ΠΑΝΕΠΙΣΤΗΜΙΟ ΑΙΓΑΙΟΥ
ΠΟΛΥΤΕΧΝΙΚΗ ΣΧΟΛΗ

ΤΜΗΜΑ ΜΗΧΑΝΙΚΩΝ ΠΛΗΡΟΦΟΡΙΑΚΩΝ ΚΑΙ ΕΠΙΚΟΙΝΩΝΙΑΚΩΝ ΣΥΣΤΗΜΑΤΩΝ

Ανάλυση κινδύνων και Αξιολόγηση Επιπτώσεων για περιπτώσεις χρήσης IoT

ΔΙΠΛΩΜΑΤΙΚΗ ΕΡΓΑΣΙΑ

της

Χριστίνας Νικολέτας Μεθενίτης

Επιβλέπων : Κωνσταντίνος Μαλιάτσος

Μέλη εξεταστικής επιτροπής: Μαρία Καρύδα, Βασιλική Διαμαντοπούλου

Σάμος, Οκτώβριος 2024

Πρόλογος και ευχαριστίες

Η παρούσα διπλωματική εργασία εκπονήθηκε στο πλαίσιο των σπουδών μου στο Τμήμα Μηχανικών Πληροφοριακών και Επικοινωνιακών Συστημάτων της Πολυτεχνικής Σχολής του Πανεπιστημίου Αιγαίου. Η ολοκλήρωσή της αποτέλεσε μια σημαντική και απαιτητική διαδικασία, γεμάτη προκλήσεις και μαθήματα, που συνέβαλαν στην ακαδημαϊκή μου ανάπτυξη.

Πρώτα απ' όλα, θα ήθελα να ευχαριστήσω τον επιβλέποντα καθηγητή μου, Κωνσταντίνο Μαλιάτσο, για την αμέριστη υποστήριξή του, τις πολύτιμες συμβουλές του και την καθοδήγησή του καθ' όλη τη διάρκεια της εργασίας. Οι γνώσεις και η εμπειρία του υπήρξαν ανεκτίμητες για την ολοκλήρωση αυτού του έργου.

Επίσης ευχαριστίες οφείλω στους συναδέλφους και συμφοιτητές μου, που με την υποστήριξή τους και τις συζητήσεις μας, μου προσέφεραν έμπνευση και κίνητρο να συνεχίσω. Οι ανταλλαγές απόψεων και οι συνεργασίες μας ήταν καθοριστικές για την πρόοδο της έρευνάς μου.

Δεν θα μπορούσα να παραλείψω την οικογένειά μου, που στάθηκε δίπλα μου με ατελείωτη υπομονή και ενθάρρυνση σε κάθε βήμα αυτού του ταξιδιού. Η υποστήριξη και η πίστη τους σε μένα υπήρξαν το θεμέλιο για την επίτευξη των στόχων μου.

Τέλος, ευχαριστώ όλους όσους, με οποιονδήποτε τρόπο, συνέβαλαν στην ολοκλήρωση αυτής της διπλωματικής εργασίας. Χωρίς τη βοήθειά τους, αυτή η προσπάθεια δεν θα είχε φτάσει στο σημερινό της αποτέλεσμα.

Σάμος, Ιούλιος 2024
ΧΡΙΣΤΙΝΑ ΝΙΚΟΛΕΤΑ ΜΕΘΕΝΙΤΗ
Τμήμα Μηχανικών Πληροφοριακών και Επικοινωνιακών Συστημάτων
ΠΑΝΕΠΙΣΤΗΜΙΟ ΑΙΓΑΙΟΥ

Περιεχόμενα

Περίληψη

Η εργασία με τίτλο "Ανάλυση κινδύνων και Αξιολόγηση Επιπτώσεων για περιπτώσεις χρήσης IoT" επικεντρώνεται στην εξέταση των πιθανών κινδύνων και των επιπτώσεων που σχετίζονται με την χρήση των συστημάτων IoT σε συγκεκριμένες περιπτώσεις χρήσης. Με την εφαρμογή μεθόδων ανάλυσης κινδύνων και αξιολόγησης επιπτώσεων, η εργασία αναλύει τις πιθανές απειλές και τις πιθανές επιπτώσεις που μπορεί να έχει η χρήση των συσκευών IoT σε διάφορα περιβάλλοντα.

Στο τελευταίο τμήμα της εργασίας, παρουσιάζεται ένα παράδειγμα εφαρμογής του IoT στην τηλεχειρουργική. Αναλύονται οι διάφοροι κίνδυνοι που μπορεί να ενέχει η χρήση των συσκευών IoT σε αυτό το περιβάλλον, καθώς και οι επιπτώσεις που μπορεί να προκύψουν από αυτούς τους κινδύνους. Μέσω αυτής της ανάλυσης, προτείνονται μέτρα ασφαλείας και προληπτικές δράσεις που μπορούν να ληφθούν για τη μείωση των κινδύνων και την αντιμετώπιση των πιθανών επιπτώσεων. Μέσω αυτής της εργασίας, προσφέρεται ένας συστηματικός τρόπος αντιμετώπισης των κινδύνων και της αξιολόγησης των επιπτώσεων για περιπτώσεις χρήσης IoT, εστιάζοντας συγκεκριμένα στην εφαρμογή τους στην τηλεχειρουργική.

Λέξεις Κλειδιά: *Internet of Things, ανάλυση κινδύνων, αξιολόγηση επιπτώσεων, τηλεχειρουργική, ασφάλεια δεδομένων, προληπτικές δράσεις, IoT, συστήματα υγείας.*

Abstract

The thesis titled "Risk Analysis and Impact Assessment for IoT Use Cases" focuses on examining the potential risks and impacts associated with the use of IoT systems in specific use cases. By applying risk analysis and impact assessment methods, the paper analyzes the possible threats and impacts that IoT device usage may have in various environments.

In the final section, an example of IoT application in tele-surgery is presented. The various risks associated with the use of IoT devices in this environment are analyzed, as well as the potential impacts that could arise from these risks. Through this analysis, security measures and preventive actions are proposed to mitigate risks and address potential impacts. This paper offers a systematic approach to handling risks and assessing impacts for IoT use cases, specifically focusing on their application in tele-surgery.

Λέξεις Κλειδιά: *Internet of Things, Risk analysis, impact assessment, telesurgery, data security, προληπτικές δράσεις, IoT, smart health.*

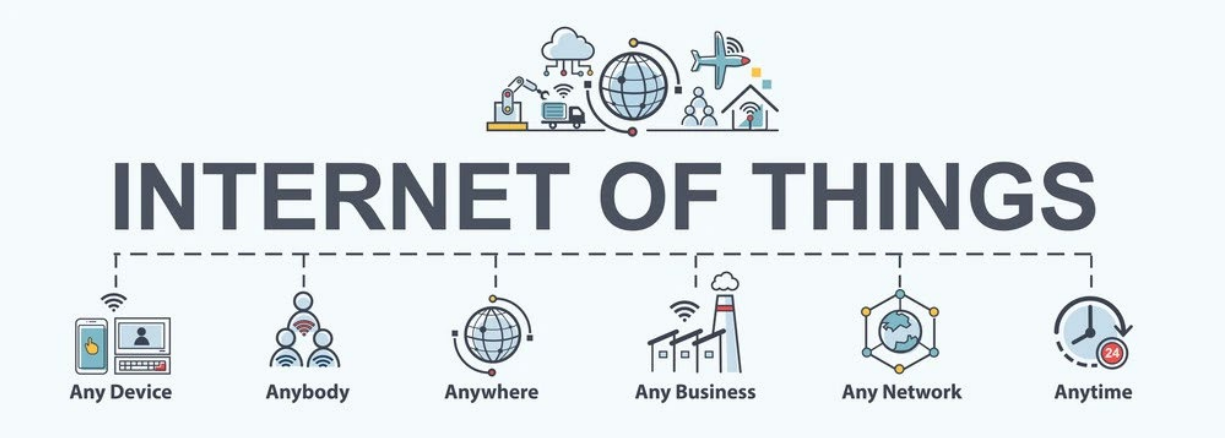
1. Εισαγωγή

1.1 Internet of Things

Το Διαδίκτυο των πραγμάτων ή Internet of Things ή Iot αποτελεί το δίκτυο επικοινωνίας πληθώρας συσκευών, π.χ. οικιακών συσκευών, αυτοκινήτων καθώς και κάθε αντικειμένου που ενσωματώνει ηλεκτρονικά μέσα, λογισμικό, αισθητήρες και συνδεσιμότητα σε δίκτυο ώστε να επιτρέπεται η ανταλλαγή δεδομένων. Απλούστερα, η φιλοσοφία του IoT είναι η σύνδεση όλων των ηλεκτρονικών συσκευών μεταξύ τους (σε τοπικό δίκτυο) ή με δυνατότητα σύνδεσης στο διαδίκτυο (παγκόσμιο ιστό). [1]

Οι συσκευές IoT μπορούν να περιλαμβάνουν οτιδήποτε, από αισθητήρες περιβάλλοντος (όπως θερμοκρασίας, υγρασίας και κίνησης) μέχρι συσκευές όπως οι έξυπνες τηλεοράσεις, οι φωτιστικές συσκευές, οι αυτόματες πύλες και άλλες ηλεκτρονικές συσκευές. Το κύριο χαρακτηριστικό του IoT είναι ότι αυτές οι συσκευές μπορούν να επικοινωνούν μεταξύ τους και να λαμβάνουν εντολές ή να ανταλλάσσουν δεδομένα μέσω του διαδικτύου, χωρίς την ανθρώπινη παρέμβαση.

Στις μέρες μας όλο και περισσότερες συσκευές είναι συνδεδεμένες στο διαδίκτυο, οι οποίες όλες συλλέγουν και μοιράζονται δεδομένα ακολουθώντας πρωτόκολλα επικοινωνίας. Η τεχνολογία IoT έχει υιοθετηθεί από πολλές εταιρίες οι οποίες θέλουν να απλοποιήσουν, να βελτιώσουν, να αυτοματοποιήσουν και να ελέγξουν διαφορετικές διαδικασίες.



Εικόνα 1: Πτυχές και στόχοι του IoT

1.2 IoT και Blockchain

Το **blockchain** και το **Internet of Things (IoT)** αποτελούν δύο διακριτά, όμως συνδεδεμένα πεδία τεχνολογίας που μπορούν να συνεργαστούν προκειμένου να βελτιώσουν την ασφάλεια, τη διαφάνεια και την αποδοτικότητα σε εφαρμογές IoT. Κάποιοι τρόποι με τους οποίους το blockchain σχετίζεται με το IoT περιλαμβάνουν:

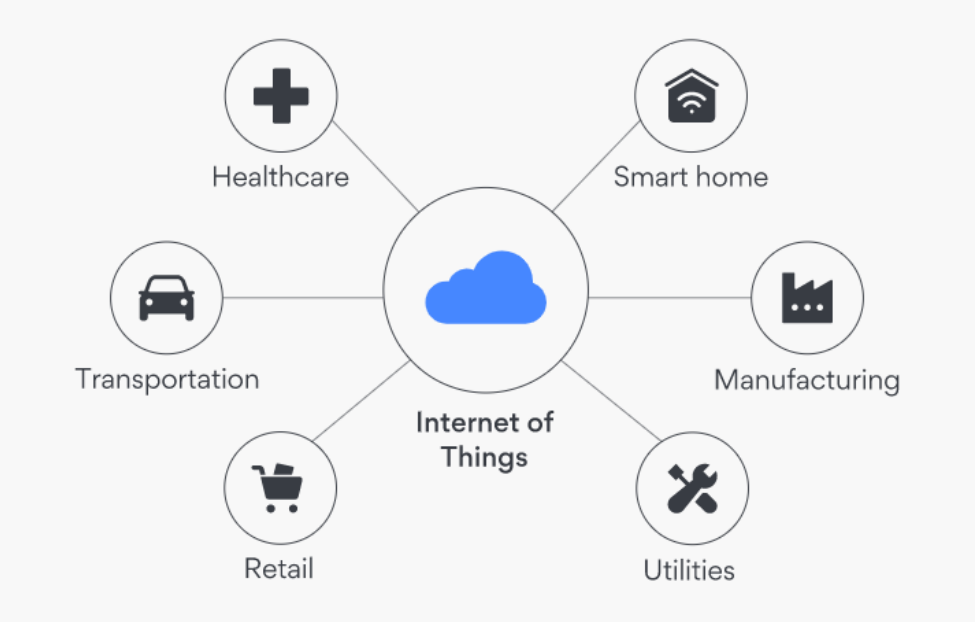
- **Προστασία:** Το blockchain μπορεί να παρέχει αυξημένη ασφάλεια στα δίκτυα IoT. Μέσω της κρυπτογραφίας και του ασφαλούς κατανεμημένου καταλόγου, μπορεί να διασφαλίσει την προστασία των δεδομένων και των συσκευών από ανεπιθύμητες επεμβάσεις.
- **Διαφάνεια:** Το blockchain καταγράφει κάθε μεταβολή ή συναλλαγή στον κατανεμημένο κατάλογο, ο οποίος είναι προσβάσιμος για όλους τους συμμετέχοντες στο δίκτυο IoT. Αυτό μπορεί να βελτιώσει τη διαφάνεια στον τρόπο λειτουργίας των συσκευών IoT.
- **Εξουσιοδότηση (authorization):** Το blockchain μπορεί να χρησιμοποιηθεί για τη διαχείριση της εξουσιοδότησης και της ταυτοποίησης συσκευών στο IoT. Αυτό μπορεί να εξασφαλίσει ότι μόνο εξουσιοδοτημένα συστήματα έχουν πρόσβαση σε συγκεκριμένα δεδομένα ή λειτουργίες.
- **Αποθήκευση δεδομένων:** Το blockchain μπορεί να χρησιμοποιηθεί για την αποθήκευση δεδομένων από τις συσκευές IoT. Αυτό δημιουργεί ένα αξιόπιστο κατανεμημένο αποθετήριο δεδομένων που μπορεί να χρησιμοποιηθεί για ανάλυση, αναφορές και άλλες εφαρμογές.
- **Έξυπνα συμβόλαια:** Το blockchain υποστηρίζει τα έξυπνα συμβόλαια, τα οποία είναι προγράμματα που εκτελούν αυτόματα συγκεκριμένες ενέργειες όταν πληρούνται συγκεκριμένες συνθήκες. Αυτό μπορεί να εφαρμοστεί στο IoT για την αυτόματη εκτέλεση λειτουργιών όταν πληρούνται συγκεκριμένα κριτήρια.

Συνολικά, το blockchain μπορεί να προσφέρει την ασφάλεια, τη διαφάνεια και την αξιοπιστία που απαιτούνται για την αποτελεσματική λειτουργία του IoT, και τα δύο αυτά πεδία μπορούν να συνεργαστούν για τη βελτίωση των εφαρμογών IoT.

1.2.1 Εφαρμογές

Μερικοί από τους τομείς που εφαρμόζονται λύσεις IoT είναι:

- Τομέας Υγείας
- Αγροτικός Τομέας
- Βιομηχανία
- «Έξυπνες Πόλεις» (Smart Cities)
- «Έξυπνα Σπίτια» (Smart Homes)
- Μεταφορές - Logistics
- Εμπόριο
- Wearable συσκευές
- «Έξυπνα» ηλεκτρικά δίκτυα (Smart Grids)
- Συνδεδεμένα Οχήματα



Εικόνα 2: Εφαρμογές του IoT

Το Internet of Things (IoT) λειτουργεί με τη συνεργασία διαφορετικών τεχνολογιών που επιτρέπουν σε συσκευές να συνδεθούν στο διαδίκτυο και να ανταλλάξουν δεδομένα με άλλες συσκευές ή με ανθρώπους. Συνήθως περιλαμβάνει τους παρακάτω βασικούς σταθμούς:

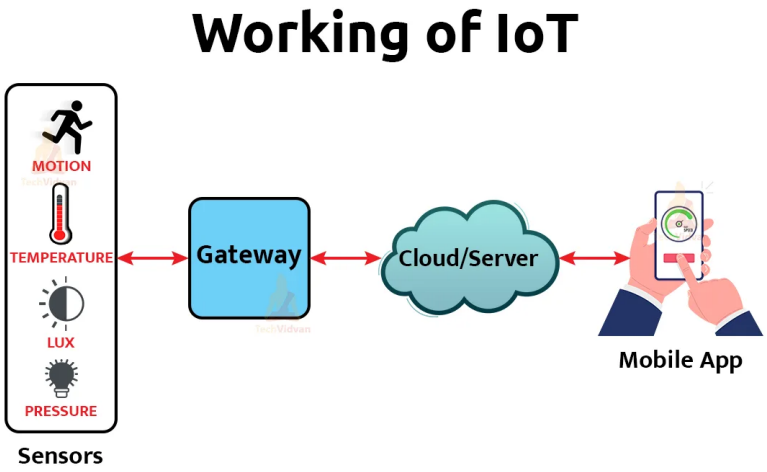
- **Αισθητήρες (Sensors) και Ενεργοποιητές (Actuators):** Οι αισθητήρες είναι μικρές συσκευές που μπορούν να ανιχνεύσουν και να μετρήσουν διάφορες παραμέτρους, όπως η θερμοκρασία, η υγρασία, η πίεση, η κίνηση και άλλα. Οι αισθητήρες συνήθως συνδέονται σε ένα μικρό-ελεγκτή ή μικρό-υπολογιστή που τους επεξεργάζεται και τα στέλνει σε μια εφαρμογή ή σε μια πλατφόρμα IoT. Οι ενεργοποιητές κατά απαίτηση ενεργούν στο περιβάλλον πραγματοποιώντας μιας ενέργεια (π.χ., άνοιγμα βάνας, κλπ).

- **Επεξεργαστές (Processors):** Οι επεξεργαστές είναι υπολογιστικές μονάδες που επεξεργάζονται τα δεδομένα που συλλέγονται από τους αισθητήρες και λαμβάνουν αποφάσεις για την εκτέλεση διαφόρων ενεργειών.
- **Δίκτυα (Networks):** Τα δίκτυα επιτρέπουν στις συσκευές να συνδέονται μεταξύ τους και με το διαδίκτυο, ώστε να μπορούν να ανταλλάσσουν δεδομένα. [1]

Στο Internet of Things, τα αντικείμενα συνδέονται μεταξύ τους μέσω δικτύων και ανταλλάσσουν δεδομένα μεταξύ τους. Για να συμβεί αυτό, τα αντικείμενα χρειάζονται έναν αισθητήρα ή έναν ενσωματωμένο υπολογιστή που να μπορεί να συλλέγει και να αναλύει δεδομένα.

Στη συνέχεια, τα δεδομένα αυτά μπορούν να αναλυθούν και να χρησιμοποιηθούν για να βελτιωθούν διάφοροι τομείς, όπως η παραγωγή, οι μεταφορές, η υγεία, η ασφάλεια, οι υποδομές και άλλοι. Τα δεδομένα μπορούν να χρησιμοποιηθούν για να παράγουν προβλέψεις και να βελτιώσουν την απόδοση, την αποτελεσματικότητα και την ασφάλεια.

Επιπλέον, το Internet of Things επιτρέπει στους χρήστες να ελέγχουν και να παρακολουθούν τα αντικείμενα από απόσταση μέσω μιας εφαρμογής στο κινητό τους τηλέφωνο ή στον υπολογιστή τους. Αυτό μπορεί να γίνει για παράδειγμα, για να ελέγξουν το σπίτι τους, το αυτοκίνητό τους, την υγεία τους ή άλλα συνδεδεμένα αντικείμενα.



Εικόνα 3: Ροή πληροοφορίας για εφαρμογή IoT με συλλογή μετρήσεων από αισθητήρες και παρουσίαση/έλεγχο από κινητό.

1.2.2 Πλεονεκτήματα

Το Internet of Things (IoT) προσφέρει πολλά πλεονεκτήματα σε διάφορους τομείς. Ανάμεσα σε αυτά είναι τα εξής:

- **Βελτιωμένη αποδοτικότητα και παραγωγικότητα:** Οι συνδεδεμένες συσκευές IoT μπορούν να παρακολουθούν, να μετρούν και να αναφέρουν δεδομένα για την απόδοση των μηχανημάτων και των διαδικασιών, επιτρέποντας στους χρήστες να βελτιώσουν την αποδοτικότητα και την παραγωγικότητα αυτών.
- **Αυτοματισμός:** Οι συσκευές IoT μπορούν να επικοινωνούν αναμεταξύ τους και να λειτουργούν αυτόνομα, χωρίς την ανάγκη ανθρώπινης παρέμβασης. Αυτό μπορεί να βελτιώσει την απόδοση και την αποδοτικότητα, καθώς και να μειώσει τον χρόνο και την ενέργεια που απαιτούνται για την εκτέλεση κάποιων διαδικασιών.
- **Αυξημένη ασφάλεια:** Οι συσκευές IoT μπορούν να παρακολουθούν τα περιβάλλοντα στοιχεία και να ανιχνεύουν ανωμαλίες ή κινδύνους. Αυτό μπορεί να βοηθήσει στην πρόληψη ατυχημάτων και αύξηση της ασφάλειας. Επίσης μπορεί να βοηθήσει στη βελτίωση της ασφάλειας σε διάφορα πεδία, όπως στη βιομηχανία και στις κατοικίες. Οι αισθητήρες μπορούν να ανιχνεύουν επικίνδυνες καταστάσεις και να ειδοποιούν τους ανθρώπους ή ακόμα και να προβαίνουν σε αυτόματες ενέργειες για να αποφευχθεί η ατυχήματα.
- **Βελτιωμένη εξοικονόμηση ενέργειας και πόρων:** Το IoT μπορεί να βοηθήσει στην εξοικονόμηση ενέργειας και πόρων με την αυτόματη ρύθμιση του φωτισμού, της θέρμανσης και του κλιματισμού. Για παράδειγμα, ένα έξυπνο σύστημα θέρμανσης και ψύξης μπορεί να ρυθμίζει αυτόματα τη θερμοκρασία σε έναν χώρο με βάση την παρουσία ανθρώπων ή τις καιρικές συνθήκες. Επίσης τα συστήματα φωτισμού IoT μπορούν να προσαρμόζουν τη φωτεινότητα και την απόδοση του φωτισμού βάσει της παρουσίας ανθρώπων ή του επιπέδου φωτισμού που απαιτείται σε έναν συγκεκριμένο χώρο. Αυτό μπορεί να οδηγήσει σε εξοικονόμηση ενέργειας και πόρων.
- **Ευκολία χρήσης και βελτιωμένη ποιότητα ζωής:** Το IoT επιτρέπει στους χρήστες να ελέγχουν και να διαχειρίζονται τις συσκευές τους από απόσταση, μέσω εφαρμογών στα κινητά τους ή από υπολογιστές, κάνοντας τη ζωή τους πιο άνετη και βολική.

Άλλο ένα πλεονέκτημα του IoT είναι η βελτιωμένη απόδοση και αποτελεσματικότητα σε πολλούς τομείς της καθημερινότητάς μας, όπως η υγεία, η προστασία του κοινού, και η ενέργεια. Για παράδειγμα, στον τομέα της υγείας, το IoT μπορεί να βοηθήσει στην παρακολούθηση των ασθενών σε πραγματικό χρόνο και να παρέχει αποτελεσματικότερη ιατρική φροντίδα. Επιπλέον, η τεχνολογία του IoT μπορεί να βελτιώσει την απόδοση των πόλεων και να βοηθήσει στην πρόληψη ατυχημάτων.

Το IoT μπορεί να βελτιώσει την ποιότητα ζωής μας, καθώς μπορεί να διευκολύνει την καθημερινή μας ζωή με πιο έξυπνες και αποτελεσματικές συσκευές και υπηρεσίες. Παραδείγματα αυτών των συσκευών είναι οι έξυπνοι θερμοστάτες, οι έξυπνες κάμερες ασφαλείας, οι έξυπνες πόρτες και οι έξυπνες συσκευές κουζίνας.

Συνολικά, το Internet of Things προσφέρει αμέτρητα πλεονεκτήματα και δυνατότητες σε πολλούς τομείς της ζωής μας. Επιτρέπει στους χρήστες να ελέγχουν και να διαχειρίζονται τις συσκευές τους από απόσταση, μέσω εφαρμογών στα κινητά τους ή από υπολογιστές. Αυτό μεταφράζεται σε αυξημένη ασφάλεια, καθώς μπορούν να ελέγχουν και να διορθώνουν πιθανά προβλήματα με τις συσκευές τους πριν καταστραφούν ή προκαλέσουν ζημιές. Επιπλέον, η ευκολία χρήσης του IoT καθιστά τη ζωή πιο άνετη και βολική για τους χρήστες. Ακόμα μπορεί να βοηθήσει στην πιο αποτελεσματική χρήση των πόρων, όπως του νερού και της ενέργειας. Για παράδειγμα, ένα σπίτι μπορεί να χρησιμοποιεί αισθητήρες για να παρακολουθεί την κατανάλωση ενέργειας και νερού και να προσαρμόζει αυτόματα τη χρήση τους για να μειώσει την κατανάλωση και το κόστος.

1.2.3 Μειονεκτήματα

Παραπάνω αναφέρθηκαν μερικά από τα πλεονεκτήματα που προσφέρει η χρήση του Internet of Things. Αν και τα οφέλη του είναι πάρα πολλά, υπάρχουν και ορισμένα μειονεκτήματα που πρέπει να ληφθούν υπόψη. Παρακάτω θα δούμε μερικά:

- **Κυβερνο-ασφάλεια και ιδιωτικότητα:** Καθώς ο αριθμός των συνδεδεμένων συσκευών αυξάνεται, το ίδιο συμβαίνει και με τον αριθμό των πιθανών σημείων εισόδου για κακόβουλους χάκερ. Αυτό μπορεί να απειλήσει την ασφάλεια και την ιδιωτικότητα των χρηστών. Οι χρήστες πρέπει να είναι προσεκτικοί και να λαμβάνουν τα απαραίτητα μέτρα για να προστατεύσουν τα δεδομένα τους.
- **Κόστος:** Η τεχνολογία IoT είναι ακόμα σχετικά νέα και, σε ορισμένες περιπτώσεις, οι τιμές των συσκευών και των υπηρεσιών μπορεί να είναι αρκετά υψηλές.
- **Εξάρτηση από το διαδίκτυο:** Η συνδεσιμότητα με το διαδίκτυο είναι απαραίτητη για τη λειτουργία των συσκευών IoT. Αυτό σημαίνει ότι χωρίς σύνδεση στο διαδίκτυο, οι συσκευές αυτές δεν μπορούν να λειτουργήσουν αποδοτικά, πράγμα που μπορεί να οδηγήσει σε προβλήματα και δυσκολίες σε περιπτώσεις διακοπής του διαδικτύου.
- **Συμβατότητα και προτυποποίηση:** Υπάρχει έλλειψη συμβατότητας μεταξύ των διαφόρων συσκευών και προτύπων που χρησιμοποιούνται στο IoT. Αυτό μπορεί να οδηγήσει σε προβλήματα συνδεσιμότητας και ενδεχομένως να αυξήσει το κόστος απόκτησης και λειτουργίας των συσκευών. Επομένως το Internet of Things αποτελείται από μια μεγάλη ποικιλία συσκευών και πρωτοκόλλων επικοινωνίας, και συνεπώς η συμβατότητα μεταξύ τους μπορεί να είναι πρόβλημα.

Συνοψίζοντας το IoT μπορεί να προκαλέσει αρκετά προβλήματα όσον αφορά την ασφάλεια των δεδομένων των χρηστών και την σωστή λειτουργία των συσκευών. Για αυτούς τους λόγους οι χρήση του πρέπει να είναι προσεκτική και να υπάρχει τακτικός ποιοτικός έλεγχος των συσκευών για την εξασφάλιση της σωστής λειτουργίας τους.

1.2.4 Κίνδυνοι χρήσης

Όσο αναφορά τους κινδύνους του Internet of Things, το IoT αποτελεί μια νέα τεχνολογική εξέλιξη που επιτρέπει σε συσκευές να συνδέονται μεταξύ τους και με το διαδίκτυο για να μοιράζονται δεδομένα και να αυτοματοποιούν διάφορες λειτουργίες. Ωστόσο, υπάρχουν και κάποιοι κίνδυνοι που πρέπει να ληφθούν υπόψη κατά τη χρήση του IoT, οι οποίοι περιλαμβάνουν:

- **Αποτυχία συστήματος:** Η αποτυχημένη συνδεσιμότητα ή η πτώση του δικτύου μπορεί να οδηγήσει στη διακοπή της λειτουργίας των συνδεδεμένων συσκευών IoT και σε επιπλέον κόστος για την επιδιόρθωση του συστήματος.
- **Φυσικοί κίνδυνοι:** Οι συσκευές IoT συχνά χρησιμοποιούνται σε περιβάλλοντα όπου υπάρχουν φυσικοί κίνδυνοι, όπως σε εργοστάσια, σταθμούς ενέργειας και κατασκευές. Η μη σωστή λειτουργία αυτών των συσκευών μπορεί να προκαλέσει ατυχήματα, πυρκαγιές, εκρήξεις και άλλους κινδύνους για τους ανθρώπους στο περιβάλλον.
- **Υγεία και ασφάλεια:** Οι συσκευές IoT χρησιμοποιούνται επίσης σε πολλούς τομείς που σχετίζονται με την υγεία και υπηρεσίες δημόσιας ασφάλειας και προστασίας πολιτών, όπως στην ιατρική και στην αστυνομία. Η λανθασμένη λειτουργία των συσκευών IoT σε αυτούς τους τομείς μπορεί να οδηγήσει σε λανθασμένες διαγνώσεις, λανθασμένα μέτρα ασφαλείας και άλλα σοβαρά προβλήματα.
- **Επιδράσεις στο περιβάλλον:** Οι συσκευές IoT μπορούν να επηρεάσουν το περιβάλλον και να προκαλέσουν κινδύνους για τη φύση και τους ανθρώπους. Για παράδειγμα, στη γεωργία, η υπερβολική χρήση αισθητήρων και συσκευών IoT για την άρδευση ή την παρακολούθηση των φυτών μπορεί να οδηγήσει σε υπερβολική χρήση νερού ή σε χρήση χημικών λιπασμάτων, με αρνητικές επιπτώσεις στην ποιότητα του εδάφους ή του νερού.
- **Ανεπιθύμητη επιβάρυνση δικτύου:** Η συνεχής αύξηση του αριθμού των συσκευών IoT μπορεί να οδηγήσει σε υπερφόρτωση των δικτύων επικοινωνίας. Αυτό μπορεί να προκαλέσει αστάθεια στις επικοινωνίες και να απαιτήσει αναβαθμίσεις και επεκτάσεις των δικτύων, προσθέτοντας περαιτέρω περιβαλλοντικό κόστος.

Συμπερασματικά, η χρήση των συσκευών IoT μπορεί να προσφέρει πολλαπλά οφέλη για τους ανθρώπους και το περιβάλλον, αλλά η παραβίαση ή η μη σωστή λειτουργία τους μπορεί να επιφέρει σημαντικούς κινδύνους για την υγεία, την ασφάλεια και το περιβάλλον. Είναι σημαντικό να λαμβάνονται όλα τα απαραίτητα μέτρα για την προστασία από αυτούς τους κινδύνους, όπως η καλή συντήρηση και η ασφαλής χρήση των συσκευών IoT.

1.2.4.1 Ζητήματα προσωπικών δεδομένων

Το Internet of Things μπορεί να προσφέρει πολλά οφέλη στην καθημερινότητα των ανθρώπων γι'αυτό και με το πέρασμα του χρόνου η χρήση του αυξάνεται συνεχώς. Όμως το IoT συνεπάγεται τη συλλογή μεγάλου όγκου προσωπικών δεδομένων από τις συνδεδεμένες συσκευές. Αυτό μπορεί να προκαλέσει διάφορα προβλήματα που σχετίζονται με την προστασία της ιδιωτικότητας και την ασφάλεια των προσωπικών δεδομένων. Ορισμένα από αυτά τα προβλήματα περιλαμβάνουν:

- **Έλλειψη διαφάνειας και έλεγχος:** Οι χρήστες μπορεί να μην έχουν πλήρη επίγνωση ή έλεγχο επί του πως συλλέγονται, χρησιμοποιούνται και κοινοποιούνται τα προσωπικά τους δεδομένα από τις συσκευές IoT. Αυτό μπορεί να δημιουργήσει ανησυχίες σχετικά με την ιδιωτικότητα και τον έλεγχο των προσωπικών δεδομένων.
- **Επιπτώσεις στην ψυχολογία και την ανθρώπινη συμπεριφορά:** Η συλλογή και η ανάλυση δεδομένων από τις συσκευές IoT μπορεί να έχει επιπτώσεις στην ψυχολογία και την ανθρώπινη συμπεριφορά. Αυτό μπορεί να συμβεί μέσω της δημιουργίας προφίλ, της παρακολούθησης και της επιρροής των ατόμων με βάση τα προσωπικά τους δεδομένα. Αυτό μπορεί να οδηγήσει σε προβλήματα σχετικά με την ιδιωτικότητα, την αυτονομία και την ελευθερία των ατόμων, καθώς και σε αλλαγές στη συμπεριφορά τους με βάση τις προτεινόμενες ενέργειες ή διαφημίσεις.
- **Κίνδυνοι από κακόβουλη χρήση:** Οι κακόβουλοι χρήστες μπορούν να εκμεταλλευτούν τις ευπάθειες των συσκευών IoT για να παραβιάσουν την ιδιωτικότητα των χρηστών, να προκαλέσουν ζημιές ή να παρακολουθούν τις δραστηριότητές τους. Αυτό μπορεί να οδηγήσει σε απώλεια εμπιστοσύνης και ανησυχία για τη χρήση του IoT.

