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

Biolab Patissia


**ΜΕΛΗ ΟΜΑΔΑΣ ΕΡΓΑΣΙΑΣ:**

1. **Πέτρος Χάνας + 3170173 + p3170173@aueb.gr**
2. **Παύλος Τσικρικάς + 3200276 + p3200276@aueb.gr**
3. **Κωνσταντίνος Κωνστάντιος + 3170085 + p3170085@aueb.gr**

# ΠΕΡΙΕΧΟΜΕΝΑ ΕΡΓΑΣΙΑΣ

# 1. ΕΙΣΑΓΩΓΗ

Η προκείμενη εργασία πραγματεύεται την ανάλυση επικινδυνότητας πληροφοριακού συστήματος σε ένα μικροβιολογικό εργαστήριο. Σκοπός είναι η κατηγοριοποίηση και η επιμέρους ανάλυση των αγαθών και η επιπρόσθετη ανάλυση των ευπαθειών αλλά και οιονεί απειλών που υπάρχουν στο σύστημα. Αυτό προϋποθέτει την ορθολογική αξιολόγηση των αδυναμιών του συστήματος συναρτώμενη με ρεαλιστικές συνθήκες αξιολόγησης αλλά και παραμετροποίηση ανάλογα με τα διεθνή πρότυπα ασφάλειας πληροφοριακών συστημάτων. Εν κατακλείδι, θα παρουσιάσουμε και τρόπους αντιμετώπισης των άνωθι ευπαθειών και απειλών τόσο εξωτερικών όσο και εσωτερικών και ως απόρροια θα εκπονηθεί μια ολοκληρωμένη πρόταση ενός σχεδίου ασφαλείας.

## 1.1 Περιγραφή Εργασίας

Η μεθοδολογία που θα ακολουθηθεί στην μελέτη δομείται βαθμωτά ως εξής:

- Προσδιορισμός και αποτίμηση αγαθών (Asset): Σε αυτό το πρωταρχικό στάδιο θα απαριθμηθούν και θα κατηγοριοποιηθούν τα αγαθά που υπάρχουν εντός του συστήματος.
- Εντοπισμός και ταξινόμηση ευπαθειών (Vulnerability classification): Αυτό είναι το σημείο στο οποίο θα ψάξουμε για να βρούμε ευπάθειες του συστήματος. Οι ευπάθειες θα καταταγούν ανάλογα με την βαρύτητά τους.
- Εντοπισμός και αξιολόγηση απειλών (Threat Assessment): Εδώ θα ταξινομηθούν αρθρωτά οι απειλές κατά φθίνουσα σειρά σημαντικότητας βάσει προτύπου $ISO27001k$.
- Ανάλυση και Εκτίμηση Επιπτώσεων (Impact Analysis & Assessment): Σε αυτό το σημείο θα προβούμε σε ανάλυση της επίπτωσης που η εκάστοτε απειλή θα είχε στο σύστημα εάν την αφήναμε να εκτυλιχθεί εντός αυτού.
- Παρουσίαση Μέσων Προστασίας (Countermeasure/ Safeguard): Σκοπός μας είναι να παρουσιάσουμε μέτρα που θα αντιμετωπίζουν τις ευπάθειες του συστήματος και θα περιορίζουν τις επιπτώσεις των απειλών.
- Υπολογισμός Επικινδυνότητας(Risk Assessment): Εν τέλει, θα παραχθεί ένα ευρετήριο με ταξινομημένους τους υφιστάμενους κινδύνους ανά σειρά σημαντικότητας βάσει των προαναφερθέντων κριτηρίων αξιολόγησης.

## 1.2 Δομή παραδοτέου

| ΕΝΟΤΗΤΑ ΕΡΓΑΣΙΑΣ | ΠΕΡΙΓΡΑΦΗ |
|---|---|
| **1. ΕΙΣΑΓΩΓΗ** | Μια πρώτη ματιά στο αντικείμενο της μελέτης. |
| **2. ΜΕΘΟΔΟΛΟΓΙΑ ΜΕΛΕΤΗΣ ΑΣΦΑΛΕΙΑΣ** | Σε αυτήν την ενότητα ακολουθούμε τα κυριότερα βήματα ανάλυσης και περιγράφουμε τα επιμέρους ζητήματα και συστατικά που απαρτίζουν το σύστημα στην εν λόγω μελέτη όπως την περιγραφή υποδομών, την καταγραφή λογισμικού και υλισμικού αλλα και των αντίστοιχων εφαρμογών. Επίσης, αναφερόμαστε σε δικτυακές υποδομές και διαδικασίες. |
| **3. ΑΠΟΤΙΜΗΣΗ ΑΓΑΘΩΝ ΤΗΣ ΕΓΚΑΤΑΣΤΑΣΗΣ** | Ανάλυση των αγαθών που εντοπίστηκαν στο σύστημα και όλων των ευπαθειών και απειλών που εντοπίστηκαν και παρουσίαση των αποτελεσμάτων της διαδικασίας. |
| **4. ΠΡΟΤΕΙΝΟΜΕΝΑ ΜΕΤΡΑ ΑΣΦΑΛΕΙΑΣ** | Παρουσίαση μέτρων ασφαλείας για την αντιμετώπιση των ευπαθειών που εντοπίσαμε στα προηγούμενα στάδια της μελέτης, αλλά και την ελάττωση των συνεπειών που μπορούν να παρουσιαστούν από αυτές. |
| **5. ΣΥΝΟΨΗ ΚΡΙΣΙΜΩΝ ΑΠΟΤΕΛΕΣΜΑΤΩΝ** | Το τελικό πόρισμα της μελέτης μαζί με τα κρίσιμα αποτελέσματα που βρέθηκαν. |

# 2. ΜΕΘΟΔΟΛΟΓΙΑ ΜΕΛΕΤΗΣ ΑΣΦΑΛΕΙΑΣ

Για τη Διαχείριση Επικινδυνότητας του Biolab Patissia 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<br>*Βήμα 2:* Αποτίμηση αγαθών πληροφοριακών συστημάτων και εγκαταστάσεων<br>*Βήμα 3:* Επιβεβαίωση και επικύρωση αποτίμησης |
| **2.** Ανάλυση επικινδυνότητας *(risk analysis)* | *Βήμα 1:* Προσδιορισμός απειλών που αφορούν κάθε Αγαθό (asset)<br>*Βήμα 2:* Εκτίμηση απειλών (threat assessment) και αδυναμιών (vulnerability assessment)<br>*Βήμα 3:* Υπολογισμός επικινδυνότητας συνδυασμών Αγαθό-Απειλή-Αδυναμία<br>*Βήμα 4:* Επιβεβαίωση και επικύρωση βαθμού επικινδυνότητας |
| **3.** Διαχείριση επικινδυνότητας *(risk management)* | *Βήμα 1:* Προσδιορισμός προτεινόμενων αντιμέτρων<br>*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 Biolab Patissia.

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

## 2.2 Εξοπλισμός & Υλισμικό (hardware)

**Αιματολογικός Αναλυτής (XS-1000i / A-001**): είναι υπεύθυνος για την αξιολόγηση και ανάλυση δειγμάτων αίματος για τη διάγνωση και τη θεραπεία ασθενειών. Κάποια από τα καθήκοντά του περιλαμβάνουν: εξέταση δειγμάτων αίματος και ανάλυση των συστατικών τους, ανίχνευση και αξιολόγηση ανωμαλιών στα δείγματα αίματος κ.ο.κ..(Εργαστήριο-Παρασκευαστήριο)

**Backup generator (A-023 - added asset):** Το εργαστήριο είναι εξοπλισμένο με μία παλιά γεννήτρια ηλεκτρικού ρεύματος σε περίπτωση διακοπής. Η γεννήτρια βρίσκεται στον αύλειο χώρο ενώ συντηρείται τακτικά. Παρόλα αυτά το μοντέλο είναι αρκετά παλιό και ξεπερασμένο.

*Λόγος επιλογής asset*: Θεωρούμε ότι το εργαστήριο είναι ήδη εξοπλισμένο με μια παλιά γεννήτρια έτσι ώστε να αντιμετωπιστεί μια διακοπή ρεύματος στο μικροβιολογικό και να μην υπάρχει σχετική ευπάθεια.

**Τοξικές Ουσίες (A-025 - added asset):** Χημικές ουσίες που απαιτούνται για τα αντιδραστήρια του εργαστηρίου και φυλάσσεται στον Βοηθητικό χώρο του εργαστηρίου μαζί με άλλα assets.

*Λόγος επιλογής asset*: Είναι εξαιρετικά σημαντικό να προφυλάξουμε τις χημικές ουσίες του εργαστηρίου καθώς είναι ένα απαραίτητο και ακριβό asset για τη λειτουργία του. Επιπλέον, οι χημικές ουσίες φυλάσσονται σε μη ασφαλή χώρο στον οποίο υπάρχουν και άλλα σημαντικά asset του εργαστηρίου.

**Workstation Computer (HP Pro G2 MT / A-002 to A-006):**

- Ανάλυση δεδομένων: μπορεί να χρησιμοποιηθεί για την επεξεργασία και ανάλυση δεδομένων που παράγονται από πειράματα που πραγματοποιήθηκαν στο εργαστήριο. Για παράδειγμα, ο υπολογιστής μπορεί να χρησιμοποιηθεί για την ανάλυση δεδομένων γενετικής αλληλουχίας ή εικόνων μικροσκοπίας.(Εργαστήριο-Παρασκευαστήριο)(Χώρος Λήψης Δειγμάτων)
- Μοντελοποίηση και προσομοίωση: μπορεί να χρησιμοποιηθεί για τη δημιουργία και εκτέλεση προσομοιώσεων και μοντέλων που σχετίζονται με βιολογικές διεργασίες. Για παράδειγμα, μπορεί να χρησιμοποιηθεί για την προσομοίωση της εξάπλωσης μιας ασθένειας σε έναν πληθυσμό ή για τη μοντελοποίηση των αλληλεπιδράσεων μεταξύ διαφορετικών μορίων.(Εργαστήριο-Παρασκευαστήριο)
- Έλεγχος οργάνων: μπορεί να χρησιμοποιηθεί για τον έλεγχο και την παρακολούθηση της απόδοσης των οργάνων που χρησιμοποιούνται στο εργαστήριο. Για παράδειγμα, μπορεί να χρησιμοποιηθεί για τον έλεγχο ενός μικροσκοπίου ή ενός φασματοφωτόμετρο.
- Συνεργασία και επικοινωνία:μπορεί να χρησιμοποιηθεί για να διευκολύνει τη συνεργασία και την επικοινωνία μεταξύ ερευνητών εντός του βιοεργαστηρίου ή με ερευνητές σε άλλα εργαστήρια. Για παράδειγμα, μπορεί να χρησιμοποιηθεί για κοινή χρήση δεδομένων, αποτελεσμάτων και ευρημάτων ή για επικοινωνία με συνεργάτες μέσω τηλεδιάσκεψης ή mail.(Γραφείο Γιατρού)

**PageWide Printers (HP OfficeJet Pro Printer / A-007):** Σταθερός εκτυπωτής για επαγγελματική χρήση με δικτυακή υποστήριξη (Ethernet/Wifi) και τεχνολογίες ασύρματης εκτύπωσης (ePrint, AirPrint και Mopria-Certified). Χρησιμοποιείται ευρέως λόγω του χαμηλού κόστους εκτύπωσης και ενεργειακής δαπάνης που απαιτείται.

**Printers (HP LaserJet Pro Printer / A-008):** Λέιζερ εκτυπωτής για υψηλής ποιότητας εκτύπωση, κατάλληλος για υψηλό φόρτο εργασίας. Χαρακτηριστικό τους η αξιοπιστία και η ταχύτητα. Παρέχει και αυτός δικτυακή υποστήριξη.

**Personal Laptop (Apple MacBook Air / A-015):** Υπολογιστής του Ιατρού για προσωπική και επαγγελματική χρήση. Στη συγκεκριμένη περίπτωση χρησιμοποιείται για επίβλεψη των ραντεβού ή των αρχείων και αποτελεσμάτων των ασθενών/πελατών από τον Ιατρό.

**Servers:**

**<u>Web Servers (A-009)</u>**

Γενικά, ένας web server σε ένα εργαστήριο χρησιμοποιείται για το hosting εφαρμογών που βασίζονται στον ιστό που επιτρέπουν στο προσωπικό του εργαστηρίου να έχει πρόσβαση και να αναλύει δεδομένα, να μοιράζεται πληροφορίες και να συνεργάζεται σε ερευνητικά έργα.

