ΑΣΦΑΛΕΙΑ ΠΛΗΡΟΦΟΡΙΑΚΩΝ ΣΥΣΤΗΜΑΤΩΝ ΚΑΙ ΚΡΙΣΙΜΩΝ ΥΠΟΔΟΜΩΝ

ΣΧΕΔΙΟ ΑΣΦΑΛΕΙΑΣ

ΣΥΓΓΡΑΦΕΙΣ: Τσολάκου Διογένης (3170164), Αργυρόπουλος Χρήστος (3170010)

ΕΡΓΑΣΙΑ ΧΕΙΜΕΡΙΝΟΥ ΕΞΑΜΗΝΟΥ 2020-21

Contents

1. ΕΙΣΑΓΩΓΗ

1.1. Περιγραφή Εργασίας

Το παρόν έγγραφο είναι ένα Σχέδιο Ασφάλειας στα πλαίσια της εργασίας του μαθήματος Ασφάλεια Πληροφοριακών Συστημάτων του Οικονομικού Πανεπιστημίου Αθηνών (ΟΠΑ). Το συγκεκριμένο Σχέδιο Ασφάλειας αφορά την ανάλυση επικινδυνότητας ενός πληροφοριακού συστήματος στο περιβάλλον Βιομηχανίας της Πληροφορικής το οποίο επεξεργάζεται προσωπικά δεδομένα.

1.2. Δομή παραδοτέου

Στην Ενότητα 2 περιγράφεται λεπτομερώς η μεθοδολογία που ακολουθήθηκε. Στην Ενότητα 3 αποτιμάται το Πληροφοριακό Σύστημα και οι εγκαταστάσεις της βιομηχανίας, καθώς παρουσιάζονται και τα αποτελέσματα της αποτίμησης αυτής. Στην Ενότητα 4, προτείνονται μέτρα ασφαλείας αναλόγως των αποτελεσμάτων της αποτίμησης. Τέλος, στην Ενότητα 5, συνοψίζονται τα κρισιμότερα αποτελέσματα της μελέτης.

2. ΜΕΘΟΔΟΛΟΓΙΑ ΜΕΛΕΤΗΣ ΑΣΦΑΛΕΙΑΣ

Για τη Διαχείριση Επικινδυνότητας του Πληροφοριακού Συστήματος 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.

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*

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

2.1. Περιγραφή Πληροφοριακού Συστήματος (ΠΣ) υπό έλεγχο

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

2.1.1. Υλικός εξοπλισμός (hardware)

Ο υλικός εξοπλισμός του ΠΣ αποτελείται από εφτά (7) workstation, από τα οποία το ένα (1) είναι ένα laptop ενώ τα άλλα έξι (6) είναι υπολογιστές, ένα (1) IP τηλέφωνο, ένα (1) tablet και έναν (1) εκτυπωτή.

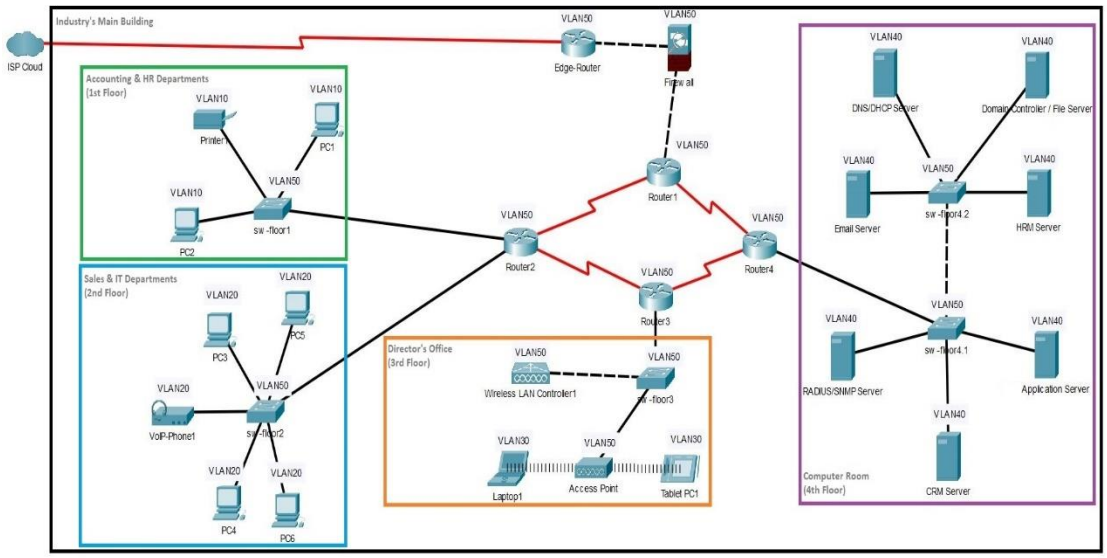
TYPE	MODEL	QUANTITY
Workstation	ThinkPad X13 Yoga (13") Intel	1
Workstation	ThinkCentre M90t	6
IP Phone	IP Phone 8811	1
Tablet	Galaxy Tab A	1
Printer	EcoTank L1800 ITS	1

