ΟΙΚΟΝΟΜΙΚΟ ΠΑΝΕΠΙΣΤΗΜΙΟ ΑΘΗΝΩΝ

ATHENS UNIVERSITY OF ECONOMICS AND BUSINESS

ΤΜΗΜΑ ΠΛΗΡΟΦΟΡΙΚΗΣ

ΑΣΦΑΛΕΙΑ ΠΛΗΡΟΦΟΡΙΑΚΩΝ ΣΥΣΤΗΜΑΤΩΝ

ΕΡΓΑΣΙΑ ΕΑΡΙΝΟΥ ΕΞΑΜΗΝΟΥ 2023

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

ΠΑΡΟΥΣΙΑΣΗ ΣΧΕΔΙΟΥ ΑΣΦΑΛΕΙΑΣ

Μικροβιολογικού Εργαστηρίου «Χίλμαν»

ΜΕΛΗ ΟΜΑΔΑ ΕΡΓΑΣΙΑΣ:

1. **Μουρελάτου Σάρα + 3200106 + 3200106@aueb.gr**
2. **Μαρκοπούλου Γεωργία + 3200100 + 3200100@aueb.gr**
3. **Φυτάλη Παναγιώτα + 3200215 + 3200215@aueb.gr**

ΠΕΡΙΕΧΟΜΕΝΑ ΕΡΓΑΣΙΑΣ

1. ΕΙΣΑΓΩΓΗ

Σκοπός της εργασίας αυτής είναι η ανάλυση επικινδυνότητας Πληροφοριακών Συστημάτων στο Μικροβιολογικό Εργαστήριο “Χίλμαν”. Η ανάλυση της επικινδυνότητας σε ένα μικροβιολογικό εργαστήριο αποτελεί από τις πιο σημαντικές διαδικασίες, καθώς από αυτή εντοπίζονται τα βασικά σημεία τρωτότητας αλλά και απειλών που μπορεί να επηρεάσουν την λειτουργία του. Η καταγραφή αυτών εξυπηρετεί στην λήψη των απαραίτητων μέτρων, ώστε να επιτευχθεί το επίπεδο ασφαλείας που αρμόζει σε ένα μικροβιολογικό εργαστήριο. Με βάση λοιπόν την περιγραφή που μας δίνεται, την σχετική εικόνα της κάτοψης του κτηρίου, το διάγραμμα συνδέσεων των πληροφοριακών συστημάτων και την αναλυτική καταγραφή του πλήθους των αγαθών που χρησιμοποιεί το σύστημα, μπορούμε να εξάγουμε την ανάλυση της επικινδυνότητας του “Χίλμαν”.

1.1 Περιγραφή Εργασίας

Η επικινδυνότητα ενός συστήματος, γενικότερα, αποδίδεται από το γινόμενο του ενδεχόμενου κινδύνου με την επίπτωση που θα έχει στο ίδιο. Το ενδεχόμενο κινδύνου δίνεται από τις απειλές και τις αδυναμίες, στις οποίες υπόκειται το σύστημα. Οι απειλές και οι αδυναμίες αναφέρονται στις απώλειες ενός ή περισσότερων από τις παραμέτρους που ορίζουν την ασφάλεια ενός πληροφοριακού συστήματος, οι παράμετροι αυτοί είναι ουσιαστικά ότι αξίζει να προστατευθεί για την λειτουργία του συστήματος, δηλαδή τα αγαθά. Η ανάλυση, δηλαδή, της επικινδυνότητας στο “Χίλμαν” θα έχει ως βάση την περιγραφή των αγαθών που έχει εγκατεστημένα και θεωρεί ότι χρήζουν προστασίας. Από την περιγραφή θα εξάγουμε όλα τα χαρακτηριστικά των αγαθών, τα οποία θα δίνουν τις ιδιότητες τις οποίες καλείται το σύστημα να προστατεύσει, καθώς και την αξία τους για το σύστημα. Για να εξάγουμε όμως τον τρόπο προστασίας τους θα πρέπει πρώτα να αξιολογήσουμε τον βαθμό κινδύνου στον οποίο υπόκεινται και τις αδυναμίες και απειλές, από τις οποίες μπορεί να οδηγηθεί το σύστημα σε ανάλογα ρήγματα ασφαλείας/παραβιάσεις. Από τα τελευταία προκαλούνται επιπτώσεις στο σύστημα από τις οποίες τελικά σε συνδυασμό με το αντίστοιχο ενδεχόμενο κινδύνου του αγαθού θα αποδοθεί η επικινδυνότητα του συγκεκριμένου αγαθού. Η συνολική επικινδυνότητα του συστήματος δίνεται ουσιαστικά από την επικινδυνότητα κάθε αγαθού που διαθέτει. Επομένως τα αντίστοιχα μέτρα προστασίας για την ασφάλεια του μικροβιολογικού εργαστηρίου θα εξαχθεί από τα απαραίτητα μέτρα προστασίας για την αντιμετώπιση κάθε απειλής και τρωτότητας αντιμετωπίζει κάθε αγαθό του συστήματος. Αυτά ουσιαστικά είναι τα βήματα της Ανάλυσης Επικινδυνότητας Πληροφοριακών Συστημάτων στο Μικροβιολογικό Εργαστήριο “Χίλμαν”.

1.2 Δομή παραδοτέου

Αρχικά έχουμε εντάξει στο ανεβασμένο φάκελο ένα αρχείο Excel με τίτλο «», στο οποίο ουσιαστικά αναφέρουμε συγκεκριμένα για τα αγαθά εγκατάστασης ορισμένες απειλές και ευπάθειες που τις διέπουν καθώς και τις ιδιότητες τους. Από αυτά τα δεδομένα εξάγουμε το μέγεθος της επικινδυνότητας στο οποίο υπόκειται κάθε αγαθό, όπως και το κατά πόσο πιθανό είναι να παρουσιαστούν οι επιπτώσεις που θα

προκληθούν στο σύστημα και καταλήγουμε στο μέγεθος του κινδύνου που μπορεί να έχει κάθε αγαθό στο σύστημα.

Στην ενότητα 1 βρίσκεται μία σύντομη περιγραφή του σκοπού εκπόνησης της συγκεκριμένης εργασίας.

Στην ενότητα 2 με χρήση και του σχετικού αρχείου Excel με τα αγαθά της εγκατάστασης περιγράψαμε συνοπτικά τους λόγους που το καθένα αποτελεί αγαθό για το σύστημα, δηλαδή την σημαντικότητα τους στην λειτουργία αυτού. Συμπληρώσαμε επίσης με βάση την περιγραφή που μας δόθηκε αλλά στοιχεία, τα οποία δεν έχουν αναφερθεί, που αξίζει να προστατευθούν λόγω του σημαντικού τους ρόλου στην ορθή λειτουργία του συστήματος (2.1). Έγινε, επιπλέον, μία σύντομη αναφορά στις βασικές δομές (2.2-2.6) που σχηματίζουν τελικά το πληροφοριακό μας σύστημα.

Στην ενότητα 3 περιγράφονται αναλυτικά τα αγαθά που αναφέρθηκαν στην προηγούμενη ενότητα, αυτό σημαίνει ανάλυση του ρόλου, της αξίας τους (στο συνολικό σύστημα) και των χαρακτηριστικών τους, δηλαδή τις ιδιότητες τους (3.1). Αναλύουμε, επίσης, τις απειλές που εντοπίζονται ανά αγαθό (3.2) καθώς και τις αδυναμίες του συστήματος σε αντιστοιχία με τα αγαθά (3.3). Τέλος, από τις παραπάνω αναλύσεις εξάγεται η τελική αποτίμηση κάθε αγαθού, δηλαδή ποια θα είναι η επίπτωση του ρήγματος ασφαλείας κάθε αγαθού στο τελικό σύστημα και ποια η επικινδυνότητα κάθε αγαθού. Το δεύτερο ζητούμενο είναι αποτέλεσμα του γινομένου του ενδεχόμενου κινδύνου του αγαθού με την επίπτωση αυτού στο σύστημα (3.4).

Στην ενότητα 4 δίνονται τα απαραίτητα μέτρα προστασίας του συστήματος, στα οποία καταλήγουμε με βάση την μελέτη με σκοπό την μείωση του ενδεχόμενου κινδύνου στον οποίο υπόκειται κάθε αγαθό καθώς και την μείωση της συνολικής επικινδυνότητας του συστήματος. Από την μελέτη αυτή θα εκλάβουμε τις απαιτήσεις που πρέπει να πληροί το σύστημα, δηλαδή την προσθήκη των απαραίτητων στοιχείων για την κάλυψη οποιουδήποτε απομένον κίνδυνο με βάση τα μέτρα προστασίας που προτάθηκαν για τα αγαθά, καθώς και τα απαραίτητα μέτρα που πρέπει να παρθούν για την εξασφάλισης της ασφάλειας, τελικά, του συστήματος. Τα μέτρα αυτά, και αυτά που αναφέρονται στα αγαθά αλλά και τα γενικότερα μέτρα προστασίας τα χωρίζουμε με βάση τις κατηγορίες που μας δόθηκαν.

Στην ενότητα 5 ουσιαστικά βρίσκεται το συμπέρασμα που εξάγεται από τις προκείμενες αναλύσεις, καθώς και μία σύντομη επισήμανση των κρίσιμων στοιχείων, δηλαδή των αγαθών της εγκατάστασης με πολύ υψηλή επικινδυνότητα, που πρέπει να ληφθούν υπόψη από την Διοίκηση του Μικροβιολογικού εργαστηρίου, ώστε να λάβει τα απαραίτητα μέτρα που προτάθηκαν.

Στο τέλος, επίσης, του αρχείου βρίσκονται οι πηγές που χρησιμοποιήσαμε κατά την εκπόνηση της εργασίας.

2. ΜΕΘΟΔΟΛΟΓΙΑ ΜΕΛΕΤΗΣ ΑΣΦΑΛΕΙΑΣ

Για τη Διαχείριση Επικινδυνότητας του “Χίλμαν” 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.

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

- 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 “Χίλμαν”.
Η σύντομη περιγραφή των αγαθών που βρίσκονται στο Excel “ MicroLab_Asset Inventory_2023” και η προσθήκη 3 επιπλέον αγαθών που περιλαμβάνει το σύστημα μαζί με την σχετική τους περιγραφή παρατίθεται παρακάτω:

A-001 LabWS001

Το συγκεκριμένο αγαθό είναι ένας αιματολογικός αναλυτής, βρίσκεται στον χώρο του Εργαστηρίου-Παρασκευαστηρίου, χρησιμοποιείται από το προσωπικό του εργαστηρίου και ανήκει στην κατηγορία του υπολογιστικού συγκροτήματος διότι αποτελείται από ένα σύνολο ιδιόκτητου λογισμικού (proprietary software) και υλικού εξοπλισμού και χρησιμοποιείται για να επεξεργασθεί τα δείγματα των ασθενών . Πιο συγκεκριμένα είναι αυτοματοποιημένο μηχάνημα μέτρησης του αριθμού διαφορετικών ειδών λευκών και ερυθρών αιμοσφαιρίων σε ένα δείγμα αίματος. Τα αποτελέσματα που παρέχει είναι γνωστά ως αιματολογικές μετρήσεις (CBC) ή αιματολογική εξέταση με διαφοροποίηση κυττάρων (CBCs με diff) και αποτελεί αγαθό ύψιστης αξίας και χρηματικής και πρακτικής για το εργαστήριο ,καθώς χωρίς

αυτό δεν θα μπορούσε να παρέχει την κεντρική υπηρεσία για την οποία δημιουργήθηκε .

A-002 PCWS001

Αυτό το αγαθό είναι ένας από τους σταθμούς εργασίας που διαθέτει το εργαστήριο και βρίσκεται στον χώρο του Εργαστηρίου-Παρασκευαστηρίου. Πρόκειται για έναν υπολογιστή που συνδέεται στο δίκτυο του εργαστηρίου και χρησιμοποιείται από το προσωπικό του εργαστηρίου αρχικά για την μεταξύ του επικοινωνία μέσω Web Server και δευτερευόντως ως βοηθητικός παράγοντας στην διαδικασία της αιματολογικής ανάλυσης και στην αυτόματη καταχώρηση των αποτελεσμάτων της, η οποία επιτυγχάνεται μέσω της σύνδεσης με την βάση δεδομένων της ORACLE στον Database server του εργαστήριου που εγκαθιδρύεται μέσω των switches και του router.Εντάσσεται στην κατηγορία του υπολογιστικού πόρου καθώς χρησιμοποιείται από το υπολογιστικό σύστημα του Εργαστηρίου-Παρασκευαστηρίου και διαχειρίζεται τα αιματολογικά αποτελέσματα.

A-003 PCWS002

Αυτό το αγαθό είναι ο δεύτερος σταθμός εργασίας του Εργαστηρίου-Παρασκευαστηρίου και αποτελεί όπως και το αγαθό A-002 έναν υπολογιστή που χρησιμοποιείται από το προσωπικό του εργαστηρίου αφενός για την μεταξύ του επικοινωνία μέσω Web Server και αφετέρου ως αρωγός στην ανάλυση των αιματολογικών δειγμάτων . Εντάσσεται κι αυτό στην κατηγορία του υπολογιστικού πόρου και είναι και τα δύο αγαθά υψηλής αξίας για το εργαστήριο καθώς συνεισφέρουν στην διεξαγωγή της σημαντικότερης λειτουργίας του.

A-004 PCWS003

Το συγκεκριμένο αγαθό είναι ο σταθμός εργασίας στον χώρο λήψης δειγμάτων και αποτελεί έναν υπολογιστή που επίσης συνδέεται στο δίκτυο του εργαστηρίου μέσω Web Server και τον διαχειρίζεται το προσωπικό του εργαστηρίου ,μέσω του οποίου επικοινωνεί με το υπόλοιπο προσωπικό του εργαστηρίου. Επίσης μέσω αυτού του υπολογιστή μεταφέρεται στην βάση δεδομένων του εργαστηρίου το αρχείο των δειγμάτων. Εντάσσεται στην κατηγορία του υπολογιστικού συγκροτήματος καθώς χρησιμοποιείται για την επεξεργασία και καταγραφή των δεδομένων των δειγμάτων και την αρχική καταχώρηση τους στο σύστημα του εργαστηρίου. Η αξία του είναι σημαντική καθώς η λειτουργία που εκτελεί αποτελεί αναπόσπαστο κομμάτι της όλης διαδικασίας ανάλυσης των δειγμάτων.

A-005 PCWS004

Το αγαθό αυτό είναι ο σταθμός εργασίας στην αίθουσα αναμονής και αποτελεί έναν υπολογιστή μέσω του οποίου η γραμματεία που τον διαχειρίζεται μπορεί να επικοινωνεί με το υπόλοιπο προσωπικό του εργαστηρίου ,να διαχειρίζεται τα ραντεβού των πελάτων , να καταχωρεί τα στοιχεία των πελατών, των προμηθευτών και των εργαζομένων του εργαστηρίου και να επικοινωνεί με την βάση δεδομένων της ORACLE στον Database server του εργαστήριου, μέσω των switches και του router , έτσι ώστε να ανακτά καινούργια και παλαιότερα αποτελέσματα εξετάσεων ασθενών , τα οποία θα μπορεί να στείλει στους ασθενείς ύστερα από αίτημα τους ,μέσω email ή fax. Το αγαθό εντάσσεται στην κατηγορία του υπολογιστικού συγκροτήματος καθώς επεξεργάζεται όλες τις πληροφορίες που αναλύθηκαν παραπάνω και είναι σημαντικής αξίας καθώς αποτελεί τον συντονιστικό παράγοντα του εργαστηρίου και εκτός από αυτό μέσω αυτού ο χρήστης αποκτά πρόσβαση σε ευαίσθητες προσωπικές πληροφορίες (πελατών και προσωπικού) υψηλής αξίας.

A-006 PCWS005

Το αγαθό αυτό είναι ο σταθμός εργασίας στο γραφείο ιατρού και αποτελεί έναν υπολογιστή μέσω του οποίου ο ιατρός ,που είναι ο χρήστης του, συνδέεται στο δίκτυο

υπολογιστών του εργαστηρίου και έχει πρόσβαση στις πληροφορίες που βρίσκονται αποθηκευμένες στην βάση δεδομένων του εργαστηρίου. Εντάσσεται στην κατηγορία του υπολογιστικού πόρου καθώς διαχειρίζεται πληροφορίες και είναι ύψιστης αξίας για το εργαστήριο καθώς μέσω αυτού του υπολογιστή γίνεται εβδομαδιαίως λήψη των αντιγράφων ασφαλείας των δεδομένων των πελατών, εξετάσεων ,προμηθευτών και υπαλλήλων .

A-007 PR0001

Το αγαθό αυτό βρίσκεται στην αίθουσα αναμονής και είναι ένας εκτυπωτής που συνδέεται στο δίκτυο υπολογιστών του εργαστηρίου και τον διαχειρίζεται η γραμματεία. Μέσω αυτού μπορούν να σταλούν με fax τα αποτελέσματα των αναλύσεων στους πελάτες και να εκτυπωθούν τα δεδομένα των αρχείων πελατών, προμηθευτών και υπαλλήλων έτσι ώστε να αρχειοθετηθούν στα ερμάρια των κρεμαστών φακέλων που βρίσκονται στο εργαστήριο . Ο εκτυπωτής χρησιμοποιείται επίσης για την εκτύπωση αποδείξεων και τιμολογίων των πελατών . Εντάσσεται στην κατηγορία του υπολογιστικού αντικειμένου καθώς αποτελεί εξάρτημα (εξοπλισμό).

A-008 PR0002

Το αγαθό αυτό βρίσκεται στο γραφείο ιατρού και είναι ένας εκτυπωτής που συνδέεται στο δίκτυο υπολογιστών του εργαστηρίου και τον διαχειρίζεται ο ιατρός. Μέσω αυτού του εκτυπωτή ο ιατρός εκτυπώνει τα αντίγραφα ασφαλείας των αρχείων των πελατών, εξετάσεων ,προμηθευτών και υπαλλήλων , τα οποία αρχειοθετεί στις αντίστοιχες βιβλιοθήκες του εργαστήριο. Επίσης μπορεί να εκτυπώνει συνταγές ασθενών. Εντάσσεται στην κατηγορία του υπολογιστικού αντικειμένου καθώς αποτελεί εξάρτημα (εξοπλισμό).

Αγαθό A-009 Web Server

Το αγαθό Web Server είναι το υλισμικό (hardware) που επιτρέπει μέσω της επικοινωνίας με το Internet να μοιράζονται δεδομένα τα συστήματα που είναι συνδεδεμένα στο Server. Είναι απαραίτητο, δηλαδή η αξία του είναι υψηλή, για το εργαστήριο, διότι με την ύπαρξη αυτού γίνεται δυνατή η μεταξύ τους επικοινωνία αλλά και με ό,τι βρίσκεται στο Internet. Επομένως το συγκεκριμένα αγαθό μπορεί να αντιπροσωπευτεί από τον όρο υπολογιστικό συγκρότημα, καθώς είναι ένα υλισμικό (με την μορφή που μας δίνεται στον βοηθητικό χώρο) το οποίο χρησιμοποιείται προκειμένου να επεξεργασθεί πληροφορίες.

Αγαθό A-010 Database Server

Το αγαθό Database Server είναι το υλισμικό που επιτρέπει, μέσω του εγκατεστημένου λογισμικού της, την δημιουργία και διαχείριση μία ή περισσότερων βάσεων δεδομένων. Η ύπαρξη μίας βάσης δεδομένων είναι πολύ σημαντική για την αποθήκευση μεγάλου όγκου δεδομένων, όπως είναι αυτά που καλείται να διαχειριστεί ένα εργαστήριο (Υψηλή αξία αγαθό). Το συγκεκριμένα αγαθό, όμοια με το αγαθό A-009, περιγράφεται και με τον όρο υπολογιστικό συγκρότημα υλισμικό (με την μορφή που μας δίνεται στον βοηθητικό χώρο).

Αγαθά A-011 A-012 Switches

Το αγαθό Switch είναι ουσιαστικά μία συσκευή που εξυπηρετεί στην ανταλλαγή πληροφοριών μεταξύ των υπολογιστών/συσκευών που είναι συνδεδεμένοι πάνω σε αυτόν, αποτελεί δηλαδή αγαθό δικτύου. Η αξία αυτού του αγαθού με βάση δικτυακό διάγραμμα συνδέσεων είναι σημαντική καθώς με αυτό συνδέονται όλοι οι υπολογιστές του εργαστηρίου για να επικοινωνούν. Η ύπαρξη του switch προσφέρει ταχύτερη σύνδεση στο internet , μέσω του συνδεδεμένου με αυτό ethernet και άμεση και ασφαλέστερη (δυσκολότερη η ανεπιθύμητη είσοδο στο δίκτυο) ανταλλαγή αρχείων και πληροφοριών μεταξύ υπολογιστών.

Αγαθό A-013 Router

Το αγαθό Router χρησιμοποιείται, με βάση και την τοποθεσία που βρίσκεται(αίθουσα αναμονής), για να συνδέει διαφορετικές συσκευές στο Internet αλλά με βάση το δικτυακό διάγραμμα συνδέσεων, συνδέεται και στους switchers που έχουν συνδεδεμένα και τις άλλες συσκευές του εργαστηρίου, κάνοντας έτσι επιτακτική την ανάγκη προστασίας του δικτύου από ενδεχόμενες επιθέσεις . Η αξία αυτού, λόγω της ύπαρξης του Web Server δεν είναι τόσο ουσιαστική, αφού αποτελεί ένα επιπλέον αγαθό για προστασία χωρίς να είναι τόσο απαραίτητο.

Αγαθό A-014 Firewall

Το αγαθό Firewall χρησιμοποιείται για την προστασία του δικτύου και των υπολογιστών από επιθέσεις ή προσπάθεια εισόδου σε μη επιτρεπτές ή μη εξουσιοδοτημένες, για τον χρήστη, εφαρμογές. Είναι πολύ σημαντικό αγαθό και μπορεί να εκφραστεί και με τον όρο υπολογιστικός πόρος καθώς χρησιμοποιείται από ένα υπολογιστικό σύστημα προκειμένου να του επιτρέψει να διαχειριστεί πληροφορίες.

Αγαθό A-015 Laptop

Το αγαθό αυτό, το οποίο βρίσκεται στο γραφείο του ιατρού, δηλαδή το διαχειρίζεται ο ίδιος, είναι ένα από τα μέσα που έχει ο ιατρός να ενημερωθεί, να επικοινωνήσει, να επεξεργαστεί πληροφορίες που είναι εξουσιοδοτημένος, κτλ. Με άλλα λόγια το αγαθό αυτό παρέχει στον ιατρό την δυνατότητα εισόδου στο σύστημα του εργαστηρίου. Η ύπαρξη και του αγαθού A-006 κάνει την ύπαρξη αυτού χαμηλότερης αξίας από ότι στην πραγματικότητα θα είχε αν ήταν το μόνο μέσο για την είσοδο του στο σύστημα.

A-016 Customer Data

Το αγαθό A-16 ανήκει στην κατηγορία των δεδομένων, είναι δηλαδή ένα σύνολο από σύμβολα που έχουν καταγραφεί. Πιο συγκεκριμένα είναι τα δεδομένα των πελατών τα οποία ειδικά σε ένα μικροβιολογικό εργαστήριο έχουν μεγάλη αξία εφόσον μπορούν να παραβιαστούν προσωπικά δεδομένα σε περίπτωση απώλειας τους, όπως επίσης και να χαθούν σημαντικές πληροφορίες που χρειάζονται οι πελάτες του εργαστηρίου.

A-017 Employee Data

Όπως και το προηγούμενο αγαθό έτσι κι αυτό ανήκει στην κατηγορία των δεδομένων και πιο συγκεκριμένα είναι το αρχείο των υπαλλήλων, το οποίο είναι απαραίτητο για το εργαστήριο εφόσον είναι πληροφορίες σχετικά με τους εργαζόμενους του και σε περίπτωση απώλειας μπορούν να παραβιαστούν τα προσωπικά τους δεδομένα.

A-018 Windows 7 pro

Το αγαθό A-018 ανήκει στην κατηγορία των υπολογιστικών συγκροτημάτων εφόσον είναι ένα λειτουργικό σύστημα της Microsoft που χρησιμοποιεί το εργαστήριο για να επεξεργασθεί πληροφορίες. Βρίσκεται στους 2 Switchers και για αυτόν τον λόγο είναι απαραίτητο να προστατευθεί με σκοπό να μπορούν όλες οι συσκευές του εργαστηρίου να επικοινωνούν και να ανταλλάσσουν πληροφορίες μεταξύ τους.

A-019 Windows 10 pro

Παρόμοια με το προηγούμενο αγαθό, το αγαθό A-019 ανήκει στην κατηγορία των υπολογιστικών συγκροτημάτων αφού κι αυτό είναι ένα λειτουργικό σύστημα. Το λειτουργικό αυτό σύστημα χρησιμοποιείται σε 5 Workstations και για τον λόγο αυτό, μια ζημιά σε αυτό θα κοστίσει πολύ στο εργαστήριο εφόσον οι workstations δεν θα μπορούν να επεξεργάζονται πλέον πληροφορίες και θα χρειάζεται η αντικατάστασή του.

