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

(Red Cell Lab)

ΜΕΛΗ ΟΜΑΔΑ ΕΡΓΑΣΙΑΣ:

1. **ΑΛΒΙΟΝΑ ΜΑΝΤΣΟ - 3200098 - p3200098@aueb.gr**
2. **ΓΕΩΡΓΙΑ ΠΕΤΣΑ - 3200155 - p3200155@aueb.gr**
3. **ΠΑΝΑΓΙΩΤΗΣ ΤΡΙΑΝΤΑΦΥΛΛΙΔΗΣ - 3200199 - p3200199@aueb.gr**

ΠΕΡΙΕΧΟΜΕΝΑ ΕΡΓΑΣΙΑΣ

1. ΕΙΣΑΓΩΓΗ

Η παρούσα εργασία περιλαμβάνει τη διεξαγωγή μιας ανάλυσης FMEA για ένα Μικροβιολογικό εργαστήριο. Κατά τη διάρκειά της εντοπίστηκαν πολλά τρωτά σημεία που το εκθέτουν σε διάφορες απειλές τόσο στον πραγματικό κόσμο όσο και στον κυβερνοχώρο, θέτοντας ενδεχομένως σε κίνδυνο την ακρίβεια και την αξιοπιστία των αποτελεσμάτων των εξετάσεων, καθώς και το απόρρητο και την ασφάλεια των δεδομένων των ασθενών.

Ο πρωταρχικός στόχος της εργασίας είναι να εντοπιστούν οι ευπάθειες των πληροφοριακών αγαθών, οι απειλές που μπορούν να εκμεταλλευτούν αυτές τις ευπάθειες, οι επιπτώσεις που σχετίζονται με τις λειτουργίες του εργαστηρίου καθώς και να γίνει μια δομημένη ιεράρχησή τους. Επιπλέον, αναπτύσσεται ένα ολοκληρωμένο σχέδιο αντιμετώπισης των κινδύνων.

Η επιτυχής ολοκλήρωση του σχεδίου που προτείνεται, θα διασφαλίσει ότι το εργαστήριο μπορεί να συνεχίσει να παρέχει ακριβή και αξιόπιστα αποτελέσματα αιματολογικών εξετάσεων, διατηρώντας παράλληλα το απόρρητο και την ασφάλεια των δεδομένων των ασθενών. Αυτό είναι καίριας σημασίας στον κλάδο της υγειονομικής περίθαλψης, όπου η ασφάλεια των δεδομένων των ασθενών είναι πρωταρχικής σημασίας.

1.1 Περιγραφή Εργασίας

Με γνώμονα την χαρτογράφηση του Πληροφοριακού Συστήματος που διεξήχθη από τον επιθεωρητή ασφαλείας μέσω της επιτόπιας καταγραφής, τα βήματα της μεθοδολογίας που επιλέγεται (Failure Mode and Effects Analysis - FMEA), την καταγραφή των πληροφοριακών αγαθών και τις νομικές απαιτήσεις στις οποίες εμπίπτει ένα μικροβιολογικό εργαστήριο, διεξάγουμε την αποτίμηση των αγαθών, τον προσδιορισμό, ανάλυση και αξιολόγηση των κινδύνων (μέσω της εξέτασης των απειλών, των ευπαθειών και των επιπτώσεων που αφορούν στην επιχείρηση). Τέλος παρουσιάζεται ένα σχέδιο αντιμετώπισης των κινδύνων που εντοπίστηκαν και προτάσεις για τον περιορισμό των επιπτώσεών τους.

1.2 Δομή παραδοτέου

Στην ενότητα 2 παρουσιάζεται η μεθοδολογία που ακολουθείται. Αρχικά περιγράφονται οι υποδομές και το Πληροφοριακό Σύστημα με καταγραφή όλων των εντοπισμένων αγαθών του εργαστηρίου. Στη συνέχεια, από τα αγαθά αυτά επιλέγονται εκείνα που πρόκειται να αξιολογηθούν στα πλαίσια της μελέτης και παρουσιάζονται κατηγοριοποιημένα, ανάλογα με τον τύπο τους (Εξοπλισμός & Υλισμικό, Λογισμικό και εφαρμογές, Δίκτυο, Δεδομένα, Διαδικασίες).

Στην ενότητα 3 αποτιμώνται τα αγαθά και παρατίθενται οι απειλές και οι ευπάθειες που αφορούν το καθένα εξ αυτών. Παρουσιάζονται, επίσης, τα αποτελέσματα της αποτίμησης σύμφωνα με τη μέθοδο FMEA.

Στην ενότητα 4, καταγράφονται τα προτεινόμενα μέτρα ασφαλείας για την αντιμετώπιση ή τον μετριασμό των ευπαθειών που αναφέρθηκαν στην ενότητα 3. Τα μέτρα αυτά διακρίνονται σε κατηγορίες ανάλογα τον σκοπό τους.

Τέλος, στην ενότητα 5 συνοψίζονται τα πιο κρίσιμα αποτελέσματα της μελέτης που έχει διενεργηθεί.

2. ΜΕΘΟΔΟΛΟΓΙΑ ΜΕΛΕΤΗΣ ΑΣΦΑΛΕΙΑΣ

Για τη Διαχείριση Επικινδυνότητας του Red Cell Lab 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 Red Cell Lab.

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

2.2 Εξοπλισμός & Υλισμικό (hardware)

Στην υποενότητα αυτή περιγράφονται συνοπτικά τα αγαθά που επιλέγουμε να εντάξουμε στην κατηγορία του Εξοπλισμού & Υλισμικού. Η επιλογή γίνεται μετά από εξέταση του τύπου των αγαθών. Συγκεκριμένα περιλαμβάνονται σταθμοί εργασίας, εκτυπωτές, διακομιστές, φορητοί υπολογιστές καθώς και ο αιματολογικός αναλυτής, εφόσον αποτελούν φυσικές συσκευές/μηχανήματα απαραίτητα για την αποθήκευση, επεξεργασία και διαχείριση πληροφοριών και την εκτέλεση λειτουργιών που υποστηρίζουν τις δραστηριότητες του εργαστηρίου. Ακολουθεί απαρίθμηση και συνοπτική περιγραφή των συγκεκριμένων αγαθών:

- **LabWS001** (A-001): Αιματολογικός Αναλυτής (Haematology Analyser).
  Βρίσκεται στο χώρο του Εργαστηρίου - Παρασκευαστηρίου.
  Μοντέλο: XS-1000i, *Κατασκευαστής*: Sysmex's XS-1000i, *Λειτουργικό Σύστημα:* Proprietary Software
  Λειτουργία: Διενέργεια ελέγχων επί των δειγμάτων αίματος.

- **PCWS001** (A-002): Σταθμός Εργασίας (Workstation).
  Βρίσκεται στο χώρο του Εργαστηρίου - Παρασκευαστηρίου.
  Μοντέλο: HP Pro G2 MT, *Κατασκευαστής*: HP, *Λειτουργικό Σύστημα:* Windows 10 Pro
  Λειτουργία: Διαχείριση και αποθήκευση αποτελεσμάτων αιματολογικών εξετάσεων (Complete Blood Count - γενική αίματος), διενέργεια ελέγχου ποιότητας αποτελεσμάτων, ερμηνεία αποτελεσμάτων και παραγωγή αναφορών. Επιπλέον επιτρέπει την επικοινωνία με τα υπόλοιπα μέρη του εργαστηρίου.

- **PCWS002** (A-003): Σταθμός Εργασίας (Workstation).
  Βρίσκεται στο χώρο του Εργαστηρίου - Παρασκευαστηρίου.
  Μοντέλο: HP Pro G2 MT, *Κατασκευαστής*: HP, *Λειτουργικό Σύστημα:* Windows 10 Pro
  Λειτουργία: Διαχείριση και αποθήκευση αποτελεσμάτων αιματολογικών εξετάσεων (Complete Blood Count - γενική αίματος), διενέργεια ελέγχου ποιότητας αποτελεσμάτων, ερμηνεία αποτελεσμάτων και παραγωγή αναφορών. Επιπλέον επιτρέπει την επικοινωνία με τα υπόλοιπα μέρη του εργαστηρίου.

- **PCWS003** (A-004): Σταθμός Εργασίας (Workstation).
  Βρίσκεται στο χώρο Λήψης Δειγμάτων.
  Μοντέλο: HP Pro G2 MT, *Κατασκευαστής*: HP, *Λειτουργικό Σύστημα:* Windows 10 Pro
  Λειτουργία: Καταγραφή των δειγμάτων αίματος με βάση το barcode και αντιστοίχιση με τα στοιχεία του εκάστοτε ασθενούς στον οποίο ανήκει το δείγμα.

- **PCWS004** (A-005): Σταθμός Εργασίας (Workstation).
  Βρίσκεται στην Αίθουσα Αναμονής.
  Μοντέλο: HP Pro G2 MT, *Κατασκευαστής*: HP, *Λειτουργικό Σύστημα:* Windows 10 Pro
  Λειτουργία: Χρησιμοποιείται από τον/τη γραμματέα για επικοινωνία μέσω email, διαχείριση επαφών με τους ασθενείς/πελάτες, εξαγωγή αποτελεσμάτων αιματολογικών εξετάσεων, οικονομική διαχείριση, αποστολή παραγγελιών προς τους προμηθευτές (όσον αφορά βελόνες, γάντια, οινόπνευμα και άλλα είδη).

- **PCWS005** (A-006): Σταθμός Εργασίας (Workstation).
  Βρίσκεται στο Γραφείο του Ιατρού.
  Μοντέλο: HP Pro G2 MT, *Κατασκευαστής*: HP, *Λειτουργικό Σύστημα:* Windows 10 Pro
  Λειτουργία: Χρησιμοποιείται από τον/την ιατρό για την παρακολούθηση του ιστορικού των ασθενών, την καταγραφή συνταγών για τους ασθενείς καθώς και για την επικοινωνία με άλλους παρόχους ιατρικών υπηρεσιών.

- **PR0001** (A-007): Εκτυπωτής (Printer).
  Βρίσκεται στην Αίθουσα Αναμονής.
  Μοντέλο: HP OfficeJet Pro Printer, *Κατασκευαστής*: HP, *Λειτουργικό Σύστημα:* Old firmware before 1708D
  Λειτουργία: Χρησιμοποιείται από τον/τη γραμματέα για την εκτύπωση των αποτελεσμάτων των αιματολογικών εξετάσεων των ασθενών και άλλου είδους χρήσιμων εγγράφων και την αποστολή με fax.

- **PR0002** (A-008): Εκτυπωτής (Printer).
  Βρίσκεται στο Γραφείο του Ιατρού.
  Μοντέλο: HP LaserJet Pro Printer, *Κατασκευαστής*: HP, *Λειτουργικό Σύστημα:* HP printer Firmware (old)
  Λειτουργία: Χρησιμοποιείται από τον/την ιατρό για την εκτύπωση των συνταγών και άλλων χρήσιμων εγγράφων συμπληρωματικών της εξέτασης.

- **SRV001** (A-009): Διακομιστής (Server).
  Βρίσκεται στον Βοηθητικό Χώρο.
  Μοντέλο: Διακομιστής Ιστού (Web Server), *Λειτουργικό Σύστημα:* Windows Server 2008 R2
  Λειτουργία: Αποθήκευση, διαχείριση και διανομή των ιστοσελίδων του ιστοτόπου.

- **SRV002** (A-010): Διακομιστής (Server).
  Βρίσκεται στον Βοηθητικό Χώρο.
  Μοντέλο: Διακομιστής Βάσης Δεδομένων (Database Server), *Λειτουργικό Σύστημα:* Microsoft Windows 2016 Server SP1 + Oracle
  Λειτουργία: Αποθήκευση και διαχείριση των βάσεων δεδομένων που σχετίζονται με τα δεδομένα υπαλλήλων/προμηθευτών και πελατών/ασθενών καθώς και παροχή πρόσβασης σε αυτά.

- **LTP001** (A-015): Φορητός Υπολογιστής (Laptop).
  Βρίσκεται στο Γραφείο του Ιατρού.
  Μοντέλο: Apple MacBook Air, *Κατασκευαστής*: Apple, *Λειτουργικό Σύστημα:* MAC-OS
  Λειτουργία: Ο προσωπικός υπολογιστής του/της ιατρού. Χρησιμοποιείται για προσωπική επικοινωνία και διαχείριση επιχειρηματικών επαφών. Χρησιμεύει επίσης ως αντικαταστάτης του σταθερού υπολογιστή αν υπάρξει ανάγκη.

Τέλος παραθέτουμε τα αγαθά που επιλέγουμε να προσθέσουμε με την αντίστοιχη τεκμηρίωση για την ένταξή τους σε αυτήν την κατηγορία:

- **BKUP001** (A-025): Εξωτερικός σκληρός δίσκος (external Hard Disk Drive).
  Βρίσκεται στο Γραφείο του Ιατρού.
  Μοντέλο: WD My Passport 5TB, *Κατασκευαστής*: Western Digital, *Λειτουργικό Σύστημα:* WD Backup software, WD Security software
  Λειτουργία: Χρησιμοποιείται για την αποθήκευση του αντιγράφου ασφαλείας (Backup) των δεδομένων των ασθενών/πελατών.

  Γίνεται σε αυτό το σημείο η παραδοχή ότι το αντίγραφο ασφαλείας αποθηκεύεται σε φυσική εξωτερική συσκευή (συγκεκριμένα στην άνωθεν περιγραφόμενη) η οποία φυλάσσεται στο γραφείο του ιατρού όπως αναφέρεται στην περιγραφή του επιθεωρητή. Το αγαθό εντάσσεται στην κατηγορία αυτή εφόσον πρόκειται για μια αποθηκευτική συσκευή (storage device) και επομένως είναι υλικό (hardware).

2.3 Λογισμικό και εφαρμογές

Στην υποενότητα αυτή περιγράφονται συνοπτικά τα αγαθά που επιλέγουμε να εντάξουμε στην κατηγορία του Λογισμικού & Εφαρμογών. Η επιλογή γίνεται μετά από εξέταση του τύπου των αγαθών. Συγκεκριμένα περιλαμβάνονται τα χρησιμοποιούμενα λειτουργικά συστήματα (εφόσον αυτό είναι που αποτελεί το λογισμικό ενός συστήματος) καθώς και ο ιστότοπος του εργαστηρίου εφόσον πρόκειται για άυλα μέρη του υπολογιστικού συστήματος, με το πρώτο να είναι σχεδιασμένο να καθοδηγεί και να οριοθετεί την εκτέλεση του υπόλοιπου λογισμικού ενώ το δεύτερο υλοποιεί μέρος της επιχειρησιακής λογικής. Ακολουθεί απαρίθμηση και συνοπτική περιγραφή των συγκεκριμένων αγαθών:

- **Windows 7 Pro** (A-018): Λειτουργικό σύστημα μεταγωγέα (Switch Software).
  Κατασκευαστής: Microsoft
  Λειτουργία: Έλεγχος κίνησης δικτύου, ασφάλεια και αποτελεσματική επικοινωνία μεταξύ των συσκευών, παροχή δυνατότητας αναβάθμισης του firmware.

- **Windows 10 Pro** (A-019): Λειτουργικό σύστημα σταθμών εργασίας (Workstation Software).
  Κατασκευαστής: Microsoft
  Λειτουργία: Παροχή της διεπαφής χρήστη για την πραγματοποίηση βασικών λειτουργιών διαχείρισης αρχείων, πόρων και συσκευών καθώς και ενασχόληση με θέματα προστασίας και ασφάλειας.

- **Website** (A-020): Ιστότοπος μικροβιολογικού εργαστηρίου. Ο Server που την υποστηρίζει βρίσκεται στον Βοηθητικό Χώρο.
  Μοντέλο: JOOMLA, *Κατασκευαστής*: JOOMLA, *Λειτουργικό Σύστημα:* LINUX REDHAT
  Λειτουργία: Οι υφιστάμενοι πελάτες/ασθενείς μπορούν να συνδέονται και να βλέπουν τα αποτελέσματα των αιματολογικών τους εξετάσεων. Οι μελλοντικοί πελάτες/ασθενείς μπορούν να ενημερώνονται για τον τρόπο επικοινωνίας και άλλες πληροφορίες.

  Τέλος παραθέτουμε τα αγαθά που επιλέγουμε να προσθέσουμε με την αντίστοιχη τεκμηρίωση για την ένταξή τους σε αυτήν την κατηγορία:

- **SysmexXN** (A-027): Λογισμικό του αιματολογικού αναλυτή (A-001).
  Κατασκευαστής: Sysmex
  Λειτουργία: Ανάλυση δειγμάτων και εξαγωγή πληροφοριών για το πλήθος των κυττάρων (ερυθρών, λευκών αιμοσφαιρίων κλπ), τα επίπεδα αιμοσφαιρίνης και τη μορφολογία των κυττάρων.

Το αγαθό αυτό εντάσσεται σε αυτήν την κατηγορία εφόσον πρόκειται για το λογισμικό που τρέχει στη συσκευή του αιματολογικού αναλυτή για τη διενέργεια των εξετάσεων. Είναι άυλο, τρέχει πάνω σε κάποιο υλικό και επιτελεί συγκεκριμένες λειτουργίες.

2.4 Δίκτυο

Στην υποενότητα αυτή περιγράφονται συνοπτικά τα αγαθά που επιλέγουμε να εντάξουμε στην κατηγορία του Δικτύου. Η επιλογή γίνεται μετά από εξέταση του τύπου των αγαθών. Συγκεκριμένα περιλαμβάνονται οι μεταγωγείς, ο δρομολογητής και το τείχος προστασίας καθώς οι μεν μεταγωγείς επιτρέπουν τη διασύνδεση και επικοινωνία των μερών του υπολογιστικού συστήματος εντός ενός δικτύου, ο δρομολογητής καθιστά δυνατή τη σύνδεση με το Διαδίκτυο μέσω του παρόχου υπηρεσιών διαδικτύου (ISP) ενώ το τείχος προστασίας θέτει τους κανόνες για την κίνηση από και προς το τμήμα του δικτύου που αφορά. Ακολουθεί απαρίθμηση και συνοπτική περιγραφή των συγκεκριμένων αγαθών:

- **SW001** (A-011): Μεταγωγέας (Switch).
  Βρίσκεται στην Αίθουσα Αναμονής.
  Μοντέλο: TP-LINK TL-SG1005D, *Κατασκευαστής*: TP-LINK, *Λειτουργικό Σύστημα:* Windows 7 Pro
  Λειτουργία: Δικτύωση των συσκευών (εκτός των διακομιστών) μεταξύ τους καθώς και με τον διαδικτυακό δρομολογητή.

- **SW002** (A-012): Μεταγωγέας (Switch).
  Βρίσκεται στον Βοηθητικό χώρο.
  Μοντέλο: TP-LINK TL-SG1005D, *Κατασκευαστής*: TP-LINK, *Λειτουργικό Σύστημα:* Windows 7 Pro
  Λειτουργία: Δικτύωση των διακομιστών (Web Server, Database Server) με τον διαδικτυακό δρομολογητή.

- **RT001** (A-013): Δρομολογητής (Router).
  Βρίσκεται στην Αίθουσα Αναμονής.
  Μοντέλο: Cisco C886VA-K9, *Κατασκευαστής*: Cisco, *Λειτουργικό Σύστημα:* Windows 7 Pro
  Λειτουργία: Παροχή πρόσβασης στο Διαδίκτυο.

- **FW001** (A-014): Τείχος Προστασίας (Firewall). Είναι διαμορφωμένο (configured) στον SRV002.
  Μοντέλο: Fortinet-Fortigate-400D, *Κατασκευαστής*: Fortinet, *Λειτουργικό Σύστημα:* Windows 10 Advanced IP Services
  Λειτουργία: Παρεμπόδιση μη εξουσιοδοτημένης δικτυακής κίνησης.

2.5 Δεδομένα

Στην υποενότητα αυτή περιγράφονται συνοπτικά τα αγαθά που επιλέγουμε να εντάξουμε στην κατηγορία των Δεδομένων. Η επιλογή γίνεται μετά από εξέταση του τύπου των αγαθών. Συγκεκριμένα περιλαμβάνονται όσα αγαθά περιέχουν προσωπικά στοιχεία, ευαίσθητες

πληροφορίες και υλικό τεκμηρίωσης της επιχείρησης. Ακολουθεί απαρίθμηση και συνοπτική περιγραφή των συγκεκριμένων αγαθών:

- **Customer Data** (A-016): Δεδομένα των Πελατών. Η ηλεκτρονική τους μορφή βρίσκεται αποθηκευμένη στον SRV002, στον Βοηθητικό χώρο.
  Λειτουργία: Υποστηρίζει την οργάνωση και εύρεση των αρχειοθετημένων αιματολογικών εξετάσεων των πελατών/ασθενών. Περιέχει προσωπικά δεδομένα.

