ΑΣΦΑΛΕΙΑ ΠΛΗΡΟΦΟΡΙΑΚΩΝ ΣΥΣΤΗΜΑΤΩΝ ΚΑΙ ΚΡΙΣΙΜΩΝ ΥΠΟΔΟΜΩΝ

ΣΧΕΔΙΟ ΑΣΦΑΛΕΙΑΣ

ΣΥΓΓΡΑΦΕΙΣ: Πλανάκη Κατερίνα icsd15169

ΣΥΓΓΡΑΦΕΙΣ: Χουβαρδάς Αντώνης icsd17217

ΕΡΓΑΣΙΑ ΕΑΡΙΝΟΥ ΕΞΑΜΗΝΟΥ 2021-22

Περιεχόμενα

1. ΕΙΣΑΓΩΓΗ

Η συγκεκριμένη είναι η δεύτερη εργασία είναι για το μάθημα Ασφάλεια πληροφοριακών και επικοινωνιακών συστημάτων. Το κύριο ζητούμενο είναι η ανάλυση ασφαλείας μιας επιχείρησης, όπου στην προκειμένη περίπτωση πρόκειται για μια κλινική, και κατ επέκταση η σύνταξη ενός σχεδίου ασφαλείας για την επίτευξη καλύτερης ασφάλειας

1.1. Περιγραφή Εργασίας

Στη συγκεκριμένη εργασία ο σκοπός είναι να αναλύσουμε την κατάσταση που βρίσκεται η ασφάλεια της κλινικής. Συγκεκριμένα αναλύθηκαν οι ευπάθειες, οι ευπάθειες και οι επιπτώσεις που θα έχουν στην κλινική αν αυτές εκμεταλλευτούν. Τέλος προτείνονται κάποια μέτρα ώστε να αντιμετωπιστούν αυτές οι ευπάθειες ώστε προστατευτούν οι κρίσιμοι πόροι και τα αγαθά της κλινικής.

1.2. Δομή παραδοτέου

Η εργασία χωρίζεται σε 4 κύριες ενότητες. Αρχίζει στο κεφάλαιο **2** με μία αναφορά στην μεθοδολογία μελέτης ασφαλείας. Σε αυτό το κεφάλαιο αναλύονται τα αγαθά και χωρίζονται σε κατηγορίες ανάλογα με το αν είναι υλισμικό, λογισμικό, δεδομένα ή διαδικασίες. Στο κεφάλαιο **3** γίνεται η αποτίμηση των πληροφοριακών συστημάτων και των εγκαταστάσεων της κλινικής. Συγκεκριμένα ταξινομούνται τα αγαθά με βάση το πόσο σημαντική είναι η προστασία τους, εντοπίζονται και καταγράφονται οι ευπάθειες και οι απειλές. Στη συνέχεια στο κεφάλαιο **4** προτείνονται κάποια μέτρα ασφαλείας και τέλος στο κεφάλαιο **5** επισημαίνονται τα πιό σημαντικά από αυτά.

2. ΜΕΘΟΔΟΛΟΓΙΑ ΜΕΛΕΤΗΣ ΑΣΦΑΛΕΙΑΣ

Για τη Διαχείριση Επικινδυνότητας του/της Κλινικής 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 ασφάλειας 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 του/της Κλινικής, τα οποία με το πέρας της μελέτης θα επικαιροποιηθούν, αναβαθμιστούν ή σε κάποιες περιπτώσεις αντικατασταθούν.

2.1.1. Υλικός εξοπλισμός (hardware)

