ΑΣΦΑΛΕΙΑ ΠΛΗΡΟΦΟΡΙΑΚΩΝ ΣΥΣΤΗΜΑΤΩΝ ΚΑΙ ΚΡΙΣΙΜΩΝ ΥΠΟΔΟΜΩΝ

ΣΧΕΔΙΟ ΑΣΦΑΛΕΙΑΣ

ΣΥΓΓΡΑΦΕΙΣ: Κωνσταντίνου Βασίλειος 3150085,Μελής Αλέξανδρος 3150102, Ιωάννης Φουρφουρής 3150190

ΕΡΓΑΣΙΑ ΧΕΙΜΕΡΙΝΟΥ ΕΞΑΜΗΝΟΥ 2018-19

Contents

Α1. ΕΙΣΑΓΩΓΗ

Κατά την διάρκεια της Δευτέρα 22 Οκτωβρίου του 2018 έως Παρασκευή 26 Οκτωβρίου του 2018 πραγματοποιήθηκε μια ανάλυση επικινδυνότητας της ασφάλειας της ξενοδοχειακής μονάδας 'Melis Luxury Hotel',το οποίο διαθέτει 30 δωμάτια και έχει προσωπικό 10 ατόμων . Η εκτίμηση είχε ζητηθεί από την 'Melis Luxury Hotel' με σκοπό να διαπιστωθεί η αποτελεσματικότητα των είδη υπαρχόντων μέτρων προστασίας και να εντοπιστούν νέες απειλές και ευπάθειες της επιχείρησης. Τα παρεχόμενα αποτελέσματα που προέκυψαν από την εκτίμηση ασφάλειας πρέπει να χρησιμοποιηθούν ως συνεισφορά στην διαδικασία διαχείρισης κινδύνου. Η ανάλυση περιλαμβάνει αρκετούς μέτριας μορφής κινδύνους οι οποίοι θα πρέπει να ληφθούν υπόψη από την διοίκηση.

Α1.1 Περιγραφή Εργασίας

Ο σκοπός αυτής της εργασία είναι να εκτιμήσει την αποδοτικότητα της ασφάλειας της ξενοδοχειακής μονάδας 'Melis Luxury Hotel', να εντοπιστούν πιθανές απειλές και ευπάθειες και να προταθούν τρόποι για την αντιμετώπιση , περιορισμό η/και την διαχείριση τους. Η παρούσα εργασία αποτελείται από 4 κεφάλαια.

Α1.1 Δομή παραδοτέου

Κεφάλαιο Α1 γίνεται μια αρχική εισαγωγή για τον σκοπό της εργασίας.

Κεφάλαιο Α2 περιγράφεται αναλυτικά η μεθοδολογία και τα βήματα πάνω στα οποία βασίζεται η εργασία καθώς επίσης καταγράφεται ο υλικός εξοπλισμός της επιχείρησης, τα λογισμικά που χρησιμοποιούνται, το δίκτυο, τα δεδομένα και τις διαδικασίες που διαχειρίζεται η επιχείρηση.

Κεφάλαιο Α3 στο κεφάλαιο αυτό παρατίθενται τα αγαθά, οι απειλές και οι ευπάθειες που προκύπτουν από την καταγραφή του πληροφοριακού συστήματος και παρουσιάζονται τα αποτελέσματα της αποτίμησης. Στη συνέχεια επεξηγούνται αναλυτικά και ταξινομούνται σύμφωνα με τον βαθμό επικινδυνότητας.

Κεφάλαιο Β2 σε αυτό το κεφάλαιο αναφέρονται προτεινόμενα μέτρα ασφαλείας που προκύπτουν από τα αγαθά, τις απειλές και τις ευπάθειες που εντοπίστηκαν στο προηγούμενο κεφάλαιο, καθώς επίσης κατατάσσονται ανά κατηγορία .

Κεφάλαιο Α4 αναφέρεται μια τελική σύνοψη της μελέτης και επισημαίνονται τα πιο κρίσιμα αποτελέσματα.

Α2. ΜΕΘΟΔΟΛΟΓΙΑ ΜΕΛΕΤΗΣ ΑΣΦΑΛΕΙΑΣ

Για τη Διαχείριση Επικινδυνότητας του Ανάλυση και Διαχείριση Επικινδυνότητας Ξενοδοχείου 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*

Α1.2 Περιγραφή Πληροφοριακού Συστήματος (ΠΣ) υπό έλεγχο

Στην ενότητα αυτή, καταγράφονται τα υφιστάμενα πληροφοριακά συστήματα του 'Melis Luxury Hotel ', τα οποία με το πέρας της μελέτης θα επικυρωθούν, αναβαθμιστούν ή σε κάποιες περιπτώσεις αντικατασταθούν.

Α1.2.1 Υλικός εξοπλισμός (hardware)

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

Σταθερός υπολογιστής (Workstation) μοντέλου Dell Optiplex 3060 SF με λειτουργικό windows 10 που βρίσκεται στο κεντρικό γραφείο με IP 192.168.1.12 και συνδέεται με wifi στο κεντρικό δίκτυο μέσω του Router B.