2.1.2. Λογισμικό και εφαρμογές

Το λογισμικό και οι εφαρμογές του ΠΣ είναι τέσσερις (4) εκδόσεις Windows, 10 Pro, 7, Server 2008 και XP, το λειτουργικό του tablet, δύο (2) εκδόσεις Ubuntu, 16.04.7 LTS και 12.04.5 LTS, το ιδιόκτητο λογισμικό της Cisco στα router, switches, access point, IP phone και wireless controller και το ιδιόκτητο λογισμικό της Epson στον εκτυπωτή.

TYPE	OPERATION SYSTEM
Workstation (x3)	Windows 10 Pro
Workstation (x2)	Windows 7
Workstation (x2)	Windows XP
Tablet (x1)	Android 9 Pie (API 28)
Server (x3)	Ubuntu 16.04.7 LTS
Server (x3)	Windows Server 2008
Server (x1)	Ubuntu 12.04.5 LTS
Router (x5)	Cisco proprietary software
Switch (x5)	Cisco proprietary software
Printer (x1)	Epson proprietary software
Phone (x1)	Cisco proprietary software
Wireless Controller (x1)	Cisco proprietary software
Access Point (x1)	Cisco proprietary software

2.1.3. Δίκτυο



Το backbone του δικτύου αποτελείται από 4 Router συνδεδεμένα μεταξύ τους. Το Router1 επικοινωνεί με το Edge Router (χωρίς το firewall που φαίνεται στην εικόνα), ενώ τα υπόλοιπα 3 Router συνδέουν τα εσωτερικά τμήματα της επιχείρησης. Το Router2 συνδέεται με τα Accounting & HR Departments και Sales & IT Departments. Το Router3 συνδέεται με το γραφείο του διευθυντή. Το Router4 συνδέεται με το Computer Room. Στον παρακάτω πίνακα φαίνεται το υλικό από το οποίο αποτελείται το δίκτυο:

TYPE	MODEL	QUANTITY
Server	HP ProLiant ML150	2
Server	HP ProLiant ML250	1
Server	HP ProLiant ML350	1
Server	HP ProLiant ML251	1
Server	HP ProLiant ML450	2
Switch	CBS250-8FP-E-2G	5
Router	RV160	4
Router	ASR 1002-HX	1
Wireless Controller	Catalyst 9800-L	1
Access Point	240AC	1

2.1.4. Δεδομένα

- Δεδομένα πελατών βιομηχανίας
- Δεδομένα υπαλλήλων βιομηχανίας

2.1.5. Διαδικασίες

- Δημιουργία νέου πελάτη
- Δημιουργία νέας τοπικής παραγγελίας
- Δημιουργία νέας απομακρυσμένης παραγγελίας
- Εξυπηρέτηση πελατών

3. ΑΠΟΤΙΜΗΣΗ ΠΣ ΚΑΙ ΕΓΚΑΤΑΣΤΑΣΕΩΝ ΒΙΟΜΗΧΑΝΙΑΣ

3.1. Αγαθά που εντοπίστηκαν

Τα πιο κρίσιμα αγαθά που εντοπίστηκαν είναι : οι server (DNS/DCHP, CRM, HRM, Application, Email, RADIUS/SNMP, Domain Controller/File Server), τα router (1, 2, 3 και ειδικότερα το 4 και το Edge) και τα switches (1, 3 και ειδικότερα τα 2, 4.1 και 4.2).

