτικό κλειδί. Το δημόσιο κλειδί είναι διαθέσιμο σε όλους ή σε όσους επιθυμεί ο χρήστης και χρησιμοποιείται για την κρυπτογράφηση των δεδομένων, ενώ το ιδιωτικό κλειδί ο κάθε χρήστης το προφυλάσσει και το κρατάει απόρρητο και χρησιμοποιείται για την αποκρυπτογράφηση. Η ασύμμετρη κρυπτογράφηση επιλύει το πρόβλημα της διανομής κλειδιών που υπάρχει στη συμμετρική κρυπτογράφηση, καθώς δεν απαιτεί την ανταλλαγή μυστικών κλειδιών μεταξύ των πλευρών.
- Προστασία τελικού σημείου (Endpoint protection): Οι τελικοί χρήστες συχνά στοχοποιούνται από κυβερνοεγκληματίες, είτε μέσω των συσκευών τους είτε μέσω επιθέσεων κοινωνικής μηχανικής. Για την προστασία τους, όλες οι συσκευές θα πρέπει να διαθέτουν λογισμικό ασφαλείας για τελικά σημεία. Αυτό το λογισμικό πρέπει να είναι ενσωματωμένο σε ένα σύστημα διαχείρισης πληροφοριών και συμβάντων ασφαλείας (Security Information and Event Management, SIEM) το οποίο επιτρέπει την παρακολούθηση και την ανάλυση πιθανών απειλών σε ολόκληρο τον οργανισμό.
- Ανίχνευση εισβολής στο δίκτυο (Network Intrusion Detection): Για την ενίσχυση της προστασίας τους από IP που έχουν συσχετιστεί με κακόβουλη δραστηριότητα, οι οργανισμοί χρησιμοποιούν συστήματα ανίχνευσης και προστασίας από εισβολές (Intrusion Detection and Prevention Systems, IDPS), τα οποία βοηθούν στην ανίχνευση και αποτροπή πιθανών επιθέσεων που μπορούν να ξεπεράσουν τα τείχη προστασίας. Τα συστήματα ανίχνευσης εισβολών (Intrusion Detection Systems, IDS) χρησιμοποιούν λογισμικό για την αυτοματοποίηση της διαδικασίας ανίχνευσης κακόβουλης δραστηριότητας, ενώ τα συστήματα προστασίας εισβολών (Intrusion Prevention Systems, IPS) όχι μόνο ανιχνεύουν αλλά προσπαθούν και να αποτρέψουν τυχόν παραβιάσεις δεδομένων. Όταν εντοπιστεί μια παραβίαση, το IDS ειδοποιεί τους διαχειριστές του συστήματος για να λάβουν τα κατάλληλα μέτρα. Από την άλλη μεριά το IPS αναλύει την κυκλοφορία του δικτύου και μπλοκάρει την κακόβουλη κίνηση πριν προκαλέσει βλάβη, αποτρέποντας την επίθεση.
- Εκπαίδευση κατά του phishing: Είναι απαραίτητη η εκπαίδευση ενός οργανισμού σχετικά με τους κινδύνους του phishing. Η εκπαίδευση μπορεί να περιλαμβάνει προσομοιωμένες επιθέσεις

phishing μέσω email, την ανάλυση των αντιδράσεων του οργανισμού, σεμινάρια κι εργαστήρια, όπου θα παρέχονται γνώσεις σχετικά με τις τελευταίες τεχνικές που χρησιμοποιούν οι κυβερνοεγκληματίες και τη συνεχή βελτίωση της ευαισθητοποίησής του. Είναι απαραίτητο να υπάρχει διαρκής ενημέρωση σχετικά με τις πιο πρόσφατες τεχνικές phishing, ώστε ο οργανισμός να μπορεί να προστατεύει όσο καλύτερα μπορεί τα δεδομένα του. Είναι σημαντικό οι προσομοιώσεις να σχεδιάζονται προσεκτικά, ώστε να μην είναι υπερβολικά αγχωτικές, καθώς μπορεί να προκαλέσουν αρνητικές αντιδράσεις και να μειώσουν την αποτελεσματικότητα της εκπαίδευσης. Με το πέρας της εκπαίδευσης, το προσωπικό του οργανισμού θα είναι σε θέση να μειώσει τις επιτυχημένες επιθέσεις, καθώς θα αναγνωρίζουν και θα αποφεύγουν κακόβουλα μηνύματα, θα υπάρχει μια αίσθηση ασφάλειας εντός του οργανισμού και παράλληλα η αποτροπή επιθέσεων συμβάλλει και στην αποφυγή οικονομικών απωλειών και ζημιάς στη φήμη του οργανισμού.

- Έλεγχος κωδικού πρόσβασης και packet sniffers: Οι ειδικοί της κυβερνοασφάλειας χρησιμοποιούν προηγμένα εργαλεία για να αξιολογούν την ασφάλεια των κωδικών πρόσβασης και να παρακολουθούν την κίνηση στα δίκτυα. Γνωρίζουν ότι οι αδύναμοι κωδικοί πρόσβασης μπορούν να εκθέσουν ολόκληρο το δίκτυο σε κίνδυνο. Μέσω τεχνικών ελέγχου οι διαχειριστές μπορούν να αξιολογούν την αντοχή των κωδικών πρόσβασης σε πιθανές επιθέσεις. Ένας ανιχνευτής πακέτων (packet sniffer) είναι ένα εργαλείο, είτε σε μορφή λογισμικού είτε υλικού, που χρησιμοποιείται για την παρακολούθηση κι ανάλυση της κίνησης του δικτύου, βοηθώντας στον εντοπισμό πιθανών απειλών ή προβλημάτων ασφαλείας.

Με την πάροδο του χρόνου, οι συγκεκριμένες άμυνες βοήθησαν στην αντιμετώπιση και εξάλειψη των επιθέσεων που προαναφέρθηκαν [34][35][36].

Το **τείχος προστασίας** αντιμετωπίζει:

- Malware, καθώς μπλοκάρει ύποπτη κίνηση στο δίκτυο
- Botnets, εμποδίζοντας μη εξουσιοδοτημένες εισερχόμενες και εξερχόμενες συνδέσεις
- DoS, αφού περιορίζει τη ροή της επιθετικής κίνησης
- Spoofing, απορρίπτοντας μη έγκυρες IP διευθύνσεις
- DNS Tunneling, καθώς μπορεί να φιλτράρει ύποπτη DNS κίνηση
- IoT επιθέσεις, περιορίζοντας μη εξουσιοδοτημένη πρόσβαση σε IoT συσκευές

Το **λογισμικό anti-virus** αντιμετωπίζει:

- Malware, εντοπίζοντας και απομακρύνοντας ιούς, Trojans κλπ
- Botnets, καθώς αποτρέπει την εγκατάσταση botnet malware
- IoT επιθέσεις, σταματώντας κακόβουλα προγράμματα που στοχεύουν IoT συσκευές
- Επιθέσεις με τεχνητή νοημοσύνη, λόγω του ότι ανιχνεύει κακόβουλα προγράμματα που χρησιμοποιούν τεχνικές με τεχνητή νοημοσύνη

Η **κρυπτογράφηση δεδομένων** αντιμετωπίζει:

- Phishing, προστατεύοντας τα δεδομένα ακόμα κι αν παραβιαστούν
- Spoofing, καθώς βεβαιώνει την αυθεντικότητα των δεδομένων
- Επιθέσεις με βάση την ταυτότητα, προστατεύοντας τα διαπιστευτήρια και τις προσωπικές πληροφορίες
- SQL Injection, καθώς μπορεί να περιορίσει την πρόσβαση σε κρυπτογραφημένες βάσεις δεδομένων
- Επιθέσεις στην αλυσίδα εφοδιασμού, διασφαλίζοντας την εμπιστευτικότητα κατά τη μεταφορά δεδομένων

Η **προστασία τελικού σημείου** αντιμετωπίζει:

- Malware, καθώς ανιχνεύει και αποτρέπει εκτελέσεις κακόβουλου λογισμικού
- Botnets, εμποδίζοντας λογισμικά που μπορούν να εντάξουν τη συσκευή σε botnet
- IoT επιθέσεις, διότι προστατεύει τις έξυπνες συσκευές από επιθέσεις
- Επιθέσεις με τεχνητή νοημοσύνη, παρακολουθώντας και προλαμβάνοντας επιθέσεις

Η **ανίχνευση εισβολής στο δίκτυο** αντιμετωπίζει:

- Botnets, διότι ανιχνεύει ανωμαλίες στην κίνηση του δικτύου
- DoS, εντοπίζοντας ύποπτη αύξηση της κίνησης
- Spoofing, καθώς εντοπίζει ψεύτικες IP διευθύνσεις και περίεργες δραστηριότητες δικτύου
- DNS Tunneling, παρακολουθώντας κακόβουλες DNS επικοινωνίες
- IoT επιθέσεις, καθώς ανιχνεύει ύποπτη κίνηση από IoT συσκευές

Η **εκπαίδευση κατά του phishing** αντιμετωπίζει:

- Phishing, εκπαιδεύοντας τους χρήστες στην αναγνώριση ύποπτων emails και συνδέσμων
- Επιθέσεις κοινωνικής μηχανικής, καθώς βελτιώνει την ευαισθητοποίηση έναντι επιθέσεων εξαπάτησης
- Επιθέσεις με βάση την ταυτότητα, εκπαιδεύοντας τους χρήστες για ασφαλείς πρακτικές πρόσβασης

Ο **έλεγχος κωδικού πρόσβασης και packet sniffers** αντιμετωπίζει:

- Επιθέσεις με βάση την ταυτότητα, εξασφαλίζοντας ισχυρούς κωδικούς και ανιχνεύοντας κλοπές διαπιστευτηρίων
- Phishing, διότι βοηθά στην προστασία λογαριασμών ακόμα και μετά από παραβίαση
- Επιθέσεις κοινωνικής μηχανικής, αποτρέποντας την κατάχρηση διαπιστευτηρίων που αποκτώνται μέσω απάτης
- IoT επιθέσεις, καθώς ασφαλείς κωδικοί μειώνουν τον κίνδυνο πρόσβασης σε IoT συσκευές

3.6 Επίλογος

Σε αυτό το κεφάλαιο αναφέρθηκε ο ορισμός της ασφάλειας πληροφοριών και της κυβερνοασφάλειας, καθώς και οι τρεις βασικοί πυλώνες της ασφάλειας πληροφοριών. Καταγράφηκαν ο όρος του ιού, η ιστορική εξέλιξη των ιών και των κακόβουλων λογισμικών, τα μέρη ενός ιού και οι φάσεις του ιού. Αναλύθηκαν οι κατηγορίες ευπαθειών της κυβερνοασφάλειας και ο έλεγχος αυτών, όπως επίσης και οι κατηγορίες και οι τύποι επιθέσεων έναντι της κυβερνοασφάλειας και οι άμυνες που μπορούν να υιοθετήσουν οι χρήστες και οι οργανισμοί για την προστασία τους.

Κεφάλαιο 4ο: Νομικά συστήματα και πλαίσια

4.1 Εισαγωγή

Σε αυτό το κεφάλαιο αναφέρονται οι τρόποι με τους οποίους τα διαφορετικά νομικά συστήματα, όπως αυτό της Ευρωπαϊκής Ένωσης (ΕΕ), των Ηνωμένων Πολιτειών Αμερικής (ΗΠΑ) και του Ηνωμένου Βασιλείου, ρυθμίζουν την κυβερνοασφάλεια στις ιατρικές συσκευές, καθώς και νομικά πλαίσια για την κυβερνοασφάλεια των ιατρικών συσκευών.

4.2 Νομικό σύστημα Ευρωπαϊκής Ένωσης

Οι ιατρικές συσκευές στην ΕΕ ρυθμίζονται από τον Κανονισμό για τις Ιατρικές Συσκευές (Medical Devices Regulation, MDR), ο οποίος τέθηκε σε πλήρη εφαρμογή το 2021 και αντικατέστησε την Οδηγία για τις Ιατρικές Συσκευές (Medical Devices Directive, MDD) και την Οδηγία για τα Ενεργές Εμφυτεύσιμες Ιατρικές Συσκευές (Active Implantable Medical Devices Directive, AIMDD).

Ο MDR δεν περιλαμβάνει ρητές διατάξεις περί κυβερνοασφάλειας. Αυτό αφήνει περιθώρια στους κατασκευαστές να μειώσουν το επίπεδο προστασίας για να περιορίσουν το κόστος παραγωγής. Ωστόσο, οι Γενικές Απαιτήσεις Ασφάλειας και Επιδόσεων (General Safety and Performance Requirements, GSPR) λειτουργούν έμμεσα ως κατευθυντήριες γραμμές για την ενσωμάτωση της κυβερνοασφάλειας στις ιατρικές συσκευές. Η συμμόρφωση με τον MDR απαιτεί από τους κατασκευαστές να εφαρμόζουν συστήματα διαχείρισης κινδύνου, διασφάλισης ποιότητας και οικονομικής διαχείρισης, ώστε να εξασφαλιστεί η ασφαλής λειτουργία των συσκευών. Οι GSPR επισημαίνουν ότι οι ιατρικές συσκευές δεν πρέπει να αποτυγχάνουν λόγω κυβερνοεπιθέσεων. [37]

Η Ομάδα Συντονισμού Ιατρικών Συσκευών (Medical Device Coordination Group, MDCG) έχει εκδώσει οδηγίες που ενισχύουν την εφαρμογή ορθών πρακτικών κυβερνοασφάλειας, υποστηρίζοντας έτσι τις απαιτήσεις του MDR και διασφαλίζοντας τη λειτουργική και πληροφοριακή ασφάλεια των ιατρικών συσκευών. [37][38]

Οι GSPR έχουν ιδιαίτερη σημασία για την κυβερνοασφάλεια των ιατρικών συσκευών, καθώς επηρεάζουν τον κύκλο ζωής των συσκευών. Παρόλο που ο MDR δεν περιλαμβάνει άμεσες διατάξεις για την κυβερνοασφάλεια, οι αρχές των κρατών μελών μπορούν να χρησιμοποιήσουν τις GSPR ως βάση για να επιβάλουν αυστηρά μέτρα προστασίας. Σύμφωνα με τις GSPR οι ιατρικές συσκευές πρέπει να είναι τελευταίας τεχνολογίας και να λειτουργούν όπως προβλέπεται. Αυτό συνεπάγεται ότι οι κατασκευαστές οφείλουν να συμμορφώνονται με πρότυπα κυβερνοασφάλειας και να εξασφαλίζουν ότι οι συσκευές αντέχουν σε κυβερνοεπιθέσεις. Η μη συμμόρφωση σε τέτοια πρότυπα θα οδηγούσε σε σοβαρές συνέπειες, όπως για παράδειγμα η διακοπή λειτουργίας ενός βηματοδότη. Οι ιατρικές συσκευές θα πρέπει να διαθέτουν ελάχιστα επίπεδα κρυπτογράφησης, έλεγχο πρόσβασης και φυσική ασφάλεια ώστε να αποτρέπουν επιθέσεις. Αν οι κατασκευαστές δεν μπορούν να εγγυηθούν την αντοχή των συσκευών τους σε κυβερνοεπιθέσεις, τότε δεν πληρούν τις απαιτήσεις του MDR και δε θεωρούνται συμμορφούμενοι με τον κανονισμό.

Οι GSPR του MDR δεν είναι αυτόνομες, αλλά πρέπει να ερμηνεύονται σε συνδυασμό με τη γενική νομοθεσία κυβερνοασφάλειας της ΕΕ. Ένα από τα σημαντικά νομοθετικά πλαίσια που επηρεάζουν την ασφάλεια των ιατρικών συσκευών είναι η Οδηγία για τα Συστήματα Δικτύων και Πληροφοριών (Network and Information Systems Directive, NIS 2). Η NIS 2 αφορά την κυβερνοασφάλεια κρίσιμων

υποδομών σε ολόκληρη την ΕΕ, καλύπτοντας τόσο ιδιωτικούς όσο και δημόσιους φορείς. Οι ιατρικές συσκευές εντάσσονται σε αυτήν την κατηγορία, καθώς ο τομέας της υγειονομικής περίθαλψης θεωρείται κρίσιμη υποδομή. Σύμφωνα με τη NIS 2, τα κράτη μέλη πρέπει να διασφαλίσουν:

- Ενσωμάτωση της νομοθεσίας στα εθνικά τους δίκαια
- Στρατηγικές και δομές επιβολής
- Εποπτεία της εφαρμογής των μέτρων κυβερνοασφάλειας

Υπάρχει ωστόσο ένα βασικό πρόβλημα, το οποίο είναι η εφαρμογή σε εθνικό επίπεδο. Τα κράτη μέλη μπορεί να υιοθετήσουν διαφορετικές προσεγγίσεις, προκαλώντας νομικό κατακερματισμό και αποκλίσεις στη συμμόρφωση. Αυτό δημιουργεί προκλήσεις στην εναρμόνιση και στην εφαρμογή ομοιόμορφων προτύπων κυβερνοασφάλειας εντός της ΕΕ. [37][38][39]

Δυο νομοθετικές πρωτοβουλίες που πρέπει επίσης να ληφθούν υπόψη είναι ο Νόμος περί Ανθεκτικότητας στον Κυβερνοχώρο (Cyber Resilience Act, CRA) και ο Νόμος περί Αλληλεγγύης στον Κυβερνοχώρο (Cyber Solidarity Act, CSA)

4.2.1 CRA

Ο CRA στοχεύει στη βελτίωση και τη ρύθμιση της ασφάλειας στον κυβερνοχώρο για όλες τις συσκευές που συνδέονται στο διαδίκτυο, συμπεριλαμβανομένων τόσο των IoT συσκευών όσο και του λογισμικού. Παρότι ο MDR αποτελεί ειδική νομοθεσία για τις ιατρικές συσκευές, ο CRA θα ασκήσει επιρροή, καθώς χρησιμοποιούν παρόμοιο λογισμικό και λειτουργικά συστήματα. Ο CRA θα ενισχύσει την ανθεκτικότητα των ιατρικών συσκευών, κάτι που ο MDR αναφέρει με πιο γενικούς όρους στα παραρτήματά του. [37][38]

4.2.2 CSA

Ο CSA αποσκοπεί στην ενίσχυση της ικανότητας της ΕΕ να προλαμβάνει και να αντιμετωπίζει κυβερνοεπιθέσεις. Περιλαμβάνει τη δημιουργία της Ευρωπαϊκής Ασπίδας του Κυβερνοχώρου (European Cyber Shield, ECS), που αποτελείται από ένα δίκτυο Κέντρων Επιχειρήσεων Ασφαλείας (Security Operation Centers, SOCs) για την έγκαιρη ανίχνευση κυβερνοαπειλών, καθώς και τον Μηχανισμό Έκτακτης Ανάγκης στον Κυβερνοχώρο (Cyber Emergency Mechanism, CEM), μέσω του οποίου θα διατίθεται χρηματοδότηση για την ενίσχυση της ετοιμότητας, της αντίδρασης και της αλληλοβοήθειας σε περιπτώσεις κυβερνοεπιθέσεων. [37][38]

Με αυτά τα μέτρα η ΕΕ ενισχύει την ασφάλεια των υποδομών της και δημιουργεί μηχανισμούς γρήγορης αντίδρασης σε απειλές, κάτι που συμβάλει σημαντικά στην προστασία των ιατρικών συσκευών από κυβερνοεπιθέσεις.

4.2.3 Νόμος για Τεχνητή Νοημοσύνη

Το ρυθμιστικό πλαίσιο της ΕΕ για την κυβερνοασφάλεια των ιατρικών συσκευών βασίζεται κυρίως στις προαναφερθείσες νομοθεσίες, ωστόσο ο προτεινόμενος Νόμος για την Τεχνητή Νοημοσύνη (AI Act) αναμένεται να επηρεάσει εξίσου σημαντικά τον κλάδο. Ο AI Act αντιμετωπίζει την τεχνητή νοημοσύνη ως προϊόν και ορίζει τις υποχρεώσεις τόσο των κατασκευαστών όσο και των χρηστών, καθώς και τους αρμόδιους φορείς ελέγχου και πιστοποίησης, ακολουθώντας μια προσέγγιση παρόμοια με αυτήν που εφαρμόζεται στη ρύθμιση των προϊόντων μέσω του MDR, δημιουργώντας σύγχυση για το ποιο ρυθμιστικό πλαίσιο θα χρησιμοποιείται σε περίπτωση όπου μια ιατρική συσκευή ενσωματώνει τεχνητή νοημοσύνη.

Παρόλα αυτά, η τεχνητή νοημοσύνη στις ιατρικές συσκευές θα εξακολουθήσει να ρυθμίζεται από τον MDR, ωστόσο οι επικαλύψεις και οι πιθανές συγκρούσεις μεταξύ του MDR και του AI Act μπορεί να δημιουργήσουν παραθυράκια που θα μπορούσαν να οδηγήσουν σε παράβαση των κανονισμών. Παράδειγμα αποτελεί ότι οι προγραμματιστές ενδέχεται να προσαρμόσουν τον σκοπό ενός προϊόντος που χρησιμοποιεί τεχνητή νοημοσύνη έτσι ώστε να μην πληροί τις απαιτήσεις σύμφωνα με τον MDR, επιτρέποντάς του να υπαχθεί μόνο στο AI Act με χαμηλότερες απαιτήσεις συμμόρφωσης. [37][38]

Ο AI Act εισάγει κανόνες για τρεις κατηγορίες κινδύνου στην τεχνητή νοημοσύνη: [38]

- Τεχνητή νοημοσύνη μη αποδεκτού κινδύνου: Αφορά εφαρμογές που περιλαμβάνουν απαγορευμένες πρακτικές, όπως οι τεχνικές υποσυνείδητης επιρροής. Αυτά τα συστήματα κρίνονται ως ιδιαίτερα επικίνδυνα για τα θεμελιώδη δικαιώματα και δεν επιτρέπεται η διάθεσή τους στην αγορά ή η λειτουργία τους
- Τεχνητή νοημοσύνη περιορισμένου κινδύνου: Περιλαμβάνει εφαρμογές όπως chatbots και deepfakes, οι οποίες επιτρέπονται με συγκεκριμένες υποχρεώσεις διαφάνειας
- Τεχνητή νοημοσύνη υψηλού κινδύνου: Περιλαμβάνει συστήματα όπως το λογισμικό ιατρικών συσκευών και οι εφαρμογές τους μπορούν να διατεθούν στην αγορά μόνο εάν πληρούν τις αυστηρές απαιτήσεις του νόμου και τις προδιαγραφές κυβερνοασφάλειας

Τα συστήματα τεχνητής νοημοσύνης που δεν εμπίπτουν σε καμία από τις παραπάνω κατηγορίες θεωρούνται χαμηλού ή ελάχιστου κινδύνου. Η συμμόρφωση με τα πρότυπα των συστημάτων υψηλού κινδύνου δεν είναι υποχρεωτική, αλλά κρίνεται σωστή η τήρησή τους.

4.2.4 Γενικός Κανονισμός για την Προστασία Δεδομένων

Η κυβερνοασφάλεια των ιατρικών συσκευών συνδέεται άμεσα και με τον Γενικό Κανονισμό για την Προστασία Δεδομένων (General Data Protection Regulation, GDPR) ο οποίος προστατεύει το θεμελιώδες δικαίωμα στην ιδιωτικότητα. Ο GDPR ρυθμίζει την επεξεργασία δεδομένων μέσω αρχών προστασίας της ιδιωτικότητας, τον ορισμό υπευθύνων προστασίας δεδομένων, καθώς και τις έννοιες του υπεύθυνου επεξεργασίας και του εκτελούντος την επεξεργασία δεδομένων, διασφαλίζοντας την ασφάλεια των προσωπικών δεδομένων που διαχειρίζονται οι ιατρικές συσκευές. [37][38][39]

4.3 Νομικό σύστημα Ηνωμένων Πολιτειών Αμερικής

Στις ΗΠΑ οι ιατρικές συσκευές ρυθμίζονται σε ομοσπονδιακό επίπεδο από το άρθρο 201 του Ομοσπονδιακού Νόμου για τα Τρόφιμα, τα Φάρμακα και τα Καλλυντικά (Federal Food, Drug and Cosmetics Act). Ο αρμόδιος ρυθμιστικός φορέας είναι ο FDA ο οποίος καθορίζει εάν ένα προϊόν πληροί τις προϋποθέσεις για να θεωρηθεί ιατροτεχνολογικό και αξιολογεί τη συμμόρφωσή του με τους ισχύοντες κανονισμούς. Δεν υπάρχει συγκεκριμένο νομοθετικό πλαίσιο που να αφορά αποκλειστικά την κυβερνοασφάλεια των ιατρικών συσκευών, πέρα από ένα εκτελεστικό διάταγμα (Executive Order, EO). [37][40]

Οι ΗΠΑ ακολουθούν μια προσέγγιση εκ των προτέρων εγκρίσεων, εστιάζοντας περισσότερο στην αρχική συμμόρφωση των προϊόντων παρά στη συνεχή εποπτεία τους μετά την κυκλοφορία. Αυτό δημιουργεί μακροπρόθεσμα προβλήματα καθώς ενδέχεται να μη ληφθούν υπόψη μελλοντικά τρωτά σημεία που εμφανίζονται σε ιατρικές συσκευές κατά τη διάρκεια του κύκλου ζωής τους. Χαρακτηριστικό παράδειγμα αποτελούν συσκευές που χρησιμοποιούνται στον τομέα της υγείας, όπως έξυπνες συσκευές με αισθητήρες, βηματοδότες και αντλίες ινσουλίνης. Οι συσκευές αυτές αποτελούν μέρος ευρύτερων συστημάτων και σε αρκετές περιπτώσεις δεν λαμβάνουν τακτικές ενημερώσεις λογισμικού από τους κατασκευαστές, ώστε να διατηρηθεί χαμηλό το κόστος. Αυτό τις καθιστά όλο και πιο ευάλωτες σε κυβερνοεπιθέσεις με την πάροδο του χρόνου. Η αρχική έγκριση ενός προϊόντος από

τον FDA δεν εγγυάται μακροπρόθεσμη συμμόρφωση, εφόσον δεν υπάρχει συνεχής εποπτεία και εκ των υστέρων έλεγχος. Χωρίς τακτική συντήρηση και επιθεώρηση, η κυβερνοασφάλεια των ιατρικών συσκευών μπορεί να αποδυναμωθεί, αυξάνοντας τον κίνδυνο παραβιάσεων και επιθέσεων.