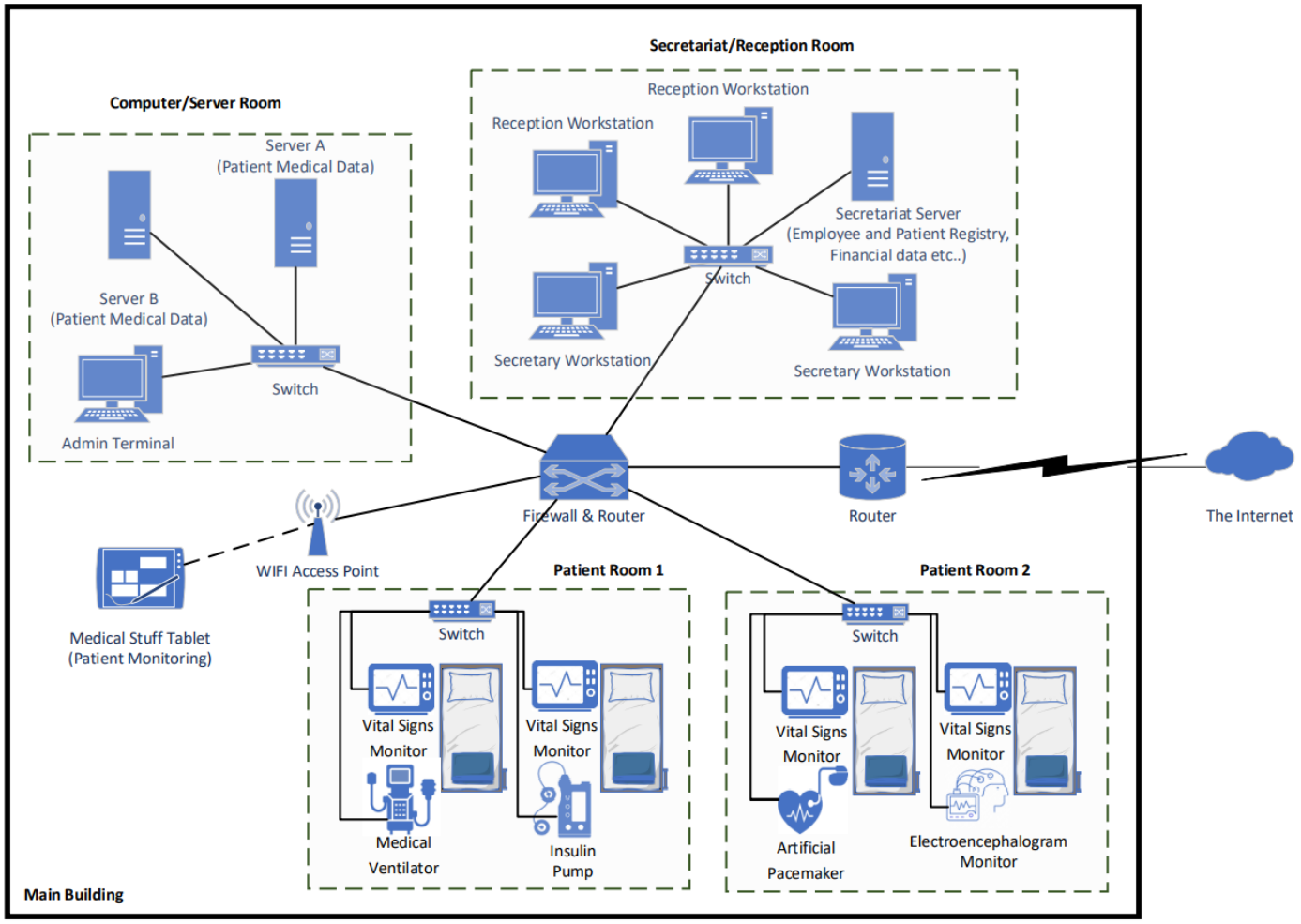
Hardware								
Inventory ID	**Asset name**	**Model**	**Type**	**Manufacturer**	**IP Address**	**Serial Number**	**Operating System**	**Location**
MED-CLIN-9011	WIFI Access Point	240AC	Access Point	Cisco	192.168.99.3	mzW}5w)nD	Cisco proprietary software	Main Building
MED-CLIN-9012	Electroencephalogram Monitor Room 2 Patient D	Arc Zenith	EEG In-hospital EMU System	Cadwell	192.168.60.5	632Ds[n)f	Linux embedded	Patient Room 2
MED-CLIN-9014	Insulin Pump Room 1 Patient B	MINIMED™ 770G	Insulin Pump	Medtronic	192.168.50.5	R6C39tDUt	Linux embedded	Patient Room 1
MED-CLIN-9015	Artificial Pacemaker Room 2 Patient C	Advisa MRI SureScan A2DR01	Pacemaker	Medtronic	192.168.60.3	7{7da((NU	Windows Embedded Compact 2013	Patient Room 2
MED-CLIN-9016	Vital Signs Monitor Room 1 Patient A	OMNI 3	Patient Monitor	Infinium	192.168.50.2	JCXUtNigF	VxWorks 5.5.1	Patient Room 1
MED-CLIN-9017	Vital Signs Monitor Room 2 Patient B	OMNI 3	Patient Monitor	Infinium	192.168.50.4	2]FW7>BZa	VxWorks 5.5.1	Patient Room 1
MED-CLIN-9018	Vital Signs Monitor Room 2 Patient C	OMNI 2	Patient Monitor	Infinium	192.168.60.2	8zJ]sNeoD	VxWorks 5.5.1	Patient Room 2
MED-CLIN-9019	Vital Signs Monitor Room 2 Patient D	OMNI 2	Patient Monitor	Infinium	192.168.60.4	3sPYNUf5D	VxWorks 5.5.1	Patient Room 2

MED-CLIN-9020	Main Router	RV160	Router	Cisco	192.168.99.1	UPvJBY5ua	Cisco proprietary software	Main Building
MED-CLIN-9021	Secretariat Server	HP ProLiant ML150	Server	HP	192.168.70.6	N}zVoVjmn	Windows Server 2012 R2 Essentials	Secretariat/Reception Room
MED-CLIN-9022	Server A	HP ProLiant ML150	Server	HP	192.168.80.2	6[9c7z2yL	Ubuntu 16.04.7 LTS	Computer/Server Room
MED-CLIN-9023	Server B	HP ProLiant ML250	Server	HP	192.168.80.3	[ZWvHSGF}	Ubuntu 16.04.7 LTS	Computer/Server Room
MED-CLIN-9024	Computer/Server Room Switch	CBS250-8FP-E-2G	Switch	Cisco	192.168.80.1	}RRQnxd8d	Cisco proprietary software	Computer/Server Room
MED-CLIN-9025	Patient Room 1 Switch	CBS250-8FP-E-2G	Switch	Cisco	192.168.50.1	oqcDXXpUF	Cisco proprietary software	Patient Room 1
MED-CLIN-9026	Patient Room 2 Switch	CBS250-8FP-E-2G	Switch	Cisco	192.168.60.1	ww9}4NTTs	Cisco proprietary software	Patient Room 2
MED-CLIN-9027	Secretariat/Reception Room Switch	CBS250-8FP-E-2G	Switch	Cisco	192.168.70.1	[L]P6M>Td	Cisco proprietary software	Secretariat/Reception Room
MED-CLIN-9028	Medical Stuff Tablet	Galaxy Tab B	Tablet	Samsung	192.168.99.4	bW)hnM(M4	Android 7 Nougat (API 24)	Main Building
MED-CLIN-9029	Medical Ventilator Room 1 Patient A	HAMILTON-MR1	Ventilator	Hamilton Medical	192.168.50.3	S}UqwG9[i	BlackBerry QNX 6.4.1	Patient Room 1
MED-CLIN-9030	Admin Terminal	ThinkCentre M90t	Workstation	Lenovo	192.168.80.4	ocfv]26Ch	Windows 10 Pro	Computer/Server Room
MED-CLIN-9031	Reception Workstation A	ThinkCentre M90t	Workstation	Lenovo	192.168.70.4	m]>TDx3w]	Windows Vista Service Pack 2 (SP2)	Secretariat/Reception Room
MED-CLIN-9032	Reception Workstation B	ThinkCentre M90t	Workstation	Lenovo	192.168.70.5	r4Eda{2Q>	Windows Vista Service Pack 2 (SP2)	Secretariat/Reception Room
MED-CLIN-9033	Secretary Workstation A	ThinkCentre M90t	Workstation	Lenovo	192.168.70.2	xbyMiB{dK	Windows Vista Service Pack 2 (SP2)	Secretariat/Reception Room
MED-CLIN-9034	Secretary Workstation B	ThinkCentre M90t	Workstation	Lenovo	192.168.70.3	[8RA4haTd	Windows Vista Service Pack 2 (SP2)	Secretariat/Reception Room
MED-CLIN-9035	Intrusion Detection System	SN710	IDS	Stormshield				Main Building