Α-020 Website

Το αγαθό αυτό ανήκει στην κατηγορία των υπολογιστικών συγκροτημάτων εφόσον είναι μια ιστοσελίδα η οποία μοιράζεται πληροφορίες με τους επισκέπτες της. Το να διατηρηθεί ασφαλής αυτή η ιστοσελίδα είναι πολύ σημαντικό από την άποψη ότι περιέχει δεδομένα των πελατών του που γίνονται διαθέσιμα με τους κωδικούς του κάθε πελάτη.

Α-021 Φυσικό αρχείο ασθενών

Το φυσικό αρχείο ασθενών αποτελεί ένα αγαθό γιατί η αξία του είναι χαμηλότερη από το αγαθό Α-016 το οποίο έχει τα ίδια δεδομένα. Τα αρχεία αυτά χρησιμοποιούνται μόνο και μόνο για να κάνουν την δουλειά της γραμματείας πιο εύκολη και είναι εύκολο με χαμηλό κόστος να τα επαναφέρουμε. Ανήκει στην κατηγορία των δεδομένων και είναι τα δεδομένα των πελατών του εργαστηρίου.

Α-022 Αρχείο Υπαλλήλων και Προμηθευτών

Το αγαθό αυτό κρατάει σε έντυπη μορφή τα δεδομένα που υπάρχουν στο αγαθό Α-016, συνεπώς ανήκει κι αυτό στην κατηγορία των δεδομένων. Το αρχείο αυτό περιέχει πληροφορίες που μόνο το εργαστήριο θα έπρεπε να έχει και βοηθάει την γραμματεία στην δουλειά της. Η αξία του δεν είναι όμως τόσο υψηλή όσο του αγαθού Α-017 που έχει τα ίδια δεδομένα.

Α-023 Χημικές Ουσίες

Οι χημικές ουσίες που βρίσκονται στον βοηθητικό χώρο είναι απαραίτητες για τα αντιδραστήρια του εργαστηρίου και επομένως είναι σημαντικές για την ανάλυση των εξετάσεων αυτών. Για τον λόγο αυτόν αποτελούν ένα αγαθό που πρέπει να προστατευθεί με αρκετά υψηλή αξία αφού είναι δύσκολο να αντικατασταθούν και από οικονομικής άποψης. Οπότε από την στιγμή που χρησιμοποιείται για να δώσει μια πληροφορία (τα αποτελέσματα των εξετάσεων) ανήκει στην κατηγορία των υπολογιστικών πόρων.

Α-024 Ιστορικό Εξετάσεων

Το ιστορικό των εξετάσεων είναι ένα αγαθό που εμπίπτει στην κατηγορία των Πληροφοριών διότι είναι δεδομένα που συνοδεύονται από την σημασία τους και η αξία του είναι μεγάλη καθώς αφορά πληροφορίες ιατρικού απορρήτου που σε καμία περίπτωση δεν πρέπει να διαρρεύσουν και είτε να δημοσιοποιηθούν είτε να γίνουν αντικείμενο εκμετάλλευσης. Το αγαθό αυτό βρίσκεται αποθηκευμένο στην βάση δεδομένων του εργαστηρίου καθώς και στα αντίγραφα ασφαλείας που κρατά ο ιατρός στο γραφείο του και περιέχει τα αποτελέσματα των αιματολογικών εξετάσεων, μαζί με την ημερομηνία και ώρα διεξαγωγής τους, κάθε πελάτη του εργαστηρίου . Το ιστορικό αυτό το διαχειρίζονται και το επεξεργάζονται οι υπεύθυνοι της αιματολογικής ανάλυσης και έχουν πρόσβαση με δικαίωμα read only η γραμματεία και ο ιατρός (δηλαδή δεν έχουν δικαίωμα τροποποίησης του).

Αγαθό Α-025 Δείγμα

Το αγαθό δείγμα είναι ουσιαστικά ένα από τα σημαντικότερα αγαθά του εργαστηρίου καθώς σε αυτό βασίζεται η λειτουργία του εργαστηρίου. Η συλλογή και η ανάλυση των δειγμάτων είναι οι διαδικασίες που δίνουν τα τελικά αποτελέσματα. Επομένως είναι εμφανές ότι χωρίς την ύπαρξη των δειγμάτων ο υπολογισμός των ζητούμενων αποτελεσμάτων θα ήταν αδύνατος και αυτό προσδίδει στο αγαθό τόσο υψηλή αξία. Για το σύστημα μας το αγαθό αυτό μπορεί να εκφρασθεί και με τον όρο υπολογιστικός πόρος, αφού χρησιμοποιείται από αυτό (το σύστημα του εργαστηρίου) προκειμένου να του επιτρέψει να διαχειριστεί πληροφορίες. Η θέση του αγαθού δεν μπορεί να προσδιοριστεί ακριβώς αφού η απολαβή του συγκεκριμένου αγαθού γίνεται στο χώρο λήψης δειγμάτων ενώ η ανάλυση του ,που ουσιαστικά θα μας δώσει τα ζητούμενα αποτελέσματα, γίνεται στο εργαστήριο-παρασκευαστήριο.

2.2 Εξοπλισμός & Υλισμικό (hardware)

Το εργαστήριο είναι εξοπλισμένο με μηχανήματα και υλισμικό σύγχρονης τεχνολογίας για να μπορεί καθημερινά να εκτελεί ορθά και ομαλά τις διαδικασίες του και να ανταποκρίνεται στις απαιτήσεις των πελατών του. Όσον αφορά τον εξοπλισμό του αρχικά καταγράφηκαν 5 σταθμοί εργασίας ,δηλαδή υπολογιστές , και ένα laptop ,μέσω των οποίων επιτυγχάνεται η επικοινωνία μεταξύ του προσωπικού αφού με την βοήθεια των switches και του router, που αποτελούν κομμάτι του εξοπλισμού, αλλά και του Web Server,που αποτελεί μέρος του υλισμικού συνδέονται όλοι στο ίδιο δίκτυο. Ακόμα μέσω αυτών των υπολογιστών παρέχεται στο προσωπικό και πρόσβαση στην βάση δεδομένων του εργαστηρίου ,στην οποία είναι αποθηκευμένα τα σημαντικά του αρχεία (πελατων, εξετάσεων, προμηθευτών, υπαλλήλων) και στην οποία συνδέονται μέσω του Database Server που αποτελεί κομμάτι του υλισμικού του εργαστηρίου. Επίσης οι σταθμοί εργασίας που βρίσκονται στον χώρο του Εργαστηρίου-Παρασκευαστηρίου βοηθούν στο έργο της ανάλυσης των δειγμάτων των ασθενών σε συνεργασία με τον αιματολογικό αναλυτή που συνιστά το σημαντικότερο και πιο δύσκολα αντικαταστάσιμο κομμάτι εξοπλισμού που διαθέτει το εργαστήριο . Στον εξοπλισμό προστίθενται οι χημικές ουσίες που φυλάσσονται στον βοηθητικό χώρο και είναι απαραίτητες για την ανάλυση των δειγμάτων, τα φιαλίδια των δειγμάτων, καθώς και οι εκτυπωτές μέσω των οποίων εκτυπώνονται τα απαραίτητα παραστατικά (αποδείξεις/τιμολόγια) για τους πελάτες αλλά και αντίγραφα των εγγράφων που υπάρχουν στην βάση δεδομένων έτσι ώστε σε περίπτωση failure του συστήματος να υπάρχουν και σε έντυπη μορφή. Επίσης με την βοήθεια των εκτυπωτών στέλνονται με fax τα αποτελέσματα των εξετάσεων στους πελάτες που το επιθυμούν. Τέλος στον βοηθητικό χώρο υπάρχει αισθητήρας πυρανίχνευσης και φορητός πυροσβεστήρας ξηράς κόνεως για την προστασία έναντι κινδύνου πυρός από εύφλεκτα υλικά και τοξικές ουσίες.

2.3 Λογισμικό και εφαρμογές

Το εργαστήριο καθημερινά απασχολείται με ένα μεγάλο πλήθος διεργασίων, από τις οποίες οι περισσότερες υποστηρίζονται με κάποιο λογισμικό που είτε διευκολύνει την εκτέλεση τους είτε είναι αναγκαίο για την εκτέλεση τους. Αρχικά, όπως είδαμε και στην λίστα των αγαθών, πρέπει να υπάρχει λογισμικό κατάλληλο για να εξυπηρετεί τα αρχεία με τα οποία είναι κατασκευασμένη μία ιστοσελίδα αλλά και να επιτρέπει τον διαμοιρασμό δεδομένων στις συσκευές που είναι συνδεδεμένες στον Web Server (το οποίο «προσφέρεται» από το Web Server που είναι εγκατεστημένο στο εργαστήριο). Η ύπαρξη, λοιπόν, του λογισμικού Web Server επιτρέπει την προβολή, την δημιουργία, την επεξεργασία και την γενικότερη διαχείριση της ιστοσελίδας του εργαστηρίου, ενώ υποστηρίζει την σύνδεση με το ηλεκτρονικό ταχυδρομείο, για την διανομή αποτελεσμάτων και αναφορών . Παράλληλα καθιστά δυνατή την επικοινωνία μεταξύ των μικροβιολογικών αναλυτών του εργαστηρίου, αλλά και την επικοινωνία με άλλους παρόχους υπηρεσιών (μέσω δικτύου). Επιπλέον πρέπει να διαθέτει λογισμικό, που επιτρέπει την διαχείριση της βάσης δεδομένων ORACLE, που προσφέρεται από την εγκατάσταση του Database Server. Το ορισμένο λογισμικό παρέχει δυνατότητες καταχώρησης, στην κοινή βάση, αποτελεσμάτων, ιστορικού εξετάσεων, αρχείου πελατών, προμηθευτών και υπαλλήλων. Το λογισμικό του συστήματος, ουσιαστικά παρέχει τις δυνατότητες των λογισμικών που προσφέρονται από την ύπαρξη Web Server και Database Server ενώ ταυτόχρονα υποστηρίζει την διεξαγωγή ορισμένων σταδίων διενέργειας των διαγνωστικών εξετάσεων (αυτό το γεγονός κάνει αυτά τα στάδια να θεωρούνται αυτοματοποιημένα), δίνει τις αντίστοιχες δυνατότητες κατά την σύνδεση εκτυπωτή ή fax με τις συσκευές καθώς και την δυνατότητα λήψης αντιγράφων ασφαλείας των πληροφοριών.

Όσον αφορά της εφαρμογές του εργαστηρίου θα βοηθούσε πρώτα να θέσουμε τι εννοούμε με την έννοια εφαρμογή. Με τον όρο εφαρμογή εννοούμε το σύνολο των πληροφοριών, λογισμικού και διαδικασιών, σχεδιασμένων προκειμένου να εκπληρώσουν ένα συγκεκριμένο σύνολο στόχων. Επομένως οι εφαρμογές του συστήματος μας περιγράφονται από το εγκατεστημένο λογισμικό, που αναφέραμε παραπάνω, τις διαδικασίες του συστήματος, που θα παρουσιάσουμε αργότερα και το σύνολο των πληροφοριών, το οποίο περιγράφεται από τα δεδομένα που βρίσκονται στην βάση δεδομένων ORACLE και την αντίστοιχη σημασία τους.

2.4 Δίκτυο

Ένα δίκτυο αποτελείται από κόμβους, οι οποίοι περιγράφουν οτιδήποτε είναι συνδεδεμένο στο δίκτυο, από τμήματα, που είναι κάθε μέρος του δικτύου που διαχωρίζεται από το υπόλοιπο δίκτυο μέσω switch, router και από το backbone, δηλαδή την κύρια σύνδεση των καλωδίων του δικτύου στην οποία συνδέονται όλα τα τμήματα. Το δίκτυο του εργαστηρίου περιγράφει ένα τοπικό δίκτυο, το οποίο σημαίνει ότι έχει έναν κόμβο που χρησιμοποιείται σαν «πύλη» (gateway) για την επίτευξη της επικοινωνίας με άλλα δίκτυα, ο οποίος στην περίπτωσή μας είναι το router που επικοινωνεί με το ISP Cloud αλλά και ο κόμβος του Web Server, ο οποίος παρέχει σύνδεση με τις σελίδες Web. Σύμφωνα με το δικτυακό διάγραμμα συνδέσεων των πληροφοριακών συστημάτων μπορούμε να αντιληφθούμε το δίκτυο του συστήματος μας. Οι κόμβοι δικτύου είναι ουσιαστικά όλες οι συνδεδεμένες συσκευές, οι οποίες διακρίνονται στα αγαθά τύπου Workstation: Laptop, Εκτυπωτές, Haematology analyser και οι υπόλοιποι υπολογιστές, οι οποίοι χρησιμοποιούνται από το προσωπικό για την διαπεραίωση των εργασιών τους και στα αγαθά εξυπηρετητών (servers), δηλαδή τον Database και Web Server. Τα τμήματα, με βάση τον ορισμό που δώσαμε, στο σύστημα μας είναι 2 και τα δύο σχηματίστηκαν εξαιτίας της ύπαρξης switch. Το 1ο τμήμα είναι αυτό που περιλαμβάνει τους κόμβους αγαθών workstation ενώ το 2ο τμήμα είναι αυτό που περιλαμβάνει τους κόμβους εξυπηρετητών (Το αγαθό Firewall στο δίκτυο του συστήματος λειτουργεί προστασία από απειλές και δεν θεωρείται κόμβος). Το backbone του δικτύου μας είναι ουσιαστικά η σύνδεση των switchers με το router.

2.5 Δεδομένα

Το εργαστήριο έχει αποθηκευμένα τα δεδομένα των υπαλλήλων του στην βάση δεδομένων “Employee Data” καθώς και σε φυσικό αρχείο σε ένα ερμάριο της ανοιχτής βιβλιοθήκης που υπάρχει στην αίθουσα αναμονής. Εκτός από τα δεδομένα των υπαλλήλων του χρειάζονται επίσης τα δεδομένα των προμηθευτών και τα δεδομένα των πελατών του. Αυτά αποθηκεύονται σε αντίστοιχες βάσεις δεδομένων. Για παράδειγμα, το αρχείο των πελατών αποθηκεύεται στην βάση δεδομένων “Customer Data”. Τα αρχεία αυτά είναι επίσης αποθηκευμένα σε έντυπη μορφή σε ένα ερμάριο της ανοιχτής βιβλιοθήκης που υπάρχει στο γραφείο του γιατρού με σκοπό την διευκόλυνση της γραμματείας. Κάποια άλλα δεδομένα που συλλέγει το εργαστήριο και είναι πολύ σημαντικά είναι το ιστορικό των εξετάσεων των ασθενών που αποθηκεύονται κι αυτά σε βάση δεδομένων. Τέλος, αποθηκεύει αντίγραφα όλων αυτών των δεδομένων που βρίσκονται στο γραφείο του ιατρού. Πρέπει να αναφερθεί ότι το εργαστήριο πολλές φορές μοιράζεται αυτά τα δεδομένα με εξωτερικούς συνεργάτες χωρίς να έχει πάρει την συναίνεση των πελατών του.

2.6 Διαδικασίες

Η πρώτη διαδικασία που παρατηρούμε να γίνεται είναι η αποθήκευση των δεδομένων υπαλλήλων, προμηθευτών και πελατών του εργαστηρίου. Όταν ο πελάτης θέλει να δει τα αποτελέσματα των εξετάσεων του και μπει στην ιστοσελίδα, πρέπει να ακολουθήσει η διαδικασία διαπίστευσης συστήματος χρήστη έτσι ώστε να του δώσει το σύστημα τα δεδομένα που χρειάζεται. Άλλη μία διαδικασία του εργαστηρίου με το οποίο ασχολούμαστε είναι η διαδικασία της δειγματοληψίας και της λήψης των

αποτελεσμάτων η οποία απαιτεί ταυτοποίηση του πελάτη για να αποθηκευτούν στην σωστή βάση δεδομένων. Στην συνέχεια, την αποστολή των αποτελεσμάτων στους πελάτες που είναι πολύ σημαντικό να σταλθεί στο email που πρέπει και όχι σε κάποιου άλλου. Τέλος, έχουμε την λήψη αντιγράφων ασφαλείας η οποία πραγματοποιείται μία φορά την εβδομάδα για λόγους ασφαλείας.

3. ΑΠΟΤΙΜΗΣΗ ΑΓΑΘΩΝ ΤΗΣ ΕΓΚΑΤΑΣΤΑΣΗΣ

Για την αποτίμηση των αγαθών της εγκατάστασης χρειάζεται να αναλύσουμε τις ιδιότητες και την αξία για το σύστημα του αγαθού, καθώς και τις απειλές, ευπάθειες του συστήματος οι οποίες μπορούν να ζημιώσουν τα αγαθά. Ιδιότητα ενός αγαθού ονομάζεται το συγκεκριμένο χαρακτηριστικό ενός αγαθού, το οποίο πρέπει να προστατευθεί. Τα αγαθά που βρίσκονται στο εργαστήριο πρέπει να χαρακτηρίζονται από ακεραιότητα, δηλαδή να διασφαλίζεται ότι η πληροφορία που περιέχει θα τροποποιηθεί μόνο από εξουσιοδοτημένους χρήστες κατά ένα εγκεκριμένο τρόπο (με τον όρο τροποποίηση εννοούμε την δημιουργία ή την μεταβολή ή την διαγραφή της πληροφορίας). Παράλληλα, θα πρέπει να έχουν εμπιστευτικότητα, εννοώντας ότι παρέχεται η διασφάλιση πως η πληροφορία μπορεί να προσπελασθεί μόνο από συγκεκριμένους χρήστες, αυτό σημαίνει ότι η δυνατότητα ανάγνωσης, προβολής ή ακόμη και γνώση ύπαρξης της συγκεκριμένης πληροφορίας είναι διαθέσιμη για ορισμένους από το σύστημα χρήστες. Τέλος, θα έχουν το χαρακτηριστικό της διαθεσιμότητας, που δίνει την διασφάλιση πρόσβασης των εξουσιοδοτημένων χρηστών, στην πληροφορία σε εύλογο χρόνο. Ως αξία αγαθού, πέρα της χρηματικής, εννοούμε την σημαντικότητα της ύπαρξής του για την λειτουργία των διαδικασιών του συστήματος. Ανάλογα με την αξία κάθε αγαθού πρέπει να υπάρχει η αντίστοιχη ασφάλεια του αγαθού, δηλαδή η προστασία των ιδιοτήτων του. Απειλή χαρακτηρίζεται οτιδήποτε μπορεί να προκαλέσει ενδεχόμενη απώλεια ενός ή περισσότερων από τις παραμέτρους που ορίζουν την ασφάλεια ενός πληροφοριακού συστήματος. Όσον αφορά τα αγαθά που είναι εγκατεστημένα στο σύστημα είναι φανερό ότι η μόνη κοινή απειλή όλων, καθώς βρίσκονται με φυσική μορφή στο εργαστήριο είναι αυτή που θα επιφέρει φυσικές ζημιές στο σύστημα, όπως η ύπαρξη μίας φωτιάς, πλημμύρας και άλλων στο ίδιο ύφος καταστροφών. Όπως αναφέρθηκε η ασφάλεια του συστήματος βασίζεται στην προστασία των ιδιοτήτων κάθε αγαθού της εγκατάστασης, δηλαδή οι κίνδυνοι του συστήματος προκαλούνται από απειλές ή αδυναμίες, οι οποίες ζημιώνουν τις ιδιότητες των αγαθών. Για να υπάρξει δηλαδή συνολική αποτίμηση της επικινδυνότητας κάθε αγαθού πρέπει να αναλυθούν οι απειλές και οι αδυναμίες που μπορεί να το προσβάλουν καθώς και η επίπτωση που θα υπάρχει στο συνολικό σύστημα αν αυτό συμβεί.

3.1 Αγαθά που εντοπίστηκαν

A-001 LabWS001

Ο αιματολογικός αναλυτής αποτελεί ένα από τα σημαντικότερα αγαθά του εργαστηρίου καθώς επιτελεί την κεντρική λειτουργία της επιχείρησης, η οποία είναι η ανάλυση των δειγμάτων των ασθενών. Η αξία του λοιπόν είναι υψηλή τόσο από άποψη αναγκαιότητας όσο και από οικονομική άποψη καθώς είναι αρκετά ακριβός εξοπλισμός και αποτελεί επένδυση για την επιχείρηση. Επίσης το λογισμικό που χρησιμοποιεί η συσκευή είναι ιδιόκτητο ,πράγμα που σημαίνει ότι έχει μια επιπλέον οικονομική επιβάρυνση η χρήση του, καθώς το εργαστήριο πρέπει να πληρώσει ειδική άδεια για να το χρησιμοποιήσει και σε κάθε καινούργια έκδοση του η οικονομική επιβάρυνση θα αυξάνεται ,καθώς προστίθενται νέες λειτουργίες και χαρακτηριστικά σε αυτό .

Επίσης αυτού του τύπου το λογισμικό αναπτύσσεται χρησιμοποιώντας closed-source code ,το οποίο σημαίνει ότι ο πηγαίος κώδικας δεν είναι διαθέσιμος στο κοινό και μόνο ο ιδιοκτήτης του μπορεί να τον τροποποιήσει. Ακόμα ο ιδιοκτήτης του λογισμικού αναλαμβάνει και την εκπαίδευση του προσωπικού έτσι ώστε να μάθουν να χειρίζονται σωστά το λογισμικό και τα μέλη του προσωπικού που χρήζουν εκπαίδευσης στην συγκεκριμένη περίπτωση είναι μόνο οι αναλυτές των δειγμάτων. Οπότε ο αιματολογικός αναλυτής διαθέτει την ιδιότητα της ακεραιότητας ,καθώς το λογισμικό που χρησιμοποιεί και τα δεδομένα του δεν μπορούν να τροποποιηθούν από μη εξουσιοδοτημένους χρήστες. Επίσης πολλοί ιδιοκτήτες λογισμικού θέτουν όρια στο πόσες συσκευές μπορούν να έχουν εγκατεστημένο και να λειτουργούν το λογισμικό τους ταυτόχρονα. Αυτά τα όρια εφαρμόζονται στην πράξη με τεχνικά μέτρα όπως, η ενεργοποίηση προϊόντος που είναι ο έλεγχος εγκυρότητας της άδειας χρήσης του λογισμικού , το software key που αποτελεί αποδεικτικό ότι το αντίγραφο του προγράμματος είναι γνήσιο και δημιουργείται με βάση κάποιο μοναδικό χαρακτηριστικό της συσκευής του χρήστη έτσι ώστε να μην μπορεί να αντιγραφεί εύκολα κλπ. Αυτό σημαίνει ότι η πρόσβαση στα δεδομένα και στο λογισμικό του αιματολογικού αναλυτή δεν μπορεί να πραγματοποιηθεί από κανένα άλλο μηχάνημα και ως εκ τούτου πληρείται η ιδιότητα της εμπιστευτικότητας, αφού πρόσβαση στα δεδομένα έχουν μόνο οι εξουσιοδοτημένοι χρήστες ,οι αναλυτές δηλαδή που τον χειρίζονται .Επίσης το συγκεκριμένο λογισμικό αναπτύσσεται από έμπειρες ομάδες προγραμματιστών και υπόκειται σε ενδελεχείς δοκιμές πριν την είσοδο του στην αγορά ,το οποίο σημαίνει ότι γενικότερα είναι υψηλής ποιότητας και αξιοπιστίας ,πράγμα πολύ σημαντικό για τον αιματολογικό αναλυτή ο οποίος πρέπει να παράγει ακριβή και αξιόπιστα αποτελέσματα ,τα οποία είναι κρίσιμα για την λήψη ορθών ιατρικών αποφάσεων. Η επιτυχημένη εκσφαλμάτωση του λογισμικού κατά ένα μεγάλο ποσοστό λοιπόν συνεπάγεται ότι ο αιματολογικός αναλυτής διαθέτει την ιδιότητα της διαθεσιμότητας ,καθώς η πρόσβαση των εξουσιοδοτημένων χρηστών στο σύστημα πραγματοποιείται σε εύλογο χρόνο.

<u>Σταθμοί Εργασίας A-002 PCWS001, A-003 PCWS002, A-004 PCWS003 , A-005 PCWS004 , A-006 PCWS005 , A-015 Laptop</u>

Όπως αναφέρθηκε και παραπάνω οι υπολογιστές αυτοί βοηθούν το προσωπικό να επικοινωνεί μεταξύ του και να έχει πρόσβαση στις απαραίτητες πληροφορίες που χρειάζεται ,μέσω της βάσης δεδομένων του εργαστηρίου ,για να φέρει σε πέρας τα εργασιακά του καθήκοντα. Η αξία τους λοιπόν είναι και οικονομική ,καθώς απαιτούν την καταβολή ενός μεγάλου χρηματικού ποσού και για την αγορά αλλά και για την συντήρηση τους ,αλλά και πρακτική καθώς χωρίς αυτούς η εύκολη,γρήγορη και ασφαλής ανταλλαγή και επεξεργασία πληροφοριών θα ήταν αδύνατη. Οι σταθμοί εργασίας διαθέτουν το Windows 10 Pro ως λειτουργικό σύστημα το οποίο περιλαμβάνει αρκετά χαρακτηριστικά ασφαλείας ,τα οποία αναλύονται και παρακάτω και του προσδίδουν τις ιδιότητες της ακεραιότητας και της εμπιστευτικότητας και ο τρόπος με τον οποίο είναι σχεδιασμένο το καθιστά αξιόπιστο ,σταθερό και ανθεκτικό σε αποτυχίες λογισμικού ή hardware προσδίδοντας του έτσι την ιδιότητα της διαθεσιμότητας. Ως μηχανήματα λοιπόν οι υπολογιστές αυτοί έχουν και τις τρείς ιδιότητες (ακεραιότητα, εμπιστευτικότητα, διαθεσιμότητα) χάρη στο λειτουργικό τους σύστημα . Επίσης στον χώρο του Εργαστηρίου- Παρασκευαστηρίου καθώς και στο γραφείο του ιατρού υπάρχουν 2 υπολογιστές οπότε σε περίπτωση διακοπής λειτουργίας του ενός ,υπάρχει διαθέσιμος ο δεύτερος άρα πληρείται η ιδιότητα της διαθεσιμότητας σε αυτές τις περιπτώσεις.

