ΑΣΦΑΛΕΙΑ ΠΛΗΡΟΦΟΡΙΑΚΩΝ ΣΥΣΤΗΜΑΤΩΝ ΚΑΙ ΚΡΙΣΙΜΩΝ ΥΠΟΔΟΜΩΝ

ΣΧΕΔΙΟ ΑΣΦΑΛΕΙΑΣ

ΣΥΓΓΡΑΦΕΙΣ:

Ευάγγελος Πατσουράκος - 3130167
Αντώνης Παναγιώτης Γερογιαννάκης - 3130034

ΕΡΓΑΣΙΑ ΧΕΙΜΕΡΙΝΟΥ ΕΞΑΜΗΝΟΥ 2018

Contents

A1. ΕΙΣΑΓΩΓΗ

Η πρόσφατη ανάκαμψη του ξενοδοχειακού κλάδου έφερε έσοδα στις ξενοδοχειακές επιχειρήσεις αλλά ταυτόχρονα ο όγκος των δεδομένων(πληροφοριών) αυτών απέκτησε μεγάλη αξία. Ως αποτέλεσμα, μια διείσδυση από μη εξουσιοδοτημένους χρήστες στις δομές και πληροφορίες του ξενοδοχείου θα αποτελέσουν μεγάλη ζημία στην επιχείρηση καθώς και στην ομαλή της λειτουργία. Για να αποφευχθεί μια τέτοια κατάσταση πρέπει να γίνεται Risk analysis πάνω από τα πληροφοριακά συστήματα των ξενοδοχείων. Συνεπώς η παρούσα αναφορά αποτελεί μια παρουσίαση ενός πλήρους σχεδίου ασφάλειας για τον πληροφοριακό σύστημα του ξενοδοχείου “Relax and Joy”, το οποίο διαθέτει αγαθά που χρήζουν προστασία από πιθανές απειλές.

A1.1 Περιγραφή Εργασίας

Η διεξαγωγή αυτής της αναφοράς θα γίνει με βάση τη μέθοδο ISO2700K για μια ξενοδοχειακή μονάδα, η οποία διαχειρίζεται έναν μεγάλο όγκο ευαίσθητων πληροφοριών που αφορούν τον οργανισμό αλλά και τους πελάτες. Η εκτίμηση κινδύνου δεν αφορά τη δημιουργία τεράστιων ποσοτήτων γραφικής εργασίας, αλλά τον εντοπισμό λογικών μέτρων για τον έλεγχο των κινδύνων στον χώρο εργασίας. Το ξενοδοχείο δεν έχει λάβει μέτρα για την προστασία των υποδομών, διαδικασιών και λογισμικού της αλλά η εκτίμησή μας για τον κίνδυνο θα βοηθήσει το κατάλυμα να αποφασίσει αν έχει καλύψει όλα όσα χρειάζεστε. Επίσης, για την πιο εμπεριστατωμένη πρόβλεψη και των ακριβή αποτελεσμάτων, η ομάδα μας διεξήγε συνέντευξη στο προσωπικό της επιχείρησης και κατέληξε σε ένα διάγραμμα του δικτύου των αγαθών του καταλύματος σε τέσσερις υποκατηγορίες (Room area, Office, Hotel dining area, Hotel Conference room) που εμφανίζεται στην ενότητα «A2.1». Σύμφωνα με τις παραπάνω συνεντεύξεις εξουσιοδότηση για κάθε “end-point” μηχάνημα κατέχουν μόνο οι αρμόδιοι υπάλληλοι (πχ. το “Office workstation” μόνο ο υπάλληλος που τον χρησιμοποιεί). Επιπλέον, το “Office” βρίσκεται στον τρίτο όροφο του ξενοδοχείου μαζί με το “Hotel Conference room”. Εν συνεχεία, το Hotel dining area στον πρώτο όροφο του ξενοδοχείου. Εν τέλει, το “Room Area” βρίσκεται στον δεύτερο όροφο και ενώ από πάνω είναι τα δωμάτια του καταλύματος που τροφοδοτούνται από το “Room Area”.

A1.2 Δομή παραδοτέου

Η αναφορά για το πληροφοριακό σύστημα του ξενοδοχείου έχει αποδομηθεί κατάλληλα σε ενότητες. Εξαιτίας αυτού, διαθέτει την κατάλληλη συνοχή και κατανόηση για οποιοδήποτε αναγνώστη είτε έχει άμεση σχέση με το αντικείμενο της πληροφορικής και της ασφάλειας είτε είναι κάποιο άλλο μέλος της επιχείρησης που χρειάζεται να κατανοήσει την κατάσταση της επιχείρησης σε επίπεδο ασφαλείας πληροφοριακών συστημάτων.

Πιο συγκεκριμένα, στην ενότητα «A.2» αναγράφεται η επεξήγηση της επιλογής της μεθόδου ISO27001. Επιπλέον, τα στάδια και τα βήματα που θα ακολουθηθούν προκειμένου κατά την ολοκλήρωση της αναφοράς να είναι βέβαιο ότι έχει καταγραφεί και αναλυθεί κάθε διαδικασία, υποδομή και λογισμικό του πληροφορικού συστήματος. Στην συνέχεια στην ενότητα «A2.1» παραθέτετε το διάγραμμα του πληροφοριακού συστήματος της ξενοδοχειακής μονάδας του ξενοδοχείου καθώς και μια σύντομη περιγραφή αυτού. Ωστόσο για πιο αναλυτική και ολοκληρωμένη εικόνα, η ενότητα «A2.1» είναι χωρισμένη σε υποενότητες. Αναλυτικότερα, η υποενότητα «A2.1.1» αφορά την καταγραφή του υλικού εξοπλισμού που διαθέτει η επιχείρηση. Έπειτα, η υποενότητα «A2.1.2» αναφέρονται τα

λογισμικά που διαθέτει το υλικό του πληροφοριακού συστήματος. Εν συνεχεία, η υποενότητα «A2.1.3» αναγράφεται μια λεπτομερής περιγραφή του δικτύου που επικοινωνεί το υλικού της επιχείρηση και των πελατών. Εν τέλει, στις ενότητες «A2.1.4» και «A2.1.5» περιέχονται οι περιγραφές των δεδομένων και διαδικασιών του πληροφοριακού συστήματος.

Η επόμενη βασική ενότητα «A3» περιέχει τον προσδιορισμό και την αποτίμηση των αγαθών του πληροφοριακού συστήματος. Ειδικότερα, στην υποενότητα «A3.1» αναφέρονται τα αγαθά που εντοπίστηκαν στο πληροφοριακό σύστημα του ξενοδοχείου. Στην συνέχεια, θα αποτυπωθούν οι απειλές που διατρέχει το υπάρχων πληροφοριακό σύστημα στην υποενότητα «A3.2». Εφόσον θα έχουν αποτυπωθεί οι απειλές, στην επόμενη υποενότητα «A3.3» θα αναγραφούν οι ευπάθειες που μπορούν να εκμεταλλευτεί κάποιος μην εξουσιοδοτημένος χρήστης. Τέλος, στο κλείνοντας την ενότητα «A3», θα αναλυθεί η επίδραση που θα προκύψει στην επιχείρηση αν εκμεταλλευτεί κάποιος αυτές τις ευπάθειες παραθέτοντας έναν πίνακα (υποενότητα «A3.4»).

Επομένως, εφόσον η αναφορά έχει καλύψει το μέρος που απαντά γιατί το πληροφορικό σύστημα έχει προβλήματα ασφαλείας, η αναφορά προχωρά στην ενότητα «B2» στις λύσεις και μέτρα που πρέπει να παρθούν ώστε να μειωθούν οι ευπάθειες του συστήματος.

Τέλος, επειδή η επιχείρηση μπορεί να μην διαθέτει το απαιτούμενο ποσό να εφαρμόσει κάθε μια από τις λύσεις που παραθέσαμε στην ενότητα «B2», έχει προστεθεί μια επιπλέον ενότητα «A4» με τα πιο κρίσιμα σημεία που πρέπει να δώσει προσοχή η επιχείρηση, δηλαδή τα αγαθά με την υψηλότερη επικινδυνότητα.

A2. ΜΕΘΟΔΟΛΟΓΙΑ ΜΕΛΕΤΗΣ ΑΣΦΑΛΕΙΑΣ

Για τη Διαχείριση Επικινδυνότητας του “Relax and Joy” χρησιμοποιήθηκε παραμετροποιημένη μέθοδος του ISO27001K[1]. Επιλέχθηκε για τη συγκεκριμένη εργασία για τους εξής λόγους:

- Αποτελεί πρότυπη μέθοδο και έχει αναπτυχθεί με σκοπό να εφαρμοστεί στην εκπαίδευση.
- Συνοδεύεται από αυτοματοποιημένο excel *(tool)* που υποστηρίζει όλα τα στάδια της εφαρμογής.
- Καλύπτει όλες τις συνιστώσες της ασφάλειας των πληροφοριακών συστημάτων, περιλαμβανομένων του τεχνικού παράγοντα, των θεμάτων διαδικασιών και προσωπικού, της φυσικής ασφάλειας, της ασφάλειας δικτύων κλπ.

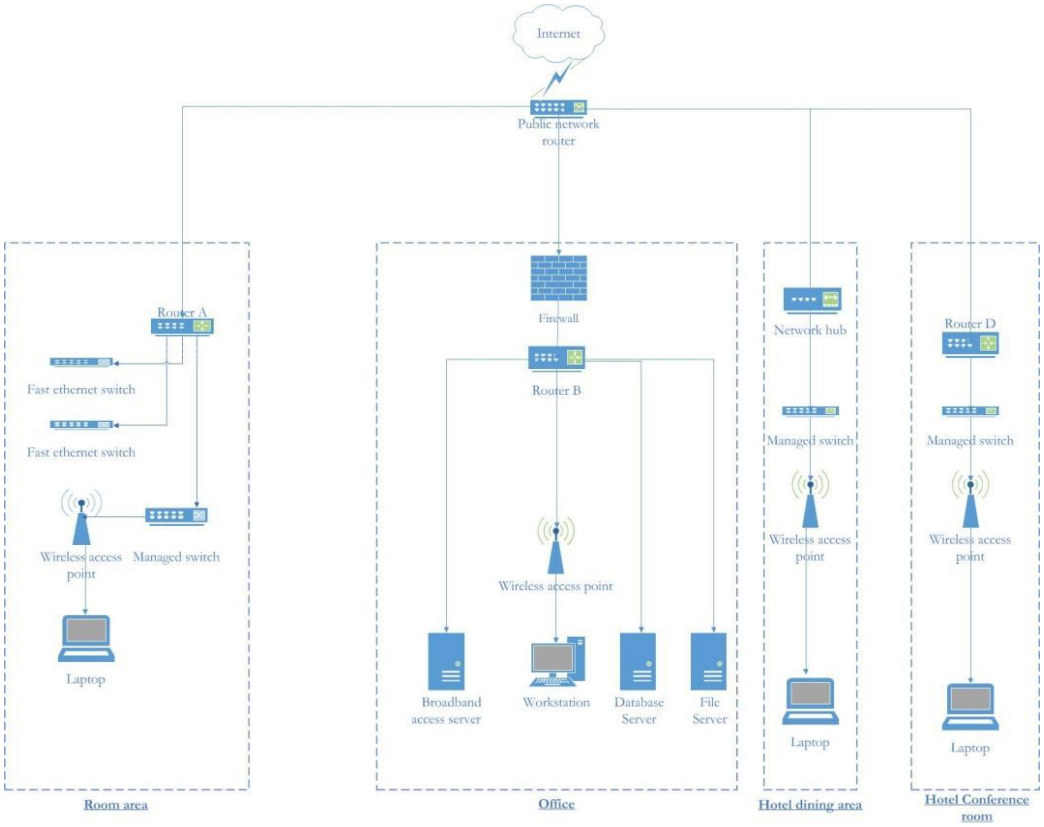
[1] http://www.iso27001security.com/html/toolkit.html

Στάδιο	Βήματα
1. Προσδιορισμός και αποτίμηση αγαθών *(identification and valuation of assets)*	*Βήμα 1*: Περιγραφή πληροφοριακών συστημάτων και εγκαταστάσεων *Βήμα 2:* Αποτίμηση αγαθών πληροφοριακών συστημάτων και εγκαταστάσεων *Βήμα 3:* Επιβεβαίωση και επικύρωση αποτίμησης
2. Ανάλυση επικινδυνότητας *(risk analysis)*	*Βήμα 1:* Προσδιορισμός απειλών που αφορούν κάθε Αγαθό (asset) *Βήμα 2:* Εκτίμηση απειλών (threat assessment) και αδυναμιών (vulnerability assessment) *Βήμα 3:* Υπολογισμός επικινδυνότητας συνδυασμών Αγαθό-Απειλή-Αδυναμία *Βήμα 4:* Επιβεβαίωση και επικύρωση βαθμού επικινδυνότητας
3. Διαχείριση επικινδυνότητας *(risk management)*	*Βήμα 1:* Προσδιορισμός προτεινόμενων αντιμέτρων *Βήμα 2:* Σχέδιο ασφάλειας πληροφοριακών συστημάτων και εγκαταστάσεων

Πίνακας 1: *Στάδια και βήματα της Ανάλυσης και Διαχείρισης επικινδυνότητας*

Α2.1 Περιγραφή Πληροφοριακού Συστήματος (ΠΣ) υπό έλεγχο

Στην ενότητα αυτή, καταγράφονται τα υφιστάμενα πληροφοριακά συστήματα του "Relax and Joy", τα οποία με το πέρας της μελέτης θα επικαιροποιηθούν, αναβαθμιστούν ή σε κάποιες περιπτώσεις αντικατασταθούν. Επιπλέον παραθέτετε ένα διάγραμμα αυτού:



A2.1.1 Υλικός εξοπλισμός (hardware)

Για την καλύτερη κατανόηση του υλικού θα προχωρήσουμε σε μια κατηγοριοποίηση του σύμφωνα με την τοποθεσία του. Κάθε αντικείμενο του συνολικού υλικού έχει καταγραφεί και έχει τοποθετηθεί σε ένα αρχείο excel.