Το ζήτημα των προσωπικών δεδομένων είναι πολύ σημαντικό καθώς μπορεί να προκαλέσει μεγάλο πρόβλημα στους χρήστες και να έχει έως και καταστροφικές επιπτώσεις στην ζωή τους. Υπάρχουν πολλά περιστατικά παραβίασης προσωπικών δεδομένων που σχετίζονται με τις συσκευές IoT. Ένα από αυτά τα περιστατικά είναι η παραβίαση της ιδιωτικότητας των χρηστών μέσω κάμερας ασφαλείας. Το 2016, στο περίστατικό με την εταιρεία κατασκευής καμερών ασφαλείας "Verkada", ανακοινώθηκε ότι ένας εξωτερικός χάκερ κατάφερε να παραβιάσει το σύστημα της εταιρείας και να αποκτήσει πρόσβαση σε χιλιάδες κάμερες που ήταν εγκατεστημένες σε διάφορες τοποθεσίες. Αυτό οδήγησε στη διαρροή ευαίσθητων εικόνων και σε παραβίαση της ιδιωτικότητας πολλών ανθρώπων. Οι εικόνες περιελάμβαναν την καταγραφή της καθημερινής ζωής ανθρώπων, συμπεριλαμβανομένων εσωτερικών χώρων και προσωπικών χώρων εργασίας. Αυτή η παραβίαση αποτελεί ένα παράδειγμα για το πώς η εσφαλμένη παραμετροποίηση ή αδυναμίες στην ασφάλεια των συσκευών IoT μπορεί να οδηγήσει στην παραβίαση προσωπικών δεδομένων.

Για την αντιμετώπιση αυτών των ζητημάτων, είναι σημαντικό οι οργανισμοί και οι κατασκευαστές των συσκευών IoT να λαμβάνουν υπόψη την προστασία των προσωπικών δεδομένων και την ασφάλεια. Οι καταναλωτές πρέπει επίσης να είναι ενήμεροι για την πολιτική προστασίας των δεδομένων και τις επιπτώσεις της χρήσης των συσκευών IoT, και να λαμβάνουν τα κατάλληλα μέτρα. Περαιτέρω ανάλυση για κινδύνους που ενέχει η χρήση του IoT παρατίθεται στο κεφάλαιο IoT και Ασφάλεια.[8][9]

1.3 Τηλεχειρουργική και Internet of Things

Η παρούσα διπλωματική εργασία εξετάζει τη συνδυαστική χρήση της τεχνολογίας Internet of Things (IoT) και της τηλεχειρουργικής, με στόχο την ενίσχυση της απόδοσης και της ασφάλειας στις εξ αποστάσεως χειρουργικές επεμβάσεις. Η εργασία επικεντρώνεται στα εξής βασικά προβλήματα και προτείνει λύσεις για αυτά:[9]

Προβλήματα που θα λυθούν

1. **Ασφάλεια Δεδομένων**: Η μεταφορά και αποθήκευση ευαίσθητων ιατρικών δεδομένων σε ένα διασυνδεδεμένο σύστημα IoT είναι κρίσιμη. Υπάρχει υψηλός κίνδυνος διαρροής ή παραβίασης των δεδομένων, ειδικά σε περιπτώσεις κυβερνοεπιθέσεων.
2. **Αξιοπιστία Συνδέσεων**: Η τηλεχειρουργική απαιτεί εξαιρετικά αξιόπιστες και σταθερές συνδέσεις δεδομένων. Η αποτυχία ή η καθυστέρηση στη μετάδοση δεδομένων μπορεί να έχει σοβαρές επιπτώσεις στην ασφάλεια και την αποτελεσματικότητα της χειρουργικής επέμβασης.
3. **Συγχρονισμός και Απόκριση**: Οι χειρουργοί χρειάζονται άμεση και ακριβή απόκριση των ρομποτικών συστημάτων στις εντολές τους. Οι καθυστερήσεις ή οι ασυγχρονισμοί μπορούν να οδηγήσουν σε χειρουργικά λάθη.
4. **Ακρίβεια και Ελεγχόμενη Κίνηση**: Οι λεπτομερείς κινήσεις των ρομποτικών συστημάτων πρέπει να είναι ακριβείς και ελεγχόμενες για την επιτυχή εκτέλεση των χειρουργικών επεμβάσεων.

Πώς σκοπεύει να τα λύσει

1. **Ενίσχυση της Ασφάλειας Δεδομένων**:
   - Εφαρμογή κρυπτογράφησης για την προστασία των δεδομένων κατά τη μετάδοση και αποθήκευση.
   - Χρήση ασφαλών πρωτοκόλλων επικοινωνίας για την αποτροπή μη εξουσιοδοτημένης πρόσβασης.
   - Ανάπτυξη συστημάτων ανίχνευσης και πρόληψης εισβολών (Intrusion Detection and Prevention Systems - IDPS) για την παρακολούθηση και αντιμετώπιση των κυβερνοεπιθέσεων.
2. **Βελτίωση της Αξιοπιστίας Συνδέσεων**:
   - Χρήση προηγμένων τεχνολογιών δικτύωσης για την εξασφάλιση σταθερών και αξιόπιστων συνδέσεων, όπως η χρήση δικτύων 5G.
   - Εφαρμογή τεχνικών αποκατάστασης σφαλμάτων και εφεδρικών συστημάτων για την αντιμετώπιση των διακοπών σύνδεσης.
3. **Βελτιστοποίηση Συγχρονισμού και Απόκρισης**:
   - Χρήση αλγορίθμων πραγματικού χρόνου για τον έλεγχο των ρομποτικών συστημάτων, εξασφαλίζοντας γρήγορη και ακριβή απόκριση στις εντολές του χειρουργού.
   - Ενσωμάτωση συστημάτων αισθητήρων για την παρακολούθηση και διόρθωση των κινήσεων σε πραγματικό χρόνο.
4. **Αύξηση Ακρίβειας και Ελέγχου Κινήσεων**:

- Ανάπτυξη ρομποτικών συστημάτων με υψηλή ακρίβεια και ευελιξία στις κινήσεις, βασισμένων σε προηγμένες τεχνολογίες μηχανικής και τεχνητής νοημοσύνης.
- Εκπαίδευση των χειρουργών στη χρήση των ρομποτικών συστημάτων μέσω εξειδικευμένων προγραμμάτων προσομοίωσης και πρακτικής.

Σκοπός της Διπλωματικής Εργασίας

Ο σκοπός της διπλωματικής αυτής εργασίας είναι να παρέχει μια ολοκληρωμένη ανάλυση των τεχνολογιών IoT και τηλεχειρουργικής, εξετάζοντας τις προκλήσεις και τις τεχνικές λύσεις που μπορούν να εφαρμοστούν για την βελτίωση της ασφάλειας, της αξιοπιστίας και της αποτελεσματικότητας των χειρουργικών επεμβάσεων από απόσταση. Μέσω της ανάλυσης αυτής, αναμένεται να συμβάλει στην ανάπτυξη καινοτόμων λύσεων που θα ενισχύσουν την ποιότητα και την αποδοτικότητα των ιατρικών υπηρεσιών, προωθώντας την ασφαλή και επιτυχή ενσωμάτωση του IoT στην τηλεχειρουργική.

Οι προτεινόμενες λύσεις και τα μέτρα που αναλύονται στην εργασία αυτή, αποσκοπούν στη δημιουργία ενός ασφαλούς και αξιόπιστου περιβάλλοντος για την εφαρμογή της τηλεχειρουργικής, με την τεχνολογία IoT να αποτελεί τον ακρογωνιαίο λίθο για την επίτευξη αυτού του στόχου.

1.4 Δομή της διπλωματικής

Η εισαγωγή περιλαμβάνει μια γενική επισκόπηση του θέματος της διπλωματικής εργασίας, εισάγοντας τον αναγνώστη στις βασικές έννοιες του Internet of Things (IoT) και της τηλεχειρουργικής, καθώς και την αλληλεπίδρασή τους. Σκοπός της εισαγωγής είναι να θέσει το πλαίσιο για την περαιτέρω ανάλυση και να παρουσιάσει τη σημασία της μελέτης.

Στο κεφάλαιο **Internet of Things**, αναλύεται το Internet of Things (IoT) και η εφαρμογή του σε διάφορους τομείς. Περιλαμβάνονται η υποενότητα **IoT και Blockchain** στην οποία εξετάζεται η σχέση μεταξύ IoT και Blockchain και πώς αυτά τα δύο μπορούν να συνδυαστούν για να παρέχουν ασφαλέστερες και πιο αξιόπιστες λύσεις. Η υποενότητα **Εφαρμογές** όπου παρουσιάζονται οι διάφορες εφαρμογές του IoT σε διάφορους τομείς όπως η βιομηχανία, η υγεία και οι έξυπνες πόλεις. Η υποενότητα **Πλεονεκτήματα** που αναλύονται τα βασικά πλεονεκτήματα του IoT, όπως η αυξημένη αποδοτικότητα και η βελτιωμένη λήψη αποφάσεων. Η υποενότητα **Μειονεκτήματα** όπου συζητούνται τα πιθανά μειονεκτήματα και τα προβλήματα που μπορεί να προκύψουν από τη χρήση του IoT. Τέλος, η υποενότητα **Κίνδυνοι χρήσης** στην οποία περιγράφονται οι κίνδυνοι που σχετίζονται με τη χρήση του IoT, όπως η ασφάλεια και η ιδιωτικότητα.

Το κεφάλαιο **Τηλεχειρουργική και Internet of Things** εξετάζει τη συνδυαστική χρήση της τηλεχειρουργικής και του IoT, αναλύοντας πώς τα έξυπνα συστήματα και οι αισθητήρες μπορούν να βελτιώσουν τις χειρουργικές διαδικασίες εξ αποστάσεως.

Στη **Δομή της διπλωματικής** παρουσιάζεται η συνολική δομή της διπλωματικής εργασίας, με περιγραφή των κεφαλαίων και των υποενοτήτων.

Στο κεφάλαιο **IoT και Ασφάλεια** αναλύονται οι βασικές αρχές ασφάλειας του IoT, οι προκλήσεις που προκύπτουν και οι απειλές που σχετίζονται με τη χρήση του IoT σε διάφορους τομείς, ιδίως στον τομέα της υγείας. Περιλαμβάνονται η υποενότητα **Βασικές αρχές** στην οποία περιγράφονται οι βασικές αρχές ασφάλειας που πρέπει να τηρούνται στο IoT. Η υποενότητα **Προκλήσεις ασφάλειας** όπου αναλύονται οι κυριότερες προκλήσεις στην ασφάλεια του IoT. Η υποενότητα **Προκλήσεις ασφάλειας στον τομέα της υγείας** στην οποία εστιάζονται οι προκλήσεις ασφάλειας που είναι ειδικές για τον τομέα της υγείας. Η υποενότητα **Τύποι εισβολέων** ‘οπου κατηγοριοποιούνται οι διάφοροι τύποι εισβολέων που μπορεί να στοχεύσουν συστήματα IoT. Η υποενότητα **Είδη επιθέσεων** στην οποία αναλύονται τα διάφορα είδη επιθέσεων που μπορούν να πραγματοποιηθούν σε συστήματα IoT. Τέλος, η υποενότητα **Αντίμετρα** στην οποία παρουσιάζονται τα αντίμετρα που μπορούν να ληφθούν για την προστασία των συστημάτων IoT.

Το κεφάλαιο **IoT και Υγεία** ασχολείται με τις εφαρμογές του IoT στον τομέα της υγείας, τα οφέλη που προκύπτουν, καθώς και τους κινδύνους και τα μέτρα αντιμετώπισής τους. Στην υποενότητα **Εφαρμογές του IoT στην υγεία,** παρουσιάζονται οι διάφορες εφαρμογές του IoT στον τομέα της υγείας. Η υποενότητα **Οφέλη εφαρμογών** αναλύει τα οφέλη που προκύπτουν από την εφαρμογή του IoT στην υγεία.

Η υποενότητα **Κίνδυνοι** περιγράφει τους κινδύνους που σχετίζονται με τη χρήση του IoT στην υγεία. Τελος, στην υποενότητα **Αντιμετώπιση κινδύνων** παρουσιάζονται τα μέτρα που μπορούν να ληφθούν για την αντιμετώπιση των κινδύνων.

Στο κεφάλαιο **OWASP** γίνεται μια εισαγωγή στο OWASP και στη μεθοδολογία που χρησιμοποιείται για την αξιολόγηση των κινδύνων ασφαλείας.

Στο κεφάλαιο **Τηλεχειρουργική** εξετάζεται η εφαρμογή της τηλεχειρουργικής, τα οφέλη της, τους κινδύνους και τις επιθέσεις που μπορεί να προκύψουν, καθώς και τον ορισμό και την ανάλυση των ρίσκων. Αναλύονται τα ρίσκα ανά οντότητα αλλά και τα ρίσκα που προκύπτουν από τη σχέση μεταξύ ζευγών οντοτήτων. Επίσης αναλύονται διάφορα σενάρια κινδύνων όπως κλώνος ιστοσελίδας χωρίς κρυπτογράφηση, κίνδυνος υποκλοπής δεδομένων από το cloud, κίνδυνος αλλοίωσης ή απώλειας δεδομένων, πολύπλοκες ή δύσχρηστες διεπαφές μπορούν να προκαλέσουν σύγχυση ή λάθη κατά τη χρήση και σφάλματα λογισμικού ή υλικού που μπορεί να προκαλέσουν καθυστερήσεις ή διακοπές στη χειρουργική διαδικασία.

Η **Βιβλιογραφία** περιλαμβάνει όλες τις πηγές που χρησιμοποιήθηκαν για τη συγγραφή της διπλωματικής εργασίας, παρέχοντας αναφορές σε βιβλία, άρθρα, και άλλες επιστημονικές πηγές.

Με αυτή τη δομή, η διπλωματική εργασία καλύπτει όλα τα σημαντικά θέματα που σχετίζονται με το IoT και την τηλεχειρουργική, προσφέροντας μια ολοκληρωμένη ανάλυση των εφαρμογών, των κινδύνων και των μέτρων ασφάλειας.

2. IoT και Ασφάλεια

2.1 Βασικές αρχές

Οι βασικές αρχές της ασφάλειας στα πληροφοριακά συστήματα είναι οι εξής:

- **Ακεραιότητα:** Αυτή η αρχή αφορά τη διατήρηση της ακεραιότητας των δεδομένων. Οι χρήστες δεν πρέπει να έχουν τη δυνατότητα να τροποποιούν ή να καταστρέφουν τα δεδομένα χωρίς την απαραίτητη άδεια. Αυτό μπορεί να επιτευχθεί με τη χρήση αλγορίθμων κρυπτογράφησης για υπογραφή δεδομένων, διασφαλίζοντας ότι τα δεδομένα είναι ακέραια και δεν μπορούν να αλλοιωθούν.
- **Εμπιστευτικότητα:** Η αρχή αυτή αφορά τη διατήρηση της εμπιστευτικότητας των δεδομένων. Οι χρήστες πρέπει να μπορούν να εμπιστεύονται ότι τα δεδομένα που δίνουν στο σύστημα παραμένουν απόρρητα. Αυτό μπορεί να επιτευχθεί με τη χρήση διαφόρων τεχνολογιών ασφαλείας όπως κρυπτογράφηση, έλεγχος πρόσβασης, και άλλα.
- **Διαθεσιμότητα**: Αυτή η αρχή αφορά τη διαθεσιμότητα των δεδομένων και του συστήματος. Το σύστημα πρέπει να είναι διαθέσιμο στους χρήστες του όταν το χρειάζονται.
- **Ευθύνη:** Η αρχή αυτή αφορά την ευθύνη των χρηστών για τη χρήση του συστήματος και των δεδομένων. Οι χρήστες πρέπει να είναι ενημερωμένοι για τους κινδύνους που συνδέονται με τη χρήση του συστήματος και να λαμβάνουν τα απαραίτητα μέτρα ασφαλείας για την προστασία των δεδομένων.
- **Αντιμετώπιση απειλών:** Η αρχή αυτή αφορά την αντιμετώπιση διαφόρων απειλών στην ασφάλεια των δεδομένων, όπως ιοί, κακόβουλο λογισμικό, διαρροές δεδομένων και επιθέσεις από κακόβουλους χρήστες. Αυτό μπορεί να επιτευχθεί με τη χρήση διαφόρων μεθόδων ασφαλείας, όπως λογισμικό ανίχνευσης και πρόληψης, αντιικών διαβιβάσεων και προστασίας από επιθέσεις **DoS (Denial of Service)**.
- **Ενημέρωση:** Η αρχή αυτή αφορά τη διατήρηση του συστήματος με ενημερωμένες εκδόσεις λογισμικού όσον αφορά νέες απειλές και ευπάθειες και την εφαρμογή και κατά συνέπεια την διατήρηση του συστήματος σε ασφαλή κατάσταση. Αυτό σημαίνει ότι πρέπει να υπάρχει σταθερή επικοινωνία με τους προμηθευτές λογισμικού και να εγκαθίστανται τακτικά αναβαθμίσεις και ενημερώσεις λογισμικού.

Ένας άλλος σημαντικός τομέας ασφάλειας στα πληροφοριακά συστήματα είναι η ασφάλεια των δεδομένων. Για να διασφαλίζεται η ασφάλεια των δεδομένων, πρέπει να εφαρμοστούν κατάλληλα μέτρα ασφαλείας όπως η κρυπτογράφηση, η πρόληψη από ανεπιθύμητη πρόσβαση, η δημιουργία αντιγράφων ασφαλείας και η επιθεώρηση των συστημάτων για πιθανές ευπάθειες.

Ακόμα ένας τομέας ασφάλειας που αφορά τα πληροφοριακά συστήματα είναι η ασφάλεια του δικτύου. Για να διασφαλιστεί η ασφάλεια του δικτύου, πρέπει να εφαρμοστούν μέτρα όπως η χρήση προηγμένων **firewall** και η επιθεώρηση της κυκλοφορίας των δεδομένων στο δίκτυο.

Για τους λόγους αυτούς, η διαχείριση κινδύνων αποτελεί ένα απαραίτητο μέσο για την ασφάλεια των πληροφοριακών συστημάτων. Η διαχείριση κινδύνων περιλαμβάνει την αξιολόγηση των κινδύνων, την ανάπτυξη μέτρων ασφαλείας για τη μείωση των κινδύνων και την παρακολούθηση της αποτελεσματικότητας τους.

Το συμπέρασμα είναι ότι η ασφάλεια στα πληροφοριακά συστήματα είναι ένα πολύπλοκο και διαρκώς εξελισσόμενο ζήτημα. Για να εξασφαλίσουμε ότι οι πληροφορίες μας παραμένουν ασφαλείς, πρέπει να εφαρμόζουμε συστηματικές και ολοκληρωμένες προσεγγίσεις που να περιλαμβάνουν την τεχνολογία, τη διαχείριση, τους ανθρώπους και τις διαδικασίες. Η ανάπτυξη μιας πολιτικής ασφαλείας είναι σημαντική για την ασφάλεια των πληροφοριών και την προστασία από τις απειλές της κυβερνοασφάλειας. Με την κατάλληλη ανάλυση κινδύνων και αξιολόγηση επιπτώσεων, μπορούμε να εντοπίσουμε τα αδύναμα σημεία του συστήματος και να λάβουμε τα κατάλληλα μέτρα για να τα αντιμετωπίσουμε και να ενισχύσουμε την ασφάλεια των πληροφοριών.

2.2 Προκλήσεις ασφάλειας

2.2.1 Προκλήσεις ασφάλειας του IoT

Το Internet of Things (IoT) είναι ένα δίκτυο συνδεδεμένων συσκευών που επιτρέπουν την ανταλλαγή δεδομένων μεταξύ τους και με άλλα συστήματα. Αυτή η τεχνολογία έχει αναπτυχθεί πολύ γρήγορα και έχει δημιουργήσει ένα μεγάλο αριθμό προκλήσεων ασφαλείας. Εδώ είναι μερικά από τα κύρια θέματα ασφαλείας που σχετίζονται με το IoT:

- **Έξουσιοδότηση:**
    - Η αυθαίρετη πρόσβαση είναι μια από τις μεγαλύτερες απειλές κατα την διακίνηση και τη αποθήκευση των δεδομένων στο cloud. Αν δεν υπάρχει σωστός μηχανισμός ελέγχου του διαμοιρασμού του δυναμικού περιεχομένου, δύναται κάποιος χρήστης να αποκτήσει πρόσβαση σε προσωπικά δεδομένα, συσκευές και συστήματα που δεν του ανήκουν.
    - Υπάρχει επίσης το ενδεχόμενο παρακολούθησης και παραβίασης της ιδιωτικότητας με δόλο: Οι συσκευές IoT μπορεί να συλλέγουν πολλά ευαίσθητα δεδομένα, όπως πληροφορίες υγείας, χρηματοοικονομικές πληροφορίες και μπορεί να οδηγήσει στην παρακολούθηση των κινήσεων των χρηστών μέσω καμερών, μικροφωνων, και άλλων αισθητήρων, και να εξασφαλίσουν πρόσβαση στα βιομετρικά τους στοιχεία. Αυτό μπορεί να παραβιάζει την ιδιωτικότητα τους, καθώς ο ίδιος ο χρήστης μπορεί να μην έχει συναινέσει στην παραχώρηση των πληροφοριών αυτών και δύναται αυτές να χρησιμοποιηθούν προς όφελος τρίτων μελών και να βλάψουν τον εκάστοτε χρήστη.
- **Κυβερνοεπίθεση:** Η κυβερνοεπίθεση είναι κίνδυνοςστην ασφάλεια του IoT, καθώς οι χρήστες μπορεί να είναι ευάλωτοι σε επιθέσεις με στόχο την απόκτηση προσωπικών πληροφοριών ή την κλοπή της ταυτότητας επίσης μπορούν να προκαλέσουν σοβαρές ζημιές σε συσκευές, κτίρια και υποδομές ή ακόμα χειρότερα σε ανθρώπους. Υπάρχουν πολλά είδη επιθέσεων, όπως η εγκατάσταση κακόβουλου λογισμικού **Malware**, οι επιθέσεις **Distributed Denial of Service** (DDoS) και οι επιθέσεις **Phishing**. Πρέπει να υπάρχει ένα ενημερωμένο πλάνο αντιμετώπισης κινδύνων και επαναφοράς του συστήματος σε περίπτωση παραβίασης της ασφάλειας.
- **Ελλειπής κρυπτογράφηση:** Η κρυπτογράφηση είναι μια σημαντική τεχνική για την προστασία των δεδομένων στο IoT. Ωστόσο, ορισμένες συσκευές IoT δεν υποστηρίζουν ισχυρή κρυπτογράφηση ή ακόμη και κανέναν τρόπο κρυπτογράφησης. Αυτό μπορεί να οδηγήσει σε παραβίαση της ασφάλειας και της ιδιωτικότητας των δεδομένων. Οι συσκευές IoT συνδέονται στο Internet μέσω ασύρματων δικτύων, όπως **Wi-Fi**, **Bluetooth** και **Zigbee**. Αυτά τα ασύρματα δίκτυα μπορούν να είναι ευπαθή σε επιθέσεις, όπως υποκλοπή και αντιγραφή δεδομένων, παρακολούθηση κίνησης και άλλα.

- **Αδυναμία ενημέρωσης:** Στις συσκευές IoT μπορεί να είναι δύσκολη η ενημέρωση του λογισμικού τους, ιδιαίτερα σε περιβάλλοντα όπου οι συσκευές είναι απομακρυσμένες ή αποκομμένες από το διαδίκτυο. Αυτό μπορεί να οδηγήσει σε ευπάθειες ασφαλείας που δεν μπορούν να διορθωθούν και μπορεί να καθιστούν τις συσκευές ευάλωτες σε κακόβουλες επιθέσεις. Για να αποτραπεί αυτό, οι κατασκευαστές πρέπει να επιλέξουν συστατικά λογισμικού με μεγαλύτερη αντοχή στον χρόνο και να παρέχουν τακτικές ενημερώσεις λογισμικού για τις συσκευές τους.

Συνολικά, η ασφάλεια στο Internet of Things είναι ένα πολύπλοκο και σημαντικό ζήτημα που απαιτεί προσεκτική προετοιμασία και λήψη μέτρων από τους κατασκευαστές, τους παρόχους υπηρεσιών και τους χρήστες. Το Internet of Things αποτελεί μια αναπτυσσόμενη τεχνολογία που υπόσχεται να βελτιώσει τη ζωή μας και να αυξήσει την αποδοτικότητα και την αυτονομία των συστημάτων. Ωστόσο, η ανάπτυξη αυτών των συσκευών έχει επίσης πολλά θέματα ασφαλείας που πρέπει να ληφθούν υπόψη. Η απουσία προτύπων ασφαλείας, η ελλιπής διαχείριση του λογισμικού, η έλλειψη απομακρυσμένων ελέγχων και η απουσία αναβαθμισμένου λογισμικού των συσκευών είναι μόνο μερικά από τα θέματα που μπορούν να οδηγήσουν σε παραβίαση της ασφάλειας και της ιδιωτικότητας των δεδομένων. Για να διασφαλίσουμε ότι οι συσκευές IoT είναι ασφαλείς, θα πρέπει να αναπτυχθούν πρότυπα ασφαλείας και να εφαρμοστούν πρακτικές ασφαλείας κατά την ανάπτυξη και τη χρήση τους. Επιπλέον, οι κατασκευαστές πρέπει να αναβαθμίζουν το λογισμικό των συσκευών τους και να διαχειρίζονται αποτελεσματικά τα προβλήματα ασφαλείας που προκύπτουν.

2.2.2 Προκλήσεις ασφάλειας στον τομέα της υγείας

Η ασφάλεια στα πληροφοριακά συστήματα είναι ένα θέμα μεγάλης σημασίας, ειδικά στον κλάδο της υγείας, όπου η ανεπάρκεια ή η κακή διαχείριση των πληροφοριών μπορεί να γίνει ζωτικής σημασίας δηλαδή να έχει σοβαρές συνέπειες στην υγεία των ασθενών και στη λειτουργία του ιατρικού συστήματος.

Εστιάζοντας στον κλάδο της υγείας για να αναπτύξουμε μια αποτελεσματική πολιτική ασφαλείας για τα πληροφοριακά συστήματα, πρέπει να ληφθούν υπόψη οι εξής πτυχές:

- Τα προσωπικά δεδομένα και η απόρρητη πληροφορία είναι εξαιρετικά ευαίσθητα στον κλάδο της υγείας. Είναι σημαντικό να διασφαλίζεται ότι οι απαραίτητες μέθοδοι προστασίας και ασφάλειας των δεδομένων έχουν ληφθεί υπόψιν, όπως η κρυπτογράφηση και ο καθορισμός πολιτικής πρόσβασης.
- Τα ιατρικά συστήματα χρειάζονται την υποστήριξη ενός ειδικευμένου ομίλου ασφάλειας για τη διαχείριση των απειλών και των ευπαθειών στα συστήματα, καθώς και για την ανάπτυξη αντιμέτρων και την επίλυση ενδεχόμενων προβλημάτων.
- Επίσης πρέπει να διασφαλιστεί ότι η κατάρτιση και η εκπαίδευση του προσωπικού που χειρίζεται τα πληροφοριακά συστήματα υγείας είναι επαρκής για να αντιληφθούν τις απειλές ασφαλείας και να τηρούν τους απαραίτητους κανόνες προστασίας των δεδομένων.
- Τέλος, πρέπει να εξεταστούν οι νομικές πτυχές της ασφάλειας στα πληροφοριακά συστήματα υγείας. Πρέπει να διασφαλίζεται ότι η πολιτική ασφάλειας συμμορφώνεται με τους ισχύοντες νόμους περί προστασίας δεδομένων και ιατρικής εμπιστευτικότητας.

Όμως πέρα από αυτά για να αναπτυχθεί μια αποτελεσματική πολιτική ασφάλειας για τα πληροφοριακά συστήματα υγείας, πρέπει να ληφθούν υπόψη και άλλοι παράγοντες, όπως:

Πρέπει να υπάρχει ενημέρωση σχετικά με τους τεχνολογικούς κινδύνους που είναι συνδεδεμένοι με τα πληροφοριακά συστήματα υγείας και να αναζητηθούν νέες τεχνολογίες-τεχνικές που μπορούν να βελτιώσουν την ασφάλεια: α) Να αξιολογηθεί ο κίνδυνος από διαφορετικές πλευρές, όπως την επίπτωση απώλειας απορρήτου των δεδομένων υγείας των ασθενών, την επίπτωση στην διαθεσιμότητα των συστημάτων, την επίπτωση στην ακεραιότητα των δεδομένων και την επίπτωση στην αξιοπιστία των συστημάτων, β) Να εξεταστεί ο τρόπος με τον οποίο τα πληροφοριακά συστήματα υγείας συνδέονται μεταξύ τους και με άλλα συστήματα υγείας. Πρέπει να διασφαλιστεί ότι η ασφάλεια των πληροφοριακών συστημάτων είναι εξίσου υψηλή σε όλα τα επίπεδα.

Το συμπέρασμα είναι ότι η ασφάλεια των πληροφοριακών συστημάτων στον τομέα της υγείας είναι ζωτικής σημασίας για την προστασία των δεδομένων υγείας των ασθενών και την εξασφάλιση της αξιοπιστίας και ακεραιότητας των πληροφοριακών συστημάτων. Για να επιτευχθεί αυτό το επίπεδο ασφάλειας, πρέπει να σχεδιαστεί και να υλοποιηθεί μια ολοκληρωμένη πολιτική ασφαλείας, η οποία θα περιλαμβάνει μέτρα όπως η προστασία της πρόσβασης σε δεδομένα, η ανίχνευση και αντιμετώπιση απειλών

ασφαλείας, η κατάρτιση του προσωπικού σε θέματα ασφαλείας και η συνεχής ενημέρωση και βελτίωση των τεχνολογιών ασφαλείας. Επιπλέον, η πολιτική ασφαλείας πρέπει να επανεξετάζεται και να ενημερώνεται τακτικά για να διασφαλιστεί η εξακρίβωση της συμμόρφωσής της με τις νέες απαιτήσεις και απειλές που ενδέχεται να εμφανιστούν.

2.3 Τύποι εισβολέων

Υπάρχουν διάφοροι τύποι εισβολέων που μπορούν να επιτεθούν σε πληροφοριακά συστήματα IoT. Ορισμένοι από αυτούς είναι οι ακόλουθοι:

- **Χάκερς:** Γενικός όρος που χρησιμοποιείται συχνά για να περιγράψει άτομα ή ομάδες με προηγμένες τεχνικές δεξιότητες που χειρίζονται συστήματα υπολογιστών ή δίκτυα για διάφορους σκοπούς, συμπεριλαμβανομένης της εκμετάλλευσης ευπαθειών σε συσκευές IoT.
- **Εγκληματίες του κυβερνοχώρου:** Άτομα ή ομάδες που επιδίδονται σε παράνομες δραστηριότητες στο διαδίκτυο, συμπεριλαμβανομένων της πειρατείας, της κλοπής δεδομένων, της απάτης και του εκβιασμού, συχνά για οικονομικό όφελος. Οι εγκληματίες του κυβερνοχώρου μπορεί να στοχεύουν σε συσκευές IoT για διάφορους κακόβουλους σκοπούς.
- **Script Kiddies:** Άτομα με περιορισμένες τεχνικές δεξιότητες που χρησιμοποιούν προϋπάρχοντα εργαλεία hacking ή σενάρια επιθέσεων για να εξαπολύσουν επιθέσεις χωρίς να κατανοούν πλήρως την υποκείμενη τεχνολογία. Τα script kiddies μπορεί να συμμετέχουν σε επιθέσεις DDoS ή να εκμεταλλεύονται γνωστές ευπάθειες σε συσκευές IoT.
- **Κρατικά υποστηριζόμενοι δράστες:** Κυβερνητικές υπηρεσίες ή οργανισμοί που εμπλέκονται σε κατασκοπεία στον κυβερνοχώρο, σαμποτάζ ή πόλεμο για πολιτικούς, οικονομικούς ή στρατιωτικούς σκοπούς. Οι κρατικά υποστηριζόμενοι φορείς ενδέχεται να στοχεύουν συσκευές IoT στο πλαίσιο ευρύτερων επιχειρήσεων στον κυβερνοχώρο.
- **Hacktivists:** Άτομα ή ομάδες που χρησιμοποιούν τεχνικές hacking για την προώθηση πολιτικών ή κοινωνικών σκοπών, συχνά με την αλλοίωση ιστότοπων, τη διαρροή ευαίσθητων πληροφοριών ή τη διακοπή διαδικτυακών υπηρεσιών. Οι χακτιβιστές μπορεί να στοχεύουν και σε συσκευές IoT για να ευαισθητοποιήσουν για θέματα ασφάλειας ή για να διαμαρτυρηθούν κατά ορισμένων οργανισμών ή κυβερνήσεων.
- **Οργανωμένες ομάδες ηλεκτρονικού εγκλήματος:** Εγκληματικές οργανώσεις ή συμμορίες που ειδικεύονται σε δραστηριότητες εγκλήματος στον κυβερνοχώρο, όπως η οικονομική απάτη, η κλοπή ταυτότητας ή η πώληση κλεμμένων δεδομένων στο dark web. Οι οργανωμένες ομάδες κυβερνοεγκλήματος ενδέχεται να στοχεύουν συσκευές IoT στο πλαίσιο των παράνομων δραστηριοτήτων τους.
- **Εσωτερικοί χρήστες:** Άτομα με εξουσιοδοτημένη πρόσβαση σε συστήματα ή δίκτυα που κάνουν κατάχρηση των προνομίων τους για κακόβουλους σκοπούς. Οι insiders μπορεί να εκμεταλλευτούν ευπάθειες σε συσκευές IoT ή να διαρρεύσουν σκόπιμα ευαίσθητες πληροφορίες.