Όσον αφορά το αγαθό A-015 το λειτουργικό σύστημα που διαθέτει είναι το MAC-OS το οποίο περιλαμβάνει αρκετά χαρακτηριστικά ασφαλείας όπως το Gatekeeper το οποίο διασφαλίζει ότι μόνο αξιόπιστο λογισμικό μπορεί να εγκατασταθεί στην συσκευή επαληθεύοντας την ηλεκτρονική υπογραφή του λογισμικού αυτού. Ακόμα παρέχει το FileVault το οποίο είναι μία λειτουργία κρυπτογράφησης κατά την οποία κρυπτογραφούνται τα δεδομένα του σκληρού δίσκου χρησιμοποιώντας την 128-

bit AES κρυπτογράφηση. Υπάρχει και το Firewall το οποίο είναι μία λειτουργία ασφάλειας δικτύου που ελέγχει και διαχειρίζεται την εισερχόμενη και εξερχόμενη κίνηση στο δίκτυο . Υποστηρίζει εντοπισμό και αφαίρεση κακόβουλου λογισμικού με τα εργαλεία Xprotect και MRT . Επιπλέον διαθέτει σύστημα προστασίας ακεραιότητας το οποίο προστατεύει αρχεία του συστήματος από το να τροποποιηθούν από λογισμικό τρίτων .Τέλος παρέχει το iCloud Keychain, το οποίο είναι μια λειτουργία ασφαλούς διαχείρισης και αποθήκευσης κωδικών πρόσβασης,στοιχείων πιστωτικών καρτών και στοιχείων του δικτύου WiFi στο οποίο είναι συνδεδεμένη η συσκευή και την αυθεντικοποίηση δύο παραγόντων ,η οποία απαιτεί από τους χρήστες να δώσουν έναν κωδικό πρόσβασης και έναν κωδικό που θα τους σταλεί στο προσωπικό τους νούμερο κινητού προκειμένου να αποκτήσουν πρόσβαση στον λογαριασμό τους. Χαρακτηριστικά τα οποία προσδίδουν εμπιστευτικότητα στο laptop του ιατρού καθώς μόνο εκείνος θα μπορεί να έχει πρόσβαση στο συγκεκριμένο σύστημα. Το laptop διαθέτει και το χαρακτηριστικό της διαθεσιμότητας καθώς το MAC-OS παρέχει αυτόματες ενημερώσεις ,οι οποίες συμβάλλουν στην ομαλή λειτουργία του συστήματος,μια λειτουργία back up που συμβάλλει στην ανάκτηση αρχείων σε περίπτωση απώλειας ή κλοπής τους, ένα mode επαναφοράς κατά το οποίο πραγματοποιούνται εργασίες συντήρησης ,συμπεριλαμβανομένης της επισκευής του startup δίσκου και της ανάκτησης των δεδομένων μέσω της λειτουργίας back up. Τέλος πολύ σημαντικό είναι ότι ο ιατρός μπορεί να συνδεθεί στο iCloud από οποιαδήποτε άλλη συσκευή σε περίπτωση που το laptop του δεν είναι διαθέσιμο και να έχει έτσι πρόσβαση στα αρχεία του.

A-007 PR0001, A-008 PR0002

Όπως έχουμε αναλύσει παραπάνω οι εκτυπωτές που διαθέτει το εργαστήριο είναι σημαντικοί για την δημιουργία αντιγράφων ασφαλείας σε έντυπη μορφή και την τήρηση φυσικού αρχείου ,για την εκτύπωση των απαραίτητων παραστατικών (απόδειξη/τιμολόγιο) ως αποδείξεις παροχής υπηρεσιών και για την αποστολή των αποτελεσμάτων των εξετάσεων μέσω fax. Είναι παλαιότερα μοντέλα οπότε δεν θεωρούνται πολύ ακριβός εξοπλισμός και δεν διαθέτουν και τα αντίστοιχα χαρακτηριστικά ασφαλείας που έχουν νεότερα μοντέλα . Παρόλα αυτά επειδή διαχειρίζονται κρίσιμες πληροφορίες είναι σημαντικό να προστατευθούν.

A-009, A010

Τα αγαθά επεξεργαστών είναι πολύ σημαντικά για το σύστημα, καθώς διαχειρίζονται βασικές απαιτήσεις του συστήματος, όπως την επικοινωνία των συσκευών με το Internet και την αποθήκευση όλων των στοιχείων των ασθενών, αποτελεσμάτων και πολλά ακόμη χρήσιμα στοιχεία για το εργαστήριο σε μία κοινή βάση. Η αξία τους, λοιπόν, είναι πολύ υψηλή, καθιστώντας τους αρκετά απαραίτητους για την λειτουργία του συστήματος ώστε να μην μας ενδιαφέρει σε σημαντικό βαθμό η χρηματική τους αξία. Αν αναλύσουμε τα δύο αγαθά ξεχωριστά υπάρχει διαχωρισμός καθώς το αγαθό A-010 υποστηρίζεται από το αγαθό A-014, το οποίο προσδίδει τελικά στον Database Server έλεγχο με σκοπό την αποτροπή των μη ειδικά εξουσιοδοτημένων χρηστών να τροποποιήσουν και να διαγράψουν τα δεδομένα που βρίσκονται στην βάση (όλοι οι αναλυτές έχουν δυνατότητα να δουν τα δεδομένα της βάσης αλλά να τα διαγραφούν ,π.χ., μπορεί να έχει μόνο ο ιατρός), αυτό το γεγονός κάνει το αγαθό A-010 να έχει ακεραιότητα. Επιπλέον, γνωρίζουμε ότι η ταχύτητα επεξεργασίας δεδομένων διαφέρει ανά επεξεργαστή. Στην δική μας περίπτωση ο Database Server υποστηρίζει μία βάση δεδομένων Oracle, η οποία υποστηρίζει παράλληλη επεξεργασία δεδομένων έτσι ο επεξεργαστής μας έχει αρκετά υψηλή ταχύτητα. Άρα το αγαθό A-010 έχει διαθεσιμότητα. Ο Web Server, ταυτόχρονα, που εγκαταστήσαμε είναι ένας από τους πιο γρήγορους εξυπηρετητές, δίνοντας και στο αγαθό A-009 την ιδιότητα διαθεσιμότητας. Ανακοινώθηκε, βέβαια, από την Microsoft όσον αφορά τον Web Server με λειτουργικό σύστημα Windows Server 2008 R2, που έχουμε εγκατεστημένο, ότι θα πάψουν να υποστηρίζονται από το έτος 2020, αυτό

σημαίνει ότι θα εξακολουθήσει να λειτουργεί ο επεξεργαστής μας αλλά δεν θα δέχονται πλέον αναβαθμίσεις για προβλήματα ασφάλειας, λειτουργίας, εφαρμογών (πχ Internet Explorer) κτλ.

A-011, A-012

Στα αγαθά Switch, βασίζεται η επικοινωνία όλων των συσκευών μεταξύ τους αλλά και η επικοινωνία των συσκευών με τους εξυπηρετητές. Τα αγαθά αυτά δηλαδή προσδίδουν την επικοινωνία του συστήματος, η οποία είναι βασική για την λειτουργία όλων των διαδικασιών που υποστηρίζει το σύστημα. Η αξία τους, λοιπόν, είναι πολύ υψηλή καθώς χωρίς αυτά το σύστημα θα διαχωριζόταν σε τμήματα όπου το καθένα θα έπρεπε να δουλεύει ανεξάρτητα από το άλλο, κάτι που θα έκανε την διαδικασία της εξαγωγής των αποτελεσμάτων πολύ πιο αργή ακόμα και ανακριβής (αφού θα έπρεπε κάθε υπολογιστής να έχει αντίγραφα όλων των δεδομένων που χρειάζονται για την εκτέλεση της διαδικασίας). Χωρίς την ύπαρξη του switch που συνδέει τους εξυπηρετητές με τις υπόλοιπες συσκευές, η επικοινωνία τους δεν θα υπάρχει, το οποίο σημαίνει ότι δεν μπορεί να γίνει αποθήκευση σε κάποια κοινή βάση των αποτελεσμάτων ή άλλων στοιχείων, κάνοντας έτσι οποιαδήποτε διαδικασία να μπορεί να υπάρχει μόνο προσωρινά ή σε έντυπη μορφή (από εκτυπωτή). Η σημαντικότητα των δύο αυτών αγαθών, επομένως, είναι αδιαμφισβήτητη. Η σύνδεση των συσκευών και των επεξεργαστών με κάποιον switch συμβαίνει με χρήση ενός καλωδίου, πράγμα που δίνει στο αγαθό εμπιστευτικότητα, αφού διασφαλίζει πως μόνο αυτοί που συνδέονται με αυτό μπορούν να μοιράζονται τις πληροφορίες που παρέχει (οι οποίες απορρέουν από τις συνδέσεις που επιτυγχάνει). Όπως ήδη γνωρίζουμε η μετάδοση της πληροφορίας μέσω καλωδίου συγκριτικά με την ασύρματη μετάδοση είναι συνήθως γρηγορότερη ή ίδιας ταχύτητας, αυτό σημαίνει ότι τα αγαθά switch προσφέρουν την μεταδιδόμενη πληροφορία σε εύλογο χρόνο, αυτό δίνει διαθεσιμότητα στα αγαθά.

A-013

Το αγαθό Router που είναι εγκατεστημένο στο σύστημα, αποτελεί την «πύλη» του δικτύου μας με το Internet, προσφέροντας έτσι στο σύστημα μας περισσότερες δυνατότητες. Παράλληλα, λειτουργεί ως την ένωση των δύο τμημάτων που δημιουργούνται από την ύπαρξη των switch, καθιστώντας δυνατή την επικοινωνία μεταξύ των συσκευών με τους εξυπηρετητές (αφού είναι διαφορετικά τμήματα), αλλά και αυτών με τον πάροχο Internet (ISP cloud). Το μοντέλο router που εγκαταστάθηκε είναι το Cisco C886VA-K9, το οποίο προσφέρει μεγαλύτερες ταχύτητες λήψης και αποστολής δεδομένων σε σχέση με άλλα μοντέλα. Επίσης διαθέτει SPI firewall, ο οποίος είναι ένας μηχανισμός που ελέγχει την κίνηση των δεδομένων για μοτίβα γνωστών τύπων επιθέσεων (πχ DDoS) και το NAT firewall, το οποίο κρύβει τις διευθύνσεις όλων των συσκευών του τοπικού μας δικτύου πίσω από μια μοναδική διεύθυνση. Με το φιλτράρισμα διευθύνσεων MAC, επιτρέπει σε συγκεκριμένες συσκευές να συνδεθούν με βάση την μοναδική διεύθυνση MAC τους, αποκλείοντας κάθε συσκευή με διεύθυνση MAC που δεν έχει οριστεί ως αποδεκτή. Αυτές οι πληροφορίες ουσιαστικά προσδίδουν στο αγαθό τις ιδιότητες εμπιστευτικότητας, διαθεσιμότητα και ακεραιότητας.

A-014

Το αγαθό Firewall, όπως ήδη περιγράψαμε, γενικότερα χρησιμοποιείται για την προστασία του δικτύου και των υπολογιστών από επιθέσεις ή προσπάθεια εισόδου σε μη επιτρεπτές ή μη εξουσιοδοτημένες, για τον χρήστη, εφαρμογές. Το συγκεκριμένο αγαθό είναι εγκατεστημένο στην σύνδεση του Switch με το Database Server και είναι αυτό, όπως αναφέραμε και αποτίμηση του αγαθού A-010, που προσφέρει στον συγκεκριμένο επεξεργαστή ακεραιότητα εμπιστευτικότητα και διαθεσιμότητα. Οι

παροχές του αγαθού αυτού σε συνδυασμό με την θέση του στο δίκτυο κάνει την ύπαρξη του στο σύστημα πολύ σημαντική, έχει δηλαδή υψηλή αξία. Από την περιγραφή της λειτουργίας του αγαθού συμπεραίνουμε ότι έχει και τις τρείς ιδιότητες : εμπιστευτικότητα, διαθεσιμότητα, ακεραιότητα.

A-016,A-017,A-024

Τόσο τα δεδομένα των πελατών (Customer Data) όσο και τα δεδομένα των υπαλλήλων (Employee Data) είναι προσωπικά δεδομένα που μόνο το εργαστήριο επιτρέπεται να έχει. Οι πελάτες όπως και οι υπάλληλοι έχουν εμπιστευθεί αυτές τις πληροφορίες με το εργαστήριο και το εμπιστεύονται. Όσον αφορά το αγαθό A-016 είναι απαραίτητο για να μπορούν να σταλθούν οι εξετάσεις στο σωστό email των ασθενών, να μπορεί να έχει πρόσβαση το εργαστήριο πρόσβαση στο ιστορικό τους καθώς και να είναι σε θέση να βγάλει τα στατιστικά αποτελέσματα που χρειάζεται. Το αγαθό A-017 που περιέχει τα δεδομένα των εργαζομένων είναι εξίσου σημαντικά έτσι ώστε να γνωρίζει το εργαστήριο την κατάστασή τους . Τα δεδομένα αυτά βρίσκονται στο Database server SRV002 ο οποίος είναι υπεύθυνος για να τα κρατάει ασφαλή. Η χρηματική αξία των δεδομένων είναι σχεδόν μηδενική όμως η αξία τους ως αγαθά είναι μεγάλη λόγω της σημαντικότητάς τους και αξίζει να προστατευθούν. Από την στιγμή που η βάση δεδομένων που αποθηκεύονται έχει τις ιδιότητες της εμπιστευτικότητας, ακεραιότητας και ασφάλειας έτσι και τα δεδομένα αυτά δεν μπορούν εύκολα να αλλοιωθούν, να έχουν πρόσβαση μη εξουσιοδοτημένοι χρήστες καθώς και μπορούμε να τα έχουμε στην διάθεση μας ανά πάσα στιγμή.

A-018,A-019

Τα αγαθά που ανήκουν στην κατηγορία του λογισμικού τόσο των switchers (A-018) όσο και των workstations (A-019) είναι από τα πιο σημαντικά αγαθά του εργαστηρίου εφόσον είναι απαραίτητα για την λειτουργία των switchers και των workstations που όπως περιγράψαμε πιο πάνω είναι αναγκαία για την σωστή λειτουργία του εργαστηρίου. Και τα windows 7 pro όπως και τα windows 10 proείναι λειτουργικά συστήματα τα οποία έχει φτιάξει η Microsoft. Όσον αφορά το δεύτερο αγαθό, δηλαδή τα windows 10 pro παρέχει προστασία έναντι ιών, spyware και άλλων κακόβουλων λογισμικών. Σκανάρει αρχεία και εφαρμογές για απειλές και ενημερώνεται συχνά για να κρατείται προστατευμένο το σύστημα. Τα δεδομένα του σκληρού δίσκου προστατεύονται επίσης από το λογισμικό αυτό καθώς προσφέρεται κρυπτογράφηση σε αυτό. Τέλος απαγορεύει την μη εξουσιοδοτημένη πρόσβαση στο σύστημα μέσω διαδικτύου ή κάποιου άλλου δικτύου. Όλα αυτά μας φτάνουν στο συμπέρασμα ότι τα windows 10 pro έχουν την ιδιότητα και της εμπιστευτικότητας καθώς και της ακεραιότητας. Τέλος, η πρόσβαση στο λειτουργικό αυτό είναι και γρήγορη και είναι προσβάσιμο κάθε στιγμή οπότε ικανοποιείται και η ιδιότητα της διαθεσιμότητας.

A-020

Το αγαθό website το οποίο είναι η ιστοσελίδα του εργαστηρίου με σκοπό να μπορούν οι ασθενείς να συνδέονται με τους κωδικούς τους σε αυτήν και να βλέπουν τα αποτελέσματα των εξετάσεών τους. Η ιστοσελίδα αυτή έχει κατασκευαστεί με την εφαρμογή JOOMLA η οποία είναι μια εφαρμογή που φτιάχνει ιστοσελίδες προσφέροντας τα απαραίτητα μέτρα προστασίας. Για να δει ένας ασθενής τα αποτελέσματά του πρέπει να συνδεθεί με τους κωδικούς του. Αυτό σημαίνει ότι δεν μπορεί κανένας άλλος χρήστης να έχει πρόσβαση στα ίδια δεδομένα. Η ιστοσελίδα δεν είναι δυνατόν να αλλοιωθεί επειδή για να αλλάξεις την ιστοσελίδα σου στο JOOMLA πρέπει να συνδεθείς με τους δικούς σου κωδικούς. Έτσι καταλαβαίνουμε ότι υπάρχει και η ιδιότητα της ακεραιότητας. Τέλος, η ιστοσελίδα αυτή είναι διαθέσιμη για κάθε πελάτη οποιαδήποτε στιγμή άρα η ιστοσελίδα έχει και την ιδιότητα της διαθεσιμότητας.

A-021,A-022

Και τα δύο αυτά αγαθά αφορούν όλα τα δεδομένα που έχουμε και σε ψηφιακή μορφή στις βάσεις δεδομένων απλά σε έντυπη μορφή. Τέτοιου είδους αγαθά όταν ειδικά βρίσκονται σε ανοιχτές βιβλιοθήκες των κοινόχρηστων χώρων όπως το αγαθό A-021 στην ανοιχτή βιβλιοθήκη της αίθουσας αναμονής χάνουν την ιδιότητα της εμπιστευτικότητας και της ακεραιότητας επειδή οποιοσδήποτε μπορεί να έχει πρόσβαση σε αυτά. Το αγαθό A-022 το οποίο βρίσκεται στο γραφείο του ιατρού είναι λίγο πιο προστατευμένο επειδή δεν είναι τόσο εκτεθειμένα. Το ότι βρίσκονται αυτά τα αρχεία σε έντυπη μορφή είναι για να είναι διαθέσιμα οποιαδήποτε στιγμή για να γίνεται η δουλειά της γραμματείας πιο εύκολη. Συνεπώς τα αγαθά αυτά έχουν την ιδιότητα της διαθεσιμότητας. Η χρηματική τους αξία μπορεί να μην είναι μεγάλη, όπως επίσης δεν είναι τόσο σημαντικά όσο τα δεδομένα ψηφιακής μορφής, όμως εξακολουθούν να υπάρχουν απειλές προς αυτά και να χρειάζεται να προστατευθούν.

A-023, A-025

Τα αγαθά χημικές ουσίες και δείγμα λειτουργούν στο σύστημα ως υπολογιστικός πόροι καθώς συνδυάζονται και δίνουν το αποτέλεσμα της σχετικής ανάλυσης. Με άλλα λόγια ο σκοπός του εργαστηρίου, η ανάλυση διαγνωστικών εξετάσεων, επιτυγχάνεται μόνο αν υπάρχουν διαθέσιμα τα αγαθά που αναλύουμε, αυτό σημαίνει ότι είναι πολύ σημαντικά για το σύστημα μας. Δηλαδή, τα συγκεκριμένα αγαθά έχουν πολύ υψηλή αξία. Τα αγαθά αυτά συσκευάζονται σε ειδικά δοχεία για την μεταφορά τους, η φύλαξη των οποίων βασίζεται κυρίως στο προσωπικό του εργαστηρίου.

3.2 Απειλές που εντοπίστηκαν

A-001 LabWS001

Ο λανθασμένος χειρισμός του συστήματος του αιματολογικού αναλυτή είτε από κάποιο δυσαρεστημένο υπάλληλο είτε από κάποιον υπάλληλο που δεν έχει ολοκληρώσει επιτυχώς την εκπαίδευση του σχετικά με την διαχείριση του λογισμικού αυτού αποτελεί ***απειλή για την ακεραιότητα*** του συγκεκριμένου αγαθού, διότι εσκεμμένα ή μη μπορεί να τροποποιηθούν με μη εγκεκριμένο τρόπο τα δεδομένα του συστήματος του. Αν συμβεί κάτι τέτοιο τα αποτελέσματα των εξετάσεων θα είναι εσφαλμένα και κατ'επέκταση και η διάγνωση βάσει αυτών . Αυτό μπορεί να θέσει σε κίνδυνο την υγεία του ασθενούς που θα ακολουθήσει την λανθασμένη θεραπεία και αν συμβαίνει κατ'εξακολούθηση θα αμαυρώσει και την φήμη του μικροβιολογικού εργαστηρίου.

Ο αιματολογικός αναλυτής βρίσκεται στον χώρο του Εργαστηρίου - Παρασκευαστηρίου στον οποίο η βοηθητική έξοδος οδηγεί στον αύλειο χώρο που δεν είναι περιφραγμένος και σε περίπτωση που κάποιος υπάλληλος ξεχάσει ανοιχτή την πόρτα ενδέχεται να μπορέσει να εισέλθει στον χώρο του εργαστηρίου ο οποιοσδήποτε που δεν έχει προφανώς εξουσιοδότηση ή κάποιο ζώο όπως ένας σκύλος και να βανδαλίσει το αγαθό ,προκαλώντας του σημαντικές φθορές και ***απειλώντας*** έτσι την ιδιότητα της ***διαθεσιμότητας*** που διαθέτει ,καθώς δεν θα βρίσκεται σε θέση να λειτουργήσει.

Η μη τήρηση των διαδικασιών συντήρησης του αιματολογικού αναλυτή σύμφωνα με τις οδηγίες του κατασκευαστή μπορεί να οδηγήσει σε τεχνική του βλάβη ,η οποία μπορεί να αποτελέσει απειλή για τον χρόνο ζωής του μηχανήματος ,δηλαδή για την ***διαθεσιμότητα*** του αλλά και για την εγκυρότητα των αποτελεσμάτων του δηλαδή την ***ακεραιότητα*** του, καθώς τα δεδομένα που διαχειρίζεται θα υποστούν αλλοιώσεις. Ο αναλυτής για παράδειγμα χρειάζεται ανά 15 μέρες καθαρισμό του εξαερισμού του αλλιώς υπάρχει ο κίνδυνος υπερθέρμανσης του και ως αποτέλεσμα μείωσης της διάρκειας ζωής του. Επίσης αν δεν καθαρίζονται τακτικά και επαρκώς τα

διάφορα εξαρτήματα του στα οποία τοποθετείται το περιεχόμενο των δειγμάτων προς ανάλυση ,είναι βέβαιο ότι τα αποτελέσματα της ανάλυσης θα είναι εσφαλμένα.

Σταθμοί Εργασίας A-002 PCWS001, A-003 PCWS002, A-004 PCWS003 , A-005 PCWS004 , A-006 PCWS005 , A-015 Laptop

Όσον αφορά τους 2 σταθμούς εργασίας που βρίσκονται στον χώρο του Εργαστηρίου -Παρασκευαστηρίου PCWS001 και PCWS002 ***απειλείται η ακεραιότητα και η εμπιστευτικότητα*** τους καθώς η βοηθητική έξοδος οδηγεί στον αύλειο χώρο ο οποίος είναι μη περιφραγμένος και σε περίπτωση που κάποιος υπάλληλος ξεχάσει ανοιχτή την πόρτα ενδέχεται να μπορέσει να εισέλθει στον χώρο του εργαστηρίου ο οποιοσδήποτε που δεν έχει προφανώς εξουσιοδότηση και να αποκτήσει πρόσβαση στα δεδομένα των σταθμών εργασίας και να μπορέσει πιθανώς να τα τροποποιήσει κατά μη εγκεκριμένο τρόπο ή και να τα κλέψει. Αυτό επίσης προϋποθέτει το σύστημα να έχει «αφεθεί» ξεκλειδωμένο από κάποιον υπάλληλο οπότε να μην υπάρχει η δικλείδα ασφαλείας του συνθηματικού για πρόσβαση στο σύστημα. Οπότε η απειλή αυτή είναι ανθρώπινη και σκόπιμη επειδή προέρχεται από ανθρώπινες και κακόβουλες ενέργειες αλλά και τυχαία επειδή προέρχεται από αμέλεια του προσωπικού του εργαστηρίου. Με την ίδια απειλή έρχονται αντιμέτωποι τόσο και οι υπόλοιποι σταθμοί εργασίας καθώς η είσοδος από χώρο σε χώρο είναι ελεύθερη και μη ελεγχόμενη όσο και το laptop το οποίο μπορεί να κλαπεί ολόκληρο και όχι μόνο τα δεδομένα του.

Μία τεχνική βλάβη της εγκατάστασης όπως η διακοπή του ρεύματος ***απειλεί την διαθεσιμότητα*** όλων των σταθμών εργασίας αλλά και του laptop σε περίπτωση που είναι παρατεταμένη. Το εργαστήριο κυριολεκτικά δεν θα μπορεί να λειτουργήσει και ενδέχεται να χαθούν και σημαντικά δεδομένα όπως για παράδειγμα αποτελέσματα μιας αιματολογικής ανάλυσης πριν αυτά προλάβουν να σταλούν στην βάση δεδομένων του εργαστηρίου.

