ΑΣΦΑΛΕΙΑ ΠΛΗΡΟΦΟΡΙΑΚΩΝ ΣΥΣΤΗΜΑΤΩΝ ΚΑΙ ΚΡΙΣΙΜΩΝ ΥΠΟΔΟΜΩΝ

ΣΧΕΔΙΟ ΑΣΦΑΛΕΙΑΣ

ΣΥΓΓΡΑΦΕΙΣ: Δουραχαλής Φίλιππος, 3170045
Νικολάου Ελένη, 3170121
Πανοπούλου Μαρία, 3170129

ΕΡΓΑΣΙΑ ΕΑΡΙΝΟΥ ΕΞΑΜΗΝΟΥ 2020-21

Contents

1. ΕΙΣΑΓΩΓΗ

Σκοπός του παρόντος εγγράφου αποτελεί η παρουσίαση μίας ολοκληρωμένης πρότασης σχεδίου ασφάλειας Πληροφοριακού Συστήματος. Βασικός στόχος της κλινικής είναι η αποτελεσματική λειτουργία της, η ορθή καταγραφή και η εξυπηρέτηση των ασθενών, με σύγχρονα, βασισμένα στις νέες διαδικτυακές τεχνολογίες και πλήρως ασφαλή μέσα.

1.1. Περιγραφή Εργασίας

Το παρόν έγγραφο αποτελεί ένα σχέδιο ασφαλείας στα πλαίσια της εργασίας «Ανάλυση και Διαχείριση Επικινδυνότητας σε περιβάλλον Κλινικής» του μαθήματος της Ασφάλειας Πληροφοριακών συστημάτων. Σκοπό έχει να εντοπιστούν πιθανές απειλές, υπάρχουσες ευπάθειες στην ασφάλειά του και να υπολογιστούν οι συνέπειες από την πραγματοποίηση μιας υπάρχουσας απειλής, μέσω ενός πρότυπου ελέγχου των υποδομών, διαδικασιών και λογισμικού του συστήματος της κλινικής.

1.2. Δομή παραδοτέου

Στην ενότητα 2 περιγράφεται η μεθοδολογία που θα ακολουθήσουμε για τη μελέτη ασφαλείας και γίνεται ο προσδιορισμός των αγαθών της κλινικής που θα ελέγξουμε. Στη συνέχεια, στην ενότητα 3 γίνεται αποτίμηση του Πληροφοριακού συστήματος και των εγκαταστάσεων της. Πιο συγκεκριμένα, εντοπίζονται τα κρισιμότερα αγαθά, οι απειλές και οι αδυναμίες, στα κεφάλαια 3.1, 3.2, 3.3, αντίστοιχα. Στην υπο-ενότητα 3.4 παρουσιάζεται πίνακας με το αντίκτυπο (Impact assesment) των απειλών (απώλεια διαθεσιμότητας, απώλεια ακεραιότητας, αποκάλυψη και αστοχία/λάθη στην τηλεπικοινωνιακή μετάδοση). Συνοδεύεται από αρχείο excel με υπολογισμό επικινδυνότητας συνδυασμών Αγαθό-Απειλή-Αδυναμία. Ακόμα, στην ενότητα 4 προτείνονται μέτρα ασφαλείας τα οποία εντάσσονται σε 11 γενικές κατηγορίες, τέλος, στην ενότητα 5 γίνεται η σύνοψη των κρισιμότερων αποτελεσμάτων.

2. ΜΕΘΟΔΟΛΟΓΙΑ ΜΕΛΕΤΗΣ ΑΣΦΑΛΕΙΑΣ

Για τη Διαχείριση Επικινδυνότητας της ΚΛΙΝΙΚΗ Α.Ε. 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 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 α-σφάλειας δικτύων κλπ.

[1] http://www.iso27001security.com/html/toolkit.html

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 Πληροφοριακού Συστήματος (ΠΣ) υπό έλεγχο

Στην ενότητα αυτή, καταγράφονται τα υφιστάμενα πληροφοριακά συστήματα της ΚΛΙΝΙΚΗ Α.Ε., τα οποία με το πέρας της μελέτης θα επικαιροποιηθούν, αναβαθμιστούν ή σε κάποιες περιπτώσεις αντικατασταθούν.

2.1.1. Υλικός εξοπλισμός (hardware)

Η κλινική περιλαμβάνει τους εξής χώρους με τον αντίστοιχο εξοπλισμό:

1. Secretariat/Reception Room

Inventory ID	Asset name	Type	Manufacturer	Operating System	Location
MED-CLIN-9033	Secretary Workstation A	Workstation	Lenovo	Windows Vista Service Pack 2 (SP2)	Secretariat/Reception Room
MED-CLIN-9034	Secretary Workstation B	Workstation	Lenovo	Windows Vista Service Pack 2 (SP2)	Secretariat/Reception Room
MED-CLIN-9031	Reception Workstation A	Workstation	Lenovo	Windows Vista Service Pack 2 (SP2)	Secretariat/Reception Room
MED-CLIN-9032	Reception Workstation B	Workstation	Lenovo	Windows Vista Service Pack 2 (SP2)	Secretariat/Reception Room

MED-CLIN-9021	Secretariat Server	Server	HP	Windows Server 2012 R2 Essentials	Secretariat/Reception Room
MED-CLIN-9027	Secretariat/Reception Room Switch	Switch	Cisco	Cisco proprietary software	Secretariat/Reception Room

Στο Secretariat/Reception Room υπάρχουν δύο Secretary Workstations, τα οποία χρησιμοποιούνται από το προσωπικό γραμματείας ως υπολογιστές για γραμματειακή υποστήριξη. Συγκεκριμένα, για την διαχείριση των ηλεκτρονικών φακέλων των ασθενών, των εξετάσεών τους , των οικονομικών οφειλών και εξοφλήσεων των ασθενών αλλά και για την καταχώρηση ραντεβού. Ακόμα, υπάρχουν δύο Reception Workstations ,τα οποία χρησιμοποιούνται από το προσωπικό υποδοχής για να εξυπηρετούν και να κατευθύνουν τους ασθενείς στα δωμάτιά τους, στο γραφείο του εκάστοτε γιατρού κλπ., μέσω των καταχωρημένων πληροφοριών στις οποίες έχουν πρόσβαση. Επίσης περιέχει και τον Secretariat Server ο οποίος προσφέρει ολοκληρωμένη παρακολούθηση όλου του εργασιακού κύκλου, περιέχει προσωπικά στοιχεία των ασθενών αλλά και πληροφορίες χρέωσης και τέλος πληροφορίες σχετικές με τη γενικότερη οικονομική δραστηριότητα της κλινικής. Στον χώρο αυτό υπάρχει και μία συσκευή switch Secretariat/Reception Room Switch στην οποία συνδέονται όλα τα προαναφερθέντα workstations και ο server ώστε να γίνεται διαχείριση των δεδομένων μέσω της επικοινωνίας workstation-server.

