
**ΤΜΗΜΑ ΠΛΗΡΟΦΟΡΙΚΗΣ**

# ΑΣΦΑΛΕΙΑ ΠΛΗΡΟΦΟΡΙΑΚΩΝ ΣΥΣΤΗΜΑΤΩΝ
## ΕΡΓΑΣΙΑ ΕΑΡΙΝΟΥ ΕΞΑΜΗΝΟΥ 2023

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

## ΠΑΡΟΥΣΙΑΣΗ ΣΧΕΔΙΟΥ ΑΣΦΑΛΕΙΑΣ
**(BioPlasma Labs)**

**ΜΕΛΗ ΟΜΑΔΑΣ ΕΡΓΑΣΙΑΣ:**

***ΝΙΚΟΛΑΣ ΚΟΥΝΤΟΥΡΙΩΤΗΣ 3170195***
***ΚΩΝΣΤΑΝΤΙΝΟΣ ΜΑΡΚΟ 3190112***
***ΔΕΣΠΟΙΝΑ ΠΑΠΑΔΟΠΟΥΛΟΥ 3180146***

**ΠΕΡΙΕΧΟΜΕΝΑ ΕΡΓΑΣΙΑΣ**

# 1. ΕΙΣΑΓΩΓΗ

Η ομάδα μας καλείται να μελετήσει και να αξιολογήσει το παρόν Πληροφοριακό Σύστημα ενός Μικροβιολογικού εργαστηρίου . Η διαδικασία αυτή θα γίνει βήμα προς βήμα και θα εντοπίσει όλα τα πιθανά λάθη που έγιναν στην υλοποίηση και στα θεμέλια του παρόντος συστήματος . Αφού βρεθούν θα εκτιμηθούν ως προς τον βαθμό επικινδυνότητας τους και με σκοπο να δημιουργηθούν ή να τροποποιηθουν ήδη υπάρχοντες μηχανισμοί για την αποτροπή ή τον εντοπισμό αυτών των λαθών .

## 1.1 Περιγραφή Εργασίας

Η εκπόνηση του σχεδίου μέτρου Ασφαλείας για το μικροβιολογικό εργαστήριο , λαμβάνει ως υπόψη την σύντομη περιγραφή του Εργαστηρίου που δόθηκε από εμπειρογνώμων , την κάτοψη του κτιρίου και την τοπολογία του δικτύου . Εκτός από αυτά τα στοιχεία για την διεξαγωγή του σχεδίου μας μας δόθηκε και λίστα με αγαθά του εργαστηρίου , καθώς και τρείς ευπάθειες .

Με βάση αυτά , η ομάδα μας καλείτε να παρουσιάσει ένα σχέδιο μέτρων ασφαλείας για το συγκεκριμένο εργαστήριο , όπου θα εφαρμόζει πολιτικές για την ασφάλεια και την προστασία των δεδομένων και πληροφοριών από απώλεια , κακόβουλη χρήση , μεταβολή ή καταστροφή .

- **Δομή Παραδοτέου :**

Στο συγκεκριμένο σχέδιο ασφάλειας ξεκινάμε με τον Πρόλογο μας και την Εισαγωγή , αναλύοντας σε πρώτη φάση το πως είναι σχηματισμένο το σχέδιο ασφάλειας και τη μεθοδολογία που θα χρησιμοποιήσουμε . Θα καταχωρήσουμε σε ενότητες και σε φάσεις την έρευνα μας όπως τις εξής :

- Σε αυτό το έγγραφο βρίσκονται λεπτομερώς τα πάντα για την έρευνα μας, στην οποία μπορείτε να συμβουλευτείτε την μεθοδολογία μελέτης ασφάλειας παρακάτω για να δείτε πως θα διεξαχθεί το συγκεκριμένο σχέδιο ασφάλειας.

- Με το έγγραφο αυτό θα παραδοθεί και το ανάλογο φύλλο Excel το οποίο περιέχει μέσα το **FMEA Calculation Table ,** το οποίο χρησιμοποιούμε για να καθορίσουμε τα ζεύγη ευπαθειών / απειλών και την αξιολόγηση τους .

# 2. ΜΕΘΟΔΟΛΟΓΙΑ ΜΕΛΕΤΗΣ ΑΣΦΑΛΕΙΑΣ

Για τη Διαχείριση Επικινδυνότητας του Μικροβιολογικού Εργαστηρίου χρησιμοποιήθηκε παραμετροποιημένη μέθοδος του **ISO 27001 K[0]** . Επιλέχθηκε η συγκεκριμένη μέθοδος γιατι αποτελεί ένα από τα πολλά παγκόσμια πρότυπα ασφάλειας . Στα πλαίσια διεξαγωγής αυτής της μελέτης ασφάλειας θα :

1. Προσδιοριστούν και θα εκτιμηθούν τα αγαθά του πληροφοριακού συστήματος και των εγκαταστάσεων του .

2. Εξεταστεί για κάθε αγαθό και για κάθε υπηρεσία ποιές είναι οι ευπάθειες του . Αφού βρεθούν οι ευπαθειες του , θα εξεταστούν οι απειλές που αφορούν το κάθε αγαθό ή υπηρεσία .

3. Εντοπιστούν οι απειλές για κάθε αγαθό θα υπολογιστεί η επικινδυνότητα του αντίκτυπου της συγκεκριμένης απειλής , για κάθε απειλή . Αυτό θα γίνει μέσω του Impact Chart που μας δίνεται μέσω του ISO27K FMEA[1] Risk Assessment .

4. Βρεθούν ποιές είναι οι ενέργειες οι οποίες θα μπορούσαν να προκαλέσουν απειλή , και μέσω του Probability Chart του ISO27K θα καθοριστεί η πιθανότητα να γίνει το συγκεκριμένο συμβάν , για κάθε συμβάν .

5. Εξεταστούν ποιοί είναι οι μηχανισμοί ελέγχου ή εντόπισης για την αποτροπή ή τον εντοπισμό της κάθε ευπάθειας του κάθε αγαθού .

6. Εκτιμηθεί ο βαθμός RPN ( Risk Priority Number ) , ο οποίος αποτελεί πολλαπλασιασμό των τριών προηγούμενων παραγόντων . Δηλαδή Impact x Likelihood x Vulnerability .

7. Κατατάσσουμε σε HIGH RISK & Low Risk τους συνδυασμούς απειλής/ευπάθειας που προκύπτουν και αναλύονται βασικά μέτρα ασφάλειας για τους συγκεκριμένους συνδυασμούς.

8. Γίνει σύνοψη των κρίσιμων αποτελεσμάτων.

Ξεκινάμε με identification & valuation of assets στο πρώτο στάδιο , με το πρώτο στάδιο . Αφού γίνει η σωστή καταγραφή των αγαθών θα γίνει στο δεύτερο με

έκτο στάδιο το risk analysis και θα καταλήξουμε στα ανάλογα μέτρα αντιμετώπισης , δηλαδή risk management , στα στάδια επτά με οκτώ .

## 2.1 Περιγραφή Υποδομών & Πληροφοριακού Συστήματος

**Το Εργαστήριο-Παρασκευαστήριο αποτελείται από έναν αιματολογικό αναλυτή ο οποίος χρησιμοποιείται για την διεξαγωγή των αποτελεσμάτων από τις αιματολογικές εξετάσεις του κάθε ασθενή, χημικές ουσίες που βοηθούν στη διαδικασία της επεξεργασίας των αιματολογικών δειγμάτων και 2 υπολογιστές desktop -οι οποίοι είναι εξοπλισμένοι με το λογισμικό των Windows 10 Pro-. Επίσης σε αυτο το χώρο γίνεται η αυτοματοποιημένη καταχώρηση αποτελεσμάτων δειγματοληψίας με χρήση barcode.**

**Στην αίθουσα αναμονής βρίσκονται άλλος ένας desktop υπολογιστής, ένας εκτυπωτής , ένα route , ένα switch καθώς και το αρχείο υπαλλήλων και προμηθευτών μέσα στην ανοιχτή βιβλιοθήκη . Στον βοηθητικό χώρο έχουμε τον web server που τρέχει σε "JOOMLA" ένας database server που έχει τα δεδομένα υπαλλήλων και εργαζομένων, ενας switch και το firewall. Στο γραφείο του γιατρου υπάρχει ακόμα ένας desktop υπολογιστής, ο προσωπικός υπολογιστής του γιατρού και το φυσικό αρχείο ασθενών στην ερμαριο. Αξίζει να σημειωθεί ότι αυτός είναι ο χώρος που αποθηκεύονται τα αντίγραφα ασφαλείας κάθε βδομάδα. Τέλος, στο χώρο λήψης δειγμάτων βρίσκεται ο τελευταίος desktop υπολογιστής του κέντρου.**

