ΑΣΦΑΛΕΙΑ ΠΛΗΡΟΦΟΡΙΑΚΩΝ ΣΥΣΤΗΜΑΤΩΝ ΚΑΙ ΚΡΙΣΙΜΩΝ ΥΠΟΔΟΜΩΝ

ΣΧΕΔΙΟ ΑΣΦΑΛΕΙΑΣ

ΣΥΓΓΡΑΦΕΙΣ:
Κυριαζής Ιωάννης 321/2018107
Παπαδόπουλος Παναγιώτης 321/2018161

ΕΡΓΑΣΙΑ ΕΑΡΙΝΟΥ ΕΞΑΜΗΝΟΥ 2020-21

Περιεχόμενα

1. ΕΙΣΑΓΩΓΗ

Σε αυτή την ενότητα θα γίνει μία μικρή εισαγωγή σχετικά με το προφίλ της παρούσας αναφοράς καθώς και τον σκοπό της.

1.1. Περιγραφή Εργασίας

Η παρούσα αναφορά αποτελεί ένα ολοκληρωμένο ΣΧΕΔΙΟ ΑΣΦΑΛΕΙΑΣ στα πλαίσια του πανεπιστημιακού μαθήματος «Ασφάλεια Πληροφοριακών και Επικοινωνιακών Συστημάτων». Στο παρόν σχέδιο θα παρουσιαστούν τόσο η μεθοδολογία που ακολούθησε η ομάδα, όσο και η αποτίμηση του πληροφοριακού συστήματος της εταιρείας καθώς και τα προτεινόμενα μέτρα ασφαλείας που μπορούν να εφαρμοστούν.

1.2. Δομή παραδοτέου

Στην 1η ενότητα δίνεται μία σύντομη εισαγωγή της παρούσας αναφοράς. Στην 2η ενότητα παρουσιάζεται σε βήματα και μερική ανάλυση η μεθοδολογία που ακολούθησε η ομάδα. Στην 3η ενότητα θα αποτιμηθεί όλο το πληροφοριακό σύστημα και οι βιομηχανικές εγκαταστάσεις της εταιρείας. Στην 4η ενότητα θα προταθούν ορισμένα μέτρα ασφαλείας που μπορούν να εφαρμοστούν. Τέλος, στην 5η ενότητα θα συνοψιστούν όλα τα κρίσιμα αποτελέσματα που προέκυψαν από τις προηγούμενες ενότητες.

2. ΜΕΘΟΔΟΛΟΓΙΑ ΜΕΛΕΤΗΣ ΑΣΦΑΛΕΙΑΣ

Για τη Διαχείριση Επικινδυνότητας του/της icsd18107_Lab02 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 του/της ΕΤΑΙΡΕΙΑ1, τα οποία με το πέρας της μελέτης θα επικαιροποιηθούν, αναβαθμιστούν ή σε κάποιες περιπτώσεις αντικατασταθούν.

2.1.1. Υλικός εξοπλισμός (hardware)

ID	Όνομα Εξοπλισμού	Μοντέλο	Τύπος	Κατ/στής
CI-A-1008	LAPTOP1	ThinkPad X13 Yoga (13") Intel	Workstation	Lenovo
CI-A-1009	PC5	ThinkCentre M90t	Workstation	Lenovo
CI-A-1010	CRM SERVER	HP ProLiant ML150	Server	HP
CI-A-1011	RADIUS/SNMP SERVER	HP ProLiant ML250	Server	HP
CI-A-1013	VOIP-PHONE1	IP Phone 8811	IP Phone	Cisco
CI-A-1014	FIREWALL	FortiGate/FortiWiFi 30E	Firewall	Fortigate
CI-A-1017	TABLET-PC1	Galaxy Tab A	Tablet	Samsung
CI-A-1018	EMAIL SERVER	HP ProLiant ML150	Server	HP
CI-A-1019	PC4	ThinkCentre M90t	Workstation	Lenovo
CI-A-1020	PC6	ThinkCentre M90t	Workstation	Lenovo
CI-A-1021	PRINTER1	EcoTank L1800 ITS	Printer	Epson
CI-A-1023	DNS/DHCP SERVER	HP ProLiant ML450	Server	HP
CI-A-1024	HRM SERVER	HP ProLiant ML450	Server	HP
CI-A-1029	WEB APPLICATION SERVER	HP ProLiant ML251	Server	HP
CI-A-1030	PC3	ThinkCentre M90t	Workstation	Lenovo
CI-A-1031	PC1	ThinkCentre M90t	Workstation	Lenovo
CI-A-1032	PC2	ThinkCentre M90t	Workstation	Lenovo
CI-A-1033	DOMAIN CONTROLLER/FILE SERVER	HP ProLiant ML350	Server	HP

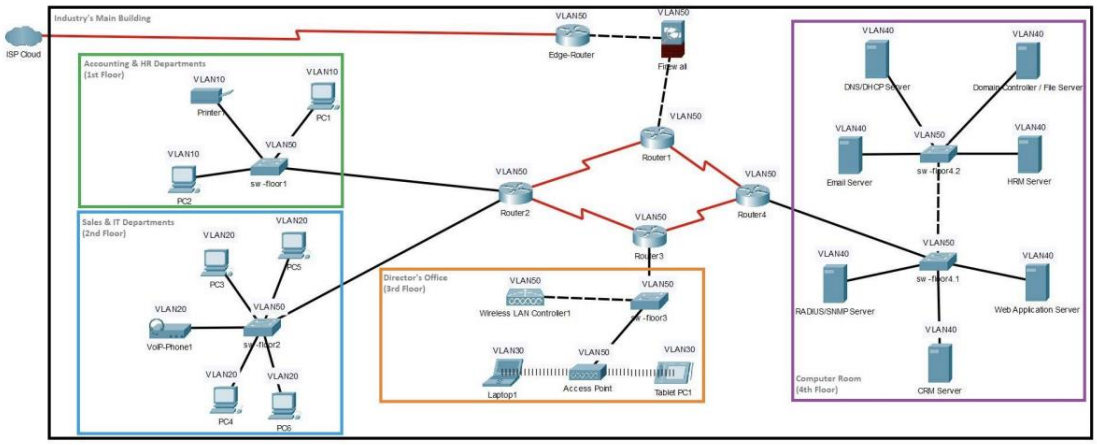
Στον παραπάνω πίνακα, αναγράφονται όλο το υλικό (hardware) που διαθέτει η εταιρεία εκτός από τις συσκευές που βοηθούν στην δημιουργία του δικτύου (routers, switches, access points κ.α.). Αναγράφονται σε πίνακα στην ενότητα 2.1.3.

2.1.2. Λογισμικό και εφαρμογές

ID	Όνομα Λογισμικού/Εφαρμογής	Τύπος	Κατασκευαστής
CI-A-1006	Windows 10 Pro	Software	Microsoft
CI-A-1007	Windows 7	Software	Microsoft
ES-00	Windows Server 2008	Software	Microsoft
ES-01	Ubuntu 16.04.7 LTS	Software	Canonical Ltd.
ES-02	Cisco proprietary software	Software	Cisco
ES-03	FortiGate proprietary software	Software	Fortigate
ES-04	Android 9 Pie (API 28)	Software	Google
ES-05	Windows XP	Software	Microsoft
ES-06	Ubuntu 12.04.5 LTS	Software	Canonical Ltd.
ES-07	Epson proprietary software	Software	Epson

Στον παραπάνω πίνακα ο οποίος παρουσιάζει το λογισμικό και της εφαρμογές που χρησιμοποιεί η εταιρεία, προσθέσαμε το λογισμικό των επιμέρους συσκευών. Σε κάθε ένα από αυτά αναθέσαμε ένα τυχαίο ID για δική μας ευκολία (ES-0X = Epipleon Software).

2.1.3. Δίκτυο



ID	Όνομα Εξοπλισμού	Μοντέλο	Τύπος	Κατασκευαστής
CI-A-1012	ROUTER2	RV160	Router	Cisco
CI-A-1015	ROUTER3	RV160	Router	Cisco
CI-A-1016	WIRELESS-LAN-CONTROLLER1	Catalyst 9800-L	Wireless Controller	Cisco
CI-A-1022	EDGE-ROUTER	ASR 1002-HX	Router	Cisco
CI-A-1025	SW-FLOOR4.1	CBS250-8FP-E-2G	Switch	Cisco
CI-A-1026	ROUTER1	RV160	Router	Cisco
CI-A-1027	SW-FLOOR4.2	CBS250-8FP-E-2G	Switch	Cisco
CI-A-1028	ROUTER4	RV160	Router	Cisco
CI-A-1034	SW-FLOOR2	CBS250-8FP-E-2G	Switch	Cisco
CI-A-1035	ACCESS POINT	240AC	Access Point	Cisco
CI-A-1036	SW-FLOOR1	CBS250-8FP-E-2G	Switch	Cisco
CI-A-1037	SW-FLOOR3	CBS250-8FP-E-2G	Switch	Cisco

Στο παραπάνω στιγμιότυπο απεικονίζεται το δίκτυο της εταιρείας καθώς και ένας πίνακας με όλες τις δικτυακές συσκευές. Όπως παρατηρούμε, η συγκεκριμένη εταιρεία διαθέτει 4 ορόφους όπου κάθε ένας από αυτούς διαθέτει αγαθά για ξεχωριστές διεργασίες.

2.1.4. Δεδομένα

ID	Όνομα Δεδομένου	Τύπος
CI-A-1000	Industry Customer Data	Data
CI-A-1001	Industry Employee Data	Data

2.1.5. Διαδικασίες

ID	Όνομα Διαδικασίας	Τύπος
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

3. ΑΠΟΤΙΜΗΣΗ ΠΣ ΚΑΙ ΕΓΚΑΤΑΣΤΑΣΕΩΝ ΒΙΟΜΗΧΑΝΙΑΣ

Σε αυτή την ενότητα θα καταγραφεί η αποτίμηση του πληροφοριακού συστήματος της εταιρείας. Θα παρουσιαστούν τα ευπαθή αγαθά ταξινομημένα κατά φθίνουσα σειρά ξεκινώντας από το πιο σημαντικό, οι απειλές που εντοπίστηκαν, οι ευπάθειες που βρέθηκαν καθώς και τα αποτελέσματα αυτής της αποτίμησης.

