ΟΙΚΟΝΟΜΙΚΟ ΠΑΝΕΠΙΣΤΗΜΙΟ ΑΘΗΝΩΝ

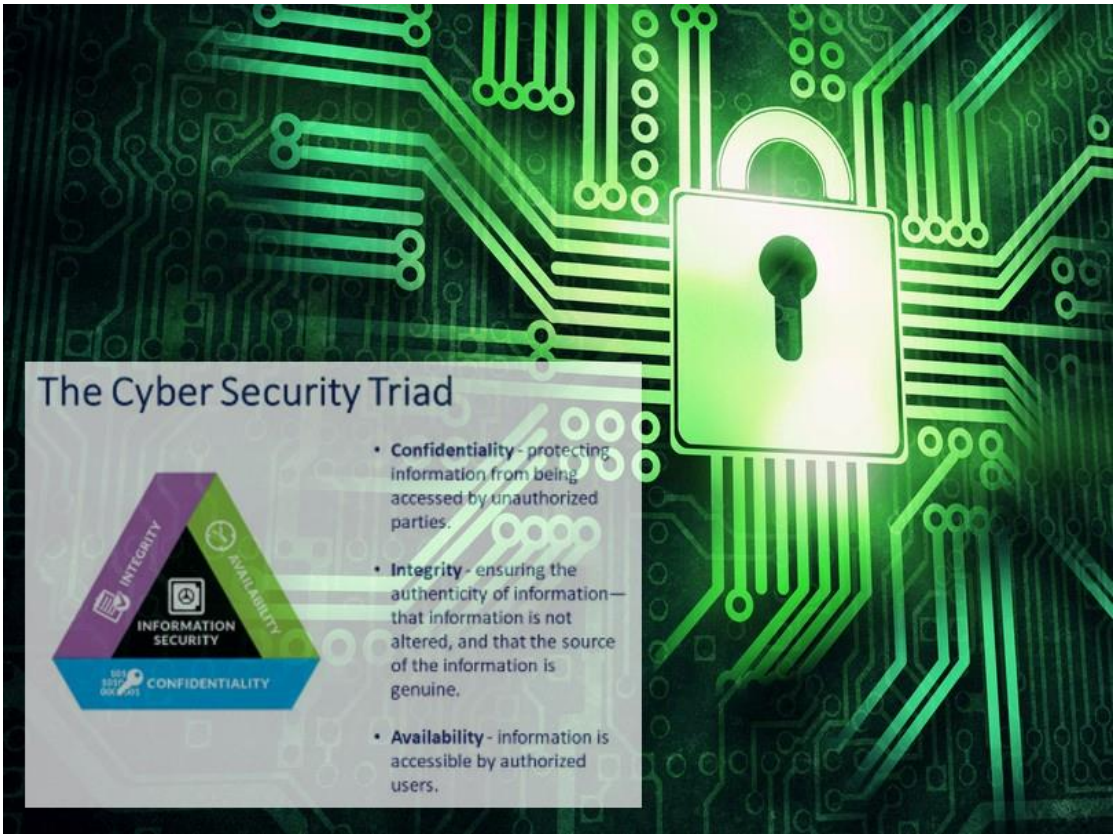
ATHENS UNIVERSITY OF ECONOMICS AND BUSINESS

ΤΜΗΜΑ ΠΛΗΡΟΦΟΡΙΚΗΣ

ΑΣΦΑΛΕΙΑ ΠΛΗΡΟΦΟΡΙΑΚΩΝ ΣΥΣΤΗΜΑΤΩΝ

ΕΡΓΑΣΙΑ ΕΑΡΙΝΟΥ ΕΞΑΜΗΝΟΥ 2023

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



Μικροβιολογικό Εργαστήριο Βιοϊατρικής Αθηνών

ΜΕΛΗ ΟΜΑΔΑ ΕΡΓΑΣΙΑΣ:

3180029 - ΓΕΩΡΓΟΠΟΥΛΟΥ ΚΩΝΣΤΑΝΤΙΝΑ - p3180029@aueb.gr

3190019 - ΒΑΚΙΡΤΖΟΓΛΟΥ ΕΛΕΝΗ ΑΝΝΑ - p3190019@aueb.gr

ΠΕΡΙΕΧΟΜΕΝΑ ΕΡΓΑΣΙΑΣ

1. ΕΙΣΑΓΩΓΗ

Στο πλαίσιο αυτής της εργασίας θα αναπτυχθεί μία ολοκληρωμένη πρόταση ενός σχεδίου ασφαλείας για ένα μικροβιολογικό εργαστήριο. Σε αυτό, θα παρουσιαστούν τα βήματα ανάλυσης επικινδυνότητας, όπου εντοπίζονται οι πιθανές απειλές και ευπάθειες του συστήματος, η αποτίμηση της επικινδυνότητας και θα προταθούν οργανωτικά και τεχνικά μέτρα που πρέπει να ληφθούν για τη διαχείριση της επικινδυνότητας και του εναπομένοντος κινδύνου.

1.1 Περιγραφή Εργασίας

Στο πλαίσιο της εργασίας θα γίνει ανάλυση της επικινδυνότητας του Βιοϊατρικού Εργαστηρίου Αθηνών. Συγκεκριμένα, θα εντοπιστούν τα αγαθά και τις απειλές που κινδυνεύουν, τις ευπάθειες που εμφανίζουν, τις επιπτώσεις του συστήματος από τη φθορά τους, τους τρόπους που οι απειλές θα αντιμετωπιστούν και θα αξιολογηθεί το impact κάθε αγαθού.

1.2 Δομή παραδοτέου

Στην ενότητα 1 παρουσιάζονται οι ενότητες της εργασίας επιγραμματικά και οι αναλύσεις που θα προκύψουν.

Στην ενότητα 2 παρουσιάζεται η μεθοδολογία που ακολουθήθηκε για τη μελέτη της ασφάλειας, σε ό,τι αφορά την περιγραφή υποδομών και του πληροφοριακού συστήματος, τον εξοπλισμό και υλισμικό (hardware), το Λογισμικό και τις εφαρμογές (software), το δίκτυο και τέλος τα δεδομένα.

Στην ενότητα 3 περιγράφονται τα κυριότερα στοιχεία από την μελέτη και την ανάλυση επικινδυνότητας που εκπονήθηκε. Δηλαδή γίνεται αποτίμηση του πληροφοριακού συστήματος και των εγκαταστάσεων για τα αγαθά, τις απειλές και τις ευπάθειες που εντοπίστηκαν, και παρουσιάζονται τα αποτελέσματα που προκύπτουν από την αποτίμηση αυτή.

Στην ενότητα 3 προτείνονται έντεκα (11) μέτρα ασφαλείας και αναλύονται σύμφωνα με τα assets του εργαστηρίου.

Τέλος, στην ενότητα 5 περιγράφονται αναλυτικότερα τα πιο κρίσιμα αποτελέσματα της παραπάνω ανάλυσης, και ακολουθεί η βιβλιογραφία.

2. ΜΕΘΟΔΟΛΟΓΙΑ ΜΕΛΕΤΗΣ ΑΣΦΑΛΕΙΑΣ

Για τη Διαχείριση Επικινδυνότητας του Βιοϊατρικού Εργαστηρίου Αθηνών χρησιμοποιήθηκε παραμετροποιημένη μέθοδος του ISO27001K[1]. Επιλέχθηκε για τη συγκεκριμένη εργασία για τους εξής λόγους:

- Αποτελεί πρότυπη μέθοδο και έχει αναπτυχθεί με σκοπό να εφαρμοστεί στην εκπαίδευση.
- Συνοδεύεται από αυτοματοποιημένο εργαλείο *(excel tool)* που υποστηρίζει όλα τα στάδια της εφαρμογής.
- Καλύπτει όλες τις συνιστώσες της ασφάλειας των πληροφοριακών συστημάτων, περιλαμβανομένων του τεχνικού παράγοντα, των θεμάτων διαδικασιών και προσωπικού, της φυσικής ασφάλειας, της ασφάλειας δικτύων κλπ.

Στάδιο	Βήματα
1. Προσδιορισμός και αποτίμηση αγαθών *(identification and valuation of assets)*	*Βήμα 1*: Περιγραφή πληροφοριακών συστημάτων και εγκαταστάσεων *Βήμα 2:* Αποτίμηση αγαθών πληροφοριακών συστημάτων και εγκαταστάσεων *Βήμα 3:* Επιβεβαίωση και επικύρωση αποτίμησης
2. Ανάλυση επικινδυνότητας *(risk analysis)*	*Βήμα 1:* Προσδιορισμός απειλών που αφορούν κάθε Αγαθό (asset) *Βήμα 2:* Εκτίμηση απειλών (threat assessment) και αδυναμιών (vulnerability assessment) *Βήμα 3:* Υπολογισμός επικινδυνότητας συνδυασμών Αγαθό-Απειλή-Αδυναμία *Βήμα 4:* Επιβεβαίωση και επικύρωση βαθμού επικινδυνότητας
3. Διαχείριση επικινδυνότητας *(risk management)*	*Βήμα 1:* Προσδιορισμός προτεινόμενων αντιμέτρων *Βήμα 2:* Σχέδιο ασφάλειας πληροφοριακών συστημάτων και εγκαταστάσεων

Πίνακας 1: *Στάδια και βήματα της Ανάλυσης και Διαχείρισης επικινδυνότητας*

2.1 Περιγραφή Υποδομών & Πληροφοριακού Συστήματος

Στην ενότητα αυτή, καταγράφονται οι υποδομές και τα πληροφοριακά συστήματα του εντοπίστηκαν κατά την μελέτη περίπτωσης και Ανάλυσης Επικινδυνότητας Πληροφοριακών Συστημάτων στο Μικροβιολογικό Εργαστήριο Βιοϊατρικής Αθηνών.

1) LabWS001: Haematology analyser, δηλαδή ένα μηχάνημα που χρησιμοποιείται για την αυτόματη ανάλυση του αίματος και την παραγωγή αναφορών για την καταμέτρηση των διαφόρων στοιχείων του αίματος, μοντέλου XS-1000i, με κατασκευαστή Sysmex's

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

XS-1000i και λειτουργικό σύστημα Proprietary Software, στο χώρο του εργαστηρίου-παρατηρητηρίου.

2) PCWS001: Υπολογιστής που σχεδιάστηκε για να χρησιμοποιηθεί από επαγγελματίες χρήστες, μοντέλου HP Pro G2 MT, με κατασκευαστή HP και λειτουργικό σύστημα Windows 10 Pro, στο χώρο του εργαστηρίου-παρατηρητηρίου.

3) PCWS002: Υπολογιστής που σχεδιάστηκε για να χρησιμοποιηθεί από επαγγελματίες χρήστες, μοντέλου HP Pro G2 MT, με κατασκευαστή HP και λειτουργικό σύστημα Windows 10 Pro, στο χώρο του εργαστηρίου-παρατηρητηρίου.

4) PCWS003: Υπολογιστής που σχεδιάστηκε για να χρησιμοποιηθεί από επαγγελματίες χρήστες, μοντέλου HP Pro G2 MT, με κατασκευαστή HP και λειτουργικό σύστημα Windows 10 Pro, στο χώρο λήψης δειγμάτων.

5) PCWS004: Υπολογιστής που σχεδιάστηκε για να χρησιμοποιηθεί από επαγγελματίες χρήστες, μοντέλου HP Pro G2 MT, με κατασκευαστή HP και λειτουργικό σύστημα Windows 10 Pro, στην αίθουσα αναμονής.

6) PCWS005: Υπολογιστής που σχεδιάστηκε για να χρησιμοποιηθεί από επαγγελματίες χρήστες, μοντέλου HP Pro G2 MT, με κατασκευαστή HP και λειτουργικό σύστημα Windows 10 Pro, στο γραφείο του ιατρού.

7) PR0001: PageWide Printers, δηλαδή εκτυπωτής με λιγότερο κόστος ανά σελίδα και γρηγορότερη εκτύπωση, ιδανικό για επιχειρήσεις, μοντέλου HP OfficeJet Pro Printer, με κατασκευαστή HP και με λειτουργικό Old firmware before 1708D, στην αίθουσα αναμονής.