Για παράδειγμα, ένας web server συγκεκριμένα σε ένα biolab μπορεί να κάνει host μια βάση δεδομένων γονιδιωματικών ή πρωτεομικών δεδομένων στα οποία οι ερευνητές μπορούν να έχουν πρόσβαση και να αναλύουν χρησιμοποιώντας εργαλεία που βασίζονται στο διαδίκτυο. Μπορεί επίσης να φιλοξενεί λογισμικό βιοπληροφορικής που επιτρέπει στους ερευνητές να εκτελούν σύνθετες αναλύσεις σε αλληλουχίες DNA ή πρωτεϊνών. Επιπλέον, μπορεί να παρέχει πρόσβαση σε συστήματα διαχείρισης πληροφοριών εργαστηρίου (LIMS) που επιτρέπουν στο προσωπικό του εργαστηρίου να διαχειρίζεται δείγματα, να παρακολουθεί πειράματα και να παρακολουθεί το απόθεμα. Εν προκειμένω, εξυπηρετεί την πλατφόρμα λήψης αποτελεσμάτων αναλύσεων/εξετάσεων για τους ασθενείς.

**<u>Data Servers (A-010)</u>**

Η κύρια λειτουργία ενός data server σε ένα εργαστήριο είναι να παρέχει μια κεντρική τοποθεσία όπου το προσωπικό του εργαστηρίου μπορεί να αποθηκεύει, να διαχειρίζεται και να έχει πρόσβαση στα ερευνητικά του δεδομένα. Ένας data server μπορεί επίσης να χρησιμεύσει ως εφεδρικό σύστημα δεδομένων, διασφαλίζοντας ότι τα ερευνητικά δεδομένα δεν θα χαθούν λόγω αστοχιών υλικού ή άλλων καταστροφών.

Οι data servers στα βιολογικά εργαστήρια μπορούν επίσης να χρησιμοποιηθούν για τη διαχείριση του ελέγχου πρόσβασης σε ευαίσθητα δεδομένα, διασφαλίζοντας ότι

μόνο εξουσιοδοτημένο προσωπικό μπορεί να έχει πρόσβαση σε εμπιστευτικές πληροφορίες. Επιπλέον, οι διακομιστές δεδομένων μπορεί να περιλαμβάνουν εργαλεία για ανάλυση και οπτικοποίηση δεδομένων, επιτρέποντας στους ερευνητές να αναλύουν γρήγορα και αποτελεσματικά τα ερευνητικά τους δεδομένα και να αντλούν πληροφορίες από αυτά.

Εν προκειμένω, ο δικός μας data server χρησιμοποιείται για: *Διατήρηση, αποθήκευση αρχείου εξετάσεων ασθενών, ιστορικού, αρχείου πελατών προμηθευτών*

## 2.3 Λογισμικό και εφαρμογές

**Windows 7 Pro (A-017):** Λειτουργικό σύστημα το οποίο χρησιμοποιείται απο τις δικτυακές μας συσκευές router και switches.

**Windows 10 Pro (A-018):** Λειτουργικό σύστημα το οποίο χρησιμοποιείται από όλους τους workstation υπολογιστές του εργαστηρίου.

**Website (Joomla / (A-020):** Είναι ένα content management system (CMS) με το οποίο έχει δημιουργηθεί (εξ'ολοκλήρου από τον ιδιοκτήτη του εργαστηρίου) η διαδικτυακή μας ιστοσελίδα, μέσω της οποίας οι ασθενείς/πελάτες μπορούν να λάβουν τα αποτελέσματα των εξετάσεων τους.

## 2.4 Δίκτυο

**Switches (TP-LINK TL-SG1005D / A-011 to A-012):**

Επιτρέπει στους χρήστες να επεκτείνουν τις συνδέσεις δικτύου τους προσθέτοντας περισσότερες συσκευές στο δίκτυο, όπως υπολογιστές, εκτυπωτές και συσκευές συνδεδεμένης αποθήκευσης δικτύου (NAS). Το TL-SG1005D υποστηρίζει ταχύτητες Gigabit Ethernet (έως 1000 Mbps) και χρησιμοποιεί αυτόματη διαπραγμάτευση για αυτόματη προσαρμογή στην υψηλότερη ταχύτητα των συνδεδεμένων συσκευών. Υποστηρίζει επίσης την τεχνολογία QoS (Quality of Service) για την ιεράρχηση της κυκλοφορίας δικτύου για καλύτερη απόδοση και έχει συμπαγή σχεδιασμό που καθιστά εύκολη την εγκατάσταση και τη χρήση.

**Router (Cisco C886VA-K9 / A-013):**

Διαθέτει ενσωματωμένο μόντεμ VDSL2/ADSL2+, υποστήριξη για έως και 20 σήραγγες VPN για ασφαλή απομακρυσμένη πρόσβαση και προηγμένες λειτουργίες ασφαλείας, όπως τείχος προστασίας, αποτροπή εισβολής και φιλτράρισμα περιεχομένου. Ο δρομολογητής υποστηρίζει επίσης λειτουργίες ποιότητας

υπηρεσίας (QoS) για να δώσει προτεραιότητα στην κυκλοφορία και να εξασφαλίσει εφαρμογές φωνής και βίντεο υψηλής ποιότητας. Επιπλέον, το C886VA-K9 είναι εύκολο στην ανάπτυξη και τη διαχείριση, με λειτουργίες όπως το Cisco Configuration Professional και το Cisco IOS Software.(Διαλειτουργικότητα-Interoperability)

**Firewall (Fortinet-Fortigate-400D / A-014):**

Προσφέρει προηγμένες δυνατότητες ασφαλείας, όπως αποτροπή εισβολών, έλεγχος εφαρμογών, φιλτράρισμα ιστού, προστασία από ιούς και δυνατότητες εικονικού ιδιωτικού δικτύου (VPN). Παρέχει τείχος προστασίας υψηλής απόδοσης και προστασία από απειλές για δίκτυα μεσαίου μεγέθους, με απόδοση έως και 16 Gbps. Η συσκευή υποστηρίζει επίσης ευέλικτες επιλογές ανάπτυξης, όπως ως αυτόνομη συσκευή, σε διαμόρφωση υψηλής διαθεσιμότητας ή ως εικονική μηχανή σε ιδιωτικό ή δημόσιο περιβάλλον cloud.

## 2.5 Δεδομένα

**Αρχείο Υπαλλήλων/Αρχείο Ασθενών - CUSTOMER DATA/EMPLOYEE DATA (A-021 and A-022)**

Διατηρείται είτε σε ηλεκτρονική μορφή (database) στον data server είτε με φυσική μορφή σε ερμάρια κρεμαστών φακέλων εντός του εργαστηρίου. Συμπεριλαμβάνεται ως υποκατηγορία στα άνωθι το αρχείο των **προμηθευτών του εργαστηρίου.**

**Αντίγραφα Ασφαλείας - Backups (A-024 added asset)**

Γίνεται λήψη αντιγράφων ασφαλείας **κάθε εβδομάδα** για την προστασία των δεδομένων σε περίπτωση που καταστραφεί ή κλαπεί ο υπολογιστής. Τα αντίγραφα ασφαλείας φυλάσσονται στο γραφείο του Ιατρού.

*Λόγος επιλογής asset:* το να προφυλάξουμε τα Backups του εργαστηρίου τα οποία περιλαμβάνουν όλες τις πληροφορίες που διαχειρίζεται το εργαστήριο συμπεριλαμβανομένων των αρχείων πελατών/ασθενών και υπαλλήλων είναι το ίδιο σημαντικό με τη προστασία των ίδιων των πληροφοριών.

## 2.6 Διαδικασίες

**Συλλογή Πληροφοριών Προσωπικών Δεδομένων**

Διαδικασία συλλογής πληροφοριών των ασθενών/πελατών του εργαστηρίου.

**Ταυτοποίηση Δειγμάτων**

Αυτοματοποίηση στα περισσότερα στάδια διενέργειας των διαγνωστικών εξετάσεων με τη ταυτοποίηση να υλοποιείται με τη χρήση barcode απο τη στιγμή της δειγματοληψίας εως και την εξαγωγή των αποτελεσμάτων.

**Διαμοιρασμός προσωπικών δεδομένων σε τρίτους**

Το εργαστήριο ενδέχεται σε ορισμένες περιπτώσεις να διαμοιράσει τα προσωπικά δεδομένα των πελατών του με συνεργαζόμενους παρόχους υπηρεσιών με σκοπό την καλύτερη εξυπηρέτηση τους. **Δεν λαμβάνει πάντα γραπτή συγκατάθεση.**

**Αποστολή Αποτελεσμάτων Εξετάσεων:**

Οι εξετάσεις των ασθενών αποστέλλονται με fax ή email στον ασθενή ή τον θεράποντα ιατρό ή δίνονται απευθείας στους ασθενείς.

**Ανέβασμα Εξετάσεων στο Website.**

Επιπλέον, τα αποτελέσματα των εξετάσεων ανεβαίνουν στο site έτσι ώστε να είναι διαθέσιμα για τους ασθενείς. Τονίζεται πως το website του εργαστηρίου έχει δημιουργηθεί εξ'ολοκλήρου από τον ιδιοκτήτη του με τη χρήση Joomla CMS.

# 3. ΑΠΟΤΙΜΗΣΗ ΑΓΑΘΩΝ ΤΗΣ ΕΓΚΑΤΑΣΤΑΣΗΣ

## 3.1 Αγαθά που εντοπίστηκαν

- Αιματολογικός Αναλυτής (A-001)
  - Τρέχοντα μέτρα προστασίας:
    - Έλεγχοι συντήρησης/λειτουργικότητας από ειδικευόμενο τεχνικό κάθε 2 χρόνια. (Αποτρεπτικό)
    - Αρχεία καταγραφής τα οποία αναλύονται. (Ανιχνευτικό)
- Σταθμός Εργασίας Εργαστηρίου (A-002)
  - Τρέχοντα μέτρα προστασίας:
    - 1FA (Αδύναμη πολιτική ελέγχου ταυτότητας) (Μόνο κωδικός πρόσβασης). (Αποτρεπτικό)
    - Το προσωπικό συμμορφώνεται με τη διαδικασία ασφαλούς μεταφοράς τοξικών ουσιών. (Αποτρεπτικό)
- Σταθμός Εργασίας Εργαστηρίου (A-003)
  - Τρέχοντα μέτρα προστασίας:
    - Τα αρχεία καταγραφής ρόλων και οι ανατεθειμένοι εκτυπώνονται από το μηχάνημα (σε μορφή json κτλ.) (Ανιχνευτικό)
    - (Αδύναμος) Έλεγχος ταυτότητας με κωδικό πρόσβασης. (Αποτρεπτικό)
- Σταθμός Εργασίας Χώρου Λήψης Δειγμάτων (A-004)
  - Τρέχοντα μέτρα προστασίας:
    - Κανένα

- Σταθμός Εργασίας Αίθουσας Αναμονής (A-005)
    - Τρέχοντα μέτρα προστασίας:
        - Κάμερα ασφαλείας (παλιά και απαρχαιωμένη). (Ανιχνευτικό)
        - Το τείχος προστασίας έχει εφαρμοστεί αλλά δεν έχει τοποθετηθεί/ρυθμιστεί σωστά. (Αποτρεπτικό)
- Σταθμός Εργασίας Γραφείου Ιατρού (A-006)
    - Τρέχοντα μέτρα προστασίας:
        - Το λειτουργικό σύστημα διατηρεί τα σημεία επαναφοράς των αντιγράφων ασφαλείας. (Αποτρεπτικό)
- Εκτυπωτής Σελίδας Αίθουσας Αναμονής (A-007)
    - Τρέχοντα μέτρα προστασίας:
        - Απαρχαιωμένο υλικολογισμό το οποίο παρέχει μερική προστασία, αλλά είναι ευάλωτο σε πιο σύγχρονες απειλές. (Αποτρεπτικό)
        - Ο εκτυπωτής βρίσκεται πίσω από το γραφείο της γραμματείας, γεγονός που μειώνει τις πιθανότητες έκθεσης. (Αποτρεπτικό)
- Εκτυπωτής Γραφείου Ιατρού (A-008)
    - Τρέχοντα μέτρα προστασίας:
        - Απαρχαιωμένο υλικολογισμό το οποίο παρέχει μερική προστασία, αλλά είναι ευάλωτο σε πιο σύγχρονες απειλές. (Αποτρεπτικό)
        - Η μνήμη έχει ρυθμιστεί να εκκενώνεται χειροκίνητα αυτήν τη στιγμή σε περίπτωση συντήρησης. (Αποτρεπτικό)
- Σέρβερ Ιστότοπου (A–009)
    - Τρέχοντα μέτρα προστασίας:
        - Αρχεία καταγραφής διακομιστή. (Ανιχνευτικό)
- Σέρβερ Βάσης Δεδομένων (A-010)
    - Τρέχοντα μέτρα προστασίας:
        - Έλεγχος ταυτότητας με κωδικό πρόσβασης. (Αποτρεπτικό)
- Μεταγωγέας Αίθουσας Αναμονής (A-011)
    - Τρέχοντα μέτρα προστασίας:
        - VLAN Tagging. (Αποτρεπτικό)
- Μεταγωγέας Βοηθητικού Χώρου (A-012)
    - Τρέχοντα μέτρα προστασίας:
        - VLAN Tagging. (Αποτρεπτικό)
- Δρομολογητής (A-013)
    - Τρέχοντα μέτρα προστασίας:
        - Απαρχαιωμένη κρυπτογράφηση δεδομένων. (Αποτρεπτικό)
        - Ο δρομολογητής έχει ένα σχετικό επίπεδο προστασίας το οποίο του επιτρέπει να ανταποκρίνεται σε παλαιότερες απειλές. (Αποτρεπτικό)
- Τείχος Προστασίας (A-014)
    - Τρέχοντα μέτρα προστασίας:
        - Το τείχος προστασίας περιορίζει την εισερχόμενη κίνηση μόνο σε εγκεκριμένες υπηρεσίες. (Αποτρεπτικό)
        - Η τωρινή έκδοση παρέχει ένα σχετικό επίπεδο προστασίας. (Αποτρεπτικό)
- Φορητός Υπολογιστής (A-015)
    - Τρέχοντα μέτρα προστασίας:

        - Ληγμένο λογισμικό προστασίας από ιούς. (Αποτρεπτικό)
        - Σάρωση συστήματος για πιθανές απειλές/παραβιάσεις ασφάλειας. (Ανιχνευτικό)
        - Τείχος προστασίας των Windows. (Αποτρεπτικό)
- Δεδομένα Πελατών (Α-016)
    - Τρέχοντα μέτρα προστασίας:
        - Κρυπτογράφηση των δεδομένων. (Αποτρεπτικό)
        - Σάρωση συστήματος για πιθανές απειλές/παραβιάσεις ασφάλειας. (Ανιχνευτικό)
- Δεδομένα Υπαλλήλων (Α-017)
    - Τρέχοντα μέτρα προστασίας:
        - Εσωτερικοί κανόνες εργαζομένων, προστασία με κωδικό πρόσβασης δεδομένων. (Αποτρεπτικό)
- Λογισμικό Windows 7 Pro (Α-018)
    - Τρέχοντα μέτρα προστασίας:
        - Μερικώς ενημερωμένο λογισμικό προστασίας από ιούς. (Αποτρεπτικό)
        - Πρόγραμμα προβολής συμβάντων, Τείχος προστασίας των WIndows. (Ανιχνευτικό)
- Λογισμικό Windows 10 Pro (Α-019)
    - Τρέχοντα μέτρα προστασίας:
        - Απαρχαιωμένο λογισμικό προστασίας από ιούς. (Αποτρεπτικό)
        - Windows Defender. (Ανιχνευτικό)
        - Ενημερωμένη έκδοση κώδικα της Microsoft. (Αποτρεπτικό)
        - Πρόγραμμα προβολής συμβάντων. (Ανιχνευτικό)
- Ιστοσελίδα (Α-020)
    - Τρέχοντα μέτρα προστασίας:
        - Κανένα
- Φυσικό Αρχείο Ασθενών (Α-021)
    - Τρέχοντα μέτρα προστασίας:
        - Μικρή κλειδαριά στο δοχείο. (Αποτρεπτικό)
- Αρχείο Υπαλλήλων & Προμηθευτών (Α-022)
    - Τρέχοντα μέτρα προστασίας:
        - Ο γραμματέας παρακολουθεί και αποτρέπει την κακόβουλη πρόσβαση σε αρχεία. (Αποτρεπτικό)
        - Ανιχνευτής πυρκαγιάς/φυσική παρακολούθηση. (Ανιχνευτικό)
- Εφεδρική Γεννήτρια (Α–023)
    - Τρέχοντα μέτρα προστασίας:
        - Συντήρηση. (Αποτρεπτικό)
        - Διάφορες ενδείξεις π.χ. συμπιεστή, θερμοκρασία που εμφανίζεται μέσω φώτων led, μετρήσεις κ.λπ. (Ανιχνευτικό)
        - Ένδειξη λυχνίας σε περίπτωση βλάβης. (Ανιχνευτικό)
- Αντίγραφα Ασφαλείας (Α-024)
    - Τρέχοντα μέτρα προστασίας:
        - Προστασία που παρέχεται από τοπικό σταθμό εργασίας. (Αποτρεπτικό)
- Χημικές ουσίες (Α-025)
    - Τρέχοντα μέτρα προστασίας:

        - Οι ουσίες φυλάσσονται σε δοχείο που δεν ανοίγει εύκολα. (Αποτρεπτικό)

## 3.2 Απειλές που εντοπίστηκαν

- Αιματολογικός Αναλυτής (A-001)
    - Μη εξουσιοδοτημένη πρόσβαση: Εάν κάποιος αποκτήσει μη εξουσιοδοτημένη πρόσβαση στον αναλυτή ή στο δίκτυο στο οποίο είναι συνδεδεμένος, ενδέχεται να μπορεί να τροποποιήσει ή να χειραγωγήσει τα αποτελέσματα ή να αποκτήσει πρόσβαση σε εμπιστευτικές πληροφορίες ασθενούς.
    - Παραβιάσεις φυσικής ασφάλειας: Εάν ο αναλυτής δεν έχει ασφαλιστεί σωστά, μπορεί να κλαπεί ή να παραβιαστεί, θέτοντας σε κίνδυνο την ακεραιότητα των αποτελεσμάτων ή την εμπιστευτικότητα των δεδομένων του ασθενούς.
    - Αστοχία εξοπλισμού: Η αστοχία του εξοπλισμού μπορεί να προκαλέσει διακοπές λειτουργίας, οδηγώντας σε καθυστερημένα ή ανακριβή αποτελέσματα ή αδυναμία ανάλυσης δειγμάτων.
- Σταθμός Εργασίας Εργαστηρίου (A-002)
    - Ο υπολογιστής και τα δεδομένα του μπορούν να αλλοιωθούν από ακατάλληλο άνθρωπο.
    - Τα μηχανικά κομμάτια του υπολογιστή θα πάψουν να λειτουργούν.
- Σταθμός Εργασίας Εργαστηρίου (A-003)
    - Υπάλληλος με κακόβουλες προθέσεις μπορεί να χρησιμοποιήσει τα ενισχυμένα δικαιώματα για να υποβαθμίσει την ασφάλεια του συστήματος.
    - Χρήση του Σταθμού Εργασίας από ανειδίκευτο άτομο με άγνωστες προθέσεις.
- Σταθμός Εργασίας Χώρου Λήψης Δειγμάτων (A-004)
    - Κλοπή των συνθηματικών πρόσβασης του υπολογιστή
    - Χρήση μεθόδων ιδιαίτερα επικίνδυνες προς ανθρώπους με άγνοια των κινδύνων, όπως το social engineering.
- Σταθμός Εργασίας Αίθουσας Αναμονής (A-005)
    - Χρήση του μηχανήματος από μη εξουσιοδοτημένο άτομο.
    - Απορρόφηση του υπαλλήλου, οδηγώντας τον σε αντιεπαγγελματικές ενέργεις οι οποίες μπορούν να οδηγήσουν σε κοστοβόρα λάθη.
- Σταθμός Εργασίας Γραφείου Ιατρού(A-006)
    - Απόσπαση σημαντικών πληροφοριών καθώς αυτές μεταφέρονται μέσω του δρομολογητή.
    - Σημαντικές πληροφορίες είναι πιθανόν να διαρρεύσουν ή να καταστραφούν από ανθρώπινο λάθος.
- Σταθερός Εκτυπωτής Αίθουσας Αναμονής (A-007)
    - Εγκατάσταση Ιομορφικού λογισμικού λόγω της σύνδεσης δικτύου.
    - Ευαίσθητα δεδομένα κινδυνεύουν να κλαπούν.
- Εκτυπωτής Γραφείου Ιατρού(A-008)
    - Κλοπή πληροφοριών των εγγράφων που εκτυπώνονται.

    - Μη εξουσιοδοτημένη πρόσβαση. Εφόσον ο εκτυπωτής παρέχει συνδεσιμότητα δικτύου κάποιο μη εξουσιοδοτημένο άτομο μπορεί να αποκτήσει πρόσβαση.
- Διακομιστής Ιστότοπου (A–009)
    - SQL Injection attack. Η συγκεκριμένη απειλή μπορεί να δώσει το δικαίωμα στον επιτιθέμενο να δει, τροποποιήσει ή διαγράψει ευαίσθητες πληροφορίες, όπως ονόματα χρηστών και κωδικούς.
    - Καταστροφική ζημιά στο hardware του διακομιστή
    - Κλοπή ή πρόκληση ζημιάς στον διακομιστή (Η πόρτα είναι μισάνοιχτη σε κεντρικό δρόμο).
- Διακομιστής Βάσης Δεδομένων (A-010)
    - Μη εξουσιοδοτημένος χρήστης έχει πρόσβαση στον διακομιστή.
    - Εισαγωγή ανεπιθύμητων χαρακτηριστικών, τα οποία θα απειλούν την άρτια λειτουργία του διακομιστή.
    - Κλοπή ή πρόκληση ζημιάς στον διακομιστή (Η πόρτα είναι μισάνοιχτη σε κεντρικό δρόμο).
- Μεταγωγέας Αίθουσας Αναμονής (A-011)
    - Κλοπή ή πρόκληση ζημιάς στον μεταγωγέα.
    - MAC address spoofing. Ο επιτιθέμενος μπορεί να προσπεράσει δικτυακά φίλτρα και την αυθεντικοποίηση, και να αποκτήσει πρόσβαση σε περιορισμένες περιοχές του δικτύου, προκαλώντας με αυτόν τον τρόπο ζημιά στο δίκτυο μας.
- Μεταγωγέας Βοηθητικού Χώρου (A-012)
    - Χειραγώγηση Spanning Tree Protocol. Μέσω αυτής της απειλής ο επιτιθέμενος μπορεί να ελέγξει την ροή της κυκλοφορίας στο δίκτυο και να την ανακατευθύνει σε μια κακόβουλη συσκευή.
    - Αναστάτωση του δικτύου ή μη εξουσιοδοτημένη πρόσβαση.
- Δρομολογητής (A-013)
    - Βιομηχανική κατασκοπεία, ανταγωνιστές κλέβουν σημαντικές πληροφορίες της επιχείρησης για να τις χρησιμοποιήσουν προς όφελος τους.
    - Κλοπή δεδομένων.
    - Πρόσβαση στις ρυθμίσεις του δρομολογητή, μεταβάλλοντας τις με τέτοιο τρόπο ώστε να διαταραχθεί η ομαλή λειτουργία του δικτύου.
- Τείχος Προστασίας (A-014)
    - Πέρασμα κακόβουλου λογισμικού.
    - Τεχνικές παράκαμψης ασφάλειας.
    - Εκμετάλλευση ευάλωτων πρωτοκόλλων, το οποίο θα οδηγήσει στην αχρήστευση του τείχους προστασίας.
- Φορητός Υπολογιστής (A-015)
    - Κλοπή δεδομένων μέσω της σύνδεσης με το διαδίκτυο.
    - Απόπειρα hacking.
    - Προσβολή από ιό.
- Δεδομένα Πελατών (A-016)
    - Αποκάλυψη ευαίσθητων πληροφοριών.
    - Εκμετάλλευση στοιχείων πελατών.
    - Εκμαίευση προσωπικών πληροφοριών/δεδομένων των πελατών.
- Δεδομένα Υπαλλήλων (A-017)
    - Αποκάλυψη επιβλαβών πληροφοριών προς την επιχείρηση.
    - Απειλή παρακράτησης δεδομένων έναντι ρήτρας (ransomware).