2.1.2. Λογισμικό και εφαρμογές

Software								
Inventory ID	**Asset name**	**Model**	**Type**	**Manufacturer**	**IP Address**	**Serial Number**	**Operating System**	**Location**
MED-CLIN-9009	Windows Server 2012 R2 Essentials	-	Software	Microsoft	-	-	-	Server
MED-CLIN-9010	Windows Vista Service Pack 2 (SP2)	-	Software	Microsoft	-	-	-	Workstation
MED-CLIN-9035*	Avast Business Antivirus	-	Software	Avast	-	-	-	Workstations, Admins Terminal
MED-CLIN-9036*	Data Loss Prevention(DLP)	-	Software	McAfee	-	-	-	Servers
MED-CLIN-9037*	Security Information and Event Management(SIEM)	-	Software	Exabeam	-	-	-	Servers

2.1.3. Δίκτυο


Secretariat/Reception Room
Computer/Server Room
Reception Workstation
Reception Workstation
Server A
(Patient Medical Data)
Secretariat Server
(Employee and Patient Registry,
Financial data etc..)
Server B
(Patient Medical Data)
Switch
Switch
Secretary Workstation
Secretary Workstation
Admin Terminal
Firewall & Router
Router
The Internet
WIFI Access Point
Medical Stuff Tablet
(Patient Monitoring)
Patient Room 1
Patient Room 2
Switch
Switch
Vital Signs
Monitor
Vital Signs
Monitor
Vital Signs
Monitor
Vital Signs
Monitor
Medical
Ventilator
Insulin
Pump
Artificial
Pacemaker
Electroencephalogram
Monitor
Main Building

2.1.4. Δεδομένα

Data								
Inventory ID	**Asset name**	**Model**	**Type**	**Manufacturer**	**IP Address**	**Serial Number**	**Operating System**	**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

Processes								
Inventory ID	**Asset name**	**Model**	**Type**	**Manufacturer**	**IP Address**	**Serial Number**	**Operating System**	**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

Η αποτίμηση έγινε με τον εξής τρόπο. Αρχικά, στο κεφάλαιο **3.1** έγινε καταγραφή όλων των αγαθών της κλινικής ταξινομημένα με βάση τη σημαντικότητα της προστασίας τους για το συμφερον της κλινικής. Για να γίνει αυτό δόθηκε μεγαλύτερη βαρύτητα στην υγεία και μετά στο κέρδος της κλινικής. Αυτό γιατί οποιοδήποτε λάθος η επίθεση θέσει σε κίνδυνο την υγεία ασθενή θα μπορούσε να είναι καταστροφικό για την κλινική. Στη συνέχεια, στο κεφάλαιο **3.2** αποτυπώνονται σε πίνακα οι σημαντικότερες ευπάθειες που εντοπίστηκαν και στο κεφάλαιο **3.3** οι απειλές. Τέλος στο **3.4** ο ενδεικτικός πίνακας της αποτίμησης του Impact ως προς την διαθεσιμότητα, ακεραιότητα, εμπιστευτικότητα.

3.1. Αγαθά που εντοπίστηκαν

1. Main Router
2. Computer/Server Room Switch
3. Secretariat/Reception Room Switch
4. Patient Room 1 Switch,Patient Room 2 Switch
5. WIFI Access Point
6. Admin Terminal
7. Medical Stuff Tablet
8. Server A,Server B
9. Secretariat Server
10. Patient Medical Data Srv A,Patient Medical Data Srv B
11. Patient Personal Data
12. Medical Ventilator Room 1 Patient A, Insulin Pump Room 1 Patient B, Artificial Pacemaker Room 2 Patient C, Electroencephalogram Monitor Room 2 Patient D
13. Patient Monitoring
14. Reception Workstation A,Reception Workstation B
15. Secretary Workstation A,Secretary Workstation B
16. Medical Clinic Financial Data
17. Medical Clinic Employee Data
18. Payroll Process

19. Vital Signs Monitor Room 1 Patient A, Vital Signs Monitor Room 2 Patient B, Vital Signs Monitor Room 2 Patient C, Vital Signs Monitor Room 2 Patient D
20. Patient Admission
21. Supply of Drugs

3.1.1 Αγαθά που προσθέσαμε

1. Avast Business security software
2. Data Loss Prevention(DLP) Software
3. Security Information and Event Management(SIEM)