8) PR0002: Εκτυπωτής, μοντέλου HP LaserJet Pro Printer, με κατασκευαστή HP και με λειτουργικό σύστημα HP printer Firmware (old) στο γραφείο του ιατρού.

9) SRV001: Server, συγκεκριμένα web server για την παροχή ιστοσελίδων στους χρήστες μέσω του πρωτοκόλλου HTTP, με λειτουργικό σύστημα Windows Server 2008 R2 στο βοηθητικό χώρο του εργαστηρίου.

10) SRV002: Server, συγκεκριμένα database server για τη διαχείριση της αποθήκευσης δεδομένων σε μια βάση δεδομένων, με λειτουργικό σύστημα Microsoft Windows 2016 Server SP1 + Oracle στο βοηθητικό χώρο του εργαστηρίου.

11) SW001: Switch, δηλαδή ένα δίκτυο σε συσκευή επιπέδου δικτύου, η οποία επιτρέπει στους υπολογιστές, τις συσκευές και άλλα δικτυακά στοιχεία να επικοινωνούν μεταξύ τους μέσω δικτύου, μοντέλου TP-LINK TL-SG1005D, με κατασκευαστή TP-LINK και με λειτουργικό σύστημα Windows 7 Pro στην αίθουσα αναμονής.

12) SW002: Switch, δηλαδή ένα δίκτυο σε συσκευή επιπέδου δικτύου, η οποία επιτρέπει στους υπολογιστές, τις συσκευές και άλλα δικτυακά στοιχεία να επικοινωνούν μεταξύ τους μέσω δικτύου, μοντέλου TP-LINK TL-SG1005D, με κατασκευαστή TP-LINK και με λειτουργικό σύστημα Windows 7 Pro στο βοηθητικό χώρο του εργαστηρίου.

13) RT001: Router, δηλαδή μια δικτυακή συσκευή που συνδέει δύο ή περισσότερα δίκτυα και επιτρέπει τη μεταφορά δεδομένων από το ένα στο άλλο, μοντέλου Cisco C886VA-K9, με κατασκευαστή Cisco και με λειτουργικό σύστημα Windows 7 Pro στην αίθουσα αναμονής.

14) FW001: Firewall, δηλαδή μια δικτυακή συσκευή ή λογισμικό που προστατεύει ένα δίκτυο από ανεπιθύμητη πρόσβαση ή εισβολή από το διαδίκτυο ή από άλλα δίκτυα, μοντέλου Fortinet-Fortigate-400D, με κατασκευαστή Fortinet και με λειτουργικό σύστημα Windows 10 Advanced IP Services στο βοηθητικό χώρο του εργαστηρίου.

15) LTP001: Laptop, μοντέλου Apple MacBook Air με καταστευαστή Apple και με λειτουργικό σύστημα MAC-OS στο γραφείο του ιατρού.

16) Customer Data: Πληροφορίες πελατών που αποθηκεύονται σε μια βάση δεδομένων στο διακομιστή δεδομένων (SRV002) και συνήθως περιλαμβάνουν προσωπικά στοιχεία.

17) Employee Data: Πληροφορίες εργαζομένων που αποθηκεύονται σε μια βάση δεδομένων στο διακομιστή δεδομένων (SRV002) και συνήθως περιλαμβάνουν προσωπικά στοιχεία.

18) Windows 7 Pro: Software, δηλαδή το σύνολο των προγραμμάτων και των ηλεκτρονικών δεδομένων που είναι απαραίτητα για τη λειτουργία ενός υπολογιστικού/ηλεκτρονικού συστήματος, με κατασκευαστή τη Microsoft, η οποία έχει σταδιακά σταματήσει την υποστήριξη του, καθώς ενημερώσεις ασφαλείας δεν εκδίδονται πλέον από την 14η Ιανουαρίου 2020. Το λογισμικό είναι εγκατεστημένο στα 2 Switch (SW001 και SW002).

19) Windows 10 Pro: Software, δηλαδή το σύνολο των προγραμμάτων και των ηλεκτρονικών δεδομένων που είναι απαραίτητα για τη λειτουργία ενός υπολογιστικού/ηλεκτρονικού συστήματος, με κατασκευαστή τη Microsoft, και είναι ένα πιο σύγχρονο, ασφαλές και ευέλικτο λειτουργικό σύστημα σε σχέση με το Windows 7. Το λογισμικό είναι εγκατεστημένο στα 5 workstations (PCWS001 - PCWS005).

20) Website: Software, μοντέλου JOOMLA και κατασκευαστή JOOMLA, δηλαδή ένα ανοιχτού κώδικα πλαίσιο διαχείρισης περιεχομένου που χρησιμοποιείται για τη δημιουργία ιστοσελίδων και εφαρμογών διαδικτύου, με λειτουργικό σύστημα LINUX REDHAT, το οποίο είναι εγκατεστημένο στον web server SRV001.

21) Φυσικό Αρχείο Ασθενών: Φάκελοι με έντυπο αρχείο που βρίσκονται σε ερμάριο – ανοιχτή βιβλιοθήκη στην αίθουσα αναμονής.

22) Αρχείο Υπαλλήλων & Προμηθευτών: Φάκελοι με έντυπο αρχείο που βρίσκονται σε ερμάριο – ανοιχτή βιβλιοθήκη στο γραφείο του ιατρού.

-EXTRAS

23) Σκανάρισμα Barcode ταυτοποίησης δειγμάτων: Διαδικασία κατά την οποία σκανάρονται barcodes για να γίνει η ταυτοποίηση των δειγμάτων με τους ασθενείς.

24) Εκτύπωση αποτελεσμάτων: Η διαδικασία κατά την οποία εκτυπώνονται τα αποτελέσματα των εξετάσεων.

25) Αποστολή αποτελεσμάτων: Η διαδικασία αποστολής των αποτελεσμάτων από το εργαστήριο στον ασθενή μέσω διαδικτύου.

26) Δημιουργία αντιγράφων ασφαλείας: Η εκτύπωση των απαραίτητων στοιχείων για τη δημιουργία αντιγράφου ασφαλείας.

27) Είσοδος στον ιστότοπο του εργαστηρίου: Το logIn στον ιστότοπο του εργαστηρίου από τον ενδιαφερόμενο/ασθενή.

28) Διαμοιρασμός προσωπικών δεδομένων πελατών: Η κοινοποίηση ιατρικών στοιχείων που αφορούν ασθενή σε εξώτερικούς ιατρούς.

29) LAN: Ακρωνύμιο του Local Area Network (Τοπικό Δίκτυο Περιοχής), δηλαδή ένα δίκτυο υπολογιστών που είναι φυσικά συνδεδεμένα στο ίδιο χώρο.

2.2 Εξοπλισμός & Υλισμικό (hardware)

Το υλικό (hardware) αποτελεί το σύνολο των φυσικών συσκευών και εξαρτημάτων που απαιτούνται για τη λειτουργία ενός υπολογιστικού συστήματος. Περιλαμβάνει τον επεξεργαστή, τη μνήμη RAM, τον σκληρό δίσκο, την κάρτα γραφικών, τη μητρική πλακέτα, το τροφοδοτικό, το περίβλημα και άλλα περιφερειακά εξαρτήματα όπως το πληκτρολόγιο, η συσκευή καταγραφής ήχου και η κάμερα. Το υλικό αποτελεί τη φυσική βάση του υπολογιστικού συστήματος και είναι υπεύθυνο για την εκτέλεση των λειτουργιών του.

Στο σύστημα του μικροβιολογικού εργαστηρίου τα αγαθά hardware είναι:

- Haematology analyser (LabWS001)
- Workstation (PCWS001 - PCWS005)
- PageWide Printers (PR0001)
- Printer (PR0002)
- Web Server (SRV001)
- Database Server (SRV002)
- Switch (SW001 & SW002)
- Router (RT001)
- Laptop (LTP001)

2.3 Λογισμικό και εφαρμογές

Το λογισμικό (software) είναι η συλλογή των προγραμμάτων, των δεδομένων και των εντολών που εκτελούνται σε μια υπολογιστική συσκευή και έτσι εκτελούνται εργασίες, αντιδρά σε εντολές και υπάρχει επικοινωνία με άλλες συσκευές. Χωρίζεται συνήθως σε δύο κατηγορίες, στο συστημικό λογισμικό (system software) και στο εφαρμοστικό λογισμικό (application software).

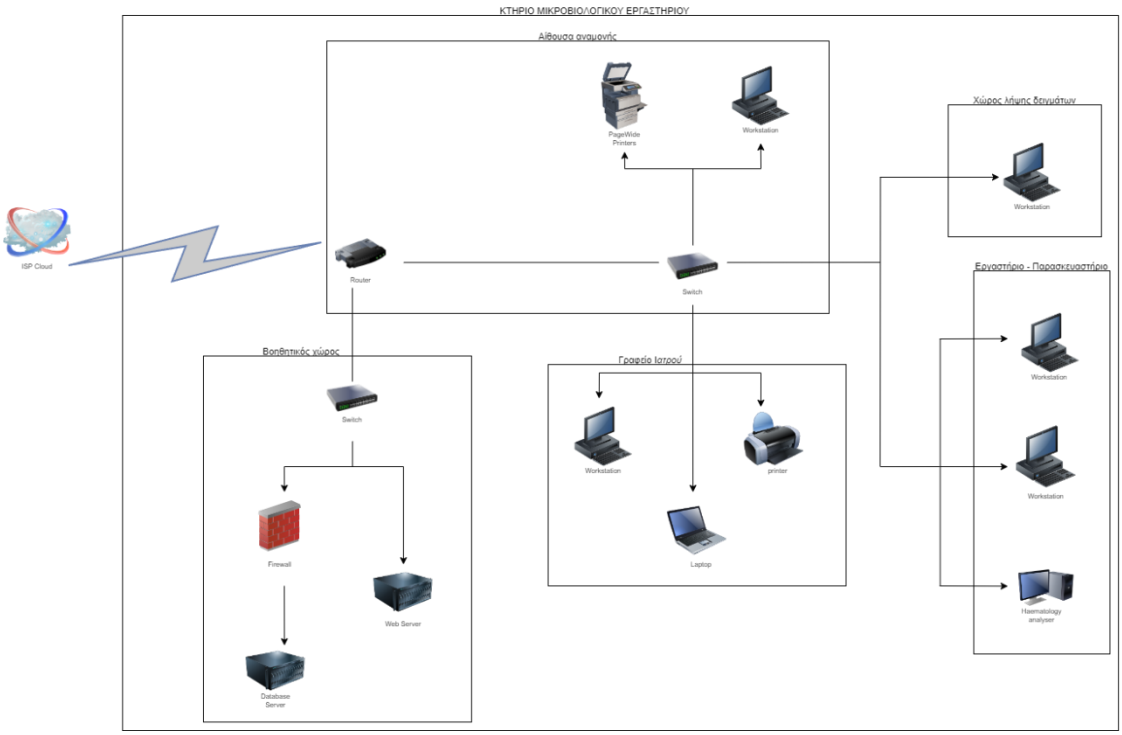
Στο σύστημα του μικροβιολογικού εργαστηρίου τα αγαθά software είναι:

- Windows 7 Pro
- Windows 10 Pro
- Website (JOOMLA)
- Firewall (FW001)

2.4 Δίκτυο

Δίκτυο είναι ένα σύνολο από δύο ή περισσότερους υπολογιστές που είναι συνδεδεμένοι μεταξύ τους, ώστε να μπορούν να ανταλλάσσουν δεδομένα και να μοιράζονται διαφορές συσκευές.

Στο μικροβιολογικό κέντρο, το δίκτυο είναι διαμορφωμένο όπως στην εικόνα παρακάτω:



Οι IP που αντιστοιχούν στο δίκτυο είναι 192.168.1.0/24 για αυτό και γίνεται αντιληπτό ότι χρησιμοποιείται ένα LAN συνδεδεμένο με ένα router.