    - Εκμαίευση προσωπικών πληροφοριών/δεδομένων των υπαλλήλων.
- Λογισμικό Windows 7 Pro (A-018)
    - Rootkits. Εάν εγκατασταθεί rootkit στο λογισμικό, μπορεί να εκτελέσει ποικίλες κακόβουλες ενέργειες, όπως η καταγραφή της πληκτρολόγησης, η καταγραφή της δραστηριότητας των χρηστών, η κλοπή κωδικών πρόσβασης ή άλλων ευαίσθητων πληροφοριών και παροχή στον εισβολέα απομακρυσμένης πρόσβασης στο σύστημα.
    - Το λογισμικό είναι ευάλωτο σε επιθέσεις που χρησιμοποιούν σύγχρονες τεχνολογίες.
    - Μιά fork bomb προκαλεί καταστροφική υπερχείλιση μνήμης στο λογισμικό
- Windows 10 Pro (A-019)
    - Προσβολή από ιομορφικό λογισμικό.
    - Keyloggers. Ο εισβολέας θα είναι σε θέση να καταγράφει κάθε πλήκτρο που πατήθηκε σε μια ηλεκτρονική συσκευή, δίνοντας του με αυτόν τον τρόπο, το δικαίωμα να προβεί σε κακόβουλες ενέργειες, όπως η κλοπή συνθηματικών, η κλοπή αριθμών πιστωτικών καρτών και άλλων εμπιστευτικών δεδομένων.
    - Zerologon" (CVE-2020-1472):Ευπάθεια στο netologon σύστημα(https://www.crowdstrike.com/blog/cve-2020-1472-zerologon-security-advisory/)
- Ιστοσελίδα(A-020)
    - Buffer Overflow. Αν ο κώδικας της ιστοσελίδας δεν φροντίζει να την προστατεύει από την υπερχείλιση του buffer (ο επιτιθέμενος μπορεί να τοποθετήσει περισσότερους χαρακτήρες στον buffer απ'ότι αυτός αναμένει να δεχθεί), υπάρχει η πιθανότητα κάποιος να εκμεταλλευτεί το γεγονός αυτό, για να κάνει την ιστοσελίδα μη ανταποκρίσιμη προς τους χρήστες ή να εισάγει κακόβουλο κώδικα στο πεδίο του buffer για να προκαλέσει σοβαρή ζημία στο σύστημα.
    - Brute-force attack. Με αυτήν την μέθοδο ο εισβολέας προσπαθεί να μαντέψει έναν κωδικό δοκιμάζοντας συστηματικά κάθε δυνατό συνδυασμό μέχρι να βρεθεί ο σωστός. Έτσι, ο εισβολέας μπορεί να έχει πρόσβαση σε λογαριασμούς χρηστών ή και σε λογαριασμό διαχειριστή, γεγονός που μπορεί να οδηγήσει μέχρι και στην κατάρρευση του ιστοτόπου.
    - SQL Injection attack. Η συγκεκριμένη απειλή μπορεί να δώσει το δικαίωμα στον επιτιθέμενο να δει, τροποποιήσει ή διαγράψει ευαίσθητες πληροφορίες, όπως ονόματα χρηστών και κωδικούς.
    - Denial-of-service attack. Αυτός ο τρόπος επίθεσης βασίζεται στην αποστολή μεγάλου όγκου κίνησης ή αιτημάτων στον στόχο, κατακλύζοντας τον και αναγκάζοντας τον να μην μπορεί να ανταποκριθεί. Ένας τέτοιος τύπος κυβερνοεπίθεσης, μπορεί να οδηγήσει στην απώλεια της υπηρεσίας της ιστοσελίδας για τους νόμιμους χρήστες της.
- Φυσικό Αρχείο Ασθενών(A-021)
    - Παραβίαση της πολιτικής απορρήτου.
    - Αποκάλυψη ευαίσθητων πληροφοριών.
    - Κλοπή πληροφοριών που στοχοποιούν ένα συγκεκριμένο άτομο.
    - Απώλεια σημαντικών πληροφοριών.
- Αρχείο Υπαλλήλων & Προμηθευτών (A-022)

    - Τα αρχεία μπορούν να κλαπούν από κακοπροαίρετο άτομο.
    - Ανταγωνιστές λαμβάνουν οικονομικά στοιχεία της επιχείρησης.
    - Αποκαλύπτονται επιχειρησιακές συμφωνίες με συνεργάτες της επιχείρησης.
    - Απώλεια σημαντικών πληροφοριών.
- Εφεδρική Γεννήτρια (A–023)
    - Λανθασμένη σχεδίαση - Επικίνδυνη λειτουργικότητα.
    - Κίνδυνος ζημιάς ή κλοπής της γεννήτριας.
    - Δηλητηρίαση λόγω μονοξειδίου του άνθρακα.
- Αντίγραφα Ασφαλείας (A-024)
    - Διαρροή ευαίσθητων δεδομένων.
    - Διαγραφή ή έκθεση εμπιστευτικών πληροφοριών.
- Χημικές ουσίες (A-025)
    - Φυσική καταστροφή του εργαστηριακού χώρου λόγω φωτιάς.
    - Μόλυνση του χώρου φύλαξης που μπορεί να προκαλέσει κινδύνους υγείας.
    - Κλοπή των χημικών ουσιών από κακόβουλους τρίτους.

## 3.3 Ευπάθειες που εντοπίστηκαν

- Αιματολογικός Αναλυτής(A-001)
    - Δυσλειτουργικό Λογισμικό: Οι αιματολογικοί αναλυτές λειτουργούν βάσει λογισμικού, το οποίο μπορεί να είναι επιρρεπές σε σφάλματα και bugs βασισμένα στον πηγαίο του κώδικα. Μια πιθανή ευπάθεια λογισμικού μπορεί να προκαλέσει εσφαλμένα αποτελέσματα και να θέσει σε κίνδυνο τη φροντίδα του ασθενούς.
    - Hardware Failure/Malfunction: Τα στοιχεία υλισμικού ενός αιματολογικού αναλυτή, όπως τα κύτταρα ροής, οι βαλβίδες και οι αισθητήρες, μπορεί να φθαρούν ή να δυσλειτουργούν, οδηγώντας σε εσφαλμένα αποτελέσματα ή σε αδυναμία ανάλυσης δειγμάτων.
    - Αναντιστοιχία βαθμονόμησης: Οι αιματολογικοί αναλυτές απαιτούν τακτική βαθμονόμηση για την εξασφάλιση ακριβών αποτελεσμάτων. Εάν η βαθμονόμηση δεν εκτελεστεί σωστά, ο αναλυτής δεν μπορεί να παράγει αξιόπιστα αποτελέσματα.
- Σταθμός Εργασίας Εργαστηρίου(A-002)
    - Ανεπαρκής έλεγχοι αυθεντικοποίησης και επικύρωσης.
    - Έκθεση του hardware σε επιβλαβείς ουσίες.
- Σταθμός Εργασίας Εργαστηρίου(A-003)
    - Παροχή περισσότερων δικαιωμάτων σε χρήστες που δεν τα χρειάζονται.
    - Αδύναμος κωδικός εισόδου.
- Σταθμός Εργασίας Χώρου Λήψης Δειγμάτων(A-004)
    - Εισαγωγή συνθηματικών σε κοινή θέα.
    - Έλλειψη ευαισθητοποίησης των εργαζομένων με τα απαραίτητα μέτρα ασφάλειας.
- Σταθμός Εργασίας Αίθουσας Αναμονής(A-005)
    - Απουσία φυσικής προστασίας - Ο υπολογιστής αφήνεται ανοιχτός σε χώρο με πελάτες.

    - Ο υπολογιστής έχει πρόσβαση σε ιστοσελίδες που δεν συνάδουν με τις διαδικασίες στις οποίες ενεργεί ένα μικροβιολογικό εργαστήριο.
- Σταθμός Εργασίας Γραφείου Ιατρού(A-006)
    - Σύνδεση με δρομολογητή που βρίσκεται σε πολυσύχναστο χώρο.
    - Ο Ιατρός δεν είναι αρκετά εξειδικευμένος με την χρήση σταθερού υπολογιστή.
- Σταθερός Εκτυπωτής  Αίθουσας Αναμονής(A-007)
    - Μη αναβαθμισμένο firmware. Παρατηρούμε ότι και οι δύο εκτυπωτές μας χρησιμοποιούν μια παλιά έκδοση υλικολογισμικού με γνωστές ευπάθειες που δίνουν χώρο στις απειλές.
    - Οι εκτυπωτές μας βρίσκονται σε μη ασφαλή τοποθεσία όπου μη εξουσιοδοτημένο προσωπικό μπορεί να έχει πρόσβαση.
- Εκτυπωτής Γραφείου Ιατρού(A-008)
    - Μη κατάλληλη ρύθμιση της εκκαθάρισης της μνήμης του εκτυπωτή, η οποία ενδέχεται να περιέχει εμπιστευτικές πληροφορίες.
    - Ασθενή ή default admin συνθηματικά.
- Διακομιστής Ιστότοπου(A–009)
    - Λάθος δομημένος κώδικας.
    - Φύλαξη σε χώρο με χημικές ουσίες.
    - Η είσοδος στον χώρο των διακομιστών είναι “ελεύθερη”.
- Διακομιστής Βάσης Δεδομένων(A-010)
    - Αδύναμοι μηχανισμοί αυθεντικοποίησης και εξουσιοδότησης.
    - Εσφαλμένες ρυθμίσεις διακομιστή.
    - Απουσία φυσικής προστασίας.
- Μεταγωγέας Αίθουσας Αναμονής(A-011)
    - Απουσία φυσικής προστασίας.
    - Εσφαλμένες ρυθμίσεις.
- Μεταγωγέας Βοηθητικού Χώρου(A-012)
    - Απαρχαιωμένο υλικολογισμικό.
    - Χειραγώγηση Spanning Tree Protocol.
    - STP root bridge misconfiguration.
- Δρομολογητής(A-013)
    - Αδύναμη κρυπτογράφηση.
    - Χρήση παλαιών τεχνολογιών.
    - Χρήση εργοστασιακών κωδικών.
- Τείχος Προστασίας(A-014)
    - Λάθος ρυθμισμένοι κανόνες.
    - Χρήση παλαιότερης έκδοσης.
    - Χαλαρή πρόσβαση στο τείχος προστασίας.
- Φορητός Υπολογιστής(A-015)
    - Σύνδεση σε άλλα δημόσια δίκτυα.
    - Απουσία λογισμικού Antivirus.
    - Σύνδεση σε μη αξιόπιστες σελίδες.
- Δεδομένα Πελατών(A-016)
    - Απειλή εκ των έσω (Insider threat).
    - Ακατάλληλη ξεφόρτωση ευαίσθητων πληροφοριών.
    - Social engineering.
- Δεδομένα Υπαλλήλων(A-017)
    - Μη κρυπτογράφηση της πληροφορίας.
    - Απουσία αντιγράφων ασφαλείας.

    - Απειλή εκ των έσω (Insider threat).
- Λογισμικό Windows 7 Pro(A-018)
    - Παλιά έκδοση του λογισμικού που δε περιέχει τα πιο πρόσφατα security patches and fixes.
    - Λογισμικό το οποίο δεν δέχεται πλέον ενημερώσεις.
    - Λογισμικό ευπαθές σε fork bombs.
- Windows 10 Pro(A-019)
    - Απουσία antivirus.
    - Εγκατάσταση μη αξιόπιστου third-party λογισμικού.
- Ιστοσελίδα(A-020)
    - Καθώς ο Ιστότοπος δεν έχει σχεδιαστεί από ειδικό σε θέματα ασφαλείας, ενδέχεται να υπάρχουν “τρύπες” στην ασφάλεια του.
    - Μη εφαρμογή ελέγχου ορίου σε εισαγωγές των χρηστών.
    - Μη έλεγχος αριθμού προσπάθειας εισόδου σε λογαριασμό χρήστη.
    - Απουσία προστασίας συνεδρίας.
- Φυσικό Αρχείο Ασθενών(A-021)
    - Τα αρχεία φυλάσσονται σε κοινή θέα.
    - Ουσίες που μπορούν να αλλοιώσουν τα φυσικά αρχεία βρίσκονται κοντά στα αρχεία.
    - Φυσικές καταστροφές.
- Αρχείο Υπαλλήλων & Προμηθευτών(A-022)
    - Τα αρχεία φυλάσσονται σε μέρος χωρίς μέτρα ασφαλείας.
    - Τα αρχεία βρίσκονται σε δωμάτιο στο οποίο πολλά άτομα έχουν πρόσβαση.
    - Φυσικές καταστροφές.
- Εφεδρική Γεννήτρια(A–023)
    - Απαρχαιωμένη συσκευή (μη συμβατή με τα σύγχρονα εργαστηριακά πρότυπα).
    - Βρίσκεται στον προαύλιο χώρο (ο οποίος δεν είναι περιφραγμένος).
    - Μη συμβατό καύσιμο (αναντιστοιχία βάσει βιομηχανικού σχεδιασμού)
- Αντίγραφα Ασφαλείας(A-024)
    - Τα δεδομένα αντιγράφων ασφαλείας διατηρούνται σε μη ασφαλής εγκαταστάσεις.
    - Βρίσκονται στον σταθμό εργασίας του Γιατρού.
- Χημικές ουσίες(A-025)
    - Φύλαξη των χημικών ουσιών σε μη ασφαλή χώρο (μισάνοιχτη πόρτα).
    - Φύλαξη των χημικών ουσιών στον ίδιο χώρο μαζί με άλλα πολύτιμα asset.
    - Φύλαξη των χημικών ουσιών σε πολυσύχναστο χώρο.