Ενώ τα συνολικά αγαθά που εντοπίστηκαν στο συγκεκριμένο Πληροφοριακό Σύστημα είναι τα εξής :

INVENTORY ID	ASSET NAME	TYPE	MODEL
CI-A-1000	Industry Customer Data	Data	-
CI-A-1001	Industry Employee Data	Data	-
CI-A-1002	Create New Customer	Process	-
CI-A-1003	Create New Order (Local)	Process	-
CI-A-1004	Create New Order (Remotely)	Process	-
CI-A-1005	Customer Support	Process	-
CI-A-1006	Windows 10 Pro	Software	-
CI-A-1007	Windows 7	Software	-
CI-A-1008	LAPTOP1	Workstation	ThinkPad X13 Yoga (13") Intel
CI-A-1009	PC5	Workstation	ThinkCentre M90t
CI-A-1010	CRM Server	Server	HP ProLiant ML150
CI-A-1012	ROUTER2	Router	RV160
CI-A-1013	VOIP-PHONE1	IP Phone	IP Phone 8811
CI-A-1011	RADIUS/SNMP SERVER	Server	HP ProLiant ML250
CI-A-1015	ROUTER3	Router	RV160
CI-A-1016	WIRELESS-LAN-CONTROLLER1	Wireless Controller	Catalyst 9800-L
CI-A-1017	TABLET-PC1	Tablet	Galaxy Tab A
CI-A-1018	EMAIL SERVER	Server	HP ProLiant ML150
CI-A-1019	PC4	Workstation	ThinkCentre M90t
CI-A-1020	PC6	Workstation	ThinkCentre M90t
CI-A-1021	PRINTER1	Printer	EcoTank L1800 ITS
CI-A-1022	EDGE-ROUTER	Router	ASR 1002-HX
CI-A-1023	DNS/DHCP SERVER	Server	HP ProLiant ML450
CI-A-1024	HRM SERVER	Server	HP ProLiant ML450
CI-A-1025	SW-FLOOR4.1	Switch	CBS250-8FP-E-2G
CI-A-1026	ROUTER1	Router	RV160
CI-A-1027	SW-FLOOR4.2	Switch	CBS250-8FP-E-2G
CI-A-1028	ROUTER4	Router	RV160
CI-A-1029	APPLICATION SERVER	Server	HP ProLiant ML251
CI-A-1030	PC3	Workstation	ThinkCentre M90t
CI-A-1031	PC1	Workstation	ThinkCentre M90t
CI-A-1032	PC2	Workstation	ThinkCentre M90t
CI-A-1033	DOMAIN CONTROLLER/FILE SERVER	Server	HP ProLiant ML350
CI-A-1034	SW-FLOOR2	Switch	CBS250-8FP-E-2G
CI-A-1035	ACCESS POINT	Access Point	240AC

CI-A-1036	SW-FLOOR1	Switch	CBS250-8FP-E-2G
CI-A-1037	SW-FLOOR3	Switch	CBS250-8FP-E-2G