Ακόμα επιθέσεις social engineering όπως το phishing ή το spear-phishing μπορεί να ξεγελάσουν το προσωπικό έτσι ώστε να αποκαλύψει ευαίσθητες πληροφορίες όπως όνομα και κωδικό χρήστη του συστήματος και να αποτελέσουν έτσι ***απειλή της εμπιστευτικότητας*** των αγαθών, καθώς μη εξουσιοδοτημένοι χρήστες θα μπορέσουν να αποκτήσουν πρόσβαση στο σύστημα και τα δεδομένα τους. Τέτοιες επιθέσεις γίνονται με την μορφή ψεύτικων email ή ιστοσελίδων που εκ πρώτης όψεως φαίνονται γνήσιες και έγκυρες .

A-007 PR0001, A-008 PR0002

Η χαμηλότερη ανάλυση της εκτύπωσης αλλοιώνει τα δεδομένα που εκτυπώνονται ***απειλώντας την ακεραιότητα*** τους και στην περίπτωση των αιματολογικών αποτελεσμάτων αν υπάρχει σημαντική απόκλιση στην καμπύλη ζαχάρου για παράδειγμα σε σχέση με τα αποτελέσματα που βρίσκονται σε ηλεκτρονική μορφή θα έχουμε ως αποτέλεσμα μία λανθασμένη διάγνωση και μία λανθασμένη θεραπεία ,θέτοντας σε κίνδυνο την υγεία του ασθενούς.

Λόγω έλλειψης σύγχρονων χαρακτηριστικών ασφαλείας οι εκτυπωτές αυτοί είναι εκτεθειμένοι σε επιθέσεις από κακόβουλο λογισμικό και hackers ,οι οποίοι αποκτούν πρόσβαση στα δεδομένα που έχουν εκτυπωθεί ,μπορούν να δώσουν εντολή να εκτυπώσουν τα δεδομένα αλλοιωμένα ,καθώς και να προκαλέσουν φυσική ζημιά «πειράζοντας» το firmware στους εκτυπωτές μέσω αντίστοιχων εντολών. Καταλαβαίνουμε επομένως ότι απειλούνται όλες οι ιδιότητες του αγαθού (***εμπιστευτικότητα*** , καθώς μη εξουσιοδοτημένος χρήστης αποκτά πρόσβαση στο σύστημα , ***ακεραιότητα*** ,καθώς τα δεδομένα μπορεί να τροποποιηθούν με μη εγκεκριμένο τρόπο από μη εξουσιοδοτημένο χρήστη και ***διαθεσιμότητα*** ,καθώς το μηχάνημα μετά την επίθεση δεν θα είναι λειτουργικό.)

Λόγω παλαιότητας η απόδοση των εκτυπωτών είναι πιο αργή σε σχέση με νεότερα μοντέλα και τους παίρνει περισσότερο χρόνο να επεξεργαστούν και να εκτυπώσουν δεδομένα και αυτή καθυστέρηση σε ώρες μεγάλου φόρτου εργασίας μπορεί να αποβεί μοιραία για την ιδιότητα της ***διαθεσιμότητας*** τους. Υπάρχει ενδεχόμενο κάποια αρχεία

να απορριφθούν από την ουρά του εκτυπωτή επειδή θα έχει γεμίσει και ως εκ τούτου να μην εκτυπωθούν ποτέ αν δεν εμφανιστεί το αντίστοιχο μήνυμα λάθους στον χρήστη. Και υπάρχει και το ενδεχόμενο να έχουμε αποτυχία του συστήματος λόγω φόρτου εργασίας και να χρειαστεί επανεκκίνηση της συσκευής.

A-009

Να έχει καταφέρει κάποιος άνθρωπος να χρησιμοποιήσει κάποια συσκευή που είναι συνδεδεμένη στο δίκτυο του εργαστηρίου, και αφού ο web server δεν έχει κάποια δικλείδα ασφάλειας για την είσοδο στον εξυπηρετητή, π.χ. για εξουσιοδοτημένους χρήστες, μπορεί να διαγράψει την ιστοσελίδα που είναι ανεβασμένη, ακόμη και να την τροποποιήσει με τρόπο που θα βλάψει το σύστημα και την λειτουργία, τελικά, του εργαστηρίου.

Το συγκεκριμένο αγαθό επιπλέον, γνωρίζουμε ότι πέρα από την ιστοσελίδα του εργαστηρίου κάνει δυνατή την σύνδεση, όλων των συσκευών που βρίσκονται στο ίδιο δίκτυο, με οποιαδήποτε Web σελίδα. Αυτές είναι πολυάριθμες και είναι πολύ εύκολη η μετάδοση κάποιου ιού από την επίσκεψη μίας μη ασφαλισμένης σελίδας. Πράγμα που μπορεί να γίνει αν κάποιο κακόβουλο πρόσωπο χρησιμοποιήσει κάποια συνδεδεμένη συσκευή στο δίκτυο.

Η πρόκληση κάποιας φωτιάς, επίσης, θεωρείται φυσική απειλή που προσβάλει το συγκεκριμένο αγαθό.

Το λειτουργικό σύστημα που υποστηρίζει ο εξυπηρετητής να παρουσιάσει ορισμένες αστοχίες που δεν θα κάνουν δυνατή π.χ. την αποθήκευση κάποιας τροποποίησης στην ιστοσελίδα του εργαστηρίου ή την επικοινωνία με το Web.

A-010

Να εισέλθει, από κάποια από τις δύο εισόδους που οδηγούν στον βοηθητικό χώρο, κάποιος άνθρωπος για να κλέψει, να καταστρέψει, να βραχυκυκλώσει με νερό τον εξυπηρετητή.

Να αποσυνδέσει κάποιο κακόβουλο πρόσωπο τον εξυπηρετητή από το switch.

Να υπάρξει κάποια μεγάλη βροχή, η οποία θα προκαλέσει πλημμύρα που θα περάσει από την βοηθητική είσοδο και θα επιφέρει βραχυκύκλωση του εξυπηρετητή από φυσικά αίτια.

Τέτοιες απειλές από φυσικά φαινόμενα είναι εύκολο να συμβούν αφού δεν έχουμε λάβει κάποιο μέτρο ασφαλείας για τον βοηθητικό χώρο, στον οποίο βρίσκονται εγκατεστημένα και τα δύο αγαθά. Παράλληλα όμως αποδεικνύεται και ότι η ανθρώπινη απειλή είναι πολύ πιθανή με βάση τον τρόπο που έχουν εγκατασταθεί τα αγαθά αυτά (Απαραίτητο είναι να αναφέρουμε ότι οποιοδήποτε ανθρώπινο λάθος είναι σκόπιμο θεωρείται απειλή).

A-011, A-012

Τα αγαθά switch, όπως και τα αγαθά servers που περιγράψαμε παραπάνω, λόγω του ότι είναι πραγματικά αντικείμενα που βρίσκονται στον χώρο και συνδέονται με το υπόλοιπο δίκτυο είναι ευάλωτα στις φυσικές απειλές.

Μία ανθρώπινη απειλή είναι να αποσυνδέσει κάποιος, σκόπιμα, οποιοδήποτε από τα δύο switch από τον router, γεγονός που αν συμβεί π.χ. την ώρα που γίνεται προσπάθεια προώθησης κάποιου αποτελέσματος στην βάση δεδομένων θα χαθεί να το γνωρίζει ο αναλυτής που την προώθησε.

Κάποιο κακόβουλο πρόσωπο, επιπλέον, μπορεί να επιφέρει φυσική βλάβη στο switch, καθώς βρίσκονται σε χώρους του εργαστηρίου (αίθουσα αναμονής) που είναι προσβάσιμη από το κοινό.

A-013

Το αγαθό Router βρίσκεται στην αίθουσα αναμονής, και αφού δεν μας έχει ορίσει ακριβώς η περιγραφή του εργαστηρίου ποιοι μπορούν να χρησιμοποιούν την ασύρματη σύνδεση που προσφέρει θεωρούμε ότι μπορεί να γίνει είσοδος και από τους

ασθενείς, που περιμένουν να εξυπηρετηθούν, για προσωπική χρήση. Το συγκεκριμένο router που έχει εγκατασταθεί περιλαμβάνει λογισμικό, το οποίο ελέγχει την εξουσιοδότηση που έχει ο χρήστης που το χρησιμοποιεί και παρέχει όσες υπηρεσίες του αναλογούν. Ένας δηλαδή ασθενής δεν μπορεί να έχει μέσω του Wi-Fi σύνδεση σε κάποιον από τους εξυπηρετητές του δικτύου. Το αγαθό αυτό, όπως και όλα τα αγαθά που ανήκουν στον εξοπλισμό του εργαστηρίου είναι ευάλωτα σε φυσικές απειλές, όπως την πρόκληση μίας φωτιάς.

A-014

Το αγαθό Firewall είναι τοποθετημένο και αυτό στον βοηθητικό χώρο κάνοντας τις φυσικές απειλές να επηρεάζουν και το ίδιο. Το συγκεκριμένο αγαθό περιλαμβάνει πολλές δικλείδες ασφαλείας κάνοντας δύσκολη, έως και αδύνατη την ανθρώπινη απειλή στο λογισμικό που υποστηρίζει το συγκεκριμένο αγαθό. Ο τρόπος όμως που μπορεί να επηρεαστεί από κάποιο άνθρωπο είναι από την καταστροφή του ίδιου του αγαθού εσκεμμένα με την είσοδο του στον βοηθητικό χώρο.

A-016

Μία απειλή που θα μπορούσε να προβληματίσει αυτό το αγαθό είναι απειλές που στοχεύουν στο να μειώσουν την ιδιότητα της ακεραιότητας του συγκεκριμένου αγαθού. Μια τέτοια απειλή, λοιπόν, είναι η αλλοίωση των δεδομένων . Δηλαδή, κάποιος μπορεί να μπει στην βάση δεδομένων που βρίσκονται τα δεδομένα των υπαλλήλων και να τα τροποποιήσει. Αυτό σημαίνει ότι μετά τα δεδομένα θα δίνουν λάθος πληροφορίες στο εργαστήριο και αυτό μπορεί να έχει σοβαρές επιπτώσεις στην λειτουργία του εργαστηρίου από την στιγμή που δεν θα γνωρίζει τις πληροφορίες που χρειάζεται.

A-017

Τα δεδομένα είναι πολύ εύκολο να υποκλαπούν από κακόβουλους χρήστες και να διαρρεύσουν προσωπικά δεδομένα των ασθενών. Αυτό μπορεί να γίνει από εξωτερικούς χρήστες οι οποίοι κανονικά δεν θα έπρεπε να έχουν πρόσβαση σε αυτά, για παράδειγμα hackers που θέλουν να χρησιμοποιήσουν τα προσωπικά δεδομένα των ασθενών για κάποιο δικό τους συμφέρον. Δηλαδή μια μη εξουσιοδοτημένη οντότητα αποκτά πρόσβαση στο αγαθό αυτό. Με αυτόν τον τρόπο το εργαστήριο εκτίθεται εφόσον ο υπεύθυνος έχει δηλώσει ότι το εργαστήριο συμμορφώνεται με τις υποχρεώσεις με την προστασία δεδομένων προσωπικού χαρακτήρα. Μια τέτοια απειλή αποτελεί απειλή κατά της εμπιστευτικότητας με τα προσωπικά δεδομένα των ασθενών να κινδυνεύουν να διαρρεύσουν.

A-018

Τα windows 7 pro μπορούν εύκολα να παραβιαστούν πλέον επειδή η Microsoft από το 2020 έχει σταματήσει να προσφέρει ασφάλεια στο συγκεκριμένο λειτουργικό και έχουν σταματήσει να γίνονται ενημερώσεις. Έτσι ένα κακόβουλο λογισμικό μπορεί να εισβάλει σε αυτό και δεν υπάρχει κανένας τρόπος για να το καταπολεμήσει. Για το εργαστήριο αν συμβεί αυτό θα είναι καταστροφικό, εφόσον τα windows 7 pro χρησιμοποιούνται στους switchers οι οποίοι συνδέουν όλες τις υπόλοιπες συσκευές μεταξύ τους, συνεπώς θα διακοπεί η σύνδεση τους ή θα αποπροσανατολιστεί. Μία τέτοια απειλή στοχεύει στην κατάρρευση της ιδιότητας της ακεραιότητας και της εμπιστευτικότητας.

A-019

Τα windows 10 pro έχουν γενικά πάρα πολύ καλή προστασία και ασφάλεια. Παρόλα αυτά είναι δυνατόν να μπει κάποιος τρίτος να χακάρει το λογισμικό και να σταματήσει κάποιες λειτουργίες του, το οποίο μπορεί να προκαλέσει ζημιά στην

ταχύτητά του και κατά συνέπεια στην διαθεσιμότητά του. Από την στιγμή που κάποιες λειτουργίες του θα έχουν διακοπεί, οι workstations θα αδυνατούν να βρουν διαθέσιμο το λογισμικό όποια στιγμή το επιθυμούν και η καθυστέρηση θα είναι μεγάλη.

A-020

Σε αυτό το αγαθό, αυτό που μπορεί να συμβεί είναι να εισβάλει ένας κακόβουλος ιός στην ιστοσελίδα και είτε να κλέψει τους κωδικούς από τους πελάτες είτε να εισάγει πλαστά έγγραφα στην βάση δεδομένων που χρησιμοποιεί η ιστοσελίδα είτε να εισάγει πλαστά μηνύματα παραπλανώντας τον χρήστη που χρησιμοποιεί την ιστοσελίδα. Μια τέτοια απειλή μπορεί να προκαλέσει προβλήματα κυρίως στην ακεραιότητα του αγαθού.

A-021

Ένα φυσικό αρχείο δεν μπορεί να έχει τις ίδιες απειλές με ένα ψηφιακό. Το αρχείο των πελατών βρίσκεται στην ανοιχτή βιβλιοθήκη της αίθουσας αναμονής. Οπότε μία ξεκάθαρη απειλή από αυτό είναι το να κλέψει κάποιος τα αρχεία και όπως και σε άλλες περιπτώσεις που αναφέραμε παραπάνω να παραβιαστούν τα προσωπικά δεδομένα των ασθενών του εργαστηρίου. Αυτή η απειλή έρχεται και χτυπάει την εμπιστευτικότητα που θα έπρεπε να έχει κάθε αγαθό.

A-022

Το αρχείο που αφορά τους υπαλλήλους και τους προμηθευτές βρίσκεται στην βιβλιοθήκη του γραφείου του ιατρού. Αυτό σημαίνει ότι δεν υπάρχει τόσο μεγάλη η πιθανότητα για απειλή παρόμοια με του προηγούμενου αγαθού. Μια φωτιά όμως που μπορεί να συμβεί σε αυτό το εργαστήριο είναι δυνατόν να καταστρέψει τα αρχεία και να πάψουν να υφίστανται. Έτσι, η ιδιότητα της διαθεσιμότητας παύει να αντιπροσωπεύει αυτό το αγαθό, αφού σταματάει να είναι διαθέσιμο γενικά.

A-023

Το συγκεκριμένο αγαθό, όπως μας δηλώνεται στην περιγραφή, βρίσκεται φυλασσόμενο στον βοηθητικό χώρο, το οποίο κάνει αδύνατη την προσβολή του από οποιαδήποτε φυσική ή ανθρώπινη απειλή πέρα από την φωτιά.

A-024

Το αγαθό αυτό έχει πολύ απόρρητες πληροφορίες και είναι σημαντικό να μην διαρρεύσουν. Οπότε μία απειλή που θα μπορούσε να βλάψει το αγαθό αυτό είναι το να αποκαλύψει κάποιος τις πληροφορίες αυτές. Αυτό μπορεί να συμβεί από χρήστες εντός οργανισμού, δηλαδή από κάποιον υπάλληλο και με αυτόν τον τρόπο χάνεται η ιδιότητα της εμπιστευτικότητας και παραβιάζονται ξανά τα προσωπικά δεδομένα των ασθενών.

A-025

Φυσικές απειλές, όπως φωτιές και πλημμύρες βλάπτουν εξίσου εύκολα τον χώρο του εργαστηρίου-παρασκευαστηρίου, όπου βρίσκεται το αγαθό κατά την ανάλυση, αφού σε αυτό υπάρχει μια βοηθητική έξοδος που οδηγεί σε έναν μη περιφραγμένο χώρο.

Ο ανθρώπινος παράγοντας μπορεί να επηρεάσει το συγκεκριμένο αγαθό μόνο αν υποθέσουμε ότι γίνεται ο άνθρωπος που εκτελεί την δειγματοληψία να αλλοιώσει επίτηδες το περιεχόμενο του δείγματος, που θα δώσει λανθασμένα τελικά αποτελέσματα.

3.3 Ευπάθειες που εντοπίστηκαν

A-001 LabWS001

Μία ευπάθεια που υπάρχει είναι η ανεπαρκής διαδικασία πρόσληψης του προσωπικού ,διότι όπως αναφέρθηκε παραπάνω ,δυσαρεστημένο προσωπικό μπορεί να προκαλέσει την πρώτη απειλή. Το προσωπικό μπορεί να είναι δυσαρεστημένο διότι μπορεί να προσλήφθηκε αρχικά για μια θέση και να κατέληξε σε μια άλλη παρά την θέληση του λόγω έλλειψης προσωπικού. Η έλλειψη προσωπικού αυξάνει το φόρτο εργασίας του υπάρχοντος προσωπικού καθώς και την καθημερινή πίεση που δέχεται και αυτό έχει ως αποτέλεσμα την δυσαρέσκεια του. Επίσης όταν δεν υπάρχει επαρκές προσωπικό εκπαιδευόμενοι αναγκάζονται να αναλάβουν θέσεις ευθύνης ,χωρίς να έχει ολοκληρωθεί πλήρως η εκπαίδευση τους και χωρίς να υπάρχει κάποιος υπεύθυνος να τους επιβλέπει και να τους καθοδηγεί με αποτέλεσμα να οδηγούνται σε πολλά λάθη ,αμέλειες και παραβλέψεις.

Μία επιπλέον ευπάθεια είναι η έλλειψη περίφραξης του αύλειου χώρου του εργαστηρίου ενώ βρίσκεται σε πολυσύχναστο πεζόδρομο της Αθήνας και η έλλειψη ειδικών πορτών ασφαλείας με ηλεκτρονικές κλειδαριές που κρίνονται αναγκαία για την προστασία των αγαθών του εργαστηρίου.

Τέλος ευπάθεια του αιματολογικού αναλυτή μπορεί να θεωρηθεί η ανάγκη που έχει να συντηρείται καθημερινώς και ενδελεχώς ακολουθώντας την προτεινόμενη από τον κατασκευαστή συντήρηση καθώς έτσι ο χρόνος ζωής του και η ακρίβεια των αποτελεσμάτων του βασίζονται στην επιμέλεια και στην πειθαρχία του προσωπικού και στην συχνότητα με την οποία εκτελείται κατάλληλος έλεγχος τήρησης των διαδικασιών από τον υπεύθυνο του εργαστηρίου.

Σταθμοί Εργασίας A-002 PCWS001, A-003 PCWS002, A-004 PCWS003 , A-005 PCWS004 , A-006 PCWS005 , A-015 Laptop

Όπως αναφέρθηκε παραπάνω η έλλειψη περίφραξης του αύλειου χώρου του εργαστηρίου και η έλλειψη ειδικών πορτών ασφαλείας με ηλεκτρονικές κλειδαριές αποτελούν μια ευπάθεια του εργαστηρίου και εκτίθενται έτσι τα συγκεκριμένα αγαθά στις αντίστοιχες απειλές που αναλύθηκαν ήδη λεπτομερώς.

Μία ακόμα ευπάθεια του εργαστηρίου είναι ότι δεν διαθέτει μηχάνημα UPS έτσι ώστε σε περίπτωση αυξομειώσεων της τάσης του ρεύματος και σε διακοπή ρεύματος να μην παρεμποδιστεί η ομαλή λειτουργία των μηχανημάτων του εργαστηρίου.

Τέλος ευπάθεια είναι επίσης η ανεπαρκής ευαισθητοποίηση του προσωπικού σχετικά με θέματα ασφαλείας ,η οποία οδηγεί σε πολλά λάθη και αμέλειες ,τα οποία μπορεί να μην καταφέρουν να τα εντοπίσουν εγκαίρως και σε κάποιες περιπτώσεις ούτε καν οι ίδιοι.

A-007 PR0001, A-008 PR0002

Οι συγκεκριμένοι εκτυπωτές λόγω της παλαιότητας τους δεν έχουν τις λειτουργίες ασφαλείας που έχουν τα νεότερα μοντέλα όπως ,αναβαθμίσεις του firmware για την αντιμετώπιση των bugs και για την αποδοτικότερη λειτουργία του εκτυπωτή , κρυπτογράφηση και επιλογή ασφαλούς εκτύπωσης κατά την οποία για να πραγματοποιηθεί η εκτύπωση πρέπει να καταχωρηθούν πρώτα ο κωδικός χρήστη και πρόσβασης που έχουν οριστεί .Επίσης δεν έχουν τις λειτουργίες των καινούργιων μοντέλων όσον αφορά την ποιότητα της εκτύπωσης και ως αποτέλεσμα έχουμε χαμηλότερη ανάλυση και ευκρίνεια στα εκτυπωμένα έγγραφα . Η κύρια ευπάθεια τους λοιπόν είναι η παλαιότητα τους που επηρεάζει και τον χρόνο και την ποιότητα απόδοσης τους αλλά και την ασφάλεια τους.

A-009

Η τυχαία είσοδος ενός ανθρώπου στον βοηθητικό χώρο, ο οποίος πέφτει πάνω στους εξυπηρετητές και αυτοί σπάνε.

Η ανεπαρκής γνώση των υπεύθυνων για τους εξυπηρετητές όσον αφορά τα λειτουργικά συστήματα που υποστηρίζουν, δηλαδή η αμάθεια π.χ. της ανακοίνωσης

της Microsoft σύμφωνα με το λειτουργικό που χρησιμοποιεί το αγαθό που έχουμε εγκαταστήσει.

A010

Για το αγαθό αυτό δεν εντοπίζονται ευπάθειες από την στιγμή που περιλαμβάνει όλες τις ιδιότητες, οι οποίες θα συνεχίζουν να πληρούνται αν υποθέσουμε ότι ο χρήστης που του έχει δοθεί εξουσιοδότηση γνωρίζει τι πρέπει να κάνει.

A-011, A-012

Ελεύθερη πρόσβαση όλων σε όλους τους χώρους κάνει τα αγαθά switch να είναι ευάλωτα σε κάποιο μη σκόπιμο ανθρώπινο λάθος.

Το αγαθό είναι στον ίδιο χώρο ,στον βοηθητικό χώρο, με επικίνδυνα/εύφλεκτά υλικά, τις χημικές ουσίες.

A-013

Η μόνη ευπάθεια που μπορεί να θεωρηθεί ότι έχει το συγκεκριμένο αγαθό είναι οποιαδήποτε ζημία υποστεί από την μη σκόπιμη λανθασμένη σύνδεση με το υπόλοιπο δίκτυο και την επικοινωνία με το ISP cloud.

A-014

Μη σκόπιμη λανθασμένη διαμόρφωση των κανόνων του για τους φραγμούς εισόδου σχετικά με το επίπεδο εξουσιοδότησης του χρήστη (Με βάση τον πίνακα FMEA Risk Assessment_2023).

A-016

Μία ευπάθεια που παρατηρούμε στο αγαθό αυτό είναι είναι η ανασφαλής κωδικοποίηση. Αυτό σημαίνει ότι η επιχείρηση δεν έχει κωδικοποιήσει τα δεδομένα αυτά το οποίο κάνει πολύ εύκολο έναν κακόβουλο χρήστη να εισβάλει σε αυτό και να κλέψει τα δεδομένα.

A-017

Η ευπάθεια που μπορούμε εύκολα να δούμε ότι υπάρχει σε αυτό το αγαθό είναι η ανεξέλεγκτη πρόσβαση που μπορεί να υπάρχει στα δεδομένα αυτά. Από την στιγμή που δεν τονίζεται το γεγονός ότι σε αυτά τα δεδομένα έχουν πρόσβαση μόνο τα μέλη του προσωπικού που χρειάζονται για να επεξεργαστούν τα δεδομένα, σημαίνει ότι ο οποιοσδήποτε μέσα στο εργαστήριο μπορεί να τα δει.

A-018

Όσον αφορά τα windows 7 pro έχουν αρκετές ευπάθειες από το 2020 και μετά που η Microsoft σταμάτησε να παρέχει σε αυτά τα windows ασφάλεια. Συνεπώς υπάρχει έλλειψη σχεδίων ασφάλειας και οι ελέγχει που κάνει για κακόβολους ιούς είναι ανεπαρκής αφού δεν γίνονται πλέον ενημερώσεις.

A-019

Τα windows 10 pro όπως περιγράψαμε από πάνω έχουν ένα πολύ καλό σχέδιο ασφάλειας που δύσκολα μπορεί να παραβιαστεί. Παρόλα αυτά η ευπάθεια που βρίσκουμε εδώ είναι να υπάρχει εκ των έσω απειλή που έχει περισσότερους κωδικούς και άλλα στοιχεία προστασίας και μπορεί να εισβάλει στο λογισμικό αυτό για κακόβουλη χρήση.

