ΑΣΦΑΛΕΙΑ ΠΛΗΡΟΦΟΡΙΑΚΩΝ ΣΥΣΤΗΜΑΤΩΝ ΚΑΙ ΚΡΙΣΙΜΩΝ ΥΠΟΔΟΜΩΝ

ΣΧΕΔΙΟ ΑΣΦΑΛΕΙΑΣ

ΣΥΓΓΡΑΦΕΙΣ: Στρίκλαντ Ελένη 3140252 και Μπούσουλας-Ραϊκίδης Ορφέας-Γεώργιος 3160111

ΕΡΓΑΣΙΑ ΧΕΙΜΕΡΙΝΟΥ ΕΞΑΜΗΝΟΥ 2018-19

A1.Contents

Α1. ΕΙΣΑΓΩΓΗ

Καλούμαστε να δημιουργήσουμε ένα ολοκληρωμένο σχέδιο ασφάλειας για το πληροφοριακό σύστημα ενός ξενοδοχείου. Σκοπός αυτού του Risk Assessment είναι ο προσδιορισμός ευπαθειών και απειλών τόσο του πληροφοριακού συστήματος όσο και των υποδομών του ξενοδοχείου "Flamel". Το σχέδιο ασφάλειας που σας παρουσιάζουμε είναι έτοιμο προς χρήση με κύριο στόχο την μείωση των κινδύνων.

Α1.1 Περιγραφή Εργασίας

Στο σχέδιο ασφάλειας θα δείτε αναλυτικά τα βήματα που ακολουθήσαμε από την καταγραφή αγαθών έως την εύρεση μέτρων ασφάλειας με τελικό στόχο την εκτενή πρόταση μας για την κάλυψη των κενών ασφάλειας που βρέθηκαν κατά τη διάρκεια της έρευνας που πραγματοποιήσαμε.

Α1.1 Δομή παραδοτέου

Ακολουθώντας την μέθοδο μελέτης ασφάλεια που παρουσιάζεται αναλυτικά παρακάτω, το παραδοτέο θα απαρτίζεται από τρία βασικά μέρη, αποτίμηση αγαθών, ανάλυση επικινδυνότητας και τέλος παρουσίαση ολοκληρωμένου σχεδίου ασφάλειας με προτεινόμενα μέτρα ασφαλείας. Στο πρώτο μέρος θα υπάρχει αναλυτική καταγραφή των αγαθών του πληροφοριακού συστήματος και των υποδομών του ξενοδοχείου, στη συνέχεια θα δείτε πίνακες με όλα τα αγαθά, τις απειλές, τις ευπάθειες καθώς και τα αποτελέσματα της έρευνάς μας ταξινομημένα με βάση την κρισιμότητα τους για το ξενοδοχείο συνοδευόμενα με πίνακα αναλυτικού υπολογισμού επικινδυνότητας. Τέλος θα ολοκληρώσουμε με την παρουσίαση προτεινόμενων μέτρων ασφαλείας και μία σύνοψη των πιο κρίσιμων αποτελεσμάτων.

Α2. ΜΕΘΟΔΟΛΟΓΙΑ ΜΕΛΕΤΗΣ ΑΣΦΑΛΕΙΑΣ

Για τη Διαχείριση Επικινδυνότητας του Σχεδίου Ασφάλειας για το Πληροφοριακό Σύστημα Ξενοδοχείου "Flamel" 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*

Α1.2 Περιγραφή Πληροφοριακού Συστήματος (ΠΣ) υπό έλεγχο

Στην ενότητα αυτή, καταγράφονται τα υφιστάμενα πληροφοριακά συστήματα του Ξενοδοχείου "Flamel" τα οποία με το πέρας της μελέτης θα επικαιροποιηθούν, αναβαθμιστούν ή σε κάποιες περιπτώσεις αντικατασταθούν. Να σημειωθεί ότι έχουμε προσθέσει τρεις επιπλέον χώρους από αυτούς που περιλαμβάνει το δοσμένο διάγραμμα, τα Αποδυτήρια των υπαλλήλων, το Λογιστήριο και την Reception του ξενοδοχείου.

Α1.2.1 Υλικός εξοπλισμός (hardware)

Θα χωρίσουμε τον εξοπλισμό του ξενοδοχείου σε κατηγορίες σύμφωνα με τη χρήση τους και την τοποθεσία τους στο κτήριο.

Servers

Το ξενοδοχείο παρέχει τρεις servers στο δωμάτιο του γραφείου, File server(AMSRV001), Broadband Access server(AMSRV002) και Database server(AMSRV003). Στο ίδιο δωμάτιο βρίσκονται επίσης και καλώδια που συνδέουν τον κεντρικό υπολογιστή και τους servers με το router. Ο AMSRV001 συνδέεται μέσω ACC005, ο AMSRV002 μέσω ACC002, ο AMSRV003 μέσω ACC004 και ο κεντρικός υπολογιστής (AMCWS005) συνδέεται μέσω ACC002 με το router.