3.2. Απειλές που εντοπίστηκαν

INVENTORY ID	ASSET NAME	TYPE	THREAT
CI-A-1000	Industry Customer Data	Data	Σκόπιμη : Κάποιος επιθυμεί πρόσβαση σε αυτά
CI-A-1001	Industry Employee Data	Data	
CI-A-1002	Create New Customer	Process	Τυχαία : Λανθασμένη εισαγωγή στοιχείων
CI-A-1003	Create New Order (Local)	Process	
CI-A-1004	Create New Order (Remotely)	Process	
CI-A-1005	Customer Support	Process	Σκόπιμη : Επίθεση DDoS
CI-A-1006	Windows 10 Pro	Software	Σκόπιμη : Επίθεση Malware
CI-A-1007	Windows 7	Software	
CI-A-1008	LAPTOP1	Workstation	Σκόπιμη : Υποκλοπή δεδομένων του διευθυντή
CI-A-1017	TABLET-PC1	Tablet	
CI-A-1010	CRM Server	Server	Φυσική : Μη τήρηση κατάλληλων συνθηκών λειτουργίας Σκόπιμη : Μη εξουσιοδοτημένη πρόσβαση στο δίκτυο της εταιρείας Σκόπιμη : Εισερχόμενο email με malware Σκόπιμη : Επίθεση cache poisoning / phishing Σκόπιμη : Αλλαγή μετρικών/στοιχείων Σκόπιμη : Επίθεση DDoS Σκόπιμη : Υποκλοπή κρίσιμων δεδομένων και παράνομη πρόσβαση σε πόρους
CI-A-1011	RADIUS/SNMP SERVER	Server	
CI-A-1018	EMAIL SERVER	Server	
CI-A-1023	DNS/DHCP SERVER	Server	
CI-A-1024	HRM SERVER	Server	
CI-A-1029	APPLICATION SERVER	Server	
CI-A-1033	DOMAIN CONTROLLER/FILE SERVER	Server	
CI-A-1012	ROUTER2	Router	Ανθρώπινη : Μη εξουσιοδοτημένη πρόσβαση Σκόπιμη : Επίθεση routing protocol Σκόπιμη : Υποκλοπή εισερχόμενης κι εξερχόμενης πληροφορίας Σκόπιμη : Επίθεση masquerade Σκόπιμη : DHCP spoofing
CI-A-1015	ROUTER3	Router	
CI-A-1022	EDGE-ROUTER	Router	
CI-A-1026	ROUTER1	Router	
CI-A-1028	ROUTER4	Router	
CI-A-1013	VOIP-PHONE1	IP Phone	Φυσική : Φθορά τηλεφωνικής γραμμής
CI-A-1016	WIRELESS-LAN-CONTROLLER1	Wireless Controller	Τυχαία : Επίθεση man-in-the-middle
CI-A-1009	PC5	Workstation	Σκόπιμη : Υποκλοπή

CI-A-1019	PC4	Workstation	δεδομένων πωλήσεων
CI-A-1020	PC6	Workstation	
CI-A-1030	PC3	Workstation	
CI-A-1021	PRINTER1	Printer	Ανθρώπινη : Υπερβολική χρήση από τους υπαλλήλους για προσωπικό όφελος Τεχνική : Υποκλοπή δεδομένων προς εκτύπωση
CI-A-1025	SW-FLOOR4.1	Switch	Σκόπιμη : MAC flooding Σκόπιμη : Επίθεση STP Σκόπιμη : Επίθεση ARP Σκόπιμη : Επίθεση VLAN hopping
CI-A-1027	SW-FLOOR4.2	Switch	
CI-A-1034	SW-FLOOR2	Switch	
CI-A-1036	SW-FLOOR1	Switch	
CI-A-1037	SW-FLOOR3	Switch	
CI-A-1031	PC1	Workstation	Σκόπιμη : Υποκλοπή λογιστικών δεδομένων Σκόπιμη : Υποκλοπή δεδομένων υπαλλήλων
CI-A-1032	PC2	Workstation	
CI-A-1035	ACCESS POINT	Access Point	Σκόπιμη : Επίθεση evil twin από υπάλληλο