**Οι desktop υπολογιστές είναι εφοδιασμένοι με Windows 10 Pro και τα switches με Windows 7 Pro.**

## 2.2 Εξοπλισμός & Υλισμικό ( hardware )

**A-001 Αιματολογικος Αναλυτης (XS-1000i)**
**A-002 Υπολογιστης Desktop (HP Pro G2 MT)**
**A-003 Υπολογιστης Desktop (HP Pro G2 MT)**
**A-004 Υπολογιστης Desktop (HP Pro G2 MT)**
**A-005 Υπολογιστης Desktop (HP Pro G2 MT)**
**A-006 Υπολογιστης Desktop (HP Pro G2 MT)**
**A-007 Εκτυπωτης (HP OfficeJet Pro Printer)**
**A-008 Εκτυπωτης (HP OfficeJet Pro Printer)**
**A-015 Apple MacBook Air**
**A-023 Χημικές Ουσίες**

## 2.3 Λογισμικό και εφαρμογές

**A-018 Λειτουργικο Συστημα (Windows 7)**
**A-019 Λειτουργικο Συστημα (Windows 10 Pro)**
**A-20 Web Development Platform (JOOMLA)**

## 2.4 Δίκτυο

**A-009 Web Server**
**A-010 Database Server**
**A-011 Switch (TP-LINK TL-SG1005D)**
**A-012 Switch (TP-LINK TL-SG1005D)**
**A-013 Router (Cisco C886VA-K9)**
**A-014 Firewall (Fortinet-Fortigate-400D)**

## 2.5 Δεδομένα

**A-016 Δεδομενα Πελατη**
**A-017 Δεδομενα Εργαζομενων**
**A-021 Φυσικο Αρχειο Ασθενων**
**A-022 Αρχειο Υπαλληλων & Προμηθευτων**

## 2.6 Διαδικασίες

**A-024 Αυτόματη Καταχώρηση Αποτελεσμάτων Δειγματοληψίας**
**A-025 Δημιουργια Αντιγραφων Ασφαλειας (καθε Εβδομαδα)**

# 3. ΑΠΟΤΙΜΗΣΗ ΑΓΑΘΩΝ ΤΗΣ ΕΓΚΑΤΑΣΤΑΣΗΣ

Στην ενοτητα αυτη θα αναφερθούν τα αγαθα που εντοπίστηκαν να έχουν ευπαθειες , οι απειλες απο τα οποια ειναι ευαλωτα να στοχοποιηθουν καθως και τα αποτελεσματα απο την αποτιμηση της επικινδυνοτητας

## 3.1 Αγαθά που εντοπίστηκαν

**A-001 Αιματολογικος Αναλυτης**

**A-002-006 Workstations**
**A-007 Printer (old firmware below 1708D)**
**A-008 Printer (HP printer Firmware)**
**A-009 Web Server**
**A-010 Database Server**
**A-011-012 Switch**
**A-013 Router**
**A-014 Firewall**
**A-015 Laptop Γιατρου**
**A-016 Customer Data**
**A-017 Employee Data**
**A-018 Windows 7 Pro**
**A-019 Windows 10 Pro**
**A-020 Joomla Website**
**A-021 Φυσικο Αρχειο Ασθενων**
**A-022 Αρχειο Υπαλληλων & Προμηθευτων**

Επιπρόσθετα Αγαθά που κρίθηκαν σημαντικά από την ομάδα μας :
**A-023 Χημικες Ουσιες**

Οι χημικές ουσίες με τις οποίες πολλοί εργαζόμενοι έχουν αλληλεπίδραση , έχουν σημαντικές επιπτώσεις αν δεν διαχειριστούν σωστά ή δεν υπάρχουν αυστηρά μέσα προστασίας . Η λάθος διαχείριση αυτού του πόρου μπορεί να προκαλέσει ζημιά στην υπηρεσία , στο υπόθεμα αλλά να έχει και κρίσιμη επίπτωση στην υγεία εργαζομένων και πελατών που βρίσκονται στο χώρο ή και στο πολυκατάστημα .

**A-024 Αυτοματη Καταχωρηση Αποτελεσματων Δειγματοληψιας**

Η διαδικασία αυτή κρίθηκε σημαντική αφού οι πληροφορίες και τα δεδομένα ανταλλάσσονται μέσω διαδικτύου και έτσι υπάρχει ο κίνδυνος να κλαπεί το σήμα και να αποκαλυφθούν αποτελέσματα εξετάσεων και σημαντικές προσωπικές πληροφορίες των πελατών .

**A-025 Δημιουργια Αντιγραφων Ασφαλειας**

Η δεύτερη διαδικασία που είναι επίσης σημαντική για την λειτουργία του εργαστηρίου είναι η δημιουργία αντιγράφων ασφαλείας . Είναι άκρως σημαντική καθώς αφορά τα δεδομένα και τις πληροφορίες που χειρίζεται το μικροβιολογικό εργαστήριο . Τα αντίγραφα αντιγράφονται σε φυσική μορφή , η οποία είναι ευάλωτη σε διάφορες απειλές .

## 3.2 Απειλες που εντοπίστηκαν

**Threat 1 (A-014 - FireWall ) :** Αφορά την πιθανή ανεπιθύμητη διαρροή των προσωπικών δεδομένων του Εργαστηρίου .

**Threat 2 (A-014 - FireWall ) :** Αφορά την πιθανή ενός DDOS επίθεση που θα οδηγήσει στην κατάρρευση του website.

**Threat 3 (A-017 - Employee Data ) :** Αφορά την πιθανή πρόσβαση των προσωπικών δεδομένων από εξωτερικό παράγοντα του Εργαστηρίου .

**Threat 4 (A-017 - Employee Data ) :** Αφορά την πιθανή επίθεση Man-in-the-Middle Attack κατά την διακίνηση τους.

**Threat 5 (A-022 - Αρχείο Υπαλλήλων & Προμηθευτών ) :** Αφορά τη πιθανή κλοπή των αρχείων από κακόβουλο πελάτη .

**Threat 6 (A-001 Αιματολογικος Αναλυτης (XS-1000i) ) :** Αφορά τη πιθανή αποτυχία διεξαγωγής σωστών αποτελεσμάτων.

**Threat 7 (A-001 Αιματολογικος Αναλυτης (XS-1000i) ) :** Αφορά τη πιθανή κλοπή του αναλυτή από κακόβουλο δράστη.

**Threat 8 (A-002 PCWS001 (Workstation) ) :** Αφορά τη πιθανή κακόβουλη δραστηριότητα των εργαζομένων.

**Threat 9 (A-002 PCWS001 (Workstation) ) :** Αφορά το πιθανό install ενός ιού σε μορφή οδηγού από έναν κακόβουλο δράστη.

**Threat 10 (A-007 Εκτυπωτης (HP OfficeJet Pro Printer)) :** Αφορά τη πιθανότητα να συμβεί ένα print spooler [7].

**Threat 11 (A-007 Εκτυπωτης (HP OfficeJet Pro Printer)) :** Αφορά τη πιθανότητα απόκτηση μη εξουσιοδοτημένης πρόσβασης με επιθετικές μεθόδους.

**Threat 12 (A-008 Εκτυπωτης (HP OfficeJet Pro Printer)) :** Ένας κακόβουλος δράστης μπορεί να χρησιμοποιεί στενογραφία για να ενσωματώσει κακόβουλο κώδικα σε ένα bitmap μιας εικόνας jpg . [15]

**Threat 13 (A-008 Εκτυπωτης (HP OfficeJet Pro Printer)) :** Ένας κακόβουλος δράστης μπορεί να πραγματοποιήσει επίθεση Ransomware εκμεταλλευόμενος δεδομένα που χρησιμοποιούνται από εκτυπωτή .

**Threat 14 (A-009 Web Server ) :** Ένας κακόβουλος δράστης μπορεί να πραγματοποιήσει επίθεση SYN Flood .

**Threat 15 (A-009 Web Server ) :** Ένας κακόβουλος δράστης βαλει malware. [3]

**Threat 16 (A-009 Web Server ) :** Η δυνατότητα να σκανάρουν τα ports του server για να μάθουν τις ευπάθειες του .

**Threat 17 (A-010 Database Server ) :** Ο κακόβουλος δράστης μπορεί να εισβάλει στο σύστημα με επιθετικό τρόπο.

**Threat 18 (A-010 Database Server ) :** Ο κακόβουλος δράστης μπορεί να λάβει προηγμένα προνόμια.

**Threat 19 (A-010 Database Server ) :**Ένας κακόβουλος δράστης μπορεί να πραγματοποιήσει επίθεση Social Engineering.

**Threat 20 (A-011 Switch (TP-LINK TL-SG1005D) ) :**Ένας κακόβουλος δράστης μπορεί να εκτελέση επίθεση MAC Overflow. [4]

**Threat 21 (A-011 Switch (TP-LINK TL-SG1005D) ) :**Ένας κακόβουλος δράστης μπορεί να εκτελέσει επίθεση ARP Spoofing.

**Threat 22 (A-012 Switch (TP-LINK TL-SG1005D) ) :**Ένας κακόβουλος δράστης μπορεί να ενσωματώσει ένα Rootkit.

**Threat 23 (A-013 Router (Cisco C886VA-K9) ) :** Ένας κακόβουλος δράστης μπορεί να πραγματοποιήσει επίθεση Ping Flood

**Threat 24 (A-013 Router (Cisco C886VA-K9) ) :** Ένας κακόβουλος δράστης μπορεί να πραγματοποιήσει επίθεση Dns Hijack. [11]

**Threat 25 (A-015 Apple MacBook Air ) :** Η πιθανότητα να γίνει διαρροή ευαίσθητων δεδομένων .

**Threat 26 (A-015 Apple MacBook Air ) :** Η πιθανότητα να μολυνθεί το δημόσιο Wi-Fi .

**Threat 27 (A-016 Δεδομενα Πελατη) :** Ένας κακόβουλος δράστης μπορεί να έχει πρόσβαση στα δεδομένα .

**Threat 28 (A-016 Δεδομενα Πελατη) :**Αφορά την πιθανή επίθεση Man-in-the-Middle Attack κατά την διακίνηση τους.

**Threat 29 (A-018 Λειτουργικο Συστημα (Windows 7)) :**Ένας κακόβουλος δράστης μπορεί να πραγματοποιήσει επίθεση Dictionary attacks.