A-020

Στην ιστοσελίδα του εργαστηρίου έχουν πρόσβαση όλοι οι πελάτες. Παρόλα αυτά η μόνη ταυτοποίηση που ζητείται είναι το username με τον κωδικό. Αυτό δεν είναι αρκετό για να εμποδίσει κάποιον χακερ. Συνεπώς δεν υπάρχουν επαρκείς έλεγχοι στην ιστοσελίδα αυτήν.

A-021

Το φυσικό αρχείο των πελατών έχει ως ευπάθεια την τοποθεσία στην οποία βρίσκεται. Βρίσκεται σε ένα ερμάριο της ανοιχτής βιβλιοθήκης στην αίθουσα αναμονής το οποίο σημαίνει ότι είναι εκτεθειμένα σε οποιονδήποτε βρίσκεται στον χώρο. Τα αρχεία αυτά είναι κανονικά απόρρητα και με την τοποθεσία που βρίσκονται δεν προστατεύονται.

A-022

Τα αρχεία αυτά βρίσκονται στο γραφείο του γιατρού το οποίο όπως βλέπουμε από την κάτοψη που μας δίνεται δεν έχει σύστημα αυτόματης πυρόσβεσης ή οτιδήποτε που θα μπορούσε να χρησιμεύσει σε τέτοια περίπτωση. Οπότε, η συνέπεια σε περίπτωση φωτιάς θα είναι καταστροφική και τα αρχεία αυτά θα χαθούν.

A-023

Η μη σκόπιμη κακομεταχείριση του αγαθού από τον αναλυτή.

A-024

Παρόλο που είναι δύσκολο να παραβιαστεί η ασφάλεια των δεδομένων αυτών, υπάρχει μία απειλή που περιγράψαμε παραπάνω από έναν υπάλληλο του εργαστηρίου. Οπότε μία ευπάθεια που έχει το αγαθό αυτό είναι ότι επιτρέπεται η πρόσβαση σε χρήστες οι οποίοι δεν είναι εμπιστοσύνης και δεν θα έπρεπε κανονικά να έχει πρόσβαση σε απόρρητα δεδομένα. Δηλαδή η διαδικασία πρόσληψης δεν είναι επαρκής με αποτέλεσμα να κινδυνεύει το αγαθό αυτό.

A-025

Ο μόνος τρόπος εξαερισμού του χώρου είναι να μένει η πόρτα μισάνοικτη καθ' όλη την διάρκεια λειτουργίας του εργαστηρίου, το οποίο επηρεάζει την διαδικασία της ανάλυσης λόγω μη καθαρού περιβάλλοντος.

3.4 Αποτελέσματα αποτίμησης

A-001 LabWS001

Το συγκεκριμένο αγαθό διαθέτει ένα αξιόπιστο, ασφαλές και σύγχρονο λογισμικό ,με αρκετές δικλείδες ασφαλείας και η διακινδύνευση των ιδιοτήτων του οφείλεται στην κακή χρήση του λογισμικού του από εξουσιοδοτημένους και μη χρήστες ,καθώς και στην κακή του συντήρηση από το αρμόδιο προσωπικό και στην αδυναμία ελέγχου τήρησης αυτής από τον υπεύθυνο. Τέλος η ανεπαρκής ασφάλεια της εγκατάστασης θέτει σε κίνδυνο και την ασφάλεια του συγκεκριμένου αγαθού.

Σταθμοί Εργασίας A-002 PCWS001, A-003 PCWS002, A-004 PCWS003 , A-005 PCWS004 , A-006 PCWS005 , A-015 Laptop

Όλοι οι παραπάνω υπολογιστές διαθέτουν σύγχρονα λειτουργικά συστήματα τα οποία τους προσφέρουν ασφάλεια ,ομαλή λειτουργία ,καλή απόδοση και άμεση ανάκτηση δεδομένων σε περίπτωση απώλειας τους. Αυτά που μπορούν να βλάψουν τα συγκεκριμένα αγαθά είναι η έλλειψη ασφάλειας των κτιριακών εγκαταστάσεων , η έλλειψη κατάλληλου εξοπλισμού σε περίπτωση προβλήματος ρευματοδότησης και η ανεπαρκής ενημέρωση και εκπαίδευση του προσωπικού σε θέματα ασφάλειας.

A-007 PR0001, A-008 PR0002

Οι συγκεκριμένοι εκτυπωτές είναι παλαιότερης γενιάς με αποτέλεσμα να μην μπορούν να αντιμετωπίσουν επαρκώς τις απειλές του σήμερα . Το κύριο πρόβλημα τους είναι η έλλειψη επαρκούς ασφάλειας ,καθώς εύκολα κακόβουλοι χρήστες θα μπορούν να αποκτήσουν πρόσβαση στα ευαίσθητα δεδομένα που διαχειρίζονται και

να τα τροποποιήσουν ή να τα δημοσιοποιήσουν παραβιάζοντας έτσι το δικαίωμα της ιδιωτικότητας των ασθενών και της επιχείρησης. Οι hackers μπορούν ακόμα να κρατούν γεμάτη την ουρά εκτύπωσης των εκτυπωτών δυσχεραίνοντας έτσι την ομαλή λειτουργία της επιχείρησης. Και τέλος η παραγωγικότητα και η απόδοση τους είναι πολύ χαμηλότερη σε σχέση με εκείνες των νέων μοντέλων.

A-009

Σύμφωνα με την παραπάνω ανάλυση για το συγκεκριμένο αγαθό συμπεραίνουμε ότι είναι ένα σχετικά ευάλωτο αγαθό που χρήζει την στήριξη περαιτέρω προστασίας. Οι απειλές αλλά και οι ευπάθειες του Web Server είναι αρκετά πιθανές να συμβούν, αφού δεν υπάρχει κάποια προστασία του χώρου που φυλάσσεται αλλά ούτε γενικότερα κάποιου άλλου χώρου του εργαστηρίου για να είναι δύσκολη η χρήση κάποιου υπολογιστή του συστήματος (που είναι συνδεδεμένος στο δίκτυο του συστήματος) από κάποιο κακόβουλο πρόσωπο. Αν προκληθεί κάτι από τα παραπάνω το σύστημα θα χάσει ένα μέγεθος της αξίας του, ανάλογο με το πόσο σημαντικό είναι στην λειτουργία του εργαστηρίου η σύνδεση του συστήματος του με το Web, και επί το πλείστων με την ιστοσελίδα του. Το γινόμενο της πιθανότητας να συμβούν τα παραπάνω με το μέγεθος της αξίας που χάνει το αγαθό δίνουν την επικινδυνότητα που προσδίδει το αγαθό στο σύστημα, η οποία σε αυτή την περίπτωση θεωρείται πως είναι μέτρια προς υψηλή.

A010

Το συγκεκριμένο αγαθό, αν και είναι εξυπηρετητής και αυτό, δεν είναι τόσο ευάλωτο σε απειλές ανθρώπινου παράγοντα, αλλά επηρεάζεται αρκετά από φυσικές απειλές και ευπάθειες που βασίζονται μόνο σε ανθρώπινα λάθη, τα οποία δεν είναι και τα πιο σύνηθες. Βέβαια αν τελικά προκληθεί ζημία εξαιτίας κάποιας απειλής/ευπάθειας επηρεάζεται σημαντικά η λειτουργία του συστήματος, αφού πια δεν υπάρχει η κοινή βάση, μέσα στην οποία ήταν αποθηκευμένα όλα τα στοιχεία ασθενών αλλά και οι αναλύσεις που έχουν διεξαχθεί. Με βάση την περιγραφή του εργαστηρίου βλέπουμε ότι τα στοιχεία αυτά υπάρχουν και σε φυσικά αρχεία αποθηκευμένα στον χώρο του εργαστηρίου, πράγμα που μειώνει την επίπτωση στο σύστημα, αλλά όχι σε μεγάλο βαθμό. Το γινόμενο λοιπόν αυτό μας δίνει επικινδυνότητα κατηγορίας μέτριας αφού ενώ μπορεί το κόστος των επιπτώσεων να είναι αρκετά υψηλή η πιθανότητα να συμβούν είναι σχετικά μικρή.

A-011, A-012

Η παραπάνω ανάλυση δείχνει ότι το αγαθό αυτό είναι κυρίως ευάλωτο σε φυσικές απειλές ή ευπάθειες που απορρέουν από την θέση που είναι εγκατεστημένα τα συγκεκριμένα αγαθά. Επομένως το αγαθό αυτό δεν έχει μεγάλη πιθανότητα να υποστεί κάποια ζημιά. Οι επιπτώσεις, όμως, που θα προκληθούν από κάποια απειλή που θα πραγματοποιηθεί θα είναι αρκετά σοβαρές για το σύστημα, καθώς αυτά τα δύο αγαθά είναι ο λόγος που υπάρχει επικοινωνία μεταξύ των συσκευών με άλλες συσκευές και του εξυπηρετητές, θέτοντας έτσι το σύστημα μας ένα ενιαίο ολοκληρωμένο σύστημα. Το γινόμενο αυτό λοιπόν δίνει μία μέτρια προς υψηλή επικινδυνότητα.

A-013

Το αγαθό Router αποτελεί το βασικότερο κομμάτι του δικτύου του συστήματος, πράγμα που θέτει οποιαδήποτε ζημιά μπορεί να προκληθεί σε αυτό πολύ σημαντική. Το συγκεκριμένο αγαθό διαθέτει όλες τις ιδιότητες, όπως αναλύσαμε, χαρακτηρίζοντας έτσι το αγαθό αρκετά ασφαλές. Το ενδεχόμενο το αγαθό αυτό να υποστεί κάποια ζημιά, όπως ήδη αναφέραμε, δεν είναι υψηλό και κυρίως θα οφείλεται σε φυσικές απειλές. Η επικινδυνότητα που προσδίδει το αγαθό, όμως, είναι σχετικά υψηλή, αφού οι επιπτώσεις που θα έχει στο σύστημα η ζημία του αγαθού είναι από τις σημαντικότερες ακόμη και αν η πιθανότητα να προκληθεί οποιαδήποτε ζημία είναι ελάχιστη.

A-014

Όμοια με το αγαθό Router, το Firewall περιλαμβάνει όλες τις ιδιότητες, εμπιστευτικότητα, διαθεσιμότητα και ακεραιότητα, κάνοντας αδύνατη την ύπαρξη οποιαδήποτε απειλής άλλης από της φυσικής. Αυτή που επηρεάζει το αγαθό σημαντικά είναι η ευπάθεια που αναφέραμε, η οποία (όπως μας δίνεται και στον πίνακα ISO27k FMEA Risk Assessment_2023) είναι πολύ σημαντική για το σύστημα, αφού έχει σημαντική συνέπεια στην εμπιστευτικότητα και ακεραιότητα του αγαθού. Οι επιπτώσεις δηλαδή που θα έχει στο σύστημα αν προκληθεί κάποια ζημία στο αγαθό είναι αρκετά σημαντικές για το ίδιο. Επομένως η επικινδυνότητα είναι αρκετά υψηλή (impact ranking 9).

A-016

Από όλα τα παραπάνω συμπεραίνουμε ότι το αγαθό αυτό είναι αρκετά καλά προστατευμένο, όμως χρειάζεται κάποιες παραπάνω λεπτομέρειες με σκοπό να γίνει τελείως ασφαλές σε συνδυασμό και με τα μέτρα προστασίας που θα πρέπει να πάρουμε και για την βάση στην οποία βρίσκονται.

A-017

Παρόμοια με το προηγούμενο το αγαθό αυτό είναι εξίσου προστατευμένο. Όμως επειδή περιέχει απόρρητες πληροφορίες και επειδή εντοπίσαμε κάποιες ευπάθειες που έχει είναι απαραίτητο να παρθούν επιπλέον μέτρα προστασίας για την κάλυψη όλων των ευπαθειών με σκοπό τα προσωπικά δεδομένα όλων να παραμείνουν ασφαλή και χωρίς να διαρρεύσουν.

A-018

Το αγαθό αυτό βλέπουμε ότι έχει πολλά προβλήματα σε θέματα ασφάλειας και είναι αρκετά ευάλωτο. Οι ευπάθειες του είναι πάρα πολλές και επειδή μία απειλή μπορεί να προκαλέσει μεγάλη ζημιά στο εργαστήριο πρέπει να κάνουμε το λογισμικό αυτό όσο πιο ασφαλή γίνεται χωρίς να παραλείπεται τίποτα.

A-019

Το λογισμικό αυτό είναι ένα από τα πιο καινούρια με αποτέλεσμα να έχει ένα πολύ καλό σύστημα ασφάλειας με πολλές μεθόδους που αποτρέπουν οποιαδήποτε κακόβουλη κίνηση. Για αυτόν ακριβώς τον λόγο πρέπει να εστιάσουμε στο ποιοι έχουν πρόσβαση σε αυτό και όχι στο πως να το κάνουμε ακόμα καλύτερο, εφόσον δεν είναι ένα ευάλωτο αγαθό.

A-020

Η ιστοσελίδα του εργαστηρίου είναι αρκετά ασφαλής, παρόλα αυτά λόγω των πληροφοριών που έχει οι κωδικοί πρόσβασης όπως αναφέραμε παραπάνω δεν επαρκούν και πρέπει να ενισχυθούν άμεσα τα μέτρα ασφαλείας που μπορούμε να πάρουμε και να γίνει η ιστοσελίδα που είναι ένα πολύ σημαντικό και χρήσιμο αγαθό όσο ασφαλέστερη γίνεται.

A-021

Το αγαθό αυτό είναι πάρα πολύ ευάλωτο και πρέπει οπωσδήποτε να ενισχυθεί η ασφάλεια του. Ο χώρος που βρίσκεται το κάνει αρκετά ευάλωτο καθώς και το γεγονός ότι δεν είναι σε ψηφιακή μορφή που είναι θεωρητικά ασφαλέστερα. Για αυτόν τον λόγο πρέπει να παρθούν μέτρα προστασίας ειδικά από την στιγμή που περιέχονται μέσα σε αυτά τα αρχεία δεδομένα που δεν πρέπει να χαθούν ή να κλαπούν.

A-022

Το αγαθό αυτό είναι σε καλύτερη κατάσταση από το προηγούμενο που ανήκουν στην ίδια κατηγορία λόγω της τοποθεσίας τους. Παρόλα αυτά δεν είναι απόλυτα ασφαλή και πρέπει να παρθούν μέτρα προστασίας με σκοπό ούτε να χαθούν αλλά ούτε να κλαπούν και τα απόρρητα αυτά δεδομένα να παραμείνουν απόρρητα.

A-023

Το αγαθό χημικές ουσίες φυλάσσεται στον βοηθητικό χώρο, επομένως είναι καλά προστατευμένο και μπορεί να προσβληθεί μόνο από κάποια φυσική απειλή που θα φέρει σε κίνδυνο όλο το εργαστήριο. Αυτό από ότι αντιλαμβανόμαστε δεν είναι πολύ πιθανό, αν όμως συμβεί τότε η καταστροφή που θα επιφέρουν οι ίδιες οι χημικές ουσίες θα είναι αρκετά σοβαρή για το σύστημα. Επομένως το γινόμενο βασίζεται στο μέγεθος της επίπτωσης που θα προκληθεί, αφού η πιθανότητα να συμβεί είναι αρκετά μικρή, το οποίο είναι αρκετά υψηλό αφού η επίπτωση θα είναι ουσιαστικά η καταστροφή του εργαστηρίου είτε από την φυσική απειλή (π.χ. την φωτιά) είτε από την μετέπειτα αντίδραση που θα προκαλέσουν οι χημικές ουσίες.

A-024

Συμπεραίνουμε, λοιπόν, από τα παραπάνω ότι το αγαθό αυτό είναι αρκετά προστατευμένο, όμως δεν είναι άτρωτο και μπορεί κι αυτό να απειληθεί. Η κύρια απειλή του είναι το ίδιο το προσωπικό οπότε δεν πρέπει να δίνεται πρόσβαση σε όλους οι οποίοι δουλεύουν στο εργαστήριο παρά μόνο σε έμπιστους υπαλλήλους.

A-025

Το αγαθό δείγμα επηρεάζεται και από ευπάθειες του συστήματος που είναι η ύπαρξη μολυσμένου αέρα λόγω μοναδικού μεθόδου εξαερισμού να είναι η μισάνοικτη πόρτα αλλά και από φυσικές απειλές. Αν υπάρξει ζημία στο συγκεκριμένο αγαθό σημαίνει ότι το αποτέλεσμα που θα δοθεί από την ανάλυση δεν θα είναι σωστό. Η πιθανότητα να συμβεί κάτι τέτοιο είναι σχετικά μεγάλη από την στιγμή που τα δείγματα επηρεάζονται σημαντικά από το περιβάλλον στο οποίο αναλύονται και μπορούν εύκολο να αλλοιωθούν από τυχόν μικρόβια που βρίσκονταν στο χώρο. Τα μικρόβια αυτά είναι λογικό να υπάρχουν λόγω αυτού που αναφέραμε παραπάνω (της μεθόδου εξαερισμού) αλλά και την σύνδεση των δωματίων εργαστήριο-παρασκευαστήριο με το χώρο δειγματοληψίας, τον οποίο επισκέπτονται όλοι οι ασθενείς. Συμπεραίνουμε λοιπόν ότι η επικινδυνότητα που προσδίδει στο σύστημα το συγκεκριμένο αγαθό είναι αρκετά υψηλή.

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

Πρώτο και κύριο βήμα στην προστασία των διαδικασιών του προσωπικού είναι η απονομή ευθυνών ,σύμφωνα με την οποία η ευθύνη για κάθε πράξη ή παράλειψη που προκαλεί μια προσβολή ενός ΠΣ μπορεί να κατανεμηθεί σε ένα ή πιο πολλά φυσικά πρόσωπα. Είναι σημαντικό οι διαδικασίες να είναι επαρκώς και λεπτομερώς ορισμένες ,έτσι ώστε κάθε μέλος του προσωπικού να γνωρίζει ποια είναι ακριβώς τα καθήκοντα του αλλά και οι ευθύνες του ,έτσι ώστε να δίνει μεγαλύτερη προσοχή στις λειτουργίες που εκτελεί καθημερινώς . Την αίσθηση ευθύνης του προσωπικού θα εντείνουν και αντίστοιχες ρήτρες στις συμβάσεις πρόσληψης του, οι οποίες θα τίθενται σε ισχύ σε περίπτωση εσκεμμένης ή μη απώλειας, κλοπής ,μερικής ή ολικής καταστροφής ενός ή περισσότερων αγαθών του εργαστηρίου. Με αυτόν τον τρόπο θα γίνεται σαφής η αξία των αγαθών που διαθέτει το εργαστήριο εξ αρχής, το πόσο σημαντική είναι η ομαλή λειτουργία και προστασία τους και η αυστηρότητα της ρήτρας θα λειτουργεί ως μέτρο πρόληψης εμφάνισης τέτοιου είδους απειλών (αμέλειας/ κακόβουλης ενέργειας) . Τέλος οι ρήτρες αυτές θα αποτελούν και ρήτρες εχεμύθειας ,καθώς το προσωπικό δεν θα πρέπει υπό καμία συνθήκη να επικοινωνήσει σε τρίτους ευαίσθητα δεδομένα της επιχείρησης ,όπως οικονομικά και περιουσιακά στοιχεία ,καθώς και απόρρητα ιατρικά στοιχεία ασθενών.

Δεύτερο και εξίσου σημαντικό βήμα είναι η πρόσληψη προσωπικού με σχετικό και επαρκές γνωστικό υπόβαθρο για τις θέσεις εργασίας που προσφέρει το εργαστήριο ,έτσι ώστε να αποφευχθούν μοιραία λάθη όπως για παράδειγμα μία λανθασμένη αιματολογική ανάλυση που θα οδηγήσει σε λανθασμένη διάγνωση και θεραπεία του ασθενούς θέτοντας έτσι σε κίνδυνο την υγεία του. Επίσης το προσωπικό πρέπει να είναι επαρκές στο πλήθος έτσι ώστε να βρίσκεται σε θέση να εξυπηρετεί ορθά και έγκαιρα το πλήθος των πελατών του εργαστηρίου αλλά και για να υπάρχει ένα υγιές εργασιακό κλίμα μέσα στο οποίο οι εργαζόμενοι θα μπορούν να είναι παραγωγικοί και να αποφεύγουν λάθη βιασύνης ή λάθη αμέλειας λόγω πίεσης φόρτου εργασίας και πίεσης χρόνου. Ως εκ τούτου θα είναι ευχαριστημένοι από την εργασία τους και θα

είναι λιγότερο πιθανό να προβούν σε κάποια κακόβουλη πράξη, που θα απειλούσε κάποιο από τα αγαθά του εργαστηρίου, προκειμένου να εκδικηθούν τον εργοδότη τους. Ακόμα ,σημαντική είναι και η πρόσληψη ειδικού προσωπικού ασφαλείας ,το οποίο θα είναι υπεύθυνο για την προστασία τόσο των αγαθών του εργαστηρίου όσο και του υπόλοιπου προσωπικού ,καθώς το εργαστήριο βρίσκεται σε πολυσύχναστο πεζόδρομο της Αθήνας και είναι μεγάλη η πιθανότητα να επιχειρήσει κάποιος να κλέψει ή να προσβάλει με οποιονδήποτε τρόπο τα αγαθά του εργαστηρίου .

Επιπλέον θα ήταν προτιμότερο η διαχείριση και η συντήρηση της ιστοσελίδας του εργαστηρίου να αποταθεί σε κάποιον ειδικό με κατάλληλο γνωστικό υπόβαθρο ώστε να μπορέσει να προστατευθεί όσο περισσότερο είναι δυνατό αυτό το αγαθό ,καθώς εκείνος θα γνωρίζει καλύτερα ποια μέτρα πρέπει να ληφθούν τόσο για την πρόληψη όσο και για την αντιμετώπιση των διάφορων απειλών . Οπότε είτε μπορεί να προσληφθεί κάποιος για την συγκεκριμένη θέση ,του οποίου αρμοδιότητα θα είναι και να λύνει οποιοδήποτε πρόβλημα προκύπτει στο δίκτυο του εργαστηρίου και στο υπόλοιπο hardware είτε μπορεί να αποταθεί μόνο η συντήρηση της ιστοσελίδας σε ένα έμπιστο εξωτερικό συνεργάτη που δραστηριοποιείται στον συγκεκριμένο κλάδο. Χάρης αυτήν την λύση θα μπορέσει και ο ιατρός του εργαστηρίου να αποφορτίσει το καθημερινό του πρόγραμμα και να αφοσιωθεί στα καθήκοντα του τομέα του ,στα οποία θα είναι πιο παραγωγικός.

Πολύ σημαντική ως μέτρο πρόληψης των απειλών κρίνεται και η εκπαίδευση και ευαισθητοποίηση του προσωπικού πάνω σε θέματα ασφαλείας των πληροφοριακών συστημάτων και των συνεπειών της μη ύπαρξής της ,καθώς και σε βασικές τεχνικές γνώσεις ,έτσι ώστε να διαχειρίζεται ορθά τον εξοπλισμό που του παρέχει το εργαστήριο για την διευκόλυνση της δουλειάς του. Υπάρχουν πολλά online και οικονομικά σεμινάρια μέσω των οποίων μπορεί να επιτευχθεί αυτό με κύρια θέματα την ασφάλεια κωδικών πρόσβασης, το κακόβουλο λογισμικό ,τους κινδύνους που ενέχει η σύνδεση σε δημόσιο WiFi , το phishing και πολλά άλλα. Καλό θα ήταν να ενημερωθούν και για την σωστή χρήση του hardware , για το τι απειλές μπορούν να το θέσουν σε κίνδυνο ,καθώς και για το ποιες πρακτικές οφείλουν να αποφεύγουν .

Επίσης όπως έχει ήδη αναφερθεί η καθημερινή και ενδελεχής συντήρηση του αιματολογικού αναλυτή οφείλει να ενταχθεί στην καθημερινότητα των εργαζομένων που τον διαχειρίζονται και να αποτελεί αναπόσπαστο κομμάτι των καθηκόντων τους, προκειμένου τα αποτελέσματα του να είναι πάντοτε το μέγιστο δυνατό ακριβή . Σε ένα μικροβιολογικό εργαστήριο η καθαριότητα είναι το άλφα και το ωμέγα και αυτό αφορά και το προσωπικό που εργάζεται στον χώρο δειγματοληψίας ,προκειμένου να εξασφαλισθεί η ασφάλεια των δειγμάτων και η αποφυγή αλλοίωσης τους . Και γενικότερα κάθε μέλος του προσωπικού οφείλει να διατηρεί τον χώρο εργασίας του καθαρό και τακτικό προκειμένου να αποφεύγονται λάθη λόγω ακαταστασίας και να μην μολύνονται τα δείγματα με ξένα σώματα. Ακόμα φαγητό και ποτό απαγορεύονται αυστηρά στους χώρους δειγματοληψίας και Εργαστηρίου-Παρασκευαστηρίου προκειμένου να διασφαλιστεί η ακεραιότητα των δειγμάτων ,αλλά και στον βοηθητικό χώρο όπου βρίσκονται τοξικές χημικές ουσίες που μπορεί να δηλητηριάσουν το φαγητό του προσωπικού και να θέσουν σε κίνδυνο την υγεία του. Επιπλέον θα πρέπει να απαγορεύεται η είσοδος κατοικίδιων στον χώρο του εργαστηρίου καθώς το τρίχωμα τους μπορεί να μολύνει το περιεχόμενο των δειγμάτων μέσω του αέρα.