3.1. Αγαθά που εντοπίστηκαν

No.	ID	Όνομα	Μοντέλο	Τύπος	Κατ/στής
1	CI-A-1033	DOMAIN CONTROLLER/FILE SERVER	HP ProLiant ML350	Server	HP
2	CI-A-1010	CRM SERVER	HP ProLiant ML150	Server	HP
3	CI-A-1011	RADIUS/SNMP SERVER	HP ProLiant ML250	Server	HP
4	CI-A-1007	Windows 7	-	Software	Microsoft
5	CI-A-1001	Industry Employee Data	-	Data	-
6	CI-A-1000	Industry Customer Data	-	Data	-
7	CI-A-1029	WEB APPLICATION SERVER	HP ProLiant ML251	Server	HP
8	CI-A-1022	EDGE-ROUTER	ASR 1002-HX	Router	Cisco
9	CI-A-1026	ROUTER1	RV160	Router	Cisco
10	CI-A-1028	ROUTER4	RV160	Router	Cisco
11	CI-A-1012	ROUTER2	RV160	Router	Cisco
12	CI-A-1015	ROUTER3	RV160	Router	Cisco
13	CI-A-1006	Windows 10 Pro	-	Software	Microsoft
14	CI-A-1018	EMAIL SERVER	HP ProLiant ML150	Server	HP
15	CI-A-1023	DNS/DHCP SERVER	HP ProLiant ML450	Server	HP
16	CI-A-1024	HRM SERVER	HP ProLiant ML450	Server	HP
17	CI-A-1025	SW-FLOOR4.1	CBS250-8FP-E-2G	Switch	Cisco
18	CI-A-1027	SW-FLOOR4.2	CBS250-8FP-E-2G	Switch	Cisco
19	CI-A-1036	SW-FLOOR1	CBS250-8FP-E-2G	Switch	Cisco
20	CI-A-1037	SW-FLOOR3	CBS250-8FP-E-2G	Switch	Cisco
21	CI-A-1034	SW-FLOOR2	CBS250-8FP-E-2G	Switch	Cisco
22	CI-A-1019	PC4	ThinkCentre M90t	Workstation	Lenovo
23	CI-A-1020	PC6	ThinkCentre M90t	Workstation	Lenovo
24	CI-A-1008	LAPTOP1	ThinkPad X13 Yoga (13") Intel	Workstation	Lenovo
25	CI-A-1017	TABLET-PC1	Galaxy Tab A	Tablet	Samsung
26	CI-A-1031	PC1	ThinkCentre M90t	Workstation	Lenovo
27	CI-A-1032	PC2	ThinkCentre M90t	Workstation	Lenovo
28	CI-A-1013	VOIP-PHONE1	IP Phone 8811	IP Phone	Cisco
29	CI-A-1038	VOIP-PHONE2	IP Phone 8811	IP Phone	Cisco
30	CI-A-1039	VOIP-PHONE3	IP Phone 8811	IP Phone	Cisco
31	CI-A-1030	PC3	ThinkCentre M90t	Workstation	Lenovo
32	CI-A-1009	PC5	ThinkCentre M90t	Workstation	Lenovo
33	CI-A-1005	Customer Support	-	Process	-
34	CI-A-1004	Create New Order (Remotely)	-	Process	-
35	CI-A-1003	Create New Order (Local)	-	Process	-
36	CI-A-1021	PRINTER1	EcoTank L1800 ITS	Printer	Epson
37	CI-A-1040	PRINTER2	EcoTank L1800 ITS	Printer	Epson
38	CI-A-1016	WIRELESS-LAN-CONTROLLER1	Catalyst 9800-L	Wireless Controller	Cisco
39	CI-A-1035	ACCESS POINT	240AC	Access Point	Cisco

Τα αγαθά που είναι σημειωμένα με ανοιχτό κόκκινο χρώμα αποτελούν τα 3 δικά μας αγαθά. Προσθέσαμε 1 IP Phone με όνομα «VOIP-PHONE2» και ID «CI-A-1038» στον 3ο όροφο που βρίσκεται το γραφείο του Διευθυντή της εταιρείας διότι κι εκείνος πρέπει να επικοινωνεί με τους υπαλλήλους του ανά πάσα ώρα και στιγμή. Επίσης προσθέσαμε 1 IP Phone με όνομα «VOIP-PHONE3» και ID «CI-A-1039» στον 1ο όροφο που βρίσκεται το τμήμα λογιστικής και εργατικού δυναμικού προκειμένου να επικοινωνούν ανά πάσα ώρα και στιγμή με τα υπόλοιπα τμήματα. Τέλος προσθέσαμε 1 εκτυπωτή με όνομα «PRINTER2» και ID «CI-A-1040» στον 3ο όροφο που βρίσκεται το γραφείο του Διευθυντή της εταιρείας διότι κι εκείνος πρέπει να λαμβάνει έντυπα από οικονομικές καταστάσεις ή άλλες αναφορές που παράγει η εταιρεία.

3.2. Απειλές που εντοπίστηκαν

No.	ID	Όνομα	Απειλές
1	CI-A-1033	DOMAIN CONTROLLER/FILE SERVER	Ένας επιτιθέμενος μπορεί να παρακάμψει την προστασία NTLMv2 εάν ένας πελάτης στέλνει επίσης απαντήσεις LMv2.
2	CI-A-1010	CRM SERVER	Μπορεί κάποιος να αποκτήσει πρόσβαση στον σέρβερ.
3	CI-A-1011	RADIUS/SNMP SERVER	Μπορεί κάποιος να αποκτήσει προνόμια.
4	CI-A-1007	Windows 7	Μπορεί να χρησιμοποιηθεί για διάδοση κακόβουλου λογισμικού.
5	CI-A-1001	Industry Employee Data	Μπορεί κάποιος να λάβει δεδομένα υπαλλήλων.
6	CI-A-1000	Industry Customer Data	Μπορεί κάποιος να γίνει ανεξέλεγκτος διαχειριστής της βάσης.
7	CI-A-1029	WEB APPLICATION SERVER	Μπορεί ένας υπάλληλος ή πελάτης να ανοίξει κακόβουλο αρχείο.
8	CI-A-1022	EDGE-ROUTER	Πρόσβαση σε δίκτυο μη εξουσιοδοτημένου χρήστη.
9	CI-A-1026	ROUTER1	Μπορεί ο εισβολέας να διαβάσει και να τροποποιήσει δεδομένα που θα έπρεπε να ήταν κρυπτογραφημένα.
10	CI-A-1028	ROUTER4	Μπορεί κάποιος να λάβει ευαίσθητες πληροφορίες από την μνήμη της συσκευής ενός negotiation request του Security Association (SA).
11	CI-A-1012	ROUTER2	Διακοπή επεξεργασίας αιτημάτων HTTPS. Ο εισβολέας στέλνει επεξεργασμένα πακέτα TLS στον διακομιστή ιστού IOx σε μια συσκευή που επηρεάζεται.
12	CI-A-1015	ROUTER3	Επιτρέπει στον εισβολέα να εκτελέσει αυθαίρετο κώδικα στην επηρεαζόμενη συσκευή με αυξημένα δικαιώματα.
13	CI-A-1006	Windows 10 Pro	Επιτρέπει απομακρυσμένη εκτέλεση κώδικα εάν ένας χρήστης προβάλλει μια ειδικά σχεδιασμένη ιστοσελίδα χρησιμοποιώντας το Microsoft Edge.
14	CI-A-1018	EMAIL SERVER	Ένας "εισβολέας" μπορεί να προκαλέσει τεράστια κυκλοφορία δεδομένων προς τον σέρβερ.
15	CI-A-1023	DNS/DHCP SERVER	Το φίλτρο lwp στο LibreOffice πριν από το 5.0.4 επιτρέπει στους απομακρυσμένους εισβολείς να προκαλέσουν DoS ή άλλο αντίκτυπο.
16	CI-A-1024	HRM SERVER	Υπάρχει αύξηση της ευπάθειας δικαιωμάτων όταν τα Windows χειρίζονται εσφαλμένα κλήσεις στον LUAFV driver (luafv.sys).
17	CI-A-1025	SW-FLOOR4.1	Ένας "εισβολέας" θα μπορούσε να στείλει ένα πακέτο με λανθασμένη μορφή σε μια συσκευή που επηρεάζεται.
18	CI-A-1027	SW-FLOOR4.2	Ένας εισβολέας θα μπορούσε να στείλει κακόβουλα πακέτα σε μια συσκευή που επηρεάζεται. Επίσης μπορεί να εκτελέσει αυθαίρετο κώδικα.
19	CI-A-1036	SW-FLOOR1	Κάποιος μπορεί να στείλει επεξεργασμένα κρυπτογραφήματα σε μια συσκευή διαμορφωμένη με IKEv1 που χρησιμοποιεί RSA-encrypted πληροφορίες.
20	CI-A-1037	SW-FLOOR3	Μπορεί κάποιος να παρέχει ένα κατασκευασμένο πιστοποιητικό σε μια συσκευή που επηρεάζεται.
21	CI-A-1034	SW-FLOOR2	Μπορεί κάποιος με διαπιστευτήρια διαχειριστή με έλεγχο ταυτότητας στη συσκευή και ενεργοποιώντας την υπό όρους, ρητή καταγραφή εντοπισμού σφαλμάτων για IPsec και προβάλλοντας το αρχείο καταγραφής.
22	CI-A-1019	PC4	Ο εισβολέας μπορεί να εκτελέσει απομακρυσμένο κώδικα όταν ο Windows Jet Database Engine χειρίζεται εσφαλμένα αντικείμενα στη μνήμη.
23	CI-A-1020	PC6	Υπάρχει ευπάθεια πλαστογράφησης όταν το Transport Layer Security (TLS) αποκτά πρόσβαση σε μη εκτεταμένες Master Secret (EMS) sessions.
24	CI-A-1008	LAPTOP1	Κίνδυνος απώλειας δεδομένων.
25	CI-A-1017	TABLET-PC1	Απομακρυσμένη εκτέλεση κώδικα χωρίς να απαιτούνται πρόσθετα δικαιώματα εκτέλεσης.
26	CI-A-1031	PC1	Τα Windows OLE επιτρέπουν σε έναν εισβολέα να εκτελεί κώδικα όταν ένα θύμα ανοίγει ένα ειδικά δημιουργημένο αρχείο ή πρόγραμμα.
27	CI-A-1032	PC2	Επιτρέπει στους τοπικούς χρήστες να γράφουν δεδομένα σε αυθαίρετες θέσεις μνήμης και, κατά συνέπεια, να αποκτήσουν προνόμια.