Επίσης οι επιθέσεις στα πληροφοριακά συστήματα (IoT) μπορούν να προέλθουν από εσωτερικούς ή εξωτερικούς εισβολείς. Οι **εσωτερικοί εισβολείς** είναι άτομα ή ομάδες που έχουν πρόσβαση στο δίκτυο ή το σύστημα και εκμεταλλεύονται αυτήν την πρόσβαση για να διαπράξουν επιθέσεις ή να προκαλέσουν ζημιές. Μπορεί να πρόκειται για εργαζόμενους, πρώην εργαζόμενους, συνεργάτες ή άλλα εξουσιοδοτημένα άτομα. Οι εσωτερικοί εισβολείς είναι αυτοί που μπορούν να απειλήσουν την ασφάλειά της

εταιρείας. Μπορεί να είναι εσωτερικοί υπάλληλοι, προγραμματιστές ή συντηρητές συστημάτων που έχουν πρόσβαση σε ευαίσθητες πληροφορίες ή και άλλοι κακόβουλοι χρήστες που έχουν κλέψει προσωπικές πληροφορίες.

Οι **εξωτερικοί εισβολείς** αποτελούν μια επιπλέον απειλή για την ασφάλεια των πληροφοριακών συστημάτων στο IoT. Οι εξωτερικοί εισβολείς μπορεί να είναι χάκερ, εγκληματίες του κυβερνοχώρου, μυστικές υπηρεσίες, ανταγωνιστές, κ.λπ. Οι εξωτερικοί εισβολείς συνήθως εκμεταλλεύονται τα κενά ασφαλείας στο δίκτυο ή το σύστημα για να αποκτήσουν πρόσβαση και να προκαλέσουν ζημιές ή να κλέψουν ευαίσθητα δεδομένα. Ένας εξωτερικός εισβολέας μπορεί να χρησιμοποιήσει και τεχνικές για να πείσει τους χρήστες να αποκαλύψουν προσωπικές τους πληροφορίες ή να εγκαταστήσουν κακόβουλο λογισμικό στις συσκευές τους.

Επίσης ένας άλλος τύπος εισβολέα σε ένα πληροφοριακό σύστημα IoT είναι ο "επιτιθέμενος μεταξύ των δικτύων" (intermediate network attacker). Αυτός ο εισβολέας εκμεταλλεύεται την αδυναμία των δικτύων IoT να ανιχνεύσουν και να προστατεύσουν τα δεδομένα που ανταλλάσσονται μεταξύ τους και των εφαρμογών. Αυτός ο επιτιθέμενος μπορεί να ακούει ή να αλλοιώνει την επικοινωνία μεταξύ διαφορετικών δικτύων IoT, καθώς και να διακόπτει τη λειτουργία τους.

Συνοψίζοντας, οι τύποι εισβολέων στα πληροφοριακά συστήματα IoT περιλαμβάνουν τον κακόβουλο χρήστη, τον χακερ και τον κακόβουλο που εκμεταλλεύεται ευπαθές λογισμικό. Κάθε τύπος εισβολέα απαιτεί διαφορετικές τακτικές και μέτρα ασφαλείας για την πρόληψη και αντιμετώπιση των επιθέσεων. Για την ασφάλεια των πληροφοριακών συστημάτων IoT, είναι σημαντικό να εφαρμοστούν βασικές αρχές ασφαλείας, όπως η προστασία των συσκευών και των δεδομένων, η διαχείριση των προνομιακών δικαιωμάτων, η ανίχνευση και αντιμετώπιση αδυναμιών και ευπάθειων, καθώς και η παρακολούθηση του δικτύου και της κίνησης δεδομένων για την έγκαιρη ανίχνευση τυχόν απειλών ή ανωμαλιών.

2.4 Είδη επιθέσεων

Στην παραπάνω υποενότητα αναφέρθηκαν διάφορα είδη εισβολέων. Στα πληροφοριακά συστήματα IoT τα διάφορα είδη εισβολέων χρησιμοποιούν διάφορα είδη επιθέσεων, μερικά από τα οποία είναι: [6]

- **Επιθέσεις άρνησης υπηρεσιών (Df-service attack, DoS attack):** Σε αυτές τις επιθέσεις, ο επιτιθέμενος προσπαθεί να καταργήσει τη λειτουργικότητα ενός IoT συστήματος, υπερ-φορτώνοντας τις υπηρεσίες του συστήματος. Οι επιθέσεις αυτές έχουν ως σκοπό να καταστήσουν τον υπολογιστή ή την υπηρεσία ανίκανη να δεχθεί άλλες συνδέσεις και έτσι να μην μπορεί να εξυπηρετήσει άλλους πιθανούς πελάτες
- **Επιθέσεις χάκερ:** Σε αυτές τις επιθέσεις, ο επιτιθέμενος εισέρχεται εκμεταλλευόμενος απροστάτευτες θύρες στο σύστημα IoT και κλέβει προσωπικά δεδομένα, παραβιάζει την ασφάλεια του συστήματος ή χρησιμοποιεί το σύστημα για επιθέσεις σε άλλους υπολογιστές.
- **Επιθέσεις κακόβουλου κώδικα:** Σε αυτές τις επιθέσεις, ο επιτιθέμενος εισάγει κακόβουλο κώδικα στο σύστημα IoT που μπορεί να προκαλέσει ζημιά, να κλέψει πληροφορίες ή να παραβιάσει την ασφάλεια του συστήματος.
- **Επιθέσεις phishing:** Σε αυτές τις επιθέσεις, οι επιτιθέμενοι στοχεύουν τους χρήστες που χρησιμοποιούν συνδεδεμένες συσκευές για να αποκτήσουν πρόσβαση στα προσωπικά τους δεδομένα ή να παρακολουθήσουν τις δραστηριότητές τους. Οι επιτιθέμενοι μπορεί να στείλουν ανεπιθύμητα ηλεκτρονικά μηνύματα που προσποιούνται ότι προέρχονται από γνωστές εταιρείες ή παρόχους υπηρεσιών IoT, καλώντας τους χρήστες να κάνουν κλικ σε παραπλανητικούς συνδέσμους ή να ανακαλύψουν τα προσωπικά τους δεδομένα.

Ένα άλλο είδος επίθεσης που συχνά συναντάται στα πληροφοριακά συστήματα IoT είναι η επίθεση χειραγώγησης δεδομένων (**Data Manipulation Attack**). Σε αυτή την επίθεση, ο επιτιθέμενος καταφέρνει να αλλοιώσει τα δεδομένα που διαβιβάζονται στο σύστημα IoT, με σκοπό να παραπλανήσει τους χρήστες και να προκαλέσει βλάβες.

Επίσης μια άλλη επίθεση που μπορεί να συμβεί στα πληροφοριακά συστήματα IoT είναι η επίθεση αποκάλυψης ευπαθειών (**Vulnerability Discovery Attack**). Σε αυτή την επίθεση, ο επιτιθέμενος αναζητά ευπάθειες στο λογισμικό ή στο υλικό των συσκευών IoT, προκειμένου να τις εκμεταλλευτεί σε δεύτερη φάση και να προκαλέσει βλάβες.

Τα είδη επιθέσεων που μπορεί να εφαρμοστούν σε ένα πληροφοριακό σύστημα IoT είναι αρκετά και το καθένα από αυτά ανάλογα με τον σκοπό που έχει ο κακόβουλος χρήστης προκαλεί και διαφορετικές βλάβες στο σύστημα. Όμως οι επιθέσεις αυτές μπορεί να είναι είτε παθητικές είτε ενεργητικές.

Η **παθητική επίθεση** στα πληροφοριακά συστήματα (IoT) αναφέρεται στην παρακολούθηση και συλλογή πληροφοριών από ένα σύστημα χωρίς να προκαλείται καμία ζημιά στο σύστημα. Για παράδειγμα, ένας επιτιθέμενος μπορεί να παρακολουθεί την κυκλοφορία δεδομένων και να υποκλέπτει μέσω ενός ανοικτού ασύρματου δικτύου, χωρίς να επηρεάζει τη λειτουργία του δικτύου.

Από την άλλη, η **ενεργητική επίθεση** στοχεύει στη διατάραξη ή την καταστροφή ενός συστήματος, επηρεάζοντας τη λειτουργία του. Αυτό μπορεί να περιλαμβάνει επιθέσεις διανομής ιών ή κακόβουλου λογισμικού στο δίκτυο IoT, επιθέσεις άρνησης υπηρεσιών (DoS) ή και επιθέσεις χάκερ που στοχεύουν στην παραβίαση της ασφάλειας και στην παραβίαση των δεδομένων που αποθηκεύονται στο δίκτυο IoT. [2]

Συνεπώς, η παθητική και η ενεργητική επίθεση αποτελούν δύο διαφορετικούς τύπους επιθέσεων που μπορούν να στοχεύουν στα πληροφοριακά συστήματα IoT και πρέπει να ληφθούν υπόψη κατά τον σχεδιασμό και την ανάπτυξη ασφαλών συστημάτων.

Συμπερασματικά, οι εξελισσόμενες τεχνολογίες IoT δημιουργούν νέες προκλήσεις για την ασφάλεια των πληροφοριακών συστημάτων, καθώς ο αριθμός των συνδεδεμένων συσκευών αυξάνεται συνεχώς. Είναι σημαντικό να λαμβάνονται όλα τα απαραίτητα μέτρα ασφαλείας για την προστασία των συσκευών IoT και της εξασφάλισης της σωστής λειτουργίας τους, ώστε να ελαχιστοποιούνται τυχόν επιθέσεις.

2.5 Αντίμετρα

Έχοντας ανάλυση και αναφέρει διάφορους από τους τύπους των εισβολέων και των επιθέσεων που μπορεί να υπάρχουν σε ένα πληροφοριακό σύστημα IoT, μπορούμε να αναφέρουμε και μερικά από τα αντίμετρα που θα μπορούσαν να εφαρμοστούν. Υπάρχουν διάφορα αντίμετρα που μπορούν να ληφθούν για την πρόληψη και αντιμετώπιση επιθέσεων. Ανάλογα με τον τύπο της επίθεσης και τον εισβολέα, οι προστατευτικές μέθοδοι και αντίμετρα μπορεί να διαφέρουν. Ορισμένα από τα βασικά αντίμετρα που μπορούν να εφαρμοστούν είναι τα εξής:

- **Επιλογή και χρήση ασφαλών συσκευών και λογισμικού:** Η επιλογή και χρήση συσκευών και λογισμικού που έχουν σχεδιαστεί με ασφάλεια, μπορεί να βοηθήσει στην αποφυγή ευπαθειών που μπορούν να χρησιμοποιηθούν για επιθέσεις.
- **Ενημέρωση και αλλαγή προεπιλογών:** Οι εργοστασιακές ρυθμίσεις συχνά δεν είναι αρκετά ασφαλείς, και μπορεί να επιτρέπουν σε κακόβουλους χρήστες να εισέλθουν στο σύστημα. Η ενημέρωση των ρυθμίσεων και η αλλαγή των προεπιλογών μπορούν να βοηθήσουν στην πρόληψη επιθέσεων.
- **Ενημέρωση και εκπαίδευση των χρηστών:** Οι χρήστες των IoT συσκευών πρέπει να ενημερώνονται συχνά για τους κινδύνους και τα μέτρα πρόληψης, καθώς και να εκπαιδεύονται για τη χρήση ασφαλών κωδικών πρόσβασης και την αντιμετώπιση κακόβουλων μηνυμάτων ηλεκτρονικού ταχυδρομείου.
- **Αναβάθμιση λογισμικού:** Οι κατασκευαστές IoT συσκευών πρέπει να παρέχουν συχνά αναβαθμίσεις λογισμικού που διορθώνουν τα ευπαθή σημεία και βελτιώνουν την ασφάλεια των συσκευών.
- **Χρήση λογισμικού ανίχνευσης κακόβουλου λογισμικού:** Η χρήση αντιιικού σε όποια συσκευή είναι δυνατή μπορεί να βοηθήσει στην ανίχνευση και την εξάλειψη ενδεχόμενων κινδύνων από κακόβουλο λογισμικό.

Επιπλέον, η χρήση κρυπτογραφημένης επικοινωνίας **(π.χ. SSL, TLS)** μπορεί να προστατεύσει την επικοινωνία μεταξύ συσκευών και πλατφορμών IoT από εξωτερικές παρεμβάσεις. Ακόμη, η χρήση διαφόρων μεθόδων αναγνώρισης των επιθέσεων μπορεί να επιτρέψει στους χρήστες να αναγνωρίζουν επιθέσεις πριν αυτές επιφέρουν βλάβη.

Εκτός από τα προαναφερθέντα αντίμετρα, υπάρχουν και άλλα που μπορούν να συμβάλλουν στην πρόληψη των επιθέσεων και των ατυχημάτων στα πληροφοριακά συστήματα (IoT). Για παράδειγμα, α) η προστασία του δικτύου και συστήματος με **firewalls και intrusion detection/prevention systems (IDS/IPS)** που μπορούν να ανιχνεύουν και να μπλοκάρουν εισβολές (εσωτερικους και εξωτερικούς). β) Η χρήση ασφαλών πιστοποιητικών και κλειδιών για την ασφαλή επικοινωνία μεταξύ των συσκευών και του cloud. γ) Η εκπαίδευση του προσωπικού για την ασφαλή χρήση των πληροφοριακών συστημάτων IoT και των κινδύνων που ενέχονται. δ) Η προσεκτική επιλογή των προμηθευτών και των συσκευών που χρησιμοποιούνται, με προσοχή στην αξιοπιστία και την ασφάλεια τους. Όλα αυτά τα αντίμετρα πρέπει να εφαρμόζονται σε συνδυασμό μεταξύ τους για να εξασφαλιστεί η ασφάλεια των πληροφοριακών συστημάτων IoT.

Συνολικά, η αποτελεσματική προστασία των πληροφοριακών συστημάτων IoT απαιτεί μια συνεκτική προσέγγιση που συνδυάζει τη χρήση κατάλληλων τεχνολογιών ασφαλείας, την εκπαίδευση των χρηστών και τη λήψη μέτρων για τη διατήρηση της ασφάλειας του συστήματος. Επίσης, οι εταιρείες πρέπει να ενισχύσουν την ασφάλεια των προϊόντων τους από τη σχεδίαση τους, χρησιμοποιώντας κρυπτογραφία, αυθεντικοποίηση, ενημερώσεις λογισμικού και άλλα μέτρα ασφαλείας.

Συνοψίζοντας όλα τα παραπάνω, μπορούμε να πούμε ότι η ασφάλεια των πληροφοριακών συστημάτων (IoT) αποτελεί έναν σημαντικό παράγοντα για την προστασία των προσωπικών και εμπιστευτικών δεδομένων. Οι επιθέσεις μπορούν να έχουν σημαντικές επιπτώσεις στους χρήστες και τις επιχειρήσεις, και έτσι οι αντίστοιχες μέθοδοι αντιμετώπισης και πρόληψης πρέπει να λαμβάνονται σοβαρά υπόψη.

3. IoT και Υγεία

3.1 Εφαρμογές του IoT στην υγεία

Οι εφαρμογές του Internet of Things (IoT) έχουν εξελιχθεί και επεκταθεί σε πολλούς τομείς της ζωής μας στις μέρες μας. Όπως είδη έχουμε αναφέρει το IoT έχει ενταχθεί στην καθημερινότητα μας μέσω απλών συσκευών, που υπήρχαν και παλαιοτέρα, όμως πλέον έχουν την δυνατότητα να συλλέγουν δεδομένα, να τα επικοινωνουν και να έχουν λειτουργίες που τις καθιστούν έξυπνες συσκευές. Ακόμα έχει ενταχθεί στις πόλεις, στο τομέα του εμπορίου και στις βιομηχανίες. Ένας όμως από τους σημαντικότερους τομείς που έχει εφαρμογή είναι ο τομέας της υγείας. Σίγουρα, ο τομέας της υγείας έχει αναπτύξει πολλές εφαρμογές του IoT που βοηθούν στην παρακολούθηση της υγείας των ανθρώπων, την αποτελεσματική παροχή υπηρεσιών υγείας και την ανακάλυψη νέων θεραπευτικών μεθόδων. Ορισμένα παραδείγματα εφαρμογών του IoT στον τομέα της υγείας περιλαμβάνουν: [4]

- **Παρακολούθηση της καρδιακής υγείας:** Η χρήση αισθητήρων καρδιακού ρυθμού και συσκευών παρακολούθησης μπορεί να βοηθήσει στην ανίχνευση και τη διάγνωση καρδιακών προβλημάτων, καθώς και στην παρακολούθηση ασθενών με υποτροπιάζουσα ανακοπή της καρδιάς.
- **Συστήματα φαρμακευτικής διαχείρισης:** Τα συστήματα IoT μπορούν να χρησιμοποιηθούν για την παρακολούθηση της χορήγησης φαρμάκων στους ασθενείς, την ειδοποίηση για έλλειψη φαρμάκων και τη διευκόλυνση της ανταλλαγής πληροφοριών μεταξύ γιατρών και ασθενών.
- **Παρακολούθηση του ύπνου:** Οι αισθητήρες που φοριούνται κατά τη διάρκεια του ύπνου μπορούν να παρακολουθήσουν την ποιότητα του ύπνου και να παρέχουν στους ασθενείς συμβουλές για τη βελτίωσή του.
- **Τηλεϊατρική:** Η χρήση της τεχνολογίας του IoT μπορεί να επιτρέψει τη διαδικτυακή συνδεσιμότητα μεταξύ γιατρών και ασθενών, και να επιτρέψει στους ασθενείς να λαμβάνουν ιατρική περίθαλψη από απόσταση.
- **Παρακολούθηση της διατροφής:** Οι αισθητήρες μπορούν να χρησιμοποιηθούν για την παρακολούθηση των διατροφικών συνηθειών των ασθενών και την παροχή συμβουλών για τη βελτίωση της υγείας.
- **Παρακολούθηση της απόδοσης του αθλητή:** Οι αισθητήρες μπορούν να χρησιμοποιηθούν για την παρακολούθηση της απόδοσης των αθλητών και την ανίχνευση τραυματισμών και επιβαρύνσεων.

Αυτά είναι μερικά παραδείγματα των εφαρμογών του IoT στον τομέα της υγείας. Υπάρχουν όμως πολλές άλλες εφαρμογές, καθώς η τεχνολογία συνεχώς εξελίσσεται.

Η **τηλεχειρουργική** είναι μία από τις εφαρμογές αυτές, με την οποία θα ασχοληθούμε αναλυτικότερα στην επόμενη ενότητα. Αυτή η τεχνολογία επιτρέπει σε χειρουργούς να πραγματοποιούν χειρουργικές επεμβάσεις από απόσταση μέσω ρομποτικών συστημάτων.

Τα ρομποτικά συστήματα της τηλεχειρουργικής αποτελούνται από μια κονσόλα ελέγχου, μια κάμερα και μία μονάδα ρομποτικής επέμβασης. Ο χειρουργός συνδέεται στην κονσόλα ελέγχου και από εκεί διεξάγει την επέμβαση. Η κάμερα βρίσκεται στην ενδοσκοπική συσκευή που εισάγεται μέσα στον ασθενή και παρέχει εικόνα στην κονσόλα ελέγχου. Η μονάδα ρομποτικής επέμβασης αντικαθιστά το χέρι του χειρουργού και επιτρέπει στον χειρουργό να ελέγχει την ενδοσκοπική συσκευή και να πραγματοποιεί την επέμβαση.

Αυτή ήταν μια σύντομη περιγραφή για το πως λειτουργεί τηλεχειρουργική. Παρακάτω θα αναφερθούν μερικά παραδείγματα χρήσης του IoT στον τομέα της υγείας.

Παράδειγμα 1

Ένα αναλυτικό παράδειγμα εφαρμογής του IoT στον τομέα της υγείας είναι οι έξυπνες ιατρικές συσκευές, όπως οι έξυπνοι αισθητήρες και ηλεκτρονικές συσκευές παρακολούθησης της υγείας.

Οι έξυπνοι αισθητήρες και ηλεκτρονικές συσκευές παρακολούθησης της υγείας μπορούν να φορεθούν στο σώμα του ασθενούς ή να εγκατασταθούν/εξαχθούν σε/από ένα αντικείμενο που χρησιμοποιείται καθημερινά, όπως το κινητό τηλέφωνο. Αυτές οι συσκευές μπορούν να παρακολουθούν την καρδιακή ρυθμό, την αρτηριακή πίεση, τη γλυκόζη του αίματος, τη θερμοκρασία του σώματος και άλλα σημαντικά βιομετρικά δεδομένα.

Αυτά τα δεδομένα μπορούν να σταλούν σε ένα σύστημα παρακολούθησης της υγείας μέσω ασύρματης σύνδεσης, όπου δύναται να αναλυθούν από εξειδικευμένους επαγγελματίες της υγείας, όπως γιατρούς ή νοσηλευτές. Η λειτουργία αυτή μπορεί να βοηθήσει στην παρακολούθηση και τη διάγνωση παθήσεων, όπως είναι η υπέρταση και άλλες ασθένειας που μπορεί να εμφανιστούν. Έπειτα οι γιατροί έχοντας τα δεδομένα μπορούν να προχωρήσουν άμεσα στην διάγνωση και την αντιμετώπιση της πάθησης του ασθενή.

Παράδειγμα 2

Ένα ακόμα παράδειγμα εφαρμογής του IoT στον τομέα της υγείας είναι η χρήση έξυπνων βιοαισθητήρων (smart sensors) για την παρακολούθηση των ασθενών στο σπίτι τους. Οι βιοαισθητήρες αυτοί μπορούν να τοποθετηθούν σε διάφορα σημεία του σπιτιού, όπως το κρεβάτι, η καρέκλα ή ακόμη και οι τουαλέτες, και να παρακολουθούν τη συμπεριφορά ή τα συμπτώματα των ασθενών και περιβαλλοντικά στοιχεία.

Με αυτόν τον τρόπο, οι γιατροί μπορούν να παρακολουθούν την κατάσταση των ασθενών τους από απόσταση και να ανιχνεύουν πρόβλημα στην υγεία τους πριν αυτό εξελιχθεί σε σοβαρότερο πρόβλημα που θα απαιτήσει άμεση ιατρική περίθαλψη. Επιπλέον, οι βιοαισθητήρες αυτοί μπορούν να στείλουν αυτόματα ειδοποιήσεις στους γιατρούς ή τους συγγενείς των ασθενών σε περίπτωση που ανιχνευθεί κάποιο πρόβλημα ή προβλέπεται κάποια ανωμαλία.

3.2 Οφέλη εφαρμογών

Οι εφαρμογές του Internet of Things (IoT) στον τομέα της υγείας έχουν πολλά οφέλη και δυνατότητες βελτίωσης της παροχής υγειονομικής περίθαλψης. Αναφέρονται κάποια από τα κύρια οφέλη:

- **Παρακολούθηση και πρόληψη:** Οι συσκευές IoT μπορούν να χρησιμοποιηθούν για τη συνεχή παρακολούθηση της κατάστασης του ασθενούς, όπως η μέτρηση της αρτηριακής πίεσης, των καρδιακών παλμών, της θερμοκρασίας και άλλων βιολογικών παραμέτρων. Αυτό μπορεί να βοηθήσει στην έγκαιρη ανίχνευση προβλημάτων υγείας και στην πρόληψή τους.
- **Αυξημένη ασφάλεια ασθενών:** Οι συσκευές IoT μπορούν να επιτρέψουν τον αυτόματο εντοπισμό και να ειδοποιήσουν σε περίπτωση έκτακτης ανάγκης ή πτώσης. Επίσης, μπορούν να διασφαλίσουν την ασφάλεια των ασθενών μέσω παραμέτρων όπως η παρακολούθηση της λήψης φαρμάκων ή η αποτροπή ανεπιθύμητων συμβάντων (π.χ. πρόβλεψη υπογλυκαιμίας).
- **Βελτιωμένη παρακολούθηση απομακρυσμένων ασθενών:** Οι συσκευές IoT επιτρέπουν την συνεχή παρακολούθηση ασθενών που βρίσκονται σε απομακρυσμένες τοποθεσίες, και στο ίδιο τους το σπίτ. Αυτό επιτρέπει στους ασθενείς να λαμβάνουν φροντίδα υγείας στο άνετο περιβάλλον τους, ενώ ταυτόχρονα παρέχεται η δυνατότητα παρακολούθησης και αξιολόγησης της κατάστασής τους από απόσταση.
- **Βελτιωμένη διαχείριση χρόνου και αποδοτικότητα:** Οι τεχνολογίες IoT μπορούν να αυτοματοποιήσουν διάφορες διαδικασίες και εργασίες, βελτιώνοντας έτσι την αποδοτικότητα και εξοικονομώντας χρόνο. Για παράδειγμα, μπορούν να γίνουν αυτόματες παραγγελίες φαρμάκων ή να αποσταλούν αυτόματες ειδοποιήσεις σε γιατρούς ή νοσηλευτές για περιπτώσεις που απαιτούν άμεση προσοχή.
- **Εξοικονόμηση κόστους:** Η χρήση του IoT μπορεί να συμβάλλει στη μείωση των ιατρικών δαπανών και τη βελτίωση της αποτελεσματικότητας των θεραπευτικών παρεμβάσεων. Η παρακολούθηση της κατάστασης των ασθενών μπορεί να βοηθήσει στην πρόληψη των επανεισαγωγών στο νοσοκομείο και στην αποφυγή επείγουσας ιατρικής περίθαλψης. Επίσης, η παρακολούθηση των ασθενών μπορεί να μειώσει τον αριθμό των απαραίτητων επισκέψεων στο ιατρείο ή το νοσοκομείο, μειώνοντας έτσι το κόστος της υγειονομικής περίθαλψης για τους ασθενείς και το σύστημα υγείας γενικότερα.

Άλλο ένα σημαντικό όφελος του IoT στον τομέα της υγείας είναι η βελτίωση της διαχείρισης των χρόνιων ασθενειών. Με τη χρήση συσκευών IoT, οι ασθενείς μπορούν να παρακολουθούν την κατάσταση της υγείας τους και να μεταφέρουν αυτές τις πληροφορίες στους γιατρούς τους. Αυτό μπορεί να βοηθήσει τους γιατρούς να παρακολουθούν την κατάσταση των ασθενών τους από απόσταση και να προβλέπουν επικείμενες επιδεινώσεις ή επιπλοκές χωρίς να αμελούνται ή απαιτούνται ιατρικές εξετάσεις.

Τέλος, οι συσκευές IoT μπορούν να χρησιμοποιηθούν για τη βελτίωση της ασφάλειας των ασθενών και του περιβάλλοντος τους. Για παράδειγμα, στα νοσοκομεία,

οι αισθητήρες IoT μπορούν να παρακολουθούν τις συνθήκες του περιβάλλοντος, όπως η θερμοκρασία και η υγρασία, για να διασφαλίσουν ότι οι ασθενείς δεν εκτίθενται σε κίνδυνο. Επίσης, οι αισθητήρες μπορούν να χρησιμοποιηθούν για να εντοπιστούν αυτόματα κινδύνους όπως η πτώση των ασθενών, και να ειδοποιούν το νοσηλευτικό προσωπικό.

Αυτά είναι μερικά από τα οφέλη που προσφέρουν οι εφαρμογές του IoT στον τομέα της υγείας. Επιτρέπουν την πιο αποτελεσματική παροχή υγειονομικής περίθαλψης, την παρακολούθηση και πρόληψη προβλημάτων υγείας και τη βελτίωση της ποιότητας ζωής των ασθενών.

3.3 Κίνδυνοι

Όπως αναφέρθηκε προηγουμένως, η σύνδεση των ιατρικών συσκευών και των δεδομένων τους με το IoT μπορεί να επιφέρει σοβαρές επιπτώσεις και κινδύνους ασφαλείας και ιδιωτικότητας. Ορισμένοι από τους κινδύνους και τις απειλές που πρέπει να ληφθούν υπόψη είναι οι εξής: [3]

- **Επιθέσεις χάκερ:** οι συνδεδεμένες συσκευές και τα δεδομένα τους μπορούν να αποτελέσουν στόχο επιθέσεων από κακόβουλους χάκερ. Η επιτυχία μιας τέτοιας επίθεσης μπορεί να έχει σοβαρές συνέπειες στην υγεία και την ασφάλεια των ασθενών.
- **Διαρροές δεδομένων:** η σύνδεση των ιατρικών συσκευών με το διαδίκτυο δημιουργεί ένα σημείο εισόδου για την απώλεια ή τη διαρροή ευαίσθητων πληροφοριών ασθενών, όπως ιατρικά ιστορικά, φωτογραφίες και άλλα προσωπικά δεδομένα.
- **Σφάλματα συστήματος:** η χρήση της τεχνολογίας IoT στην υγεία απαιτεί την αξιόπιστη λειτουργία του συστήματος για να εξασφαλιστεί η ακρίβεια των δεδομένων και η ασφάλεια των ασθενών.

Σημαντικός κίνδυνος στη χρήση του IoT στον τομέα της υγείας είναι η διαρροή των προσωπικών δεδομένων. Οι συσκευές IoT συλλέγουν μεγάλο όγκο προσωπικών δεδομένων των ασθενών, όπως πληροφορίες υγείας, διαγνωστικά αποτελέσματα και ιατρικά ιστορικά, τα οποία είναι ευαίσθητα και πρέπει να προστατεύονται από τρίτους.

Επιπλέον, οι συσκευές IoT μπορεί να είναι ευάλωτες σε κυβερνοεπιθέσεις και κακόβουλο λογισμικό, τα οποία μπορεί να προκαλέσουν ως κλιμακωτά αποτελέσματα (cascading effects) σοβαρά προβλήματα υγείας. Για παράδειγμα, ένα κακόβουλο λογισμικό μπορεί να διακόψει τη λειτουργία ιατρικού εξοπλισμού, να παραβιάσει τα προσωπικά δεδομένα του ασθενούς ή ακόμα και να παρεμποδίσει την ασφαλή παρακολούθηση της υγείας του ασθενούς.

Τέλος, η υπερβολική εξάρτηση από τις συσκευές IoT μπορεί να οδηγήσει σε μειωμένη διαθεσιμότητα των ιατρικών επαγγελματιών και σε απώλεια των δεξιοτήτων και της εμπειρίας που απαιτούνται.

Εκτός από τις επιθέσεις που μπορεί να υπάρξουν και τους κακόβουλους χρήστες που θέλουν να βλάψουν με κάποιον τρόπο το σύστημα ή τους ασθενείς υπάρχουν και ορισμένα λάθη που μπορεί να κάνουν οι χρήστες ή οι γιατροί και να αφήσουν κενά ασφαλείας στα συστήματα υγείας IoT περιλαμβάνουν, όπως: [6]

- **Χρήση αδύναμων κωδικών πρόσβασης**: Η χρήση εύκολων κωδικών πρόσβασης, όπως 1234 ή password, είναι ένα από τα πιο κοινά λάθη που κάνουν οι χρήστες και διευκολύνει τους κακόβουλους επιτιθέμενους να προσπελάσουν τα συστήματα.
- **Μη ενημέρωση των συστημάτων λογισμικού:** Η μη ενημέρωση του λογισμικού των συστημάτων είναι ένα άλλο κοινό λάθος που μπορεί να οδηγήσει σε

εκμετάλλευση κενών ασφαλείας και ευπαθειών από κακόβουλους επιτιθέμενους.

- **Χρήση διεπαφών δικτύου που δεν είναι ασφαλής:** Η χρήση μη ασφαλών διεπαφών δικτύου για τη σύνδεση στα συστήματα IoT μπορεί να αφήσει ανοιχτό ένα παράθυρο για επιθέσεις.
- **Χρήση αναποτελεσματικών μεθόδων κρυπτογράφησης:** Ο κίνδυνος προκύπτει αν οι χρήστες και οι γιατροί δεν χρησιμοποιούν αποτελεσματικές μεθόδους κρυπτογράφησης για τις επικοινωνίες τους.

