ΤΜΗΜΑ ΠΛΗΡΟΦΟΡΙΚΗΣ

ΑΣΦΑΛΕΙΑ ΠΛΗΡΟΦΟΡΙΑΚΩΝ ΣΥΣΤΗΜΑΤΩΝ

ΕΡΓΑΣΙΑ ΕΑΡΙΝΟΥ ΕΞΑΜΗΝΟΥ 2023

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

ΠΑΡΟΥΣΙΑΣΗ ΣΧΕΔΙΟΥ ΑΣΦΑΛΕΙΑΣ

BioAnalytix Lab

ΜΕΛΗ ΟΜΑΔΑ ΕΡΓΑΣΙΑΣ:

1. **Πάνος Δημήτριος p3200127 3200127@aueb.gr**
2. **Δημάκης Κωνσταντίνος p3200255 3200255@aueb.gr**
3. **Τσιβουράκης Ανδρέας p3200209 3200209@aueb.gr**

ΠΕΡΙΕΧΟΜΕΝΑ ΕΡΓΑΣΙΑΣ

1. ΕΙΣΑΓΩΓΗ

Για την σωστή λειτουργία και προστασία του μικροβιολογικού εργαστηρίου BioAnalytix η ασφάλεια των πληροφοριακών συστημάτων αλλά και των βοηθητικών εξαρτημάτων αποτελεί ένα σημαντικό παράγοντα. Στο χώρο εργασίας διαχειρίζονται και αποθηκεύονται προσωπικά δεδομένα πελάτων αλλά και της εταιρείας τα οποία είναι απαραίτητο να φυλάσσονται διότι η απώλεια τους θα προκαλέσει παραβίαση νόμων και κανονισμών. Με εξέλιξη των κυβερνοεπιθέσεων αλλά και την αύξηση των δημιουργικών φυσικών κλοπών υπάρχει σημαντική ανάγκη για την φύλαξη των στοιχείων που επεξεργάζονται και διατηρούνται στο εργαστήριο για την αποτροπή των ανεπιθύμητων ενεργειών και την διατήρηση της εμπιστευτικότητας, ακεραιότητας και διαθεσιμότητας

1.1 Περιγραφή Εργασίας

Με την αναγνώριση της ανάγκης της προστασίας των πληροφοριακών συστημάτων του μικροβιολογικού εργαστηρίου BioAnalytix πραγματοποιούμε την μελέτη για την επίτευξη του συγκεκριμένου στόχου. Αρχικά αναλύσαμε τις παρατηρήσεις του επιθεωρητή ασφάλειας, την τοπολογία του δικτύου και την κάτοψη των χώρων του εργαστηρίου και βρήκαμε κρίσιμες περιοχές. Έπειτα βρήκαμε αγαθά τα οποία χρειάζονται να προστατευτούν από μη εξουσιοδοτημένους χρήστες και φυσικές καταστροφές και βρήκαμε την προσφορά του καθενός. Στην συνέχεια προσδιορίζουμε τις ευπάθειες και τους κινδύνους που απειλούν τα αγαθά, τους αναλύουμε εκφράζοντας τους τρόπους αξιοποίησης τους, περιγράφουμε τις επιπτώσεις που θα προσφέρουν και δίνουμε εκτιμήσεις επικινδυνότητας και επιπτώσεων. Τέλος προτείνουμε τρόπος αποτροπής των κακόβουλων ενεργειών ή αντιμετώπισης σε περίπτωση που λάβουνε θέση ώστε να εξασφαλίζεται η ασφάλεια στα αγαθά του μικροβιολογικού εργαστηρίου.

1.2 Δομή παραδοτέου

Στην ενότητα 2 αναλύουμε τις υποδομές του μικροβιολογικού εργαστηρίου με βάση τα σχέδια και την τοπολογία του δικτύου βρίσκοντας έτσι κρίσιμες περιοχές και εντοπίζουμε αγαθά τα οποία ομαδοποιούμε εκφράζοντας για το καθένα την χρησιμότητα του. Στην ενότητα 3 αναφέρουμε τις απειλές που μπορούν να προκύψουν, τις ευπάθειες κάθε αγαθού και παρουσιάζουμε εκτιμήσεις για την επικινδυνότητα και την πιθανότητα πραγματοποίησης επιθέσεων. Στην ενότητα 4 περιγράφουμε μέτρα ασφάλειας ανάλογα των ευπαθειών και τον κινδύνων των οποίων εντοπίσαμε για κάθε αγαθό, διαχωρισμένα για κάθε απειλή. Στην ενότητα 5 εκφράζουμε τα ευρήματα με την μεγαλύτερη επικινδυνότητα, όπου τα μέτρα πρόληψης είναι απαραίτητα και πρέπει να ληφθούν υπόψιν από το εργαστήριο για την διατήρηση της εμπιστευτικότητας, της ακεραιότητας και της διαθεσιμότητας.

2. ΜΕΘΟΔΟΛΟΓΙΑ ΜΕΛΕΤΗΣ ΑΣΦΑΛΕΙΑΣ

Για τη Διαχείριση Επικινδυνότητας του BioAnalytix 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 BioAnalytix Lab.

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

Επιγραμματικά τα αγαθά τα οποία εντοπίστηκαν είναι:

- Αιματολογικός Αναλυτής
- 5 Υπολογιστές Desktop
- 2 Εκτυπωτές
- 2 Server
- 2 Switches
- Router
- Firewall
- Laptop
- Customer Data
- Employee Data
- Λογισμικό Windows 7 Pro
- Λογισμικό Windows 10
- Website
- Φυσικό Αρχείο Ασθενών
- Αρχείο Υπαλλήλων & Προμηθευτών
- Αρχείο Προμήθειων Αποθήκης
- Bar Code Scanner
- Digital Microscope
- Δείγματα & Φάρμακα
- Αρχείο Προγραμματισμένων Ραντεβού
- Φυσικό Αρχείο Πληρωμών και Αποδείξεων

2.2 Εξοπλισμός & Υλισμικό (hardware)

Τα αγαθά που ανήκουν στην κατηγορία του hardware είναι:

- Αιματολογικός Αναλυτής
- 5 Υπολογιστές Desktop
- 2 Εκτυπωτές
- Laptop
- Digital Microscope
- Bar Code Scanner
- Δείγματα και Φάρμακα

2.3 Λογισμικό και εφαρμογές

Τα αγαθά που υπόκεινται στο λογισμικό είναι:

- Λογισμικό Windows 7 Pro
- Λογισμικό Windows 10
- Website
- Firewall

2.4 Δίκτυο

Τα συστατικά μέρη του δικτυού είναι:

- 2 Server
- 2 Switches
- Router

2.5 Δεδομένα

Τα δεδομένα του συστήματος βρίσκονται σε:

- Customer Data
- Employee Data
- Φυσικό Αρχείο Ασθενών
- Αρχείο Υπάλληλων και Προμηθευτών
- Αρχείο Προμήθειων Αποθήκης
- Αρχείο Προγραμματισμένων Ραντεβού
- Φυσικό Αρχείο Πληρωμών και Αποδείξεων