2. Computer/Server Room

Inventory ID	Asset name	Type	Manufacturer	Operating System	Location
MED-CLIN-9022	Server A	Server	HP	Ubuntu 16.04.7 LTS	Computer/Server Room
MED-CLIN-9023	Server B	Server	HP	Ubuntu 16.04.7 LTS	Computer/Server Room
MED-CLIN-9030	Admin Terminal	Workstation	Lenovo	Windows 10 Pro	Computer/Server Room
MED-CLIN-9024	Computer/Server Room Switch	Switch	Cisco	Cisco proprietary software	Computer/Server Room

Στο Computer/Server Room υπάρχουν δύο servers Server A , Server B οι οποίοι συλλέγουν συστηματικά πληροφορίες των ασθενών σε ψηφιακή μορφή. Ακόμα, υπάρχει και μία συσκευή - workstation Admin Terminal την οποία χρησιμοποιεί ο διαχειριστής του computer room για να

διαχειρίζεται τους δύο servers και να φροντίζει για την ομαλή λειτουργία τους και σύνδεσή τους με το υπόλοιπο δίκτυο της κλινικής. Τέλος, μέσω μίας συσκευής switch Computer /Server Room Switch που βρίσκεται στον συγκεκριμένο χώρο και οι τρεις αυτές συσκευές επικοινωνούν μεταξύ τους , αλλά και με το υπόλοιπο δίκτυο.

3. Patient Room 1

Inventory ID	Asset name	Type	Manufacturer	Operating System	Location
MED-CLIN-9016	Vital Signs Monitor Room 1 Patient A	Patient Monitor	Infinium	VxWorks 5.5.1	Patient Room 1
MED-CLIN-9017	Vital Signs Monitor Room 1 Patient B	Patient Monitor	Infinium	VxWorks 5.5.1	Patient Room 1
MED-CLIN-9029	Medical Ventilator Room 1 Patient A	Ventilator	Hamilton Medical	BlackBerry QNX 6.4.1	Patient Room 1
MED-CLIN-9014	Insulin Pump Room 1 Patient B	Insulin Pump	Medtronic	Linux embedded	Patient Room 1
MED-CLIN-9025	Patient Room 1 Switch	Switch	Cisco	Cisco proprietary software	Patient Room 1

Στο Patient Room 1 υπάρχουν δύο συσκευές Vital Signs Monitor οι οποίες συνδέονται η καθεμία με έναν ασθενή που βρίσκεται σε ένα κλινικό κρεβάτι και καταγράφουν συνεχώς δεδομένα όπως θερμοκρασία σώματος , παλμοί , πίεση και οξυγόνο. Στη συνέχεια , στο χώρο βρίσκεται μια συσκευή Medical Ventilator η οποία συνδέεται με τον Patient A και προσφέρει μηχανικό εξαερισμό, για να παρέχει αναπνοές σε έναν ασθενή που σωματικά δεν μπορεί να αναπνεύσει ή να αναπνεύσει επαρκώς. Ακόμα, υπάρχει και μία συσκευή Insulin Pump η οποία συνδέεται με τον Patient B και παρέχει ινσουλίνη στον ασθενή. Τέλος, οι 4 προαναφερθείσες συσκευές συνδέονται σε μία συσκευή switch Patient Room 1 Switch για να επικοινωνούν με το υπόλοιπο δίκτυο.

4. Patient Room 2

Inventory ID	Asset name	Type	Manufacturer	Operating System	Location
MED-CLIN-9018	Vital Signs Monitor Room 2 Patient C	Patient Monitor	Infinium	VxWorks 5.5.1	Patient Room 2

MED-CLIN-9019	Vital Signs Monitor Room 2 Patient D	Patient Monitor	Infinium	VxWorks 5.5.1	Patient Room 2
MED-CLIN-9015	Artificial Pacemaker Room 2 Patient C	Pacemaker	Medtronic	Windows Embedded Compact 2013	Patient Room 2
MED-CLIN-9012	Electroencephalogram Monitor Room 2 Patient D	EEG In-hospital EMU System	Cadwell	Linux embedded	Patient Room 2
MED-CLIN-9026	Patient Room 2 Switch	Switch	Cisco	Cisco proprietary software	Patient Room 2

Στο Patient Room 2 υπάρχουν δύο συσκευές Vital Signs Monitor .Ακόμα, στο χώρο βρίσκεται μία συσκευή Artificial Pacemaker η οποία είναι καρδιακός βηματοδότης και συνδέεται με τον Patient C για να δημιουργεί ηλεκτρικά ερεθίσματα που μεταβαίνουν στην καρδιά. Στη συνέχεια, υπάρχει και η συσκευή Electroengephalogram Monitor η οποία συνδέεται με τον Patient D και καταγράφει την ηλεκτρική δραστηριότητα των μυών του εγκεφάλου . Τέλος, οι 4 προαναφερθείσες συσκευές συνδέονται σε μία συσκευή switch Patient Room 2 Switch για να επικοινωνούν με το υπόλοιπο δίκτυο.

5. Main Building

Inventory ID	Asset name	Type	Manufacturer	Operating System	Location
MED-CLIN-9028	Medical Stuff Tablet	Tablet	Samsung	Android 7 Nougat (API 24)	Main Building
MED-CLIN-9011	WIFI Access Point	Access Point	Cisco	Cisco proprietary software	Main Building
MED-CLIN-9013	Firewall & Router	Firewall	FortiGate	FortiGate proprietary software	Main Building
MED-CLIN-9020	Main Router	Router	Cisco	Cisco proprietary software	Main Building

Στο χώρο του κτηρίου υπάρχει συσκευή tablet Medical Stuff Tablet την οποία χρησιμοποιούν τα μέλη του προσωπικού και συνδέεται σε ένα Wifi Access Point . Αυτό μαζί με τα 4 switches των δωματίων συνδέονται στο Firewall & Router και δημιουργείται το δίκτυο της κλινικής. Τέλος, σε αυτό συνδέεται και μία συσκευή Router : Main Router ώστε να γίνεται η σύνδεση με το διαδίκτυο.