- **Employee Data** (A-017): Δεδομένα των Υπαλλήλων. Η ηλεκτρονική τους μορφή βρίσκεται αποθηκευμένη στον SRV002, στον Βοηθητικό χώρο.
  Λειτουργία: Υποστηρίζει τις υποχρεώσεις κατάθεσης έναντι των εργαζομένων και τις πληρωμές. Περιέχει προσωπικά δεδομένα.

- **Φυσικό Αρχείο Ασθενών** (A-021): Φάκελοι με έντυπο αρχείο σε Ερμάριο - Ανοικτή Βιβλιοθήκη στην Αίθουσα Αναμονής.
  Λειτουργία: Υποστηρίζει την οργάνωση και εύρεση των αρχειοθετημένων αιματολογικών εξετάσεων των πελατών/ασθενών. Περιέχει προσωπικά δεδομένα.

- **Αρχείο Υπαλλήλων & Προμηθευτών** (A-022): Φάκελοι με έντυπο αρχείο σε Ερμάριο - Ανοικτή Βιβλιοθήκη στο Γραφείο Ιατρού.
  Λειτουργία: Υποστηρίζει τις υποχρεώσεις κατάθεσης έναντι των εργαζομένων και τις πληρωμές. Περιέχει λογιστικές εγγραφές.

2.6 Διαδικασίες

Στην υποενότητα αυτή περιγράφονται συνοπτικά τα αγαθά που επιλέγουμε να εντάξουμε στην κατηγορία των Διαδικασιών. Πρόκειται για διαδικασίες/υπηρεσίες που αφορούν την επιχειρησιακή λειτουργία του μικροβιολογικού εργαστηρίου. Καθώς μεταξύ των ήδη καταγεγραμμένων αγαθών δεν εμφανίζεται κάποιο που κρίνεται ότι ανήκει σε αυτή την κατηγορία, τα αγαθά που απαριθμούνται παρακάτω έχουν προστεθεί από εμάς. Σημειώνουμε επιπλέον για κάθε αγαθό την αντίστοιχη τεκμηρίωση για την ένταξή του σε αυτήν την κατηγορία.

- **Διαμοιρασμός Προσωπικών Δεδομένων των ασθενών με συνεργαζόμενους παρόχους υπηρεσιών** (A-023)
  Λειτουργία (Σκοπός): Χρησιμοποιείται για την καλύτερη εξυπηρέτηση των πελατών.

  Ως προς την ένταξη του αγαθού αυτού στην κατηγορία των διαδικασιών, σημειώνεται ότι πρόκειται για ένα σύνολο επιμέρους ενεργειών που έχουν έναν κοινό σκοπό (την καλύτερη εξυπηρέτηση των ασθενών/πελατών) και υιοθετούνται για την υποστήριξη υψηλότερων επιχειρησιακών στόχων του εργαστηρίου (π.χ. εξαγωγή επαρκών - σύμφωνα με το αίτημα - αποτελεσμάτων των εξετάσεων των ασθενών/πελατών σε εύλογο χρόνο).

- **Λήψη Αντιγράφων Ασφαλείας** (A-024)
  Λειτουργία (Σκοπός): Χρησιμοποιείται για τη διασφάλιση της διαθεσιμότητας των ιατρικών δεδομένων των ασθενών σε περίπτωση αποτυχίας του συστήματος ή κλοπής του υπολογιστή.

Το αγαθό εντάσσεται στην κατηγορία των διαδικασιών καθώς πρόκειται για την ενέργεια της λήψης αντιγράφων ασφαλείας της οποίας τα ποιοτικά χαρακτηριστικά (π.χ. συχνότητα εκτέλεσης) θα εξεταστούν. Επιπλέον αφορά τη λειτουργία του εργαστηρίου καθώς εκτελείται σε εβδομαδιαία βάση από μέλος του προσωπικού του.

- **Αποστολή αποτελεσμάτων αιματολογικών εξετάσεων στους ασθενείς/πελάτες (A-026)**
  Λειτουργία (Σκοπός): Χρησιμοποιείται για την αυθημερόν αποστολή των αποτελεσμάτων των εξετάσεων/αναλύσεων.

  Όσον αφορά την κατηγορία του αγαθού, συμπεριλαμβάνεται στις διαδικασίες εφόσον πρόκειται για ενέργεια που αφορά μια βασική λειτουργία του μικροβιολογικού εργαστηρίου, την γνωστοποίηση των αποτελεσμάτων των εξετάσεων στους ενδιαφερόμενους ασθενείς ή τους θεράποντες ιατρούς αυτών.

3. ΑΠΟΤΙΜΗΣΗ ΑΓΑΘΩΝ ΤΗΣ ΕΓΚΑΤΑΣΤΑΣΗΣ

Στην ενότητα αυτή, καταγράφονται τα πληροφοριακά αγαθά που αξιολογούνται, οι απειλές και ευπάθειές που τα αφορούν και παρουσιάζονται τα αποτελέσματα της αποτίμησης τους, στο πλαίσιο της μελέτης περίπτωσης και Ανάλυσης Επικινδυνότητας Πληροφοριακών Συστημάτων στο Μικροβιολογικό Εργαστήριο Red Cell Lab.

3.1 Αγαθά που εντοπίστηκαν

Εκ των άνωθεν αναφερόμενων αγαθών, μετά από προσεκτική εξέτασή τους θεωρούνται πληροφοριακά αγαθά άξια προστασίας όλα όσα εντοπίστηκαν στην προηγούμενη ενότητα. Στην υποενότητα αυτή παρατίθενται με σημειωμένη την αιτιολόγηση της θεώρησής τους ως πληροφοριακά αγαθά.

LabWS001, PCWS001-005, LTP001: Ο αιματολογικός αναλυτής (haematology analyzer), οι σταθμοί εργασίας (workstations) και ο φορητός υπολογιστής (laptop). Χρησιμοποιούνται για την πρόσβαση, επεξεργασία και διαχείριση ευαίσθητων πληροφοριών (προσωπικά δεδομένα, ιατρικό ιστορικό κ.α.) στα πλαίσια του επιχειρησιακού περιβάλλοντος. Η ενδεχόμενη μη εξουσιοδοτημένη πρόσβαση στις συσκευές αυτές δύναται να οδηγήσει σε σοβαρές επιπτώσεις και συνέπειες για το εργαστήριο από τις οικονομικές επιβαρύνσεις που συνεπάγεται η φυσική βλάβη ή απώλεια έως τις νομικές επιπτώσεις λόγω της παραβίασης του απορρήτου των προσωπικών και ιατρικών δεδομένων των ασθενών.

PR001-002: Οι εκτυπωτές. Είναι συνδεδεμένοι με άλλες συσκευές εντός του δικτύου, αποθηκεύουν προσωρινά τα δεδομένα ασθενών (αρχείο ή και θεραπείες, ιατρικό ιστορικό) και μπορεί να είναι ευπαθείς σε διάφορες διαδικτυακές επιθέσεις. Λόγω του ότι μπορεί να χρησιμοποιηθούν ως πρώτο σημείο στο οποίο ένας επιτιθέμενος μπορεί να εισχωρήσει και ενδέχεται να αποτελέσουν σημείο εισόδου για πρόσβαση στο συνολικό εσωτερικό δίκτυο (και μέσω αυτού σε άλλα σημαντικά σημεία του Πληροφοριακού συστήματος) θεωρούμε ότι είναι αγαθά τα οποία χρήζουν προστασίας.

SW001 - 002: Οι μεταγωγείς (switches). Όσον αφορά τους μεταγωγείς, είναι εκείνοι που παρέχουν την τμηματοποίηση του δικτύου και τον έλεγχο πρόσβασης (network segmentation & access control) προστατεύοντας έτσι τα ιατρικά δεδομένα. Είναι από τα σημαντικότερα αγαθά που χρήζουν προστασίας καθώς διαμορφώνουν και επιβάλλουν πολιτικές ασφαλείας οι οποίες

μπορούν να περιορίσουν την πρόσβαση και επικοινωνία από τμήματα του δικτύου σε άλλα τμήματα. Αυτό το χαρακτηριστικό είναι αρκετά σημαντικό καθώς σε περίπτωση μόλυνσης ενός υπολογιστή, αποτρέπεται η εξάπλωση του κακόβουλου λογισμικού στους υπόλοιπους τομείς (τμήματα) του εργαστηρίου. Συνοπτικά οι μεταγωγείς είναι αρωγοί της προστασίας ευαίσθητων προσωπικών δεδομένων και πληροφοριών των ασθενών αλλά και υπεύθυνοι για την απομόνωση των τμημάτων.

RT001: Ο δρομολογητής (router). Είναι αυτός που παρέχει την διασύνδεση των μερών του υπολογιστικού συστήματος με το Διαδίκτυο. Προκειμένου να επιτευχθεί η ασφαλής ανταλλαγή πληροφοριών μεταξύ του εσωτερικού δικτύου και του κόσμου της πληροφορίας, οι δρομολογητές παρέχουν γενικά κάποια μέτρα προστασίας όπως το τείχος προστασίας, ανίχνευση και πρόληψη εισβολών (intrusion detection & prevention). Διασφαλίζοντας λοιπόν την προστασία και σωστή διαμόρφωση των ρυθμίσεων του δρομολογητή προστατεύονται όλες οι ροές δεδομένων εντός και εκτός του δικτύου, διαδραματίζοντας σημαντικό ρόλο στην εμπιστευτικότητα, ακεραιότητα και διαθεσιμότητα των πληροφοριών.

SRV001-002: Οι διακομιστές (Servers). Ο Database Server αποθηκεύει σημαντικά δεδομένα και εμπιστευτικές πληροφορίες όπως προσωπικά και ιατρικά δεδομένα ασθενών, προσωπικά δεδομένα υπαλλήλων και άλλα κρίσιμα για το εργαστήριο δεδομένα που θα πρέπει να προστατευθούν ώστε να μην οδηγηθεί το εργαστήριο σε σοβαρές νομικές και οικονομικές συνέπειες. Ο Web Server παρέχει την πρόσβαση στον ιστότοπο του εργαστηρίου του οποίου η διαθεσιμότητα είναι σημαντική για τις διαδικασίες του εργαστηρίου. Έχει γίνει επιπλέον η παραδοχή ότι λειτουργεί και ως Mail Server. Και οι δύο χρησιμοποιούνται για την παροχή πρόσβασης σε πολλές συσκευές και από οποιαδήποτε τοποθεσία, γεγονός που θα μπορούσε να οδηγήσει σε ανεπιθύμητες και επικίνδυνες μη εξουσιοδοτημένες προσβάσεις. Μια πιθανή παραβίαση ή βλάβη τους δύναται να επηρεάσει την επιχειρηματική συνέχεια (business continuity) μέσω της μη διαθεσιμότητας δεδομένων και πληροφοριών (προσωρινά ή μόνιμα). Τέλος, μέσω της θεώρησής τους ως υλικού με σημαντικό οικονομικό κόστος αγοράς/αντικατάστασης, αξίζουν να προστατευθούν και φυσικά.

FW001: Το τείχος προστασίας (Firewall). Από τις συσκευές που είναι μέρος του δικτύου, είναι εκείνη που προστατεύει τον Database Server από κακόβουλες επιθέσεις χρηστών, που στοχεύουν στην υποκλοπή δεδομένων τόσο των ευαίσθητων στοιχείων ασθενών & προσωπικού, όσο και των επιχειρησιακών δράσεων του εργαστηρίου. Για την αποφυγή οποιασδήποτε έκθεσης του μικροβιολογικού εργαστηρίου σε νομικά ζητήματα όπως πρόστιμα, διώξεις κ.λπ. που οδηγούν από οικονομικές επιβαρύνσεις, μέχρι και σε δυσφήμιση, θεωρείται αναγκαία η προστασία του από εσωτερικές και εξωτερικές επιθέσεις, αλλά και η σωστή διαμόρφωση των ρυθμίσεων του.

Windows 7 Pro & Windows 10 Pro: Τα λειτουργικά συστήματα Windows 7 Pro & Windows 10 Pro. Το Windows 10 Pro λειτουργικό σύστημα συμβάλλει στην εκτέλεση λειτουργιών του εργαστηρίου, με την παροχή συγκεκριμένων εφαρμογών και προγραμμάτων (Microsoft 365, Windows Defender κ.λπ.), που εξυπηρετούν στην οργάνωση και επεξεργασία πληροφοριών αλλά και στην μερική προστασία του υπολογιστή από κυβερνοεπιθέσεις. Ωστόσο, πολλές φορές ορισμένες ρυθμίσεις του λειτουργικού δεν είναι κατάλληλα διαμορφωμένες από τους νόμιμους χρήστες του, με αποτέλεσμα ορισμένες προσπάθειες κακόβουλων χρηστών να υποκλέπτουν ή ακόμη και να τροποποιούν πληροφορίες που δεν είναι κρυπτογραφημένες, με σκοπό να γίνουν γνωστές σε τρίτους και να επέλθουν ανεπιθύμητες καταστάσεις που θα δυσχέραιναν τη θέση της επιχείρησης. Από την άλλη, το Windows 7 Pro λειτουργεί ως λογισμικο στο μεταγωγέα του δικτύου αφού διαχειρίζεται τη ροή των πακέτων στο εσωτερικό δίκτυο του εργαστηρίου. Ωστόσο, από τις 14 Ιανουαρίου 2020 και έπειτα, η έκδοση αυτού του

λογισμικού σταμάτησε να δέχεται συγκεκριμένα πακέτα αναβαθμίσεων κάνοντάς το ευάλωτο σε μολύνσεις από κακόβουλα λογισμικά που θα μπορούσαν να οδηγήσουν τόσο στην πτώση απόδοσης του δικτύου, όσο και στην υποκλοπή δεδομένων. Αξιολογώντας τα παραπάνω, δύναται να υποθέσει κανείς την σημασία της προστασίας τους ως λειτουργικό μέρος στις διεργασίες της επιχείρησης.

Στο σημείο αυτό, έχει γίνει παραδοχή ότι το λειτουργικό σύστημα Windows 7 Pro πάνω στους μεταγωγείς είναι εφικτό να λειτουργήσει παρόλο που ένας TP-LINK TL-SG1005D Switch έχει ένα σταθερό σύνολο χαρακτηριστικών που είναι ενσωματωμένα στο υλικό του και δεν μπορεί να χρησιμοποιήσει κάποιο λειτουργικό σύστημα όπως τα Windows 7 Pro.

Website: Ο ιστότοπος του εργαστηρίου. Χρησιμοποιείται για την μετάδοση ευαίσθητων πληροφοριών (sensitive data) η υποκλοπή των οποίων μπορεί να βλάψει τόσο το εργαστήριο λόγω νομικών συνεπειών και δυσφήμησης όσο και τους ασθενείς. Επιπλέον ο ιστότοπος αυξάνει την επιφάνεια που είναι εκμεταλλεύσιμη από κυβερνοεπιθέσεις αφού είναι ευπαθής σε ιομορφικό λογισμικό. Μέσω του ιστοτόπου μπορούν να ζημιωθουν οι Servers που αλληλεπιδρούν με αυτό. Συνεπώς, κρίνεται άξιο προστασίας.

Customer Data, Employee Data, **Φυσικό Αρχείο Ασθενών, Αρχείο Υπαλλήλων & Προμηθευτών:** Περιλαμβάνουν ευαίσθητες πληροφορίες (sensitive information) όπως προσωπικά και ιατρικά δεδομένα ασθενών, προσωπικά δεδομένα υπαλλήλων, λογιστικά και οικονομικά δεδομένα του εργαστηρίου (σε σχέση με τους υπαλλήλους και τους προμηθευτές). Εξαιτίας της φύσης της επιχείρησης (μικροβιολογικό εργαστήριο) οι πληροφορίες των ασθενών είναι σημαντικό να προστατευθούν για λόγους συμβατότητας με τις (αυστηρές) ισχύουσες νομοθεσίες που αναφέρονται στο ιατρικό απόρρητο. Από την άλλη, οι πληροφορίες που αφορούν τους υπαλλήλους και τους προμηθευτές ενδέχεται να είναι προσωπικές (π.χ. διεύθυνση και στοιχεία επικοινωνίας) και δεν θα ήταν θεμιτό να γνωστοποιηθούν σε τρίτους. Τέλος, ειδικά για τα φυσικά αρχεία ας σημειωθεί ότι η διαθεσιμότητα τους είναι χρήσιμη για τις καθημερινές λειτουργίες της επιχείρησης και μια φυσική καταστροφή τους θα πρέπει να ακολουθηθεί από μια κοστοβόρα και χρονοβόρα ανάκαμψη. Για τους λόγους αυτούς τα αρχεία αξίζει να προστατευθούν.

Ακολουθούν τα επιπλέον αγαθά που επιλέγονται:

Διαμοιρασμός Προσωπικών Δεδομένων των ασθενών με συνεργαζόμενους παρόχους υπηρεσιών: Η επιλογή του συγκεκριμένου αγαθού έγινε μετά από αξιολόγηση της σημαντικότητας των ευπαθειών που γίνονται φανερές από την περιγραφή του επιθεωρητή. Με γνώμονα τις υποβόσκουσες ευπάθειες που αφορούν το αγαθό αυτό (εξαιτίας του χαρακτηριστικού της μη γραπτής συναίνεσης των ασθενών σε ορισμένες περιπτώσεις), τις απειλές που μπορούν να εκμεταλλευτούν τις ευπάθειες αυτές και τις νομικές και ηθικές επιπτώσεις, θεωρήθηκε σκόπιμο να εξεταστεί το αγαθό, να καταδειχθούν οι αλυσίδες ευπαθειών, απειλών και επιπτώσεων που το αφορούν ώστε σε τελικό στάδιο της μελέτης να προταθούν και τα κατάλληλα μέτρα ασφαλείας.

Λήψη Αντιγράφων Ασφαλείας: Το αγαθό αυτό επιλέχθηκε καθώς η διαδικασία της λήψης αντιγράφων ασφαλείας θεωρείται αρκετά σημαντική καθώς είναι αρωγός της διασφάλισης της διαθεσιμότητας, ακεραιότητας των δεδομένων και της επανάκτησής τους σε περίπτωση απώλειας λόγω αστοχιών του συστήματος, κυβερνοεπιθέσεων ή φυσικών καταστροφών.

Συμβάλλουν στην διασφάλιση της ακεραιότητας μέσω της σύγκρισης της τρέχουσας κατάστασης και τιμών των δεδομένων με το αντίγραφο ασφαλείας προκειμένου να διαπιστωθεί τυχόν ανεπιθύμητη τροποποίηση. Στη διαδικασία αυτή κρίνεται ιδιαίτερα σημαντικός παράγοντας η συχνότητα λήψης των αντιγράφων ασφαλείας καθώς μία μειωμένη συχνότητα αυξάνει τις πιθανότητες εμφάνισης ανεπιθύμητων επιπτώσεων από την απώλεια των δεδομένων (Η συχνότητα που αναφέρει ο επιθεωρητής στην περίπτωση αυτή θεωρείται ανεπαρκής, δεδομένων των λειτουργιών ενός αιματολογικού εργαστηρίου, καθώς ορισμένες αναλύσεις είναι χρονοβόρες και κοστοβόρες ώστε να επαναληφθούν εάν χαθούν τα αποτελέσματά τους).

BKUP001: Η επιλογή του συγκεκριμένου αγαθού έγινε κατόπιν προσθήκης ενός άλλου αγαθού, της διαδικασίας "Λήψη Αντιγράφων Ασφαλείας" **(A-024)** για λόγους πληρότητας της ανάλυσης. Το αντίγραφο ασφαλείας προσθέτει ένα επιπλέον στρώμα προστασίας έναντι της απώλειας δεδομένων λόγω αστοχιών του συστήματος, κυβερνοεπιθέσεων ή φυσικών καταστροφών, αφού επιτρέπει την ανάκτησή τους. Επιπλέον, πρόκειται για έναν εξωτερικό σκληρό δίσκο, και επομένως θα πρέπει να προστατευθεί και φυσικά.