## 3.4 Αποτελέσματα αποτίμησης

Συνοπτικά σε μορφή πίνακα παρουσιάζεται η αποτίμηση συνολικά για το εκάστοτε αγαθό από την λίστα αλλά και για τα δικά μας ευρήματα:

| A/A | Asset | Asset Name | Function | Potential Vulnerability | Potential | Potential | Confidentialit | Integrity | Availability | Impact | Likelihoo | Current Controls | | Vulnerability | Risk |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | | | | | | | | | | | Preventive Controls | Detective Controls | | |
| 1 | A-001 | LabWS001 (Haematology analyser) | To analyze blood samples and to provide said metrics | Malfunctional Software/Hardware | Physical Security Breach | Obstruction of core lab functions | Low | Low | High | 8 | 2 | Maintenance/Operability controls by a specified technician every 2 yrs. | Control logs that are being analyzed | 5 | 80 |
| 2 | A-002 | PCWS001 (Workstation) | Analyze the metrics and crawl said data (Lab) | Non-sufficient authentication controls | Non-authorized personnel access/Data leakage | Exposure of Sensitive Data _ GDPR Penalty | High | High | Low | 7 | 3 | 1FA (Weak Authentication Policy)(Password Only) | | 5 | 105 |
| 3 | A-003 | PCWS002 (Workstation) | Modelling and Simulation | Non-assigned personnel acquires access to higher role | Non-modular system security plan | Undermining the core system security | High | High | Low | 6 | 3 | | Role logs and asignees are printed out by the machine (in .json from etc.) | 6 | 108 |
| 4 | A-004 | PCWS003 (Workstation) | Sending data samples to lab | Confidential Data (passwords) are in plain sight | Password Leakage | Exposure of key lab procedures | Medium | Medium | Low | 4 | 5 | | | 3 | 60 |
| 5 | A-005 | PCWS004 (Workstation) | Appointment scheduling - Customer data management | Workstation is left unsupervised in a crowded room | Customer personal data and appointment details leakage | Exposure of Sensitive Data _ GDPR Penalty | High | High | Low | 6 | 3 | | Security camera (old and outdated) | 5 | 90 |
| 6 | A-006 | PCWS005 (Workstation) | Data and appointment management. Also keeps lab's backups | Non tech-savvy user (doctor) | Sensitive data or backup leakage or destruction | Sensitive data exposure - GDPR Penalty + Backup deletion | High | High | Low | 9 | 3 | OS keeps backup restoration points | | 5 | 135 |
| 7 | A-007 | PR0001 (PageWide Printers) | Used to print various lab documents that contain sensitive client and lab procedure data | Old non-updated firmware | Virus infections | Exposure of Sensitive Data _ GDPR Penalty | High | Low | Low | 4 | 4 | Outdated firmware provides some security but not to more recent threats | | 6 | 96 |
| 8 | A-008 | PR0002 (Printer) | Used to print various lab documents that contain sensitive client and lab procedure data | Default admin passwords | Remote access of printer from anauthorized individual | Exposure of Sensitive Data and Lab Procedures | High | Low | Low | 5 | 3 | Outdated firmware provides some security but not to more recent threats | | 5 | 75 |
| 9 | A-009 | SRV001 (Web Server) | Web server is hosting our website application in order for clients to receive their results remotely | Web server is being kept on premises / unsecured location | Mulfunction due to misconfiguration / hardware | Lab's website is unavailable | None | None | High | 8 | 3 | | Server logs | 6 | 144 |
| 10 | A-010 | SRV002 (Database Server) | Our database server keeps all clients medical results and personal data | Database server is being kept on premises / unsecured location | Anauthorized access or even theft of clients personal data | Exposure of Sensitive Data _ GDPR Penalty | High | High | Low | 9 | 3 | | | 10 | 270 |
| 11 | A-011 | SW001 (Switch) | Network Extension | Obsolete firmware | VLAN Hopping | Modification of network transmitted data between VLANs / unauthorized access | Low | Medium | Medium | 5 | 5 | VLAN Tagging | | 6 | 150 |
| 12 | A-012 | SW002 (Switch) | Network Extension | Non-corresponding settings | Switch Flooding | Modification of network transmitted data between VLANs / unauthorized access | Low | Medium | Medium | 5 | 5 | VLAN Tagging | | 6 | 150 |
| 13 | A-013 | RT001 (Router) | Forwards data packets between computer networks, allowing devices on different networks to communicate with each other. | Weak encryption | Industrial espionage | Data breaches, theft of intellectual property | Medium | Medium | Low | 3 | 4 | Outdated data encryprion | | 4 | 48 |
| 14 | A-014 | FW001 (Firewall) | To block unauthorized network traffic | Rules not appropriately configured | Data Leakage | Exposure of Sensitive Data _ GDPR Penalty | High | High | Low | 9 | 5 | Firewall restricts ingoing traffic to only approved services | | 5 | 225 |
| 15 | A-015 | LTP001 (Laptop) | For personal use and business appoinment review | Lack of antivirus software | Compromized software | Key losses in lab data collection | Medium | Medium | Low | 3 | 5 | Expired antivirus software | System scan for possible threats/breaches of security | 3 | 60 |
| 16 | A-016 | Customer Data | All customers' data | Dumping of sensitive data | Sensitive data exposure | Deterioration of business solvency | High | High | Low | 7 | 4 | Data Password Encryprion | System scan for possible threats/breaches of security | 6 | 168 |
| 17 | A-017 | Employee Data | Supports Employees Filing Obligations, Payments, Personal Records | Non encrypted Data | Insider gets access to Employee Data | Exposure of Personal Data _ GDPR Penalty | High | Low | Low | 7 | 4 | Internal Employee Rules, Data password protection | | 4 | 112 |
| 18 | A-018 | Windows 7 Pro | OS for routers and switches | Old/Deprecated version of the software that does not contain the latest security patches and fixes. | Rootkits | Disruption of business operations and downtime | Medium | Medium | High | 7 | 2 | Partially updated antivirus software | Event Viewer,Windows Firewall | 3 | 42 |
| 19 | A-019 | Windows 10 Pro | OS for workstations | Lack of trustworthy antivirus software | Virus attack | Increased costs for IT recovery and remediation efforts | Medium | Medium | Medium | 8 | 2 | Outdated antivirus software | Windows Defender | 2 | 32 |
| 20 | A-020 | Website (JOOMLA) | Lab's website where clients can login to receive their results | MySQL Injection | Malicious person gets access to clients sensitive data | Exposure of Sensitive Data _ GDPR Penalty | High | High | Low | 7 | 5 | None due to faulty website design as the website is not created by a professional | | 9 | 315 |
| 21 | A-021 | Φυσικό Αρχείο Ασθενών | Contains most clients data and test results | Data is kept in physical form in a room without a fire sensor | Potential fire hazard can destroy client records | Client data destruction | None | Medium | Low | 4 | 2 | | | 8 | 64 |
| 22 | A-022 | Αρχείο Υπαλλήλων & Προμηθευτών | Supports Filing Obligations, Payments, Accounting Records | Files kept in unsecured place, in an easy accessible library without lockers | Files are stolen by malicious customer | Personal data Loss, accounting data loss | Medium | High | Medium | 6 | 4 | Secretary monitors and prevents malicious access to files | | 3 | 72 |
| 23 | A-023 | Εφεδρική Γεννήτρια | Provides backup electricity for limited time duration in case of an emergency black-out | Obsolete Device (non compliant to modern lab standards) | Faulty design-Hazardous functionality | Serious infrastructural damage | None | None | High | 9 | 1 | Maintenance | Various indications e.g.pressurizer, temperature that are being displayed via led lights, metrics etc. | 7 | 63 |
| 24 | A-024 | Αντίγραφα Ασφαλείας | Data Protection in case of stolen/broken hardware (PC) | Backup data are being kept on premises / unsecured location | Sensitive Data Leakage | Exposure of Personal Data _ GDPR Penalty. Also exposure of data immediately correlated to the lab personnel | High | High | Low | 9 | 3 | Protection provided by local workstation | | 9 | 243 |
| 25 | A-025 | Χημικές Ουσίες | Auxiliary means to complete lab tasks | Storage in a busy space (along with other assets) | Substances are highly hazardous regarding the health empolyees | Catastrophic consequenses regarding lab operation | None | None | High | 9 | 3 | | | 9 | 243 |

| | | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 26 | A-001 | LabWS001 (Haematology analyser) | To analyze blood samples and to provide said metrics | Calibration inconsistencies | Inaccurate test results | May compromise lab's functionality and reputation | Low | High | Low | 3 | 2 | Maintenance/Operability controls by a specified technician every 2 yrs. | Control logs that are being analyzed | 4 | 24 |
| 27 | A-002 | PCWS001 (Workstation) | Analyze the metrics and crawl said data (Lab) | Workstation exposure to dangerous substances | Hardware mulfunction | Workstation unavailability, could impact lab's function | None | Low | Mid | 2 | 1 | Staff is complying to secure toxic substance transport procedure | | 3 | 6 |
| 28 | A-003 | PCWS002 (Workstation) | Modelling and Simulation | Weak password authentication | Unauthorized access to the workstation | Could compromise sensitive data and lab procedures | High | High | Low | 7 | 3 | Weak Password authentication | | 5 | 105 |
| 29 | A-004 | PCWS003 (Workstation) | Sending data samples to lab | Workstation operator is lacking of security training | Lab's and data security is compromised | Client data exposure/mismanagement | High | High | Low | 6 | 3 | | | 6 | 108 |
| 30 | A-005 | PCWS004 (Workstation) | Appointment scheduling - Customer data management | Workstation can browse third party websites and applications that are not relevant to the labs procedures | Human error can cause security breach | Lab's security is compromised | Medium | Medium | Medium | 5 | 3 | Firewall is implemented but not properly placed/configured | | 4 | 60 |
| 31 | A-006 | PCWS005 (Workstation) | Data and appointment management. Also keeps lab's backups | Workstation is connected to a router that is located in a different busy area (waiting room) | Traffic sniffing/ Man the middle attacks | Malicious actor can retreive or tamper with sensitive data | High | High | Low | 8 | 2 | OS keeps backup restoration points | | 7 | 112 |
| 32 | A-007 | PR0001 (PageWide Printers) | Used to print various lab documents that contain sensitive client and lab procedure data | Printer is kept at an unsecured crowded room | Anauthorized access to sensitive documents | Exposure of Sensitive Data _ GDPR Penalty | High | Low | Low | 2 | 2 | Printer is located behind the secretary's office which reduces chances of exposure | | 3 | 12 |
| 33 | A-008 | PR0002 (Printer) | Used to print various lab documents that contain sensitive client and lab procedure data | Misconfiguration in printer's memory purging settings | Anauthorized access to printer's memory / data leakage | Exposure of Sensitive Data and Lab Procedures | High | Low | Low | 3 | 3 | Memory is set to be purged manually at this time in case of maintenance | | 5 | 45 |
| 34 | A-009 | SRV001 (Web Server) | Web server is hosting our website application in order for clients to receive their results remotely | Web server settings misconfiguration | Could cause webserver downtime | Website is unavailable to the public / Clients can't access their results | None | None | Medium | 8 | 2 | | Server logs | 6 | 96 |
| 35 | A-010 | SRV002 (Database Server) | Our database server keeps all clients medical results and personal data | Weak authentication mechanisms | Anauthorized access to the database data | Exposure or damage of Sensitive Data _ GDPR Penalty | High | High | Low | 7 | 4 | Password authentication | | 6 | 168 |
| 36 | A-011 | SW001 (Switch) | Network Extension | Switch settings misconfiguration | Mac address spoofing - Attacker can pretend to be a trusted device retreiving lab's sensitive data | Exposure of Sensitive Data _ GDPR Penalty | High | Low | Low | 7 | 3 | VLAN Tagging | | 5 | 105 |
| 37 | A-012 | SW002 (Switch) | Network Extension | STP root bridge misconfiguration | STP manipulation attack | Network compromise - Sensitive data exposure, damage or manipulation | High | High | Low | 7 | 2 | VLAN Tagging | | 6 | 84 |
| 38 | A-013 | RT001 (Router) | Forwards data packets between computer networks, allowing devices on different networks to communicate with each other. | Older Router model (2010) | Device no longer receives security updates / Vulnerable to newer cyber attacks | Network compromise - Sensitive data exposure, damage or manipulation | High | High | Low | 7 | 1 | Router provides some level of security especially with older threats | | 6 | 42 |
| 39 | A-014 | FW001 (Firewall) | To block unauthorized network traffic | Non-updated OS version | Firewall's security bypass | Network compromise - Sensitive data exposure, damage or manipulation | High | High | Low | 7 | 2 | Current version provides some level of security | | 6 | 84 |
| 40 | A-015 | LTP001 (Laptop) | For personal use and business appoinment review | Device connectes to other public networks | Compromized device | Client and lab data leakage / manipulation | High | High | Low | 4 | 3 | Windows Firewall | | 4 | 48 |
| 41 | A-016 | Customer Data | All customers' data | Social Engineering | Extortion of personal data/customer data | Exposure of Personal Data - GDPR Penalty. Negative impact on lab's trustworthiness | High | Low | Low | 4 | 5 | | | 4 | 80 |
| 42 | A-017 | Employee Data | Supports Employees Filing Obligations, Payments, Personal Records | Insider threat | Unauthorized access to sensitive data | Exposure/Manipulation of sensitive data against the lab's and its employees benefit | High | High | Low | 6 | 5 | Internal Employee Rules, Data password protection | | 4 | 120 |
| 43 | A-018 | Windows 7 Pro | OS for routers and switches | OS susceptible to fork bomb attacks | Catastrophic memory overflow | Core System OS Failure | Medium | Medium | High | 7 | 2 | Partially updated antivirus software | Event Viewer, Windows Firewall | 3 | 42 |
| 44 | A-019 | Windows 10 Pro | OS for workstations | Zerologon(CVE-2020-1472) | Severe Weakening of the main domain controller | Core System OS undermining-exposure of sensitive logs | High | High | Low | 6 | 4 | Microsoft Update Patch | Event Viewer | 4 | 96 |
| 45 | A-020 | Website (JOOMLA) | Lab's website where clients can login to receive their results | Website is created by the lab owner - Limitless login attempts can be performed | Brute force attacks | Unauthorized access to admin or clients accounts - Sensitive data leakage or tampering | High | High | Low | 7 | 3 | | | 9 | 189 |
| 46 | A-021 | Φυσικό Αρχείο Ασθενών | Contains most clients data and test results | Data is being kept in an area vulnerable to accidents | Accident caused by employee/client | Damage or destruction of the patient's physical archives | Low | High | Medium | 4 | 2 | Small lock on the container | | 3 | 24 |
| 47 | A-022 | Αρχείο Υπαλλήλων & Προμηθευτών | Supports Filing Obligations, Payments, Accounting Records | Substances that can alter (or even destroy the files) are stored nearby | Destruction or serious obfuscation of the files | Sensitive data loss | None | High | HIgh | 8 | 5 | | Fire Detector/Physical Monitoring | 6 | 240 |
| 48 | A-023 | Εφεδρική Γεννήτρια | Provides backup electricity for limited time duration in case of an emergency black-out | Generator is kept at unsecured backyard (no fence) | Damage or theft by malicious individual | Lab remains with no electricity backup - Can directly hurt lab's availability | None | None | High | 8 | 2 | | Led indicator in case of damage | 7 | 112 |
| 49 | A-024 | Αντίγραφα Ασφαλείας | Data Protection in case of stolen/broken hardware (PC) | Data backups are being kept in the doctor's workstation | Deletion or exposure of confidential information | Exposure of Personal Data _ GDPR Penalty. Also exposure of data immediately correlated to the lab personnel | High | HIgh | Low | 6 | 4 | Protection provided by local workstation | | 5 | 120 |
| 50 | A-025 | Χημικές Ουσίες | Auxiliary means to complete lab tasks | The substances are being held in a room with open doors | Valuable substances could be stolen by malicious people | The lab is burdened with the expense of acquiring new materials for its operation | None | High | High | 7 | 3 | Substances are kept in hard to open containers | | 5 | 105 |