Ακόμα ένα ζήτημα που τέθηκε είναι ότι το εργαστήριο δεν λαμβάνει πάντα γραπτή συναίνεση των ασθενών για να μοιραστεί τα προσωπικά τους δεδομένα με συνεργαζόμενους παρόχους υπηρεσιών ,γεγονός το οποίο δεν είναι σύννομο και οφείλει να διακοπεί. Τα δεδομένα προσωπικού χαρακτήρα υπόκεινται σε επεξεργασία η οποία διενεργείται σύμφωνα με τις αρχές της νομιμότητας, της αντικειμενικότητας και της διαφάνειας, λαμβάνοντας υπόψη τυχόν επιπλέον περιορισμούς που επιβάλλει ο σκοπός της επεξεργασίας. Ο σκοπός είναι βασικό στοιχείο του δικαιώματος και αποτελεί γνώμονα αξιολόγησης των υπολοίπων αρχών. Τα δεδομένα υπόκεινται σε επεξεργασία για καθορισμένους, ρητούς και νόμιμους σκοπούς, ενώ δεν υποβάλλονται σε περαιτέρω επεξεργασία κατά τρόπο ασύμβατο προς τους σκοπούς αυτούς. Τα

δεδομένα πρέπει να είναι κατάλληλα, συναφή και να περιορίζονται μόνο στον αναγκαίο βαθμό για τους σκοπούς της επεξεργασίας τους. Η αρχή της «ελαχιστοποίησης των τηρούμενων δεδομένων» (data minimisation) αποτελεί βασικό γνώμονα της νομιμότητας της επεξεργασίας. Τα δεδομένα πρέπει να είναι ακριβή και να επικαιροποιούνται, εφόσον απαιτείται. Επιπλέον, εύλογα μέτρα πρέπει να τηρούνται για την άμεση διαγραφή ή διόρθωση των δεδομένων και πρέπει να δίνεται η δυνατότητα στα υποκείμενα να διορθώνουν τα δεδομένα τους. Τα δεδομένα πρέπει να υποβάλλονται σε σύννομη και θεμιτή επεξεργασία με διαφανή τρόπο σε σχέση με το υποκείμενο των δεδομένων. Η επεξεργασία είναι σύννομη, μόνο εάν και εφόσον, το υποκείμενο των δεδομένων, έχει συναινέσει στην επεξεργασία των δεδομένων προσωπικού χαρακτήρα του, για έναν ή περισσότερους συγκεκριμένους σκοπούς και η επεξεργασία είναι απαραίτητη για τους σκοπούς των έννομων συμφερόντων που επιδιώκει εκτελών την επεξεργασία ή τρίτος, εκτός εάν έναντι των συμφερόντων αυτών υπερισχύει το συμφέρον ή τα θεμελιώδη δικαιώματα και οι ελευθερίες του υποκειμένου των δεδομένων που επιβάλλουν την προστασία των δεδομένων προσωπικού χαρακτήρα, ιδίως εάν το υποκείμενο των δεδομένων είναι παιδί. Η διαφάνεια, απαιτεί η ενημέρωση του υποκειμένου να είναι συνοπτική, εύκολα προσβάσιμη, σαφής και απλά διατυπωμένη. Τα δεδομένα προσωπικού χαρακτήρα, πρέπει να υποβάλλονται σε επεξεργασία κατά τρόπο που εγγυάται επαρκώς την ενδεδειγμένη ασφάλεια τους, την προστασία τους από μη εξουσιοδοτημένη ή παράνομη επεξεργασία, τυχαία απώλεια, καταστροφή ή φθορά, με τη χρήση κατάλληλων τεχνικών και οργανωτικών μέτρων. Σε περίπτωση μη συμμόρφωσης σύμφωνα με την αρχή της λογοδοσίας ο εκτελών την επεξεργασία φέρει την ευθύνη, συνεπώς οφείλει να είναι σε θέση να αποδείξει, την συμμόρφωση με τις αρχές που διέπουν την επεξεργασία των προσωπικών δεδομένων που στην προκείμενη περίπτωση είναι ο ιατρός ,ο οποίος θα διωχθεί νομικά .

Τέλος ,ο υπεύθυνος του εργαστηρίου οφείλει να διενεργεί ενδελεχή έλεγχο σε καθημερινή βάση για κάποιες διαδικασίες(πχ συντήρηση αιματολογικού αναλύτη, καθαριότητα των χώρων),σε μηνιαία βάση για άλλες και να βεβαιώνεται ότι κατά την διενέργεια αυτών των διαδικασιών τηρούνται τα αντίστοιχα πρότυπα που προβλέπονται. Αυτή η τακτική θα αποτελέσει ένα μέτρο ανίχνευσης απειλών ή ανίχνευσης και ανάλυσης περιστατικών ασφαλείας ,συνεισφέροντας έτσι στην προστασία των αγαθών του εργαστηρίου. Επίσης ο υπεύθυνος οφείλει να είναι οδηγός και σύμβουλος του προσωπικού και να είναι σε θέση να επιλύσει οποιοδήποτε ζήτημα προκύψει προτείνοντας τις κατάλληλες λύσεις ,εξασφαλίζοντας έτσι την ομαλή λειτουργία του εργαστηρίου.

4.2. Ταυτοποίηση και αυθεντικοποίηση

Με τον όρο ταυτοποίηση εννοούμε την διαδικασία με την οποία το υπολογιστικό μας σύστημα θα αναγνωρίζει ένα χρήστη. Ενώ την αυθεντικοποίηση, ως μέτρο προστασίας, ονομάζουμε την διαδικασία που αποσκοπεί στην επιβεβαίωση της ταυτότητας ενός χρήστη, δηλαδή τον έλεγχο του μοναδικού για τον συγκεκριμένο χρήστη χαρακτηριστικού. Η είσοδος στο υπολογιστικό σύστημα του εργαστηρίου είναι δυνατή από κάποια από τις συνδεδεμένες συσκευές του συστήματος στα αγαθά Switch αλλά και από την σύνδεση χρηστών μέσω Wi-Fi. Όπως έχουμε ήδη αναφέρει το εργαστήριο απασχολεί αρκετούς υπαλλήλους, με τις ειδικότητες αναλυτών, ιατρού, δειγματοληπτών, κ.τ.λ., οι οποίοι δεν χρησιμοποιούν με τους ίδιους σκοπούς το υπολογιστικό σύστημα και αυτός είναι ο λόγος που πρέπει να ληφθούν τα απαραίτητα μέτρα ταυτοποίησης και αυθεντικοποίησης του χρήστη που το χρησιμοποιεί κάθε φορά, ώστε να μην υπάρχουν βλάβες προερχόμενες από ανθρώπινη αμέλεια, αλλά ούτε από κάποια ανθρώπινη απειλή. Θα πρέπει, λοιπόν, να εντάξουμε κάποια μέτρα που θα εκπληρώνουν αυτήν την ταυτοποίηση και αυθεντικοποίηση του χρήστη.

- Θα πρέπει να δώσουμε σε όλα τα πρόσωπο που έχουν κάποια αρμοδιότητα στο εργαστήριο (υπάλληλοι), συγκεκριμένα ονόματα χρήστη (μοναδικά) και κωδικούς, με τους οποίους θα μπορούν γενικότερα να χρησιμοποιήσουν οποιαδήποτε συνδεδεμένη συσκευή στο σύστημα.
- Με βάση την διαβάθμιση των πληροφοριών, βλέπουμε ότι δεδομένα όπως οι δαπάνες του εργαστηρίου δεν θα πρέπει να είναι προσπελάσιμα από όλους τους χρήστες του συστήματος. Αυτό μπορεί να εξασφαλιστεί αν για την ταυτοποίηση του χρήστη που προσπαθεί να επεξεργαστεί μία συγκεκριμένη, υψηλής αξία, πληροφορία, γίνεται με άλλο τρόπο πέρα του ονόματος και κωδικού χρήστη, θα μπορούσε να υπάρχει ως δεύτερο διαπιστευτήριο το δακτυλικό αποτύπωμα.
- Όπως αναφέρθηκε ως μέτρο προστασίας όσον αφορά την ταυτοποίηση των χρηστών είναι η απόκτηση όλων των χρηστών κάποιο ονόματος που θα αναγνωρίζει το σύστημα και ένας κωδικός. Ο συνδυασμός των δύο αυτών στοιχείων θα είναι αυτό που θα τους ταυτοποιεί στο σύστημα. Ο κωδικός δεν θα πρέπει να αποθηκεύεται ούτε σε φυσική ούτε σε ηλεκτρονική μορφή, ώστε να μην δημιουργηθεί νέος κίνδυνος, όπως η κλοπή τους. Από την στιγμή, όμως, που θέλουμε το σύστημα να το αναγνωρίζει θα πρέπει να περιέχει κάπου αποθηκευμένους τους κωδικούς, για να γίνει αυτό, χωρίς να δημιουργήσει νέους κινδύνους, θα πρέπει να βρίσκονται αποθηκευμένοι σε μη αναγνωρίσιμη μορφή από την οποία δεν θα είναι εφικτή η ανάκτηση τους μορφής.
- Επιπλέον, να ορισθεί ένα χρονικό διάστημα, κατά το πέρας του οποίου θα πρέπει να αλλαχθούν οι κωδικοί των χρηστών, καθώς και να επιβληθεί η αλλαγή του κωδικού, που λειτούργησε βοηθητικά για την δημιουργία του «προφίλ» του χρήστη, κατευθείαν από όταν ο χρήστης τα παραλάβει.
- Η χρήση, παράλληλα, του απαραίτητου μέτρου σχολιασμού κατά την αλλαγή του κωδικού, δηλαδή αδύναμος, επαρκής, ισχυρός, και η αποτροπή αποθήκευσης αλλαγής του κωδικού αν αυτό σχολιάζεται ως «αδύναμο» δίνει μία ακόμη πιο δυνατή ταυτοποίηση, χωρίς ευκολία «μίμησης» του χρήστη, στο σύστημα.
- Η τοποθέτηση ενός ορίου για επανάληψη δοκιμής λανθασμένων κωδικών (μέχρι 3 φορές) και η ανάκτηση εισόδου στο σύστημα του συγκεκριμένου χρήστη μετά την επικοινωνία τους με τους αντίστοιχους αρμόδιους κάνει την ταυτοποίηση του χρήστη μία πολύ ακριβής λειτουργία του συστήματος.
- Άλλη μία τεχνική ταυτοποίησης και αυθεντικοποίησης χρηστών θα μπορούσε να ήταν με την δημιουργία Smartcards για τους υπαλλήλους, το οποίο όμως θα κόστιζε παραπάνω από την δημιουργία απλώς ενός «προφίλ» χρήστη.

4.3. Έλεγχος προσπέλασης και χρήσης πόρων

Ο έλεγχος προσπέλασης και χρήσης πόρων βασίζεται στην ύπαρξη της απαραίτητης ταυτοποίησης και αυθεντικοποίησης του χρήστη, την οποία αναλύσαμε στην ενότητα 4.2. Περιγράφει, με άλλα λόγια, το κατά πόσο το σύστημα μας εξασφαλίζει την ασφάλεια των αγαθών του, μέσω την ελεγχόμενης επεξεργασίας αυτών, από συγκεκριμένα πρόσωπα, καθώς και της προβολής ορισμένων πληροφοριών σε συγκεκριμένους μόνο χρήστες. Με την ανάλυση που κάναμε σχετικά με τα αγαθά της εγκατάστασης, βλέπουμε ότι ορισμένα όπως το Router, έχουν ήδη εγκατεστημένο κάποιο λογισμικό με το οποίο επιτρέπεται η πρόσβαση σε ορισμένες μόνο MAC διευθύνσεις, πράγμα που δίνει ένα σχετικό έλεγχο προσπέλασης στην σύνδεση με το δίκτυο αλλά και το διαδίκτυο. Από την άλλη πλευρά, η σύνδεση του δικτύου με τον εξυπηρετητή Web και διάφορες άλλες ευπάθειες του συστήματος, χρήζουν επιτακτική ανάγκη την προσθήκη ενός επιπρόσθετου ελέγχου για την προσπέλαση και την χρήση των πόρων του συστήματος. Με πόρους του συστήματος

μπορούμε να εννοούμε ακόμα και φυσικά αγαθά, όπως τους φυσικό αρχείο ασθενών, των οποίων ο έλεγχος προέρχεται από την προστασία της φυσικής κατάστασης του αντικειμένου που θα περιγράφει στην κατηγορία ασφάλεια εξοπλισμού. Με βάση τα μέτρα που λάβαμε για την ταυτοποίηση και την αυθεντικοποίηση των χρηστών ο έλεγχος προσπέλασης και χρήσης πόρων μπορεί να επιτευχθεί με μέτρα όπως τα εξής:

- Θα πρέπει σε κάθε όνομα χρήστη, το οποίο αντιστοιχεί σε κάποιον υπάλληλο, με βάση την αρμοδιότητα του να έχει πρόσβαση, στις απαραίτητες για τον ίδιο, υπηρεσίες, δηλαδή ο ιατρός θα έχει σίγουρα πρόσβαση στην βάση δεδομένων που περιέχει όλες τις αναλύσεις που έχουν πραγματοποιηθεί, ώστε να μπορεί να κάνει τους απαραίτητους ελέγχους αυτών αλλά και την ενημέρωση των ασθενών. Οι υπάλληλοι, από την άλλη, οι οποίοι απασχολούνται με την ιστοσελίδα του εργαστηρίου θα πρέπει να έχουν πρόσβαση στην εξυπηρετητή του Web για να έχουν όλες τις δυνατότητες τροποποίησης της. Βλέπουμε, δηλαδή ότι η σύνδεση του ιατρού με τις δυνατότητες που δίνει ο εξυπηρετητής Web για την διαχείριση της ιστοσελίδας δεν είναι απαραίτητη, ίσα ίσα λόγω μη γνωστικού υπόβαθρου για την διαχείριση μίας ιστοσελίδας θα μπορούσε να προκαλέσει κάποια ζημιά. Ιδιαίτερα σημαντική θα ήταν η βλάβη που θα προκαλούσε η σύνδεση κάποιου υπαλλήλου , ο οποίος δεν έχει τις απαραίτητες γνώσεις για την Oracle (την βάση δεδομένων), αφού αυτή θα είχε ως επίπτωση την κατάρριψη της ακεραιότητας του βασικού στοιχείου του συστήματος (τις τελικές αναλύσεις). Επομένως είναι φανερό ότι με την αντιστοιχία ονόματος χρήστη και επίπεδο εξουσιοδότησης, που θα αντιστοιχεί στις αρμοδιότητες του, δεν θα είναι δυνατή κάποια υποβίβαση του συστήματος από ανθρώπινη αμέλεια λόγω μη γνωστικού υπόβαθρου για το αντικείμενο. Αυτή η αντιστοιχία θα εκπληρώνεται από το σύστημα αν κάθε φορά που γίνει προσπάθεια χρήσης κάποιας ευαίσθητης πληροφορίας, όπως προσπάθεια σύνδεσης με την βάση δεδομένων να ξανά ζητείται όνομα και κωδικός χρήστη.
- Την απαραίτητη ασφάλεια στο σύστημα, όσον αφορά την προσπέλαση και χρήση των πόρων, μπορεί να την δώσει και η διαβάθμιση πληροφοριών με βάση τον χαρακτήρα του χρήστη στο σύστημα. Δηλαδή σε αυτό το μέτρο, οι, οριζόμενοι από κάποιο διοικητικό πρόχωπο του εργαστηρίου, υπεύθυνοι των πόρων χαρακτηρίζουν τις πληροφορίες με βάση το είδος και την κρισιμότητα του δεδομένου. Ουσιαστικά μπορεί να κάνει τον διαχωρισμό, σε πληροφορίες δημόσιας χρήσης, όπως είναι η σύνδεση με το διαδίκτυο ή προβολή της σελίδας ως πελάτης κ.τ.λ,. Σε πληροφορίες που χρήζουν, για την κατανόησή τους, τις απαραίτητες γνώσεις πάνω σε αυτές (π.χ. διαχειριστής ιστοσελίδας), και τέλος σε πληροφορίες εμπιστευτικού επιπέδου, όπως τα δεδομένα που βρίσκονται στην βάση μας, τα δεδομένα που αντιστοιχούν τα ονόματα χρήστη με τους κωδικούς, ή στοιχείων που πρέπει να γνωρίζουν μόνο ορισμένα μέλη του εργαστηρίου, όπως τις δαπάνες, τις εισφορές του εργαστηρίου. Η διάκριση αυτή των πόρων θα εξυπηρετήσει τελικά στην κατανομή των απαραίτητων εξουσιοδοτήσεων των χρηστών.
- Για την τήρηση της ασφάλειας των αγαθών, η οποία μπορεί να προσβληθεί από αμέλεια κάποιου χρήστη που δεν γνωρίζει το αντικείμενο, δώσαμε την λύση της κατηγοριοποίησης των χρηστών και της ανάλογης σε αυτούς εξουσιοδότηση στο σύστημα. Ένα ακόμη μέτρο προστασίας θα είναι να δοθεί η σαφή ανάλυση του τρόπου χρήσης του συγκεκριμένου πληροφοριακού συστήματος που τους παρέχει το εργαστήριο, εξασφαλίζοντας έτσι την γνώση του χρήστη για τους πόρους που μπορεί να χρησιμοποιήσει και τον τρόπο που του επιτρέπεται να το κάνει.
- Για τον έλεγχο προσπέλασης και χρήσης τον πόρων κρίνεται απαραίτητο να δημιουργηθούν σχετικά αρχεία καταγραφής όλων των ενεργειών που εκτέλεσε ο κάθε χρήστης, μαζί με το όνομα χρήστη. Με αυτόν τον τρόπο αν υπάρξει

κάποια «παράκαμψη» της επιτρεπόμενης για τον χρήστη είσοδο στο σύστημα θα είναι καταγεγραμμένη. Για να προκύψει ο σχετικός έλεγχος με βάση αυτά τα αρχεία, πρέπει να διασφαλίζεται η απαραίτητη προστασία και η ακεραιότητα τους. Αυτό θα προκύψει αν τα διαχειρίζεται μόνο ο υπεύθυνος ασφάλειας του εργαστηρίου, το οποίο σημαίνει ότι πρέπει να έχει μοναδική πρόσβαση με ειδική για αυτών εξουσιοδότηση, η οποία μπορεί να επιτυγχάνεται μέσω της ταυτοποίησης του από το σύστημα, με δαχτυλικό αποτύπωμα (ο οποίος τρόπος ταυτοποίησης χρήστη είναι ένας από τους πιο έμπιστους).

- Ως ένα επιπλέον μέτρο για τον έλεγχο προσπέλασης πόρων, μπορούν να εγκατασταθούν ορισμένες προσωπικές ερωτήσεις, οι οποίες θα έχουν άμεση σχέση με τον χρήστη που προσπαθεί να συνδεθεί. Οι συγκεκριμένες ερωτήσεις θα έχουν λάβει την απάντηση τους κατά την δημιουργία του «προφίλ» του χρήστη και θα είναι απαραίτητες μόνο για υψηλής αξίας πληροφορίας, όπως για την είσοδο του αρμόδιου χρήστη στα αρχεία καταγραφής δραστηριότητας.
- Η είσοδος στο σύστημα για ορισμένους υπαλλήλους μπορεί να είναι απαραίτητη και για εκτός γραφείου δραστηριότητες. Για παράδειγμα, ο ιατρός πρέπει να έχει μία σχετική ελευθερία στην χρήση του συστήματος και από το σπίτι του, καθώς ο ρόλος του είναι πολύ σημαντικός για την επιβεβαίωση των αποτελεσμάτων. Αυτό σημαίνει ότι θα πρέπει να δημιουργηθεί ένας συνδυασμός ισχυρότερης ταυτοποίησης του χρήστη αλλά και η κρυπτογράφηση των πληροφοριών κατά την μεταφορά τους από το ένα σύστημα στο άλλο. Κάθε προσπάθεια απομακρυσμένης πρόσβασης θα καταγράφεται στο αρχείο που δημιουργήθηκε ενώ μπορούμε να εντάξουμε, ως επιπλέον μέτρο προστασίας για την χρήση της συγκεκριμένης δυνατότητας, ένα ενημερωτικό μήνυμα που θα αποστέλλεται με κάθε προσπάθεια στο υπεύθυνο ασφαλείας αλλά και τον χρήστη που έχει αυτή την εξουσιοδότηση, π.χ. στον ιατρό.

4.4. Διαχείριση εμπιστευτικών δεδομένων

Το εργαστήριό μας έχει πολλούς πελάτες οι οποίοι δείχνουν εμπιστοσύνη σε αυτό και του δίνουν πολλά δεδομένα και πληροφορίες που δεν πρέπει να διαρρεύσουν και είναι πολύ εμπιστευτικές. Το εργαστήριο για κάθε πελάτη κρατάει το ιστορικό των εξετάσεων του και τα αποτελέσματά του. Σύμφωνα με τον υπεύθυνο, το εργαστήριο συμμορφώνεται με τις υποχρεώσεις για την προστασία δεδομένων προσωπικού χαρακτήρα και την διαχείριση προσωπικών δεδομένων. Παρόλα αυτά πιο πάνω εντοπίσαμε αρκετά κενά στην ασφάλεια των δεδομένων αυτών, όπως και των δεδομένων των υπαλλήλων και των προμηθευτών. Επιπλέον, το εργαστήριο δίνει πολλές φορές τις προσωπικές αυτές πληροφορίες στους συνεργαζόμενους παρόχους υπηρεσιών για την καλύτερη εξυπηρέτηση των ασθενών χωρίς όμως να έχει πάρει την συγκατάθεση τους. Οπότε για την προστασία τους πρέπει να ληφθούν κάποια περαιτέρω μέτρα προστασίας.

- Αρχικά είναι απαραίτητο να παίρνει το εργαστήριο την συγκατάθεση των πελατών του για να μοιραστεί τα δεδομένα τους έτσι ώστε να μην χάνεται η εμπιστοσύνη που υπάρχει μεταξύ του εργαστηρίου και των πελατών του.
- Πρέπει να χρησιμοποιείται ένας μηχανισμός εξουσιοδότησης, ο οποίος ελέγχει τα δεδομένα και τα προγράμματα καθώς επίσης επιβλέπει την υλοποίηση των πολιτικών εξουσιοδότησης. Ελέγχει δηλαδή ποιος χρήστης πάει να μπει στην βάση δεδομένων και δεν επιτρέπει την πρόσβαση σε μη εξουσιοδοτημένους χρήστες.
- Είναι απαραίτητο ο ιδιοκτήτης των δεδομένων και στην περίπτωση μας το εργαστήριο να αποφασίζει για το ποιος θα μπορεί να προσπελάσει τα δεδομένα μας και να κατέχει το δικαίωμα εκχώρησης δικαιωμάτων. Η

ιδιοκτησία δίνεται σε μία συγκεκριμένη οντότητα, ή σε έναν συγκεκριμένο υπάλληλο και δίνονται συγκεκριμένα δικαιώματα στον καθένα.

- Επιπλέον πρέπει να υπάρχει επιπλέον προστασία με κωδικούς και συνθηματικά με σκοπό να μπορούν να μπουν μόνο εξουσιοδοτημένοι χρήστες στην βάση δεδομένων και εάν κάποιος κάνει λάθος τα συνθηματικά για ένα συγκεκριμένο αριθμό και πάνω να αποκλείεται και να του απαγορεύεται η πρόσβαση. Για έναν τέτοιον χρήστη πρέπει να επανεξετάζεται η εξουσιοδότηση του για να έχουν δικαίωμα πρόσβασης.
- Ένα ακόμα μέτρο προστασίας που θα πρέπει να κάνει ο υπάλληλος που είναι υπεύθυνος για την βάση δεδομένων είναι να μην αφήνει εκτεθειμένο και ανοιχτό τον υπολογιστή που έχει πρόσβαση στα δεδομένα για να μην μπορεί κάποιος τρίτος να εκμεταλλευτεί το γεγονός αυτό και να τα κλέψει ή να τα αλλοιώσει.
- Τα δεδομένα των πελατών όπως και των υπαλλήλων είναι επίσης σε φυσική μορφή στις βιβλιοθήκες του εργαστηρίου. Πρέπει λοιπόν να προστατεύσουμε και αυτά τα δεδομένα. Αυτό που πρέπει να γίνει, είναι να μεταφερθούν τα αρχεία αυτά σε μη κοινόχρηστους χώρους δηλαδή σε κάποιον διαμορφωμένο χώρο που θα έχει πρόσβαση μόνο η γραμματεία που της χρειάζονται για την δουλειά της. Για να γίνει αυτό πρέπει να υπάρχει προστασία στην πόρτα ή στο ερμάριο που θα βρίσκονται. Για παράδειγμα, κάποιος κωδικός, δαχτυλικό αποτύπωμα ή αναγνώριση της ίριδας του ματιού.