2.6 Διαδικασίες

Παραδείγματα Διαδικασιών οι οποίες λαμβάνουν χώρα στο Εργαστήριο BioAnalytix Lab:

- Συλλογή δειγμάτων / αγαθά που υπάγονται: Αιματολογικός Αναλυτής, Δείγματα και Φάρμακα, Φυσικό Αρχείο Ασθενών
- Καλλιέργεια βακτηρίων / αγαθά που υπάγονται: Αιματολογικός Αναλυτής, Μικροσκόπιο, Δείγματα και Φάρμακα
- Συνταγογράφηση εξετάσεων / αγαθά που υπάγονται: Υπολογιστής Desktop, Φυσικό Αρχείο Ασθενών, Customer Data
- Ανέβασμα στατιστικών στη βάση δεδομένων / αγαθά που υπάγονται: Database Server, Customer Data, Employee Data
- Χορήγηση Φαρμάκων / αγαθά που υπάγονται: Υπολογιστής Desktop, Δείγματα και Φάρμακα, Customer Data
- Έλεγχος Αποθήκης / αγαθά που υπάγονται: Αρχείο Προμήθειων Αποθήκης
- Επικοινωνία Υπολογιστών: Switches, Router
- Εκτύπωση εγγράφων / αγαθά που υπάγονται: Workstation, Εκτυπωτές
- Μισθοδοσία / αγαθά που υπάγονται: Workstation, Employee Data

3. ΑΠΟΤΙΜΗΣΗ ΑΓΑΘΩΝ ΤΗΣ ΕΓΚΑΤΑΣΤΑΣΗΣ

Το αγαθό είναι κάτι το οποίο έχει αξία και αξίζει να προστατευτεί. Σε ένα χώρο όπως ένα μικροβιολόγο εργαστήριο όπου υπάρχει πληθώρα αγαθών υπάρχει και πιθανή πληθώρα ευπαθειών δηλαδή σημείων του φυσικού περιβάλλοντος, του υλικού, του λογισμικού ή των διαδικασιών, τα οποία ενδέχεται να προσδίδουν σε κάποιους τη δυνατότητα να προβούν σε ενέργειες μη επιθυμητές από αυτούς που ανέπτυξαν ή από αυτούς που ελέγχουν το Πληροφοριακό Σύστημα – συγκεκριμένα το σύστημα του εργαστήριου BioAnalytix Lab. Οι αδυναμίες αυτές μπορεί να οδηγήσουν σε πραγματικές απειλές για το σύστημα του εργαστηρίου δηλαδή γεγονότα που προκαλούν αρνητικές συνέπειες στα αγαθά. Παρακάτω γίνεται αποτίμηση τόσο των αγαθών του συστήματος όσο και των απειλών και των αδυναμιών που υπόκεινται τα συγκεκριμένα αγαθά καθώς και τα αποτελέσματα της αποτίμησης επικινδυνότητάς.

3.1 Αγαθά που εντοπίστηκαν

Τα αγαθά τα οποία βρίσκονται στην κατοχή του Εργαστήριου BioAnalytix Lab και χρησιμοποιούνται στην ανάλυση αποτίμησης επικινδυνότητας είναι:

- Αιματολογικός Αναλυτής – μετρά και κατηγοριοποιεί τα είδη των αιμοκυττάρων και μετρά διάφορα χαρακτηριστικά των αυτών. Χρησιμοποιεί Proprietary Software και φυλάσσεται στο Εργαστήριο – Παρασκευαστήριο.
- 5 Υπολογιστές Desktop – για την εκπόνηση εργασιών ανάλογα με τον χώρο στον οποίο βρίσκονται. Διαθέτουν Windows 10 Pro λογισμικό και υπάρχουν 2 από αυτούς στο Παρασκευαστήριο και οι υπόλοιποι διαμοιράζονται στο Χώρο Λήψης Δειγμάτων, στο Χώρο Αναμονής και στο Γραφείο του Ιατρού.
- 2 Εκτυπωτές – παραγωγή φυσικού εγγράφου το οποίο προϋπάρχει σε ψηφιακή μορφή. Διαμοιράζονται στο Χώρο Αναμονής και στο Γραφείο του Ιατρού.
- 2 Server – αποθηκεύουν περιεχόμενο που μπορούν να προσπελάσουν οι χρήστες μέσω των browsers τους. Υπάρχει ενας web και ένας database server και είναι τοποθετημένοι σε Βοηθητικό Χώρο.
- 2 Switches –συμβάλει στην επικοινωνία μεταξύ των υπολοίπων digital assets του εργαστήριου. Χρησιμοποιούν Windows 7 Pro και υπάρχει ένας στην Αίθουσα Αναμονής και ένας στον Βοηθητικό Χώρο.
- Router – διαχειρίζεται την κίνηση μεταξύ των υποδικτύων. Χρησιμοποίει Windows 7 Pro και βρίσκεται στην Αίθουσα Αναμονής.
- Firewall – σύστημα ελέγχου πρόσβασης, αποτρέπει την μη ταυτοποιημένη κίνηση μέσα στο δίκτυο. Το σύστημα που χρησιμοποιεί είναι Windows 10 Advanced IP Services και είναι εγκατεστημένο στον Βοηθητικό Χώρο.
- Laptop – φορητός υπολογιστής Apple MacBook Air με λογισμικό MAC-OS για χρήση προσωπικών δεδομένων του Ιατρού διότι βρίσκεται στο Γραφείο του
- Customer Data – συνολικά συγκεντρωμένα δεδομένα πελάτων, είναι εγκατεστημένα στον database server

- Employee Data - συνολικά συγκεντρωμένα δεδομένα εργαζομένων, είναι εγκατεστημένα στον database server
- Λογισμικό Windows 7 Pro – λογισμικό για τη διαχείριση του δικτύου, εγκατεστημένο στα switches
- Λογισμικό Windows 10 – λογισμικό για διαχείριση αρχείων και πόρων, εγκατεστημένο στους 5 υπολογιστές desktops
- Website – JOOMLA εφαρμογή, ανοιχτό σημείο πρόσβασης για τους χρήστες, βρίσκεται στον web server
- Φυσικό Αρχείο Ασθενών – αποθηκευμένα έγγραφα πληροφοριών ασθενών και αποτελεσμάτων εξετάσεων, βρίσκεται στο Ερμάριο - Ανοικτή Βιβλιοθήκη σε Αίθουσα Αναμονής
- Αρχείο Υπαλλήλων & Προμηθευτών - αποθηκευμένα έγγραφα πληροφοριών εργαζομένων και συνεργατών, βρίσκεται στο Ερμάριο - Ανοικτή Βιβλιοθήκη σε Αίθουσα Αναμονής

Τα αγαθά τα οποία επιλέχθηκαν προσωπικά από την ομάδα είναι:

- Αρχείο Προμήθειων Αποθήκης – αποθηκευμένα αποθέματα και ποσότητες αγαθών απαραίτητα για το εργαστήριο (φάρμακα, σύριγγές, γάζες), βρίσκεται σε Ανοικτή Βιβλιοθήκη σε Γραφείο Ιατρού
- Bar Code Scanner – παρέχει ασφαλή είσοδο στους χώρους του εργαστήριου μέσω τους συστήματος BarCodeOS®, υπάρχει στο Εργαστήριο - Παρασκευαστήριο
- Digital Microscope – υποστήριξη στην έρευνα, βρίσκεται στο Χώρο Λήψης Δειγμάτων - Εργαστήριο
- Δείγματα & Φάρμακα – χημικές ουσίες που παρέχονται στους πελάτες, φυλάσσονται στο Χώρο Λήψης Δειγμάτων - Εργαστήριο
- Αρχείο Προγραμματισμένων Ραντεβού – αρχείο που βοηθά στην εύρυθμη λειτουργία του εργαστήριου, βρίσκεται σε Αίθουσα Αναμονής - Γραφείο Ιατρού
- Φυσικό Αρχείο Πληρωμών και Αποδείξεων – αποθηκευμένα στοιχεία πληρωμών των πελατών, βρίσκεται σε Γραφείο Υποδοχής - Γραφείο Ιατρού

Τα αγαθά τα οποία επιλέχθηκαν είναι πληροφοριακά αγαθά που θεωρούνται αρκετά σημαντικά στην λειτουργία του εργαστηρίου BioAnalytix Lab και είναι άξια προστασίας από απειλές του συστήματος. Η σπουδαιότητα τους που οδήγησε και στην επιλογή τούς έγκειται στη διασφάλιση ακριβών και αξιόπιστων πειραματικών αποτελεσμάτων, την προώθηση της ασφάλειας, την αύξηση της αποδοτικότητας και της παραγωγικότητας, τη μείωση του κόστους και τη διατήρηση της συμμόρφωσης με τους κανονισμούς και τα πρότυπα πιστοποίησης.

3.2 Απειλές που εντοπίστηκαν

ΠΑΡΑΒΙΑΣΗ ΑΣΦΑΛΕΙΑΣ	ΤΥΠΟΣ ΣΥΝΕΠΕΙΑΣ	ΒΑΘΜΟΣ ΣΥΝΕΠΕΙΑΣ	LIKEHOOD RANK
Διαρροή Δεδομένων	Έμμεση	9	5
Μη ταυτοποιημένη είσοδος χρήστη σε περιοχή με προσωπικά δεδομένων υπάλληλων	Έμμεση	7	4
Κλοπή αγαθού από εξωτερικούς χρήστες	Άμεση	6	4
Μη εξουσιοδοτημένη χρήση εφαρμογής	Έμμεση	7	4
Καταστροφή λογισμικού και υλικού	Άμεση	9	3
Φωτιά	Άμεση	8	3
Πλημμύρα	Άμεση	8	3
Παραποίηση επικοινωνίας	Έμμεση	7	4
Κλοπή αγαθού από εσωτερικούς χρήστες	Άμεση	6	3
Τεχνικό Σφάλμα	Άμεση	9	5
Παραποίηση Αποτελεσμάτων	Έμμεση	6	4
Είσοδος κακόβολου κώδικα	Έμμεση	9	5
Λάθος χειρισμός δεδομένων	Έμμεση	6	3
Λανθασμένη αποτίμηση δεδομένων	Έμμεση	6	3
Λάθος συντήρησης βάσης δεδομένων	Έμμεση	6	3
Διαρροή νερού	Άμεση	8	3
Εσκεμμένη Τροποποίηση Δεδομένων και Αποτελεσμάτων	Έμμεση	7	5
Πλαστοπροσωπία χρήστη από κακόβουλους εξωτερικούς χρήστες	Έμμεση	7	4
Τεχνική βλάβη υπολογιστή	Άμεση	8	5
Τεχνική βλάβη συστήματος ελέγχου πρόσβασης	Έμμεση	8	4

3.3 Ευπάθειες που εντοπίστηκαν

Επιγραμματικά οι ευπάθειες που παρατηρήσαμε ταξινομούνται ως εξής:

HARDWARE:

- Μη ελεγχόμενη υγρασία
- Παραγωγή ψεύτικου barcode

SOFTWARE:

- Οι κανόνες του συστήματος ελέγχου πρόσβασης να μην είναι καταλληλά διαμορφωμένοι
- Χαμηλά μετρά ταυτοποίησης χρηστών
- Ανεπαρκής έλεγχος εισόδου/εξόδου και ελέγχου δραστηριότητας
- Ανεπαρκή συστήματα αντιγράφων ασφάλειας και μετρά ανάκτησης από καταστροφές
- Default διαπιστευτήρια λογισμικού τα οποία είναι ευρέως γνωστά και εύκολα προσπελάσιμα από οποιονδήποτε
- Μη ενημερωμένο/παλιωμένο λογισμικό
- Ανεπάρκεια WAF και φτωχή ανάπτυξη λογισμικού ιστοσελίδας
- Λανθασμένες ρυθμίσεις λογισμικού

ΔΙΚΤΥΟ:

- Η συνδεσιμότητα του δικτύου επιτρέπει μη ταυτοποιημένη πρόσβαση στο σύστημα
- Ανασφάλεια στα ασύρματα δίκτυα
- Αδύναμοι κωδικοί πρόσβασης
- Μη ασφαλή και επικυρωμένη μεταφόρτωση αρχείων
- Μη κρυπτογραφημένα δεδομένα (μεταφορά και λήψη)

ΠΡΟΣΩΠΙΚΟ:

- Φάκελοι με δεδομένα κρατούνται σε μη ασφαλή μέρη, ευκολά πρόσβαση από μη ειδικευμένο προσωπικό
- Κακεντρεχείς ή αφελείς δράσεις από υπάλληλους
- Ανειδίκευτο προσωπικό

ΤΟΠΟΘΕΣΙΑ:

- Διακοπές Ρεύματος
- Ελλιπή μετρά προστασίας από Φωτιά
- Ελλιπή μετρά προστασίας από πλημμύρα
- Ελλιπή μετρά φυσικής προστασίας(μη περιφραγμένη περιοχή)

ΟΡΓΑΝΩΤΙΚΕΣ:

- Φάκελοι με δεδομένα κρατούνται σε μη ασφαλή μέρη, ευκολά πρόσβαση από μη ειδικευμένο προσωπικό
- Εύκολη είσοδος στο γραφείο του Ιατρού από τον κεντρικό πολυσύχναστο δρόμο

- Φάκελοι με δεδομένα φυλάσσονται στην αίθουσα αναμονής η οποία είναι ευκολά πρόσβαση και όχι ασφαλής
- Συσκευές ορατές και εύκολα προσβάσιμες από επισκέπτες και εξωτερικούς χρήστες