Αποστολή αποτελεσμάτων των αιματολογικών εξετάσεων στους ασθενείς/πελάτες: Η επιλογή του αγαθού αυτού γίνεται καθώς η αποστολή των αποτελεσμάτων μέσω fax φαίνεται παρωχημένη, ενώ και η αποστολή των e-mail επισφαλής (λόγω μη χρήσης κρυπτογράφησης). Τα τελευταία χρόνια είναι σύνηθες τα αποτελέσματα των εξετάσεων αν δεν παραλαμβάνονται από το εργαστήριο με φυσική παρουσία του ασθενούς να αποστέλλονται με e-mail. Όμως σε περίπτωση που τα αποτελέσματα που αποστέλλονται δεν είναι κρυπτογραφημένα ή δεν απαιτούν κωδικούς για την προσπέλασή τους, είναι ευάλωτα σε ανθρώπινα λάθη μέσω των οποίων μπορεί να επέλθει δυσφήμηση ή και νομικές συνέπειες. Τεχνικές όπως η αποστολή αποτελεσμάτων με fax αποφεύγονται για λόγους ασφαλείας. Με έναυσμα το γεγονός αυτό, επιλέγεται η αποστολή των αποτελεσμάτων ως αγαθό για να παρουσιαστούν οι ευπάθειες και να εξεταστούν οι ενδεχόμενες απειλές.

SysmexXN: Το λογισμικό (software) το οποίο χρησιμοποιείται από τον αιματολογικό αναλυτή **(A-001)**. Η επιλογή του συγκεκριμένου αγαθού έγινε κατόπιν εξέτασης της διαδικασίας παραγωγής και εξαγωγής αποτελεσμάτων του αιματολογικού εργαστηρίου. Θεωρήθηκε βασικό στοιχείο της διεργασίας της ανάλυσης των αιματολογικών δειγμάτων καθώς είναι υπεύθυνο για την επεξεργασία ευαίσθητων προσωπικών δεδομένων των ασθενών και έτσι οφείλει να διατηρεί την ακεραιότητα, εμπιστευτικότητα και η διαθεσιμότητα τους. Οποιαδήποτε ευπάθεια του συγκεκριμένου αγαθού θα μπορούσε να οδηγήσει σε μη εξουσιοδοτημένη πρόσβαση και τροποποίηση των δεδομένων, και έτσι να υπάρξει σοβαρή βλάβη των ασθενών (εξαιτίας τροποποίησης αποτελεσμάτων όπως μεταβολή κάποιας τιμής του αίματος σε άλλη και άρα διαμόρφωση διαφορετικής διάγνωσης από τον ιατρό). Αποτελεί έναν από τους πιο συνήθεις στόχους κακόβουλων επιθέσεων (καθώς βρίσκεται στο στάδιο ανάλυσης δεδομένων και άρα πιο ευάλωτο σε πιθανές μεταβολές αποτελεσμάτων και κακόβουλο κώδικα). Σε περίπτωση στοχοποίησης του, το αποτέλεσμα θα είναι η παραβίαση και τροποποίηση ευαίσθητων πληροφοριών ασθενών (παραβιάσεις απορρήτου) καθιστώντας νομικά υπόλογη την επιχείρηση. Επομένως θεωρούμε απαραίτητη τη προστασία του, καθώς όταν το λογισμικό ενός αιματολογικού αναλυτή είναι ασφαλές και ενημερωμένο ελαχιστοποιούνται οι κίνδυνοι από απειλές στον κυβερνοχώρο (και άρα οι νομικές ευθύνες περιορίζονται).

3.2 Απειλές που εντοπίστηκαν

Οι απειλές που εντοπίστηκαν παρουσιάζονται ομαδοποιημένες ανά αγαθό.

Εξετάζοντας το **FW001 - Τείχος Προστασίας (Firewall)** (A-014) εντοπίστηκαν οι εξής απειλές:

- Διαρροή Δεδομένων, εφόσον το τείχος προστασίας θέτει τους κανόνες για την κίνηση από και προς το τμήμα του δικτύου που αφορά
- Απόκτηση πρόσβασης στο εσωτερικό δίκτυο της επιχείρησης (intranet) από μη εξουσιοδοτημένο εξωτερικό χρήστη
- Έκρηξη / φωτιά, καθώς πρόκειται και για φυσική συσκευή
- Βανδαλισμός, για τον ίδιο λόγο

Εξετάζοντας τα **Δεδομένα των Υπαλλήλων (Employee Data)** (A-017) εντοπίστηκαν οι εξής απειλές:

- Απειλή εκ των έσω, καθώς κάποιος υπάλληλος μπορεί να αποκτήσει πρόσβαση στα δεδομένα των υπαλλήλων

Αντίστοιχα για τα **Δεδομένα των Πελατών (Customer Data)** (A-016) εντοπίστηκαν οι εξής απειλές:

- Απειλή εκ των έσω, καθώς κάποιος υπάλληλος μπορεί να δει τα δεδομένα των πελατών

Εξετάζοντας το **Αρχείο Υπαλλήλων & Προμηθευτών** (A-022) εντοπίστηκαν οι εξής απειλές:

- Κλοπή των δεδομένων από κακόβουλο πελάτη, αφού πρόκειται για φυσικά αρχεία
- Έκρηξη / φωτιά, για τον ίδιο λόγο

Αντίστοιχα, για τ**ο Φυσικό Αρχείο Ασθενών** (A-021) εντοπίστηκαν οι εξής απειλές:

- Κλοπή των δεδομένων από κακόβουλο πελάτη, αφού πρόκειται για φυσικά αρχεία
- Έκρηξη / φωτιά για τον ίδιο λόγο

Εξετάζοντας τους **SRV001 - Διακομιστής Ιστού (Web Server)** (A-009) και **SR002- Διακομιστής Βάσης Δεδομένων (Database Server)** (A-010) εφόσον είναι τοποθετημένοι στο ίδιο δωμάτιο και έχει γίνει η ένταξή τους σαν αγαθό εξοπλισμου & hardware υπόκεινται σε ορισμένες ίδιες απειλές οι οποίες είναι οι εξής:

- Υγρασία από το εξωτερικό περιβάλλον
- Σκόνη από το εξωτερικό περιβάλλον.
- Υψηλές θερμοκρασίες από το εξωτερικό περιβάλλον
- Πλημμύρα
- Έκρηξη / φωτιά ,εφόσον πρόκειται για φυσική συσκευή
- Βανδαλισμός, για τον ίδιο λόγο
- Διαρροή νερού (εφόσον πρόκειται για ηλεκτρονική συσκευή με κυκλώματα η οποία χαλάει αν έρθει σε επαφή με νερό)
- Σεισμός, είναι μία φυσική καταστροφή που πιθανώς μπορεί να καταστρέψει τους Διακομιστές

Συγκεκριμένα για τον **SRV001** έχουμε επιπλέον:

- Denial of Service (DOS) επίθεση, εφόσον πρόκειται για Διακομιστή

- File inclusion επίθεση (αναφέρεται στην συμπερίληψη και εκτέλεση κακόβουλων αρχείων στον Διακομιστή)

Εξετάζοντας τον **LabWS001 - Αιματολογικό αναλυτή (Hematology Analyzer)** (A-001) εντοπίστηκαν οι εξής απειλές:

- Πρόσβασης στα δεδομένα του αιματολογικού αναλυτή από κακόβουλο άγνωστο προς το εργαστήριο άτομο (όχι πελάτη ή μέλος του προσωπικού)
- Πρόσβασης στα δεδομένα του αιματολογικού αναλυτή από μη-εξουσιοδοτημένο προσωπικό (απειλή εκ των έσω)

Εξετάζοντας τον **SW001 - Μεταγωγέα (Switch)** (A-011) εντοπίστηκαν οι εξής απειλές:

- Απόκτηση πρόσβασης στο εσωτερικό δίκτυο της επιχείρησης (intranet) από μη εξουσιοδοτημένο εξωτερικό χρήστη
- Πρόκληση βλάβης λόγω ατυχήματος (π.χ. χύσιμο καφέ ή άλλου υγρού, κλωτσιά κ.λπ.), εφόσον πρόκειται για φυσική συσκευή

Εξετάζοντας τον **SW002 - Μεταγωγέα (Switch)** (A-012) εντοπίστηκαν οι εξής απειλές:

- Απόκτηση πρόσβασης στο εσωτερικό δίκτυο της επιχείρησης (intranet) από μη εξουσιοδοτημένο εξωτερικό χρήστη
- Βανδαλισμός, εφόσον πρόκειται για φυσική συσκευή

Εξετάζοντας το **RT001 - Δρομολογητής (Router)** (A-013) εντοπίστηκαν οι εξής απειλές:

- Διαρροή Δεδομένων, εφόσον παρέχει το μόνη δίοδο επικοινωνίας του εσωτερικού δικτύου του εργαστηρίου (intranet) με το Διαδίκτυο, είναι δηλαδή το σημείο από όπου περνά όλη η κίνηση από και προς το εσωτερικό δίκτυο.
- Απόκτηση πρόσβασης στο εσωτερικό δίκτυο της επιχείρησης (intranet) από μη εξουσιοδοτημένο εξωτερικό χρήστη, για τον ίδιο λόγο
- Κυβερνοεπίθεση (με μειωμένη προσπάθεια)
- Πρόκληση βλάβης λόγω ατυχήματος (π.χ. χύσιμο καφέ ή άλλου υγρού, κλωτσιά κ.λπ.), εφόσον πρόκειται για φυσική συσκευή

Αντίστοιχα, εξετάζοντας τον **PR0001 - Εκτυπωτή (Printer)** (A-007) εντοπίστηκαν οι εξής απειλές:

- Εκτέλεση αυθαίρετου κώδικα (arbitrary code execution) (η οποία στοχεύει στην διαρροή δεδομένων) [1] [2]

Ακολούθως για τον **PR0002 - Εκτυπωτή (Printer)** (A-008) εντοπίστηκαν οι εξής απειλές:

- Κυβερνοεπίθεση (με μειωμένη προσπάθεια)

Για τα **PCWS001 - Σταθμός Εργασίας (Workstation)** (A-002) και **PCWS002- Σταθμός Εργασίας (Workstation)** (A-003) εντοπίστηκαν οι εξής απειλές:

- Πρόσβαση από μη εξουσιοδοτημένο προσωπικό (απειλή εκ των έσω)
- Πρόσβαση από κακόβουλο άγνωστο προς το εργαστήριο άτομο (όχι πελάτη ή μέλος του προσωπικού)

Όσον αφορά το **PCWS003 - Σταθμός Εργασίας (Workstation)** (A-004) εντοπίστηκαν οι εξής απειλές:

- Πρόσβαση από μη εξουσιοδοτημένο προσωπικό (απειλή εκ των έσω)

Αντίστοιχα για το **PCWS004 - Σταθμός Εργασίας (Workstation)** (A-005) εντοπίστηκαν οι εξής απειλές:

- Μόλυνση από κακόβουλο λογισμικό μέσω συνημμένων στα μηνύματα e-mail (phishing attack)
- Μη εξουσιοδοτημένη πρόσβαση (από το προσωπικό (απειλή εκ των έσω) ή τους πελάτες)

Για το **PCWS005 - Σταθμός Εργασίας (Workstation)** (A-006) εντοπίστηκαν οι εξής απειλές:

- Πρόσβαση από μη εξουσιοδοτημένο προσωπικό (απειλή εκ των έσω)
- Πρόσβαση από κακόβουλο άγνωστο προς το εργαστήριο άτομο (όχι πελάτη ή μέλος του προσωπικού)

Επιπλέον, για όλους τους Σταθμούς Εργασίας (Workstations) εντοπίστηκαν οι εξής απειλές:

- Ransomware επίθεση
- Data exfiltration επίθεση

Εξετάζοντας το **LTP001 - Φορητός Υπολογιστής (Laptop)** (A-015) εντοπίστηκαν οι εξής απειλές:

- Φυσική κλοπή, εφόσον πρόκειται για φορητή συσκευή
- Μη εξουσιοδοτημένη πρόσβαση (από το προσωπικό (απειλή εκ των έσω) ή τους πελάτες)

Εξετάζοντας το **Website - Ιστότοπο** (A-020) εντοπίστηκαν οι παρακάτω απειλές :

- Account takeover για τους λογαριασμούς των ασθενών/πελατών
- SQL injection
- XSS attack
- Man-in-the-middle-attack

Ακολούθως, σε σχέση με τα **Windows 10 Pro** (A-019) εντοπίστηκαν οι παρακάτω απειλές:

- Διαρροή Δεδομένων, καθώς είναι το λειτουργικό σύστημα των σταθμών εργασίας

Επιπροσθέτως, στα **Windows 7 Pro** (A-018) εντοπίστηκαν οι παρακάτω απειλές:

- Απόκτηση πρόσβασης στο εσωτερικό δίκτυο της επιχείρησης (intranet) από μη εξουσιοδοτημένο εξωτερικό χρήστη, καθώς όπως σημειώνεται πρόκειται για το λειτουργικό σύστημα των μεταγωγέων και του δρομολογητή

Για την διαδικασία **"Διαμοιρασμός Προσωπικών Δεδομένων των ασθενών σε συνεργαζόμενους παρόχους"** (A-023) εντοπίστηκαν οι εξής απειλές:

- Μήνυση (Lawsuit) εκ μέρους των ασθενών/πελατών
- Εκμετάλλευση δεδομένων από τρίτους για το προσωπικό τους όφελος

Όσον αφορά τη διαδικασία **"Λήψη αντιγράφων ασφαλείας"**(A-024) εντοπίστηκαν οι εξής απειλές:

- Απώλεια δεδομένων (και μάλιστα μεγάλος όγκος δεδομένων που χάνονται)

Εξετάζοντας το **BKUP001 - Αντίγραφα ασφαλείας (Physical Backup)** (A-025) εντοπίστηκαν οι εξής απειλές:

- Απομαγνητισμός της συσκευής από κακόβουλο άτομο
- Φυσική κλοπή (απειλή εκ των έσω, πελάτη ή άγνωστο)

Ως προς τη διαδικασία "**Αποστολή Αποτελεσμάτων των αιματολογικών εξετάσεων στους ασθενείς/πελάτες**" (A-027) εντοπίστηκαν οι εξής απειλές:

- Παραβίαση δεδομένων
- Packet sniffing
- Eavesdropping

Τέλος για το **SysmexXN - Λογισμικό αιματολογικού αναλυτή** (A-026) εντοπίστηκαν οι εξής απειλές:

- Επίθεση από ιούς ή κακόβουλο λογισμικό

3.3 Ευπάθειες που εντοπίστηκαν

Οι ευπάθειες που εντοπίσαμε παρουσιάζονται ομαδοποιημένες ανά αγαθό. Αναφέρεται επίσης με πλάγια γράμματα ποια απειλή μπορεί να εκμεταλλευτεί την εκάστοτε ευπάθεια.

Εξετάζοντας το **FW001 - Τείχος Προστασίας (Firewall)** (A-014) εντοπίστηκε ότι:

- Οι κανόνες του ενδέχεται να μην είναι διαμορφωμένοι σωστά: Η *Διαρροή Δεδομένων* ενδέχεται να εκμεταλλευτεί τη συγκεκριμένη ευπάθεια
- Βρίσκεται τοποθετημένο πλησίων χημικών ουσιών: Μία πιθανή *έκρηξη (ή και φωτιά)* μπορεί να προκληθεί/ενταθεί λόγω των χημικών ουσιών που βρίσκονται στο δωμάτιο και είναι εύφλεκτες.
- Προκαθορισμένα/ κοινότυπα διαπιστευτήρια σύνδεσης (credentials): Δημιουργούν πρόσφορο έδαφος για την *απόκτηση πρόσβασης στο εσωτερικό δίκτυο της επιχείρησης (intranet) από μη εξουσιοδοτημένο εξωτερικό χρήστη*
- Βρίσκεται τοποθετημένο σε δωμάτιο με ανοικτή πόρτα (αναφέρεται ότι διατηρείται ανοικτή για τον εξαερισμό του χώρου): Επομένως η απειλή του *βανδαλισμού* ενδέχεται να εκμεταλλευτεί τη συγκεκριμένη ευπάθεια.

Εξετάζοντας τα **Δεδομένα των Υπαλλήλων (Employee Data)** (A-017) εντοπίστηκε ότι:

- Δεν είναι κρυπτογραφημένα: Λόγω αυτού, εμφανίζεται η *εκ των έσω απειλή*, καθώς κάποιος υπάλληλος μπορεί να αποκτήσει πρόσβαση στα δεδομένα των υπαλλήλων και να μπορέσει να τα διαβάσει απερίσπαστος.

Ομοίως, εξετάζοντας τα **Δεδομένα των Πελατών (Customer Data)** (A-016) εντοπίστηκε ότι:

- Δεν είναι κρυπτογραφημένα: Λόγω αυτού, εμφανίζεται η *εκ των έσω απειλή*, καθώς κάποιος υπάλληλος μπορεί να αποκτήσει πρόσβαση στα δεδομένα των πελατών και να μπορέσει να τα διαβάσει απερίσπαστος.

Όσον αφορά το **Αρχείο Υπαλλήλων & Προμηθευτών** (A-022) εντοπίστηκε ότι:

- Τα φυσικά αρχεία φυλάσσονται σε μη-ασφαλή χώρο (ερμάριο χωρίς κλειδαριά), ο οποίος είναι εύκολα προσβάσιμος από τους πελάτες: Έτσι, δημιουργείται η απειλή της *κλοπής των δεδομένων από κακόβουλο πελάτη.*
- Τα φυσικά αρχεία φυλάσσονται σε μη-πυρίμαχο ερμάριο: Έτσι, δημιουργείται η απειλή *έκρηξης / φωτιάς.*

Αντιστοίχως, για το **Φυσικό Αρχείο Ασθενών** **(A-021)** εντοπίστηκαν οι εξής ευπάθειες:

- Τα φυσικά αρχεία φυλάσσονται σε μη-ασφαλή χώρο (ερμάριο χωρίς κλειδαριά), ο οποίος είναι εύκολα προσβάσιμος από τους πελάτες: Έτσι, δημιουργείται η απειλή της *κλοπής των δεδομένων από κακόβουλο πελάτη*
- Τα φυσικά αρχεία φυλάσσονται σε μη-προστατευμένο από φωτιά ερμάριο: Ως εκ τούτου, δημιουργείται η απειλή της *έκρηξης / φωτιάς*

Εξετάζοντας τους **SRV001 - Διακομιστής Ιστού (Web Server)** **(A-009)** και **SR002- Διακομιστής Βάσης Δεδομένων (Database Server)** **(A-010)** εφόσον είναι τοποθετημένοι στο ίδιο δωμάτιο και έχει γίνει η ένταξή τους σαν αγαθό εξοπλισμού & hardware υπόκεινται σε ορισμένες ίδιες ευπάθειες οι οποίες είναι οι εξής [3] [4] [5]:

- Βρίσκονται τοποθετημένοι σε δωμάτιο με ανοικτή πόρτα και έτσι η θερμοκρασία και *οι καιρικές συνθήκες του εξωτερικού περιβάλλοντος* εισχωρούν στο χώρο που οι ίδιοι οι Διακομιστές φιλοξενούνται. Αποτελώντας μέρος του hardware, είναι αρκετά ευάλωτοι στην υγρασία από το εξωτερικό περιβάλλον.
- Ομοίως, είναι ευαίσθητοι στη σκόνη. Λόγω της ανοικτής πόρτας (και της εγγύτητας με τον πολυσύχναστο δρόμο) εμφανίζεται η απειλή της δημιουργίας σκόνης (που προέρχεται κυρίως από το εξωτερικό περιβάλλον) πάνω στους Διακομιστές
- Ομοίως, είναι γνωστό ότι οι servers έχουν συγκεκριμένα όρια αποδεκτών θερμοκρασιών. Είναι ευάλωτοι σε υψηλές θερμοκρασίες: *Υψηλές θερμοκρασίες από το εξωτερικό περιβάλλον* επικρατούν στο δωμάτιο.
- Είναι τοποθετημένοι στο ισόγειο (και άρα πιθανότερη η εμφάνιση *πλημμύρας*).
- Βρίσκονται τοποθετημένοι πλησίων χημικών ουσιών: Μία πιθανή *έκρηξη (ή και φωτιά)* μπορεί να προκληθεί/ενταθεί λόγω των χημικών ουσιών που βρίσκονται στο δωμάτιο και είναι εύφλεκτες [6].
- Βρίσκονται τοποθετημένοι πλησίων νιπτήρα (και άρα μια *διαρροή νερού* είναι πιθανότερο να συμβεί και να εκμεταλλευτεί αυτήν την ευπάθεια)
- Έλλειψη αντισεισμικών ραφιών (anti-seismic racks). Ένας πιθανός *σεισμός*, είναι ένα φυσικό φαινόμενο που πιθανώς μπορεί να καταστρέψει τους Διακομιστές.