**Threat 30 (A-018 Λειτουργικο Συστημα (Windows 7)) :**Ένας κακόβουλος δράστης μπορεί να πραγματοποιήσει επίθεση Buffer Overflow .

**Threat 31 (A-019 Λειτουργικο Συστημα (Windows 10 Pro)) :**Αφορά το πιθανό install ενός ιού από έναν κακόβουλο δράστη.

**Threat 32 (A-019 Λειτουργικο Συστημα (Windows 10 Pro)) :**Ο κακόβουλος δράστης μπορεί να έχει πρόσβαση στο σύστημα.

**Threat 33 (A-20 Web Development Platform (JOOMLA)) :** Μπορεί να δεχτεί επίθεση SQL Injection. [14]

**Threat 34 (A-20 Web Development Platform (JOOMLA)) :**Ένας κακόβουλος δράστης μπορεί να πραγματοποιήσει επίθεση Buffer Overflow .[14]

**Threat 35 (A-20 Web Development Platform (JOOMLA)) :**Ένας κακόβουλος δράστης μπορεί να πραγματοποιήσει επίθεση XSS[6] για την υποκλοπή λογαριασμών πελατών. [14]

**Threat 36 (A-021 Φυσικο Αρχειο Ασθενων) :**Ένας κακόβουλος δράστης μπορεί να πραγματοποιήσει επίθεση Social Engineering.

**Threat 37 (A-021 Φυσικο Αρχειο Ασθενων) :**Η πιθανότητα καταστροφής τους από φυσικά αίτια.

**Threat 38 (A-022 Αρχειο Υπαλληλων & Προμηθευτων) :** Η πιθανότητα κάποιας φυσικής καταστροφής (π χ σεισμος , πλημμύρα etc)

**Threat 39 (A-023 Χημικες Ουσιες ) :** Οι χημικες ουσιες έχουν αξία για το λόγο αυτό μπορεί να κλαπούν για κακόβουλους υπαλλήλους ή πελάτες

**Threat 40 (A-023 Χημικες Ουσιες ) :** Ο μη σωστός αερισμός (μπορεί να καταστρέψει τις χημικές ιδιότητες των ουσιών)

**Threat 41 (A-024 Αυτοματη Καταχωρηση Αποτελεσματων Δειγματοληψιας):** Κακοβουλος δράστης "παρακολουθεί" το δίκτυο και τις ευαίσθητες πληροφορίες που λαμβάνουν χώρα με το σκανάρισμα των προϊόντων και των αποτελεσμάτων

**Threat 42 (A-024 Αυτοματη Καταχωρηση Αποτελεσματων Δειγματοληψιας):**
Αποτυχία Firmware των Scanners

**Threat 43 (A-025 Δημιουργια Αντιγραφων Ασφαλειας):**Social Engineering attack

**Threat 44 (A-025 Δημιουργια Αντιγραφων Ασφαλειας):**Η πιθανότητα κάποιας φυσικής καταστροφής (π χ σεισμος , πλημμύρα etc)

## 3.3 Ευπάθειες που εντοπίστηκαν

**Vulnerability 1 : Firewall rules δεν έχουν εγκατασταθεί σωστα**
**[αφορά το Firewall ]**

**Vulnerability 2 – Ξεπερασμένη Τεχνολογία software στο Firewall**
**[αφορά το Firewall]**

**Vulnerability 3 – Μη κρυπτογραφημένα δεδομένα**
**[αφορά α)Employee Data**
**β)Customer Data]**

**Vulnerability 4 – Μη ασφαλές δίκτυο μετάδοσης**
**[αφορά τα a)Employee Data που μεταφέρονται συνεχόμενα από τον database server**
**b)Customer Data**

**c)Αυτόματη Καταχώρηση Αποτελεσμάτων Δειγματοληψίας]**

**Vulnerability 5 – Τα αρχεια βρίσκονται σε ευκολα προσβάσιμη βιβλιοθήκη χωρίς λουκέτα**
**[αφορά α)τα αρχεία Υπαλλήλων και Προμηθευτών**
**β)Φυσικό Αρχείο Ασθενών]**

**Vulnerability 6 – Μη εξειδικευμένο προσωπικό να έχει πρόσβαση σε αιματολογικό αναλυτή**
**[αφορά τον Αιματολογικό Αναλυτή]**

**Vulnerability 7 – Εργαστήριο που η πόρτα παραμένει ανοιχτή ενώ η κεντρική πόρτα οδηγεί σε κεντρικό δρόμο**
**[αφορά α) Αιματολογικό αναλυτή**
**β) Χημικές ουσίες**
**γ) Workstation ]**

**Vulnerability 8 – Unsecured Remote Access σε workstation**
**[αφορά α) Workstation ] [8]**

**Vulnerability 9 – Η μη ενεργοποίηση του Print Spooler**
**[αφορά τον Εκτυπωτή με firmware παλαιότερο του 1708D ]**

**Vulnerability 10 – Firmware Εκτυπωτη παλαιότερο του 1708D**
**[αφορά τον Εκτυπωτή με firmware παλαιότερο του 1708D ]**

**Vulnerability 11 – Built-in memory δεν εχει ασφαλείς μηχανισμούς**
**[αφορά α) εκτυπωτή με HP firmware**
**β)Αυτόματη Καταχωρηση Αποτελεσματων Δειγματοληψιας]**
**Vulnerability 12 – Μη χρησιμοποίηση RST-SYN cookies**
**[αφορά Web server]**

**Vulnerability 13 – Μη ύπαρξη firewall ανάμεσα σε switch και webserver**
**[αφορά Web server]**

**Vulnerability 14 – Ports που δε χρησιμοποιούνται παραμένουν ανοιχτά**
**[αφορά Web server]**

**Vulnerability 15 – Μη χρησιμοποίηση ισχυρών passwords**

**[αφορά α)Database server**
**β)Laptop**
**γ)Windows 7 pro] [2]**

**Vulnerability 16 – Είσοδος για server room βρίσκεται σε κεντρική είσοδο**
**[αφορά α)Web server**
**β)Database server**
**γ)Firewall**
**δ)Switch]**

**Vulnerability 17 – Δεν ρυθμίζονται σωστά οι πίνακες του switch MAC [9]**
**[αφορά to Switch]**

**Vulnerability 18 – Μη χρησιμοποίηση static ARP**
**[αφορά το Switch]**

**Vulnerability 19 – Μη σωστή ρύθμιση των φίλτρων του router**
**[αφορά Router]**

**Vulnerability 20 – DNS misconfiguration**
**[αφορά Router]**

**Vulnerability 21 – Συνδεσιμότητα συσκευών σε Public wifis**
**[αφορά α)Laptop**
**β)Workstation]**

**Vulnerability 22 – Μη επιδιορθωμένα τρωτά σημεία λογισμικού**
**[αφορά τα Windows 7 pro]**

**Vulnerability 23 – Μη χρησιμοποίηση antivirus**
**[αφορά τα a)Windows 7 pro**
**b)Windows 10 pro]**

**Vulnerability 24 – Χρήση μονο administrator account**
**[αφορά τα a)Windows 7 pro**
**b)Windows 10 pro]**

**Vulnerability 25 – Ιστοσελίδα μην εχει σωστή ρύθμιση SQL**
**[αφορά Website]**

**Vulnerability 26 – Ιστοσελίδα δεν έχει κατασκευαστεί από επαγγελματία**
**[αφορά Website]**

**Vulnerability 27 – Third party App Exposure**
**[αφορά Website]**

**Vulnerability 28 –Αρχεία τοποθετημένα σε υπόγειο (όπου είναι ευάλωτα σε φυσική καταστροφή)**
**[αφορά α)Φυσικό Αρχείο Ασθενών**
**β)Αρχείο Υπαλλήλων & Προμηθευτών**
**γ)Δημιουργία Αντιγράφων Ασφαλείας ]**

**Vulnerability 29 – Μη ύπαρξη συστήματος Εξαερισμού**
**[αφορά Χημικές Ουσίες)]**

**Vulnerability 30 – Αντίγραφο ασφαλείας βρίσκεται απροστάτευτο στη βιβλιοθήκη του γιατρού**
**[αφορά Δημιουργία Αντιγράφων Ασφαλείας ]**

## 3.4 Αποτελέσματα αποτίμησης

Με βάση τα αγαθά και τις ανάλογες ευπάθειες για κάθε αγαθό , χρησιμοποιήσαμε τη μέθοδο **FMEA** για να κάνουμε ένα ολοκληρωμένο **Risk Assessment** . Το κρίσιμο κριτήριο αξιολόγησης για αυτή τη μέθοδο είναι το **RPN ( = Risk Priority Number )** . Ακολουθήσαμε τη συγκεκριμένη μεθοδολογία για τη διεξαγωγή του σχεδίου μας .