Το πληροφοριακό σύστημα του ξενοδοχείου διαθέτει αγαθά τύπου hardware, data και software τα οποία είναι τοποθετημένα σε διαφορετικούς χώρους. Ο πιο σημαντικός από αυτούς είναι ο χώρος του "Office" ο οποίος διαθέτει ένα firewall που συνδέεται με το public network router. Ο χώρος διαθέτει το δικό του router που με την σειρά του συνδέεται με τρείς servers και ένα wireless access point. Ταυτόχρονα, το access point τροφοδοτεί με δεδομένα τα workstation του χώρου που είναι στον αριθμό πέντε. Ωστόσο, συμβατικά τα συμπεριλαμβάνουμε σαν έναν αγαθό για την καλύτερη ανάλυση.

Η εταιρία στον ίδιο όροφο διαθέτει ένα δωμάτιο που ονομάζεται "Room area" όπου ο σκοπός του είναι να τροφοδοτεί με ίντερνετ τα laptop των δωματίων των πελατών. Στο σύνολό του διαθέτει ένα wireless access point, ένα managed switch, router που συνδέεται με το public network switch και δύο fast internet switches.

Οι χώροι "Hotel dining area" και "Hotel Conference room" διαθέτουν παρόμοιο υλικό. Το πρώτο διαθέτει ένα network hub που συνδέεται με το public network router ενώ το δεύτερο διαθέτει ένα router που συνδέεται σ' αυτό. Παράλληλα, το network hub με την σειρά του συνδέεται με ένα managed switch που δρομολογεί την πληροφορία σε ένα wireless access point. Τέλος, το wireless point διαχέει την πληροφορία στα laptop του χώρου.

A2.1.2 Λογισμικό και εφαρμογές

Η ενότητα αυτή απαρτίζεται από το λογισμικό που τρέχει το υλικό του πληροφοριακού συστήματος της επιχείρησης καθώς και τις εφαρμογές που χρησιμοποιούνται. Πιο συγκεκριμένα, τα αγαθά **AMLPS001**, **AMLPS002**, **AMLPS003** διαθέτουν λειτουργικό σύστημα **MAC-OS** ενώ τα workstations **AMCSW004** διαθέτουν **Windows 10**. Ταυτόχρονα, τα αγαθά **AMCRT006**, **AMCRT003**, **AMCRT004** διαθέτουν υλικολογισμικό **Archer C60(EU)_V1_160712.** Έπειτα, το public network router υποστηρίζει το κατάλληλο υλικολογισμικό της NETGEAR «**Firmware Version 1.0.2.10**». Στην συνέχεια τα Fast Ethernet Switches **AMSW001**, **AMSW002** έχουν εγκατεστημένο κατάλληλο υλικολογισμικό της NETGEAR. Ωστόσο, οι server **AMSRV001**, **AMSRV002**, **AMSRV003** της εταιρίας διαθέτουν λειτουργικό **Windows Server 2008 R2**, **Windows Server 2008 R2**, **Microsoft Windows 2016 Server SP1** αντίστοιχα. Έπειτα το Network Hub **AMHB001** έχει εγκατεστημένο υλικολογισμικό **LB-LINK BL-WR1100.** Ακόμη, το firewall **AMFW001** διαθέτει υλικολιγισμικό «**Fortinet FortiOS 5.4.6**». Τα wireless access points **AMWAP001**, **AMWAP002**, **AMWAP003** έχουν υλικολογισμικό «**Cisco Unified Wireless Network Software Release 8.2.111.0**». Τέλος, τα Managed Switches **AMCSW007**, **AMCSW006**, **AMCSW004** διαθέτουν υλικολογισμικό «**Rev.B firmware 1.01.018**».

Επιπλέον, η επιχείρηση διαθέτει εφαρμογές για την εύρυθμη λειτουργία της. (+) Ο **AMSRV002** ως προς broadband access server μπορεί και παρέχει static IP για το Web Site της επιχείρησης. Συνεπώς, το Website **A-0033** είναι εφαρμογή της επιχείρησης.

A2.1.3 Δίκτυο

Μια διεύθυνση IP είναι μια διεύθυνση που χρησιμοποιείται για την μοναδική αναγνώριση μιας συσκευής σε ένα δίκτυο IP. Δεδομένης μιας διεύθυνσης IP, η κλάση της μπορεί να καθοριστεί από τα τρία bits υψηλής τάξης. Συνεπώς, η ομάδας σύλλεξε τις IP που αντιστοιχεί κάθε υλικό του πληροφοριακού συστήματος και το εύρος των διευθύνσεων της επιχείρησης εμπίπτουν στην κλάση(Class) C, δηλαδή από 192.0.0.0 έως 223.255.255.255. Ταυτόχρονα, σχηματικά και θεωρητικά έχουμε 4 υποδίκτυα, όμως επειδή κάθε DHCP server σε κάθε router μοιράζει 192.168.1.x IP έχουμε ένα δίκτυο και μπορεί να υποστηρίξει 254 χρήστες(192.168.1.*/24 = 192.168.1.1 - 192.168.1.254).

Ως προς την συνδεσμολογία του δικτύου, το (ANSW003) public network switch το οποίο είναι τύπου Unmanaged switch* με IP = 192.168.1.93 τροφοδοτείτε κατευθείαν από τον ISP provider. Στην συνέχεια, το (ANSW003) public network switch μεταφέρει τα δεδομένα που έλαβε στο (AMFW001) firewall με IP = 192.168.1.13 όπου με την σειρά του φιλτράρει τα δεδομένα και τα στέλνει στο (AMHB001) Network Hub. Το (AMHB001) Network Hub*** έχει IP = 192.168.1.14 και κάνει αναμετάδοση τα δεδομένα στα τέσσερα router που βρίσκονται στους τέσσερις διαφορετικούς χώρους της επιχείρησης.

Φτάνοντας τα δεδομένα στο “Room Area” δηλαδή στο (AMCRT004) Router A με IP = 192.168.1.45, το router τροφοδοτεί τρία switch. Τα δύο είναι (AMSW002 κ’ AMSW001) fast Ethernet switches**** με IP = 192.168.1.9 κ’ 192.168.1.11, ενώ το εναπομένοντα switch είναι τύπου Managed Switch** με IP = 192.168.1.34. Ταυτόχρονα το Managed Switch συνδέεται με το (AMWAP004) Wireless Access Point με IP = 192.168.1.18 το οποίο τροφοδοτεί ασύρματα ένα laptop με IP = 192.168.1.31 και Asset name AMLPS001.

Το επόμενο router που δέχεται τα πακέτα του hub βρίσκεται στην περιοχή του “Office” με IP = 192.168.1.44 και asset name AMCRT003. Το AMCRT003 με την σειρά του ανταλλάσει δεδομένα με δύο κόμβους τύπου server και ένα Wireless access point. Οι server AMSRV003 και AMSRV002 έχουν IP = 192.168.1.56 και 192.168.1.3 αντίστοιχα. Το Wireless Access Point AMWAP003 έχει IP = 192.168.1.17 και συνδέεται ασύρματα με το Workstation AMCWS005 που έχει IP = 192.168.1.12.

Παράλληλα, το επόμενο router που συνδέεται με το hub είναι το Router AMCRT006 στο “Hotel dining room” όπου έχει IP = 192.168.1.47 . Το AMCRT006 με την σειρά του ανταλλάσει δεδομένα με το Managed Switch AMCSW006 που έχει IP = 192.168.1.36. Έπειτα, το Managed Switch AMCSW006 συνδέεται με το Wireless Access Point AMWAP001 έχει IP = 192.168.1.10 και συνδέεται ασύρματα με το Laptop AMLPS003 που έχει IP = 192.168.1.30.

Τέλος, το επόμενο router που συνδέεται με το hub είναι το Router AMCRT005 στο “ Hotel Conference Room” όπου έχει IP = 192.168.1.46. Το AMCRT005 με την σειρά του ανταλλάσει δεδομένα με το Managed Switch AMCSW007 που έχει IP = 192.168.1.37. Έπειτα, το Managed Switch AMCSW007 συνδέεται με το Wireless Access Point AMWAP002 έχει IP = 192.168.1.16 και συνδέεται ασύρματα με το Laptop AMLPS003 που έχει IP = 192.168.1.32.

* Unmanaged Switch: Δεν απαιτούν καμία ρύθμιση. Πρόκειται για ένα είδος Ethernet network switch, που είναι τοποθέτησης και άμεσης λειτουργίας.

** Managed Switch: Συνήθως παρέχουν τις πιο ολοκληρωμένες λειτουργίες για ένα δίκτυο. Λόγω των ποικίλων και πλούσιων χαρακτηριστικών τους όπως VLAN, CLI, SNMP, δρομολόγηση IP, QoS κ.λπ.

*** Network Hub: Είναι ένας κόμβος που δεν μπορεί να διακρίνει ποια θύρα πρέπει να λάβει ένα πακέτο. Το πέρασμα σε κάθε θύρα που είναι συνδεμένο εξασφαλίζει ότι θα φτάσει στον προορισμό του.

**** Fast internet switch : Εάν είναι συνδεδεμένος σε υπολογιστή ή δίκτυο που έχει σχεδιαστεί για υψηλότερες ταχύτητες, επιτρέπει ταχύτερη πρόσβαση στο Internet.

A2.1.4 Δεδομένα

Τα δεδομένα που αποθηκεύει η επιχείρηση είναι δύο τύπων. Τα δεδομένα A-0025 που αφορούν τους επισκέπτες και τα δεδομένα A-0026 που είναι στοιχεία υπαλλήλων του ξενοδοχείου. Ο τρόπος που αποθηκεύονται είναι στον server AMSRV003.

(+)Το AMSRV002 έχει πλέον τη δυνατότητα να συγκεντρώνει και να τερματίζει την κυκλοφορία από ένα δίκτυο LMDS (τοπικό σύστημα πολλαπλών σημείων διανομής). Συνεπώς, το traffic log A-0031 που διατηρεί είναι κρίσιμη πληροφορία του πληροφοριακού συστήματος της επιχείρησης, η οποία και αποθηκεύεται στον server AMSRV002.

(+)Ταυτόχρονα, τα workstation της εταιρίας είναι ένα σημαντικό αγαθό. Ως αποτέλεσμα, οι πληροφορία που αποθηκεύεται τοπικά A-0032 είναι ένα αγαθό που χρήζει προστασία (πχ. email/calendar).

(+) Τέλος, για την υποστήριξη δυναμικού προγραμματισμού υπάρχει μια βάση δεδομένων A-0034 που χρησιμοποιείται από το Website A-0033 και αποθηκεύεται στον Database Server AMSRV002.

A2.1.5 Διαδικασίες

Οι διαδικασίες που διαθέτει το πληροφοριακό σύστημα του ξενοδοχείου είναι εξής:

- Διαδικασία πληρωμών που βρίσκεται στο/α Workstation του “Office”
- Διαδικασία κρατήσεων που βρίσκεται και αυτή στο/α Workstation του “Office”

A3. ΑΠΟΤΙΜΗΣΗ ΠΣ ΚΑΙ ΕΓΚΑΤΑΣΤΑΣΕΩΝ

Η ενότητα αποτίμηση του πληροφοριακού συστήματος και εγκαταστάσεων του καταλύματος έχει σκοπό της σύντομη περιγραφή των αγαθών που βρέθηκαν στην ενότητα «A2» και στην συνέχεια να καταγραφούν απειλές και ευπάθειες με σκοπό, στο τελευταίο μέρος της ενότητας, να καταλήξουμε σε κάποια αποτελέσματα επικινδυνότητας για τα αγαθά τις επιχείρησης.

A3.1 Αγαθά που εντοπίστηκαν

Συνεπώς, το πληροφοριακό σύστημα της επιχείρησης διαθέτει στον χώρο “Office” :

- Το (Inventory ID) A-0001, με όνομα (Asset name) AMSRV001 είναι τύπου «**Server**», μοντέλου «Oracle File Server», κατασκευαστή «Dell» και έχει Serial number: CGF1545562
- Το (Inventory ID) A-0002, με όνομα (Asset name) AMCWS005 είναι τύπου «**Workstation**», μοντέλου «Dell Optiplex 3060 SFF», κατασκευαστή «Dell» και έχει Serial number: CZ04544026

- Το (Inventory ID) A-0003, με όνομα (Asset name) AMSRV002 είναι τύπου « **Server**» ,μοντέλου «Alcatel 7410 Broadband Access Server», κατασκευαστή «Alcatel» και έχει Serial number: CZF1545832
- Το (Inventory ID) A-0004, με όνομα (Asset name) AMSRV003 είναι τύπου « **Server**», μοντέλου «Oracle Database Server», κατασκευαστή «Oracle» και έχει Serial number: TP35652386
- Το (Inventory ID) A-0009, με όνομα (Asset name) AMCRT003 είναι τύπου «**Route**r», μοντέλου «TP-LINK Archer C60 v1», κατασκευαστής «TP-LINK» και έχει Serial number: SV23425885
- Το (Inventory ID) A-0013 με όνομα (Asset name) AMFW001 είναι τύπου «**Firewall**» μοντέλου «Fortinet-Fortigate-100D», κατασκευαστή «Fortinet» και έχει Serial number: SV23412388
- Το (Inventory ID) A-0017, με όνομα (Asset name) AMWAP003 είναι τύπου «**Wireless Access Point**», μοντέλου «Cisco Aironet 3802I Radio», κατασκευαστή «Cisco» και έχει Serial number: SK23454541

Ταυτόχρονα, ο χώρος του "Hotel Dining Room" είναι εξοπλισμένος με τα εξής:

- Το (Inventory ID) A-0007 με όνομα (Asset name) AMCSW006 είναι τύπου «**Managed Switch**» μοντέλου « D-Link DGS-1100-10MPP», κατασκευαστή «D-Link» και έχει Serial number: SV84561922
- Το (Inventory ID) A-0014 με όνομα (Asset name) AMHB001 είναι τύπου «**Network Hub**» μοντέλου «LB-Link BL-S515», κατασκευαστή «LB-Link» και έχει Serial number: HF23454687
- Το (Inventory ID) A-0015 με όνομα (Asset name) AMWAP001 είναι τύπου «**Wireless Access Point**» μοντέλου «Cisco Aironet 3802I Radio», κατασκευαστή «Cisco» και έχει Serial number: SK23454549
- Το (Inventory ID) A-0024 με όνομα (Asset name) AMLPS003 είναι τύπου «**Laptop**» μοντέλου «Apple MacBook Pro 13.3», κατασκευαστή «Apple» και έχει Serial number: DF51454548

Επιπλέον, ο χώρος του "Room area" διαθέτει τα εξής υλικό:

- Το (Inventory ID) A-0005 με όνομα (Asset name) AMCSW004 είναι τύπου «**Managed Switch**» μοντέλου «D-Link DGS-1100-10MPP», κατασκευαστή «D-Link» και έχει Serial number: SV84561921
- Το (Inventory ID) A-0010 με όνομα (Asset name) AMCRT004 είναι τύπου «**Router**» μοντέλου «TP-LINK Archer C60 v1», κατασκευαστή «TP-LINK» και έχει Serial number: SV23425875
- Το (Inventory ID) A-0018 με όνομα (Asset name) AMWAP004 είναι τύπου «**Wireless Access Point**» μοντέλου «Cisco Aironet 3802I Radio», κατασκευαστή «Cisco» και έχει Serial number: SK23454543
- Το (Inventory ID) A-0019 με όνομα (Asset name) AMSW001 είναι τύπου «**Fast Ethernet Switch**» μοντέλου «FS108 32 Port Fast Ethernet Switch», κατασκευαστή « NETGEAR» και έχει Serial number: SP25655879
- Το (Inventory ID) A-0020 με όνομα (Asset name) AMSW002 είναι τύπου «**Fast Ethernet Switch**» μοντέλου «FS108 32 Port Fast Ethernet Switch», κατασκευαστή «NETGEAR» και έχει Serial number: SP25655889

- Το (Inventory ID) A-0022 με όνομα (Asset name) AMLPS001 είναι τύπου «**Laptop**» μοντέλου «Apple MacBook Pro 13.3», κατασκευαστή «Apple» και έχει Serial number: FR61454548

Τέλος, όσο αναφορά το υλικό, ο χώρος "Hotel Conference Room" περιέχει:

- Το (Inventory ID) A-0008 με όνομα (Asset name) AMCSW007 είναι τύπου «**Managed Switch**» μοντέλου «D-Link DGS-1100-10MPP», κατασκευαστή «D-Link» και έχει Serial number: SV45773924
- Το (Inventory ID) A-0012 με όνομα (Asset name) AMCRT006 είναι τύπου «**Router**» μοντέλου «TP-LINK Archer C60 v1», κατασκευαστή «TP-LINK» και έχει Serial number: SV23425855
- Το (Inventory ID) A-0016 με όνομα (Asset name) AMWAP002 είναι τύπου «**Wireless Access Point**» μοντέλου «Cisco Aironet 3802I Radio», κατασκευαστή «Cisco» και έχει Serial number: SK23454540
- Το (Inventory ID) A-0023 με όνομα (Asset name) AMLPS002 είναι τύπου «**Laptop**» μοντέλου «Apple MacBook Pro 13.3», κατασκευαστή «Apple» και έχει Serial number: HY51454548

A3.2 Απειλές που εντοπίστηκαν

Μια απειλή είναι οτιδήποτε μπορεί να εκμεταλλευτεί μια ευπάθεια του ΠΣ για να παραβιάσει την ασφάλειά του και να προκαλέσει βλάβη στα περιουσιακά σας στοιχεία ή να οδηγήσει σε πτώση του συστήματος ή και σε νομικές συνέπειες.

Οι απειλές που εντοπίστηκαν είναι διακρίνονται σε περιβαλλοντικές απειλές, αποτυχία συστήματος, τυχαία ανθρώπινη παρέμβαση, κακόβουλες ανθρώπινες ενέργειες (παρεμβολές, παρεμπόδιση ή πλαστοπροσωπία).

1. Αποτυχία συστήματος:
    a. <u>Αποτυχία στις υπηρεσίες επικοινωνίας:</u>
    Η αποτυχία στις υπηρεσίες επικοινωνίας έχει ως αποτέλεσμα την απώλεια της διαθεσιμότητας της πληροφορίας σε αυτές τις υπηρεσίες. Αν οι υπηρεσίες δεν είναι διαθέσιμες ο υπάλληλος δεν μπορεί να επικοινωνήσει με το website να στείλει email, να έχει πρόσβαση στον file server ή να ολοκληρώσει διαδικασίες πληρωμής και κρατήσεων που βρίσκονται στο δίκτυο.
    b. <u>Λάθη κατά την συντήρηση λογισμικού (Software maintenance error):</u>
    Οι διαδικασίες και το λογισμικό που διαθέτουν τα αγαθά της επιχείρησης είτε κατά την συντήρηση είτε κατά την εγκατάσταση μπορεί να απειλήσουν την ακεραιότητα, εμπιστευτικότητα των δεδομένων και την διαθεσιμότητα των διαδικασιών που διαθέτει η επιχείρηση. Αυτό έπεται από το γεγονός ότι κανένα λογισμικό δεν εγγυάται μηδενική πιθανότητα σφαλμάτων.
    c. <u>Τεχνικά λάθη ή λάθη στην συντήρηση του υλικού (Hardware maintenance error):</u>
    Λάθη που μπορούν να προκύψουν από το υλικό ή το δίκτυο του πληροφοριακού συστήματος. Αυτή η απειλή προκύπτει από κατασκευαστικά λάθη, θερμοκρασία στους χώρους, κατά την μεταφορά

των αγαθών ή και την δομή του δικτύου της εταιρείας. Μια τέτοια απειλή μπορεί να απειλήσει συγκεκριμένα την διαθεσιμότητα των servers και των διαδικασιών και των αγαθών όπως workstations.

d. Σφάλματα κατά την μετάδοση (Communications infiltration):
Τα λάθη κατά την μετάδοση των δεδομένων μπορεί να απειλήσουν την ακεραιότητα τους (δεδομένα file server ή δεδομένα database server ή δεδομένα υπαλλήλων και κρατήσεων) και να οδηγήσουν σε απώλεια της διαθεσιμότητας. Μια τέτοια απειλή μπορεί να προκύψει από αποτυχία κάθε κόμβου του δικτύου της επιχείρησης όπως το router ή του wireless access point της επιχείρησης που βρίσκεται στο "Office" ή κάποιου άλλου managed switch.

2. Τυχαία ανθρώπινη παρέμβαση:
   a. Λάθος δρομολόγηση (Accidental misrouting):
   Η λανθασμένη δρομολόγηση ενός μηνύματος στο λάθος πρόσωπο μπορεί να οδηγήσει σε απώλεια της εμπιστευτικότητας αυτών τον μηνυμάτων αν δεν είναι κρυπτογραφημένα και απώλεια της διαθεσιμότητας στο προορισμένο άτομο μιας και δεν θα φτάσει ποτέ το μήνυμα. Η απώλεια της ακεραιότητας μπορεί να συμβεί αν τα μηνύματα που έλαβε ο εσφαλμένος χρήστης τα τροποποιήσει και τα στείλει στην αυθεντική διεύθυνση.
   b. Λάθος χρήστη (User error):
   Λάθη σε ενέργειες από τους χρήστες μπορούν να οδηγήσουν της ακεραιότητας, διαθεσιμότητας και εμπιστευτικότητας των δεδομένων της επιχείρησης. Πιο συγκεκριμένα, λάθος set-up σε security features όπως το firewall μπορεί να οδηγήσουν σε ανεπιθύμητη κίνηση στο χώρο του "Office και ως πιθανή συνέπεια να είναι η απώλεια της εμπιστευτικότητας, διαθεσιμότητας και ακεραιότητας των δεδομένων τις επιχείρησης. Επιπλέον, η απενεργοποίηση workstations της επιχείρησης όταν προκύπτει κάποιο σφάλμα στις διαδικασίες εισαγωγής δεδομένων στο website, πληρωμής και κρατήσεων μπορεί να επηρεαστεί η ακεραιότητα τους.
   c. Καταστροφή εξοπλισμού (Accidental Hardware disruption):
   Κάποιος εργαζόμενος ή πελάτης μετά από κάποιο τυχαίο γεγονός (ατύχημα) μπορεί να προκαλέσει βλάβη στα αγαθά είτε τύπου hardware είτε τύπου πληροφορίας.
   d. Μη εξουσιοδοτημένη χρήση μιας εφαρμογής (Unauthorized use of an application):
   Πρόκειται για απειλή στην οποία είναι ευάλωτοι υπαλληλοι που δεν διαθέτουν την κατάλληλη εκπαίδευση. Οι υπάλληλοι χρησιμοποιούν τους εταιρικούς υπολογιστές όμοια με τους προσωπικούς τους κάνοντας χρήση εφαρμογών πέρα της δικαιοδοσίας του ξενοδοχείου που είναι κακόβουλες και μπορεί να βλάψουν το workstation και τα δεδομένα του. Παρατηρήθηκε στο ξενοδοχείο ότι οι υπάλληλοι χρησιμοποιούν ανεξέλεγκτα το internet κατεβάζοντας αρχεία και προγράμματα από τα οποία η επιχείρηση μπορεί να κινδυνέψει. Τα αγαθά που κινδυνεύουν με αυτή την ενέργεια είναι: οι servers και όλοι οι ηλεκτρονικοί υπολογιστές που βρίσκονται στο δίκτυο.
   e. Ακούσια διαγραφή πληροφοριών (Accidental deletion of data):
   Αποτελεί απειλή που ένα άτομο της επιχείρησης μπορεί να διαγράψει σημαντική πληροφορία του συστήματος λανθασμένα κατά την εκτέλεση

κάποιας λειτουργίας του συστήματος, συνεπώς απειλείται κάθε αγαθό της κατηγορίας της πληροφορίας.

3. Κακόβουλες ανθρώπινες ενέργειες (παρεμβολές, παρεμπόδιση ή πλαστοπροσωπία):
    a. Πλαστοπροσωπία (Masquerading of identity):
    Η πλαστοπροσωπία για την παραποίηση της ταυτότητας ενός κακόβουλο χρήστη. Πιο συγκεκριμένα, ένας χρήστης της επιχείρησης έχει εξαπατηθεί ως προς την ταυτότητα του ατόμου με το οποίο επικοινωνεί. Κατά συνέπεια, μπορεί να αποκαλύψει ευαίσθητες πληροφορίες όπως δεδομένα πελατών ή υπαλλήλων προκαλώντας οικονομική ζημιά στην επιχείρηση αλλά και απώλεια της εμπιστευτικότητας των διαδικασιών της.
    b. Εισαγωγή ζημιογόνου ή αποδιοργανωτικού λογισμικού (Introduction of damaging or disruptive software):
    Η εισαγωγή τέτοιο λογισμικού αναφέρεται σε ιούς, worms, Trojan Horses και άλλα ανεπιθύμητα λογισμικά. Ο σκοπός ενός τέτοιου λογισμικού είναι η απώλεια της ακεραιότητας των δεδομένων όπως αυτών που βρίσκονται στους servers και τοπικά στα workstations ή ακόμα η απώλεια της διαθεσιμότητας κάποιου server ή υπηρεσίας της επιχείρησης με σκοπό να πλήξει την επιχείρηση οικονομικά.
    c. Κλοπή (Theft):
    Η κλοπή περιλαμβάνει δεδομένα, εξοπλισμό ή λογισμικό της επιχείρησης από υπαλλήλους ή κακόβουλους επισκέπτες. Ως αποτέλεσμα, η επιχείρηση μπορεί να εξαπατηθεί και να χάσει δεδομένα από Credit Cards, από πληρωμές υπαλλήλων, υπηρεσιών και κρατήσεων προκαλώντας οικονομική ζημία στην επιχείρηση.
    d. Κακόβουλη καταστροφή δεδομένων ή υπηρεσιών(Malicious destruction of data or services):
    Αφορά την καταστροφή κρίσιμων δεδομένων από άτομα της επιχείρησης. Η καταστροφή βάσεων δεδομένων, κρίσιμων αρχείων στον file server μπορούν να προκαλέσουν ζημιά στην διαθεσιμότητα των δεδομένων και των υπηρεσιών (διαδικασιών) της.
    e. Επίθεση άρνησης παροχής υπηρεσιών (Denial of Service):
    Μια επίθεση άρνησης παροχής υπηρεσιών διακόπτει ή αρνείται εντελώς την υπηρεσία σε νόμιμους χρήστες, δίκτυα, συστήματα και πόρους. Το δίκτυο υπερφορτώνεται με αιτήματα ασταμάτητα με αποτέλεσμα να μην μπορεί να ανταποκριθεί. Τέτοιες επιθέσεις δέχονται αρχικά τα routers και στην συνέχεια μπορεί να δεχτεί το website της επιχείρησης και οι server της και να πλήξει την διαθεσιμότητα.
    f. Repudiation:
    Με δεδομένο ότι υπάρχει διεργασίες κρατήσεων και πληρωμών, όταν γίνεται μέσω Internet θα πρέπει να συμφωνούν και οι δύο πλευρές με την συναλλαγή. Αν ένα μέλος αρνηθεί την συναλλαγή που γίνεται τότε έχουμε repudiation της συναλλαγής. Χρειάζεται κατάλληλες πολιτικές και την διασφάλιση της ακεραιότητας των διαδικασιών που θα άφηναν ακάλυπτη την επιχείρηση από συναλλαγές δεν μπορούν να απορριφθούν.
    g. Eavesdropping or Sniffing attack:

Αποτελεί απειλή κατά την οποία ο επιτιθέμενος παρακολουθεί την κίνηση που περνάει από το δίκτυο του ξενοδοχείου.Η κίνηση αποθηκεύεται για μετέπειτα ανάλυση ώστε να αποσπάσει χρήσιμη πληροφορία για την επιχείρηση όπως email και passwords. Η απειλή αυτή προκύπτει από την δομή του δικτύου του ξενοδοχείου και απειλεί την ακεραιότητα των αγαθών της πληροφορίας.

h. Social Engineering:
Το Social Engineering είναι παρόμοιο με το Masquerading αλλά η διαφορά είναι ότι η εξαπάτηση γίνεται κατευθείαν στον υπάλληλο της επιχείρησης και όχι αλλάζοντας ταυτότητα. Ειδικότερα, ένας κακόβουλους επισκέπτης εξαπατά το προσωπικό για μια μη ύποπτη κίνηση όπως μια φωτοτυπία από ένα USB stick ή η απόσπαση πληροφορίας μέσω τηλεφώνου ή email. Το αποτέλεσμα μιας τετοιας απειλής μπορεί να απειλήσει τα αγαθά που βρίσκονται στο "Office" και κυρίως εκεί που βρίσκονται σημαντικά δεδομένα και υπηρεσίες.

i. Web site intrusion:
Οι προσπάθειες παραβίαση του Website παρουσιάζεται συχνά ως και καθημερινά. Μια επιτυχημένη παραβίαση του Website μπορεί να απειλήσει την διαθεσιμότητα του.