Ο FDA έχει εισαγάγει πολιτικές που σχετίζονται με τις Λειτουργίες Λογισμικού Συσκευών (Device Software Functions) και τις Κινητές Ιατρικές Εφαρμογές (Mobile Medical Applications) και μαζί με τα άρθρα 3060 και 3060α του Νόμου για τις Θεραπείες του 21ου Αιώνα (21st Century Cures Act) θέτουν απαιτήσεις κυβερνοασφάλειας, ώστε να διασφαλίζεται η ασφαλής και ορθή λειτουργία των ιατρικών συσκευών. Αυτό σημαίνει ότι η κυβερνοασφάλεια λαμβάνεται υπόψη πιο συγκεκριμένα κατά την αξιολόγηση των ιατρικών συσκευών.

Όπως και στην ΕΕ, για να χαρακτηριστεί ένα λογισμικό ως ιατροτεχνολογικό προϊόν από τον FDA, ο κατασκευαστής πρέπει να το έχει σχεδιάσει για διάγνωση, θεραπεία, μετριασμό, αποκατάσταση ή πρόληψη ασθενειών ή άλλων παθήσεων και επιπλέον η λειτουργία του πρέπει να επηρεάζει κάποια σωματική δομή ή λειτουργία. Ο FDA διατηρεί το δικαίωμα να αποφασίζει αν ένα λογισμικό αποτελεί ιατροτεχνολογικό προϊόν, ανεξάρτητα από το αν πληροί όλα τα τυπικά κριτήρια. Αυτό του επιτρέπει να ταξινομεί προϊόντα ως ιατροτεχνολογικά, ακόμα και αν δεν καλύπτονται από το άρθρο 201. Με αυτόν τον τρόπο αποτρέπεται η παραβίαση των κανονισμών από κατασκευαστές που προσπαθούν να αποφύγουν τη ρύθμιση των προϊόντων τους ως ιατρικές συσκευές.

Σε αντίθεση με τον MDR της ΕΕ, ο οποίος βασίζεται σε καθορισμένες απαιτήσεις και δίνει μεγαλύτερη ευθύνη στον κατασκευαστή για την έναρξη της διαδικασίας πιστοποίησης, η προσέγγιση του FDA θεωρείται πιο συγκεντρωτική και λιγότερο διαφανής. Μια βασική διαφορά μεταξύ των ΗΠΑ και της ΕΕ στη ρύθμιση των ιατρικών συσκευών είναι η ευρεία εξουσία του FDA. Ο οργανισμός μπορεί να αποσύρει συσκευές από την αγορά αν δεν έχουν καταχωριστεί ή αν δεν συμμορφώνονται με τις κανονιστικές απαιτήσεις. Αυτό τον καθιστά τον μοναδικό κεντρικό φορέα αποφάσεων για το ποια προϊόντα θεωρούνται ιατροτεχνολογικά στις ΗΠΑ, σε αντίθεση με την πολύπλοκη και βασισμένη στους κατασκευαστές διαδικασία της ΕΕ. Το συγκεντρωτικό σύστημα των ΗΠΑ μπορεί να περιορίσει τις προσπάθειες παράβασης από κατασκευαστές, καθώς ο FDA έχει τη δυνατότητα να ταξινομήσει περισσότερα προϊόντα ως ιατροτεχνολογικά. Ωστόσο η ευχέρεια αυτή μπορεί να οδηγήσει και σε περισσότερα μη ρυθμιζόμενα προϊόντα, όπως chatbots ή εφαρμογές παρακολούθησης που ενδέχεται να έχουν ιατρικές χρήσεις, αλλά δεν αναγνωρίζονται ως ιατροτεχνολογικά προϊόντα. Η προσέγγιση του FDA, η οποία βασίζεται σε μη δεσμευτικές κατευθυντήριες γραμμές, μπορεί να δημιουργήσει αβεβαιότητα για τους κατασκευαστές, καθώς αντί για σαφή νομοθετικά πλαίσια, πολλές αποφάσεις λαμβάνονται κατά περίπτωση. Αυτό μπορεί να καταστήσει τη διαδικασία έγκρισης πιο χρονοβόρα και δαπανηρή σε σχέση με τον MDR, ο οποίος προσφέρει μεγαλύτερη νομική σαφήνεια και προβλεψιμότητα. [37][40]

Στις ΗΠΑ η προστασία των δεδομένων και η κυβερνοασφάλεια δεν ρυθμίζονται από ένα ενιαίο ομοσπονδιακό πλαίσιο, όπως γίνεται στην ΕΕ με τον GDPR. Αντιθέτως, η νομοθεσία για την κυβερνοασφάλεια βασίζεται σε διάφορους εξειδικευμένους νόμους που καλύπτουν διαφορετικές πτυχές της προστασία δεδομένων και της ασφάλειας των πληροφοριών. Μερικοί από τους βασικούς νόμους που σχετίζονται με την κυβερνοασφάλεια στις ΗΠΑ περιλαμβάνουν: [37]

- Νόμος για το Απόρρητο των Ηλεκτρονικών Επικοινωνιών (1986) ο οποίος ρυθμίζει την παρακολούθηση και την πρόσβαση στις ηλεκτρονικές επικοινωνίες
- Νόμος για την Ασφάλεια στον Κυβερνοχώρο (2015) που επικεντρώνεται στην κοινοποίηση πληροφοριών για απειλές στον κυβερνοχώρο μεταξύ του ιδιωτικού τομέα και της κυβέρνησης

- Νόμος για την Αναφορά Περιστατικών στον Κυβερνοχώρο για Κρίσιμες Υποδομές (2022) ο οποίος απαιτεί από συγκεκριμένους οργανισμούς να αναφέρουν κυβερνοεπιθέσεις και περιστατικά ασφαλείας
- Νόμος για την Ενίσχυση της Αμερικανικής Ασφάλειας στον Κυβερνοχώρο (2022) που προβλέπει μέτρα βελτίωσης της προστασίας κρίσιμων συστημάτων και δικτύων

Σε αντίθεση με την ΕΕ, όπου η νομοθεσία για την προστασία των δεδομένων και την κυβερνοασφάλεια είναι ενιαία και αυστηρή, στις ΗΠΑ η προσέγγιση είναι αποσπασματική και βασισμένη σε ειδικές ρυθμίσεις. Αυτό μπορεί να οδηγήσει σε κενά προστασίας, καθώς η εφαρμογή των νόμων εξαρτάται από τον τομέα και τη συγκεκριμένη νομοθεσία που ισχύει για κάθε περίπτωση. [37][40]

4.4 Νομικό σύστημα Ηνωμένου Βασιλείου

Η έξοδος του Ηνωμένου Βασιλείου από την Ευρώπη ή αλλιώς Brexit, έγινε τον Ιανουάριο του 2020. Μετά το Brexit, το ρυθμιστικό πλαίσιο για τις ιατρικές συσκευές έχει πλέον διαφοροποιηθεί μεταξύ της Μεγάλης Βρετανίας (Αγγλία, Σκωτία, Ουαλία) και της Βόρειας Ιρλανδίας, σε σχέση με αυτό της ΕΕ που ακολουθούσαν. Οι βασικές διατάξεις για τις ιατρικές συσκευές στο Ηνωμένο Βασίλειο εξακολουθούν να περιλαμβάνονται στους MDR του 2002 όπως έχουν τροποποιηθεί. Υπάρχουν δύο διαφορετικές ερμηνείες αυτών των κανονισμών, μία που ισχύει για τη Μεγάλη Βρετανία και μία που ισχύει για τη Βόρεια Ιρλανδία.

Η Μεγάλη Βρετανία διατηρεί ένα καθεστώς παρόμοιο με εκείνο που ίσχυε πριν το Brexit, καθώς οι διατάξεις της αντικατοπτρίζουν τις παλαιότερες οδηγίες της ΕΕ (MDD και AIMDD). Ανεξάρτητη πλέον από την ΕΕ, η Μεγάλη Βρετανία έχει πλέον τη δυνατότητα να διαμορφώσει νέα και διαφοροποιημένη νομοθεσία στον τομέα αυτό.

Η Βόρεια Ιρλανδία αντίθετα εξακολουθεί να ακολουθεί το ρυθμιστικό πλαίσιο της ΕΕ, συμπεριλαμβανομένου του κανονισμού MDR, καθώς υπόκειται στις συμφωνίες που διέπουν τη σχέση της με την ΕΕ μετά το Brexit. [37]

Στη Μεγάλη Βρετανία, οι MDR, όπως εφαρμόζονται μετά το Brexit, δεν περιλαμβάνουν συγκεκριμένες διατάξεις για την ασφάλεια στον κυβερνοχώρο. Αυτό σημαίνει ότι η ρύθμιση της κυβερνοασφάλειας στις ιατρικές συσκευές παραμένει έμμεση και εξαρτάται από άλλες ρυθμίσεις και οδηγίες. Τροποποιήσεις στους κανονισμούς του 2002 ενδέχεται να δημιουργούν έμμεσες απαιτήσεις κυβερνοασφάλειας, ανάλογες με εκείνες του κανονισμού MDR της ΕΕ. Ειδικότερα:

- Οι κατασκευαστές πρέπει να αποδεικνύουν ότι οι συσκευές τους συμμορφώνονται με τις βασικές απαιτήσεις του κανονισμού
- Εάν μια συσκευή δεν συμμορφώνεται με τα διεθνή πρότυπα, τότε η εθνική αρχή μπορεί να απαιτήσει επιπλέον μέτρα κυβερνοασφάλειας
- Η κυβερνοασφάλεια ενδέχεται να ενσωματωθεί με έμμεσο τρόπο μέσω των απαιτήσεων συμμόρφωσης

Εκτός από τις τροποποιήσεις UK MDR 2002, η Μεγάλη Βρετανία βασίζεται επίσης:

- Στις παλαιότερες οδηγίες της ΕΕ (MDD και AIMDD)
- Σε εξειδικευμένες οδηγίες της κυβέρνησης του Ηνωμένου Βασιλείου
- Στο έγγραφο καθοδήγησης MEDDEV 2.1/6, το οποίο είναι ελλιπές σε θέματα κυβερνοασφάλειας και αφήνει μεγάλο μέρος της ρύθμισης στην ευχέρεια της κυβέρνησης

Ο κύριος κίνδυνος αυτού του συστήματος είναι η έλλειψη προληπτικών μέτρων, δηλαδή πόσο διασφαλίζεται η συμμόρφωση πριν προκληθεί ζημιά. [37]

Μετά το Brexit, η κυβέρνηση της Μεγάλης Βρετανίας ξεκίνησε μια δημόσια διαβούλευση σχετικά με την κατεύθυνση των κανονισμών για τις ιατρικές συσκευές, προσδιορίζοντας προτάσεις για πιθανές αλλαγές. Η κυβέρνηση δεσμεύτηκε να ενσωματώσει την ασφάλεια στον κυβερνοχώρο ως βασική απαίτηση, ωστόσο η δέσμευση αυτή δεν είναι επαρκώς ανεπτυγμένη σε άλλες περιοχές της κυβερνητικής απάντησης. Αυτό δημιουργεί έναν αναδυόμενο κίνδυνο για τη Μεγάλη Βρετανία, καθώς η απουσία σαφών κανόνων για την κυβερνοασφάλεια μπορεί να καταστήσει δύσκολη τη συμμόρφωση των ιατρικών συσκευών σε διεθνείς απαιτήσεις. Προκύπτουν επίσης σοβαρά προβλήματα για τις εισαγωγές και εξαγωγές καθώς:

- Οι συσκευές που αγοράζονται και διατίθενται στην αγορά της ΕΕ πρέπει να συμμορφώνονται με τους κανονισμούς της ΕΕ (MDR) και τις αυστηρές απαιτήσεις για την ασφάλεια στον κυβερνοχώρο
- Τα προϊόντα που αγοράζονται και διατίθενται στην αγορά των ΗΠΑ πρέπει να συμμορφώνονται με τις απαιτήσεις του FDA, οι οποίες συχνά συμπεριλαμβάνουν και τις απαιτήσεις της ΕΕ
- Ελάχιστα περιθώρια υπάρχουν για τη Μεγάλη Βρετανία να θεσπίσει νομοθεσία που να αποκλίνει σημαντικά από τις απαιτήσεις αυτές

Το αποτέλεσμα είναι ότι οι ιατρικές συσκευές από τη Μεγάλη Βρετανία μπορεί να βρουν προβλήματα στην αγορά λόγω των συσσωρευμένων κανονιστικών απαιτήσεων από διαφορετικές αγορές (ΕΕ και ΗΠΑ), οπότε οι εξαγωγές τους να είναι περιορισμένες. Η Μεγάλη Βρετανία θα πρέπει να επιτύχει την ευθυγράμμιση των κανόνων της με τις απαιτήσεις της ΕΕ ή των ΗΠΑ, για να διευκολύνει την εξαγωγή ιατρικών συσκευών από το Ηνωμένο Βασίλειο και να διασφαλίσει τη συμμόρφωση με τις αυστηρές διεθνείς απαιτήσεις για την ασφάλεια στον κυβερνοχώρο. Η προστασία δεδομένων στο Ηνωμένο Βασίλειο αντιμετωπίζει επίσης παρόμοιες προκλήσεις, καθώς οι κανονισμοί προστασίας δεδομένων δεν επεκτείνονται πέρα από τα προσωπικά δεδομένα, αφήνοντας κενά στην κυβερνοασφάλεια των ιατρικών συσκευών. [37]

4.5 Επίλογος

Σε αυτό το κεφάλαιο έγινε αναφορά στον τρόπο με τον οποίο τα νομικά συστήματα και τα νομικά πλαίσια της ΕΕ, των ΗΠΑ και του Ηνωμένου Βασιλείου, ρυθμίζουν την κυβερνοασφάλεια στις ιατρικές συσκευές.

Κεφάλαιο 5ο: Πρότυπα κυβερνοασφάλειας

5.1 Εισαγωγή

Στο κεφάλαιο αυτό γίνεται αναφορά στους διεθνείς οργανισμούς που παρέχουν πρότυπα κυβερνοασφάλειας που θα πρέπει να ακολουθούν οι κατασκευαστές των ιατρικών συσκευών, όπως ISO και IEC, καθώς και σε πρότυπα κυβερνοασφάλειας που έχουν θεσπιστεί από ιδιωτικούς φορείς.

5.2 ISO και IEC

Ο Διεθνής Οργανισμός Τυποποίησης (International Organization for Standardization, ISO) διαδραματίζει καθοριστικό ρόλο στη διεθνή τυποποίηση, διευκολύνοντας το εμπόριο και τη συνεργασία μεταξύ επιχειρήσεων και κρατών παγκοσμίως. Από την ίδρυσή του το 1946, έχει δημοσιεύσει χιλιάδες πρότυπα που καλύπτουν μια ευρεία γκάμα τομέων, από τη διαχείριση ποιότητας και την ασφάλεια στον κυβερνοχώρο έως τις ιατρικές συσκευές και την περιβαλλοντική διαχείριση. Τα διεθνή πρότυπα του ISO εξασφαλίζουν ότι οι επιχειρήσεις λειτουργούν με αποτελεσματικότητα και ασφάλεια, προστατεύοντας καταναλωτές και οργανισμούς. Με την ταχεία ανάπτυξη της τεχνολογίας και την παγκόσμια διασύνδεση των αγορών, η σημασία των προτύπων ISO συνεχίζει να αυξάνεται, διαμορφώνοντας ένα αποδοτικό, ασφαλές και αξιόπιστο παγκόσμιο σύστημα παραγωγής και υπηρεσιών. [41]

Η Διεθνής Ηλεκτροτεχνική Επιτροπή (International Electrotechnical Commission, IEC) είναι ένας κορυφαίος διεθνής οργανισμός τυποποίησης, που ειδικεύεται σε ηλεκτρικές και ηλεκτρονικές τεχνολογίες. Ιδρύθηκε το 1906 και παίζει κρίσιμο ρόλο στην ανάπτυξη και προώθηση προτύπων που εξασφαλίζουν την ασφάλεια, τη διαλειτουργικότητα και την αποδοτικότητα των ηλεκτροτεχνικών προϊόντων και συστημάτων σε όλο τον κόσμο. Η IEC διαχειρίζεται τέσσερα παγκόσμια συστήματα αξιολόγησης της συμμόρφωσης, τα οποία πιστοποιούν εάν ένας εξοπλισμός, σύστημα ή εξάρτημα συμμορφώνεται με τα διεθνή της πρότυπα. Αυτό διασφαλίζει την ποιότητα και την ασφάλεια των προϊόντων που χρησιμοποιούνται παγκοσμίως, ενισχύοντας την καινοτομία και το εμπόριο. [42]

5.2.1 Πρότυπα ISO και IEC για ιατρικές συσκευές

Για τη διασφάλιση της ασφάλειας και της αποτελεσματικότητας των ιατρικών συσκευών, τόσο η ΕΕ όσο και οι ΗΠΑ έχουν υιοθετήσει πρότυπα ISO και IEC για τη συμμόρφωση των συσκευών: [43]

- **IEC 62304**: Επικεντρώνεται στο λογισμικό και στις διαδικασίες του κύκλου ζωής του λογισμικού των ιατρικών συσκευών
- **IEC 62366**: Επικεντρώνεται στην εφαρμογή της μηχανικής ευχρηστίας για ιατρικές συσκευές
- **IEC 82304**: Αναφέρεται στις γενικές απαιτήσεις για την ασφάλεια των συσκευών
- **IEC 80001-1**: Εστιάζει στην εφαρμογή της διαχείρισης κινδύνου για δίκτυα πληροφορικής που ενσωματώνουν ιατρικές συσκευές
- **IEC 80001-2-8**: Παρουσιάζει ένα πλαίσιο για τη διαχείριση των τρωτών σημείων ασφαλείας των δικτυακών συσκευών και προτείνει ελέγχους
- **IEC 80002**: Παρέχει ένα πλαίσιο για την αξιολόγηση των κινδύνων κυβερνοασφάλειας που σχετίζονται με τις ιατρικές συσκευές
- **ISO 14971**: Δίνει μια προσέγγιση διαχείρισης κινδύνων με επίκεντρο το προϊόν για τον εντοπισμό κινδύνων ιατρικών συσκευών
- **ISO 13485**: Καθορίζει τις απαιτήσεις για ένα σύστημα διαχείρισης ποιότητας ειδικά σχεδιασμένο για ιατρικές συσκευές

- **ISO 60601-1 Series**: Ορίζει τις γενικές απαιτήσεις ασφαλείας και βασικών επιδόσεων για ηλεκτρικές ιατρικές συσκευές και διασφαλίζει ότι οι ιατρικές συσκευές είναι ασφαλείς τόσο για τους ασθενείς όσο και για τους χειριστές τους
- **ISO 60601-2 Series**: Περιλαμβάνει ειδικά πρότυπα για συγκεκριμένους τύπους ιατρικών συσκευών, καθορίζοντας τις επιπλέον απαιτήσεις ασφαλείας και απόδοσης ανάλογα με τη λειτουργία της κάθε συσκευής
- **ISO/DTS 11633-1**: Αφορά την ασφάλεια και την αξιοπιστία των επικοινωνιών σε δίκτυα που χρησιμοποιούνται σε ιατρικά περιβάλλοντα και εστιάζει στη διαχείριση κινδύνων και στην προστασία των δεδομένων που διακινούνται μέσω αυτών των δικτύων
- **ISO/TR 11633-2**: Συμπληρώνει το ISO/DTS 11633-1 και παρέχει κατευθυντήριες γραμμές για την εφαρμογή μέτρων ασφαλείας στις επικοινωνίες ιατρικών συσκευών και συστημάτων
- **ISO/TR 22696**: Παρέχει οδηγίες για την ταυτοποίηση και αυθεντικοποίηση συνδεδεμένων προσωπικών συσκευών υγείας και προσφέρει κατευθυντήριες γραμμές για τη διαχείριση της ασφάλειας των υπηρεσιών υγείας όταν χρησιμοποιούνται συνδεδεμένες προσωπικές συσκευές υγείας, με στόχο την προστασία των ευαίσθητων προσωπικών δεδομένων και την αποτροπή πιθανών απειλών που μπορεί να επηρεάσουν τόσο τα συστήματα υγείας όσο και την ανθρώπινη ζωή
- **ISO 27799**: Περιλαμβάνει κατευθυντήριες γραμμές για τη διαχείριση της ασφάλειας των πληροφοριών στον τομέα της υγειονομικής περίθαλψης
- **ISO 10993-x**: Καθορίζει τις διαδικασίες για τη βιολογική αξιολόγηση των ιατρικών συσκευών με στόχο την ασφάλεια και την αποτελεσματικότητά τους

5.3 Άλλα πρότυπα ιατρικών συσκευών

Πέρα από τα πρότυπα ISO και IEC, υπάρχουν και πρότυπα τα οποία ανέπτυξαν και δημοσίευσαν ιδιωτικοί οργανισμοί και αφορούν τη διαχείρισης της ασφάλειας των ιατρικών συσκευών στον κυβερνοχώρο. Τα πιο γνωστά πρότυπα είναι τέσσερα.