Για την εύρεση του RPN εντοπίσαμε πρώτα για κάθε αγαθό τις πιο κρίσιμες ευπάθειες . Αφού βρίσκονται πλέον καταγεγραμμένες οι ευπάθειες , μετά από ανάλυση και συζήτηση για το πως μπορεί να υπάρξει απειλή που θα εκμεταλλευτεί τη συγκεκριμένη ευπάθεια , την αξιολογήσαμε ως προς το **Impact ( business or service )** που μπορεί να έχει η συγκεκριμένη απειλή . Αξιολογούμε το **Impact** με βάση το **Impact Chart (1 - 10)** που δίνεται μαζί με τα FMEA Guidelines .

Αφού καθοριστεί το μέγεθος της ζημιάς που μπορεί να υποστεί η επιχείρηση ή η υπηρεσία , στο επόμενο στάδιο πρέπει να αναγνωρίσουμε το λόγο που έγινε η συγκεκριμένη ζημιά . Για κάθε ευπάθεια βρήκαμε πως υπάρχει τουλάχιστον μία **απειλή** η οποία μπορεί να φέρει σημαντικές επιπτώσεις στην επιχείρηση του μικροβιολογικού εργαστηρίου . Χρησιμοποιώντας τον βοηθητικό πίνακα **Probability**

**Chart (1 - 10)** στα **FMEA Guidelines ,** καθορίζουμε τη συχνότητα με την οποία μπορούν να συμβούν αυτές οι απειλές .

Γίνεται περαιτέρω ανάλυση , για κάθε αγαθό , ως προς την **Εμπιστευτικότητα , Ακεραιότητα και Διαθεσιμότητα του κάθε αγαθού .** Για την βαθμολόγηση αυτών των τριών παραγόντων χρησιμοποιήθηκε ένας άξονας Low-Medium-High .

Αφού γίνει η σωστή αξιολόγηση όλων αυτών των προηγούμενων παραγόντων , προχωράμε στο να αναλύσουμε ποιοι τρόποι αντιμετώπισης είναι αποτελεσματικότεροι . Υπάρχουν δύο κύριοι τρόποι , **της πρόληψης και της ανίχνευσης [5].**

**Θεωρώντας πως τα μέτρα πρόληψης και ανίχνευσης είναι υλοποιημένα ,** προχωράμε αξιολογώντας την ευπάθεια για το συγκεκριμένο αγαθό . Χρησιμοποιώντας τον πίνακα **Vulnerability** κρίνουμε από το **1-10** την συγκεκριμένη ευπάθεια και τις επιπλοκές της στην επιχείρηση .

Ο αριθμός **RPN** υπολογίζεται πολλαπλασιάζοντας τα τρία βασικά κριτήρια **Impact , Likelihood & Vulnerability .** Η μέγιστη τιμή που μπορεί να λάβει η τιμή αυτή είναι 1000 ( 10 * 10 * 10) . **Στο συγκεκριμένο σχέδιο ασφάλειας θα ασχοληθούμε με τις 10% πιο κρίσιμες ευπάθειες .** Δηλαδή όσοι συνδυασμοί Ευπάθειας/Απειλής για κάθε αγαθό έχουν RPN > 100 ( το 10% του μέγιστου αριθμού RPN ) θα βαθμολογηθούν ως **HIGH RISK** και θα αντιμετωπιστούν ανάλογα .

**Ο πίνακας αυτός θα αναπαριστά τις τιμές του FMEA Calculation ως εξής , για κάθε συνδυασμό απειλής / ευπάθειας :**

| Confidentiality | Integrity | Availability | Impact Rank | Likelihood | Vuln. Rank | RPN |
|---|---|---|---|---|---|---|
| | | | | | | |

## HIGH RISK THREATS (RPN >= 100)

**Threat 9 (A-002 PCWS001 (Workstation) ) :**

Αν προστεθεί ο μηχανισμός του να κλειδώνεται η πόρτα , πάλι υπάρχει ο κίνδυνος να παραβιαστεί και να προσβληθεί ολόκληρο το σύστημα .

| | | | | | | |
|---|---|---|---|---|---|---|
| High | High | Low | **8** | **7** | **6** | **336** |

**Threat 1 (A-014 FireWall ) :**

Αν γίνει σωστή απαγόρευση κίνησης μπορεί να περιοριστεί η πιθανότητα προσβολής , αλλά ο κίνδυνος παραμένει σχετικά υψηλός .

| | | | | | | |
|---|---|---|---|---|---|---|
| High | High | Low | **9** | **5** | **5** | **225** |

**Threat 6 (A-001 Αιματολογικος Αναλυτης (XS-1000i) ) :**

Παρόλο που αν επιτευχθεί η σωστή εκπαίδευση του προσωπικού , υπάρχει ο κίνδυνος να γίνει μοιραίο λάθος και να επηρεαστούν τα αποτελέσματα .

| | | | | | | |
|---|---|---|---|---|---|---|
| Medium | High | High | **5** | **10** | **4** | **200** |

**Threat 7 (A-001 Αιματολογικος Αναλυτης (XS-1000i) ) :**

Αν προστεθεί κλειστό κύκλωμα καμερών ασφαλείας θα μπορεί να εντοπιστεί το πρόβλημα σε συνδυασμό με συναγερμό που θα ενεργοποιείται με τη κλοπή της συσκευής . αλλά δεν μπορεί να αποτραπεί εξ'ολοκλήρου .

| | | | | | | |
|---|---|---|---|---|---|---|
| High | High | High | **7** | **4** | **7** | **196** |

**Threat 15 (A-009 Web Server ) :**

Ακόμα και αν προστεθεί δεύτερο Firewall , υπάρχει ο κίνδυνος προσβολής του συστήματος και πρέπει να υπάρχει περαιτέρω προσοχή .

| | | | | | | |
|---|---|---|---|---|---|---|
| High | High | Low | **8** | **8** | **3** | **192** |

**Threat 32 (A-019 Λειτουργικο Συστημα (Windows 10 Pro)) :**

Πρέπει να περιοριστεί η χρήση των υπολογιστικών πόρων από ειδικούς και μόνο . Παρόλο που είναι ένας καλός τρόπος επίλυσης του προβλήματος , υπάρχει ακόμα ο μικρός κίνδυνος ενός Insider Attack.

| | | | | | | |
|---|---|---|---|---|---|---|
| High | High | Low | **9** | **7** | **3** | **189** |

**Threat 3 (A-017 - Employee Data ) :**

Ακόμα και αν προστεθούν κανόνες και κωδικοί ασφαλείας , τα αρχεία αυτά είναι σε αρκετά προσβάσιμη θέση από πολλούς υπαλλήλους και έτσι ο κίνδυνος ενός Insider Attack υπάρχει σε μεγάλο βαθμό .

| | | | | | | |
|---|---|---|---|---|---|---|
| High | Low | Low | **7** | **4** | **6** | **168** |

**Threat 43 (A-025 Δημιουργια Αντιγραφων Ασφαλειας):**

Η διαδικασία αυτή έχει ως αποτρεπτικό μηχανισμό το κλείδωμα τον αντιγράφων ασφαλείας για να μην είναι προσβάσιμος από όλους , αλλά ακόμα υπάρχει ο κίνδυνος ενός Insider Attack .

| | | | | | | |
|---|---|---|---|---|---|---|
| High | High | Low | **8** | **7** | **3** | **168** |

**Threat 19 (A-010 Database Server ) :**

Ακόμα και αν υπάρχει προσωπικό Security το οποίο φυλάσσει το αγαθό δεν σημαίνει πως εξαφανίζεται η απειλή .

| | | | | | | |
|---|---|---|---|---|---|---|
| High | High | Low | **8** | **4** | **5** | **160** |

**Threat 35 (A-20 Web Development Platform (JOOMLA)) :**

Το ρίσκο που συνοδεύεται μαζί με τη χρήση ενός μιας εφαρμογής που φτιάχτηκε από τρίτη οντότητα , επηρεάζει την εμπιστευτικότητα σε κρίσιμο βαθμό . Ο μηχανισμός που προτείνουμε είναι να δημιουργηθεί ιστοσελίδα από επαγγελματίες χωρίς την χρήση τρίτων εφαρμογών .