2.1.2. Λογισμικό και εφαρμογές

Η κλινική κατέχει άδειες για τα παρακάτω λειτουργικά συστήματα:

- Windows Server 2012 R2 Essentials (MED-CLIN-9009) που είναι εγκατεστημένο στον διακομιστή της γραμματείας (MED-CLIN-9021)
- Windows Vista Service Pack 2 που είναι εγκατεστημένο στους σταθμούς εργασίας Α και Β της υποδοχής (MED-CLIN-9031 και MED-CLIN-9032) καθώς και στους σταθμούς εργασίας Α και Β της γραμματείας (MED-CLIN-9033 και MED-CLIN-9034).
- Ubuntu 16.04.7 LTS (MED-CLIN-9035), που είναι εγκατεστημένο στους διακομιστές Α και Β (MED-CLIN-9022 και MED-CLIN-9023) που περιέχουν τα δεδομένα των ασθενών.
- Windows 10 Pro, που είναι εγκατεστημένο στον υπολογιστή του διαχειριστή συστήματος (MED-CLIN-9030). Όλα τα ανωτέρω λογισμικά φαίνονται στον ακόλουθο πίνακα:

2.1.3. Δίκτυο

Το δίκτυο της κλινικής χωρίζεται σε 4 διακριτά υποδίκτυα. Τα διαφορετικά υποδίκτυα διαμορφώνονται μέσω ενός δρομολογητή MED-CLIN-9013. Οι συσκευές σε κάθε υποδίκτυο συνδέονται σε ένα switch, το οποίο με τη σειρά του συνδέεται με τον κεντρικό δρομολογητή ώστε να είναι δυνατή η επικοινωνία μεταξύ των υποδικτύων. Αναλυτικότερα:

1. Το πρώτο υποδίκτυο VLAN50 ορίζεται στο εύρος 192.168.50.0/24 στην αίθουσα ασθενών 1 και περιλαμβάνει τέσσερις συσκευές συνδεδεμένες σε ένα switch (MED-CLIN-9025).
2. Το υποδίκτυο VLAN60 περιέχει τις συσκευές στην αίθουσα ασθενών 2, οι οποίες και εδώ συνδέονται με το switch (MED-CLIN-9026).
3. Το υποδίκτυο VLAN 70 ορίζεται εντός του χώρου της γραμματείας και της υποδοχής και περιλαμβάνει τους τέσσερις σταθμούς εργασίας που βρίσκονται εκεί καθώς και τον διακομιστή της γραμματείας, τα οποία συνδέονται με το switch που είναι τοποθετημένο εκεί (MED-CLIN-9027).
4. Τέλος, στην αίθουσα των υπολογιστών και των διακομιστών ορίζεται το υποδίκτυο VLAN 80 οποίο διασυνδέει τον υπολογιστή του διαχειριστή και τους διακομιστές μέσω του switch (MED-CLIN-9024).

Πέραν των switches, στον κεντρικό δρομολογητή συνδέεται επίσης ένα main router (MED-CLIN-9020) το οποίο επιτρέπει την πρόσβαση στο διαδίκτυο, καθώς και ένα σημείο πρόσβασης (MED-CLIN-9011) το οποίο διασυνδέει ασύρματα τα tablet του προσωπικού με τα υπόλοιπα υποδίκτυα και το διαδίκτυο.

2.1.4. Δεδομένα

Τα δεδομένα που διαχειρίζεται η κλινική αφορούν μεν στη δική της λειτουργία αυτή καθ' αυτή, αλλά και δεδομένα των ασθενών της. Στην πρώτη κατηγορία αποθηκεύονται δεδομένα των εργαζομένων (Medical Clinic Employee Data) ενδεικτικά, για σκοπούς παρακολούθησης του εργασιακού κύκλου και παρακολούθησης της εξέλιξης τους. Στη συνέχεια, υπάρχουν τα οικονομικά-λογιστικά δεδομένα (Medical Clinic Financial Data), το αρχείο των οικονομικών συναλλαγών της κλινικής με πελάτες, εργαζόμενους, προμηθευτές και οτιδήποτε άλλο διαχειρίζεται η γραμματεία. Όσον αφορά τα δεδομένα των ασθενών, γίνεται συλλογή αρχικά προσωπικών τους δεδομένων, ατομικών

χαρακτηριστικών αλλά και χρέωσης, για τη διατήρηση του αρχείου εισαγωγών και τη διεκπεραίωση αιτημάτων που σχετίζονται με την ασφαλιστική κάλυψή τους, στο σύνολο Patient Personal Data. Και τα τρία προηγούμενα set δεδομένων βρίσκονται αποθηκευμένα στον Secretariat Server, στον χώρο υποδοχής-γραμματείας. Διατηρούνται, τέλος, τα δεδομένα του κάθε ασθενή σχετικά με την ιατρική του παρακολούθηση, όπως ιατρικό ιστορικό, φάρμακα, αλλεργίες κ.α., τα οποία ενημερώνονται συστηματικά και αποθηκεύονται σε ξεχωριστούς servers και χώρο από τα προηγούμενα set δεδομένων που αναφέραμε.

Παρακάτω φαίνεται ο πίνακας των συνόλων δεδομένων με τους αντίστοιχους κωδικούς:

Inventory ID	Asset name	Type	Location
MED-CLIN-9000	Medical Clinic Employee Data	Data	Secretariat Server
MED-CLIN-9001	Medical Clinic Financial Data	Data	Secretariat Server
MED-CLIN-9002	Patient Medical Data Srv A	Data	Server A
MED-CLIN-9003	Patient Medical Data Srv B	Data	Server B
MED-CLIN-9004	Patient Personal Data	Data	Secretariat Server

2.1.5. Διαδικασίες

Στην κλινική μπορούμε να ξεχωρίσουμε τέσσερις βασικές διαδικασίες. Η πρώτη αφορά την εισαγωγή ασθενών στην κλινική (Patient Admission), την καταχώρηση των προσωπικών αλλά και ιατρικών δεδομένων ενός νέου ασθενή ή την διασταύρωση και επικύρωση των ήδη υπάρχοντων (Patient Personal Data) σε περίπτωση που έχει ξαναγίνει εισαγωγή παλαιότερα. Στη συνέχεια, έχουμε τη διαδικασία παρακολούθησης των ασθενών (Patient Monitoring) που περιλαμβάνει τη συστηματική συλλογή πληροφοριών και ενημέρωση των δεδομένων των ασθενών (Patient Medical Data) σχετικά με την ιατρική τους κατάσταση. Ακόμη μία διαδικασία είναι η μισθοδοσία των υπαλλήλων της κλινικής (Payroll Process) η οποία βασίζεται στα δεδομένα των υπαλλήλων (Medical Clinic Employee Data) για να παράγει αντίστοιχα οικονομικά-λογιστικά δεδομένα (Medical Clinic Financial Data). Τέλος, υπάρχει η διαδικασία παροχής φαρμακευτικών σκευασμάτων (Supply of Drugs) κατά την οποία ελέγχονται ελλείψεις στα αποθέματα φαρμάκων που διαθέτει η εταιρεία και δρομολογούνται αντίστοιχες παραγγελίες προς τους προμηθευτές. Οι περισσότερες απ' τις διαδικασίες που αναφέραμε λαμβάνουν χώρα στην αίθουσα της γραμματείας, εκτός από την παρακολούθηση των ασθενών η οποία γίνεται ξεχωριστά στο δωμάτιο των υπολογιστών (όπου και αποθηκεύονται τα αντίστοιχα δεδομένα).