5.3.1 TIR57

Η Τεχνική Έκθεση Πληροφοριών 57 (Technical Information Report 57, TIR57) με τίτλο 'Αρχές για την διαχείρισης κινδύνων ασφαλείας ιατρικών συσκευών' δημοσιεύθηκε από την Ένωση για την Προώθηση των Ιατρικών Οργάνων (Association for the Advancement of Medical Instrumentation, AAMI). Η έκθεση αυτή παρέχει κατευθυντήριες γραμμές για τους μηχανικούς ιατρικών συσκευών, προκειμένου να ενσωματώσουν τη διαχείριση κινδύνων στον τομέα της κυβερνοασφάλειας στη διαδικασία ανάπτυξης της συσκευής. Οι οδηγίες αυτές τους βοηθούν να αναγνωρίζουν και να αποτρέπουν προληπτικά πιθανές απειλές πριν την κυκλοφορία της συσκευής στην αγορά. Η έκθεση προσφέρει ένα σύνολο βημάτων για τον εντοπισμό και την αξιολόγηση των κινδύνων και των τρωτών σημείων, τη διαχείριση των κινδύνων ασφαλείας, καθώς και την παρακολούθηση της αποτελεσματικότητας αυτών των ελέγχων. Το TIR57 βασίζεται στις αρχές του ISO 14971 και εστιάζει ειδικά στην ασφάλεια στον κυβερνοχώρο. Το TIR57 ανήκει στον κατάλογο αναγνωρισμένων προτύπων του FDA και σημαίνει ότι οι κατασκευαστές που τον εφαρμόζουν, πληρούν τις απαιτήσεις που έχει θέσει ο FDA για τις υποβολές πριν από την κυκλοφορία των συσκευών στην αγορά. [44]

5.3.2 UL 2900 Series

Η σειρά προτύπων UL (Underwriters Laboratories) 2900 αποτελείται από τρία αλληλένδετα έγγραφα με τίτλο "Software Cybersecurity for Network-Connectable Products". Σύμφωνα με την UL, η σειρά αυτή λειτουργεί ως ένα πλαίσιο δοκιμών που επιτρέπει στους κατασκευαστές να αποδεικνύουν αντικειμενικά τη συμμόρφωσή τους με τις απαιτήσεις του FDA για την κυβερνοασφάλεια των ιατρικών

συσκευών. Παρέχει επαναλαμβανόμενα κριτήρια δοκιμών, τα οποία εστιάζουν στον εντοπισμό των ευπαθειών μιας συσκευής, την αντιμετώπιση κακόβουλου λογισμικού και τη δοκιμή των μέτρων ασφαλείας. Από πλευράς ελέγχου προϊόντος, το UL 2900 απαιτεί την πλήρη χαρτογράφηση όλων των διεπαφών και καναλιών επικοινωνίας του προϊόντος, ενώ επιβάλλει την εφαρμογή μέτρων διαχείρισης κινδύνου σύμφωνα με καθιερωμένες αρχές, όπως αυτές του TIR57. Το πρότυπο βασίζεται σε ήδη υπάρχοντα πρότυπα και διαδικασίες, ενσωματώνοντας το πλαίσιο κυβερνοασφάλειας του NIST, γεγονός που το καθιστά συμβατό με άλλα πρότυπα όπως το DTSec που θα εξεταστεί στη συνέχεια. Το UL 2900 απαιτεί την αξιολόγηση των προϊόντων έναντι όλων των γνωστών τρωτών σημείων, σύμφωνα με την Εθνική Βάση Δεδομένων Τρωτών Σημείων (National Vulnerability Database, NVD) και τα πρότυπα CYBEX της Διεθνούς Ένωσης Τηλεπικοινωνιών (International Telecommunications Union, ITU). Το UL 2900-1, που αφορά τις γενικές απαιτήσεις, εγκρίθηκε από το Αμερικανικό Ινστιτούτο Εθνικών Προτύπων (American National Standards Institute, ANSI) ως εθνικό πρότυπο συναίνεσης και το 2017 προστέθηκε στον κατάλογο των αναγνωρισμένων προτύπων του FDA. [44]

5.3.3 DTSec

Το 2016, η Diabetes Technology Society (DTS) ανέπτυξε το πρώτο πρότυπο κυβερνοασφάλειας ευρείας συναίνεσης με συγκεκριμένες απαιτήσεις επιδόσεων για ιατρικές συσκευές. Ονομάστηκε DTSec (DTS Cybersecurity Standard for Connected Diabetes Devices) και περιλαμβάνει τόσο κριτήρια επιδόσεων όσο και μέτρα διασφάλισης. Ο βασικός σκοπός του είναι η ενίσχυση της εμπιστοσύνης στην ασφάλεια των διασυνδεδεμένων ιατρικών συσκευών μέσω ανεξάρτητων αξιολογήσεων από ειδικούς στον τομέα της ασφάλειας. Παρόλο που σχεδιάστηκε αρχικά για συσκευές διαχείρισης τους διαβήτη, το DTSec μπορεί να εφαρμοστεί και σε άλλες ιατρικές συσκευές, συμβάλλοντας στην προστασία κρίσιμων συστημάτων υψηλής αξίας. Το 2017, οι οργανισμοί IEEE (Institute of Electrical and Electronics Engineers) και UL υπέγραψαν συμφωνία κοινής ανάπτυξης προτύπων με στόχο της δημιουργία ενός προτύπου συναίνεσης για την ασφάλεια ασύρματων συσκευών διαβήτη, βασισμένου στο DTSec. Η DTS παρέδωσε το πρότυπο στους δύο αυτούς φορείς και στόχος της συνεργασίας τους είναι η εξέλιξη του προτύπου σε εθνικό επίπεδο, ώστε να καλύπτει όλες τις ιατρικές συσκευές και η αναγνώρισή του ως διεθνές πρότυπο. [44]

5.3.4 DTMoSt

Το 2017 η DTS ξεκίνησε την ανάπτυξη του δεύτερου προτύπου κυβερνοασφάλειας με την ονομασία DTMoSt (Diabetes Technology Society Mobile Platform Security and Safety Standard). Ένα αρχικό προσχέδιο του προτύπου δημοσιεύτηκε στις αρχές του 2018 για δημόσια διαβούλευση. Το DTMoSt βασίζεται στις αρχές του DTSec, εστιάζοντας στην ασφαλή χρήση κινητών τηλεφώνων για τον έλεγχο φορητών ή εμφυτεύσιμων συσκευών διαβήτη. Η ενσωμάτωση των κινητών τηλεφώνων στη διαδικασία αυτή απαιτεί ιδιαίτερη προσοχή, καθώς οι πολλαπλές λειτουργίες τους και οι εφαρμογές που εκτελούν, καταναλώνουν σημαντική υπολογιστική ισχύ και επηρεάζουν τη διαθεσιμότητα πόρων. Ο έλεγχος φυσιολογικών διεργασιών που μεταβάλλονται γρήγορα σε πραγματικό χρόνο μέσω κινητού τηλεφώνου μπορεί να επιβαρύνει το λειτουργικό σύστημα, αυξάνοντας τον κίνδυνο δυσλειτουργίας, με πιθανώς σοβαρές συνέπειες για τους διαβητικούς ασθενείς. Η υιοθέτηση διασυνδεδεμένων ιατρικών συσκευών αυξάνεται και αυτό σημαίνει ότι οι επαγγελματίες υγείας που συνταγογραφούν και επιβλέπουν τη χρήση τους, θα χρειάζονται όλο και περισσότερο διαβεβαίωση για την σωστή κυβερνοασφάλειά τους. Το DTMoSt στοχεύει στην παροχή εγγυήσεων ότι τα κινητά τηλέφωνα μπορούν να ελέγχουν με ασφάλεια συσκευές διαβήτη, συμβάλλοντας στην προστασία των ασθενών και στη βελτίωση της αξιοπιστίας αυτών των τεχνολογιών. [44]

5.4 Επίλογος

Σε αυτό το κεφάλαιο έγινε αναφορά στα πρότυπα κυβερνοασφάλειας που θα πρέπει να ακολουθούν οι κατασκευαστές των ιατρικών συσκευών. Αυτά τα πρότυπα θεσπίζονται είτε από διεθνείς οργανισμούς, όπως ISO και IEC, είτε από ιδιωτικούς φορείς, όπως TIR57, UL2900, DTSec και DTMoSt.

Κεφάλαιο 6ο: Ευπάθειες κυβερνοασφάλειας ιατρικών συσκευών

6.1 Εισαγωγή

Σε αυτό κεφάλαιο γίνεται αναφορά στις ευπάθειες κυβερνοασφάλειας των ιατρικών συσκευών. Παρουσιάζονται τα επίπεδα ευπαθειών στις ιατρικές συσκευές και οι κύριες ευπάθειες στις ιατρικές συσκευές και στη νοσηλεία. Περιγράφονται πως οι αστοχίες υλικού και τα σφάλματα λογισμικού επηρεάζουν στις ιατρικές συσκευές, αναλύονται περιπτώσεις επιθέσεων που εκμεταλλεύτηκαν συγκεκριμένες ευπάθειες ιατρικών συσκευών και εξετάζονται τρόποι για τον μετριασμό των ευπαθειών.

6.2 Επίπεδα ευπαθειών ιατρικών συσκευών

Οι πρόσφατες τεχνολογικές εξελίξεις έχουν επιφέρει σημαντικές αλλαγές στον τομέα στις υγειονομικής περίθαλψης, με τη δυνατότητα να αναβαθμίσουν την ποιότητα στις φροντίδας των ασθενών. Ενδεικτικό παράδειγμα είναι η αυξανόμενη διασυνδεσιμότητα μεταξύ ιατρικών συσκευών και άλλων κλινικών συστημάτων. Παρόλο που αυτή η συνδεσιμότητα βελτιώνει την αποδοτικότητα των υπηρεσιών υγείας και τη ροή των πληροφοριών, παράλληλα καθιστά στις ιατρικές συσκευές ευάλωτες σε κυβερνοεπιθέσεις. Σε αντίθεση με τα περισσότερα δικτυωμένα συστήματα πληροφορικής, η διασυνδεσιμότητα ων ιατρικών συσκευών εγείρει αυξημένες ανησυχίες καθώς ενδέχεται να επηρεάσει άμεσα την ποιότητα στις κλινικής φροντίδας και την ασφάλεια των ασθενών. Με την αυξημένη διασύνδεση, εμφανίζονται και νέες ευπάθειες στις ιατρικές συσκευές. Οι ευπάθειες αυτές χωρίζονται σε κατηγορίες. [45]

Η κατηγοριοποίηση των επιπέδων των ευπαθειών κυβερνοασφάλειας στις ιατρικές συσκευές βασίζεται στην κρισιμότητά στις, δηλαδή στη σοβαρότητα στις επίπτωσης που μπορεί να έχει μια κυβερνοεπίθεση στη λειτουργικότητα στις συσκευής και στην ασφάλεια του ασθενούς. Δεν βασίζεται σε ένα μοναδικό παγκόσμιο πρότυπο, αλλά ακολουθείται από οργανισμούς και προδιαγραφές που σχετίζονται με τη διαχείριση κινδύνων στην κυβερνοασφάλεια των ιατρικών συσκευών, στις ο FDA, το NIST και το ISO 14971. Τα επίπεδα αυτά είναι τέσσερα και διακρίνονται στις παρακάτω κατηγορίες: [45]

- **Χαμηλό**: Υπάρχει μικρή πιθανότητα εκμετάλλευσης από στις επιτιθέμενους και η πιθανή παραβίαση επηρεάζει μόνο μη κρίσιμα δεδομένα ή λειτουργίες (στις διαρροή μη ευαίσθητων δεδομένων). Η ευπάθεια δεν επηρεάζει άμεσα την υγεία του ασθενούς. Παραδείγματα ευπαθειών χαμηλού επιπέδου αποτελούν οι μη ασφαλείς κωδικοί πρόσβασης σε βοηθητικές λειτουργίες και η διαρροή μη κρυπτογραφημένων αρχείων καταγραφής που δεν περιέχουν προσωπικά δεδομένα. Πιθανά μέτρα αντιμετώπισης ευπαθειών αυτού του επιπέδου είναι η τακτική ενημέρωση του λογισμικού και των ρυθμίσεων ασφαλείας, καθώς και η αλλαγή κωδικών πρόσβασης και η ενίσχυση πολιτικών ελέγχου ταυτότητας.
- **Μέτριο**: Υπάρχει αυξημένη πιθανότητα εκμετάλλευσης από στις επιτιθέμενους και η πιθανή παραβίαση δίνει πρόσβαση σε προσωπικά δεδομένα ασθενών. Επηρεάζει στις τη λειτουργία στις συσκευής, αλλά όχι κρίσιμες λειτουργίες που σχετίζονται με τη ζωή του ασθενούς. Παραδείγματα ευπαθειών μέτριου επιπέδου αποτελούν η ανεπαρκής προστασία ασυρμάτων συνδέσεων, η χρήση αδύναμων αλγορίθμων κρυπτογράφησης και οι ευπάθειες που επιτρέπουν μη εξουσιοδοτημένη πρόσβαση σε δεδομένα χρήστη. Για την αντιμετώπιση τέτοιων ευπαθειών, είναι απαραίτητη η χρήσης ισχυρής κρυπτογράφησης για την προστασία των δεδομένων, η ενίσχυση του ελέγχου ταυτότητας και η διάγνωση ευπαθειών μέσω penetration testing.
- **Υψηλό**: Είναι πολύ πιθανή η εκμετάλλευση από στις επιτιθέμενους και μπορεί να οδηγήσει σε σημαντικές παραβιάσεις ευαίσθητων δεδομένων ασθενών. Υπάρχει στις δυνατότητα παρεμβολής σε κρίσιμες λειτουργίες στις συσκευής, γεγονός που αυξάνει τον κίνδυνο για την υγεία του ασθενούς. Παραδείγματα τέτοιων ευπαθειών είναι το SQL injection που τροποποιεί και διαγράφει ιατρικά δεδομένα, οι ευπάθειες που επιτρέπουν την απομακρυσμένη

τροποποίηση ρυθμίσεων στις συσκευής και η μη εξουσιοδοτημένη πρόσβαση σε συσκευές που ρυθμίζουν δόσεις φαρμάκων και στις κρίσιμες λειτουργίες. Για την αντιμετώπιση ευπαθειών αυτού του επιπέδου, χρειάζεται αυστηρότερη διαχείριση ταυτοποίησης χρηστών και ελέγχου πρόσβασης, ανίχνευση εισβολών στο δίκτυο και πιστοποίηση συμμόρφωσης με τα πρότυπα κυβερνοασφάλειας, στις ISO 27799.

- **Πολύ υψηλό**: Υπάρχει άμεσος κίνδυνος για τη ζωή του ασθενούς και μια πιθανή επίθεση μπορεί να οδηγήσει σε πλήρη δυσλειτουργία στις συσκευής. Οι επιτιθέμενοι έχουν τη δυνατότητα ελέγχου ζωτικής σημασίας ιατρικών λειτουργιών και υπάρχει στις κίνδυνος για πιθανή μαζική επίθεση ransomware. Παραδείγματα τέτοιων ευπαθειών αποτελούν η ανασφαλής απομακρυσμένη πρόσβαση σε εμφυτεύσιμες συσκευές, ενημερώσεις λογισμικού χωρίς επαλήθευση στις γνησιότητάς στις και εκτεθειμένες διασυνδέσεις σε δίκτυα χωρίς ισχυρή κρυπτογράφηση. Για την αντιμετώπισή στις, χρειάζεται αυστηρή πολιτική ασφαλείας και ελέγχων για στις ενημερώσεις λογισμικού, απομόνωση των κρίσιμων ιατρικών συσκευών από δημόσια δίκτυα και η ανάπτυξη στρατηγικών αποκατάστασης (Disaster Recovery).

6.3 Ευπάθειες ιατρικών συσκευών και ιατρικού τομέα

Οι ευπάθειες των ιατρικών συσκευών είναι κρίσιμος τομέας που απαιτεί ιδιαίτερη προσοχή, καθώς οι κυβερνοεπιθέσεις μπορούν να θέσουν σε σοβαρό κίνδυνο τη σωστή λειτουργία των ιατρικών συσκευών, την προστασία των ευαίσθητων δεδομένων των ασθενών και την ασφάλεια των ασθενών. Παρακάτω μελετώνται οι κύριες ευπάθειες που υπάρχουν στις ιατρικές συσκευές και στον ιατρικό τομέα.

6.3.1 Ευπάθειες ιατρικών συσκευών

Οι παρακάτω ευπάθειες αφορούν τόσο σε σταθερές όσο σε φορητές και εμφυτεύσιμες. [45][46][47][48]

Η **μη ασφαλής αποθήκευση και μετάδοση δεδομένων** στις ιατρικές συσκευές και κυρίως στις εμφυτεύσιμες, είναι καίρια ευπάθεια. Οι ιατρικές συσκευές καταγράφουν και αποθηκεύουν κρίσιμες ιατρικές πληροφορίες, όπως επίπεδα γλυκόζης και καρδιακούς παλμούς. Εάν δεν χρησιμοποιείται ισχυρή κρυπτογράφηση, τότε υπάρχει κίνδυνος διαρροής και παραποίησης αυτών των δεδομένων, γεγονός που μπορεί να οδηγήσει σε λανθασμένη διάγνωση ή επικίνδυνη παρέμβαση στη θεραπεία του ασθενούς.

Η **έλλειψη ισχυρού μηχανισμού ταυτοποίησης και εξουσιοδότησης** σε πολλές ιατρικές συσκευές, οι οποίες δεν διαθέτουν αυστηρούς ελέγχους ταυτότητας πριν συνδεθούν σε εξωτερικά συστήματα, μπορεί να επιτρέψει σε μη εξουσιοδοτημένους χρήστες να αποκτήσουν πρόσβαση και να τροποποιήσουν κρίσιμες ρυθμίσεις της συσκευής, θέτοντας σε κίνδυνο την ασφάλεια και την υγεία των ασθενών.

Πολλές εμφυτεύσιμες ιατρικές συσκευές παρουσιάζουν **αδυναμία ασφαλών ενημερώσεων λογισμικού**, καθώς υποστηρίζουν καθόλου ενημερώσεις λογισμικού είτε τις εκτελούν χωρίς κατάλληλη κρυπτογράφηση και διαδικασίες επαλήθευσης της αυθεντικότητας της ενημέρωσης. Η αδυναμία αυτή μπορεί να επιτρέψει την εγκατάσταση κακόβουλου λογισμικού, εκθέτοντας τη συσκευή σε σοβαρούς κινδύνους ασφαλείας.

Πολλές ιατρικές συσκευές διαθέτουν **παλαιάς τεχνολογίας λογισμικό και λειτουργικό σύστημα**. Οι συσκευές αυτές δεν αναβαθμίζονται ποτέ με αποτέλεσμα το λογισμικό τους να μένει παρωχημένο και να δημιουργείται ασυμβατότητα μεταξύ συστημάτων. Με αυτόν τον τρόπο δημιουργούνται τρωτά σημεία, όπως λανθασμένες ρυθμίσεις και κενά ασφαλείας.

Οι εμφυτεύσιμες ιατρικές συσκευές παρουσιάζουν **ευπάθειες στα πρωτόκολλα ασύρματης επικοινωνίας**, καθώς επικοινωνούν με εξωτερικές συσκευές μέσω τεχνολογιών όπως RFID και Wi-Fi. Εάν τα πρωτόκολλα αυτά είναι μη ασφαλή ή δε διαθέτουν κρυπτογράφηση, κακόβουλοι χρήστες μπορούν να υποκλέψουν ή να τροποποιήσουν τα δεδομένα, δημιουργώντας με αυτόν τον τρόπο

σοβαρούς κινδύνους για την ακεραιότητα και την ασφάλεια της συσκευής. Σε περίπτωση χρήσης ραδιοσυχνοτήτων, υπάρχει χαμηλή πιθανότητα επιτυχίας μιας επίθεσης, καθώς η επίθεση θα πρέπει να γίνει σε κοντινή απόσταση, όμως η επιτυχής σάρωση μιας ραδιοσυχνότητας μπορεί να δώσει τη δυνατότητα ανάγνωσης και εγγραφής οποιασδήποτε έγκυρης θέσης μνήμης στη συσκευή. Σε περίπτωση επικοινωνίας μέσω Wi-Fi, ο επιτιθέμενος θα μπορούσε να καταγράψει τα πακέτα ανταλλαγής δεδομένων και να εξαγάγει ευαίσθητες πληροφορίες, όπως τους σειριακούς αριθμούς συσκευών.

Ορισμένες ιατρικές συσκευές διαθέτουν **χαμηλή επεξεργαστική ισχύς και περιορισμένους πόρους ασφάλειας**, διότι είναι σχεδιασμένες για μέγιστη ενεργειακή αποδοτικότητα και μακροχρόνια λειτουργία, γεγονός που περιορίζει την ικανότητά τους να υποστηρίζουν ισχυρούς μηχανισμούς κρυπτογράφησης και προηγμένες τεχνικές ανίχνευσης απειλών. Αυτό τις καθιστά ευάλωτες, καθώς δε μπορούν εύκολα να εφαρμόσουν σύγχρονα μέτρα ασφαλείας που απαιτούν υψηλή υπολογιστική ισχύ.

Πολλές ιατρικές συσκευές παρουσιάζουν **απουσία μηχανισμών ανίχνευσης ύποπτης δραστηριότητας και αυτοάμυνας**. Στηρίζονται αποκλειστικά στη χειροκίνητη παρακολούθηση από τον χρήστη ή τον γιατρό, γεγονός που αυξάνει τον κίνδυνο καθυστερημένης αντίδρασης σε πιθανές απειλές.

Αρκετές ιατρικές συσκευές έχουν **ανεπαρκείς προδιαγραφές ασφαλείας στο στάδιο του σχεδιασμού**, καθώς αναπτύσσονται με προτεραιότητα τη λειτουργικότητα και την ευχρηστία, ενώ η ασφάλεια παραμελείται αρκετά συχνά. Η απουσία αρχών ασφαλείας κατά το σχεδιασμό της συσκευής μπορεί να οδηγήσει σε σοβαρά κενά ασφαλείας, αφήνοντας τις συσκευές εκτεθειμένες σε επιθέσεις που θα μπορούσαν να είχαν προβλεφθεί και αποτραπεί από το στάδιο του σχεδιασμού.

Η **φυσική ασφάλεια των συσκευών** αποτελεί κρίσιμο παράγοντα για τη διατήρηση της διαθεσιμότητας και της αξιόπιστης λειτουργίας τους. Παραβιάσεις όπως κλοπή, μη εξουσιοδοτημένη πρόσβαση ή ηλεκτρομαγνητική παρεμβολή μπορούν να διαταράξουν τη λειτουργία μιας συσκευής, ακόμη κι αν οι προστασίες είναι επαρκείς. Τέτοιες παρεμβάσεις ενδέχεται να προκαλέσουν διακοπή της επικοινωνίας, απώλεια δεδομένων ή ακατάλληλη λειτουργία της συσκευής με δυνητικά σοβαρές συνέπειες για την υγεία του ασθενούς. Απαιτούνται μέτρα όπως ασφαλής τοποθέτηση, περιορισμένη φυσική πρόσβαση και προστασία από κινδύνους του περιβάλλοντος.

6.3.2 Ευπάθειες στη νοσηλεία

Οι βασικές ευπάθειες κατά τη διάρκεια της νοσηλείας στα νοσοκομεία και στις κλινικές είναι οι ακόλουθες: [47][48]

- Ευπάθειες web server: Όλες οι νοσοκομειακές μονάδες χρησιμοποιούν web servers για τη διαχείριση και την επικοινωνία δεδομένων. Ωστόσο, οι servers αυτοί ενδέχεται να περιέχουν αδυναμίες, όπως ελλιπής έλεγχος εισόδου, μη ασφαλής διαχείριση συνεδριών ή παρωχημένες βιβλιοθήκες. Τέτοιες αδυναμίες μπορούν να εντοπιστούν και να αξιοποιηθούν πολύ εύκολα από τους επιτιθέμενους.
- Ζητήματα ασφάλειας βάσεων δεδομένων: Τόσο τα νοσοκομεία όσο και οι ιατρικές συσκευές αξιοποιούν βάσεις δεδομένων, βασισμένες στην SQL, για την αποθήκευση και επεξεργασία ευαίσθητων ιατρικών πληροφοριών. Αν οι βάσεις αυτές δεν έχουν σωστά διαμορφωμένα μέτρα ασφαλείας, γίνονται ευάλωτες σε SQL injection επιθέσεις, επιτρέποντας έτσι σε κακόβουλους χρήστες να αποκτήσουν πρόσβαση, να αλλοιώσουν ή να διαγράψουν κρίσιμα δεδομένα, θέτοντας σε κίνδυνο την ακεραιότητα, την εμπιστευτικότητα και τη διαθεσιμότητα της πληροφορίας που σχετίζεται άμεσα με την υγεία του ασθενούς.
- Λανθασμένα διαχειριζόμενες ασύρματες συνδέσεις: Η αυξημένη χρήση ασύρματων τεχνολογιών για τη μετάδοση δεδομένων μεταξύ ιατρικών συστημάτων και συσκευών, ενισχύει την έκθεση σε κυβερνοεπιθέσεις. Όταν τα δίκτυα του νοσοκομείου ή της κλινικής δεν

προστατεύονται επαρκώς με ισχυρά μέτρα ασφαλείας, όπως κρυπτογράφηση και έλεγχος ταυτότητας, ή γίνεται παραμέληση των ενημερώσεων και των ρυθμίσεών τους, οι επιτιθέμενοι μπορούν να παρακολουθήσουν, να αλλοιώσουν και να κλέψουν δεδομένα.

- Ανεπαρκείς πρακτικές κυβερνοασφάλειας: Πολλοί φορείς υγειονομικής περίθαλψης δεν εφαρμόζουν ενοποιημένες και τυποποιημένες πολιτικές ασφάλειας, γεγονός που οδηγεί σε ασυνέπεια στα επίπεδα προστασίας μεταξύ των συστημάτων και των συσκευών. Η απουσία καθορισμένων πρωτοκόλλων για την ανίχνευση, την ανταπόκριση και την πρόληψη κυβερνοαπειλών καθιστά τα περιβάλλοντα αυτά ευάλωτα σε κυβερνοεπιθέσεις.
- Έλλειψη εκπαίδευσης του προσωπικού και συστηματικής παρακολούθησης κινδύνων: Ενισχύει την πιθανότητα παραβιάσεων ασφαλείας που θα μπορούσαν να επηρεάσουν τα ιατρικά δεδομένα, καθώς το προσωπικό της ιατρικής μονάδας δεν είναι εξοικειωμένο με τον εξοπλισμό και το λογισμικό που διαθέτει η μονάδα.
- Κίνδυνοι από τρίτους προμηθευτές: Πολλοί υγειονομικοί φορείς εξαρτώνται από εξωτερικούς προμηθευτές για την παροχή λογισμικού, τεχνικής υποστήριξης και κρίσιμων υπηρεσιών. Αν αυτοί οι τρίτοι δεν εφαρμόζουν αυστηρές πολιτικές κυβερνοασφάλειας, μπορούν άθελά τους να λειτουργήσουν ως δίαυλοι εισόδου για κακόβουλες επιθέσεις. Οι ευπάθειες στα συστήματα των προμηθευτών μπορούν να χρησιμοποιηθούν για την παράκαμψη των εσωτερικών μηχανισμών προστασίας του νοσοκομείου, προκαλώντας παραβιάσεις δεδομένων, διακοπές λειτουργίας και υπονόμευση της εμπιστοσύνης των ασθενών.