| | | | | | | |
|---|---|---|---|---|---|---|
| High | Medium | Low | **8** | **4** | **5** | **160** |

**Threat 31 (A-019 Λειτουργικο Συστημα (Windows 10 Pro)) :**

Με τη προσθήκη antivirus και να γίνονται συστηματικοί έλεγχοι στα αρχεία του υπολογιστή τότε περιορίζεται ως κάποιο σημείο η απειλή .

| | | | | | | |
|---|---|---|---|---|---|---|
| High | High | Medium | **9** | **5** | **3** | **135** |

**Threat 36 (A-021 Φυσικο Αρχειο Ασθενων) :**

Με την πρόσθεση του μηχανισμού να φυλάσσονται τα αρχεία και να υπάρχει πρόσβαση σε μερικούς χρήστες , και την πρόσθεση κυκλού συστήματος καμερών ασφαλείας περιορίζεται σημαντικά η απειλή , αλλά συνεχίζει και υπάρχει ο κίνδυνος .

| | | | | | | |
|---|---|---|---|---|---|---|
| High | High | Low | **8** | **8** | **2** | **128** |

**Threat 40 (A-023 Χημικες Ουσιες ) :**

Αν προστεθεί σύστημα εξαερισμού για να μπορεί να κλείνει η πόρτα και να προστεθούν ανάλογοι συναγερμοί για τα προϊόντα θα μειωθεί η επικινδυνότητα αυτής της απειλής δραστικά .

| | | | | | | |
|---|---|---|---|---|---|---|
| Low | Low | Medium | **7** | **8** | **2** | **112** |

**Threat 23 (A-013 Router (Cisco C886VA-K9) ) :**

Με την χρήση ενός Firewall για τον εντοπισμό της κίνησης και το router να χειρίζεται τη κίνηση όπως προβλέπεται , μειώνεται δραστικά η πιθανότητα εμφάνισης της απειλής .

| | | | | | | |
|---|---|---|---|---|---|---|
| Low | Low | High | **9** | **4** | **3** | **108** |

**Threat 37 (A-021 Φυσικο Αρχειο Ασθενων) :**

Με την φύλαξη των φυσικών αρχείων σε ένα vault επιτυγχάνουμε την εξασφάλιση της ακεραιότητας των αρχείων αλλά πάλι υπάρχει ο κίνδυνος να κλαπούν .

| | | | | | | |
|---|---|---|---|---|---|---|
| Low | Medium | High | **9** | **4** | **3** | **108** |

**Threat 38 (A-022 Αρχειο Υπαλληλων & Προμηθευτων) :**

Αν προστεθεί μηχανισμός για την προφύλαξη των αρχείων ο οποίος προφυλάσσει τα δεδομένα σε stainless steel vault , τότε επιτυγχάνεται η προστασία των αρχείων αλλά ακόμα υπάρχει ο κίνδυνος να κλαπούν.

| | | | | | | |
|---|---|---|---|---|---|---|
| Low | Medium | High | **9** | **4** | **3** | **108** |

**Threat 42 (A-024 Αυτοματη Καταχωρηση Αποτελεσματων Δειγματοληψιας):**

Με μια δεύτερη ειδική ομάδα να επιτηρεί το δίκτυο και να γίνονται συχνοί έλεγχοι του δικτύου θα περιοριστούν σε σημαντικό βαθμό οι απειλές , αλλά όχι να εξαφανιστούν .

| | | | | | | |
|---|---|---|---|---|---|---|
| High | High | Low | **9** | **4** | **3** | **108** |

**Threat 29 (A-018 Λειτουργικο Συστημα (Windows 7)) :**

Δεν είναι αρκετή η χρήση δυνατών κωδικών για μέτρο ασφάλειας για το συγκεκριμένο αγαθό , μιας και τα dictionary attacks είναι πιο εξειδικευμένο εργαλείο για συγκεκριμένους χρήστες , με τη σωστή γνώση ένας κακόβουλος ηθοποιός μπορεί να προκαλέσει ζημιά στο σύστημα ή να αποκαλύψει πληροφορίες .

| | | | | | | |
|---|---|---|---|---|---|---|
| High | High | Low | **7** | **5** | **3** | **105** |

## LOWER RISK THREATS (RPN < 100)

**Threat 17 (A-010 Database Server ) :**

Γι Αυτή την ευπάθεια ο μηχανισμός που προσθέσαμε εξολοθρεύει την απειλή , γιατι ενα απλό brute force attack χρειάζεται πολυωνυμικό χρόνο για να καταφέρει να βρει ένα περίπλοκο κωδικό .

| | | | | | | |
|---|---|---|---|---|---|---|
| High | High | Low | **7** | **7** | **2** | **98** |

**Threat 4 (A-017 - Employee Data ) :**

Με τη χρήση encryption καταφέρνουμε να κάνουμε καλύτερο safeguard του αγαθού και έτσι να μην αποτελεί HIGH RISK THREAT .

| | | | | | | |
|---|---|---|---|---|---|---|
| High | Low | Low | **8** | **3** | **4** | **96** |

**Threat 33 (A-20 Web Development Platform (JOOMLA)) :**

Αν προσλάβουμε ένα επαγγελματία να δημιουργήσει την ιστοσελίδα με τη σωστή σύνδεση του backend με front-end , περιορίζεται σημαντικά η απειλή ενός SQL injection .

| | | | | | | |
|---|---|---|---|---|---|---|
| High | High | Medium | **8** | **6** | **2** | **96** |

**Threat 5 (A-022 - Αρχείο Υπαλλήλων & Προμηθευτών ) :**

Αν εκπαιδευτεί το προσωπικό που βρίσκεται κοντά στο γραφείο να απαγορεύει την είσοδο και να ελέγχει τη κίνηση του γραφείου τότε μειώνεται σημαντικά η επικινδυνότητα της απειλής.

| | | | | | | |
|---|---|---|---|---|---|---|
| Medium | High | Medium | **6** | **5** | **3** | **90** |

**Threat 25 (A-015 Apple MacBook Air ) :**

Με τη χρήση του encryption επιτυγχάνουμε τη μείωση της επικινδυνότητας της απειλής να κλαπούν αρχεία .

| | | | | | | |
|---|---|---|---|---|---|---|
| High | High | Low | **9** | **5** | **2** | **90** |

**Threat 41 (A-024 Αυτοματη Καταχωρηση Αποτελεσματων Δειγματοληψιας):**

Η χρήση ενός end-to-end encryption αλγόριθμου , θα περιορίσει σημαντικά την κλοπή ή την επιτήρηση της επικοινωνίας μέσω του διαδικτύου.

| | | | | | | |
|---|---|---|---|---|---|---|
| High | Low | Low | **9** | **5** | **2** | **90** |

**Threat 8 (A-002 PCWS001 (Workstation) ) :**

Αν χρησιμοποιείται two factor authentication για την remote πρόσβαση και υπάρχει firewall για τη διαχείριση εισερχόμενης κίνησης τότε ο παράγοντας επικινδυνότητας της ευπάθειας μειώνεται δραστικά .

| | | | | | | |
|---|---|---|---|---|---|---|
| High | High | Low | **7** | **6** | **2** | **84** |

**Threat 24 (A-013 Router (Cisco C886VA-K9) ) :**

Οι μηχανισμοί προσθήκης επιπρόσθετου Firewall και εντοπισμού , dns query , περιορίζουν σε σημαντικό βαθμό την απειλή .

| | | | | | | |
|---|---|---|---|---|---|---|
| High | Medium | High | **9** | **4** | **2** | **72** |

**Threat 39 (A-023 Χημικες Ουσιες ) :**

Αν κλειδώνεται η πόρτα και εγκατασταθεί ένα κλειστό σύστημα ασφαλείας καμερών τότε μειώνεται δραστικά το Vuln. Rating.

| | | | | | | |
|---|---|---|---|---|---|---|
| High | Medium | Medium | **8** | **3** | **3** | **72** |

**Threat 44 (A-025 Δημιουργια Αντιγραφων Ασφαλειας):**

Αν γίνεται η δημιουργία αντιγράφων και σε ψηφιακή μορφή , τότε μειώνεται το ρίσκο να καταστραφούν τα δεδομένα γιατι υπάρχουν σε διαφορετικές μορφές .

| | | | | | | |
|---|---|---|---|---|---|---|
| Low | Medium | Medium | **9** | **4** | **2** | **72** |

**Threat 27 (A-016 Δεδομενα Πελατη) :**

Για την διατήρηση της ακεραιότητας και της εμπιστευτικότητας των δεδομένων , χρησιμοποιείται ειδικός αλγόριθμος κρυπτογραφίας για να προστατευτούν οι πληροφορίες και τα δεδομένα . Έτσι δεν αποτελεί σημαντική απειλή πλέον για τα δεδομένα .

| | | | | | | |
|---|---|---|---|---|---|---|
| High | High | Low | **7** | **5** | **2** | **70** |

**Threat 18 (A-010 Database Server ) :**

Αν υπάρχει συνεχή ανανέωση του λογισμικού του Server , τότε το ρίσκο εμφάνισης της απειλής μειώνεται δραστικά , μαζί με τη βαθμολογία ευπάθειας .