3.4 Αποτελέσματα αποτίμησης

ΑΓΑΘΟ	ΕΥΠΑΘΕΙΑ	ΑΠΕΙΛΗ	IMPACT	LIKEHOOD	VULN. RANK	RPN
Firewall	Οι κανόνες δεν είναι καταλληλά διαμορφωμένοι	Διαρροή Δεδομένων	9	5	5	225
Employee Data	Μη κρυπτογραφημένα δεδομένα	Μη ταυτοποιημένη είσοδος χρήστη σε περιοχή με προσωπικά στοιχεία υπαλλήλων	7	4	4	112
Αρχείο Υπάλληλων και Προμηθευτών	Φάκελοι φυλάσσονται σε μη ασφαλές μέρος	Κλοπή αγαθού από εξωτερικούς χρήστες	6	4	3	72
Αιματολογικός Αναλυτής	Η συνδεσιμότητα του δικτύου επιτρέπει μη ταυτοποιημένη πρόσβαση στο σύστημα	Μη εξουσιοδοτημένη χρήση εφαρμογής	7	4	3	84
Αιματολογικός Αναλυτής	Διακοπή Ρεύματος	Καταστροφή υλικού και λογισμικού	9	3	5	135
Workstation	Ελλιπή μετρά προστασίας από φωτιά	Φωτιά	8	3	2	48
Workstation	Ελλιπή μετρά προστασίας από πλημμύρα	Πλημμύρα	8	3	3	72
Workstation	Μη ασφαλή ασύρματα δίκτυα	Παραποίηση Επικοινωνίας	7	4	4	112
Workstation	Ελλιπή μετρά φυσικής προστασίας(μη περιφραγμένη περιοχή)	Κλοπή αγαθού από εξωτερικούς χρήστες	6	4	3	72
Workstation	Κακεντρεχείς η αφελείς δράσεις από υπάλληλους	Κλοπή αγαθού από εσωτερικούς χρήστες	6	3	3	54
Printer	Μη ελεγχόμενη υγρασία	Τεχνικό σφάλμα	9	5	3	135
Printer	Μη κρυπτογραφημένα δεδομένα	Κλοπή αγαθού(προσωπικών δεδομένων) από εξωτερικούς χρήστες	7	3	3	63

Laser Printer	Μη ασφαλή και επικυρωμένη μεταφορά δικτυών	Παραποίηση και τροποποίηση αποτελεσμάτων	6	4	4	96
Laser Printer	Ελλιπή μέτρα προστασίας περιοχής(μη περιφραγμένη περιοχή)	Κλοπή αγαθού από εξωτερικό χρήστη	6	4	4	72
Web Server	Αδύναμη ταυτοποίηση και επικύρωση	Μη εξουσιοδοτημένη χρήση εφαρμογής	7	4	5	140
Web Server	Εσφαλμένη διαμόρφωση διακοσμητή	Μη ταυτοποιημένη είσοδος χρήστη σε περιοχή με προσωπικά στοιχεία υπαλλήλων	7	4	5	140
Web Server	Ανεπαρκής έλεγχος εισόδου/εξόδου και ελέγχου δραστηριότητας	Είσοδος κακόβολου κώδικα	9	5	5	140
Database Server	Ανεπαρκή συστήματα αντιγράφων ασφάλειας και μέτρων ανάκτησης από καταστροφές	Σφάλμα ελέγχου δεδομένων	8	5	5	200
Database Server	Μη επικυρωμένο προσωπικό	Λανθασμένη αποτίμηση δεδομένων	6	3	5	90
Database Server	Χαμηλά μέτρα προστασίας βάσης δεδομένων	Λάθος συντήρησης βάσης δεδομένων	6	3	5	90
Switch	Ελλιπή μέτρα προστασίας από πλημμύρα	Ρίψη νερού	8	3	3	72
Switch	Έλλειψη antivirus λογισμικού	Μη επικυρωμένη είσοδος στην εφαρμογή	7	4	5	140
Router	Εσφαλμένη διαμόρφωση κανόνων συστήματος ελέγχου πρόσβασης	Μη επικυρωμένη είσοδος και αλλαγές στα δεδομένα	8	5	5	200
Router	Default διαπιστευτήρια λογισμικού τα οποία είναι ευρέως γνωστά και εύκολα προστασία από οποιονδήποτε	Πλαστοπροσωπία χρήστη από κακόβουλους εξωτερικούς χρήστες	8	5	5	200

Laptop	Παλαιωμένο λογισμικού	Μη επικυρωμένη είσοδος σε προσωπικά δεδομένα του Ιατρου	8	4	5	160
Laptop	Είσοδος στο γραφείο του Ιατρού από τον πολυσύχναστο δρόμο	Κλοπή αγαθού από εξωτερικούς χρήστες	9	4	4	144
Customer Data	Μη κρυπτογραφημένα δεδομένα	Είσοδος στην περιοχή των δεδομένων από μη ταυτοποιημένους χρήστες	7	4	4	112
SOFTWARE	Παλαιωμένα συστήματα	Παραποίηση επικοινωνίας	9	5	5	225
SOFTWARE	Αδύναμοι κωδικοί	Διαρροή και απώλεια δεδομένων	9	5	5	225
WEBSITE	Ανεπάρκεια WAF και φτωχή ανάπτυξη λογισμικού ιστοσελίδας	Είσοδος στα δεδομένα από μη ταυτοποιημένους χρήστες	8	5	5	200
WEBSITE	Μη ασφαλή και επικυρωμένη μεταφόρτωση αρχείων	Είσοδος κακόβολου κώδικα & cyber attacks	8	5	5	200
Φυσικό Αρχείο Ασθενών	Φάκελοι με δεδομένα φυλάσσονται στην αίθουσα αναμονής η οποία είναι ευκολά πρόσβαση και όχι ασφαλής	Προσβασιμότητα και κλοπή αγαθού από εξωτερικούς χρήστες	6	4	3	72
Αρχείο Προμήθειων	Είσοδος στο γραφείο του Ιατρού από τον πολυσύχναστο δρόμο	Προσβασιμότητα και κλοπή αγαθού από εξωτερικούς χρήστες	6	4	3	72
Δείγματα και Φάρμακα	Μη ειδικευόμενο προσωπικό	Κίνδυνος κατανάλωσης και επιχορήγησής λάθος φαρμάκων και ποσοτήτων	7	4	4	112
Αρχείο Προγραμματισμένων Ραντεβού	Φάκελοι με δεδομένα φυλάσσονται στην αίθουσα αναμονής η οποία είναι ευκολά	Προσβασιμότητα και κλοπή αγαθού από εξωτερικούς χρήστες	6	4	3	72

	πρόσβαση και όχι ασφαλής					
Digital Microscope	Εσφαλμένη διαμόρφωση	Εκμετάλλευση από κακόβολου εξωτερικό χρήστη για είσοδο στο σύστημα	8	4	4	128
Digital Microscope	Αδύναμοι κωδικοί	Εκμετάλλευση από κακόβολου εξωτερικό χρήστη για είσοδος στο σύστημα	8	4	4	128
Barcode Scanner	Παραγωγή ψεύτικου barcode	Μη ταυτοποιημένοι χρήστες έχουν πρόσβαση σε δείγματα εργαστήριου	6	4	4	96
Barcode Scanner	Συσκευές είναι ορατές και όχι φυλαγμένες σε ασφαλές μέρος	Μη ταυτοποιημένη χρήση της εφαρμογής του συστήματος	3	4	3	36
Αρχείο Πληρωμών και Αποδείξεων	Φύλαξη φακέλων σε μη προστατευμένη περιοχή	Κλοπή αγαθού από κακόβολου χρήστη	7	4	4	112

