ΟΙΚΟΝΟΜΙΚΟ ΠΑΝΕΠΙΣΤΗΜΙΟ ΑΘΗΝΩΝ

ATHENS UNIVERSITY OF ECONOMICS AND BUSINESS

ΤΜΉΜΑ ΠΛΗΡΟΦΟΡΙΚΉΣ

ΑΣΦΑΛΕΙΑ ΠΛΗΡΟΦΟΡΙΑΚΩΝ ΣΥΣΤΗΜΑΤΩΝ

ΕΡΓΑΣΙΑ ΕΑΡΙΝΟΥ ΕΞΑΜΗΝΟΥ 2023

ΘΕΜΑ ΕΡΓΑΣΙΑΣ: Μελέτη Περίπτωσης Ανάλυσης Επικινδυνότητας Πληροφοριακών Συστημάτων σε Μικροβιολογικό Εργαστήριο

ΠΑΡΟΥΣΙΑΣΗ ΣΧΕΔΙΟΥ ΑΣΦΑΛΕΙΑΣ

Microbial Mirth Mansion

ΜΕΛΗ ΟΜΑΔΑΣ ΕΡΓΑΣΙΑΣ:

1. **ΑΝΔΡΙΝΟΠΟΥΛΟΣ ΚΩΝΣΤΑΝΤΙΝΟΣ 3190009**

   p3190009@aueb.gr

2. **ΚΟΥΡΟΣ ΓΕΩΡΓΙΟΣ 3190095 p3190095@aueb.gr**

3. **ΤΣΑΜΗ ΚΩΝΣΤΑΝΤΙΝΑ 3190322 p3190322@aueb.gr**

ΠΕΡΙΕΧΟΜΕΝΑ ΕΡΓΑΣΙΑΣ

1. ΕΙΣΑΓΩΓΗ

Στόχος της εργασίας είναι να πραγματοποιηθεί μια πλήρης μελέτη περίπτωσης ασφαλείας στο μικροβιολογικό εργαστήριο Microbial Mirth Mansion. Παρακάτω αναπτύσσεται ένα σχέδιο ασφαλείας όπου περιγράφονται τα αγαθά της επιχείρησης και οι λειτουργίες τους, παρουσιάζονται απειλές και ευπάθειες τους και τρόποι αποφυγής και εντοπισμού των συγκεκριμένων κινδύνων.

1.1 Περιγραφή Εργασίας

Αρχικά, παρουσιάζεται η μεθοδολογία μελέτης ασφάλειας που θα ακολουθήσουμε. Στην συνέχεια, περιγράφουμε τις υποδομές και το πληροφοριακό σύστημα και κατηγοριοποιούμε τα αγαθά σε hardware, software, δεδομένα και διαδικασίες. Στην συνέχεια, γίνεται αποτίμηση των αγαθών της εγκατάστασης εντοπίζουμε τις απειλές και τις ευπάθειες των αγαθών και καταλήγουμε στα αποτελέσματα της αποτίμησης. Έπειτα, προτείνονται μέτρα ασφαλείας για τα εκάστοτε αγαθά και συνοψίζουμε με την ανάλυση των κρισιμότερων αποτελεσμάτων.

1.2 Δομή παραδοτέου

Στην ενότητα 2 παρουσιάζεται η μεθοδολογία που ακολουθήσαμε, στην ενότητα 3 περιγράφονται τα κυριότερα στοιχεία από την μελέτη και την ανάλυση επικινδυνότητας που εκπονήθηκε. Στην ενότητα 4, αναλύονται τα προτεινόμενα μέτρα ασφαλείας για κάθε αγαθό και στην ενότητα 5 γίνεται μια σύνοψη των πιο κρίσιμων αποτελεσμάτων.