3.3. Ευπάθειες που εντοπίστηκαν

INVENTORY ID	ASSET NAME	TYPE	VULNERABILITY
CI-A-1000	Industry Customer Data	Data	Τεχνική : Μη κρυπτογραφημένα
CI-A-1001	Industry Employee Data	Data	
CI-A-1002	Create New Customer	Process	Τεχνική : Ανεπαρκής έλεγχος εισαγόμενων στοιχείων πελάτη/παραγγελίας
CI-A-1003	Create New Order (Local)	Process	
CI-A-1004	Create New Order (Remotely)	Process	
CI-A-1005	Customer Support	Process	Τεχνική : Αδύναμος server
CI-A-1007	Windows 7	Software	Τεχνική : Δεν υποστηρίζεται και δεν λαμβάνει ενημερώσεις
CI-A-1006	Windows 10 Pro	Software	Τεχνική : Μη τακτικές ενημερώσεις
CI-A-1009	PC5	Workstation	
CI-A-1030	PC3	Workstation	
CI-A-1008	LAPTOP1	Workstation	Ανθρώπινη : Αδύναμος κωδικός πρόσβασης
CI-A-1010	CRM Server	Server	Τεχνική : Χαλασμένο κλιματιστικό Ανθρώπινη : Χρήση default configuration Τεχνική : Αδύναμο spam filter Τεχνική : Μη έλεγχος εισαγόμενης πληροφορίας στην cache
CI-A-1011	RADIUS/SNMP SERVER	Server	
CI-A-1018	EMAIL SERVER	Server	
CI-A-1023	DNS/DHCP SERVER	Server	
CI-A-1024	HRM SERVER	Server	
CI-A-1029	APPLICATION SERVER	Server	
CI-A-1033	DOMAIN CONTROLLER/FILE SERVER	Server	
CI-A-1012	ROUTER2	Router	Τεχνική : Παλιό firmware

CI-A-1015	ROUTER3	Router	Τεχνική : Μη τακτικές ενημερώσεις
CI-A-1022	EDGE-ROUTER	Router	
CI-A-1026	ROUTER1	Router	
CI-A-1028	ROUTER4	Router	
CI-A-1013	VOIP-PHONE1	IP Phone	Ανθρώπινη : Ακάλυπτα καλώδια
CI-A-1016	WIRELESS-LAN-CONTROLLER1	Wireless Controller	Ανθρώπινη : Λανθασμένο configuration
CI-A-1017	TABLET-PC1	Tablet	Ανθρώπινη : Αδύναμος κωδικός πρόσβασης
CI-A-1019	PC4	Workstation	Τεχνική : Χρήση παλιού λειτουργικού συστήματος
CI-A-1020	PC6	Workstation	
CI-A-1031	PC1	Workstation	
CI-A-1032	PC2	Workstation	
CI-A-1021	PRINTER1	Printer	Τεχνική : Απεριόριστη απομακρυσμένη πρόσβαση Τεχνική : Μη κρυπτογραφημένες μεταδόσεις δεδομένων
CI-A-1025	SW-FLOOR4.1	Switch	Τεχνική : Απεριόριστος αριθμός MAC ανά port Τεχνική : Υποδοχή ARP πακέτων σε μη εμπιστευόμενα port
CI-A-1027	SW-FLOOR4.2	Switch	
CI-A-1034	SW-FLOOR2	Switch	
CI-A-1036	SW-FLOOR1	Switch	
CI-A-1037	SW-FLOOR3	Switch	
CI-A-1035	ACCESS POINT	Access Point	Τεχνική : Μη χρήση VPN

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 κίνησης	Μη παράδοση	Απώλεια ακολουθίας μηνυμάτων
Domain Controller/File Server	5	7	8	10	10	10	10	10	8	9	5	9	2	6	8	4	7	7	6	6	7	7	6	5
Industry Employee Data	1	2	3	5	8	8	8	8	5	6	2	6	5	6	6	-	-	-	-	-	-	-	-	-
Edge-Router	6	6	7	7	8	7	8	8	6	8	3	6	2	7	7	4	6	6	6	6	7	8	6	5
Industry Customer Data	3	5	6	7	8	9	9	9	7	8	3	7	4	7	9	-	-	-	-	-	-	-	-	-
Create New Customer	3	3	4	4	5	5	5	5	3	2	1	4	1	2	3	-	-	-	-	-	-	-	-	-
Create New Order (Local)	3	3	4	4	5	5	6	6	3	4	2	4	1	3	4	-	-	-	-	-	-	-	-	-
Create New Order (Remote)	3	4	4	5	5	6	6	6	4	4	2	4	1	3	4	2	5	5	3	4	4	5	6	6
Customer Support	1	1	2	2	3	3	4	4	2	4	1	2	1	3	3	1	3	3	2	2	2	1	3	3