Συγκεκριμένα για τον **SRV001** εντοπίστηκαν τα εξής:

- Απουσία Τείχους Προστασίας: Αυτό μπορεί να γίνει εκμεταλλεύσιμο από μια πιθανή *File Inclusion επίθεση.*
- Έχει περιορισμένους πόρους (ΚΜΕ, μνήμη, χώρο δίσκου), λόγω παλαιότητας του μοντέλου [7]: Έτσι, μια πιθανή *Denial-of-Service επίθεση* καθίσταται εφικτή.

  Σημειώνεται ότι ο SRV002 με λειτουργικό σύστημα Microsoft Windows 2016 Server SP1 + Oracle είναι EOL αλλά η υποστήριξή του συνεχίζεται μέχρι το 2027.[8]

Ως προς το **LabWS001 - Αιματολογικός αναλυτή (Hematology Analyzer)** **(A-001)** εντοπίστηκαν οι εξής ευπάθειες:

- Βρίσκεται σε δωμάτιο προσβάσιμο από μη περιφραγμένο αύλειο χώρο: Ως εκ τούτου δημιουργείται το έδαφος για την *πρόσβαση στα δεδομένα του αναλυτή από κακόβουλο άγνωστο προς το εργαστήριο άτομο (όχι πελάτη ή μέλος του προσωπικού).*
- Είναι τοποθετημένο σε δωμάτιο με ελεύθερη/μη ελεγχόμενη πρόσβαση (δεν υπάρχει πλήρης διαχωρισμός καθηκόντων): Λόγω αυτού, εμφανίζεται η *εκ των έσω απειλή* καθώς ένα μη εξουσιοδοτημένο μέλος του προσωπικού μπορεί να αποκτήσει πρόσβαση στον αναλυτή χωρίς να είναι αναγκαίο για τα τρέχοντα καθήκοντά του ή να είναι ακόμη και αθέμιτο.

Εξετάζοντας τον **SW001 - Μεταγωγέα (Switch)** (A-011) εντοπίστηκε ότι:

- Εσφαλμένη διαμόρφωση των ρυθμίσεων του Μεταγωγέα. Ενέχει την απειλή της *απόκτησης πρόσβασης στο εσωτερικό δίκτυο της επιχείρησης (intranet) από μη εξουσιοδοτημένο εξωτερικό χρήστη.*
- Βρίσκεται κοντά στον καναπέ στο δωμάτιο αναμονής των πελατών: Συνεπώς, είναι δυνατή η *πρόκληση βλάβης λόγω ατυχήματος (π.χ. χύσιμο καφέ ή άλλου υγρού, κλωτσιά κ.λπ.)* λόγω της τοποθεσίας του και του γεγονότος ότι οι πελάτες που βρίσκονται χρησιμοποιούν την πολυθρόνα ή βρίσκονται στο δωμάτιο μπορεί να φανούν απρόσεκτοι ή είναι παιδιά

Εξετάζοντας τον **SW002 - Μεταγωγέα (Switch)** (A-012) εντοπίστηκε ότι:

- Εσφαλμένη διαμόρφωση των ρυθμίσεων του Μεταγωγέα. Ενέχει την απειλή της *απόκτησης πρόσβασης στο εσωτερικό δίκτυο της επιχείρησης (intranet) από μη εξουσιοδοτημένο εξωτερικό χρήστη.*
- Είναι τοποθετημένο σε δωμάτιο με ανοικτή πόρτα (αναφέρεται ότι διατηρείται ανοικτή για τον εξαερισμό του χώρου): Επομένως η απειλή του *βανδαλισμού* ενδέχεται να εκμεταλλευτεί τη συγκεκριμένη ευπάθεια.

Αντιστοίχως για τον **RT001 - Δρομολογητή (Router)** (A-012) εντοπίστηκαν οι εξής ευπάθειες:

- Πρόκειται για outdated προϊόν. Τα προϊόντα αυτά είναι γνωστά και με τον όρο End Of Life (EOL) [9] : Η ευπάθεια αυτή διευκολύνει τις *κυβερνοεπιθέσεις,* αφού εκείνες μπορούν να εκμεταλλευτούν τις αδυναμίες του προϊόντος για τις οποίες δεν υπάρχει καμία μέριμνα από τον κατασκευαστή, εφόσον το προϊόν θεωρείται ληγμένο. (Για τον λόγο αυτό αναφέρθηκε στην ενότητα 3.2 ως απειλή η “Κυβερνοεπίθεση (με μειωμένη προσπάθεια)” όσον αφορά το αγαθό αυτό).
- Παρέχει μόνο ένα βασικό (ενσωματωμένο) τείχος προστασίας (SPI Firewall) [10] : Το γεγονός αυτό δημιουργεί τις συνθήκες για την εκδήλωση *Διαρροής Δεδομένων.*
- Εσφαλμένη διαμόρφωση των ρυθμίσεων του Δρομολογητή. Ενέχει την απειλή της *απόκτησης πρόσβασης στο εσωτερικό δίκτυο της επιχείρησης (intranet) από μη εξουσιοδοτημένο εξωτερικό χρήστη.*
- Βρίσκεται κοντά στον καναπέ στο δωμάτιο αναμονής των πελατών: Όπως και για τον **SW001 - Μεταγωγέα (Switch)** (A-011), είναι δυνατή η *πρόκληση βλάβης λόγω ατυχήματος (π.χ. χύσιμο καφέ ή άλλου υγρού, κλωτσιά κ.λπ.)* λόγω της τοποθεσίας του και του γεγονότος ότι οι πελάτες που βρίσκονται χρησιμοποιούν τον καναπέ ή βρίσκονται στο δωμάτιο μπορεί να φανούν απρόσεκτοι ή είναι παιδιά.

Αντίστοιχα, εξετάζοντας τον **PR0001 - Εκτυπωτή (Printer)** (A-007) εντοπίστηκαν οι εξής ευπάθειες:

- Εσφαλμένα περιορίζει (ή δεν περιορίζει καθόλου) την πρόσβαση από μη-εξουσιοδοτημένο χρήστη [11], γεγονός το οποίο μπορεί να γίνει εκμεταλλεύσιμο από την απειλή της *εκτέλεσης αυθαίρετου κώδικα (η οποία να στοχεύει στην διαρροή δεδομένων) []*.

Ακολούθως για τον **PR0002 - Εκτυπωτή (Printer)** **(A-008)** εντοπίστηκαν οι εξής απειλές:

- Πρόκειται για outdated προϊόν. Τα προϊόντα αυτά είναι γνωστά και με τον όρο End Of Life (EOL): Η ευπάθεια αυτή διευκολύνει τις *κυβερνοεπιθέσεις,* αφού εκείνες μπορούν να εκμεταλλευτούν τις αδυναμίες του προϊόντος για τις οποίες δεν υπάρχει καμία μέριμνα από τον κατασκευαστή, εφόσον το προϊόν θεωρείται ληγμένο. (Για τον λόγο αυτό αναφέρθηκε στην ενότητα **3.2** ως απειλή η "Κυβερνοεπίθεση (με μειωμένη προσπάθεια)" όσον αφορά το αγαθό αυτό).

  Στο σημείο αυτό γίνεται η παραδοχή ότι πρόκειται για EOL προϊόν αφού το firmware του αναφέρεται στο asset inventory ως old.

Όσον αφορά τα **PCWS001 - Σταθμός Εργασίας (Workstation)** **(A-002)** και **PCWS002 - Σταθμός Εργασίας (Workstation)** **(A-003)** εντοπίστηκαν οι εξής ευπάθειες:

- Βρίσκεται σε δωμάτιο προσβάσιμο από μη περιφραγμένο αύλειο χώρο: Ως εκ τούτου δημιουργείται το έδαφος για την *πρόσβαση στα δεδομένα του αναλυτή από κακόβουλο άγνωστο προς το εργαστήριο άτομο (όχι πελάτη ή μέλος του προσωπικού).*
- Είναι τοποθετημένο σε δωμάτιο με ελεύθερη/μη ελεγχόμενη πρόσβαση (δεν υπάρχει πλήρης διαχωρισμός καθηκόντων): Λόγω αυτού, εμφανίζεται η *εκ των έσω απειλή* καθώς ένα μη εξουσιοδοτημένο μέλος του προσωπικού μπορεί να αποκτήσει πρόσβαση χωρίς αυτό να είναι αναγκαίο για τα τρέχοντα καθήκοντά του ή να είναι ακόμη και αθέμιτο.

Αναφορικά με το **PCWS003 - Σταθμός Εργασίας (Workstation)** **(A-004)** εντοπίστηκε ότι:

- Βρίσκεται σε δωμάτιο με ελεύθερη/μη ελεγχόμενη πρόσβαση (δεν υπάρχει πλήρης διαχωρισμός καθηκόντων): Λόγω αυτού, εμφανίζεται η *εκ των έσω απειλή* καθώς ένα μη εξουσιοδοτημένο μέλος του προσωπικού μπορεί να αποκτήσει πρόσβαση χωρίς αυτό να είναι αναγκαίο για τα τρέχοντα καθήκοντά του ή να είναι ακόμη και αθέμιτο.

Για το **PCWS004 - Σταθμός Εργασίας (Workstation)** **(A-005)** εντοπίστηκε ότι:

- Χρησιμοποιείται από τον/τη γραμματέα, ο/η οποίος/-α χρησιμοποιεί εκτενώς την επικοινωνία μέσω e-mail (με τους πελάτες, τους προμηθευτές καθώς τα υπόλοιπα ενδιαφερόμενα μέρη (stakeholders) της επιχείρησης): Το γεγονός αυτό είναι εκμεταλλεύσιμο από τη *μόλυνση με κακόβουλο λογισμικό μέσω συνημμένων στα μηνύματα e-mail (phishing attack).*
- Βρίσκεται σε ευρέως προσβάσιμο χώρο και ορισμένες φορές δεν εποπτεύεται από τον/τη γραμματέα (όταν εκείνος/-η πρέπει να μεταφερθεί σε άλλο χώρο ή να εκτελέσει κάποιο άλλο καθήκον τη δεδομένη στιγμή). Στις περιπτώσεις αυτές ο υπολογιστής αφήνεται συχνά ενεργός για λόγους διευκόλυνσης: Συνεπώς είναι δυνατή η *μη εξουσιοδοτημένη πρόσβαση από το προσωπικό (απειλή εκ των έσω) ή τους πελάτες που παρευρίσκονται στον χώρο.*

Για το **PCWS005 - Σταθμός Εργασίας (Workstation)** **(A-006)** εντοπίστηκαν τα εξής:

- Βρίσκεται σε δωμάτιο με ελεύθερη/μη ελεγχόμενη πρόσβαση (δεν υπάρχει πλήρης διαχωρισμός καθηκόντων): Λόγω αυτού, εμφανίζεται η *εκ των έσω απειλή* καθώς ένα μη εξουσιοδοτημένο μέλος του προσωπικού μπορεί να αποκτήσει πρόσβαση χωρίς αυτό να είναι αναγκαίο για τα τρέχοντα καθήκοντά του ή να είναι ακόμη και αθέμιτο.

- Είναι τοποθετημένο σε χώρο προσβάσιμο από πολυσύχναστο πεζόδρομο: Έτσι, δημιουργείται το έδαφος για *πρόσβαση στα δεδομένα από κακόβουλο άγνωστο προς το εργαστήριο άτομο (όχι πελάτη ή μέλος του προσωπικού).*

Για τα **PCWS001, PCWS002, PCWS003 - Σταθμοί Εργασίας (Workstations)** **(A-002, A-003, A-004)** από κοινού εντοπίστηκε ότι:

- Υπάρχουν κοινοί κωδικοί (credentials) για την είσοδο στους προαναφερθέντες υπολογιστές λόγω της έλλειψης πλήρους διαχωρισμού καθηκόντων (καταμερισμός των έργων): Έτσι τα άτομα του προσωπικού μοιράζονται κοινούς κωδικούς πρόσβασης για την είσοδο τους στο σύστημα, ενδυναμώνοντας την *εκ των έσω απειλή μη εξουσιοδοτημένης πρόσβασης στους υπολογιστές (και τις πληροφορίες που διαθέτουν)*. (Π.χ, η Γραμματεία δύναται να δει πληροφορίες του υπολογιστή στο εργαστήριο).

Επιπλέον, για **όλους τους Σταθμούς Εργασίας** (Workstations) εντοπίστηκαν οι εξής ευπάθειες:

- Απουσία Τείχους Προστασίας, το οποίο μπορεί να γίνει εκμεταλλεύσιμο από μία *Ransomware επίθεση*, καθώς *κακόβουλοι χρήστες μπορούν να κρυπτογραφήσουν τα δεδομένα και να ζητήσουν λύτρα για το κλειδί της αποκρυπτογράφησης.*
- Επιπλέον η απουσία Τείχους Προστασίας, μπορεί να οδηγήσει και σε *επίθεση Data Exfiltration*.

Για το **LPT001 - Φορητό Υπολογιστή (Laptop)** **(A-015)** εντοπίστηκε ότι:

- Ο κωδικός πρόσβασης είναι αδύναμος, με ελάχιστα ψηφία και σχετίζεται με προσωπικά δεδομένα του ιδιοκτήτη του (π.χ. ημερομηνία γέννησης). Έτσι καθίσταται ευάλωτο, τόσο σε *απειλές εκ των έσω* από συναδέλφους του που γνωρίζουν κάποια από τα στοιχειώδη προσωπικά του στοιχεία, όσο και από *brute force attacks* διότι είναι μικρός ο κωδικός με μηδαμινά ξεχωριστά στοιχεία.
- Η τοποθεσία του πλησίον πολυσύχναστου πεζόδρομου καθώς και η φορητότητα και το μέγεθός του: Καθίσταται εύκολη λεία για τυχόν *ληστές* που βρίσκονται στον πεζόδρομο έξω από το γραφείο του ιατρού.

Για τον **Ιστότοπο (Website)** **(A-020)** εντοπίστηκαν τα εξής:

- Απουσία πιστοποιητικού SSL/TLS: Έτσι καθίσταται εφικτή οποιαδήποτε *Man-in-the-middle* επίθεση.
- Η έκδοση του JOOMLA που χρησιμοποιείται για τον Ιστότοπο είναι παρωχημένη (3.8.8) οπότε η επικύρωση και καθαρισμός εισόδου (input validation and sanitization) δεν γίνονται ορθά. Έτσι, καθίσταται εφικτή μία SQL injection επίθεση [12].

  Στο σημείο αυτό γίνεται η παραδοχή ότι η έκδοση JOOMLA που χρησιμοποιείται είναι η 3.8.8 και δεν έχει ανανεωθεί τα τελευταία έτη. Επίσης επειδή ο ιατρός έφτιαξε το website είναι εύλογο να υποθέσουμε ότι δεν έχει μεριμνήσει για καλές πρακτικές ασφάλειας όπως updates και upgrades για εκμετάλλευση νέων patches, extension για multi-factor authentication και εγκατάσταση μόνο έμπιστων third-party extensions

  (με αυτήν την παραδοχή μπορούμε να συμπεράνουμε κάποιες ευπάθειες που οδηγούν σε πρόσβαση-σε προσωπικα δεδομένα- από εξωτερικούς χρήστες, privilege escalation κλπ)

- Μη υποστήριξη αυθεντικοποίησης πολλαπλών παραγόντων (MFA). Υφίσταται μόνο η χρήση κωδικού πρόσβασης για την είσοδο εξουσιοδοτημένων χρηστών. Κακόβουλοι χρήστες μπορούν να δοκιμάσουν να εισέλθουν με brute force attacks στον ιστότοπο και να έχουν υπό την κυριαρχία τους τον λογαριασμό του θύματος (account takeover).

- Πρόκειται για outdated προϊόν. Τα προϊόντα αυτά είναι γνωστά και με τον όρο End Of Life (EOL). Δεν υπάρχει, λοιπόν, καμία μέριμνα από τον κατασκευαστή (patches), εφόσον το προϊόν θεωρείται ληγμένο: Αυτό δύναται να οδηγήσει στη μόλυνση του ιστότοπου από μη *ασφαλή κώδικα (Cross-Site Scripting - XSS Attack* [13]*)*, και να υποκλαπούν από στοιχεία πρόσβασης χρηστών, μέχρι και πληροφορίες του ιατρικού απορρήτου.

Ως προς, το **Λειτουργικό Σύστημα Windows 10 Pro (Windows 10 Pro)** **(A-019)** εντοπίστηκε το εξής:

- Απενεργοποιημένο BitLocker ώστε πολλά δεδομένα που μεταφέρονται από τους υπολογιστές του εργαστηρίου και τρέχουν Windows 10 Pro δεν κρυπτογραφούνται: Αυτό εντείνει το ενδεχόμενο μιας σοβαρής και εκτεταμένης *διαρροής δεδομένων* σε τρίτους.

Ακολούθως για το **Λειτουργικό Σύστημα Windows 7 Pro (Windows 7 Pro)** **(A-018)** εντοπίστηκε το εξής:

- Πρόκειται για outdated προϊόν. Τα προϊόντα αυτά είναι γνωστά και με τον όρο End Of Life (EOL) [14]. Δεν υπάρχει, λοιπόν, καμία μέριμνα από τον κατασκευαστή (patches), εφόσον το προϊόν θεωρείται ληγμένο. Το συγκεκριμένο λειτουργικό σύστημα έχει μάλιστα σταματήσει και να υποστηρίζεται από την εταιρεία Microsoft [15]: Έτσι, αυτό είναι εκμεταλλεύσιμο από την απειλή της *απόκτησης πρόσβασης στο εσωτερικό δίκτυο της επιχείρησης (intranet) από μη-εξουσιοδοτημένο εξωτερικό χρήστη*. Προβλήματα δηλαδή τα οποία προέκυψαν μετά την τελευταία αναβάθμιση είναι πιθανό να τα εκμεταλλευτούν κακόβουλοι χρήστες.

Όσον αφορά τον **Διαμοιρασμό Προσωπικών Δεδομένων των ασθενών με συνεργαζόμενους παρόχους** **(A-023)** παρατηρήθηκαν τα εξής :

- Δεν δίνεται άδεια παροχής των προσωπικών δεδομένων από τον πελάτη, ενέργεια που δεν είναι σύμφωνο με τις αυστηρές ισχύουσες νομοθεσίες για την προστασία προσωπικών δεδομένων: Σε αυτήν την περίπτωση, ο ασθενής μπορεί να κινηθεί νομικά και να προβεί σε *μήνυση*.
- Απουσία ελέγχου επί των δεδομένων αφότου διαμοιραστούν με άλλους παρόχους: Το εργαστήριο χάνει τον έλεγχο των δειγμάτων και των δεδομένων των ασθενών του αφότου τα μοιράζεται με *συνεργαζόμενους παρόχους οι οποίοι μπορούν να τα εκμεταλλευτούν προς όφελος τους.*

Για το **BKUP001 - Φυσικό Αντίγραφο Ασφαλείας (Backup)** **(A-025)** εντοπίστηκε το εξής:

- Πρόκειται για μαγνητική συσκευή αποθήκευσης: Το γεγονός αυτό επιτρέπει τον (σχετικά εύκολο) απομαγνητισμό της συσκευής από κακόβουλο άτομο.
- Το μέγεθος του, η φορητότητα του και η τοποθεσία του το καθιστούν ευάλωτο σε *φυσικές κλοπές, τόσο από άτομα του εργαστηρίου, πελάτες του, όσο και από αγνώστους.*

Για την **Λήψη Αντιγράφων Ασφαλείας** **(A-024)** βρέθηκε ότι :

- Πραγματοποιείται μια φορά την εβδομάδα. Η συχνότητα αυτή θεωρείται ανεπαρκής, δεδομένων των λειτουργιών ενός αιματολογικού εργαστηρίου, καθώς ορισμένες αναλύσεις είναι χρονοβόρες και κοστοβόρες ώστε να επαναληφθούν εάν χαθούν τα αποτελέσματά τους, ενώ και τα δείγματα απορρίπτονται συνήθως μετά τη διεξαγωγή ελέγχου ποιότητας των αποτελεσμάτων.: Η απειλή που προκύπτει, λοιπόν, είναι η απώλεια δεδομένων και μάλιστα σχετικά μεγάλου όγκου.