Παρακάτω φαίνεται ο πίνακας των διαδικασιών με τους αντίστοιχους κωδικούς:

Inventory ID	Asset name	Type	Location
MED-CLIN-9005	Patient Admission	Process	Secretariat Server
MED-CLIN-9006	Patient Monitoring	Process	Computer/Server Room
MED-CLIN-9007	Payroll Process	Process	Secretariat Server
MED-CLIN-9008	Supply of Drugs	Process	Secretariat Server

3. ΑΠΟΤΙΜΗΣΗ ΠΣ ΚΑΙ ΕΓΚΑΤΑΣΤΑΣΕΩΝ ΚΛΙΝΙΚΗΣ

Στη συγκεκριμένη ενότητα πραγματοποιούμε την Ανάλυση Επικινδυνότητας (Risk Analysis) του Πληροφοριακού συστήματος της εταιρείας, η δομή του οποίου παρουσιάζεται στην ενότητα 2. Παρακάτω θα αναλύσουμε τα αγαθά με αυξημένη επικινδυνότητα, τις αντίστοιχες απειλές και ευπάθειες.

3.1. Αγαθά που εντοπίστηκαν

ΌΝΟΜΑ ΑΓΑΘΟΎ	ΠΕΡΙΓΡΑΦΗ
Medical Clinic Employee Data	Προσωπικά δεδομένα και πληροφορίες σχετικά με τους εργαζομένους της κλινικής
Medical Clinic Financial Data	Οικονομικά στοιχεία της επιχείρησης
Patient Medical Data	Ευαίσθητα προσωπικά δεδομένα που αφορούν το ιατρικό ιστορικό των ασθενών της κλινικής, όπως νοσήματα, θεραπείες, αγωγές κ.τ.λ.
Patient Personal Data	Τα προσωπικά δεδομένα των ασθενών της κλινικής, όπως ον/μο, κατοικία, τηλέφωνο κ.τ.λ.
Patient Admission	Διαδικασία που δείχνει τα απαραίτητα βήματα για να προστεθεί ένας νέος ασθενής στην κλινική.
Patient Monitoring	Διαδικασία που περιγράφει την θεραπεία που θα ακολουθήσει ένας ασθενής καθώς και πως πρέπει να ελέγχεται η υγεία του κατά τη διαμονή του στην κλινική.
Payroll Process	Διαδικασία μισθοδοσίας. Ορίζει κάθε πότε γίνεται η καταβολή των μισθών καθώς και ο τρόπος με τον οποίο γίνεται η καταβολή και η ενημέρωση των εργαζομένων
Supply of Drugs	Η διαδικασία που ορίζει τον τρόπο που η κλινική προμηθεύεται τα φάρμακα και όλες τις λεπτομέρειες που σχετίζονται με αυτά (είδος, ποσότητα, απόθεμα κ.τ.λ.)
Windows Server 2012 R2 Essentials	Λειτουργικό Σύστημα που χρησιμοποιείται στον διακομιστή της γραμματείας
Windows Vista Service Pack 2	Λειτουργικό Σύστημα που χρησιμοποιείται στους υπολογιστές της γραμματείας και της υποδοχής
WIFI Access Point	Παρέχει ασύρματη πρόσβαση στο δίκτυο σε όλες τις συνδεδεμένες συσκευές
Firewall & Router	Δρομολογεί την κίνηση μέσα στο δίκτυο της κλινικής και καθιστά δυνατή την επικοινωνία μεταξύ των διαφόρων υποδικτύων

Insulin Pump	Συσκευή που ελέγχει το σάκχαρο και εισχωρεί ινσουλίνη στον ασθενή όταν είναι απαραίτητο.
Vital Signs Monitor	Συσκευή παρακολούθησης των ζωτικών ενδείξεων του ασθενούς.
Main Router	Συνδέει το εσωτερικό δίκτυο της επιχείρησης με το διαδίκτυο
Secretariat Server	Ο διακομιστής της γραμματείας. Περιλαμβάνει τα προσωπικά δεδομένα των ασθενών και των υπαλλήλων καθώς και πληροφορίες σχετικά με την οικονομική διαχείριση της κλινικής
Servers A & B	Διακομιστές που περιέχουν τα προσωπικά δεδομένα των ασθενών καθώς και δεδομένα που σχετίζονται με το ιατρικό ιστορικό και τις θεραπείες τους
Switch	Συσκευή που διασυνδέει ενσύρματα τις συσκευές σε ένα υποδίκτυο
Medical Staff Tablet	Φορητή συσκευή που χρησιμοποιείται από το προσωπικό της κλινικής για τους σκοπούς εκπλήρωσης των καθηκόντων τους
Admin Terminal	Ο υπολογιστής που χρησιμοποιείται αποκλειστικά από τον διαχειριστή του συστήματος
Reception/Secretary Workstation	Υπολογιστής που χρησιμοποιείται από εξουσιοδοτημένο προσωπικό της κλινικής και περιέχει ειδικές εφαρμογές

3.2. Απειλές που εντοπίστηκαν

ΌΝΟΜΑ ΑΓΑΘΟΥ	ΑΠΕΙΛΕΣ
Medical Clinic Employee Data	1. Insider Employee gets employee personal data 2. Critical data loss 3. Rainbow table attack
Medical Clinic Financial Data	1. Critical data loss 2. Insider Employee/ Competitor gets clinic's financial data
Patient Personal Data	1. Attacker/Insider employee can view raw patient data 2. Critical data loss.
Patient Medical Data	1. Destruction (e.g. fire or flood) of original data or backup data may result in total loss of all data 2. Insider Employee gets/changes patients' medical data.

Patient Admission	1. Medical Identity Theft
Patient Monitoring	1. User mistakes inputs. 2. Network failure interrupts process, patients' medical data is not accessible and cannot be modified.
Payroll Process	1. Payroll Fraud e.g. Time Theft
Supply Of Drugs	1. Network failure interrupts process, order is not completed and data is lost
Windows Server 2012 R2	1. Remote code execution
Windows Vista Service Pack 2	1. Attacker installs malware
WIFI Access Point	1. Unauthorized access to the network 2. Evil Twin attack
Firewall & Router	1. DoS attack 2. Remote attacker executes arbitrary code.
Insulin Pump	1. Attacker can connect to device via bluetooth.
Vital Signs Monitor	1. Remote Code Execution
Main Router	1. Access to the network of unauthorized user 2. DDoS attack overwhelms router 3. Unauthorized access to router configurations.
Secretariat Server	1. Attacker connects remotely to server 2. Certain data is accessible by unauthorized employees
Server A & B	1. SQL Injection 2. Brute force attacks can crack the password 3. Service not working due to hardware or software failure.