3.2. Απειλές που εντοπίστηκαν

Threats Detected		
Inventory ID	**Asset name**	**Threats**
MED-CLIN-9020	Main Router	1. Ένας εισβολέας θα μπορούσε να εκμεταλλευτεί τα τρωτά σημεία και να αυξήσει τα δικαιώματα σύνδεσης στον χρήστη root, 2. Στη συνέχεια θα μπορούσε να στείλει κακόβουλα αιτήματα HTTP και να εκτελέσει κακόβουλο κώδικα στον δρομολογητή. 3. Να πάρει τον έλεγχο του router και να μπορέσει να υποκλέψει πληροφορίες που μετακινούνται στο δίκτυο., 4. Να προσπαθήσει να προχωρήσει και στους υπόλοιπους client.
MED-CLIN-9011	WIFI Access Point	Μια επιτυχημένη εκμετάλλευση θα μπορούσε να επιτρέψει στον εισβολέα να κάνει υποκλοπές δεδομένων καθώς και phising στους υπόλοιπους ώστε να προσπαθήσουν να κάνουν enumeration με σκοπό να εκμεταλευθούν εν τέλει περεταίρω κρίσιμους πόρους, servers κτλ.
MED-CLIN-9024	Computer/Server Room Switch	MAC flooding, Switch spoofing
MED-CLIN-9027	Secretariat/Reception Room Switch	MAC flooding, Switch spoofing
MED-CLIN-9025	Patient Room 1 Switch	MAC flooding, Switch spoofing
MED-CLIN-9026	Patient Room 2 Switch	MAC flooding, Switch spoofing
MED-CLIN-9030	Admin Terminal	1. Malware, 2. RansomWare, 3. Spyware, 4. Phishing(Λάθος από το προσωπικό)

MED-CLIN-9028	Medical Stuff Tablet	1. Malware, 2. RansomWare, 3. Spyware, 4. Easy to steal, 5. Phishing, 6. Social Engineering Attacks
MED-CLIN-9022	Server A	1. Malware, 2. RansomWare, 3. Spyware
MED-CLIN-9023	Server B	1. Malware, 2. RansomWare, 3. Spyware
MED-CLIN-9021	Secretariat Server	1. Malware, 2. RansomWare, 3. Spyware
MED-CLIN-9002	Patient Medical Data Srv A	1. Malware, 2. RansomWare, 3. Spyware
MED-CLIN-9003	Patient Medical Data Srv B	1. Malware, 2. RansomWare, 3. Spyware
MED-CLIN-9004	Patient Personal Data	1.Malware, 2. RansomWare
MED-CLIN-9029	Medical Ventilator Room 1 Patient A	1. Malware, 2. Σφάλματα από το προσωπικό της κλινικής
MED-CLIN-9012	Electroencephalogram Monitor Room 2 Patient D	1. Malware, 2. Σφάλματα από το προσωπικό της κλινικής
MED-CLIN-9014	Insulin Pump Room 1 Patient B	1. Malware, 2. Σφάλματα από το προσωπικό της κλινικής
MED-CLIN-9015	Artificial Pacemaker Room 2 Patient C	1. Malware, 2. Σφάλματα από το προσωπικό της κλινικής
MED-CLIN-9031	Reception Workstation A	1. Malware, 2. RansomWare, 3. Spyware, 4. Phishing(Από λάθος υπαλλήλου), 5. Είσοδος στο σύστημα ατόμου που δεν τη δικαιούται
MED-CLIN-9032	Reception Workstation B	1. Malware, 2. RansomWare, 3. Spyware, 4. Phishing(Από λάθος υπαλλήλου), 5. Είσοδος στο σύστημα ατόμου που δεν τη δικαιούται
MED-CLIN-9033	Secretary Workstation A	1. Malware, 2. RansomWare, 3. Spyware, 4. Phishing(Από λάθος υπαλλήλου), 5. Είσοδος στο σύστημα ατόμου που δεν τη δικαιούται
MED-CLIN-9034	Secretary Workstation B	1. Malware, 2. RansomWare, 3. Spyware, 4. Phishing(Από λάθος υπαλλήλου), 5. Είσοδος στο σύστημα ατόμου που δεν τη δικαιούται
MED-CLIN-9000	Medical Clinic Employee Data	Είσοδος ατόμου στο σύστημα που δεν τη δικαιούται
MED-CLIN-9001	Medical Clinic Financial Data	Είσοδος ατόμου στο σύστημα που δεν τη δικαιούται
MED-CLIN-9005	Patient Admission	1. Λάθη στις διαδικασίας εξέτασης, παρακολούθησης, θεραπείας και φροντίδας
MED-CLIN-9006	Patient Monitoring	Σφάλματα από το προσωπικό της κλινικής
MED-CLIN-9007	Payroll Process	1. Λάθη στις επιμέρους διαδικασίες ώστε να γίνει εν τέλει η διαδικασία πληρωμής
MED-CLIN-9016	Vital Signs Monitor Room 1 Patient A	1. MalWare
MED-CLIN-9017	Vital Signs Monitor Room 2 Patient B	1. MalWare
MED-CLIN-9018	Vital Signs Monitor Room 2 Patient C	1. MalWare
MED-CLIN-9019	Vital Signs Monitor Room 2 Patient D	1. MalWare
MED-CLIN-9008	Supply of Drugs	1. Μη διαθεσιμότητα σε φάρμακα που έχουν ανάγκη οι ασθενείς