4. Περιβαλλοντικές απειλές: Οι περιβαλλοντικές απειλές περιλαμβάνουν φυσικές καταστροφές και άλλες περιβαλλοντικές συνθήκες. Αυτές οι απειλές καταλήγουν στην απώλεια της διαθεσιμότητας.

    a. Φυσικές καταστροφές:
        - Σεισμοί:
        Η Ελλάδα είναι μια σεισμογενής χώρα. Συνεπώς, αποτελεί απειλή για καταστροφή μέρους του κτιρίου και κατά συνέπεια των αγαθών της επιχείρησης που βρίσκονται σε αυτό. Συγκεκριμένα, για το ξενοδοχείο σας, είναι παλιάς κατασκευής οπότε σε ένα σενάριο υψηλής σεισμικής δόνησης μπορεί να απειληθεί το hardware της εταιρίας και η διαθεσιμότητα της πληροφορίας.
        - Πυρκαγιά:
        Μια από τις πιο κοινές αιτίες βλάβης στις εγκαταστάσεις επεξεργασίας πληροφοριών. Μπορεί να προκύψει από ένα φυσικό γεγονός ή μπορεί να ξεκινήσει σκόπιμα ή τυχαία. Η πυρκαγιά μπορεί να προκληθεί από ηλεκτρικό σφάλμα, ακατάλληλη αποθήκευση ή κακή λειτουργία συσκευών θέρμανσης και να καταστρέψει μερικώς ή ολοσχερώς τα αγαθά της επιχείρησης είτε αν είναι hardware είτε λογισμικό είτε πληροφορία.
        - Πλημμύρα:
        Αποτελεί απειλή για τα αγαθά που βρίσκονται στους κατώτερους ορόφους του ξενοδοχείου όπως το Hotel Dining room. Τα αγαθά με την μεγαλύτερη επικινδυνότητα είναι τα AMLPS003, AMHB001, AMWAP001 και AMCSW006.

    b. Περιβαλλοντικές συνθήκες: επηρεάζουν την απόδοση και την αξιοπιστία των αγαθών, καθώς και τον χειρισμό, την αποθήκευση, τη συντήρηση και την ανταλλαγή πληροφοριών.
        - Πτώση του τροφοδοτικού συστήματος:

Η αποτυχία βασικών υπηρεσιών κοινής ωφέλειας, όπως η ισχύς, μπορεί να απειλήσει τη διαθεσιμότητα πληροφοριών. Μπορεί να οδηγήσει σε αποτυχίες υλικού, τεχνικές βλάβες ή προβλήματα με μέσα αποθήκευσης. Τα αγαθά που κινδυνεύουν από μια τέτοια απειλή είναι αυτά που απαιτούν τροφοδοσία.

Τα πιο σημαντικά αγαθά είναι αυτά που απαρτίζουν το χώρο του "Office" δηλαδή οι servers και τα workstation στα οποία βρίσκονται οι διαδικασίες πληρωμής και κράτησης.

- Διακυμάνσεις στην ισχύ:

  Η παροχή ηλεκτρικού ρεύματος μπορεί να επηρεαστεί από διάφορους παράγοντες, π.χ. χρήση από άλλους καταναλωτές στην ίδια κτιριακή εγκατάσταση. Οι διακυμάνσεις στην ισχύ ενδέχεται να προκαλέσουν βλάβη στον εξοπλισμό. Τα αγαθά που κινδυνεύουν από μια τέτοια απειλή είναι αυτά που απαιτούν τροφοδοσία.

Α3.3 Ευπάθειες που εντοπίστηκαν

Ευπάθεια είναι μια αδυναμία που μπορεί να εκμεταλλευτεί ένας κακόβουλος χρήστης, και να εκτελέσει μη εξουσιοδοτημένες ενέργειες(απειλές) μέσα στο πληροφοριακό σύστημα της επιχείρησης.

Για την καλύτερη οργάνωση και παρουσίαση των ευπαθειών τις ομαδοποιούμε σύμφωνα με τις απειλές.

Για την απειλή του σεισμού εντοπίστηκαν οι εξής ευπάθειες:

- Έλλειψη ασκήσεων εκπαίδευσης σε περιπτώσεις σεισμού.
- Μη διαθέσιμες πολιτικές και διαδικασίες για την αναπλήρωση της πληροφορίας. Ως αποτέλεσμα, η απώλεια της πληροφορίας έχει αντίκτυπο στην διαθεσιμότητα των διαδικασιών του ξενοδοχειακού χώρου.
- Μη διαθέσιμα αντίγραφα ασφαλείας του συστήματος. Η έλλειψη αυτών οδηγεί σε απώλεια σημαντικών πληροφοριών πελατών και κρατήσεων για την εύρυθμη λειτουργία της επιχείρησης.

Για την απειλή πυρκαγιά εντοπίστηκαν οι εξής ευπάθειες:

- Έλλειψη πυροσβεστικών κρουνών ή αυτόματο σύστημα καταστολής πυρκαγιάς. Μπορεί να οδηγήσει σε πλήρη καταστροφή τόσο των αγαθών του hardware, όσο και του software.
- Έλλειψη συσκευών ανίχνευσης πυρκαγιάς. Η απώλεια αυτών των συσκευών οδηγεί στην παραπάνω ευπάθεια.
- Μη διαθέσιμες πολιτικές και διαδικασίες για την αναπλήρωση της πληροφορίας. Ως αποτέλεσμα, η απώλεια της πληροφορίας έχει αντίκτυπο στην διαθεσιμότητα των διαδικασιών του ξενοδοχειακού χώρου.
- Μη διαθέσιμα αντίγραφα ασφαλείας του συστήματος. Η έλλειψη αυτών οδηγεί σε απώλεια σημαντικών πληροφοριών πελατών και κρατήσεων για την εύρυθμη λειτουργία της επιχείρησης.

Για την απειλή της πλημμύρας εντοπίστηκαν οι εξής ευπάθειες:

- Μη διαθέσιμες πολιτικές και διαδικασίες για την αναπλήρωση της πληροφορίας. Ως αποτέλεσμα, η απώλεια της πληροφορίας έχει αντίκτυπο στην διαθεσιμότητα των διαδικασιών του ξενοδοχειακού χώρου.
- Μη διαθέσιμα αντίγραφα ασφαλείας του συστήματος. Η έλλειψη αυτών οδηγεί σε απώλεια σημαντικών πληροφοριών πελατών και κρατήσεων για την εύρυθμη λειτουργία της επιχείρησης.

Για την απειλή της πτώσης του τροφοδοτικού συστήματος εντοπίστηκαν οι εξής ευπάθειες:

- Έλλειψη εναλλακτικής πηγής τροφοδοσίας όπως H/Z ή UPS. Η έλλειψη αυτών των συσκευών έχει ως αποτέλεσμα την απώλεια δεδομένων κρατήσεων και πληρωμών που δεν έχουν αποθηκευτεί στον file server καθώς επίσης και σε καταστροφή του hardware με συνέπεια την απώλεια της διαθεσιμότητα των διαδικασιών κρατήσεων, πληρωμών και website.
- Μη διαθέσιμες πολιτικές και διαδικασίες για την αναπλήρωση της πληροφορίας. Ως αποτέλεσμα, η απώλεια της πληροφορίας έχει αντίκτυπο στην διαθεσιμότητα των διαδικασιών του ξενοδοχειακού χώρου.
- Μη διαθέσιμα αντίγραφα ασφαλείας του συστήματος. Η έλλειψη αυτών οδηγεί σε απώλεια σημαντικών πληροφοριών πελατών και κρατήσεων για την εύρυθμη λειτουργία της επιχείρησης.

Για την απειλή της διακύμανσης της ισχύος εντοπίστηκαν οι εξής ευπάθειες:

- Έλλειψη εναλλακτικής πηγής τροφοδοσίας όπως UPS και πρίζες σταθεροποίησης ηλεκτρικού φορτίου. Κατα συνέπεια, σε μια διακύμανση της τάσης είναι πιθανόν να υπάρξει μερική ή ολική καταστροφή εξοπλισμού με αποτέλεσμα την απώλεια της διαθεσιμότητα των διαδικασιών κρατήσεων, πληρωμών και website.
- Μη διαθέσιμες πολιτικές και διαδικασίες για την αναπλήρωση της πληροφορίας. Ως αποτέλεσμα, η απώλεια της πληροφορίας έχει αντίκτυπο στην διαθεσιμότητα των διαδικασιών του ξενοδοχειακού χώρου.
- Μη διαθέσιμα αντίγραφα ασφαλείας του συστήματος. Η έλλειψη αυτών οδηγεί σε απώλεια σημαντικών πληροφοριών πελατών και κρατήσεων για την εύρυθμη λειτουργία της επιχείρησης.

Για την απειλή της αποτυχίας στις υπηρεσίες επικοινωνίας διακρίνονται οι εξής ευπάθειες:

- Έλλειψη απαραίτητων αντιγράφων ασφαλείας. Η έλλειψη των αντιγράφων έχουν ως συνέπεια την διαθεσιμότητας των δεδομένων μέσω αυτών των υπηρεσιών όπως email ή επικοινωνία μεταξύ διαδικασιών.
- Ακατάλληλη δομή του δικτύου της επιχείρησης. Όταν δεν υπάρχει η κατάλληλη δομή δικτύου σε μια αποτυχία επικοινωνίας υπηρεσιών μπορεί να προκύψει ζημιά σε αγαθά όπως routers ή servers ακόμη και σε software failure.

Για την απειλή κατά την λανθασμένη συντήρηση λογισμικού (Software maintenance error) βρέθηκαν οι εξής ευπάθειες:

- Ανεπαρκής γνώση από ασφάλεια πληροφοριακών συστημάτων. Συνεπώς, η συντήρηση λογισμικού δημιουργεί κενά ασφαλείας σε χρήσιμα αγαθά όπως είναι τα workstation, οι servers και το website προκαλλόντας πλήγμα στην διαθεσιμότητα της πληροφορίας.

- Μη έγκυρη ενημέρωση λογισμικού των αγαθών που ως αποτέλεσμα δημιουργούνται καινούργιες ευπάθειες όπως αναγράφεται πιο συγκεκριμένα παρακάτω στην ενότητα αυτή.

Για την απειλή “Τεχνικά λάθη ή λάθη στην συντήρηση του υλικού (Hardware maintenance error)” προέκυψαν οι παρακάτω ευπάθειες:

- Μη εξειδικευμένο προσωπικό για την συντήρηση του υλικού με αποτέλεσμα να προκύπτει μερική ή ολική ζημία σε όλα τα αγαθά της επιχείρησης.
- Μη ενημερωμένο λογισμικό ή κακή ποιότητα κατασκευής που ως αποτέλεσμα δημιουργούνται καινούργιες ευπάθειες όπως αναγράφεται πιο συγκεκριμένα παρακάτω στην ενότητα αυτή.
- Έλλειψη μηχανημάτων σταθεροποιήσεις θερμοκρασίας σε χώρους της επιχείρησης στην τοποθεσία των servers με αποτέλεσμα να δημιουργούνται περιπτώσεις crashing και να πλήττεται η διαθεσιμότητα των δεδομένων πληρωμων, κρατήσεων, της ιστοσελίδας αλλά και τα αρχεία για την λειτουργία των workstation.
- Έλλειψη αντιγράφων ασφαλείας στην περίπτωση καταστροφής ενός server όπου συνεπάγει και την καταστροφή των δεδομένων του.

Ως προς την απειλή “Σφάλματα κατά την μετάδοση (Communications infiltration)” προκύπτουν οι εξής ευπάθειες:

- Η έλλειψη δημιουργίας αντιγράφων ασφαλείας και διαδικασιών με αποτέλεσμα σε μια λάθος μετάδοση πληροφορίας να έχει βλάψει την ακεραιότητα των δεδομένων πληρωμών, κρατήσεων κλπ.
- Ακατάλληλη δομή του δικτύου και καλωδίωση που έχει ως συνέπεια τα πολλαπλά σφάλματα κατα την μετάδοση και τελικά την ακεραιότητα των δεδομένων της επιχείρησης.

Ως προς την απειλή “Λάθος χρήστη (User error)” προέκυψαν οι παρακάτω ευπάθειες:

- Περίπλοκη διεπαφή των διαδικασιών που έχουν ως συνέπεια το προσωπικό να μπερδεύεται και εσφαλμένα να αποκαλύπτουν πληροφορίες όπως κωδικοί που βρίσκονται στις διαδικασίες πληρωμης και κρατήσεων ή ακόμα κάποιου server.
- Μη εγγεγραμμένες διαδικασίες που πρέπει να ακολουθεί το προσωπικό σε ρουτίνες όπως πληρωμή υπαλλήλων ή διαχείριση κρατήσεων με αποτέλεσμα να βλάπτεται η ακεραιότητα των δεδομένων.