Laptops

Υπάρχουν τρία laptop στο ξενοδοχείο. Το laptop(AMLPS001) που βρίσκεται στο Room Area και αντιπροσωπεύει όλα τα laptop για όλα τα δωμάτια του ξενοδοχείου, το laptop(AMLPS002) το οποίο βρίσκεται στο χώρο διασκέψεων και τέλος το laptop(AMLPS003) που βρίσκεται στο εστιατόριο. Και τα τρία μπορούν να συνδεθούν στο ίντερνετ μέσω των wireless access points.

Κάμερες

Στο ξενοδοχείο έχουν τοποθετηθεί τρεις κάμερες. Η κάμερα(CA0001) βρίσκεται στον χώρο με τα αποδυτήρια των υπαλλήλων όπου αφήνουν τα προσωπικά τους αντικείμενα συμπεριλαμβανομένου τα iPads και τις κάρτες πρόσβασης. Η κάμερα(CA0002) βρίσκεται στο χώρο του γραφείου όπου βρίσκονται και οι servers και τέλος η κάμερα(CA0003) βρίσκεται στην reception του ξενοδοχείου η οποία είναι και συνδεδεμένη στο ίντερνετ.

Περιφερειακά

- Στο χώρο διασκέψεων υπάρχει ένας προτζέκτορας(AMPR001).
- Στο γραφείο υπάρχει ένας εκτυπωτής(AMPN001).
- Στη reception του ξενοδοχείου υπάρχει μηχανημα POS(POS01).

Κάρτες-Κλειδιά Πρόσβασης

Οι υπάλληλοι του ξενοδοχείου χρησιμοποιούν κάρτες κλειδιά για να έχουν πρόσβαση είτε στα δωμάτια των πελατών είτε στους υπόλοιπους χώρους τους ξενοδοχείου όπως το γραφείο. Οι κάρτες-κλειδιά βρίσκονται στα αποδυτήρια με σκοπό ο κάθε υπάλληλος να κρατά την δική του κάρτα στην οποία αναγράφεται το όνομα, το επώνυμο και ο κωδικός του.

Tablets Ενδοεπικοινωνίας

Κάθε υπάλληλος κατέχει από ένα tablet το οποίο παρέχει ποικίλες λειτουργίες όπως την επικοινωνία με συναδέλφους αλλά και τους πελάτες, πρόσβαση σε χάρτη του ξενοδοχείου κτλ. Υπάρχουν 30 Tablets (AMIC001 έως AMIC030) για όλους τους υπαλλήλους και βρίσκονται στα αποδυτήρια των υπαλλήλων.

A1.2.2 Λογισμικό και εφαρμογές

Οι υπάλληλοι του ξενοδοχείου, όπως αναφέρθηκε, χρησιμοποιούν tablets για την ενδοεπικοινωνία τους και χρησιμοποιούν μία εφαρμογή της εταιρίας Intercom. Μέσω αυτής της εφαρμογής μπορούν να επικοινωνούν με άλλους συναδέλφους, να ανταποκρίνονται γρήγορα σε τυχόν υπηρεσίες δωματίου, καθώς και για την υλοποίηση αιτημάτων των πελατών.

Να σημειωθεί επίσης ότι στον κεντρικό υπολογιστή του γραφείου έχει εγκατασταθεί λογισμικό Windows 10.

A1.2.3 Δίκτυο

Το Public Network Router(ANSW003) συνδέεται σύμφωνα με το δοσμένο σχέδιο με τρία router και ένα hub. Θα δούμε όλα τα αγαθά που αφορούν το δίκτυο και πως συνδέονται ανά δωμάτιο.

Office

Το ANSW003 συνδέεται μέσω ACC014 με το firewall(AMFW001), το οποίο με τη σειρά του συνδέεται μέσω ACC001 με το router B(AMCRT003).

Room Area

Το ANSW003 είναι συνδεδεμένο με το router A(AMCRT004) μέσω ACC013. Το router βρίσκεται στον πρώτο όροφο του ξενοδοχείου. Στο AMCRT004 είναι συνδεδεμένα δύο fast ethernet switch με κωδικούς AMSW001 και AMSW002 μέσω ACC006 και ACC007 αντίστοιχα. Επίσης είναι συνδεδεμένο με ένα managed switch(AMCSW004) μέσω ACC008 το οποίο με τη σειρά του συνδέεται με wireless access point(AMWAP004). Τα fast ethernet switch ανανεώνονται ανά δύο ορόφους έτσι ώστε οι πελάτες τους

ξενοδοχείου να μπορούν να συνδεθούν και μέσω καλωδίων στο ιντερνετ. Αυτό επιτυγχάνεται μέσω καλωδίων που ξεκινούν από τα switches και καταλήγουν σε πρίζες σε κάθε δωμάτιο του ξενοδοχείου.