Τα αποτελέσματα αποτίμησης της επικινδυνότητάς του πληροφοριακού συστήματος και οι διαδικασίες στις οποίες πρέπει να προβούμε προκύπτουν με κύριο γνώμονα το Risk Priority Number(RPN) κάθε απειλής που ξεσπά πάνω σε ένα συγκεκριμένο αγαθό. Το RPN προκύπτει από το γινόμενο των σειρών κατάταξης για την επίπτωση των απειλών, την πιθανότητα της αποτυχίας και του μεγέθους της ευπάθειας έπειτα από εφαρμογή μέτρων πρόληψης ή εντοπισμού. Με βάση τα νούμερά αυτά εκεί που εμφανίζεται υψηλότερος βαθμός RPN αξίζει να δοθεί μεγαλύτερη προσοχή στην αντιμετώπιση των ευπαθειών και απειλών πάνω σε ένα αγαθό παρότι σε ένα αγαθό με μικρότερο αριθμό RPN που φυσικά χρήζει αντιμετώπισης και επίβλεψης αλλά τα μέτρα αυτά φαίνονται να είναι πιο δραστικά.

Συνολικά παρατηρούμε:

- **RPN > 150**: Τα αγαθά στα οποία εμφανίζεται τόσο μεγάλο RPN είναι digital αγαθά όπως switches, routers, database server, software και website συστήματα και firewall συστήματα πρόσβασης ελέγχου τα οποία υπόκεινται σε απειλές τύπου διαρροής και καταστροφής δεδομένων, πλαστοπροσωπίας χρήστη, εισόδου κακεντρεχούς κώδικα και εισόδου κακόβολου εξωτερικού χρήστη. Αυτό συμβαίνει γιατί τα αγαθά αυτά είναι κύρια συστατικά στοιχεία της δομής του δικτυού και η αποτυχία και η λανθασμένη χρήση αυτών μπορεί να οδηγήσει σε ευρεία αποδιοργάνωση των υπολοίπων συσκευών του δικτύου και με μεγάλη πιθανότητα να οφείλεται για μεγάλες απώλειες της επιχείρησης τόσο οικονομικές αλλά κατά κύριο λόγων δεδομένων και εμπιστευτικών πληροφοριών. Κάτι τέτοιο συντελεί στην ρήξη της εμπιστευτικότητας και της ακεραιότητας του συστήματος.
- **100 < RPN < 150**: Τα αγαθά τα οποία υπάγονται σε αυτή την κατηγορία είναι συσκευές οι οποίες χειρίζονται και επεξεργάζονται δεδομένα όσο και μερικά

από τα δεδομένα. Για παράδειγμα είναι οι υπολογιστές desktop, οι εκτυπωτές, τα εργαστηριακά όργανα δηλαδή το μικροσκόπιο και ο αιματολογικός αναλυτής και τα αρχεία με τα δεδομένα των υπαλλήλων. Τα αγαθά αυτά εμφανίζουν αρκετά υψηλό RPN αλλά όχι όσο τα αγαθά της πρώτης κατηγορίας καθώς η εύρυθμη λειτουργίας του επηρεάζεται άμεσα από αυτή των αγαθών την πρώτης κατηγορίας. Οι απειλές και οι ευπάθειες που συναντούμε είναι τόσο φυσικές(φωτιά, ρίψη νερού, κλοπή) όσο και πάνω στον εξοπλισμό(σφάλματα εφαρμογής, μη επικυρωμένη είσοδος στην εφαρμογή, παραποίηση επικοινωνίας). Εξακολουθεί όμως η καταστροφή/λανθασμένη χρήση/κακόβουλη μεταχείριση τους να υποβαθμίζει την εμπιστευτικότητα, την ακεραιότητα και την προσβασιμότητα του συστήματος χωρίς όμως να θεωρείται τόσο καταστροφική. Αυτό συμβαίνει γιατί παραδείγματος χάριν η καταστροφή ενός εκτυπωτή από φωτιά θα επηρεάσει μόνο το χρήστη η το τμήμα όπου ανήκει ο εκτυπωτής, παρά όλο το δίκτυο του εργαστηρίου.

- **RPN < 100**: Η κατηγορία αυτή περιλαμβάνει κατά κύριο λόγω φυσικά αγαθά(αρχεία δεδομένων) όσο και κάποιες από τις προηγούμενες κατηγορίες αγαθών που όμως στην περίπτωση αυτή απειλούνται από ευπάθειες και κινδύνους που είναι εύκολα αντιμετωπίσιμοι. Αυτό οφείλεται στο γεγονός ότι τα αγαθά αυτά είναι υποκείμενο μικρότερο ρίσκου σε σχέση με τα digital αγαθά. Η απώλεια και η ζημιά αυτών δεν είναι τυπικά καταστροφική. Παρόλο που αν συνέβαινε κάτι τέτοιο θα μπορούσε να προκαλέσει κάποια ταλαιπωρία είναι συνήθως δυνατή η ανάκτηση τους με την ελάχιστη αποδιοργάνωση.

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

Η λανθασμένη εκτίμηση των δεδομένων στα υλικά συστήματα ή οι λανθασμένες δόσεις φαρμάκων και μολύνσεων προκαλούνται από εργαζόμενους με λανθασμένα προσόντα. Για την αντιμετώπιση τους χρειάζεται :

- Πρόσληψη και επανεκπαίδευση προσωπικού ώστε να περιοριστεί ο αριθμός των λαθών και να υπάρχει σωστή λειτουργία του εργαστηρίου.

4.2. Ταυτοποίηση και αυθεντικοποίηση

Η αποτροπή χρήσης συστημάτων και πρόσβαση σε χώρους από μη εξουσιοδοτημένους χρήστες μπορεί να προκαλέσει κλοπή αγαθών ή και τροποποίηση δεδομένων. Για την προστασία και σωστή ταυτοποίηση για είσοδο και χρήση συστημάτων χρειαζόμαστε:

- Χρήση δυνατών κωδικών πρόσβασης. Με συνθηματικά που δεν μπορούν να εντοπιστούν εύκολα μειώνονται δραματικά οι πιθανότητας πρόσβασης μη εξουσιοδοτημένων χρηστών στα συστήματα.
- Χρήση πολλαπλών τρόπων ταυτοποίησης. Η χρήση κωδικού πρόσβασης μόνη της μπορεί να μην είναι αρκετά ασφαλή σε κάποιες περιπτώσεις επομένως χρειάζονται περισσότερα μέτρα όπως η αποστολή νέο κωδικού σε μια εξασφαλισμένη συσκευή, χρήση βιομετρικών τεχνολογιών όπως δακτυλικό αποτύπωμα ή αναγνώριση προσώπου, φωνής.

4.3. Έλεγχος προσπέλασης και χρήσης πόρων

Είναι σημαντικό τα αγαθά και τα συστήματα να χειρίζονται μόνο από εξουσιοδοτημένους χρήστες. Κάθε είδος άλλης χρήσης είναι απαραίτητο να απαγορευτεί. Για αποφυγή χρήσης των πόρων από τρίτους χρειάζεται να :

- Οι συσκευές προφυλάσσονται σε ασφαλή τοποθεσίες οι οποίες θα είναι προσβάσιμες μόνο από το προσωπικό και χρειάζονται κωδικό πρόσβασης και χρήση. Έτσι εκμηδενίζεται η πιθανότητα κλοπής αλλά χρήσης από μη εξουσιοδοτημένους χρήστες.