Εξυπηρετητής (file server) μοντέλου oracle file server με λειτουργικό windows server 2008 R2 ο όποιος βρίσκεται στο κεντρικό γραφείο με IP 192.168.1.8 και συνδέεται με ethernet στο κεντρικό δίκτυο μέσω του Router B.

Εξυπηρετητής (Broadband access server) μοντέλου Alcatel 7410 Broadband Access Server με λειτουργικό Windows Server 2008 R2 ο οποίος βρίσκεται στο κεντρικό γραφείο και έχει IP 192.168.1.3και συνδέεται με ethernet στο κεντρικό δίκτυο μέσω του Router B.

Εξυπηρετητής (Database server) μοντέλου Oracle Database Server με λειτουργικό Microsoft Windows 2016 Server SP1 ο οποίος βρίσκεται στο κεντρικό γραφείο με IP 192.168.1.56 και συνδέεται με ethernet στο κεντρικό δίκτυο μέσω του Router B.

Managed Switch μοντέλου D-Link DGS-1100-10MPP με λειτουργικό D-Link proprietary sorftware ο οποίος βρίσκεται στη περιοχή δωματίων και έχει IP 192.168.1.34 και συνδέεται με ethernet στο κεντρικό δίκτυο μέσω του Router A.

Managed Switch μοντέλου D-Link DGS-1100-10MPP με λειτουργικό D-Link proprietary sorftware ο οποίος βρίσκεται στο εστιατόριο και έχει IP 192.168.1.36 και συνδέεται με ethernet στο κεντρικό δίκτυο μέσω του Public Router .

Managed Switch μοντέλου D-Link DGS-1100-10MPP με λειτουργικό D-Link proprietary sorftware ο οποίος βρίσκεται στην αίθουσα συνεδριάσεων και έχει IP 192.168.1.37 και συνδέεται με ethernet στο κεντρικό δίκτυο μέσω του Router D.

Router μοντέλου TP-LINK Archer C69 v1 με λειτουργικό TP-Link Proprietary software το οποίο βρίσκεται στο κεντρικό γραφείο με IP 192.168.1.44 και συνδέεται με ethernet στο κεντρικό δίκτυο μέσω του Router B.

Router μοντέλου TP-LINK Archer C69 v1 με λειτουργικό TP-Link Proprietary software το οποίο βρίσκεται στην αίθουσα συνεδριάσεων με IP 192.168.1.47 και συνδέεται με ethernet στο κεντρικό δίκτυο μέσω του Router D.

Router μοντέλου TP-LINK Archer C69 v1 με λειτουργικό TP-Link Proprietary software το οποίο βρίσκεται στη περιοχή των δωματίων με IP 192.168.1.45 και συνδέεται με ethernet στο κεντρικό δίκτυο μέσω του Router A.

Network Hub μοντέλου LB-Link BL-S515 με LB-Link Proprietary software το οποίο βρίσκεται στο εστιατόριο με IP 192.168.1.14 και συνδέεται με ethernet στο κεντρικό δίκτυο μέσω του Public Router .

Wireless Access Point μοντέλου Cisco Aironet 38021 Radio με λειτουργικό Cisco proprietary software το οποίο βρίσκεται στο εστιατόριο και έχει IP 192.168.1.10 και συνδέεται με ethernet στο κεντρικό δίκτυο μέσω του Public Router .

Wireless Access Point μοντέλου Cisco Aironet 38021 Radio με λειτουργικό Cisco proprietary software το οποίο βρίσκεται στην αίθουσα συνεδριάσεων και έχει IP

192.168.1.16 και συνδέεται με ethernet στο κεντρικό δίκτυο μέσω του Managed Swich .

Wireless Access Point μοντέλου Cisco Aironet 38021 Radio με λειτουργικό Cisco proprietary software το οποίο βρίσκεται στο κεντρικό γραφείο και έχει IP 192.168.1.17 και συνδέεται με ethernet στο κεντρικό δίκτυο μέσω του Router B .

Wireless Access Point μοντέλου Cisco Aironet 38021 Radio με λειτουργικό Cisco proprietary software το οποίο βρίσκεται στη περιοχή των δωματίων και έχει IP 192.168.1.18 και συνδέεται με ethernet στο κεντρικό δίκτυο μέσω του Router A.

Fast Ethernet Switch μοντέλου FS108 32 Port Fast Ethernet Switch με λειτουργικό NETGEAR Proprietary software το οποίο βρίσκεται στη περιοχή των δωματίων με IP 192.198.1.11 και συνδέεται με ethernet στο κεντρικό δίκτυο μέσω του Router A .

Fast Ethernet Switch μοντέλου FS108 32 Port Fast Ethernet Switch με λειτουργικό NETGEAR Proprietary software το οποίο βρίσκεται στη περιοχή των δωματίων με IP 192.198.1.9 και συνδέεται με ethernet στο κεντρικό δίκτυο μέσω του Router B .

Public network Router μοντέλου FS110 Network Router με λειτουργικό NETGEAR proprietary softwarer με IP 192.168.1.93 το οποίο βρίσκεται στο server room και συνδέεται με οπτική ίνα στον πάροχο.