Hotel Dining Area

Στο χώρο του εστιατορίου το ANSW003 συνδέεται με το AMHB001, ένα network hub μέσω ACC015, το οποίο κατ επέκταση συνδέεται και αυτό με managed switch(AMCSW006) μέσω ACC009. Το δωμάτιο έχει και αυτό wireless access point(AMWAP001) και το switch συνδέεται με αυτό μέσω ACC010.

Hotel Conference Room

Στον χώρο διασκέψεων υπάρχει το router D(AMCRT006) το οποίο συνδέεται με το ANSW003 μέσω ACC016. Το router συνδέεται μέσω ACC011 με το managed switch(AMCSW007) το οποίο με τη σειρά του συνδέεται με το wireless access point(AMWAP002) μέσω ACC012.

A1.2.4 Δεδομένα

Όσον αφορά τα δεδομένα του ξενοδοχείου τα χωρίσαμε σε ψηφιακή μορφή και σε μορφή εγγράφων ότι βρίσκεται δηλαδή στον server AMSRV001 και AMSRV003 και σε έγγραφα στο Λογιστήριο αντίστοιχα.

Oracle Database Server - AMSRV003

Στον server AMSRV003 είναι αποθηκευμένα όλα τα δεδομένα των υπαλλήλων του ξενοδοχείου πρώην και νυν καθώς και τα δεδομένα των πελατών. Σε κάθε υπάλληλο αντιστοιχεί ένας κωδικός και αποθηκεύονται τα στοιχείου του και η θέση του, ενώ για κάθε πελάτη αποθηκεύονται εκτός από τα στοιχεία του, το ιστορικό διαμονής του, οι αγορές του καθώς και ο τρόπος πληρωμής και κατ' επέκταση τα στοιχεία της πιστωτικής του κάρτας.

Oracle File Server - AMSRV001

Στον server AMSRV001 αποθηκεύονται οι κασέτες και των τριών καμερών ασφάλειας και διατηρούνται για δύο χρόνια από την πρώτη μέρα καταγραφής τους.

Λογιστήριο

Στο λογιστήριο βρίσκονται όλα τα δεδομένα όσον αφορά τις διαδικασίες της κράτησης δωματίων και πληρωμής υπαλλήλων εγγράφως. Σε έγγραφη μορφή βρίσκονται και οι καρτέλες των υπαλλήλων καθώς και των πελατών με όλα τα στοιχεία τους και το ιστορικό της διαμονής τους στο ξενοδοχείο "Flamel".

A1.2.5 Διαδικασίες

Οι διαδικασίες που βρέθηκαν ως αγαθά για το ξενοδοχείο "Flamel" είναι η πληρωμή των υπαλλήλων και η κράτηση δωματίων των πελατών. Και οι δύο πραγματοποιούνται στον υπολογιστή του γραφείου.

Α3. ΑΠΟΤΙΜΗΣΗ ΠΣ ΚΑΙ ΕΓΚΑΤΑΣΤΑΣΕΩΝ

Α1.3 Αγαθά που εντοπίστηκαν¶

Asset name	Model	Priority
AMSRV001	Oracle File Server	HIGH
AMSRV003	Oracle Database Server	HIGH
AMSRV002	Alcatel 7410 Broadband Access Server	HIGH
Payment Process	-	HIGH
AMCWS005	Dell Optiplex 3060 SFF	HIGH
Hotel Guest Data	-	HIGH
Hotel Employee Data	-	HIGH
CCTV Data	-	HIGH
Reservation Process	-	HIGH
Hotel Employee Key Cards	-	HIGH
Payment Process	-	HIGH

AMHB001	LB-Link BL-S515	MEDIUM
AMWAP001-AMWAP004	Cisco Aironet 3802I Radio	MEDIUM
AMSW001-AMSW002	FS108 32 Port Fast Ethernet Switch	MEDIUM
ANSW003	FS110 Network Router	MEDIUM
AMLPS001-AMLPS003	Apple MacBook Pro 13.3	MEDIUM
AMCSW004/AMCSW006/AMCSW007	D-Link DGS-1100-10MPP	MEDIUM
AMCRT003	TP-LINK Archer C60 v1	MEDIUM
Windows 10	-	MEDIUM
AMCRT004	TP-LINK Archer C60 v1	MEDIUM
AMCRT006	TP-LINK Archer C60 v1	MEDIUM
AMFW001	Fortinet-Fortigate-100D	MEDIUM
CA0003	DS-2CD3132-I	MEDIUM
CA0001-CA0002	DS-2CD3132	MEDIUM
InterCommunication App	-	MEDIUM
POS01	VX 675	MEDIUM
AMIC001-AMIC030	iPad Pro	LOW
Cables ACC001-ACC016	-	LOW
AMPN001	HP OfficeJet Pro 6978	LOW
AMPR001	Casio Slim XJ-A247 DLP	LOW
Payment Hard Copy/ Reservation Hard Copy	-	LOW