6.4 Βλάβες υλικού και σφάλματα λογισμικού

Μια γενική αστοχία υλικού μπορεί να επηρεάσει τόσο τα ηλεκτρονικά όσο και τα μη ηλεκτρονικά εξαρτήματα μιας ιατρικής συσκευής. Τέτοιες αποτυχίες μπορεί να οφείλονται σε μη ορατά κατασκευαστικά ελαττώματα ή φαινόμενα φθοράς. Παράλληλα, παροδικά σφάλματα μπορεί να προκληθούν από περιβαλλοντικούς παράγοντες, όπως ηλεκτρικός θόρυβος, διακυμάνσεις τάσης, ακραίες θερμοκρασίες, κραδασμοί και ηλεκτρομαγνητικές παρεμβολές. [49]

Οι ηλεκτρομαγνητικές παρεμβολές μπορούν να προκαλέσουν είτε παροδική διαταραχή είτε μόνιμη δυσλειτουργία σε κρίσιμες συσκευές όπως οι απινιδωτές και οι βηματοδότες, γεγονός που ενισχύει την ανάγκη για αυστηρότερο σχεδιασμό και προστασία των συστημάτων από τέτοια φαινόμενα. Μια δυσλειτουργία σε έναν βηματοδότη ή έναν απινιδωτή μπορεί να αποδειχθεί θανατηφόρα. Το ίδιο ισχύει και για συσκευές νευροδιαμόρφωσης, όπως αυτές που χρησιμοποιούνται για τη νόσο του Parkinson και για την επιληψία. Οι συσκευές αυτές απαιτούν εξαιρετικά υψηλό επίπεδο αξιοπιστίας και αντοχής καθώς επηρεάζουν άμεσα τη λειτουργία του εγκεφάλου. Παράδειγμα αποτελεί το σύστημα βαθιάς εγκεφαλικής διέγερσης της Medtronic, στο οποίο εμφυτεύονται ηλεκτρόδια στον εγκέφαλο που συνδέονται με έναν νευροδιεγέρτη. Αυτός ο διεγέρτης μπορεί να προγραμματιστεί εξωτερικά. Παρόλα αυτά, ισχυρές ηλεκτρομαγνητικές παρεμβολές ενδέχεται να τροποποιήσουν τις παραμέτρους, να απενεργοποιήσουν το σύστημα και να προκαλέσουν απρόσμενες ηλεκτρικές διεγέρσεις, κάτι που μπορεί να οδηγήσει σε ανεπιθύμητες σωματικές αντιδράσεις.

Η αξιοπιστία του λογισμικού είναι το ίδιο σημαντική με εκείνη του υλικού, ειδικά στις εμφυτεύσιμες ιατρικές συσκευές, οι οποίες βασίζονται σε ένα μεγάλο βαθμό στο ενσωματωμένο λογισμικό τους. Είναι γνωστή η δυσκολία του σχεδιασμού ενός λογισμικού χωρίς καθόλου σφάλματα, ειδικά στην περίπτωση πολύπλοκων συσκευών που καλούνται να λειτουργήσουν σε συνθήκες που δεν μπορούν πάντα να προβλεφθούν. Το πιο ανησυχητικό γεγονός είναι ότι πολλά από τα σφάλματα δεν εμφανίζονται στη φάση των δοκιμών, αλλά κάνουν την εμφάνισή τους αφού τεθεί σε χρήση η συσκευή.

Μία στις τέσσερις ανακλήσεις ιατρικών συσκευών κατά το πρώτο μισό του 2010 φαίνεται πως οφείλονταν σε προβλήματα λογισμικού. Μέχρι σήμερα δεν υπάρχει μια κοινώς αποδεκτή τεχνική ή μεθοδολογία για την ανάπτυξη ή την αξιόπιστη επαλήθευση του λογισμικού που χρησιμοποιείται σε

ιατρικές συσκευές. Ο FDA έχει την ευθύνη να αξιολογεί τους κινδύνους που ενέχουν οι καινούργιες συσκευές και να παρακολουθεί την ασφάλεια και αποτελεσματικότητά τους μετά την κυκλοφορία τους στην αγορά. Ωστόσο ο έλεγχος του εστιάζει κυρίως στη διαδικασία ανάπτυξης του λογισμικού και όχι στο λογισμικό ως τελικό προϊόν. [49]

6.5 Εκμετάλλευση ευπαθειών

Παρακάτω γίνεται ανάλυση πάνω στις ευπάθειες που μπορεί να εκμεταλλευτεί ένας επιτιθέμενος ανάλογα την κατηγορία και τον τύπο της ιατρικής συσκευής. [15][48][49]

6.5.1 Σταθερές ιατρικές συσκευές

- Μηχανήματα ακτινογραφίας και μαγνητικής τομογραφίας: Ευπάθειες όπως το μη ενημερωμένο λογισμικό, έλλειψη μηχανισμού αυθεντικοποίησης, έλλειψη anti-virus και μη κρυπτογραφημένα δεδομένα οδηγούν σε μη εξουσιοδοτημένη πρόσβαση και σε επιθέσεις όπως το spoofing, το ransomware και το man-in-the-middle.
- Αξονικός τομογράφος: Έλλειψη μηχανισμού αυθεντικοποίησης, εργοστασιακοί κωδικοί πρόσβασης που δεν έχουν αλλαχτεί και το μη ενημερωμένο ή παλιό λειτουργικό σύστημα μπορούν να οδηγήσουν σε επιθέσεις όπως Ransomware, DOS και σε μη εξουσιοδοτημένη πρόσβαση.
- Μηχάνημα αναισθησίας και αναπνευστήρας : Παλιό λειτουργικό σύστημα και εργοστασιακοί κωδικοί πρόσβασης οδηγούν σε μη εξουσιοδοτημένη πρόσβαση, DOS και Ransomware.
- Συστήματα και λογισμικά ιατρικής απεικόνισης: Οι εργοστασιακοί κωδικοί πρόσβασης που δεν έχουν αλλαχτεί μπορούν να οδηγήσουν σε μη εξουσιοδοτημένη πρόσβαση και αποκάλυψη πληροφοριών.
- Αναλυτής αερίων αίματος: Η έλλειψη κρυπτογράφησης και μηχανισμού αυθεντικοποίησης μπορούν να οδηγήσουν σε αποκάλυψη ή παραποίηση πληροφοριών και μη εξουσιοδοτημένη πρόσβαση.

6.5.2 Φορητές ιατρικές συσκευές

- Smartwatch και Apple watch: Οι μη κρυπτογραφημένες συνδέσεις λόγω της αμεταποίητης διεύθυνσης MAC του BLE και το αδύναμο σύστημα ασφαλείας με βάση το κλειδί μπορεί να οδηγήσουν σε αλλοίωση των δεδομένων.
- Xiaomi MiBand: Η έλλειψη μηχανισμών ελέγχου ταυτότητας και η μη ενσωμάτωση του απορρήτου του πρωτοκόλλου επικοινωνίας ενδέχεται να οδηγήσουν σε αλλοίωση ή αποκάλυψη δεδομένων.
- Huawei Talkband: Η έλλειψη κρυπτογράφησης, ελέγχου ταυτότητας και ακεραιότητας οδηγούν σε αποκάλυψη δεδομένων και τροποποίηση firmware.
- Ανιχνευτής δραστηριότητας εγκεφάλου: Η αδύναμη κρυπτογράφηση δεδομένων, οι ευπάθειες στο firmware και ο ανεπαρκής έλεγχος πρόσβασης ενδέχεται να επιτρέψουν στον επιτιθέμενο να παραβιάσει και να συλλέξει ευαίσθητα δεδομένα του ασθενούς και να κάνει επιθέσεις τύπου ransomware.
- Αισθητήρας πτώσης και εντοπισμού: Η έλλειψη κρυπτογράφησης, οι ευπάθειες στους τρόπους επικοινωνίας (Wi-Fi, BLE), ο ανεπαρκής έλεγχος ταυτότητας και η έλλειψη φυσικής προστασίας μπορεί να οδηγήσουν σε παραβίαση και υποκλοπή δεδομένων και επιθέσεις όπως spoofing και sniffing.
- Φορητά συστήματα παρακολούθησης εγκυμοσύνης: Τα κενά ασφαλείας στην αποθήκευση δεδομένων, η ελλιπής φυσική ασφάλεια, η έλλειψη κρυπτογράφησης και οι ευπάθειες σε πρωτόκολλα επικοινωνίας μπορεί να οδηγήσουν σε επιθέσεις τύπου man-in-the-middle, sniffing, spoofing και σε εκμετάλλευση των ευαίσθητων ιατρικών δεδομένων.

6.5.3 Εμφυτεύσιμες ιατρικές συσκευές

- Απινιδωτής: Η έλλειψη μηχανισμού ελέγχου ταυτότητας, κρυπτογράφησης και ακεραιότητας, καθώς και ένα ελάττωμα κατά την υλοποίηση της συσκευής το οποίο τη διατηρεί σε κατάσταση αναμονής και επιτρέπει στον επιτιθέμενο να παρέμβει από κοντινή απόσταση στη συσκευή, μπορούν να οδηγήσουν σε επιθέσεις όπως DOS, spoofing, παραποίηση, υποκλοπή και αποκάλυψη δεδομένων.
- Αντλία ινσουλίνης: Η απουσία μηχανισμού πρόληψης κατά επιθέσεων DOS και η έλλειψη μηχανισμού κρυπτογράφησης λόγω της οποίας τα μηνύματα μεταδίδονται σε απλό κείμενο, οδηγούν σε επιθέσεις όπως DOS, man-in-the-middle, υποκλοπή δεδομένων και μη εξουσιοδοτημένη πρόσβαση.
- Βηματοδότης: Η έλλειψη κρυπτογράφησης και ελέγχου ταυτότητας, οι βλάβες στο υλικό και τα σφάλματα στο λογισμικό, η ανεπαρκής επαλήθευση της αυθεντικότητας των δεδομένων και η μεταφορά των πακέτων ως απλό κείμενο οδηγούν σε υποκλοπή, παραποίηση και αποκάλυψη δεδομένων και επιθέσεις παρεμβολής.
- Καρδιακό μόνιτορ: Οι βλάβες υλικού και τα σφάλματα λογισμικού, η έλλειψη επαρκούς κρυπτογράφησης και η ανεπαρκής επαλήθευση της αυθεντικότητας των δεδομένων οδηγούν σε παραποίηση και υποκλοπή δεδομένων, επιθέσεις παρεμβολής και μη εξουσιοδοτημένη πρόσβαση.
- Βιοαισθητήρες (όπως επιταχυνσιόμετρο): Η έλλειψη κρυπτογράφησης και μηχανισμού ελέγχου ταυτότητας οδηγούν σε επιθέσεις τύπου spoofing και sniffing καθώς και σε υποκλοπή και παραποίηση δεδομένων.
- Γαστρικός ηλεκτρικός διεγέρτης: Η έλλειψη μηχανισμού ελέγχου ταυτότητας και κρυπτογράφησης, καθώς και βλάβες στο υλικό και σφάλματα στο λογισμικό της συσκευής, μπορούν να οδηγήσουν σε υποκλοπή και αποκάλυψη δεδομένων, καθώς και επιθέσεις παρεμβολής.
- Συσκευές χορήγησης φαρμάκων: Η έλλειψη μηχανισμού ελέγχου ταυτότητας οδηγεί σε επιθέσεις όπως man-in-the-middle, μη εξουσιοδοτημένη πρόσβαση, υποκλοπή και αποκάλυψη δεδομένων.
- Νευροδιεγέρτης: Η έλλειψη κρυπτογράφησης, η παράληψη ενημερώσεων λογισμικού και οι ευπάθειες στα πρωτόκολλα επικοινωνίας οδηγούν σε επιθέσεις spoofing, DOS και υποκλοπή δεδομένων.

6.6 Μετριασμός ευπαθειών

Υπάρχουν διάφορα πιθανά εργαλεία, μέτρα και ενέργειες μετρίασης των ευπαθειών των ιατρικών συσκευών: [50]

Η **τμηματοποίηση δικτύου και το τείχος προστασία** αποτελούν απαραίτητα εργαλεία για τη μείωση του κινδύνου εκμετάλλευσης ευπαθειών, καθώς πλέον οι περισσότερες επιθέσεις γίνονται εξ αποστάσεως και δεν απαιτούν υψηλό επίπεδο τεχνικής πολυπλοκότητας. Ένα πολύ σημαντικό μέτρο όπου παίζουν καθοριστικό ρόλο αυτά τα δύο εργαλεία, είναι ο περιορισμός της πρόσβασης σε κρίσιμα συστήματα μόνο σε εξουσιοδοτημένο προσωπικό. Η εφαρμογή όμως τέτοιων μέτρων δεν είναι εφικτή πάντα, καθώς υπάρχουν περιπτώσεις όπου η ιατρική συσκευή ενημερώνει το λογισμικό και τη βάση δεδομένων της απευθείας μέσω διαδικτύου χωρίς να χρειάζεται φυσική παρέμβαση, όπως επίσης έχουν σχεδιαστεί ιατρικές συσκευές ώστε να χρησιμοποιούνται και εκτός νοσοκομείου από τους ίδιους τους ασθενείς.

Είναι απαραίτητη η **βελτίωση της αποδοτικότητας στις διαδικασίες ανάκλησης**. Η ανάκληση ιατρικών συσκευών είναι πολύπλοκη διαδικασία που απαιτεί συντονισμένη επικοινωνία μεταξύ κατασκευαστών, παρόχων υγειονομικής περίθαλψης και ασθενών. Πολλές φορές παρουσιάζονται καθυστερήσεις και ασυνέπειες σε αυτή την αλυσίδα, ειδικά όταν προκύπτουν δυσκολίες στον εντοπισμό των υπεύθυνων για την απομάκρυνση των προϊόντων από τα αποθέματα των νοσοκομείων. Παρόλο

που οι κατασκευαστές εντοπίζουν γρήγορα τις περισσότερες συσκευές που χρειάζονται ανάκληση, η διαδικασία αυτή μπορεί να διαρκέσει μήνες και απαιτεί συνεχής επικοινωνία με παρόχους ή διανομείς. Ένα τέτοιο χαρακτηριστικό παράδειγμα αποτελεί η ανάκληση κάποιων μοντέλων αναπνευστήρων, που θεωρήθηκε απαραίτητη καθώς υπήρχαν κίνδυνοι για την υγεία των ασθενών. Η ανάκληση ξεκίνησε δυο μήνες μετά την ανίχνευση του προβλήματος, αλλά ακόμη και δυο χρόνια μετά την έναρξη της διαδικασίας, σχεδόν εννιά χιλιάδες συσκευές δεν επιστράφηκαν, σύμφωνα με στοιχεία του κατασκευαστή.

Οι κατασκευαστές πρέπει να **ενεργούν σύμφωνα με τον κανονισμό**. Ήδη οι κυβερνήσεις προσπαθούν να επιβάλουν στους κατασκευαστές ιατρικών συσκευών να δώσουν μεγαλύτερη έμφαση στην κυβερνοασφάλεια των συσκευών, τόσο πριν όσο και μετά τη διάθεσή τους στην αγορά. Υπάρχουν κανονισμοί που το επιβάλουν αυτό τόσο στις ΗΠΑ όσο και στην ΕΕ, με τον πιο γνωστό να είναι ο CRA της ΕΕ. Ο CRA θα απαιτεί από τις εταιρείες να εφαρμόζουν πιο αυστηρά μέτρα, όπως διαδικασίες ανίχνευσης και διόρθωσης ευπαθειών και ασφαλείς ενημερώσεις λογισμικού.

Σημαντική είναι η **ενίσχυση της ασφάλειας μέσω προτύπων**, καθώς η αξιοποίηση αναγνωρισμένων προτύπων παίζει καθοριστικό ρόλο τόσο στην πρόληψη όσο και στην αποφυγή κυβερνοαπειλών, ειδικότερα όταν αυτές προέρχονται από ανεπαρκή σχεδιασμό των ίδιων των προϊόντων. Χαρακτηριστικό παράδειγμα αποτελεί η περίπτωση μιας αντλίας έγχυσης ινσουλίνης, όπου διαπιστώθηκε ότι δεν είχε κανένα μηχανισμό ελέγχου ταυτότητας, αφήνοντάς την πλήρως εκτεθειμένη. Πρότυπα όπως τα IEC και τα ISO μπορούν να βοηθήσουν στην ενίσχυση της ασφάλειας καθώς και στον εντοπισμό γνωστών ευπαθειών.

Κρίσιμο ρόλο παίζει η **διαφάνεια στην εφοδιαστική αλυσίδα λογισμικού**. Η αυξανόμενη εξάρτηση από το λογισμικό κάνει πιο σημαντική τη διαφάνεια στην αλυσίδα εφοδιασμού του. Οι κυβερνήσεις υιοθετούν πρωτοβουλίες που στοχεύουν στην παρακολούθηση των εξαρτήσεων λογισμικού, ώστε να μειώνονται οι κίνδυνοι και να είναι πιο άμεση η αντιμετώπιση πιθανών απειλών. Χαρακτηριστικό παράδειγμα αυτής της προσπάθειας είναι το SBOM (Software Bill of Materials) το οποίο είναι μια αναλυτική λίστα με όλα τα στοιχεία λογισμικού που χρησιμοποιούνται σε ένα προϊόν. Από το 2023 και έπειτα, οι κατασκευαστές ιατρικών συσκευών είναι υποχρεωμένοι να αποστέλλουν το SBOM στον FDA.

Η **χρήση και αξιοποίηση εργαλείων ελέγχου ασφάλειας λογισμικού** ή αναλυτών κώδικα, είναι ένα βήμα για τη βελτίωση της ποιότητας του λογισμικού που χρησιμοποιείται στις ιατρικές συσκευές. Είτε πρόκειται για κατασκευαστές, είτε για ερευνητικά κέντρα ή οργανισμούς υγείας, αυτά τα εργαλεία μπορούν να εντοπίσουν σφάλματα και ευπάθειες νωρίς, πριν επηρεάσουν την ασφάλεια των χρηστών. Με την άνοδο και την εξέλιξη της τεχνητής νοημοσύνης, αναμένεται οι τεχνολογίες αυτές να γίνουν ακόμη πιο αποτελεσματικές και χρήσιμες.

Η **ευαισθητοποίηση** είναι ένα πρόβλημα πληροφόρησης. Όταν η πληροφόρηση είναι υπερβολικά μεγάλη ή πολύ γενική, γίνεται δύσκολο να εστιάσει κάποιος στις πραγματικά σημαντικές πτυχές. Υπάρχει όλο και μεγαλύτερη ανάγκη για λύσεις που προσφέρουν περιεκτική αλλά στοχευμένη ενημέρωση, ειδικά σχεδιασμένη ώστε να είναι κατανοητή από το διοικητικό και το μη τεχνικό προσωπικό.

6.7 Επίλογος

Στο κεφάλαιο αυτό έγινε αναφορά στα επίπεδα ευπαθειών των ιατρικών συσκευών και έγινε ανάλυση των κύριων ευπαθειών τόσο των ιατρικών συσκευών όσο της νοσηλείας γενικότερα. Παρουσιάστηκαν οι βλάβες υλικού και τα σφάλματα λογισμικού και αναλύθηκαν οι ευπάθειες που μπορούν να

εκμεταλλευτούν οι επιτιθέμενοι ανάλογα με το είδος της ιατρικής συσκευής. Καταγράφηκαν μέτρα και ενέργειες για τον μετριασμό των ευπαθειών των ιατρικών συσκευών.

Κεφάλαιο 7ο: Επιθέσεις κυβερνοασφάλειας ιατρικών συσκευών

7.1 Εισαγωγή

Στο κεφάλαιο αυτό γίνεται ανάλυση των επιθέσεων έναντι ιατρικών συσκευών. Γίνεται αναφορά στο κίνητρο των επιτιθέμενων καθώς και στους τύπους επιτιθέμενων και στις κατηγορίες επιθέσεων. Αναλύονται οι στόχοι των επιθέσεων και τα είδη των επιθέσεων τόσο στις ιατρικές συσκευές όσο και στα συστήματα των ιατρικών μονάδων. Παρουσιάζεται η μεθοδολογία STRIDE για την κατανόηση των απειλών των ιατρικών συσκευών.

7.2 Κίνητρα επιθέσεων

Οι κυβερνοεπιθέσεις έναντι του τομέα υγείας και των ιατρικών συσκευών έχουν αυξηθεί δραματικά τα τελευταία χρόνια. Λόγω αυτών των επιθέσεων, έχει αποδυναμωθεί η ασφάλεια των δικτύων στους χώρους υγείας και έχουν προκληθεί σοβαρές οικονομικές ζημιές. Πέρα όμως των οικονομικών συνεπειών, οι επιθέσεις έχουν άμεσο αντίκτυπο στην υγεία και την περίθαλψη των ασθενών, καθώς καθυστερούν θεραπείες, εκθέτουν ευαίσθητα ιατρικά δεδομένα, προκαλούν δυσλειτουργίες και ρίχνουν ακόμη και ολόκληρο το σύστημα του νοσοκομείου. Για να προβούν σε αυτές τις ενέργειες, οι επιτιθέμενοι έχουν κάποια κίνητρα που τους ωθούν να παρεμποδίζουν την ομαλή λειτουργία των ιατρικών συσκευών και του ιατρικού τομέα γενικότερα: [51]

- Οικονομικός εκβιασμός: Το πιο συνηθισμένο κίνητρο αποτελεί το οικονομικό. Ο επιτιθέμενος κλειδώνει μια συσκευή ή και ολόκληρο το σύστημα του νοσοκομείου και απαιτεί χρήματα για να το ξεκλειδώσει. Τη διαδικασία αυτή την φέρνει εις πέρας με τη βοήθεια του κακόβουλου λογισμικού ransomware. Δεδομένου ότι πολλές από τις συσκευές είναι κρίσιμες για τις ζωές των ανθρώπων και οι ζωές τους βρίσκονται σε κίνδυνο χωρίς αυτές, πολλά νοσοκομεία και ασθενείς αναγκάζονται να πληρώσουν τα λύτρα για να επαναφέρουν τη συσκευή και τα συστήματα στην κανονική τους λειτουργία.
- Κλοπή προσωπικών και ευαίσθητων ιατρικών δεδομένων: Οι ιατρικές συσκευές καταγράφουν και αποθηκεύουν προσωπικές και ευαίσθητες πληροφορίες, όπως ιστορικά, διαγνώσεις και βιομετρικά δεδομένα. Οι πληροφορίες αυτές μπορούν να πουληθούν στη μαύρη αγορά για ένα πολύ μεγάλο ποσό ή να χρησιμοποιηθούν για ταυτότητες κλοπής.
- Κατασκοπεία ή τεχνολογική κλοπή: Όταν σε ένα περιστατικό εμπλέκονται κυβερνητικοί ή επιχειρηματικοί φορείς, οι κυβερνοεπιθέσεις μπορεί να έχουν ως στόχο την υποκλοπή τεχνολογικών ή ερευνητικών δεδομένων. Ως παράδειγμα μπορεί να αποτελέσει μια εμφυτεύσιμη συσκευή υψηλής τεχνολογίας, η οποία είναι ελκυστικός στόχος για κρατικά υποστηριζόμενους χάκερ, οι οποίοι επιδιώκουν να αποκτήσουν πρόσβαση σε βιομηχανικά μυστικά ή ευαίσθητα κλινικά δεδομένα, ενισχύοντας έτσι τον ανταγωνισμό ή και ακόμα την γεωπολιτική επιρροή.
- Σαμποτάζ: Οι κυβερνοεπιθέσεις δεν είναι όλες υποκινούμενες από οικονομικά συμφέροντα. Σε αρκετές περιπτώσεις, ο στόχος είναι η αποσταθεροποίηση του συστήματος υγείας. Ένας χάκερ μπορεί να επιχειρήσει να θέσει εκτός λειτουργίας κρίσιμες υποδομές, προκαλώντας πανικό ή και ακόμη κίνδυνο για τις ζωές των ασθενών. Συνήθως πίσω από τέτοιες ενέργειες κρύβονται ιδεολογικά, πολιτικά ή τρομοκρατικά κίνητρα. Χαρακτηριστικό παράδειγμα αποτελεί η κυβερνοεπίθεση στο πανεπιστημιακό νοσοκομείο του Ντίσελντορφ το 2020, η οποία προκάλεσε τον πρώτο γνωστό θάνατο ασθενούς λόγω καθυστερημένης φροντίδας, μετά από κυβερνοεπίθεση.
- Επέκταση επίθεσης σε ολόκληρο το δίκτυο: Μια ιατρική συσκευή συχνά αποτελεί τον πιο αδύναμο κρίκο στην αλυσίδα ασφάλειας ενός ευρύτερου συστήματος. Οι επιτιθέμενοι στοχεύουν τις ιατρικές συσκευές ως σημεία εισόδου για να διεισδύσουν στο δίκτυο ενός οργανισμού. Από εκεί μπορούν να κινηθούν προς άλλες κρίσιμες υποδομές, όπως οι

διακομιστές νοσοκομείων, τα οικονομικά συστήματα ή τα συστήματα αποθήκευσης ιατρικών δεδομένων.

7.3 Τύποι επιτιθέμενων και κατηγορίες επιθέσεων

Οι επιθέσεις στις ιατρικές συσκευές προέρχονται από δύο βασικές κατηγορίες επιτιθέμενων: τους ενεργητικούς και τους παθητικούς. [3][52]

7.3.1 Ενεργητικοί επιτιθέμενοι

Οι ενεργητικοί επιτιθέμενοι έχουν τη δυνατότητα να υποκλέπτουν την επικοινωνία μεταξύ συσκευών, του δικτυακού ελεγκτή (network controller) και των επιτηρητών. Μπορούν να επαναλαμβάνουν, να παραποιούν ή να εισάγουν μηνύματα και να στέλνουν ψευδείς εντολές, θέτοντας σε κίνδυνο την ομαλή λειτουργία της συσκευής. Σε περίπτωση που επιτύχουν, δεν παραβιάζουν μόνο την ιδιωτικότητα των ασθενών, αλλά υπάρχει και ενδεχόμενο να σταλούν λανθασμένες ιατρικές ενέργειες, όπως η χορήγηση φαρμάκου χωρίς λόγο ή η αποτυχία ειδοποίησης του ιατρικού προσωπικού σε ιδιαίτερα κρίσιμες καταστάσεις. Η ανίχνευση ενός ενεργητικού επιτιθέμενου είναι αρκετά πιθανή, αλλά οι επιπτώσεις που μπορεί να έχει μια επιτυχής επίθεση είναι καταστροφικές.