28	CI-A-1013	VOIP-PHONE1	Ο "εισβολέας" αναλαμβάνει ακόμη και τμήματα του δικτύου VoIP και πραγματοποιεί ακριβά κλήσεις.
29	CI-A-1038	VOIP-PHONE2	Ο εισβολέας για να αποκαλύψει αδυναμίες ασφάλειας στην απάτη τηλεφωνικού κέντρου χρησιμοποιεί την πλαστογράφηση.
30	CI-A-1039	VOIP-PHONE3	Βοηθά τον εισβολέα να συλλέξει πληροφορίες όπως την προέλευση της κλήσης και άλλα δεδομένα σχετικά με την εταιρεία.
31	CI-A-1030	PC3	Ο εισβολέας μπορεί να ανακτήσει πληροφορίες όταν ο πυρήνας των Windows χειρίζεται ακατάλληλα αντικείμενα στη μνήμη.
32	CI-A-1009	PC5	Υπάρχει μια αύξηση της ευπάθειας των δικαιωμάτων όταν ο Windows Error Reporting Manager χειρίζεται εσφαλμένα μια διακοπή της διαδικασίας.
33	CI-A-1005	Customer Support	Ένας δράστης θα μπορούσε να τηλεφωνίσει στο κέντρο εξυπηρέτησης πελατών προωθώντας την γραμμή σε μία άλλη υψηλής χρέωσης.
34	CI-A-1004	Create New Order (Remotely)	Ένας πελάτης πραγματοποιεί μια παραγγελία χωρίς να έχει ταυτοποιηθεί.
35	CI-A-1003	Create New Order (Local)	Ένας πελάτης που θέλει να κάνει την παραγγελία με φυσική παρουσία στην εταιρεία, ίσως επιθυμεί να επιβλέψει την δουλειά των υπαλλήλων ή να τους αποσπάσει πληροφορίες.
36	CI-A-1021	PRINTER1	Επιτρέπει στους τοπικούς χρήστες να αποκτήσουν προνόμια μέσω ενός Trojan horse file.
37	CI-A-1040	PRINTER2	Ένας εισβολέας μπορεί να έχει πρόσβαση στο δίκτυο της εταιρείας και να λάβει κρίσιμα δεδομένα.
38	CI-A-1016	WIRELESS-LAN-CONTROLLER1	Θέμα ευπάθειας αποκάλυψης πληροφοριών.
39	CI-A-1035	ACCESS POINT	Επιτρέπει σε έναν επικυρωμένο, τοπικό εισβολέα να έχει πρόσβαση σε ευαίσθητες πληροφορίες συστήματος σε μια επηρεαζόμενη συσκευή.

3.3. Ευπάθειες που εντοπίστηκαν

No.	ID	Όνομα	Ευπάθειες
1	CI-A-1033	DOMAIN CONTROLLER/FILE SERVER	Windows NTLM Security Feature Bypass.
2	CI-A-1010	CRM SERVER	Υπερχείλιση buffer της υπηρεσίας Windows Telnet.
3	CI-A-1011	RADIUS/SNMP SERVER	Υπερχείλιση και ανάθεση δικαιωμάτων (Ubuntu Kernel Bug).
4	CI-A-1007	Windows 7	Πεπαλαιωμένο λειτουργικό σύστημα που δεν υποστηρίζεται από επιπρόσθετες ενημερώσεις.
5	CI-A-1001	Industry Employee Data	Μη κρυπτογραφημένη βάση δεδομένων.
6	CI-A-1000	Industry Customer Data	Πληθώρα δικαιωμάτων σε χρήστες και ομάδες.
7	CI-A-1029	WEB APPLICATION SERVER	Το libmspack 0.9.1alpha επηρεάζεται από Buffer Overflow.
8	CI-A-1022	EDGE-ROUTER	Δεν υπάρχει πιστοποίηση του αποστολέα ενός πακέτου.
9	CI-A-1026	ROUTER1	Ευπάθεια στη δυνατότητα πελάτη HTTP του λογισμικού Cisco IOS και IOS XE.
10	CI-A-1028	ROUTER4	Υλοποίηση του διακομιστή IKEv1 στο Cisco IOS και PIX.
11	CI-A-1012	ROUTER2	Μια ευπάθεια στο περιβάλλον εφαρμογών IOx πολλαπλών πλατφορμών Cisco.
12	CI-A-1015	ROUTER3	Ευπάθεια στη λειτουργικότητα FTP layer layer gateway (ALG) που χρησιμοποιείται από το Network Address Translation (NAT), NAT IPv6 to IPv4 (NAT64) και το Zone-Based Policy Firewall (ZBFW) στο λογισμικό Cisco IOS XE.
13	CI-A-1006	Windows 10 Pro	Microsoft Edge Vulnerability.
14	CI-A-1018	EMAIL SERVER	Denial of Service.
15	CI-A-1023	DNS/DHCP SERVER	Denial of Service, Υπερχείλιση και Διαφθορά μνήμης.
16	CI-A-1024	HRM SERVER	Windows Elevation of Privilege.
17	CI-A-1025	SW-FLOOR4.1	Ευπάθεια στον κώδικα RADIUS Change of Authorization (CoA) του Cisco TrustSec.
18	CI-A-1027	SW-FLOOR4.2	Ευπάθεια στο υποσύστημα ποιότητας υπηρεσίας (QoS) του λογισμικού Cisco IOS και του λογισμικού Cisco IOS XE. Η ευπάθεια οφείλεται σε εσφαλμένο έλεγχο ορίων συγκεκριμένων τιμών σε πακέτα που προορίζονται για τη θύρα UDP 18999 μιας επηρεαζόμενης συσκευής.
19	CI-A-1036	SW-FLOOR1	Ευπάθεια κατά την εφαρμογή των κρυπτογραφημένων RSA στο λογισμικό Cisco IOS και στο λογισμικό Cisco IOS XE.
20	CI-A-1037	SW-FLOOR3	Μια ευπάθεια στην εφαρμογή Cisco Network Plug and Play των Cisco IOS 12.4 έως 15.6 και Cisco IOS XE 3.3 έως 16.4. Η ευπάθεια οφείλεται σε ανεπαρκή επικύρωση πιστοποιητικού από το επηρεαζόμενο λογισμικό.
21	CI-A-1034	SW-FLOOR2	Μια ευπάθεια στην υπό όρους, ρητή καταγραφή εντοπισμού σφαλμάτων για τη δυνατότητα IPsec του λογισμικού Cisco IOS XE. Η ευπάθεια οφείλεται στη λανθασμένη εφαρμογή της καταγραφής εντοπισμού σφαλμάτων υπό όρους IPsec.
22	CI-A-1019	PC4	Jet Database Engine Remote Code Execution Vulnerability.
23	CI-A-1020	PC6	Microsoft Windows Transport Layer Security Spoofing Vulnerability.

24	CI-A-1008	LAPTOP1	Μη πιστοποιημένο και αξιόπιστο Antivirus.
25	CI-A-1017	TABLET-PC1	IHEVCD_PARSE_HEADERS.C IHEVCD_PARSE_BUFFERING_PERIOD_SEI OUT-OF-BOUNDS WRITE.
26	CI-A-1031	PC1	Windows olecnv32.dll Remote Code Execution Vulnerability.
27	CI-A-1032	PC2	Το Microsoft Windows XP SP3 δεν επικυρώνει διευθύνσεις σε συγκεκριμένες ρουτίνες χειριστή IRP.
28	CI-A-1013	VOIP-PHONE1	Κλοπή υπηρεσιών και ταυτότητας μέσω μη κρυπτογραφημένων πληροφοριών.
29	CI-A-1038	VOIP-PHONE2	Vishing (VoIP-based phishing).
30	CI-A-1039	VOIP-PHONE3	Voice over Misconfigured Internet Telephones, ή VOMIT.
31	CI-A-1030	PC3	Windows Kernel Information Disclosure Vulnerability.
32	CI-A-1009	PC5	Windows Error Reporting Manager Elevation of Privilege Vulnerability.
33	CI-A-1005	Customer Support	Τηλεφωνική απάτη.
34	CI-A-1004	Create New Order (Remotely)	Πραγματοποίηση παραγγελίας από μη εγκεκριμένο πελάτη.
35	CI-A-1003	Create New Order (Local)	Διαθεσιμότητα σημαντικών δεδομένων σε έναν απλό υπολογιστή.
36	CI-A-1021	PRINTER1	Το EPSON Network Utility 4.10 χρησιμοποιεί αδύναμα δικαιώματα.
37	CI-A-1040	PRINTER2	Απεριόριστη απομακρυσμένη πρόσβαση.
38	CI-A-1016	WIRELESS-LAN-CONTROLLER1	Ευπάθεια στη δυνατότητα Αυτόνομης Δικτύωσης του Λογισμικού Cisco IOS και του Λογισμικού Cisco IOS XE.
39	CI-A-1035	ACCESS POINT	Ευπάθεια στη δυνατότητα ασφαλούς αποθήκευσης (Secure Storage) του λογισμικού Cisco IOS και IOS XE.

3.4. Αποτελέσματα αποτίμησης

Το αγαθό "DOMAIN CONTROLLER/FILE SERVER" αποτελεί κρίσιμη υποδομή για την εταιρεία διότι αυθεντικοποιεί τους χρήστες και είναι η κύρια αποθήκη δεδομένων της βιομηχανικής μονάδας. Η ευπάθεια που περιγράφεται, δεν τρέφει κίνδυνο όσον αφορά την διαθεσιμότητα του πόρου όμως είναι δυνατή η τροποποίηση ορισμένων αρχείων συστήματος ή πληροφοριών.

Το αγαθό " CRM SERVER" αποτελεί κρίσιμη υποδομή για την εταιρεία διότι αυτοματοποιεί όλες τις βιομηχανικές διεργασίας. Η ευπάθεια που περιγράφεται, τρέφει σοβαρό κίνδυνο όσον αφορά την διαθεσιμότητα του πόρου έως και την ολική καταστροφή του. Λόγω αυτού η επικοινωνία δυσκολεύει, παραβιάζονται τα δικαιώματα πρόσβασης και η διαρροή δεδομένων είναι σίγουρη.

Το αγαθό " RADIUS/SNMP SERVER" αποτελεί κρίσιμη υποδομή για την εταιρεία παρακολουθεί ολόκληρο το δίκτυο και ταυτοποιεί υπαλλήλους και πελάτες. Η ευπάθεια που περιγράφεται, τρέφει σοβαρό κίνδυνο όσον αφορά την διαθεσιμότητα του πόρου έως και την ολική καταστροφή του. Λόγω αυτού η επικοινωνία δυσκολεύει, παραβιάζονται τα δικαιώματα πρόσβασης και η διαρροή δεδομένων είναι σίγουρη.

