Ασφάλεια ΠΛΗΡΟΦΟΡΙΑΚΩΝ ΣΥΣΤΗΜΑΤΩΝ ΚΑΙ ΚΡΙΣΙΜΩΝ ΥΠΟΔΟΜΩΝ

ΣΧΕΔΙΟ ΑΣΦΑΛΕΙΑΣ

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

ΕΡΓΑΣΙΑ ΧΕΙΜΕΡΙΝΟΥ ΕΞΑΜΗΝΟΥ 2018

Contents

[Α1. ΕΙΣΑΓΩΓΗ 3](#_Toc496710107)

[Α1.1 Περιγραφή Εργασίας 3](#_Toc496710108)

[Α1.2 Δομή παραδοτέου 3](#_Toc496710109)

[Α2. ΜΕΘΟΔΟΛΟΓΙΑ ΜΕΛΕΤΗΣ ΑΣΦΑΛΕΙΑΣ 3](#_Toc496710110)

[Α2.1 Περιγραφή Πληροφοριακού Συστήματος (ΠΣ) υπό έλεγχο 4](#_Toc496710111)

[Α2.1.1 Υλικός εξοπλισμός (hardware) 4](#_Toc496710112)

[Α2.1.2 Λογισμικό και εφαρμογές 4](#_Toc496710113)

[Α2.1.3 Δίκτυο 4](#_Toc496710114)

[Α2.1.4 Δεδομένα 4](#_Toc496710115)

[Α2.1.5 Διαδικασίες 4](#_Toc496710116)

[Α3. ΑΠΟΤΙΜΗΣΗ ΠΣ ΚΑΙ ΕΓΚΑΤΑΣΤΑΣΕΩΝ ΟΠΑ 4](#_Toc496710117)

[Α3.1 Αγαθά που εντοπίστηκαν 4](#_Toc496710118)

[Α3.2 Απειλές που εντοπίστηκαν 4](#_Toc496710119)

[Α3.3 Ευπάθειες που εντοπίστηκαν 4](#_Toc496710120)

[Α3.4 Αποτελέσματα αποτίμησης 4](#_Toc496710121)

[Β2. ΠΡΟΤΕΙΝΟΜΕΝΑ ΜΕΤΡΑ ΑΣΦΑΛΕΙΑΣ 6](#_Toc496710122)

[Α4. ΣΥΝΟΨΗ ΠΙΟ ΚΡΙΣΙΜΩΝ ΑΠΟΤΕΛΕΣΜΑΤΩΝ 8](#_Toc496710123)

# ΕΙΣΑΓΩΓΗ

TODO

Κατά την διάρκεια Δευτέρα 22 Οκτωβρίου του 2018 έως Παρασκευή 26 Οκτωβρίου του 2018 πραγματοποιήθηκε μια ανάλυση επικινδυνότητας της ασφάλειας της ξενοδοχειακής μονάδας ‘Melis Luxury Hotel’. Η εκτίμηση είχε ζητηθεί από την ‘Melis Luxury Hotel’ με σκοπό να διαπιστωθεί η αποτελεσματικότητα των είδη υπαρχόντων μέτρων προστασίας και να εντοπιστούν νέες απειλές και ευπάθειες της επιχείρησης. Τα παρεχόμενα αποτελέσματα είναι τα αποτελέσματα της εκτίμησης ασφαλείας που διενεργήθηκε και πρέπει να χρησιμοποιηθούν ως συνεισφορά σε μια μεγαλύτερη διαδικασία διαχείρισης κινδύνου. Η ανάλυση περιλαμβάνει αρκετούς μέτριας μορφής κινδύνους οι οποίοι θα πρέπει να απευθυνθούν από την διοίκηση.

## Περιγραφή Εργασίας

Ο σκοπός αυτής της εργασία είναι να εκτιμήσει την αποδοτικότητα της ασφάλειας της ξενοδοχειακής μονάδας ‘Melis Luxury Hotel’, να εντοπιστούν πιθανές απειλές και ευπάθειες και να προταθούν τρόποι για την αντιμετώπιση , περιορισμό η/και την διαχείριση τους.