Επιπλέον, ένα σημαντικό σφάλμα που μπορεί να γίνει είναι η αδυναμία ασφαλούς αποθήκευσης και διαχείρισης των δεδομένων υγείας. Οι χρήστες ή οι γιατροί μπορεί να χρησιμοποιήσουν μη ασφαλείς συσκευές αποθήκευσης ή να αποθηκεύουν τα δεδομένα σε μη έμπιστα υπολογιστικά συστήματα, ανοίγοντας την πόρτα για δυνητικές κλοπές δεδομένων.

Συμπερασματικά, για να αποφευχθούν αυτά τα λάθη, είναι σημαντικό να εκπαιδεύονται οι χρήστες και οι γιατροί σχετικά με την ασφάλεια και την προστασία δεδομένων και να χρησιμοποιούνται αξιόπιστες συσκευές και λογισμικά με ενημερωμένα συστήματα ασφαλείας. Επίσης, είναι σημαντικό να γίνεται ασφαλής αποθήκευση και διαχείριση των δεδομένων υγείας μέσω ασφαλών υπολογιστικών συστημάτων και συσκευών αποθήκευσης.

3.4 Αντιμετώπιση κινδύνων

Αναγνωρίζονται διάφορες τεχνικές για να αποφευχθούν οι επιθέσεις στα συστήματα του IoT στον τομέα της υγείας. Ορισμένες από αυτές είναι οι εξής:

- **Αυξημένη ασφάλεια των συσκευών:** Οι κατασκευαστές πρέπει να ενσωματώνουν υψηλά επίπεδα ασφάλειας στις συσκευές τους, καθώς και τη δυνατότητα αναβάθμισης και ενημέρωσης του λογισμικού τους. Επίσης οι εταιρείες που κάνουν χρήση αυτών πρέπει να ενημερώνουν συχνά το λογισμικό στις συσκευές για να διορθώνουν κάθε ευπάθεια ή σημείο εισόδου για επιθέσεις.
- **Ενισχυμένη ασφάλεια δικτύου και συσκευών:** Οι εταιρείες μπορούν να χρησιμοποιήσουν τεχνολογίες ασφάλειας όπως κρυπτογράφηση δεδομένων, πιστοποιητικά ασφαλείας, διακριτικοί κωδικοί πρόσβασης και δίκτυα επιτήρησης για να προστατεύσουν τα δίκτυα και τις συσκευές από επιθέσεις.
- **Εκπαίδευση και ευαισθητοποίηση των χρηστών:** Το προσωπικό πρέπει να εκπαιδεύεται για τις βασικές αρχές της ασφάλειας των δικτύων και της προστασίας των δεδομένων και να είναι σε θέση να αναγνωρίζει τις απειλές και τα πιθανά σημεία εισόδου για επιθέσεις.

4. Εργαλείο αξιολόγησης κινδύνου OWASP

4.1 Εισαγωγή

Το **OWASP** έχει την ικανότητα εκτίμησης του σχετικού κινδύνου σε κάθε κατάσταση, έχοντας πρώτα καταγράψει τα τρωτά σημεία του συστήματος. Σε πρώιμο στάδιο του κύκλου ζωής, μπορούν να εντοπιστούν οι ανησυχίες για την ασφάλεια στην αρχιτεκτονική ή το σχεδιασμό χρησιμοποιώντας τη μοντελοποίηση απειλών. Σε δεύτερο στάδιο, μπορούν να εντοπιστούν ζητήματα ασφάλειας χρησιμοποιώντας αναθεώρηση κώδικα ή δοκιμές διείσδυσης (penetration tests). Μερικά από τα προβλήματα μπορεί να μην ανακαλυφθούν έως ότου η εφαρμογή τεθεί σε παραγωγή και εκτεθεί σε κίνδυνο. [12]

Με το OWASP είναι δυνατόν να εκτιμηθεί η σοβαρότητα όλων αυτών των κινδύνων για το σύστημα και να ληφθεί τεκμηριωμένη απόφαση σχετικά με το τι πρέπει να γίνει για τους κινδύνους αυτούς. Η ύπαρξη του για την αξιολόγηση των κινδύνων θα εξοικονομήσει χρόνο και θα εξαλείψει τις διαφωνίες σχετικά με τις προτεραιότητες. Το OWASP θα βοηθήσει να διασφαλιστεί ότι το σύστημα δεν θα αποσπάται από δευτερεύοντες κινδύνους, ενώ θα αγνοεί σοβαρότερους κινδύνους που δενείναι εύκολα κατανοητοί ή εντοπίσιμοι.

4.2 Μεθοδολογία

Υπάρχουν πολλές διαφορετικές προσεγγίσεις για την ανάλυση κινδύνου. Η προσέγγιση OWASP που παρουσιάζεται εδώ βασίζεται σε αυτές τις τυπικές μεθοδολογίες και είναι προσαρμοσμένη για ασφάλεια εφαρμογών. Ο ορισμός του κινδύνο είναι ο εξής:

Κίνδυνος = Πιθανότητα * Αντίκτυπος (Risk = Likelihood * Impact)

Συνοπτικά τα βήματα είναι τα εξής:

Βήμα 1: Προσδιορισμός κινδύνου

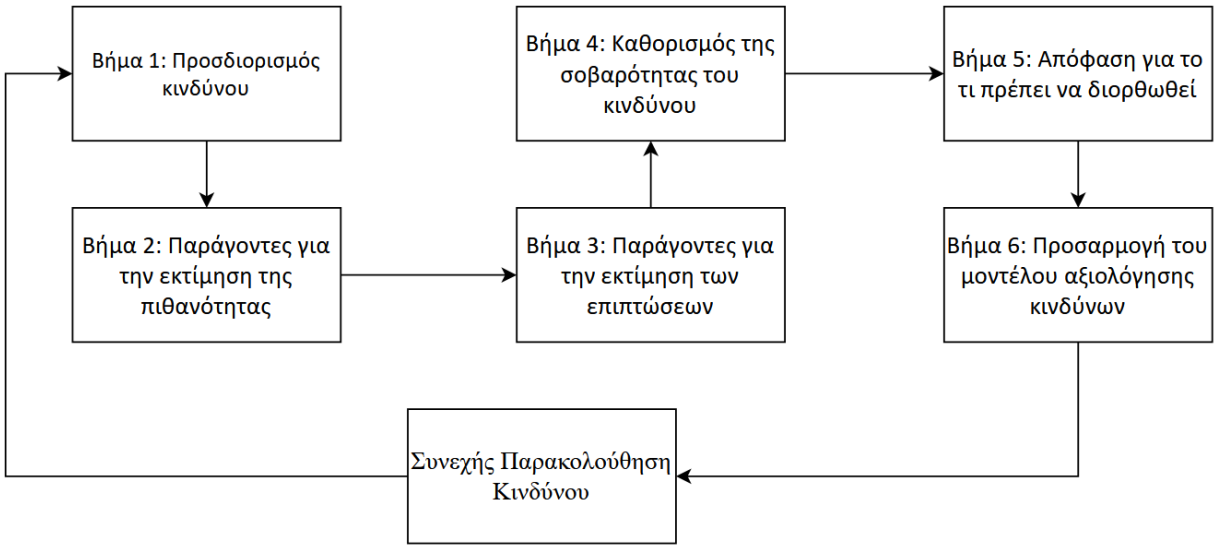
Βήμα 2: Παράγοντες για την εκτίμηση της πιθανότητας

Βήμα 3: Παράγοντες για την εκτίμηση των επιπτώσεων

Βήμα 4: Καθορισμός της σοβαρότητας του κινδύνου

Βήμα 5: Απόφαση για το τι πρέπει να διορθωθεί

Βήμα 6: Προσαρμογή του μοντέλου αξιολόγησης κινδύνων



Εικόνα 4: Βήματα ανάλυσης κινδύνου OWASP

4.2.1 Βήμα 1: Προσδιορισμός κινδύνου

Το πρώτο βήμα είναι ο εντοπισμός ενός κινδύνου ασφαλείας που πρέπει να αξιολογηθεί. Πρέπει να συγκεντρωθούν πληροφορίες σχετικά με τον παράγοντα απειλής που εμπλέκεται, την επίθεση που θα χρησιμοποιηθεί, την ευπάθεια που εμπλέκεται και τον αντίκτυπο μιας επιτυχημένης εκμετάλλευσης μιας ευπάθειας στην επιχείρηση. Μπορεί να υπάρχουν πολλαπλές πιθανές ομάδες επιτιθέμενων ή ακόμη και πολλαπλές πιθανές επιπτώσεις στην επιχείρηση. Σε γενικές γραμμές, είναι καλύτερο να προτιμάτε τη χειρότερη δυνατή επιλογή, καθώς αυτή θα έχει ως αποτέλεσμα τον υψηλότερο συνολικό κίνδυνο.

4.2.2 Βήμα 2: Παράγοντες για την εκτίμηση της πιθανότητας

Μόλις εντοπίσουμε έναν πιθανό κίνδυνο και θέλουμε να καταλάβουμε πόσο σοβαρός είναι, το πρώτο βήμα είναι να εκτιμήσουμε την "πιθανότητα". Σε υψηλότερο επίπεδο, πρόκειται για ένα πρόχειρο μέτρο του πόσο πιθανό είναι να αποκαλυφθεί και να αξιοποιηθεί η συγκεκριμένη ευπάθεια από έναν επιτιθέμενο. Δεν είναι απαραίτητο να είναι υπερβολικά ακριβής αυτή η εκτίμηση. Γενικά, αρκεί να προσδιορίστεί αν η πιθανότητα είναι χαμηλή, μεσαία ή υψηλή.

Υπάρχουν διάφοροι παράγοντες που μπορούν να βοηθήσουν στον προσδιορισμό της πιθανότητας. Η πρώτη ομάδα παραγόντων σχετίζεται με τον εμπλεκόμενο παράγοντα απειλής. Ο στόχος είναι να εκτιμηθεί η πιθανότητα μιας επιτυχημένης επίθεσης από μια ομάδα πιθανών επιτιθέμενων. Μπορεί να υπάρχουν πολλαπλοί παράγοντες απειλής που μπορούν να εκμεταλλευτούν μια συγκεκριμένη ευπάθεια, οπότε είναι καλύτερο να χρησιμοποιηθεί το χειρότερο σενάριο. Για παράδειγμα, ένας εσωτερικός χρήστης μπορεί να είναι πολύ πιο πιθανός επιτιθέμενος από έναν ανώνυμο εξωτερικό, αλλά αυτό εξαρτάται από διάφορους παράγοντες.

Κάθε παράγοντας έχει ένα σύνολο επιλογών και κάθε επιλογή έχει μια βαθμολογία πιθανότητας από 0 έως 9 που συνδέεται με αυτήν. Αυτοί οι αριθμοί θα χρησιμοποιηθούν αργότερα για την εκτίμηση της συνολικής πιθανότητας.

Παράγοντες παράγοντα απειλής

Η πρώτη ομάδα παραγόντων σχετίζεται με τον παράγοντα απειλής που εμπλέκεται. Ο στόχος είναι να εκτιμηθεί η πιθανότητα επιτυχούς επίθεσης από αυτή την ομάδα παραγόντων απειλής. Χρησιμοποείται ο παράγοντας απειλής της χειρότερης περίπτωσης.

Επίπεδο δεξιοτήτων - Πόσο τεχνικά καταρτισμένη είναι αυτή η ομάδα απειλητικών παραγόντων; Καμία τεχνική δεξιότητα (1), κάποιες τεχνικές δεξιότητες (3), προχωρημένος χρήστης υπολογιστών (5), δεξιότητες δικτύου και προγραμματισμού (6), δεξιότητες διείσδυσης στην ασφάλεια (9)

Κίνητρο - Πόσο κίνητρο έχει αυτή η ομάδα παραγόντων απειλής να βρει και να εκμεταλλευτεί αυτή την ευπάθεια; Χαμηλή ή καθόλου ανταμοιβή (1), πιθανή ανταμοιβή (4), υψηλή ανταμοιβή (9)

Ευκαιρία - Ποιοι πόροι και ευκαιρίες απαιτούνται για αυτή την ομάδα παραγόντων απειλής για να βρει και να εκμεταλλευτεί αυτή την ευπάθεια; Απαιτείται πλήρης πρόσβαση ή ακριβοί πόροι (0), απαιτείται ειδική πρόσβαση ή πόροι (4), απαιτείται κάποια πρόσβαση ή πόροι (7), δεν απαιτείται καμία πρόσβαση ή πόροι (9)

Μέγεθος - Πόσο μεγάλη και με ποια εξειδίκευση είναι αυτή η ομάδα παραγόντων απειλής; Προγραμματιστές (2), διαχειριστές συστημάτων (2), χρήστες του εσωτερικού δικτύου (4), συνεργάτες (5), πιστοποιημένοι χρήστες (6), ανώνυμοι χρήστες του Διαδικτύου (9)

Παράγοντες τρωτότητας

Η επόμενη ομάδα παραγόντων σχετίζεται με την ευπάθεια που υπάρχει. Ο στόχος είναι να εκτιμηθεί η πιθανότητα ανακάλυψης και εκμετάλλευσης της συγκεκριμένης ευπάθειας. Ας υποθέσουμε τον παράγοντα απειλής που επιλέχθηκε παραπάνω.

Ευκολία ανακάλυψης - Πόσο εύκολο είναι για αυτή την ομάδα παραγόντων απειλής να ανακαλύψει αυτή την ευπάθεια; Πρακτικά αδύνατο (1), δύσκολο (3), εύκολο (7), διαθέσιμα αυτοματοποιημένα εργαλεία (9)

Ευκολία εκμετάλλευσης - Πόσο εύκολο είναι για αυτή την ομάδα παραγόντων απειλής να εκμεταλλευτεί πραγματικά αυτή την ευπάθεια; Θεωρητικά (1), δύσκολα (3), εύκολα (5), διαθέσιμα αυτοματοποιημένα εργαλεία (9)

Ευαισθητοποίηση - Πόσο γνωστή είναι αυτή η ευπάθεια σε αυτή την ομάδα παραγόντων απειλών; Άγνωστη (1), κρυφή (4), προφανής (6), δημόσια γνώση (9)

Ανίχνευση εισβολής - Πόσο πιθανό είναι να εντοπιστεί ένα exploit (διείσδυση εκμετάλλευσης ευπάθειας); Ενεργή ανίχνευση στην εφαρμογή (1), καταγραφή και επανεξέταση (3), καταγραφή χωρίς επανεξέταση (8), μη καταγραφή (9)

4.2.3 Βήμα 3: Παράγοντες για την εκτίμηση των επιπτώσεων

Για μια επιτυχημένη επίθεση, υπάρχουν δύο είδη επιπτώσεων. Η πρώτη είναι ο "τεχνικός αντίκτυπος" στην εφαρμογή, τα δεδομένα που χρησιμοποιεί και τις λειτουργίες που παρέχει. Η άλλη είναι ο "επιχειρηματικός αντίκτυπος" στην επιχείρηση και την εταιρεία που διαχειρίζεται την εφαρμογή.

Ο επιχειρηματικός αντίκτυπος είναι πιο σημαντικός. Ωστόσο, ενδέχεται να μην υπάρχει πρόσβαση σε όλες τις πληροφορίες που απαιτούνται για να υπολογίσουμε τις επιχειρηματικές συνέπειες μιας επιτυχημένης εκμετάλλευσης. Στην περίπτωση αυτή, η παροχή όσο το δυνατόν περισσότερων λεπτομερειών σχετικά με τον τεχνικό κίνδυνο θα επιτρέψει στον αρμόδιο εκπρόσωπο της επιχείρησης να λάβει απόφαση σχετικά με τον επιχειρηματικό κίνδυνο.

Και πάλι, κάθε παράγοντας έχει ένα σύνολο επιλογών και κάθε επιλογή έχει μια βαθμολογία επιπτώσεων από 0 έως 9 που συνδέεται με αυτήν. Θα χρησιμοποιήσουμε αυτούς τους αριθμούς αργότερα για να εκτιμήσουμε τον συνολικό αντίκτυπο.

Τεχνικοί παράγοντες αντίκτυπου

Ο τεχνικός αντίκτυπος μπορεί να αναλυθεί σε παράγοντες που ευθυγραμμίζονται με τους παραδοσιακούς τομείς ασφάλειας: εμπιστευτικότητα, ακεραιότητα, διαθεσιμότητα και υπευθυνότητα. Ο στόχος είναι να εκτιμηθεί το μέγεθος των επιπτώσεων στο σύστημα σε περίπτωση εκμετάλλευσης της ευπάθειας.

Απώλεια εμπιστευτικότητας - Πόσα δεδομένα θα μπορούσαν να αποκαλυφθούν και πόσο ευαίσθητα είναι; Αποκάλυψη ελάχιστων μη ευαίσθητων δεδομένων (2), αποκάλυψη ελάχιστων κρίσιμων δεδομένων (6), αποκάλυψη εκτεταμένων μη ευαίσθητων δεδομένων (6), αποκάλυψη εκτεταμένων κρίσιμων δεδομένων (7), αποκάλυψη όλων των δεδομένων (9).

Απώλεια ακεραιότητας - Πόσα δεδομένα θα μπορούσαν να καταστραφούν και πόσο κατεστραμμένα είναι; Ελάχιστα ελαφρά κατεστραμμένα δεδομένα (1), ελάχιστα σοβαρά κατεστραμμένα δεδομένα (3), εκτεταμένα ελαφρά κατεστραμμένα δεδομένα (5), εκτεταμένα σοβαρά κατεστραμμένα δεδομένα (7), όλα τα δεδομένα πλήρως κατεστραμμένα (9)

Απώλεια διαθεσιμότητας - Σε ποιο βαθμό μια υπηρεσία θα μπορούσε να χαθεί και πόσο ζωτικής σημασίας είναι; Ελάχιστη διακοπή δευτερευουσών υπηρεσιών (1), ελάχιστη διακοπή πρωτογενών υπηρεσιών (5), εκτεταμένη διακοπή δευτερευουσών υπηρεσιών (5), εκτεταμένη διακοπή πρωτογενών υπηρεσιών (7), πλήρης απώλεια όλων των υπηρεσιών (9)

Απώλεια λογοδοσίας υπευθύνου - Οι ενέργειες των παραγόντων απειλής μπορούν να αποδοθούν σε ένα άτομο; Πλήρως ανιχνεύσιμο (1), ενδεχομένως ανιχνεύσιμο (7), εντελώς ανώνυμο (9)

Παράγοντες επιχειρηματικού αντίκτυπου

Ο επιχειρηματικός αντίκτυπος απορρέει από τον τεχνικό αντίκτυπο, αλλά απαιτεί βαθιά κατανόηση του τι είναι σημαντικό για την εταιρεία που διαχειρίζεται την εφαρμογή. Ο επιχειρηματικός κίνδυνος είναι αυτό που δικαιολογεί την επένδυση στη διόρθωση των προβλημάτων ασφαλείας.

Πολλές εταιρείες διαθέτουν έναν οδηγό ταξινόμησης περιουσιακών στοιχείων ή/και μια αναφορά επιχειρηματικού αντίκτυπου για να βοηθήσουν στην επισημοποίηση του τι είναι σημαντικό για την επιχείρησή τους.

Οι παρακάτω παράγοντες είναι κοινοί για πολλές επιχειρήσεις, αλλά αυτός ο τομέας είναι ακόμη πιο μοναδικός και εξατομικευμένος για μια εταιρεία από τους παράγοντες που σχετίζονται με τον παράγοντα απειλής, την ευπάθεια και τον τεχνικό αντίκτυπο.

Οικονομική ζημία - Πόση οικονομική ζημία θα προκύψει από μια εκμετάλλευση ευπάθειας; Λιγότερο από το κόστος επιδιόρθωσης της ευπάθειας (1), μικρή επίπτωση στα ετήσια κέρδη (3), σημαντική επίπτωση στα ετήσια κέρδη (7), πτώχευση (9)

Ζημία φήμης - Θα προκαλέσει ζημία φήμης που θα βλάψει την επιχείρηση; Ελάχιστη ζημία (1), απώλεια σημαντικών λογαριασμών (4), απώλεια υπεραξίας (5), ζημία εμπορικού σήματος (9)

Μη συμμόρφωση - Πόση έκθεση συνεπάγεται η μη συμμόρφωση; Ελάχιστη παραβίαση (2), σαφής παραβίαση (5), παραβίαση υψηλού προφίλ (7)

Παραβίαση του απορρήτου - Πόσα προσωπικά αναγνωρίσιμα στοιχεία θα μπορούσαν να αποκαλυφθούν; Ενός ατόμου (3), εκατοντάδων ατόμων (5), χιλιάδων ατόμων (7), εκατομμυρίων ατόμων (9)

4.2.4 Βήμα 4: Καθορισμός της σοβαρότητας του κινδύνου

Σε αυτό το βήμα, η εκτίμηση της πιθανότητας και η εκτίμηση των επιπτώσεων συνδυάζονται για τον υπολογισμό της συνολικής σοβαρότητας του κινδύνου. Αυτό γίνεται υπολογίζοντας αν η πιθανότητα είναι χαμηλή, μεσαία ή υψηλή και στη συνέχεια το ίδιο γίνεται για τον αντίκτυπο. Η κλίμακα από 0 έως 9 χωρίζεται σε τρία μέρη:

Likelihood and Impact Levels	
0 to <3	LOW
3 to <6	MEDIUM
6 to 9	HIGH

Εικόνα 5: Πιθανότητα εμφάνισης και σοβαρότητα του κινδύνου

Άτυπη μέθοδος

Σε πολλά περιβάλλοντα, δεν είναι κακό να επανεξετάζουμε τους παράγοντες. Θα πρέπει να γίνει ανάλυση των παραγόντων κινδύνου και να εντοπίσουμε τους βασικούς "κινητήριους" παράγοντες που ελέγχουν το αποτέλεσμα στον υπολογισμό του μέσου ρίσκου. Ενδέχεται η αρχική εντύπωση να ήταν λανθασμένη εξετάζοντας πτυχές του κινδύνου που δεν ήταν προφανείς.

Επαναλαμβανόμενη μέθοδος

Εάν είναι απαραίτητη η δικαολόγηση των αξιολογήσεων ή είναι σημαντικό να τις καταστήσουμε επαναλήψιμες, τότε είναι απαραίτητο να περάσουμε από μια πιο επίσημη διαδικασία αξιολόγησης των παραγόντων και υπολογισμού του αποτελέσματος. Υπάρχει αρκετή αβεβαιότητα σε αυτές τις εκτιμήσεις και οι παράγοντες αυτοί έχουν ως στόχο να βοηθήσουν στην κατάληξη ενός λογικού αποτελέσματος. Η διαδικασία αυτή μπορεί να υποστηριχθεί από αυτοματοποιημένα εργαλεία για να διευκολυνθεί ο υπολογισμός.

Το πρώτο βήμα είναι η επιλογή μιας από τις επιλογές που σχετίζονται με κάθε παράγοντα και η εισαγωγή του σχετικού αριθμού στον πίνακα. Στη συνέχεια, απλά παίρνουμε το μέσο όρο των βαθμολογιών για να υπολογίσουμε τη συνολική πιθανότητα. Για παράδειγμα:

'"Threat agent factors"'					'"Vulnerability factors"'			
Skill level	Motive	Opportunity	Size		Ease of discovery	Ease of exploit	Awareness	Intrusion detection
5	2	7	1		3	6	9	2
Overall likelihood=4.375 (MEDIUM)								

Εικόνα 6: Παράγοντες απειλής, τρωτότητας και συνολική πιθανότητα

Στη συνέχεια, υπολογίζουμε το συνολικό αντίκτυπο. Η διαδικασία είναι παρόμοια και εδώ. Σε πολλές περιπτώσεις η απάντηση θα είναι προφανής, αλλά μπορούμε να κάνουμε μια εκτίμηση με βάση τους παράγοντες ή με τον υπολογισμό του μέσου όρου των βαθμολογιών για κάθε έναν από τους παράγοντες. Και πάλι, λιγότερο από 3 είναι χαμηλός αντίκτυπος, από 3 έως λιγότερο από 6 είναι μέτριος και από 6 έως 9 είναι υψηλός. Για παράδειγμα:

Technical Impact					**Business Impact**			
Loss of confidentiality	Loss of integrity	Loss of availability	Loss of accountability		Financial damage	Reputation damage	Non-compliance	Privacy violation
9	7	5	8		1	2	1	5
Overall technical impact=7.25 (HIGH)					Overall business impact=2.25 (LOW)			

Εικόνα 7: Τεχνική και επιχειρηματική επίπτωση κινδύνου

Καθορισμός της σοβαρότητας

Όπως και αν καταλήξουμε στις εκτιμήσεις πιθανότητας και επιπτώσεων, μπορούμε τώρα να τις συνδυάσουμε για να λάβουμε μια τελική βαθμολογία σοβαρότητας για αυτόν τον κίνδυνο. Αν έχουμε καλές πληροφορίες για τις επιχειρηματικές επιπτώσεις, θα πρέπει να τις χρησιμοποιήσουμε αντί για τις πληροφορίες για τις τεχνικές επιπτώσεις. Αν όμως δεν έχουμε πληροφορίες για την επιχείρηση, τότε ο τεχνικός αντίκτυπος είναι η επόμενη καλύτερη επιλογή.

Overall Risk Severity				
Impact	HIGH	Medium	High	Critical
	MEDIUM	Low	Medium	High
	LOW	Note	Low	Medium
		LOW	MEDIUM	HIGH
	Likelihood			

Εικόνα 8: Συνολική επίπτωση κινδύνου

Στο παραπάνω παράδειγμα, η πιθανότητα είναι μέτρια και ο τεχνικός αντίκτυπος είναι υψηλός, οπότε από καθαρά τεχνική άποψη φαίνεται ότι η συνολική σοβαρότητα είναι υψηλή. Ωστόσο, σημειώνεται ότι ο επιχειρηματικός αντίκτυπος είναι στην πραγματικότητα χαμηλός, οπότε η συνολική σοβαρότητα περιγράφεται επίσης ως χαμηλή. Αυτός είναι ο λόγος για τον οποίο η κατανόηση του επιχειρηματικού πλαισίου των ευπαθειών που αξιολογούνται είναι τόσο σημαντική για τη λήψη ορθών αποφάσεων σχετικά με τον κίνδυνο. Η μη κατανόηση αυτού του πλαισίου μπορεί να οδηγήσει στην έλλειψη εμπιστοσύνης μεταξύ των ομάδων επιχειρήσεων και ασφάλειας που υπάρχει σε πολλούς οργανισμούς.

4.2.5 Βήμα 5: Απόφαση για το τι πρέπει να διορθωθεί

Αφού ταξινομηθούν οι κίνδυνοι από την εφαρμογή, θα καταρτιστεί ένας κατάλογος προτεραιοτήτων για το τι πρέπει να διορθωθεί. Κατά γενικό κανόνα, οι πιο σοβαροί κίνδυνοι θα πρέπει να διορθώνονται πρώτοι. Το συνολικό προφίλ κινδύνου δεν έχει πρακτικό όφελος με το να διορθώνονται λιγότερο σημαντικοί κίνδυνοι, ακόμη και αν είναι εύκολο ή φθηνό να διορθωθούν.

Επίσης δεν αξίζει να διορθωθούν όλοι οι κίνδυνοι και κάποια απώλεια όχι μόνο αναμένεται, αλλά και δικαιολογείται με βάση το κόστος διόρθωσης του προβλήματος. Για παράδειγμα, αν θα κόστιζε 100.000 δολάρια η εφαρμογή ελέγχων για την ανάσχεση μια απάτης ύψους 2.000 δολαρίων ετησίως, θα χρειαστούν 50 χρόνια απόδοσης της επένδυσης για να παταχθεί η απώλεια. Αλλά μπορεί να υπάρξει ζημιά στη φήμη από την απάτη που θα μπορούσε να κοστίσει στον οργανισμό πολύ περισσότερο.

4.2.6 Βήμα 6: Προσαρμογή του μοντέλου αξιολόγησης κινδύνου

Η ύπαρξη ενός πλαισίου κατάταξης κινδύνου που μπορεί να προσαρμοστεί για μια επιχείρηση είναι κρίσιμη. Ένα προσαρμοσμένο μοντέλο είναι πολύ πιο πιθανό να παράγει αποτελέσματα που ταιριάζουν με τις αντιλήψεις των ανθρώπων σχετικά με το τι είναι σοβαρός κίνδυνος. Μπορεί να χαθεί πολύς χρόνος για διαφωνίες σχετικά με τις αξιολογήσεις κινδύνου, εάν αυτές δεν υποστηρίζονται από ένα τέτοιο μοντέλο. Υπάρχουν διάφοροι τρόποι για να προσαρμόσουμε αυτό το μοντέλο για τον οργανισμό.

Προσθήκη παραγόντων

Μπορεί να επιλεγούν διαφορετικοί παράγοντες που αντιπροσωπεύουν καλύτερα αυτό που είναι σημαντικό για τον συγκεκριμένο οργανισμό. Για παράδειγμα, μια στρατιωτική εφαρμογή θα μπορούσε να προσθέσει παράγοντες επιπτώσεων που σχετίζονται με την απώλεια ανθρώπινων ζωών ή διαβαθμισμένων πληροφοριών. Μπορεί επίσης να προσθέσουμε παράγοντες πιθανότητας, όπως το παράθυρο ευκαιρίας για έναν εισβολέα ή η ισχύς του αλγορίθμου κρυπτογράφησης.

Επιλογές προσαρμογής

Υπάρχουν ορισμένες προεπιλογές που σχετίζονται με κάθε παράγοντα, αλλά το μοντέλο θα είναι πολύ πιο αποτελεσματικό αν προσαρμόσουμε αυτές τις επιλογές στην επιχείρηση. Για παράδειγμα, να χρησιμοποιήσουμε τα ονόματα των διαφόρων ομάδων και τα ονόματα της εταιρείας για διαφορετικές ταξινομήσεις πληροφοριών. Μπορεί επίσης να αλλάξουμε τις βαθμολογίες που σχετίζονται με τις επιλογές. Ο καλύτερος τρόπος για τον εντοπισμό των σωστών βαθμολογιών είναι να συγκρίνουμε τις βαθμολογίες που παράγει το μοντέλο με τις βαθμολογίες που παράγει μια ομάδα εμπειρογνωμόνων. Μπορούμε να συντονίσουμε το μοντέλο προσαρμόζοντας προσεκτικά τις βαθμολογίες ώστε να ταιριάζουν.

Συντελεστές στάθμισης

Το αρχικό μοντέλο υποθέτει ότι όλοι οι παράγοντες είναι εξίσου σημαντικοί. Μπορούμε να δώσουμε έμφαση στους παράγοντες που είναι πιο σημαντικοί για τη συγκεκριμένη επιχείρηση. Αυτό καθιστά το μοντέλο λίγο πιο περίπλοκο, καθώς θα πρέπει να χρησιμοποιήσουμε έναν σταθμισμένο μέσο όρο. Αλλά κατά τα άλλα όλα λειτουργούν το ίδιο. Και πάλι είναι δυνατή η ρύθμιση του μοντέλου με την αντιστοίχισή του με αξιολογήσεις κινδύνου που η επιχείρηση συμφωνεί ότι είναι ακριβείς.

5. IoT και Τηλεχειρουργική

5.1 Εφαρμογή

Η τηλεχειρουργική είναι μια διαδικασία επέμβασης στο σώμα που γίνεται από απόσταση μέσω της χρήσης τηλεπικοινωνιακών και δικτυακών τεχνολογιών. Η διαδικασία αυτή απαιτεί τη χρήση ρομποτικών συστημάτων, ηλεκτρονικών συσκευών και υψηλής ταχύτητας δικτύων για τη μετάδοση δεδομένων και εικόνων σε πραγματικό χρόνο από τον τόπο όπου βρίσκεται ο χειρουργός στον τόπο όπου βρίσκεται ο ασθενής.[10]

Ένα παράδειγμα είναι η χρήση της τηλεχειρουργικής σε μακρινές ή απομακρυσμένες περιοχές, όπου η παρουσία των κορυφαίων χειρουργών σε αυτές τις περιοχές μπορεί να είναι δύσκολη. Με την τηλεχειρουργική, οι χειρουργοί μπορούν να παρακολουθούν και να ελέγχουν την εγχείρηση από απόσταση, χρησιμοποιώντας αισθητήρες, κάμερες και ρομποτικά συστήματα για να πραγματοποιήσουν την επέμβαση.