Το αγαθό "WINDOWS 7" αποτελεί κρίσιμη υποδομή για την εταιρεία διότι είναι εργαλείο σωστής λειτουργίας της βιομηχανικής μονάδας. Η ευπάθεια που περιγράφεται, τρέφει σοβαρό κίνδυνο όσον αφορά την διαθεσιμότητα του πόρου έως και την ολική καταστροφή του. Λόγω αυτού η επικοινωνία δυσκολεύει, παραβιάζονται τα δικαιώματα πρόσβασης και η διαρροή δεδομένων είναι σίγουρη. Το πρόβλημα μπορεί να εξαπλωθεί και σε υπόλοιπα συστήματα.

Το αγαθό "INDUSTRY EMPLOYEE DATA" αποτελεί κρίσιμη υποδομή για την εταιρεία διότι διαθέτει όλα τα δεδομένα των υπαλλήλων της βιομηχανικής μονάδας. Η ευπάθεια που περιγράφεται, τρέφει σοβαρό κίνδυνο όσον αφορά την διαθεσιμότητα του πόρου. Λόγω αυτού παραβιάζονται τα δικαιώματα πρόσβασης και η διαρροή δεδομένων είναι σίγουρη. Πρόκειται για βάση δεδομένων όπου η προστασία της πρέπει να είναι μέγιστη διότι διαχειρίζεται προσωπικά δεδομένα.

Το αγαθό " INDUSTRY CUSTOMER DATA " αποτελεί κρίσιμη υποδομή για την εταιρεία διότι διαθέτει όλα τα δεδομένα των πελατών της βιομηχανικής μονάδας. Η ευπάθεια που περιγράφεται, τρέφει σοβαρό κίνδυνο όσον αφορά την διαθεσιμότητα του πόρου. Λόγω αυτού παραβιάζονται τα δικαιώματα πρόσβασης και η διαρροή δεδομένων είναι σίγουρη. Πρόκειται για βάση δεδομένων όπου η προστασία της πρέπει να είναι μέγιστη διότι διαχειρίζεται προσωπικά δεδομένα.

Το αγαθό "WEB APPLICATION SERVER" αποτελεί κρίσιμη υποδομή για την εταιρεία διότι χρησιμοποιείται ως διακομιστής που υιοθετεί την ιστοσελίδα και το ηλεκτρονικό κατάστημα της βιομηχανικής μονάδας. Η ευπάθεια που περιγράφεται, τρέφει μετρίου επιπέδου κίνδυνο όσον αφορά την διαθεσιμότητα του πόρου. Λόγω αυτού η ιστοσελίδα δεν θα είναι διαθέσιμη με αποτέλεσμα να μην είναι εμφανής στο κοινό. Επίσης υπάρχει μεγάλη πιθανότητα διαρροής δεδομένων.

Το αγαθό "EDGE-ROUTER" αποτελεί κρίσιμη υποδομή για την εταιρεία διότι φιλτράρει όλα τα πακέτα που περνούν στο δίκτυο της βιομηχανικής μονάδας. Η ευπάθεια που περιγράφεται, τρέφει σοβαρό κίνδυνο όχι μόνο για την διαθεσιμότητα του πόρου αλλά και για την ακεραιότητα όλου του δικτύου. Λόγω αυτού η επικοινωνία διαλύεται, παραβιάζονται τα δικαιώματα πρόσβασης και η διαρροή δεδομένων είναι σίγουρη. Πρόκειται για εξαιρετικά σημαντικό δρομολογητή διότι συνδέει όλο το δίκτυο της εταιρείας με το διαδίκτυο.

Το αγαθό "ROUTER1" αποτελεί κρίσιμη υποδομή για την εταιρεία διότι βοηθά στην αποστολή και λήψη πακέτων δεδομένων μεταξύ ενός ή περισσοτέρων διακομιστών, άλλων δρομολογητών και πελατών, κατά μήκος πολλαπλών δικτύων της βιομηχανικής μονάδας. Η ευπάθεια που περιγράφεται, τρέφει μετρίου επιπέδου κίνδυνο όχι μόνο για την διαθεσιμότητα του πόρου αλλά και για την ακεραιότητα όλου του δικτύου. Λόγω αυτού η επικοινωνία επιτυγχάνεται με διακοπές και η τροποποίηση ορισμένων αρχείων του συστήματος είναι εφικτή.

Το αγαθό "ROUTER4" αποτελεί κρίσιμη υποδομή για την εταιρεία διότι βοηθά στην αποστολή και λήψη πακέτων δεδομένων μεταξύ ενός ή περισσοτέρων διακομιστών, άλλων δρομολογητών και πελατών, κατά μήκος πολλαπλών δικτύων της βιομηχανικής μονάδας. Η ευπάθεια που περιγράφεται, τρέφει μετρίου επιπέδου κίνδυνο όχι μόνο για την διαθεσιμότητα του πόρου αλλά και για την ακεραιότητα όλου του δικτύου. Λόγω αυτού η επικοινωνία επιτυγχάνεται με διακοπές και η τροποποίηση ορισμένων αρχείων του συστήματος είναι εφικτή.

Το αγαθό "ROUTER2" αποτελεί κρίσιμη υποδομή για την εταιρεία διότι βοηθά στην αποστολή και λήψη πακέτων δεδομένων μεταξύ ενός ή περισσοτέρων διακομιστών, άλλων δρομολογητών και πελατών, κατά μήκος πολλαπλών δικτύων της βιομηχανικής μονάδας. Η ευπάθεια που περιγράφεται, τρέφει μετρίου επιπέδου κίνδυνο όχι μόνο για την διαθεσιμότητα του πόρου αλλά και για την ακεραιότητα όλου του δικτύου. Λόγω αυτού η επικοινωνία επιτυγχάνεται με διακοπές και η τροποποίηση ορισμένων αρχείων του συστήματος είναι εφικτή.

Το αγαθό "ROUTER3" αποτελεί κρίσιμη υποδομή για την εταιρεία διότι βοηθά στην αποστολή και λήψη πακέτων δεδομένων μεταξύ ενός ή περισσοτέρων διακομιστών, άλλων δρομολογητών και πελατών, κατά μήκος πολλαπλών δικτύων της βιομηχανικής μονάδας. Η ευπάθεια που περιγράφεται, τρέφει σοβαρό κίνδυνο όχι μόνο για την διαθεσιμότητα του πόρου αλλά και για την ακεραιότητα όλου του δικτύου. Λόγω αυτού η επικοινωνία διαλύεται, παραβιάζονται τα δικαιώματα πρόσβασης και η διαρροή δεδομένων είναι σίγουρη. Θέτει όλο το δίκτυο εκτός λειτουργίας ανεξαρτήτως σημασίας αυτού του δρομολογητή.

Το αγαθό "WINDOWS 10 PRO" αποτελεί κρίσιμη υποδομή για την εταιρεία διότι είναι εργαλείο σωστής λειτουργίας της βιομηχανικής μονάδας. Η ευπάθεια που περιγράφεται, τρέφει σοβαρό κίνδυνο όσον αφορά την διαθεσιμότητα του πόρου έως και την ολική καταστροφή του. Λόγω αυτού η επικοινωνία δυσκολεύει, παραβιάζονται τα δικαιώματα πρόσβασης και η διαρροή δεδομένων είναι σίγουρη. Το πρόβλημα μπορεί να εξαπλωθεί και σε υπόλοιπα συστήματα.

Το αγαθό "EMAIL SERVER" αποτελεί κρίσιμη υποδομή για την εταιρεία διότι υιοθετεί όλα τα ηλεκτρονικά μηνύματα μεταξύ πελατών και υπαλλήλων της βιομηχανικής μονάδας. Η ευπάθεια που περιγράφεται, τρέφει μετρίου επιπέδου κίνδυνο όσον αφορά την διαθεσιμότητα του πόρου. Λόγω αυτού η επικοινωνία μεταξύ υπαλλήλων ή πελατών-υπαλλήλων δεν θα είναι διαθέσιμη. Επίσης υπάρχει μεγάλη πιθανότητα διαρροής δεδομένων.

Το αγαθό "DNS / DHCP SERVER" αποτελεί κρίσιμη υποδομή για την εταιρεία διότι βοηθά στην δέσμευση και αντιστοίχιση των διευθύνσεων δικτύου στους hosts καθώς και στην ονοματοδοσία στα δίκτυα υπολογιστών που χρησιμοποιούν το πρωτόκολλο IP. Η ευπάθεια που περιγράφεται, τρέφει σοβαρό κίνδυνο όσον αφορά την διαθεσιμότητα του πόρου έως και την ολική καταστροφή του. Λόγω αυτού η επικοινωνία διαλύεται, παραβιάζονται τα δικαιώματα πρόσβασης και η διαρροή δεδομένων είναι σίγουρη. Υπάρχει μεγάλη πιθανότητα να καταστραφεί υλικό (hardware) του διακομιστή.

Το αγαθό "HRM SERVER" αποτελεί κρίσιμη υποδομή για την εταιρεία διότι βοηθά στην παρακολούθηση του εργασιακού κύκλου της βιομηχανικής μονάδας. Επομένως η απώλειά του, θα προκαλέσει επικοινωνιακά και δομικά προβλήματα στην εταιρεία. Η ευπάθεια που περιγράφεται, τρέφει μετρίου επιπέδου κίνδυνο όσον αφορά την διαθεσιμότητα του πόρου. Λόγω αυτού η επίβλεψη του εργατικού δυναμικού θα είναι αρκετά δύσκολη διότι θα συμβαίνουν διακοπές στην διαθεσιμότητά του. Επίσης υπάρχει μεγάλη πιθανότητα διαρροής δεδομένων.

Το αγαθό "SW-FLOOR4.1" αποτελεί κρίσιμη υποδομή για την εταιρεία διότι διαχειρίζεται την κυκλοφορία μεταξύ δύο συσκευών να μην παρεμποδίζουν τις άλλες συσκευές στο ίδιο δίκτυο της βιομηχανικής μονάδας. Η ευπάθεια που περιγράφεται, τρέφει σοβαρό κίνδυνο όχι μόνο για την διαθεσιμότητα του πόρου αλλά και για την ακεραιότητα όλου του δικτύου. Λόγω αυτού η επικοινωνία με τον 4ο όροφο διαλύεται συνολικά, παραβιάζονται τα δικαιώματα πρόσβασης και η διαρροή δεδομένων είναι σίγουρη. Θέτει όλο το δίκτυο εκτός λειτουργίας διότι ο συγκεκριμένος μεταγωγέας τροφοδοτεί όλο το δωμάτιο που είναι τοποθετημένοι οι διακομιστές.