2.5 Δεδομένα

Τα δεδομένα είναι πληροφορίες ή παράμετροι που μπορούν να αναγνωστούν ή να αποθηκευτούν από υπολογιστές ή άλλες ηλεκτρονικές συσκευές, που αποτελούν ένα σύνολο στοιχείων για πρόσωπα, καταστάσεις ή/και γεγονότα.

Στο σύστημα του μικροβιολογικού εργαστηρίου τα δεδομένα είναι:

- Customer Data
- Employee Data

2.6 Διαδικασίες

Διαδικασίες είναι μια σειρά από συγκεκριμένες εκτελούμενες πράξεις από τους ανθρώπους και τα συστήματα με τέτοιο τρόπο ώστε να επιτευχθεί ένα συγκεκριμένο αποτέλεσμα.

Στο σύστημά του μικροβιολογικού εργαστηρίου οι διαδικασίες είναι:

- Σκανάρισμα Barcode ταυτοποίησης δειγμάτων
- Εκτύπωση αποτελεσμάτων
- Αποστολή αποτελεσμάτων

- Δημιουργία αντιγράφων ασφαλείας
- Είσοδος στον ιστότοπο του εργαστηρίου
- Διαμοιρασμός προσωπικών δεδομένων πελατών

3. ΑΠΟΤΙΜΗΣΗ ΑΓΑΘΩΝ ΤΗΣ ΕΓΚΑΤΑΣΤΑΣΗΣ

Η CIA είναι ένα ακρωνύμιο που αναφέρεται στις τρεις βασικές αρχές της ασφάλειας πληροφοριών: την εμπιστευτικότητα, την ακεραιότητα και τη διαθεσιμότητα. Κάθε έλεγχος ασφαλείας και κάθε ευπάθεια ασφαλείας μπορεί να εξεταστεί σύμφωνα με αυτές τις βασικές έννοιες. Για να θεωρηθεί ένα πρόγραμμα ασφαλείας ολοκληρωμένο και πλήρες, πρέπει να καλύπτει επαρκώς την CIA.

Confidentiality (εμπιστευτικότητα) αναφέρεται στη διασφάλιση ότι οι πληροφορίες παραμένουν μυστικές και προστατεύονται από μη εξουσιοδοτημένους χρήστες. Αυτό σημαίνει ότι οι πληροφορίες πρέπει να προστατεύονται από ανθρώπους, διαδικτυακές απειλές, επιθέσεις με malware και άλλους κινδύνους. Οι τεχνολογίες που χρησιμοποιούνται για τη διασφάλιση της εμπιστευτικότητας περιλαμβάνουν την κρυπτογράφηση, τον έλεγχο πρόσβασης και τη διαχείριση ταυτοτήτων.

Integrity (ακεραιότητα) αφορά τη διατήρηση της ακεραιότητας των δεδομένων και των πληροφοριών. Αυτό σημαίνει ότι οι πληροφορίες πρέπει να παραμένουν ακέραιες και να μην έχουν τροποποιηθεί ή παραβιαστεί η ακεραιότητά τους. Για να διατηρηθεί η ακεραιότητα, απαιτείται η χρήση μέσων ασφάλειας, όπως η κρυπτογράφηση, η αντίγραφα ασφαλείας, οι περιορισμοί πρόσβασης και άλλα. Η διασφάλιση της ακεραιότητας είναι σημαντική για την εξασφάλιση της αξιοπιστίας και της εγκυρότητας των πληροφοριών και των δεδομένων.

Availability (διαθεσιμότητα) αφορά τη δυνατότητα πρόσβασης και χρήσης των πληροφοριών και των συστημάτων από τους εξουσιοδοτημένους χρήστες, όταν αυτοί το απαιτούν. Η εξασφάλιση της διαθεσιμότητας είναι σημαντική για να διατηρηθεί η συνέχεια των επιχειρησιακών διαδικασιών και να αποφευχθεί οποιαδήποτε διακοπή λειτουργίας των συστημάτων και των υπηρεσιών.

3.1 Αγαθά που εντοπίστηκαν

1. Haematology analyser
2. Workstation
3. PageWide Printers
4. Printer
5. Database Server
6. Web Server
7. Switch
8. Router
9. Firewall
10. Laptop
11. Customer Data
12. Employee Data
13. Windows 7 Pro Software
14. Windows 10 Pro Software
15. JOOMLA Software

16. Φυσικό Αρχείο Ασθενών
17. Αρχείο Υπαλλήλων & Προμηθευτών
18. Σκανάρισμα Barcode ταυτοποίησης δειγμάτων
19. Εκτύπωση αποτελεσμάτων
20. Αποστολή αποτελεσμάτων
21. Δημιουργία αντιγράφων ασφαλείας
22. Είσοδος στον ιστότοπο του εργαστηρίου
23. Διαμοιρασμός προσωπικών δεδομένων πελατών
24. LAN

3.2 Απειλές που εντοπίστηκαν

1) Εξοπλισμός & Υλισμικό (hardware)

- Haematology analyser (LabWS001):

  Μη εξουσιοδοτημένη εγκατάσταση λογισμικού: Επιτρέπει σε ανεπιθύμητα προγράμματα ή ιούς να επηρεάσουν την ασφάλεια του συστήματος προκαλώντας διαρροή δεδομένων ή και καταστροφή του εξοπλισμού.

- Workstation (PCWS001 - PCWS005):

  Αλλοίωση ταυτότητας: Κακόβουλος χρήστης που καταφέρνει να παρουσιαστεί ως εξουσιοδοτημένος χρήστης ή συσκευή στο σύστημα του εργαστηρίου, δίνοντας του πρόσβαση σε ευαίσθητα δεδομένα και επιτρέποντας του να τα υποκλέψει, να τα καταστρέψει ή/και να τα τροποποιήσει. Πιθανοί τρόποι επίτευξης αυτού του σκοπού είναι το phishing και social engineering.
  Μη εξουσιοδοτημένη εγκατάσταση λογισμικού: Επιτρέπει σε ανεπιθύμητα προγράμματα ή ιούς να επηρεάσουν την ασφάλεια του συστήματος προκαλώντας διαρροή δεδομένων ή και καταστροφή του εξοπλισμού. Οι πιο συνηθισμένες επιθέσεις για αυτό τον σκοπό είναι μέσω malware ή κακόβουλων email attachments.
  Hardware maintenance: Κακόβουλη τροποποίηση ή αντικατάσταση του hardware, ώστε να είναι ευκολότερη η πρόσβαση σε αυτό το workstation ή να κλαπούν άμεσα προσωπικά δεδομένα. Συνήθως γίνεται από κάποιον με φυσική πρόσβαση στη συσκευή.

- PageWide Printers (PR0001):

  Operations' error: Σφάλμα που σχετίζεται με την εκτέλεση μιας λειτουργίας ή εργασίας, το οποίο μπορεί να προκληθεί από μη εξουσιοδοτημένη πρόσβαση στον εκτυπωτή ή από μη εξουσιοδοτημένη εγκατάσταση λογισμικού.
  Κλοπή Δεδομένων: Αυτοί οι εκτυπωτές περιέχουν σκληρούς δίσκους ή άλλους αποθηκευτικούς χώρους, κάνοντας τους ευάλωτους σε πιθανή διαρροή δεδομένων αν αποκτηθεί κακόβουλη πρόσβαση σε αυτόν.

- Printer (PR0002):

Υπερφόρτωση με εντολές εκτέλεσης: Κακόβουλος χρήστης έχει τη δυνατότητα να στέλνει πολλές εντολές για να εκτελέσει ο εκτυπωτής έχοντας ως συνέπεια την προσωρινή αδυναμία εκτέλεσης καμίας εντολής λόγω υπερφότωσης. Συνηθίζονται οι επιθέσεις DDoS.
Μη εξουσιοδοτημένη χρήση: Είναι δυνατή η εκτέλεση εντολών που επιθυμεί ο επιτιθέμενος, ο οποίος έχει αποκτήσει παράνομη πρόσβαση στον εκτυπωτή, αποτρέποντας την εκτέλεση των εντολών που επιθυμεί ο ιδιοκτήτης του.
Κλοπή εγγράφων: Απόκτηση πρόσβασης σε εκτυπωτές και ώστε να κλαπούν ευαίσθητες πληροφορίες που εκτυπώνονται.

- Web Server (SRV001):

  Μη εξουσιοδοτημένη εγκατάσταση λογισμικού: Συνήθως οι χειρότερες επιπτώσεις προκύπτουν από κακόβουλο λογισμικό, malware, που μπορεί να εισαχθεί στον διακομιστή ιστού για να αναγκάσει τον server να λειτουργήσει ελαττωματικά ή για να προσπαθήσει να κλέψει δεδομένα από τον server.
  SQL Injection: Η επίθεση SQL Injection γίνεται στη βάση δεδομένων που αναζητά να εκμεταλλευτεί τα σημεία εισόδου που δεν επικυρώνονται σωστά.
  Εκτέλεση κακόβουλου κώδικα: Εφαρμόζεται μέσω επίθεσης Cross-Site Scripting (XSS), κατά την οποία αναζητάται ευπάθεια του Web Server ώστε να εισαγάγει και να εκτελέσει κακόβουλο κώδικα.
  Κατάργηση του διακοσμητή: Οι επιθέσεις DDoS είναι οι πιο κοινές για να καταργήσουν τον Web Server με την αποστολή μεγάλου όγκου κινήσεων προς αυτόν.
  Κλοπή δεδομένων: Πέρα από SQL Injection και XSS επιθέσεις, μπορεί να επιτευχθεί από τον επιτιθέμενο κλοπή δεδομένων μέσω δοκιμών σε κωδικούς πρόσβασης για τον web server (Brute Force Attacks).

- Database Server (SRV002):

  Κατάχρηση πόρων συστήματος: Οι επιθέσεις DDoS είναι οι πιο κοινές για να υπερφορτώσουν τον Database Server με την αποστολή μεγάλου όγκου κινήσεων προς αυτόν, οδηγώντας πολλές φορές σε κατάργηση του.
  Αλλοίωση δεδομένων: Ο Database Server μπορεί να αποτελέσει στόχο για επιθέσεις hacking ή προσβληθεί από κακόβουλο λογισμικό, με σκοπό την τροποποίηση, κλοπή ή/και διαγραφή δεδομένων.
  SQL Injection: Η επίθεση SQL Injection γίνεται στη βάση δεδομένων που αναζητά να εκμεταλλευτεί τα σημεία εισόδου που δεν επικυρώνονται σωστά.

- Switch (SW001 & SW002):

  Εσφαλμένη δρομολόγηση πακέτων: Παραπλάνηση του switch από τον επιτιθέμενο, ο οποίος δηλώνει ψευδείς διευθύνσεις στα πακέτα που στέλνει ώστε να λάβει ανεπιθύμητη πρόσβαση στο δίκτυο. Αυτή η επίθεση είναι γνωστή ως MAC spoofing.
  Κατάρρευση του switch: Αποστολή μεγάλου αριθμού πλαισίων με ψευδείς διευθύνσεις MAC (MAC flooding).
  Παρακολούθηση κίνησης δικτύου: Οι επιτιθέμενοι εκμεταλλεύονται ευπάθειες στο λογισμικό του switch ή στο firmware, αποκτώντας πρόσβαση ως διαχειριστής του δικτύου.

Φυσική πρόσβαση: Κάποιος με φυσική πρόσβαση στο switch έχει τη δυνατότητα με αλλαγές στις ρυθμίσεις του, να παρακολουθήσει την κίνηση του δικτύου, να αποκτήσει πρόσβαση σε ευαίσθητα δεδομένα και πληροφορίες και να προκαλέσει σημαντική ζημιά στο δίκτυο.