Αναλυτικά ένα παράδειγμα είναι η ρομποτική απομακρυσμένη επέμβαση σε καρδιακό επείγον περιστατικό. Σε αυτήν τη διαδικασία, ο χειρουργός βρίσκεται σε ένα απομακρυσμένο σημείο και χρησιμοποιεί ένα ρομποτικό σύστημα για να διενεργήσει την επέμβαση. Η διαδικασία λειτουργεί ως εξής: [5]

- **Συλλογή πληροφοριών:** Αρχικά, ο πάσχων που βρίσκεται σε έκτακτη καρδιακή ανάγκη μεταφέρεται σε ένα νοσοκομείο όπου υπάρχει η δυνατότητα εκτέλεσης ρομποτικής απομακρυσμένης επέμβασης. Εκεί, συλλέγονται πληροφορίες για την κατάσταση του πάσχοντος, κρίνεται το πως αντιμετωπίζεται αυτήν την στιγμή η κατάσταση και οι ειδικότητες που απαιτούνται.
- **Σύνδεση με τον εξειδικευμένο χειρουργό:** Ο ειδικός χειρουργός που θα εκτελέσει την επέμβαση συνδέεται με την ομάδα που βρίσκεται στο νοσοκομείο μέσω δικτύου υψηλής ταχύτητας και εξετάζει τις πληροφορίες του πάσχοντος.
- **Αξιολόγηση και προετοιμασία:** Ο χειρουργός αξιολογεί την κατάσταση του ασθενούς μέσω εικονικών συστημάτων και εξετάζει την εφαρμογή της ρομποτικής απομακρυσμένης επέμβασης στη συγκεκριμένη περίπτωση. Εξετάζει τις ακτινογραφίες, τα ηλεκτροκαρδιογραφήματα και άλλες διαθέσιμες πληροφορίες για την καρδιακή πάθηση.
- **Εκτέλεση της επέμβασης:** Με βάση τις πληροφορίες που συλλέχθηκαν και την αξιολόγηση του χειρουργού, ξεκινά η εκτέλεση της ρομποτικής

απομακρυσμένης επέμβασης. Ο χειρουργός χειρίζεται τα χειρουργικά εργαλεία μέσω ειδικών χειριστηρίων και διεπαφών, ενώ ο ρομποτικός βραχίονας εκτελεί τις ακριβείς κινήσεις στον ασθενή. Η διαδικασία μπορεί να περιλαμβάνει επισκευή βαλβίδων, τοποθέτηση στεφανιαίων ενθεμάτων ή άλλων καρδιακών επεμβάσεων.

- **Παρακολούθηση και αξιολόγηση:** Κατά τη διάρκεια της επέμβασης, η ομάδα του νοσοκομείου παρακολουθεί συνεχώς την πρόοδο και την κατάσταση του ασθενούς. Ο χειρουργός λαμβάνει αποφάσεις και πραγματοποιεί απαιτούμενες ρυθμίσεις κατά τη διάρκεια της επέμβασης για να διασφαλίσει την επιτυχή ολοκλήρωσή της. Κατά τη διάρκεια της επέμβασης, ο χειρουργός λαμβάνει πληροφορίες από τους βιοαισθητήρες που βρίσκονται στον ασθενή, όπως τον καρδιακό ρυθμό, την αρτηριακή πίεση και άλλες παραμέτρους, για να παρακολουθεί την αντίδραση του ασθενούς στην επέμβαση.

Η διαδικασία αυτή συνεχίζεται μέχρι την ολοκλήρωση της επέμβασης. Μετά την ολοκλήρωση, ο ασθενής παρακολουθείται για μια περίοδο ανάρρωσης, κατά την οποία ο χειρουργός και οι ιατροί παρακολουθούν την πρόοδο του και λαμβάνουν αποφάσεις για την περαιτέρω φροντίδα.

Συνολικά, η τηλεχειρουργική είναι μια πολύπλοκη διαδικασία που βασίζεται σε προηγμένες αναδυόμενες τεχνολογίες, όπως η ρομποτική, η ασύρματη επικοινωνία, η εικονική πραγματικότητα και η τεχνητή νοημοσύνη. Η χρήση αυτών των τεχνολογιών μπορεί να βελτιώσει την ασφάλεια, την ακρίβεια και την αποτελεσματικότητα των εγχειρήσεων, και να επιτρέψει στους γιατρούς να πραγματοποιούν επεμβάσεις από απόσταση.

Στις μέρες μας έχουν πραγματοποιηθεί πολλές επιτυχημένες τηλεχειρουργικές επεμβάσεις στην πραγματικότητα. Από το 2001, όταν πραγματοποιήθηκε η πρώτη επιτυχημένη απομακρυσμένη χειρουργική επέμβαση στη Γαλλία, οι τεχνολογικές εξελίξεις στην τηλεχειρουργική έχουν σημειώσει σημαντική πρόοδο. Σήμερα, οι επεμβάσεις τηλεχειρουργικής περιλαμβάνουν διάφορες επεμβάσεις σε όλο το φάσμα της χειρουργικής, όπως ανοικτή χειρουργική, λαπαροσκοπική χειρουργική, ρομποτική χειρουργική και μικροεπεμβατική χειρουργική. Οι επεμβάσεις αυτές επιτρέπουν στους χειρουργούς να εκτελούν πολύπλοκες επεμβάσεις από απομακρυσμένες τοποθεσίες, με μεγάλη ακρίβεια και ελάχιστο τραυματισμό για τον ασθενή.

Παρακάτω αναφέρονται περισσότερες λεπτομέρειες για το πως λειτουργεί μια απομακρυσμένη επέμβαση.

Η επικοινωνία μεταξύ του χειρουργού και του ρομπότ γίνεται μέσω ενός ειδικού συστήματος που ονομάζεται "τηλεχειρουργικό σύστημα". Αυτό το σύστημα περιλαμβάνει δύο βασικά στοιχεία: το ρομποτικό σύστημα και τον ελεγκτή.

Το ρομποτικό σύστημα αποτελείται από μια σειρά ρομπότ που τοποθετούνται κοντά στον ασθενή και ελέγχονται από έναν χειρουργό. Κάθε ρομπότ έχει εξοπλισμό που του επιτρέπει να εκτελεί διάφορες κινήσεις, όπως να κάνει τομές, να ράβει, να δένει και να διαστέλλει τα ιστούς. Τα ρομπότ είναι επίσης εξοπλισμένα με κάμερες, έτσι ώστε ο χειρουργός να μπορεί να βλέπει την περιοχή που εργάζεται.

Ο ελεγκτής είναι ένας ειδικός υπολογιστής που βρίσκεται στον χειρουργικό χώρο και είναι συνδεδεμένος με τα ρομπότ. Ο χειρουργός χρησιμοποιεί τον ελεγκτή για να καθοδηγήσει τα ρομπότ κατά τη διάρκεια της επέμβασης. Ο ελεγκτής είναι εξοπλισμένος με οθόνες, όπου ο χειρουργός μπορεί να βλέπει σε πραγματικό χρόνο τι συμβαίνει με τον ασθενή.

Η επικοινωνία ανάμεσα στον χειρουργό και το ρομπότ γίνεται μέσω ενός συστήματος επικοινωνίας που συνήθως βασίζεται στο διαδίκτυο. Αυτό σημαίνει ότι ο χειρουργός μπορεί να βρίσκεται σε έναν άλλο τόπο, ακόμη και σε άλλη χώρα, και να ελέγχει το ρομπότ απομακρυσμένα.

Ο χειρουργός φοράει ένα ειδικό γάντι με αισθητήρες και αναλαμβάνει τον έλεγχο των χειριστηρίων που κινούν τους βραχίονες του ρομπότ. Οι αισθητήρες στο γάντι μεταδίδουν τις κινήσεις του χειρουργού στο ρομπότ, το οποίο τις επεξεργάζεται και τις μεταφράζει σε αντίστοιχες κινήσεις των εργαλείων που χρησιμοποιούνται στην επέμβαση. Επιπλέον, το σύστημα επικοινωνίας επιτρέπει στο χειρουργό να βλέπει την επέμβαση σε πραγματικό χρόνο μέσω οθόνης, καθώς και να λαμβάνει πληροφορίες για την κατάσταση του ασθενούς, όπως την πίεση του αίματος και τη συχνότητα των παλμών.

Στη συνέχεια, ο χειρουργός συνδέεται με το ρομπότ μέσω ενός ενσύρματου ή ασύρματου δικτύου. Η σύνδεση μπορεί να είναι επικοινωνία μεταξύ υπολογιστών ή δίκτυο ταχείας μεταφοράς δεδομένων (5G). Η τηλεχειρουργική συσκευή έχει συνήθως ενσωματωμένο βίντεο στην οθόνη, καθώς και ψηφιακή εικόνα υψηλής ευκρίνειας για να βοηθήσει τον χειρουργό να δει καθαρά την περιοχή που εργάζεται.

Όταν ο χειρουργός στέλνει εντολές στο ρομπότ για τηλεχειρουργική επέμβαση, στέλνονται δεδομένα σχετικά με τη θέση και την κίνηση του χειρουργικού εργαλείου που χρησιμοποιείται από το ρομπότ. Αυτά τα δεδομένα περιλαμβάνουν συνήθως τη θέση του χειρουργικού εργαλείου στον χώρο, τη γωνία και την κατεύθυνση της κίνησης του εργαλείου, καθώς και άλλες παραμέτρους, όπως η πίεση και η ταχύτητα κίνησης του εργαλείου. Επίσης, στέλνονται και δεδομένα σχετικά με την κατάσταση του ασθενή, όπως η καρδιακή του λειτουργία και τα επίπεδα οξυγόνου στο κύτταρα του αίματο. Αυτά τα δεδομένα συλλέγονται από αισθητήρες που είναι τοποθετημένοι στον ασθενή κατά τη διάρκεια της επέμβασης και στέλνονται στον χειρουργό μέσω του συστήματος.

Με αυτόν τον τρόπο, ο χειρουργός μπορεί να ελέγχει τις κινήσεις του ρομπότ και να εκτελεί χειρουργικές επεμβάσεις από απόσταση. Συνήθως, η εικόνα που βλέπει ο χειρουργός είναι πολύ καθαρή και λεπτομερής (υψηλής ευκρίνειας), επιτρέποντάς του να εκτελεί ακριβείς κινήσεις. Το σύστημα επίσης επιτρέπει στους χειρουργούς να χρησιμοποιούν άλλα εργαλεία και τεχνικές, όπως την αναισθησία, προκειμένου να ελαχιστοποιήσουν τον πόνο των ασθενών κατά τη διάρκεια της επέμβασης.

Πέρα από το ρομπότ και τον χειρούργο για να λειτουργήσει μια εφαρμογή IoT στον τομέα της υγείας, απαιτείται και η συλλογή δεδομένων από διάφορες πηγές, όπως αισθητήρες, φορητές συσκευές υγείας, αλλά και δεδομενα κλινικές ή ασθενοφόρα. Αυτά τα δεδομένα μπορούν να αποθηκευτούν σε μια βάση δεδομένων που μπορεί να είναι τοπική ή κατανεμημένη.

Η τοπική αποθήκευση δεδομένων μπορεί να γίνει στη συσκευή που συλλέγει τα δεδομένα, ενώ η συγκεντρωτική αποθήκευση μπορεί να γίνει σε έναν κεντρικό

διακομιστή. Η κατανεμημένη αποθήκευση δεδομένων επιτρέπει την εξόρυξη δεδομένων και την ανάλυση τους για τη βελτίωση των ιατρικών πρακτικών και τη βελτίωση της ποιότητας της περίθαλψης. Επίσης, η κατανεμημένη αποθήκευση μπορεί να διευκολύνει τον διαμοιρασμό δεδομένων μεταξύ των ιατρικών εγκαταστάσεων και ειδικών για τη διαβίβαση πληροφοριών που μπορούν να βοηθήσουν στη διάγνωση και τη θεραπεία.

Συνήθως υπάρχει μια βάση δεδομένων που συλλέγει και αποθηκεύει τα δεδομένα που συλλέγονται από το IoT συστήματα υγείας. Αυτή η βάση δεδομένων μπορεί να είναι κεντρική ή κατανεμημένη, ανάλογα με το πόσα συστήματα συλλέγουν δεδομένα και πόσο μεγάλο είναι το όγκος των δεδομένων που πρέπει να αποθηκευτούν.

Η βάση δεδομένων μπορεί να περιέχει πληροφορίες όπως το ιατρικό ιστορικό του ασθενούς, τα αποτελέσματα εξετάσεων, τις συνταγές φαρμάκων, τα συμπτώματα και άλλες σημαντικές πληροφορίες σχετικά με την υγεία του ασθενούς. Οι ιατρικοί επαγγελματίες μπορούν να αποκτήσουν πρόσβαση σε αυτές τις πληροφορίες μέσω ειδικών εφαρμογών που συνδέονται με τη βάση δεδομένων. Είναι σημαντικό να τονιστεί ότι η συλλογή και αποθήκευση δεδομένων υγείας επιβάλλει αυστηρούς κανόνες προστασίας δεδομένων για τη διατήρηση της απόρρητης φύσης των πληροφοριών των ασθενών.

5.2 Οφέλη

Στην παραπάνω υποενότητα αναφέραμε παραδείγματα και αναλύσαμε το πως λειτουργεί η τηλεχειρουργική. Σε αυτήν την υποενότητα αναφέρουμε μερικά από τα οφέλη που μας παρέχει η τηλεχειρουργική. Αρχικά η τηλεχειρουργική επιτρέπει στους χειρουργούς να πραγματοποιούν επεμβάσεις με ακρίβεια και ασφάλεια από απόσταση, χρησιμοποιώντας λιγότερη ενέργεια και εξοικονομώντας χρόνο και κόστος.

Επιπλέον, μπορεί να βοηθήσει στην αντιμετώπιση κάποιων προβλημάτων που σχετίζονται με την πρόσβαση στην υγειονομική περίθαλψη. Για παράδειγμα, η τηλεχειρουργική μπορεί να βοηθήσει στην επίλυση του προβλήματος της παροχής υπηρεσιών υγείας σε απομακρυσμένες περιοχές, όπου δεν υπάρχουν εξειδικευμένοι χειρουργοί.

Ακόμα, μπορεί να μειώσει τον κίνδυνο λανθασμένων επεμβάσεων και να βελτιώσει την ποιότητα των επεμβάσεων. Η απόσταση ανάμεσα στο χειρουργό και τον ασθενή μπορεί να μειώσει την πιθανότητα μετάδοσης μολυσματικών νοσημάτων και άλλων επιπλοκών.

Επίσης, η τηλεχειρουργική μπορεί να επιτρέπει σε ασθενείς να λαμβάνουν πρόσβαση σε εξειδικευμένη περίθαλψη από μακριά. Για παράδειγμα, ένας ασθενής σε μια απομακρυσμένη περιοχή μπορεί να συμβουλευτεί έναν εξειδικευμένο χειρουργό μέσω της τηλεϊατρικής και να λάβει την κατάλληλη αγωγή.

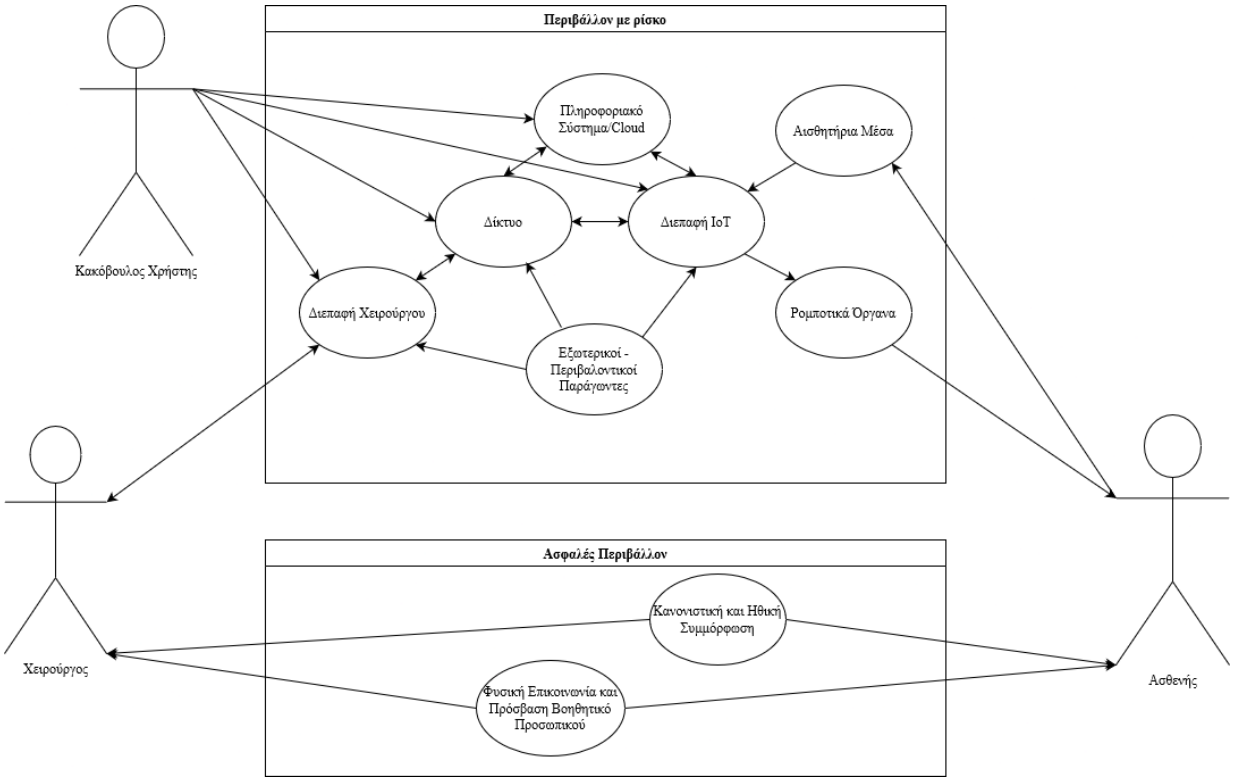
Η τηλεϊατρική και η τηλεχειρουργική επιτρέπουν επίσης την ανάπτυξη πιο προηγμένων χειρουργικών επεμβάσεων. Ένα παράδειγμα είναι η ρομποτική χειρουργική, που συνδυάζει τη χρήση ρομποτικών συστημάτων με τηλεχειρουργική τεχνολογία για να δώσει στον χειρουργό μεγαλύτερη ακρίβεια και ευελιξία στην εκτέλεση επεμβάσεων. Η ρομποτική χειρουργική μπορεί να μειώσει τον κίνδυνο επιπλοκών και να επιτρέψει στους χειρουργούς να εκτελούν επεμβάσεις που παραδοσιακά θεωρούνταν δύσκολες ή ακόμη και αδύνατες.

Όμως το βασικό όφελος για άλλη μια φορά είναι ότι η τηλεϊατρική και η τηλεχειρουργική μπορούν να βελτιώσουν την πρόσβαση σε ιατρική περίθαλψη σε απομακρυσμένες ή απομακρυσμένες περιοχές. Σε περιοχές όπου οι γιατροί και οι εξειδικευμένοι χειρουργοί είναι λίγοι ή δεν υπάρχουν καθόλου, η τηλεϊατρική και η τηλεχειρουργική μπορούν να επιτρέψουν στους ασθενείς να λάβουν προσαρμοσμένη υψηλής ποιότητας ιατρική περίθαλψη από μακριά.

5.3 Κίνδυνοι και επιθέσεις

Η τηλεχειρουργική επέμβαση είναι μια πολύπλοκη διαδικασία και μπορεί να αντιμετωπίσει πολλούς κινδύνους και προκλήσεις. Στην ανάλυση κινδύνου υπάρχουν δύο ομάδες ή περιβάλλοντα από οντότητες:

- **Ασφαλές περιβάλλον:** Ένα ασφαλές περιβάλλον αναφέρεται σε ένα σύστημα, δίκτυο ή περιβάλλον εργασίας όπου οι απειλές και οι ευπάθειες είτε είναι ανύπαρκτες είτε τις θεωρούμε εκτός αντικειμένου της ανάλυσης μας.
- **Περιβάλλον με ρίσκο:** Ένα περιβάλλον με ρίσκο αναφέρεται σε μια κατάσταση όπου υπάρχουν πιθανότητες επίθεσης, απώλειας δεδομένων ή παραβίασης της ασφάλειας. Αυτό μπορεί να συμβαίνει λόγω αδυναμιών στην ασφάλεια του συστήματος, ελλιπούς εκπαίδευσης των χρηστών, ή ανεπαρκών μέτρων ασφαλείας.



Εικόνα 9: Διάγραμμα περίπτωσης χρήσης

Ως ασφαλής έχει οριστεί η οντότητα «Κανονιστική και Ηθική Συμμόρφωση» η οποία περιλαμβάνει ότι ο χειρουργός και το βοηθητικό προσωπικό (π.χ. νοσοκόμες/-οι) δεν θα ενεργήσουν με δόλο προς τον ασθενή, ούτε θέλουν να παραβιάσουν τους κανονισμούς ή να προκαλέσουν με οποιονδήποτε τρόπο βλάβη στην υγεία του. Επίσης ως ασφαλής έχει οριστεί και η οντότητα « Φυσική Επικοινωνία και Πρόσβαση Βοηθητικό Προσωπικού» η οποία περιλαμβάνει την ασφαλή επικοινωνία του

χειρουργού με το προσωπικό και αποκλείει την περίπτωση κάποιος άλλος να μπορεί να πάρει την θέση του χειρουργού ή κάποιου νοσοκόμου ή να κλέψει/ αποσπάσει πληροφορίες από το προσωπικό. Οι οντότητες αυτές ορίστηκαν ως ασφαλές διότι οι κίνδυνοι αυτοί μπορεί να υπάρξουν και σε ένα κανονικό χειρουργείο και στην συγκεκριμένη περίπτωση θέλουμε να εστιάσουμε στους κινδύνους που μπορεί να προέλθουν απο την απομακρυσμένη σύνδεση και την χρήση του IoT.

Ως περιβάλλον με ρίσκο έχει οριστεί η οντότητα «Διεπαφή Χειρουργού», «Δίκτυο», «Διεπαφή IoT», «Αισθητήρια Μέσα», «Ρομποτικά Όργανα», «Πληροφοριακό Σύστημα/ Database» και «Εξωτερικοί Περιβαλλοντικοί Παράγοντες». Οι κίνδυνοι που υπάρχουν στις οντότητες αυτές θα παρουσιαστούναναλυτικά στην συνέχεια, καθώς θα παρουσιαστεί και η σχέση και οι κίνδυνοι μεταξύ της μιας οντότητας με την άλλην.

5.4 Ορισμός ρίσκων

Ορισμένοι από τους κινδύνους που ενδέχεται να υπάρχουν είναι οι εξής: [11]

- **Φυσικά φαινόμενα:** Η τηλεχειρουργική, ως μια τεχνολογικά προηγμένη ιατρική πρακτική, μπορεί να επηρεαστεί από σπάνιες αλλά πιθανές απειλές όπως οι πυρκαγιές, οι πλημμύρες ή οι σεισμοί. Ο εξειδικευμένος εξοπλισμός, όπως τα ρομποτικά συστήματα χειρουργικής, οι εξ αποστάσεως ελεγχόμενες συσκευές και οι υπολογιστές που απαιτούνται για την τηλεχειρουργική, είναι ευάλωτοι σε αυτού του είδους τα φαινόμενα. Συνήθως, αυτός ο εξοπλισμός είναι τοποθετημένος στο ισόγειο ή στο υπόγειο των νοσοκομείων -είτε λόγω κανονιστικών απαιτήσεων είτε λόγω βάρους και διαστάσεων- και επομένως διατρέχουν μεγαλύτερο κίνδυνο ζημιών από φυσικά φαινόμενα. Οι βλάβες μπορεί να προκληθούν από περιστατικά όπως πλημμύρες από σπασμένους σωλήνες ή από μεγαλύτερες καταστροφές όπως σεισμοί και πυρκαγιές, και ενδέχεται να επηρεάσουν όχι μόνο τον εξοπλισμό τηλεχειρουργικής αλλά και τη συνολική λειτουργία του νοσοκομείου και την αλυσίδα εφοδιασμού του. Επίσης, οι φυσικές δυνάμεις μπορεί να καταστρέψουν τις υποδομές του δικτύου και των συστημάτων υπολογιστικού νέφους που είναι κρίσιμα για την τηλεχειρουργική. Παρά το γεγονός ότι η πιθανότητα τέτοιων απειλών είναι χαμηλή, ο αντίκτυπός τους μπορεί να είναι τεράστιος.
- **Αποτυχία Αλυσίδας Παραγωγής:**
    - **Αποτυχία Παρόχου Υπηρεσιών Cloud (CSP):** Στην τηλεχειρουργική, οι διαδικασίες όπως η διαχείριση των αρχείων ασθενών, ο έλεγχος των συσκευών τηλεχειρουργικής και η αποθήκευση των δεδομένων των επεμβάσεων μπορεί να ανατίθενται σε παρόχους υπηρεσιών cloud. Αυτό σημαίνει ότι ένα σημαντικό μέρος της λειτουργικότητας της τηλεχειρουργικής εξαρτάται από υπηρεσίες cloud τρίτων. Σε περιφερειακά ή μικρότερα νοσοκομεία, ολόκληρο το σύστημα τηλεχειρουργικής και η αποθήκευση των δεδομένων ενδέχεται να φιλοξενούνται εξ ολοκλήρου σε υποδομές cloud. Η διαθεσιμότητα των υπηρεσιών cloud εξαρτάται σε μεγάλο βαθμό από τον πάροχο. Για παράδειγμα, η πτώχευση ή η αποτυχία του παρόχου μπορεί να απειλήσει τη συνεχή διαθεσιμότητα των υπηρεσιών cloud, προκαλώντας λειτουργικές διακοπές και πιθανή απώλεια δεδομένων, τα οποία είναι κρίσιμα για την τηλεχειρουργική. Για να αντιμετωπιστούν αυτές οι απειλές, οι οργανισμοί υγειονομικής περίθαλψης πρέπει να εξετάζουν και να διερευνούν θέματα πλεονασμού και ανθεκτικότητας των υπηρεσιών τους.
    - **Αποτυχία Παρόχου Δικτύου:** Η αποτυχία δικτύου στην τηλεχειρουργική μπορεί να έχει καταστροφικές συνέπειες. Η σύνδεση στο δίκτυο είναι ζωτικής σημασίας για την πραγματοποίηση απομακρυσμένων επεμβάσεων, καθώς επιτρέπει την αδιάλειπτη επικοινωνία μεταξύ του χειρουργού και του ρομποτικού εξοπλισμού. Επιπλέον, η σύνδεση στο δίκτυο είναι απαραίτητη για την πρόσβαση στις υπηρεσίες υγειονομικής περίθαλψης που βασίζονται στο cloud, οι οποίες είναι κρίσιμες για την

αποθήκευση και διαχείριση των δεδομένων τηλεχειρουργικής. Μια αποτυχία δικτύου μπορεί να επηρεάσει την παροχή αυτών των υπηρεσιών και να διακόψει τη συνεργασία μεταξύ διαφορετικών εσωτερικών και εξωτερικών εταίρων, με αποτέλεσμα τη διακοπή της ροής πληροφοριών και της υποστήριξης που απαιτείται για την επιτυχή διεξαγωγή τηλεχειρουργικών επεμβάσεων.

- **Διακοπή Παροχής Ρεύματος:** Η απώλεια ηλεκτρικής ενέργειας στην τηλεχειρουργική μπορεί να έχει σοβαρές συνέπειες, ανάλογα με τον εξοπλισμό που επηρεάζεται. Οι μονάδες εντατικής θεραπείας, οι χειρουργικές αίθουσες και οι διακομιστές συνήθως προστατεύονται από πηγές αδιάλειπτης τροφοδοσίας (UPS) ή μπαταρίες. Ωστόσο, η διακοπή ρεύματος μπορεί να θέσει σε κίνδυνο άλλον εξοπλισμό τηλεχειρουργικής, όπως τα ρομποτικά συστήματα και τις συσκευές απεικόνισης. Επιπλέον, η παροχή ρεύματος είναι κρίσιμη για τη διαθεσιμότητα των υπηρεσιών cloud, που χρησιμοποιούνται για την αποθήκευση και διαχείριση των δεδομένων τηλεχειρουργικών επεμβάσεων. Η διακοπή ρεύματος μπορεί να επηρεάσει την πρόσβαση στα δεδομένα αυτά, επηρεάζοντας τη συνεχή παρακολούθηση και λειτουργία των συστημάτων, θέτοντας σε κίνδυνο τη δυνατότητα απομακρυσμένης επέμβασης.
- **Αποτυχία Υλικού (H/W):** Η αποτυχία υλικού στην τηλεχειρουργική μπορεί να περιορίσει τη διαθεσιμότητα των υπηρεσιών, γεγονός που μπορεί να επηρεάσει σοβαρά την υγεία των ασθενών, ιδιαίτερα σε περιπτώσεις έκτακτης ανάγκης. Μια αποτυχία ιατρικής συσκευής, όπως ενός ρομποτικού συστήματος χειρουργικής ή ενός συστήματος απεικόνισης, μπορεί να επηρεάσει τη διαθεσιμότητα δεδομένων ή του συστήματος συνολιά σε πραγματικό χρόνο, γεγονός που ενδέχεται να βλάψει την υγεία του ασθενούς. Η αξιοπιστία του εξοπλισμού είναι ζωτικής σημασίας για τη διασφάλιση ότι οι χειρουργικές επεμβάσεις μπορούν να πραγματοποιούνται χωρίς διακοπές και ότι οι γιατροί έχουν συνεχή πρόσβαση στα απαραίτητα δεδομένα κατά τη διάρκεια της επέμβασης.

- **Ανθρώπινο σφάλμα:**
  - **Μη εξουσιοδοτημένη Πρόσβαση σε Δεδομένα:** Στην τηλεχειρουργική, οι χρήστες του cloud ενδέχεται να αποκτήσουν μη εξουσιοδοτημένη πρόσβαση σε δεδομένα λόγω ανεπαρκούς διαχείρισης της πρόσβασης ή έλλειψης ευαισθητοποίησης, γεγονός που μπορεί να προκαλέσει ακούσια αποκάλυψη ευαίσθητων δεδομένων. Για παράδειγμα, τα δεδομένα των επεμβάσεων που αποθηκεύονται στο cloud μπορεί να είναι προσβάσιμα από περισσότερους χρήστες σε σχέση με μια παραδοσιακή λύση αποθήκευσης, αυξάνοντας τον κίνδυνο παραβίασης της ιδιωτικότητας των ασθενών. Η αυστηρή διαχείριση της πρόσβασης και η ευαισθητοποίηση των χρηστών είναι κρίσιμες για την προστασία των δεδομένων στην τηλεχειρουργική.
  - **Σφάλματα από Διαχειριστές Υπηρεσιών Cloud/Προσωπικό Υποστήριξης:** Στην τηλεχειρουργική, σφάλματα από διαχειριστές υπηρεσιών cloud ή προσωπικό υποστήριξης μπορεί να έχουν σοβαρές επιπτώσεις. Εάν τα δεδομένα τηλεχειρουργικών επεμβάσεων δεν διαγραφούν κατάλληλα από το cloud αποθήκευσης ή από τα μέσα

δημιουργίας αντιγράφων ασφαλείας, αυτά τα δεδομένα μπορεί να είναι προσβάσιμα από άλλους πελάτες του ίδιου cloud παρόχου, οδηγώντας σε παραβίαση δεδομένων. Επιπλέον, τα σφάλματα διαμόρφωσης από το προσωπικό υποστήριξης υπηρεσιών cloud μπορεί να αφήνουν τρωτά σημεία χωρίς επιδιόρθωση, δημιουργώντας ανοιχτά σημεία εισόδου για κακόβουλους επιτιθέμενους. Τέτοια σφάλματα μπορεί να εκθέσουν ευαίσθητα δεδομένα ασθενών και να επηρεάσουν την ασφάλεια και την αποτελεσματικότητα των τηλεχειρουργικών επεμβάσεων.

- **Επιθέσεις εισβολής κακόβουλου λογισμικού (π.χ. virus, ransomware, worms):** Στην τηλεχειρουργική, τα συστήματα πληροφορικής είναι στενά διασυνδεδεμένα και δύσκολα απομονώνονται χωρίς να δημιουργηθεί διακοπή των υπηρεσιών, δημιουργώντας ένα εύφορο έδαφος για επιθέσεις με κακόβουλο λογισμικό. Οργανισμοί με μεγάλο αριθμό συσκευών ενδέχεται να δυσκολεύονται να ενημερώνουν τις άδειες και τα λογισμικά τους λόγω του αυξημένου κόστους και του χρόνου που απαιτείται για τη συντήρηση. Το adware είναι ένας από τους ευκολότερους τρόπους διανομής κακόβουλου λογισμικού και συχνά αγνοείται από τους χρήστες. Το ransomware, όπως αυτό της περίπτωσης Wannacry, είναι ίσως η πιο γνωστή απειλή για τους οργανισμούς υγειονομικής περίθαλψης. Το ransomware πραγματοποιεί συνήθως αδιάκριτες επιθέσεις χαμηλού κόστους. Η υποδομή της υγειονομικής περίθαλψης είναι ευάλωτη για δύο κύριους λόγους: (i) η υποδομή λογισμικού είναι δύσκολο να διατηρηθεί ενημερωμένη, επειδή είναι δύσκολο να βρεθεί κατάλληλη χρονοθυρίδα για διακοπή λειτουργίας, (ii) πολλά μηχανήματα εκτελούν παλαιό λογισμικό που λειτουργεί μόνο με συγκεκριμένες εκδόσεις λειτουργικών συστημάτων ή οδηγών, καθιστώντας τα εύκολους στόχους. Αυτές οι παλαιές συσκευές λειτουργούν ως δεξαμενές για το κακόβουλο λογισμικό, βοηθώντας το να εξαπλωθεί μέσω του δικτύου. Τα περιβάλλοντα cloud είναι επίσης ευάλωτα σε επιθέσεις έγχυσης κακόβουλου λογισμικού, οι οποίες αποτελούν υποκατηγορία των επιθέσεων που βασίζονται στον ιστό. Οι επιτιθέμενοι εκμεταλλεύονται τα τρωτά σημεία μιας διαδικτυακής εφαρμογής ή αδύναμα passwords και ενσωματώνουν κακόβουλο κώδικα στην κανονική πορεία δράσης. Όλα τα μοντέλα υπηρεσιών cloud είναι εξίσου ευάλωτα σε αυτού του είδους τις κακόβουλες ενέργειες. Μόλις εκτελεστεί ο κακόβουλος κώδικας, ο επιτιθέμενος μπορεί να κρυφακούσει, να χειριστεί ή να κλέψει δεδομένα και να υποκινήσει περαιτέρω επιθέσεις.