3.3. Ευπάθειες που εντοπίστηκαν

Vulnerabilities Detected		
Inventory ID	**Asset name**	**Vulnerabilities**
MED-CLIN-9020	Main Router	1. Ανεπαρκείς μηχανισμοί επιβολής εξουσιοδότησης, 2. Λανθασμένη επαλήθευση εικόνων λογισμικού στη συσκευή προορισμού , 3. Ευπάθεια άρνησης υπηρεσίας GUI, 4. Ευπάθεια απομακρυσμένης εκτέλεσης κώδικα
MED-CLIN-9011	WIFI Access Point	Ακατάλληλη επικύρωση των εισροών που παρέχονται από χρήστη
MED-CLIN-9024	Computer/Server Room Switch	Η ευπάθεια απομακρυσμένης εκτέλεσης κώδικα φαίνεται να είναι ακόμα ενεργοποιημένη από προεπιλογή
MED-CLIN-9027	Secretariat/Reception Room Switch	Η ευπάθεια απομακρυσμένης εκτέλεσης κώδικα φαίνεται να είναι ακόμα ενεργοποιημένη από προεπιλογή
MED-CLIN-9025	Patient Room 1 Switch	Η ευπάθεια απομακρυσμένης εκτέλεσης κώδικα φαίνεται να είναι ακόμα ενεργοποιημένη από προεπιλογή
MED-CLIN-9026	Patient Room 2 Switch	Η ευπάθεια απομακρυσμένης εκτέλεσης κώδικα φαίνεται να είναι ακόμα ενεργοποιημένη από προεπιλογή
MED-CLIN-9030	Admin Terminal	1. Παλιό λειτουργικό σύστημα, 2. Λάθος από το χειριστή, 3. Παλιό Antivirus, 4. Πρόσβαση από άτομο που δε τη δικαιούται
MED-CLIN-9028	Medical Stuff Tablet	1. Παλιό λειτουργικό σύστημα, 2. Λάθος απο το χειριστή, 3. Παλιό Antivirus, 4. Πρόσβαση απο άτομο που δε τη δικαιούται
MED-CLIN-9022	Server A	1. Παλιό λειτουργικό σύστημα (Ubuntu 16.04.7 LTS), 2. Data not encrypted, 3.Weak or nonexistent authentication,
MED-CLIN-9023	Server B	1. Παλιό λειτουργικό σύστημα(Ubuntu 16.04.7 LTS), 2. Data not encrypted, 3.Weak or nonexistent authentication,
MED-CLIN-9021	Secretariat Server	1. Παλιό λειτουργικό σύστημα(Windows Server 2012 R2 Essentials), 2. Data not encrypted, 3.Weak or nonexistent authentication,
MED-CLIN-9002	Patient Medical Data Srv A	1. Δεν κρατιέται αντίγραφο ασφαλείας της βάσης δεδομένων
MED-CLIN-9003	Patient Medical Data Srv B	1. Δεν κρατιέται αντίγραφο ασφαλείας της βάσης δεδομένων
MED-CLIN-9004	Patient Personal Data	Τα δεδομένα δεν είναι κρυπτογραφημένα
MED-CLIN-9029	Medical Ventilator Room 1 Patient A	1. Παλιό λειτουργικό σύστημα, 2. Ελλιπής εκπαίδευση προσωπικού

MED-CLIN-9012	Electroencephalogram Monitor Room 2 Patient D	1. Παλιό λειτουργικό σύστημα, 2. Ελλιπής εκπαίδευση προσωπικού
MED-CLIN-9014	Insulin Pump Room 1 Patient B	1. Παλιό λειτουργικό σύστημα, 2. Ελλιπής εκπαίδευση προσωπικού
MED-CLIN-9015	Artificial Pacemaker Room 2 Patient C	1. Παλιό λειτουργικό σύστημα, 2. Ελλιπής εκπαίδευση προσωπικού
MED-CLIN-9031	Reception Workstation A	1. Παλιό λειτουργικό σύστημα(Windows Vista Service Pack 2 (SP2)), 2. Υπαρξη accounts υπαλλήλων που δεν εργάζονται πλέον στην εταιρεία
MED-CLIN-9032	Reception Workstation B	1. Παλιό λειτουργικό σύστημα(Windows Vista Service Pack 2 (SP2)), 2. Υπαρξη accounts υπαλλήλων που δεν εργάζονται πλέον στην εταιρία
MED-CLIN-9033	Secretary Workstation A	1. Παλιό λειτουργικό σύστημα(Windows Vista Service Pack 2 (SP2)), 2. Υπαρξη accounts υπαλλήλων που δεν εργάζονται πλέον στην εταιρία
MED-CLIN-9034	Secretary Workstation B	1. Παλιό λειτουργικό σύστημα(Windows Vista Service Pack 2 (SP2)), 2. Υπαρξη accounts υπαλλήλων που δεν εργάζονται πλέον στην εταιρία
MED-CLIN-9000	Medical Clinic Employee Data	Τα δεδομένα δεν είναι κρυπτογραφημένα
MED-CLIN-9001	Medical Clinic Financial Data	Τα δεδομένα δεν είναι κρυπτογραφημένα
MED-CLIN-9005	Patient Admission	1. Ελλιπής εκπαίδευση προσωπικού
MED-CLIN-9006	Patient Monitoring	Σφάλματα από το προσωπικό της κλινικής
MED-CLIN-9007	Payroll Process	1. Οργανωτική ασυνέπεια , 2. μη διαθεσιμότητα εργαζομένων
MED-CLIN-9016	Vital Signs Monitor Room 1 Patient A	1. Παλιό λειτουργικό σύστημα, 2. Ελλιπής εκπαίδευση προσωπικού
MED-CLIN-9017	Vital Signs Monitor Room 2 Patient B	1. Παλιό λειτουργικό σύστημα, 2. Ελλιπής εκπαίδευση προσωπικού
MED-CLIN-9018	Vital Signs Monitor Room 2 Patient C	1. Παλιό λειτουργικό σύστημα, 2. Ελλιπής εκπαίδευση προσωπικού
MED-CLIN-9019	Vital Signs Monitor Room 2 Patient D	1. Παλιό λειτουργικό σύστημα, 2. Ελλιπής εκπαίδευση προσωπικού
MED-CLIN-9008	Supply of Drugs	1. Ελλιπής εκπαίδευση προσωπικού

3.4. Αποτελέσματα αποτίμησης

Ο παρακάτω φαίνεται ο ενδεικτικός πίνακας της αποτίμησης του Impact, για κάθε αγαθό της κλινικής που χρειάζεται προστασία, ως προς την διαθεσιμότητα, ακεραιότητα, εμπιστευτικότητα.