- Router (RT001):

  Παρεμβολή επικοινωνίας: Σε ένα router η παρεμβολή επικοινωνίας μεταξύ συσκευών (Man-in-the-middle), ώστε να αποκτηθεί πρόσβαση στα δεδομένα που μεταδίδονται.
  Τεχνικές αποτυχίες: Οι τεχνικές αποτυχίες σε ένα router μπορούν να οδηγήσουν σε απώλεια υπηρεσιών δικτύου, διακοπή σύνδεσης με άλλους κόμβους και άλλες προβλήματα στη λειτουργικότητα του δικτύου.
  Μη εξουσιοδοτημένη πρόσβαση στο δίκτυο: Ο επιτιθέμενος προσπαθεί να εισέλθει στο δίκτυο μέσω του router.
  Απώλεια ή τροποποίηση δεδομένων

- Laptop (LTP001):

  Ζημιές στο σύστημα: Προκαλούνται συνήθως από κακόβουλο λογισμικό, όπως malware, και αλλοιώνουν το σύστημα του laptop.
  Κλοπή ή αλλοίωση προσωπικών δεδομένων: Με οποιονδήποτε τρόπο αν κάποιος επιτιθέμενος αποκτήσει πρόσβαση στο laptop μπορεί να κλέψει στοιχεία που είναι αποθηκευμένα σε αυτό.
  Κλοπή της συσκευής laptop: Είναι ένας ακόμη τρόπος κλοπής δεδομένων αφού ο επιτιθέμενος θα έχει άμεση πρόσβαση στη συσκευή.
  Επιθέσεις φορητού σημείου πρόσβασης: Με αυτού του τύπου τις επιθέσεις όταν ο χρήστης συνδέεται σε ένα ανοιχτό ή ασφαλές δίκτυο Wi-Fi που ελέγχεται από έναν κακόβουλο χρήστη ή έναν επιτιθέμενο μπορεί να έρθει αντιμέτωπος με spoofing attacks ή/και malware.

2) Λογισμικό και εφαρμογές

- Windows 7 Pro:

  Εγκατάσταση κακόβουλου λογισμικού: Είναι εφικτή η εγκατάσταση λογισμικού που μπορεί να προκαλέσει ανεπιθύμητες ενέργειες. Ένα τέτοιο σύνηθες λογισμικό είναι το ransomware που κλειδώνει τον υπολογιστή ή τα δεδομένα και στη συνέχεια ζητάει πληρωμή από το θύμα για να αποκατασταθεί η πρόσβαση.
  Εκμετάλλευση ευπαθειών: Δεν γίνονται πλέον αναβαθμίσεις σε αυτό το λειτουργικό σύστημα, και η εκμετάλλευση πιθανών ευπαθειών του είναι ευκολότερη.
  Αδυναμία αναγνώρισης κακόβουλου λογισμικού: Η έλλειψη ενημερωμένου λογισμικού ασφαλείας καθιστά αδύνατη και την αναγνώριση κακόβουλων λειτουργιών.

Καταστροφή λειτουργικού συστήματος: Με κακόβουλες αλλαγές στον κώδικα του λογισμικού μπορούν να ενσωματωθούν ιοί στο σύστημα ή να δημιουργηθούν κενά για να εξασφαλισθεί πλήρης πρόσβαση στο σύστημα.

- Windows 10 Pro:

  Αποκρυπτογράφηση κρυπτογραφημένων δεδομένων: Αν αποκτηθεί πρόσβαση στο λογισμικό, μπορεί να επιτρέψει στον εισβολέα να αποκρυπτογραφήσει κρυπτογραφημένα δεδομένα και κωδικούς και να λάβει προνόμια υπερχρήστη.

  Παραπλάνηση χρηστών: Συνήθως εφαρμόζονται τεχνικές με ανεπιθύμητα emails, που αποστέλλονται σε μεγάλο αριθμό χρηστών και μπορεί να περιέχουν συνημμένα αρχεία ή συνδέσμους που, αν κάνει κλικ ο χρήστης, θα προκαλέσουν τη λήψη κακόβουλου λογισμικού, με διαφημίσεις συνήθως σε μέσα κοινωνικής δικτύωσης, και με phishing, όπου με μηνύματα που φαίνονται αξιόπιστα ο χρήστης καλείται να δώσεις προσωπικά στοιχεία.

  Απόκτηση προσωπικών πληροφοριών: Η πρόσβαση σε πληροφορίες επιδιώκεται με malware, phishing και Zero-day επιθέσεις, οι οποίες εφαρμόζονται όταν βρίσκεται κάποια ευκαιρία εκμετάλλευσης λογισμικού.

  Κατάρρευση λειτουργικού συστήματος: Με την πρόσβαση σε κώδικα του λειτουργικού, ο εισβολέας μπορεί να τον αλλοιώσει με αποτέλεσμα τη δυσλειτουργία του, ακόμη και την πλήρη κατάρρευσή του. Μια τεχνική που στοχεύει σε αυτό είναι οι επιθέσεις Zero-day.

- Website (JOOMLA):

  Έλεγχος λογαριασμού: Επιτιθέμενοι κλέβουν τα στοιχεία σύνδεσης ενός χρήστη και χρησιμοποιούν αυτά τα στοιχεία για να αναλάβουν τον έλεγχο του λογαριασμού τους, επίθεση γνωστή ως Session hijacking.
  Εισαγωγή κακόβουλου κώδικα: Εισάγεται κακόβουλος κώδικας στην ιστοσελίδα και εκτελείται με σκοπό το σύστημα να προβάλλει πληροφορίες που δεν θα έπρεπε να είναι προσβάσιμες (File Inclusion (FI)).
  Μη εξουσιοδοτημένη πρόσβαση στα δεδομένα της βάσης: Ο επιτιθέμενος με SQL Injection αποκτά πρόσβαση σε δεδομένα της βάσης της ιστοσελίδας, τα οποία μπορει να αλλοιώσει με κάθε τρόπο.

- Firewall (FW001):

  Αδυναμία σύνδεσης: Ο επιτιθέμενος μπορεί να εμποδίσει την εφαρμογή του firewall κάνοντας έτσι το δίκτυο που προστατεύει ευάλωτο.
  Απόκτηση πρόσβασης σε προστατευμένα δίκτυα: Με την απόκτηση πρόσβασης σε δίκτυα που δεν θα έπρεπε ο επιτιθέμενος μπορεί να προκαλέσει επιπλέον ζημιές σε κώδικα, λειτουργικό και σε δεδομένα καθώς είναι ευκολότερη η παραβίασή τους αφού βρίσκεται στο δίκτυό τους.
  Παραβίαση εμπιστευτικότητας και ακεραιότητας των δεδομένων: Επιδιώκεται καθώς κακόβουλα πακέτα μεταδοθούν στο δίκτυο και προκαλούν ζημιές στα δεδομένα.

3) Δίκτυο

- LAN:

  Αδύνατη μεταφορά δεδομένων: Διακόπτοντας τη σύνδεση ορισμένων components του δικτύου, δεν είναι δυνατή η μετάδοση σε δεδομένα που περνούν από αυτό το component.
  Παρακολούθηση κινήσεων δικτύου: Με την πρόσβαση στο LAN ένας κακόβουλος χρήστης μπορεί παρακολουθώντας το δίκτυο να ανακτήσει πληροφορίες.
  Αδυναμία σύνδεσης: Συνήθως με επιθέσεις DDoS, που υπερφορτώνουν το δίκτυο, αποτρέποντας τη χρήση του.
  Μείωση απόδοσης δικτύου: Συνήθως με ανεπιθύμητη αλληλογραφία η οποία στέλνεται σε μεγάλα μαζικά μηνύματα για να καταναλώσει μεγάλο μέρος της διαθέσιμης εύρυθμης ζώνης του δικτύου ώστε να προκαλέσει σημαντικές καθυστερήσεις στην ανταπόκριση του δικτύου.
  Παραπλάνηση χρήστη: Οι επιθέσεις, όπως MAC spoofing και ARP spoofing, στοχεύουν στην παραποίηση της διεύθυνσης MAC ενός υπολογιστή, προκειμένου να αποκτήσουν πρόσβαση στο δίκτυο ή να καταστρέψουν τη λειτουργία του.

4) Δεδομένα

- Customer Data:

  Παραποίηση πληροφοριών: Με επιθέσεις κατά τις οποίες ο κακόβουλος χρήστης αποκτά πρόσβαση σε πληροφορίες (με χρήση κακόβουλου λογισικου) που αφορούν τον πελάτη, έχει τη δυνατότητα να τις παραποιήσει δημιουργώντας σημαντικότατο πρόβλημα καθώς πρόκειται για ιατρικά δεδομένα.
  Διαρροή δεδομένων: Τα δεδομένα που αφορούν την υγεία αποτελούν προσωπικά στοιχεία και ο κάθε επιτιθέμενος που έχει πρόσβαση σε αυτά μπορεί να τα διαρρεύσει.
  Κλοπή: Η πρόσβαση σε χώρους που αποθηκεύονται τα δεδομένα των πελατών είναι εύκολη.

- Employee Data:

  Αλλοίωση πληροφοριών: Με κακόβουλο λογισμό μπορεί να αποκτηθεί πρόσβαση σε πληροφορίες που αφορούν τους εργαζόμενους του εργαστηρίου.
  Κλοπή: Η πρόσβαση σε χώρους που αποθηκεύονται τα δεδομένα των πελατών είναι εύκολη.

5) Διαδικασίες

- Σκανάρισμα Barcode ταυτοποίησης δειγμάτων:

Παρακολούθηση σκαναρίσματος: Αν ο κακόβουλος χρήστης έχει εισέλθει στο σύστημα του σαρωτή μπορεί να δέχεται τα δεδομένα που σκανάρει. Αυτό γίνεται εφικτό με την προσθήκη κακόβουλου λογισμικού στο σύστημα του σαρωτή.
Διαρροές δεδομένων: Η αντιγραφή ή η παραβίαση των αποτελεσμάτων μπορεί να οδηγήσει στη διαρροή ευαίσθητων δεδομένων.

- Εκτύπωση αποτελεσμάτων:

  Παρακολούθηση εκτυπώσεων: Με την κατάληψη ενός εκτυπωτή μπορεί να δοθεί εντολή για εκτύπωση ευαίσθητων πληροφοριών.
  Κλοπή: Με την εκτύπωση ευαίσθητων πληροφοριών κυρίως πελατών είναι εύκολη η κλοπή τους καθώς υπάρχουν επιπλέον αντίγραφα.

- Αποστολή αποτελεσμάτων:

  Παραβίαση προσωπικών δεδομένων: Αν έχει αποκτηθεί πρόσβαση σε υπολογιστές ή σε δίκτυα από που στέλνονται ή λαμβάνονται τα αποτελέσματα, γίνεται εύκολη η διαρροή τους. Ο επιτιθέμενος αυτό το επιδιώκει συνήθως με malware και phishing για πρόσβαση στον υπολογιστή, ενώ μέσω δικτυού είναι πιο σύνηθες να χρησιμοποιούνται τεχνικές όπως MAC και ARP spoofing.

- Δημιουργία αντιγράφων ασφαλείας:

  Κλοπή: Με την αντιγραφή ευαίσθητων πληροφοριών είναι εύκολη η κλοπή τους καθώς υπάρχουν επιπλέον αντίγραφα, εύκολα προσβάσημα καθώς φυλάσσονται σε μη κλειδωμένο χώρο.

- Είσοδος στον ιστότοπο του εργαστηρίου:

  Παραπλάνηση χρήστη: Ο κακόβουλος χρήστης δημιουργεί περιβάλλον όμοιο με αυτό του εργαστηρίου στο οποίο ο ανυποψίαστος χρήστης βάζει τα στοιχεία του για να συνδεθεί. Με αυτόν τον τρόπο αποκτά πρόσβαση στο λογαριασμό του καθώς πλέον γνωρίζει τα στοιχεία σύνδεσής του (phising).

- Διαμοιρασμός προσωπικών δεδομένων πελατών:

  Διαρροή προσωπικών δεδομένων πελατών: Αν ο τρόπος που διαμοιράζονται τα προσωπικά δεδομένα των πελατών δεν είναι ασφαλής μπορεί εύκολα να γίνει αντιληπτός από κακόβουλους χρήστες.