Switch	1. MAC flooding 2. Switch is damaged due to power failure.
Medical Stuff Tablet	1. SIM swapping 2. Tablet is misplaced and lost. 3. Unintentionally install malware
Admin Terminal	1. Unauthorized access.
Reception/Secretary Workstation	1. Unauthorized access to workstation 2. Spear-Phising attacks

3.3. Ευπάθειες που εντοπίστηκαν

ΌΝΟΜΑ ΑΓΑΘΟΥ	ΕΥΠΑΘΕΙΕΣ
Medical Clinic Employee Data	1. Database not encrypted 2. Backup not configured Employees' passwords are not salted.
Medical Clinic Financial Data	1. Backup not configured. 2. Database not encrypted.
Patient Medical Data	1. Backup stored in the same location as original/Backup not configured. 2. Database not encrypted.
Patient Personal Data	1. Data is not encrypted 2. Backup not configured.
Patient Admission	1. Insufficient checks before admitting patient
Petient Monitoring	1. Data inputs are not sufficiently checked. 2. No network connection.
Payroll Process	1. Payroll software parameters have not been properly set
Supply Of Drugs	1. No network connection.

Windows Server 2012 R2	1. CVE-2021-34527 Windows Print Spooler Remote Code Execution Vulnerability 2. CVE-2020-0674 Scripting Engine Memory Corruption Vulnerability 3. EternalBlue
Windows Vista Service Pack 2	1. Product support has ended
WIFI Access Point	1. Default password still in use / Not using advanced wireless security (e.g. WPA2 - Enterprise) 2. Duplicate SSIDs are permitted
Firewall & Router	1. Inadequate firewall rules 2. Depreciated software (4.3.8 and prior).
Insulin Pump	1. Remote connection enabled.
Vital Signs Monitor	1. Software has not been updated (URGENT/11)
Main Router	1. Incomplete package sender authentication 2. Not properly configured packet filtering. 3. Default router credentials.
Secretariat Server	1. Active Directory not properly configured 2. Firewall rules not configured for Remote Desktop
Server A & B	1. SQL input is not sanitized 2. Weak password used for login 3. No backup server available.
Switch	1. Port security not configured 2. Unstable External Power Supply
Medical Stuff Tablet	1. Device uses a SIM card 2. Portability and absent or not strong authentication. 3. Access to the internet is not restricted
Admin Terminal	1. Weak password used for login.
Reception/Secretary Workstation	1. E-mails not filtered 2. Workstations are easily accessible by unauthorized personnel and clients

3.4. Αποτελέσματα αποτίμησης

	Απώλεια διαθεσιμότητας							Απώλεια ακεραιότητας					Αποκάλυψη			Αστοχίες και λάθη στην τηλεπικοινωνιακή μετάδοση								
Αγαθά των ΠΣ	3 ώρες	12 ώρες	1 μέρα	2 μέρες	1 εβδομάδα	2 εβδομάδες	1 μήνας	Ολική καταστροφή	Μερική Απώλεια	Σκόπιμη αλλοίωση	Λάθη μικρής κλίμακας	Λάθη μεγάλης Κλίμακας	Εσωτερικούς	Παρόχους Υπηρεσιών	Εξωτερικούς	Επανάληψη μηνυμάτων	Αποποίηση αποστολέα	Αποποίηση παραλήπτη	Άρνηση αποστολής ή παραλαβής	Παρεμβολή λανθασμένων μηνυμάτων	Λανθασμένη δρομολόγηση	Παρακολούθηση/ένωσης	Μη παράδοση	Απώλεια ακολουθίας μηνυμάτων
MEDICAL CLINIC EMPLOYEE DATA	1	2	3	3	6	8	8	8	8	8	6	8	4	7	8							8		
MEDICAL CLINIC FINANCIAL DATA	1	2	3	3	5	6	6	8	8	7	3	6	7	8	8							8		
PATIENT MEDICAL DATA	5	6	7	8	9	9	9	10	10	10	8	10	7	9	10							10		
PATIENT PERSONAL DATA	3	5	6	7	8	9	9	9	9	8	3	6	7	9	9							9		
PATIENT ADMISSION	3	5	6	6	6	7	7	7	6	7	4	7	1	4	7									
PATIENT MONITORING	5	6	7	8	9	10	10	10	6	10	5	9	7	9	9									
PAYROLL PROCESS	1	2	2	3	5	6	6	7	4	7	3	6	2	4	7									
SUPPLY OF DRUGS	2	2	2	3	5	6	6	7	4	7	3	6	2	4	7								6	
WINDOWS SERVER 2012 R2	3	3	5	6	7	9	9	9	6	9	6	9												
WINDOWS VISTA SERVICE PACK 2	3	3	5	6	7	8	8	8	6	8	6	8												
WIFI ACCESS POINT	2	3	3	5	5	6	7	7	5	7	3	7	3	4	6	3	5	5	5	5	6	7	5	4
FIREWALL & ROUTER	5	7	8	9	10	10	10	10	8	7	6	8	3	5	9	5	4	4	6	6	9	10	6	5
INSULIN PUMP	3	4	6	7	7	7	7	7	4	8	3	8	1	1	1	5			6	8	5	2	6	6
VITAL SIGNS MONITOR	6	7	8	9	10	10	10	10	7	10	3	5	1	1	1	2			8	10	5	2	8	7
MAIN ROUTER	3	6	7	8	10	10	10	10	8	7	6	9	3	5	8	5	5	5	6	6	10	10	6	5

SECRETARIAT SERVER	5	6	8	8	9	10	10	10	5	10	7	10	5	8	10	3			8	4	8	10	8	3
SERVER A & B	6	8	8	9	10	10	10	10	7	10	7	10	6	8	10	4			9	6	8	10	9	5
COMPUTER/ SERVER ROOM SWITCH	3	5	6	7	9	9	9	9	5	7	4	7	2	3	7	5			3	5	8	7	3	4
PATIENT ROOM 1 SWITCH	2	4	6	6	7	8	8	8	7	8	3	6	2	3	7	4			3	5	6	6	3	4
PATIENT ROOM 2 SWITCH	2	4	6	6	7	8	8	8	7	8	3	6	2	3	7	4			3	5	6	6	3	4
SECRETERIAT/ RECEPTION ROOM SWITCH	4	5	6	7	9	9	9	9	5	7	4	7	3	5	7	3			3	4	8	7	3	3
MEDICAL STUFF TABLET	2	3	4	5	6	6	6	6	4	8	3	7	2	5	8	3			5	3	5	7	5	2
ADMIN TERMINAL	2	3	5	7	7	8	9	9	5	9	7	10	3	5	7	4			7	4	6	7	7	3
RECEPTION WORKSTATION	3	3	5	6	6	7	8	8	4	8	6	8	2	4	7	3			6	3	4	7	6	2
SECRETARY WORKSTATION	3	4	6	6	7	8	8	8	6	8	6	8	2	4	7	3			6	3	4	7	6	2

4. ΠΡΟΤΕΙΝΟΜΕΝΑ ΜΕΤΡΑ ΑΣΦΑΛΕΙΑΣ

Τα προτεινόμενα Μέτρα Προστασίας εντάσσονται σε έντεκα (11) γενικές κατηγορίες:

Α1. Προσωπικό – Προστασία Διαδικασιών Προσωπικού

Α2. Ταυτοποίηση και αυθεντικοποίηση

Α3. Έλεγχος προσπέλασης και χρήσης πόρων

Α4. Διαχείριση εμπιστευτικών δεδομένων

Α5. Προστασία από τη χρήση υπηρεσιών από τρίτους

Α6. Προστασία λογισμικού

Α7. Διαχείριση ασφάλειας δικτύου

Α8. Προστασία από ιομορφικό λογισμικό

Α9. Ασφαλής χρήση διαδικτυακών υπηρεσιών

Α10. Ασφάλεια εξοπλισμού

Α11. Φυσική ασφάλεια κτιριακής εγκατάστασης

Τα μέτρα έχουν εφαρμογή στο ΠΣ της ΚΛΙΝΙΚΗ Α.Ε.