Φορητός υπολογιστής (Laptops) μοντέλου Apple MacBook Pro 13.3 με λειτουργικό MAC-OS που βρίσκεται στο εστιατόριο με IP 192.168.1.30 και συνδέεται με wifi στο κεντρικό δίκτυο μέσω του Public Router.

Φορητός υπολογιστής (Laptops) μοντέλου Apple MacBook Pro 13.3 με λειτουργικό MAC-OS που βρίσκεται στη περιοχή δωματίων με IP 192.168.1.31 και συνδέεται με wifi στο κεντρικό δίκτυο μέσω του Router A.

Φορητός υπολογιστής (Laptops) μοντέλου Apple MacBook Pro 13.3 με λειτουργικό MAC-OS που βρίσκεται στην αίθουσα συνεδριάσεων με IP 192.168.1.32 και συνδέεται με wifi στο κεντρικό δίκτυο μέσω του Router D.

Τείχος προστασίας (Firewall) μοντέλου Fortinet-Fortinet-100D με λειτουργικό Fortinet propietary software το οποίο βρίσκεται στο κεντρικό γραφείο με IP 192.168.1.13 και συνδέεται με ethernet στο κεντρικό δίκτυο μέσω του Router B.

<u>Παραδοχή</u>
Εξυπηρετητής (Web Server) μοντέλου T2015 RAQ WEB με λειτουργικό Apache LDAP Studio 0.6.0 το οποίο βρίσκετε στο κεντρικό γραφείο με IP 192.168.1.94 και συνδέεται με ethernet στο κεντρικό δίκτυο μέσω του Router B.

<u>Παραδοχή</u>
Εξυπηρετητής (mail Server) μοντέλου QB Server Xpress Mail Xpress Console με λειτουργικό Ubuntu 12.04.5 LTS το οποίο βρίσκεται στο κεντρικό γραφείο με IP 192.168.1.96 και συνδέεται με ethernet στο κεντρικό δίκτυο μέσω του Router B.

<u>Παραδοχή</u>

Σταθερά τηλέφωνα(VoIP) μοντέλου Cisco Unified IP Phone 7912G τα οποία βρίσκονται διάσπαρτα στα δωμάτια , γραφείο εστιατόριο, αίθουσα συνεδριάσεων με IP από 192.168.1.100 έως 192.168.1.150 και συνδέεται με ethernet στο κεντρικό δίκτυο.

Παραδοχή
Εκτυπωτές μοντέλου HP LaserJet Pro MFP M426fdw 16.0.18002.756-501 Driver-Product Software 16.0.18002.756-501 τα οποία βρίσκονται διάσπαρτα στα δωμάτια , γραφείο εστιατόριο, αίθουσα συνεδριάσεων με IP από 192.168.1.201 έως 192.168.1.206 και συνδέεται με ethernet στο κεντρικό δίκτυο.

Παραδοχή
Σταθερός υπολογιστής (Workstation) μοντέλου Dell Optiplex 3060 SF με λειτουργικό windows 10 που βρίσκεται στην κεντρική reseption με IP 192.168.1.220 και συνδέεται με ethernet στο κεντρικό δίκτυο μέσω του Router A.

Παραδοχή
Ups που βρίσκεται στο κεντρικό γραφείο.

A1.2.2 Λογισμικό και εφαρμογές

Windows 10 το οποίο βρίσκεται στο σταθερό υπολογιστή (workstation).

Windows Server 2008 R2 το οποίο βρίσκεται στον File Server και στον Broadband Access Server.

Microsoft Windows 2016 Server SP1 το οποίο βρίσκεται Database Server.

D-Link proprietary software το οποίο βρίσκεται στους Manage Switches.

TP-Link proprietary software το οποίο βρίσκεται στους Routers.

Cisco proprietary software το οποίο βρίσκεται στους Wireless Access Points .

LB-Link proprietary software το οποίο βρίσκεται στα Network Hubs.

NETGEAR proprietary software το οποίο βρίσκεται στα Fast Ethernet Switches και στο Public Network Router.

MAC-OS το οποίο βρίσκεται στα Laptops.

My Sql το οποίο βρίσκεται στον Database Server.

Παραδοχή
Microsoft Office το οποίο βρίσκεται στο Workstation και στα Laptops.

Παραδοχή
Chrome Browser το οποίο βρίσκεται στο Workstation και στα Laptops.

Παραδοχή
Postfix το οποίο βρίσκεται στον Mail Server.

Παραδοχή
Ubuntu 12.04.5 LTS το οποίο βρίσκεται στον Mail Server.

Παραδοχή
Apache2 το οποίο βρίσκεται στον Web Server.

Παραδοχή
PHP5 το οποίο βρίσκεται στον Web Server.

Παραδοχή
Λογισμικό κρατήσεων το οποίο βρίσκεται στο Workstation.

Παραδοχή
Λογισμικό Πληρωμών το οποίο βρίσκεται στο Workstation.