| | | | | | | |
|---|---|---|---|---|---|---|
| High | High | Low | **8** | **4** | **2** | **64** |

**Threat 30 (A-018 Λειτουργικο Συστημα (Windows 7)) :**

Αν το λογισμικό ανανεωθεί και γίνονται συχνοί έλεγχοι , τότε μειώνεται η ζημιά και η περίπτωση προσβολής αλλά όχι κατα σημαντικό βαθμό .

| | | | | | | |
|---|---|---|---|---|---|---|
| High | Medium | Low | **8** | **4** | **2** | **64** |

**Threat 26 (A-015 Apple MacBook Air ) :**

Η γνώση οτι η συνδεση σε δημοσια wifi ειναι επικινδυνη ειναι αρκετη για να μειωσει κατα πολυ τον κινδυνο .

| | | | | | | |
|---|---|---|---|---|---|---|
| High | Low | Low | **8** | **4** | **2** | **64** |

**Threat 22 (A-012 Switch (TP-LINK TL-SG1005D) ) :**

Αν κλειδώνεται η πόρτα στο βοηθητικό χώρο και υπάρχει συνεχής έλεγχος στα πίσω μέρη του μηχανήματος και γενικά στο hardware , τότε μειώνεται η σημαντικότητα της απειλής .

| | | | | | | |
|---|---|---|---|---|---|---|
| High | High | Low | **5** | **3** | **4** | **60** |

**Threat 12 (A-008 Εκτυπωτης (HP OfficeJet Pro Printer)) :**

Αν υλοποιηθούν τα ανάλογα μέτρα για τη σωστή διαχείριση της μνήμης του εκτυπωτή , τότε μειώνεται δραστικά η επικινδυνότητα της απειλής .

| | | | | | | |
|---|---|---|---|---|---|---|
| High | Low | Low | **9** | **3** | **2** | **54** |

**Threat 34 (A-20 Web Development Platform (JOOMLA)) :**

Με τη πρόσληψη επαγγελματιών για τη σχεδίαση της ιστοσελίδας , μειώνονται τα ρίσκα σημαντικά . Αν παράλληλα με τη νέα ιστοσελίδα γίνεται συστηματικά Fuzz Testing , τότε επιτυγχάνουμε ένα υψηλό μέσο προστασίας για τα δεδομένα μας .

| | | | | | | |
|---|---|---|---|---|---|---|
| High | High | Medium | **9** | **3** | **2** | **54** |

**Threat 14 (A-009 Web Server ) :**

Με τη χρήση αρκετών μηχανισμών reverse cache-poisoning και συνεχή επίβλεψη των logs του δικτύου θα εξολοθρευτεί η απειλή .

| | | | | | | |
|---|---|---|---|---|---|---|
| Low | Low | High | **9** | **4** | **1** | **36** |

**Threat 2 (A-014 - FireWall ) :**

Με τη συστηματική ανανέωση του Firewall και την υλοποίηση αλγορίθμων μηχανικής μάθησης οι οποίοι είναι ικανοί να ξεχωρίσουν malicious traffic , η συχνότητα εμφάνισης της ευπάθειας πέφτει δραστικά .

| | | | | | | |
|---|---|---|---|---|---|---|
| Low | Low | High | **8** | **2** | **2** | **32** |

**Threat 21 (A-011 Switch (TP-LINK TL-SG1005D) ) :**

Με τη χρήση Static ARP και το συστηματικό έλεγχο της Arp Cache η περίπτωση εμφάνισης της ευπάθειας εκμηδενίζεται .

| | | | | | | |
|---|---|---|---|---|---|---|
| High | Low | Low | **5** | **6** | **1** | **30** |

**Threat 13 (A-008 Εκτυπωτης (HP OfficeJet Pro Printer)) :**

Με την τακτική ανανέωση του λογισμικού του Firewall θα επιτεύξουμε την δραστική μείωση της πιθανότητας εμφάνισης αυτής της ευπάθειας .

| | | | | | | |
|---|---|---|---|---|---|---|
| High | Low | Low | **7** | **2** | **2** | **28** |

**Threat 28 (A-016 Δεδομενα Πελατη) :**

Αν γίνει σωστή υλοποίηση ενός μηχανισμού encryption για τα δεδομένα των πελατών , τότε η πιθανότητα να προσβληθεί η ακεραιότητα και η εμπιστευτικότητα τους μηδενίζεται .

| | | | | | | |
|---|---|---|---|---|---|---|
| High | Low | Low | **7** | **3** | **1** | **21** |

**Threat 16 (A-009 Web Server ) :**

Αν κλείσουν όλα τα αχρείαστα ports και προστεθούν οι ανάλογοι εργαζόμενοι να επιτηρούν το δίκτυο τότε η απειλή μηδενίζεται .

| | | | | | | |
|---|---|---|---|---|---|---|
| Low | Low | Low | **4** | **5** | **1** | **20** |

**Threat 11 (A-007 Εκτυπωτης (HP OfficeJet Pro Printer)) :**

Με την αλλαγή του εκτυπωτή με ένα πιο πρόσφατο μοντέλο της HP , η πιθανότητα εμφάνισης της απειλής μηδενίζεται .

| | | | | | | |
|---|---|---|---|---|---|---|
| High | Low | Low | **8** | **2** | **1** | **16** |

**Threat 20 (A-011 Switch (TP-LINK TL-SG1005D) ) :**

Αν γίνει ο σωστός μηχανισμός στο switch για το configuration των MAC Tables , τότε η απειλή εξολοθρεύεται .

| | | | | | | |
|---|---|---|---|---|---|---|
| Low | Medium | High | **5** | **3** | **2** | **15** |

**Threat 10 (A-007 Εκτυπωτης (HP OfficeJet Pro Printer)) :**

Απενεργοποιώντας την επιλογή του Windows Spooler , η απειλή παύει να υπάρχει .

| | | | | | | |
|---|---|---|---|---|---|---|
| High | High | Medium | **6** | **2** | **1** | **12** |

# 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 - Προστασίας Διαδικασιών Προσωπικού

-Το προσωπικό δε θα πρέπει να χρησιμοποιεί στους υπολογιστές του administrator privileges αλλά απλούς Users με όσο το δυνατόν λιγότερο privileges και μόνο όταν είναι ανάγκη να συνδέονται στον administrator.

-Στο προσωπικό θα πρέπει να γίνεται κατάλληλη εκπαίδευση για κακοβουλους πελατες που εισέρχονται στο κέντρο και τι θα πρέπει να προσέχουν.

-Το προσωπικό δε θα πρέπει να πατάει σε συνδέσμους που δεν έχουν πιστοποιηθεί.

-Το προσωπικό να κλείνει με λουκέτο κάθε φορά τις πόρτες εργαστηρίου και του δωματίου των server.

-Να γίνεται συχνή ενημέρωση για πιθανούς κινδύνους που αφορούν τα αγαθά της επιχείρησης .

-Το προσωπικό είναι το πιο σημαντικό μέρος της επιχείρησης αφού σε αυτούς εμπιστευόμαστε όλα τα αγαθά της επιχείρησης , γι ‘ αυτό φέρουν ευθύνη και οι εργοδότες που δεν κατάφεραν να διακρίνουν από πιο πριν τη ποιότητα και τον χαρακτήρα του εργαζομένου.

## 4.2 Ταυτοποίηση και αυθεντικοποίηση

-Η είσοδος στο εργαστήριο να γίνεται με εισαγωγή ΔΥΝΑΤΟΥ κωδικού.

-BioMetrics τα οποία είναι μοναδικά για τον κάθε πελάτη / χρήστη ( π χ. υλοποίηση ενός fingerprint scanner ) .

-Two Factor Authentication για οποιαδήποτε πρόσβαση στο σύστημα.

## 4.3 Έλεγχος προσπέλασης και χρήσης πόρων

-Ο αιματολογικός αναλυτής θα πρέπει να εξοπλιστεί με gps tracker και alarm σε περίπτωση που κλαπεί από κακόβουλο χρήστη .

-Η χρήση των υπολογιστικών πόρων να γίνεται monitored [13] από ειδική cybersecurity ομάδα .

-FireWall να επιτηρεί προβλεπόμενα την εισερχόμενη κίνηση του δικτύου .

## 4.4 Διαχείριση εμπιστευτικών δεδομένων

-Τα δεδομένα και αποτελέσματα των ασθενών θα πρέπει να έχουν υπογράψει συμφωνητικό που δίνει τα δικαιώματα στην BioPlasma Labs να μπορεί να δώσει τα δεδομένα τους σε τρίτους.

-Φυσικά δεδομένα τοποθετούνται σε ασφαλή μέρος που γνωρίζει μόνο το προσωπικο.