- **Κακόβουλες Επιθέσεις:**
  - **Επιθέσεις Κοινωνικής Μηχανικής (Phishing, Baiting, Κλωνοποίηση Συσκευών):** Στον τομέα της τηλεχειρουργικής, οι επιθέσεις κοινωνικής μηχανικής, όπως phishing, baiting και κλωνοποίηση συσκευών, είναι συχνές και αποτελούν σημαντικό κίνδυνο. Τα μολυσμένα email (phishing, spam και spear-phishing) είναι ο κυρίαρχος φορέας επίθεσης για την εισαγωγή κακόβουλου λογισμικού. Σύμφωνα με την έκθεση DBIR της Verizon, το 92,4% των περιστατικών κακόβουλου λογισμικού προήλθαν από παραβιάσεις ηλεκτρονικού ταχυδρομείου. Οι οργανισμοί

υγειονομικής περίθαλψης συχνά επιτρέπουν την πρόσβαση σε επαγγελματικούς και προσωπικούς λογαριασμούς email από τους ίδιους υπολογιστές, αυξάνοντας τον κίνδυνο. Οι διευθύνσεις email των κλινικών ιατρών είναι εύκολα προσβάσιμες μέσω δημόσιων καταλόγων ή παρουσιάσεων στο διαδίκτυο. Η χρήση επαγγελματικών λογαριασμών email για προσωπικά θέματα (και το αντίστροφο) θεωρείται κακή πρακτική. Η κλωνοποίηση συσκευών, όπως οι κάρτες ταυτότητας, απαιτεί υψηλό επίπεδο εξειδίκευσης και φυσική προσέγγιση του θύματος, αλλά η εφαρμογή της ταυτοποίησης δύο παραγόντων (2FA) έχει μειώσει σημαντικά τον κίνδυνο αυτού του είδους επίθεσης. Στα περιβάλλοντα cloud, οι επιθέσεις κοινωνικής μηχανικής στοχεύουν συχνά στην κλοπή διαπιστευτηρίων χρηστών για λύσεις SaaS μέσω phishing, spam ή spear-phishing emails. Αυτές οι επιθέσεις επικεντρώνονται στον πιο αδύναμο κρίκο της αλυσίδας ασφαλείας, τον ανθρώπινο παράγοντα. Ο τομέας της υγειονομικής περίθαλψης συχνά παρουσιάζει λιγότερη εξοικείωση με την πληροφορική, αυξάνοντας την ευπάθεια σε τέτοιες επιθέσεις. Ο ισχυρός έλεγχος ταυτότητας που παρέχεται από τον πάροχο υπηρεσιών cloud είναι κρίσιμος για την πρόληψη αυτών των επιθέσεων, ενώ οι επιτυχείς επιθέσεις μπορούν να οδηγήσουν σε παραβιάσεις δεδομένων, διαρροές ή κλοπή πληροφοριών.

- **Παραποίηση Ιατρικών Συσκευών:** Η έλλειψη ασφαλούς επικοινωνίας μεταξύ ιατρικών συσκευών και διακομιστών μπορεί να οδηγήσει σε παραποίηση των δεδομένων. Επιθέσεις τύπου "Man-in-the-Middle" (MITM) μπορούν να τροποποιήσουν τις πληροφορίες που προέρχονται από ζωτικά σημεία, εργαστηριακές ή παθολογικές αναφορές, καθώς και εικόνες DICOM από αξονικές τομογραφίες, μαγνητικές τομογραφίες ή υπερήχους. Αυτό το είδος επίθεσης μπορεί να επηρεάσει τη διαδρομή των δεδομένων προς τον διακομιστή PACS (Picture Archiving and Communication System), θέτοντας σε κίνδυνο την ακριβή διάγνωση και θεραπεία των ασθενών.
- **Μη Ασφαλείς Διεπαφές και API:** Στην τηλεχειρουργική, οι διεπαφές χρήστη και τα API (Application Programming Interfaces) είναι κρίσιμα για την αλληλεπίδραση μεταξύ χειρουργικών ρομπότ, συστημάτων παρακολούθησης και υπηρεσιών cloud. Αυτές οι διεπαφές επιτρέπουν τη διαχείριση και τον έλεγχο των συσκευών από απομακρυσμένα σημεία, αλλά εάν δεν είναι σωστά σχεδιασμένες ή δεν διαθέτουν επαρκή μέτρα ασφαλείας, μπορούν να αποτελέσουν στόχο για κακόβουλους επιτιθέμενους. Η έλλειψη κρυπτογράφησης και ελέγχου πρόσβασης μπορεί να δώσει την ευκαιρία σε επιθέσεις που θα μπορούσαν να επηρεάσουν τη λειτουργία του χειρουργικού ρομπότ ή να διαρρεύσουν ευαίσθητα ιατρικά δεδομένα. Επίσης, παραβιασμένα ή σπασμένα API μπορούν να προκαλέσουν σοβαρές διαταραχές στην πραγματική χειρουργική διαδικασία, θέτοντας σε κίνδυνο την ασφάλεια του ασθενούς.
- **Άρνηση Παροχής Υπηρεσιών (DoS):** Στην τηλεχειρουργική, οι επιθέσεις άρνησης παροχής υπηρεσιών (DoS) μπορούν να επηρεάσουν σοβαρά τη λειτουργία των συστημάτων. Οι επιθέσεις DoS στοχεύουν στην

υπερφόρτωση των πόρων του δικτύου ή του cloud που υποστηρίζουν τις εφαρμογές τηλεχειρουργικής, πλημμυρίζοντας τα με αιτήματα από πολλές πηγές. Αυτό μπορεί να προκαλέσει την αδυναμία πρόσβασης στις υπηρεσίες ή την καθυστέρηση στην επεξεργασία κρίσιμων δεδομένων και εντολών, θέτοντας σε κίνδυνο τη λειτουργία των χειρουργικών ρομπότ και την ασφάλεια των ασθενών. Η ανικανότητα διαχείρισης αυτών των αιτημάτων μπορεί να οδηγήσει σε διακοπή της χειρουργικής διαδικασίας ή σε άλλες σοβαρές δυσλειτουργίες, υπογραμμίζοντας την ανάγκη για ισχυρές στρατηγικές προστασίας και διαχείρισης της κυκλοφορίας.

- **Υποκλοπή Δεδομένων κατά τη Μεταφορά (Man-in-the-Middle Attack):** Στην τηλεχειρουργική, όπου η επικοινωνία μεταξύ των χειρουργικών ρομπότ και των συστημάτων cloud είναι κρίσιμη, η υποκλοπή δεδομένων κατά τη μεταφορά αποτελεί σοβαρή απειλή. Κατά τη διαδικασία μετάδοσης δεδομένων από τις συσκευές του χειρουργικού ρομπότ προς τον πάροχο υπηρεσιών cloud, μια επίθεση τύπου Man-in-the-Middle μπορεί να υποκλέψει τα δεδομένα, θέτοντας σε κίνδυνο την ακεραιότητά τους. Αυτό μπορεί να έχει σοβαρές συνέπειες, όπως παραποίηση δεδομένων που σχετίζονται με τη χειρουργική διαδικασία ή διαρροές ευαίσθητων ιατρικών πληροφοριών, επηρεάζοντας την αποτελεσματικότητα και την ασφάλεια της επέμβασης. Ενισχυμένα μέτρα κρυπτογράφησης και ασφαλή πρωτόκολλα επικοινωνίας είναι απαραίτητα για την προστασία των δεδομένων κατά τη μεταφορά.
- **Τεχνικές Αστοχίες ή Επιθέσεις που Σχετίζονται με το Δίκτυο:** Στην τηλεχειρουργική, οι τεχνικές αστοχίες ή οι επιθέσεις που σχετίζονται με το δίκτυο μπορούν να έχουν σοβαρές επιπτώσεις στη λειτουργία των συστημάτων. Παράγοντες όπως η απώλεια συνδεσιμότητας στο Διαδίκτυο λόγω βλαβών είτε στο χώρο του πελάτη είτε στον πάροχο υπηρεσιών cloud, είτε στο χειρουργείο, προσωρινές μειώσεις του εύρους ζώνης δικτύου που επηρεάζουν τη μεταφορά δεδομένων, και διαταραχές στην παγκόσμια υποδομή δρομολόγησης του Διαδικτύου μπορούν να επηρεάσουν την ομαλή λειτουργία της τηλεχειρουργικής. Αυτές οι τεχνικές αστοχίες ή επιθέσεις ενδέχεται να προκαλέσουν καθυστερήσεις στη μετάδοση δεδομένων μεταξύ των χειρουργικών ρομπότ και των συστημάτων cloud, με αποτέλεσμα την επιβράδυνση της χειρουργικής διαδικασίας ή ακόμη και την αποτυχία της παρέμβασης, θέτοντας σε κίνδυνο την ασφάλεια του ασθενούς.

- **Αποτυχία Συστήματος:**
  - **Αποτυχία Λογισμικού:** Κάθε λογισμικό ενδέχεται να παρουσιάσει σφάλματα, και αυτό ισχύει ιδιαίτερα για τις κρίσιμες εφαρμογές στην τηλεχειρουργική. Συσκευές όπως ρομπότ χειρουργικής, συστήματα ελέγχου αναισθησίας, και άλλες ιατρικές συσκευές απαιτούν ιδιαίτερα αυστηρά μέτρα ασφαλείας λόγω των σοβαρών συνεπειών που μπορεί να έχουν σφάλματα στη λειτουργία τους. Σοβαρές βλάβες, όπως η υπερδοσολογία φαρμάκων ή η αποτυχία ακριβούς ελέγχου του χειρουργικού εξοπλισμού, μπορούν να προκαλέσουν σοβαρές σωματικές βλάβες. Οι διακομιστές που υποστηρίζουν τα συστήματα

τηλεχειρουργικής είναι επίσης ευάλωτοι σε σφάλματα, όχι μόνο λόγω της πιθανής αστοχίας του ειδικού λογισμικού τους, αλλά και λόγω εξαρτήσεων από άλλες πλατφόρμες, όπως λειτουργικά συστήματα και βάσεις δεδομένων, που μπορούν επίσης να αποτύχουν. Επιπλέον, τα σφάλματα συχνά εμφανίζονται μετά από ενημερώσεις λογισμικού και μπορεί να εκδηλωθούν ως λανθάνοντα σφάλματα που διακόπτουν τη λειτουργία ή μειώνουν την απόδοση των υπηρεσιών. Η ανάλυση αρχείων καταγραφής είναι κρίσιμη για την κατανόηση της αιτίας των σφαλμάτων, και η αποκατάσταση τους απαιτεί προσεκτική παρακολούθηση και επανεκκίνηση των διακομιστών. Ειδικά προετοιμασμένες δοκιμές είναι απαραίτητες για την εξασφάλιση της ομαλής λειτουργίας του συστήματος, αν και η εκτέλεση αυτών των δοκιμών μπορεί να είναι δύσκολη λόγω της συνεχιζόμενης λειτουργίας των συστημάτων (ιατρικές υπηρεσίες δεν μπορούν απλά να κλείσουν). Οι συχνές βλάβες των διακομιστών μπορούν να υποβαθμίσουν την ποιότητα της ιατρικής περίθαλψης και να μειώσουν την εμπιστοσύνη στο ίδρυμα. Η αποτυχία λογισμικού μπορεί να επηρεάσει σοβαρά τις υπηρεσίες cloud και την προσβασιμότητα δεδομένων ιατρικών συσκευών, θέτοντας σε κίνδυνο την ασφάλεια των ασθενών και την επιτυχία της χειρουργικής διαδικασίας.

- **Ξεπερασμένο Υλικό και Λογισμικό στην Τηλεχειρουργική:** Η έλλειψη τακτικών διαδικασιών για την ενημέρωση του υλικολογισμικού σε ιατρικές και τεχνολογικές συσκευές μπορεί να είναι κρίσιμη απειλή για τα συστήματα τηλεχειρουργικής. Η χρήση παλαιών εκδόσεων υλικολογισμικού σε συσκευές όπως ρομπότ χειρουργικής, συστήματα αναισθησίας και διακομιστές που υποστηρίζουν την τηλεχειρουργική μπορεί να δημιουργήσει ευάλωτα σημεία που μπορεί να εκμεταλλευτούν επιτιθέμενοι. Αυτές οι παλαιές τεχνολογίες ενδέχεται να στερούνται σύγχρονων μηχανισμών ασφαλείας και ενημερώσεων, αφήνοντας κερκόπορτες για κακόβουλους φορείς που επιθυμούν να αποκτήσουν πρόσβαση σε ευαίσθητα δεδομένα υγειονομικής περίθαλψης ή να επηρεάσουν την ομαλή λειτουργία των συστημάτων. Οι επιθέσεις μπορούν να οδηγήσουν σε σοβαρές διαταραχές της χειρουργικής διαδικασίας, όπως αδυναμία ακριβούς ελέγχου του χειρουργικού ρομπότ ή αποτυχία των συστημάτων παρακολούθησης της ασθενή. Η τακτική ανανέωση του υλικολογισμικού είναι απαραίτητη για την ελαχιστοποίηση των κινδύνων και τη διασφάλιση της ασφάλειας και της αποτελεσματικότητας των συστημάτων τηλεχειρουργικής.

Για την ανάλυση κινδύνων και την αξιολόγηση επιπτώσεων όσον αφορά την αξιοποίηση του IoT στην τηλεχειρουργική, είναι σημαντικό εκτός από το να εντοπιστούν, να κατηγοριοποιηθούν οι κίνδυνοι που αφορούν κάθε οντότητα αλλά και κάθε σχέση μεταξύ αυτών. Ακολουθεί η κατηγοριοποίηση των ρίσκων - κινδύνων τους οποίους ενέχει το σενάριο που εξετάζουμε:

5.4.1 Ρίσκα ανά Οντότητα

Χειρουργός:

- Η παραπάνω οντότητα έχει καθοριστεί ότι ανήκει στο ασφαλές περιβάλλον για την ανάλυση ρίσκων που πραγματοποιούμε στο πλαίσιο αυτού του παραδείγματος.

Ασθενής:

- Η παραπάνω οντότητα έχει καθοριστεί ότι ανήκει στο ασφαλές περιβάλλον για την ανάλυση ρίσκων που πραγματοποιούμε στο πλαίσιο αυτού του παραδείγματος.

Πληροφοριακό Σύστημα/Cloud:

- Ασφάλεια δεδομένων: Κίνδυνος υποκλοπής δεδομένων από το cloud.
- Ακεραιότητα δεδομένων: Κίνδυνος αλλοίωσης ή απώλειας δεδομένων.

Διεπαφή Χειρουργού:

- Μη φιλική διεπαφή: Πολύπλοκες ή δύσχρηστες διεπαφές μπορούν να προκαλέσουν σύγχυση ή λάθη κατά τη χρήση.
- Τεχνικά προβλήματα: Σφάλματα λογισμικού ή υλικού που μπορεί να προκαλέσουν καθυστερήσεις ή διακοπές στη χειρουργική διαδικασία.

Δίκτυο:

- Ασφάλεια δεδομένων: Κίνδυνος υποκλοπής ή παραβίασης ευαίσθητων δεδομένων.
- Καθυστερήσεις (latency): Μεγάλη καθυστέρηση στη μετάδοση δεδομένων μπορεί να επηρεάσει την ακρίβεια της τηλεχειρουργικής.
- Αδυναμία πρόσβασης: Προβλήματα πρόσβασης στο δίκτυο μπορεί να διακόψουν τη διαδικασία.

Διεπαφή IoT:

- Σφάλματα λογισμικού: Σφάλματα που μπορεί να επηρεάσουν την καταγραφή και μετάδοση δεδομένων από τους αισθητήρες.
- Ασφάλεια δεδομένων: Παραβίαση της διεπαφής IoT από κακόβουλους χρήστες.

Αισθητήρια Μέσα:

- Λανθασμένες ενδείξεις: Ακατάλληλο καλιμπράρισμα ή ελαττωματικά αισθητήρια μπορεί να παράγουν λανθασμένα δεδομένα.
- Αποτυχία λειτουργίας: Διακοπή λειτουργίας αισθητήρων μπορεί να σταματήσει την παροχή κρίσιμων δεδομένων.

Ρομποτικά Όργανα:

- Αναξιοπιστία: Αστοχία συστημάτων ή μηχανική βλάβη μπορεί να θέσει σε κίνδυνο τη διαδικασία.
- Ακρίβεια κίνησης: Οποιαδήποτε απόκλιση στην ακρίβεια των κινήσεων μπορεί να οδηγήσει σε σοβαρές επιπτώσεις για τον ασθενή.

Εξωτερικοί/Περιβαλλοντικοί Παράγοντες:

- Θερμοκρασία και υγρασία: Ακραίες τιμές μπορεί να επηρεάσουν τη λειτουργία του εξοπλισμού.
- Φυσικές καταστροφές: Πλημμύρες, φωτιές ή σεισμοί μπορεί να καταστρέψουν τον εξοπλισμό, προκαλώντας απώλεια δεδομένων ή διακοπή υπηρεσιών.

Κακόβουλος Χρήστης:

- Επιθέσεις από κακόβουλους actors: Παραβιάσεις ασφαλείας, υποκλοπές δεδομένων, επιθέσεις DDoS, κ.λπ.

5.4.2 Ρίσκα στη Σχέση Μεταξύ Οντοτήτων

Σχέση: Χειρουργού - Διεπαφή Χειρουργού:

- Κλώνος ιστοσελίδας χωρίς κρυπτογράφηση.
- Υπερβολική εξάρτηση μπορεί να μειώσει την ικανότητα του χειρουργού να αναλάβει δράση σε περίπτωση αποτυχίας συστήματος.

Σχέση: Διεπαφή Χειρουργού - Δίκτυο:

- Απώλεια σύνδεσης δικτύου (από οποιαδήποτε αιτία, π.χ.: διακοπή ρεύματος).
- Παραβίαση διεπαφής από μη εξουσιοδοτημένο χρήστη: Κίνδυνος υποκλοπής πληροφοριών λόγω μη ασφαλών συνδέσεων.
- Παραβίαση διεπαφής από μη εξουσιοδοτημένο χρήστη: Κίνδυνος τροποποίησης εντολών στο σύστημα.
- Ασυμβατότητες μπορεί να προκαλέσουν αποτυχία επικοινωνίας ή εσφαλμένη μετάδοση δεδομένων.

Σχέση: Δίκτυο - Διεπαφή IoT:

- Απώλεια σύνδεσης δικτύου.
- Σφάλμα λογισμικού με αποτέλεσμα αδυναμία αποστολής δεδομένων.

Σχέση: Ασθενής - Αισθητήρια Μέσα:

- Ακρίβεια μέτρησης: Ανακρίβειες στη μέτρηση των βιομετρικών δεδομένων μπορεί να οδηγήσουν σε λανθασμένες διαγνώσεις.

Σχέση: Αισθητήρια Μέσα - Διεπαφή IoT:

- Συμβατότητα πρωτοκόλλων: Ασυμβατότητες μεταξύ των πρωτοκόλλων επικοινωνίας των αισθητήρων και του IoT μπορεί να προκαλέσουν απώλεια ή αλλοίωση δεδομένων.

Σχέση: Διεπαφή IoT - Ρομποτικά Όργανα:

- Χρονοκαθυστερήσεις: Καθυστερήσεις στην επεξεργασία ή μεταφορά δεδομένων μπορεί να επηρεάσουν την απόκριση των ρομποτικών οργάνων.

Σχέση: Εξωτερικοί/Περιβαλλοντικοί Παράγοντες - Διεπαφή Χειρουργού:

- Διακοπή της παροχής ρεύματος ή καταστροφή του εξοπλισμού μπορεί να εμποδίσει τον χειρουργό από την παροχή εντολών.

Σχέση: Εξωτερικοί/Περιβαλλοντικοί Παράγοντες - Δίκτυο:

- Διακοπή επικοινωνίας: Περιβαλλοντικοί παράγοντες όπως φυσικές καταστροφές μπορεί να διακόψουν την επικοινωνία.

Σχέση: Εξωτερικοί/Περιβαλλοντικοί Παράγοντες - Διεπαφή IoT:

- Φωτιά με αποτέλεσμα την καταστροφή του τερματικού από το οποίο παρέχεται η πρόσβαση στη διεπαφή του IoT.
- Πλημμύρες, φωτιές ή σεισμοί μπορεί να καταστρέψουν τον εξοπλισμό, προκαλώντας απώλεια δεδομένων ή διακοπή υπηρεσιών.

Σχέση: Πληροφοριακό Σύστημα/Cloud - Διεπαφή IoT:

- Διαθεσιμότητα υπηρεσιών: Αδυναμία πρόσβασης σε δεδομένα ή υπηρεσίες σε περίπτωση διακοπής της υπηρεσίας cloud.
- Φυσικές καταστροφές: Πλημμύρες, φωτιές ή σεισμοί μπορεί να καταστρέψουν τον εξοπλισμό, προκαλώντας απώλεια δεδομένων ή διακοπή υπηρεσιών.

Σχέση: Πληροφοριακό Σύστημα/Cloud - Δίκτυο:

- Ακεραιότητα δεδομένων: Κίνδυνος απώλειας ή αλλοίωσης δεδομένων λόγω προβλημάτων/εισβολών στο δίκτυο ή το cloud.

Σχέση: Κακόβουλος Χρήστης - Πληροφοριακό Σύστημα/Cloud:

- Παραβίαση ασφαλείας και υποκλοπή δεδομένων.
- Επιθέσεις DDoS που διαταράσσουν τις υπηρεσίες cloud.

Σχέση: Κακόβουλος Χρήστης - Δίκτυο:

- Υποκλοπή δεδομένων κατά τη μετάδοση.
- Επιθέσεις DDoS που διακόπτουν την επικοινωνία.

Σχέση: Κακόβουλος Χρήστης - Διεπαφή IoT:

- Παραβίαση της διεπαφής IoT και αλλοίωση δεδομένων.
- Εισαγωγή κακόβουλου λογισμικού στους αισθητήρες.

Σχέση: Κακόβουλος Χρήστης - Διεπαφή Χειρουργού:

- Κλώνος ιστοσελίδας για υποκλοπή πληροφοριών.
- Τροποποίηση εντολών στο σύστημα.

5.5 Ανάλυση ρίσκων με βάση την μεθοδολογία OWASP

5.5.1 Κλώνος ιστοσελίδας χωρίς κρυπτογράφηση

Βήμα 1: Προσδιορισμός κινδύνου

Στην τηλεχειρουργική, η χρήση μη κρυπτογραφημένων ιστοσελίδων μπορεί να εκθέσει τις επικοινωνίες σε επιθέσεις τύπου "man-in-the-middle". Σε αυτό το σενάριο, ένας κακόβουλος χρήστης δημιουργεί έναν κλώνο της ιστοσελίδας διαχείρισης των ρομποτικών συστημάτων χωρίς κρυπτογράφηση και ανακατευθύνει τους χρήστες εκεί μέσω phishing emails, κακόβουλων συνδέσμων ή παραβίασης του DNS (Domain Name Server – που αντιστοιχεί ονόματα σε διευθύνσεις). Οι χρήστες εισάγουν τα διαπιστευτήριά τους και τις ενέργειές τους στην κλωνοποιημένη ιστοσελίδα, πιστεύοντας ότι είναι η αυθεντική. Αυτό έχει ως αποτέλεσμα την αποκάλυψη ευαίσθητων δεδομένων στον επιτιθέμενο και τη δυνατότητα διακοπής ή λανθασμένης εκτέλεσης των χειρουργικών διαδικασιών, με δυνητικά θανάσιμες συνέπειες για τους ασθενείς.

Βήμα 2: Παράγοντες για την εκτίμηση της πιθανότητας

Η πιθανότητα παραβίασης κατά τη διάρκεια του χειρουργείου μπορεί να συμβεί (είναι πιθανή).

Παράγοντες Απειλής:

- **Επίπεδο δεξιοτήτων**: 9 (Security penetration skills)
  - *Αιτιολόγηση*: Οι επιθέσεις αυτές μπορεί να πραγματοποιηθούν από χρήστες με υψηλές τεχνικές δεξιότητες και προγραμματιστικές γνώσεις.
- **Κίνητρο**: 9 (High reward)
  - *Αιτιολόγηση*: Η πρόσβαση σε ευαίσθητα ιατρικά δεδομένα και δυνατότητα παρέμβασης σε χειρουργικές ενέργειες αποτελεί ισχυρό κίνητρο για τους επιτιθέμενους, ενώ μπορεί να υπάρχει και οικονομικό κίνητρο.
- **Ευκαιρία**: 2 (Requires special access or resources)
  - *Αιτιολόγηση*: Η επίθεση απαιτεί συγκεκριμένες γνώσεις και πρόσβαση στο δίκτυο της εφαρμογής, καθιστώντας την πιο δύσκολη αλλά όχι αδύνατη.
- **Μέγεθος**: 2 (Developer)
  - *Αιτιολόγηση*: Η επίθεση μπορεί να πραγματοποιηθεί από προγραμματιστές και άτομα με υψηλές δεξιότητες.

Παράγοντες Τρωτότητας:

- **Ευκολία ανακάλυψης**: 2 (Very difficult)
  - *Αιτιολόγηση*: Η ανακάλυψη της ευπάθειας απαιτεί εξειδικευμένες γνώσεις και εργαλεία, καθιστώντας την ανακάλυψή της πολύ δύσκολη.
- **Ευκολία εκμετάλλευσης**: 2 (Very difficult)
  - *Αιτιολόγηση*: Η εκμετάλλευση της ευπάθειας απαιτεί εξειδικευμένες γνώσεις και εργαλεία, καθιστώντας την εκμετάλλευση της πολύ δύσκολη.
- **Ευαισθητοποίηση**: 1 (Unknown)

    - *Αιτιολόγηση*: Η ευαισθητοποίηση της συγκεκριμένης ευπάθειας είναι ελάχιστη ή άγνωστη.
- **Ανίχνευση εισβολής**: 2 (Active detection in application - Logs and reviewed)
    - *Αιτιολόγηση*: Υπάρχουν μηχανισμοί ανίχνευσης και καταγραφής, αλλά μπορεί να μην είναι επαρκείς για την άμεση αναγνώριση της επίθεσης.

Υπολογισμός Πιθανότητας Απειλής:

- **Threat Agent Factor (TAF)**: (9 + 9 + 2 + 2) / 4 = 5.5
- **Vulnerability Factor (VF)**: (2 + 2 + 1 + 2) / 4 = 1.75
- **Likelihood Factor (LF)**: (5.5 + 1.75) / 2 = 3.62

Βήμα 3: Παράγοντες για την εκτίμηση των επιπτώσεων

Τεχνικοί Παράγοντες Αντίκτυπου:

- **Απώλεια εμπιστευτικότητας**: 9 (All data disclosed)
    - *Αιτιολόγηση*: Η αποκάλυψη όλων των ευαίσθητων δεδομένων είναι πιθανή σε περίπτωση επιτυχούς επίθεσης.
- **Απώλεια ακεραιότητας**: 3 (Minimal seriously corrupt data)
    - *Αιτιολόγηση*: Η ακεραιότητα των δεδομένων μπορεί να διαταραχθεί, αλλά πιθανότατα σε περιορισμένο βαθμό ή θα είναι δυνατή η ανίχνευση.
- **Απώλεια διαθεσιμότητας**: 9 (All services completely lost)
    - *Αιτιολόγηση*: Η διαθεσιμότητα των υπηρεσιών μπορεί να επηρεαστεί πλήρως, ιδίως αν οι ενέργειες του χειρούργου δεν μεταδοθούν στα ρομποτικά μέσα.
- **Απώλεια υπευθυνότητας**: 8 (Complete anonymity)
    - *Αιτιολόγηση*: Οι επιτιθέμενοι μπορεί να παραμείνουν ανώνυμοι, καθιστώντας δύσκολη την ανίχνευση και τον εντοπισμό τους.

Παράγοντες Επιχειρηματικού Αντίκτυπου:

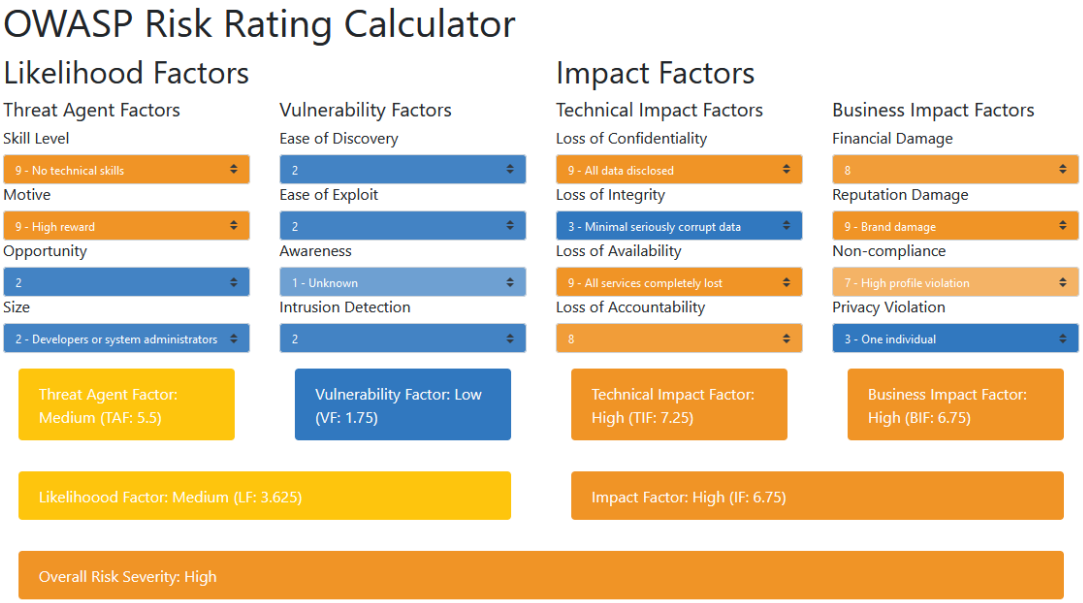
- **Οικονομική ζημία**: 8 (Significant impact on annual profit)
    - *Αιτιολόγηση*: Η παραβίαση μπορεί να οδηγήσει σε σημαντική οικονομική ζημία λόγω απώλειας δεδομένων και διαθεσιμότητας υπηρεσιών.
- **Ζημία φήμης**: 9 (Brand damage)
    - *Αιτιολόγηση*: Η ζημία φήμης θα είναι σημαντική, ιδίως σε περίπτωση αποκάλυψης ιατρικών δεδομένων και διακοπής των χειρουργικών επεμβάσεων.
- **Μη συμμόρφωση**: 7 (High profile violation)
    - *Αιτιολόγηση*: Η παραβίαση μπορεί να οδηγήσει σε σοβαρές συνέπειες μη συμμόρφωσης με κανονισμούς περί απορρήτου και ασφάλειας.
- **Παραβίαση του απορρήτου**: 3 (One individual)
    - *Αιτιολόγηση*: Η παραβίαση απορρήτου μπορεί να επηρεάσει ένα ή περισσότερα άτομα, αλλά είναι πιθανό να επικεντρωθεί σε έναν ασθενή.

Υπολογισμός Επιπτώσεων:

- **Technical Impact Factor (TIF)**: (9 + 3 + 9 + 8) / 4 = 7.25

- **Business Impact Factor (BIF)**: (8 + 9 + 7 + 3) / 4 = 6.75
- **Impact Factor (IF)**: (7.25 + 6.75) / 2 = 7

Βήμα 4: Καθορισμός της σοβαρότητας του κινδύνου



Εικόνα 10: Στιγμιότυπο οθόνης σοβαρότητας κινδύνου κλώνου ιστοσελίδας χωρίς κρυπτογράφηση

Συνολική Εκτίμηση Ρίσκου:

- **Likelihood Factor (LF)**: 3.65
- **Impact Factor (IF)**: 7
- **Overall Risk Severity**: 3.65 * 7 = 25.55 (High)

5.5.2 Κίνδυνος υποκλοπής δεδομένων από το cloud

Βήμα 1: Προσδιορισμός κινδύνου

Η υποκλοπή δεδομένων από το cloud μπορεί να οδηγήσει σε απώλεια ευαίσθητων ιατρικών πληροφοριών, βλάπτοντας την ιδιωτικότητα των ασθενών και την αξιοπιστία της ιατρικής υπηρεσίας.