3.3 Ευπάθειες που εντοπίστηκαν

1) Εξοπλισμός & Υλισμικό (hardware)

- Haematology analyser (LabWS001):

Ανεξέλεγκτη χρήση πληροφοριακών συστημάτων: Για παράδειγμα η μη τήρηση κανόνων ασφαλείας, όπως η χρήση πολύπλοκων κωδικών πρόσβασης, η περιορισμένη πρόσβαση σε ευαίσθητα δεδομένα, οι χρήστες που επιτρέπουν σε άλλους να χρησιμοποιούν τους λογαριασμούς τους ή αν δεν κλείνουν τη συνεδρία τους όταν τελειώνουν τη χρήση του συστήματος, τότε κακόβουλα άτομα μπορούν να αποκτήσουν πρόσβαση στα ευαίσθητα δεδομένα.
Ανεπαρκής συντήρηση: Η συντήρηση των υλικών του αναλυτή χαρακτηρίζεται απαραίτητη διότι η οποιαδήποτε ευπάθεια σε αυτό μπορεί να προκαλέσει δυσλειτουργία στο σύστημα.
Αδυναμίες αυθεντικοποίησης και εξουσιοδότησης: Οι αναλυτές δεν διαθέτουν ισχυρά μέτρα αυθεντικοποίησης και εξουσιοδότησης για την προστασία των δεδομένων από μη εξουσιοδοτημένη πρόσβαση.
Ευπάθειες λογισμικού: Τα «κενά» σε ένα λειτουργικό σύστημα μπορούν να είναι ευκαιρίες για εκμετάλλευση από κακόβουλα άτομα που στοχεύουν στην λήψη πληροφοριών ή την καταστροφή του μηχανήματος. Τέτοια «κενά» συνήθως δημιουργούνται από σπάνιες ενημερώσεις του συστήματος.
Ευπάθειες φυσικής ασφάλειας: Ο τόπος που βρίσκεται το μηχάνημα δεν είναι ιδιαίτερα ασφαλής καθώς απουσιάζει κατάλληλη προστασία του ίδιου και των πληροφοριών που έχει καταγράψει.

- Workstation (PCWS001 - PCWS005):

  Μη ελεγχόμενη λήψη από το Διαδίκτυο: Οι χρήστες μπορεί να κατεβάσουν κακόβουλο λογισμικό, ιούς ή άλλες απειλές από ιστοσελίδες ή από άλλους πόρους στο Διαδίκτυο.
  Ανεπαρκής διαχείριση κωδικού πρόσβασης: Η χρήση αδύναμων κωδικών πρόσβασης μπορεί να κάνει εύκολη την πρόσβαση στον υπολογιστή από κακόβουλους χρήστες.
  Κακή διαχείριση των δικαιωμάτων πρόσβασης: Οι χρήστες με υψηλότερα δικαιώματα πρόσβασης μπορεί να έχουν πρόσβαση σε δεδομένα ή εφαρμογές που δεν θα έπρεπε να έχουν πρόσβαση.
  Μη ενημερωμένα λογισμικά: Ένα μη ενημερωμένο λειτουργικά σύστημα μπορεί να επιτρέψει σε κακόβουλο λογισμικό να εισχωρήσει στο workstation.

- PageWide Printers (PR0001):

  Ανεπαρκής εποπτεία: Ο εκτυπωτής πρέπει να βρίσκεται σε χώρο που δεν θα υπάρχει άμεση πρόσβαση από οποιονδήποτε καθώς μπορεί να υπάρξει διαρροή προσωπικών δεδομένων.
  Μη ορθή διαχείριση: Η λανθασμένη διαχείριση των εκτυπωτών μπορεί να επιτρέψει σε επιτιθέμενους να αποκτήσουν πρόσβαση στα δεδομένα τους ή να τα καταστρέψουν.
  Προστασία δεδομένων στη μνήμη: Καθώς αυτοί οι εκτυπωτές περιέχουν σκληρούς δίσκους ή άλλους αποθηκευτικούς χώρους, πρέπει να διαγράφονται όποια ευαίσθητα στοιχεία διατηρούνται εκεί.

- Printer (PR0002):

Ανεπαρκής εποπτεία: Ο εκτυπωτής πρέπει να βρίσκεται σε χώρο που δεν θα υπάρχει άμεση πρόσβαση από οποιονδήποτε καθώς μπορεί να υπάρξει διαρροή προσωπικών δεδομένων.
Μη ορθή διαχείριση: Η λανθασμένη διαχείριση των εκτυπωτών μπορεί να επιτρέψει σε επιτιθέμενους να αποκτήσουν πρόσβαση στα δεδομένα τους ή να τα καταστρέψουν.

- Web Server (SRV001):

  Ελαττωματικό υλικό: Η χρήση ελαττωματικού υλικό που μπορεί να προκαλέσει διακοπή της λειτουργίας του διακομιστή.
  Ευπάθειες λογισμικού: Η ευπάθεια του λογισμικού μπορεί να επιτρέψει την εισβολή στο διακομιστή, καταστροφή δεδομένων ή κλοπή ευαίσθητων πληροφοριών από έναν επιτιθέμενο.
  Έλλειψη πολιτικής ελέγχου πρόσβασης: Δεν υπάρχουν κανόνες που να περιορίζουν ποιοι χρήστες ή συσκευές έχουν πρόσβαση στον server και ποια δεδομένα μπορούν να ανακτήσουν.
  Ευπάθειες δικτύου: Ο web server γίνεται ευάλωτος σε επιθέσεις όπως Cross-site scripting (XSS) και DDoS.

- Database Server (SRV002):

  Έλλειψη πολιτικής ελέγχου πρόσβασης: Δεν υπάρχουν κανόνες που να περιορίζουν ποιοι χρήστες ή συσκευές έχουν πρόσβαση στον server και ποια δεδομένα μπορούν να ανακτήσουν.
  Ελαττωματικό υλικό: Η χρήση ελαττωματικού υλικό που μπορεί να προκαλέσει διακοπή της λειτουργίας του διακομιστή.
  Έλλειψη κρυπτογραφίας: Με μη κρυπτογραφημένα δεδομένα, αν ο επιτιθέμενος αποκτήσει πρόσβαση στη βάση, αποκτά πρόσβαση και στα δεδομένα της.

- Switch (SW001 & SW002):

  Παραβίαση του MAC filtering: Έχει ως συνέπεια να γίνει το δίκτυο ευάλωτο σε επιθέσεις που αφορούν τη MAC (MAC και ARP flooding και spoofing)
  Επικοινωνία μεταξύ διαφορετικών VLANs: Συνήθως με VLAN hopping, ο επιτιθέμενος προσπαθεί να αποκτήσει πρόσβαση σε δεδομένα και πληροφορίες που διαμοιράζονται ανάμεσα σε VLANs.
  Ανεπαρκής προστασία υλικού: Το υλικό οφείλει να προστατεύεται πέρα από τους άμεσους παράγοντες που μπορούν να προκαλέσουν φθορές στο υλικό, αλλά και από εξωγενείς παράγοντες όπως οι απότομες αλλαγές τάσης ρεύματος, διότι αν διακοπεί η λειτουργία του switch, η είσοδος στο δίκτυο του συστήματος γίνεται πιο εύκολη.

- Router (RT001):

  Ανεπαρκής προστασία υλικού: Η συσκευή του router αποτελεί κομβικό σημείο στο δίκτυο και πολλές φορές γίνεται στόχος.
  Ανεπάρκεια κωδικού πρόσβασης: Η χρήση αδύναμων κωδικών πρόσβασης μπορεί να κάνει εύκολη την πρόσβαση από κακόβουλους χρήστες.

Ελλιπής έλεγχος ταυτότητας αποστολέα πακέτου: Συνήθως με spoofing επιθέσεις ο επιτιθέμενος παραπλανεί τον χρήστη και μπορεί να του στείλει κακόβουλο λογισμικό.

- Laptop (LTP001):

  Μη ελεγχόμενη λήψη από το Διαδίκτυο: Οι χρήστες μπορεί να κατεβάσουν κακόβουλο λογισμικό, ιούς ή άλλες απειλές από ιστοσελίδες ή από άλλους πόρους στο Διαδίκτυο.
  Μη ενημερωμένα λογισμικά: Ένα μη ενημερωμένο λειτουργικά σύστημα μπορεί να επιτρέψει σε κακόβουλο λογισμικό να εισχωρήσει.
  Απώλεια κωδικού πρόσβασης: Αν δεν γίνεται χρήση κωδικού πρόσβασης κατά την έναρξη του laptop, δεν υπάρχει δυνατότητα αυθεντικοποίησης και έτσι οποιοδήποτε επιχειρήσει να ψάξει δεδομένα σε αυτή τη συσκευή μπορεί να το καταφέρει.

2) Λογισμικό και εφαρμογές

- Windows 7 Pro:

  Stop supporting: Αυτό το λογισμικό έχει ήδη σταματήσει να δέχεται ενημερώσεις ασφαλείας για αυτό και γίνεται ευκολότερο σε κάποιον κακόβουλο χρήστη να σπάσει το σύστημα ασφαλείας του. Τα επόμενα χρόνια θα σταματήσει να υποστηρίζεται γενικώς.
  Μη ασφαλής λήψη βιβλιοθηκών: Οποιαδήποτε βιβλιοθήκη έχει τροποποιηθεί με κακόβουλο λογισμικό, ο χρήστης δεν μπορεί να το αντιληφθεί έγκαιρα, λόγω μη ενημερωμένων συστημάτων ασφάλειας.
  Ευπάθεια πρωτοκόλλου SMB (Server Message Block): Ο επιτιθέμενος μπορεί να αποκτήσει πρόσβαση σε δεδομένα (είτε ανάγνωση είτε τροποποίηση δεδομένων).
  Ευπάθεια στο Internet Explorer: Επιχειρείται έλεγχος του συτήματος.

- Windows 10 Pro:

  Ευπάθεια πρωτοκόλλου SMB (Server Message Block): Ο επιτιθέμενος μπορεί να αποκτήσει πρόσβαση σε δεδομένα (είτε ανάγνωση είτε τροποποίηση δεδομένων), μέσω ανακατεύθυνσης του χρήστη.
  Ανεπαρκώς προστατευμένα δίκτυα: Στα Windows 10 Pro επιχειρείται η διείσδυση στο σύστημα μέσω μη προστατευμένων δικτύων που έχουν «προσβληθεί» από κακόβουλο λογισμικό.
  Διάβρωση κρυπτογραφημένων συνδέσεων: Αυτό μπορεί να συμβεί όταν ένα κακόβουλο λογισμικό ή κακόβουλος χρήστης καταφέρει να εγκαταστήσει ένα πιστοποιητικό στον υπολογιστή σας, το οποίο παρουσιάζεται ως αξιόπιστο από το λειτουργικό σύστημα.

- Website (JOOMLA):

Αδυναμίες στον έλεγχο πρόσβασης: Αυτή η αδυναμία επιτρέπει πρόσβαση σε άτομα που δεν έχουν τα απαραίτητα δικαιώματα, και συνήθως επηρεάζεται από μη επαρκείς κωδικούς πρόσβασης των χρηστών.
Ασφάλεια του κώδικα: Συνήθως αυτός ο τύπος website δέχεται επιθέσεις τύπου SQL injection και cross-site scripting (XSS).

- Firewall (FW001):

Ανεπαρκής ρύθμιση: Αν η ρύθμιση δεν είναι σωστή, μπορεί να επιτραπεί η πρόσβαση σε επιθέτους ή να αποκλειστεί η πρόσβαση σε έγκυρους χρήστες.
Αδυναμίες προστασίας από DDoS επιθέσεις: Ένα σύνηθες φαινόμενο στα firewalls είναι η αδυναμία αντιμετώπισης DDoS επιθέσεων, επηρεάζοντας τη διαθεσιμότητα του δικτύου.
Αδυναμία αναγνώρισης σωστής πολιτικής ασφαλείας: Οι μη ορθά καθορισμένες πολιτικές ασφαλείας μπορούν να οδηγήσουν σε ανοικτά σημεία που επιτρέπουν την είσοδο κακόβουλων εισβολέων στο δίκτυο.
Αδυναμία ανίχνευσης επιθέσεων: Ένα Firewall μπορεί να μην είναι εξοπλισμένο με τις κατάλληλες τεχνολογίες, είτε να μην έχει ενημερωθεί πρόσφατα, ώστε να ανιχνεύσει επιθέσεις.