4.5. Προστασία από τη χρήση υπηρεσιών από τρίτους

Όπως αναφέρθηκε και στα κεφάλαιο 4.2, 4.3 πρώτο και κύριο μέτρο προστασίας από την χρήση υπηρεσιών από τρίτους είναι η αυθεντικοποίηση και ταυτοποίηση των χρηστών που επιχειρούν να αποκτήσουν πρόσβαση στο σύστημα και ο έλεγχος προσπέλασης και χρήσης των πόρων του. Αυτό συνοπτικότερα θα επιτευχθεί με χρήση ισχυρών κωδικών πρόσβασης και βιομετρικών «κωδικών» (όπως το δακτυλικό αποτύπωμα) και με τήρηση διαβάθμισης όσον αφορά την πρόσβαση στα δεδομένα ,δηλαδή να μην μπορούν όλοι οι εξουσιοδοτημένοι χρήστες του συστήματος να έχουν πρόσβαση σε όλα τα διαθέσιμα δεδομένα. Ο έλεγχος πρόσβασης θα είναι βασισμένος σε ρόλους και θα επιτρέπει την πρόσβαση σε πόρους βασισμένο στο ρόλο που έχει το υποκείμενο στο σύστημα. Ο διαχειριστής του συστήματος ,που σε αυτήν την περίπτωση είναι ο υπεύθυνος ιατρός σε συνεργασία με κάποιον υπεύθυνο ασφαλείας , χρειάζεται μόνο να δημιουργήσει κάποιους ρόλους και να προσθέτει ή να αφαιρεί εργαζομένους από τη λίστα καθώς αυτοί έρχονται ή φεύγουν. Οι διαχειριστές του συστήματος αναθέτουν ένα ρόλο σε κάθε χρήστη και μετά δίνουν δικαιώματα πρόσβασης σε αυτό το ρόλο. Αυτό θα διαφυλάξει την ιδιότητα της διαθεσιμότητας των αγαθών ,αφού κανένας μη εξουσιοδοτημένος χρήστης είτε εσωτερικός είτε εξωτερικός δεν θα μπορεί να αποκτήσει πρόσβαση στα δεδομένα του συστήματος.

Επίσης βαρύνουσας σημασίας είναι και η ασφάλεια του δικτύου του εργαστηρίου όπως θα αναλυθεί παρακάτω ,το οποίο αποτελεί το μέσο πρόσβασης κακόβουλων χρηστών στο σύστημα σε περίπτωση που μείνει απροστάτευτο. Συνοπτικά χρειάζεται λοιπόν οι 2 servers να παραμείνουν προστατευμένοι με χρήση του Firewall , να είναι εξασφαλισμένη η ομαλή λειτουργία των λειτουργικών συστημάτων των υπολογιστών του δικτύου τα οποία τους προσφέρουν σύστημα antivirus για προστασία από επιθέσεις κακόβουλου λογισμικού και να εξασφαλισθεί η συνεχής διαθεσιμότητα του router ,το οποίο αποτελεί ένα από τα βασικά συστατικά του δικτύου , είτε με την αγορά ενός δεύτερου router για αποκλειστική χρήση των ασθενών είτε με την αλλαγή της συχνότητας εκπομπής στα μέγιστα GHz τα οποία μπορεί να υποστηρίξει το router μας.

Επιπλέον οι εκτυπωτές του εργαστηρίου είναι ο πιο αδύναμος κρίκος στο δίκτυο του εργαστηρίου καθώς λόγω παλαιότητας δεν διαθέτουν τα απαραίτητα μέσα προστασίας έναντι των hackers και πολύ εύκολα μπορούν να αποτελέσουν την κερκόπορτα μέσω της οποίας θα δοθεί μη εξουσιοδοτημένη πρόσβαση σε αυτούς στα ευαίσθητα δεδομένα του εργαστηρίου , όπως αντίγραφα ασφαλείας ,προσωπικά στοιχεία ασθενών καθώς και το ιατρικό ιστορικό τους . Είναι λοιπόν αναγκαία η αντικατάσταση τους ,ως μέσο προληπτικό μέσο προστασίας έναντι κακόβουλων επιθέσεων, μέσα σε ένα εύλογο χρονικό διάστημα.

Επίσης κρίνεται απαραίτητη η εγκατάσταση ηλεκτρονικών κλειδαριών στους χώρους, δηλαδή κλειδαριών οι οποίες ζητάνε κωδικό για να επιτρέψουν την πρόσβαση, όπως τον βοηθητικό χώρο, στην εσωτερική αλλά και στην βοηθητική είσοδο, στο εργαστήριο-παρασκευαστήριο, αλλά και στο γραφείο του ιατρού. Σε όλους τους χώρους του εργαστηρίου θα επιτρέπεται η πρόσβαση του ιατρού και στους χώρους του παρασκευαστηρίου, δειγματοληψίας και βοηθητικού χώρου θα επιτρέπεται η πρόσβαση μόνο των αναλυτών και του ιατρού, οι οποίοι διαθέτουν το κατάλληλο γνωστικό υπόβαθρο για την διαχείριση των αγαθών που βρίσκονται μέσα στους συγκεκριμένους χώρους. Στον βοηθητικό χώρο θα επιτρέπεται και η πρόσβαση οποιουδήποτε τεχνικού ασφαλείας κληθεί από τον υπεύθυνο του εργαστηρίου διότι στον χώρο αυτόν βρίσκονται και οι servers του εργαστηρίου. Αυτό το μέσο προστασίας μειώνει την απειλή που προέρχεται από την χρήση των συσκευών του συστήματος από κάποιον μη εξουσιοδοτημένο χρήστη αλλά και την φυσική ασφάλεια των αγαθών από κάποια ζημιά που θα προκαλούσε στις ίδιες τις συσκευές. Τέλος γενικότερα η κτιριακή ασφάλεια της εγκατάστασης όπως θα αναλυθεί παρακάτω είναι πολύ σημαντική για την προστασία από την χρήση υπηρεσιών από τρίτους καθώς θα τους καθιστά πολύ δύσκολη την είσοδο στην εγκατάσταση και κατ ‘ επέκταση την εκτέλεση κακόβουλων ενεργειών εις βάρος των αγαθών της.

4.6 Προστασία λογισμικού

Το λογισμικό είναι η πιο σημαντική κατηγορία αγαθών επειδή η απειλή στο λογισμικό μπορεί να προκαλέσει προβλήματα και σε άλλα αγαθά που βασίζονται σε αυτό. Πρέπει λοιπόν το λογισμικό να έχει λάβει όλα τα απαραίτητα μέτρα προστασίας και να είναι σίγουρο ότι καμία απειλή δεν θα μπορέσει να του προκαλέσει πρόβλημα. Τα μέτρα προστασίας που πρέπει να λάβει είναι:

- Η εγκατάσταση προγραμμάτων anti-virus τα οποία ελέγχουν κάθε κίνηση και κάθε αλλαγή που πάει να γίνει στο λογισμικό και σκανάρουν για τυχόν ιούς ή κακόβουλους χρήστες που θέλουν να εισβάλλουν στο λογισμικό και να διακόψουν τις λειτουργίες του.
- Επιπλέον πρέπει να εγκατασταθεί ένα τείχος προστασίας firewall έτσι ώστε να ρυθμίσει την κυκλοφορία στα δεδομένα ανάμεσα σε δύο δίκτυα και να προληφθεί κάποια επίθεση στο τοπικό δίκτυο και να τα αντιμετωπίσει.
- Όταν γίνει η εγκατάσταση των δύο παραπάνω είναι πάρα πολύ σημαντικό να γίνονται τακτικά οι ενημερώσεις τους για να παραμείνουν ασφαλή εφόσον ενημερώνονται με αποτελεσματική αντιμετώπιση νέων εχθρών.
- Το προσωπικό πρέπει να είναι ενημερωμένο όσον αφορά την ασφάλεια του λογισμικού, τι ελέγχους πρέπει να κάνει όταν λαμβάνει αρχεία από εξωτερικούς χρήστες και πώς να ενημερώνει τα προγράμματα κατά των ιών.
- Πρέπει επιπλέον το ίδιο να ενημερώνεται το λογισμικό κάθε φορά που βγαίνει νέα έκδοση η οποία είναι πιο ασφαλής από τις προηγούμενες και γίνεται πιο δύσκολη η εισβολή ενός κακόβουλου ιού.
- Τέλος, πρέπει ο χρήστης του λογισμικού να μην προσπαθεί να κατεβάσει αρχεία από άγνωστες πηγές που δεν ξέρει από πού προέρχονται και αν είναι

ασφαλής καθώς και να μην επισκέπτεται ιστοσελίδες οι οποίες δεν έχουν το σύμβολο ότι είναι ασφαλής και φιλικές προς τον χρήστη.

4.7 Διαχείριση ασφάλειας δικτύου

Η διαχείριση ασφάλειας δικτύου μπορεί να επιτευχθεί και με φυσικούς αλλά και με λογικούς ελέγχους. Αρχικά με ασφάλεια δικτύου εννοούμε την προστασία των ιδιοτήτων του δικτύου, δηλαδή της εμπιστευτικότητας, της διαθεσιμότητας και της ακεραιότητας του. Το δίκτυο όπως περιγράψαμε αποτελείται από τις συσκευές, όπως υπολογιστές, εκτυπωτές κ.τ.λ., από τους εξυπηρετητές, τα αγαθά switch, το router και το firewall. Αυτό σημαίνει ότι μπορεί να κινδυνέψει το δίκτυο από όλες τις ευπάθειες του συστήματος σχετικά με τα αγαθά που το αποτελούν, όπως και από τις αντίστοιχες απειλές τους. Το δίκτυο του συστήματος είναι πολύ σημαντικό για την λειτουργία του εργαστηρίου, όπως έχουμε ήδη αναφέρει, και σε αυτό στηρίζεται η εκτέλεση όλων των δραστηριοτήτων που αναλαμβάνει. Συμπεραίνουμε δηλαδή ότι η προστασία του συγκεκριμένου στοιχείου είναι από τις πιο σημαντικές ενέργειες που πρέπει να διασφαλίσει το σύστημα. Όπως έχουμε ήδη αναλύσει πολλά από τα αγαθά που αποτελούν το σύστημα περιέχουν λογισμικό το οποίο τους προσφέρει μια επιπλέον ασφάλεια από ανθρώπινες απειλές, αλλά υπάρχουν ακόμα αγαθά του δικτύου που πρέπει να λάβουν επιπρόσθετα μέτρα προστασίας για την συνολική τελικά ασφάλεια του δικτύου.

- Τα μέτρα προστασίας που αναφέρονται στην ασφάλεια της φυσικής κατάστασης των συγκεκριμένων αγαθών μπορεί να περιλαμβάνονται και σε παρακάτω ανάλυση (ασφάλεια εξοπλισμού) όμως κρίνεται απαραίτητη μία σύντομη αναφορά και σε αυτό το σημείο, καθώς είναι όντως σημαντική για την ασφάλεια του δικτύου. Αυτό σημαίνει ότι η αλλαγή θέσης, η επιπρόσθετη ασφάλιση συγκεκριμένων αγαθών, όπως οι εξυπηρετητές, μειώνουν όλους τους κινδύνους που προέρχονται από την εύκολη πρόσβαση τους από το κοινό και κατά συνέπεια αυξάνουν την ασφάλεια του δικτύου.
- Σημαντικό ρόλο στο δίκτυο του συστήματος έχουν οι εξυπηρετητές. Όπως βλέπουμε από το δικτυακό διάγραμμα συνδέσεων, η σύνδεση του αγαθού Database Server στο δίκτυο γίνεται με την «συνοδεία» του αγαθού Firewall, το οποίο χρησιμοποιείται για προστασία όπως ήδη γνωρίζουμε. Η εγκατάσταση ενός αντίστοιχου αγαθού και στην σύνδεση με τον εξυπηρετητή Web θα ενισχύσει την αξία του συγκεκριμένου αγαθού, προσδίδοντάς του τις ιδιότητες εμπιστευτικότητα διαθεσιμότητα και ακεραιότητα.
- Με την υπόθεση ότι στις συσκευές έχουν ενταχθεί τα κατάλληλα μέτρα για την ταυτοποίηση των χρηστών και την ανάλογη εξουσιοδότηση τους για την χρήση των πόρων, κρίνεται απαραίτητο να υπάρξει εγκατάσταση antivirus αλλά και κάποιου ανιχνευτικού μέσου κακόβουλων ενεργειών που στοχεύουν στην υποβάθμιση της ασφάλειάς του. Αυτά τα μέτρα είναι σημαντικά, διότι η σύνδεση που παρέχεται στους χρήστες με το διαδίκτυο αλλά και το Web (από τον σχετικό εξυπηρετητή) κάνει τους χρήστες, όπως έχουμε ήδη αναφέρει, πολύ ευάλωτους σε διάφορους κινδύνους στο διαδίκτυο, τους οποίους δεν είναι δυνατόν να γνωρίζουν.
- Παράλληλα μπορούν οι υπεύθυνοι ασφαλείας να κλειδώσουν ορισμένες σελίδες που βρίσκονται στο διαδίκτυο για τις οποίες γνωρίζουν ότι μπορεί να βλάψουν το σύστημα, προστατεύοντας έτσι το δίκτυο από την «μόλυνση» τους

από ιούς, οι οποίοι μεταφέρθηκαν σε αυτό μέσω των συσκευών που το αποτελούν.

- Ένα ακόμη μέτρο προστασίας θεωρείται και η αποσύνδεση από το δίκτυο όσων συσκευών δεν είναι απαραίτητων για την λειτουργία του. Για παράδειγμα η αποσύνδεση ενός εκτυπωτή από την στιγμή που δεν χρησιμοποιείται εκείνη την ώρα δίνει στο δίκτυο υψηλότερη ταχύτητα καθώς μειώνονται οι συνδεδεμένες συσκευές σε αυτόν.
- Η θέση των αγαθών switch στο σύστημα τους κάνει πολύ σημαντικούς για την ασφάλεια των δικτύων. Όπως γνωρίζουμε για την λειτουργία του συγκεκριμένου αγαθού είναι προϋπόθεση η ύπαρξη καλωδίων. Επομένως το είδος καλωδίων που θα επιλεγεί, τα οποία είδη διακρίνονται με βάση τις αντοχές σε παρεμβολές, θόρυβο και υποκλοπές.
- Βλέπουμε ότι ουσιαστικά το δίκτυο στηρίζεται από την ύπαρξη του αγαθού router, μέσω του οποίου είναι δυνατή η επικοινωνία των πόρων μεταξύ τους αλλά και με το διαδίκτυο. Επιπλέον το αγαθό αυτό δίνει πρόσβαση στο διαδίκτυο και σε εξωτερικούς χρήστες, ασθενείς (το οποίο το συμπεράναμε από την θέση που βρίσκεται στο εργαστήριο). Το router, ουσιαστικά, συνδέει τις συσκευές επιτρέποντας την ανταλλαγή πακέτων δεδομένων μεταξύ τους, αυτό το επιτυγχάνει αποδίδοντας σε καθεμία συσκευή μία τοπική διεύθυνση IP, εξασφαλίζοντας έτσι ότι τα δεδομένα φτάνουν στον σωστό προορισμό. Αυτό σημαίνει ότι για κάθε συνδεδεμένη συσκευή στο αγαθό αποδίδεται από το ίδιο μία ξεχωριστή διεύθυνση IP. Όπως αναφέραμε οι συσκευές που τελικά συνδέονται στο router δεν είναι μόνο τα δύο switch αλλά και όσα άτομα θέλουν να χρησιμοποιήσουν το διαδίκτυο στον χώρο του εργαστήριο. Από αυτό προκύπτει ότι το ενδεχόμενο της «υπερφόρτωσης» του δεν είναι τόσο δύσκολο να πραγματοποιηθεί, καθώς συνδέονται στο δίκτυο πολλές συσκευές ταυτόχρονα. Θα μπορούσαμε σε αυτό το πλαίσιο να προτείνουμε την αγορά ενός ακόμα router-modem με το οποίο θα εξυπηρετούνταν αποκλειστικά οι πελάτες. Από την στιγμή που η παραμονή των ασθενών στο εργαστήριο δεν γίνεται για μεγάλο χρονικό διάστημα αυτή η λύση δεν είναι και η πιο αποδοτική αφού θα έχει ορισμένη οικονομική επιβάρυνση στο εργαστήριο, χωρίς να αποδίδει σε βελτίωση κάποιας λειτουργίας του. Θα μπορούσε μία λύση να θεωρηθεί η αλλαγή του δικτύου σε κλειστό, ώστε να έχουν είσοδο μόνο οι συσκευές που συνδέονται σε αυτό. Άλλη μία λύση θα ήταν η αλλαγή της συχνότητας εκπομπής στα μέγιστα GHz τα οποία μπορεί να υποστηρίξει το router μας.

4.8 Προστασία από ιομορφικό λογισμικό

Υπάρχουν πάρα πολλά είδη ιών τα οποία μπορούν να προσβάλουν τα πληροφοριακά μας συστήματα. Μερικοί από αυτούς οι οποίοι μπορούν να υποβαθμίσουν την αξία των αγαθών μας είναι: ο ιός WannaCry ο οποίος έχει χτυπήσει πολλά νοσοκομεία, οπότε είναι ένας εχθρός για το μικροβιολογικό μας εργαστήριο. Αυτό που κάνει είναι να εκμεταλλεύεται τα κενά ασφαλείας που έχουν τα Windows με σκοπό να θέσει σε ομηρία τους υπολογιστές και να ζητά λύτρα σε Bitcoin, αλλιώς θα διέγραφε τα αρχεία του πληροφοριακού συστήματος. Ο ιός Trojan “BlackEnergy” είναι επίσης ένας ιός που θα μπορούσε να επιτεθεί στο μικροβιολογικό μας εργαστήριο εφόσον στοχεύει σε επιχειρήσεις. Ο συγκεκριμένος ιός εκμεταλλεύεται είτε κενά ασφάλειας που μπορεί να υπάρχουν στο λογισμικό είτε χρησιμοποιεί τεχνικές social engineering μέσω emails spear-phishing και παραπλανητικών εγγράφων είτε τα συνδυάζει και τα δύο. Τέλος, ο ιός Mirai μπορεί επίσης να προσβάλει το πληροφοριακό σύστημα μας αφού σκανάρει μέσω internet για συσκευές με εκτεθειμένες Telnet ports, στην συνέχεια χρησιμοποιεί default credentials για να κάνει login σε αυτές και να εγκαταστήσει το Mirai DdoS Malware.

- Για να προστατευθούμε από τον ιό WannaCry πρέπει να γίνεται τακτικό backup σε Critical Data και να προστατευθούν με αυτόν τον τρόπο τα αρχεία μας.
- Για τον ιό WannaCry αυτό που επίσης πρέπει να γίνει είναι να μην είναι ανοιχτές οι θύρες SMB ports [UDP 137, 138 and TCP 139, 445] και Disable SMBv1.
- Για να προστατευθούμε από τον ιό Trojan “BlackEnergy” πρέπει να συνδυάσουμε διάφορα μέσα προστασίας τα οποία είναι:
    - Να έχουμε ένα διοικητικό λειτουργικό σύστημα και να λάβουμε μέτρα που να βασίζονται στην ασφάλεια του δικτύου.
    - Να έχουμε συστήματα ελέγχου ασφάλειας και συστήματα που αξιολογούν τις ευπάθειες και τις διαχειρίζονται
    - Να γίνεται σε τακτά χρονικά διαστήματα έλεγχος των εφαρμογών
    - Να γίνεται έλεγχος πρόσβασης για τους εξουσιοδοτημένους χρήστες
    - Να ενημερωθεί το προσωπικό για όλα αυτά τα μέτρα προστασίας και για τον συγκεκριμένο ιό.

- Για να προστατευθούμε από το Mirai Botnet Malware δεν πρέπει να έχουμε default username και πρέπει να αλλάζουμε το password και το username ανά τακτά χρονικά διαστήματα καθώς και να χρησιμοποιούμε ισχυρούς κωδικούς πρόσβασης.
- Είναι σημαντικό να είμαστε προσεχτικοί με τα spam mails και να μην τα ανοίγουμε.
- Τέλος, πρέπει να γίνονται οι ενημερώσεις σε firmware και software.

4.9 Ασφαλής χρήση διαδικτυακών υπηρεσιών

Η διαδικτυακές υπηρεσίες γίνονται διαθέσιμες όταν υπάρχει επικοινωνία με κάποιο ISP, την επικοινωνία αυτή την παρέχει στο δίκτυο μας το router. Άρα η χρήση τους είναι δυνατή από όλα τα πρόσωπα που χρησιμοποιούν κάποια συσκευή συνδεδεμένη στο δίκτυο. Η σύνδεση με το διαδίκτυο για οποιοδήποτε σύστημα είναι πολύ σημαντική, καθώς του προσφέρει συνολικά περισσότερες δυνατότητες. Παρόλα αυτά εγγενή πολλούς κινδύνους από τους οποίους πρέπει να προστατεύσουμε το σύστημα, καθώς η «δηλητηρίαση» του δικτύου από κάποιον ιό που μπορεί να μεταφερθεί από την χρήση του διαδικτύου θα είναι καταλυτική για την λειτουργία του. Αρχικά, την σύνδεση με το διαδίκτυο την παρέχει το router σε όλες τις συνδεδεμένες συσκευές, τις οποίες χρησιμοποιούν τα μέλη του εργαστηρίου. Επομένως, η προστασία από τυχόν κινδύνους βασίζεται από το ίδιο το δίκτυο και πόσες ελευθερίες παρέχει στους χρήστες για την αναζήτηση στο διαδίκτυο αλλά και την ορθή χρήση των δυνατοτήτων που προσφέρει μία τέτοια σύνδεση από τους χρήστες. Με άλλα λόγια για την ασφαλή χρήση διαδικτυακών υπηρεσιών πρέπει να λάβουμε υπόψη τόσο τα μέτρα προστασίας του δικτύου όσο και την τήρηση συνετής χρήση του από τους υπαλλήλους.

- Το σύνολο των υπολογιστών που διαθέτει το εργαστήριο υποστηρίζουν λειτουργικό σύστημα Windows 10 Pro και MAC-OS, τα οποία έχουν ενσωματωμένο προσωπικό firewall, το οποίο ελέγχει την επικοινωνία από και προς τον προσωπικό υπολογιστή και προλαμβάνει τη διάδοση ιών και ανεπιθύμητων εφαρμογών. Συμπληρωματικά με αυτό μπορούμε να εγκαταστήσουμε και κάποιο antivirus, γνωστής και αξιόπιστης εταιρείας, ώστε να επιτύχουμε μεγαλύτερο ποσοστό ασφάλειας κατά την περιήγηση στο διαδίκτυο.
- Η πραγματοποίηση όλων των ενημερώσεων στα προγράμματα πλοήγησης στο Διαδίκτυο (όπως το chrome, Safari κ.τ.λ.), καθώς και η ενεργοποίηση των ενσωματωμένων χαρακτηριστικών προστασίας που διαθέτουν, όπως η φραγή των αναδυόμενων παραθύρων, διαχείριση των cookies είναι οι ελάχιστες δυνατές ενέργειες που μπορεί να κάνει ο χρήστης που χρησιμοποιεί το διαδίκτυο στον υπολογιστή του.

- Επίσης, θα μπορούσε ο υπεύθυνος ασφαλείας να θέσει ορισμένες παραμέτρους κατά την πλοήγηση στο διαδίκτυο των χρηστών, όπως το κλείδωμα ορισμένων ιστοσελίδων οι οποίες μπορεί να περιέχουν ιό, αλλά ακόμα και την απαγόρευση άσκοπης πλοήγησης, δηλαδή κλείδωμα ιστοσελίδων όπως το facebook, online παιχνιδιών ή άλλων τέτοιων εφαρμογών που δεν είναι απαραίτητες για κάποια διαδικασία του συστήματος, ώστε να μειωθούν οι πιθανότητες να προσβληθεί ο υπολογιστής από κάποιον ιό.
- Βασικά μέτρα προστασίας πρέπει να παρθούν από τους ίδιους τους χρήστες, ώστε να εξασφαλιστεί η ασφάλεια των διαδικτυακών υπηρεσιών που τους διαθέτει το σύστημα. Κάθε χρήστης του συστήματος θα πρέπει να γνωρίζει ότι αν υπάρχει κάποια ένδειξη, όπως η αισθητά πιο αργή εκκίνηση ή/και λειτουργία του συστήματος, ή εμφάνιση κάποιου σχετικού μηνύματος από το antivirus που έχει εγκατασταθεί, θα πρέπει να αναφερθεί στον υπεύθυνο ασφαλείας του εργαστηρίου. Παράλληλα οι χρήστες δεν θα πρέπει να εκμεταλλεύονται χωρίς κάποιον σκοπό του εργαστηρίου την σύνδεση με το διαδίκτυο. Όλες αυτές τις πληροφορίες πρέπει να τις γνωρίζει κάθε χρήστης ενός υπολογιστή, το οποίο μπορεί να συμβεί με την υπόδειξη του συγκεκριμένου χρήστη όταν του δοθεί κάποια συσκευή.
- Μία σημαντική διαδικασία του εργαστηρίου είναι η αποστολή, μέσω ηλεκτρονικού ταχυδρομείο, των αποτελεσμάτων στον ασθενή. Το ηλεκτρονικό ταχυδρομείο αποτελεί μία διαδικτυακή υπηρεσία και αυτό σημαίνει ότι το πρόσωπο του εργαστηρίου που θα αναλάβει την αποστολή θα πρέπει να γνωρίζει βασικούς κινδύνους που εγκυμονεί μία ηλεκτρονική αποστολή. Για παράδειγμα, θα πρέπει να γνωρίζει ότι δεν συνίσταται το άνοιγμα συνημμένων αρχείων ή URL που προέρχονται από άγνωστους αποστολείς.
- Η παρακολούθηση της δραστηριότητας του λογαριασμού του ηλεκτρονικού ταχυδρομείου από τον υπεύθυνο ασφαλείας, για τυχόν εξωτερικές συνδέσεις στον λογαριασμό ή αλλαγή κωδικού η οποία δεν προέκυψε από δική του υπόδειξη από τον αρμόδιο υπάλληλο.
- Η γνώση, παράλληλα, μόνο του υπεύθυνου ασφαλείας και του αρμόδιου για την αποστολή των email, ο οποίος θα είναι μοναδικός, του κωδικού πρόσβασης είναι πολύ σημαντικός, καθώς και η αλλαγή του ανά τακτά χρονικά διαστήματα.
- Όπως αναφέρθηκε η χρήση του ηλεκτρονικού ταχυδρομείου γίνεται για την αποστολή των αποτελεσμάτων στους ασθενείς, αυτό σημαίνει ότι οι πληροφορίες που μεταδίδουμε έχουν υψηλό βαθμό εμπιστευτικότητας και προκειμένου να υπάρχει άλλη μία δικλείδα προστασίας, από την στιγμή που στέλνονται μέσω διαδικτύου, καλούμαστε να εγκαταστήσουμε κάποιο είδος κρυπτογράφησης του μηνύματος που αποστέλλουμε. Ο κωδικός για το κλειδί της κρυπτογράφησης θα είναι ξεχωριστό ανά ασθενή, αλλά εύκολα μνημονικό από τον ίδιο, θα μπορούσε ας πούμε να είναι το τηλέφωνο επικοινωνίας του ή το όνομα του.