Το αγαθό "SW-FLOOR4.2" αποτελεί κρίσιμη υποδομή για την εταιρεία διότι διαχειρίζεται την κυκλοφορία μεταξύ δύο συσκευών να μην παρεμποδίζουν τις άλλες συσκευές στο ίδιο δίκτυο της βιομηχανικής μονάδας. Η ευπάθεια που περιγράφεται, τρέφει σοβαρό κίνδυνο όχι μόνο για την διαθεσιμότητα του πόρου αλλά και για την ακεραιότητα όλου του δικτύου. Λόγω αυτού η επικοινωνία με τον 4ο όροφο διαλύεται στο ήμισυ, παραβιάζονται τα δικαιώματα πρόσβασης και η διαρροή δεδομένων είναι σίγουρη. Θέτει όλο το δίκτυο εκτός λειτουργίας διότι ο συγκεκριμένος μεταγωγέας τροφοδοτεί το μισό δωμάτιο που είναι τοποθετημένοι οι διακομιστές.

Το αγαθό "SW-FLOOR1" αποτελεί κρίσιμη υποδομή για την εταιρεία διότι διαχειρίζεται την κυκλοφορία μεταξύ δύο συσκευών να μην παρεμποδίζουν τις άλλες συσκευές στο ίδιο δίκτυο της βιομηχανικής μονάδας. Η ευπάθεια που περιγράφεται, τρέφει μετρίου επιπέδου κίνδυνο όσον αφορά την αποκάλυψη δεδομένων. Λόγω αυτού υπάρχει μεγάλη πιθανότητα να διαρρεύσουν δεδομένα που βρίσκονται μέσα στους υπολογιστές των υπαλλήλων του 1ου ορόφου.

Το αγαθό "SW-FLOOR3" αποτελεί κρίσιμη υποδομή για την εταιρεία διότι διαχειρίζεται την κυκλοφορία μεταξύ δύο συσκευών να μην παρεμποδίζουν τις άλλες συσκευές στο ίδιο δίκτυο της βιομηχανικής μονάδας. Η ευπάθεια που περιγράφεται, τρέφει μετρίου επιπέδου κίνδυνο όσον αφορά την αποκάλυψη δεδομένων. Λόγω αυτού υπάρχει μεγάλη πιθανότητα να διαρρεύσουν δεδομένα που βρίσκονται στους υπολογιστές του διευθυντή. Κατατάσσεται σε μετρίου επιπέδου διότι θεωρείται ότι ο διευθυντής έχει λάβει έστω και στοιχειώδη μέτρα προκειμένου να μην εξαπλωθεί το πρόβλημα στους διακομιστές.

Το αγαθό "SW-FLOOR2" αποτελεί κρίσιμη υποδομή για την εταιρεία διότι διαχειρίζεται την κυκλοφορία μεταξύ δύο συσκευών να μην παρεμποδίζουν τις άλλες συσκευές στο ίδιο δίκτυο της βιομηχανικής μονάδας. Η ευπάθεια που περιγράφεται, τρέφει μετρίου επιπέδου κίνδυνο όσον αφορά την αποκάλυψη δεδομένων. Λόγω αυτού υπάρχει μεγάλη πιθανότητα να διαρρεύσουν δεδομένα που βρίσκονται μέσα στους υπολογιστές των υπαλλήλων του 2ου ορόφου.

Το αγαθό "PC4" αποτελεί κρίσιμη υποδομή για την εταιρεία διότι αποτελεί υπολογιστή υπαλλήλου για το τμήμα πωλήσεων και IT της βιομηχανικής μονάδας. Η ευπάθεια που περιγράφεται, τρέφει σοβαρό κίνδυνο όχι μόνο για την διαθεσιμότητα του πόρου αλλά και για την ακεραιότητα όλου του δικτύου. Λόγω αυτού, ο εισβολέας μπορεί να αποκτήσει πρόσβαση σε κάθε συσκευή του δικτύου με

αποτέλεσμα να τροποποιήσει, να διαγράψει ή και να κλέψει δεδομένα. Θέτει όλο το δίκτυο εκτός λειτουργίας διότι η απομακρυσμένη εκτέλεση κώδικα αποτελεί σοβαρή απειλή για κάθε σύστημα.

Το αγαθό "PC6" αποτελεί κρίσιμη υποδομή για την εταιρεία διότι είναι υπολογιστής υπαλλήλου για το τμήμα πωλήσεων και IT της βιομηχανικής μονάδας. Η ευπάθεια που περιγράφεται, τρέφει μετρίου επιπέδου κίνδυνο όσον αφορά την αποκάλυψη δεδομένων. Λόγω αυτού υπάρχει μεγάλη πιθανότητα να διαρρεύσουν δεδομένα που βρίσκονται μέσα στους υπολογιστές των υπαλλήλων του 2ου ορόφου.

Το αγαθό "LAPTOP1" αποτελεί κρίσιμη υποδομή για την εταιρεία διότι είναι διαχειριστικό εργαλείο της βιομηχανικής μονάδας που κατέχει ο διευθυντής. Η ευπάθεια που περιγράφεται, τρέφει σοβαρό κίνδυνο όχι μόνο για την διαθεσιμότητα του πόρου αλλά και για την ακεραιότητα όλου του δικτύου. Ένα μη πιστοποιημένο Antivirus μπορεί να έχει καταστροφικές συνέπειες τόσο με το θέμα των προσωπικών και επαγγελματικών δεδομένων, όσο και με την ολική υλική καταστροφή συστημάτων και δικτύων. Γι' αυτό, ένα αξιόπιστο Antivirus μπορεί να μειώσει αρκετά την πιθανότητα της έκθεσης συστήματος ή συστημάτων σε ακίνδυνους ή και σοβαρούς ιούς.

Το αγαθό "TABLET-PC1" αποτελεί κρίσιμη υποδομή για την εταιρεία διότι είναι διαχειριστικό εργαλείο της βιομηχανικής μονάδας που κατέχει ο διευθυντής. Η ευπάθεια που περιγράφεται, τρέφει σοβαρό κίνδυνο όχι μόνο για την διαθεσιμότητα του πόρου αλλά και για την ακεραιότητα όλου του δικτύου. Η απομακρυσμένη εκτέλεση κώδικα από τον εισβολέα στο συγκεκριμένο αγαθό, μπορεί να έχει ολέθριες συνέπειες τόσο με το θέμα των προσωπικών και επαγγελματικών δεδομένων, όσο και με τα συστήματα και δίκτυα της εταιρείας.

Το αγαθό "PC1" αποτελεί κρίσιμη υποδομή για την εταιρεία διότι είναι υπολογιστής υπαλλήλου για το τμήμα λογιστικής και διαχείρισης εργατικού δυναμικού της βιομηχανικής μονάδας. Η ευπάθεια που περιγράφεται, τρέφει σοβαρό κίνδυνο όχι μόνο για την διαθεσιμότητα του πόρου αλλά και για την ακεραιότητα όλου του δικτύου. Λόγω αυτού, ο εισβολέας μπορεί να αποκτήσει πρόσβαση σε κάθε συσκευή του δικτύου με αποτέλεσμα να τροποποιήσει, να διαγράψει ή και να κλέψει δεδομένα. Θέτει όλο το δίκτυο εκτός λειτουργίας διότι η απομακρυσμένη εκτέλεση κώδικα αποτελεί σοβαρή απειλή για κάθε σύστημα. Κάποιος μπορεί να πάρει πρόσβαση στο συγκεκριμένο αγαθό εάν ο χρήστης του ανοίξει ένα παραπλανητικό αρχείο ή πρόγραμμα.

Το αγαθό "PC2" αποτελεί κρίσιμη υποδομή για την εταιρεία διότι είναι υπολογιστής υπαλλήλου για το τμήμα λογιστικής και διαχείρισης εργατικού δυναμικού της βιομηχανικής μονάδας. Η ευπάθεια που περιγράφεται, τρέφει σοβαρό κίνδυνο όχι μόνο για την διαθεσιμότητα του πόρου αλλά και για την ακεραιότητα όλου του δικτύου. Λόγω αυτού, ο εισβολέας μπορεί να αποκτήσει πρόσβαση σε κάθε συσκευή του δικτύου με αποτέλεσμα να τροποποιήσει, να διαγράψει ή και να κλέψει δεδομένα. Θέτει όλο το δίκτυο εκτός λειτουργίας διότι αποκτά δικαιώματα διαχειριστή με αποτέλεσμα να μπορεί να διαχειριστεί ο ίδιος όλο το δίκτυο.

Το αγαθό "VOIP-PHONE1" αποτελεί κρίσιμη υποδομή για την εταιρεία διότι είναι επικοινωνιακό εργαλείο του τμήματος πωλήσεων και IT με όλα τα υπόλοιπα τμήματα της βιομηχανικής μονάδας. Η ευπάθεια που περιγράφεται, τρέφει σοβαρό κίνδυνο όχι μόνο για την διαθεσιμότητα του πόρου αλλά και για την ακεραιότητα όλου του δικτύου. Τα μη κρυπτογραφημένα αρχεία μπορούν να αποκαλύψουν σημαντικές πληροφορίες που αφορούν την λειτουργία της εταιρείας αλλά και να διαρρεύσουν απόρρητες συνομιλίες. Με αυτό τον τρόπο, ο δράστης θα γνωρίζει τα πάντα για την εταιρεία προκειμένου να την εκμεταλλευτεί με κάθε τρόπο.

Το δικό μας αγαθό "VOIP-PHONE2" αποτελεί κρίσιμη υποδομή για την εταιρεία διότι είναι επικοινωνιακό εργαλείο του διευθυντή με όλα τα υπόλοιπα τμήματα της βιομηχανικής μονάδας. Η ευπάθεια που περιγράφεται, τρέφει σοβαρό κίνδυνο για την διαθεσιμότητα του πόρου και τα επαγγελματικά δεδομένα. Το VoIP based phishing μπορεί να έχει ολέθριες συνέπειες για τα επαγγελματικά δεδομένα της εταιρείας. Ο δράστης χρησιμοποιεί πλαστογράφηση ταυτότητας

κάνοντας τον υπάλληλο της εταιρείας. Έτσι έχει πρόσβαση σε αρκετά δεδομένα που μπορεί να εκμεταλλευτεί.