Αναφορικά με την **Αποστολή αποτελεσμάτων των αιματολογικών εξετάσεων στους ασθενείς/πελάτες** **(A-027)** προέκυψε ότι :

- Εκτελείται από τον/τη γραμματέα, τόσο η σύνταξη των μηνυμάτων, όσο και ο έλεγχος της αποστολής τους μέσω e-mail ή fax: Με βάση αυτό, σε πιθανά λογικά λάθη της γραμματέας, δύναται να υπάρξει *αναντιστοιχία μεταξύ ασθενών και ιατρικών αποτελεσμάτων*, δηλαδή *διαρροή δεδομένων.*
- Τα δεδομένα δεν κρυπτογραφούνται όταν στέλνεται e-mail, καθώς οι θύρες 587, 993, 995 που σχετίζονται με αυτό δεν χρησιμοποιούνται: Το γεγονός αυτό είναι εκμεταλλεύσιμο από ένα πιθανό *packet sniffing.*
- Γίνεται μετάδοση αναλογικού σήματος όταν στέλνεται fax, καθώς ο εκτυπωτής έχει παρωχημένο firmware (before 1708D): Ως εκ τούτου προκύπτει η απειλή της *ωτακουσίας (eavesdropping*).

Για το **Λογισμικό SysmexXN (SysmexXN) (A-026),** έπειτα από ανάλυση, παρουσιάστηκε ότι:

- Απουσία ενημερώσεων του λογισμικού: Η απουσία updates & patches αφήνει τρωτό το σύστημα σε *ιούς και κακόβουλες επιθέσεις*.

3.4 Αποτελέσματα αποτίμησης

Στην υποενότητα αυτή παρουσιάζεται ένας συγκεντρωτικός πίνακας στο πλαίσιο της FMEA ανάλυσης, όπου καταδεικνύονται οι τριπλέτες {Πληροφοριακό αγαθό (Asset) – Ευπάθεια που φέρει (Potential Vulnerability) – Απειλή που εκμεταλλεύεται την ευπάθεια (Potential Threat)}. Για κάθε μία από αυτές αξιολογείται η επίπτωση στην Εμπιστευτικότητα, Ακεραιότητα και Διαθεσιμότητα (Ασφάλεια).

Στη συνέχεια εκτιμάται ο βαθμός επίπτωσης *{I}* και η πιθανότητα εμφάνισης *{L}* (σε κλίμακα 1-10).

Τέλος εντοπίζονται και καταγράφονται τα υπάρχοντα μέτρα (Current Controls), και εκτιμάται ο βαθμός ευπάθειας *{V}* μετά την εφαρμογή των μέτρων αυτών (σε κλίμακα 1-10).

Η τελευταία στήλη περιλαμβάνει το RPN που υπολογίζεται σύμφωνα με τον τύπο *{I x L x V}*.

Ο πίνακας παρουσιάζεται ταξινομημένος σε φθίνουσα σειρά του RPN, οπότε υψηλότερα φαίνονται τα High Risks.

Σημειώνεται ότι τυχόν επανάληψη στο ζεύγος {Ευπάθεια - Απειλή} γίνεται λόγω διαφοροποίησης στην επίπτωση, την πιθανότητα εμφάνισης ή/ και τον βαθμό ευπάθειας (οπότε δε θα ήταν ενδεικτική των προβλημάτων μία πιθανή ομαδοποίησή τους).

Asset ID	Asset Name (Type)	Function	Potential Vulnerability	Potential Threat	Potential Business Consequence (Impact)	Confidentiality Impact *(Select L, M, H)*	Integrity Impact *(Select L, M, H)*	Availability Impact *(Select L, M, H)*	Impact Ranking *(see Impact Table)*	Likelihood Ranking *(see Likelihood Table)*	Current Controls		Vulnerability Ranking After Controls Implementation (see Vuln Table)	Risk Priority Number (RPN)
											Preventive Controls	Detective Controls		
A-013	RT001	To provide access to the internet	Outdated product (EOL)	Cyber attack (effortless)	Exposure of Sensitive Data _ GDPR Penalty, malware distribution and network manipulation leading to other equipment malfunctioning, network outage and communication inability	High	High	High	9	7			10	630
A-009	SRV001	To store, process and deliver the webpages of the website to users	Web Server has limited resources (CPU, memory, disk space)	Denial-Of-Service (DOS) attack	Unavailability of website and e-mail services.	Low	Low	High	8	7			8	448
A-020	Website	Existing customers can login and view blood test results. Prospective customers may be informed about contact information	The version of JOOMLA (website) that is running is older (3.8.8) and therefore input validation and sanitization is improper	SQL injection	Sensitive information exposure, modification and deletion _ GDPR Penalty	High	High	Medium	9	6			8	432
A-007	PR0001	Used by the secretary to print the blood test results or additional files, send fax	Incorrectly (or even does not) restricts access from unauthorized actor	Arbitrary code execution (aiming to data leakage)	Reading sensitive information	High	Low	Low	7	8			7	392
A-027	Αποστολή αποτελεσμάτων των αιματολογικών εξετάσεων στους ασθενείς/πελάτες	Used for same-day dispatch of blood test results.	Lack of encryption when sending email (587, 993, 995 ports aren't used)	Packet sniffing attack	Sensitive information reveal, Reputational damage	High	Low	Low	7	7			8	392
A-014	FW001 (Firewall)	To block unauthorized network traffic	Default log-in credentials	Outsider gains access to the intranet	Create backdoors, resulting in protocol-level attacks, malicius configuration of rules, possible exposure of data	High	High	Low	8	7	Log-in credentials exist, but are default		6	336
A-009, A-010	SRV001, SRV002	**srv1:** To store, process and deliver the webpages of the website to users **srv2:** To store and manage the databases associated with Employee Data and Customer Data and provide access to users	Sensitive to humidity located in a place in direct contact with the external environment	Humidity from the external environment	Corrosion causing permanent damage to the servers, electrical issues such as short circuits, which can permanently damage the server's components and cause it to malfunction resulting in data loss or website downtime, and unavailability of e-mail services	Low	Low	High	8	6	Physical backup exists		7	336
A-020	Website	Existing customers can login and view blood test results. Prospective customers may be informed about contact information	Outdated or unpatched software	XSS attack	Exposure of customer's login credentials leading to sensitive data reveal (Health Data) _ GDPR Penalty	High	Low	Low	7	6			8	336
A-026	SysmexXN	Provide the software to analyze blood samples, providing information about cell counts, hemoglobin levels, and cell morphology	Unpatched software	Virus or Malware attack	Steal sensitive patient data or cause other harm (slow performance, etc)	High	High	Medium	8	6			7	336

A-009	SRV001	To store, process and deliver the webpages of the website to users	Lack of firewall protection	File inclusion attack (include and execute malicious files on the server)	Complete loss of control of the server Exposure of sensitive data _ GDPR Penalty, Operational Disruption, Reputational damage	High	High	Medium	7	5			9	315
A-018	Windows 7 Pro	To control network traffic, ensure security, enable efficient communication between devices, enable firmware upgrades	Software is outdated (EOL & not supported anymore - lack of security patches)	Unauthorized acces to the intranet	changes to network settings causing operational disruption	Medium	Medium	Medium (network downtime prohibits authorized users to gain access to information)	5	6			10	300
A-008	PR0002	Used by the doctor to print prescriptions, or any other additional files needed for the examination	Its firmware is outdated (EOL)	Cyber attacks (effortless)	Incorrect diagnoses, incorrect treatments (putting patients' health at risk), inabillity to print critical reports or other documents, causing delays, errors.	Medium	Medium	Medium	7	6			7	294
A-023	Διαμοιρασμός Προσωπικών Δεδομένων των ασθενών σε συνεργαζόμενους παρόχους υπηρεσιών	To better serve the patients	Not always written consent is provided by the patient	Lawsuit	GDPR Penalty (GDPR (9)(2)(a) article violation), Reputational damage	High	Low	Low	7	6	Third-parties are considered reliable		7	294
A-009, A-010	SRV001, SRV002	**srv1:** To store, process and deliver the webpages of the website to users **srv2:** To store and manage the databases associated with Employee Data and Customer Data and provide access to users	Sensitive to dust, located very close to a busy road and in direct contact with the external environment	Dust from the external environment	Dust can accumulate on the server's internal components and block the airflow, leading to overheating and causing the server to shut down, resulting in data loss or website downtime, and unavailability of e-mail services	Low	Low	High	8	6	Stuff cleans servers to prevent dust accumulation, backup plan recovery		6	288
A-009, A-010	SRV001, SRV002	**srv1:** To store, process and deliver the webpages of the website to users **srv2:** To store and manage the databases associated with Employee Data and Customer Data and provide access to users	Senitive to high temprature, located in a place in direct contact with the external environment	High temprature (especially during summer time)	Fail due to overheat. Downtime, data loss, or hardware damage leading to not available data (not available test results), email services and website.	Low	Low	High	8	6	Integrated cooling system (fans), backup plan recovery		6	288
A-013	RT001	To provide access to the internet	Placed near the sofa in the waiting room	Accidental damage (spill of coffee, kick etc)	Disrupt the network causing downtime and communication inability	Medium	Medium	High	8	5			7	280
A-019	Windows 10 Pro	To provide the user interface for essential tasks as file, resource and external device management, deal with protection and security issues	Disabled BitLocker (lack of data encryption)	Data Leakage	Non compliance with article 32 of GDPR - Penalty	High	High	Low	7	5			8	280
A-002, A-003, A-004, A-005, A-006	GROUPING OF ALL WORKSTATIONS	(omitted)	Lack of firewall protection	Ransomware attack	High ransom payment in exchange for the decryption key	Medium	Medium	High	9	5	Educated employees on how to identify and avoid phishing emails and other common ransomware delivery methods, Windows Defender is used, backup implementation		6	270
A-020	Website	Existing customers can login and view blood test results. Prospective customers may be informed about contact information	Only parssword authentication (MFA is not supported)	Account takeover	Exposure of Sensitive Data (Health Data) _ GDPR Penalty	High	Low	Low	7	6	Only strong passwords acceptd (10 digits, symbols, numbers and capitals included)		6	252
A-020	Website	Existing customers can login and view blood test results. Prospective customers may be informed about contact information	No SSL/TLS certificate (lack of data encryption)	Man-in-the-middle attack	Exposure of Sensitive Data (Health Data) _ GDPR Penalty	High	High	Low	7	5			7	245
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
A-013	RT001	To provide access to the internet	Only basic (intergrated) firewall protection	Data Leakage	Exposure of Sensitive Data _ GDPR Penalty	High	Medium	Low	7	5	There is basic integrated firewall protection		6	210

A-002, A-003, A-004, A-005, A-006	GROUPING OF ALL WORKSTATIONS	(omitted)	Lack of firewall protection	Data exfiltration (a.k.a. data extrusion or data exportation)	Exposure of Sensitive Data _ GDPR Penalty, Legal and Financial Impact, Privacy violation, Reputational Damage, Potentially compromise the integrity of data by altering or deleting it,	High	Medium	Low	7	5	Windows Defender is used		6	210
A-027	Αποστολή αποτελεσμάτων των αιματολογικών εξετάσεων στους ασθενείς/πελάτες	Used for same-day dispatch of blood test results.	Human Error (faulse address/phone number typing)	Data breach	Sensitive information reveal, Reputational damage	High	Low	Low	7	7	Secretary is aware and somewhat cautius		4	196
A-011	SW001	To network the devices (except for servers) and the internet router	Placed near the sofa in the waiting room	Accidental damage (spill of coffee, kick etc)	Disrupt the network causing downtime and communication inability	Low	Low	High	5	5			7	175
A-023	Διαμοιρασμός Προσωπικών Δεδομένων των ασθενών με συνεργαζόμενους παρόχους υπηρεσιών	To better serve the patients	Sharing health care data with third-parties (Loss of control over the shared data)	Third-party exploitation of data for their personal interest	Fabrication or/and exposure of Sensitive Data (Health Data) _ GDPR Penalty, Reputational damage	High	High	Medium	7	4	Third-parties are considered reliable		6	168
A-027	Αποστολή αποτελεσμάτων των αιματολογικών εξετάσεων στους ασθενείς/πελάτες	Used for same-day dispatch of blood test results.	Transmission of analog signals when using fax (printer has old firmware before 1708D)	Eavesdropping attack	Sensitive information reveal, potential modification of the content, possible interception and block of fax transmissions	High	Medium	Medium	7	4			6	168
A-009, A-010	SRV001, SRV002	**srv1:** To store, process and deliver the webpages of the website to users **srv2:** To store and manage the databases associated with Employee Data and Customer Data and provide access to users	Located on ground floor without flood sensors	Flood	Server Destruction or damage leading to unavailability of the website and e-mail services, and potential data loss (unavailability of test results etc), Cost of replacement	Low	Low	High	9	3	Backup plan recovery		6	162
A-009, A-010	SRV001, SRV002	**srv1:** To store, process and deliver the webpages of the website to users **srv2:** To store and manage the databases associated with Employee Data and Customer Data and provide access to users	Placed near chemical substances	Explosion/ fire outbreak	Server Destruction leading to unavailability of the website and e-mail services, and potential data loss (unavailability of test results etc), Cost of replacement	Low	Low	High	8	4	Fire extinguisher, backup plan recovery	Fire detection system	5	160
A-009, A-010	SRV001, SRV002	**srv1:** To store, process and deliver the webpages of the website to users **srv2:** To store and manage the databases associated with Employee Data and Customer Data and provide access to users	Placed in an open-door room	Vandalism	Server Theft, Server Destruction or damage leading to unavailability of the website, e-mail services and potential data loss (unavailability of test results etc), Cost of replacement	Low	Low	High	8	5	Backup plan recovery	CCTV	4	160
A-012	SW002	To network the 2 servers and the internet router	Placed in an open-door room	Vandalism	Switch Physical Theft, Destruction or Damage resulting in website, data and e-mail services being unavailable, Cost of replacement	Low	Low	High	8	5		CCTV	4	160
A-015	LTP001	The personal laptop of the doctor. Used for personal communication and business contact management.Used as a desktop replacement if needed.	Portable device, placed in a room with access to a busy pedestrian precinct	Physical Theft	Exposure of doctor's personal data (by unlocking the device or through the storage disk), Cost of laptop raplacement	High	Low	Medium	8	5	Doctor is present in the room (most of the time) and prevents malicius access		4	160
A-002, A-003, A-004	GROUPING OF ALL THESE WORKSTATIONS	**PC1:** To manage and store blood test data (CBC, hematocrit levels, blood chemistry values), perform quality control, interpretation and report generation, communication within the laboratory **PC2**: To manage and store blood test data (CBC, hematocrit levels, blood chemistry values), perform quality control, interpretation and report generation, communication within the laboratory **PC3:** To register blood sample according to barcode and associate it with patient	Shared passwords (due to lack of segregation of duties)	Acces by unauthorized personnel (insider threat)	Removal/ Modification of crucial information regarding treatment plans, prescriptions etc.	Medium	High	Low	5	5	Internal Employee Rules		6	150
A-024	Λήψη Αντιγράφων Ασφαλείας	To ensure the availability of patients' health care data in case of a system failure, or physical theft of the computer	Performed once a week (quite low frequency)	Data Loss (and high volume of data being lost)	Imposssible data recovery or Increased recovery time (In some cases all blood tests done within the week should be re-executed impacting the laboratory's operations and their patients)	Low	Low	High	5	5	Backup plan exists		6	150
A-015	LTP001	The personal laptop of the doctor. Used for personal communication and business contact management.Used as a desktop replacement if needed.	Weak password	Unauthorized access (by personnel (insider threat) or brute force attack)	Exposure of doctor's personal data, possible denial of access for the doctor	High	Medium	Low	6	4	Built-in firewall and antivirus software (basic)		6	144

A-025	BKUP001	To provide a means of recovery in case the primary data storage is lost or damaged	Small in size portable device, placed in an easily accessible room	Physical theft (by insider - insider threat -, customer, or stranger)	Loss of access to critical data, Cost of new external HDD	High	Low	Medium	9	5	HDD backup is placed insede a locked drawer, doctor is present in the room (most of the time) and prevents malicius access		3	135
A-009, A-010	SRV001, SRV002	**srv1:** To store, process and deliver the webpages of the website to users **srv2:** To store and manage the databases associated with Employee Data and Customer Data and provide access to users	Lack of anti-seismic racks	Earthquake	Server Destruction, Cost of replacement	Low	Low	High	9	2	Backup plan recovery		7	126
A-017, A-016	Employee Data, Customer Data	**A17**:Supports Employees Filing Obligations, Payments, Personal Records **A16:** Supports organizing and finding blood test records of customers/patients, includes personal information	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
A-002, A-003	PCWS001, PCWS002	**PC1:** To manage and store blood test data (CBC, hematocrit levels, blood chemistry values), perform quality control, interpretation and report generation, communication within the laboratory **PC2**: To manage and store blood test data (CBC, hematocrit levels, blood chemistry values), perform quality control, interpretation and report generation, communication within the laboratory	Placed in a room with unrestricted physical access (lack of segregation of duties)	Access by unauthorized personnel (insider threat)	Manipulating test results, Remove/Modify critical information	High	High	Low	7	4	Internal Employee Rules		4	112
A-002, A-003	PCWS001, PCWS002	**PC1:** To manage and store blood test data (CBC, hematocrit levels, blood chemistry values), perform quality control, interpretation and report generation, communication within the laboratory **PC2**: To manage and store blood test data (CBC, hematocrit levels, blood chemistry values), perform quality control, interpretation and report generation, communication within the laboratory	Placed in a room with access to an unfenced courtyard	Access by malicious stranger	Manipulating test results, Remove/Modify critical information, cause damage to the device	Medium	High	High	7	4	Personnel almost always present in the room and prevents malicius access		4	112
A-014	FW001 (Firewall)	To block unauthorized network traffic	Placed in an open-door room	Vandalism	Firewall Physical Theft, Firewall Destruction or Damage, Cost of replacement	High	High	Low	8	3		CCTV	4	96
A-021	Φυσικό Αρχείο Ασθενών	Supports organizing and finding blood test records of patients	Files kept in not secured place, in easy accessible library without lockers	Files are stolen by malicious customer	Exposure of Personal Data _ GDPR Penalty	High	Low	Medium	7	4	Secretary monitors and prevents malicious access to files		3	84
A-006	PCWS005	Used by the doctor for monitoring the patient personal records, registering the prescriptions, communication with other healthcare providers (including sending and receiving patient referrals) etc.	Placed in a room with access to a busy pedestrian precinct	Acess by malicious stranger	Removal/ Modification of crucial information regarding treatment plans, prescriptions etc., cause damage to the device	High	Medium	Medium	7	4	Doctor is present in the room (most of the time) and prevents malicius access		3	84
A-009, A-010	SRV001, SRV002	**srv1:** To store, process and deliver the webpages of the website to users **srv2:** To store and manage the databases associated with Employee Data and Customer Data and provide access to users	Placed near water tap	Water leak	Server short circuit resulting in unavailability of the website and e-mail services for some period of time, and unavailability of data	Low	Low	High	5	4	Stuff aware and cautius, backup plan recovery		4	80
A-001	LabWS001	To run tests on blood samples.	Placed in a room with access to an unfenced courtyard	Access by malicious stranger	Manipulating test results, Remove/Modify critical information, cause damage to the device	Low	High	Medium	5	4	Personnel almost always present in the room and prevents malicius access		4	80
A-001	LabWS001	To run tests on blood samples.	Placed in a room with unrestricted physical access (lack of segregation of duties)	Access by unauthorized personnel (insider threat)	Manipulating test results, Remove/Modify critical information	High	High	Low	5	4	Internal Employee Rules		4	80

A-004, A-006	PCWS003, PCWS005	**PC3:** To register blood sample according to barcode and associate it with patient **PC5**: Used by the doctor for monitoring the patient personal records, registering the prescriptions, communication with other healthcare providers (including sending and receiving patient referrals) etc.	Placed in a room with unrestricted physical access (lack of segregation of duties)	Access by unauthorized personnel (insider threat)	Removal/ Modification of important information	High	High	Low	5	4	Internal Employee Rules		4	80
A-014	FW001 (Firewall)	To block unauthorized network traffic	Placed near chemical substances	Explosion/ fire outbreak	Firewall Destruction, Cost of replacement	High	High	Low	9	4	Fire extinguisher	Fire detection system	2	72
A-022	Αρχείο Υπαλλήλων & Προμηθευτών	Supports Filing Obligations, Payments, Accounting Records	Files kept in not secured place, in 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
A-025	BKUP001	To provide a means of recovery in case the primary data storage is lost or damaged	Magnetic Storage Device, placed in an easily accessible room	Degaussion (Demagnetizatization) by malicious actor	Loss of access/ modification of critical data	Low	Medium	Medium	8	3	HDD backup is placed insede a locked drawer, doctor is present in the room (most of the time) and prevents malicius access		3	72
A-005	PCWS004	Used by the secretary for email communication, customer contacts management, blood test results, financial management, orders to suppliers	Used by a secretary who extensively uses e-mail communication (with customers and stakeholders)	Malware infection through e-mail attachments (phishing attack)	Data Breach_GDPR Penalty, Operational disruption, system malfunctioning/ disabled	High	High	Low	7	4	Secretary is aware and cautius, Windows Defender is used		2	56
A-013	RT001	To provide access to the internet	Misconfiguration	Outsider gains access to the intranet	Sneak sensitive information, such as network traffic logs, configuration details, and authentication credentials , potentially cause connectivity problems, slow performance	High	Medium	Medium	6	4	Automation tools are used (such as network configuration management software)	Automation tools are used (such as network configuration management software)	2	48
A-005	PCWS004	Used by the secretary for email communication, customer contacts management, blood test results, financial management, orders to suppliers	Placed in a public area and sometimes left unattended	Unauthorized access (by personnel (insider threat) or customers)	Removal/Modification of important information regarding business procedures (e.g. appointments schedule etc.)	Medium	Medium	Low	4	3	Internal Employee Rules		4	48
A-011, A-012	SW001 - SW002	**SW1**: To network the devices (except for servers) and the internet router **SW2**: To network the 2 servers and the internet router	Misconfiguration	Outsider gains access to the intranet	Data loss, connectivity problems, slow performance	Medium	Medium	Medium	6	3	Automation tools are used (such as network configuration management software)	Automation tools are used (such as network configuration management software)	2	36
A-022, A-021	Αρχείο Υπαλλήλων & Προμηθευτών, Φυσικό Αρχείο Ασθενών	**A22:** Supports Filing Obligations, Payments, Accounting Records **A21:** Supports organizing and finding blood test records of patients	Files are kept in non fire-proof cabinet	Fire outbreak	Physical File destruction and hassle of recovery process (time and resources consumption)	Low	Low	Medium	3	2	Fire extinguisher	Fire detection system	3	18

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

Δεν προτείνονται σχετικά μέτρα.