Βήμα 2: Παράγοντες για την εκτίμηση της πιθανότητας

Παράγοντες Απειλής:

- **Επίπεδο δεξιοτήτων:** 8 (Advanced technical skills required)
    - Αιτιολόγηση: Απαιτούνται εξειδικευμένες γνώσεις και τεχνικές για την παραβίαση ασφαλείας δεδομένων στο cloud.
- **Κίνητρο:** 9 (High reward)

    - Αιτιολόγηση: Η πρόσβαση σε ευαίσθητα ιατρικά δεδομένα είναι ένα ισχυρό κίνητρο.
- **Ευκαιρία:** 3 (Requires significant resources)
    - Αιτιολόγηση: Η επίθεση απαιτεί συγκεκριμένα εργαλεία και πόρους.
- **Μέγεθος:** 7 (Large number of potential attackers)
    - Αιτιολόγηση: Πολλοί δυνητικοί επιτιθέμενοι με δυνατότητα πρόσβασης στο Διαδίκτυο.

Παράγοντες Τρωτότητας:

- **Ευκολία ανακάλυψης:** 4 (Moderately difficult)
    - Αιτιολόγηση: Η ευπάθεια μπορεί να ανακαλυφθεί μέσω εξελιγμένων εργαλείων.
- **Ευκολία εκμετάλλευσης:** 5 (Moderately difficult)
    - Αιτιολόγηση: Η εκμετάλλευση της ευπάθειας απαιτεί εξειδικευμένες γνώσεις και εργαλεία.
- **Ευαισθητοποίηση:** 2 (Somewhat known)
    - Αιτιολόγηση: Η ευπάθεια είναι μερικώς γνωστή σε ορισμένους κύκλους.
- **Ανίχνευση εισβολής:** 3 (Limited logging and review)
    - Αιτιολόγηση: Υπάρχει κάποια δυνατότητα ανίχνευσης, αλλά όχι πλήρης.

Υπολογισμός Πιθανότητας Απειλής:

- **Threat Agent Factor (TAF):** (8 + 9 + 3 + 7) / 4 = 6.75
- **Vulnerability Factor (VF):** (4 + 5 + 2 + 3) / 4 = 3.5
- **Likelihood Factor (LF):** (6.75 + 3.5) / 2 = 5.125

Βήμα 3: Παράγοντες για την εκτίμηση των επιπτώσεων

Τεχνικοί Παράγοντες Αντίκτυπου:

- **Απώλεια εμπιστευτικότητας:** 9 (All data disclosed)
    - Αιτιολόγηση: Πιθανή ανακάλυψη όλων των ευαίσθητων δεδομένων.
- **Απώλεια ακεραιότητας:** 4 (Significant data corruption)
    - Αιτιολόγηση: Δυνητική αλλοίωση δεδομένων.
- **Απώλεια διαθεσιμότητας:** 7 (Extended downtime)
    - Αιτιολόγηση: Σημαντική διακοπή της διαθεσιμότητας των υπηρεσιών.
- **Απώλεια υπευθυνότητας:** 6 (Partial anonymity)
    - Αιτιολόγηση: Οι επιτιθέμενοι μπορεί να είναι μερικώς ανώνυμοι.

Παράγοντες Επιχειρηματικού Αντίκτυπου:

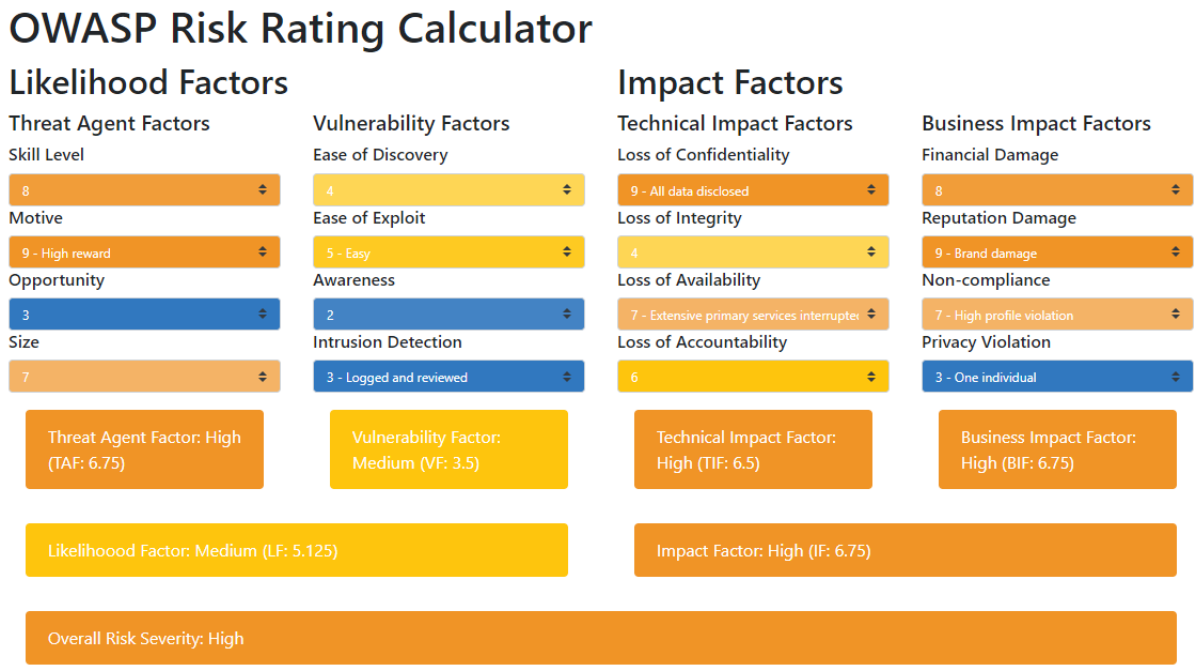
- **Οικονομική ζημία:** 8 (Significant impact on annual profit)
    - Αιτιολόγηση: Σημαντικές οικονομικές ζημίες λόγω απώλειας δεδομένων.
- **Ζημία φήμης:** 9 (Brand damage)
    - Αιτιολόγηση: Σοβαρή ζημία στη φήμη της εταιρείας.

- **Μη συμμόρφωση:** 7 (High profile violation)
  - Αιτιολόγηση: Παραβίαση κανονισμών και συμμόρφωσης.
- **Παραβίαση του απορρήτου:** 3 (One individual)
  - Αιτιολόγηση: Επηρεάζει έναν ή περισσότερους ασθενείς.

Υπολογισμός Επιπτώσεων:

- **Technical Impact Factor (TIF):** (9 + 4 + 7 + 6) / 4 = 6.5
- **Business Impact Factor (BIF):** (8 + 9 + 7 + 3) / 4 = 6.75
- **Impact Factor (IF):** (6.5 + 6.75) / 2 = 6.625

Βήμα 4: Καθορισμός της σοβαρότητας του κινδύνου



Εικόνα 11: Στιγμιότυπο οθόνης σοβαρότητας κινδύνου υποκλοπής δεδομένων από το cloud

Συνολική Εκτίμηση Ρίσκου:

- **Likelihood Factor (LF):** 5.125
- **Impact Factor (IF):** 6.625
- **Overall Risk Severity:** 5.125 * 6.625 = 33.95 (High)

5.5.3 Κίνδυνος αλλοίωσης ή απώλειας δεδομένων

Βήμα 1: Προσδιορισμός κινδύνου

Η αλλοίωση ή απώλεια δεδομένων μπορεί να οδηγήσει σε λανθασμένες διαγνώσεις και θεραπείες, με πιθανές σοβαρές επιπτώσεις για την υγεία των ασθενών.

Βήμα 2: Παράγοντες για την εκτίμηση της πιθανότητας

Παράγοντες Απειλής:

- **Επίπεδο δεξιοτήτων:** 7 (Advanced technical skills required)
    - Αιτιολόγηση: Απαιτούνται εξειδικευμένες γνώσεις για την αλλοίωση ή διαγραφή δεδομένων.
- **Κίνητρο:** 8 (High reward)
    - Αιτιολόγηση: Η αλλοίωση ή απώλεια δεδομένων μπορεί να προκαλέσει σοβαρές επιπτώσεις.
- **Ευκαιρία:** 4 (Requires significant resources)
    - Αιτιολόγηση: Η επίθεση απαιτεί συγκεκριμένα εργαλεία και πόρους.
- **Μέγεθος:** 6 (Moderate number of potential attackers)
    - Αιτιολόγηση: Μέτριος αριθμός δυνητικών επιτιθέμενων.

Παράγοντες Τρωτότητας:

- **Ευκολία ανακάλυψης:** 4 (Moderately difficult)
    - Αιτιολόγηση: Η ευπάθεια μπορεί να ανακαλυφθεί μέσω εξελιγμένων εργαλείων.
- **Ευκολία εκμετάλλευσης:** 5 (Moderately difficult)
    - Αιτιολόγηση: Η εκμετάλλευση της ευπάθειας απαιτεί εξειδικευμένες γνώσεις και εργαλεία.
- **Ευαισθητοποίηση:** 2 (Somewhat known)
    - Αιτιολόγηση: Η ευπάθεια είναι μερικώς γνωστή σε ορισμένους κύκλους.
- **Ανίχνευση εισβολής:** 3 (Limited logging and review)
    - Αιτιολόγηση: Υπάρχει κάποια δυνατότητα ανίχνευσης, αλλά όχι πλήρης.

Υπολογισμός Πιθανότητας Απειλής:

- **Threat Agent Factor (TAF):** (7 + 8 + 4 + 6) / 4 = 6.25
- **Vulnerability Factor (VF):** (4 + 5 + 2 + 3) / 4 = 3.5
- **Likelihood Factor (LF):** (6.25 + 3.5) / 2 = 4.875

Βήμα 3: Παράγοντες για την εκτίμηση των επιπτώσεων

Τεχνικοί Παράγοντες Αντίκτυπου:

- **Απώλεια εμπιστευτικότητας:** 6 (Significant data disclosure)
    - Αιτιολόγηση: Πιθανή αποκάλυψη ευαίσθητων δεδομένων.
- **Απώλεια ακεραιότητας:** 8 (Extensive data corruption)
    - Αιτιολόγηση: Δυνητική αλλοίωση σημαντικού μέρους των δεδομένων.
- **Απώλεια διαθεσιμότητας:** 6 (Extended downtime)
    - Αιτιολόγηση: Σημαντική διακοπή της διαθεσιμότητας των υπηρεσιών.
- **Απώλεια υπευθυνότητας:** 5 (Partial anonymity)
    - Αιτιολόγηση: Οι επιτιθέμενοι μπορεί να είναι μερικώς ανώνυμοι.

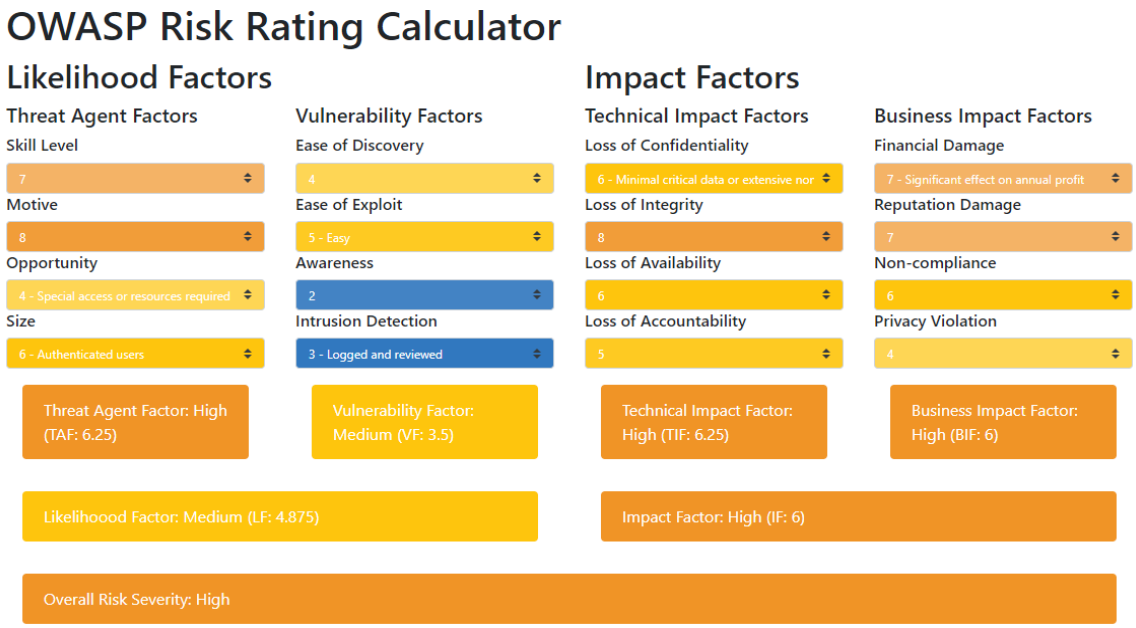
Παράγοντες Επιχειρηματικού Αντίκτυπου:

- **Οικονομική ζημία:** 7 (Moderate impact on annual profit)
    - Αιτιολόγηση: Μέτριες οικονομικές ζημίες λόγω απώλειας δεδομένων.
- **Ζημία φήμης:** 7 (Moderate brand damage)
    - Αιτιολόγηση: Μέτρια ζημία στη φήμη της εταιρείας.
- **Μη συμμόρφωση:** 6 (Moderate violation)
    - Αιτιολόγηση: Παραβίαση κανονισμών και συμμόρφωσης.
- **Παραβίαση του απορρήτου:** 4 (Multiple individuals)
    - Αιτιολόγηση: Επηρεάζει περισσότερους από έναν ασθενείς.

Υπολογισμός Επιπτώσεων:

- **Technical Impact Factor (TIF):** (6 + 8 + 6 + 5) / 4 = 6.25
- **Business Impact Factor (BIF):** (7 + 7 + 6 + 4) / 4 = 6
- **Impact Factor (IF):** (6.25 + 6) / 2 = 6.125

Βήμα 4: Καθορισμός της σοβαρότητας του κινδύνου



Εικόνα 12: Στιγμιότυπο οθόνης σοβαρότητας κινδύνου αλλοίωσης ή απώλειας δεδομένων

Συνολική Εκτίμηση Ρίσκου:

- **Likelihood Factor (LF):** 4.875
- **Impact Factor (IF):** 6.125
- **Overall Risk Severity:** 4.875 * 6.125 = 29.85 (High)

5.5.4 Πολύπλοκες ή δύσχρηστες διεπαφές μπορούν να προκαλέσουν σύγχυση ή λάθη κατά τη χρήση

Βήμα 1: Προσδιορισμός κινδύνου

Μια πολύπλοκη ή δύσχρηστη διεπαφή μπορεί να οδηγήσει σε λάθη κατά τη διάρκεια της χειρουργικής διαδικασίας, με αποτέλεσμα τη λανθασμένη χρήση των ρομποτικών συστημάτων και δυνητικά σοβαρές επιπτώσεις για την υγεία των ασθενών.

Βήμα 2: Παράγοντες για την εκτίμηση της πιθανότητας

Παράγοντες Απειλής:

- **Επίπεδο δεξιοτήτων:** 6 (Moderate technical skills required)
  - Αιτιολόγηση: Απαιτούνται μέτριες τεχνικές δεξιότητες για την κατανόηση της διεπαφής.
- **Κίνητρο:** 7 (Moderate reward)
  - Αιτιολόγηση: Η αποφυγή λαθών κατά τη χρήση των ρομποτικών συστημάτων είναι σημαντικό κίνητρο.
- **Ευκαιρία:** 5 (Common access to resources)
  - Αιτιολόγηση: Η διεπαφή είναι διαθέσιμη σε πολλούς χρήστες.
- **Μέγεθος:** 5 (Moderate number of potential attackers)
  - Αιτιολόγηση: Μέτριος αριθμός δυνητικών χρηστών.

Παράγοντες Τρωτότητας:

- **Ευκολία ανακάλυψης:** 3 (Difficult)
  - Αιτιολόγηση: Η δυσκολία της διεπαφής μπορεί να ανακαλυφθεί μέσω χρήσης και ανατροφοδότησης.
- **Ευκολία εκμετάλλευσης:** 6 (Moderate)
  - Αιτιολόγηση: Οι χρήστες μπορεί να δυσκολευτούν να χρησιμοποιήσουν σωστά την διεπαφή.
- **Ευαισθητοποίηση:** 2 (Somewhat known)
  - Αιτιολόγηση: Η ευπάθεια είναι μερικώς γνωστή στους χρήστες.
- **Ανίχνευση εισβολής:** 3 (Limited logging and review)
  - Αιτιολόγηση: Υπάρχει κάποια δυνατότητα ανίχνευσης, αλλά όχι πλήρης.

Υπολογισμός Πιθανότητας Απειλής:

- **Threat Agent Factor (TAF):** (6 + 7 + 5 + 5) / 4 = 5.75
- **Vulnerability Factor (VF):** (3 + 6 + 2 + 3) / 4 = 3.5
- **Likelihood Factor (LF):** (5.75 + 3.5) / 2 = 4.625

Βήμα 3: Παράγοντες για την εκτίμηση των επιπτώσεων

Τεχνικοί Παράγοντες Αντίκτυπου:

- **Απώλεια εμπιστευτικότητας:** 4 (Minimal data disclosure)
    - Αιτιολόγηση: Η εμπιστευτικότητα των δεδομένων μπορεί να επηρεαστεί ελάχιστα.
- **Απώλεια ακεραιότητας:** 7 (Significant data corruption)
    - Αιτιολόγηση: Δυνητική αλλοίωση σημαντικού μέρους των δεδομένων.
- **Απώλεια διαθεσιμότητας:** 6 (Extended downtime)
    - Αιτιολόγηση: Σημαντική διακοπή της διαθεσιμότητας των υπηρεσιών.
- **Απώλεια υπευθυνότητας:** 5 (Partial anonymity)
    - Αιτιολόγηση: Οι επιτιθέμενοι μπορεί να είναι μερικώς ανώνυμοι.

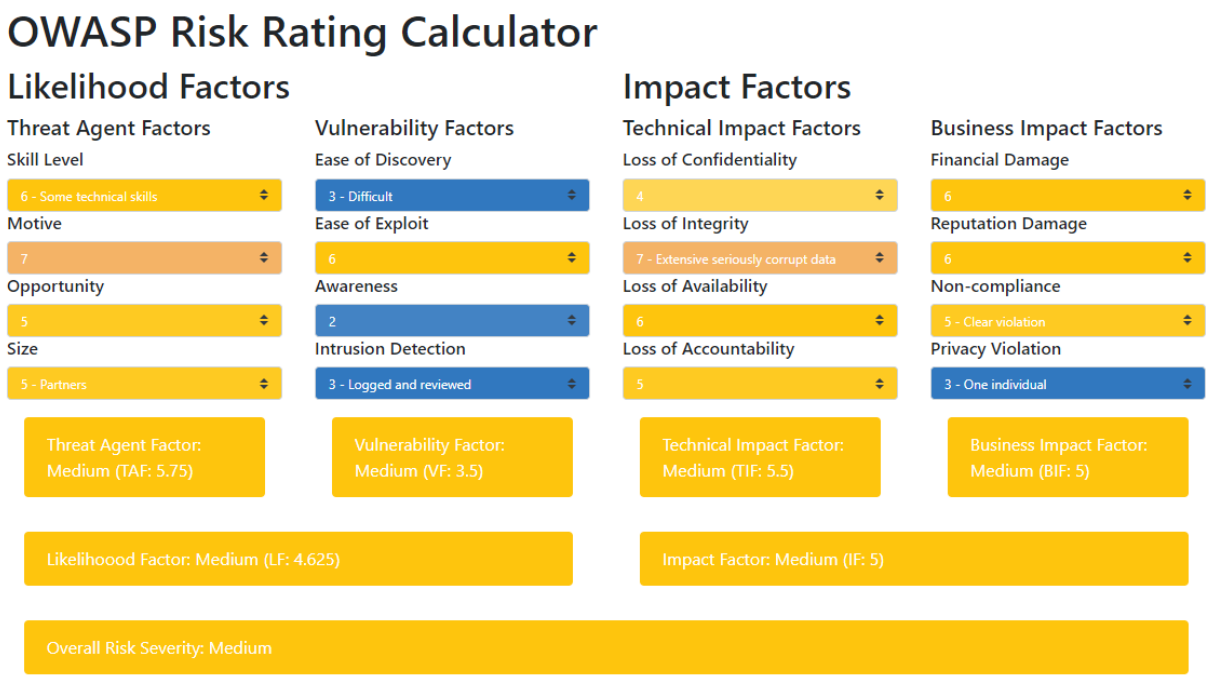
Παράγοντες Επιχειρηματικού Αντίκτυπου:

- **Οικονομική ζημία:** 6 (Moderate impact on annual profit)
    - Αιτιολόγηση: Μέτριες οικονομικές ζημίες λόγω απώλειας δεδομένων.
- **Ζημία φήμης:** 6 (Moderate brand damage)
    - Αιτιολόγηση: Μέτρια ζημία στη φήμη της εταιρείας.
- **Μη συμμόρφωση:** 5 (Moderate violation)
    - Αιτιολόγηση: Παραβίαση κανονισμών και συμμόρφωσης.
- **Παραβίαση του απορρήτου:** 3 (One individual)
    - Αιτιολόγηση: Επηρεάζει έναν ή περισσότερους ασθενείς.

Υπολογισμός Επιπτώσεων:

- **Technical Impact Factor (TIF):** (4 + 7 + 6 + 5) / 4 = 5.5
- **Business Impact Factor (BIF):** (6 + 6 + 5 + 3) / 4 = 5
- **Impact Factor (IF):** (5.5 + 5) / 2 = 5.25

Βήμα 4: Καθορισμός της σοβαρότητας του κινδύνου



Εικόνα 13: Στιγμιότυπο οθόνης σοβαρότητας κινδύνου πολυπλοκότητας των διεπαφών

Συνολική Εκτίμηση Ρίσκου:

- **Likelihood Factor (LF):** 4.625
- **Impact Factor (IF):** 5.25
- **Overall Risk Severity:** 4.625 * 5.25 = 24.28 (Medium)

5.5.5 Σφάλματα λογισμικού ή υλικού που μπορεί να προκαλέσουν καθυστερήσεις ή διακοπές στη χειρουργική διαδικασία

Βήμα 1: Προσδιορισμός κινδύνου

Τα σφάλματα λογισμικού ή υλικού μπορούν να προκαλέσουν καθυστερήσεις ή διακοπές στη χειρουργική διαδικασία, θέτοντας σε κίνδυνο την ασφάλεια των ασθενών και την επιτυχία της επέμβασης.

Βήμα 2: Παράγοντες για την εκτίμηση της πιθανότητας

Παράγοντες Απειλής:

- **Επίπεδο δεξιοτήτων:** 6 (Moderate technical skills required)
    - Αιτιολόγηση: Απαιτούνται μέτριες τεχνικές δεξιότητες για τη διαχείριση και επίλυση των σφαλμάτων.
- **Κίνητρο:** 8 (High reward)

    - Αιτιολόγηση: Η αποφυγή καθυστερήσεων και διακοπών στη χειρουργική διαδικασία είναι ισχυρό κίνητρο.
- **Ευκαιρία:** 5 (Common access to resources)
    - Αιτιολόγηση: Η διεπαφή είναι διαθέσιμη σε πολλούς χρήστες.
- **Μέγεθος:** 5 (Moderate number of potential attackers)
    - Αιτιολόγηση: Μέτριος αριθμός δυνητικών χρηστών.

Παράγοντες Τρωτότητας:

- **Ευκολία ανακάλυψης:** 4 (Moderately difficult)
    - Αιτιολόγηση: Τα σφάλματα μπορεί να ανακαλυφθούν μέσω χρήσης και ανατροφοδότησης.
- **Ευκολία εκμετάλλευσης:** 5 (Moderately difficult)
    - Αιτιολόγηση: Οι χρήστες μπορεί να δυσκολευτούν να χρησιμοποιήσουν σωστά τη διεπαφή όταν προκύψουν σφάλματα.
- **Ευαισθητοποίηση:** 2 (Somewhat known)
    - Αιτιολόγηση: Η ευπάθεια είναι μερικώς γνωστή στους χρήστες.
- **Ανίχνευση εισβολής:** 3 (Limited logging and review)
    - Αιτιολόγηση: Υπάρχει κάποια δυνατότητα ανίχνευσης, αλλά όχι πλήρης.

Υπολογισμός Πιθανότητας Απειλής:

- **Threat Agent Factor (TAF):** (6 + 8 + 5 + 5) / 4 = 6
- **Vulnerability Factor (VF):** (4 + 5 + 2 + 3) / 4 = 3.5
- **Likelihood Factor (LF):** (6 + 3.5) / 2 = 4.75

Βήμα 3: Παράγοντες για την εκτίμηση των επιπτώσεων

Τεχνικοί Παράγοντες Αντίκτυπου:

- **Απώλεια εμπιστευτικότητας:** 3 (Minimal data disclosure)
    - Αιτιολόγηση: Η εμπιστευτικότητα των δεδομένων μπορεί να επηρεαστεί ελάχιστα.
- **Απώλεια ακεραιότητας:** 6 (Moderate data corruption)
    - Αιτιολόγηση: Δυνητική αλλοίωση δεδομένων.
- **Απώλεια διαθεσιμότητας:** 7 (Extended downtime)
    - Αιτιολόγηση: Σημαντική διακοπή της διαθεσιμότητας των υπηρεσιών.
- **Απώλεια υπευθυνότητας:** 5
    - Αιτιολόγηση: Οι επιτιθέμενοι μπορεί να είναι μερικώς ανώνυμοι.

Παράγοντες Επιχειρηματικού Αντίκτυπου:

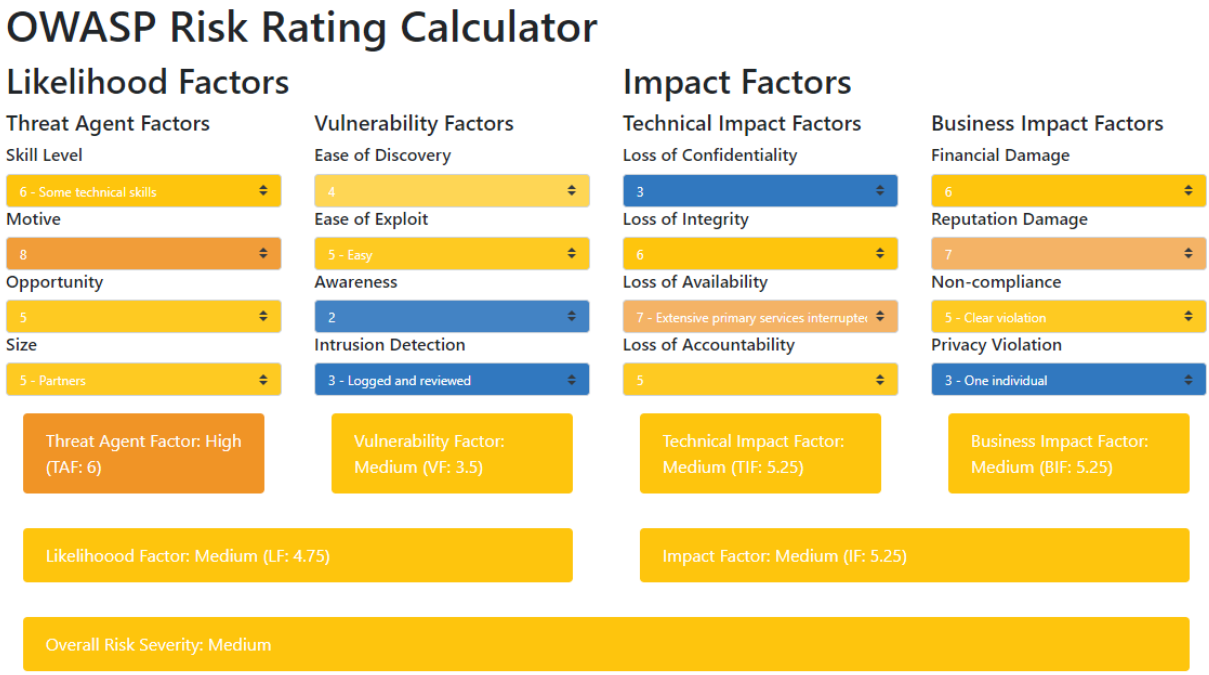
- **Οικονομική ζημία:** 6 (Moderate impact on annual profit)
    - Αιτιολόγηση: Μέτριες οικονομικές ζημίες λόγω απώλειας δεδομένων.
- **Ζημία φήμης:** 7 (Moderate brand damage)
    - Αιτιολόγηση: Μέτρια ζημία στη φήμη της εταιρείας.

- **Μη συμμόρφωση:** 5 (Moderate violation)
    - Αιτιολόγηση: Παραβίαση κανονισμών και συμμόρφωσης.
- **Παραβίαση του απορρήτου:** 3 (One individual)
    - Αιτιολόγηση: Επηρεάζει έναν ή περισσότερους ασθενείς.

Υπολογισμός Επιπτώσεων:

- **Technical Impact Factor (TIF):** (3 + 6 + 7 + 5) / 4 = 5.25
- **Business Impact Factor (BIF):** (6 + 7 + 5 + 3) / 4 = 5.25
- **Impact Factor (IF):** (5.25 + 5.25) / 2 = 5.25

Βήμα 4: Καθορισμός της σοβαρότητας του κινδύνου



Εικόνα 14: Στιγμιότυπο οθόνης σοβαρότητας κινδύνου σφαλμάτων λογισμικού ή υλικού

Συνολική Εκτίμηση Ρίσκου:

- **Likelihood Factor (LF):** 4.75
- **Impact Factor (IF):** 5.25
- **Overall Risk Severity:** 4.75 * 5.25 = 24.94 (Medium)

5.5.6 Βήμα 5: Απόφαση για το τι πρέπει να διορθωθεί

Στο βήμα αυτό λαμβάνοντας υπόψη τα αποτελέσματα των πέντε σεναρίων ρίσκου που είδαμε παραπάνω πρέπει να τους ταξινομήσουμε. Για να ταξινομήσουμε τους κινδύνους από τον πιο σοβαρό στον λιγότερο σοβαρό, θα χρησιμοποιήσουμε την συνολική εκτίμηση ρίσκου (Overall Risk Severity) για κάθε σενάριο:

- **Κίνδυνος υποκλοπής δεδομένων από το cloud**
  - Overall Risk Severity: 33.95 (High)
- **Κίνδυνος αλλοίωσης ή απώλειας δεδομένων**
  - Overall Risk Severity: 29.85 (High)
- **Κλώνος ιστοσελίδας χωρίς κρυπτογράφηση**
  - Overall Risk Severity: 25.55 (High)
- **Σφάλματα λογισμικού ή υλικού που μπορεί να προκαλέσουν καθυστερήσεις ή διακοπές στη χειρουργική διαδικασία**
  - Overall Risk Severity: 24.94 (Medium)
- **Πολύπλοκες ή δύσχρηστες διεπαφές που μπορούν να προκαλέσουν σύγχυση ή λάθη κατά τη χρήση**
  - Overall Risk Severity: 24.28 (Medium)

Για να αποφασίσουμε τι πρέπει να διορθωθεί πρώτα, θα πρέπει να εξετάσουμε, τη σοβαρότητα των επιπτώσεων, την πιθανότητα εμφάνισης των κινδύνων και το κόστος και την ευκολία των διορθωτικών ενεργειών.

Εξέταση Κινδύνων

- **Κίνδυνος υποκλοπής δεδομένων από το cloud (33.95 - High)**
  - **Σοβαρότητα:** Πολύ υψηλή, με πιθανότητα αποκάλυψης όλων των ευαίσθητων δεδομένων.
  - **Πιθανότητα:** Μέτρια προς υψηλή.
  - **Διορθωτικά Μέτρα:** Ενίσχυση της ασφάλειας του cloud, χρήση κρυπτογράφησης, εφαρμογή πολιτικών ασφαλείας.
  - **Προτεραιότητα Διορθωτικών Ενεργειών:** Πολύ υψηλή. Η προστασία των δεδομένων είναι κρίσιμη.
- **Κίνδυνος αλλοίωσης ή απώλειας δεδομένων (29.85 - High)**
  - **Σοβαρότητα:** Πολύ υψηλή, με πιθανότητα λανθασμένων διαγνώσεων και θεραπειών.
  - **Πιθανότητα:** Μέτρια.
  - **Διορθωτικά Μέτρα:** Εφαρμογή συστημάτων backup, χρήση λογισμικού ανίχνευσης και αποκατάστασης.