2. ΜΕΘΟΔΟΛΟΓΙΑ ΜΕΛΕΤΗΣ ΑΣΦΑΛΕΙΑΣ

Για τη Διαχείριση Επικινδυνότητας του Microbial Mirth Mansion χρησιμοποιήθηκε παραμετροποιημένη μέθοδος του ISO27001K[1]. Επιλέχθηκε για τη συγκεκριμένη εργασία για τους εξής λόγους:

- Αποτελεί πρότυπη μέθοδο και έχει αναπτυχθεί με σκοπό να εφαρμοστεί στην εκπαίδευση.
- Συνοδεύεται από αυτοματοποιημένο εργαλείο *(excel tool)* που υποστηρίζει όλα τα στάδια της εφαρμογής.
- Καλύπτει όλες τις συνιστώσες της ασφάλειας των πληροφοριακών συστημάτων, περιλαμβανομένων του τεχνικού παράγοντα, των θεμάτων διαδικασιών και προσωπικού, της φυσικής ασφάλειας, της ασφάλειας δικτύων κλπ.

Στάδιο	Βήματα
1. Προσδιορισμός και αποτίμηση αγαθών *(identification and valuation of assets)*	*Βήμα 1*: Περιγραφή πληροφοριακών συστημάτων και εγκαταστάσεων *Βήμα 2:* Αποτίμηση αγαθών πληροφοριακών συστημάτων και εγκαταστάσεων *Βήμα 3:* Επιβεβαίωση και επικύρωση αποτίμησης
2. Ανάλυση επικινδυνότητας *(risk analysis)*	*Βήμα 1:* Προσδιορισμός απειλών που αφορούν κάθε Αγαθό (asset) *Βήμα 2:* Εκτίμηση απειλών (threat assessment) και αδυναμιών (vulnerability assessment) *Βήμα 3:* Υπολογισμός επικινδυνότητας συνδυασμών Αγαθό-Απειλή-Αδυναμία *Βήμα 4:* Επιβεβαίωση και επικύρωση βαθμού επικινδυνότητας
3. Διαχείριση επικινδυνότητας *(risk management)*	*Βήμα 1:* Προσδιορισμός προτεινόμενων αντιμέτρων *Βήμα 2:* Σχέδιο ασφάλειας πληροφοριακών συστημάτων και εγκαταστάσεων

Πίνακας 1: *Στάδια και βήματα της Ανάλυσης και Διαχείρισης επικινδυνότητας*

2.1 Περιγραφή Υποδομών & Πληροφοριακού Συστήματος

Στην ενότητα αυτή, καταγράφονται οι υποδομές και τα πληροφοριακά συστήματα του εντοπίστηκαν κατά την μελέτη περίπτωσης και Ανάλυσης Επικινδυνότητας Πληροφοριακών Συστημάτων στο Μικροβιολογικό Εργαστήριο Microbial Mirth Mansion.

[1] https://www.iso27001security.com/index.html

Τα αγαθά που αναφέρονται είναι τα εξής:

- Ένας Αιματολογικός αναλυτής
- Πέντε workstations με λογισμικό Windows 10 Pro
- Ένας μεγάλος εκτυπωτής
- Ένας μικρός εκτυπωτής
- Ένας Web Server
- Ένας Database Server
- Δύο Switches με λογισμικό Windows 7 Pro
- Ένα Router
- Ένα Firewall
- Ένα Laptop
- Το website του εργαστηρίου
- Δύο φάκελοι με έντυπα αρχεία ασθενών, υπαλλήλων και προμηθευτών
- Δεδομένα πελατών
- Δεδομένα υπαλλήλων

Πρόσθετα αγαθά

- Barcode scanner: Θα τοποθετηθεί στην είσοδο του Εργαστηρίου-Παρασκευαστηρίου ούτως ώστε μόνο εξουσιοδοτημένο προσωπικό να έχει είσοδο σε αυτό μέσω μιας προσωπικής κάρτας που θα αναγνωρίζει τον κάτοχο.
- Κάμερα: Θα τοποθετηθεί στον χώρο Αναμονής για γενική παρακολούθηση/ασφάλεια του χώρου.
- Alarm system: Θα τοποθετηθεί στον Βοηθητικό χώρο για ασφάλεια/προειδοποίηση από ανεπιθύμητους επισκέπτες.