4.1. Προσωπικό – Προστασία Διαδικασιών Προσωπικού

ID ΑΓΑΘΟΥ	ΑΓΑΘΟ	ΠΡΟΤΕΙΝΟΜΕΝΟ ΜΕΤΡΟ ΑΣΦΑΛΕΙΑΣ
MED-CLIN-9031 **MED-CLIN-9032** **MED-CLIN-9033** **MED-CLIN-9034**	**Reception/Secretary Workstation**	Strong user passwords
MED-CLIN-9031 **MED-CLIN-9032** **MED-CLIN-9033** **MED-CLIN-9034**	**Reception/Secretary Workstation**	Change passwords on regular basis
MED-CLIN-9030	**Admin Terminal**	Use strong passwords that are changed regularly
MED-CLIN-9028	**Medical Stuff Tablet**	Use strong passwords that are changed regularly
MED-CLIN-9028	**Medical Stuff Tablet**	Avoid visiting and downloading from untrusted websites
MED-CLIN-9005	**Patient Admission**	Stricter checks of client information before admitting patients
MED-CLIN-9007	**Payroll Process**	Payroll software parameters checked on regular basis.
MED-CLIN-9006	**Patient Monitoring**	Check input integrity
MED-CLIN-9008	**Supply Of Drugs**	Save data locally to be retrieved and finish process when network connection is restored
MED-CLIN-9000	**Medical Clinic Employee Data**	Internal Employee Rules and Procedures
MED-CLIN-9002 **MED-CLIN-9003**	**Patient Medical Data**	Internal Employee Rules and Procedures available

4.2. Ταυτοποίηση και αυθεντικοποίηση

ID ΑΓΑΘΟΥ	ΑΓΑΘΟ	ΠΡΟΤΕΙΝΟΜΕΝΟ ΜΕΤΡΟ ΑΣΦΑΛΕΙΑΣ
MED-CLIN-9022 MED-CLIN-9023	**Server A & B**	Use SSH keys instead of conventional password
MED-CLIN-9011	**WIFI Access Point**	Prevent unauthorized access to your network by changing default password and configuring WPA2-Enterprise security
MED-CLIN-9000	**Medical Clinic Employee Data**	Salt passwords along hashing

4.3. Έλεγχος προσπέλασης και χρήσης πόρων

ID ΑΓΑΘΟΥ	ΑΓΑΘΟ	ΠΡΟΤΕΙΝΟΜΕΝΟ ΜΕΤΡΟ ΑΣΦΑΛΕΙΑΣ
MED-CLIN-9001	**Medical Clinic Financial Data**	Grant access based on strict user requirements
MED-CLIN-9004	**Patient Personal Data**	Grant access based on strict user requirements
MED-CLIN-9021	**Secretariat Server**	Configure Active Directory
MED-CLIN-9021	**Secretariat Server**	Configure Firewall rules for Remote Desktop
MED-CLIN-9028	**Medical Stuff Tablet**	Minimize SIM swapping threat by agreeing on certain security steps during transactions between clinic's authorized personnel and provider.
MED-CLIN-9014	**Insulin Pump**	Disable remote control of device
MED-CLIN-9000	**Medical Clinic Employee Data**	Internal Employee Rules and Procedures available
MED-CLIN-9002 MED-CLIN-9003	**Patient Medical Data**	Internal Employee Rules and Procedures available

4.4. Διαχείριση εμπιστευτικών δεδομένων

ID ΑΓΑΘΟΥ	ΑΓΑΘΟ	ΠΡΟΤΕΙΝΟΜΕΝΟ ΜΕΤΡΟ ΑΣΦΑΛΕΙΑΣ
MED-CLIN-9000	**Medical Clinic Employee Data**	Keep backup compatible with 3-2-1 backup rule.
MED-CLIN-9001	**Medical Clinic Financial Data**	Keep backup compatible with 3-2-1 backup rule.
MED-CLIN-9004	**Patient Personal Data**	Keep backup compatible with 3-2-1 backup rule.
MED-CLIN-9002 MED-CLIN-9003	**Patient Medical Data**	Keep backup compatible with 3-2-1 backup rules and in different storage device.
MED-CLIN-9006	**Patient Monitoring**	Check input integrity
MED-CLIN-9022 MED-CLIN-9023	**Server A & B**	Deploy a remote backup server.
MED-CLIN-9001	**Medical Clinic Financial Data**	Use a database encryption tool.

MED-CLIN-9004	**Patient Personal Data**	Use a database encryption tool.

4.5. Προστασία από τη χρήση υπηρεσιών από τρίτους

ID ΑΓΑΘΟΥ	ΑΓΑΘΟ	ΠΡΟΤΕΙΝΟΜΕΝΟ ΜΕΤΡΟ ΑΣΦΑΛΕΙΑΣ
MED-CLIN-9031 **MED-CLIN-9032** **MED-CLIN-9033** **MED-CLIN-9034**	**Reception/ Secretary Workstation**	Change physical location of computer, so that it cannot be reached from the reception lobby.
MED-CLIN-9011	**WIFI Access Point**	Prevent unauthorized access to your network by changing default password and configuring WPA2-Enterprise security.
MED-CLIN-9031 **MED-CLIN-9032** **MED-CLIN-9033** **MED-CLIN-9034**	**Reception/Secretary Workstation**	Monitoring System for checking who accesses the reception/secretary room

4.6. Προστασία λογισμικού

ID ΑΓΑΘΟΥ	ΑΓΑΘΟ	ΠΡΟΤΕΙΝΟΜΕΝΟ ΜΕΤΡΟ ΑΣΦΑΛΕΙΑΣ
MED-CLIN-9009	**Windows Server 2012 R2**	Install latest software patches
MED-CLIN-9010	**Windows Vista Service Pack 2**	Grant access only to specific websites, avoid downloads and minimize internet use in general
MED-CLIN-9016 **MED-CLIN-9017** **MED-CLIN-9018** **MED-CLIN-9019**	**Vital Signs Monitor**	Immediately install latest software patches.