Hotel Guest/Employee Hard Copy	-	LOW
Outlets RJ45	-	LOW

A1.4 Απειλές που εντοπίστηκαν

Παρακάτω αναφέρονται οι πιο σημαντικές απειλές που βρέθηκαν σύμφωνα με το αρχείο ISO27k FMEA ανά κατηγορίες καθώς και τα αγαθά που προσέβαλαν.

- Illegitimate access/Unauthorized changes to data
  - CCTV/Employee data.
  - Firewall
  - Laptop
  - Database Server/Broadband Access Server
  - Network
- Malware Attack/Malicious Code
  - Windows 10
  - PC
  - Switch
- Unintentional change of data in an information system
  - File Server
- Technical failure/Malfunction of equipment
  - Outlets
  - Public Network Router
  - Printer
  - POS
- Information leakage/Compromising confidential information/Disclosure of information
  - Employee/Guest data
  - CCTV data
- Insider threat
  - File Server
  - Laptop
- Falsification of records/Unauthorized changes or modification of administrative settings
  - Employee/Guest data
  - Hard Copies
  - Reservation/Payment process
  - Firewall.
- User error/Human Error/Disaster Caused by human
  - Cables
  - Software
  - Tablet.
- Theft
  - Access key cards
  - Tablet
- Fire
  - Hard Copies

- Access to the network by unauthorized person
    - Devices that are connected to the internet e.g. CCTV security camera
- Failure of communication links
    - Fast ethernet switch
    - Managed switch
- Loss of electricity/Fuse tripping
    - Firewall
    - Projector
- Unauthorized physical access
    - Access Key Cards
- Eavesdropping
    - Broadband Access Server
    - Network Hub
- Remote attackers bypass authentication
    - Network Hub
- Fraud
    - POS
- Unauthorized use of software
    - PC
- Interruption of business processes
    - Payment/Reservation process

A1.5 Ευπάθειες που εντοπίστηκαν

Παρακάτω θα δούμε κάποιες από τις πιο σημαντικές ευπάθειες και που μπορούν να οδηγήσουν. Να σημειωθεί ότι σαν impact καταγράφονται πρώτου ή δεύτερου βαθμού σενάρια.

- Not encrypted database
    - Data Corruption
    - Destruction of records
    - Loss of reliability
- Inadequate replacement of older equipment/Equipment sensitivity to changes in voltage/ Inadequate maintenance
    - Devices not available
    - Loss of power
- Default passwords not changed
    - Malware Attack
    - Illegitimate access to data
- Inadequate control of physical access/Lack of physical protection
    - Theft
    - Leakage of hotel data
    - Destruction of equipment
    - Disaster caused by human
- Inadequate network management
    - Illegitimate access to the network
- Inadequate classification of information
    - Loss of reliability and integrity

- Lack of systems for identification and authentication
    - Cannot execute hotel processes
    - Unauthorized access to personal data
- Lack of access control policy
    - Data Corruption
    - Leakage of hotel data
- Inadequate supervision of employee/Human-User error/Inadequate training of employees
    - Hotel hardware/devices not available/broken
    - Not using software correctly
    - Delay to execute hotel process
- Software errors/Software Not updated/Undocumented software
    - Unauthorized access to network
    - Not available software
    - Backdoor for later attacks
    - Modification of administrative settings
- Unmotivated employees
    - Strike
    - Industrial espionage
- Inadequate capacity management
    - Cannot update back up
    - Data corruption
- Unprotected public network connections
    - GDPR Violation
    - Breach of legislation
- Inadequate protection of cryptographic keys
    - Unauthorized access to network
    - Unauthorized access to data
    - Loss of reliability

A1.6 Αποτελέσματα αποτίμησης

Παρακάτω αναπαρίσταται πίνακας με όλα τα αγαθά και το impact που θα δεχτεί το ξενοδοχείο εάν προσβληθεί η διαθεσιμότητα, η ακεραιότητα και η εμπιστευτικότητα αυτών. Το impact έχει υπολογιστή με βάση τη χειρότερη περίπτωση και η κλίμακα είναι από 1 έως 10.