Windows 10 Pro	4	5	6	7	7	7	7	7	5	7	3	5	1	1	2	-	-	-	-	-	-	-	-	-
Windows 7	4	5	6	7	7	7	7	7	5	7	3	5	1	1	3	-	-	-	-	-	-	-	-	-
LAPTOP1	3	4	5	5	6	7	7	7	4	6	2	4	4	5	6	-	-	-	-	-	-	7	-	-
PC5	2	3	4	4	5	5	5	5	3	4	3	4	1	3	5	-	-	-	-	-	-	4	-	-
CRM Server	4	5	6	7	8	8	8	8	6	8	4	6	2	5	7	3	6	6	5	6	6	5	7	7
RADIUS/SNMP Server	5	6	6	7	8	8	9	9	7	9	5	8	2	6	7	4	7	7	6	6	7	8	8	8
ROUTER2	4	5	5	6	8	8	8	8	6	8	5	7	1	5	8	4	6	6	6	7	7	8	8	8
VOIP-PHONE1	1	2	2	3	4	4	4	4	2	3	1	3	1	1	1	1	2	2	3	3	4	4	4	3
ROUTER3	4	5	5	6	8	8	8	8	6	8	5	7	1	5	8	4	5	5	6	7	7	8	8	8
WIRELESS-LAN-CONTROLLER1	3	4	4	5	6	7	7	7	4	7	3	5	2	5	7	3	5	5	6	7	7	7	6	6
TABLET-PC1	2	2	2	3	4	5	6	6	2	3	1	3	3	5	6	-	-	-	-	-	-	5	-	-
EMAIL SERVER	4	4	5	6	7	8	9	9	4	8	5	7	2	4	6	4	7	7	6	8	8	8	9	7

PC4	2	3	4	4	5	5	5	5	3	4	3	4	1	3	5	-	-	-	-	-	-	4	-	-
PC6	2	3	4	4	5	5	5	5	3	4	3	4	1	3	5	-	-	-	-	-	-	4	-	-
PRINTER1	1	3	3	4	4	6	6	6	4	6	2	4	1	3	5	2	2	4	3	4	5	6	4	3
DNS/DCHP SERVER	7	7	8	8	9	9	9	9	7	9	6	8	3	6	9	5	6	6	6	8	9	8	7	8
HRM SERVER	4	5	5	5	6	7	8	8	6	7	3	6	4	5	6	3	4	4	5	7	5	7	5	5
SW-FLOOR4.1	5	6	7	8	9	9	9	9	6	8	6	8	3	6	8	5	7	7	4	5	7	8	7	8
ROUTER1	4	5	5	6	8	8	8	8	6	8	5	7	1	5	8	4	7	7	6	7	7	8	8	8
SW-FLOOR4.2	5	6	7	8	9	9	9	9	6	8	6	8	3	6	8	5	6	6	4	5	7	8	7	8
ROUTER4	5	6	6	7	9	9	9	9	7	9	6	8	2	6	9	5	7	7	7	8	8	9	9	9
APPLICATION SERVER	6	7	7	8	9	10	10	10	7	9	6	8	3	7	9	6	7	7	6	8	8	8	6	8
PC3	2	3	4	4	5	5	5	5	3	4	3	4	1	3	5	-	-	-	-	-	-	4	-	-
PC1	2	3	4	4	5	6	7	7	4	5	3	5	3	5	7	-	-	-	-	-	-	6	-	-

PC2	2	3	4	4	5	6	7	7	4	5	3	5	3	5	7	-	-	-	-	-	-	6	-	-
SW-FLOOR2	4	5	6	7	8	8	8	8	5	7	5	7	2	5	7	4	6	6	3	4	6	7	6	7
ACCESS POINT	2	3	3	4	5	6	6	7	3	6	2	4	4	5	7	3	4	4	5	7	6	6	5	5
SW-FLOOR1	4	5	6	7	8	8	8	8	5	7	5	7	2	5	7	4	5	5	3	4	6	7	6	7
SW-FLOOR3	4	5	6	7	8	8	8	8	5	7	5	7	2	5	7	4	5	5	3	4	6	7	6	7

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 της BitByBit.