7.3.2 Παθητικοί επιτιθέμενοι

Οι παθητικοί επιτιθέμενοι περιορίζονται στην παρακολούθηση της επικοινωνίας, δεν επεμβαίνουν δηλαδή άμεσα στη λειτουργία της συσκευής. Έχουν ως στόχο να αποκτήσουν πρόσβαση σε ευαίσθητα και προσωπικά δεδομένα μέσω κρυπτογραφικής ανάλυσης, χωρίς να επηρεάσουν τη λειτουργία των συσκευών και χωρίς να γίνουν αντιληπτοί από το σύστημα. Παρόλο που είναι πιο διακριτικοί, παραμένουν εξίσου επικίνδυνοι στο κομμάτι της παραβίασης της ιδιωτικότητας. Η ανίχνευση ενός παθητικού επιτιθέμενου είναι πολύ δύσκολη και η κύρια επίπτωση που έχουν οι επιθέσεις τους είναι η διαρροή δεδομένων.

7.3.3 Κατηγορίες επιθέσεων

Υπάρχουν πέντε διαφορετικές κατηγορίες επιθέσεων, από τις οποίες οι τέσσερις αποτελούν ενεργητικές επιθέσεις και η μία μόνο παθητική επίθεση, σύμφωνα με την Εικόνα 12: [52]

	Attack class				
Entity	Destroy	Reprogram	Disturb	Denial of service	Eavesdrop
Coordinator	✓	✓	✓	✓	
Medical device	✓	✓	✓	✓	
Network	✓		✓	✓	✓
Alarm system	✓	✓	✓	✓	

Εικόνα 12 Κατηγορίες επιθέσεων

- Καταστροφή (Destroy) : Οι επιθέσεις αυτής της κατηγορίας έχουν άμεσο αντίκτυπο, καταστρέφοντας ή διακόπτοντας τη λειτουργία της συσκευής και των συστημάτων. Στόχος των επιθέσεων αυτής της κατηγορίας είναι η άμεση πρόκληση βλάβη, είτε μέσω χειραγώγησης του εξοπλισμού είτε μέσω φυσικής καταστροφής. Χαρακτηριστικό παράδειγμα αποτελεί η πρόκληση ζημιάς σε μια αντλία έγχυσης φαρμάκου, όπως η κοπή ή αποσύνδεση του σωλήνα μετάδοσης του φαρμάκου, που θα μπορούσε να σταματήσει τη θεραπεία του ασθενούς και να έχει σοβαρές κλινικές συνέπειες.

- Επαναπρογραμματισμός (Reprogram) : Στην κατηγορία αυτή ο επιτιθέμενος τροποποιεί κρίσιμα δεδομένα ή τον κώδικα λειτουργίας μιας συσκευής, με στόχο την αλλοίωση της προκαθορισμένης συμπεριφοράς. Παράδειγμα αποτελεί μια αντλία έγχυσης φαρμάκου η οποία μπορεί να επαναπρογραμματιστεί ώστε να χορηγεί μεγαλύτερη δόση φαρμάκου από την προβλεπόμενη, έχοντας έτσι επικίνδυνες συνέπειες για τον ασθενή. Η συγκεκριμένη κατηγορία επιθέσεων μπορεί να πραγματοποιηθεί είτε τοπικά, μέσω φυσικής πρόσβασης στη συσκευή, είτε εξ αποστάσεων, εάν η συσκευή υποστηρίζει δυνατότητες προγραμματισμού μέσω δικτύου.
- Διαταραχή (Disturb) : Σε αυτή την κατηγορία επιθέσεων, ο επιτιθέμενος στοχεύει στην τροποποίηση των δεδομένων που ανταλλάσσονται ή είναι διαθέσιμα εντός του περιβάλλοντος διαλειτουργικότητας, επηρεάζοντας τη σωστή λειτουργία των ιατρικών συσκευών. Οι επιτιθέμενοι μέσω επιθέσεων, όπως επίθεση επανάληψης (replay attack) ή επίθεση man-in-the-middle, μπορούν να εισάγουν τροποποιημένα ή ψευδή δεδομένα, να παραποιήσουν εντολές ή να ανακατευθύνουν την επικοινωνία. Αποτέλεσμα αυτών είναι η σύγχυση του συστήματος ή η λήψη λανθασμένων αποφάσεων που φέρουν επιπτώσεις στην ασφάλεια και την υγεία του ασθενούς.
- Άρνηση παροχής υπηρεσιών (Denial of service): Σε αυτή την κατηγορία, οι επιτιθέμενοι αποσκοπούν στην παρεμπόδιση της ομαλής λειτουργίας ενός συστήματος, στοχεύοντας κυρίως το δίκτυο, αλλά επηρεάζοντας παράλληλα και τις ιατρικές συσκευές. Μέσω καταχρηστικής χρήσης λειτουργιών ή υπερφόρτωσης πόρων, οι επιτιθέμενοι μπορούν να προκαλέσουν προσωρινή ή μόνιμη αδυναμία παροχής υπηρεσιών. Παράδειγμα αποτελεί η εκτέλεση εντολών που υπερφορτώνουν μια αντλία έγχυσης φαρμάκων, οδηγώντας την στο να καταστραφεί και καθιστώντας τη συσκευή μη λειτουργική για θεραπευτικούς σκοπούς.
- Υποκλοπές (Eavesdrop) : Η μόνη κατηγορία παθητικών επιθέσεων. Επικεντρώνεται στην παθητική παρακολούθηση της επικοινωνίας εντός του δικτύου των εμφυτεύσιμων ιατρικών συσκευών, με στόχο την άντληση ευαίσθητων ή ιατρικών πληροφοριών. Σε αντίθεση με τις άλλες κατηγορίες, οι υποκλοπές δεν αφήνουν εμφανή ίχνη και πολλές φορές παραμένουν αόρατες για μεγάλα χρονικά διαστήματα, γεγονός που καθιστά ιδιαίτερα δύσκολο τον εντοπισμό και την αντιμετώπισή τους. Οι επιπτώσεις που έχουν στην ιδιωτικότητα των ασθενών και στην ασφάλεια των δεδομένων είναι δυνητικά σοβαρές, παρά τη σιωπηλή φύση τους.

7.4 Ομάδες στόχων των επιτιθέμενων

Οι επιτιθέμενοι μπορούν να στοχεύσουν σε τέσσερις κύριες ομάδες στόχων όταν επιδιώκουν να διαταράξουν την ομαλή λειτουργία των ιατρικών συσκευών και των ιατρικών συστημάτων: [3]

Μια από τις βασικές ομάδες στόχων είναι η **σωματική ασφάλεια και ακεραιότητα του ασθενούς**, ώστε να προκληθεί βλάβη ή κίνδυνος για τη ζωή του. Οι επιθέσεις στοχεύουν κρίσιμα λειτουργικά σημεία του συστήματος των ιατρικών συσκευών, όπως η επεξεργασία δεδομένων, η επικοινωνία και η ενεργοποίηση λειτουργιών. Παραδείγματα τέτοιων επιθέσεων αποτελούν η χορήγηση υπερβολικής δόσης φαρμάκου μέσω τροποποιημένης εντολής στη συσκευή, παραποίηση του λογισμικού, παρέμβαση σε εμφυτεύσιμες συσκευές όπως ο βηματοδότης και τροποποίηση των ηλεκτρονικών ιατρικών φακέλων ώστε να εμφανίζονται παραπλανητικά στοιχεία για την κατάσταση της υγείας του ασθενούς

Η **ασφάλεια των δεδομένων των ασθενών** αποτελεί κι αυτή μια από τις βασικές ομάδες στόχων των επιτιθέμενων, καθώς επιδιώκεται η απόκτηση πρόσβασης στα προσωπικά δεδομένα υγείας ενός ασθενή χωρίς την απαιτούμενη εξουσιοδότηση. Παραβιάσεις τέτοιου είδους μπορούν να έχουν σοβαρές συνέπειες, καθώς οδηγούν σε διακρίσεις, εκβιασμούς ή κατάχρηση των πληροφοριών, όπως η άρνηση παροχής υπηρεσιών σε άτομα που πάσχουν από συγκεκριμένες παθήσεις. Η παραβίαση των δεδομένων του ασθενή μπορεί να γίνει με διάφορους τρόπους όπως η ανάκτηση δεδομένων που παραμένουν αποθηκευμένα σε ιατρικές συσκευές χωρίς να γίνει η διαγραφή τους μετά τη χρήση, μη

εξουσιοδοτημένη πρόσβαση στα ιατρικά αρχεία από το προσωπικό για κακόβουλη πρόθεση και κλοπή και κατάχρηση ιατρικών δεδομένων με στόχο την υποβολή ψευδών αιτήσεων ασφάλισης.

Η φυσική ασφάλεια των ιατρικών συσκευών αποτελεί έναν ακόμα βασικό στόχο, καθώς περιλαμβάνει τόσο τις συσκευές όσο και τα δικτυακά στοιχεία που τις υποστηρίζουν. Οι επιτιθέμενοι προκαλούν άρνηση παροχής υπηρεσιών, καθιστώντας τις συσκευές ανίκανες να εκτελέσουν τις λειτουργίες τους. Πέρα από τη διακοπή λειτουργίας, άλλες συνέπειες τέτοιων επιθέσεων είναι η απώλεια ιδιωτικότητας και η φυσική καταστροφή της συσκευής. Παραδείγματα αποτελούν η μεταφόρτωση κακόβουλου υλικολογισμικού σε αντλίες έγχυσης φαρμάκων, μέσω απομακρυσμένης ενημέρωσης, το οποίο αλλάζει κρίσιμες παραμέτρους και η κατανάλωση πόρων καθώς μια συσκευή μπορεί να δεχτεί συνεχή ερωτήματα με σκοπό να εξαντληθεί η μπαταρία της και να την καταστήσει μη λειτουργική σε κρίσιμες στιγμές.

Η **ασφάλεια δεδομένων και η προστασία του απορρήτου** αποτελούν ακόμη έναν κρίσιμο στόχο για τους επιτιθέμενους, καθώς οι επιθέσεις γίνονται στο ίδιο το ιατρικό ίδρυμα και στις δομές πληροφορικής που υποστηρίζουν τα συστήματα ιατρικών συσκευών. Σε αντίθεση με τις επιθέσεις που αφορούν μεμονωμένους ασθενείς, εδώ οι επιτιθέμενοι επιδιώκουν την ευρεία πρόσβαση σε ιατρικά δεδομένα ή λειτουργικές πληροφορίες του οργανισμού, μέσω παραβίασης της αλληλεπίδρασης μεταξύ του συστήματος των συσκευών και του εσωτερικού δικτύου του ιδρύματος. Συνέπειες αυτών των επιθέσεων είναι η παραβίαση δεδομένων μεγάλου πλήθους ασθενών, η αποσταθεροποίηση των λειτουργιών του δικτύου, η υπονόμευση εμπιστοσύνης προς το φορέα υγείας και η παραβίαση κανονιστικών απαιτήσεων περί απορρήτου. Μερικά παραδείγματα επιθέσεων αποτελούν η ανάλυση δικτυακής κίνησης που αποκαλύπτει συσχετίσεις μεταξύ ασθενών και υψηλής συχνότητας ανεπιθύμητων ιατρικών συμβάντων, παθητική παρακολούθηση ασύρματου δικτύου που αποκαλύπτει ευπάθειες συγκεκριμένης μάρκας ιατρικής συσκευής και η επίθεση άρνησης παροχής υπηρεσιών στο δίκτυο του νοσοκομείου που διακόπτει κρίσιμες υπηρεσίες. [3]

7.5 Είδη επιθέσεων ιατρικών συσκευών

Το **ransomware** αποτελεί μια από τις πιο διαδεδομένες και επικίνδυνες μορφές κυβερνοεπιθέσεων. Το κακόβουλο αυτό λογισμικό κλειδώνει την πρόσβαση σε συστήματα ή δεδομένα απαιτώντας από το θύμα την καταβολή λύτρων για την αποκατάσταση της πρόσβασης. Εάν το θύμα αρνηθεί να πληρώσει, διατρέχει κίνδυνο μόνιμης απώλειας των δεδομένων του ή παρατεταμένης διακοπής των λειτουργιών της συσκευής. Μπορεί να θέσει εκτός λειτουργίας κρίσιμες ιατρικές συσκευές, να παραλύσει ολόκληρα δίκτυα και να καθυστερήσει θεραπείες, κάτι το οποίο θα θέσει σε κίνδυνο ανθρώπινες ζωές. Στην περίπτωση εμφυτεύσιμης συσκευής, κινδυνεύει άμεσα η ζωή του ασθενή, καθώς η παύση της λειτουργίας της συσκευής, οδηγεί τις περισσότερες φορές τον ασθενή σε θάνατο. Παράδειγμα επιτυχούς ransomware επίθεσης αποτελεί η επίθεση που έγινε τον Αύγουστο του 2024 στην κλινική McLaren Health Care, όπου η κλινική αναγκάστηκε να διακόψει εντελώς τη λειτουργία των ιατρικών συσκευών της μέχρι τη διευθέτηση του προβλήματος, αφήνοντας τους ασθενείς χωρίς πρόσβαση στις υπηρεσίες φροντίδας τους. Οι γενικές επιπτώσεις που φέρουν οι ransomware επιθέσεις είναι η μη διαθεσιμότητα αρχείων υγείας, η απενεργοποίηση ιατρικών συσκευών, η υπονομευμένη ακρίβεια και αξιοπιστία των δεδομένων και το οικονομικό κόστος για την αποκατάσταση και την αποπληρωμή των λύτρων. [4]

Οι επιθέσεις **DoS** και **DDoS** αποτελούν συχνή μορφή κυβερνοεπιθέσεων, κατά τις οποίες ο επιτιθέμενος κατακλύζει την ιατρική συσκευή με υπερβολική κίνηση, με στόχο να την καταστήσει μη διαθέσιμη για τον χρήστη και τον ασθενή. Μια πιο εξειδικευμένη μορφή DoS είναι η επίθεση εξάντλησης πόρων, η οποία εκμεταλλεύεται τη χαμηλή ενέργεια που έχει η μπαταρία της ιατρικής συσκευής και έχει ως στόχο

να εξαντλήσει τη μπαταρία ή τους υπολογιστικούς πόρους της συσκευής μέσω συνεχούς αποστολής αιτημάτων ή παρεμβολών και επαναλαμβανόμενων ενεργοποιήσεων λειτουργιών. Η απενεργοποίηση της συσκευής, ιδιαίτερα αν είναι φορητή ή εμφυτεύσιμη, όπως αντλία ινσουλίνης, απινιδωτής και βηματοδότης, φέρει σοβαρές συνέπειες καθώς μπορεί να διακόψει κρίσιμες λειτουργίες της συσκευής, θέτοντας έτσι τη ζωή του ασθενούς σε κίνδυνο. Το 2018 παρουσιάστηκε στο συνέδριο Black Hat από τους ερευνητές Billy Rios και Jonathan Butts το πώς μπορεί ένας επιτιθέμενος να απενεργοποιήσει εξ αποστάσεως μια εμφυτεύσιμη αντλία ινσουλίνης της Medtronic, εμποδίζοντάς την να χορηγήσει την απαραίτητη δόση ινσουλίνης στο ασθενή. Οι ίδιοι ερευνητές απέδειξαν ότι μπορούσαν να αναλάβουν τον πλήρη έλεγχο ενός βηματοδότη, εγκαθιστώντας κακόβουλο λογισμικό στη συσκευή. Μπορούσαν με αυτόν τον τρόπο να αποστείλουν εντολές που ενεργοποιούσε ή απενεργοποιούσε το ηλεκτροσόκ της συσκευής, διακόπτοντας έτσι τη θεραπευτική της λειτουργία. [4] [15] [49] [53]

Η επίθεση **τροποποίησης υλικολογισμικού** αφορά την παραποίηση του λογισμικού χαμηλού επιπέδου που είναι αποθηκευμένο στη μη πτητική μνήμη μιας ιατρικής συσκευής, συνήθως φορητής και ελέγχει την αλληλεπίδραση του λογισμικού με το υλικό. Ο επιτιθέμενος μπορεί να εισάγει κακόβουλο κώδικα ώστε να εκτελεί μη προγραμματισμένες εντολές και να εγκαθιστά παλαιότερη έκδοση υλικολογισμικού που είναι πιο ευάλωτη σε άλλες επιθέσεις. Μια τέτοια επίθεση σε αντλία ινσουλίνης θα μπορούσε να την επηρεάσει με τέτοιο τρόπο, ώστε να δίνει λανθασμένη δόση στον ασθενή και να βάζει τη ζωή του έτσι σε κίνδυνο. Το 2018 ο FDA εξέδωσε μια προειδοποίηση για κάποιες συσκευές της Medtronic όπου επικοινωνούσαν ασύρματα με απινιδωτές και βηματοδότες. Οι συσκευές αυτές δεν επαλήθευαν ψηφιακά την αυθεντικότητα του υλικολογισμικού που λάμβαναν κατά τη διάρκεια ενημερώσεων, δίνοντας έτσι ευκαιρία σε ενδεχόμενους επιτιθέμενους να πραγματοποιήσουν μη εξουσιοδοτημένες ενημερώσεις υλικολογισμικού μέσω ασύρματης επικοινωνίας. Η Medtronic έδρασε άμεσα κλειδώνοντας τις καινούριες ενημερώσεις που ήταν να γίνουν στις συγκεκριμένες συσκευές και προκειμένου να γίνουν αυτές οι ενημερώσεις, ένας τεχνικός της Medtronic θα έπρεπε με μια συσκευή USB να τις εγκαταστήσει από κοντά. [15] [54]

Η **υποκλοπή** (eavesdropping) αναφέρεται στη μη εξουσιοδοτημένη πρόσβαση σε ευαίσθητες προσωπικές πληροφορίες των χρηστών σε πραγματικό χρόνο. Αποτελεί κρίσιμη απειλή, καθώς μπορεί να αποτελέσει σημείο εισόδου για την εκτέλεση περαιτέρω επιθέσεων, που θα μπορούσαν να αποτελέσουν άμεσο κίνδυνο στον ασθενή. Τεχνολογίες όπως το BLE και το RF είναι ιδιαίτερα ευάλωτες στην υποκλοπή, καθώς και εμφυτεύσιμες συσκευές που χρησιμοποιούν αυτές τις τεχνολογίες, φορητές ιατρικές συσκευές και συσκευές που χρησιμοποιούν στατική διεύθυνση MAC. Οι επιτιθέμενοι μπορούν να αποσπάσουν πληροφορίες όπως η κατάσταση της υγείας του ασθενούς, προσωπικά δεδομένα και τους κωδικούς μια συσκευής, τους οποίους μπορούν να τους χρησιμοποιήσουν σε μεταγενέστερη επίθεση. Το 2008 μια ερευνητική ομάδα από τα πανεπιστήμια του Ουάσιγκτον και της Μασαχουσέτης χρησιμοποίησαν ένα παλιό απινιδωτή, τον οποίο ανέλυσαν σε συνθήκες εργαστηρίου. Χρησιμοποιώντας το λογισμικό defined radio και εργαλεία υποκλοπής, κατάφεραν να υποκλέψουν ασύρματα ευαίσθητες ιατρικές πληροφορίες του ασθενούς και να απενεργοποιήσουν τον απινιδωτή χωρίς καμία φυσική πρόσβαση στη συσκευή. [15] [55]

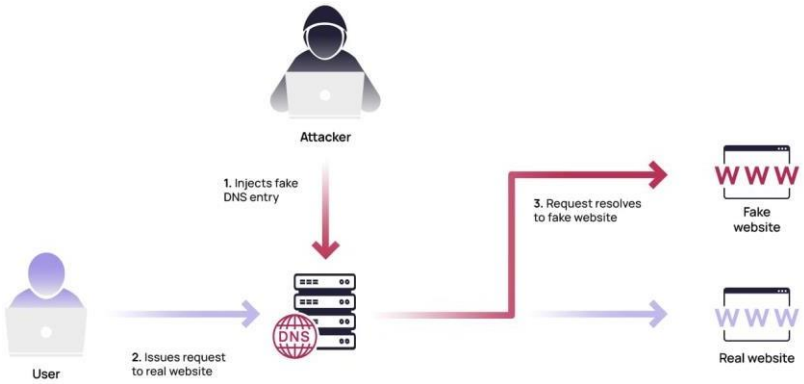
Το **sniffing** είναι ένα είδος παθητικής επίθεσης, κατά την οποία ο επιτιθέμενος παρακολουθεί παθητικά την κυκλοφορία του δικτύου για να αποκτήσει πρόσβαση σε ευαίσθητες πληροφορίες, χωρίς απαραίτητα να παρεμβαίνει ή να τροποποιεί δεδομένα. Ιδιαίτερα ευάλωτες είναι οι φορητές συσκευές όπως οι fitness trackers, καθώς έχουν στατική MAC διεύθυνση και μπορεί να εντοπιστεί εύκολα από κάποιον επιτιθέμενο. Το sniffing έχει αποδειχθεί αποτελεσματικό ακόμα και στις εμφυτεύσιμες και στις σταθερές ιατρικές συσκευές, καθώς μελέτες έχουν δείξει την υποκλοπή σημάτων από εμφυτευμένα

επιταχυνσιόμετρα, όπως και την παρακολούθηση της κυκλοφορίας από 52 διαφορετικούς τύπους ιατρικών συσκευών. [15]

Η επίθεση **αποκάλυψης πληροφορΙών** (information disclosure) αφορά τη μη εξουσιοδοτημένη πρόσβαση σε ευαίσθητα δεδομένα, εξαιτίας αδυναμιών κατά τη σχεδίαση της συσκευής, ελλιπών μηχανισμών ασφαλείας ή αδυναμίες στα πρωτόκολλα επικοινωνίας. Η επίθεση αυτή αφορά όλα τα είδη συσκευών, ακόμα και τις σταθερές συσκευές, καθώς η έλλειψη επικύρωσης εισόδου, μηχανισμών ελέγχου πρόσβασης και αυθεντικοποίησης δημιουργεί πρόσθετους κινδύνους. Έχουν αναφερθεί επιθέσεις μέσω ακουστικών και ηλεκτρομαγνητικών διαρροών, στις οποίες καταγράφηκαν πληροφορίες που αφορούσαν τη φυσιολογία των ασθενών, όπως τα πιεσόμετρα. [15]

Οι επιθέσεις **man-in-the-middle** αφορούν την παρακολούθηση και την αλλοίωση της επικοινωνίας μεταξύ δύο οντοτήτων από έναν κακόβουλο ενδιάμεσο. Τέτοιες επιθέσεις είναι διαδεδομένες σε όλα τα είδη ιατρικών συσκευών, καθώς πολλές από αυτές παρουσιάζουν ευπάθειες στα πρωτόκολλα επικοινωνίας και έλλειψη μηχανισμών ελέγχου ταυτότητας. Ο επιτιθέμενος μπορεί να παρακολουθεί παθητικά την κυκλοφορία, αποκτώντας πρόσβαση σε ευαίσθητες πληροφορίες των ασθενών χωρίς να γίνει αντιληπτός ή να υποκλέπτει και να τροποποιεί ενεργά τα δεδομένα πριν τα αναμεταδώσει, όπως για παράδειγμα να παραποιήσει και να αλλοιώσει μετρήσεις σε μια ιατρική οθόνη ή σε ένα φορητό αισθητήρα, οδηγώντας έτσι σε λανθασμένη διάγνωση και δημιουργώντας κίνδυνο για την ασφάλεια του ασθενούς. Σε μια προσομοίωση που έγινε στα πλαίσια μιας έρευνας το 2020 από το τμήμα μηχανοτρονικής και βιοϊατρικής μηχανικής του πανεπιστημίου Air στο Πακιστάν, ο επιτιθέμενος παρενέβη στην επικοινωνία ενός βηματοδότη και τροποποίησε τις παραμέτρους ελέγχου της συσκευής. Αυτό είχε ως αποτέλεσμα την αλλαγή του καρδιακού ρυθμού του ασθενούς από 72 παλμούς σε 52 κατά τη διάρκεια της επίθεσης. [15] [56]

Η **μη εξουσΙΟδοτημένη πρόσβαση** και οι επιθέσεις **spoofing** αποτελούν κρίσιμες απειλές για την ασφάλεια των ιατρικών συσκευών, καθώς επιτρέπουν στον επιτιθέμενο να αποκτήσει παράνομη πρόσβαση σε συστήματα ή να πλαστογραφήσει έγκυρες οντότητες, όπως ένα γιατρό ή ένα νοσοκομείο, με στόχο να εξαπατήσει και να προκαλέσει ζημιά στον ασθενή. Οι επιθέσεις αυτές αξιοποιούν υπάρχουσες αδυναμίες στα πρωτόκολλα επικοινωνίας και στους μηχανισμούς ελέγχου ταυτότητας σε όλα τα είδη ιατρικών συσκευών. Το spoofing δημιουργεί κινδύνους, όπως η παροχή ψευδών δεδομένων στον γιατρό, που οδηγούν σε λάθος διάγνωση ή θεραπεία, και η υποκλοπή και η παρέμβαση σε wearable συσκευές. [15]