	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
AMCWS005 Dell Optiplex	1	2	3	3	5	5	6	7	5	6	2	5	4	5	7	1	6	3	2	5	5	7	4	2
AMSRV001 Oracle File Server	3	3	4	4	6	7	7	8	6	7	4	6	4	7	7	1	6	5	5	4	3	7	5	3
AMSRV002 Broadband Access Server	1	1	2	2	3	4	5	6	4	6	2	5	1	1	4	1	6	5	6	3	5	4	4	2
AMSRV003 Oracle Database Server	3	4	4	5	6	7	7	8	7	7	4	6	4	7	7	1	6	5	5	4	3	7	5	3
AMCSW004 Managed Switch	1	2	3	3	4	4	5	6	4	5	2	4	1	1	2	1	4	4	3	2	5	7	4	2
AMCSW006 Managed Switch	1	1	2	3	3	4	4	6	4	5	2	4	1	1	2	1	4	4	3	2	5	7	4	2
AMCSW007 Managed Switch	1	1	2	3	3	4	4	6	4	5	2	4	1	1	2	1	4	4	3	2	5	7	4	2
AMCRT003 Router	3	4	4	5	6	7	8	8	7	7	2	4	2	2	3	1	7	7	5	2	5	7	4	2
AMCRT004 Router	1	1	2	3	4	5	6	7	6	6	2	4	2	2	3	1	7	7	5	2	5	7	4	2
AMCRT006 Router	1	1	1	1	2	2	4	7	6	6	2	4	2	2	3	1	7	7	5	2	5	7	4	2
AMFW001 Firewall	3	3	4	4	5	6	7	8	6	7	3	5	2	4	6	1	7	7	2	1	5	4	5	3

AMHB001 Network Hub	1	1	1	2	3	3	3	6	4	5	2	4	1	1	2	1	5	5	2	5	2	7	4	2
AMWAP001 Wireless Access Point	1	1	2	2	3	3	3	6	4	5	2	4	2	3	4	1	6	6	5	2	5	7	4	2
AMWAP002 Wireless Access Point	1	1	2	2	3	3	3	6	4	5	2	4	2	3	4	1	6	6	5	2	5	7	4	2
AMWAP003 Wireless Access Point	1	2	3	3	4	5	6	6	4	5	2	4	2	3	4	1	6	6	5	2	5	7	4	2
AMWAP004 Wireless Access Point	1	1	2	3	4	4	5	6	4	5	2	4	2	3	4	1	6	6	5	2	5	7	4	2
AMSW001 Fast Ethernet Switch	1	1	2	2	3	3	4	6	4	5	2	4	1	1	2	1	4	4	3	2	5	7	4	2
AMSW002 Fast Ethernet Switch	1	1	2	2	3	3	4	6	4	5	2	4	1	1	2	1	4	4	3	2	5	7	4	2
ANSW003 Public Network Router	4	4	5	5	6	7	8	8	7	7	3	6	2	4	7	1	7	7	5	2	5	7	5	3
AMLPS001 Mac Laptop	1	1	1	1	2	2	3	6	3	4	2	3	5	6	7	1	1	1	1	1	1	7	1	1
AMLPS002 Mac Laptop	1	1	2	2	3	3	3	6	3	4	2	3	1	3	3	1	1	1	1	1	1	3	1	1
AMLPS003 Mac Laptop	1	1	1	1	2	2	3	6	3	4	2	3	5	6	7	1	1	1	1	1	1	7	1	1
Hotel Guest Data	4	5	6	6	7	8	9	8	5	7	3	6	4	6	7	-	-	-	-	-	-	-	-	-
Hotel Employee Data	4	4	5	5	6	6	7	7	5	4	2	6	2	6	6	-	-	-	-	-	-	-	-	-
Windows 10	1	2	3	3	5	5	6	5	4	6	3	5	1	1	1	1	1	1	1	1	1	3	1	1
Payment Process	1	1	1	1	2	2	5	6	5	7	2	5	1	1	1	1	7	7	5	3	3	4	3	1
Reservation Process	1	2	2	3	4	5	5	6	5	7	2	5	1	1	1	1	7	7	5	3	3	4	3	1
Hotel Guest Hard Copy	1	1	3	3	6	6	7	7	5	6	2	5	3	6	7	-	-	-	-	-	-	-	-	-