2.2 Εξοπλισμός & Υλισμικό (hardware)

- Αιματολογικός αναλυτής
- Workstations
- Μικρός εκτυπωτής
- Μεγάλος εκτυπωτής
- Switches
- Router
- Laptop
- Web server
- Database server
- Κάμερα

- Alarm system
- Barcode scanner

2.3 Λογισμικό και εφαρμογές

- Firewall
- Windows 7 Pro Software
- Windows 10 Pro Software
- Το website

2.4 Δίκτυο

Το δίκτυο του εργαστηρίου αποτελείται από 2 υποδίκτυα όσα είναι και τα switches. Το ένα υποδίκτυο είναι του Εργαστηρίου-Παρασκευαστηρίου, του χώρου λήψης δειγμάτων και της αίθουσας αναμονής, το οποίο συνδέεται μέσω ενός router με το switch του δεύτερου υποδίκτυο το οποίο αποτελείται από τον βοηθητικό χώρο.

2.5 Δεδομένα

- Δύο φάκελοι με έντυπα αρχεία ασθενών, υπαλλήλων και προμηθευτών.
- Δεδομένα πελατών.
- Δεδομένα υπαλλήλων.

2.6 Διαδικασίες

Γενικά, μια διαδικασία αναφέρεται σε μια σειρά βημάτων ή ενεργειών που ακολουθούνται με συγκεκριμένη σειρά για την εκτέλεση μιας συγκεκριμένης εργασίας ή την επίτευξη ενός επιθυμητού αποτελέσματος. Στο σύστημα μας οι διαδικασίες είναι οι εξής:

- Χρήση barcode για την ταυτοποίηση δειγμάτων.
- Καταχώρηση αναλύσεων και αποτελεσμάτων στο πληροφοριακό σύστημα.
- Εκτύπωση αποτελεσμάτων ασθενών.
- Ηλεκτρονική διανομή αποτελεσμάτων και αναφορών.
- Στατιστική ανάλυση αποτελεσμάτων και αναφορών.
- Λήψη αντιγράφων ασφαλείας εβδομαδιαία.
- Αποστολή αποτελεσμάτων εξετάσεων/αναλύσεων με fax ή email στον ασθενή ή στον ιατρό του.
- Σύνδεση Ιατρού-Ασθενή στον διαδικτυακό ιστότοπο.
- Λήψη αποτελεσμάτων από τον διαδικτυακό ιστότοπο του μικροβιολογικού εργαστηρίου.
- Διαμοιρασμός προσωπικών δεδομένων ασθενών με συνεργαζόμενους παρόχους υπηρεσιών.

3. ΑΠΟΤΙΜΗΣΗ ΑΓΑΘΩΝ ΤΗΣ ΕΓΚΑΤΑΣΤΑΣΗΣ

Η αποτίμηση των αγαθών στην ασφάλεια των πληροφοριών είναι ζωτικής σημασίας για την αποτελεσματική διαχείριση των κινδύνων και βοηθά τους οργανισμούς να ιεραρχούν τις επενδύσεις τους στην ασφάλεια και να κατανέμουν τους πόρους πιο αποτελεσματικά. Βοηθά επίσης να διασφαλιστεί ότι τα πιο κρίσιμα αγαθά του οργανισμού προστατεύονται επαρκώς έναντι των απειλών ασφαλείας.

3.1 Αγαθά που εντοπίστηκαν

Τα αγαθά που εντοπίστηκαν και αξίζει να προστατευτούν είναι τα εξής:

- **Web server:** εξυπηρετεί αιτήματα χρηστών που επισκέπτονται την ιστοσελίδα του εργαστηρίου.
- **Database Server**: εκεί αποθηκεύονται όλα τα δεδομένα του εργαστηρίου.
- **Customer Data**: περιλαμβάνουν τα προσωπικά δεδομένα των όλων πελατών του μικροβιολογικού εργαστηρίου.
- **Employee Data**: περιλαμβάνουν τα προσωπικά δεδομένα όλων των εργαζομένων του μικροβιολογικού εργαστηρίου.
- **Workstations:** ισχυροί σταθεροί υπολογιστές σχεδιασμένοι για απαιτητικές εφαρμογές.
- **Laptop:** Ο προσωπικός υπολογιστής του ιατρού.
- **Windows 7 Pro:** λειτουργικό σύστημα που αναπτύχθηκε από τη Microsoft
- **Windows 10 Pro:** λειτουργικό σύστημα που αναπτύχθηκε από τη Microsoft
- **Website:** ο διαδικτυακός ιστότοπος του εργαστηρίου.
- **Αιματολογικός αναλυτής:** χρησιμοποιείται για την καταμέτρηση και την αναγνώριση των κυττάρων του αίματος σε υψηλή ταχύτητα με ακρίβεια.
- **Switches:** είναι μια συσκευές δικτύου που συνδέουν συσκευές μεταξύ τους σε ένα τοπικό δίκτυο (LAN).
- **Αρχείο Προμηθευτών και Υπαλλήλων:** φυσικά αρχεία σε ερμάρια κρεμαστών φακέλων.
- **Αρχείο ασθενών/πελατών:** φυσικά αρχεία σε ερμάρια κρεμαστών φακέλων.
- **Router:** συνδέει πολλά δίκτυα μαζί.
- **Printer:** Συσκευή που μετατρέπει ηλεκτρονικά δεδομένα σε έντυπη μορφή.
- **Page wide printer:** Συσκευή που μετατρέπει ηλεκτρονικά δεδομένα σε έντυπη μορφή πιο γρήγορα από έναν μικρό εκτυπωτή και χρησιμοποιείται συνήθως σε μεγάλες εγκαταστάσεις και γραφεία.

- **Firewall:** Τείχος προστασίας ανάμεσα σε υπολογιστές ή δίκτυο και Διαδικτύου, επιτρέπει ή απορρίπτει πακέτα δεδομένων που περνούν από ένα δίκτυο υπολογιστών σε ένα άλλο.
- **Κάμερα:** Παρακολούθηση σημαντικών χώρων του μικροβιολογικού εργαστηρίου.
- **Alarm system:** Σύστημα συναγερμού για την αποτροπή κλοπής/καταστροφής περιουσιακών στοιχείων.
- **Barcode scanner:** Συσκευή που τοποθετείται στην είσοδο ενός χώρου για την περιορισμένη και ελεγχόμενη είσοδο σε αυτόν.

3.2 Απειλές που εντοπίστηκαν

ASSETS	THREATS
Web server	• Execute arbitrary code specially via crafted packets • Malware Infections • DDoS Attacks • Data Theft
Database server	• Data breaches • Ransomware attacks • Man-in-the-middle attack
Customer Data	• Data Loss • Data Theft • Data Misuse
Employee Data	• Identity Theft • Data Misuse
Workstations	• System overheat • USB drop attacks
Laptop	• Unauthorized Physical Access • USB drop attacks • Easy to be stolen

Windows 7 pro	• Ransomware attack • Reverse shell attack
Windows 10 pro	• Zero-day attacks • Remote code execution • Viruses
Website	• Phishing attacks • XXS attacks
Haematology analyzer	• Insider threats (damage to the software or data) • Unauthorized access (changes to test results) • Data loss
Switches	• ARP spoofing • MAC flooding
Router	• Unauthorized access
IP Camera	• Malware attacks
Barcode Scanner	• Can be infected by malicious hardware/software
Alarm system	• Physical tampering • Cyber Attack
Supplier's and employees' files	• Files can be stolen by malicious person
Customers' files	• Insider can get access to customer files
Page Wide Printer	• Remote Code Execution • Man-in-the-middle Attack
Printer	• Reconfigure, reset and denial of service from unauthorized user
Firewall	• Rules not appropriately configured

3.3 Ευπάθειες που εντοπίστηκαν

ASSETS	VULNERABILITIES
Web server	• Remote Code Execution/Buffer overflow attack • No HTTPS • Unpatched software • Insecure configuration/No firewall
Database server	• Human Factor(employees can accidentally expose sensitive data or fall for phishing attacks) • Outdated Software/OS • Unencrypted Communications
Customer Data	• Human Error/Hardware Failure • No Encryption • Not complying with GDPR/No security awareness
Employee Data	• No Encryption • Not complying with GDPR/No security awareness
Workstations	• No USB access control • No cooling system
Laptop	• No USB access control • Weak passwords • No Physical security
Windows 7 pro	• Lack of security updates • Outdated Software • Wrong security measures
Windows 10 pro	• Wrong Security Measures • Human error
Website	• No security awareness • No Input Validation