- Δυνατότητα πρόσβασης μόνο με ταυτοποίηση στην οποία θα υπάρχει χρήση δυνατού συνθηματικού. Πετυχαίνετε η παρακολούθηση χρήσης των πόρων αλλά και προτροπή χρήση τους από τρίτους.

- Παρακολούθηση, έλεγχος και καταγραφή δραστηριότητας σε όλα τα συστήματα. Με το συγκεκριμένο μέτρο υπάρχει πλήρης έλεγχος για τα πρόσωπα που χρησιμοποιούν τους πόρους αλλά και επίγνωση για τις μετατροπές τις οποίες συμβαίνουν σε αυτά, με αποτέλεσμα να υπάρχει πιο γρήγορη αντίδραση σε περίπτωση ανάγκης και δυνατότητα αναγνώρισης του προσώπου.

4.4. Διαχείριση εμπιστευτικών δεδομένων

Η μεταφορά μη κρυπτογραφημένων μηνυμάτων και πρόσβαση των πελατών και εξωτερικών χρηστών σε δεδομένα του εργαστηρίου αυξάνει δραματικά την πιθανότητα κλοπής και επεξεργασίας των αγαθών. Για την αποτροπή των συγκεκριμένων ενεργειών είναι απαραίτητη :

- Εφαρμογή κρυπτογράφησης σε όλες τις μεταδόσεις δεδομένων μέσω δημόσιων δικτύων χρησιμοποιώντας πρωτόκολλο TLS, το οποίο χρησιμοποιείται σε διαδικτυακή κίνηση και εξασφαλίζει την προστατευμένη επικοινωνία.
- Διατήρηση δεδομένων σε χώρους προσβάσιμους μόνο από το προσωπικό και σε ασφαλή μέρη. Φυσικά δεδομένα θα πρέπει να βρίσκονται σε κλειδωμένα ντουλάπια και τα ψηφιακά δεδομένα σε ασφαλή συστήματα. Σε κάθε περίπτωση πρέπει να μην είναι προσβάσιμα από πελάτες ή εξωτερικούς χρήστες

4.5. Προστασία από τη χρήση υπηρεσιών από τρίτους

Η απώλεια δεδομένων μπορεί να συμβεί με την φυσική παρέμβαση ενός τρίτου ή την απόκτηση ελέγχου στα συστήματα διαχείρισης τους. Τέτοιες επιθέσεις προκαλούν σοβαρά οικονομικά προβλήματα στο εργαστήριο. Η αποτροπή τους μπορεί να επιτευχθεί με :

- Χρήση πλήρους συστήματος ασφάλειας με κάμερες για την διαρκή παρακολούθηση των αγαθών. Ως συνέπεια θα έχουμε την αποφυγή χρήση των συστημάτων και φυσικών αγαθών από τρίτους.
- Για την χρήση κάποιων συστημάτων ή την είσοδο σε κάποιους χώρους είναι ωφέλιμη η πολλαπλή ταυτοποίηση. Έτσι θα περιοριστεί η πιθανότητα πρόσβασης από εξωτερικούς χρήστες οι οποίοι δεν έχουν άδεια χρήσης. Διάφοροι τρόποι ταυτοποίησης είναι η αναγνώριση ίριδας, υπογραφής και αμφιβληστροειδούς.
- Εγκατάσταση λογισμικού αποτροπής επιθέσεων ώστε να υπάρχει προστασία των ψηφιακών αγαθών. Είναι απαραίτητη η αποτροπή επιθέσεων και η απόκτηση πρόσβασης τρίτων στα συστήματα του εργαστηρίου οι οποίου μπορούν να κλέψουν, να μεταδώσουν και να τροποποιήσουν τα δεδομένα.

4.6 Προστασία λογισμικού

Λογισμικό το οποίο δεν έχει δομηθεί καθώς και έλλειψη ενημερώσεών του μπορεί να εμφανίσει τρόπους εισβολής από μη εξουσιοδοτημένους χρήστες. Τρόποι αποφυγής της είναι :

- Θεμελίωση λογισμικού με ορθό και προστατευμένο κώδικα ώστε να μηδενιστούν τα κρίσιμα σημεία τα οποία μπορούν να παράγουν απειλές και κινδύνους με την αξιοποίηση τους από εξωτερικούς χρήστες.
- Τακτική ενημέρωση λογισμικού και περιορισμός χρήσης του, μόνο από ισχυρά αλληλέγγυους εργαζόμενους. Οι ενημερώσεις θα διορθώσουν προηγούμενα λάθη και θα προστατεύσουν από εξερευνημένες κερκοπορτες,

θα προσφέρουν νέες δυνατότητες και θα κρατήσουν το λογισμικό στην μέγιστη δυνατότητα του. Με την περιορισμένη χρήση θα περιοριστούν τα λάθη από τους εργάτες και θα γίνεται σωστή και αξιόπιστη λειτουργία του λογισμικού.

4.7 Διαχείριση ασφάλειας δικτύου

Η πτωχή ανάπτυξη εφαρμογών διαδικτύου, η απενεργοποίηση του firewall και προεπιλεγμένα διαπιστευτήρια σύνδεσης προωθούν την πρόσβαση τρίτων στα εταιρικά δεδομένα παρακολουθώντας την αποστολή μηνυμάτων ή αποκτώντας δικαιώματα. Τρόποι αντιμετώπισης για τις συγκεκριμένες ενέργειες είναι :

- Χρήση Firewall σε όλα τα πληροφοριακά συστήματα. Με την υποστήριξη του περιορίζεται η κίνηση παρακολουθώντας την εισερχόμενη και εξερχόμενη κίνηση και αποφασίζει ποια θα επιτρέψει και ποια θα αποκλείσει.
- Χρήση πρωτοκόλλου TLS το οποίο προστατεύει κρυπτογραφώντας μηνύματα σε όλες τις μεταδόσεις του δικτύου προσφέροντας προστασίας στην επικοινωνία. Η συγκεκριμένη ενέργεια καταφέρεται όταν τα δεδομένα μέσω ενός κλειδιού κρυπτογραφούνται όταν φεύγουν από τον αποστολέα και έπειτα αποκρυπτογράφονται όταν φτάνουν στον παραλήπτη.
- Χρήση του Web Application Firewall, όπου το συγκεκριμένο εργαλείο προστατεύει διαδικτυακές εφαρμογές από κυβερνοεπιθέσεις όπως SQL injections. Βρίσκεται ενδιάμεσα της εφαρμογής και του χρήστη και ελέγχει όλα τα εισερχόμενα αιτήματα και τις εξερχόμενες απαντήσεις.
- Απενεργοποίηση περιττών ενεργειών όπως η απομακρυσμένη διαχείριση ή το UPnP ώστε να υπάρξει μείωση πιθανότητας επίθεσης στους δρομολογητές του εργαστηρίου οι οποίοι προωθούν πακέτα σε όλες τις συσκευές του δικτύου.