Για την απειλή λάθος δρομολόγηση (Accidental misrouting) βρέθηκαν οι εξής ευπάθειες:

- Έλλειψη απόδειξης των μηνυμάτων όπως η ψηφιακή υπογραφή με αποτέλεσμα να είναι ευπαθής οι διαδικασίες όπως αυτές της πληρωμής και των κρατήσεων ή ακόμη τα website της εταιρείας. Κατα συνέπεια, ένας κακόβουλος χρήστης μπορεί να κάνει κάποιο phishing attack και να αποκτήσει δικαιώματα στους servers της επιχείρησης ή τα workstation της.
- Έλλειψη κρυπτογράφησης των δεδομένων και των διαδικασιών. Ως αποτέλεσμα σε οποιαδήποτε λάθος δρομολόγηση ο λανθασμένος χρήστης να δει το περιεχόμενο των δεδομένων που είτε μπορεί να είναι κάποιος πληρωμής, κάρτα πελάτη ή ακόμη κάποια κράτηση ή κάποιος κωδικός για κάποιο αγαθό όπως workstation ή wifi.

Για την απειλή της καταστροφή εξοπλισμού (Accidental Hardware disruption) βρέθηκαν οι εξης ευπάθειες:

- Μη διαθέσιμη πολιτική για τα αντικείμενα που επιτρέπεται να φέρει ο εργαζόμενος κοντά σε εξοπλισμό της επιχείρησης. Κατα συνέπεια τα αγαθά τύπου υλικού μπορούν να υποστούν ολικές ζημιές και να πλήξουν την διαθεσιμότητα των υπηρεσιών της επιχείρησης .
- Μη διαθέσιμα αντίγραφα ασφαλείας. Ως αποτέλεσμα μαζι με το hardware μπορεί να υπάρξει απώλεια δεδομένων της επιχείρησης αν είναι κάποιος server.
- Έλλειψη εφεδρικού εξοπλισμού για τα πιο απαραίτητα αγαθά της επιχείρησης. Ως αποτέλεσμα η επιχείρηση να χάσει την διαθεσιμότητα των αγαθών της για αρκετή ώρα έως ότου αντικατασταθούν.

Για την απειλή της μη εξουσιοδοτημένη χρήση μιας εφαρμογής (Unauthorized use of an application) βρέθηκαν οι εξης ευπάθειες:

- Έλλειψη πολιτικών που περιορίζουν το προσωπικό στη χρήση λογισμικού με άδεια χρήσης. Ως συνέπειες, μπορούν να επιφέρουν πρόστιμα στην επιχείρηση.

Για την απειλή της ακούσια διαγραφή πληροφοριών (Accidental deletion of data) βρέθηκαν οι εξης ευπάθειες:

- Εσφαλμένη ρύθμιση δικαιωμάτων ασφαλείας για κάθε χρήστη. Ως αποτέλεσμα, οποιοδήποτε χρήστης μπορεί να δει και να διαγράψει ευαισθητες πληροφορίες για την επιχείρηση οπως δεδομένα πληρωμών και κρατησεων ή δεδομένα website.
- Ανεπαρκής εκπαίδευση σε θέματα ασφάλειας.
- Έλλειψη πολιτικών διαγραφής της πληροφορίας. Συνεπώς, αυθαίρετα οι χρήστες διαγράφουν πληροφορία απο τους servers χωρίς να υπάρχει έγκριση από κάποιον αρμόδιο.
- Μη διαθέσιμα αντίγραφα ασφαλείας. Ως αποτέλεσμα μπορεί να υπάρξει απώλεια δεδομένων της επιχείρησης.
- Περίπλοκη διεπαφή των διαδικασιών που έχουν ως συνέπεια το προσωπικό να μπερδεύεται και εσφαλμένα να διαγράφουν πληροφορίες όπως πληροφορία που βρίσκονται στις διαδικασίες πληρωμης και κρατήσεων ή ακόμα κάποιου server.

Για την απειλή της πλαστοπροσωπίας (Masquerading of identity) βρέθηκαν οι εξης ευπάθειες:

- Έλλειψη μηχανισμών αναγνώρισης και επαλήθευσης με συνέπεια την απομακρυσμένη σύνδεση κακόβουλων χρηστών ή την ψεύτικη ταυτότητα πελατών που στοχεύουν στην απόσπαση σημαντικής πληροφορίας της επιχείρησης.
- Μη ασφαλής και σαφής τρόπος αποθήκευσης των passwords. Ως συνέπεια, η επιχείρηση είναι ευάλωτη στην αποκάλυψη τους άρα και στην πλήρη πρόσβαση σε σημαντικά αγαθά της επιχείρησης όπως routers, managed switches, servers και workstations.

Για την απειλή της εισαγωγή ζημιογόνου ή αποδιοργανωτικού λογισμικού (Introduction of damaging or disruptive software) βρέθηκαν οι εξης ευπάθειες:

- Η επιχείρηση δεν διαθέτει κανένα λογισμικό τύπου Anti-Virus. Κατα συνέπεια, οποιαδήποτε αγαθό που διαθέτει λειτουργικό σύστημα ή υλικολογισμικό είναι ευάλωτο σε μια εισαγωγή ζημιογόνου λογισμικού με πολλαπλες επικινδυνότητες.

- Μη ελεγχόμενο κατέβασμα εφαρμογών και χρήση τους απο το ιντερνετ.
- Μη διαθέσιμη πολιτική για το άνοιγμα των attachment στα email. Ως αποτέλεσμα, η επιχείρηση μολύνεται από ιούς στα workstation και κατ επέκταση στα αγαθά του δικτύου.
- Δεν υπάρχει διαθέσιμη πολιτική για τα floppy disk των εργαζομένων που έχουν ως συνέπεια την μόλυνση των workstations.

Για την απειλή της επίθεσης ransomware βρέθηκαν οι εξης ευπάθειες:

- Δεν υπάρχουν πρόσφατα και πολύ συχνά backups. Η συνέπεια αυτού είναι οτι σε μία ενδεχόμενη επίθεση ransomware η επιχείρηση θα είναι αναγκασμένη να πληρώσει επειδή δεν θα μπορεί να επαναφέρει τα αρχεία της απο ένα προσφάτως ενημερωμένο backup.

Για την απειλή της κλοπής (Theft) βρέθηκαν οι εξης ευπάθειες:

- Ο πιο σημαντικός χώρος του ξενοδοχείου είναι το office room στο οποίο βρίσκονται οι servers της επιχείρησης. Κατα την ερευνά μας, λοιπόν, στο χώρο αυτό δεν εντοπίστηκαν κάμερες και συστήματα παρακολούθησης της συμπεριφοράς των εργαζομένων, γεγονός που μπορεί να οδηγήσει στην κλοπή τόσο ψηφιακών δεδομένων όσο και υλικού εξοπλισμού της επιχείρησης.
- Επίσης, κάμερες και συστήματα παρακολούθησης δεν βρέθηκαν και στο υπόλοιπο ξενοδοχείο, οπότε η κλοπή είναι πολύ δύσκολο να εντοπιστεί.

Για την απειλή της Κακόβουλης καταστροφής δεδομένων ή υπηρεσιών(Malicious destruction of data or services) βρέθηκαν οι εξης ευπάθειες:

- Η επιχείρηση δεν διαθέτει πρόσφατα backups και σε μερικές περιπτώσεις δεν διαθέτει καθόλου, πράγμα το οποίο είναι καταστροφικό σε περίπτωση καταστροφής ή κρυπτογράφησης(όπως αναφέρθηκε παραπάνω) των δεδομένων.
- Δεν υπάρχει διαθέσιμη πολιτική για τα δικαιώματα του κάθε εργαζομένου στην επιχείρηση. Έτσι, ακόμα και ένας απλός υπάλληλος έχει πρόσβαση σε σημαντικές πληροφορίες, τις οποίες μπορεί να διαγράψει ή καταστρέψει άθελά του ή εσκεμμένα.

Για την απειλή της Επίθεση άρνησης παροχής υπηρεσιών (Denial of Service) βρέθηκαν οι εξης ευπάθειες:

- Δεν εντοπίστηκε λογισμικό το οποίο να σκανάρει το δίκτυο και να αποτρέπει συνδέσεις που χτυπούν ακατάπαυστα τα routers και τους servers του ξενοδοχειακού συστήματος.

Για την απειλή Repudiation βρέθηκαν οι εξης ευπάθειες:

- Έλλειψη ψηφιακών υπογραφών. Ως αποτέλεσμα κατα την άρνηση της συναλλαγής που παίρνει μέρος, αν το ένα μέλος της αρνηθεί έχουμε άρνηση της συναλλαγής χωρίς να καλύπτει την επιχείρηση απο την ακεραιότητα και την εγκυρότητα των δεδομένων πληρωμών και κρατήσεων.

Για την απειλή της Eavesdropping or Sniffing attack βρέθηκαν οι εξης ευπάθειες:

- Η μεταφορά αρχείων και η επικοινωνία των υπολογιστών με τους servers γίνεται με την χρήση του απλού πρωτοκόλλου ftp το οποίο δεν διαθέτει κανένα είδος κρυπτογράφησης.
- Το ftp πρωτόκολλο δεν έχει παραμετροποιηθεί σωστά και έτσι επιτρέπεται η ανώνυμη πρόσβαση(anonymous login).
- Η επιχείρηση δεν χρησιμοποιεί ssh για την μεταφορά αρχείων.
- Η χρήση του Wireless internet σημαίνει ότι όλη η κυκλοφορία μεταδίδεται σε οποιοδήποτε μηχάνημα που βρίσκεται στην εμβέλεια του wireless access point.
- Αμερόληπτη δρομολόγηση του hub AMHB001 στο δίκτυο του Hotel Dining Room. Συνεπώς περνάει όλη η κίνηση στους υπολογιστές που συνδέονται στο wireless access point του χώρου.

Για την απειλή Social Engineering βρέθηκαν οι εξης ευπάθειες:

- Ανειδίκευτο προσωπικό που δεν έχει ενημερωθεί για τους κινδύνους του social engineering και πως αυτό μπορεί να πλήξει την επιχείρηση. (phishing attack)
- Έλλειψη επαλήθευσης της ταυτότητας που οδηγεί στην αποδοχή ψευδών πληροφοριών ή / και στην παροχή πληροφοριών σε μια μη εξειδικευμένη οντότητα.
- Έλλειψη διαβάθμισης των δικαιωμάτων του προσωπικού για την πρόσβαση και την επεξεργασία πληροφοριών. Ως συνέπεια,
- Έλλειψη πολιτικής που να απαιτεί την εξακρίβωση της ταυτότητας του αιτούντος και μετά την ολοκλήρωση του αιτήματος που μπορεί να έχει ως συνέπεια την υποκλοπή πληροφοριών της αίτησης κατά την ολοκλήρωση.

Για την απειλή DarkHotel hacking βρέθηκαν οι εξης ευπάθειες:

- Έλλειψη virtual private networks (VPN) στην επιχείρηση κατα την διαδικασία κρατήσεων που χρησιμοποιούνται ευαισθητα δεδομένα και update στα windows 10 workstations. Ως συνέπεια, με την υποκλοπή των δεδομένων οι κακόβουλοι χρήστες ανεβάζουν κακόβουλο λογισμικό στον server και στοχεύουν τον πελάτη της συναλλαγής. (CVE-2018-8373) (CVE- 2018-8174)

Για την απειλή του Web site intrusion βρέθηκαν οι εξης ευπάθειες:

- Έγινε έλεγχος στο κώδικα του website και στα σημεία εισαγωγής κειμένου από το χρήστη δεν χρησιμοποιούνται γνωστές συναρτήσεις όπως htmlspecialchars() ή prepare statements με αποτέλεσμα να γίνονται επιθέσεις sql injection.
- Έλλειψη intrusion detection software πριν το server που φιλοξενεί το website. Συνεπώς, η κίνηση σε αυτό δεν φιλτράρεται από και προς τον server απειλώντας την διαθεσιμότητα του.
- Ανεπαρκής Firewall πολιτικές με αποτέλεσμα η ανεπιθύμητη κυκλοφορία να περνάει στα αγαθά του office και κατ επέκταση στο website.
- Έλλειψη update στο Operating System security patches του server αφήνοντας εκτεθειμένο τον server σε πολλαπλές επιθέσεις.