# 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

Στην αρχή καταγράφονται οι απειλές και ευπάθειες που σχετίζονται με την ανάγκη για την εφαρμογή των κάτωθι μέτρων ασφαλείας.

1. Κλοπή των συνθηματικών πρόσβασης του υπολογιστή. - Εισαγωγή συνθηματικών σε κοινή θέα.
2. Χρήση μεθόδων ιδιαίτερα επικίνδυνες προς ανθρώπους με άγνοια των κινδύνων, όπως το social engineering / phishing. - Έλλειψη ευαισθητοποίησης των εργαζομένων με τα απαραίτητα μέτρα ασφάλειας.
3. Εκμαίευση προσωπικών πληροφοριών/δεδομένων των πελατών. - Social engineering.

Έπειτα, τα μέτρα ασφαλείας.

- Καλλιέργεια κουλτούρας ασφάλειας και προστασίας. Παρότρυνση για υιοθέτηση της από τους εργαζομένους με ανταμοιβές. (1)
- Επιμόρφωση των υπαλλήλων για την ασφάλεια και την προστασία. Οι υπάλληλοι δεν θα κάνουν τα ίδια λάθη εν έγνοια των κινδύνων που υποβόσκουν από αυτά. (2)
- Εκπαίδευση των υπαλλήλων στην σωστή χρήση του ηλεκτρονικού ταχυδρομείου. (3)

## 4.2. Ταυτοποίηση και αυθεντικοποίηση

1. Ανεπαρκής έλεγχοι αυθεντικοποίησης και επικύρωσης. - Ο υπολογιστής και τα δεδομένα του μπορούν να αλλοιωθούν από ακατάλληλο άνθρωπο.
2. Ασθενή ή default admin κωδικοί. - Εγκατάσταση Ιομορφικού λογισμικού λόγω της σύνδεσης δικτύου.
3. Αδύναμοι μηχανισμοί αυθεντικοποίησης και εξουσιοδότησης. - Μη εξουσιοδοτημένος χρήστης έχει πρόσβαση στον διακομιστή.
4. Χρήση εργοστασιακών κωδικών. - Πρόσβαση στις ρυθμίσεις του δρομολογητή.

- Χρησιμοποίηση two-factor authentication. Η πρόσβαση στα μηχανήματα θα απαιτεί δύο βήματα ως εκ τούτου θα είναι πιο δύσκολη η παραβίαση ενός μηχανήματος. (1)
- Θέσπιση πολιτικών σχετικές με την επιλογή κωδικών. Οι κωδικοί που επιλέγονται θα πρέπει να είναι δυνατοί και περίπλοκοι (χρήση συμβόλων, αριθμών, κεφαλαίων γραμμάτων…). (2, 4)
- Χρήση σύγχρονων μέσων αυθεντικοποίησης. Για παράδειγμα θα μπορούσαν να χρησιμοποιηθούν βιομετρικοί παράμετροι για την αυθεντικοποίηση και αυθεντικοποίηση των χρηστών. (3)

### 4.3. Έλεγχος προσπέλασης και χρήσης πόρων

1. Παροχή περισσότερων δικαιωμάτων σε χρήστες που δεν τα χρειάζονται. - Υπάλληλος με κακόβουλες προθέσεις μπορεί να χρησιμοποιήσει τα ενισχυμένα δικαιώματα για να υποβαθμίσει την ασφάλεια του συστήματος.
2. Απουσία αντιγράφων ασφαλείας. - Απειλή παρακράτησης δεδομένων έναντι ρήτρας (ransomware).

- Επιβολή access controls. Με την επιβολή ελέγχων προσπέλασης, όπως το role-based access control, μπορούμε να περιορίσουμε τον αριθμό των πόρων στους οποίους έχει πρόσβαση ένα χρήστης, και να του δώσουμε μόνο όσους έχει πραγματικά ανάγκη. (1)
- Εφαρμογή του πρωτοκόλλου του ελάχιστου προνομίου (least privilege). Ο χρήστης έχει στην διαθεσιμότητα τους ελάχιστα δυνατούς πόρους, έτσι ώστε να κάνει την δουλειά του. (1)
- Λήψη ημερησίων αντιγράφων ασφαλείας με σκοπό την προφύλαξη από τυχόν απόπειρες ransomware. (2)

### 4.4. Διαχείριση εμπιστευτικών δεδομένων

1. Οι εκτυπωτές μας βρίσκονται σε μη ασφαλή τοποθεσία όπου μη εξουσιοδοτημένο προσωπικό μπορεί να έχει πρόσβαση. - Κλοπή πληροφοριών των εγγράφων που εκτυπώνονται.
2. Τα αρχεία βρίσκονται σε δωμάτιο στο οποίο πολλά άτομα έχουν πρόσβαση. - Ανταγωνιστές λαμβάνουν οικονομικά στοιχεία της επιχείρησης.
3. Απειλή εκ των έσω (Insider threat). - Εκμετάλλευση στοιχείων πελατών.
4. Ακατάλληλη ξεφόρτωση ευαίσθητων πληροφοριών. - Αποκάλυψη ευαίσθητων πληροφοριών.

5. Μη κρυπτογράφηση της πληροφορίας. - Παραβίαση της πολιτικής απορρήτου.
6. Τα αρχεία φυλάσσονται σε κοινή θέα. - Αποκάλυψη επιβλαβών πληροφοριών προς την επιχείρηση
7. Τα αρχεία φυλάσσονται σε μέρος χωρίς μέτρα ασφαλείας. - Τα αρχεία μπορούν να κλαπούν από κακοπροαίρετο άτομο.

- Περιορισμός της πρόσβασης σε εμπιστευτικά δεδομένα. Τα εμπιστευτικά δεδομένα της επιχείρησης θα φυλάσσονται σε χώρους στους οποίους θα εισέρχονται μόνο αρμόδιοι. (1, 2)
- Non-disclosure agreements. Μερικές φορές είναι απαραίτητο οι υπάλληλοι να έχουν πρόσβαση σε ευαίσθητα δεδομένα. Με την υπογραφή συμφωνίας εχεμύθειας, υπάλληλος που θα αποκαλύψει εμπιστευτικές πληροφορίες θα έρθει αντιμέτωπος με βαριές ποινικές κυρώσεις. (3)
- Εφαρμογή πολιτικής εμπιστευτικότητας. Ο κάθε υπάλληλος θα γνωρίζει πως πρέπει να διαχειριστεί ευαίσθητα δεδομένα. Με αυτόν τον τρόπο ελαχιστοποιείται η πιθανότητα ανθρώπινου λάθους. (4)
- Κρυπτογράφηση των ηλεκτρονικών δεδομένων. Μόνο εξουσιοδοτημένο προσωπικό που γνωρίζει τον αλγόριθμο κρυπτογράφησης - αποκρυπτογράφησης θα είναι σε θέση να εξάγει πληροφορία από τα δεδομένα. (5)
- Λήψη φυσικών μέσων προστασίας. Εγκατάσταση καμερών ασφαλείας, συστήματα συναγερμού, τοποθέτηση κλειδαριών σε ερμάρια. (6, 7)

## 4.5 Προστασία από τη χρήση υπηρεσιών από τρίτους

1. Αναντιστοιχία βαθμονόμησης: Οι αιματολογικοί αναλυτές απαιτούν τακτική βαθμονόμηση για την εξασφάλιση ακριβών αποτελεσμάτων. Εάν η βαθμονόμηση δεν εκτελεστεί σωστά, ο αναλυτής δεν μπορεί να παράγει αξιόπιστα αποτελέσματα. - Μη εξουσιοδοτημένη πρόσβαση: Εάν κάποιος αποκτήσει μη εξουσιοδοτημένη πρόσβαση στον αναλυτή ή στο δίκτυο στο οποίο είναι συνδεδεμένος, ενδέχεται να μπορεί να τροποποιήσει ή να χειραγωγήσει τα αποτελέσματα ή να αποκτήσει πρόσβαση σε εμπιστευτικές πληροφορίες ασθενούς.
2. Οι εκτυπωτές μας βρίσκονται σε μη ασφαλή τοποθεσία όπου μη εξουσιοδοτημένο προσωπικό μπορεί να έχει πρόσβαση. - Μη εξουσιοδοτημένη πρόσβαση. Εφόσον ο εκτυπωτής παρέχει συνδεσιμότητα δικτύου κάποιο μη εξουσιοδοτημένο άτομο μπορεί να αποκτήσει πρόσβαση.
3. Απουσία φυσικής προστασίας. Ο υπολογιστής αφείνεται ανοιχτός σε χώρο με πελάτες. - Χρήση του μηχανήματος από μη εξουσιοδοτημένο άτομο.
4. Φύλαξη των χημικών ουσιών σε πολυσύχναστο χώρο. - Κλοπή των χημικών ουσιών από κακόβουλους τρίτους

- Παρακολούθηση και καταγραφή συνδέσεων (monitoring and logging). Με αυτόν τον τρόπο θα ανιχνεύονται τυχόν ύποπτες συνδέσεις ή απόπειρες σύνδεσης. (1)