Hotel Employee Hard Copy	1	1	3	3	6	6	7	7	5	6	2	5	2	5	7	-	-	-	-	-	-	-	-	-
Payment Hard Copy	1	1	3	3	6	6	7	7	5	6	2	5	2	5	7	-	-	-	-	-	-	-	-	-
Reservation Hard Copy	1	1	3	3	6	6	7	7	5	6	2	5	2	5	7	-	-	-	-	-	-	-	-	-
AMPR001 Projector	1	1	2	2	2	2	2	3	2	3	2	2	1	1	1	-	-	-	-	-	-	-	-	-
AMPN001 Printer	1	1	1	3	4	4	4	3	2	4	3	4	1	4	4	3	2	2	2	2	2	3	3	2
ACC001-ACC012 Cables	1	1	2	2	3	3	4	2	2	2	1	2	1	1	1	-	-	-	-	-	-	-	-	-
ACC013-ACC016 Cables	2	2	3	4	5	5	6	3	2	3	1	2	1	1	1	-	-	-	-	-	-	-	-	-
Hotel Employee Key Cards	1	1	1	1	2	2	3	5	4	6	2	5	1	4	7	-	-	-	-	-	-	-	-	-
AMIC001 - AMIC030 iPad Pro	2	2	3	3	4	5	6	3	2	5	2	5	1	6	7	2	6	6	3	5	6	7	5	2
InterCommunication App	2	2	3	3	4	5	6	8	5	7	2	5	1	4	6	2	2	2	3	3	4	7	5	2
CA0001 CCTV	1	1	2	2	3	4	5	5	3	5	2	6	2	4	5	1	4	4	1	2	1	3	2	1
CA0002 CCTV	1	1	2	2	3	4	5	5	3	5	2	6	2	4	5	1	4	4	1	2	1	3	2	1
CA0003 CCTV	2	2	3	3	4	5	5	6	4	6	2	6	3	5	6	1	4	4	1	2	1	6	3	2
POS01 POS	1	1	1	1	2	3	4	6	4	7	3	3	1	1	4	1	6	6	3	3	6	7	6	4
CCTV Data	4	4	5	5	6	7	8	10	9	10	5	8	2	6	7	-	-	-	-	-	-	-	-	-
Outlets RJ45	1	1	1	1	1	1	2	2	2	2	2	2	1	1	1	-	-	-	-	-	-	-	-	-

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

Παρακάτω παρουσιάζονται τα μέτρα ασφάλειας που προτείνουμε για το ΠΣ του Ξενοδοχείου “Flamel” ανα κατηγορία σύμφωνα με τις ευπάθειες που βρέθηκαν.

Α1 Προσωπικό – Προστασία Διαδικασιών Προσωπικού

- Εκπαίδευση όλου του προσωπικού σε θέματα ασφάλειας πληροφοριακών συστημάτων, με σκοπό την αποφυγή λαθών και την εκτέλεση κακόβουλου λογισμικού στα συστήματα του ξενοδοχείου, καθώς και πλήρη ενημέρωση τους ως προς την πολιτική προστασίας του πληροφοριακού συστήματος του ξενοδοχείου.
- Θέσπιση επίσημης πειθαρχικής διαδικασίας για τους υπαλλήλους που έχουν παραβεί τους κανόνες της πολιτικής προστασίας του πληροφοριακού συστήματος του ξενοδοχείου.
- Τα δικαιώματα εισόδου σε χώρους προσωπικού (π.χ. κάρτες-κλειδιά) θα πρέπει να αφαιρούνται από τους υπαλλήλους που δεν δουλεύουν πλέον για το ξενοδοχείο ή ο ρόλος τους στην εταιρία δεν χρειάζεται αυτά τα δικαιώματα.
- Οποιοσδήποτε εξοπλισμός δίνεται στους υπαλλήλους θα πρέπει να επιστρέφεται στο ξενοδοχείο σε περίπτωση που δεν δουλεύουν πλέον για το ξενοδοχείο.

Α2 Ταυτοποίηση και αυθεντικοποίηση

- Η ταυτοποίηση του πελάτη είναι απαραίτητη για την ορθή ολοκλήρωση της διαδικασίας πληρωμής και της διαδικασίας κράτησης.
- Η είσοδος δεδομένων στα προγράμματα του ξενοδοχείου, θα πρέπει να επικυρώνεται, έτσι ώστε να εξασφαλίζεται ότι τα δεδομένα είναι ορθά.
- Όλοι οι χρήστες του πληροφοριακού συστήματος του ξενοδοχείου θα πρέπει να διαθέτουν αποκλειστικό αναγνωριστικό (αναγνωριστικό χρήστη) μόνο για προσωπική τους χρήση και πρέπει να επιλέγει κατάλληλη τεχνική επαλήθευσης ταυτότητας για να τεκμηριώνεται η ταυτότητα του χρήστη.

- Για τους χρήστες που συνδέονται απομακρυσμένα στο δίκτυο του ξενοδοχείου χρειάζεται να γίνονται οι κατάλληλοι έλεγχοι ταυτοποίησης.