Παρακάτω, παραθέτουμε κάποιες αναγνωρισμένες ευπάθειες που έχουν εντοπιστεί και καταγραφεί στην Διεθνή Βάση Δεδομένων των Ευπαθειών (https://nvd.nist.gov/)

- Για τα αγαθά που διαθέτουν λειτουργικό σύστημα MAC-OS βρέθηκαν οι εξής ευπάθειες:
    - (CVE-2015-5889) Χρησιμοποιώντας την εντολή rsh σε εκδόσεις Apple OS X πριν από την έκδοση 10.11 κακόβουλοι χρήστες μπορούν να συνδεδούν απομακρυσμένα στο υπολογιστή μας έχοντας δικαιώματα διαχειριστή, εκμεταλλευόμενοι πίνακες τοπικών μεταβλητών.
    - (CVE-2014-4492) Εκμεταλλευόμενοι την κοινή βιβλιοθήκη libnetcore έως και την έκδοση Apple OS X 10.10.2 δεν επιβεβαιώνεται ότι μερικές μεταβλητές έχουν τον αναμενόμενο τύπο δεδομένων και έτσι επιτρέπεται σε κακόβουλους χρήστες να εκτελέσουν αυθαίρετα κώδικα πάνω στο δίκτυο.
    - (CVE-2015-1100) Ο πυρήνας σε εκδόσεις Apple OS X 10.10.3 και προηγούμενες επιτρέπει σε κακόβουλους χρήστες να πραγματοποιήσουν denial of service ή να αποκτήσουν πληροφορία σε ευαίσθητες περιοχές μνήμης μέσω κακόβουλης εφαρμογής

- Για τα αγαθά που διαθέτουν λειτουργικό σύστημα Windows 10 βρέθηκαν οι εξής ευπάθειες:(ενδεικτίκα οι πιο σοβαρές)
    - (CVE-2018-8209) Ένας κακόβουλος χρήστης μπορεί να έχει πρόσβαση σε πληροφορίες του συστήματός μας όταν τα Windows επιτρέπουν την πρόσβαση σ' έναν τοπικό χρήστη να αποκτήσει δικαιώματα στο Wireless LAN προφίλ του διαχειριστή.
    - (CVE-2018-8414) Ένας κακόβουλος χρήστης έχει την δυνατότητα να εκτελέσει ιομορφικό λογισμικό όταν ο πυρήνας των Windows δεν επικυρώνει σωστά τα paths των αρχείων του συστήματός.
    - (CVE-2018-8406) Όταν ο πυρήνας των γραφικών DirectX διαχειρίζεται ακατάλληλα αντικείμενα στην μνήμη τότε υπάρχει πιθανότητα ένας κακόβουλος χρήστης να εκμεταλλευτεί την ευπάθεια προαγωγής δικαιωμάτων. Δηλαδή από δικαιώματα απλού χρήστη να αποκτήσει δικαιώματα διαχειριστή ή και δικαιώματα συστήματος.
    - (CVE-2018-8206) Όταν τα Windows διαχειρίζονται ακατάλληλα συνδέσεις FTP(= Files Transfer Protocol) τότε το αγαθό είναι ευπαθές σε επιθέσεις denial of service.
    - (CVE-2018-8225) Όταν το Windows Domain Name System (DNS) DNSAPI.dll αποτύχει να διαχειριστεί σωστά τα DNS αιτήματα τότε το λειτουργικό είναι ευπαθές σε remote code execution.

- Για τα αγαθά που διαθέτουν λειτουργικό σύστημα Archer C60(EU)_V1_160712 σύμφωνα με τον ιστότοπο (https://nvd.nist.gov/) , δεν βρέθηκαν συγκεκριμένες ευπάθειες(link).
- Τα unmanaged switches δεν διαθέτουν λογισμικό για configuration άρα δεν εμπίπτουν σε ευπάθειες λογισμικού. Τα αγαθά που βρίσκονται σε αυτήν την κατηγορία είναι τα AMSW001, AMSW002, AMSW003 και ANSW003.

- Για τα αγαθά που διαθέτουν λειτουργικό σύστημα Windows Servers 2016 βρέθηκαν οι εξής ευπάθειες:

- (CVE-2018-8495) Όταν ο πυρήνας του Windows server δεν μπορεί να διαχειριστεί σωστά τα URIs τότε τα αγαθά που διαθέτουν το εν λόγω λογισμικό είναι ευπαθείς σε remote code execution.
- (CVE-2018-8493) Όταν η στοίβα TCP/IP των Windows παρουσιάζει σφάλματα στην διαχείριση των τμημάτων των πακέτων IP τότε ένας κακόβουλος χρήστης έχει την δυνατότητα να εκμεταλλευτεί την ευπάθεια αυτή και να αποκτήσει σημαντική πληροφορία του ξενοδοχείου.
- (CVE-2018-8423) Ο Database engine του εν λόγω λογισμικού "Microsoft JET Database Engine" παρουσίασε ευπάθεια remote code execution. Ταυτόχρονα, εκμεταλλευόμενος κάποιος την προηγούμενη ευπάθεια μπορεί εκθέσει τον server σε μια νέα ευπάθεια υπερχείλισης μνήμης(= buffer overflow) [CVE-2018-8393] [CVE-2018-8392].

- Για τα αγαθά τύπου Wireless Access Point με κατάλληλο λογισμικό Cisco εντοπίστηκαν οι εξής ευπάθειες:
  - (CVE-2018-0226) Εντοπίστηκε ευπάθεια στην ανάθεση και διαχείριση του default χρήστη μέσω του SSH shell της Cisco, την οποία ένας επιτιθέμενος μπορεί να εκμεταλλευτεί για να κερδίσει μη εξουσιοδοτημένα δικαιώματα στο απειλούμενο access point του ξενοδοχείου. Η ευπάθεια υπάρχει επειδή ο controller, που επηρεάζεται, ρυθμίζει τον προεπιλεγμένο λογαριασμό χρήστη SSH για ένα access point ώστε να είναι ο πρώτος SSH λογαριασμός χρήστη ο οποίος δημιουργήθηκε για τον controller, αν ενας διαχειριστής προστεθεί απο τους λογαριασμους χρηστών απευθείας στον controller αντι να χρησιμοποιησει τον προεπιλεγμένο λογαριασμό ή τον οδηγό δημιουργίας ονόματος SSH. Παρόλο που ο λογαριασμός χρήστη έχει δικαιώματα μόνο για ανάγνωση του controller, ο λογαριασμός θα μπορούσε να έχει δικαιώματα διαχειριστή για ένα συνδεδεμένο σημείο πρόσβασης.
  - (CVE-2017-12281) Εντοπίστηκε ευπάθεια στην εφαρμογή της διαδικασίας του Protected Extensible Authentication Protocol (PEAP) για αυτόνομες διαμορφώσεις(configuration) που θα μπορούσαν να επιτρέψουν χωρίς εξουσιοδότηση γειτονικούς επιτηθέμενους να προσπεράσουν το σύστημα ταυτοποίησης και να συνδεθούν στο δικτυο. Η ευπάθεια αυτή συμβαίνει καθώς το access point δεν μπορεί να τρέξει σε αυτόνομη λειτουργία με τις προεπιλεγμένες ρυθμίσεις διότι είναι λανθασμένες.
  - (CVE-2017-3873) Τα access point εμπίπτουν σε ευπάθεια στο υποσύστημα Plug-and-Play(PnP) που τρέχουν Lightweight Access Point (AP) or Mobility Express image ως αποτέλεσμα θα μπορούσε να επιτρέψει σε έναν παραβάτη χωρίς εξουσιοδότηση να εκτελέσει αυθαίρετο κώδικα με δικαιώματα προφίλ root.
- Τα αγαθά που διαθέτουν λογισμικό **Rev.B firmware 1.01.018** διαθέτουν τις εξής ευπάθειες:
  - (CVE-2016-10125) Οι συσκευές D-Link DGS-1100 με Firmware Rev. 1.01.018 διαθέτουν ένα ιδιωτικό κλειδί SSL με κωδικό hardcoded, το οποίο επιτρέπει στους man-in-the-middle επιτηθέμενους να κάνουν spoof συσκευές κάνοντας κατάχρηση σε μια περίοδο σύνδεσης HTTPS.
- Για το αγαθό τύπου firewall με λογισμικό **FortiOS 5.4.6** εντοπίστηκαν οι εξής ευπάθειες:

    - (CVE-2017-14186) Το SSL VPN web portal επιτρέπει σε απομακρυσμένους χρήστες να εισχωρήσουν αυθαίρετα web scripts ή HTML κώδικα σε περιεχόμενο του browser τερματικού του ξενοδοχείου μέσω login redir παραμέτρου κάνοντας το ευπαθές σε σε Cross-site Scripting (XSS).
    - (CVE-2018-9194)(CVE-2018-9192)Μια ανάκτηση αρχικού κειμένου από κρυπτογραφημένα μηνύματα ή Man-in-the-middle (MiTM) επίθεση σε RSA PKCS #1 v1.5 κρυπτογραφία μπορεί να πραγματοποιηθεί χωρίς την χρήση του μυστικού κλειδιού του σέρβερ. Το λογισμικό είναι ευπαθές σε τετοιες επιθέσεις κάτω από το VIP SSL ή SSL Deep Inspection feature οταν το CPx χρησιμοποιείται.
- Για τα αγαθά που διαθέτουν λειτουργικό σύστημα Windows Server 2008 R2 βρέθηκαν οι εξής ευπάθειες:
    - (CVE-2018-0976)Υπάρχει ευπάθεια άρνησης εξυπηρέτησης στο Remote Desktop Protocol (RDP) όταν ένας εισβολέας συνδέεται με το σύστημα προορισμού χρησιμοποιώντας το RDP και στέλνει ειδικά επεξεργασμένα αιτήματα.
    - (CVE-2018-0975, CVE-2018-0887, CVE-2018-0960, CVE-2018-0968, CVE-2018-0969, CVE-2018-0970, CVE-2018-0971, CVE-2018-0972, CVE-2018-0973, CVE-2018-0974) Μια ευπάθεια αποκάλυψης πληροφοριών υπάρχει στον πυρήνα των Windows που θα μπορούσε να επιτρέψει σε έναν εισβολέα να ανακτήσει πληροφορίες που θα μπορούσαν να οδηγήσουν σε παράκαμψη του Kernel Address Space Layout Randomization (ASLR) bypass.
    - (CVE-2018-1036)Υπάρχει ευπάθεια προαγωγή των προνομίων όταν το NTFS ελέγχει ακατάλληλα την πρόσβαση

Επιπλέον, μετά τη μελέτη μας στην συνδεσμολογία του δικτύου παρατηρήθηκε ότι:

- Πριν το public network router ANSW003 δεν υπάρχει κάποιο firewall ή IDS με αποτέλεσμα όλη η κίνηση από τον ISP provider να μην φιλτράρεται και να μεταφέρεται στο υπόλοιπο δίκτυο.
- Το δίκτυο δεν είναι αυστηρά χωρισμένο σε υποδίκτυα ανάλογα τον χώρο.
    - Δηλαδή, για τους τέσσερις χώρους θα έπρεπε να χωριστεί σε τεσσερα υποδικτυα 192.168.1*/26
- Οι servers AMSRV001, AMSRV002, AMSRV003 συνδέονται απευθείας με το router AMCRT003 με αποτέλεσμα αν ένας κακόβουλος χρήστης αποκτήσει πρόσβαση σ αυτό να αποκτήσει κατευθείαν και στους σερβερς.
- Στο office υπάρχει wireless access point AMWAP003 πράγμα που σημαίνει ότι κάποιος που δεν βρίσκεται στο γραφείο αλλά σε κοντινούς ορόφους μπορεί να έχει πρόσβαση σ αυτό.
- Το Hotel dining area διαθέτει network hub αντί για router πράγμα που σημαίνει η κίνηση δρομολογείται σε οποιαδήποτε συσκευή συνδεθεί στο hub είτε είναι άτομο της επιχείρησης είτε κάποιος κακόβουλος χρήστης.
- Τα workstation περνάνε την σύνδεση τους απο τον απομακρυσμένο broadband access server πράγμα που κάνει ευάλωτο το δίκτυο σε man in the middle attacks καθώς όλα τα πακέτα περνάνε από εκεί.

A3.4 Αποτελέσματα αποτίμησης

Παρακάτω παρουσιάζουμε τις συνέπειες που θα έχει η απώλεια διαθεσιμότητας, ακεραιότητας και εμπιστευτικότητας για όλα τα αγαθά της επιχείρησης.

Servers & Server Data(AMSRV001,AMSRV002,AMSRV003, Traffic log, Hotel Guest Data, Hotel Employee Data)

Αρχικά, αξίζει να αναφέρουμε ότι οι servers μιας οποιασδήποτε επιχείρησης είναι το πιο σημαντικό κομμάτι της, αφού από εκεί αντλεί όλα τα δεδομένα της. Συνεπώς, η απώλεια τόσο στην διαθεσιμότητα, όσο και στην ακεραιότητα και την εμπιστευτικότητα έχουν τρομερές συνέπειες για το ξενοδοχείο. Συνεπώς, η απώλεια της διαθεσιμότητας των πληροφοριών των server είναι πολύ σημαντική συνέπεια και όσο μεγαλώνει το χρονικό διάστημα της απώλειας αυτής, οι τιμές μεγαλώνουν αφού το ξενοδοχείο δεν θα μπορεί να έχει πρόσβαση σε πληροφορίες πελατών, πληρωμών και κρατήσεων. Συνεχίζοντας στην απώλεια της ακεραιότητας, οι τιμές είναι μονίμως ανεβασμένες αφού μιλάμε για προσωπικά δεδομένα όπως πληρωμές κρατήσεων, προσωπικά στοιχεία τα οποία προστατεύονται από το GDPR και με την αποκάλυψη ή την αλλοίωσή τους οι πελάτες του ξενοδοχείου μπορούν να κινηθούν δικαστικά. Τέλος, η απώλεια πληροφοριών κατα την τηλεπικοινωνιακή μετάδοση είναι εξίσου σημαντική αφού όλες οι πληροφορίες πρέπει να φτάνουν στους servers χωρίς λάθη, αστοχίες και με την σειρά που έχουν σταλθεί.

Workstation & Workstation's Data(AMCWS005)

Πρόκειται για τους υπολογιστές που υπάρχουν στο γραφείο του ξενοδοχείου. Γι αυτόν τον λόγο οι τιμές στον πίνακα είναι υψηλές, αφού σε περίπτωση μη ορθής λειτουργίας των υπολογιστών, δεν θα μπορεί να λειτουργήσουν οι διαδικασίες των πληρωμών, των κρατήσεων και γενικότερα τα check-in και check-out του ξενοδοχείου. Επίσης σε περίπτωση υποκλοπής τοπικών δεδομένων ο κακόβουλος μπορεί να αποκτήσει σημαντική πληροφορία όπως mail πελατών ή επικοινωνίες μεταξύ εργαζομένων.

Managed Switches(AMCSW004,AMCSW006,AMCSW007)

Τα managed switches συνήθως παρέχουν τις πιο ολοκληρωμένες λειτουργίες για ένα δίκτυο. Λόγω των ποικίλων και πλούσιων χαρακτηριστικών τους όπως τα VLAN, CLI, SNMP, routing IP, QoS κ.λπ., τα managed switch χρησιμοποιούνται συχνά στο κεντρικό στρώμα σε ένα δίκτυο, ειδικά σε μεγάλα και σύνθετα κέντρα δεδομένων. Τα managed switches μπορούν να απομονώσουν την κυκλοφορία δεδομένων με βάση διαφορετικές ομάδες, όπως χρήστες, επισκέπτες, αντίγραφα ασφαλείας, διαχείριση και διακομιστές. Αυτό όχι μόνο προσφέρει στους διαχειριστές έναν καλύτερο τρόπο για τον έλεγχο της κυκλοφορίας δεδομένων, αλλά παρέχει επίσης ισχυρή προστασία για όλο το δίκτυο. Παραθέτοντας λίγα πράγματα για την λειτουργία και την σημαντικότητα των managed switch, καταλαβαίνουμε ότι σε τυχόν απώλειά τους, η επιχείρηση θα ζημιωθεί. Συνεπώς οι τιμές στον πίνακα παρακάτω αναμένονται υψηλές.