Το δικό μας αγαθό "VOIP-PHONE3" αποτελεί κρίσιμη υποδομή για την εταιρεία διότι είναι επικοινωνιακό εργαλείο του τμήματος λογιστικής και διαχείρισης εργατικού δυναμικού της βιομηχανικής μονάδας. Η ευπάθεια που περιγράφεται, τρέφει σοβαρό κίνδυνο για την διαθεσιμότητα του πόρου και τα επαγγελματικά δεδομένα. Το VOMIT επιτρέπει στον δράστη να συλλέξει δεδομένα που αφορούν την προέλευση κλήσεων, κωδικούς πρόσβασης, ονόματα πελατών και υπαλλήλων, τηλεφωνικούς αριθμούς, τραπεζικούς λογαριασμούς και άλλα δεδομένα της εταιρείας.

Το αγαθό "PC3" αποτελεί κρίσιμη υποδομή για την εταιρεία διότι είναι υπολογιστής υπαλλήλου για το τμήμα πωλήσεων και IT της βιομηχανικής μονάδας. Η ευπάθεια που περιγράφεται, τρέφει μετρίου επιπέδου κίνδυνο για τα δεδομένα της εταιρείας. Λόγω αυτού, ο εισβολέας να ανακτήσει πληροφορίες όταν ο πυρήνας των Windows χειρίζεται ακατάλληλα αντικείμενα στη μνήμη. Παρόλο που δεν υπάρχει επίδραση στην διαθεσιμότητα του πόρου, υπάρχει μεγάλη πιθανότητα να διαρρεύσουν ορισμένα δεδομένα που είναι απευθείας αποθηκευμένα στο συγκεκριμένο αγαθό.

Το αγαθό "PC5" αποτελεί κρίσιμη υποδομή για την εταιρεία διότι είναι υπολογιστής υπαλλήλου για το τμήμα πωλήσεων και IT της βιομηχανικής μονάδας. Η ευπάθεια που περιγράφεται, τρέφει σοβαρό κίνδυνο όχι μόνο για την διαθεσιμότητα του πόρου αλλά και για την ακεραιότητα όλου του δικτύου. Υπάρχει μια αύξηση της ευπάθειας των δικαιωμάτων όταν ο Windows Error Reporting Manager χειρίζεται εσφαλμένα μια διακοπή της διαδικασίας. Αυτό μπορεί να το εκμεταλλευτεί ένας εισβολέας και να γίνει διαχειριστής του συστήματος. Αυτό συνεπάγεται σε διαρροή δεδομένων και αδυναμία χρήσης του συγκεκριμένου αγαθού από τους υπαλλήλους.

Το αγαθό "Customer Support" αποτελεί κρίσιμη υποδομή για την εταιρεία διότι βοηθά στην επικοινωνία της εταιρείας με όλους τους πελάτες της. Η ευπάθεια που περιγράφεται, τρέφει μετρίου επιπέδου κίνδυνο όχι μόνο για την εμπιστευτικότητα των δεδομένων αλλά και για την ακεραιότητα του αγαθού. Η τηλεφωνική απάτη είναι αρκετά διαδεδομένη σε εταιρείες όπως η τρέχουσα. Ένας δράστης θα μπορούσε να τηλεφωνήσει στο κέντρο εξυπηρέτησης πελατών προωθώντας την γραμμή σε μία άλλη υψηλής χρέωσης. Έτσι μπορούν να βγάλουν χρήματα.

Το αγαθό "Create New Order (Remotely)" αποτελεί κρίσιμη υποδομή για την εταιρεία διότι είναι μέσο πώλησης προϊόντων και υπηρεσιών που προσφέρει η βιομηχανική μονάδα. Η ευπάθεια που περιγράφεται, τρέφει μετρίου επιπέδου κίνδυνο όχι μόνο για την διαθεσιμότητα του πόρου αλλά και για την ακεραιότητα του αγαθού. Ένας πελάτης ο οποίος δεν είναι εγκεκριμένος (ψεύτικος πελάτης), μπορεί να πραγματοποιήσει μία παραγγελία χωρίς να έχει ταυτοποιηθεί. Έτσι, μπορεί να παραλάβει παραγγελία χωρίς να πληρώσει ή ακόμα και να κλέψει δεδομένα παρακολουθώντας την λειτουργία της εταιρείας για να την εκμεταλλευτεί αναλόγως.

Το αγαθό "Create New Order (Local)" αποτελεί κρίσιμη υποδομή για την εταιρεία διότι είναι μέσο πώλησης προϊόντων και υπηρεσιών που προσφέρει η βιομηχανική μονάδα. Η ευπάθεια που περιγράφεται, τρέφει μετρίου επιπέδου κίνδυνο όχι μόνο για την διαθεσιμότητα του πόρου αλλά και για την ακεραιότητα του αγαθού. Ένας πελάτης που θέλει να κάνει την παραγγελία με φυσική παρουσία στην εταιρεία, ίσως επιθυμεί να επιβλέψει την δουλειά των υπαλλήλων ή να τους αποσπάσει πληροφορίες. Αυτό μπορεί να γίνει εάν τα δεδομένα είναι τοποθετημένα τοπικά στους υπολογιστές των υπαλλήλων. Έτσι μπορεί να λάβει σημαντικά δεδομένα που αφορούν την λειτουργία της εταιρείας ή ακόμα και ονόματα και πληροφορίες υπαλλήλων και πελατών.

Το αγαθό "PRINTER1" αποτελεί κρίσιμη υποδομή για την εταιρεία διότι είναι εργαλείο που εκτυπώνει σημαντικά έγγραφα για την οικονομική διαχείριση της βιομηχανικής μονάδας. Η ευπάθεια που περιγράφεται, τρέφει σοβαρό κίνδυνο όχι μόνο για την διαθεσιμότητα του πόρου αλλά και για την ακεραιότητά του. Επιτρέπει στους τοπικούς χρήστες να αποκτήσουν προνόμια μέσω ενός Trojan horse file. Αυτό έχει ως αποτέλεσμα όχι μόνο την αναστολή λειτουργίας ολόκληρου του πόρου αλλά και την διαρροή ορισμένων δεδομένων που υπάρχουν εντός της συσκευής.

Το δικό μας αγαθό "PRINTER2" αποτελεί κρίσιμη υποδομή για την εταιρεία διότι είναι εργαλείο που εκτυπώνει σημαντικά έγγραφα για την οικονομική και λειτουργική διαχείριση της βιομηχανικής μονάδας από τον διευθυντή. Η ευπάθεια που περιγράφεται, τρέφει σοβαρό κίνδυνο όχι μόνο για την διαθεσιμότητα του πόρου αλλά και για την ακεραιότητά του. Ένας εισβολέας μπορεί να έχει πρόσβαση στο δίκτυο της εταιρείας και να λάβει κρίσιμα δεδομένα όπως οικονομικά έγγραφα, εσωτερικούς κανονισμούς και άλλα.

Το αγαθό "WIRELESS-LAN-CONTROLLER1" αποτελεί κρίσιμη υποδομή για την εταιρεία διότι διαχειρίζεται σημεία πρόσβασης ασύρματου δικτύου που επιτρέπουν στις ασύρματες συσκευές να συνδεθούν στο δίκτυο της βιομηχανικής μονάδας. Η ευπάθεια που περιγράφεται, τρέφει μετρίου επιπέδου κίνδυνο όσον αφορά την αποκάλυψη δεδομένων και την ακεραιότητα του αγαθού. Θα μπορούσε να επιτρέψει σε έναν μη εξουσιοδοτημένο, παρακείμενο εισβολέα να επαναφέρει το Autonomic Control Plane (ACP) ενός επηρεαζόμενου συστήματος και να δει πακέτα ACP που μεταφέρονται σε καθαρό κείμενο εντός ενός επηρεαζόμενου συστήματος. Παρόλο που δεν υπάρχει επίδραση στην διαθεσιμότητα του πόρου, υπάρχει μεγάλη πιθανότητα να διαρρεύσουν ορισμένα δεδομένα που είναι απευθείας αποθηκευμένα στο συγκεκριμένο αγαθό.

Το αγαθό "ACCESS-POINT" αποτελεί κρίσιμη υποδομή για την εταιρεία διότι Συνδέει μεταξύ τους ασύρματες συσκευές επικοινωνίας για τον σχηματισμό ενός ασύρματου δικτύου της βιομηχανικής μονάδας. Η ευπάθεια που περιγράφεται, τρέφει μετρίου επιπέδου κίνδυνο όσον αφορά την αποκάλυψη δεδομένων και την ακεραιότητα του αγαθού. Επιτρέπει σε έναν επικυρωμένο, τοπικό εισβολέα να έχει πρόσβαση σε ευαίσθητες πληροφορίες συστήματος σε μια επηρεαζόμενη συσκευή. Θα μπορούσε να εκμεταλλευτεί αυτήν την ευπάθεια ανακτώντας τα περιεχόμενα συγκεκριμένων θέσεων μνήμης μιας επηρεαζόμενης συσκευής. Παρόλο που δεν υπάρχει επίδραση στην διαθεσιμότητα του πόρου, υπάρχει μεγάλη πιθανότητα να διαρρεύσουν ορισμένα δεδομένα που είναι απευθείας αποθηκευμένα στο συγκεκριμένο αγαθό.