A3 Έλεγχος προσπέλασης και χρήσης πόρων

- Οι χρήστες του πληροφοριακού συστήματος του ξενοδοχείου επιτρέπεται να έχουν πρόσβαση μόνο στις υπηρεσίες για τις οποίες είναι εξουσιοδοτημένοι.
- Οι υποχρεώσεις και οι τομείς αρμοδιοτήτων των υπαλλήλων πρέπει να διαχωρίζονται για να μειωθούν οι ευκαιρίες για μη εξουσιοδοτημένη ή ακούσια τροποποίηση ή κατάχρηση των περιουσιακών στοιχείων του ξενοδοχείου.
- Η πρόσβαση στα λειτουργικά συστήματα απαιτείται να ελέγχεται μέσω ασφαλούς διαδικασίας σύνδεσης.
- Η πρόσβαση στις πληροφορίες και στις λειτουργίες του συστήματος εφαρμογών από τους πελάτες και τους υπαλλήλους πρέπει να περιορίζεται σύμφωνα με την καθορισμένη πολιτική ελέγχου πρόσβασης του ξενοδοχείου.

A4 Διαχείριση εμπιστευτικών δεδομένων

- Κρυπτογράφηση των ευαίσθητων δεδομένων των πελατών και υπαλλήλων του ξενοδοχείου με σκοπό την αποφυγή της επεξεργασίας τους σε περίπτωση που διαρρεύσουν.
- Η προστασία των δεδομένων και η προστασία της ιδιωτικής ζωής ιδιαίτερα των πελατών διασφαλίζονται όπως απαιτείται από τη σχετική νομοθεσία.
- Μόνο αυστηρά εξουσιοδοτημένοι χρήστες θα πρέπει να έχουν πρόσβαση στη βάση δεδομένων. Το ίδιο θα πρέπει να ισχύει και για το λογιστήριο, το οποίο περιέχει όλα τα δεδομένα αλλά σε έγγραφη μορφή.
- Ταξινόμηση των πληροφοριών βάσει της αξίας τους, των νομικών απαιτήσεων και της ευαισθησίας τους.
- Τα αρχεία καταγραφής ελέγχου που καταγράφουν πληροφορίες και δραστηριότητες των πελατών θα πρέπει να διατηρούνται για μια συμφωνημένη περίοδο με σκοπό να βοηθήσουν σε μελλοντικές έρευνες και πρόσβαση παρακολούθηση ελέγχου (πχ CCTV Data).

A5 Προστασία από τη χρήση υπηρεσιών από τρίτους

- Για την χρήση των διαδικτυακών υπηρεσιών που παρέχονται στους πελάτες του ξενοδοχείου από το ξενοδοχείο, θα πρέπει να οριστεί επίσημη διαδικασία εγγραφής και απεγγραφής χρήστη, έτσι ώστε μέσω αυτής να δίνεται και να αφαιρείται το δικαίωμα πρόσβασης στο πληροφοριακό σύστημα του ξενοδοχείου και τις υπηρεσίες αυτού.
- Οι δραστηριότητες των χρηστών που χρησιμοποιούν τις υπηρεσίες του ξενοδοχείου, θα πρέπει να καταγράφονται σε αρχεία καταγραφής τα οποία θα αποθηκεύονται για προσυμφωνημένη χρονική περίοδο, έτσι ώστε να συνδράμουν σε μελλοντικές έρευνες και την επιτήρηση της ορθής χρήσης των υπηρεσιών του πληροφοριακού συστήματος του ξενοδοχείου.
- Η κατανομή και η χρήση των προνομίων σε χρήστες πρέπει να περιορίζεται και να ελέγχεται.
- Η διοίκηση υποχρεούται να ελέγχει τακτικά τα δικαιώματα πρόσβασης στις υπηρεσίες τόσο των πελατών όσο και των υπαλλήλων του ξενοδοχείου.

A6 Προστασία λογισμικού

- Όλα τα λογισμικά που διαθέτει το ξενοδοχείο στους υπαλλήλους θα πρέπει να είναι αυθεντικά και πλήρως ενημερωμένα.
- Παροχή IDS λογισμικού σε όλες τις συσκευές για τυχόν παραβιάσεις της πολιτικής του ξενοδοχείου.

- Η πρόσβαση στον πηγαίο κώδικα των προγραμμάτων θα πρέπει να είναι αυστηρά εξουσιοδοτημένη.
- Θα πρέπει να υπάρχει διαδικασία ελέγχου πριν την εγκατάσταση νέου λογισμικού σε συσκευές.

A7 Διαχείριση ασφάλειας δικτύου

- Απαιτείται αυστηρός έλεγχος της φυσικής και λογικής πρόσβασης σε θύρες πρόσβασης του δικτύου του ξενοδοχείου, ώστε να μην μένουν ανοιχτές θύρες που δεν χρειάζονται.
- Αντικατάσταση του διανομέα δικτύου στην τραπεζαρία του ξενοδοχείου με συσκευή τύπου switch, ώστε τα πακέτα να μην δρομολογούνται σε όλους.
- Το δίκτυο του ξενοδοχείου πρέπει να διαχωριστεί έτσι ώστε τα ευαίσθητα και σημαντικά συστήματα του, όπως οι διακομιστές , να μην βρίσκονται στην ίδια εξωτερική δημόσια σύνδεση με το υποδίκτυο των πελατών.