## Δομή παραδοτέου

TODO

# ΜΕΘΟΔΟΛΟΓΙΑ ΜΕΛΕΤΗΣ ΑΣΦΑΛΕΙΑΣ

Για τη Διαχείριση Επικινδυνότητας του INSERT\_NAME\_ERGASIAS χρη­σιμοποιήθηκε παραμετροποιημένη μέθοδος του ISO27001K[[1]](#footnote-2). Επιλέχθηκε για τη συγκεκριμένη εργασία για τους εξής λόγους:

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

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

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

## Περιγραφή Πληροφοριακού Συστήματος (ΠΣ) υπό έλεγχο

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

### Υλικός εξοπλισμός (hardware)

* Σταθεροί υπολογιστές (Workstation)
* Φορητοί υπολογιστές (Laptops)
* Εξυπηρετητής (Broadband access server)
* Εξυπηρετητής (Database server)
* Εξυπηρετητής (File server)
* Κινητά τηλέφωνα
* Σταθερά τηλέφωνα
* Σκληροί δίσκοι
* USB
* Συσκευή κλιματισμού(air-condition)
* Switch
* Hub
* Firewall
* Router

### Λογισμικό και εφαρμογές

* Windows 10
* Windows Server 2008 R2
* Microsoft Windows 2016 Server SP1
* D-Link proprietary software
* TP-Link proprietary software
* Cisco proprietary software
* LB-Link proprietary software
* NETGEAR proprietary software
* MAC-OS
* My Sql (Υπόθεση)
* Microsoft Office (Υπόθεση)
* Chrome Browser(Υπόθεση)
* Avast free antivirus (Υπόθεση)
* Λογισμικό κρατήσεων
* Λογισμικό Πληρωμών

### Δίκτυο

* Wifi
* Ethernet
* Switch
* Hub
* Firewall
* Router

### Δεδομένα

* Χάρτινα έγγραφα
* Δεδομένα πελατών ξενοδοχείου (Όνομα,Επίθετο , αριθμός πιστωτικής κάρτας,ημερομηνία γέννησης,αριθμός ταυτότητας ,διεύθυνση, τηλέφωνο ,email)
* Δεδομένα υπαλλήλων ξενοδοχείου(Όνομα,Επίθετο , αριθμός λογαριασμού κάρτας,ημερομηνία γέννησης,αριθμός ταυτότητας ,ΑΦΉ,ΑΜΆΚΑ,διεύθυνση, τηλέφωνο ,email)
* Λογιστικά δεδομένα ξενοδοχείου
* Δεδομένα λειτουργίας ξενοδοχείου

### Διαδικασίες

* Διαδικασίες πληρωμής
* Διαδικασίες κρατήσεων
* Διαδικασίες παραγγελίας προμηθειών

# ΑΠΟΤΙΜΗΣΗ ΠΣ ΚΑΙ ΕΓΚΑΤΑΣΤΑΣΕΩΝ ΟΠΑ

TODO

## Αγαθά που εντοπίστηκαν

* Σταθεροί υπολογιστές (Workstation)
* Φορητοί υπολογιστές (Laptops)
* Εξυπηρετητής (Broadband access server)
* Εξυπηρετητής (Database server)
* Εξυπηρετητής (File server)
* Routers
* Switches
* Hubs
* Wifi
* Ethernets
* Χάρτινα έγγραφα
* Δεδομένα πελατών ξενοδοχείου
* Δεδομένα υπαλλήλων ξενοδοχείου
* Λογιστικά δεδομένα
* Σταθερά τηλέφωνα
* Χάρτινα έγγραφα
* Φορητοί υπολογιστές (Laptops)
* Προσωπικό ξενοδοχείου
* Δωμάτια
* Back ups
* Windows 10
* Windows Server 2008 R2
* My sql
* Διαδικασίες πληρωμής
* Διαδικασίες κρατήσεων
* Διαδικασίες παραγγελίας προμήθειών
* bill added from hire
* τοπολογια δικτιου
* υπαρχοντα μετρα ασφαλειας

## Απειλές που εντοπίστηκαν

TODO (monolektika)

* Πλαστογραφία : προσωποποίηση τεχνικού ανελκυστήρα πρόσβαση σε χωρους χωρίς κατάλληλη άδεια
* κατάχρηση πόρων του συστήματος : κατέβασμα torrent αρχείων από το room area
* αποτυχία λογισμικού κρατήσεων :
* λανθασμένος τρόπος συντήρησης λογισμικού: δεν υπάρχει επιλογή συντήρησης από τον κατασκευαστή
* αποτυχία λειτουργίας κεντρικής μονάδας κλιματισμού : server room εφεδρικό κλιματιστικό
* κλοπή : μηχανημάτων στο γραφείο λόγο μη ελενχομενης πρόσβαση σε αυτό
* ηθελημένη ζημιά από προσωπικό: λόγο εύκολης πρόσβασης του σύνολου του προσωπικού στο γραφείο
* πολύωρη πτώση ρεύματος
* αποτυχία Hardware

## Ευπάθειες που εντοπίστηκαν

TODO

* έλλειψη εφεδρικού κλιματιστικού
* έλλειψη εφεδρικού router
* έλλειψη ηλεκτρογενιτριας
* έλλειψη συστήματος αναγνώρισης
* έλλειψη ξεχωριστού δωματίου Εξυπηρετητών
* έλλειψη σύμβασης συντήρησης λογισμικού
* έλλειψη διαθέσιμων ανταλλακτικών πχ σκληροί δίσκοι
* έλλειψη κριπτογραφίας

## Αποτελέσματα αποτίμησης

TODO – Ενδεικτικός πίνακας που πρέπει να χρησιμοποιηθεί μαζί με κείμενο ανάλυσης υπάρχει στην επόμενη σελίδα.