4.2 Ταυτοποίηση και αυθεντικοποίηση

Όσον αφορά τη χρήση των υπολογιστών και του αιματολογικού αναλυτή παρατηρήθηκε ότι για την είσοδο στο σύστημα χρησιμοποιούνται κοινοί κωδικοί πρόσβασης, ενώ δεν υπάρχει και πλήρης διαχωρισμός καθηκόντων. Αυτές οι τακτικές δεν θεωρούνται κατάλληλες σε ένα μικροβιολογικό εργαστήριο καθώς η πρόσβαση σε εμπιστευτικές πληροφορίες και δεδομένα οφείλει να γίνεται από τους αρμόδιους εργαζόμενους (μετριάζοντας έτσι την πιθανότητα εμφάνισης κάποιας απειλής εκ των έσω). Πηγαίνοντας ένα βήμα παρακάτω το συλλογισμό μας, προτείνουμε την **δημιουργία συστήματος ελέγχου πρόσβασης βασισμένο σε ρόλους (RBAC)**. Έτσι, εξασφαλίζεται ότι οι εργαζόμενοι θα έχουν πρόσβαση σε φακέλους ανάλογα με την ειδικότητα και τις αρμοδιότητές τους. (Προφανώς και **οι κωδικοί πρόσβασης απαιτείται να είναι διαφορετικοί για κάθε ρόλο**).

Όσον αφορά το Τείχος Προστασίας (firewall) παρατηρήθηκε ότι τα **διαπιστευτήρια σύνδεσης (credentials)** είναι τα προκαθορισμένα/ κοινότυπα (default). Έτσι είναι εξαιρετικά εύκολο κάποιος τρίτος να αποκτήσει πρόσβαση (guessing - brute force attack). Υπογραμμίζουμε την ανάγκη **άμεσης αλλαγής τους σε ισχυρότερα.**

Στον Ιστότοπο του εργαστηρίου δεν υποστηρίζεται η **αυθεντικοποίηση πολλαπλών παραγόντων (MFA)**. Παρότι ο κωδικός πρόσβασης που χρησιμοποιείται είναι ισχυρός, προτείνουμε να ληφθεί μέριμνα για την αυθεντικοποίηση εφόσον τα δεδομένα που δύνανται να προσπελαστούν λόγω μιας πιθανής εισόδου μη εξουσιοδοτημένου χρήστη στον λογαριασμό ενός ασθενή είναι ευαίσθητα (ιατρικό απόρρητο). Το JOOMLA δεν παρέχει ενσωματωμένο **MFA**, ωστόσο **διατίθενται επεκτάσεις από τρίτους φορείς (third-party extensions)**. Εφιστούμε την προσοχή στην επιλογή μιας αξιόπιστης και ευυπόληπτης λύσης,

ειδάλλως μπορεί να προκύψουν προβλήματα με την ασφάλεια των δεδομένων. Προτείνουμε συγκεκριμένα το *Google Authenticator* [16] που είναι δωρεάν και ευρέως χρησιμοποιούμενο. Υλοποιεί **two-factor authentication (2FA)** παράγοντας εξαψήφιους κωδικούς μιας χρήσης (one-time passwords (OTP)) κάθε 30 δευτερόλεπτα. Ο κωδικός αυτός μπορεί να εισαχθεί μόνο μια φορά και είναι έγκυρος για ένα μικρό χρονικό διάστημα, καθιστώντας δύσκολο για κάποιον επιτιθέμενο να αποκτήσει πρόσβαση στον λογαριασμό, ακόμη και αν βρει τον κωδικό. Άλλες λύσεις που όμως απαιτούν συνδρομή είναι οι Duo Security, Authy, and YubiKey, οι οποίες έχουν περισσότερες δυνατότητες αλλά θεωρούμε ότι δεν είναι αναγκαίο το κόστος για καταφυγή σε αυτές.

4.3 Έλεγχος προσπέλασης και χρήσης πόρων

Εντοπίστηκε ότι ο εκτυπωτής της γραμματέως δεν έχει σωστά διαμορφωθεί ως προς το περιορισμό της πρόσβασης σε αυτόν. Προτείνουμε αρχικά την **εγκαθίδρυση ελέγχου πρόσβασης (access control)** μέσω της δημιουργίας **ισχυρών κωδικών,** καθώς και της **πρόσβασης στον εκτυπωτή από συγκεκριμένες IP** (αυτό υποστηρίζεται και από το πλάνο κατάτμησης του δικτύου). Ένα επιπλέον μέτρο που αμβλύνει την επίπτωση μιας πιθανής μη εξουσιοδοτημένης πρόσβασης στον εκτυπωτή είναι **η κρυπτογράφηση των δεδομένων που στέλνονται από και προς αυτόν.** Έτσι ακόμα και σε περίπτωση διαρροής τους, αυτά δεν θα είναι ορατά. Εφιστούμε επίσης την προσοχή σας στις **τακτικές αναβαθμίσεις (updates) του firmware** καθώς συνήθως περιλαμβάνουν καινούρια security patches.

4.4 Διαχείριση εμπιστευτικών δεδομένων

Όπως εντοπίστηκε παραπάνω, η διαδικασία του Διαμοιρασμού Προσωπικών Δεδομένων των ασθενών με συνεργαζόμενους παρόχους υπηρεσιών είναι προβληματική, εφόσον όπως αναφέρει ο επιθεωρητής δεν δίνεται πάντα άδεια παροχής των προσωπικών δεδομένων από τον ασθενή/πελάτη. Συγκεκριμένα, σύμφωνα με το άρθρο (9)(2)(α) του GDPR [17] το εργαστήριο οφείλει να ζητά **ρητή συναίνεση για τον διαμοιρασμό των προσωπικών και ιατρικών δεδομένων των ασθενών με συνεργαζόμενους παρόχους υπηρεσιών**. Με αυτόν τον τρόπο εξασφαλίζεται η συμμόρφωση με τη νομοθεσία και η αποφυγή σοβαρών νομικών κυρώσεων και υψηλών προστίμων [18].

Ως προς το πρόβλημα της απουσίας ελέγχου επί των δεδομένων αφότου αυτά διαμοιραστούν με άλλους παρόχους και της απειλής εκείνοι να τα εκμεταλλευτούν κακόβουλα προς όφελος τους, προτείνονται τα εξής:

1. Να μοιράζονται μόνο τα δεδομένα που είναι **απολύτως απαραίτητα** για την εκτέλεση των διαδικασιών.
2. Να υιοθετηθεί η πρακτική της **υπογραφής συμφωνητικού για τον διαμοιρασμό των δεδομένων**, ανεξαρτήτως του βαθμού εμπιστοσύνης προς τους συνεργάτες. Η συμφωνία αυτή θα υπογραμμίζει τον τρόπο με τον οποίο θα χρησιμοποιηθούν τα δεδομένα αυτά και οποιαδήποτε αθέτησή της θα επιφέρει νομικές συνέπειες στα συμβαλλόμενα μέρη. Έτσι μειώνεται το κίνητρο για κακόβουλες ενέργειες.
3. Να **παρακολουθείται η πρόσβαση στα δεδομένα**, ότι δηλαδή γίνεται μόνο από άτομα που το εργαστήριο έχει εξουσιοδοτήσει, καθώς και η καταλληλότητα της διαχείρισής τους, ότι δηλαδή χρησιμοποιούνται με τον σωστό τρόπο που έχει προσυμφωνηθεί. Αυτό μπορεί να επιτευχθεί αν τα δεδομένα βρίσκονται σε κοινόχρηστα (με το

εργαστήριο) ηλεκτρονικά αρχεία, τουλάχιστον αυτά για τα οποία δεν απαιτείται φυσική αποστολή τους.

4. Όσον αφορά τα δείγματα, να διατηρείται ένα μέρος τους γνωστό και ως **residual sample**, ενδεχομένως αυτό που ήδη διατηρείται για την διενέργεια των ελέγχων ποιότητας των αποτελεσμάτων (quality control), ώστε να χρησιμεύει ως αντίγραφο ασφαλείας.

Η αποστολή των αποτελεσμάτων μέσω fax φαίνεται παρωχημένη. Τέτοιες τεχνικές αποφεύγονται για λόγους ασφαλείας. Προτείνουμε την **κατάργηση της αποστολής των εξετάσεων στους ασθενείς μέσω fax**, και την **υιοθέτηση ασφαλέστερων μεθόδων, όπως είναι η αποστολή των e-mail κρυπτογραφημένα και με απαίτηση εισαγωγής κωδικού** (π.χ. .zip αρχείο με κωδικό - ΑΜΚΑ ή οποιοδήποτε κλειδί θεωρείται ασφαλές) για την προσπέλασή τους. Έτσι, μετριάζουμε τις επιπτώσεις ενός ανθρώπινου λάθους, εξασφαλίζοντας ότι ακόμη και σε εσφαλμένη πληκτρολόγηση κάποιας ηλεκτρονικής διεύθυνσης από τη γραμματεία το αρχείο που θα έχει σταλεί σε λάθος παραλήπτη δεν θα είναι δυνατό να διαβαστεί (και έτσι διατηρούμε στο ακέραιο την εμπιστευτικότητα των δεδομένων). Εκτός από το ανθρώπινο λάθος ωστόσο, λόγω του ότι τα πακέτα που υπάρχουν στο δίκτυο είναι κρυπτογραφημένα εξασφαλίζουμε και ότι σε περίπτωση κλοπής τους (packet-sniffing attack, man-in-the-middle attack) θα είναι αδύνατη η αποκρυπτογράφησή τους.

Όπως αναφέρεται και σε σχετική έρευνα που διεξήχθη από τον HIPAA[19], **η κατάλληλη συχνότητα εκτέλεσης λήψης αντιγράφων ασφαλείας σε ένα μικροβιολογικό εργαστήριο είναι μία φορά την ημέρα**. Το μικροβιολογικό εργαστήριο παράγει καθημερινά μεγάλο όγκο δεδομένων και η λήψη αντιγράφων ασφαλείας μόνο μία φορά την εβδομάδα πέρα από ελλιπής θεωρείται και αρκετά κοστοβόρα (σε περίπτωση απώλειας των δεδομένων το εργαστήριο πρέπει να επαναλάβει τις εξετάσεις μιας ολόκληρης εβδομάδας με κάποιες εξετάσεις να είναι τόσο χρονοβόρες όσο και κοστοβόρες οδηγώντας έτσι σε μεγάλο κόστος - εφόσον θεωρούνται ήδη πληρωμένες από τους ασθενείς, αλλά και στη χειρότερη περίπτωση κάποια -αν όχι όλα τα- δείγματα θα έχουν ήδη απορριφθεί, γεγονός το οποίο θα έχει μεγάλη επίπτωση στη φήμη της επιχείρησης). Ένας άλλος σημαντικός παράγοντας είναι η συμμόρφωση με τους κανόνες του GDPR οι οποίοι αναφέρουν ρητά πως οι υγειονομικοί οργανισμοί πρέπει να φροντίζουν για την διαθεσιμότητα των δεδομένων των ασθενών [20].

Ως προς την διαθεσιμότητα των δεδομένων και πληροφοριών του εργαστηρίου, κρίνεται σημαντική η **αποθήκευση του αντιγράφου ασφαλείας στο Cloud**. Συγκεκριμένα, πληροφορίες του φυσικού, τώρα, αντιγράφου ασφαλείας (εξωτερικός σκληρός δίσκος - HDD) όπως προσωπικά δεδομένα ασθενών και υπαλλήλων, αποτελέσματα εξετάσεων κ.λπ. μπορούν να διαφυλλάσονται στο Cloud ώστε να εξασφαλίζεται το αδιάβλητό τους από φυσικές καταστροφές ή κακόβουλες ενέργειες. Με αυτόν τον τρόπο εξαλείφεται και ο κίνδυνος απώλειας και αλλοίωσης των αντιγράφων ασφαλείας από εξωγενείς παράγοντες (μαγνήτες, κλοπές) καθώς οι πληροφορίες βρίσκονται απομακρυσμένα σε άλλους υπολογιστές [21]. Επιπλέον το κόστος αυτής της λύσης είναι σχετικά χαμηλό.

Προκειμένου να διασφαλιστεί η εμπιστευτικότητα των δεδομένων που βρίσκονται σε όλους τους υπολογιστές που τρέχουν **Windows 10 Pro**, είναι **απαραίτητη η ενεργοποίηση του BitLocker**. Αυτό χρησιμοποιεί ισχυρούς αλγόριθμους κρυπτογράφησης και έτσι σε περίπτωση κλοπής του σκληρού δίσκου διασφαλίζεται ότι τα δεδομένα που περιέχει δεν θα είναι ορατά χωρίς το σωστό κλειδί ανάκτησης BitLocker.

Για το σύνολο των υπολογιστών, όσον αφορά την απειλή της Data exfiltration επίθεσης, αυτή εκμεταλλεύεται κυρίως την απουσία Τείχους Προστασίας (Firewall) στους υπολογιστές για να

εκδηλωθεί. Πέραν αυτού του γεγονότος (διορθώνεται με την πρόταση του πλάνου του δικτύου), το πρόβλημα μπορεί να μετριαστεί με την **εγκατάσταση Data Loss Prevention (DLP)** εργαλείων που σαρώνουν και παρακολουθούν τα δεδομένα καθώς κινούνται στο δίκτυο είτε αυτά στέλνονται με email, είτε με διαμοιραζόμενα αρχεία κ.λπ. Εργαλεία αυτής της μορφής υπάρχουν πολλά, με καλές αναλογίες ποιότητας-κόστους.

Αναφορικά με την προστασία των εμπιστευτικών δεδομένων που φιλοξενούνται στον Διακομιστή (Database Server), προτείνεται η **διαμόρφωση (configuration) της βάσης δεδομένων για χρήση κρυπτογράφησης** ώστε να χρησιμοποιεί **Advanced Encryption Standard (AES)** για τις συγκεκριμένες στήλες ή πίνακες που απαιτούν κρυπτογράφηση. Αυτό γίνεται με τη δημιουργία νέων στηλών για την αποθήκευση των κρυπτογραφημένων δεδομένων ή την τροποποίηση υπαρχουσών στηλών για χρήση κρυπτογράφησης.

Στο σημείο αυτό αναφέρουμε ότι στις ευπάθειες που σχετίζονται με το φυσικό αρχείο ασθενών και υπάλληλων/προμηθευτών αποδεχόμαστε τον εναπομείναντα κίνδυνο διότι μία πιθανή χρήση κλειδαριάς για παράδειγμα θα δυσχέραινε το έργο της γραμματείας. Προτείνεται να συνεχιστεί η ήδη εφαρμοζόμενη εποπτεία του χώρου από τη γραμματεία

4.5 Προστασία από τη χρήση υπηρεσιών από τρίτους

Δεν προτείνονται σχετικά μέτρα.

4.6 Προστασία λογισμικού

Για τον Ιστότοπο του εργαστηρίου παρατηρήθηκε ότι δημιουργήθηκε από το λογισμικό JOOMLA παλαιότερης έκδοσης (3.8.8). Αυτο το καθιστά ιδιαίτερα ευάλωτο σε μολύνσεις από επιβλαβείς κώδικες (XSS Attack) με σκοπό κακόβουλοι χρήστες να υποκλέψουν, αλλοιώσουν ή και αφαιρέσουν πληροφορίες των ασθενών ή ακόμη και να τροποποιήσουν το περιεχόμενο του Ιστοτόπου. Ως αντίμετρο προτείνεται η **χρήση επεκτάσεων (extensions)** του JOOMLA **όπως το JSecure, SecurityCheck και RSFirewall** που διασφαλίζουν την αυθεντικοποίηση εισόδου, κωδικοποίηση εξόδου και το CSP (Content Security Policy). Ακόμη, προτείνεται και η **αναβάθμιση του λογισμικού του JOOMLA στην τελευταία έκδοσή του (4.3.0)**. Επιπλέον, για την αντιμετώπιση του SQL Injection, προτείνουμε την υλοποίηση **Web Application Firewall (WAF)**, το οποίο φιλτράρει κακόβουλη κίνηση και έτσι σταματάει (blocks) προσπάθειες για SQL Injection. (Υπάρχει πληθώρα open-source WAFs τα οποία μπορούν να ενσωματωθούν με το JOOMLA).

*Με την αναβάθμιση της έκδοσης του JOOMLA ΣΕ 4.3.0, αναβαθμίζεται και ο κώδικας της εφαρμογής ώστε να υπάρχει input validation & sanitization, prepared statements κ.λπ.).

4.7 Διαχείριση ασφάλειας δικτύου

Ως προς τις ευπάθειες που σχετίζονται με την **έλλειψη Τείχους Προστασίας** (Firewall) και τις επικείμενες απειλές που μπορούν να εκμεταλλευτούν το γεγονός αυτό κυρίως στους Σταθμούς Εργασίας (Workstation), τον Διακομιστή Ιστού (Web Server), στους Εκτυπωτές (Printers) και τον Δρομολογητή (Router) (ουσιαστικά μόνο ο Διακομιστής Βάσεων Δεδομένων (Database Server) καλύπτεται από το υπάρχον Τείχος Προστασίας), προτείνεται η **μετακίνηση του Τείχους Προστασίας** κατά πως φαίνεται στο ακόλουθο σχήμα.