4.8 Προστασία από ιομορφικό λογισμικό

Μη ενημερωμένο λογισμικό, λανθασμένη χρήση των συστημάτων και αγνόηση προστασίας τους μεγαλώνουν την πιθανότητα έκθεσης σε ιομορφικό λογισμικό. Η απόκτηση ενός ιού θα προκαλέσει διαταράξεις στην ομαλή λειτουργία του εργαστηρίου και θα προκαλέσει οικονομικές ζημίες. Για την αποτροπή τέτοιων προβλημάτων χρειάζεται :

- Εγκατάσταση antivirus για τον εντοπισμό πιθανών κακόβουλων λογισμικών και την αποφυγή την ζημιών τους. Με την σωστή επιλογή προστατευτικού λογισμικού γίνεται έλεγχος στην κίνηση του διαδικτύου, των εισερχόμενων μηνυμάτων και προσφέρει υποστήριξε σε εισερχόμενους κινδύνους.
- Εκπαίδευση προσωπικού για την σωστή χρήση του διαδικτύου. Είναι απαραίτητα η αποφυγή ύποπτων ιστοσελίδων, ο έλεγχος ύποπτων mail και links ώστε να μια επίθεση γίνει αποδεκτή από τους ίδιους του υπαλλήλους.
- Τακτική ενημέρωση λογισμικού. Με την εγκατάσταση των τελευταίων εκδόσεων του λογισμικού διορθώνονται λάθη που έχουν παρατηρηθεί μέχρι στιγμής και αποφεύγονται κίνδυνοι οι οποίοι μπορούσαν να αξιοποιηθούν από μη εξουσιοδοτημένους χρήστες.

4.9 Ασφαλής χρήση διαδικτυακών υπηρεσιών

Τα συνδεδεμένα συστήματα στο διαδίκτυο βρίσκονται αντιμέτωπα με διάφορους κινδύνους οι οποίοι μπορούν να προκαλέσουν απώλεια δεδομένων. Ο περιορισμός των ευπαθειών γίνεται με :

- Χρήση Firewall σε όλα τα πληροφοριακά συστήματα. Με την υποστήριξη του περιορίζεται η κίνηση παρακολουθώντας την εισερχόμενη και εξερχόμενη κίνηση και αποφασίζει ποια θα επιτρέψει και ποια θα αποκλείσει.
- Χρήση Web Application Firewall για την προστασία διαδικτυακών εφαρμογών. Το συγκεκριμένο εργαλείο ελέγχει την κίνηση μηνυμάτων στο δίκτυο και ρυθμίζει τα εισερχόμενα αιτήματα και τις εξερχόμενες απαντήσεις.

4.10 Ασφάλεια εξοπλισμού

Οι φυσικές ζημιές όπως οι πυρκαγιές και οι πλημμύρες όσο και η παρέμβαση των πελάτων προκαλούν σοβαρά προβλήματα στον χώρο εργασίας. Για τον περιορισμό των ζημιών είναι σημαντική :

- Εγκατάσταση ανιχνευτών καπνού, συναγερμών πυρκαγιάς και πυροσβεστήρες. Έτσι σε περίπτωση πυρκαγιά θα αποτραπεί η καταστροφή ή θα περιοριστούν οι ζημιές.
- Εξόπλιση του εργαστηρίου με αντλίες φρεατίου και ανύψωση αγαθών. Με την συγκεκριμένη ενέργεια υπάρχει προστασία των πολύτιμων στοιχείων σε περίπτωση πλημμύρας και γρήγορη αντιμετώπιση του προβλήματος.
- Τοποθέτηση εξοπλισμού σε χώρους οι οποίοι δεν είναι προσβάσιμοι σε μη εξουσιοδοτημένους χρήστες και παρακολουθούνται συνεχώς. Έτσι υπάρχει αποφυγή κλοπής και ζημιά από εξωτερικούς χρήστες.

4.11 Φυσική ασφάλεια κτιριακής εγκατάστασης

Η τοποθεσία του εργαστηρίου και η συγκεκριμένη δομή των χωρών αυξάνουν τα ενδεχόμενα εισβολής στο εργαστήριο. Επίσης υπάρχει ανάγκη αντιμετώπισης φυσικών ζημιών. Για την επίτευξη των στόχων είναι σημαντική :

- Εγκατάσταση ενός πλήρους συστήματος ασφαλείας. Με κάμερες ασφαλείας θα παρακολουθούνται τα άτομα που χρησιμοποιούν πόρους και αγαθά, σε περίπτωση κλοπής θα υπάρχει παρακολούθηση, έξαρση συναγερμού και άμεση παρέμβαση από την ομάδα ασφάλειας. Επίσης θα υπάρχει αποζημίωση σε περίπτωση κλοπών.
- Προσθήκη αισθητήρων καπνού και πυροσβεστήρων. Έτσι υπάρχει η δυνατότητα αποτροπής πυρκαγιάς αλλά και σε περίπτωση που λάβει χώρο να αντιμετωπιστεί χωρίς να προκαλέσει σοβαρές ζημιές.
- Αξιοποίηση αντλιών φρεατίου σε περίπτωση πλημμύρας ώστε να αποτρέψουμε τις καταστροφές που θα προκληθούν από το νερό.
- Έλεγχος και παρακολούθηση των ατόμων που εισέρχονται στο εργαστήριο και χρήση θωρακισμένων πορτών. Εφόσον είναι τοποθετημένο σε ένα εμπορικό κέντρο και έχει πρόσβαση σε ένα πολυσύχναστο δρόμο είναι σημαντικό να υπάρχει έλεγχος στην είσοδο των ατόμων ώστε να αποτραπούν επικίνδυνα περιστατικά.

*Κάποια μέτρα βρίσκονται σε διάφορες κατηγορίες εφόσον αντιμετωπίζουν πολλαπλά είδη κινδύνων και ευπαθειών.

5 ΣΥΝΟΨΗ ΚΡΙΣΙΜΩΝ ΑΠΟΤΕΛΕΣΜΑΤΩΝ

Η μελέτη που πραγματοποιήθηκε στον χώρο του μικροβιολογικού εργαστηρίου BioAnalytix Lab, οδήγησε στην διαπίστωση ότι υπάρχουν πολλές ευπάθειες και απειλές στα πληροφοριακά του συστήματα. Προκειμένου να διασφαλιστεί η ορθή λειτουργία και η προστασία του εργαστηρίου, είναι απαραίτητη η λήψη ορισμένων μέτρων προστασίας, τουλάχιστον απέναντι στις απειλές με τις υψηλότερες μονάδες επικινδυνότητας της μονάδας RPN (Risk Priority Number). Παρακάτω αναφέρονται οι απειλές με τις υψηλότερες επικινδυνότητες, τα μέτρα που πρέπει να παρθούν, καθώς και οι λόγοι για τους οποίους πρέπει να πραγματοποιηθούν οι παρακάτω αλλαγές στα συστήματα του εργαστηρίου.