4.1. Προσωπικό – Προστασία Διαδικασιών Προσωπικού

- Ύπαρξη επαλήθευσης των στοιχείων που εισάγονται για τη δημιουργία νέου πελάτη ή νέας παραγγελίας (CI-A-1002, CI-A-1003, CI-A-1004)
- Ύπαρξη ορίου στο πλήθος εισερχόμενων πακέτων από μια διεύθυνση για αποφυγή DDoS (CI-A-1005)

4.2. Ταυτοποίηση και αυθεντικοποίηση

- Τήρηση κανόνων ισχυρών κωδικών (CI-A-1008, CI-A-1017)

4.3. Έλεγχος προσπέλασης και χρήσης πόρων

- Χρήση κατάλληλου configuration που ενισχύει την προστασία της βάσης δεδομένων (CI-A-1011)

4.4. Διαχείριση εμπιστευτικών δεδομένων

- Κρυπτογράφηση της βάσης δεδομένων (CI-A-1000, CI-A-1001)

4.5. Προστασία από τη χρήση υπηρεσιών από τρίτους

- Τήρηση κανόνων ισχυρών κωδικών (CI-A-1009, CI-A-1019, CI-A-1020, CI-A-1030, CI-A-1031, CI-A-1032)
- Χρήση ελέγχου ταυτότητας δύο παραγόντων στους υπολογιστές (CI-A-1009, CI-A-1019, CI-A-1020, CI-A-1030, CI-A-1031, CI-A-1032)

4.6. Προστασία λογισμικού

- Τακτικές ενημερώσεις στα Windows 10 και στους υπολογιστές που τα χρησιμοποιούν (CI-A-1006, CI-A-1008, CI-A-1009, CI-A-1030)

- Χρήση πρόσφατου λογισμικού (CI-A-1007, CI-A-1019, CI-A-1020, CI-A-1031, CI-A-1032)

4.7. Διαχείριση ασφάλειας δικτύου

- Χρήση Firewall μεταξύ του Edge-Router και του ISP (CI-A-1012, CI-A-1015, CI-A-1022, CI-A-1026, CI-A-1028)
- Διαχείριση χρηστών που έχουν πρόσβαση στον server και τον ρόλο τους (CI-A-1011, CI-A-1024, CI-A-1033)
- Χρήση ξεχωριστού κωδικού για την πρόσβαση στον server (CI-A-1011, CI-A-1024, CI-A-1033)
- Χρήση κατάλληλων ρυθμίσεων(configuration) (CI-A-1016, CI-A-1024, CI-A-1029)
- Χρήση της πιο πρόσφατης έκδοσης του DNS Server (CI-A-1023)
- Εκτέλεση μόνο των απαραίτητων υπηρεσιών που επιτρέπονται στον DNS Server (CI-A-1023)
- Χρήση ορίου στο πλήθος MAC διευθύνσεων ανά port (CI-A-1025, CI-A-1027, CI-A-1034, CI-A-1036, , CI-A-1037)
- Λήψη ARP πακέτων μόνο σε εμπιστευόμενα ports (CI-A-1025, CI-A-1027, CI-A-1034, CI-A-1036, , CI-A-1037)
- Ύπαρξη ορίου στο πλήθος εισερχόμενων πακέτων από μια διεύθυνση για αποφυγή DDoS (CI-A-1029)
- Χρήση VPN (CI-A-1035)

4.8. Προστασία από ιομορφικό λογισμικό

- Χρήση ισχυρών αντικών προγραμμάτων (CI-A-1008, CI-A-1009, CI-A-1017, CI-A-1019, CI-A-1020, CI-A-1030, CI-A-1031, CI-A-1032)
- Τακτική ενημέρωση του firmware των router (CI-A-1012, CI-A-1015, CI-A-1022, CI-A-1026, CI-A-1028)
- Τακτικές αλλαγές κωδικών των router (CI-A-1012, CI-A-1015, CI-A-1022, CI-A-1026, CI-A-1028)