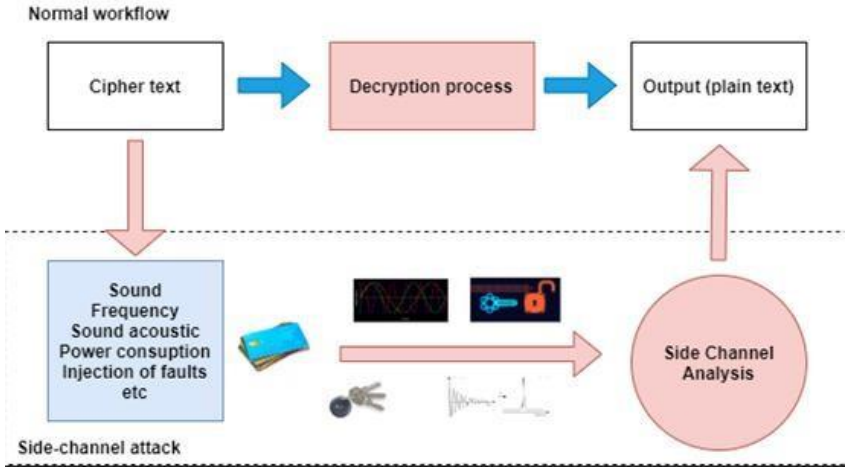
Εικόνα 13 Επίθεση spoofing

Η επίθεση **επανάληψης** (replay attack) στο πλαίσιο των ιατρικών συσκευών αναφέρεται στην υποκλοπή και επαναμετάδοση έγκυρων πακέτων δεδομένων με σκοπό την παραπλάνηση, αλλοίωση ή

πλαστοπροσωπία της συσκευής ή του χρήστη. Οι επιθέσεις τέτοιου είδους εκμεταλλεύονται ελλείψεις στην κρυπτογράφηση και στους μηχανισμούς ελέγχου ταυτότητας. Έχουν κρίσιμες επιπτώσεις καθώς μπορούν να παραποιήσουν την ακολουθία λήψης πακέτων σε εμφυτεύσιμες ιατρικές συσκευές, να εμποδίσουν την ενεργοποίηση θεραπείας ή και να επανεκπέμψουν επανειλημμένα το ίδιο πακέτο σε ιατρικές συσκευές, δημιουργώντας ψευδείς ενδείξεις ή αποκρύπτοντας καταστάσεις επικίνδυνες για την υγεία του ασθενούς. Το 2008 η ίδια ερευνητική ομάδα που κατάφερε να υποκλέψει ευαίσθητες ιατρικές πληροφορίες από τον απινιδωτή, κατάφεραν να παρακολουθήσουν και να καταγράψουν τα ασύρματα σήματα που ανταλλάσσονταν μεταξύ της συσκευής και του εξωτερικού προγραμματιστή της και έπειτα τα δεδομένα αυτά να επαναληφθούν για να ενεργοποιηθούν συγκεκριμένες λειτουργίες του απινιδωτή, όπως η απενεργοποίηση του και η αλλαγή ρυθμίσεων. [15] [46] [55]

Οι επιθέσεις **παραποίησης καΙ τροποποίησης** (tampering and modification) αφορούν τη σκόπιμη αλλοίωση δεδομένων από μη εξουσιοδοτημένες οντότητες, εκμεταλλευόμενες αδυναμίες στους μηχανισμούς κρυπτογράφησης, αυθεντικοποίησης και ελέγχου ακεραιότητας. Ένα είδος συσκευής που εκμεταλλεύονται αυτού του είδους οι επιθέσεις είναι τα fitness trackers, καθώς εκμεταλλεύονται το γεγονός ότι χρησιμοποιούν στατικές MAC διευθύνσεις. Εκμεταλλεύονται ωστόσο και εμφυτεύσιμες και σταθερές ιατρικές συσκευές, λόγω της ανεπάρκειας κρυπτογράφησης και ελέγχου ταυτότητας. [15]

Οι επιθέσεις **μέσω παράπλευρων καναλιών** (side-channel attacks) εκμεταλλεύονται την πληροφορία που διαρρέει μέσω φυσικών καναλιών όπως η κατανάλωση ενέργειας, ο χρόνος εκτέλεσης και η ηλεκτρομαγνητική εκπομπή. Χρησιμοποιούνται για την παραβίαση της ιδιωτικότητας και της ασφάλειας των ιατρικών συσκευών. Η πιο επικίνδυνη μορφή επίθεσης μέσω παράπλευρων καναλιών είναι η ηλεκτρομαγνητική παρεμβολή, η οποία μπορεί να επηρεάσει τα κυκλώματα των ιατρικών συσκευών, προκαλώντας αποτυχία στη λειτουργία των συσκευών. Η ηλεκτρομαγνητική παρεμβολή μπορεί να εμποδίσει την ενεργοποίηση εμφυτεύσιμων καρδιολογικών συσκευών, ενεργοποιώντας το σοκ απινίδωσης εάν ένας επιτιθέμενος βρίσκεται κοντά στη συσκευή. Οι αισθητήρες κίνησης σε smartwatches μπορούν επίσης να χρησιμοποιηθούν ως παράπλευρο κανάλι, προκειμένου να συλλεχθούν κρίσιμες πληροφορίες, όπως προσωπικές συνήθειες και κωδικούς πρόσβασης. Συγκεκριμένα, αναλύοντας την κίνηση του χεριού μεταξύ πατημάτων πλήκτρων, μπορεί να γίνει σύνθεση μοτίβων εισαγωγής κλειδιού. [15] [49]



Εικόνα 14 Επίθεση μέσω παράπλευρων καναλιών

7.6 Είδη επιθέσεων συστημάτων ιατρικών μονάδων

Η **επίθεση συλλογής πληροφοριών** (information collection) στοχεύει στη συλλογή ευαίσθητων δεδομένων μέσω εκμετάλλευσης διαφορετικών ευπαθειών του συστήματος της υγειονομικής μονάδας. Οι επιτιθέμενοι εκμεταλλεύονται γνωστές ευπάθειες, όπως αδυναμίες στο λειτουργικό σύστημα και παραβίαση αδύναμων κωδικών πρόσβασης. Δημιουργεί σοβαρές συνέπειες, δεδομένου ότι οι επιτιθέμενοι μπορεί να αποκτήσουν πρόσβαση σε προσωπικά δεδομένα υγείας, ιατρικά αρχεία και ευαίσθητες πληροφορίες που αφορούν τον ασθενή. Με τη διαρροή αυτών των πληροφοριών, θέτονται σε κίνδυνο τόσο η ιδιωτικότητα των ασθενών, όσο και η ασφάλεια και η ακεραιότητα των ιατρικών υπηρεσιών. [48]

Οι **επιθέσεις σε βάσεις δεδομένων** είναι ιδιαίτερα κρίσιμες, καθώς οι βάσεις δεδομένων περιέχουν ιατρικά αρχεία των ασθενών, πληροφορίες των ιατρικών συσκευών και δεδομένα που σχετίζονται με την παρακολούθηση και τη διάγνωση των ασθενών. Μια τέτοια επίθεση μπορεί να προκαλέσει σοβαρές συνέπειες, όπως καθυστέρηση στην παροχή θεραπείας, παραποίηση ή απώλεια ιατρικών δεδομένων ή και κίνδυνο για τη ζωή των ασθενών. Οι πιο σημαντικές επιθέσεις αυτού του είδους είναι: [48]

- Επίθεση με παραβίαση κωδικού πρόσβασης: Γίνεται όταν ο κακόβουλος χρήστης αποκτήσει πρόσβαση σε έναν λογαριασμό ή μια υπηρεσία χρησιμοποιώντας έναν κωδικό πρόσβασης που είτε έχει υποκλαπεί είτε έχει μαντευτεί. Εάν ένας επιτιθέμενος καταφέρει να παραβιάσει έναν λογαριασμό ιατρικού προσωπικού ή ενός συστήματος, μπορεί να αποκτήσει πρόσβαση σε κρίσιμα δεδομένα και να προκαλέσει σοβαρές διαταραχές στη διαδικασία λήψης αποφάσεων για την υγεία του ασθενούς.
- Ανύψωση προνομίων: Αναφέρεται στη διαδικασία κατά την οποία ένας κακόβουλος χρήστης αποκτά αυξημένα δικαιώματα πρόσβασης σε έναν υπολογιστή. Μπορεί να επιτρέψει στον επιτιθέμενο να αποκτήσει πλήρη πρόσβαση σε ευαίσθητα δεδομένα ή να εκτελέσει ενέργειες που κανονικά θα απαιτούσαν εξουσιοδότηση.
- SQL Injection: Είναι μια τεχνική επίθεσης όπου ο επιτιθέμενος εισάγει κακόβουλο SQL κώδικα σε φόρμες ή άλλα σημεία εισαγωγής δεδομένων στις εφαρμογές που συνδέονται με βάσεις δεδομένων. Ο επιτιθέμενος μπορεί να αποκτήσει πλήρη πρόσβαση στα δεδομένα της βάσης, να τα παραποιήσει ή να τα καταστρέψει. Αυτό μπορεί να οδηγήσει στην παραποίηση ιατρικών αρχείων, διαρροή προσωπικών δεδομένων ασθενών και σοβαρές νομικές και ηθικές συνέπειες
- Κλοπή αντιγράφων ασφαλείας: Αναφέρεται στην παράνομη απόκτηση και κλοπή των αντιγράφων ασφαλείας της βάσης δεδομένων, τα οποία περιέχουν τα πλήρη αρχεία δεδομένων. Τα κλεμμένα αντίγραφα ασφαλείας μπορεί να περιέχουν ευαίσθητα ιατρικά δεδομένα, τα οποία ενδέχεται να εκτεθούν ή να χρησιμοποιηθούν για κακόβουλους σκοπούς, θέτοντας σε κίνδυνο την ιδιωτικότητα των ασθενών

Οι **επιθέσεις σε ιστοσελίδες** στον ιατρικό τομέα αποτελούν σημαντική απειλή για τη λειτουργικότητα και την ασφάλεια των πληροφοριακών συστημάτων υγείας. Δεδομένου ότι οι επαγγελματίες υγείας βασίζονται σε διαδικτυακές εφαρμογές για να έχουν πρόσβαση σε ιατρικά δεδομένα, να συνταγογραφούν φάρμακα και να συντονίζουν τη θεραπεία των ασθενών, μια επίθεση μπορεί να οδηγήσει σοβαρές επιπτώσεις. Αυτές είναι η παραποίηση ιατρικών πληροφοριών, η καθυστέρηση θεραπείας, η διαρροή ευαίσθητων δεδομένων των ασθενών και ηθικές συνέπειες για τους παρόχους υγείας. Βασικές επιθέσεις αυτού του τύπου είναι: [46] [48]

- Επιθέσεις έγχυσης κώδικα: Ο επιτιθέμενος εισάγει κακόβουλο κώδικα μέσω πεδίων εισόδου, με σκοπό να παρακάμψει λειτουργίες της εφαρμογής και να αποκτήσει πρόσβαση σε δεδομένα.
- Cross-Site Scripting: Έγχυση κακόβουλου script το οποίο εκτελείται στο πρόγραμμα περιήγησης άλλου χρήστη. Μπορεί να οδηγήσει σε υποκλοπή διαπιστευτηρίων και ανακατεύθυνση σε πλαστές σελίδες.
- XML external entities: Κακόβουλη επεξεργασία XML εισόδου που επιτρέπει ανάγνωση αρχείων ή απομακρυσμένη εκτέλεση εντολών.

7.7 Μεθοδολογία STRIDE

Η μεθοδολογία STRIDE αποτελεί ένα ιδιαίτερα χρήσιμο εργαλείο για την κατηγοριοποίηση και κατανόηση των απειλών κατά των εμφυτεύσιμων ιατρικών συσκευών, με στόχο τον εντοπισμό των παραβιάσεων στις βασικές υπηρεσίες ασφαλείας. Τα αρχικά STRIDE προέρχονται από τις λέξεις: **S**poofing, **T**ampering, **R**epudiation, **I**nformation disclosure, **D**enial of Service, **E**levation of privilege. Η κάθε μια από αυτές τις επιθέσεις, απειλεί και μια υπηρεσία ασφαλείας: [14]

Πίνακας 1 Επιθέσεις - Υπηρεσίες ασφαλείας

Επίθεση	Υπηρεσία ασφαλείας
Spoofing	Ταυτοποίηση
Tampering	Ακεραιότητα
Repudiation	Μη αποποίηση ευθύνης
Information Disclosure	Εμπιστευτικότητα
Denial of Service	Διαθεσιμότητα
Elevation of privilege	Εξουσιοδότηση

Με την ταυτοποίηση εννοείται η επιβεβαίωση της ταυτότητας τόσο των συσκευών, όσο και των χρηστών. Η ταυτότητα των μερών πρέπει να εξακριβώνεται πριν από οποιαδήποτε ενέργεια. Παράδειγμα παραβίασης αυτής της υπηρεσίας είναι όταν ο επιτιθέμενος προσποιείται έναν γιατρό ή ειδικό υγείας και αποκτά πρόσβαση σε μια εμφυτεύσιμη ιατρική συσκευή, μέσω ασύρματης διεπαφής χωρίς πιστοποίηση.

Η ακεραιότητα αναφέρεται στη διατήρηση της ορθότητας και μη αλλοίωσης των δεδομένων. Τα δεδομένα πρέπει να τροποποιούνται μόνο από εξουσιοδοτημένα μέρη. Παράδειγμα παραβίασης της ακεραιότητας είναι η τροποποίηση θεραπευτικών ρυθμίσεων της συσκευής, όπως οι αλλαγή παραμέτρων ενός απινιδωτή, οι επιθέσεις έγχυσης και η αλλοίωση της μνήμης.

Με τη μη αποποίηση ευθύνης εννοείται η καταγραφή και επιβεβαίωση ενεργειών. Οι ενέργειες που εκτελούνται προς ή από την εμφυτεύσιμη ιατρική συσκευή πρέπει να καταγράφονται με ασφάλεια σε ένα αρχείο καταγραφής πρόσβασης. Παράδειγμα παραβίασης της υπηρεσίας αυτής είναι οι μη ανιχνεύσιμες τροποποιήσεις και η απουσία ειδοποιήσεων για κακόβουλες ενέργειες.

Η εμπιστευτικότητα αναφέρεται στη προστασία δεδομένων από μη εξουσιοδοτημένη πρόσβαση. Τα δεδομένα θα πρέπει να είναι προσβάσιμα μόνο από μέλη με την κατάλληλη εξουσιοδότηση. Παράδειγμα παραβίασης της εμπιστευτικότητας είναι η υποκλοπή ιατρικών δεδομένων και η διαρροή τους μέσω ασύρματης παρακολούθησης και ο εντοπισμός θέσης ασθενή μέσω μετάδοσης.

Με τη διαθεσιμότητα εννοείται η συνεχής λειτουργία και πρόσβαση στη συσκευή. Οι υπηρεσίες μιας εμφυτεύσιμης ιατρικής συσκευής θα πρέπει πάντα να είναι διαθέσιμες στους εξουσιοδοτημένους χρήστες. Παράδειγμα παραβίασής της είναι η εξάντληση της μπαταρίας μιας συσκευής με συνεχείς αιτήσεις, μπλοκάροντας την πρόσβαση στη συσκευή ή τη λειτουργικότητά της.

Η εξουσιοδότηση αναφέρεται στον έλεγχο πρόσβασης σε ευαίσθητες λειτουργίες. Μια ενέργεια θα πρέπει να εκτελείται μόνο αν ο αιτών διαθέτει τα κατάλληλα προνόμια. Παράδειγμα παραβίασης της

εξουσιοδότησης είναι όταν ένας χρήστης χωρίς την κατάλληλη εξουσιοδότηση αποκτά πρόσβαση διαχειριστή και εκτελεί κρίσιμες εντολές. [14]

7.8 Επίλογος

Στο κεφάλαιο αυτό έγινε αναφορά στα κίνητρα των επιθέσεων έναντι των ιατρικών συσκευών. Αναλύθηκαν οι τύποι των επιτιθέμενων και οι κατηγορίες των επιθέσεων. Καταγράφηκαν οι ομάδες στόχοι των επιτιθέμενων. Παρουσιάστηκαν τα είδη επιθέσεων τόσο στις ιατρικές συσκευές όσο και στις ιατρικές μονάδες και η μεθοδολογία STRIDE.

Κεφάλαιο 8ο: Ενέργειες κυβερνοασφάλειας και αντιμετώπιση κυβερνοεπιθέσεων

8.1 Εισαγωγή

Στο κεφάλαιο αυτό αναλύονται οι ενέργειες, όσον αφορά την κυβερνοασφάλεια, που θα πρέπει να ακολουθούν οι κατασκευαστές πριν την κυκλοφορία της ιατρικής συσκευής στην αγορά και οι ενέργειες που θα πρέπει να ακολουθήσουν οι εμπλεκόμενοι φορείς υγείας που έχουν προμηθευτεί τις ιατρικές συσκευές που έχουν κυκλοφορήσει στην αγορά. Γίνεται αναφορά στους τρόπους με τους οποίους μπορούν να καταπολεμηθούν και αντιμετωπιστούν οι επιθέσεις έναντι ιατρικών συσκευών.

8.2 Ενέργειες πριν την κυκλοφορία

Παρόλο που η κυβερνοασφάλεια είναι σημαντική σε όλη τη διάρκεια ζωής μιας ιατρικής συσκευής, τα πιο κρίσιμα μέτρα θα πρέπει να λαμβάνονται ήδη από το στάδιο του σχεδιασμού και ανάπτυξης της συσκευής. Οι κατασκευαστές έχουν τη δυνατότητα, πριν η συσκευή φτάσει στα χέρια των χρηστών, να ενσωματώσουν μέτρα που θα κάνουν τη συσκευή πιο ασφαλή και αξιόπιστη μέχρι το τέλος της λειτουργίας της. Είναι σημαντικό να σχεδιάζονται τα χαρακτηριστικά ασφαλείας, να εφαρμόζονται στρατηγικές διαχείρισης κινδύνων, να γίνονται δοκιμές ασφαλείας, να παρέχονται σαφείς οδηγίες χρήσης και να υπάρχει πρόβλεψη για τη διαχείριση πιθανών θεμάτων μετά την κυκλοφορία του προϊόντος. Θα πρέπει επίσης να λαμβάνεται υπόψη ο τρόπος και οι συνθήκες χρήσης της συσκευής, να προβλέπονται σενάρια κακής χρήσης και να επισημαίνονται οι πιθανοί κίνδυνοι στα εγχειρίδια λειτουργείας με κατανοητό τρόπο. [43] [57] [58]

Για να εξασφαλιστεί ότι μια ιατρική συσκευή θα είναι ασφαλή και αξιόπιστη σε βάθος χρόνου, είναι σημαντική η υιοθέτηση ενός οργανωμένου πλαισίου που ονομάζεται **Πλαίσιο Ασφαλούς Ανάπτυξης Προϊόντος** (Secure Product Development Framework, SPDF). Ο βασικός του σκοπός είναι να διασφαλίσει ότι η συσκευή θα είναι αποτελεσματική, λειτουργική και ανθεκτική σε κινδύνους καθ' όλη τη διάρκεια του κύκλου ζωής της. Το SPDF καλύπτει όλα τα στάδια της πορείας μιας ιατρικής συσκευής, από το σχεδιασμό και την ανάπτυξη μέχρι την κυκλοφορία του στην αγορά και την υποστήριξή του μετά την πώληση. Ακολουθώντας αυτή τη διαδικασία, μειώνονται οι ανάγκες για μελλοντικές επανασχεδιάσεις λόγω τεχνολογικών αλλαγών ή αναβαθμίσεων λογισμικού. Οι συσκευές που αναπτύσσονται βάσει SPDF είναι ευκολότερο να ενσωματωθούν σε υφιστάμενα δίκτυα υγειονομικής περίθαλψης και μπορούν να λειτουργήσουν με τα καθιερωμένα πρωτόκολλα ασφαλείας.

Για να αποφευχθούν προβλήματα που μπορεί να θέσουν σε κίνδυνο την υγεία των ασθενών ή να προκαλέσουν βλάβες στις ιατρικές συσκευές, είναι σημαντικό να εφαρμόζονται αρχές σχεδιασμού της κυβερνοασφάλειας. Οι κατευθυντήριες γραμμές αυτών των αρχών αναλύονται στη συνέχεια.

Ο κατασκευαστής χρειάζεται να μεριμνήσει για την **ασφαλή επικοινωνία** και να λάβει υπόψη του με ποιον τρόπο η συσκευή θα συνδέεται με άλλα συστήματα ή δίκτυα. Αυτές οι διασυνδέσεις μπορεί να γίνονται είτε μέσω καλωδίων είτε ασύρματα. Επιπλέον, ο κατασκευαστής θα πρέπει να μελετήσει το πώς θα διασφαλίζεται η ασφαλής ανταλλαγή δεδομένων από και προς τη συσκευή, ώστε να αποτρέπεται η μη εξουσιοδοτημένη πρόσβαση ή αλλοίωση των πληροφοριών. Θα πρέπει να οριστούν μηχανισμοί μέσω των οποίων οι συσκευές θα μπορούν να αναγνωρίζουν η μια την άλλη, να προσδιοριστεί αν απαιτείται η χρήση κρυπτογράφησης και να εξεταστεί αν θα ήταν χρήσιμο να διακόπτονται οι συνδέσεις αυτόματα μετά από ένα συγκεκριμένο χρονικό διάστημα.

Ο κατασκευαστής οφείλει να νοιάζεται για την **προστασία των δεδομένων**. Πρέπει να εξετάζει αν τα δεδομένα που αποθηκεύονται στη συσκευή ή διακινούνται από αυτή χρειάζεται να είναι κρυπτογραφημένα και προστατευμένα με κωδικό πρόσβασης. Παράλληλα είναι σημαντικό τα μηνύματα και τα πεδία εισαγωγής στα πρωτόκολλα επικοινωνίας να κρυπτογραφούνται, ώστε να διασφαλίζεται η εμπιστευτικότητα των πληροφοριών που ανταλλάσσονται.

Μια καλή πρακτική για τον κατασκευαστή είναι να εξετάσει αν πρέπει να ενσωματωθούν χαρακτηριστικά σε επίπεδο συστήματος που να αποτρέπουν την απώλεια δεδομένων, εξασφαλίζοντας την **ακεραιότητα της συσκευής**. Παράλληλα θα πρέπει να δίνεται η δυνατότητα για έλεγχο με λογισμικό προστασίας από κακόβουλο λογισμικό, ώστε να μειώνεται ο κίνδυνος από ιούς και ransomware. Το λογισμικό της συσκευής οφείλει να είναι επαρκώς θωρακισμένο ώστε να αποτρέπεται οποιαδήποτε μη εξουσιοδοτημένη τροποποίηση.

Η συσκευή θα πρέπει να υποστηρίζει μηχανισμούς **αυθεντικοποίησης χρήστη**, όπως κωδικούς πρόσβασης ή βιομετρικά στοιχεία, ώστε να αποτρέπεται η πρόσβαση από μη εξουσιοδοτημένους χρήστες. Είναι σημαντικό να υπάρχουν διαφορετικοί ρόλοι χρηστών με καθορισμένα επίπεδα πρόσβασης, ενώ παράλληλα σε περιπτώσεις έκτακτης ανάγκης η συσκευή θα πρέπει να μπορεί να χρησιμοποιηθεί χωρίς καθυστέρηση. Τα διαπιστευτήρια κάθε χρήστη πρέπει να παραμένουν αυστηρά προσωπικά και να μη διαμοιράζονται εντός του δικτύου.

Ο κατασκευαστής θα πρέπει να καθορίσει πώς θα πραγματοποιούνται η **συντήρηση του λογισμικού** και οι ενημερώσεις της συσκευής, ώστε να διατηρείται προστατευμένη από τις νέες κυβερνοαπειλές. Θα πρέπει να αποφασιστεί αν οι ενημερώσεις θα γίνονται αυτόματα ή θα απαιτούν ενέργεια από τον χρήστη. Είναι σημαντικό επίσης να καθορίσει ποιες συνδέσεις θα χρησιμοποιούνται για τις ενημερώσεις, καθώς και να διασφαλίζεται η αυθεντικότητα τόσο της σύνδεσης όσο και των ίδιων των αρχείων ενημέρωσης. Πρέπει να εξετάζεται η συχνότητα των ενημερώσεων, αν θα είναι τακτικές ή προγραμματισμένες, καθώς και η διαδικασία με την οποία θα ενημερώνεται ή θα ελέγχεται το λειτουργικό σύστημα της συσκευής, λογισμικό ανοιχτού κώδικα ή το λογισμικό τρίτων κατασκευαστών που μπορεί να χρησιμοποιείται.