3) Δίκτυο

- LAN:

Λειτουργία συστήματος: Το σύστημα επιτρέπει σε οποιονδήποτε σταθμό να συνδεθεί σε αυτό το δίκτυο χωρίς να απαιτείται καμία μορφή ελέγχου ταυτότητας.
Μετάδοση δεδομένων: Η μετάδοση δεδομένων μέσω του αέρα χρησιμοποιώντας ραδιοσυχνότητες ή υπέρυθρες, το κάνει ευάλωτο σε πιθανές παρεμβολές.
Μη ασφαλή πρωτόκολλα δικτύου: Μέσω του LAN επιτρέπεται η χρήση μη ασφαλών πρωτόκολλων δικτύου, όπως HTTP αντί για HTTPS το οποίο είναι ασφαλές.

4) Δεδομένα

- Customer Data:

Μη κρυπτογραφημένη βάση δεδομένων: Αν ο επιτιθέμενος αποκτήσει πρόσβαση στη βάση, αποκτά πρόσβαση και στα δεδομένα της.
Ανεπαρκής επίγνωση ασφαλείας: Δεν γίνεται εύκολα αντιληπτό αν τα δεδομένα έχουν τροποποιηθεί ή αν κάποιος έχει αποκτήσει πρόσβαση ανάγνωσης σε αυτά.

- Employee Data:

Μη κρυπτογραφημένη βάση δεδομένων: Αν ο επιτιθέμενος αποκτήσει πρόσβαση στη βάση, αποκτά πρόσβαση και στα δεδομένα της.

Ανεπαρκής επίγνωση ασφαλείας: Δεν γίνεται εύκολα αντιληπτό αν τα δεδομένα έχουν τροποποιηθεί ή αν κάποιος έχει αποκτήσει πρόσβαση ανάγνωσης σε αυτά.

5) Διαδικασίες

- Σκανάρισμα Barcode ταυτοποίησης δειγμάτων:

  Αδυναμία επαρκούς ελέγχου και αναγνώρισης του σωστού barcode: Δεν υπάρχει έλεγχος που να διασφαλίζει ότι έχει γίνει σωστή ανάγνωση του barcode και αν ο σαρωτής έχει προσβληθεί από κακόβουλο λογισμικό μπορεί να μετατρέψει το αποτέλεσμα της σάρωσης ώστε να οδηγήσει σε μη ασφαλείς ιστοσελίδες, λήψεις κ.α.
  Αδυναμία ανίχνευσης κακόβουλου λογισμικού: Δεν μπορεί να αναγνωριστει το κακόβουλο λογισμικό.
  Αδυναμία ελέγχου του προσώπου που σκανάρει το Barcode: Το Barcode μπορεί να σαρωθεί από οποιονδήποτε, χωρίς απαραίτητα να έχει εξουσιοδοτημένη πρόσβαση στις πληροφορίες που διαθέτει.
  Κλοπή: Αδυναμίες στην προστασία των barcode από κλοπή ή αντιγραφή, καθιστώντας δυνατή την παραποίηση των δεδομένων του δείγματος.

- Εκτύπωση αποτελεσμάτων:

  Χώρος εκτύπωσης: Ο χώρος που γίνεται αυτή η διαδικασία δεν θεωρείται κατάλληλος λόγω εύκολης πρόσβασης και κατά συνέπεια διαρροής αποτελεσμάτων.
  Μη εξουσιοδοτημένη εκτύπωση: Μπορεί να υπάρξει η δυνατότητα για μη εξουσιοδοτημένα άτομα να εκτυπώσουν αποτελέσματα, επιτρέποντάς τους να αποκτήσουν πρόσβαση σε ευαίσθητα προσωπικά δεδομένα.
  Απώλεια δεδομένων: Μπορεί να συμβεί η απώλεια των δεδομένων λόγω τεχνικών προβλημάτων με τον εκτυπωτή, όπως μη αναγνώριση της συσκευής από το δίκτυο ή της κάρτας μνήμης.
  Απώλεια εμπιστευτικότητας: Αν οι αποτυπώσεις ή αντίγραφα των εκτυπωμένων αποτελεσμάτων πέσουν σε λάθος χέρια ή διαρρεύσουν σε μη ασφαλείς αποθήκες, μπορεί να διακυβευθεί η εμπιστευτικότητα των αποτελεσμάτων.

- Αποστολή αποτελεσμάτων:

  Τρόπος αποστολής: Δεν διευκρινίζεται ο ασφαλής τρόπος αποστολής δεδομένων που αφορούν πελάτες. Η αποστολή αποτελεσμάτων μέσω μη ασφαλών διαδικασιών (όπως απλό email) μπορεί να εκθέσει τα αποτελέσματα σε κίνδυνο κλοπής ή διαρροής.
  Ανεπαρκής κρυπτογράφηση: Η αποστολή αποτελεσμάτων μέσω κρυπτογραφημένων συνδέσεων μπορεί να παρέχει ένα βαθμό ασφάλειας, αλλά αν η κρυπτογράφηση δεν είναι επαρκής, τα αποτελέσματα εξακολουθούν να είναι ευάλωτα σε επιθέσεις.
  Μη ασφαλείς συνδέσεις: Οι αποστολές αποτελεσμάτων μέσω μη ασφαλών συνδέσεων μπορούν να εκθέσουν τα αποτελέσματα σε κίνδυνο παρεμβολής από εξωτερικούς.

- Δημιουργία αντιγράφων ασφαλείας:

  Μη συχνή ενημέρωση των αντιγράφων ασφαλείας: Η μη τακτική ενημέρωση των αντιγράφων ασφαλείας μπορεί να οδηγήσει στην απώλεια δεδομένων σε περίπτωση ατυχήματος ή καταστροφής του χώρου φύλαξης.
  Χώρος φύλαξης των αντιγράφων: Δεν προστατεύεται ο χώρος που αποθηκεύονται τα αντίγραφα και έτσι είναι εύκολη η πρόσβαση στα δεδομένα τους.
  Μη επαρκή αποθήκευση και προστασία των αντιγράφων ασφαλείας: Αν οι αντίστοιχες αντίγραφες δεν αποθηκεύονται σε ασφαλή τοποθεσία ή δεν προστατεύονται επαρκώς, μπορεί να προκύψουν κινδύνοι όπως η απώλεια, η κλοπή ή η καταστροφή των δεδομένων.

- Είσοδος στον ιστότοπο του εργαστηρίου:

  Διαδικασία ελέγχου πρόσβασης: Με διαδικασίες spoofing από επιτιθέμενους μπορούν να αποκτήσουν πρόσβαση σε περιεχόμενο που δεν έχουν δικαίωμα να δουν.
  Κλοπή δεδομένων εισόδου: Αν κάποιος κλέψει τα δεδομένα εισόδου (email, password κλπ) μπορεί να αποκτήσει πρόσβαση στο λογαριασμό του πελάτη.

- Διαμοιρασμός προσωπικών δεδομένων πελατών:

  Αποστολή χωρίς άδεια: Η αποστολή αυτών των δεδομένων αρκετές φορ=ές γίνεται εν αγνοία των πελατών.
  Τρόπος αποστολής: Δεν διευκρινίζεται ο ασφαλής τρόπος αποστολής δεδομένων που αφορούν πελάτες. Η αποστολή αποτελεσμάτων μέσω μη ασφαλών διαδικασιών (όπως απλό email) μπορεί να εκθέσει τα αποτελέσματα σε κίνδυνο κλοπής ή διαρροής.
  Ανεπαρκής κρυπτογράφηση: Η αποστολή αποτελεσμάτων μέσω κρυπτογραφημένων συνδέσεων μπορεί να παρέχει ένα βαθμό ασφάλειας, αλλά αν η κρυπτογράφηση δεν είναι επαρκής, τα αποτελέσματα εξακολουθούν να είναι ευάλωτα σε επιθέσεις.
  Μη ασφαλείς συνδέσεις: Οι αποστολές αποτελεσμάτων μέσω μη ασφαλών συνδέσεων μπορούν να εκθέσουν τα αποτελέσματα σε κίνδυνο παρεμβολής από εξωτερικούς.

3.4 Αποτελέσματα αποτίμησης

1. Haematology analyser

   C: Διαρροή ή απώλεια ευαίσθητων πληροφοριών, διακοπή λειτουργίας του αναλυτή, μη εξουσιοδοτημένη πρόσβαση στο σύστημα
   I: Μείωση αποδοτικότητας του αναλυτή, απώλεια της εγκυρότητας των αποτελεσμάτων ανάλυσης, λάθη στη διάγνωση και στην αντιμετώπιση των ασθενών

A: Διακοπή εργασιών του αναλυτή, καθυστέρηση στην επεξεργασία δειγμάτων, απώλεια δεδομένων

2. Workstation

   C: Παραβίαση απόρρητων δεδομένων που αφορούν πελάτες-ασθενείς, προκαλώντας διαρροή ή/και απώλειά τους
   I: Παραποίηση πληροφοριών για πελάτες
   A: Απώλεια λειτουργικότητας, διακοπή της παροχής υπηρεσιών που εξυπηρετεί ο υπολογιστής, καθυστέρηση εκτέλεσης κρίσιμων εργασιών

3. PageWide Printers

   C: Διαρροή πληροφοριών μέσω ανάκτησης τους από τη μνήμη του εκτυπωτή
   I: Αλλοίωση των εκτυπωμένων εγγράφων, απώλεια δεδομένων αν δε διατηρείται η ακεραιότητά τους, εσφαλμένη αντιγραφή δεδομένων μπορεί να προκαλέσει σύγχυση στους πελάτες ή τον εργαζόμενο
   A: Απώλεια λειτουργικότητας του εκτυπωτή λόγω αποτυχίας υποσυστημάτων ή λογισμικού, δυσκολία στην επισκευή και συντήρηση, μεγάλη καθυστέρηση κατά την εκτέλεση της εκτύπωσης

4. Printer

   C: Δυνατότητα πρόσβασης σε εκτυπωμένα έγγραφα, διαρροή πληροφοριών σχετικά με τα δεδομένα της εργαστηρίου ή των ασθενών και οι κακόβουλοι χρήστες μπορούν να τα χρησιμοποιήσουν για τους σκοπούς τους
   I: Αλλοίωση των εκτυπωμένων εγγράφων, απώλεια δεδομένων αν δε διατηρείται η ακεραιότητά τους, εσφαλμένη αντιγραφή δεδομένων μπορεί να προκαλέσει σύγχυση στους πελάτες ή τον εργαζόμενο
   A: Απώλεια λειτουργικότητας του εκτυπωτή λόγω αποτυχίας υποσυστημάτων ή λογισμικού, δυσκολία στην επισκευή και συντήρηση, μεγάλη καθυστέρηση κατά την εκτέλεση της εκτύπωσης

5. Database Server

   C: Αποκάλυψη ευαίσθητων δεδομένων λόγω μη εξουσιοδοτημένης πρόσβασης, απάτη μέσω των προσωπικών δεδομένων που κλάπηκαν,
   I: Υπονόμευση ακεραιότητας δεδομένων, απώλεια εμπιστευτικότητας
   A: Αδυναμία ολοκλήρωσης ηλεκτρονικών συναλλαγών λόγω προβλημάτων στη βάση δεδομένων, διακοπή λειτουργίας του database server με τη χρήση διαφόρων επιθέσεων, μείωση απόδοσης για όσα services του συστήματος που χρησιμοποιούν τον database server

6. Web Server

   C: Κλοπή των στοιχείων εγγραφής των χρηστών και χρήση τους για αθέμητους σκοπούς, ανεπιθύμητες διαφημίσεις στο περιεχόμενο του webserver