Επίσης, προκειμένου να αντιμετωπιστεί κάποιο **πιθανό λάθος στη διαμόρφωση** (misconfiguration) στους κανόνες του Τείχους Προστασίας (διακυβεύοντας την ασφάλεια

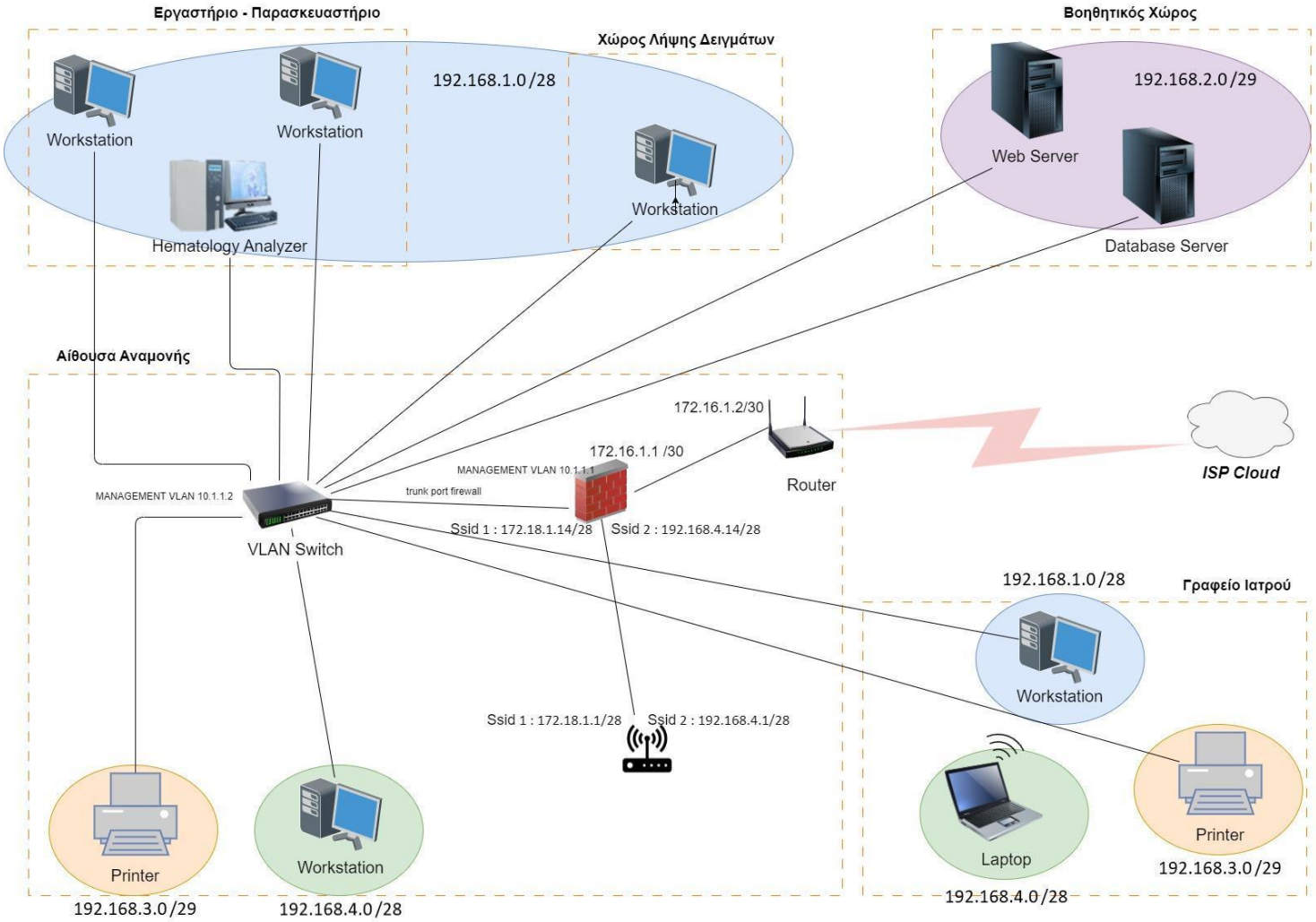
ολόκληρου του δικτύου), προτείνουμε την **πρόσληψη ειδικού** (Τεχνικός Δικτύων) ώστε να εξασφαλιστεί η σωστή διαμόρφωση των κανόνων του. Επιπροσθέτως, επειδή το Firewall θεωρείται ένα κύριο συστατικό της ασφαλούς λειτουργίας του δικτύου και των πακέτων που λαμβάνονται και στέλνονται από το εσωτερικό δίκτυο (intranet) θεωρούμε πως η επιπλέον διαφύλαξη της ασφάλειας του είναι απαραίτητη. Έτσι, προτείνεται η εγκατάσταση **Firewall management software** όπως το *Cisco ASDM*, όπως και η χρήση **Automated testing tools** τα οποία μπορούν να προσομοιώσουν διάφορους τύπους κυκλοφορίας των πακέτων εξετάζοντας πώς οι κανόνες του Firewall ανταποκρίνονται. Τέλος, προτείνουμε και τη χρήση **Network monitoring tools** που αναγνωρίζουν μη-συνηθισμένη ή μη-εξουσιοδοτημένη κίνηση, η οποία προσπαθεί να προσπεράσει το Τείχος Προστασίας.

Προτείνουμε επιπλέον **να αντικατασταθεί ο Μεταγωγέας** που έχει παρωχημένο (και άρα unpatched) λειτουργικό σύστημα (Windows 7 Pro) και μειωμένη χωρητικότητα από έναν **καινούριο, L2 (Layer-2) managed με 24 πόρτες (ώστε να μπορεί να υποστηρίξει τη σύνδεση όλων των συσκευών) και αυξημένη χωρητικότητα.** Συγκεκριμένα η πρότασή μας είναι ένας *D-link Dgs-1210-24 Network Switch Managed L2 Gigabit Ethernet (10/100/1000) Black 1u* [22], μια αρκετά προσιτή λύση.

Σε αυτό το σημείο αναφέρεται ότι ως προς το λογισμικό Windows 7 Pro που χρησιμοποιείται από το Switch - εφόσον θα αντικατασταθεί -, δεν χρειάζεται να αναφερθούν αντίμετρα.

Επιπροσθέτως, παρατηρήθηκε ότι **ο Δρομολογητής (Router)** που χρησιμοποιείται είναι End Of Life [9] :γεγονός που τον καθιστά εξαιρετικά ευπαθή σε κοινότυπες διαδικτυακές επιθέσεις. Πρότασή μας είναι λοιπόν η **αντικατάσταση του με έναν νεότερο,** και συγκεκριμένα κάποιον εκ των *Cisco RV340, RV345, RV345P, and RV340W Dual WAN Security Route*r (ανάλογα και με τον προϋπολογισμό). Αυτοί προσφέρουν σημαντικά πλεονεκτήματα όπως Intrusion Prevention and Detection System, Antivirus, Automatic software download and update (κ.α.)[23] μειώνοντας έτσι σημαντικά απειλές που επηρεάζουν την ακεραιότητα, εμπιστευτικότητα και ακεραιότητα των δεδομένων.

Στο σημείο αυτό παρουσιάζουμε το δικτυακό διάγραμμα συνδέσεων των πληροφοριακών συστημάτων όπως κρίνουμε ότι είναι κατάλληλο να διαμορφωθεί.



(Προφανώς οι υπολογιστές, εκτυπωτές, Διακομιστές κ.λπ. παίρνουν κάποια IP ανάλογα με το subnet στο οποίο ανήκουν.

Σημειώνεται ότι χρειάστηκε ασύρματο Δίκτυο διότι ο φορητός υπολογιστής που χρησιμοποιείται από τον ιατρό δεν διαθέτει κάρτα δικτύου, και άρα χρειάζεται να συνδεθεί ασύρματα.)

Παρακάτω φαίνονται με περισσότερη ανάλυση τα VLANS, subnets.

HOSTS	NETWORK ID	1st. ADDRESS	Last ADDRESS	BROADCAST	SUBNET MASK	/ MASK	HOSTS(-2)	Location Name
16	192.168.1.0	192.168.1.1	192.168.1.14	192.168.1.15	255.255.255.240	/28	16 (14)	ergastirio
8	192.168.2.0	192.168.2.1	192.168.2.6	192.168.2.7	255.255.255.248	/29	8(6)	servers
8	192.168.3.0	192.168.3.1	192.168.3.6	192.168.3.7	255.255.255.248	/29	8(6)	printers
16	192.168.4.0	192.168.4.1	192.168.4.14	192.168.4.15	255.255.255.240	/28	16 (14)	wireless (personnel)
16	10.1.1.0/28	10.1.1.1	10.1.1.6	10.1.1.7	255.255.255.248	/29	8(6)	VLAN management

RT

HOSTS	NETWORK ID	1st. ADDRESS	Last ADDRESS	BROADCAST	SUBNET MASK	/ MASK	HOSTS(-2)	Location Name		
4	172.16.1.0	172.16.1.1	172.16.1.2	172.16.1.3	255.255.255.252	/30	4(2)	router-fw communication	router only	WAN port

FW

HOSTS	NETWORK ID	firewall ADDRESS	Last ADDRESS	BROADCAST	SUBNET MASK	/ MASK	HOSTS(-2)	Location Name	
16	192.168.1.0	192.168.1.14	192.168.1.14	192.168.1.15	255.255.255.240	/28	16 (14)	VLAN ergastirio	
8	192.168.2.0	192.168.2.6	192.168.2.6	192.168.2.7	255.255.255.248	/29	8(6)	VLAN servers	
8	192.168.3.0	192.168.3.6	192.168.3.6	192.168.3.7	255.255.255.248	/29	8(6)	VLAN printers	
16	192.168.4.0	192.168.4.14	192.168.4.14	192.168.4.15	255.255.255.240	/28	16 (14)	VLAN wireless (personnel)	
4	172.17.1.0	172.17.1.1	172.17.1.2	172.17.1.3	255.255.255.252	/30	4(2)	fw-wireless comunication	
16	172.18.1.0	172.18.1.1	172.18.1.14	172.18.1.15	255.255.255.240	/28	16(14)	VLAN wireless guest	Internet ONLY
16	10.1.1.0/28	10.1.1.6	10.1.1.6	10.1.1.7	255.255.255.248	/29	8(6)	VLAN management	
4	172.16.1.0	172.16.1.2	172.16.1.2	172.16.1.3	255.255.255.252	/30	4(2)	router-fw communication	

Συγκεκριμένα, όσον αφορά την κατάτμηση του δικτύου (subnetting), αναφερόμαστε στα κύρια σημεία της πρότασής μας:

Το σημαντικότερο σημείο που πρέπει να αναφερθεί είναι ότι έχουμε διαμορφώσει έτσι το δίκτυο ώστε να έχουμε **διαφορετικές (τοπικές) IP διευθύνσεις ανά ζώνη** (όπως φαίνεται και στο σχήμα με τα αντίστοιχα χρώματα). Τονίζεται επίσης ότι ενώ για τα VLANs του **Εργαστηρίου,** των **Διακομιστών**, των **Εκτυπωτών** και το **wireless VLAN του Προσωπικού** χρησιμοποιούνται οι διευθύνσεις δικτύου 192.168.1.0/28, 192.168.2.0/29, 192.168.3.0/29, 192.168.4.0/28 για τη σύνδεση στο **wireless LAN των Επισκεπτών (guest)** η διεύθυνση δικτύου είναι 172.18.1.0/28 έτσι ώστε να εξασφαλίζεται ότι και στην περίπτωση που κάποιος κακόβουλος πελάτης θελήσει να αποκτήσει πρόσβαση στο εσωτερικό δίκτυο, η IP που εκείνος θα βλέπει θα είναι κάποια στο εύρος 172.18.1.2-13/28 και έτσι δεν θα μπορεί να "δει" τις υπόλοιπες διευθύνσεις που χρησιμοποιούνται στο εσωτερικό δίκτυο.

Άλλο ένα σημείο που θέλουμε να τονίσουμε είναι ότι χρησιμοποιούμε **κεραία για την ασύρματη σύνδεση με 2 Service Set Identifier (Ssid)**, τα οποία εξασφαλίζουν σύνδεση στο ασύρματο δίκτυο με συμμετοχή σε ένα από τα δύο διαφορετικά λογικά groups, **guest ή personnel**. Όσοι ανήκουν στο personnel μπορούν να έχουν πρόσβαση σε δεδομένα από τους servers, ενώ οι guests επικοινωνούν μόνο με τον Δρομολογητή.

Ένα επιπλέον σημείο που θα θέλαμε να τονίσουμε όσον αφορά τον Διακομιστή Ιστού (Web Server) είναι ότι ανοιχτές πόρτες (διπλής κατεύθυνσης) είναι μόνο οι εξής: 80 (HTTP), 443 (HTTPS). Από μέσα προς τα έξω (δηλ. μόνο στέλνουν αιτήματα) οι 25 (SMTP), 110 (POP3), ενώ από έξω προς τα μέσα (δηλ. μόνο ακούνε) οι , 587 (SMTP SSL/TLS), 993 (IMAP SSL/TLS), 995 (POP3 SSL/TLS) (αυτές οι πόρτες δίνουν πιστοποίηση και έπειτα η επικοινωνία γίνεται μέσω δυναμικών θυρών).

> (Αναλυτικότερα, επειδή θεωρούμε επισφαλή την μη-κρυπτογραφημένη λήψη e-mail, οι μόνες πόρτες που μπορούν να χρησιμοποιηθούν γι' αυτά είναι οι 587, 993, 995. Ωστόσο επειδή κάποιοι παλαιότεροι email servers μπορεί να χρησιμοποιούν κάποιες εκ των 25, 110 αφήνονται ανοικτές ως προς την αποστολή των emails σε αυτούς).

(Έχει γίνει παραδοχή πως ο web server λειτουργεί και σαν mail server και συγκεκριμένα για τα εσωτερικά mail χρησιμοποιούμε IMAP ενώ για τα εξωτερικά (των πελατών) χρησιμοποιούμε POP3 για να μην καταλαμβάνουν αδίκως χώρο στον server.)

Η διαχείριση του firewall επιτρέπεται μόνο από το management VLAN (πρόσβαση έχει μόνο ένας συγκεκριμένος υπολογιστής ο οποίος συνδέεται με θύρα ethernet απευθείας πάνω στο firewall (η οποία έχει χαρακτηριστεί management θύρα). Το ίδιο συμβαίνει και για τη διαχείριση του Switch.

4.8 Προστασία από ιομορφικό λογισμικό

Όσον αφορά την **μόλυνση από κακόβουλο λογισμικό μέσω συνημμένων στα email** του υπολογιστή του/της γραμματέα, **δεν κρίνεται σκόπιμο να προταθεί κάποιο επιπλέον μέτρο,** εφόσον ήδη υλοποιούνται αποτελεσματικά μέτρα (υφίσταται Antivirus που εντοπίζει και φιλτράρει πιθανώς μολυσματικά ή και επικίνδυνα email, ενώ και ο/η γραμματέας είναι ενήμερος/-η για το θέμα αυτό ώστε να κινείται προσεκτικά).

Όσον αφορά το λογισμικό που χρησιμοποιείται στον αιματολογικό αναλυτή (**SysmexXN - 1000**) παρατηρήθηκε ότι δεν είναι ενημερωμένο. Αυτό εντείνει τον κίνδυνο μόλυνσής του από κακόβουλο λογισμικό (malware) ή ιό (virus). Υπογραμμίζεται η ανάγκη για **τακτική ενημέρωσή του με τα τελευταία updates** ώστε ο κίνδυνος μόλυνσης να μετριαστεί. Ένα ακόμη μέτρο που προτείνουμε είναι η **εγκατάσταση και χρήση Antivirus στον αιματολογικό αναλυτή** εφόσον αυτός συνδέεται και στο δίκτυο.

4.9 Ασφαλής χρήση διαδικτυακών υπηρεσιών

Η ασφαλής χρήση του Ιστοτόπου (Website) θεωρείται καίριας σημασίας για την ομαλή λειτουργία του εργαστηρίου. Κατά την έρευνα μας παρατηρήθηκε ότι δεν υπάρχει SSL/TLS πιστοποιητικό (certificate) γεγονός που αφήνει τον Ιστότοπο ευπαθή σε επιθέσεις Man-in-the-middle (MITM), οδηγώνας σε διαρροή δεδομένων (εφόσον αυτά δεν είναι κρυπτογραφημένα) και έτσι σε GDPR πρόστιμο[18]. (Το JOOMLA δεν προσφέρει SSL/TLS certificate καθώς πρόκειται για ένα σύστημα διαχείρισης περιεχομένου (Content Management System - CMS) που εκτελείται σε Διακομιστή Ιστού (Web Server)). Για να αντιμετωπιστεί αυτό, κρίνεται απαραίτητη και επιτακτικής σημασίας **η εγκατάσταση SSL/TLS certificate** ώστε να κρυπτογραφείται η επικοινωνία μεταξύ του Ιστοτόπου και του προγράμματος περιήγησης του χρήστη, καθιστώντας έτσι δύσκολο για τους εισβολείς να υποκλέψουν και να τροποποιήσουν τα δεδομένα*. Επιπλέον, ο **Διακομιστής Ιστού** (Web Server) **μπορεί να ρυθμιστε**ί (configured) ώστε να **περιορίζει την πρόσβαση σε ευαίσθητα αρχεία και καταλόγους** και να αποτρέπει τη μη εξουσιοδοτημένη πρόσβαση στον ίδιο.

*Για την απόκτηση του πιστοποιητικού είναι απαραίτητη η διαμεσολάβηση μιας ανεξάρτητης αρχής πιστοποίησης (Certificate Authority-CA).

Όσον αφορά τον Διακομιστή Ιστού (Web Server) παρατηρήθηκε ότι πέρα από το λειτουργικό του σύστημα το οποίο είναι Windows Server 2008 R2 (το οποίο δεν υποστηρίζεται πλέον από τη Microsoft)[7] έχει και περιορισμένους πόρους σε CPU, memory, disk space. Έτσι, αν είναι οικονομικά εφικτό προτείνουμε την **ολική αντικατάσταση του Διακομιστή** με έναν νεότερο. Αν ωστόσο αυτό **δεν είναι προσιτό** για την επιχείρηση, υπάρχουν και άλλα μέτρα τα οποία προτείνουμε για να περιορίσουμε όσο το δυνατόν τους κινδύνους από DOS Attack . Αυτά περιλαμβάνουν την **αναβάθμιση των πόρων CPU, memory, disk space** όπως και την **αναβάθμιση του υπάρχοντος λειτουργικού συστήματος με ένα νεότερο** (προσοχή στις απαιτήσεις μεταξύ software και hardware για τη συμβατότητα). Άλλα μέτρα τα οποία μπορούν να ληφθούν για τον περιορισμό της απειλής είναι η επανεξέταση (review) του **κώδικα της εφαρμογής** ώστε να μειωθεί ο φόρτος του Διακομιστή. Αυτό επιτυγχάνεται με τη βελτιστοποίηση του κώδικα, τη συμπίεση αρχείων και την ελαχιστοποίηση του server-side scripting. Τέλος ένα επιπλέον μέτρο που μπορεί

να ληφθεί είναι το **rate-limiting**. Αυτό περιλαμβάνει μηχανισμούς για τον περιορισμό του αριθμού των αιτημάτων που μπορούν να υποβληθούν στον Διακομιστή ανά μονάδα χρόνου.

4.10 Ασφάλεια εξοπλισμού

Προκειμένου να επιτευχθεί η ασφάλεια του εξοπλισμού που βρίσκεται στον *Βοηθητικό χώρο* θεωρούμε απαραίτητη τη **μετεγκατάσταση των χημικών ουσιών** (που απαιτούνται για τα αντιδραστήρια του εργαστηρίου) και τα οποία φυλάσσονται σε αυτόν, στον χώρο όπου πραγματοποιούνται επί του πρακτέου τα αντιδραστήρια, δηλαδή **στον χώρο του *Εργαστηρίου - Παρασκευαστηρίου*.** Έτσι, μειώνουμε την πιθανότητα εμφάνισης κάποιας μη-ηθελημένης (ή και επιτηδευμένης) έκρηξης συσχετισμένης με τις εύφλεκτες χημικές ουσίες, και ταυτοχρόνως, μειώνουμε την ζημιά που θα υποστεί ο εξοπλισμός του *Βοηθητικού χώρου* καθώς μία τυχαία εμφάνιση φωτιάς δεν θα ενταθεί από τις εύφλεκτες χημικές ουσίες και έτσι το σύστημα πυρανίχνευσης θα δράσει εγκαίρως.