Πρέπει να λαμβάνεται υπόψη ο περιορισμός της **φυσικής πρόσβασης** στη συσκευή. Οι θύρες δικτύου, οι υποδοχές USB και άλλα σημεία που θα μπορούσαν να χρησιμοποιηθούν για κακόβουλη πρόσβαση, δεν θα πρέπει να είναι προσβάσιμα από μη εξουσιοδοτημένα άτομα. Το φυσικό περίβλημα της συσκευής θα πρέπει να διαθέτει μηχανισμούς όπως κλειδαριές ή άλλες μορφές ελεγχόμενης πρόσβασης ώστε να αποτρέπονται παρεμβάσεις που θα μπορούσαν να θέσουν σε κίνδυνο την ασφάλεια του συστήματος.

Ο κατασκευαστής θα πρέπει να φροντίζει για την **αξιοπιστία** και τη **διαθεσιμότητα** της συσκευής. Θα πρέπει να ενσωματώνει μηχανισμούς στο σχεδιασμό της συσκευής που να της επιτρέπουν να εντοπίζει απόπειρες επίθεσης, να αντιμετωπίζει τις επιθέσεις, να ανταποκρίνεται κατάλληλα όταν προκύψουν και να μπορεί να επανέλθει σε ασφαλή λειτουργία μετά από ένα τέτοιο περιστατικό. [43] [57] [58]

8.3 Ενέργειες μετά την κυκλοφορία

Παρόλο που η προσέγγιση της κυβερνοασφάλειας μετά την κυκλοφορία μιας ιατρικής συσκευής στην αγορά βασίζεται σε πολλές παρόμοιες κατευθυντήριες αρχές με εκείνες που ισχύουν πριν την κυκλοφορία τα συσκευής, υπάρχουν συγκεκριμένες απαιτήσεις που αφορούν την περίοδο μετά την κυκλοφορία. Οι διαδικασίες επιτήρησης μετά την κυκλοφορία καθορίζουν τα απαραίτητα βήματα για τη διατήρηση της ακεραιότητας, της λειτουργικότητας και της ασφάλειας της ιατρικής συσκευής καθ' όλη τη διάρκεια του κύκλου ζωής της. Οι ενέργειες αυτές απευθύνονται σε όλους τους εμπλεκόμενους

φορείς και πρέπει να υλοποιούνται με την κατάλληλη τεκμηρίωση και αναφορά, ώστε να εξασφαλίζεται η έγκαιρη και επαρκής αντίδραση σε περιπτώσεις δυσλειτουργιών ή περιστατικών που ενδέχεται να προκαλέσουν ζημιά στην υγεία του ασθενή. Όλοι οι εμπλεκόμενοι στην ανάπτυξη και χρήση ιατρικών συσκευών οφείλουν να αξιολογούν τακτικά τη χρηστικότητα, την αποτελεσματικότητα και την ασφάλεια των συσκευών τους, εφαρμόζοντα τις κατάλληλες διορθωτικές και προληπτικές ενέργειες όπου κρίνεται αναγκαίο.[43] [57] [58]

Καθώς οι απειλές έναντι της κυβερνοασφάλειας εξελίσσονται συνεχώς και γίνονται όλο και πιο πολύπλοκες, ορισμένα από τα μέτρα ασφαλείας που εφαρμόζονται πριν από την κυκλοφορία μιας ιατρικής συσκευής ενδέχεται να μην επαρκούν στο περιβάλλον μετά τη διάθεσή της στην αγορά. Οι ενέργειες πριν από την κυκλοφορία εμπίπτουν κυρίως στην ευθύνη του κατασκευαστή, ενώ η διατήρηση της κυβερνοασφάλειας μετά την κυκλοφορία εμπλέκει παρόχους υγειονομικής περίθαλψης, ασθενείς και τεχνικό προσωπικό.

Οι πάροχοι υγειονομικής περίθαλψης φέρουν την ευθύνη για τη δημιουργία ενός κατάλληλου περιβάλλοντος λειτουργίας για την ασφαλή χρήση των ιατρικών συσκευών. Από πλευράς κυβερνοασφάλειας, αυτό συνεπάγεται την ανάγκη προσαρμογής της υποδομής του δικτύου τους, με στόχο την ελαχιστοποίηση των κινδύνων, χωρίς όμως να διακυβεύονται οι διαγνωστικές και θεραπευτικές δυνατότητες της συσκευής. Τα πιο σημαντικά βήματα που οφείλουν να εφαρμόσουν οι πάροχοι είναι:

- Υποδομή πληροφορικής που είναι έτοιμη να υποστηρίξει τη χρήση ιατρικών συσκευών
- Σύνδεση της νέας ιατρικής συσκευής στο υπάρχον δίκτυο πληροφορικής
- Προσαρμογή ή αναβάθμιση του λειτουργικού συστήματος και των ρυθμίσεων δικτύου

Οι πάροχοι υγειονομικής περίθαλψης θα πρέπει επίσης να εφαρμόσουν ορισμένες από τις γενικές αρχές της κυβερνοασφάλειας:

- Αποτροπή μη εξουσιοδοτημένων φυσικών παρεμβάσεων στη συσκευή, στα δίκτυα και στα δεδομένα
- Καταγραφή όλων των υπαρχόντων στοιχείων του συστήματος και παρακολούθηση μελλοντικών αλλαγών στη διαμόρφωσή τους
- Χρήση προτεινόμενων ρυθμίσεων ασφαλείας και προστατευτικών μηχανισμών
- Εφαρμογή πολιτικών ελέγχου πρόσβασης στο δίκτυο της ιατρικής συσκευής
- Διατήρηση των πιο πρόσφατων εγκατεστημένων ενημερώσεων ασφαλείας
- Αντιμετώπιση απειλών λογισμικού μέσω εργαλείων προστασίας από ιούς και malware
- Ορισμός χρονικού περιορισμού για τις συνδέσεις, ώστε να αποφεύγεται η ανεπιθύμητη χρήση ή πρόσβαση

Η σωστή λειτουργία της ιατρικής συσκευής εξαρτάται σε μεγάλο βαθμό από την εκπαίδευση όλων των χρηστών του, δηλαδή οι ιατροί, οι νοσηλευτές, οι τεχνικοί, οι ειδικοί πληροφορικής και οι εκπρόσωποι της εταιρείας. Θα πρέπει να γνωρίζουν πώς να χρησιμοποιούν τη συσκευή με ασφάλεια. Σε περιπτώσεις όπου η συσκευή χρησιμοποιείται στο σπίτι, οι ασθενείς οφείλουν να λάβουν την ίδια ενημέρωση και να ακολουθούν τις ίδιες πρακτικές. Η ανθρώπινη συμπεριφορά αποτελεί συχνά τον πιο ευάλωτο κρίκο στην αλυσίδα ασφάλειας και για αυτό η εκπαίδευση πρέπει να έχει μέγιστη προτεραιότητα.

Καμία στρατηγική για την κυβερνοασφάλεια δε μπορεί να θεωρηθεί επαρκής χωρίς την ενεργή και συνεχή ανταλλαγή πληροφοριών μεταξύ όλων των εμπλεκόμενων μερών, δηλαδή κατασκευαστών, παρόχων υγειονομικής περίθαλψης, ασθενών και ρυθμιστικών αρχών. Μέσω αυτής της συνεργασίας μπορεί να δημιουργηθεί ένα παγκόσμιο δίκτυο ιατρικών συσκευών όπου όλοι οι φορείς είναι σε θέση να προβλέπουν και να αντιδρούν αποτελεσματικά σε κυβερνοεπιθέσεις. Ορισμένες βασικές αρχές

μπορούν να καθοδηγήσουν την προσπάθεια αυτή, αν και η τελική εφαρμογή πρέπει να προσαρμόζεται στο εκάστοτε ρυθμιστικό και λειτουργικό πλαίσιο κάθε χρήστη:

- Οι πληροφορίες για την κυβερνοασφάλεια πρέπει να διανέμονται σε όλα τα εμπλεκόμενα μέρη κατά τη διάρκεια του κύκλου ζωής της ιατρικής συσκευής, όπως κατασκευαστές, προμηθευτές εξαρτημάτων, διανομείς, πάροχοι, τελικοί χρήστες και κοινό.
- Οι κοινοποιούμενες πληροφορίες πρέπει να είναι κατανοητές και πρακτικές για κάθε κατηγορία αποδεκτών, καθώς δεν είναι κάθε πληροφορία χρήσιμη για όλους.
- Η ανταλλαγή πληροφοριών πρέπει να γίνεται ανεξάρτητα από οικονομικά ή εμπορικά συμφέροντα, με κύριο στόχο την προστασία των ασθενών.
- Οι πληροφορίες πρέπει να είναι εναρμονισμένες σε διεθνές επίπεδο και να διαμοιράζονται ταυτόχρονα μεταξύ αρχών, ώστε οι φορείς κάθε περιοχής να μπορούν να αντιδράσουν σωστά.

Οι βασικοί τύποι των πληροφοριών θα πρέπει να περιλαμβάνουν:

- Ποιες ιατρικές συσκευές επηρεάζονται και με ποιον τρόπο από μια ευπάθεια
- Ποια συγκεκριμένα εξαρτήματα παρουσιάζουν τις καταγεγραμμένες ευπάθειες
- Ποιος εξοπλισμός πληροφορικής μπορεί να επηρεάσει την κυβερνοασφάλεια της συσκευής
- Αν υπάρχει διαθεσιμότητα εκμετάλλευσης κώδικα και τι τύποι επιθέσεων μπορούν να πραγματοποιηθούν
- Αν έχει επιβεβαιωθεί ότι συνέβη περιστατικό κυβερνοασφάλειας
- Ποια διαθέσιμα μέτρα προστασίας μπορούν να εφαρμοστούν
- Οδηγίες για προσωρινή χρήση και ασφαλή ενσωμάτωση της συσκευής στο περιβάλλον
- Ποια είναι η προτεινόμενη διαμόρφωση συστημάτων πληροφορικής για μείωση του κινδύνου από κυβερνοαπειλές

Για την ενίσχυση της διαφάνειας σχετικά με τα τρωτά σημεία στην κυβερνοασφάλεια, χρειάζεται μια πιο επίσημη διαδικασία ανταλλαγής πληροφοριών, όπως η συντονισμένη αποκάλυψη ευπαθειών. Αποτελεί μια επίσημη διαδικασία που περιλαμβάνει τη συλλογή και αξιολόγηση πληροφοριών για τις ευπάθειες, την ανάπτυξη μέτρων μετριασμού, την πρόταση λύσεων και την κοινοποίηση αυτών των πληροφοριών σε όλους τους εμπλεκόμενους φορείς των ιατρικών συσκευών. Η προσέγγιση αυτή επιτρέπει στους τελικούς χρήστες να κάνουν πιο ενημερωμένες ενέργειες για την προστασία της συσκευής, του δικτύου και ως αποτέλεσμα του ασθενούς. Ένας τρόπος για τους κατασκευαστές να διανέμουν έγκαιρα πληροφορίες είναι η χρήση δελτίων και κοινοποιήσεων, διασφαλίζοντας παράλληλα την τήρηση των διοικητικών απαιτήσεων της αντίστοιχης αγοράς. Η προσέγγιση που θα μπορούσαν να υιοθετήσουν οι κατασκευαστές δεν επικεντρώνεται στον αριθμό των κοινοποιούμενων ευπαθειών, αλλά στην έγκαιρη ανταπόκριση στις κυβερνοαπειλές. [43] [57] [58]

8.4 Διαχείριση κινδύνων ασφάλειας

Για να αξιολογηθούν πλήρως οι κυβερνοαπειλές που σχετίζονται με μια ιατρική συσκευή, είναι απαραίτητο να εξετάζεται όχι μόνο η ίδια η συσκευή, αλλά και το περιβάλλον στο οποίο θα λειτουργήσει. Είναι σημαντικό να ενσωματωθεί μια δυναμική προσέγγιση διαχείρισης κινδύνου στο σύστημα ποιότητας του κατασκευαστή, ώστε να μειώνονται οι πιθανότητες παραβίασης και μη εξουσιοδοτημένης πρόσβασης. Η προσέγγιση αυτή θα πρέπει να περιλαμβάνει τεχνικούς κανόνες, εκπαιδευτικά μέτρα για τους χρήστες και πολιτικές, ενσωματώνοντας ασφαλείς μεθόδους σχεδιασμού, ελεγμένες διαδικασίες παραγωγής και ενέργειες πρόληψης. Η διαχείριση των κινδύνων ασφάλειας θα πρέπει να εστιάζει στο πόσο ευάλωτο είναι το σύστημα απέναντι σε γνωστές απειλές και πιθανά σενάρια κινδύνου. [43] [57] [58]

Οι βασικές αρχές διαχείρισης κινδύνων για την ασφάλεια και την προστασία των ιατρικών συσκευών θα πρέπει να εφαρμόζονται καθ' όλη τη διάρκεια του κύκλου ζωής μιας συσκευής. Οι κυβερνοεπιθέσεις

που επηρεάζουν τη λειτουργία της συσκευής ή υποβαθμίζουν την ασφάλεια της ενδέχεται να επηρεάσουν αρνητικά τις διαγνωστικές ή θεραπευτικές της δυνατότητες. Αυτό θα έχει ως αποτέλεσμα τη λανθασμένη ιατρική αξιολόγηση και την πρόκληση ζημιάς στην υγεία του ασθενούς. Για το λόγο αυτό, είναι σημαντικό οι κατασκευαστές να ενσωματώνουν τις διαδικασίες διαχείρισης κινδύνου και κυβερνοασφάλειας ακολουθώντας τα παρακάτω βήματα:

1. Ανάλυση κινδύνου ασφαλείας
2. Αξιολόγηση του κινδύνου ασφαλείας
3. Έλεγχος του κινδύνου ασφαλείας
4. Αξιολόγηση του υπολειπόμενου κινδύνου
5. Παροχή πληροφοριών για την παραγωγή και έκθεση διαχείρισης κινδύνων

Στη βιβλιογραφία αναλύεται μόνο το πρώτο στάδιο με λεπτομέρεια. Βλέποντας σε βάθος το πρώτο στάδιο της διαδικασίας, δηλαδή την ανάλυση κινδύνων, πρέπει να επικεντρώνεται στον εντοπισμό των κινδύνων και στην εκτίμηση της σοβαρότητας της πιθανής βλάβης στους ασθενείς, σε περίπτωση που τρίτοι εκμεταλλευτούν τα ευάλωτα σημεία της ασφάλειας της συσκευής. Θα πρέπει να λαμβάνονται υπόψη τρόποι περιορισμού και αντιστάθμισης αυτών των κινδύνων. Η ανάλυση κινδύνου είναι στενά συνδεδεμένη με τη φάση σχεδιασμού της συσκευής, καθώς σε αυτό το στάδιο ενσωματώνονται τεχνικές όπως η μοντελοποίηση απειλών, η εκτίμηση κινδύνων και η αξιολόγηση της ενδεχόμενης βλάβης για τον ασθενή. Ο σχεδιασμός μιας ασφαλούς αρχιτεκτονικής, μέσα από διαδικασίες όπως η αξιολόγηση κινδύνων ασφαλείας, η ανάλυση πιθανών επιθέσεων και η ταξινόμηση των ευπαθειών, εξασφαλίζει την ολοκληρωμένη εφαρμογή της διαχείρισης κινδύνου.

Κατά τη φάση της κατασκευής, είναι σημαντικό να πραγματοποιείται **αξΙΟλόγηση των κΙΝδύνων ασφαλείας**, των πιθανών απειλών και των μηχανισμών προστασίας σε όλη τη διάρκεια του κύκλου ζωής της συσκευής. Οι οδηγίες για την κυβερνοασφάλεια θα πρέπει να εστιάζουν σε συγκεκριμένες απειλές και ευπάθειες, με στόχο τη διαμόρφωση απαιτήσεων που συμβάλλουν στην αποτροπή αυτών των κινδύνων.

Η διαδικασία εντοπισμού και αντιμετώπισης των κινδύνων στο ιατρικό σύστημα περιλαμβάνει την αναγνώριση απειλών που σχετίζονται με τα εξαρτήματα της συσκευής, την παραγωγή, τον σχεδιασμό, την εγκατάστασή της στο περιβάλλον του χρήστη και τη μετέπειτα συντήρησή της. Για να υποστηρίξουν **μοντελοποίηση των απεΙλών**, οι κατασκευαστές θα πρέπει να παρέχουν χρήσιμες πληροφορίες, όπως διαγράμματα του συστήματος και οδηγίες εγκατάστασης. Κατά τη φάση αυτή, οι κατασκευαστές θα πρέπει να λαμβάνουν υπόψη ακόμη και τα πιο ακραία σενάρια και να εξετάζουν πώς ο σχεδιασμός του συστήματος θα μπορούσε να επιτρέψει τέτοια περιστατικά.

Είναι σημαντικό να χρησιμοποιείται μια συγκεκριμένη μεθοδολογία **βαθμολόγησης των τρωτών σημείων** για να εκτιμηθεί πόσο εύκολα μπορούν να αξιοποιηθούν οι κίνδυνοι και πόσο σοβαρές θα μπορούσαν να είναι οι συνέπειές τους. Τα τρωτά σημεία που εντοπίζονται κατά τον σχεδιασμό και την ανάπτυξη της συσκευής θα πρέπει να ελέγχονται και να αξιολογούνται με βάση ένα καθιερωμένο και αναγνωρισμένο σύστημα βαθμολόγησης, ώστε να διασφαλίζεται η συνέπεια και η ακρίβεια στην εκτίμηση του κινδύνου.

Στο στάδιο του σχεδιασμού και της ανάπτυξης, είναι απαραίτητο να πραγματοποιούνται δοκιμές ασφαλείας ώστε να εντοπιστούν πιθανά κρίσιμα τρωτά σημεία στον κώδικα και να επιβεβαιωθεί ότι έχουν ενσωματωθεί σωστά οι μηχανισμοί προστασίας. Θα πρέπει να λαμβάνεται υπόψη τόσο το μελλοντικό δίκτυο στο οποίο θα λειτουργεί η συσκευή όσο και ο τρόπος με τον οποίο αναμένεται να χρησιμοποιηθεί. Οι βασικοί παράγοντες που θα πρέπει να αξιολογούν οι κατασκευαστές είναι:

- Οι κατασκευαστές θα πρέπει να ελέγχουν συστηματικά τόσο το λογισμικό όσο και τα εξαρτήματα της συσκευής, ώστε να εντοπίζονται έγκαιρα γνωστά σφάλματα ή αδυναμίες. Τεχνικές όπως η σάρωση για ευπάθειες και η ανάλυση της σύνθεσης του λογισμικού αποτελούν ενδεικτικά παραδείγματα διαδικασιών που θα πρέπει να εφαρμόζονται σε τακτική βάση.
- Χρήση τεχνικών δοκιμών όπως οι αναλύσεις ασφάλειας και η αναζήτηση εναλλακτικών σημείων εισόδου μέσω της ανάγνωσης κρυφών αρχείων, ρυθμίσεων, ροών δεδομένων ή καταχωρητών του υλικού.
- Αξιολόγηση της τρωτότητας που περιλαμβάνει την ανάλυση του πιθανού αντίκτυπού της σε συσκευές άλλων κατασκευαστών, τον εντοπισμό των απαραίτητων διορθωτικών ενεργειών και την επιδιόρθωση ή τον περιορισμό της τρωτότητας.

Δεδομένης της συνεχούς εξέλιξης των τεχνολογιών και των απειλών στον τομέα της κυβερνοασφάλειας, οι κατασκευαστές οφείλουν να αναπτύσσουν ένα ολοκληρωμένο σχέδιο διαχείρισης κυβερνοασφάλειας που θα καλύπτει ολόκληρο τον κύκλο ζωής της συσκευής. Το σχέδιο θα πρέπει να ενσωματώνεται στην ανάπτυξη της συσκευής και να εστιάζει σε:

- Προληπτική παρακολούθηση και αναγνώριση καινούργιων τρωτών σημείων στην κυβερνοασφάλεια, αξιολόγηση των απειλών τους και κατάλληλες αντιδράσεις.
- Επίσημη δημοσιοποίηση των γνωστών τρωτών σημείων με τις ανάλογες προτεινόμενες στρατηγικές μετριασμού, οι οποίες κοινοποιούνται σε όλα τα μέλη που εμπλέκονται στη χρήση ιατρικών συσκευών.
- Καθορισμένο και κοινόχρηστο σχέδιο ενημέρωσης λογισμικού, το οποίο είτε θα ενεργοποιείται κατόπιν αιτήματος είτε θα εφαρμόζεται περιοδικά.
- Σχέδιο αποκατάστασης για την επανέναρξη της κανονικής λειτουργίας της συσκευής, μετά από ενδεχόμενο περιστατικό κυβερνοασφάλειας
- Ανταλλαγή πληροφοριών σχετικά με τους κινδύνους ασφαλείας

Οι κατασκευαστές πρέπει να παρέχουν πλήρη και λεπτομερή τεκμηρίωση που αφορά την ασφάλεια της ιατρικής συσκευής. Η τεκμηρίωση αυτή μπορεί να περιλαμβάνει πληροφορίες σχετικές με την επισήμανση, τον τελικό χρήστη, τις κανονιστικές απαιτήσεις, το σχεδιασμό του συστήματος (τόσο λογισμικά όσο και σε θέμα υλικού), τη διαχείριση κινδύνων και τα αποτελέσματα των δοκιμών ασφαλείας. Αυτές οι πληροφορίες θα πρέπει να είναι διαθέσιμες σε μορφή εγχειριδίων χρήσης, κατευθυντήριων οδηγιών ή τεχνικών συστάσεων, ώστε να διευκολύνεται η κατανόηση και η σωστή εφαρμογή μέτρων ασφαλείας από όλους τους εμπλεκόμενους. [43] [57] [58]

8.5 Ιατρικές συσκευές με ξεπερασμένες τεχνολογίες

Ένα μεγάλο ποσοστό ιατρικών συσκευών που κυκλοφορούν δε μπορεί να αντιμετωπίσει επαρκώς τις σύγχρονες απειλές της κυβερνοασφάλειας, καθώς βασίζονται σε ξεπερασμένες ή μη ασφαλείς τεχνολογίες. Ορισμένες από αυτές τις συσκευές σχεδιάστηκαν χωρίς πρόβλεψη για την κυβερνοασφάλεια, κάτι που αποτελεί σοβαρό πρόβλημα τόσο για τη λειτουργικότητά τους όσο και για την προστασία των δεδομένων. Οι προηγμένες ιατρικές δυνατότητες που ενσωματώνουν μερικές συσκευές υπερβαίνουν τις δυνατότητες ασφαλείας τους, προσφέροντας οφέλη στους χρήστες, αλλά αυξάνοντας ταυτόχρονα την ευπάθειά τους. Μια συσκευή δεν είναι απαραίτητα μη ασφαλής λόγω παλαιότητας, καθώς και νεότερες συσκευές μπορεί να φέρουν απαρχαιωμένες τεχνολογίες ασφάλειας, ενώ παλαιότερες μπορεί να παραμένουν ασφαλείς εφόσον έχει γίνει σωστή ενημέρωση των συστημάτων τους. [57] [58]

Για να περιοριστεί η κυκλοφορία νέων ιατρικών συσκευών με ανεπαρκή ασφάλεια, πέρα από την ενσωμάτωση μέτρων κυβερνοασφάλειας στη φάση του σχεδιασμού, οι κατασκευαστές οφείλουν να δηλώνουν ξεκάθαρα πότε λήγει η υποστήριξη και ο κύκλος ζωής της συσκευής, ώστε να γνωρίζουν οι πελάτες πότε θα σταματήσει η επίσημη τεχνική και ασφαλιστική κάλυψη. Όταν πλησιάζει η ημερομηνία

λήξης της υποστήριξης, πρέπει να ενημερώνονται ότι η συσκευή δεν θα θεωρείται πλέον ασφαλής ως προς τις σύγχρονες απειλές και θα πρέπει να αποσυρθεί. Αν η συσκευή συνεχίσει να χρησιμοποιείται μετά από αυτή την ημερομηνία, η ευθύνη για τη διατήρηση της ασφάλειας, καθώς και για τις συνέπειες οποιασδήποτε αστοχίας, βαραίνει αποκλειστικά τον υγειονομικό φορέα ή τον χρήστη.