I: Αλλαγή δεδομένων παραπλανώντας το χρήστη, παραποίηση λειτουργίας του λειτουργικού συστήματος, αλλαγές στη δομή του διακομιστή
A: Σημαντικές καθυστερήσεις στο σύστημα, παρεμπόδιση της λειτουργίας του server

7. Switch

C: Πρόσβαση σε πακέτα δικτύου δίνοντας πληροφορίες για το χρήστη χωρίς εξουσιοδότηση, επίθεση στους υπόλοιπους χρήστες του δικτύου
I: Εσφαλμένη δρομολόγηση πακέτων, αλλοίωση δεδομένων κατά τη μεταφορά τους
A: Σοβαρές καθυστερήσεις στις συνδέσεις δικτύου, ανεπαρκής χωρητικότητα του switch λόγω μεγάλου όγκου πακέτων, μείωση διαθεσιμότητας του δικτύου ώστε να μην είναι σε θέση να δρομολογήσει την κίνηση δεδομένων από τη μία πλευρά στην άλλη

8. Router

C: Κλοπή δεδομένων μετά από είσοδο στο LAN, παραβίαση ελέγχου πρόσβασης
I: Δημιουργία κακόβουλων διαδρομών δρομολόγησης, τροποποίηση δεδομένων που δρομολογούνται μέσω του router
A: Καθυστερήσεις στη σύνδεση του διαδικτύου, περιορισμένη δυνατότητα μεταφοράς δεδομένων, αδυναμία επικοινωνίας μεταξύ συσκευών που συνδέονται στο ίδιο router

9. Firewall

C: Παραβίαση δικτύου, παραβίαση εισόδου σε δεδομένα της βάσης, παρακολούθηση κίνησης δεδομένων
I: Μη εξουσιοδοτημένες προσθήκες στους κανόνες του firewall, τροποποίηση προσβασιμότητας
A: Αδυναμία αντιμετώπισης επεισοδίων κυκλοφορίας δεδομένων, ανασφάλεια διαθεσιμότητας των δικτυακών συσκευών, αδυναμία σύνδεσης στο δίκτυο ή σε δεδομένα

10. Laptop

C: Παραβίαση απόρρητων δεδομένων που αφορούν πελάτες-ασθενείς, προκαλώντας διαρροή ή/και απώλειά τους, αποκάλυψη ευαίσθητων πληροφοριών σε περίπτωση κλοπής του laptop.
I: Παραποίηση πληροφοριών για πελάτες
A: Απώλεια λειτουργικότητας, διακοπή της παροχής υπηρεσιών που εξυπηρετεί ο υπολογιστής, καθυστέρηση εκτέλεσης κρίσιμων εργασιών

11. Customer Data

C: Αποκάλυψη σημαντικών πληροφοριών που αφορούν ασθενείς, θέτεται σε κίνδυνο την ιδιωτικότητα και την ασφάλεια των πελατών, κλονισμός εμπιστοσύνης πελατών ως προς το εργαστήριο
I: Παραποίηση σημαντικών πληροφοριών (ακόμη και διαγνωστικών αποτελεσμάτων)
A: Δύσκολη πρόσβαση εργαζομένων και ασθενών στις πληροφορίες που τους αφορούν, αποτυχία συστημάτων επεξεργασίας δεδομένων, καθυστέρηση στη διαθεσιμότητα των δεδομένων λόγω υψηλού φόρτου στο σύστημα ή λόγω περιορισμένων πόρων

12. Employee Data

C: Διαρροή προσωπικών στοιχείων υπαλλήλων με πολλές περιπτώσεις αμφισβήτησης της θέσης τους στον εργασιακό τους χώρο, αποκάλυψη των μισθολογικών πληροφοριών των εργαζομένων, απώλεια της εμπιστοσύνης των εργαζομένων αναφορικά με την ικανότητα της εταιρείας να προστατεύει τις προσωπικές τους πληροφορίες.
I: Σφάλματα διαχείρισης δεδομένων λόγω λανθασμένων πληροφοριών
A: Δυσκολία στη διαχείριση δεδομένων που αφορούν τους υπαλλήλους όπως αρχεία και ηλεκτρονικά μηνύματα

13. Windows 7 Pro Software

C: Παρακολούθηση κώδικα και δεδομένων που οδηγεί σε πιθανή κατάρρευση του συστήματος λόγω ευκολότερης εισβολής, κίνδυνος διαρροής των πληροφοριών, κίνδυνος απώλειας δεδομένων, κίνδυνος παραβίασης δικαιωμάτων πρόσβασης
I: Αλλαγές στον κώδικα του λογισμικού που προκαλούν ευκολότερη ενσωμάτωση κακόβουλων λογισμικών
A: Καθυστέρηση στο λειτουργικό σύστημα, αναποτελεσματικότητα λογισμικού, μη διαθεσιμότητα του συστήματος λόγω προβλημάτων συμβατότητας με νεότερα λογισμικά ή hardware

14. Windows 10 Pro Software

C: Κίνδυνος φιλοξενίας κακόβουλων ιστότοπων, ανεπιθύμητη πρόσβαση σε προσωπικά δεδομένα
I: Πιθανότητα αποκρυπτογράφησης κρυπτογραφημένων δεδομένων και κωδικών, κίνδυνος λήψης προνομίων υπερχρηστών, μη επιθυμητή αλλαγή στις ρυθμίσεις του λειτουργικού συστήματος
A: Κατάρρευση του συστήματος λόγω αναμονής πολλών εργασιών, καθυστέρηση buffer, αναστολή των υπηρεσιών του λειτουργικού συστήματος λόγω ανεπάρκειας πόρων, δυσκολίες στη συνεργασία μεταξύ συσκευών ή/και δικτύων

15. JOOMLA Software

C: Συνέπειες για την εικόνα και τη φήμη του JOOMLA, διαρροή των προσωπικών δεδομένων
I: Αλλαγή στην λειτουργία του λογισμικού, μεταβολές σε δεδομένα
A: Διακοπή της λειτουργίας του λογισμικού από σφάλματα προγράμματος ή κακόβουλες επιθέσεις, ανικανότητα των χρηστών να έχουν πρόσβαση σε περιεχόμενο και λειτουργίες, μειωμένη ποιότητα εμπειρίας κατά τη χρήση του

16. Φυσικό Αρχείο Ασθενών

C: Προβλήματα στην ιδιωτικότητα λόγω διαρροής προσωπικών δεδομένων κυρίως όταν αφορούν κάποια πάθηση, απώλεια της εμπιστοσύνης σχετικά με το χώρο φύλαξης των πληροφοριών του εργαστηρίου
I: Εύκολη παραποίηση δεδομένων λόγω εύκολης πρόσβασης στο χώρο αποθήκευσής τους, εσφαλμένα αποτελέσματα αν χαθεί το κεντρικό αρχείο από τους υπολογιστές
A: Καταστροφή του αρχείου από φυσικούς παράγοντες, όπως πλημμύρες ή πυρκαγιές

17. Αρχείο Υπαλλήλων & Προμηθευτών

C: Προβλήματα στην ιδιωτικότητα λόγω διαρροής προσωπικών δεδομένων, απώλεια της εμπιστοσύνης σχετικά με το χώρο φύλαξης των πληροφοριών του εργαστηρίου, πιθανή δυσκολία εργαζομένου στην εύρεση μελλοντική εργασίας
I: Εύκολη παραποίηση δεδομένων λόγω εύκολης πρόσβασης στο χώρο αποθήκευσής τους, εσφαλμένες πληροφορίες αν χαθεί το κεντρικό αρχείο από τους υπολογιστές
A: Καταστροφή του αρχείου από φυσικούς παράγοντες, όπως πλημμύρες ή πυρκαγιές

18. Σκανάρισμα Barcode ταυτοποίησης δειγμάτων

C: Έλλειψη εμπιστοσύνης για την αδυναμία σκαναρίσματος από τρίτους, διαρροή δεδομένων από το σημείο που γίνει το σκανάρισμα
I: Εσφαλμένα αποτελέσματα λόγω πιθανής αλλοίωσης του barcode, με επιτυχής ταυτοποίηση και σύνδεση δειγμάτων με ασθενή
A: Καθυστέρηση διαδικασίας, αναμονή για ταυτοποίηση πολλών δειγμάτων

19. Εκτύπωση αποτελεσμάτων

C: Κλοπή εκτυπωμένων χαρτιών, παρακολούθηση κατά την εκτύπωση, απομνημόνευση προσωπικών στοιχείων ασθενών από τρίτους και διαρροή τους
I: Αλλοίωση εκτυπώσεων με κατεστραμμένα χαρτιά ή μελάνια
A: Έλλειψη υλών απαραίτητων για εκτυπώσεις όπως μελάνι και χαρτί

20. Αποστολή αποτελεσμάτων

C: Ευκολότερη κλοπή αποτελεσμάτων καθώς αποστέλνονται μέσω διαδικτύου
I: Πιθανή τροποποίηση αποτελεσμάτων από κακόβουλους χρήστες που έχουν εισέλθει στο σύστημα
A: Καθυστέρηση στη διαδικασία αποστολής και λήψης των αποτελεσμάτων από τον ασθενή, πρόβλημα στη διαδικασία αποστολής

21. Δημιουργία αντιγράφων ασφαλείας

C: Κλοπή αντιγράφων καθώς η πρόσβαση σε αυτά είναι εύκολη (σε μη φυλασσόμενο χώρο), διαρροή δεδομένων κατά τη διαδικασία δημιουργίας των αντιγράφων
I: Αλλοίωση πληροφοριών κατά τη διαδικασία της δημιουργίας των αντιγράφων
A: Απώλεια των αντιγράφων είτε από κλοπή είτε λόγω καταστροφή τους

22. Είσοδος στον ιστότοπο του εργαστηρίου

C: Έλλειψη εμπιστοσύνης στο σύστημα που χρησιμοποιεί το εργαστήριο για την επικοινωνία του με τους πελάτες-ασθενείς, κλοπή στοιχείων σύνδεσης
I: Εμφάνιση εσφαλμένων αποτελεσμάτων, σύγχυση ασθενών
A: Αδυναμία σύνδεσης των πελατών στο σύστημα για να μάθουν τα αποτελέσματα των εξετάσεών τους, καθυστέρηση διαδικασίας με πιθανό κόστος καθώς αφορούν θέματα υγείας

23. Διαμοιρασμός προσωπικών δεδομένων πελατών

C: Κλονισμός εμπιστευτικότητας, δυσφήμιση εργαστηρίου, κλοπή δεδομένων κατά τη διαδικασία διαμοιρασμού
I: Εσφαλμένη δημοσίευση στοιχείων πελατών λόγω τροποποίησης από τρίτους
A: Αδυναμία ασφαλούς διαμοιρασμού δεδομένων, καθυστέρηση διαδικασίας η οποία δεν θα έπρεπε να υπάρχει καθώς τα δεδομένα διαμοιράζονται για τη λήψη επιπλέον πληροφοριών περί των αποτελεσμάτων

24. LAN

C: Παρακολούθηση κινήσεων δικτύου, ανίχνευση πληροφοριών μέσω των παλμών του δικτύου, ευκολότερες επιθέσεις σε μερικώς ασφαλές δίκτυο, Αποκάλυψη των εμπιστευτικών πληροφοριών της εταιρείας ή/και των ασθενών
I: Αδύνατη τη μεταφορά των δεδομένων λόγω τροποποίησης ή διακοπής σε components του δικτύου
A: Καθυστέρηση διάδοσης πληροφοριών, αποκοπή από την πρόσβαση σε κοινόχρηστα αρχεία και πόρους, δυσκολία στον εντοπισμό και διόρθωση σφαλμάτων, αδυναμία σύνδεσης νέων χρηστών στο δίκτυο.

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

PageWide Printers: Διαγραφή μνήμης της συσκευής μετά από εκτύπωση προσωπικών δεδομένων.

Windows 7 Pro Software: Αποφυγή ύποπτων link και λήψεων, αντικατάσταση λογισμικού με νεότερο, επανεγκατάσταση για να αποφευχθεί χρήση τροποποιημένου κώδικα.