Hematology analyzer	• No physical security • No firewall
Switches	• Not regularly updating switch firmware • Not implementing strong access control
Router	• Not changing default login credentials
Camera	• Weak authentication
Barcode scanner	• Vulnerable to counterfeiting
Alarm system	• Insider threats • Outdated software
Supplier and employees file	• Files kept in not secured place in easy accessible library without lockers
Customer file	• Files kept in not secured place in easy accessible library without lockers
Page wide printer	• Old firmware
Printer	• Outdated software
Firewall	• Data leakage

3.4 Αποτελέσματα αποτίμησης

Με βάση τα δεδομένα που παρουσιάζουν την αποτίμηση των αγαθών, παρατηρείται ότι οι βαθμολογίες (RPN) που έχουν ανατεθεί στα διάφορα αγαθά έχουν αρκετά μεγάλη απόκλιση μεταξύ τους. Συγκεκριμένα, μπορούμε να διαπιστώσουμε ότι η εγκατάσταση έχει υψηλό βαθμό ευπάθειας σε θέματα υποδομής και ανθρώπινου παράγοντα, που αυξάνουν τον κίνδυνο απώλειας δεδομένων και παραβίασης της ασφάλειας του συστήματος. Συνάμα, η απουσία εκπαίδευσης των εργαζομένων και η έλλειψη αποτελεσματικής πολιτικής ασφαλείας είναι παράγοντες που μπορούν να αυξήσουν τον κίνδυνο ασφαλείας. Η χρήση του συστήματος αξιολόγησης κινδύνου RPN συμβάλλει στη κατανόηση των σημαντικότερων σημείων κινδύνου έτσι ώστε να λάβουμε κατάλληλα μέτρα για να τα αντιμετωπίσουμε. Ωστόσο, είναι ζωτικής σημασίας να αναφερθεί πως η αξιολόγηση των κινδύνων και η εφαρμογή μέτρων πρόληψης και εντοπισμού μπορεί να είναι υποκειμενική και να επηρεάζεται από ποικίλους παράγοντες, όπως η γνώση και η εμπειρία των αξιολογητών. Ως προς την συμπλήρωση του CIA (Confidentiality-Integrity-Availability) ακολουθήσαμε ορισμένα κριτήρια ώστε να συμπληρώσουμε τις τιμές (High, Medium, Low) με την περισσότερη δυνατή ορθότητα για κάθε αγαθό. Συγκεκριμένα, για την εμπιστευτικότητα, όταν διαπιστωνόταν προσπέλαση των δεδομένων των ασθενών, υπαλλήλων, ιατρών από οποιονδήποτε εκτός του προσωπικού του μικροβιολογικού εργαστηρίου οριζόταν High (π.χ. USB drop attacks at workstations). Για την ακεραιότητα, όταν είχαμε παραποίηση, διαγραφή ή και εισαγωγή πλαστών ή εσφαλμένων δεδομένων από κακόβουλους μη εξουσιοδοτημένους χρήστες, οριζόταν ως High (π.χ. Reverse Shell Attacks due to outdated Windows 7 pro OS system. Και για την διαθεσιμότητα, την ορίζαμε High αν τα δεδομένα έπαυαν να είναι προσβάσιμα (π.χ. data theft/misuse due to non-encrypted customer data) και Medium εάν υπήρχε μια προσωρινή αδυναμία πρόσβασης (π.χ. phishing website attacks). Επιπρόσθετα, τα μέτρα πρόληψης που προτείνονται για κάθε απειλή-ευπάθεια αγαθού αποτελούν την καλύτερη και αποτελεσματικότερη λύση κατά την προσωπική μας γνώμη, χωρίς αυτό να σημαίνει ότι η κάθε πρόληψη επιλύει στο 100% το πρόβλημα καθώς και ότι δεν είναι η μοναδική πρόληψη που μπορούμε να εφαρμόσουμε στην εκάστοτε απειλή-ευπάθεια αγαθού. Τέλος πρέπει να τονίσουμε πως αποφασίστηκε να στοχοποιηθεί το 8% των κινδύνων που έχουν εντοπιστεί. Συνεπώς κάθε RPN μεγαλύτερο από 80 (= 8% του 1000-max RPN value) απαιτεί αναθεώρηση και πιθανόν βελτιώσεις ελέγχου και θεωρείται ως κίνδυνος υψηλής προτεραιότητας αντιμετώπισης.