Για να διευκολύνουν την αντικατάσταση παρωχημένων ιατρικών συσκευών, οι ρυθμιστικές αρχές μπορούν να παροτρύνουν τους κατασκευαστές να εφαρμόζουν προσωρινούς μηχανισμούς ασφαλείας για να περιορίσουν τις γνωστές ευπάθειες μετά τη λήξη του κύκλου ζωής των συσκευών τους. Αυτό θα δώσει στους παρόχους υγειονομικής περίθαλψης επαρκή χρόνο να προετοιμαστούν για την αντικατάσταση των συστημάτων που δεν υποστηρίζονται πλέον. [57] [58]

8.6 Διαδικασίες αντιμετώπισης κυβερνοεπιθέσεων

Οι **μηχανισμοί ελέγχου ταυτότητας** εξασφαλίζουν ότι μόνο εξουσιοδοτημένα άτομα μπορούν να χρησιμοποιούν τις λειτουργίες μιας ιατρικής συσκευής. Πριν επιτραπεί οποιαδήποτε ενέργεια, όπως η ανάγνωση δεδομένων, αξιολογούνται τα δικαιώματα του χρήστη για να διαπιστωθεί εάν είναι κατάλληλα εξουσιοδοτημένος. Οι επιτρεπόμενες και μη επιτρεπόμενες λειτουργίες καθορίζονται από πολιτικές πρόσβασης, οι οποίες ορίζουν ποιος μπορεί να εκτελεί ποιες ενέργειες και υπό ποιες συνθήκες. Για να εφαρμοστεί ο έλεγχος πρόσβασης, είναι προαπαιτούμενη η αυθεντικοποίηση, καθώς οι αποφάσεις βασίζονται στην ταυτοποιημένη οντότητα του χρήστη. [13] [14] [15]

Οι **μηχανισμοί ακεραιότητας ροής ελέγχου** που βασίζονται στην απομόνωση, χρησιμοποιούνται για να προστατέψουν κρίσιμους πόρους και λειτουργίες. Οι μηχανισμοί αυτοί διαχωρίζουν τους πόρους και τις λειτουργίες της συσκευής σε διαφορετικές ζώνες, με τρόπο τέτοιο ώστε το λογισμικό που διαχειρίζεται τις ιατρικές λειτουργίες να είναι απομονωμένο και μη προσβάσιμο από εφαρμογές τρίτων. Η επικοινωνία μεταξύ αυτών των ζωνών γίνεται μέσω κλήσεων του συστήματος ή καθορισμένων σημείων εισόδου, διασφαλίζοντας ότι μόνο κάποιος με εξουσιοδοτημένη πρόσβαση μπορεί να παρέμβει στις ζώνες αυτές. Η προσέγγιση αυτή ωστόσο, δεν αποτρέπει επιθέσεις που προέρχονται από το εσωτερικό, όπως τροποποίηση του firmware.

Η **ανίχνευση ανωμαλιών** αποτελεί μια κρίσιμη τεχνική για τον εντοπισμό κυβερνοεπιθέσεων σε ιατρικές συσκευές. Η μέθοδος βασίζεται στη συνεχή παρακολούθηση της κανονικής λειτουργίας της συσκευής και στον εντοπισμό αποκλίσεων από αυτή. Καταγράφεται και δημιουργείται ένα προφίλ φυσιολογικής συμπεριφοράς με βάση τις ενέργειες της συσκευής, τις εντολές που δέχεται και τη συνδεσιμότητά της. Το σύστημα έπειτα ελέγχει σε πραγματικό χρόνο τη δραστηριότητα της συσκευής και επισημαίνει κάθε ύποπτη μεταβολή, όπως εντολές από άγνωστες πηγές ή αιφνίδιες αλλαγές στις ρυθμίσεις. Βασικό πλεονέκτημα της τεχνική αυτής είναι ότι μπορεί να ανιχνεύσει τόσο απειλές που έχουν συμβεί όσο και καινούργιες απειλές.

Η **αυτόματη απομόνωση** ιατρικής συσκευής έχει ως βασική αρχή την αποσύνδεση της συσκευής από το δίκτυο ή από άλλες κρίσιμες υποδομές, σε περίπτωση που ξεπερνά τα αποδεκτά όρια λειτουργίας ή παρουσιάζει ενδείξεις παραβίασης. Σκοπός είναι να περιοριστεί άμεσα η εξάπλωση της απειλής και να διασφαλιστεί η προστασία των δεδομένων και της ασφάλειας του ασθενούς. Η απομόνωση μπορεί να επιτευχθεί μέσω διαφορετικών τεχνικών, όπως η χρήση firewall, η απενεργοποίηση επιλεγμένων λειτουργιών ή η μετάβαση της συσκευής σε ασφαλή λειτουργία, η οποία επιτρέπει τη συνέχιση μόνο των απαραίτητων λειτουργιών.

Ο **μηχανισμός διακοπής επικοινωνίας** (kill switch) έχει σχεδιαστεί για την άμεση διακοπή της λειτουργίας ή της δικτυακής συνδεσιμότητας της συσκευής, σε περίπτωση εντοπισμού κακόβουλης δραστηριότητας ή προσπάθειας παραβίασης. Πρόκειται για έναν ενσωματωμένο μηχανισμό ασφαλείας,

ο οποίος μπορεί να ενεργοποιηθεί είτε αυτόματα από το ίδιο το σύστημα όταν ανιχνεύσει απειλητική ενέργεια είτε χειροκίνητα από εξουσιοδοτημένο προσωπικό. Ο κύριος στόχος του μηχανισμού είναι να αποτρέψει την εξάπλωση της επίθεσης ή την εκτέλεση εντολών που θα μπορούσαν να υπονομεύσουν τη λειτουργική ακεραιότητα της συσκευής ή να θέσουν σε κίνδυνο την ασφάλεια του ασθενούς. Η ενεργοποίηση του kill switch ενδέχεται να οδηγήσει σε προσωρινή διακοπή λειτουργίας της συσκευής, οπότε η χρήση του είναι απαραίτητη σε σενάρια υψηλού κινδύνου.

Το **live patching** και οι μηχανισμοί **runtime protection** επιτρέπουν την ενημέρωση και προστασία των συσκευών σε πραγματικό χρόνο χωρίς την ανάγκη επανεκκίνησης ή διακοπής λειτουργιών. Μειώνεται δραστικά το χρονικό διάστημα κατά το οποίο μια συσκευή παραμένει εκτεθειμένη σε νέες επιθέσεις, παρέχοντας συνεχή προστασία. Οι τεχνικές runtime protection επιτρέπουν την παρακολούθηση της εκτέλεσης του συστήματος σε πραγματικό χρόνο, ανιχνεύοντας αποκλίσεις από τη φυσιολογική συμπεριφορά και παρέχοντας έγκαιρη απόκριση σε παραβιάσεις, πριν προκληθούν σοβαρές επιπτώσεις. [13] [14] [15]

8.7 Επίλογος

Σε αυτό το κεφάλαιο αναλύθηκαν οι ενέργειες που πρέπει να γίνονται στα μέτρα κυβερνοασφάλειας των ιατρικών συσκευών πριν και μετά την κυκλοφορία τους στην αγορά. Παρουσιάστηκαν οι τρόποι με τους οποίους μπορούν να αντιμετωπιστούν οι κυβερνοεπιθέσεις έναντι ιατρικών συσκευών.

Κεφάλαιο 9ο: Συμπεράσματα

Έχοντας το πρώτο κεφάλαιο ως εισαγωγικό το οποίο περιγράφει τα περιεχόμενα των υπόλοιπων κεφαλαίων, ξεκινώντας από το δεύτερο κεφάλαιο, έγινε ανάλυση στην εξέλιξη των ιατρικών συσκευών με την πάροδο του χρόνου, στην κατηγοριοποίησή τους, καθώς και στα πρωτόκολλα επικοινωνίας που χρησιμοποιούν. Στο τρίτο κεφάλαιο έγινε αναφορά στους όρους ασφάλειας πληροφοριών και κυβερνοασφάλειας, αναλύθηκε η εξέλιξη του ιού του υπολογιστή, καθώς και τα μέρη και οι φάσεις ενός ιού και έγινε εκτενής αναφορά τόσο στις ευπάθειες της κυβερνοασφάλειας, όσο και στις επιθέσεις κυβερνοασφάλειας. Στο τέταρτο κεφάλαιο αναφέρθηκαν οι τρόποι με τους οποίους τα νομικά συστήματα ρυθμίζουν την κυβερνοασφάλεια των ιατρικών συσκευών και νομικά πλαίσια για την κυβερνοασφάλεια των ιατρικών συσκευών. Στο πέμπτο κεφάλαιο παρουσιάστηκαν πρότυπα κυβερνοασφάλειας τόσο από διεθνείς οργανισμούς, όσο και από ιδιωτικούς φορείς, που θα πρέπει να ακολουθούν οι κατασκευαστές των ιατρικών συσκευών. Στο έκτο κεφάλαιο αναλύθηκαν οι ευπάθειες κυβερνοασφάλειας των ιατρικών συσκευών, τόσο σε επίπεδο υλικού όσο και σε λογισμικού και εξετάστηκαν τρόποι μετρίασης των ευπαθειών. Στο έβδομο κεφάλαιο μελετήθηκαν τα κίνητρα και οι τύποι των επιτιθέμενων, καθώς και οι κατηγορίες των επιθέσεων. Αναλύθηκαν επίσης οι ομάδες στόχων που θέλουν να βλάψουν οι κυβερνοεπιθέσεις, καθώς και τα είδη των επιθέσεων. Παρουσιάστηκε έπειτα η μεθοδολογία STRIDE. Στο όγδοο και τελευταίο κεφάλαιο παρουσιάστηκαν οι ενέργειες που πρέπει να γίνονται για την κυβερνοασφάλεια της συσκευής, τόσο πριν την κυκλοφορία της όσο και μετά, καθώς και οι τρόποι με τους οποίους μπορούν να αντιμετωπιστούν οι κυβερνοεπιθέσεις έναντι ιατρικών συσκευών.

Παίρνοντας ως γνώμονα όλα όσα έχουν αναφερθεί στα παραπάνω κεφάλαια, γίνεται αντιληπτή η σημαντικότητα της σωστής προετοιμασίας και εφαρμογής των μέτρων κυβερνοασφάλειας που πρέπει να λαμβάνει μια ιατρική συσκευή, καθώς οι απειλές είναι πολυάριθμες και ο χρόνος αντίδρασης μικρός, με αποτέλεσμα να βρίσκεται σε κίνδυνο τόσο η ασφάλεια όσο και η ζωή των ασθενών. Παρόλα αυτά, αποδεικνύεται ότι μελλοντικά όσο και να βελτιωθούν τα μέτρα κυβερνοασφάλειας των ιατρικών συσκευών, οι επιτιθέμενοι πάντα θα βελτιώνουν και αυτοί τις γνώσεις τους και θα είναι σε θέση πάλι να βρουν νέους τρόπους για να απειλήσουν την ακεραιότητα και τη σωστή λειτουργία των ιατρικών συσκευών. Η κυβερνοασφάλεια των ιατρικών συσκευών θα πρέπει να αντιμετωπίζεται ως μια διαρκής και δυναμική διαδικασία, η οποία απαιτεί συνεχή αξιολόγηση, τακτική ενημέρωση και προσαρμογή στις νέες τεχνολογικές και απειλητικές εξελίξεις. Η στενή συνεργασία μεταξύ κατασκευαστών, επαγγελματιών υγείας και ειδικών κυβερνοασφάλειας είναι καθοριστική για την ανάπτυξη ενός ασφαλούς ψηφιακού περιβάλλοντος στον τομέα της υγείας.

Ως μελλοντικές έρευνες, καθώς εξελίσσονται συνεχώς οι ιατρικές συσκευές, θα ήταν σκόπιμο να μελετηθούν ακόμα περισσότεροι και πιο εξειδικευμένοι τρόποι αντιμετώπισης των ευπαθειών και των επιθέσεων, όπως να υπάρχει πιο ισχυρή ενσωματωμένη κρυπτογράφηση στις συσκευές, πιο ισχυρές μπαταρίες που θα αντέχουν σε επιθέσεις εξάντλησης πόρων, πιο ισχυροί μηχανισμοί ελέγχου ταυτότητας, όπως με τη χρήση βιομετρικών στοιχείων και μηχανισμοί μηχανικής μάθησης που θα ανιχνεύουν νωρίτερα τις επερχόμενες επιθέσεις.

ΒΙΒΛΙΟΓΡΑΦΙΑ

[1] World Health Organization "Health products policy and standards: assistive and medical technology; medical devices" Last Visit: Nov. 4, 2024. [Online]. Available: https://www.who.int/teams/health-product-policy-and-standards/assistive-and-medical-technology/medical-devices

[2] K. Asanuma "Definition of the Terms 'Medical Device' and 'In Vitro Diagnostic (IVD) Medical Device'" Global Harmonization Task Force (revision of GHTF/SG1/N29:2005), May 16, 2012

[3] D. Arney, K. Venkatasubramanian, O. Sokolsky, I. Lee "Biomedical Devices and Systems Security", 33rd Annual International Conference of the IEEE Engineering in Medicine and Biology Society (EMBC '11), 2376-2379. August 2011. doi: 10.1109/IEMBS.2011.6090663

[4] A. Alsuwaidi, A. Hassan, F. Alkhatri, H. Ali, M. Qbea'H, S. Alrabaee "Security Vulnerabilities Detected in Medical Devices" 12th Annual Undergraduate Research Conference on Applied Computing (URC), Dubai, United Arab Emirates, 2020. May 25th 2020. doi: 10.1109/URC49805.2020.9099192

[5] UMass Diabetes Center of Excellence "The First Human Insulin Injection to Treat Diabetes Leonard Thompson | January 11 & 23, 1922" Last Visit: Nov. 19, 2024. [Online]. Available: https://www.umassmed.edu/dcoe/diabetes-education/patient-resources/first-insulin-injection/

[6] American Diabetes Association "The History of a Wonderful Thing We Call Insulin", Last Visit: Nov. 19, 2024. [Online]. Available: https://diabetes.org/blog/history-wonderful-thing-we-call-insulin

[7] K. Sansurooah "Security risks of medical devices in wireless environments", 4th Australian eHealth Informatics and Security Conference, Perth, Western Australia, Dec. 2015. doi: 10.14221/aeis.2015.1

[8] Omnipod "What is Omnipod", Last Visit: Nov. 19, 2024. [Online]. Available: https://www.omnipod.com/what-is-omnipod/omnipod-5

[9] Understanding Animal Research "History of the Pacemaker", Last Visit: Nov. 25, 2024. [Online]. Available: https://www.understandinganimalresearch.org.uk/news/top-ten-medical-inventions-pacemakers

[10] Wikipedia "Pacemaker", Last Visit: Nov. 25, 2024. [Online]. Available: https://en.wikipedia.org/wiki/Pacemaker#History

[11] Healthcare-in-Europe "Pacemakers with internet connection", Last Visit: Nov. 25, 2024. [Online]. Available: https://healthcare-in-europe.com/en/news/pacemakers-with-internet-connection.html

[12] AF-Ablation "Arrythmological Procedures and Therapies / Implantable Devices System / Wireless Pacemaker", Last Visit: Nov. 25, 2024. [Online]. Available: https://af-ablation.org/en/arrythmological-procedures-and-therapies/implantable-devices-system/wireless-pacemaker/

[13] C. Thyagarajan, S. Vijay Bhanu, S. Suthir "Survey on IoT based Cyber Security Issues and Autonomous Solutions for Implantable Medical Devices", International Journal on Recent and Innovation Trends in Computing and Communication, vol. 11, no. 8, June 29th, 2023. doi: 10.17762/ijritcc.v11i8s.7188

[14] C. Camara Nunez "Cybersecurity in Implantable Medical Devices", Carlos III University of Madrid, Doctoral thesis, Dec. 19, 2017.

[15] T. Yaqoob, H. Abbas, M. Atiquzzaman “Security Vulnerabilities, Attacks, Countermeasures, and Regulations of Networked Medical Devices – A Review”, IEEE Communications Surveys & Tutorials, vol. 21, no. 4, p. 3723 – 3768, April 30th, 2019. doi: 10.1109/COMST.2019.2914094

[16] NIST Computer Security Resource Center “Information Security”, Last Visit: Jan. 16th, 2025. [Online]. Available: https://csrc.nist.gov/glossary/term/information_security

[17] IBM “What is information security (InfoSec)?”, Last Visit: Jan. 16th, 2025. [Online]. Available: https://www.ibm.com/think/topics/information-security

[18] Microsoft “What is information security (InfoSec)?” Last Visit: Jan. 16th, 2025. [Online]. Available: https://www.microsoft.com/en-us/security/business/security-101/what-is-information-security-infosec#key-elements-of-InfoSec

[19] Cisco “What is cybersecurity?”, Last Visit: Jan. 17th, 2025. [Online]. Available: https://www.cisco.com/site/us/en/learn/topics/security/what-is-cybersecurity.html

[20] Cisco “What is information security?”, Last Visit: Jan. 17th, 2025. [Online]. Available: https://www.cisco.com/site/us/en/learn/topics/security/what-is-information-security-infosec.html

[21] NIST Computer Security Resource Center “Virus”, Last Visit: Jan. 17th, 2025. [Online]. Available: https://csrc.nist.gov/glossary/term/virus

[22] Kaspersky “A Brief History of Computer Viruses & What the Future Holds”, Last Visit: Jan. 17th, 2025. [Online]. Available: https://www.kaspersky.com/resource-center/threats/a-brief-history-of-computer-viruses-and-what-the-future-holds

[23] IBM “The history of malware: A primer on the evolution of cyber threats”, Last Visit: Jan. 17th, 2025. [Online]. Available: https://www.ibm.com/think/topics/malware-history

[24] Wikipedia “Ransomware”, Last Visit: Jan. 24th, 2025. [Online]. Available: https://el.wikipedia.org/wiki/Ransomware

[25] Wikipedia “Computer Virus”, Last Visit: Jan. 17th, 2025. [Online]. Available: https://en.wikipedia.org/wiki/Computer_virus

[26] M. Humayun, M. Niazi, N. Jhanjhi, M. Alshayeb, S. Mahmood “Cybersecurity Threats and Vulnerabilities : Systematic Mapping Study", College of Computer and Information Science, Jouf University, Al-Jouf, Saudi Arabia, Jan. 2020.

[27] V. Hegde “Cybersecurity for Medical Devices”, 2018 Annual Reliability and Maintainability Symposium (RAMS), Reno, NV, USA, Jan. 2018. doi: 10.1109/RAM.2018.8463049

[28] Checkpoint “Top 8 Cyber Security Vulnerabilities”, Last Visit: Jan. 27th, 2025. [Online]. Available: https://www.checkpoint.com/cyber-hub/cyber-security/top-8-cyber-security-vulnerabilities/

[29] Keeper Security “Common Types of Cybersecurity Vulnerabilities”, Last Visit: Jan. 27th, 2025. [Online]. Available: https://www.keepersecurity.com/blog/2023/12/27/common-types-of-cybersecurity-vulnerabilities/

[30] K. Bennouk, N. Ait Aali, Y. El Bouzerki El Idrissi, B. Sebai, A. Zakaria Faroukhi, D. Mahouachi “A Comprehensive Review and Assessment of Cybersecurity Vulnerability Detection Methodologies”, Journal of Cybersecurity and Privacy, vol. 4, p. 853 – 908, Oct. 2024. doi: 10.3390/jcp4040040

[31] Crowdstrike “12 Most common types of Cyberattacks”, Last Visit: Jan 29th, 2025. [Online]. Available: https://www.crowdstrike.com/en-us/cybersecurity-101/cyberattacks/common-cyberattacks/

[32] O. Aslan, S. Serkant Aktug, M. Ozkan-Okay, A. Asim Yilmaz, E. Akin “A Comprehensive Review of Cyber Security Vulnerabilities, Threats, Attacks, and Solutions”, Electronics 2023, 12(6), 1333, Mar. 13th, 2023. doi: 10.3390/electronics12061333

[33] Rapid7 “Types of Cybersecurity Attacks”, Last Visit: Feb. 4th, 2025. [Online]. Available: https://www.rapid7.com/fundamentals/types-of-attacks/

[34] DeVry University “9 Essential Cyber Security Tools and Techniques”, Last Visit: Feb. 4th, 2025. [Online]. Available: https://www.devry.edu/blog/cyber-security-tools-and-techniques.html#firewalls

[35] Wikipedia “Antivirus software”, Last Visit: Feb. 18th, 2025. [Online]. Available: https://en.wikipedia.org/wiki/Antivirus_software

[36] Wikipedia “Encryption”, Last Visit: Feb. 18th, 2025. [Online]. Available: https://en.wikipedia.org/wiki/Encryption

[37] K. Rosager Ludvigsen “The Role of Cybersecurity in Medical Devices Regulation: Future Considerations and Solutions”, Law, Technology and Humans, vol. 5, 2023. doi: 10.5204/lthj.3080

[38] E. Biasin, B. Yasar, E. Kamenjasevic “New Cybersecurity Requirements for Medical Devices in the EU: The Forthcoming European Health Data Space, Data Act, and Artificial Intelligence Act”, Law, Technology and Humans, vol. 5, 2023. doi: 10.5204/lthj.3068

[39] T. Melvin “The European Medical Device Regulation – What Biomedical Engineers Need to Know”, IEEE Journal of Translational Engineering in Health and Medicine, vol. 10, July 28th, 2022. doi: 10.1109/JTEHM.2022.3194415

[40] T. Yaqoob, H. Abbas, N. Shafqat “Integrated Security, Safety, and Privacy Risk Assessment Framework for Medical Devices”, IEEE Journal of Biomedical and Health Informatics, vol. 24, no. 6, p. 1752 – 1761, Nov. 19th, 2019. doi: 10.1109/JBHI.2019.2952906

[41] ISO “About ISO”, Last Visit: Mar. 18th, 2025. [Online]. Available: https://www.iso.org/about

[42] Wikipedia “International Electrotechnical Commission”, Last Visit: Mar. 18th, 2025. [Online]. Available: https://en.wikipedia.org/wiki/International_Electrotechnical_Commission

[43] K. Dong-Won, C. Jin-Young, H. Keun-Hee “Medical Device Safety Management Using Cybersecurity Risk Analysis”, IEEE Access, vol. 8, p. 115370 – 115382, June 17th, 2020. doi: 10.1109/ACCESS.2020.3003032

[44] S. Yuan, A. Fernando, D. C. Klonoff “Standards for Medical Device Cybersecurity in 2018”, Journal of Diabetes Science and Technology, vol. 12, no. 4, Mar. 24th, 2018. doi: 10.1177/19322968187636

[45] P. AH Williams, A. J. Woodward “Cybersecurity vulnerabilities in medical devices: a complex environment and multifaceted problem”, Medical Devices: Evidence and Research, p. 305 – 316, July 20th, 2015. doi: 10.2147/MDER.S50048

[46] A. Longras, H. Oliveira, S. Paiva “Security Vulnerabilities on Implantable Medical Devices”, 15th Iberian Conference on Information Systems and Technologies (CISTI), Seville, Spain, June 2020. doi: 10.23919/CISTI49556.2020.9141043

[47] S. B. Schwartz “Medical Devices: A Practical Guide for Securing Patient Data”, Safeguarding Health Information: Building Assurance through HIPAA Security, Sep. 23th, 2014.

[48] A. Razaque, F. Amsaad, M. Jaro Khan, S. Hariri, S. Chen, C. Siting, X. Ji “Survey: Cybersecurity Vulnerabilities, Attacks and Solutions in the Medical Domain”, IEEE Access, vol. 7, p. 168774 – 168797, Oct. 31st, 2019. doi: 10.1109/ACCESS.2019.2950849

[49] M. Zhang, A. Raghunathan, N. K. Jha “Trustworthiness of Medical Devices and Body Area Networks”, Proceedings of the IEEE, vol. 102, no. 8, p. 1174 – 1188, June 6th, 2014. doi: 10.1109/JPROC.2014.2322103

[50] L. Bracciale, P. Loreti, G. Bianchi “Cybersecurity vulnerability analysis of medical devices purchased by national health services”, Nature.com Sci Rep 13, vol. 19509, Nov. 9th, 2023. doi: 10.1038/s41598-023-45927-1

[51] American College of Surgeons “Surgeons Need to Engage in Battle against Cyberattacks”, Last Visit: Apr. 29th, 2025. [Online]. Available: https://www.facs.org/for-medical-professionals/news-publications/news-and-articles/bulletin/2025/april-2025-volume-110-issue-4/surgeons-need-to-engage-in-battle-against-cyberattacks/

[52] K. K. Venkatasubramanian, E. Y. Vasserman, O. Sokolsky, I. Lee “Security and Interoperable Medical Device Systems: Part 1”, IEEE Security & Privacy, vol. 10, no. 5, p. 61 – 63, Oct. 4th, 2012. doi: 10.1109/MSP.2012.128

[53] The Guardian “Hackable implanted medical devices could cause deaths, researchers say”, Last Visit: May 2nd, 2025. [Online]. Available: https://www.theguardian.com/technology/2018/aug/09/implanted-medical-devices-hacking-risks-medtronic

[54] The Register “It’s the real Heart Bleed: Medtronic locks out vulnerable pacemaker programmer kit”, Last Visit: May 2nd, 2025. [Online]. Available: https://www.theregister.com/2018/10/12/medtronic_pacemaker_programmer_security/

[55] D. Halperin, T. S. Heydt-Benjamin, B. Ransford, S. S. Clark, B. Defend, W. Morgan, K. Fu, T. Kohno, W. H. Maisel “Pacemakers and Implantable Cardiac Defibrillators: Software Radio Attacks and Zero-Power Defenses”, IEEE Symposium on Security and Privacy, Oakland, CA, USA, May 28th, 2008. doi: 10.1109/SP.2008.31

[56] M. Muneeb Ur Rehman, H. Zia Ur Rehman, Z. Hameed Khan “Cyber-Attacks on Medical Implants: A Case Study of Cardiac Pacemaker Vulnerability”, International Journal of Computing and Digital Systems, vol. 9, no. 6, Nov. 2020. doi: 10.12785/ijcds/0906020

[57] L. Jelic “Cybersecurity, Data Protection, and Artificial Intelligence in Medical Devices”, Inspection of Medical Devices, Series in Biomedical Engineering, p. 417 – 445, Nov. 27th, 2023. doi: 10.1007/978-3-031-43444-0_17

[58] H. Hamidovic, J. Kabil, E. Sehic “Management of Cybersecurity in Medical Devices”, DIEC, Tuzla, Bosnia and Herzegovina, July 2020.