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  | **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 ακολου-  θίας μηνυμάτων |
| **ΑΓΑΘΟ 1** |  |  | 1 | 2 | 3 | 5 |  | 7 | | 5 | 6 | 3 | 5 | 2 | | 3 | 3 | 5 | | 5 | 5 | 5 | 5 | 3 | 3 | 5 | 5 |
| **ΑΓΑΘΟ 2** |  |  | 1 | 2 | 3 | 5 |  | 7 | | 5 | 6 | 3 | 5 | 2 | | 4 | 4 | 5 | | 5 | 5 | 5 | 5 | 4 | 4 | 5 | 5 |
| **ΑΓΑΘΟ 3** |  |  |  |  | 1 | 2 | 3 | 5 | | 4 | 4 | 2 | 4 | 4 | | 6 | 6 | 4 | | 4 | 4 | 4 | 4 | 6 | 6 | 4 | 4 |

# ΠΡΟΤΕΙΝΟΜΕΝΑ ΜΕΤΡΑ ΑΣΦΑΛΕΙΑΣ

Τα προτεινόμενα Μέτρα Προστασίας εντάσσονται σε έντεκα (11) γε­­νι­­κές κα­­τη­­γορίες:

1. Προσωπικό – Προστασία Διαδικασιών Προσωπικού
2. Ταυτοποίηση και αυθεντικοποίηση
3. Έλεγχος προσπέλασης και χρήσης πόρων
4. Διαχείριση εμπιστευτικών δεδομένων
5. Προστασία από τη χρήση υπηρεσιών από τρίτους
6. Προστασία λογισμικού
7. Διαχείριση ασφάλειας δικτύου
8. Προστασία από ιομορφικό λογισμικό
9. Ασφαλής χρήση διαδικτυακών υπηρεσιών
10. Ασφάλεια εξοπλισμού
11. Φυσική ασφάλεια κτιριακής εγκατάστασης

Τα μέτρα έχουν εφαρμογή στο ΠΣ του INSERT\_NAME\_HERE.

###### Προσωπικό – Προστασία Διαδικασιών Προσωπικού

TODO – Εισαγωγή μέτρων κατάλληλων με τις ευπάθειες και απειλές που εντοπίσατε

###### Ταυτοποίηση και αυθεντικοποίηση

TODO – Εισαγωγή μέτρων κατάλληλων με τις ευπάθειες και απειλές που εντοπίσατε

###### Έλεγχος προσπέλασης και χρήσης πόρων

TODO – Εισαγωγή μέτρων κατάλληλων με τις ευπάθειες και απειλές που εντοπίσατε

###### Διαχείριση εμπιστευτικών δεδομένων

TODO – Εισαγωγή μέτρων κατάλληλων με τις ευπάθειες και απειλές που εντοπίσατε

###### Προστασία από τη χρήση υπηρεσιών από τρίτους

TODO – Εισαγωγή μέτρων κατάλληλων με τις ευπάθειες και απειλές που εντοπίσατε

###### Προστασία λογισμικού

TODO – Εισαγωγή μέτρων κατάλληλων με τις ευπάθειες και απειλές που εντοπίσατε

###### Διαχείριση ασφάλειας δικτύου

TODO – Εισαγωγή μέτρων κατάλληλων με τις ευπάθειες και απειλές που εντοπίσατε

###### Προστασία από ιομορφικό λογισμικό

TODO – Εισαγωγή μέτρων κατάλληλων με τις ευπάθειες και απειλές που εντοπίσατε

###### Ασφαλής χρήση διαδικτυακών υπηρεσιών

TODO – Εισαγωγή μέτρων κατάλληλων με τις ευπάθειες και απειλές που εντοπίσατε

###### Ασφάλεια εξοπλισμού

TODO – Εισαγωγή μέτρων κατάλληλων με τις ευπάθειες και απειλές που εντοπίσατε

###### Φυσική ασφάλεια κτιριακής εγκατάστασης

TODO – Εισαγωγή μέτρων κατάλληλων με τις ευπάθειες και απειλές που εντοπίσατε

# ΣΥΝΟΨΗ ΠΙΟ ΚΡΙΣΙΜΩΝ ΑΠΟΤΕΛΕΣΜΑΤΩΝ

TODO – Παρουσίαση του 5% ευρημάτων με την υψηλότερη επικινδυνότητα (high risk)

1. <http://www.iso27001security.com/html/toolkit.html> [↑](#footnote-ref-2)