    - **Προτεραιότητα Διορθωτικών Ενεργειών:** Υψηλή. Η διασφάλιση της ακεραιότητας των δεδομένων είναι κρίσιμη.
- **Κλώνος ιστοσελίδας χωρίς κρυπτογράφηση(25.55 - High)**
    - **Σοβαρότητα:** Υψηλή, με δυνατότητα αποκάλυψης διαπιστευτηρίων και λανθασμένων χειρουργικών διαδικασιών.
    - **Πιθανότητα:** Μέτρια προς υψηλή.
    - **Διορθωτικά Μέτρα:** Εφαρμογή κρυπτογράφησης, εκπαίδευση χρηστών, χρήση συστημάτων ανίχνευσης phishing.
    - **Προτεραιότητα Διορθωτικών Ενεργειών:** Υψηλή. Η προστασία από phishing είναι κρίσιμη για την ασφάλεια.
- **Σφάλματα λογισμικού ή υλικού (24.94 - Medium)**
    - **Σοβαρότητα:** Μέτρια, με δυνατότητα καθυστερήσεων ή διακοπών στη χειρουργική διαδικασία.
    - **Πιθανότητα:** Μέτρια.
    - **Διορθωτικά Μέτρα:** Συχνές αναβαθμίσεις λογισμικού, τακτική συντήρηση εξοπλισμού.
    - **Προτεραιότητα Διορθωτικών Ενεργειών:** Μέτρια. Η εξασφάλιση της λειτουργικότητας είναι σημαντική.
- **Πολύπλοκες ή δύσχρηστες διεπαφές (24.28 - Medium)**
    - **Σοβαρότητα:** Μέτρια, με δυνατότητα σύγχυσης ή λαθών κατά τη χρήση.
    - **Πιθανότητα:** Μέτρια.
    - **Διορθωτικά Μέτρα:** Βελτίωση σχεδιασμού διεπαφών, εκπαίδευση χρηστών.
    - **Προτεραιότητα Διορθωτικών Ενεργειών:** Μέτρια. Η βελτίωση της εμπειρίας χρήστη είναι σημαντική.

Προτεινόμενη Σειρά Διορθωτικών Ενεργειών

- **Κίνδυνος υποκλοπής δεδομένων από το cloud**
    - **Προτεραιότητα:** Πολύ υψηλή
    - **Διορθωτικά Μέτρα:** Ενίσχυση ασφάλειας, κρυπτογράφηση, πολιτικές ασφαλείας
- **Κίνδυνος αλλοίωσης ή απώλειας δεδομένων**
    - **Προτεραιότητα:** Υψηλή
    - **Διορθωτικά Μέτρα:** Συστήματα backup, λογισμικό ανίχνευσης και αποκατάστασης
- **Κλώνος ιστοσελίδας χωρίς κρυπτογράφηση**
    - **Προτεραιότητα:** Υψηλή
    - **Διορθωτικά Μέτρα:** Κρυπτογράφηση, εκπαίδευση χρηστών, ανίχνευση phishing
- **Σφάλματα λογισμικού ή υλικού**
    - **Προτεραιότητα:** Μέτρια

    - **Διορθωτικά Μέτρα:** Αναβαθμίσεις λογισμικού, συντήρηση εξοπλισμού
- **Πολύπλοκες ή δύσχρηστες διεπαφές**
    - **Προτεραιότητα:** Μέτρια
    - **Διορθωτικά Μέτρα:** Βελτίωση σχεδιασμού, εκπαίδευση χρηστών

Με αυτή την προσέγγιση, μπορούμε να επικεντρωθούμε αρχικά στους κινδύνους με τη μεγαλύτερη σοβαρότητα και να προχωρήσουμε στη σταδιακή εφαρμογή των διορθωτικών μέτρων για όλους τους κινδύνους, εξασφαλίζοντας μια ασφαλή και αποδοτική λειτουργία των συστημάτων IoT.

5.5.7 Βήμα 6: Προσαρμογή του μοντέλου αξιολόγησης κινδύνου

Για την προσαρμογή του μοντέλου αξιολόγησης κινδύνου, πρέπει να λάβουμε υπόψη τις ιδιαιτερότητες και τις προτεραιότητες της συγκεκριμένης εφαρμογής στην τηλεχειρουργική. Ακολουθούν μερικά βήματα για την προσαρμογή του μοντέλου:

- **Προσθήκη παραγόντων**
  - Προσθήκη παραγόντων που αντιπροσωπεύουν καλύτερα τους κινδύνους για την τηλεχειρουργική. Για παράδειγμα, προσθήκη παραγόντων που σχετίζονται με την ασφάλεια των ασθενών και την προστασία των ιατρικών δεδομένων.
- **Επιλογές προσαρμογής**
  - Προσαρμογή των βαθμολογιών και των ονομάτων των παραγόντων ώστε να ταιριάζουν με την συγκεκριμένη επιχείρηση ή εφαρμογή. Για παράδειγμα, η προσαρμογή των κατηγοριών κινδύνου στις ανάγκες του ιατρικού τομέα.
- **Συντελεστές στάθμισης**
  - Χρήση σταθμισμένων μέσων για να δοθεί έμφαση στους παράγοντες που είναι πιο σημαντικοί για την επιχείρηση. Για παράδειγμα, μεγαλύτερη έμφαση στην ασφάλεια των ασθενών σε σχέση με άλλους παράγοντες.

Ακολουθούν οι προσαρμοσμένοι παράγοντες και συντελεστές στάθμισης για το μοντέλο αξιολόγησης κινδύνου:

Προσαρμοσμένοι Παράγοντες και Συντελεστές Στάθμισης

1. **Ασφάλεια Ασθενών (30%)**
   - Έμφαση στην ασφάλεια και προστασία των ασθενών κατά τη διάρκεια της χειρουργικής διαδικασίας.
   - **Σκέψη:** Η ασφάλεια των ασθενών είναι η πρωταρχική προτεραιότητα σε κάθε ιατρική διαδικασία, πόσο μάλλον στην τηλεχειρουργική. Οποιοσδήποτε κίνδυνος που μπορεί να απειλήσει την ασφάλεια του ασθενούς πρέπει να έχει τη μέγιστη προσοχή και έμφαση.
2. **Προστασία Δεδομένων (25%)**
   - Έμφαση στην προστασία των ευαίσθητων ιατρικών δεδομένων από παραβιάσεις και υποκλοπές.
   - **Σκέψη:** Τα ιατρικά δεδομένα είναι εξαιρετικά ευαίσθητα και η προστασία τους από παραβιάσεις είναι ζωτικής σημασίας. Η διαρροή ή υποκλοπή αυτών των δεδομένων μπορεί να έχει σοβαρές επιπτώσεις στην ιδιωτικότητα και την ασφάλεια των ασθενών.
3. **Διαθεσιμότητα Υπηρεσιών (20%)**
   - Έμφαση στη διασφάλιση της αδιάλειπτης λειτουργίας των ιατρικών υπηρεσιών και συστημάτων.

- **Σκέψη:** Η αδιάλειπτη λειτουργία των ιατρικών υπηρεσιών είναι κρίσιμη για την επιτυχία των χειρουργικών επεμβάσεων. Οποιαδήποτε διακοπή ή καθυστέρηση μπορεί να θέσει σε κίνδυνο τη ζωή του ασθενούς.

4. **Οικονομικές Επιπτώσεις (15%)**
   - Έμφαση στις οικονομικές ζημίες που μπορεί να προκύψουν από παραβιάσεις ή διακοπές των υπηρεσιών.
   - **Σκέψη:** Οι οικονομικές επιπτώσεις από τις παραβιάσεις ή τις διακοπές μπορούν να είναι σημαντικές, αλλά δεν είναι τόσο κρίσιμες όσο η ασφάλεια των ασθενών και η προστασία των δεδομένων (τουλάχιστον με κοινωνικά κριτήρια). Ωστόσο, παραμένουν σημαντικός παράγοντας που πρέπει να ληφθεί υπόψη.
5. **Φήμη και Εμπιστοσύνη (10%)**
   - Έμφαση στη διατήρηση της φήμης και της εμπιστοσύνης των ασθενών και των πελατών στην επιχείρηση.
   - **Σκέψη:** Η διατήρηση της φήμης και της εμπιστοσύνης των ασθενών και των πελατών είναι σημαντική για τη βιωσιμότητα της επιχείρησης, αλλά έχει μικρότερη βαρύτητα σε σύγκριση με την ασφάλεια και την προστασία των δεδομένων.

Με βάση αυτά τα βήματα, μπορούμε να προχωρήσουμε στην αξιολόγηση και προσαρμογή του μοντέλου αξιολόγησης κινδύνου για την τηλεχειρουργική, διασφαλίζοντας ότι καλύπτει τις ανάγκες και τις προτεραιότητες της εφαρμογής.

5.5.8 Αποτελέσματα εφαρμογής διορθωτικών ενεργειών

Σε αυτην την υποενότητα θα λάβουμε υπόψη τα διορθωτικά μέτρα που προτάθηκαν για την κάθε απειλή και θα ξανά βαθμολογήσουμε το ρίσκο.

5.5.8.1 Κλώνος ιστοσελίδας χωρίς κρυπτογράφηση

Διορθωτικά Μέτρα:

- Εφαρμογή κρυπτογράφησης
- Εκπαίδευση χρηστών
- Χρήση συστημάτων ανίχνευσης phishing

Βελτιωμένη Εκτίμηση:

Likelihood Factor (LF):

- **Επίπεδο δεξιοτήτων**: 9 (Security penetration skills)
- **Κίνητρο**: 9 (High reward)
- **Ευκαιρία**: 2 (Requires special access or resources)
- **Μέγεθος**: 2 (Developers or system administrators)

Παραμένει ίδιο **Threat Agent Factor (TAF):** (9 + 9 + 2 + 2) / 4 = 5.5

- **Ευκολία ανακάλυψης**: 2 (Very difficult)
- **Ευκολία εκμετάλλευσης**: 1 (Very difficult) Με την εφαρμογή ισχυρής κρυπτογράφησης και τακτικής εκπαίδευσης χρηστών, η εκμετάλλευση του συστήματος μπορεί να γίνει πολύ δύσκολη, από 2 σε 1.
- **Επίγνωση**: 1 (Unknown)
- **Ανίχνευση εισβολής**: 2 (Active detection in application - Logs and reviewed

Νέο **Vulnerability Factor (VF):** (2 + 1 + 1 + 2) / 4 = 1.5

Νέο **Likelihood Factor (LF):** (5.5 + 1.5) / 2 = 3.5

Impact Factor (IF):

- **Απώλεια εμπιστευτικότητας**: 4 (All data disclosed)Μειώνεται με την κρυπτογράφηση και την εκπαίδευση από 9 σε 4.
- **Απώλεια ακεραιότητας**: 3 (Minimal seriously corrupt data)
- **Απώλεια διαθεσιμότητας**: 9 (All services completely lost)
- **Απώλεια υπευθυνότητας**: 8 (Complete anonymity)

Νέο **Technical Impact Factor (TIF):** (4 + 3 + 9 + 8) / 4 = 6

- **Οικονομική ζημία**: 8 (Significant impact on annual profit)
- **Ζημία φήμης**: 9 (Brand damage)
- **Μη συμμόρφωση**: 7 (High profile violation)
- **Παραβίαση του απορρήτου**: 3 (One individual)

Παραμένει ίδιο **Business Impact Factor (BIF):** (8 + 9 + 7 + 3) / 4 = 6.75

Νέο **Impact Factor (IF):** (6 + 6.75) / 2 = 6.375

Νέο Overall Risk Severity: 3.5 * 6.375 = 22.31 (Medium)

5.5.8.2 Κίνδυνος υποκλοπής δεδομένων από το cloud

Διορθωτικά Μέτρα:

- Ενίσχυση της ασφάλειας του cloud
- Χρήση κρυπτογράφησης
- Εφαρμογή πολιτικών ασφαλείας

Βελτιωμένη Εκτίμηση:

Likelihood Factor (LF):

- **Επίπεδο δεξιοτήτων:** 8 (Advanced technical skills required)
- **Κίνητρο:** 9 (High reward)
- **Ευκαιρία:** 3 (Requires significant resources)
- **Μέγεθος:** 7 (Large number of potential attackers)

Παραμένει ίδιο **Threat Agent Factor (TAF):** (8 + 9 + 3 + 7) / 4 = 6.75

- **Ευκολία ανακάλυψης:** 4 (Moderately difficult)
- **Ευκολία εκμετάλλευσης:** 2 (Difficult) Η εφαρμογή ισχυρής κρυπτογράφησης και αυστηρών πολιτικών ασφαλείας θα μπορούσε να μειώσει σημαντικά την ευκολία εκμετάλλευσης από 5 σε 2.
- **Ευαισθητοποίηση:** 2 (Somewhat known)
- **Ανίχνευση εισβολής:** 3 (Limited logging and review)

Νέο **Vulnerability Factor (VF):** (4 + 2 + 2 + 3) / 4 = 2.75

Νέο **Likelihood Factor (LF):** (6.75 + 2.75) / 2 = 4.75

Impact Factor (IF):

- **Απώλεια εμπιστευτικότητας:** 5 Η χρήση ισχυρής κρυπτογράφησης θα μπορούσε να μειώσει την πιθανότητα απώλειας εμπιστευτικότητας από 9 σε 5.
- **Απώλεια ακεραιότητας:** 4 (Significant data corruption)
- **Απώλεια διαθεσιμότητας:** 7 (Extended downtime) Το ενισχυμένο cloud security μειώνει το downtime.
- **Απώλεια υπευθυνότητας:** 6 (Partial anonymity)

Νέο **Technical Impact Factor (TIF):** (5 + 4 + 7 + 6) / 4 = 5.5

- **Οικονομική ζημία:** 8 (Significant impact on annual profit)
- **Ζημία φήμης:** 9 (Brand damage)
- **Μη συμμόρφωση:** 7 (High profile violation)
- **Παραβίαση του απορρήτου:** 3 (One individual)

Παραμένει ίδιο **Business Impact Factor (BIF):** (8 + 9 + 7 + 3) / 4 = 6.75

Νέο **Impact Factor (IF):** (5.5 + 6.75) / 2 = 6.125

Νέο Overall Risk Severity: 4.75 * 6.125 = 29.59 (High)

5.5.8.3 Κίνδυνος αλλοίωσης ή απώλειας δεδομένων

Διορθωτικά Μέτρα:

- Εφαρμογή συστημάτων backup
- Χρήση λογισμικού ανίχνευσης και αποκατάστασης

Βελτιωμένη Εκτίμηση:

Likelihood Factor (LF):

- **Επίπεδο δεξιοτήτων:** 7 (Advanced technical skills required)
- **Κίνητρο:** 8 (High reward)
- **Ευκαιρία:** 4 (Requires significant resources)
- **Μέγεθος:** 6 (Moderate number of potential attackers)

Παραμένει ίδιο **Threat Agent Factor (TAF):** (7 + 8 + 4 + 6) / 4 = 6.25

- **Ευκολία ανακάλυψης:** 4 (Moderately difficult)
- **Ευκολία εκμετάλλευσης:** 2 (Difficult) Με την πλήρη εφαρμογή συστημάτων backup και ανίχνευσης, η ευκολία εκμετάλλευσης μπορεί να μειωθεί δραστικά από 5 σε 2.
- **Ευαισθητοποίηση:** 2 (Somewhat known)
- **Ανίχνευση εισβολής:** 3 (Limited logging and review)

Νέο **Vulnerability Factor (VF):** (4 + 2 + 2 + 3) / 4 = 2.75

Νέο **Likelihood Factor (LF):** (6.25 + 2.75) / 2 = 4.5

Impact Factor (IF):

- **Απώλεια εμπιστευτικότητας:** 6 (Significant data disclosure) Παραμένει σταθερή, καθώς οι μηχανισμοί προστασίας επικεντρώνονται περισσότερο στην ακεραιότητα.
- **Απώλεια ακεραιότητας:** 4 Το σύστημα backup μειώνει την πιθανότητα σημαντικής αλλοίωσης από 8 σε 4.
- **Απώλεια διαθεσιμότητας:** 6 (Extended downtime) Το backup σύστημα μειώνει το downtime.
- **Απώλεια υπευθυνότητας:** 5 (Partial anonymity)

Νέο **Technical Impact Factor (TIF):** (6 + 4 + 4 + 5) / 4 = 4.75

- **Οικονομική ζημία:** 7 (Moderate impact on annual profit)
- **Ζημία φήμης:** 7 (Moderate brand damage)
- **Μη συμμόρφωση:** 6 (Moderate violation)
- **Παραβίαση του απορρήτου:** 4 (Multiple individuals)

Παραμένει ίδιο **Business Impact Factor (BIF):** (7 + 7 + 6 + 4) / 4 = 6

Νέο **Impact Factor (IF):** (4.75 + 6) / 2 = 5.375

Νέο Overall Risk Severity: 4.5 * 5.375 = 24.19 (Medium)

5.5.8.4 Πολύπλοκες ή δύσχρηστες διεπαφές

Διορθωτικά Μέτρα:

- Βελτίωση σχεδιασμού διεπαφών
- Εκπαίδευση χρηστών

Βελτιωμένη Εκτίμηση:

Likelihood Factor (LF):

- **Επίπεδο δεξιοτήτων:** 6 (Moderate technical skills required)
- **Κίνητρο:** 7 (Moderate reward)
- **Ευκαιρία:** 5 (Common access to resources)
- **Μέγεθος:** 5 (Moderate number of potential attackers)

Παραμένει ίδιο **Threat Agent Factor (TAF):** (6 + 7 + 5 + 5) / 4 = 5.75

- **Ευκολία ανακάλυψης:** 3 (Difficult)
- **Ευκολία εκμετάλλευσης:** 2 (Difficult) Με τη βελτίωση της διεπαφής και την εκπαίδευση των χρηστών, η πιθανότητα λαθών μειώνεται δραστικά από 6 σε 2.
- **Ευαισθητοποίηση:** 2 (Somewhat known)
- **Ανίχνευση εισβολής:** 3 (Limited logging and review)

Νέο **Vulnerability Factor (VF):** (3 + 2 + 2 + 3) / 4 = 2.5

Νέο **Likelihood Factor (LF):** (5.75 + 2.5) / 2 = 4.125

Impact Factor (IF):

- **Απώλεια εμπιστευτικότητας:** 4 (Minimal data disclosure)
- **Απώλεια ακεραιότητας:** 3 (Minimal seriously corrupt data) Μειώνεται με την καλύτερη διεπαφή από 7 σε 3.
- **Απώλεια διαθεσιμότητας:** 3 Μειώνεται η πιθανότητα παρατεταμένου downtime από 6 σε 3.
- **Απώλεια υπευθυνότητας:** 5 (Partial anonymity)

Νέο **Technical Impact Factor (TIF):** (4 + 3 + 3 + 5) / 4 = 3.75

- **Οικονομική ζημία:** 6 (Moderate impact on annual profit)
- **Ζημία φήμης:** 6 (Moderate brand damage)
- **Μη συμμόρφωση:** 5 (Moderate violation)
- **Παραβίαση του απορρήτου:** 3 (One individual)

Παραμένει ίδιο **Business Impact Factor (BIF):** (6 + 6 + 5 + 3) / 4 = 5

Νέος **Impact Factor (IF):** (3.75 + 5) / 2 = 4.375

Νέο Overall Risk Severity: 4.125 * 4.375 = 18.05 (Low)

5.5.8.5 Σφάλματα λογισμικού ή υλικού

Διορθωτικά Μέτρα:

- Συχνές αναβαθμίσεις λογισμικού
- Τακτική συντήρηση εξοπλισμού

Βελτιωμένη Εκτίμηση:

Likelihood Factor (LF):

- **Επίπεδο δεξιοτήτων:** 6 (Moderate technical skills required)
- **Κίνητρο:** 8 (High reward)
- **Ευκαιρία:** 5 (Common access to resources)
- **Μέγεθος:** 5 (Moderate number of potential attackers)

Παραμένει ίδιο **Threat Agent Factor (TAF):** (6 + 8 + 5 + 5) / 4 = 6

- **Ευκολία ανακάλυψης:** 4 (Moderately difficult)
- **Ευκολία εκμετάλλευσης:** 2 Η τακτική συντήρηση και οι αναβαθμίσεις μειώνουν την πιθανότητα εμφάνισης σφαλμάτων από 5 σε 2.
- **Ευαισθητοποίηση:** 2 (Somewhat known)
- **Ανίχνευση εισβολής:** 3 (Limited logging and review)

Νέο **Vulnerability Factor (VF):** (4 + 2 + 2 + 3) / 4 = 2.75

Νέο **Likelihood Factor (LF):** (6 + 2.75) / 2 = 4.375

Impact Factor (IF):

- **Απώλεια εμπιστευτικότητας:** 3 (Minimal data disclosure)
- **Απώλεια ακεραιότητας:** 6 (Moderate data corruption)
- **Απώλεια διαθεσιμότητας:** 4 Μειώνεται λόγω της συντήρησης και της τακτικής αναβάθμισης από 7 σε 4.
- **Απώλεια υπευθυνότητας:** 5

Νέο **Technical Impact Factor (TIF):** (3 + 6 + 4 + 5) / 4 = 4.5

- **Οικονομική ζημία:** 6 (Moderate impact on annual profit)
- **Ζημία φήμης:** 7 (Moderate brand damage)
- **Μη συμμόρφωση:** 5 (Moderate violation)
- **Παραβίαση του απορρήτου:** 3 (One individual)

Παραμένει ίδιο **Business Impact Factor (BIF):** (6 + 7 + 5 + 3) / 4 = 5.25

Νέο **Impact Factor (IF):** (4.5 + 5.25) / 2 = 4.875

Νέο Overall Risk Severity: 4.375 * 4.875 = 21.34 (Low)

5.5.8.6 Κατάταξη κινδύνων μετα την εφαρμογη των διορθωτικών μέτρων

Με βάση τις νέες αξιολογήσεις και την ενίσχυση της αποτελεσματικότητας των διορθωτικών μέτρων, οι συνολικές εκτιμήσεις ρίσκου έχουν μειωθεί αισθητά, με αποτέλεσμα να φαίνεται ξεκάθαρα η αποτελεσματικότητα των μέτρων.

Τελική Κατάταξη:

1. **Κίνδυνος υποκλοπής δεδομένων από το cloud:** 29.59 (Medium)
2. **Κίνδυνος αλλοίωσης ή απώλειας δεδομένων:** 24.19 (Medium)
3. **Κλώνος ιστοσελίδας χωρίς κρυπτογράφηση:** 22.31 (Medium)
4. **Σφάλματα λογισμικού ή υλικού:** 21.34 (Low)
5. **Πολύπλοκες ή δύσχρηστες διεπαφές:** 18.05 (Low)

Με αυτή την ανάλυση, φαίνεται ότι τα διορθωτικά μέτρα έχουν σημαντικό αντίκτυπο στη μείωση των κινδύνων, όπως είναι λογικό να συμβαίνει μετά την εφαρμογή ισχυρών και αποτελεσματικών λύσεων.

Σενάριο Κινδύνου	Προηγούμενη Κατάταξη	Προηγούμενο Overall Risk Severity	Ενημερωμένη Κατάταξη	Ενημερωμένο Overall Risk Severity
Κίνδυνος υποκλοπής δεδομένων από το cloud	1	33.95 (High)	1	29.59 (High)
Κίνδυνος αλλοίωσης ή απώλειας δεδομένων	2	29.85 (High)	2	24.19 (Medium)
Κλώνος ιστοσελίδας χωρίς κρυπτογράφηση	3	25.55 (High)	3	22.31 (Medium)
Σφάλματα λογισμικού ή υλικού	4	24.94 (Medium)	4	21.34 (Low)
Πολύπλοκες ή δύσχρηστες διεπαφές	5	24.28 (Medium)	5	18.05 (Low)

5.6 Αποτελέσματα Εφαρμογής με Βάση τους Συντελεστές Στάθμισης

Με βάση τους συντελεστές στάθμισης της επιχείρησης που είδαμε παραπάνω, τα σενάρια ρίσκου μπορούν να ταξινομηθούν διαφορετικά αν τους λάβουμε υπόψιν μας. Όπως βλέπουμε στον παρακάτω πίνακα η σειρά αλλάζει την προτεραιότητα των κινδύνων, αν ως προτεραιότητα βάλουμε τους συντελεστές στάθμισης (1. Ασφάλεια Ασθενών, 2. Προστασία Δεδομένων, 3. Διαθεσιμότητα Υπηρεσιών, 4. Οικονομικές Επιπτώσεις, 5. Φήμη και Εμπιστοσύνη). Η σειρά αλλάζει διότι πλέον δεν ταξινομούμε τους κινδύνους με βάση το υψηλότερο ρίσκο αλλά με βάση για το ποιος παράγοντας είναι πιο σημαντικός για τον οργανισμό υγείας. Στην περίπτωση αυτή κατατάσσονται με βάση την ασφάλεια των ασθενών.

Σενάριο Κινδύνου	Ενημερωμένη Κατάταξη με βάση τις διορθωτικές ενέργειες	Ενημερωμένο Overall Risk Severity	Ενημερωμένη Κατάταξη με βάση του συντελεστές στάθμισης
Κίνδυνος υποκλοπής δεδομένων από το cloud	1	29.59 (High)	5
Κίνδυνος αλλοίωσης ή απώλειας δεδομένων	2	24.19 (Medium)	1
Κλώνος ιστοσελίδας χωρίς κρυπτογράφηση	3	22.31 (Medium)	2
Σφάλματα λογισμικού ή υλικού	4	21.34 (Low)	3
Πολύπλοκες ή δύσχρηστες διεπαφές	5	18.05 (Low)	4

5.7 Μελλοντικά Βήματα και Προοπτικές

Η τηλεχειρουργική, σε συνδυασμό με το Internet of Things (IoT), αποτελεί μια καινοτόμο προσέγγιση που μπορεί να φέρει επανάσταση στον τομέα της ιατρικής. Η ενότητα αυτή αναλύει τα κρίσιμα σημεία της τηλεχειρουργικής και παρουσιάζει τα μελλοντικά βήματα και τις προοπτικές αυτής της τεχνολογίας.

Μελλοντικά Βήματα

- **Βελτίωση της Ασφάλειας και της Αξιοπιστίας:**
  - Ένα από τα σημαντικότερα μελλοντικά βήματα στην τηλεχειρουργική είναι η βελτίωση της ασφάλειας και της αξιοπιστίας των συστημάτων. Η ανάπτυξη προηγμένων αλγορίθμων κρυπτογράφησης και η χρήση π.χ. τεχνολογιών blockchain μπορούν να διασφαλίσουν την ακεραιότητα των δεδομένων και να αποτρέψουν τις κυβερνοεπιθέσεις.
- **Ανάπτυξη Προηγμένων Ρομποτικών Συστημάτων:**
  - Τα ρομποτικά συστήματα που χρησιμοποιούνται στην τηλεχειρουργική συνεχώς εξελίσσονται. Η ανάπτυξη ρομπότ με αυξημένη ακρίβεια και ευελιξία, καθώς και η ενσωμάτωση τεχνητής νοημοσύνης (Artificial Intelligence - AI), μπορεί να βελτιώσει τις χειρουργικές επεμβάσεις και να μειώσει τα περιθώρια λάθους.
- **Ενίσχυση της Δικτύωσης και της Συνδεσιμότητας:**
  - Η χρήση δικτύων 5G και η ενίσχυση της συνδεσιμότητας των IoT συσκευών μπορούν να βελτιώσουν την ταχύτητα και την αξιοπιστία των τηλεχειρουργικών επεμβάσεων. Αυτό θα επιτρέψει την πραγματοποίηση πιο περίπλοκων επεμβάσεων από απόσταση, με μικρότερο κίνδυνο καθυστερήσεων και διακοπών. Ντετερμινιστικά δίκτυα με χρονική ευαισθησία όσον αφορά την λανθάνουσα καθυστέρηση θα βοηθήσουν την ανάπτυξη της τηλεχειρουργικής.
- **Εκπαίδευση και Κατάρτιση:**
  - Η εκπαίδευση και κατάρτιση των χειρουργών στη χρήση των νέων τεχνολογιών είναι κρίσιμη για την επιτυχία της τηλεχειρουργικής. Η ανάπτυξη προγραμμάτων εκπαίδευσης που χρησιμοποιούν εικονική πραγματικότητα (VR) και προσομοιώσεις μπορεί να βοηθήσει τους χειρουργούς να εξοικειωθούν με τα νέα συστήματα και να βελτιώσουν τις δεξιότητές τους.

Προοπτικές

- **Εξατομικευμένη Ιατρική:**
  - Η χρήση των δεδομένων που συλλέγονται από τις IoT συσκευές μπορεί να οδηγήσει σε εξατομικευμένες ιατρικές λύσεις. Οι χειρουργικές επεμβάσεις μπορούν να προσαρμόζονται στις συγκεκριμένες ανάγκες του κάθε ασθενούς, βελτιώνοντας τα αποτελέσματα και μειώνοντας τους κινδύνους.

- **Διεθνής Συνεργασία:**
    - Η τηλεχειρουργική μπορεί να διευκολύνει τη συνεργασία μεταξύ χειρουργών από διαφορετικές χώρες. Οι ειδικοί μπορούν να συνεργάζονται σε πραγματικό χρόνο, μοιραζόμενοι τις γνώσεις και τις εμπειρίες τους, και προσφέροντας τις καλύτερες δυνατές λύσεις για τους ασθενείς.
- **Πρόσβαση σε Απομακρυσμένες Περιοχές:**
    - Η τηλεχειρουργική μπορεί να προσφέρει πρόσβαση σε εξειδικευμένες ιατρικές υπηρεσίες σε απομακρυσμένες και υποανάπτυκτες περιοχές. Αυτό μπορεί να βελτιώσει την υγειονομική περίθαλψη σε περιοχές που δεν έχουν πρόσβαση σε εξειδικευμένους χειρουργούς και προηγμένα ιατρικά κέντρα.
- **Μείωση του Κόστους:**
    - Αν και η αρχική επένδυση για την ανάπτυξη και την εγκατάσταση των τηλεχειρουργικών συστημάτων μπορεί να είναι υψηλή, η μακροπρόθεσμη χρήση τους μπορεί να μειώσει το κόστος των χειρουργικών επεμβάσεων. Η μείωση των μετακινήσεων των χειρουργών και των ασθενών, καθώς και η αύξηση της αποδοτικότητας των επεμβάσεων, μπορεί να οδηγήσει σε σημαντική εξοικονόμηση πόρων.

Συμπέρασμα

Η τηλεχειρουργική σε συνδυασμό με το IoT προσφέρει τεράστιες δυνατότητες και προοπτικές για το μέλλον της ιατρικής. Η συνεχής ανάπτυξη και βελτίωση των τεχνολογιών αυτών μπορεί να οδηγήσει σε ασφαλέστερες, αποδοτικότερες και πιο προσιτές χειρουργικές επεμβάσεις, βελτιώνοντας την ποιότητα ζωής των ασθενών και καθιστώντας την υγειονομική περίθαλψη πιο προσιτή σε όλους.

6. Βιβλιογραφία

1. **Stephanie B. Baker, Wei Xiang, Ian Atkinson** (2017). *Internet of Things for Smart Healthcare: Technologies, Challenges, and Opportunities.* IEEE
2. **Daojing He, Ran Ye, Sammy Chan, Mohsen Guizani, Yanping Xu** (2018). *Privacy in the Internet of Things for Smart Healthcare.* IEEE
3. **Shariq Aziz Butt, Jorge Luis Diaz-Martinez, Tauseef Jamal, Arshad Ali, Emiro De-La-Hoz-Franco, Muhammad Shoaib** (2019). *IoT Smart Health Security Threats.* IEEE
4. **Prabha Sundaravadivel, Elias Kougianos, Saraju P. Mohanty, Madhavi K. Ganapathiraju** (2017). *Everything You Wanted to Know about Smart Health Care: Evaluating the Different Technologies and Components of the Internet of Things for Better Health.* IEEE
5. **Luca Catarinucci, Danilo de Donno, Luca Mainetti, Luca Palano, Luigi Patrono, Maria Laura Stefanizzi, Luciano Tarricone** (2015). *An IoT-Aware Architecture for Smart Healthcare Systems.* IEEE
6. **Chunxiao Li, Anand Raghunathan, Niraj K. Jha** (2011). Hijacking an insulin pump: Security attacks and defenses for a diabetes therapy system. IEEE
7. **Francesk Mulita, Georgios-IoannisVerras, Christos-Nikolaos Anagnostopoulos, Konstantinos Kotis** (2022). A Smarter Health through the Internet of Surgical Things (IoST). Sensors. MDPI
8. **Vipul Patel, Shady Saikali, Marcio Covas Moschovas, Ela Patel, Richard Satava, Prokar Dasgupta, Mischa Dohler, Justin W. Collins, David Albala, Jacques Marescaux** (2024). *Technical and Ethical Considerations in Telesurgery*. Journal of Robotic Surgery, 15(4), 635–641. Springer.
9. **Piccinini, A., Ricci, G., Sirignano, A., & Zoja, R.** (2022). *Telemedicine Applications in the Era of COVID-19: Telesurgery Issues*. International Journal of Environmental Research and Public Health, 19(1), 323. MDPI.
10. **Barba, P., Stramiello, J., Funk, E. K., Richter, F., Yip, M. C., & Orosco, R. K.** (2022). *Remote Telesurgery in Humans: A Systematic Review*. Surgical Endoscopy, 36(5), 2771–2777. Springer.
11. **Kostas Maliatsos, Costas Lambrinoudakis, Andreas Menegatos, Christos Lyvas, Athanasios Kanatas, Christos Kalloniatis (UPRC), Rosella Omana Mancilla (ENG), Pietro De Vito (STAM), Alkiviadis Giannakoulias (ED)** (2021) D2.2 Analysis NIS directive Cross domain threats and proof of concepts.
12. OWASP Risk Rating Methodology