- **[1-A014]** Η μη ορθή ρύθμιση των κανόνων του firewall του δικτύου, μπορεί να οδηγήσει στην είσοδο και εκτέλεση κακόβουλων υπηρεσιών στο δίκτυο του εργαστηρίου. Επομένως, το firewall πρέπει να απαγορεύει την είσοδο συγκεκριμένων υπηρεσιών, καθώς διαφορετικά μπορεί να προκύψουν διαρροές δεδομένων τόσο των πληροφοριακών συστημάτων του εργαστηρίου, όσο και προσωπικών δεδομένων των πελατών.
- **[17-A009]** Έλλειψη ταυτοποίησης χρηστών και παρακολούθησης των κινήσεων, είναι πιθανό να επιτρέψει την είσοδο κακόβουλων χρηστών, που θα μπορούν να προκαλέσουν βλάβες στα συστήματα με μεγαλύτερη ευκολία απ' ότι θα έπρεπε. Συνεπώς, είναι απαραίτητη η υλοποίηση ταυτοποίησης χρηστών που συνδέονται στο Web Server, καθώς επίσης και η παρακολούθηση των αρχείων καταγραφής συμβάντων προκειμένου να γίνει έγκαιρα η ανίχνευση οποιασδήποτε κακόβουλης δραστηριότητας.
- **[27-A018]** Συστήματα τα οποία παραμένουν outdated όσον αφορά την έκδοση του λογισμικό τους, αποτελούν μια πολύ σοβαρή ευπάθεια για όλο το δίκτυο στο οποίο ανήκουν. Η εγκατάσταση anti-virus λογισμικού σε όλα τα συστήματα, επιτρέπει την προστασία τους από κακόβουλες εφαρμογές, και επιθέσεις στις οποίες διαφορετικά δεν θα είχαν τρόπο φύλαξης.
- **[28-A019]** Η χρήση ασθενών κωδικών πρόσβασης στα συστήματα του εργαστηρίου μπορεί να προκαλέσει διαρροές δεδομένων, καθώς η πρόσβαση σε αυτά τα συστήματα δεν θα αποτελέσει ιδιαίτερη δυσκολία στον κακόβουλο χρήστη. Η συχνή ενημέρωση των πληροφοριακών συστημάτων στις τελευταίες εκδόσεις των λογισμικών που χρησιμοποιούνε, καθώς και η εγκατάσταση anti-malware λογισμικού, θα προστατεύσουν τα συστήματα από πιθανές επιθέσεις.

Παραπάνω αναφέραμε τις κύριες απειλές, που εκτιμήθηκαν με γνώμονα το δείκτη RPN, του πληροφοριακού συστήματος του εργαστήριου BioAnalytix Lab τα οποία είναι αυτά που πρέπει να αντιμετωπιστούν και να τεθούν σε κατάσταση ασφάλειας άμεσα. Θα θέλαμε να αναφέραμε, εφόσον ληφθούν τα μετρά που έχουμε συστήσει για τις παραπάνω απειλές των αγαθών, τα επόμενα σε προτεραιότητα αγαθά που αντιμετωπίζουν σοβαρές απειλές και θα είναι αυτά που θα πρέπει να έχει στην προσοχή του το σύστημα μετέπειτα στη διαδικασία αντιμετώπισης των απειλών και των ευπαθειών. Αυτά είναι:

- **[18-A010]** Σε περίπτωση μιας καταστροφικής επίθεσης στα πληροφοριακά συστήματα του εργαστηρίου, η έλλειψη αντιγράφων ασφαλείας θα σήμαινε πως δεν θα υπήρχε κανένας τρόπος για να επαναφερθούν τα συστήματα σε προηγούμενη κατάσταση, πριν γίνει η επίθεση. Επομένως, η δημιουργία αντιγράφων ασφαλείας καθώς και η ύπαρξη πλάνου ανάκαμψης του συστήματος σε περίπτωση που πραγματοποιηθεί κάποια επίθεση, θα βοηθούσε πολύ στην αποκατάσταση του συστήματος, και πιθανόν και στην αποκατάσταση χαμένων δεδομένων.
- **[23-A013]** Εσφαλμένη ρύθμιση των κανόνων του firewall θα μπορούσε να δώσει εξουσιοδοτημένη πρόσβαση στον κακόβουλο χρήστη, δίνοντας του την δυνατότητα να κάνει αλλαγές που θα προκαλούσαν προβλήματα στα πληροφοριακά συστήματα του εργαστηρίου. Η πρόσβαση στις ρυθμίσεις του firewall θα πρέπει να είναι περιορισμένη, προκειμένου να μην μπορούν χρήστες εκτός των διαχειριστών να κάνουν αλλαγές στο σύστημα. Επιπλέον, πρέπει να γίνεται συχνή ενημέρωση στην τελευταία έκδοση του firewall, για μεγαλύτερη ασφάλεια στο δίκτυο του εργαστηρίου.
- **[29-A020]** Η ιστοσελίδα του μικροβιολογικού εργαστηρίου δεν χρησιμοποιεί Web Application Firewall (WAF), το οποίο μπορεί να οδηγήσει σε κακόβουλους χρήστες να έχουν πρόσβαση σε προσωπικά δεδομένα πελατών αλλά και δεδομένα του εργαστηρίου. Προκειμένου να αποφευχθεί αυτό, πρέπει να υλοποιηθεί κάποιο WAF, να υλοποιηθεί μια καλύτερη αναπτυξιακή προσέγγιση για την ιστοσελίδα με την χρήση κώδικα, καθώς επίσης και να δημιουργούνται συχνά αντίγραφα ασφαλείας για την ιστοσελίδα, σε περίπτωση που είναι αναγκαία η αποκατάσταση σε μια προηγούμενη κατάσταση της ιστοσελίδας.
- **[39-A020]** Ένας κακόβουλος χρήστης μπορεί να έχει την δυνατότητα να κάνει upload ενός κακόβουλου αρχείου, με την πρόθεση να μολύνει την ιστοσελίδα και να αποκτήσει τον έλεγχο. Με την υλοποίηση ταυτοποίησης των χρηστών που συνδέονται στην ιστοσελίδα, καθώς και παρακολούθησης των κινήσεων που πραγματοποιούν οι χρήστες, είναι εφικτή η αποφυγή κάποιας κακόβουλης δραστηριότητας που διαφορετικά θα προκαλούσε προβλήματα στην λειτουργία της ιστοσελίδας και κατ' επέκταση του εργαστηρίου.
- **[40-A013]** Η χρήση ορισμένων default login credentials μέσω του router, δίνει την δυνατότητα σε κακόβουλους χρήστες να παριστάνουν άλλους χρήστες του συστήματος, προκειμένου να πραγματοποιήσουν κάποια κακόβουλη δραστηριότητα χωρίς να φαίνεται ποιος την κάνει πραγματικά. Αφαιρώντας ορισμένες μη απαραίτητες υπηρεσίες, όπως για παράδειγμα την υπηρεσία UpnP ή και το remote management, μπορούμε να μειώσουμε το attack surface του router, βελτιώνοντας έτσι την ασφάλεια του δικτύου του εργαστηρίου ως σύνολο.