4. ΠΡΟΤΕΙΝΟΜΕΝΑ ΜΕΤΡΑ ΑΣΦΑΛΕΙΑΣ

Τα προτεινόμενα Μέτρα Προστασίας εντάσσονται σε έντεκα (11) γενικές κατηγορίες:

1. Προσωπικό – Προστασία Διαδικασιών Προσωπικού
2. Ταυτοποίηση και αυθεντικοποίηση
3. Έλεγχος προσπέλασης και χρήσης πόρων
4. Διαχείριση εμπιστευτικών δεδομένων
5. Προστασία από τη χρήση υπηρεσιών από τρίτους
6. Προστασία λογισμικού
7. Διαχείριση ασφάλειας δικτύου
8. Προστασία από ιομορφικό λογισμικό
9. Ασφαλής χρήση διαδικτυακών υπηρεσιών
10. Ασφάλεια εξοπλισμού
11. Φυσική ασφάλεια κτιριακής εγκατάστασης

4.1. Προσωπικό – Προστασία Διαδικασιών Προσωπικού

Αγαθό	Μέτρα ασφαλείας
Employee Data	Εσωτερικοί κανόνες υπαλλήλων, προστασία δεδομένων με κωδικό πρόσβασης και κρυπτογράφηση ευαίσθητων δεδομένων
Αρχείο Υπαλλήλων & Προμηθευτών	Ο/Η γραμματέας παρακολουθεί και αποτρέπει την κακόβουλη πρόσβαση σε αρχεία, και κλειδαριές στα ερμάρια

4.2. Ταυτοποίηση και αυθεντικοποίηση

Αγαθό	Μέτρα ασφαλείας
Laptop	Χρήση και συχνή αλλαγή περίπλοκων κωδικών
Barcode Scanner	Διατήρηση ενημερωμένου υλικολογισμικού

Router	Αλλαγή default κωδικών/Γενική χρήση ισχυρού ελέγχου ταυτότητας
Κάμερα	Χρήση και συχνή αλλαγή περίπλοκων κωδικών

4.3. Έλεγχος προσπέλασης και χρήσης πόρων

Αγαθό	Μέτρα ασφάλειας
Barcode Scanner	Διατήρηση του firmware ενημερωμένου
Laptop	Χρήση περίπλοκων κωδικών και συχνή αλλαγή τους, ύπαρξη φυσικής ασφάλειας

4.4. Διαχείριση εμπιστευτικών δεδομένων

Αγαθό	Μέτρα ασφαλείας
Employee/Customer Data	Κρυπτογράφηση Δεδομένων
Database Server	Χρησιμοποιήση ασφαλών μεθόδων επικοινωνιών και συχνά Back ups

4.5 Προστασία από τη χρήση υπηρεσιών από τρίτους

Αγαθό	Μέτρα ασφαλείας
Laptop, Workstation,Hematology analyzer	Χρήση ισχυρών κωδικών και ανανέωσή τους τακτικά
Printer, Page wide printer	΄Υπαρξη φυσικής ασφάλειας
Web Server	Χρήση ισχυρών/καλών πρακτικών προγραμματισμού

4.6 Προστασία λογισμικού

Αγαθό	Μέτρα ασφαλείας
Firewall	Τακτικά updates
Web Server	Χρήση ισχυρών/τακτικών μεθόδων προγραμματισμού
Windows 10 pro	Χρήση Windows Firewall, εφαρμογή ελέγχου προσπέλασης
Barcode scanner	Διατήρηση ενημερωμένου υλικολογισμικού
Alarm system	Συνεχή ενημέρωση λογισμικού

4.7 Διαχείριση ασφάλειας δικτύου

Αγαθό	Μέτρα ασφαλείας
Firewall	Περιορισμός της εισερχόμενης κίνησης μόνο σε εγκεκριμένες υπηρεσίες
Router, Switches	Αλλαγή των default password και ανανέωση τους κατά διαστήματα, περιορισμός των MAC addresses που έχουν πρόσβαση στο δίκτυο
Web server	Χρήση HTTPS, χρήση firewall
Database server	Χρήση κρυπτογράφησης στις επικοινωνίες