Routers(AMCRT003,AMCRT004,AMCRT006,ANSW003)

Η δουλειά ενός router είναι να δρομολογήσει τα πακέτα σε άλλα δίκτυα μέχρις ότου το πακέτο τελικά φτάσει στον προορισμό του. Χωρίς αυτά θα ήταν αδύνατο να

επικοινωνήσουν οι διάφορες συσκευές μέσα στο δίκτυο. Συνεπώς η απώλεια της διαθεσιμότητας τους, η καταστροφή τους, η αποκάλυψη πληροφοριών αλλα και τα λάθη κατα την μετάδοση και δρομολόγηση των μηνυμάτων θα έχουν καταστροφικές συνέπειες για το ξενοδοχείο.

Firewall(AMFW001)

Το firewall είναι το λογισμικό το οποίο φιλτράρει την εισερχόμενη κίνηση στο δίκτυο και αποτρέπει,επιτρέπει αντίστοιχα ανάλογα την παραμετροποίηση που του έχει γίνει. Η απώλεια της διαθεσιμότητας του firewall είναι αρκετά σημαντική και μπορεί να οδηγήσει σε πολλά προβλήματα όπως dos attacks, αιτήματα από κακόβουλους χρήστες για σύνδεση στο δίκτυο, κ.α. Γιαύτο οι συγκεκριμενες τιμές στο πινακακι είναι υψηλές. Από την άλλη πλευρά, η απώλεια της ακεραιότητας, η αποκάλυψη των πληροφοριών και τα λάθη στην μετάδοση έχουν χαμηλότερες τιμές και η τελευταία κατηγορία μηδενικές, αφού το firewall δεν διαθέτει δεδομένα ούτε δρομολογεί πακέτα.

Network Hub(AMHB001)

Το network hub κάνει την ίδια δουλειά που κάνει και το managed switch με την διαφορά ότι όταν τα πακέτα φτάνουν σε αυτό τα προωθεί σε όλους τους κόμβους που είναι συνδεδεμένοι. Συνεπώς, οι τιμές στον πίνακα είναι ίδιες.

Wireless Access Point(AMWAP001,AMWAP002,AMWAP003,AMWAP004)

Οι wireless access point συσκευές είναι υπεύθυνες για την παροχή wifi στο ξενοδοχείο. Η απώλεια της διαθεσιμότητας τους δεν είναι τόσο σοβαρό πρόβλημα αφού οι υπολογιστές που είναι απαραίτητο να έχουν πρόσβαση στο internet θα είναι συνδεδεμένες με καλώδιο ethernet. Επιπλέον,ούτε η απώλεια της ακεραιότητας, η αποκάλυψη πληροφοριών και η λανθασμένη τηλεπικοινωνιακή μετάδοση μπορούν να επιφέρουν σοβαρές συνέπειες αφού τα wireless access point δεν διαθέτουν δεδομένα αλλά ούτε δρομολογούν πακέτα. Η επιπτώσεις είναι μεγαλύτερες στο χώρο του office καθώς αρκετή κίνηση πακέτων περνά από εκεί.

Ατομικοί υπολογιστές(AMLPS001,AMLPS002,AMLPS003)

Πρόκειται για τους υπολογιστές που βρίσκονται στο χώρο του dining room, conference room και room area. Ένας κακόβουλος χρήστης μέσω των ευπαθειών μπορεί να αποκτήσει δικαιώματα διαχειριστή που σημαίνει ότι μπορεί να αποκτήσει δικαιώματα διαχειριστή πλήττοντας την ακεραιότητα, την εμπιστευτικότητα και την διαθεσιμότητα τους. Συνεπώς, στην διαθεσιμότητας λόγω ότι δεν είναι σημαντικά έχει μικρή ως μεσαία συνέπεια, ενώ στην ακεραιότητα τους είναι μεσαία ενώ στην εμπιστευτικότητα επειδή η επιχείρηση επικοινωνεί με αυτά τα αγαθά θα το θέσουμε σε υψηλότερες τιμές.

Website & Website Data

Σχετικά με την ιστοσελίδα του ξενοδοχείου που σχετίζεται με την πληροφόρηση για τις υπηρεσίες που προσφέρει το ξενοδοχείο, καταλήγουμε ότι δεν είναι μείζον σημασίας,

καθώς δεν έχει κάποιο σημαντικό αντίκτυπο στο ξενοδοχείο πέρα από την κακόβουλη τροποποίηση της σελίδας ή την πλήξη της διαθεσιμότητάς της.

Fast Ethernet Switch(AMSW001, AMSW002)

Το unmanaged routers του Fast Ethernet Switch βρίσκονται στο Room Area και προσφέρουν μια πιο γρήγορη εμπειρία χρήσης στους επισκέπτες. Συνολικά δεν αποτελούν μεγάλο πλήγμα στην επιχείρηση.

Διαδικασίες (Payment process, Reservation process)
Οι διαδικασίες της επιχείρησης καθώς και τα δεδομένα που φέρουν είναι ζωτικής σημασίας για την ομαλή λειτουργία της επιχείρησης. Αυτό σημαίνει ότι η διαθεσιμότητα καθώς και η μετάδοση της πληροφορίας χρήζει την προσοχή σε ζητήματα ασφαλείας

	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
AMSR V001	5	5	6	8	9	10	10	10	10	10	8	10	10	10	10	10	9	9	10	5	10	10	10	8
AMC WS005	9	10	10	10	10	10	10	10	8	8	5	7	8	8	10	7	10	9	8	5	10	10	10	8
AMSR V002	5	5	6	8	9	10	10	10	10	10	8	10	10	10	10	10	9	9	10	8	10	10	10	8
AMSR V003	7	7	8	9	9	10	10	10	10	10	8	10	10	10	10	10	9	9	10	8	10	10	10	8
AMCS W004	3	4	5	7	9	10	10	10	8	8	7	9	6	8	10	7	8	8	8	8	10	10	8	8

AMCS W006	3	4	5	7	9	10	10	10	8	8	7	9	6	8	10	7	8	8	8	8	10	10	8	8
AMCS W007	3	4	5	7	9	10	10	10	8	8	7	9	6	8	10	7	8	8	8	8	10	10	8	8
AMCR T003	5	7	8	9	10	10	10	10	9	8	7	9	8	8	10	8	7	7	9	9	10	10	10	9
AMCR T004	5	7	8	9	10	10	10	10	9	8	7	9	8	8	10	8	7	7	9	9	10	10	10	9
AMCR T006	5	7	8	9	10	10	10	10	9	8	7	9	8	8	10	8	7	7	9	9	10	10	10	9
AMFW 001	3	5	7	8	10	10	10	10	8	7	5	8	5	5	5	1	1	1	1	1	1	1	1	1
AMHB 001	3	4	5	7	9	10	10	10	8	8	7	9	6	8	10	7	?	?	8	8	10	10	8	8
AMW AP001	2	2	3	4	5	6	6	7	6	8	4	5	7	7	8	6	8	8	8	9	9	9	6	5
AMW AP002	2	2	3	4	5	6	6	7	6	8	4	5	7	7	8	6	8	8	8	9	9	9	6	5
AMW AP003	6	7	8	8	9	10	10	10	9	9	7	9	10	8	10	9	9	9	9	10	10	10	10	10
AMW AP004	2	2	3	4	5	6	6	7	6	8	4	5	7	7	8	6	8	8	8	9	9	9	6	5
AMSW 001	2	2	3	4	5	6	6	7	6	8	4	5	4	2	2	2	2	2	2	2	5	3	2	2

AMSW 002	2	2	3	4	5	6	6	7	6	8	4	5	4	2	2	2	2	2	2	2	5	3	2	2
ANSW 003	5	7	8	9	10	10	10	10	9	8	7	9	8	7	9	8	7	7	9	9	10	10	10	9
AMLP S001	2	2	3	4	5	6	6	7	6	8	4	5	4	2	2	2	2	2	2	2	5	3	2	2
AMLP S002	2	2	3	4	5	6	6	7	6	8	4	5	4	2	2	2	2	2	2	2	5	3	2	2
AMLP S003	2	2	3	4	5	6	6	7	6	8	4	5	4	2	2	2	2	2	2	2	5	3	2	2
Hotel Guest Data	10	10	10	10	10	10	10	10	9	10	9	10	10	10	10	-	-	-	-	-	-	-	-	-
Hotel Employee Data	5	5	5	5	6	7	8	10	9	9	7	9	10	7	10	-	-	-	-	-	-	-	-	-
Payment Process	6	7	8	8	9	9	9	10	6	9	10	10	10	10	10	10	10	10	10	10	10	10	10	10
Reservation Process	6	7	8	8	9	9	9	10	6	9	10	10	10	10	10	10	10	10	10	10	10	10	10	10
Traffic Log	7	7	8	9	9	10	10	10	10	10	8	10	10	10	10	10	9	9	10	8	10	10	10	8

Data																							
Workstation Data	2	3	4	4	6	6	7	8	7	10	6	7	9	9	10	7	8	8	1	7	10	10	7	9
Website	4	5	6	6	7	7	8	8	6	7	5	6	3	4	6	7	7	7	7	7	8	8	6	5
Website Database	4	5	6	6	7	7	8	8	6	7	5	6	3	4	6	7	7	7	7	7	8	8	6	5

Σημείωση: Τα νούμερα στον παραπάνω πίνακα είναι παραδείγματα και όχι μέρος της εργασίας.

B2. 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

Σε αυτό το σημείο, έχοντας ερευνήσει το ξενοδοχειακό συγκρότημα και παραθέσει τις σημαντικότερες απειλές και ευπάθειες σας παρουσιάζουμε τα μέτρα ασφαλείας που πρέπει να παρθούν για την ασφαλέστερη και ομαλότερη λειτουργία του ξενοδοχείου.

Τα μέτρα έχουν εφαρμογή στο ΠΣ του Relax and Joy.

Α1 Προσωπικό – Προστασία Διαδικασιών Προσωπικού

- Συνεχής εκπαίδευση και αξιολόγηση του προσωπικού, για την τήρηση των κανόνων ασφαλείας και τρόπου λειτουργίας του ξενοδοχείου.
- Συνεχής ενημέρωση του προσωπικού για τα σχέδια ασφαλείας της επιχείρησης.
- Εκπαίδευση και χρήση κρυπτογραφίας για την χρήση ψηφιακών υπογραφών και κρυπτογράφηση σημαντικών δεδομένων που μεταφέρονται στο δίκτυο.
- Ορισμός υπευθύνου επεξεργασίας για την επίβλεψη και την αναθεώρηση στις διαδικασίες ασφαλείας καθώς και τον εντοπισμό νέων απειλών και ευπαθειών.
- Καταγραφή του ρόλου του προσωπικού ώστε να αποδοθούν συγκεκριμένες εργασίες και δικαιώματα. Οι ρόλοι αυτοί πρέπει να δημιουργούνται εγγράφως και να υπογράφεται από κάθε εργαζόμενο. Οι εργαζόμενοι έχουν δικαίωμα πρόσβασης για ανάγνωση μόνο του ρόλου και των προσωπικών στοιχείων του. Τέλος ο υπεύθυνος επεξεργασίας πρέπει να επαναλαμβάνει την διαδικασία αυτή ώστε να κρατάει τα δεδομένα αυτά ενημερωμένα.
- Καθορισμός διαδικασίας απόλυσης του προσωπικού με έμφαση στην ασφάλεια η οποία θα τηρείται κατά την αποχώρηση του υπαλλήλου. Μια τέτοια διαδικασία που μπορεί να ακολουθηθεί είναι:
    - Κατάργηση όλων των λογαριασμών πρόσβασης, των εξουσιοδοτήσεων και των κωδικών-συνθηματικών πρόσβασης.
    - Κατάργηση των λογαριασμών ηλεκτρονικού ταχυδρομείου και μη ανάθεσή τους σε άλλον ή άλλους υπαλλήλους (μη επαναχρησιμοποίηση τους).

- Επιστροφή οποιουδήποτε εξοπλισμού έχει παρασχεθεί στον υπάλληλο και ανήκει στον υπεύθυνο επεξεργασίας, (συμπεριλαμβανομένων υπολογιστών, κλειδιών, ηλεκτρονικών καρτών εισόδου/εξόδου, κ.λπ).

- Άμεση πρόσβαση στο προσωπικό σε documentation για διαδικασίες ασφαλείας.
- Επιβράβευση προσωπικού για εντοπισμό σφαλμάτων και κενών ασφαλείας μέσω feedback ή διαπιστευτηρίων.

A2 Ταυτοποίηση και αυθεντικοποίηση

- Επιβολή ισχυρών κωδικών στο προσωπικού που να τηρούνται οι παρακάτω κανόνες:
  - Να επιτρέπεται ίδιος κωδικός μεταξύ χρηστών
  - Κατά το login δεν πρέπει να υπάρχει ένδειξη «λάθος password» ή «λάθος username» αλλά «λάθος password ή username»
  - Να επιτρέπονται τρία λάθη στο login
  - Να ενθαρρύνει τους χρήστες να κάνουν συνδυασμούς γραμμάτων, αριθμών, ειδικών χαρακτήρων και σημείων στίξης κατά την δημιουργία των κωδικών τους
  - Ο κωδικός πρέπει να είναι αυστηρά μεγαλύτερος του 8
  - Αλλαγή κωδικού ανά τακτά χρονικά διαστήματα
  - Two factor authentication μέσω email ή sms
  - Last login session details
  - Χρόνος αδράνειας
- Τα συνθηματικά δεν πρέπει να είναι εγγεγραμμένα σε φυσικά μέσα (πχ postit, κόλλες Α4) ούτε να αποστέλνονται μέσω email.
- Σε περίπτωση τριών αποτυχημένων προσπαθειών πρόσβασης θα πρέπει να απαγορεύεται η πρόσβαση και να αποστέλλεται ειδοποίηση στον υπεύθυνο επεξεργασίας για να εξετάσει την εξουσιοδότηση του χρήστη και να επαναφέρει τον κωδικό.
- Η αποθήκευση των κωδικών να γίνεται με την χρήση τεχνικών salting, hashing και κρυπτογράφησης.
- Μια καλή λύση θα ήταν η εδραίωση ενός συστήματος Kerberos.