- Ανίχνευση και άμεση αντιμετώπιση εισβολών. Χρήση συστημάτων ανίχνευσης εισβολών και αποτροπής εισβολών. (2)
- Ασφάλεια τελικών σημείων (Endpoint security). Σήμερα, αρκετές επιθέσεις στοχεύουν απευθείας στα τελικά σημεία του δικτύου (σταθμοι εργασίας, φορητοί υπολογιστές, εκτυπωτές…). Η προστασία τους θα αποτρέψει τρίτους από την εκμετάλλευσή τους. (2)
- Πρακτικές φυσικής ασφάλειας. Εκπαίδευση των χρηστών των μηχανημάτων να κλειδώνουν τις συσκευές τους όταν απομακρύνονται από αυτές, να αποφεύγουν να σημειώνουν κωδικούς σε ανοιχτούς χώρους και να εφαρμοστεί πολιτική κλειδώματος χώρων. (3, 4)

### 4.6 Προστασία λογισμικού

1. Δυσλειτουργικό Λογισμικό: Οι αιματολογικοί αναλυτές λειτουργούν βάσει λογισμικού, το οποίο μπορεί να είναι επιρρεπές σε σφάλματα και bugs βασισμένα στον πηγαίο του κώδικα. Μια πιθανή ευπάθεια λογισμικού μπορεί να προκαλέσει εσφαλμένα αποτελέσματα και να θέσει σε κίνδυνο τη φροντίδα του ασθενούς. - Αστοχία εξοπλισμού: Η αστοχία του εξοπλισμού μπορεί να προκαλέσει διακοπές λειτουργίας, οδηγώντας σε καθυστερημένα ή ανακριβή αποτελέσματα ή αδυναμία ανάλυσης δειγμάτων.
2. Μη αναβαθμισμένο firmware. Παρατηρούμε ότι και οι δύο εκτυπωτές μας χρησιμοποιούν μια παλιά έκδοση υλικολογισμικού με γνωστές ευπάθειες που δίνουν χώρο στις απειλές. - Μη εξουσιοδοτημένη πρόσβαση. Εφόσον ο εκτυπωτής παρέχει συνδεσιμότητα δικτύου κάποιο μη εξουσιοδοτημένο άτομο μπορεί να αποκτήσει πρόσβαση.
3. Εσφαλμένες ρυθμίσεις διακομιστή. - Εισαγωγή ανεπιθύμητων χαρακτηριστικών.
4. Λάθος δομημένος κώδικας. - SQL Injection attack.
5. Παλιά έκδοση του λογισμικού που δε περιέχει τα πιο πρόσφατα security patches and fixes. - Keyloggers
6. Εγκατάσταση μη αξιόπιστου third-party λογισμικού. - Rootkits

Θα πρέπει να προσέξουμε τα λογισμικά που θα χρησιμοποιούμε να έχουν τα εξής:

- Ασφαλείς πρακτικές κωδικοποίησης. Κατά την διάρκεια ανάπτυξης του λογισμικού θα πρέπει να ακολουθηθούν ασφαλείς πρακτικές κωδικοποίησης, έτσι ώστε να μειωθεί η πιθανότητα να βρεθεί ελάττωμα στην ασφάλεια του λογισμικού. (1, 4)
- Τακτικές κριτικές κώδικα. Βοηθούν στην ανίχνευση πιθανών ευπαθειών. (1, 4)
- Επικύρωση εισόδου. Αποτρέπει στην αποφυγή εκπόνησης απειλών όπως injection attacks. (4)
- Τακτικές ενημερώσεις και αναβαθμίσεις. Το λογισμικό πρέπει να ενημερώνεται διαρκώς ώστε να μπορεί να συμβαδίζει με τις τελευταίες εξελίξεις που παρουσιάζονται στον χώρο της ασφάλειας των πληροφοριακών συστημάτων. Χωρίς, τις ενημερώσεις, το σύστημα θα καθιστάται ευάλωτο σε καινοτόμες απειλές. (2, 5)

- Δοκιμασία σε penetration testing. Η ασφάλεια του λογισμικού πρέπει να δοκιμαστεί σε όσο το δυνατόν πλησιέστερες με την πραγματικότητα συνθήκες. (3)
- Επαλήθευση των third party programs που χρησιμοποιούνται από το λογισμικό. Η ασφάλεια τους πρέπει να εγγυάται από αρμόδιο φορέα. (6)

## 4.7 Διαχείριση ασφάλειας δικτύου

1. Σύνδεση με δρομολογητή που βρίσκεται σε πολυσύχναστο χώρο. - Απόσπαση σημαντικών πληροφοριών καθώς αυτές μεταφέρονται μέσω του δρομολογητή.
2. Εσφαλμένες ρυθμίσεις. - VLAN hopping/Switch flooding.
3. Απαρχαιωμένο υλικολογισμικό. - MAC address spoofing.
4. Αδύναμη κρυπτογράφηση. - Βιομηχανική κατασκοπεία.
5. Χρήση παλαιότερης έκδοσης. - Τεχνικές παράκαμψης ασφάλειας.
6. Χαλαρή πρόσβαση στο τείχος προστασίας. - Εκμετάλλευση ευάλωτων πρωτοκόλλων.
7. Σύνδεση σε δημόσιο δίκτυο. - Κλοπή δεδομένων μέσω της σύνδεσης με το διαδίκτυο.

- Ενίσχυση του τείχους προστασίας. Η σωστή ρύθμιση του τείχους προστασίας μπορεί να αποτρέψει μη εξουσιοδοτημένη πρόσβαση στο δίκτυο και να αποτρέψει κακόβουλη κυκλοφορία από το να μπει στο δίκτυο. (6)
- Τμηματοποίηση του δικτύου (e.g. VLAN). Η τμηματοποίηση του δικτύου μπορεί να περιορίσει το αντίκτυπο πιθανών παραβιάσεων της ασφάλειας απομονώνοντας ευαίσθητα δεδομένα και συστήματα από λιγότερο ασφαλείς περιοχές του δικτύου. (1, 2)
- Κρυπτογράφηση. Η κρυπτογράφηση μπορεί να βοηθήσει στην προστασία των δεδομένων κατά την μεταφορά αυτών στο δίκτυο μας, καθιστώντας πιο δύσκολη την ερμηνεία τους από τους επιτιθέμενους. (4)
- Τακτικές αξιολογήσεις ευπάθειας δικτύου. Οι τακτικές αξιολογήσεις μπορούν να βοηθήσουν στον εντοπισμό πιθανών τρωτών σημείων και αδυναμιών σε ένα δίκτυο, επιτρέποντας στους διαχειριστές του δικτύου να τις αντιμετωπίσουν προτού τις εκμεταλλευτούν οι εισβολείς. (1, 2)
- Παρακολούθηση και καταγραφή δικτύου. Η παρακολούθηση και η καταγραφή της δραστηριότητας του δικτύου μπορεί να βοηθήσει στον εντοπισμό πιθανών παραβιάσεων ασφάλειας και άλλης ύποπτης δραστηριότητας, επιτρέποντας στις ομάδες ασφαλείας να αναλάβουν δράση για να αποτρέψουν περαιτέρω επίθεση. (1, 2)
- Τακτική ενημέρωση του λογισμικού του δρομολογητή. Οι τακτικές ενημερώσεις των συσκευών που αποτελούν το δίκτυο, ειδικά του δρομολογητή, είναι απαραίτητες για να αποτραπεί η εύκολη είσοδος από τους παραβάτες. (5)
- IP Whitelisting. Το IP Whitelisting συμβάλλει στον περιορισμό και τον έλεγχο της πρόσβασης μόνο σε αξιόπιστους χρήστες. (7)

## 4.8 Προστασία από ιομορφικό λογισμικό

1. Απουσία λογισμικού Antivirus. - Προσβολή από ιό.
2. Απουσία antivirus. - Προσβολή από ιομορφικό λογισμικό.
3. Παλιά έκδοση του λογισμικού που δε περιέχει τα πιο πρόσφατα security patches and fixes. - Προσβολή από ιομορφικό λογισμικό
4. Μη αναβαθμισμένο firmware. Παρατηρούμε ότι και οι δύο εκτυπωτές μας χρησιμοποιούν μια παλιά έκδοση υλικολογισμικού με γνωστές ευπάθειες που δίνουν χώρο στις απειλές. - Εγκατάσταση Ιομορφικού λογισμικού λόγω της σύνδεσης δικτύου.

- Εγκατάσταση antivirus προγράμματος. (1, 2)
- Εγκατάσταση anti-spyware και anti-malware προγράμματα. (1, 2)
- Τακτική ενημέρωση τους συστήματος. (3, 4)
- Ρύθμιση αυτόματων σαρώσεων. (1, 2, 3, 4)
- Αναβάθμιση firmware. (4)

## 4.9 Ασφαλής χρήση διαδικτυακών υπηρεσιών

1. Σύνδεση σε μη αξιόπιστες σελίδες. - Απόπειρα hacking.
2. Καθώς ο Ιστότοπος δεν έχει σχεδιαστεί από ειδικό σε θέματα ασφαλείας, ενδέχεται να υπάρχουν “τρύπες” στην ασφάλεια του. - Denial-of-service attack.
3. Μη εφαρμογή ελέγχου ορίου σε εισαγωγές των χρηστών. - Buffer Overflow.
4. Μη έλεγχος αριθμού προσπάθειας εισόδου σε λογαριασμό χρήστη. - Brute-force attack.
5. Απουσία προστασίας συνεδρίας. - Denial-of-service attack.

- Αποφυγή ύποπτων ιστοσελίδων. Ένας ασφαλής τρόπος διαχωρισμού επικίνδυνων ιστοσελίδων είναι μέσω του πρωτοκόλλου που χρησιμοποιεί η ιστοσελίδα. Ιστοσελίδες οι οποίες είναι ασφαλής χρησιμοποιούν το https, αυτό σημαίνει πως έχουν πιστοποιητικό που βεβαιώνει ότι η σύνδεση είναι ασφαλής. (1)
- Έλεγχος στα αρχεία που κατεβαίνουν από το διαδίκτυο. Πολλές φορές απειλές κρύβονται μέσα σε επικίνδυνα αρχεία. Με το σκανάρισμα των αρχείων που κατεβαίνουν από το διαδίκτυο μπορούμε να αποτρέψουμε δόλιος κινδύνους από το να προκαλέσουν ζημιά. (1)
- Επανασχεδιασμός της ιστοσελίδας της επιχείρησης μας από επαγγελματία developer. (2)
- Εφαρμογή ελέγχου ορίου στις εισαγωγές των χρηστών. Για να αποτρέψουμε τυχόν επιθέσεις Buffer Overflow, θα χρειαστεί σε κάθε είσοδο που πληκτρολογεί ο χρήστης να εφαρμοστεί όριο στους χαρακτήρες που μπορεί να εισάγει. (3)
- Όριο στις απόπειρες που μπορεί να κάνει ένας χρήστης για να συνδεθεί στον λογαριασμό του. Για να προστατέψουμε τους λογαριασμούς της ιστοσελίδας μας από Brute-force attack επιθέσεις, θα χρειαστεί να εφαρμόσουμε όριο

στον αριθμό των απόπειρων για είσοδο που μπορούν να γίνουν σε ένα χρονικό διάστημα. (4)
- Χρήση cookies ασφάλειας. Η χρήση τους θα διασφαλίζει ότι τα δεδομένα της περιόδου σύνδεσης είναι κρυπτογραφημένα και δεν μπορούν εύκολα να υποκλαπούν από τους εισβολείς. (5)

## 4.10 Ασφάλεια εξοπλισμού

1. Hardware Failure/Malfunction: Τα στοιχεία υλισμικού ενός αιματολογικού αναλυτή, όπως τα κύτταρα ροής, οι βαλβίδες και οι αισθητήρες, μπορεί να φθαρούν ή να δυσλειτουργούν, οδηγώντας σε εσφαλμένα αποτελέσματα ή σε αδυναμία ανάλυσης δειγμάτων. - Παραβιάσεις φυσικής ασφάλειας: Εάν ο αναλυτής δεν έχει ασφαλιστεί σωστά, μπορεί να κλαπεί ή να παραβιαστεί, θέτοντας σε κίνδυνο την ακεραιότητα των αποτελεσμάτων ή την εμπιστευτικότητα των δεδομένων του ασθενούς.
2. Έκθεση του hardware σε επιβλαβείς ουσίες. - Τα μηχανικά κομμάτια του υπολογιστή θα πάψουν να λειτουργούν.
3. Φύλαξη σε χώρο με χημικές ουσίες. - Καταστροφική ζημιά στο hardware του διακομιστή
4. Φύλαξη των χημικών ουσιών στον ίδιο χώρο μαζί με άλλα πολύτιμα asset. - Μόλυνση του χώρου φύλαξης που μπορεί να προκαλέσει κινδύνους υγείας.