	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 κίνησης	Μη παράδοση	Απώλεια ακολουθίας μηνυμάτων
Main Router	8	9	10	10	10	10	10	10	7	8	7	10	5	6	8	7	8	8	7	7	10	8	7	7
Computer/Server Room Switch	7	7	8	9	9	9	9	9	7	7	6	8	5	6	8	6	6	6	7	6	9	7	7	6
Secretariat/Reception Room Switch	6	7	8	9	9	9	9	9	7	7	6	8	5	6	8	6	6	6	6	6	9	7	7	6
Patient Room 1 Switch	6	7	8	9	9	9	9	9	7	7	6	8	5	6	8	6	6	6	6	6	9	7	7	6
Patient Room 2 Switch	6	7	8	9	9	9	9	9	7	7	6	8	5	6	8	6	6	6	6	6	9	7	7	4
WIFI Access Point	5	6	7	8	9	9	9	8	6	7	6	7	5	6	7	5	5	5	5	5	9	8	5	5
Admin Terminal	5	6	7	9	9	9	9	7	6	7	6	7	5	6	7	1	1	1	1	1	1	1	1	1
Medical Stuff Tablet	6	9	9	9	9	9	9	7	6	7	6	7	5	6	7	1	1	1	1	1	1	1	1	1
Server A,Server B	6	8	8	9	9	9	9	7	5	8	6	7	5	6	8	1	1	1	1	1	1	1	1	1

Secretariat Server	6	8	8	9	9	9	9	7	5	8	6	7	5	6	8	1	1	1	1	1	1	1	1	1
Patient Medical Data Srv A, Patient Medical Data Srv B	6	8	8	9	9	9	9	7	5	8	6	7	5	6	8	1	1	1	1	1	1	1	1	1
Patient Personal Data	6	8	8	9	9	9	9	9	7	7	7	9	5	6	7	1	1	1	1	1	1	1	1	1
Medical Ventilator Room 1 Patient A	8	9	9	9	9	9	9	9	7	6	4	7	5	6	7	1	7	7	9	8	1	1	8	1
Insulin Pump Room 1 Patient B	8	9	9	9	9	9	9	9	7	6	4	7	5	6	7	1	7	7	9	8	1	1	8	1
Artificial Pacemaker Room 2 Patient C	8	9	9	9	9	9	9	9	7	6	4	7	5	6	7	1	7	7	9	8	1	1	8	1
Electroencephalogram Monitor Room 2 Patient D	8	9	9	9	9	9	9	9	7	6	4	7	5	6	7	1	7	7	9	8	1	1	8	1
Patient Monitoring	6	6	7	7	8	9	9	7	5	5	4	6	5	5	6	1	1	1	1	1	1	1	1	1
Reception Workstation A,Reception Workstation B	5	6	7	7	7	7	7	6	6	7	6	7	5	6	7	1	1	1	1	1	1	1	1	1
Secretary Workstation A,Secretary Workstation B	5	6	7	7	7	7	7	6	6	7	6	7	5	6	7	1	1	1	1	1	1	1	1	1
Medical Clinic Financial Data	5	6	8	8	8	8	8	8	7	7	6	9	5	6	7	1	1	1	1	1	1	1	1	1

Medical Clinic Employee Data	5	6	8	8	8	8	8	8	7	7	6	8	5	6	7	1	1	1	1	1	1	1	1	1
Payroll Process	2	3	4	5	5	6	6	6	5	3	4	6	5	4	6	1	1	1	1	1	1	1	1	1
Vital Signs Monitor Room 1 Patient A, Vital Signs Monitor Room 2 Patient B, Vital Signs Monitor Room 2 Patient C, Vital Signs Monitor Room 2 Patient D	2	3	4	5	5	6	6	6	5	3	4	6	5	4	6	1	1	1	1	1	1	1	1	1
Patient Admission	2	3	4	5	6	7	7	7	5	3	4	6	5	4	6	1	1	1	1	1	1	1	1	1
Supply of Drugs	2	5	6	6	6	7	7	7	4	4	4	7	5	5	6	1	1	1	1	1	1	1	1	1

4. ΠΡΟΤΕΙΝΟΜΕΝΑ ΜΕΤΡΑ ΑΣΦΑΛΕΙΑΣ

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

A1. Προσωπικό – Προστασία Διαδικασιών Προσωπικού

A2. Ταυτοποίηση και αυθεντικοποίηση

A3. Έλεγχος προσπέλασης και χρήσης πόρων

A4. Διαχείριση εμπιστευτικών δεδομένων

A5. Προστασία από τη χρήση υπηρεσιών από τρίτους

A6. Προστασία λογισμικού

A7. Διαχείριση ασφάλειας δικτύου

A8. Προστασία από ιομορφικό λογισμικό

A9. Ασφαλής χρήση διαδικτυακών υπηρεσιών

A10. Ασφάλεια εξοπλισμού

A11. Φυσική ασφάλεια κτιριακής εγκατάστασης

Τα μέτρα έχουν εφαρμογή στο ΠΣ του/της Κλινικής.

4.1. Προσωπικό – Προστασία Διαδικασιών Προσωπικού

Μέτρα :

1) Εκπαίδευση προσωπικού
2) Παρακολούθηση απώλειας προσωπικού(Sick Days)
3) Οδηγίες σχετικά με την απώλεια συσκευής
4) Προσοχή για email που έχουν στόχο Phishing
5) Log Monitoring

Για τα αγαθά :

1) Admin Terminal , **MED-CLIN-9030**
2) Medical Stuff Tablet, **MED-CLIN-9028**
3) Medical Ventilator Room 1 Patient A, **MED-CLIN-9029**
4) Insulin Pump Room 1 Patient B, **MED-CLIN-9014**
5) Artificial Pacemaker Room 2 Patient C, **MED-CLIN-9015**
6) Electroencephalogram Monitor Room 2 Patient D, **MED-CLIN-9012**
7) Patient Monitoring, **MED-CLIN-9006**
8) Reception Workstation A,Reception Workstation B, **MED-CLIN-9031**, **MED-CLIN-9032**
9) Secretary Workstation A,Secretary Workstation B, **MED-CLIN-9033**, **MED-CLIN-9034**
10) Payroll Process,
11) Vital Signs Monitor Room 1 Patient A, Vital Signs Monitor Room 2 Patient B, Vital Signs Monitor Room 2 Patient C, Vital Signs Monitor Room 2 Patient D, **MED-CLIN-9016** ,**MED-CLIN-9017** ,**MED-CLIN-9018** ,**MED-CLIN-9019**
12) Patient Admission, **MED-CLIN-9005**
13) Supply of Drugs, **MED-CLIN-9008**