4.8 Προστασία από ιομορφικό λογισμικό

Αγαθό	Μέτρα ασφαλείας
Web server	Updates software, χρήση firewall, χρήση ισχυρών/καλών προγραμματιστικών τεχνικών
Database server	Κρυπτογράφηση επικοινωνιών, τακτικά backup

Workstations,Laptop	USB blocker
Windows 7, 10 pro	Windows firewall, software up to date
Website	HTTPS
Barcode scanner	Keep firmware up to date

4.9 Ασφαλής χρήση διαδικτυακών υπηρεσιών

Αγαθό	Μέτρα ασφαλείας
Website	Phishing attacks, XSS attacks

4.10 Ασφάλεια εξοπλισμού

Αγαθό	Μέτρα ασφάλειας
Workstation	Cooling system, USB blocker
Laptop	΄Υπαρξη φυσικής επίβλεψης, τακτικά backup στα δεδομένα,ασφαλιστική κάλυψη
Printer	Λογισμικό up to date
Page wide printer	Firmware up to date

4.11 Φυσική ασφάλεια κτιριακής εγκατάστασης

Αγαθό	Μέτρα ασφαλείας
Φυσικό αρχείο ασθενών, Αρχείο Υπαλλήλων & Προμηθευτών	Χρήση κλειδαριών στα ερμάρια
Printer	Λογισμικό up to date
Page wide printer	Firmware up to date
Laptop, Workstations,Αιματολογικός αναλυτής	Φύλαξη του κτιρίου και συναγερμός, ασφαλιστική κάλυψη

5 ΣΥΝΟΨΗ ΚΡΙΣΙΜΩΝ ΑΠΟΤΕΛΕΣΜΑΤΩΝ

- **Router:**

  Ο router είναι μια συσκευή δικτύου που προωθεί πακέτα δεδομένων μεταξύ δικτύων υπολογιστών. Αποτελεί ζωτικό μέρος κάθε δικτύου και η μη εξουσιοδοτημένη πρόσβαση μπορεί να έχει σοβαρές συνέπειες στην επιχείρηση. Ένας από τους μεγαλύτερους κινδύνους της μη εξουσιοδοτημένης πρόσβασης σε έναν router είναι ότι μπορεί να επιτρέψει σε έναν επιτιθέμενο να αναλάβει τον έλεγχο του δικτύου. Αυτό θα μπορούσε να επιτρέψει στον επιτιθέμενο να κλέψει δεδομένα, να διακόψει την κυκλοφορία του δικτύου ή ακόμη και να εκτελέσει DDoS attack. Επίσης, μπορεί να επιτρέψει στον εισβολέα να αποκτήσει πρόσβαση στις συσκευές του δικτύου με αποτέλεσμα να μπορεί να υποκλέψει προσωπικές πληροφορίες και να εγκαταστήσει κακόβουλο λογισμικό. Εκτός από αυτούς τους κινδύνους, η μη εξουσιοδοτημένη πρόσβαση μπορεί επίσης να οδηγήσει σε απώλεια παραγωγικότητας και εσόδων της επιχείρησης. Εάν διακοπεί η λειτουργία του δικτύου ενδέχεται να χαθούν χρήματα λόγω διακοπής λειτουργίας του ή απώλειας δεδομένων των πελατών, υπαλλήλων κλπ. Για να αποτραπεί η μη εξουσιοδοτημένη πρόσβαση είναι σημαντικό να γίνει αλλαγή των default credentials και η χρήση ισχυρών κωδικών πρόσβασης. Τέλος, θα πρέπει να διατηρείτε ενημερωμένο το υλικολογισμικό του router γιατί πολλές φορές περιλαμβάνουν επιδιορθώσεις που μπορούν να βοηθήσουν στην προστασία του router από γνωστές ευπάθειες.