A1.2.3 Δίκτυο

Τείχος προστασίας (Firewall) μοντέλου Fortinet-Fortinet-100D με λειτουργικό Fortinet proprietary software το οποίο βρίσκεται στο κεντρικό γραφείο με IP 192.168.1.13

Managed Switch μοντέλου D-Link DGS-1100-10MPP με λειτουργικό D-Link proprietary sorftware ο οποίος βρίσκεται στη περιοχή δωματίων και έχει IP 192.168.1.34

Managed Switch μοντέλου D-Link DGS-1100-10MPP με λειτουργικό D-Link proprietary sorftware ο οποίος βρίσκεται στο εστιατόριο και έχει IP 192.168.1.36

Managed Switch μοντέλου D-Link DGS-1100-10MPP με λειτουργικό D-Link proprietary sorftware ο οποίος βρίσκεται στην αίθουσα συνεδριάσεων και έχει IP 192.168.1.37

Router μοντέλου TP-LINK Archer C69 v1 με λειτουργικό TP-Link Proprietary software το οποίο βρίσκεται στο κεντρικό γραφείο με IP 192.168.1.44

Router μοντέλου TP-LINK Archer C69 v1 με λειτουργικό TP-Link Proprietary software το οποίο βρίσκεται στην αίθουσα συνεδριάσεων με IP 192.168.1.47

Router μοντέλου TP-LINK Archer C69 v1 με λειτουργικό TP-Link Proprietary software το οποίο βρίσκεται στη περιοχή των δωματίων με IP 192.168.1.45

Network Hub μοντέλου LB-Link BL-S515 με LB-Link Proprietary software το οποίο βρίσκεται στο εστιατόριο με IP 192.168.1.14

A1.2.4 Δεδομένα

Παραδοχή
Χάρτινα έγγραφα τα οποία βρίσκονται στο κεντρικό γραφείο.

Παραδοχή
Δεδομένα πελατών ξενοδοχείου (Hotel Guest Data) (Όνομα, Επίθετο , αριθμός πιστωτικής κάρτας, ημερομηνία γέννησης, αριθμός ταυτότητας ,διεύθυνση, τηλέφωνο ,email, Αριθμός δωματίου , Φύλο, κωδικός(αν από online κράτηση) ,IP (αν από online κράτηση),) τα οποία βρίσκονται στον DataBase Server .

Παραδοχή
Δεδομένα υπαλλήλων ξενοδοχείου (Hotel Employee Data) (Όνομα, Επίθετο , αριθμός λογαριασμού κάρτας, ημερομηνία γέννησης ,αριθμός ταυτότητας , ΑΦΜ, ΑΜΚΑ, διεύθυνση , τηλέφωνο ,email , Ιατρικά στοιχεία (αναπηρία δυσλεξία) , Ποινικό μητρώο , Στρατολογικές υποχρεώσεις , μισθοδοσία) τα οποία βρίσκονται στον DataBase Server .

Παραδοχή
Λογιστικά δεδομένα ξενοδοχείου τα οποία βρίσκονται στον DataBase Server .

Παραδοχή
Δεδομένα λειτουργίας ξενοδοχείου τα οποία βρίσκονται στον DataBase Server .

A1.2.5 Διαδικασίες

Διαδικασίες πληρωμής (Payment Process) που βρίσκονται στο Σταθερό υπολογιστή (Workstation) στο κεντρικό γραφείο

Διαδικασίες κρατήσεων (Reservation Process) που βρίσκονται στο Σταθερό υπολογιστή (Workstation) στο κεντρικό γραφείο

Παραδοχή
Διαδικασίες παραγγελίας προμηθειών που βρίσκονται στο Σταθερό υπολογιστή (Workstation) στο κεντρικό γραφείο

A3.ΑΠΟΤΙΜΗΣΗ ΠΣ ΚΑΙ ΕΓΚΑΤΑΣΤΑΣΕΩΝ ΕΡΓΑΣΙΑΣ ΟΠΑ

Στην ενότητα αυτή γίνεται μια αποτίμηση του πληροφοριακού συστήματος καταγράφεται ο εξοπλισμός, τα αγαθά ,οι ευπάθειες και οι απειλές .

A1.3 Αγαθά που εντοπίστηκαν

- Δεδομένα υπαλλήλων ξενοδοχείου
- Δεδομένα πελατών ξενοδοχείου
- Εξυπηρετητής (Database server)

- Σταθεροί υπολογιστές (Workstation)
- Εξυπηρετητής (Broadband access server)
- Εξυπηρετητής (File server)
- Δεδομένα προμηθειών
- Λογιστικά δεδομένα
- Προσωπικό ξενοδοχείου
- Back ups
- Διαδικασίες πληρωμής
- Διαδικασίες κρατήσεων
- Διαδικασίες παραγγελίας προμηθειών
- Πελάτες
- Χάρτινα έγγραφα
- Εξυπηρετητής (Web Server)
- Εξυπηρετητής (Mail Server)
- Routers
- Φορητοί υπολογιστές (Laptops)
- Switches
- Hubs
- WiFi
- Ethernet's
- Δωμάτια
- Τοπολογία δικτύου
- Υπάρχοντα μετρά ασφάλειας
- Εκτυπωτές
- Κτιριακή εγκατάσταση