4.7. Διαχείριση ασφάλειας δικτύου

ID ΑΓΑΘΟΥ	ΑΓΑΘΟ	ΠΡΟΤΕΙΝΟΜΕΝΟ ΜΕΤΡΟ ΑΣΦΑΛΕΙΑΣ
MED-CLIN-9020	**Main Router**	Mandatory Access Control
MED-CLIN-9020	**Main Router**	Avoid DOS attacks by filtering incoming traffic
MED-CLIN-9020	**Main Router**	Prevent unauthorized access to router configurations by changing default credentials
MED-CLIN-9013	**Firewall & Router**	During firewall Setup: 1) Implement narrow permissions and widen later if required. 2) Disable firewall ports and adequately protect the ones that must stay open
MED-CLIN-9013	**Firewall & Router**	Upgrade to the latest version of FortiOS, recommended by FortiGuard and prevent system compromise by remote attackers.
MED-CLIN-9011	**WIFI Access Point**	Avoid Evil Twin Attack by deploying WIPS (Wireless Intrusion Prevention

		System)
MED-CLIN-9024 **MED-CLIN-9025** **MED-CLIN-9026** **MED-CLIN-9027**	**Switch(es)**	Configure Port Security to avoid MAC flooding attack

4.8. Προστασία από ιομορφικό λογισμικό

ID ΑΓΑΘΟΥ	ΑΓΑΘΟ	ΠΡΟΤΕΙΝΟΜΕΝΟ ΜΕΤΡΟ ΑΣΦΑΛΕΙΑΣ
MED-CLIN-9022 **MED-CLIN-9023**	**Server A & B**	Sanitizing Input fields to avoid SQL Injection attacks
MED-CLIN-9028 **MED-CLIN-9010** **MED-CLIN-9009**	**Medical Stuff Tablet & Windows Vista Service Pack 2 & Windows Server 2012 R2**	Install trusted antivirus software
MED-CLIN-9009	**Windows Server 2012 R2**	Install latest software patches
MED-CLIN-9010	**Windows Vista Service Pack 2**	Grant access only to specific websites, avoid downloads and minimize internet use in general

4.9. Ασφαλής χρήση διαδικτυακών υπηρεσιών

ID ΑΓΑΘΟΥ	ΑΓΑΘΟ	ΠΡΟΤΕΙΝΟΜΕΝΟ ΜΕΤΡΟ ΑΣΦΑΛΕΙΑΣ
MED-CLIN-9031 **MED-CLIN-9032** **MED-CLIN-9033** **MED-CLIN-9034**	**Reception / Secretary Workstation**	Enable filtering of e-mails. Add spam filters
MED-CLIN-9010	**Windows Vista Service Pack 2**	Grant access only to specific websites, avoid downloads and minimize internet use in general
MED-CLIN-9028	**Medical Stuff Tablet**	Avoid visiting and downloading from untrusted websites

4.10. Ασφάλεια εξοπλισμού

ID ΑΓΑΘΟΥ	ΑΓΑΘΟ	ΠΡΟΤΕΙΝΟΜΕΝΟ ΜΕΤΡΟ ΑΣΦΑΛΕΙΑΣ
MED-CLIN-9028	**Medical Stuff Tablet**	Gps and lost device location enabled.
MED-CLIN-9024 **MED-CLIN-9025** **MED-CLIN-9026** **MED-CLIN-9027**	**Switch(es)**	Add a voltage regulator device (controls power supply)
MED-CLIN-9022 **MED-CLIN-9023**	**Server A & B**	Ensure room temperature is ideal for hardware - install Air-condition system.
MED-CLIN-9014	**Insulin pump**	Disable remote control of device.

4.11. Φυσική ασφάλεια κτιριακής εγκατάστασης

ID ΑΓΑΘΟΥ	ΑΓΑΘΟ	ΠΡΟΤΕΙΝΟΜΕΝΟ ΜΕΤΡΟ ΑΣΦΑΛΕΙΑΣ
MED-CLIN-9031 **MED-CLIN-9032** **MED-CLIN-9033** **MED-CLIN-9034**	**Reception/Secretary Workstation**	Install Monitoring System for checking who accesses the reception/secretary room
MED-CLIN-9022 **MED-CLIN-9023**	**Server A & B**	Install Air-Condition System

5. ΣΥΝΟΨΗ ΠΙΟ ΚΡΙΣΙΜΩΝ ΑΠΟΤΕΛΕΣΜΑΤΩΝ

Από την μελέτη επικινδυνότητας που διενεργήθηκε και παρουσιάζεται στο Risk Assessment Spreadsheet, το 5% των ευρημάτων συνοψίζονται στα παρακάτω αποτελέσματα:

Asset Name	Function	Potential Vulnerability	Potential Threat	Potential Business Consequence (Impact)	Impact	Likelihood	Vulnerability	RPN
Patient Medical Data	Patients' medical information	Database is not encrypted	Insider Employee gets/changes patients' medical data	Violation of medical confidentiality. Impact on clinic's reputation. Patient treatmnets affected	10	8	8	640
Patient Personal Data	Patients' personal information	Database is not encrypted	Attacker/Insider employee (with unauthorised access), can view raw patient data	Violation of GDPR rules and financial impact via imposed fines	9	8	8	576
Secretariat Server	Server which contains employees', payroll and patients' personal information, as well as software to complete the clinic's various responsibilities	Firewall rules not configured for Remote Desktop	Attacker connects remotely to server	Unauthorized access to server	10	6	7	420
Server A & B	Database servers containing patients' medical information	Weak password used for login	Brute force attacks can crack the password	Attacker gains root access to server	10	7	6	420

Υπάρχει ισοβαθμία στον δείκτη RPN των τελευταίων αγαθών οπότε θεωρήσαμε σωστό να παρουσιάσουμε και τα δύο.

Patient Medical Data

Τα Patient Medical Data αποτελούν προσωπικά δεδομένα των ασθενών της κλινικής και αφορούν συνολικά την κατάσταση της υγείας τους και την ιατρική τους περίθαλψη. Είναι πληροφορίες που συλλέγονται συστηματικά κατά την διάρκεια της νοσηλείας τους στην κλινική αλλά δύναται να διατηρούνται και ως ιστορικό από προηγούμενες εισαγωγές. Συμπεραίνουμε άρα, ότι ανήκουν στα ειδικής κατηγορίας προσωπικά δεδομένα ή αλλιώς ευαίσθητα δεδομένα και εμπίπτουν στους κανόνες που ορίζουν οι οδηγίες της ευρωπαϊκής ένωσης (βλ. GDPR). Πρέπει, σύμφωνα με αυτούς, να υπάρχει εγγύηση απ' την πλευρά της κλινικής ότι έχουν ληφθεί ικανοποιητικά μέτρα για την προστασία τους από μη εξουσιοδοτημένη ή παράνομη πρόσβαση, επεξεργασία, καταστροφή ή φθορά. Επομένως, ως ευπάθεια (vulnerability) η έλλειψη μηχανισμού κρυπτογράφησης των δεδομένων αυτών θέτει σε υψηλό κίνδυνο την ακεραιότητα και την εμπιστευτικότητά τους. Παράλληλα, οι επιπτώσεις μίας τέτοιας παραβίασης και σε συνδυασμό με την έλλειψη επαρκών μέτρων ασφαλείας επιφέρει χρηματικά πρόστιμα μεγάλου μεγέθους, συν το κόστος στην εμπιστοσύνη των ασθενών. Λαμβάνοντας όλα αυτά υπόψιν, οι τιμές σε vulnerability και impact είναι αρκετά αυξημένες. Τέλος, το likelihood εμφανίζεται κι εκείνο αυξημένο καθώς κρίνουμε ότι λόγω της βαρύτητας του συγκεκριμένου αγαθού, η πιθανότητα να καταστεί πρωταρχικός στόχος μίας επικείμενης επίθεσης είναι ιδιαίτερα μεγάλη.