Για τον μετριασμό ή τον εκμηδενισμό των συνεπειών ενός πιθανού σεισμού προτείνουμε την αγορά **αντισεισμικών ραφιών** (seismic racks) που φιλοξενούν τους Διακομιστές και τους προφυλάσσουν από κραδασμούς και δονήσεις. Υπάρχουν μάλιστα μοντέλα κλειστά από όλες τις πλευρές με **κατάλληλο ανθεκτικό υλικό (σκληρυμένο γυαλί ή ανοξείδωτο ατσάλι)** που προφυλάσσουν εν μέρει τους Διακομιστές και από άλλους εξωγενείς παράγοντες όπως η **σκόνη** και η **υγρασία**. Στα θετικά στοιχεία προστίθεται και το **ενσωματωμένο σύστημα κλιματισμού (με ανεμιστήρες (fans))** για την διατήρηση της θερμοκρασίας των διακομιστών στα επίπεδα αποδοτικής λειτουργίας. Προτείνουμε συγκεκριμένα κάποιο εκ των *KB series server cabinets* [24], με την επιλογή να εξαρτάται από τις ακριβείς διαστάσεις των Διακομιστών. Τα προϊόντα της σειράς αυτής ενσωματώνουν όλα τα προαναφερθέντα* αλλά προσθέτουν και την **ύπαρξη φυσικής κλειδαριάς** για το άνοιγμα και κλείσιμο της πόρτας τους. Το γεγονός αυτό αποτελεί ένα ακόμη μέτρο ελέγχου πρόσβασης. Το φυσικό κλειδί μπορεί να παραμένει μόνο στον ιδιοκτήτη του εργαστηρίου ώστε να διασφαλίζεται ότι η πρόσβαση στους Διακομιστές θα διενεργείται κατόπιν γνώσης και φυσικής παρουσίας του.

*Σημειώνουμε ότι η σειρά που προτείνουμε περιλαμβάνει ροδάκια, τα οποία όμως είναι αποσπώμενα και μπορούν να αντικατασταθούν από αντισεισμικούς βραχίονες (seismic brackets) για την απειλή του σεισμού.

Πέραν αυτού, είναι σημαντική και η **τοποθέτηση συστήματος κλιματισμού** (A/C) στον *Βοηθητικό χώρο* προκειμένου να διατηρείται η **θερμοκρασία** του δωματίου στα **κατάλληλα όρια αποδοτικής λειτουργίας των Διακομιστών**. Έτσι, επιτυγχάνουμε τη μέγιστη δυνατή απόδοση των Διακομιστών, και ταυτοχρόνως τους προστατεύουμε από πρόκληση ζημιάς από τρίτους (δηλαδή βανδαλισμούς, κλοπές, κ.λπ.), απειλές οι οποίες αναφέρθηκαν και άνωθεν. Επιπροσθέτως, προστατεύονται και ο Μεταγωγέας όπως και το Τείχος προστασίας που βρίσκονται στον ίδιο χώρο (εάν τελικά αποφασιστεί να διατηρηθούν σε αυτόν).

Επιπλέον, για την διατήρηση της θερμοκρασίας στον *Βοηθητικό χώρο* προτείνουμε αρχικά την **εγκατάσταση ενός door bottom sealing strip** προκειμένου να μην είναι δυνατή η εισχώρηση της εξωτερικής θερμοκρασίας στο εσωτερικό του δωματίου. Επίσης, καθίσταται αναγκαία η **εγκατάσταση αφυγραντήρα** (προτείνεται ο *Frigidaire 50-Pint Dehumidifier* [25]) ούτως ώστε να διατηρούνται τα επίπεδα υγρασίας μεταξύ 40-60, εύρος το οποίο θεωρείται κατάλληλο για ηλεκτρονικές συσκευές. Διασφαλίζοντας την κατάλληλη θερμοκρασία και επίπεδα υγρασίας στο χώρο εξασφαλίζεται η μέγιστη δυνατή απόδοση των **Διακομιστών** καθώς και η εξάλειψη κινδύνων καταστροφής ή αποτυχίας τους λόγω φυσικών παραγόντων.

Επιπροσθέτως, κρίνεται αναγκαία η **σωστή συντήρηση** μέσω συχνών καθαρισμών τους. Συγκεκριμένα συστήνεται **κάθε 6 μήνες με 1 χρόνο να γίνεται ολικός καθαρισμός του κάθε Διακομιστή**, που αποτρέπει την συσσώρευση σκόνης, η οποία μπορεί να οδηγήσει σε υπερθέρμανση και καταστροφή τους. Ωστόσο, η διαδικασία αυτή απαιτεί εξειδικευμένο προσωπικό με κατάλληλα εργαλεία, το οποίο θα είναι ιδιαίτερα προσεκτικό να μην αγγίξει κανένα εσωτερικό μέρος των Διακομιστών. (Λόγω της φύσης του καθαρισμού ηλεκτρονικών συσκευών προτείνεται η εκ των προτέρων **γνωστοποίηση μέσω ανακοίνωσης στον ιστότοπο για την προγραμματισμένη μη-διαθεσιμότητα των ηλεκτρονικών υπηρεσιών** εφόσον προκειμένου να γίνει η συντήρησή τους χρειάζεται πρώτα η απενεργοποίησή τους).

Επιπλέον, έπειτα από την αξιολόγηση που διενεργήθηκε από τον επιθεωρητή κρίθηκε απαραίτητη **η απενεργοποίηση της γενικής παροχής του νερού στον *Βοηθητικό χώρο*.** (**Ιδανικά** προτείνεται η **αφαίρεση της βρύσης που βρίσκεται ακριβώς δίπλα από τους Διακομιστές**, διότι δεν προσδίδει καμία χρησιμότητα στον χώρο - ίσα ίσα, επιφορτίζει τους Διακομιστές με τον κίνδυνο βραχυκυκλώματος). Με αυτόν τον τρόπο αντιμετωπίζουμε την απειλή της διαρροής νερού στον χώρο και μειώνουμε την πιθανότητα πρόκλησης βλάβης στους Διακομιστές λόγω τυχαίων παραγόντων.

Συνεχίζοντας, ως προς τη φυσική ασφάλεια του εξοπλισμού του **Δρομολογητή** και του **Μεταγωγέα**, κρίνεται απαραίτητη η **μετεγκατάσταση τους πίσω από το γραφείο της γραμματέως** (τώρα, βρίσκονται δίπλα από το καθιστικό (καναπέ) της *Αίθουσας Αναμονής* και έτσι είναι αρκετά πιθανή η μη-ηθελημένη πρόκληση κάποιου ατυχήματος και κατά συνέπεια βλάβης στον Δρομολογητή ή/ και του Μεταγωγέα, διακυβεύοντας την ασφάλεια όλου του εσωτερικού δικτύου, αλλά και αυξάνοντας αρκετά το κόστος για μια πιθανή επαναγορά τους).

Τέλος, για την ανίχνευση και κατά συνέπεια έγκαιρη αντιμετώπιση πλημμύρας ή διαρροής νερού στον Βοηθητικό χώρο, προτείνουμε την **εγκατάσταση αισθητήρα πλημμύρας (flood sensor)** και συγκεκριμένα του μοντέλου *Zircon Leak Alert WiFi* [26] το οποίο έχει καλή αναλογία απόδοσης - κόστους και προσφέρει άμεση ενημέρωση σε όλες τις συσκευές που έχουν εγκαταστήσει τη σχετική εφαρμογή (*Zircon App*).

4.11 Φυσική ασφάλεια κτιριακής εγκατάστασης

Ο ***Βοηθητικός χώρος*** όπου φυλάσσονται οι Διακομιστές (Web Server, Database Server)- οι οποίοι όπως αναφέρθηκε στην ενότητα 3.3 είναι ευάλωτοι στις εξωτερικές συνθήκες (θερμοκρασία, σκόνη, πλημμύρα, υγρασία) - χρήζει ιδιαίτερης προσοχής. Αυτό περιλαμβάνει το **κλείσιμο της πόρτας** η οποία παραμένει ανοιχτή για τον εξαερισμό του χώρου,

Εν συνεχεία κρίνεται αρκετά σημαντική η ύπαρξη κάποιας προστασίας του εξωτερικού χώρου, είτε αυτό περιλαμβάνει την **περίφραξη του αύλειου χώρου**, είτε την πρόσληψη ενός **φρουρού (security) ο οποίος θα επιτηρεί την περίμετρο του Μικροβιολογικού Εργαστηρίου**. Έτσι εξασφαλίζεται ότι η πρόσβαση στον εσωτερικό χώρου του Εργαστηρίου θα είναι εφικτή μόνο από την κεντρική είσοδο, εκμηδενίζοντας σχεδόν την πιθανότητα μη-εξουσιοδοτημένης πρόσβασης στα μέρη του εργαστηρίου (και συνεπώς επέρχεται περιορισμός της πιθανότητας κλοπής σημαντικών δεδομένων όπως είναι το φυσικό αντίγραφο ασφαλείας (backup), ο φορητός υπολογιστής (laptop) του ιατρού, η μη εξουσιοδοτημένη φυσική πρόσβαση στους υπολογιστές και τον αιματολογικό αναλυτή του εργαστηρίου. Αυτό μειώνει σημαντικά και το κόστος από μία πιθανή νομική παράβαση, που χωρίς αυτά τα μέτρα θα ήταν αρκετά σημαντική). Εάν ωστόσο δεν είναι δυνατή (λόγω περιορισμένων οικονομικών πόρων της επιχείρησης) η υιοθέτηση κάποιων εκ των δύο μέτρων προστασίας, προτείνουμε την **επιβολή του κανόνα "Κλειστή και κλειδωμένη πόρτα"** όσο δεν βρίσκονται μέσα στο χώρο του Εργαστηρίου-Παρασκευαστηρίου και στο Γραφείο του Ιατρού εξουσιοδοτημένα πρόσωπα.

5 ΣΥΝΟΨΗ ΚΡΙΣΙΜΩΝ ΑΠΟΤΕΛΕΣΜΑΤΩΝ

Τα κρισιμότερα ευρήματα με την υψηλότερη επικινδυνότητα (High Risk) που εντοπίστηκαν κατά την FMEA ανάλυση, και άρα για τα οποία κρίνουμε ότι πρέπει να ληφθούν μέτρα με απόλυτη προτεραιότητα από τη Διοίκηση του Μικροβιολογικού Εργαστηρίου είναι τα εξής:

- **Ο Δρομολογητής (Router) είναι outdated προϊόν**[9]. Αυτό σημαίνει ότι δεν υπάρχουν πλέον patches και updates με συνέπεια γνωστές ευπάθειες να μην αντιμετωπίζονται οδηγώντας σε πολλών ειδών επικίνδυνες κυβερνοεπιθέσεις. Έτσι, η επιχείρηση φέρει ευθύνη για έκθεση ευαίσθητων δεδομένων (μη-συμμόρφωση με το GDPR), αλλά μπορεί να προκληθεί και δυσλειτουργία του εξοπλισμού και του δικτύου παρακωλύοντας τις λειτουργίες της επιχείρησης.
- **Ο Διακομιστής Ιστού (Web Server) είναι αρκετά παλιός και έχει περιορισμένους πόρους**, που μπορούν να εξαντληθούν από μία Denial-Of-Service (DOS) επίθεση, οδηγώντας σε πλήρη ανικανότητα του Διακομιστή να εξυπηρετήσει αιτήματα των χρηστών (ασθενών και προσωπικού) που αφορούν στον Ιστότοπο και τις υπηρεσίες e-mail. Αυτό παραβιάζει βασικές διαδικασίες της επιχείρησης.
  (Έχει γίνει η παραδοχή ότι ο Web Server λειτουργεί και ως Mail Server).
- **Ο ιστότοπος έχει δημιουργηθεί με παλιά έκδοση JOOMLA** που είναι αρκετά ευπαθής σε επιθέσεις (SQL injection, XSS attack), δεν χρησιμοποιεί ισχυρό μέσο αυθεντικοποίησης των χρηστών και δεν διαθέτει SSL/TLS πιστοποιητικό (δεν κρυπτογραφεί την επικοινωνία), οδηγώντας στην έκθεση ευαίσθητων δεδομένων των ασθενών ή/ και τροποποίηση – διαγραφή τους, και επιφέροντας κυρώσεις μη συμμόρφωσης με το GDPR.
- **Ο εκτυπωτής της γραμματέως δεν ελέγχει τη πρόσβαση σε αυτόν,** με αποτέλεσμα να είναι δυνατή η εκτέλεση αυθαίρετου κώδικα με σκοπό να υποκλαπούν τα δεδομένα του (ευαίσθητες πληροφορίες). Επίσης, **το firmware του εκτυπωτή του Ιατρού είναι παρωχημένο**. Παρότι η λήψη μέτρων που αφορούν στους εκτυπωτές δεν φαίνεται επιτακτική ανάγκη, αυτοί αποτελούν ένα από τα πιο **ανυποψίαστα τρωτά σημεία**.
- **Η αποστολή των αποτελεσμάτων των αιματολογικών εξετάσεων στους ασθενείς μέσω e-mail χωρίς τη χρήση κρυπτογράφησης** μπορεί να οδηγήσει στην υποκλοπή και κατά συνέπεια ανάγνωση κατά τη μετάδοσή του, απειλώντας την ασφάλεια και την ιδιωτικότητα των ασθενών με πιθανή έκθεση των προσωπικών δεδομένων.
- **Το Τείχος Προστασίας (Firewall) έχει κοινότυπα/ προκαθορισμένα διαπιστευτήρια σύνδεσης** οπότε δεν παρεμποδίζει σχεδόν μηδαμινά μια πιθανή προσπάθεια σύνδεσης στο εσωτερικό δίκτυο. Έτσι μπορούν να αλλαχθούν οι κανόνες του Τείχους κακόβουλα, και ενδεχομένως να εκτεθούν ευαίσθητες πληροφορίες ασθενών.
- **Οι Διακομιστές είναι ευαίσθητοι σε περιβαλλοντικές συνθήκες** και ταυτόχρονα αρκετά εκτεθειμένοι σε αυτές στον χώρο που βρίσκονται. Αυτό μπορεί μέχρι και να τους καταστρέψει επηρεάζοντας καίριες εργασίες και λειτουργίες της επιχείρησης
- **Το λογισμικό του αιματολογικού αναλυτή είναι παρωχημένο** που σημαίνει ότι δεν υπάρχουν πλέον patches και updates με συνέπεια γνωστές ευπάθειες να μην αντιμετωπίζονται οδηγώντας σε προσβολή από κακόβουλο λογισμικό και ιούς, με σκοπό την κλοπή ευαίσθητων προσωπικών δεδομένων των ασθενών και πρόκληση δυσλειτουργιών στο σύστημα.
- **Οι σταθμοί εργασίας που χρησιμοποιούν Windows 10 Pro δεν έχουν ενεργοποιημένο το BitLocker**, ένα καίριο στοιχείο που χρησιμοποιείται στην κρυπτογράφηση των δεδομένων του σκληρού δίσκου. Μία πιθανή διαρροή

δεδομένων θα φέρει την επιχείρηση αντιμέτωπη με ισχυρές νομικές συνέπειες (μη συμμόρφωση με το άρθρο 32 του GDPR [27]).

- **Το Τείχος προστασίας δεν καλύπτει όλους τους υπολογιστικούς πόρους** (παρά μόνο τον Database Server), αφήνοντάς τους **εκτεθειμένους σε πολλαπλούς κινδύνους** (έκθεση προσωπικών δεδομένων ασθενών, διακοπή λειτουργιών, λύτρα για την ανάκτηση των δεδομένων) διακυβεύοντας την ασφάλεια ολόκληρου του υπολογιστικού συστήματος.
- **Ο Διαμοιρασμός Προσωπικών Δεδομένων των ασθενών με συνεργαζόμενους παρόχους υπηρεσιών χωρίς την γραπτή συναίνεση** των εμπλεκόμενων ασθενών παραβιάζει το άρθρο (9)(2)(α) του GDPR [28] επιφέροντας αυστηρές κυρώσεις και πρόστιμο [18] σε μια ενδεχόμενη μήνυση.
- **Η τοποθεσία του Δρομολογητή και του Μεταγωγέα είναι επισφαλής σε ατυχήματα** που μπορούν να οδηγήσουν σε προβλήματα στο δίκτυο (διακοπή της σύνδεσης, αδυναμία επικοινωνίας ή και καταστροφή τους) και τελικά παρεμπόδιση των λειτουργιών της επιχείρησης.

6 ΑΝΑΦΟΡΕΣ

[1] : NVD - CVE-2017-2741 (nist.gov)
[2] : CVE-2017-2741 : A potential security vulnerability has been identified with HP PageWide Printers, HP OfficeJet Pro Printers, with firmwa (cvedetails.com)
[3]: Physical security for your servers | ISJ (internationalsecurityjournal.com)
[4]: Why Server Room Needs Environmental Monitoring? - AKCP Monitoring
[5]: 5 Factors to Consider for Data Center Environmental Monitoring | FS Community
[6]:Different Chemicals and Media used in a Microbiology Laboratory (yourarticlelibrary.com) (σελ. 8)
[7]: End of support for Windows Server 2008 and Windows Server 2008 R2 | Microsoft Learn
[8]: Windows Server 2016 - Microsoft Lifecycle | Microsoft Learn
[9]: End-of-Sale and End-of-Life Announcement for the Select Cisco 881, 886, and 887 Integrated Services Routers - Cisco
[10]: What is SPI firewall | NordVPN
[11]: CWE - CWE-284: Improper Access Control (4.11) (mitre.org)
[12]: [20200306] - Core - SQL injection in Featured Articles menu parameters (joomla.org)
[13]: [20180602] - Core - XSS vulnerability in language switcher module (joomla.org)
[14]: Windows 7 End of Life: everything you need to know about the death of Windows 7 | TechRadar
[15]: Windows 7 support ended on January 14, 2020 - Microsoft Support
[16]: Έλεγχος ταυτότητας - Κέντρο ασφαλείας Google (safety.google)
[17]: Art. 9 GDPR – Processing of special categories of personal data - General Data Protection Regulation (GDPR) (gdpr-info.eu)
[18]: Fines / Penalties - General Data Protection Regulation (GDPR) (gdpr-info.eu)
[19]: NIST SP 800-111, Guide to Storage Encryption Technologies for End User Devices
[20]: https://eur-lex.europa.eu/eli/reg/2016/679/oj
[21]: What are the pros and cons of cloud backup? | TechTarget
[22]: D-link Dgs-1210-24 Network Switch Managed L2 Gigabit Ethernet (10/100/1000) Black 1u | Public
[23]: Cisco RV340, RV345, RV345P, and RV340W Dual WAN Security Router Data Sheet - Cisco
[24]: Server Rack and Cabinet – Lepin Network
[25]: Amazon.com - Frigidaire 50 Pint Dehumidifier, White –
[26]: Leak Alert™ WiFi Setup – Zircon Corporation
[27]: Art. 32 GDPR – Security of processing - General Data Protection Regulation (GDPR) (gdpr-info.eu)
[28]: Art. 9 GDPR – Processing of special categories of personal data - General Data Protection Regulation (GDPR) (gdpr-info.eu)

7 ΒΙΒΛΙΟΓΡΑΦΙΑ

Insight into a Microbiology Lab - YouTube
Behind the scenes: What happens to a blood sample? - YouTube
ΑΙΜΟΛΗΨΙΑ ΚΑΙ ΜΕΤΑΦΟΡΑ ΔΕΙΓΜΑΤΩΝ ΣΤΟ ΕΡΓΑΣΤΗΡΙΟ (venizeleio.gr)

Common Mistakes and Best Practices for Designing Network Security Zones - YouTube
Data Center Segmentation Best Practices - YouTube
Network Architecture Review - YouTube

Recital 35 - Health Data - General Data Protection Regulation (GDPR) (gdpr-info.eu)
Separation of duties — AccountingTools

SQL Injection | OWASP Foundation
What is SQL Injection? Tutorial & Examples | Web Security Academy (portswigger.net)
Cross Site Scripting (XSS) | OWASP Foundation
Exfiltration - Firewalls.com
What is DLP (Data Loss Prevention)? | Fortinet
Microsoft Windows 7 : List of security vulnerabilities (cvedetails.com)
Windows 10 most critical vulnerabilities in 2022 | CalCom (calcomsoftware.com)