	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	Αποτυχημένη αποστολέα	Αποτυχημένη παραλήπτη	Άρνηση αποστολής ή παραλαβής	Παρεμβολή λανθασμένων μηνυμάτων	Λανθασμένη δρομολόγηση	Παραποίηση κίνησης	Μη παράδοση	Απώλεια ακολουθίας μηνυμάτων
DOMAIN CONTROLLER / FILE SERVER	1	1	2	2	2	1	1	1	3	3	3	2	1	1	3	1	1	1	1	3	3	1	1	3
CRM SERVER	1	2	5	6	8	8	8	8	5	8	2	8	7	3	8									
RADIUS / SNMP SERVER	1	5	8	8	8	8	8	8	4	7	4	7	3	3	8	5	6	6	7	8	8	7	7	6
WINDOWS 7	8	8	8	8	8	6	3	8	3	8	5	8	3	2	8	3	8	8	3	4	5	4	3	3
INDUSTRY EMPLOYEE DATA	1	3	6	8	8	8	6	5	5	7	6	7	4	2	8	3	4	8	8	7	2	3	7	8
INDUSTRY CUSTOMER DATA	1	2	5	8	8	8	6	6	6	8	5	5	2	1	8	3	4	8	8	7	2	3	7	8
WEB APPLICATION SERVER	1	2	2	2	2	1	1	1	6	5	6	4	2	2	2	6	6	6	6	5	5	6	6	4
EDGE-ROUTER	2	6	8	8	7	4	2	2	2	2	2	2	1	1	2	4	7	7	8	8	8	7	8	6
ROUTER1	1	1	1	2	2	2	2	1	4	4	4	1	2	2	4	2	4	4	4	4	4	4	4	3
ROUTER4	1	1	1	2	2	2	1	1	2	2	2	1	2	1	4	1	2	2	2	2	2	2	2	1
ROUTER2	2	3	3	3	3	3	2	1	2	2	2	1	1	1	2	2	3	3	3	3	3	3	3	1
ROUTER3	2	6	8	8	8	7	4	3	2	2	2	1	1	1	2	3	7	7	8	8	8	7	8	6
WINDOWS 10 PRO	2	3	8	8	8	6	4	3	7	5	7	6	3	1	6	5	8	8	6	7	7	6	5	5
EMAIL SERVER	2	8	8	8	6	4	3	3	7	7	8	6	2	1	8	6	8	8	8	8	7	6	8	8
DNS/DHCP SERVER	4	7	9	9	9	7	6	7	9	9	6	9	7	4	9	4	6	6	6	4	9	6	9	5
HRM SERVER	5	7	7	7	7	6	4	4	5	5	3	4	4	2	7	3	5	5	5	7	4	4	7	5

SW-FLOOR4.1	3	7	9	9	7	5	5	2	2	2	2	2	1	1	2	9	9	9	7	5	9	8	9	6
SW-FLOOR4.2	4	8	8	8	6	5	3	3	7	7	8	6	3	4	8	8	8	8	6	4	8	7	8	5
SW-FLOOR1	1	1	2	2	1	1	1	2	2	2	2	1	4	3	5	5	5	5	3	2	5	3	5	2
SW-FLOOR3	1	1	2	2	1	1	1	2	2	2	2	1	4	3	5	5	5	5	3	2	5	3	5	2
SW-FLOOR2	1	1	2	2	1	1	1	2	2	2	2	1	4	3	5	5	5	5	3	2	5	3	5	2
PC4	4	8	8	8	7	7	5	8	8	8	8	6	6	3	8	4	7	7	8	8	2	7	8	7
PC6	1	2	2	2	2	2	1	3	6	6	6	5	2	1	2	3	5	5	6	6	2	5	6	5
LAPTOP1	5	9	9	9	9	9	9	8	7	9	9	7	8	6	9	5	8	8	9	9	6	8	9	7
TABLET-PC1	4	6	8	8	8	7	5	6	7	7	8	6	7	5	8	4	7	7	8	8	5	7	8	6
PC1	2	4	5	9	9	7	9	8	7	7	7	7	6	3	9	4	7	7	9	9	1	9	8	7
PC2	2	9	9	9	7	5	8	9	7	7	7	7	6	3	9	4	7	7	9	9	1	9	8	7
VOIP-PHONE1	8	8	8	7	5	3	3	6	7	8	5	6	3	6	8	6	8	8	7	7	2	7	8	6
VOIP-PHONE2	7	7	7	6	6	4	3	5	6	7	5	6	3	6	7	1	7	7	6	3	6	7	7	2
VOIP-PHONE3	7	7	7	5	5	6	3	2	7	7	7	5	4	6	7	1	7	7	5	5	5	7	7	6
PC3	1	2	2	2	2	2	1	1	2	2	2	2	2	1	7	3	5	5	7	7	1	5	7	5
PC5	4	9	9	9	7	5	7	9	7	7	7	9	7	4	9	4	7	7	9	9	2	7	8	7
CUSTOMER SUPPORT	1	1	1	1	1	1	1	1	2	2	4	2	3	1	5	5	5	5	4	5	1	1	5	4
CREATE NEW ORDER (REMOTELY)	4	4	4	4	4	4	3	4	4	3	2	4	2	1	4	4	1	1	4	3	1	2	4	3
CREATE NEW ORDER (LOCAL)	5	5	5	5	5	5	3	5	4	3	2	5	4	3	5	5	2	2	5	4	1	3	5	4
PRINTER1	7	7	7	6	5	5	4	4	7	6	7	5	5	2	7	6	5	5	6	2	4	6	7	7
PRINTER2	7	7	7	6	5	5	4	4	7	6	7	5	5	2	7	6	5	5	6	2	4	6	7	7
WIRELESS-LAN-CONTROLLER	1	1	2	2	2	2	2	3	4	3	4	4	3	2	4	4	4	4	2	2	2	2	4	2
ACCESS-POINT	2	2	2	2	2	1	1	1	1	2	2	2	3	2	5	5	5	5	2	2	2	2	5	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 του/της ΕΤΑΙΡΕΙΑ1.

4.1. Προσωπικό – Προστασία Διαδικασιών Προσωπικού

Τα αγαθά με ID «CI-A-1013», «CI-A-1021», «CI-A-1038», «CI-A-1008», «CI-A-1039», «CI-A-1017», «CI-A-1009», «CI-A-1019», «CI-A-1020», «CI-A-1030», «CI-A-1031», «CI-A-1032» και «CI-A-1040» αφορούν εργαλεία για διαδικασίες που εκτελούν οι υπάλληλοι εντός της εταιρείας. Προτείνεται αφενός συνεχής εκσυγχρονισμός τόσο του υλικού όσο και του λογισμικού, αφετέρου η χρήση δυνατών κωδικών πρόσβασης, η κρυπτογράφηση όλων των δεδομένων, η ταυτοποίηση αποστολέα και παραλήπτη μηνυμάτων και η χρήση firewall για αποκλεισμό ανώνυμων και κατά τα άλλα επικίνδυνων τρίτων από την πρόσβαση στον συνδεδεμένο εξοπλισμό. Έτσι μειώνεται η πιθανότητα κλοπής προσωπικών δεδομένων μέσω διαδικασιών της εταιρείας.

4.2. Ταυτοποίηση και αυθεντικοποίηση

Τα αγαθά με ID «CI-A-1010», «CI-A-1011» και «CI-A-1033» αφορούν την ταυτοποίηση και την αυθεντικοποίηση. Προτείνεται αφενός ενημέρωση των λειτουργικών συστημάτων στις νεότερες εκδόσεις, αφετέρου η άμεση απενεργοποίηση όλων των περιττών υπηρεσιών που είναι ενεργές στα παραπάνω αγαθά. Έτσι μειώνεται η πιθανότητα επίθεσης χωρίς να γίνει αντιληπτή.

4.3. Έλεγχος προσπέλασης και χρήσης πόρων

Τα αγαθά με ID «CI-A-1008», «CI-A-1040», «CI-A-1038», «CI-A-1017», «CI-A-1024» και «CI-A-1011» αφορούν διαχείριση και την επίβλεψη όλου του δικτύου συμπεριλαμβανομένου των συσκευών και του βιομηχανικού εξοπλισμού. Προτείνεται αφενός ενημέρωση των λειτουργικών συστημάτων στις νεότερες εκδόσεις, αφετέρου η συνεχή επαλήθευση αποστολέα ή παραλήπτη μηνυμάτων, η χρήση firewall για αποκλεισμό ανώνυμων και κατά τα άλλα επικίνδυνων τρίτων από την πρόσβαση στον συνδεδεμένο εξοπλισμό, η αγορά αξιόπιστου και αυθεντικού Antivirus και η αποφυγή εκτέλεσης άγνωστων εφαρμογών. Έτσι μειώνεται η πιθανότητα ώστε οι πόροι της εταιρείας να γίνουν στόχοι επιθέσεων με αποτέλεσμα την μερική ή ολική απώλειας λειτουργίας τους.

4.4. Διαχείριση εμπιστευτικών δεδομένων

Τα αγαθά με ID «CI-A-1000», «CI-A-1001», «CI-A-1002», «CI-A-1003», «CI-A-1004» και «CI-A-1005» αφορούν βάσεις δεδομένων ή διαδικασίες που διαχειρίζονται κρίσιμα προσωπικά δεδομένα. Προτείνεται αφενός η ταυτοποίηση κάθε πελάτη και τηλεφωνικής ή διαδικτυακής κλήσης, αφετέρου η θέσπιση κανονισμών και διαδικασιών για κατά γράμμα τήρηση από όλους τους υπαλλήλους. Έτσι μειώνεται η πιθανότητα έκθεσης των προσωπικών δεδομένων πελατών και υπαλλήλων.

4.5. Προστασία από τη χρήση υπηρεσιών από τρίτους

Τα αγαθά με ID «CI-A-1008», «CI-A-1009», «CI-A-1017», «CI-A-1019», «CI-A-1020», «CI-A-1030», «CI-A-1031» και «CI-A-1032» αφορούν εργαλεία συνεχής χρήσης. Προτείνεται αφενός ενημέρωση των λειτουργικών συστημάτων στις νεότερες εκδόσεις, αφετέρου η εγκατάσταση αξιόπιστων και αυθεντικών εφαρμογών. Έτσι μειώνεται η πιθανότητα έκθεσης των ίδιων των εργαλείων καθημερινής χρήσης σε άγνωστα προγράμματα που μπορεί να διαθέτουν ιομορφικό λογισμικό.

4.6. Προστασία λογισμικού

Τα αγαθά με ID «CI-A-1006», «CI-A-1007» καθώς και τα λειτουργικά συστήματα όλων των επιμέρους συσκευών αφορούν εργαλεία συνεχής χρήσης. Προτείνεται αφενός ενημέρωση των λειτουργικών συστημάτων και των εφαρμογών τους στις νεότερες εκδόσεις, αφετέρου η επιλογή αυθεντικού λογισμικού. Έτσι μειώνεται η πιθανότητα έκθεσης των συστημάτων σε επιθέσεις που προέρχονται από πειρατικά προγράμματα.

4.7. Διαχείριση ασφάλειας δικτύου

Τα αγαθά με ID «CI-A-1018», «CI-A-1023», «CI-A-1022», «CI-A-1025», «CI-A-1027», «CI-A-1026», «CI-A-1035», «CI-A-1012», «CI-A-1015», «CI-A-1036», «CI-A-1034», «CI-A-1037», «CI-A-1016», «CI-A-1028» και «CI-A-10» αφορούν δικτυακό εξοπλισμό που διαθέτει η εταιρεία. Προτείνεται αφενός ενημέρωση των λειτουργικών συστημάτων στις νεότερες εκδόσεις, αφετέρου το κλείσιμο των περιττών θυρών των δρομολογητών, η θέσπιση κανονισμών και διαδικασιών για κατά γράμμα τήρηση από όλους τους υπαλλήλους, η απενεργοποίηση της λειτουργίας αφαλούς αποθήκευσης και ο υποχρεωτικός έλεγχος πρόσβασης στο δίκτυο. Έτσι μειώνεται η πιθανότητα ευπαθειών που προέρχονται από το δικτυακό κομμάτι της εταιρείας.