- **Αιματολογικός Αναλυτής**:

  Ο αιματολογικός αναλυτής είναι μια ιατρική συσκευή που χρησιμοποιείται για την καταμέτρηση και τον προσδιορισμό των κυττάρων του αίματος. Αποτελεί αναγκαίο αγαθό της εγκατάστασης μας. Χωρίς φυσική ασφάλεια κινδυνεύει να παραβιαστεί ή και να κλαπεί. Αυτό θα μπορούσε να έχει σοβαρές συνέπειες καθώς θα μπορούσε να οδηγήσει σε απώλεια δεδομένων ασθενών ή και σε εξάπλωση ασθενειών. Άλλη μια απειλή, είναι οι εργαζόμενοι με κακόβουλο κίνητρο οι οποίοι θα μπορούσαν να προκαλέσουν ζημιά στο λογισμικό, τα δεδομένα και το υλικό. Η προστασία περιλαμβάνει την εγκατάσταση καμερών ασφαλείας και συναγερμών. Επίσης, είναι σημαντικό να περιορίζεται η πρόσβαση συσκευής μονο στους εξουσιοδοτημένος χρήστες. Εκτός από την φυσική ασφάλεια, μπορούν να εφαρμοστούν μέτρα ασφάλειας και για την προστασία των δεδομένων του. Αυτό μπορεί να περιλαμβάνει την εγκατάσταση αντιικού λογισμικού, firewalls, την κρυπτογράφηση των δεδομένων και την τακτική έγκαιρη ενημέρωση του λογισμικού.

- **Database Server:**

Ο database server έχει αποθηκευμένα τα δεδομένα των πελατών και των υπαλλήλων. Για αυτό αποτελεί πολύτιμο αγαθό της εταιρείας το οποίο πρέπει να προστατευθεί από διάφορες απειλές που μπορεί να προκύψουν από διάφορες ευπάθειες. Ένας από τους μεγαλύτερους κινδύνους με τους οποίους μπορούμε να έρθουμε αντιμέτωποι είναι η πιθανότητα του Data breach (παραβίαση δεδομένων). Τα Data Breach, είναι ένα περιστατικό ασφαλείας κατα το οποίο ευαίσθητα/εμπιστευτικά δεδομένα παραβιάζονται από μη εξουσιοδοτημένα άτομα. Το Data Breach μπορεί να προκληθεί από πολλούς παράγοντες όπως το ανθρώπινο λάθος και απο το social engineering. Αυτό θα μπορούσε να οδηγήσει στην κλοπή ευαίσθητων δεδομένων, τα οποία θα έχουν σοβαρές συνέπειες στην επιχείρηση και στους ασθενείς. Ακόμα ένας κίνδυνος είναι η πιθανότητα για malware infections τα οποία μπορούν να επηρεάσουν το σύστημα και να υποκλέψουν δεδομένα. Για να προστατεύσουμε την βάση δεδομένων, ένας τρόπος είναι η χρήση ισχυρών περίπλοκων κωδικών, η συνεχής και έγκαιρη του λογισμικού για security patches έναντι γνωστών ευπαθειών. Επίσης, τα δεδομένα θα πρέπει να είναι κρυπτογραφημένα και να έχουν πρόσβαση σε αυτά μόνο εξουσιοδοτημένοι.

ΒΙΒΛΙΟΓΡΑΦΙΑ

- https://www.upguard.com/blog/top-20-critical-windows-server-2008-vulnerabilities-and-remediation-tips
- https://www.cisco.com/c/en/us/products/collateral/routers/887-integrated-services-router-isr/data_sheet_c78_459542.html
- https://stack.watch/product/microsoft/windows-server-2016/
- https://www.kaspersky.com/resource-center/threats/ransomware-attacks-and-types
- https://en.wikipedia.org/wiki/Man-in-the-middle_attack
- https://www.trellix.com/en-us/security-awareness/cybersecurity/what-is-a-zero-day-exploit.html
- https://www.csoonline.com/article/3269028/what-is-xss-cross-site-scripting-attacks-explained.html
- https://en.wikipedia.org/wiki/Phishing
- https://en.wikipedia.org/wiki/Denial-of-service_attack
- https://www.geeksforgeeks.org/how-to-prevent-mac-flooding/
- https://www.varonis.com/blog/arp-poisoning
- https://www.makeuseof.com/what-is-a-usb-drop-attack/
- https://www.i-scoop.eu/cybersecurity/cia-confidentiality-integrity-availability-security/