Patient Personal Data

Τα Patient Personal Data είναι τα προσωπικά δεδομένα των ασθενών της κλινικής και περιλαμβάνουν ενδεικτικά ονοματεπώνυμο, ημερομηνία γέννησης, διεύθυνση κατοικίας και άλλες πληροφορίες . Όπως , αντιλαμβανόμαστε αποτελούν κρίσιμο αγαθό γιατί αφορά στα προσωπικά δεδομένα του κάθε ανθρώπου και γι'αυτό χρήζει προσεκτικής διαχείρισης και διαφύλαξης. Η ευπάθεια να μην είναι κρυπτογραφημένη η βάση δεδομένων που τα περιέχει είναι βαθμολογικά ιδιαίτερα μεγάλη καθώς είναι πολύ υψηλή η σοβαρότητα των επιπτώσεων που μπορούν να προκύψουν από την εκμετάλλευσή της. Μη παρέχοντας κρυπτογράφηση στη βάση , μπορεί κάποιος χωρίς εξουσιοδοτημένη πρόσβαση να εισβάλλει και να δει τα δεδομένα. Αυτό, αδιαμφισβήτητα αποτελεί παράβαση των κανόνων GDPR και θα έχει οικονομικές επιπτώσεις στην κλινική εξαιτίας των προστίμων που θα καλεστεί να πληρώσει. Όπως είναι φυσικό λοιπόν, η επίπτωση του να πραγματοποιηθεί αυτή η απειλή είναι επίσης βαθμολογικά μεγάλη καθώς η πιθανότητα πραγματοποίησής της, και αυτό γιατί είναι αρκετά πιθανό κάποιος εξωτερικός-ανταγωνιστής να θέλει να βλάψει οικονομικά την κλινική. Συμπερασματικά , κρίνεται απαραίτητο να υπάρχουν μέτρα προστασίας που θα αποτρέψουν να πραγματοποιηθεί αυτή η απειλή εξαιτίας της συγκεκριμένης ευπάθειας. Πρώτον, χρειάζεται ένα εργαλείο που θα κρυπτογραφεί τη βάση και δεύτερον, να παρέχεται πρόσβαση σε εκείνη βάσει αυστηρών απαιτήσεων χρήστη.

Secretariat Server

Ο Secretariat Server είναι ο server της γραμματείας. Περιλαμβάνει τα προσωπικά δεδομένα των ασθενών και των υπαλλήλων καθώς και πληροφορίες σχετικά με την οικονομική διαχείριση της κλινικής. Ακόμα, προσφέρει ολοκληρωμένη παρακολούθηση όλου του εργασιακού κύκλου. Τα δεδομένα λοιπόν που περιέχει , το καθιστούν αρκετά κρίσιμο αγαθό το οποίο πρέπει να προστατεύεται από κακόβουλες κινήσεις. Η ευπάθεια να μην έχουν καθοριστεί κανόνες για το Firewall που αφορούν το Remote Desktop είναι σοβαρή και σε βαθμό μεγάλη επειδή καθιστά δυνατή την απομακρυσμένη σύνδεση από κάποιον στον server. Η επίπτωση από την πραγματοποίηση της συγκεκριμένης απειλής αγγίζει βαθμολογικά το 10 καθώς έχουμε μη εξουσιοδοτημένη πρόσβαση στο μηχάνημα. Η πιθανότητα να συμβεί αυτό είναι σχετικά μεγάλη αφού ο server είναι αρκετά εκτεθειμένος. Γι' αυτό , είναι σημαντικό να εφαρμοστεί ένα δραστικό μέτρο προστασίας που θα αποτρέψει κάθε πιθανή εισβολή στο μηχάνημα και αυτό θα είναι ο καθορισμός κανόνων για το Firewall σχετικά με το Remote Desktop.

Server A & B

Παραπάνω αναφερθήκαμε στη σημασία των ιατρικών δεδομένων των ασθενών και της διαφύλαξής τους από πιθανές παραβιάσεις. Οι Server A και B είναι αυτοί στους οποίους αποθηκεύονται τα Patient Medical Data και βρίσκονται σε ένα ειδικό δωμάτιο υπολογιστών. Η ευπάθεια της έλλειψης ισχυρού κωδικού για την είσοδο στον server μπορεί να οδηγήσει, κατά προέκταση, σε παράνομη πρόσβαση στα εργαλεία διαχείρισης των δεδομένων που βρίσκονται αποθηκευμένα σε αυτόν. Υπάρχει κάποια στοιχειώδης ασφάλεια με τη χρήση κωδικών πρόσβασης που να αποτρέπει σε κάποιο βαθμό μία επίθεση (vulnerability:6) αλλά όχι επαρκώς, ενώ το impact μίας τέτοιας παραβίασης παραμένει αυξημένο. Παράλληλα, η πρόσβαση σε έναν βασικό server της κλινικής όπως είναι οι A & B, δεν αφορά μόνο στα απροστάτευτα και μη κρυπτογραφημένα δεδομένα, αλλά ανεξάρτητα αυτού, δύναται να επιφέρει σοβαρές επιπτώσεις και σε διεργασίες της κλινικής. Η βασική λειτουργία των server είναι η συστηματική αποθήκευση δεδομένων των ασθενών και η δυνατότητα ανάκτησής τους ανά πάσα στιγμή από το ιατρικό προσωπικό. Ένας εισβολέας ή μη εξουσιοδοτημένος χρήστης που εισέρχεται, εν δυνάμει κακόβουλα, στον server, είναι πολύ πιθανόν να προκαλέσει μεταβολές στις βασικές ρυθμίσεις του, ακόμη και βλάβη. Όλα αυτά έχουν μεγάλες συνέπειες για την παρακολούθηση των ασθενών και επιφυλάσσουν σοβαρούς κινδύνους για την υγεία τους. Λαμβάνοντας υπόψιν όλα τα προηγούμενα, δικαίως το συγκεκριμένο αγαθό με την ευπάθεια αυτή, χρήζει ιδιαίτερης προσοχής και μέριμνας.