4.2. Ταυτοποίηση και αυθεντικοποίηση

Μέτρα :

1) Υποχρεωτικός έλεγχος εισόδου,
2) Διπλή αυθεντικοποίηση
3) Συχνή αλλαγή κωδικών
4) Ασφαλές WPA password

Για τα αγαθά :

1) Main Router, **MED-CLIN-9020**
2) Admin Terminal , **MED-CLIN-9030**
3) Computer/Server Room Switch, **MED-CLIN-9024**
4) Secretariat/Reception Room Switch, **MED-CLIN-9027**
5) Patient Room 1 Switch, **MED-CLIN-9025**
6) Patient Room 2 Switch, **MED-CLIN-9026**
7) WIFI Access Point, **MED-CLIN-9011**
8) Reception Workstation A,Reception Workstation B, **MED-CLIN-9031**, **MED-CLIN-9032**
9) Secretary Workstation A,Secretary Workstation B, **MED-CLIN-9033**, **MED-CLIN-9034**
10) Medical Stuff Tablet, **MED-CLIN-9028**

4.3. Έλεγχος προσπέλασης και χρήσης πόρων

Μέτρα :

1) Διπλή αυθεντικοποίηση
2) Απενεργοποίηση λογαριασμών παλαιών εργαζομένων
3) Κρυπτογράφηση δεδομένων
4) Log Monitoring
5) Έλεγχος αν τα δεδομένα συμπίπτουν με τα backup

Για τα αγαθά :

1) Admin Terminal , **MED-CLIN-9030**
2) Reception Workstation A,Reception Workstation B, **MED-CLIN-9031**, **MED-CLIN-9032**
3) Secretary Workstation A,Secretary Workstation B, **MED-CLIN-9033**, **MED-CLIN-9034**
4) Medical Stuff Tablet, **MED-CLIN-9028**
5) Patient Monitoring, **MED-CLIN-9006**

4.4. Διαχείριση εμπιστευτικών δεδομένων

Μετρα:

1) Ημερήσια αντίγραφα ασφαλείας
2) Κρυπτογράφηση δεδομένων
3) Log Monitoring
4) Canary Tokens(traps)
5) Οι back up servers να φυλάσσονται σε μέρη χωρίς πρόσβαση στο ιντερνετ

Για τα αγαθά:

1) Server A,Server B, **MED-CLIN-9022, MED-CLIN-9023**
2) Secretariat Server, **MED-CLIN-9021**
3) Patient Medical Data Srv A, Patient Medical Data Srv B, **MED-CLIN-9002, MED-CLIN-9003**
4) Patient Personal Data, **MED-CLIN-9004**
5) Medical Clinic Financial Data, **MED-CLIN-9001**
6) Medical Clinic Employee Data, **MED-CLIN-9000**
7) Patient Monitoring, **MED-CLIN-9006**

4.5. Προστασία από τη χρήση υπηρεσιών από τρίτους

Μέτρα:

1) Απενεργοποίηση λογαριασμών παλαιών εργαζομένων
2) Οδηγίες σχετικά με την απώλεια συσκευής
3) Log Monitoring
4) Canary Tokens(traps)

Για τα αγαθά:

1) Admin Terminal , **MED-CLIN-9030**
2) Reception Workstation A,Reception Workstation B, **MED-CLIN-9031**, **MED-CLIN-9032**
3) Secretary Workstation A,Secretary Workstation B, **MED-CLIN-9033**, **MED-CLIN-9034**
4) Medical Stuff Tablet, **MED-CLIN-9028**

4.6. Προστασία λογισμικού

Μέτρα:

1) Αναβάθμιση λειτουργικού συστήματος
2) Εγκατάσταση Antivirus και συνεχείς αναβαθμίσεις στα μηχανήματα
3) Εγκατάσταση μόνο απαραίτητων υπηρεσιών σε αυτά
4) Προστασία Firewall
5) Frequent vulnerability scans(Nessus)

Για τα αγαθά:

1) Admin Terminal , **MED-CLIN-9030**
2) Reception Workstation A,Reception Workstation B, **MED-CLIN-9031**, **MED-CLIN-9032**
3) Secretary Workstation A,Secretary Workstation B, **MED-CLIN-9033**, **MED-CLIN-9034**
4) Medical Stuff Tablet, **MED-CLIN-9028**
5) Medical Ventilator Room 1 Patient A, **MED-CLIN-9029**
6) Insulin Pump Room 1 Patient B, **MED-CLIN-9014**
7) Artificial Pacemaker Room 2 Patient C, **MED-CLIN-9015**
8) Electroencephalogram Monitor Room 2 Patient D, **MED-CLIN-9012**
9) Vital Signs Monitor Room 1 Patient A, Vital Signs Monitor Room 2 Patient B, Vital Signs Monitor Room 2 Patient C, Vital Signs Monitor Room 2 Patient D, **MED-CLIN-9016** ,**MED-CLIN-9017** ,**MED-CLIN-9018** ,**MED-CLIN-9019**
10) Server A,Server B, **MED-CLIN-9022, MED-CLIN-9023**
11) Secretariat Server, **MED-CLIN-9021**

12) Patient Medical Data Srv A, Patient Medical Data Srv B, **MED-CLIN-9002, MED-CLIN-9003**

4.7. Διαχείριση ασφάλειας δικτύου

Μέτρα:

1) Segmentation - Zero Trust Response
2) Η ενεργοποίηση του telnet στους switches
3) Η καλύτερη αντικατάσταση για το telnet είναι το SSH
4) Ασφαλές WPA password
5) Οι back up servers να φυλάσσονται σε μέρη χωρίς πρόσβαση στο ιντερνετ