A3 Έλεγχος προσπέλασης και χρήσης πόρων

- Χρήση συστήματος με card readers για την είσοδο έξοδο των υπαλλήλων σε χώρους που υπάρχουν οι servers για την προστασία από μη εξουσιοδοτημένου προσωπικό.
- Κάθε πόρος/μηχάνημα του οργανισμού πρέπει να περιέχει διαδικασία επιβεβαίωσης για εγκατάσταση νέου λογισμικού ή πρόσβαση σε url που βρίσκεται εκτός του firewall.
- Καθορισμός δικαιωμάτων που να περιορίζουν την χρήση και προσπέλαση πόρων του ΠΣ.
- Ενημέρωση του υπευθύνου ασφαλείας σε περίπτωση που υπάρχει ύποπτη κίνηση σε κάποιον πόρο.
- Μια καλή λύση θα ήταν η εδραίωση ενός συστήματος Kerberos για την προσπέλαση αρχείων από τους servers.

A4 Διαχείριση εμπιστευτικών δεδομένων

- Εφαρμογή μεθόδων κρυπτογράφησης δεδομένων που είναι αποθηκευμένα στους servers όπως δεδομένων διαδικασιών ή username και password.
- Δημιουργία διαδικασιών αντιγράφων ασφαλείας κατά την διάρκεια της νύχτας για την αποφυγή απώλειας πληροφορίας από κάποια τυχαία ή σκόπιμη απειλή.
- Απαγόρευση διαχείρισης δεδομένων εκτός του χώρου της επιχείρησης εκτός αν εδραιωθεί VPN δίκτυο για remote access υπαλλήλων.
- Απλοποίηση των μηνυμάτων και της διεπαφής για την αποφυγή λανθασμένης διαγραφής και επεξεργασίας δεδομένων.
- Χρήση τεχνικών κρυπτογράφησης όπως ο RSA που είναι πρωτόκολλο κοινά αποδεκτό από την επιστημονική κοινότητα.

A5 Προστασία από τη χρήση υπηρεσιών από τρίτους

- Για την χρήση διαδικασιών του ξενοδοχείου απαιτείται one time passwords που θα εκδίδονται μετά την έγκριση του υπευθύνου ασφαλείας και μέσω ενός δικτύου VPN με χρήση πρωτοκόλλου https.
- Ο υπεύθυνος επεξεργασίας πρέπει να αναπτύξει διαδικασία ασφαλούς υλοποίησης/συντήρησης λογισμικού (πχ Web Site, Proccess Payment), ώστε να εντοπιστούν τυχόν ευπάθειες αυτού προτού γίνει χρήση από τρίτους χρήστες. Εφόσον η ανάπτυξη/συντήρησης της εφαρμογής γίνεται από εξωτερικό παράγοντα ο υπεύθυνος επεξεργασίας θα πρέπει να καθορίσει τις προδιαγραφές του συστήματος καθώς να προβεί σε ένα Service Level Agreement με την αρμόδια εταιρία.
- Χρήση intrusion detection software για την κίνηση πληροφοριών από και προς τους servers με κανόνες που διασφαλίζουν την ακεραιότητα τους.
- Χρήση δύο διαφορετικών VLAN δικτύων. Το ένα θα διατίθεται για το προσωπικό και το άλλο στους επισκέπτες.
- Έξοδος του χρήστη από διαδικασίες ή εφαρμογές ή λειτουργικό μετά από ένα χρονικό διάστημα αδράνειας.
- Απόρριψη κάθε μη τακτοποιημένης συσκευής από μηχανήματα της εταιρίας.

A6 Προστασία λογισμικού

- Αναβάθμιση λειτουργικών συστημάτων όλων των κόμβων του δικτύου.
- Όταν θα πραγματοποιείται ενημέρωση λογισμικού θα πρέπει να μην αλλάζουν ρυθμίσεις στο λογισμικό που αφορούν θέματα ασφαλείας.
- Ενημέρωση εργαζομένων που είναι αρμόδιοι για το software σε θέματα νέων απειλών, για προϊόντα antivirus και κενά ασφαλείας.
- Θα πρέπει όλοι οι ηλεκτρονικοί υπολογιστές και ο εξοπλισμός πληροφορικής καθώς και οι διαδικασίες να ενημερώνονται άμεσα με updates τα καινούργια patches.
- Εφαρμογή τεχνικών TDDE για ανάπτυξη και συντήρηση εφαρμογών καθώς και συχνά testing.
- Έλεγχος εφαρμογών πριν την εκκίνησή τους για πιθανή ύποπτη αλλαγή του πηγαίου κώδικα.
- Εδραίωση πολιτικής για της εξουσιοδοτημένες εφαρμογές.

A7 Διαχείριση ασφάλειας δικτύου

- Χωρισμός του δικτύου σε σαφή υποδίκτυα ανά χώρο με μάσκα 255.255.255.192/26

    - Room Area: 192.168.1.1 - 192.168.1.62
    - Office: 192.168.1.65 - 192.168.1.126
    - Hotel dining room: 192.168.1.129 - 192.168.1.190
    - Hotel Conference room: 192.168.1.193 - 192.168.1.254
- Προσθήκη firewall πριν το router ή hub του κάθε υποδικτύου για αποφυγή αθέμητης κυκλοφορίας στο δίκτυο και intrusion detection software πριν το public router για το μπλοκάρισμα κίνησης από το internet.
- Αλλαγή του wireless access point στον υποδίκτυο του office σε router για την αποφυγή εξωτερικών κακόβουλων χρηστών.
- Αλλαγή του network hub στο Hotel Dining Room σε router.
- Χρήση συστήματος IPS για ανίχνευση και αποτροπή κακόβουλης δραστηριότητας σε πραγματικό χρόνο. Η χρήση του θα γίνεται σε συνεργασία με τα firewall για την ανάλυση των πακέτων πριν φτάσουν στα router της επιχείρησης.
- Τακτικός έλεγχος του traffic log του broadband server για την ανάλυση της κίνησης του δικτύου.
- Περιορισμός των αιτημάτων(Rate limiting) στους server για την αποφυγή επιθέσεων όπως Denial of service.
- Ρύθμιση των configuration των server ώστε να μπλοκαριστούν αθέμητες ανοιχτές port.
- Απαραίτητες κρυπτογραφημένες συνεδρίες για την αποφυγή επιθέσεων όπως XSS.

A8 Προστασία από ιομορφικό λογισμικό

- Θα πρέπει να πραγματοποιείται λήψη ημερήσιου backup των δεδομένων με καθορισμένες ασφαλείς μεθόδους και σε καθορισμένους χρόνους ώστε σε περίπτωση που εντοπιστεί κάποιο ιομορφικό λογισμικό να μπορεί να επανέλθει το μηχάνημα στην αρχική του κατάσταση.
- Εγκατάσταση antivirus σε όλους τους υπολογιστές της επιχείρησης ώστε να υπάρχει πρόληψη κατά των πιο γνωστών ιον.
- Χρήση anti-ransomware προγραμμάτων τα οποία εμποδίζουν την ακεραιότητα των δεδομένων και των διαδικασιών από τέτοιες επιθέσεις.
- Δημιουργία πολιτικών δικαιωμάτων και αδειοδότησης χρήσης προγραμμάτων για όλους τους χρήστες.
- Πολιτικές απαγόρευσης σε πειρατικά site και torrents που μπορεί να προκαλέσουν ζημία στην επιχείρηση.
- Πολιτικές

A9 Ασφαλής χρήση διαδικτυακών υπηρεσιών

- Χρήση ψηφιακών υπογραφών για την αλληλογραφία και επικοινωνία της εταιρίας.
- Χρήση κρυπτογράφησης δημοσίου κλειδιού σε κάθε συναλλαγή ή επικοινωνία της εταιρίας πάνω στο δίκτυο.
- Χρήση TLS/SSL πρωτοκόλλου με σκοπό οι διαδικασίες της επιχείρησης να είναι ασφαλής μέσω κρυπτογραφημένων συνδέσεων με τον πελάτη.
- Πρέπει να υπάρχει διαδικασία για τον επαρκή έλεγχο των δικτυακών συνδέσεων του εσωτερικού δικτύου του υπευθύνου επεξεργασίας από και προς το διαδίκτυο ή άλλα εξωτερικά, μη έμπιστα, δίκτυα όπως μέσω του σημείου ελέγχου της περιμέτρου (firewall). Οι συνδέσεις που ενεργοποιούνται μέσω του firewall και οι

υπηρεσίες που εξυπηρετούν πρέπει να εγκρίνονται από τον υπεύθυνο ασφαλείας. Πρέπει, επίσης, να τηρείται επικαιροποιημένος κατάλογος με τις εγκεκριμένες συνδέσεις από και προς το δίκτυο του υπευθύνου επεξεργασίας και τις υπηρεσίες που εξυπηρετούν.

- Πρέπει να αποφεύγεται η χρήση ευπαθών ως προς την ασφάλεια πρωτοκόλλων όπως FTP, telnet (όπου δεν γίνεται κρυπτογράφηση) και, όταν υπηρεσίες τέτοιων πρωτοκόλλων είναι αναγκαίες, να γίνεται χρήση των αντίστοιχων ασφαλών (όπως, για παράδειγμα, SFTP, SSH).

A10 Ασφάλεια εξοπλισμού

- Δημιουργία αποθέματος για αναπλήρωση κρίσιμου εξοπλισμού.
- Αγορά μηχανημάτων UPS για εναλλακτική πηγή ρεύματος ή ενεργοποίηση αυτόν για την σταθεροποίηση της τάσης.
- Πρέπει να υπάρχουν τα κατάλληλα μέτρα ελέγχου φυσικής πρόσβασης στους κρίσιμους χώρους όπου βρίσκεται ο φυσικός εξοπλισμός που υποστηρίζει τα πληροφοριακά συστήματα και την επεξεργασία προσωπικών δεδομένων, έτσι ώστε να επιτρέπεται η πρόσβαση μόνο σε εξουσιοδοτημένο προσωπικό (για παράδειγμα, κάποιοι χώροι όπως αυτοί που βρίσκεται ο δικτυακός εξοπλισμός και οι servers πρέπει να είναι μόνιμα κλειδωμένοι). Σε ορισμένες δε περιπτώσεις θα ήταν ιδανικό να καταγράφεται κάθε πρόσβαση σε συγκεκριμένο φυσικό χώρο.
- Τοποθέτηση εξοπλισμού σε περιοχές της κτηριακής εγκατάστασης που δεν είναι ευπαθή σε φυσικές καταστροφές, πχ ισόγειο σε πλημμύρες.
- Εγκατάσταση κρυφών καμερών CCTV σε σημαντικούς για την επιχείρηση χώρους.

A11 Φυσική ασφάλεια κτιριακής εγκατάστασης

- Εγκατάσταση κρυφών καμερών CCTV σε σημαντικούς για την επιχείρηση χώρους.
- Σύστημα πυροπροστασίας, ανιχνευτών καπνού και τοποθέτηση πυροσβεστικών κρουνών.
- Αγορά και εγκατάσταση γεννήτριας Η/Ζ.
- Συναγερμός πόρτες και παράθυρα ασφαλείας σε δωμάτια και computer rooms.
- Αδιάλειπτη παροχή ρεύματος μέσω σταθεροποιητών/γεννητριών σε περίπτωση διακοπής ρεύματος μέσω μηχανημάτων UPS ή Η/Ζ.

Α4. ΣΥΝΟΨΗ ΠΙΟ ΚΡΙΣΙΜΩΝ ΑΠΟΤΕΛΕΣΜΑΤΩΝ

Τα πιο κρίσιμα προβλήματα που βρέθηκαν κατά την έρευνα μας είναι οι ευπάθειες που αφορούν τις διαδικασίες που συνεργάζονται με τους servers και τα δεδομένα της επιχείρησης. Αποτελούν τις σημαντικότερες απειλές καθώς υπάρχει η περίπτωση οικονομικής ζημίας της επιχείρησης καθώς απώλεια της διαθεσιμότητας των υπηρεσιών της. Συνεπώς, είναι απαραίτητη η αλλαγή της πρόσβασης μέσω wireless στην τοποθεσία του office ώστε το δίκτυο να έχει περιορισμένη πρόσβαση από τους υπαλλήλους καθώς και η εφαρμογή κρυπτογραφίας πάνω στα session. Επίσης πρέπει να γίνει αναβάθμιση του λειτουργικού συστήματος κάθε κόμβου για να έχει τα τελευταία security patches και updates, καθώς το παλαιό λογισμικό είναι εξαιρετικά ευπαθές. Επειδή τα δεδομένα της επιχείρησης είναι επίσης στο 5% των πιο κρίσιμων αγαθών της επιχείρησης είναι απαραίτητη η κρυπτογραφία τους αλλά και η δημιουργία τακτικών αντιγράφων ασφαλείας. Τέλος, το δίκτυο πρέπει να δομηθεί σε στατικά υποδίκτυα καθώς ο επιτιθέμενος με την απόκτηση ενός wireless access point ή server έχει την δυνατότητα να αποκτήσει πρόσβαση στους άλλους servers καθώς και τα workstations όπου και βρίσκονται οι διαδικασίες και τα δεδομένα της επιχείρησης.