-Hashing Data Using encryption algorithms (SHA-256)

## 4.5 Προστασία από τη χρήση υπηρεσιών από τρίτους

-Χρήση προτύπων κανόνων δημιουργίας κωδικών

-Δημιουργία ιστοσελίδας με εργαλεία που δεν εμπλέκουν τρίτες οντότητες η εφαρμογές από τρίτους.
-Δωματια ανοιγουν με keycards

## 4.6 Προστασία Λογισμικού

-Συνεχής ενημέρωση Λογισμικού υπολογιστής και λειτουργικών συστημάτων ώστε να κάνουν τα κατάλληλα security updates.

-Upgrade firmware printer και scanner ανά 2 χρόνια και εξάμηνος έλεγχος τους
-Επικύρωση και απολύμανση όλων των εισροών χρήστη για την αποφυγή κοινών επιθέσεων όπως δέσμες ενεργειών μεταξύ τοποθεσιών (XSS) και ένεση SQL

## 4.7 Διαχείριση ασφάλειας δικτύου

-Monitoring του δικτύου μέσω IPS και IDS

-Κλείσιμο των ports που δεν χρησιμοποιούνται ή που δεν περιμένουν σύντομα κάποια σύνδεση

-Μόνο οι αναγκαίες συσκευές να είναι στο ίδιο LAN με τους υπολογιστές , τα switches , routers και το firewall. Άλλες συσκευές και IOT να είναι σε διαφορετικό δίκτυο ώστε να αποφευχθεί η διείσδυση απ τη μια συσκευή στην άλλη. Αυτό θα μπορούσε να γίνει με χρήση 2 routers οπου συσκευές, όπως το λαπτοπ και ο printer, είναι συνδεδεμένες στον 2ο router.

-Χρήση δεύτερου firewall πριν τη σύνδεση του router με τον web server

-Χρηση router που εχει hardware-based firewall protection

## 4.8 Προστασία από ιομορφικό λογισμικό

-Σύγχρονο antivirus εγκατεστημένο στους workstations .

-Endpoint Protection anti-malware.

-Email & Web filters

-Σωστή ενημέρωση προσωπικού για να προστατεύονται από phishing scams.

-Συνεχής έλεγχος των υπολογιστών και των υποδομών της επιχείρησης για την αποφυγή εγκατάστασης malware σε φυσική μορφή .

## 4.9 Ασφαλής χρήση διαδικτυακών υπηρεσιών

-Πελάτες θα πρέπει να προσέχουν όταν συνδέονται στην ιστοσελίδα ότι ο σύνδεσμος της ιστοσελίδας δεν είναι άλλο άπο το bioplasmalabs.com οτιδήποτε άλλο είναι μέρος κάποιου phishing attack .

-Χρηση διαφορετικων κωδικων απο αλλους λογαριασμους που εχει ηδη ο χρήστης στο site.

-Ενημέρωση προσωπικού για την προσοχή από τα κοντινά δημόσια WiFi που μπορεί να είναι μολυσμένα.

## 4.10 Ασφάλεια εξοπλισμού

-Οι χημικές ουσίες θα πρέπει να αποθηκεύονται πίσω στον χώρο αποθήκευσης τους αφού χρησιμοποιηθουν.

-Ο αιματολογικός αναλυτής πρέπει να καθαρίζεται προσεκτικά απ’τον εφημερεύοντα αναλυτη πριν το τέλος της βάρδιας του και να περνάει από συντήρηση μετά από το χρονικό διάστημα που προτείνει ο παρασκευαστής του.

-Οι ηλεκτρονικοί υπολογιστές που βρίσκονται στο χώρο μαζί με τους εκτυπωτές , τα switches το router πρέπει να επιφυλάσσονται από το προσωπικό και να επιτηρείται από κλειστό κύκλωμα καμερών ασφαλείας .

## 4.11 Φυσική ασφάλεια κτιριακής εγκατάστασης

-Αύλειος χώρος να περιφρακτεί για την αποφυγή εισόδου μη εξουσιοδοτημένων ατόμων στο Εργαστήριο-Παρασκευαστήριο.

-Η βοηθητική είσοδος στο βοηθητικό χώρο όπου βρίσκονται οι servers να εξοπλιστεί με κλειδαριά και πόρτα ασφαλείας για την αποφυγή φυσικής κακόβουλης διείσδυσης στο δίκτυο.

-Τζαμια και πορτες με δυνατη μονωση εναντια του νερου σε περιπτωση πλημμυρας

# 5. ΣΥΝΟΨΗ ΚΡΙΣΙΜΩΝ ΑΠΟΤΕΛΕΣΜΑΤΩΝ

Συνοψίζοντας όλα τα προηγούμενα που έχουμε αναλύσει στο σχέδιο , να αναφέρουμε και πως για την αντιμετώπιση αυτών των κρίσιμων προβλημάτων απαιτείται η συνεχής έρευνα και ασχολία . Τα θέματα ασφάλειας συνήθως παραβλέπονται λόγω κόστους , ενώ στη πραγματικότητα το κέρδος που αποκτάς με την ασφάλεια ως επίκεντρο είναι και εξασφαλισμένο και διατηρήσιμο . **“Security must pay , not cost” ,** είναι η φράση που θα πρέπει να έχουν οι υπεύθυνοι του εργαστηρίου συνεχίζοντας με την υλοποίηση των παρακάτω μέτρων για την εξασφάλιση της ακεραιότητας , της διαθεσιμότητας και της εμπιστευτικότητας .

**HIGH RISK THREATS ( RPN > 100 ) , in descending order :**

**Threat 9 (PCWS001 (Workstation) ) :** **RPN : 336**

Η απειλη των Insider Attacks ή των κακόβουλων actors μπορεί να προκαλέσει τεράστια ζημιά στην υλική και στη τεχνική υποδομή του εργαστηρίου , είναι μία από τις σημαντικότερες απειλές που πρέπει να αποκλειστούν . Καλείται η διεύθυνση του εργαστηρίου να διοργανώσει ειδικά σεμινάρια εκπαίδευσης του προσωπικού για να αποφευχθεί εντελώς το πρόβλημα . Αποτέλεσμα , έχει η προστασία και η επίβλεψη των αγαθών από το προσωπικό για τη συνεχή και αναμενόμενη λειτουργία τους .

**Threat 1 (A-014 - FireWall ) :** **RPN : 225**

Η εισερχόμενη κίνηση πρέπει συνεχώς να επιβλέπεται και να ελέγχεται , αφού η πρόσβαση μπορεί να γίνει από οποιοδήποτε actor . Πρέπει το σύστημα να είναι σε ετοιμότητα να διαχειριστεί την κακόβουλη εισερχόμενη κίνηση για να αποφευχθεί η επίθεση DDoS , η οποία βλάπτει τη διαθεσιμότητα των δεδομένων σε μεγάλο βαθμό . Για την επίλυση αυτού του προβλήματος προτείνουμε να υπάρχουν μηχανισμοί οι οποίοι να μπλοκάρουν την εισερχόμενη κακόβουλη κίνηση , ή να επιτρέπουν μόνο εισερχόμενη κίνηση από whitelisted addresses .

**Threat 6 (A-001 Αιματολογικος Αναλυτης (XS-1000i) ) :** **RPN : 200**

Ο αιματολογικός αναλυτής είναι ο ακρογωνιαίος λίθος της επιχείρησης . Για την διαχείριση του πρέπει να υπάρχει προσωπικό το οποίο να είναι άρτια εκπαιδευμένο για την εκπόνηση αναλύσεων . Αν δεν γίνει όπως πρέπει , τότε υπάρχει ο σοβαρός κίνδυνος τα δεδομένα που παράγονται να είναι αλλοιωμένα ή και λανθασμένα . Αυτό το σφάλμα επιφέρει τεράστιες επιπτώσεις για θέματα υγείας . Καλείται η διοίκηση να εκπαιδεύει το προσωπικό , μέσω επαγγελματιών , για την ολόσωστη χρήση του αναλυτή .

**Threat 7 (A-001 Αιματολογικος Αναλυτης (XS-1000i) ) :** **RPN : 196**

Όπως αναφέραμε και παραπάνω , ο αιματολογικός αναλυτής πρέπει να είναι σε ασφαλής τοποθεσία και υπό σωστή διαχείριση . Αν κάποιος κακόβουλος actor αποφασίσει να το κλέψει , τότε η επιχείρηση θα υποστεί τεράστια ζημιά . Γι Αυτό καλείται η επιχείρηση να λάβει τα σωστά μέτρα όπως : εγκατάσταση κλειστού κυκλώματος ασφαλείας καμερών για την επιτήρηση του αγαθού μαζί με GPS Tracker πάνω στη συσκευή σε περίπτωση που χαθεί . Στη περίπτωση που ο μηχανισμός δεν είναι αρκετός να μπορεί να βρεθεί το μηχάνημα μετά από τη κλοπή του .

**Threat 15 (A-009 Web Server ) :** **RPN : 192**

Η προστασία του διακοσμητή θεωρείται εξίσου σημαντική με τα δεδομένα που έχουμε , γιατι μέσω της ιστοσελίδας ένας κακόβουλος actor μπορεί να προσπελάσει τα security permissions , αν δεν υπάρχουν τα σωστά firewall configurations και να βλάψει την ακεραιότητα και την εμπιστευτικότητα των αγαθών αυτών . Η εγκατάσταση ενός δεύτερου FireWall πριν τη σύνδεση στον Web Server για την επιπρόσθετη διαχείριση κίνησης περιορίζει σημαντικά την απειλή .