(Σημείωση)Τα Extra αγαθά που προσθέσαμε είναι:
- Δεδομένα υπαλλήλων ξενοδοχείου
- Δεδομένα πελατών ξενοδοχείου
- Δεδομένα προμηθειών
- Λογιστικά δεδομένα
- Προσωπικό ξενοδοχείου
- Back ups
- Διαδικασίες παραγγελίας προμηθειών
- Πελάτες
- Χάρτινα έγγραφα
- Εξυπηρετητής (Web Server)
- Εξυπηρετητής (Mail Server)
- Δωμάτια
- Τοπολογία δικτύου
- Υπάρχοντα μετρά ασφάλειας
- Εκτυπωτές
- Κτιριακή εγκατάσταση

A1.4 Απειλές που εντοπίστηκαν

Σταθεροί υπολογιστές (Workstation)

Εγκατάστασή ιομορφικού λογισμικού,
Είσοδος στο σύστημα μέσω wifi,
Πρόσβαση στις διαδικασίες κράτησης ,παραγγελιών και πληρωμής,
Παρακολούθηση διαδικασιών,
Αποτυχία λογισμικού πληρωμών, κρατήσεων, παραγγελιών (κακογραμμένα).

Προσωπικό

Πλαστοπροσωπία : προσωποποίηση πελάτη με σκοπό άντληση πληροφοριών του πελάτη, κατάχρηση πόρων του συστήματος ,
Ανθρώπινο λάθος.

Εξυπηρετητής (Database server)

Υποκλοπή ,επεξεργασία ,τροποποίηση δεδομένων ,
Αποτυχία λογισμικού mySql ,
Μη εξουσιοδοτημένη πρόσβαση με SqlInjection.

Τεχνική βλάβη/Αποτυχία Hardware.

Αποτυχία λειτουργίας κεντρικής μονάδας κλιματισμού ,
Αποτυχία Hardware Workstation, Server, Router, σκληρών δίσκων, φορητών υπολογιστών.

Φυσική κλοπή

Μηχανημάτων στο γραφείο , εγγράφων, backups , φορητών υπολογιστών.

Ηθελημένη ζημιά από προσωπικό σε

Μηχανήματα και έγγραφα

Ακούσια ζημία από προσωπικό σε

Μηχανήματα και έγγραφα

Πολύωρη πτώση ρεύματος.

Καταστροφή μηχανημάτων , εγγράφων και κτιρίου από πυρκαγιά .

A1.5 Ευπάθειες που εντοπίστηκαν

(1) Workstation: Απόκτηση πρόσβασης ως admin λόγω remote code execution Windows 10 με Microsoft Windows PDF βιβλιοθήκη.

(2) Apple MacBook Pro 13.3: Απόκτηση πρόσβασης λόγω memory coraption Apple Safari Multiple Memory Corruptio Vulnerabilities, έλλειψη antivirus.

(3) Εξυπηρετητής (Broadband access server): (Execute CodeOverflow)

(4) Εξυπηρετητής (File server): (Execute CodeOverflow)

(5) Εξυπηρετητής (Database server): (Execute Code Overflow) sql injection μέσω της σελίδας.

(6) Fortinet (firewall): ( )

(7) Routers: Έλλειψη ενημερώσεων και εργοστασιακούς κωδικούς

(8) Switch: Έλλειψη ενημερώσεων και εργοστασιακούς κωδικούς

(9) Χάρτινα έγγραφα: Βρίσκονται σε φανερά σημεία

(10) Έλλειψη εφεδρικού κλιματιστικού.

(11) Εύκολη πρόσβαση του συνόλου του προσωπικού στο γραφείο συνεπώς και στα μηχανήματα που βρίσκονται εκεί.

(12) Έλλειψη λογισμικού προστασίας AntiVirus σε Workstation υπολογιστές.

(13) Έλλειψη πολιτικής αναβάθμισης συστημάτων.

(14) Έλλειψη κουλτούρας ασφαλείας.

(15) Μη τήρηση πολίτικης ασφαλείας.

(16) Mac os μη αναβαθμισμένο λειτουργικό σύστημα και εφαρμογές.

(17) Έλλειψη εφεδρικού κλιματιστικού.

(18) Έλλειψη εφεδρικού router.

(19) Έλλειψη ηλεκτρογεννήτριας Για περίπτωση πολύωρης πτώσης ρεύματος .

(20) Έλλειψη συστήματος αναγνώρισης και καταγραφής προσωπικού εντός και εκτός του γραφείου.

(21) Έλλειψη ξεχωριστού δωματίου Εξυπηρετητών (ServerRoom).

(22) Έλλειψη σύμβασης συντήρησης λογισμικού με την κατασκευάστρια εταιρεία.

(23) Έλλειψη διαθέσιμων ανταλλακτικών πχ σκληροί δίσκοι .

(24) Έλλειψη κρυπτογραφημένων δεδομένων backup.

(25) Χρήση κωδικών passwords με μικρό μήκος.

(26) Έλλειψη hashing κωδικών.

(27) Workstation: δυνατότητα χρήσης υπηρεσιών χωρίς ταυτοποίηση.

(28) Τοπολογία δικτύου: Σύνδεση όλων των χρηστών στο ίδιο δίκτυο.

(29) Μη κρυπτογραφημένα πακέτα στο δίκτυο.