4.10 Ασφάλεια εξοπλισμού

Η ασφάλεια του εξοπλισμού στηρίζεται πολύ στην ασφάλεια της κτιριακής εγκατάστασης ,εφόσον είναι λογικό το ότι όταν το εγκατάσταση δεν είναι ασφαλής ,τα αντικείμενα που βρίσκονται μέσα σε αυτήν είναι εκτεθειμένα στις διάφορες απειλές που απειλούν και την ίδια. Επομένως χρειάζεται να τηρηθούν αρχικά όλα τα μέτρα ασφαλείας που αναλύονται στην ενότητα 4.11 προκειμένου να προχωρήσουμε στην ασφάλεια των επιμέρους συσκευών.

Ένα UPS (Αδιάλειπτη παροχή ρεύματος) είναι απαραίτητο για κάθε επιχείρηση καθώς αποτελεί μια συσκευή η οποία παρέχει ηλεκτρική ενέργεια σε άλλες συσκευές, στην περίπτωση διακοπής ρεύματος και αυξομειώσεων τάσης. Σε περίπτωση διακοπής του ρεύματος, οι συσκευές μπορεί λόγω της απότομης διακοπής λειτουργίας

να πάθουν βλάβη. Το UPS μας δίνει τη δυνατότητα να κρατήσουμε σε λειτουργία τις συσκευές μας και να τις τερματίσουμε σωστά, καθώς και να εξέλθουμε σωστά από το σύστημα χωρίς να χάσουμε ευαίσθητα δεδομένα. Βλάβη, όπως καμένα τροφοδοτικά ή ολική καταστροφή, στις συσκευές μπορεί να προκληθεί και από την αυξομείωση της τάσης του ρεύματος . Επίσης καλό θα είναι να μην συνδεθούν οι εκτυπωτές στο UPS καθώς καταναλώνουν πολλή ενέργεια κατά την έναρξη τους ,ενέργεια που είναι περισσότερο απαραίτητη για τις υπόλοιπες συσκευές του δικτύου.

Όπως αναφέρθηκε παραπάνω δεν θα πρέπει να επιτρέπεται η είσοδος κατοικίδιων στον χώρο του εργαστήριου προκείμενου να αποφευχθεί η απειλή πρόκλησης φυσικής ζημιάς στα αγαθά, όπως για παράδειγμα κάποιος σκύλος θα μπορούσε να θεωρήσει ότι το router είναι παιχνίδι και να το πετάξει κάτω και να σπάσει, με αποτέλεσμα την διατάραξη της ομαλής λειτουργίας του εργαστηρίου. Και καλό θα ήταν να αφιερωθεί ένας χώρος στην είσοδο του εργαστηρίου από την εξωτερική μεριά όπου θα μπορούν οι πελάτες να δένουν τα κατοικίδια τους έως ότου εξυπηρετηθούν .

Η συντήρηση του αιματολογικού αναλυτή είναι από τις κύριες προτεραιότητες που πρέπει να λαμβάνει υπόψιν του το προσωπικό και να τηρεί την διαδικασία της ευλαβικά και με συνέπεια. Σε καθημερινή βάση πρέπει να καθαρίζει το εξωτερικό του αναλυτή με ένα υγρό πανί για να αφαιρέσει τυχόν βρωμιά ή σκόνη,να ελέγξει ότι οι αναλώσιμες ουσίες βρίσκονται στο σωστό επίπεδο και ότι το δοχείο απορριμμάτων δεν είναι γεμάτο και να βεβαιωθεί ότι ο αναλυτής έχει βαθμονομηθεί σωστά. Σε εβδομαδιαία βάση πρέπει να καθαρίζεται το εξάρτημα του ανιχνευτή δείγματος με ένα πανί που δεν αφήνει χνούδι και να ελέγχεται για τυχόν φθορές , να ελέγχεται ότι η θερμοκρασία του είναι εντός των συνιστομένων ορίων και να βεβαιώνεται ότι όλα τα στοιχεία ελέγχου και οι ρυθμίσεις λειτουργούν σωστά. Σε μηνιαία βάση να ελέγχεται η απόδοση του αναλυτή χρησιμοποιώντας δείγματα ελέγχου ποιότητας, να επιβεβαιώνεται ότι το μηχάνημα είναι ακόμα σωστά βαθμονομημένο και ότι τα αποτελέσματα αυτού του ελέγχου είναι εντός αποδεκτών ορίων και να επιθεωρούνται η σωλήνωση και η ηλεκτρική σύνδεση του αναλυτή για τυχόν φθορές. Κάθε δεκαπέντε μέρες να διενεργείται μια προληπτική επιθεώρηση συντήρησης για να διαπιστωθεί οποιαδήποτε φθορά έχει προκύψει στα εξαρτήματα του αναλυτή.Και τέλος κάθε χρόνο να διενεργείται μία πλήρη βαθμονόμηση και πιστοποίηση του αναλυτή ,να αντικαθίστανται σπασμένα ή φθαρμένα εξαρτήματα του και να επιβεβαιώνεται ότι ο αναλυτής συνεχίζει και λειτουργεί σύμφωνα με τις οδηγίες του κατασκευαστή.

Όπως έχει ήδη αναφερθεί οι υπάρχοντες εκτυπωτές δεν είναι ασφαλείς για χρήση και χρήζουν άμεσης αντικατάστασης, καθώς μπορούν εύκολα να αποτελέσουν την εκκίνηση ρήγματος της ασφάλειας του δικτύου του εργαστηρίου εφόσον δεν διαθέτουν σύγχρονο firmware με τις κατάλληλες αναβαθμίσεις ασφαλείας και κάθε έγγραφο που έχει ή πρόκειται να εκτυπωθεί διατρέχει τον κίνδυνο υποκλοπής ή/και αλλοίωσης των δεδομένων του .

Τα καλώδια των συσκευών οφείλουν να μην είναι ορατά όσο το δυνατόν γίνεται αλλά να είναι αποθηκευμένα μέσα σε ειδικά κανάλια εγκατεστημένα στους τοίχους για να αποφευχθεί ο κίνδυνος αλλοίωσης ή εσκεμμένης καταστροφής τους, η οποία θα έχει ως αποτέλεσμα την διακινδύνευση κάποιου ή κάποιων αγαθών (πχ αιματολογικού αναλυτή και των αποτελεσμάτων του πριν αυτά μεταφερθούν στην βάση δεδομένων του εργαστηρίου).

Ακόμα το προσωπικό οφείλει να είναι προσεκτικό κατά την σύνδεση και την αποσύνδεση των διάφορων συσκευών στην παροχή του ρεύματος πιάνοντας τα καλώδια μόνο από τις κατάλληλες υποδοχές (φις) για να μην υποστούν τα καλώδια ζημιά και απογυμνωθούν από το εξωτερικό προστατευτικό τους στρώμα ,διότι αν συμβεί αυτό θα υπάρχει ο κίνδυνος ηλεκτροπληξίας και ο κίνδυνος η συσκευή να πάψει να είναι διαθέσιμη. Οποιοδήποτε καλώδιο υποστεί την παραμικρή φθορά πρέπει να αντικαθίσταται το συντομότερο δυνατό.

Επίσης θα πρέπει οι ανεμιστήρες που διαθέτουν τα διάφορα μηχανήματα hardware (πχ λάπτοπ, server) να ελέγχονται τακτικά και να καθαρίζονται σε

περίπτωση συσσώρευσης σκόνης καθώς έτσι θα αποφευχθεί η υπερθέρμανση τους μαζί με τον κίνδυνο εκδήλωσης πυρκαγιάς, καθώς το ξέσπασμα μίας πυρκαγιάς στον χώρο του εργαστηρίου όπου υπάρχουν και εύφλεκτα υλικά θα μπορούσε να αποβεί μοιραία τόσο για τα αγαθά του εργαστηρίου που θα μετατρέπονταν σε στάχτη όσο και για τους ανθρώπους που θα βρίσκονταν στον χώρο εκείνη την στιγμή.

4.11 Φυσική ασφάλεια κτιριακής εγκατάστασης

Η συνεχής συντήρηση του κτιρίου πρέπει να αποτελεί σκοπό του υπεύθυνου του εργαστηρίου καθώς συμβάλει στη διατήρηση της αξίας του ακινήτου, στην πρόληψη των ατυχημάτων των εργαζομένων και επισκεπτών του εργαστηρίου και στην ασφάλεια των αγαθών που βρίσκονται μέσα σε αυτό. Είναι απαραίτητη λοιπόν η εκτίμηση κινδύνου για το κτίριο από έναν μηχανικό , ειδικότερα αν το κτίριο είναι παλιό, σε περίπτωση που δεν έχει ήδη εκτελεστεί, έτσι ώστε να προταθούν από εκείνον οι κατάλληλες εργασίες συντήρησης .

Επιπλέον δεν πρέπει να υπάρχουν εκτεθειμένα ηλεκτροφόρα καλώδια σε κανέναν χώρο(εξωτερικό /εσωτερικό) του εργαστηρίου καθώς ο κίνδυνος ηλεκτροπληξίας του προσωπικού ή οποιουδήποτε άλλου θα είναι μεγάλος και μπορεί να οδηγήσει σε εγκαύματα και σοβαρές βλάβες, ακόμη και θάνατο.

Χρειάζεται να ληφθεί μέριμνα για τις υδραυλικές εγκαταστάσεις του κτιρίου ώστε να βρίσκονται πάντοτε σε καλή κατάσταση, ώστε να αποφευχθεί το ενδεχόμενο της απειλής από πλημμύρα ,η οποία θα βραχυκύκλωνε όλες τις ηλεκτρονικές συσκευές του εργαστηρίου και θα κατέστρεφε και τα αρχεία που φυλάσσονται σε έντυπη μορφή εντός του χώρου, καθώς και τα δείγματα.

Επίσης η περίφραξη του αύλειου χώρου καθώς και η τοποθέτηση πορτών ασφαλείας σε κάθε είσοδο και έξοδο του εργαστηρίου είναι αναγκαίες ,καθώς θα προστατεύουν τα αγαθά του από οποιαδήποτε ανεπιθύμητη και κακόβουλη εισβολή τρίτου. Υπάρχουν πόρτες ασφαλείας που κλείνουν μέσα σε λίγα δευτερόλεπτα μόνες τους αφότου κάποιος τις ανοίξει ,πράγμα το οποίο αποτελεί προληπτικό μέτρο ασφαλείας για την αμέλεια του προσωπικού να ξεχάσει φεύγοντας κάποια πόρτα ανοικτή. Επιπλέον αν και τετριμμένο αξίζει να αναφερθεί ότι μετά το πέρας του ωραρίου λειτουργίας του εργαστηρίου όλες οι πόρτες πρέπει να κλειδώνονται για την αποφυγή κλοπής ή βανδαλισμού των αγαθών του εργαστηρίου. Και όπως αναφέρθηκε και παραπάνω είναι πολύ σημαντική και η εγκατάσταση ηλεκτρονικών κλειδαριών στις πόρτες εντός του χώρου του εργαστηρίου ως ένα πρόσθετο μέτρο πρόληψης της μη εξουσιοδοτημένης πρόσβασης στα αγαθά του εργαστηρίου.

Ακόμα το δάπεδο όλων των χώρων του εργαστηρίου θα πρέπει να είναι ομαλό χωρίς ζημιές και λακούβες επειδή για παράδειγμα αν ένα μέλος του προσωπικού μεταφέρει τα δείγματα από τον χώρο δειγματοληψίας στον χώρο του παρασκευαστηρίου και σκοντάψει λόγω ανωμαλίας του δαπέδου (πχ έλλειψη ενός πλακακίου) θα του πέσουν οι σωλήνες με τα δείγματα και θα σπάσουν οδηγώντας έτσι σε απώλεια αυτού του αγαθού. Ένα άλλο πιθανό σενάριο είναι κάποιος ασθενής που κρατάει κάποιο υγρό στα χέρια του όπως ένα ποτήρι νερό ,καθώς περπατάει να σκοντάψει και το νερό να χυθεί σε κάποια ηλεκτρονική συσκευή ,όπως το router ,με αποτέλεσμα το βραχυκύκλωμα αυτού του αγαθού και πιθανώς την ολική καταστροφή του καθώς και την ισοπέδωση του δικτύου του εργαστηρίου, που θα είχε ως αποτέλεσμα την παύση όλων των λειτουργιών του εώς ότου αποκατασταθεί η βλάβη.

Ως μέτρο ανίχνευσης θα ήταν χρήσιμο να τοποθετηθούν κάμερες ασφαλείας (μία σε κάθε εσωτερικό και εξωτερικό χώρο) και στον κάθε έναν από αυτούς να είναι στραμμένες προς το αγαθό που προστατεύουν. Για παράδειγμα στον χώρο του παρασκευαστηρίου θα μπορούσε να τοποθετηθεί σε μία συγκεκριμένη γωνία έτσι ώστε να «βλέπει» όσο είναι δυνατόν και τα τρία αγαθά του χώρου (2 σταθμοί εργασίας και

αιματολογικός αναλυτής).Αυτό θα συνεισφέρει στην εποπτεία όλων των χώρων την ίδια στιγμή από το προσωπικό ασφαλείας ,το οποίο με το που εντοπίσει μία ύποπτη κίνηση θα είναι σε θέση να επέμβει εγκαίρως και να διασφαλίσει την ακεραιότητα του αγαθού που βρίσκεται σε κίνδυνο ,αλλά και στην ταυτοποίηση ενός πιθανού δράστη που θα καταφέρει να παρεισφρήσει στο εργαστήριο και να υποβαθμίσει την αξία των αγαθών του, δηλαδή να τους προκαλέσει ζημιά . Επομένως σε περίπτωση που ο δράστης αυτός κλέψει είτε εξοπλισμό είτε πληροφορίες αυτά θα μπορέσουν να ανακτηθούν ενώ σε περίπτωση που απλά προκαλέσει υλικές ζημιές στον εξοπλισμό θα μπορέσει ο υπεύθυνος του εργαστηρίου να τον διώξει νομικά και να διεκδικήσει αποζημίωση από εκείνον.

Το προσωπικό ασφαλείας εφόσον προσληφθεί θα μεριμνήσει για την ασφάλεια τόσο του εξοπλισμού όσο και του συνόλου της εγκατάστασης ,κάνοντας τακτικές περιπόλους κυρίως στα «τρωτά» σημεία της εγκατάστασης και ελέγχοντας ανά τακτά χρονικά διαστήματα το live video από τις κάμερες ασφαλείας προκειμένου να εντοπίσει άμεσα οποιαδήποτε ύποπτη ενέργεια και να λάβει ανάλογη δράση για την διαφύλαξη των ιδιοτήτων των αγαθών του εργαστηρίου .

Επίσης χρήσιμη θα ήταν η εγκατάσταση επιπλέον αισθητήρων πυρανίχνευσης, πυροσβεστήρων και αυτόματου συστήματος πυρόσβεσης σε όλους τους εσωτερικούς χώρους έτσι ώστε σε περίπτωση ξεσπάσματος πυρκαγιάς να αποφευχθεί η ολική ή ακόμα και η μερική ζημιά του εξοπλισμού ή του φυσικού αρχείου που τηρείται.

Τέλος η εγκατάσταση ενός ειδικού ηλεκτρομηχανολογικού εξοπλισμού (ειδικές χοάνες εξαερισμού,φίλτρα αέρος κλπ) είναι απαραίτητη, αφού το εργαστήριο βρίσκεται σε ισόγειο και έχει άμεση επαφή με πολυσύχναστο πεζόδρομο ενώ παράλληλα εξυπηρετεί μεγάλο πλήθος ανθρώπων ημερησίως (κάνοντας την πόρτα να παραμένει μισάνοικτη για τον αερισμό μία λύση μη επαρκή).Το γεγονός ότι στο εργαστήριο γίνεται η ανάλυση των δειγμάτων καθιστά επιτακτική ανάγκη να μην επηρεάζεται η κατάσταση των δειγμάτων από κανένα εξωτερικό παράγοντα που μπορεί να αλλοιώσει το αποτέλεσμα. Επομένως είναι εμφανές ότι το αγαθό του ειδικού ηλεκτρομηχανολογικού εξοπλισμού έχει ύψιστη αξία στην λειτουργία του εργαστηρίου. Όσον αφορά όμως την αξία ως έννοια κόστους, η τόσο αναγκαία εγκατάσταση του ορισμένου ειδικού εξαερισμού σε όλους τους χώρους κάνει εμφανές ότι θα υπάρχει μεγάλη χρηματική επιβάρυνση, η οποία, όμως, μπορεί να βελτιωθεί αν σε χώρους που δεν επηρεάζουν τις διαδικασίες της δειγματοληψίας και της ανάλυσης αποτελεσμάτων, εγκατασταθούν κλασικοί εξαερισμοί (π.χ. στον χώρο αναμονής, στο γραφείο του ιατρού, κτλ), και με διάφορους άλλους τρόπους, οι οποίοι όμως δεν θα αλλοιώνουν εν τέλη την σημαντικότητα του αγαθού.

5. ΣΥΝΟΨΗ ΚΡΙΣΙΜΩΝ ΑΠΟΤΕΛΕΣΜΑΤΩΝ

Η παραπάνω ανάλυση αντιπροσωπεύει τα βασικά αγαθά του συστήματος που το καθένα ξεχωριστά έχει την δική του θέση, λειτουργία και αξία μέσα στο εργαστήριο. Σε αυτά βασίζεται η λειτουργία του συστήματος του εργαστηρίου και αξίζουν όλα να προστατευθούν με τον καλύτερο δυνατό τρόπο. Πιο πάνω αναφέραμε τα μέτρα προστασίας για κάθε αγαθό ξεχωριστά που πρέπει να παρθούν για να έχουμε ένα ασφαλές από όλες τις απόψεις εργαστήριο. Επειδή όμως δεν είναι δυνατόν να φτιάξουμε και να διορθώσουμε την ασφάλεια όλων των αγαθών ταυτόχρονα πρέπει να τα ιεραρχήσουμε και να ξεκινήσουμε την διαδικασία της καλύτερης προστασίας στα αγαθά που έχουν την μεγαλύτερη αξία.

Τα πιο σημαντικά αγαθά, λοιπόν, είναι αυτά τα οποία αν προσβληθούν από κάποια απειλή δεν θα μπορεί το εργαστήριο είτε να λειτουργήσει γενικά είτε να εγγυηθεί στους πελάτες τους για την προστασία των εξετάσεων και των προσωπικών δεδομένων τους. Όσον αφορά την λειτουργία του εργαστηρίου, δεν μπορεί να λειτουργήσει σωστά αν πάθει κάποια ζημιά ο αιματολογικός αναλυτής εφόσον χωρίς αυτόν δεν μπορεί να γίνει η ανάλυση των εξετάσεων που είναι και η βασική λειτουργία του εργαστηρίου. Για τον ίδιο ακριβώς λόγο είναι σημαντικές και οι χημικές ουσίες από την στιγμή που είναι απαραίτητες για την ανάλυση των εξετάσεων. Σε αυτά τα δύο αγαθά το εργαστήριο πρέπει να δώσει ιδιαίτερη βάση. Τα αγαθά αυτά έχουν μεγάλο ποσοστό επικινδυνότητας όχι μόνο επειδή είναι ευάλωτα σε πολλών ειδών απειλές που περιγράψαμε ήδη αλλά και επειδή οι επιπτώσεις αν προσβληθούν από μία απειλή είναι καταστροφική για το εργαστήριο εφόσον δεν θα μπορεί να λειτουργήσει αν δεν τα φτιάξει όπως πριν, κάτι το οποίο θα είναι δύσκολο επειδή έχουν πολύ υψηλή οικονομική αξία.

Την ίδια αξία όμως έχουν και αγαθά που σχετίζονται με τα πληροφοριακά συστήματα του εργαστηρίου. Τέτοια αγαθά είναι οι σταθμοί εργασίας οι οποίοι δίνουν πρόσβαση στα δεδομένα, οι servers που αποθηκεύουν τα απαραίτητα στοιχεία και τις εξετάσεις των ασθενών, τα δεδομένα μας ως σύνολο αφού είναι προσωπικά δεδομένα και είναι απαραίτητο να δοθεί βάση στην προστασία τους. Για την προστασία των προσωπικών δεδομένων πρέπει να κρατηθούν ασφαλή και τα λειτουργικά συστήματα εφόσον όπως περιγράψαμε και παραπάνω αν προσβληθούν από κάποιον ιό υπάρχει μεγάλη πιθανότητα να μην μείνουν ακέραια τα δεδομένα, όπως και η ιστοσελίδα για τον λόγο ότι αν μπει ένας κακόβουλος χρήστης τα δεδομένα θα μείνουν εκτεθειμένα σε αυτόν. Το router είναι επίσης ένα αγαθό με υψηλή αξία εφόσον συνδέει όλες τις συσκευές στο διαδίκτυο δίνοντας τους πολλές περισσότερες δυνατότητες και επιπλέον συμβάλει στην επικοινωνία όλων των συσκευών μεταξύ τους. Τέλος, πρέπει να φροντίσουμε οπωσδήποτε για την ασφάλεια των switchers γιατί είναι απαραίτητα για την επικοινωνία των συσκευών μεταξύ τους άρα και για την ορθή λειτουργία του. Τα παραπάνω αγαθά είναι επίσης αρκετά ευάλωτα και έχουν αρκετά υψηλό ποσοστό επικινδυνότητας διότι αν πάθει κάποια ζημιά κάποιο από αυτά η επικοινωνία στο εργαστήριο θα διακοπεί και θα είναι δύσκολο να συνεχίσει η ομαλή λειτουργία του εργαστηρίου.

Αγαθά όπως οι εκτυπωτές και τα φυσικά αρχεία των δεδομένων είναι σημαντικά αλλά σε μικρότερο βαθμό, οπότε πρέπει να εστιάσουμε αρχικά σε όλα τα υπόλοιπα και όταν βεβαιωθούμε ότι όλα είναι ασφαλή τότε θα έρθει και η σειρά αυτών. Αυτό γίνεται επειδή δεν έχουν τόσο μεγάλη επικινδυνότητα όσο τα υπόλοιπα, επειδή αν υποστούν κάποια ζημιά ούτε μεγάλη χρηματική αξία έχουν και το εργαστήριο μπορεί να λειτουργήσει και χωρίς αυτά μέχρι να τα αντικαταστήσει.

Στο τέλος αυτής της ανάλυσης το εργαστήριο είναι έτοιμο να αρχίσει να εφαρμόζει ένα-ένα τα μέτρα προστασίας που αναφέραμε, με το πιο σημαντικό από αυτά που είναι μέτρο σχεδόν για όλα τα αγαθά, είναι η εκπαίδευση των υπαλλήλων στην σωστή χρήση των αγαθών και τους τρόπους που μπορούν οι ίδιοι να τα

κρατήσουν ασφαλή. Όταν εφαρμοστούν όλα τα μέτρα για όλα τα αγαθά το εργαστήριό μας θα είναι ασφαλές από όλες τις απειλές που εντοπίστηκαν.

ΠΗΓΕΣ

- Κύρια πηγή αποτέλεσαν οι ανεβασμένες διαλέξεις του μαθήματος, των τριών πρώτων διαλέξεων
- Τέλος υποστήριξης των Windows Server 2008 και Windows Server 2008 R2 - Τεχνική Στήριξη Πληροφοριακών Συστημάτων Σχολικών Μονάδων (sch.gr)
- FortiGate 400D Data Sheet (avfirewalls.com)
- Who needs Windows 10 Pro: 5 reasons to upgrade | PCWorld
- Cisco C886VA VDSL2 Modem Router με 4 Θύρες Ethernet | Skroutz.gr
- Microsoft Windows 7 Pro Reviews, Specs, Pricing & Support | Spiceworks
- Compare Windows 10 Home vs Pro | Microsoft Windows
- HP Desktop Pro G2 Specifications | HP® Customer Support
- HP OfficeJet Pro Printers | Explore the range - HP Store UK
- https://support.microsoft.com/en-us/windows/windows-7-support-ended-on-january-14-2020-b75d4580-2cc7-895a-2c9c-1466d9a53962