**Threat 32 (A-019 Λειτουργικο Συστημα (Windows 10 Pro)) :** **RPN : 189**

Ένα σημαντικό κομμάτι για τη διαχείριση των υπολογιστικών πόρων και των δεδομένων του εργαστηρίου έχει να κάνει με το ποιός έχει πρόσβαση σε αυτά . Το ένα σύστημα να ξεχωρίζει τους χρήστες του σε Admins και Users θεωρείται από τις βασικές τακτικές αντιμετώπισης . Ο Admin έχει δικαιώματα root για την επεξεργασία , προσθήκη και διαγραφή δεδομένων και υπολογιστικών πόρων και ο user έχει πρόσβαση μόνο στους δικούς του υπολογιστικούς πόρους ή δεδομένα . Η διάκριση αυτών των δύο και η αποτροπή του χρήστη να γίνεται admin είναι καλό practice και πρέπει να υλοποιηθεί άμεσα για να μην τεθεί σε ρίσκο η ακεραιότητα και την εμπιστευτικότητα .

**Threat 3 (A-017 - Employee Data ) :** **RPN : 168**

Τα προσωπικά δεδομένα των εργαζομένων , και των πελατών , πρέπει να είναι ασφαλισμένα . Ο σύγχρονος τρόπος ψηφιακής ασφάλειας είναι με συγκεκριμένους αλγόριθμους για την προστασία των κωδικών και να υπάρχουν συγκεκριμένοι

κανόνες για τους εργαζομένους . Οι παρόντες μηχανισμοί δεν είναι αρκετοί για να εξαλείψουν την απειλή , και γι αυτό χρειάζεται συνεχής έρευνα για την εξασφάλιση της εμπιστευτικότητας των δεδομένων .

**Threat 43 (A-025 Δημιουργια Αντιγραφων Ασφαλειας):** **RPN : 168**

Τα αντίγραφα ασφαλείας είναι σημαντικά για οποιαδήποτε επιχείρηση να υπάρχουν στο γραφείο . Τα αντίγραφα αυτά όμως , πρέπει με κάποιο τρόπο να προστατευτούν από κακόβουλους actors οι οποίοι επιθυμούν να τα κλέψουν με οποιοδήποτε τρόπο . Ακόμα και αν μετακινηθούν σε διαφορετικό δωμάτιο ο κίνδυνος να πέσουν στα λάθος χέρια ακόμα υπάρχει σε υψηλό βαθμό . Πρέπει η διοίκηση να λάβει τα ανάλογα μέτρα για να υπάρχει συνεχής έλεγχος και έξτρα μέσων προστασίας όπως Κάμερες , Προσωπικό , για την ασφάλεια του αγαθού .

**Threat 19 (A-010 Database Server ) :** **RPN : 160**

Η υπαρξη security μπορει να μειωνει κατα πολυ τον κινδυνο αλλα δεν παυει να μην υπαρχει καθως ο security guard μπορει να μην ειναι στον ρολο του ολη την ωρα ή να ξεγελαστει απο καποιον κακοβουλο actor.Γι’αυτο ειναι συνετο να υπαρχει καταλληλη ενημερωση και ταυτοποιηση προτου καποιος εισελθει στο δωματιο και αλλαγες βαρδιας οταν λειπει ο security ειτε με υπαλληλο ειτε με 2ο security.

**Threat 35 (A-20 Web Development Platform (JOOMLA)) :** **RPN : 160**

Παρολο που η ιστοσελιδα μπορει να φτιαχτει απο επαγγελματια ειναι δυνατο να εχει και μια ομαδα απο πισω του καθως η δημιουργια μιας ιστοσελίδας εχει αρκετους τομεις που πρεπει να προσεχθει η αρχιτεκτονικη της αλλιως και παλι θα ειναι ευαλωτη.

**Threat 31 (A-019 Λειτουργικο Συστημα (Windows 10 Pro)) :** **RPN : 135**

Μονο η εγκατασταση antivirus δεν θα εμποδίσει τον υπολογιστη απο το να υποστη επιθεση απο ιο ή Malware .Ειναι αναγκαιο τα windows 10 pro να κανουν συχνα ενημερωσεις καθως και η ενημερωση του ιδιου του χρηστη με νεες επιθεσεις που βρισκουν οι κακοβουλοι χρηστη και τροπους να αμυνθεί εναντιον τους

**Threat 36 (A-021 Φυσικο Αρχειο Ασθενων) :** **RPN : 128**

Ο χωρος φυλαξης παρολο που μπορει να γινει γνωστος στους κακοβουλους χρηστες ειναι καλο η επιτηρηση του συστηματος να ειναι συνεχομενη απ’τις καμερες του συστηματος και να λειτουργησει σε περιπτωση διακοπης ρευματος με εναλλακτικη πηγη ρευματος καθως και
να υπαρχει ειδικος συναγερμος σε περιπτωση που μια καμερα υποστη ζημια

**Threat 40 (A-023  Χημικες Ουσιες ) :** **RPN : 112**

Η χρηση συστηματος εξαερισμου μειωνει δραστικα τον κινδυνο σε σχεση με το να αφηνεται η πορτα ανοιχτη αλλα σε περιπτωση διακοπης ρευματος θα πρεπει να φροντισουμε το συστημα εξαερισμου να ειναι συνδεδεμενο με μια γεννητρια ρευματος για να μην διακοπει η λειτουργια του

**Threat 23  (A-013 Router (Cisco C886VA-K9) ) :** **RPN : 108**

Η χρηση του firewall Μειωνει δραστικα την απειλη αλλα εκτος απο αυτο προτεινεται ειδικη ομαδα να κοιταει τα στατιστικα των συνδεσεων ανα συγκεκριμενες ωρες με το σκοπο του εντοπισμου μη φυσιολογικης συμπεριφορας

**Threat 37  (A-021 Φυσικο Αρχειο Ασθενων)  :** **RPN : 108**

Ενα χρηματοκιβωτιο δε θα εμποδίσει παντα την κλοπη των αρχειων καθως μπορει να κλεψουν και αυτο μαζι.Αρα ειναι καλο να χρησιμοποιουνται μεθοδοι καταστροφης των πληροφοριων που εχει μεσα (αδειασμα paint bomb) οταν εντοπιστει προσβαση ειτε με βιαιο τροπο ανοιγματος του,ειτε με πολλους λαθος δοκιμες του κωδικου

**Threat 38  (A-022 Αρχειο Υπαλληλων & Προμηθευτων) :** **RPN : 108**

Ενα χρηματοκιβωτιο δε θα εμποδίσει παντα την κλοπη των αρχειων καθως μπορει να κλεψουν και αυτο μαζι.Αρα ειναι καλο να χρησιμοποιουνται μεθοδοι καταστροφης των πληροφοριων που εχει μεσα (αδειασμα paint bomb) οταν εντοπιστει προσβαση ειτε με βιαιο τροπο ανοιγματος του,ειτε με πολλους λαθος δοκιμες του κωδικου

**Threat 42 (A-024 Αυτοματη Καταχωρηση Αποτελεσματων Δειγματοληψιας):** **RPN : 108**

Ενω μια ειδικη ομαδα ειναι καλο να επιτηρεί την κινηση του δικτυου θα πρεπει να υπαρχει
συνεχης εκπαιδευση πανω στο δικτυο για πιθανα 0 day attacks και με τεχνικης μηχανικης μαθησης και συμπεριφορων του δικτύου να εντοπιζονται κακοβουλες συμπεριφορες

**Threat 29  (A-018 Λειτουργικο Συστημα (Windows 7)) :** **RPN : 105**

Η χρηση μονο δυνατων passwords δεν ειναι παντα αρκετη διοτι εκτος απο dictionary attacks μπορει καποιος κακοβουλος χρηστης να γνωριζει τον κωδικο μας .Χρησιμοποιωντας μεθοδους οπως OTP κωδικους και authenticator apps ( Microsoft authenticator,authy, duo mobile etc)

# ΒΙΒΛΙΟΓΡΑΦΙΑ :


**[0]** ISO Security Guidelines **( Used as guideline )**

**[1]** What is FMEA ? Failure Mode and Effects Analysis

**[2]** Windows Vulnerabilities

**[3]** Threats And Vulnerabilities

**[4]** Network property secure

**[5]** IDS vs IPS

**[6]** OWASP XSS

**[7]** Print Spooler Exploits

**[8]** RDP Securing Remote Desktop

**[9]** Security Stack Exchange MAC Overflow

**[10]** Network Security Measures **( Used as guideline )**

**[11]** DNS Hijacking

**[12]** Online Business Security Measures Guidelines **( Used as guideline )**

**[13]** What is Network Monitoring ?

**[14]** Joomla Vulnerabilities

**[15]** Steganography and Vulnerabilities in popular archives formats