A1.6 Αποτελέσματα αποτίμησης

Στον παρακάτω πίνακα παρουσιάζονται αναλυτικά οι επιπτώσεις που θα δημιουργηθούν στην επιχείρηση αν υπάρξει εκμετάλλευση των ευπαθειών του κάθε αγαθού. Για την καλύτερη κατανόηση του πίνακα βαθμολογούνται οι επιπτώσεις με αριθμούς κλίμακας από το 1 μέχρι το 10 , επιπλέον όπου υπάρχουν κενά σημαίνει ότι δεν υπάρχει αντίκτυπο στο συγκεκριμένο αγαθό. Επιπρόσθετα ο βαθμός επίπτωσης μπορεί να αυξηθεί με τον συνδυασμό δύο η περισσότερων ευπαθειών. Χαρακτηριστικό παράδειγμα αποτελεί η απώλεια της διαθεσιμότητας του Firewall για 12 ώρες με σχετικά μικρή επίπτωση στην επιχείρηση . Αν όμως συνδυαστεί με σκόπιμη αλλοίωση του Public Router τότε είναι πιο εύκολο να πραγματοποιηθεί το exploit από κάποιο κακόβουλο παράγοντα με αποτέλεσμα την αύξηση των επιπτώσεων.

	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
Database server		1	2	4	6	8	9	10	6	7	4	6	3		7		6	7	4	5	5	7	3	
Public Router Cisco 2911		1	2	4	5	6	7	8	4	4	1				1	1	3	3	1	1	4	5	1	2
Hotel Guest Data		1	2	4	6	8	9	10	6	8	3	5	4	6	8	1	6	6	2	3	6	7	2	2
Web server		1	2	3	4	5	6	7	5	7	1	5	2	3	4	1	6	6	2	3	6	6	2	1

	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
Workstation		1	2	5	7	8	9	10	5	8	2	5	3	3	7		5	5	2	6	6	6	3	3
MacBook Pro 13.3					1	2	5	6	4	1	1	2	1	1	5		2	2	1	2	5	4	2	2
Broadband access server		1	2	5	7	8	9	10	5	3	1	3	1	1	2	2	5	5	2	6	7	7	3	3
Fortinet (firewall)	1	2	3	4	7	8	8	9	5	7	1	2	1	6	6		3	3	3	4	6	6	2	2
Routers			1	2	3	5	6	7	4	4	1	4	1	1	1	1	3	3	1	1	4	5	1	2
Paper documents				1	2	3	4	10	8	9	5	8	5	6	9									
Personel	7	8	9	9	9	9	9	10	6	3	3	5												
Servers	1	2	4	6	8	9	10	6	7	4	6	3		7		6	7	4	5	5	7	3		1

	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 ακολου-θίας μηνυμάτων
Process	1	2	4	5	7	8	9	10	6	8	2	8	3	4	9	5	6	7	3	4	6	6	3	2
Back ups	2	3	3	3	6	6	6	10	8	9	2	8	6	7	9									

Β2. 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 'Melis Luxury

Α1 Προσωπικό – Προστασία Διαδικασιών Προσωπικού

Διεξαγωγή ενημερωτικών σεμιναρίων για την εφαρμογή της Πολιτικής Ασφάλειας σε όλους τους χρήστες του ΠΣ.(αντιμετώπιση ευπαθειών 14,15)

Έκτακτες ενημερώσεις για οποιαδήποτε αλλαγή των διαδικασιών της Πολιτικής Ασφάλεια και των μέτρων ασφαλείας.(αντιμετώπιση ευπαθειών 14,15)

Εκπαίδευση όλων των χρηστών ως προς την δημιουργία κουλτούρας ασφάλειας

.(αντιμετώπιση ευπαθειών 14,15)

Συνεχή ενημέρωση για νέες λύσεις και προϊόντα ασφάλειας. (αντιμετώπιση ευπαθειών 14,15)

Α2 Ταυτοποίηση και αυθεντικοποίηση

Χρήση κάρτας προσωπικού τεχνολογίας RFID για την είσοδο έξοδο στο κεντρικό γραφείο και στους υπολοίπους χώρους.(αντιμετώπιση ευπαθειών 11)

Χρήση συνθηματικών τουλάχιστον 8 χαρακτήρων με τουλάχιστον 1 αριθμό 1 κεφαλαίο και ένα.(αντιμετώπιση ευπαθειών 14,25)

Τακτική αλλαγή και αλλαγή μετά αμέσως μετά από υποψία αποκάλυψης.(αντιμετώπιση ευπαθειών 14,15)

Ασφαλής χορήγηση προσωρινών passwords με λογική αλλαγής τους από τους ίδιους τους χρήστες σε επόμενη φάση.(αντιμετώπιση ευπαθειών 14,15)

Αλλαγή προκαθορισμένων από τον κατασκευαστή (default) συνθηματικών (πχ .routers).(αντιμετώπιση ευπαθειών 7,8,14,15)

Αποθήκευση κωδικών μόνο σε κρυπτογραφημένη/hashing μορφή(αντιμετώπιση ευπαθειών 14,26).