A8 Προστασία από ιομορφικό λογισμικό

- Οι χρήστες θα πρέπει να ακολουθούν καλές πρακτικές ασφαλείας κατά την επιλογή και χρήση των κωδικών πρόσβασης με σκοπό την προστασία από μη εξουσιοδοτημένη πρόσβαση.
- Εγκατάσταση λογισμικού προστασίας από ιομορφικό λογισμικό και λογισμικό υποκλοπής.
- Εφαρμογή ελέγχων ανίχνευσης, πρόληψης και αποκατάστασης για προστασία από κακόβουλο λογισμικό.

A9 Ασφαλής χρήση διαδικτυακών υπηρεσιών

- Οι χρήστες των υπηρεσιών του πληροφοριακού συστήματος του ξενοδοχείου είτε πελάτες είτε υπάλληλοι οφείλουν να εξασφαλίζουν ότι ο εξοπλισμός, που είτε ανήκει στο ξενοδοχείο και τους έχει δοθεί από αυτό, είτε ανήκει στους ίδιους και τους έχει εκχωρηθεί άδεια πρόσβασης στις υπηρεσίες του πληροφοριακού συστήματος του ξενοδοχείου, είναι ασφαλής και δεν μπορούν να τον χρησιμοποιήσουν μη εξουσιοδοτημένοι χρήστες.
- Οι μη ενεργές συνδέσεις χρηστών θα πρέπει να τερματίζονται μετά από ορισμένο χρονικό διάστημα.
- Οι πληροφορίες που αφορούν τα ηλεκτρονικά μηνύματα, όπως αυτά στο σύστημα ενδοεπικοινωνίας των υπαλλήλων, πρέπει να προστατεύονται κατάλληλα

A10 Ασφάλεια εξοπλισμού

- Συντήρηση, συνεχής παροχή υποστήριξης στα μηχανήματα για βλάβες μικρού βαθμού και άμεση αντικατάσταση σε πολύ φθαρμένα μηχανήματα και εξοπλισμό με βλάβες μεγάλου βαθμού.
- Εγκατασταση UPS για την παροχή ηλεκτρικής ενέργειας σε περίπτωση διακοπής ρεύματος.
- Τοποθέτηση όλων των εκτεθειμένων καλωδίων σε κανάλια προστασίας καλωδίων.
- Όλα τα είδη εξοπλισμού που περιέχουν μέσα αποθήκευσης πρέπει να ελέγχονται για να εξασφαλιστεί πως οτιδήποτε ευαίσθητα δεδομένα και λογισμικό με άδεια χρήσης έχουν αφαιρεθεί ή έχουν επικυρωθεί με ασφάλιση πριν από τη διάθεση τους.

A11 Φυσική ασφάλεια κτιριακής εγκατάστασης

- Εγκατάσταση καμερών ασφαλείας σε όλους τους χώρους του ξενοδοχείου εκτός από τα δωμάτια των πελατών.
- Πόρτες ασφαλείας στους χώρους με τα πιο ευαίσθητα αγαθά (πχ. Office) και πρόσβαση μόνο από εξουσιοδοτημένα άτομα (IT).
- Πρόσληψη φρουρών ασφαλείας σε όλες τις εισόδους του ξενοδοχείου.

- Τα πρόσωπα που μπορούν να εισέλθουν στις εγκαταστάσεις θα πρέπει να ελέγχονται και να ταυτοποιούνται για τυχόν μη εξουσιοδοτημένη πρόσβαση.

Α4. ΣΥΝΟΨΗ ΠΙΟ ΚΡΙΣΙΜΩΝ ΑΠΟΤΕΛΕΣΜΑΤΩΝ

Παρακάτω παρουσιάζονται οι τρεις μεγαλύτεροι κίνδυνοι με βάση το RPN τους. Με βάση αυτόν τον πίνακα, τα αγαθά που θα προσβληθούν είναι το υλικό από τις κάμερες ασφαλείας, το router που παρέχει πρόσβαση στο διαδίκτυο στο χώρο του γραφείου καθώς και ο κεντρικός υπολογιστής του δωματίου.

Asset Name	Function	Potential Vulnerability	Potential Threat	Potential Business Consequence (Impact)	Impact	Likelihood	Vulnerability	RPN
CCTV Data	Security Footage of the hotel	Not encrypted database	Unauthorized access to CCTV Data	Destruction of security footage	9	5	9	405
AMCRT003 Router	Network in the Office	Wi-Fi enabled needlessly / Use of Old Encryption Protocol (WEP)	Illegitimate access	Unauthorized access network to after the firewall	7	7	8	392
AMCWS005 Dell Optiplex	Workstation	Default passwords not changed	Unauthorized use of software	Illegitimate access to data	7	8	6	336