Για τα αγαθά:

1) Main Router, **MED-CLIN-9020**
2) Computer/Server Room Switch, **MED-CLIN-9024**
3) Secretariat/Reception Room Switch, **MED-CLIN-9027**
4) Patient Room 1 Switch, **MED-CLIN-9025**
5) Patient Room 2 Switch, **MED-CLIN-9026**
6) WIFI Access Point, **MED-CLIN-9011**
7) Server A,Server B, **MED-CLIN-9022, MED-CLIN-9023**
8) Secretariat Server, **MED-CLIN-9021**
9) Patient Medical Data Srv A, Patient Medical Data Srv B, **MED-CLIN-9002, MED-CLIN-9003**

4.8. Προστασία από ιομορφικό λογισμικό

Μέτρα:

1) Αναβάθμιση λειτουργικού συστήματος
2) Εγκατάσταση Antivirus και συνεχείς αναβαθμίσεις στα μηχανήματα
3) Εγκατάσταση μόνο απαραίτητων υπηρεσιών σε αυτά
4) Προστασία Firewall
5) Frequent vulnerability scans(Nessus)

Για τα αγαθά:

1) Admin Terminal , **MED-CLIN-9030**
2) Reception Workstation A,Reception Workstation B, **MED-CLIN-9031**, **MED-CLIN-9032**
3) Secretary Workstation A,Secretary Workstation B, **MED-CLIN-9033**, **MED-CLIN-9034**
4) Medical Stuff Tablet, **MED-CLIN-9028**
5) Medical Ventilator Room 1 Patient A, **MED-CLIN-9029**
6) Insulin Pump Room 1 Patient B, **MED-CLIN-9014**
7) Artificial Pacemaker Room 2 Patient C, **MED-CLIN-9015**
8) Electroencephalogram Monitor Room 2 Patient D, **MED-CLIN-9012**
9) Vital Signs Monitor Room 1 Patient A, Vital Signs Monitor Room 2 Patient B, Vital Signs Monitor Room 2 Patient C, Vital Signs Monitor Room 2 Patient D, **MED-CLIN-9016** ,**MED-CLIN-9017** ,**MED-CLIN-9018** ,**MED-CLIN-9019**
10) Server A,Server B, **MED-CLIN-9022, MED-CLIN-9023**
11) Secretariat Server, **MED-CLIN-9021**

12) Patient Medical Data Srv A, Patient Medical Data Srv B, **MED-CLIN-9002, MED-CLIN-9003**

4.9. Ασφαλής χρήση διαδικτυακών υπηρεσιών

Μέτρα:

1) Προστασία Firewall
2) Εγκατάσταση Antivirus και συνεχείς αναβαθμίσεις στα μηχανήματα

Για τα αγαθά:

1) Admin Terminal , **MED-CLIN-9030**
2) Reception Workstation A,Reception Workstation B, **MED-CLIN-9031**, **MED-CLIN-9032**
3) Secretary Workstation A,Secretary Workstation B, **MED-CLIN-9033**, **MED-CLIN-9034**
4) Medical Stuff Tablet, **MED-CLIN-9028**

4.10. Ασφάλεια εξοπλισμού

Μέτρα:

1) Εφεδρικές υλικές Βάσεις δεδομένων σε απομονωμένα από το δίκτυο δωμάτια

Για τα αγαθά:

1) Server A,Server B, **MED-CLIN-9022, MED-CLIN-9023**
2) Secretariat Server, **MED-CLIN-9021**
3) Patient Medical Data Srv A, Patient Medical Data Srv B, **MED-CLIN-9002, MED-CLIN-9003**

4.11. Φυσική ασφάλεια κτιριακής εγκατάστασης

Μέτρα:

1) Έλεγχοι φυσικής εισόδου στις εγκαταστάσεις
2) CCTV
3) Πυροσβεστήρες

Για τα αγαθά:

Όλα τα αγαθά που βρίσκονται στη λίστα με τα Hardware

5. ΣΥΝΟΨΗ ΠΙΟ ΚΡΙΣΙΜΩΝ ΑΠΟΤΕΛΕΣΜΑΤΩΝ

Τα πιο κρίσιμα αποτελέσματα που βγήκαν από τη μελέτη είναι ότι τα πιο σημαντικά αγαθά για την εταιρία είναι το router, τα switches και το Wifi Access Point. Η καλή προστασία των αγαθών αυτών είναι ζωτικής σημασίας για την κλινική καθώς είναι οι βασικές οδοί για κάποιον επιτιθέμενο να εισχωρήσει στα συστήματα της εταιρείας.

6. ΑΝΑΦΟΡΕΣ

1. https://www.techepages.com/cvss-10-critical-vulnerabilities-on-cisco-rv160-and-rv260-series-routers/

2. https://www.cisco.com/c/en/us/support/docs/csa/cisco-sa-rv160-260-rce-XZeFkNHf.html

3. https://web.mit.edu/rhel-doc/4/RH-DOCS/rhel-sg-en-4/s1-risk-serv.html

4. https://vulmon.com/searchpage?q=microsoft+windows+server+2012

5. https://routersecurity.org/whatcangowrong.php#:~:text=One%20section%20details%20what%20can,redirected%2C%20changed%2C%20or%20denied.

6. https://www.ncbi.nlm.nih.gov/pmc/articles/PMC8398009/

7. https://www.google.com/search?q=enumeration+in+hacking&rlz=1C1YTUH_enGR983GR983&oq=enumeration++in+hacking&aqs=chrome..69i57j0i512j0i22i30l4j0i390l3.6473j0j7&sourceid=chrome&ie=UTF-8

8. https://www.paloaltonetworks.com/blog/2019/01/you-want-network-segmentation-but-you-need-zero-trust/

9. https://technologyadvice.com/security-software/