- Τακτική συντήρηση λογισμικού. Ο τακτικός έλεγχος για την λειτουργικότητα των μηχανημάτων είναι απαραίτητος, ώστε τα μηχανήματα να συνεχίσουν να λειτουργούν δίχως να εμφανίζουν προβλήματα. Ο έλεγχος πρέπει να είναι μηνιαίως έως και ετήσιος, ανάλογα με το είδος και την σημασία του εκάστοτε μηχανήματος. (1)
- Σωστή τοποθέτηση. Ο εξοπλισμός πρέπει να βρίσκεται σε κατάλληλο δωμάτιο με κατάλληλη θερμοκρασία, μακριά από επιβλαβείς ουσίες. Με αυτόν τον τρόπο, η διάρκεια ζωής του εξοπλισμού θα επεκταθεί και η πιθανότητα ζημιάς στο hardware θα μειωθεί. (2)
- Θέσπιση ειδικού χώρου για την αποθήκευση επικίνδυνων περιουσιακών στοιχείων της επιχείρησης. Ο χώρος πρέπει να είναι καλά προστατευμένος και πρέπει να αναγνωρίζεται από ειδική σήμανση, για να αποφευχθούν ατυχήματα. Η ασφάλεια των επικίνδυνων περιουσιακών στοιχείων της επιχείρησης έχει άμεση συσχέτιση με την ασφάλεια του εξοπλισμού της επιχείρησης, καθώς η πρώτη ενισχύει την δεύτερη. (3, 4)
- Εκπαίδευση του προσωπικού στην σωστή χρήση του εξοπλισμού. Παροχή εκπαίδευσης στο προσωπικό για να επιβεβαιωθεί πως υπάρχει επίγνωση των πιθανών κινδύνων και γνώση του σωστού χειρισμού του εξοπλισμού. (1, 4)

## 4.11 Φυσική ασφάλεια κτιριακής εγκατάστασης

1. Η είσοδος στον χώρο των διακομιστών είναι “ελεύθερη”. - Κλοπή ή πρόκληση ζημιάς στον διακομιστή (Η πόρτα είναι μισάνοιχτη σε κεντρικό δρόμο).
2. Απειλή εκ των έσω (Insider threat). - Εκμαίευση προσωπικών πληροφοριών/δεδομένων των υπαλλήλων.

3. Φυσικές καταστροφές. - Απώλεια σημαντικών πληροφοριών.
4. Φύλαξη των χημικών ουσιών σε μη ασφαλή χώρο (μισάνοιχτη πόρτα). - Φυσική καταστροφή του εργαστηριακού χώρου λόγω φωτιάς.

- Τοποθέτηση πορτών ασφαλείας. Κάθε πόρτα του εργαστηρίου θα πρέπει να αντικατασταθεί από πόρτα ασφαλείας για να προφυλαχθεί το ίδιο από κακόβουλους εισβολείς. (1)
- Εγκατάσταση σύγχρονων καμερών σε κάθε δωμάτιο του κτιρίου και πέριξ αυτού. Το μέτρο αυτό πέρα από το να ενεργεί σαν ένα αποθαρρυντικό στοιχείο για τους φιλόδοξους εισβολείς, θα συμβάλει στην αναγνώριση των υπαίτιων που έχουν προβεί σε κακόβουλες ενέργειες στο χώρο της επιχείρησης. (2)
- Το κτίριο οφείλει να συμμορφώνεται με τους κανόνες ασφαλείας και τους νόμους που επιβάλλονται από το κράτος. Για να αποφευχθούν σοβαρές επιπτώσεις από φυσικές καταστροφές, το κτίριο πρέπει να τηρεί ορισμένες προδιαγραφές σχετικές με την ασφάλεια του. (3)
- Σχεδίαση ανεπτυγμένου συστήματος εξαερισμού. Σε χώρους όπου διαχειρίζονται επικίνδυνες ουσίες, είναι απαραίτητο να εγκατασταθεί προηγμένο σύστημα εξαερισμού, έτσι ώστε να διασφαλιστεί η ασφάλεια του προσωπικού και των πελατών της επιχείρησης. (4)
- Στήσιμο φράχτη προστασίας. Ο αύλειος χώρος της επιχείρησης μας είναι απροστάτευτος, ένας σύγχρονος φράχτης προστασίας θα δρούσε ως μέτρο προστασίες ενάντιας σε εισβολείς. (1)
- Τοποθέτηση συναγερμού ασφαλείας. Ανίχνευση μη εξουσιοδοτημένης εισόδου. Οι συναγερμοί μπορούν να είναι συνδεδεμένοι με υπηρεσία παρακολούθησης που θα ανταποκρίνεται γρήγορα στους συναγερμούς. (1, 2)
- Επαρκής φωτισμός. Θα πρέπει να εξασφαλιστεί ότι οι χώροι του κτιρίου, τόσο στο εσωτερικό όσο και στο εξωτερικό, είναι επαρκώς φωτισμένοι. Αυτό μπορεί να αποτρέψει την εγκληματική δραστηριότητα και να βοηθήσει το προσωπικό ασφάλειας να εντοπίσει ύποπτη συμπεριφορά. (1, 2)

# 5 ΣΥΝΟΨΗ ΚΡΙΣΙΜΩΝ ΑΠΟΤΕΛΕΣΜΑΤΩΝ

| ASSET | RISK |
|---|---|
| **A-020**<br>Website(JOOMLA) | **315** |
| **A-010**<br>Database Server (SRV002) | **270** |
| **A-024**<br>Αντίγραφα Ασφαλείας | **243** |
| **A-025**<br>Χημικές Ουσίες | **243** |
| **A-014**<br>Firewall | **225** |

---

Για την προστασία του website κρίνεται ως απαραίτητη η τακτική συντήρηση του κώδικα από ομάδα επαγγελματιών developers έτσι ώστε να αποφευχθεί σωρεία επιθέσεων από εξωγενείς παράγοντες (κακόβουλους χακερς, ιομορφικό λογισμικό κ.τ.λ.) μέσω της εξάλειψης προϋπαρχουσών αλλά και συμφυών με την αναδρομική συντήρηση ευπαθειών που ενδεχομένως να εμφανιστούν. Έτσι, με την επιβολή ενός role-based access model που θα επιτρέπει την πρόσβαση στα νευραλγικά components του website μόνο στους εξουσιοδοτημένους χρήστες (μέσω 2FA), την χρήση απαραίτητης κρυπτογράφησης (TLS/SSL), την χρήση ισχυρών κωδικών ταυτοποίησης αλλά και την επιλογή ενός αξιόπιστου παρόχου hosting ιστοσελίδων δύναται να εγγυηθεί η ασφαλής και ακώλυτη λειτουργία του διαδικτυακού μας ιστότοπου.

Όσον αφορά τον database server, ισχύουν εν μέρει τα άνωθι μέτρα προστασίας αλλά εδώ πρέπει να δοθεί ιδιαίτερη σημασία στην ορθή αυθεντικοποίηση των χρηστών και διαχειριστών του server. Η επιβολή ενός θεσμοθετημένου μοντέλου role-based access θα καταστεί κρίσιμη έτσι ώστε να περιορίσουμε τον αριθμό των χρηστών που έχουν πρόσβαση αποκλειστικά και μόνο στους απολύτως απαραίτητους. Επίσης, οφείλει να δοθεί προσοχή και στην ενεργή παρακολούθηση (monitoring) του server έτσι ώστε να μπορέσουμε σε πραγματικό να ανιχνεύσουμε και να εξουδετερώσουμε τυχόν απειλές. Δεν πρέπει να παραληφθεί και η τακτική τήρηση των πρωτοκόλλων για αποθήκευση των δεδομένων σε αντίγραφα ασφαλείας έτσι ώστε να μην οδηγηθούμε σε καταστροφική απώλεια δεδομένων με αδυναμία ανάκτησης αυτών.

Η προστασία των αντιγράφων ασφαλείας ενός εργαστηρίου είναι ζωτικής σημασίας για τη διατήρηση των δεδομένων και την αποφυγή απώλειας των αρχείων μας. Έτσι, αποθηκεύουμε τα αντίγραφα ασφαλείας σε ασφαλές μέρος που είναι προσβάσιμο μόνο από εξουσιοδοτημένα άτομα. Μπορούμε να αποθηκεύσετε

τα αντίγραφα ασφαλείας σε ένα απομακρυσμένο διακομιστή, σε ένα φυσικό ασφαλές μέρος, ή σε μια ασφαλή νεφοϋπολογιστική υπηρεσία αποθήκευσης.

Οι χημικές ουσίες είναι απαραίτητες για την απρόσκοπτη λειτουργία του εργαστηρίου καθώς αποτελούν πρώτη ύλη για πολλαπλές ανάγκες και λειτουργίες-κλειδιά του εργαστηρίου. Όμως, καθώς είναι εξαιρετικά εύφλεκτες αλλά και επικίνδυνες ακόμη και για το προσωπικό του εργαστηρίου οφείλουν να διατηρηθούν σε χώρο όπου εξασφαλίζεται η τήρηση όλων των προαπαιτούμενων μέτρων ασφαλείας όπως πυρασφάλεια, τακτική καθαριότητα και εξαερισμός αλλά και βιοασφάλεια του χώρου. Επιπλέον, πρέπει να γίνεται τακτικός έλεγχος των χημικών ουσιών και να απορρίπτονται οι παλιές και παρωχημένες ουσίες και μαζί με αυτό να πραγματοποιείται λελογισμένη διαχείριση των χημικών αποβλήτων του εργαστηρίου.

Το τείχος ασφαλείας αποτελεί το “σιδηρούν παραπέτασμα” μεταξύ εξωτερικών κινήσεων του διαδικτύου και των συσκευών που στελεχώνουν την δικτυακή υποδομή του εργαστηρίου. Έτσι, κρίνεται απαραίτητη η επαρκής προστασία του έτσι ώστε να μπορούν οι μεταγωγείς και ο δρομολογητής να επιτελέσουν την λειτουργία τους ανενόχλητοι δίχως την απόπειρα διεισδυσης από εξωγενείς κακόβουλους εισβολείς. Περιορίζεται λοιπόν η κίνηση δικτύου σε μη εγκεκριμένες υπηρεσίες ή χρήστες.

## 6. Βιβλιογραφία


https://www.datasunrise.com/potential-db-threats/10-common-vulnerabilities/

https://www.toptal.com/security/10-most-common-web-security-vulnerabilities

https://study.com/academy/lesson/vulnerabilities-issues-in-web-servers.html

https://www.cvedetails.com/vulnerability-list/vendor_id-3496/Joomla.html

https://readwrite.com/vulnerabilities-in-modern-routers-netgear-cisco-linksys-etc/

https://www.apriorit.com/dev-blog/771-cybersecurity-vulnerabilities-in-routers

https://www.trustnetinc.com/firewall-vulnerabilities/

https://www.brightfin.com/resources/top-5-laptop-security-threats-for-your-enterprise/

https://www.n-able.com/features/computer-security-vulnerabilities

https://www.xcitium.com/blog/news/computer-vulnerability-definition/

https://societyinsurance.com/blog/common-data-threats-and-vulnerabilities/#:~:text=Non%2DTechnical%20Vulnerabilities%20%E2%80%93%20Why%20is,loss%20of%20data%20or%20information.

https://www.commonplaces.com/blog/6-common-website-security-vulnerabilities/

https://brightsec.com/blog/security-misconfiguration/

https://www.sonitrolwesterncanada.com/blog/7-ways-to-ensure-safety-and-security-in-the-workplace

https://www.nationwide.com/business/solutions-center/cybersecurity/train-employees

https://auth0.com/blog/4-ways-to-strengthen-identity-authentication-for-technical-roles/

https://penneo.com/blog/data-confidentiality/

https://www.cypressdatadefense.com/blog/unauthorized-data-access/

https://www.cynet.com/network-attacks/unauthorized-access-5-best-practices-to-avoid-the-next-data-breach/

https://www.cypressdatadefense.com/blog/unauthorized-data-access/

https://www.silasg.com/resources/six-simple-steps-improve-software-security-reducing-code-errors

https://www.sunnyvalley.io/docs/network-security-tutorials/what-are-ways-to-improve-network-security

https://mytekrescue.com/how-to-increase-network-security-in-a-few-easy-ways/

https://www.chicagoitsolutions.com/2022/07/22/11-ways-to-protect-your-computer-from-viruses/

https://library.automationdirect.com/5-steps-to-improve-machine-safety/?utm_source=adc-newsletter&utm_medium=email&utm_campaign=6-30-15

https://www.360connect.com/product-blog/6-ways-to-improve-business-physical-security/

https://www.orbit-computer-solutions.com/network-security-stp-manipulation-attacks/