4.8. Προστασία από ιομορφικό λογισμικό

Τα αγαθά με ID «CI-A-1008», «CI-A-1009», «CI-A-1017», «CI-A-1019», «CI-A-1020», «CI-A-1030», «CI-A-1031» και «CI-A-1032» αφορούν εργαλεία συνεχής χρήσης. Προτείνεται αφενός ενημέρωση των λειτουργικών συστημάτων στις νεότερες εκδόσεις, αφετέρου η εγκατάσταση αξιόπιστων και αυθεντικών Antivirus. Έτσι μειώνεται η πιθανότητα έκθεσης των συστημάτων σε επικίνδυνους ιούς.

4.9. Ασφαλής χρήση διαδικτυακών υπηρεσιών

Τα αγαθά με ID «CI-A-1008», «CI-A-1009», «CI-A-1017», «CI-A-1019», «CI-A-1020», «CI-A-1030», «CI-A-1031» και «CI-A-1032» αφορούν εργαλεία συνεχής χρήσης. Προτείνεται αφενός ενημέρωση των λειτουργικών συστημάτων και των εφαρμογών τους στις νεότερες εκδόσεις, αφετέρου η είσοδος μόνο σε αξιόπιστες ιστοσελίδες, η χρήση AdBlocker για απόκρυψη διαφημίσεων και η χρήση firewall για αποκλεισμό ανώνυμων και κατά τα άλλα επικίνδυνων τρίτων από την πρόσβαση στον συνδεδεμένο εξοπλισμό. Έτσι μειώνεται η πιθανότητα έκθεσης των ίδιων των εργαλείων καθημερινής χρήσης σε άγνωστα προγράμματα που μπορεί να διαθέτουν ιομορφικό λογισμικό.

4.10. Ασφάλεια εξοπλισμού

Τα αγαθά με ID «CI-A-1010», «CI-A-1011», «CI-A-1018», «CI-A-1023», «CI-A-1024», «CI-A-1029» και «CI-A-1033» αφορούν τον κύριο εξοπλισμό της εταιρείας δηλαδή όλους τους διακομιστές που χρησιμοποιούνται για το χτίσιμο όλων των προσφερόμενων υπηρεσιών. Προτείνεται αφενός ενημέρωση των λειτουργικών συστημάτων στις νεότερες εκδόσεις, αφετέρου η απενεργοποίηση όλων των περιττών υπηρεσιών, η δημιουργία ενός σχεδίου επικοινωνίας και η προειδοποίηση όλων των υπαλλήλων να μην ανοίγουν άγνωστα αρχεία που τους αποστέλλονται μέσω spam μηνυμάτων ή που είναι εγκατεστημένα αυτόματα στον υπολογιστή τους. Έτσι μειώνεται η πιθανότητα καταστροφής κρίσιμων ηλεκτρονικών υποδομών της εταιρείας.

4.11. Φυσική ασφάλεια κτιριακής εγκατάστασης

Τα αγαθά με ID «CI-A-1010», «CI-A-1011», «CI-A-1018», «CI-A-1023», «CI-A-1024», «CI-A-1029» και «CI-A-1033», τα οποία αποτελούν την ηλεκτρονική υποδομή της εταιρείας, πρέπει να βρίσκονται σε δωμάτιο δροσερό και χωρίς απευθείας έκθεση στον ήλιο έτσι ώστε να μην επιτυγχάνεται υπερθέρμανση των συστημάτων. Επίσης πρέπει να υπάρχει πυροσβεστικός μηχανισμός για πρόληψη πυρκαγιάς και σχετικό ύψος στα συστήματα ώστε σε περίπτωση πλημμύρας να μπορούν να είναι σχετικά ασφαλή. Το κτίριο πρέπει να είναι ελεγμένο από τις αρμόδιες αρχές αναφορικά με την ενεργειακή κλάση, την αντισεισμική προστασία, την αντιπυρική προστασία, την αντιπλημμυρική προστασία και την αντικλεπτική προστασία. Επιπλέον, το κτίριο πρέπει να είναι προστατευμένο από υγρασία και έντομα διότι αποτελούν μεγάλη απειλή για καλώδια και συσκευές. Έτσι μειώνεται η πιθανότητα στεγαστικού προβλήματος των συστημάτων της εταιρείας.

5. ΣΥΝΟΨΗ ΠΙΟ ΚΡΙΣΙΜΩΝ ΑΠΟΤΕΛΕΣΜΑΤΩΝ

Μέσα από την παραπάνω αναφορά, αντιληφθήκαμε 2 πολύ ευπαθή αγαθά από τα 40 συνολικά (5% του 40). Τα συγκεκριμένα αγαθά συνυπολογίζουν την κρισιμότητα της λειτουργίας τους όσο και την υψηλή ευπάθειά τους.

Αρχικά θα παρουσιαστεί το αγαθό με όνομα «CRM SERVER» και ID «CI-A-1010». Δεν επιλέχθηκε τυχαία διότι αποτελεί το πιο ευπαθές και πιο σημαντικό. Διαχειρίζεται τις αλληλεπιδράσεις της βιομηχανίας με τους πελάτες της αυτοματοποιώντας διεργασίες πωλήσεων που πραγματοποιούνται στο χώρο της βιομηχανίας (local sales). Είναι εξαιρετικά σημαντικό αγαθό διότι συνδυάζει όλους τους διακομιστές μαζί προκειμένου να προσφέρει τις καλύτερες υπηρεσίες στον πελάτη. Χρησιμοποιεί άμεσα τα δεδομένα από τις βάσεις δεδομένων, από τα ηλεκτρονικά μηνύματα, από τον σέρβερ που υιοθετεί την ιστοσελίδα της εταιρείας, από τον Radius/SNMP server που βοηθά στην ταυτοποίηση ενός πελάτη ή υπαλλήλου και παρακολουθεί ολόκληρο το δίκτυο. Επομένως εάν απειληθεί εκείνος, θα υποκύψουν πάρα πολύ εύκολα και οι υπόλοιποι διακομιστές. Με την ευπάθεια «Υπερχείλιση buffer της υπηρεσίας Windows Telnet», ο "εισβολέας" μπορεί να αποκτήσει πρόσβαση στον σέρβερ και να εκτελέσει κώδικα που μπορεί όχι μόνο να αποκτήσει πλήρη πρόσβαση στα συστήματα, αλλά και να καταστρέψει ή να κλέψει εντελώς όλα τα δεδομένα από τον συγκεκριμένο διακομιστή και από όλους τους συνεργαζόμενους. Γίνεται αντιληπτό ότι όσες περισσότερες υπηρεσίες είναι ενεργοποιημένες σε έναν διακομιστή, τόσο πιο ευάλωτος είναι. Συμπερασματικά, πρέπει να ελέγχονται όλα τα λειτουργικά συστήματα για πιθανών ενεργοποιημένες περιττές υπηρεσίες.

Τέλος θα παρουσιαστεί το αγαθό με όνομα «LAPTOP1» και ID «CI-A-1008». Δεν επιλέχθηκε τυχαία ούτε αυτό το αγαθό διότι αποτελεί το δεύτερο πιο ευπαθές. Φαίνεται ασήμαντο διότι είναι απλώς ένας φορητός υπολογιστής, όμως αποτελεί εργαλείο που διαθέτει ο διευθυντής. Είναι σημαντικό αγαθό διότι περιέχει διαχειριστικά έγγραφα, οικονομικές καταστάσεις, κωδικούς πρόσβασης και λοιπά δεδομένα που κατέχει ο διευθυντής για να επιβλέπει την ορθή λειτουργία της βιομηχανικής μονάδας. Χρησιμοποιεί άμεσα τα δεδομένα από όλους τους διακομιστές. Επιπλέον είναι πολύ πιο εκτεθειμένος στο διαδίκτυο διότι ίσως να έχει πρόσβαση και σε διαφορετικά δίκτυα. Επομένως εάν απειληθεί εκείνος, θα υποκύψει συνολικά όλη η εταιρεία. Με την ευπάθεια «Μη πιστοποιημένο και αξιόπιστο Antivirus», μπορεί εύκολα να κολλήσει κάποιο ιό (σοβαρό ή μη) ο οποίος μπορεί είτε να κλέψει κρίσιμα προσωπικά και επαγγελματικά δεδομένα είτε να τον θέσει εκτός λειτουργίας. Υπάρχει, επίσης, πιθανότητα χαρτογράφησης όλου του δικτύου της βιομηχανικής μονάδας, λαμβάνοντας όλες τις διευθύνσεις IP και τις πληροφορίες των διακομιστών και του εξοπλισμού κάνοντας τους εξαιρετικά ευάλωτους. Γίνεται αντιληπτό ότι όλες οι εταιρείες που επιθυμούν να προσφέρουν ασφαλείς και εξαιρετικής ποιότητας υπηρεσίες προς τους πελάτες, πρέπει να χρησιμοποιούν προγράμματα και Antivirus υψηλότατης αξιοπιστίας και αυθεντικότητας προκειμένου να εκμηδενιστούν τέτοιου είδους κίνδυνοι. Όσο ασφαλής και να είναι ένας σέρβερ, το ανθρώπινο λάθος ή η ανθρώπινη αμέλεια (phishing) έχουν πιο οδυνηρές επιπτώσεις από απευθείας επίθεση στον σέρβερ. Συμπερασματικά, η αγορά προγραμμάτων και Antivirus πρέπει να γίνεται με ιδιαίτερη προσοχή και μέριμνα.

Συνοψίζοντας το ΣΧΕΔΙΟ ΑΣΦΑΛΕΙΑΣ, παρατηρήσαμε πεπαλαιωμένα και μη ενημερωμένα λειτουργικά συστήματα στους υπολογιστές της εταιρείας. Αυτό πρέπει να διορθωθεί οπωσδήποτε διότι αναβαθμίζει αρκετά την ασφάλεια των επιμέρους συσκευών και συνεπώς γενικά το «τείχος προστασίας» απέναντι σε κάποιον που θέλει να αποκτήσει πρόσβαση στα συστήματα.