4.9. Ασφαλής χρήση διαδικτυακών υπηρεσιών

- Χρήση ισχυρού spam filter (CI-A-1018)
- Αποκλεισμός επικίνδυνων ιστοσελίδων (CI-A-1012, CI-A-1015, CI-A-1022, CI-A-1026, CI-A-1028)
- Ενημέρωση των web browser (CI-A-1008, CI-A-1009, CI-A-1019, CI-A-1020, CI-A-1030, CI-A-1031, CI-A-1032)

4.10. Ασφάλεια εξοπλισμού

- Ελεγχόμενη πρόσβαση στα δωμάτια του χώρου, π.χ. χρήση κάρτα υπαλλήλου (CI-A-1008, CI-A-1009, CI-A-1013, CI-A-1019, CI-A-1020, CI-A-1021, CI-A-1030, CI-A-1031, CI-A-1032)
- Χρήση θερμομέτρου για να παρακολουθεί τη θερμοκρασία δωματίου και να προειδοποιεί όταν αυτή ξεπεράσει τα όρια (CI-A-1010)
- Κατάλληλη διαχείριση καλωδίων τηλεφώνου (CI-A-1013)
- Μηνιαίος έλεγχος καλωδίων τηλεφώνου (CI-A-1013)

4.11. Φυσική ασφάλεια κτιριακής εγκατάστασης

- Φύλαξη του κτιρίου
- Κάμερες
- Πυροσβεστήρες
- Αισθητήρες καπνού

5. ΣΥΝΟΨΗ ΠΙΟ ΚΡΙΣΙΜΩΝ ΑΠΟΤΕΛΕΣΜΑΤΩΝ

Τα πιο κρίσιμα αγαθά που εντοπίστηκαν κατά την ανάλυση είναι τα εξής:

1. EMAIL SERVER (CI-A-1018)
   Ο Email Server έχει το υψηλότερο RPN με τιμή 576 μονάδες, λόγω της επικοινωνίας του με το διαδίκτυο και της ευκολίας να γίνει αντικείμενο εκμετάλλευσης η ευπάθειά του.
2. RADIUS/SNMP SERVER (CI-A-1011)
   Ο Radius/SNMT Server έχει RPN ίσο με 504 μονάδες, λόγω της βαρύτητας του καθώς διαχειρίζεται ολόκληρο το δίκτυο της εταιρείας και τις συσκευές του και καθώς προσφέρει τις λειτουργίες της ταυτοποίησης και αυθεντικοποίησης.
3. DNS/DHCP SERVER (CI-A-1023), SW-FLOOR4.1 (CI-A-1025), SW-FLOOR4.2 (CI-A-1027), PC1 (CI-A-1031), PC2 (CI-A-1032)
   Τα συγκεκριμένα αγαθά έχουν RPN ίσο με 441 μονάδες.
   Ο DNS Server εκτελεί τις κρίσιμες λειτουργίες της ονοματοδοσίας δικτύων και της δέσμευσης διευθύνσεων του δικτύου, επιπλέον είναι ευάλωτος λόγω της ανεξέλεγκτης εισαγωγής δεδομένων στην cache.
   Τα SW-FLOOR4.1 και SW-FLOOR4.2 γεφυρώνουν την επικοινωνία των server με το υπόλοιπο δίκτυο και για αυτό τον λόγο αποτελούν σημαντικότατο αγαθό για τη σωστή λειτουργία της εταιρείας.
   Τα PC1 και PC2 βρίσκονται τόσο ψηλά λόγω της διαχείρισης των λογιστικών δεδομένων της εταιρείας και των προσωπικών δεδομένων των υπαλλήλων της αλλά και του παλιού λειτουργικού τους συστήματος (Windows XP) που τα καθιστά ευάλωτα σε επιθέσεις αφού δεν λαμβάνουν ενημερώσεις και τεχνική υποστήριξη.