Περιορισμός του αριθμού των προσπαθειών αυθεντικοποίησης και ενημέρωση του χρήστη.(αντιμετώπιση ευπαθειών 14,15)

Περιοδική αναθεώρηση και έλεγχος των δικαιωμάτων πρόσβασης στο σύστημα των χρηστών. Η περίοδος των 6 μηνών συνιστάται. Ιδίως σε ότι αφορά δικαιώματα πρόσβασης σε εξαιρετικής σημασίας πόρους του συστήματος η περίοδος των 3 μηνών θεωρείται κατάλληλη.(αντιμετώπιση ευπαθειών 14,15)

A3 Έλεγχος προσπέλασης και χρήσης πόρων

Χρήση κάρτας προσωπικού τεχνολογίας RFID για την είσοδο έξοδο στο κεντρικό γραφείο και στους υπολοίπους χώρους.(αντιμετώπιση ευπαθειών 14,11)

Περιορισμός πρόσβασης μόνο σε εξουσιοδοτημένους χρήστες.(αντιμετώπιση ευπαθειών 14,11)

Καθορισμός διαφορετικών κατηγοριών χρηστών με συγκεκριμένα και αυστηρά καθορισμένα δικαιώματα (αντιμετώπιση ευπαθειών 14,15).

Δυνατότητα ενεργοποίησης του logging σε επίπεδο βάσης δεδομένων με ταυτόχρονη αποθήκευση των log αρχείων στο λειτουργικό σύστημα και με δυνατότητα πρόσβασης σε αυτά μόνο από εξουσιοδοτημένα πρόσωπα.(αντιμετώπιση ευπαθειών 14,15)

A4 Διαχείριση εμπιστευτικών δεδομένων

Χρήση κρυπτογραφίας για διαχείρισης εμπιστευτικών δεδομένων.(αντιμετώπιση ευπαθειών 14,15)

Χρήση Hash για την αποθήκευση password.(αντιμετώπιση ευπαθειών 14,15)

Αποθήκευση χάρτινων δεδομένων σε ελεγχόμενους χορούς με περιορισμένη πρόσβαση.(αντιμετώπιση ευπαθειών 14,15)

Καθημερινή δημιουργία backups.(αντιμετώπιση ευπαθειών 14,15)

Τα αντίγραφα ασφάλειας θα πρέπει να φυλάσσονται σε διαφορετικούς χώρους από τον χώρο που φιλοξενείται και λειτουργεί το κύριο πληροφοριακό σύστημα.(αντιμετώπιση ευπαθειών 14,15)

A5 Προστασία από τη χρήση υπηρεσιών από τρίτους

Έλεγχος ταυτοποίησης και αυθεντικοποίησης για την χρήση υπηρεσιών (πληρωμής κράτησης ,προμηθειών).(αντιμετώπιση ευπαθειών 14,15)

Παραχώρηση πρόσβασης σε υπηρεσίες μόνο σε εξουσιοδοτημένα άτομα.(αντιμετώπιση ευπαθειών 14,27)

Δυνατότητα χρήσης των υπηρεσιών μόνο από μηχανήματα εντός του δικτύου.(αντιμετώπιση ευπαθειών 14)

A6 Προστασία λογισμικού

Σύναψη σύμβασης συντήρησης λογισμικού.(αντιμετώπιση ευπαθειών 22)

Δημιουργία backup προγραμμάτων λογισμικού σε χρήση.(αντιμετώπιση ευπαθειών 24)

Εγκατάσταση λογισμικού Antivirus.(αντιμετώπιση ευπαθειών 1,3,4,5,12,14,15)

Εκτέλεση ευαίσθητου λογισμικού σε virtual machine(sandbox).(αντιμετώπιση ευπαθειών)

Διαρκής ενημέρωση και αναβάθμιση (update, patching) όλων των συστημάτων.(αντιμετώπιση ευπαθειών 1,2,3,4,5,6,7,8,13,14,15,16)

A7 Διαχείριση ασφάλειας δικτύου

Σπάσιμο του δικτύου σε υποδίκτυα. (αντιμετώπιση ευπαθειών 28)

Συστηματική ενημέρωση λογισμικού switches, hub, router, firewall.(αντιμετώπιση ευπαθειών 6,7,8,14,)

Φιλτράρισμα εξερχόμενης κίνησης δικτύου.(αντιμετώπιση ευπαθειών 14,25)

Κρυπτογραφία πακέτων(αντιμετώπιση ευπαθειών 14,29)

A8 Προστασία από ιομορφικό λογισμικό

Εγκατάσταση λογισμικού Antivirus .(αντιμετώπιση ευπαθειών 1,2,3,4,5,12)

Χρήση λογισμικού ids (intrusion detection software).(αντιμετώπιση ευπαθειών 1,2,3,4,5,6,14)

A9 Ασφαλής χρήση διαδικτυακών υπηρεσιών

Χρήση προτύπου https στην σελίδα του ξενοδοχείου.(αντιμετώπιση ευπαθειών)

Αποκλεισμός πρόσβαση σε σελίδες χωρίς https.