Windows 10 Pro Software: Ανταπόκριση μόνο σε πιστοποιημένα και αυθεντικοποιημένα emails.

Εκτύπωση αποτελεσμάτων: Το προσωπικό να είναι βέβαιο ότι οι πληροφορίες που εκτυπώνουν δεν είναι ορατές από τρίτους και δεν αφήνουν τα έγγραφα που εκτύπωσαν σε κοινή θέα.

Haematology analyser: Εκπαίδευση προσωπικού για ορθή χρήση.

LAN: Επανεκκίνηση δικτύου.

4.2. Ταυτοποίηση και αυθεντικοποίηση

Είσοδος στον ιστότοπο του εργαστηρίου: Η είσοδος να απαιτεί επιπλέον ταυτοποίηση, πέρα από email και κωδικό πρόσβασης, για παράδειγμα OTP μηνύματα.

Διαμοιρασμός προσωπικών δεδομένων πελατών: Ταυτοποίηση αποστολέα και παραλήπτη πριν γίνει η μεταφορά των δεδομένων.

Αποστολή αποτελεσμάτων: Εμφάνιση αποτελεσμάτων στην ιστοσελίδα του εργαστηρίου ύστερα από συνεννόηση εργαζομένων και ασθενούς.

Σκανάρισμα Barcode ταυτοποίησης δειγμάτων: Επιπλέον δεδομένα για την ταυτοποίηση του δείγματος.

Router: Επαλήθευση του DNS

4.3. Έλεγχος προσπέλασης και χρήσης πόρων

Workstation: Χρήση κωδικού κατά την ενεργοποίηση της συσκευής.

Laptop: Χρήση κωδικού ασφαλείας σε αρχεία που αφορούν προσωπικά δεδομένα, χρήση antivirus.

Router: Συχνές αλλαγές στο password με μεγάλη δυναμική.

Customer Data: Αποθήκευση σε φακέλους που προστατεύονται με firewall ή κωδικό, κρυπτογράφηση δεδομένων.

Employee Data: Περιορισμός προσβασιμότητας ακόμα και από το ίδιο το προσωπικό.

4.4. Διαχείριση εμπιστευτικών δεδομένων

Customer Data: Δημιουργία αντιγράφων ασφαλείας που να αποθηκεύονται σε εξωτερικούς σκληρούς δίσκους.

Haematology analyser: Αποθήκευση των αναλύσεων σε προστατευόμενο cloud.

Database Server: Κρυπτογράφηση.

Δημιουργία αντιγράφων ασφαλείας: Δημιουργία αντιγράφων μια φορά την εβδομάδα τουλάχιστον για να υπάρχει ενημερωμένο αρχείο.

4.5. Προστασία από τη χρήση υπηρεσιών από τρίτους

Customer Data: Κρυπτογράφηση όλων στοιχείων.

Employee Data: Κρυπτογράφηση των ευαίσθητων προσωπικών στοιχείων των εργαζομένων, χρήση κανόνων μεταξύ εργαζομένων, χρήση κωδικού.

Είσοδος στον ιστότοπο του εργαστηρίου: Αποθήκευση κρυπτογραφημένων στοιχείων εισόδου με χρήση salt.

PageWide Printers: Χρήση εκτυπωτών μόνο από το προσωπικό.

Printers: Χρήση εκτυπωτών μόνο από το προσωπικό.

4.6 Προστασία λογισμικού

Windows 10 Pro Software: Άμεση εγκατάσταση τελευταίων ενημερώσεων συστήματος.

JOOMLA Software: Άμεση εγκατάσταση τελευταίων ενημερώσεων συστήματος και διορθώσεων ασφαλείας.

Workstation: Χρήση αυθεντικοποιημένου λογισμικού.

Laptop: Χρήση αυθεντικοποιημένου λογισμικού.

Firewall: Εγκατάσταση ενημερώσεων.

4.7 Διαχείριση ασφάλειας δικτύου

Router: Ενεργοποίηση του WPA2 παρέχει ασφάλεια στην ασύρματη σύνδεση και απενεργοποίηση Remote Management.

Switch: Απομόνωση της κίνησης δικτύου από διαφορετικές ομάδες χρηστών, μέσω χρήσης VLANs**.**

LAN: Εφαρμογή μέτρων πρόληψης απόκρυψης διευθύνσεων.

4.8 Προστασία από ιομορφικό λογισμικό

Workstation: Χρήση VM για επικίνδυνες από επιθέσεις κινήσεις, χρήση web filters.

LAN: Χρήση firewall και WPA2.

Windows 10 Pro Software: Άμεση εγκατάσταση τελευταίων ενημερώσεων σε antivirus.

Database Server: Πλήρως ενημερωμένο firewall που τον προστατεύει.

Web Server: Χρήση αντιικού.

4.9 Ασφαλής χρήση διαδικτυακών υπηρεσιών

Switch: Απόκρυψη διευθύνσεων MAC και IP.

LAN: Απόκρυψη διευθύνσεων MAC και IP.

Web Server: Χρήση SSL ή TLS πιστοποιητικού και ενεργοποίηση HTTPS, εγκατάσταση συστήματος για την αποτροπή DDoS επιθέσεων.

4.10 Ασφάλεια εξοπλισμού

Haematology analyser: Χρήση UPS για την εξασφάλιση ομαλής λειτουργίας και απενεργοποίησης του.

Workstation: Φυσική προστασία του μηχανήματος.

Router: Χρήση UPS.

4.11 Φυσική ασφάλεια κτιριακής εγκατάστασης

PageWide Printers: Το μηχάνημα επειδή βρίσκεται σε χώρο με αρκετή πρόσβαση πρέπει να ελέγχεται από ποιόν χρησιμοποιείται.

Φυσικό Αρχείο Ασθενών: Ο χώρος φύλαξης των αρχείων πρέπει να κλειδώνεται.

Αρχείο Υπαλλήλων & Προμηθευτών: : Ο χώρος φύλαξης των αρχείων πρέπει να ασφαλιστεί.

Δημιουργία αντιγράφων ασφαλείας: Ο χώρος που γίνεται η διαδικασία δημιουργίας αντιγράφων των αρχείων των πελατών πρέπει να είναι περιορισμένης προσβασιμότητας.

5 ΣΥΝΟΨΗ ΚΡΙΣΙΜΩΝ ΑΠΟΤΕΛΕΣΜΑΤΩΝ

1. Windows 7 Pro: Η Microsoft διέκοψε την υποστήριξη και τις ενημερώσεις ασφαλείας για το λειτουργικό σύστημα Windows 7 από τον Ιανουάριο του 2020. Αυτό σημαίνει ότι δεν υπάρχουν πλέον νέες ενημερώσεις ασφαλείας που να διορθώνουν τυχόν ευπάθειες ασφαλείας του συστήματος, και επομένως, το σύστημα αυτό είναι πιθανόν να είναι ευάλωτο σε επιθέσεις και κακόβουλο λογισμικό. Για τον λόγο αυτό, είναι σημαντικό να ληφθούν μέτρα προστασίας, όπως η χρήση ενός ενημερωμένου και ενεργού antivirus, η απενεργοποίηση μη απαραίτητων υπηρεσιών και λειτουργιών του συστήματος, η ρύθμιση ενός ενισχυμένου firewall και η περιορισμένη χρήση του συστήματος σε επικίνδυνα περιβάλλοντα, όπως ανοιχτά δίκτυα Wi-Fi και ακατάσχετα emails ή ιστοσελίδες.

2. Switch: Η προστασία των switch είναι σημαντική γιατί μπορούν να υποστούν διάφορες επιθέσεις που θα οδηγήσουν σε σημαντική ζημιά στο δίκτυο και στην ασφάλεια των δεδομένων. Ακόμη και αν το προσωπικό που χρησιμοποιεί το switch είναι ενημερωμένο σχετικά με την ασφάλεια, μπορεί να συμβεί κάποιο λάθος ή να γίνει κάποιο λάθος από κάποιον χρήστη που δεν γνωρίζει τις βέλτιστες πρακτικές ασφαλείας. Επιπλέον, κάποιος επιτιθέμενος μπορεί να καταφέρει να πάρει πρόσβαση στο switch μέσω του δικτύου και να πραγματοποιήσει επιθέσεις. Για αυτό το λόγο, είναι σημαντικό να εφαρμόζονται επαρκείς μέτρα προστασίας, όπως η χρήση κατάλληλων κωδικών πρόσβασης, η περιορισμένη πρόσβαση σε εξουσιοδοτημένους χρήστες, η κρυπτογράφηση της κίνησης δικτύου και η συνεχής παρακολούθηση και ενημέρωση των συστημάτων ασφαλείας.

3. Firewall: Τα firewalls είναι απαραίτητα για την ασφάλεια των συστημάτων δικτύου, καθώς αποτελούν το πρώτο επίπεδο άμυνας κατά εισερχόμενων απειλών από το διαδίκτυο. Όταν οι υπολογιστές συνδέονται με το διαδίκτυο, είναι εκτεθειμένοι σε απειλές από κακόβουλους χρήστες και κακόβουλο λογισμικό. Τα firewalls ανιχνεύουν και φιλτράρουν αυτές τις απειλές, επιτρέποντας μόνο την είσοδο στο δίκτυο των εγκεκριμένων υπηρεσιών και των εγκεκριμένων πρωτοκόλλων. Επιπλέον, παρέχουν προστασία από τις εσωτερικές απειλές, όπως τους ιούς που διαδίδονται από υπολογιστές που βρίσκονται στο ίδιο δίκτυο. Αυτό είναι εξίσου σημαντικό με την προστασία από εξωτερικές απειλές, καθώς οι εσωτερικές απειλές μπορούν να προκαλέσουν σοβαρή ζημιά στο δίκτυο, συμπεριλαμβανομένης της απώλειας δεδομένων ή της κατάρρευσης του δικτύου.

ΒΙΒΛΙΟΓΡΑΦΙΑ

https://www.certmike.com/confidentiality-integrity-and-availability-the-cia-triad/

https://www.techtarget.com/searchnetworking/definition/local-area-network-LAN

https://www.upguard.com/blog/top-10-windows-7-vulnerabilities-and-remediation-tips

https://www.upguard.com/blog/top-10-windows-10-security-vulnerabilities-and-how-to-fix-them

https://www.europarl.europa.eu/news/en/headlines/society/20220120STO21428/cybersecurity-main-and-emerging-threats?&at_campaign=20234-Digital&at_medium=Google_Ads&at_platform=Search&at_creation=RSA&at_goal=TR_G&at_audience=cyber%20threats&at_topic=Cybersecurity&at_location=GR&gclid=Cj0KCQjw0tKiBhC6ARIsAAOXutlnexLy1OnsRGEk1CpKuA1WY2cCPmnlD79q6jtdQ3rVaC6VPkyF-K4aAgIrEALw_wcB

https://support.huawei.com/enterprise/en/doc/EDOC1100015134/a7811eb0/evaluation-on-security-risks-of-the-switch-module-on-the-network

https://www.ccexpert.us/scnd/threats-to-and-attacks-on-routers.html

https://www.datasunrise.com/potential-db-threats/top-db-threats/

https://www.checkpoint.com/cyber-hub/cyber-security/what-is-data-center/data-center-threats-and-vulnerabilities/

https://www.techfunnel.com/information-technology/web-server-vulnerabilities-attacks-how-to-protect-your-organization/

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

https://www.practicallynetworked.com/lan-security-threats/

https://www.ncbi.nlm.nih.gov/pmc/articles/PMC5784285/

https://www.coursehero.com/file/pomno5/The-top-risk-threats-and-vulnerabilities-in-a-workstation-domain-are-as-followed/

https://www.bridewell.com/insights/blogs/detail/why-laptops-are-one-of-your-business-s-biggest-security-risks

https://www.arcserve.com/blog/printer-security-risks-and-tips-it-service-providers

https://societyinsurance.com/blog/common-data-threats-and-vulnerabilities/