A10 Ασφάλεια εξοπλισμού

Δημιουργία ξεχωριστού δωματίου για εξυπηρετητές (Server room) .(αντιμετώπιση ευπαθειών 21,)

Εγκατάσταση εφεδρικού κλιματισμού.(αντιμετώπιση ευπαθειών 17)

Περιορισμός πρόσβασης μόνο σε εξουσιοδοτημένους χρήστες.(αντιμετώπιση ευπαθειών 14,15,11)

Πρόσληψη αρμοδίου ασφαλείας.(αντιμετώπιση ευπαθειών 14,15)

Εγκατάσταση ηλεκτρογεννήτριας.(αντιμετώπιση ευπαθειών 19)

Εφεδρικός εξοπλισμός για κρίσιμο υλικό εξοπλισμό(πχ.router, hard drive). (αντιμετώπιση ευπαθειών ,17,18,23)

Είναι απαραίτητο να υπάρχει ένα Service Level Agreements (SLA) με προμηθευτές για τους χρόνους αποκατάστασης των διαφόρων συστημάτων μετά από βλάβες / αναβαθμίσεις / αντικαταστάσεις .

A11 Φυσική ασφάλεια κτιριακής εγκατάστασης

Αποφυγή εγκατάστασης εξοπλισμού κοντά σε εύφλεκτα υλικά Εγκατάσταση κλειστού συστήματος παρακολούθησης.(αντιμετώπιση ευπαθειών 11,)

Απαγόρευση καπνίσματος στις εγκαταστάσεις του εξοπλισμού.

Χρήση κλιματισμού για την διατήρηση της ενδεικνυόμενης θερμοκρασίας λειτουργίας των ευαίσθητων συστημάτων.(αντιμετώπιση ευπαθειών 18)

Θα πρέπει κατάλληλα να οριστούν υπεύθυνα άτομα για τις δραστηριότητες που αφορούν κτιριακές επιδιορθώσεις και παροχή πληροφοριών για επικοινωνία μαζί τους.

A4. ΣΥΝΟΨΗ ΠΙΟ ΚΡΙΣΙΜΩΝ ΑΠΟΤΕΛΕΣΜΑΤΩΝ

Μετά, από την ανάλυση επικινδυνότητας των αγαθών του ξενοδοχείου, καταλήξαμε στα παρακάτω αγαθά με την υψηλότερη επικινδυνότητα . Αρχικά ιδιαίτερη κρισιμότητα παρουσιάζεται στα δεδομένα των επισκεπτών στα οποία περιέχονται τα στοιχεία του πελάτη και ο αριθμός της πιστωτικής κάρτας , καθώς επίσης τα δεδομένα των υπαλλήλων στα οποία εμπεριέχονται τα ιατρικά δεδομένα. Η ευπάθεια σε αυτή την περίπτωση είναι ότι τα δεδομένα αυτά βρίσκονται στη βάση δεδομένων σε μη κρυπτογραφημένη μορφή που σημαίνει ότι ένας κακόβουλος χρήστης μπορεί πολύ εύκολα να τα παρακολουθήσει ακόμα και να τα τροποποιήσει με την είσοδο του στο σύστημα .Η επιπτώσεις της απειλής που αναφέρθηκε παραπάνω έχουν οικονομικό αντίκτυπο για την επιχείρηση αλλά εξίσου υποβαθμίζουν την φήμη και την αξιοπιστία της, επιπρόσθετα εκτίθενται τα προσωπικά δεδομένα των πελατών και υπαλλήλων. Αρκετά κρίσιμη χαρακτηρίζεται και η διαδικασία κρατήσεων η οποία αποτελείται από το λογισμικό το οποίο χρησιμοποιεί το ξενοδοχείο για να πραγματοποιούνται οι κρατήσεις .Η ευπάθεια του συγκεκριμένου αγαθού αποδίδεται στην έλλειψη συμβολαίου με την κατασκευάστρια εταιρία του λογισμικού το οποίο να εγγυάται την διατήρηση της σωστής λειτουργίας του και την επιδιόρθωση σε πιθανές δυσλειτουργίες. Η εφαρμογή κρατήσεων είναι πολύ σημαντικό κομμάτι της λειτουργίας του ξενοδοχείου, έτσι σε ενδεχόμενη βλάβη της δεν θα μπορούν να πραγματοποιηθούν οι ηλεκτρονικές οικονομικές συναλλαγές των κρατήσεων κάτι το οποίο θα έχει τεράστιες οικονομικές επιπτώσεις ειδικά σε τουριστική περίοδο . Τέλος αξίζει να σημειωθεί η κρισιμότητα της κατάστασης των server στους οποίους είναι αποθηκευμένες όλες οι πληροφορίες που διαχειρίζεται η επιχείρηση. Με κύρια ευπάθεια την απουσία εγκατεστημένου λογισμικού antivirus κάτι το οποίο τους καθιστά ευάλωτους στην εγκατάσταση ιομορφικών λογισμικών. Ένα πιθανό αποτέλεσμα της επίθεσης από κακόβουλο λογισμικό θα ήταν η αχρήστευση του πληροφοριακού συστήματος της

επιχείρησης που βρίσκεται στον server κάτι το οποίο θα είχε μεγάλη οικονομική ζημία και θα προκαλούσε δυσλειτουργία στο ξενοδοχείο.

Πηγές που χρησιμοποιήθηκαν.

https://www.cvedetails.com/

https://www.iso.org/isoiec-27001-information-security.html

https://www.nist.gov/