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

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

## Περιγραφή Εργασίας

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

## Δομή παραδοτέου

Η παρούσα εργασία αποτελείται από 5 κεφάλαια.

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

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

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

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

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

# ΜΕΘΟΔΟΛΟΓΙΑ ΜΕΛΕΤΗΣ ΑΣΦΑΛΕΙΑΣ

Για τη Διαχείριση Επικινδυνότητας του Ανάλυση και Διαχείριση Επικινδυνότητας Ξενοδοχείου 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)

Σταθερός υπολογιστής (Workstation) μοντέλου Dell Optiplex 3060 SF με λειτουργικό windows 10 που βρίσκεται στο κεντρικό γραφείο με IP 192.168.1.12

Φορητός υπολογιστής (Laptops) μοντέλου Apple MacBook Pro 13.3 με λειτουργικό MAC-OS που βρίσκεται στο στο εστιατόριο με IP 192.168.1.30

Εξυπηρετητής (Broadband access server) μοντέλου Alcatel 7410 Broadband Access Server με λειτουργικό Windows Server 2008 R2 ο οποίος βρίσκεται στο κεντρικό γραφείο και έχει IP 192.168.1.3

Φορητός υπολογιστής (Laptops) μοντέλου Apple MacBook Pro 13.3 με λειτουργικό MAC-OS που βρίσκεται στη περιοχή δωματίων με IP 192.168.1.31

Φορητός υπολογιστής (Laptops) μοντέλου Apple MacBook Pro 13.3 με λειτουργικό MAC-OS που βρίσκεται στην αίθουσα συνεδριάσεων με IP 192.168.1.32

Εξυπηρετητής (Database server) μοντέλου Oracle Database Server με λειτουργικό Microsoft Windows 2016 Server SP1 ο οποίος βρίσκεται στο κεντρικό γραφείο με ΙP 192.168.1.56

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

Managed Switch μοντέλου D-Link DGS-1100-10MPP με λειτουργικό D-Link proprietary sorftware ο οποίος βρίσκεται στη περιοχή δωματίων και έχει IP [192.168.1.34](http://192.168.1.34/?fbclid=IwAR3BETAA7TAfx648FnN2VO_M-uYalXnkoQVtxLXjt2zGlildRJjVAalFbds)

Managed Switch μοντέλου D-Link DGS-1100-10MPP με λειτουργικό D-Link proprietary sorftware ο οποίος βρίσκεται στο εστιατόριο και έχει IP [192.168.1.36](http://192.168.1.36/?fbclid=IwAR2FkCHNb9bfIZnccTzMrxcYi3_9SECe2bxclzRM-6B555FQxdJwBocbowE)

Managed Switch μοντέλου D-Link DGS-1100-10MPP με λειτουργικό D-Link proprietary sorftware ο οποίος βρίσκεται στην αίθουσα συνεδριάσεων και έχει IP [192.168.1.37](http://192.168.1.37/?fbclid=IwAR37APX9JmzyiOsr9k_XYQ4rJvMs2WPY-ABXFaR3ypBu9-cbg7i1iMC26nY)

Εξυπηρετητής ( file server ) μοντέλου oracle file server με λειτουργικό windows server 2008 R2 ο όποιος βρίσκεται στο κεντρικο γραφείο με IP [192.168.1.8](https://l.facebook.com/l.php?u=http%3A%2F%2F192.168.1.8%2F%3Ffbclid%3DIwAR1I2bVM-6JG0YifeOlvyRuVdGYf6j0ZdIrYsx1nkxbHPtPgT27CF39Y424&h=AT11qZsmuFne93lytqk8T0ZeQ_-X04zE2seFSt8U1PSuPQHoV9_T3Mnzdan_idQabf5aZDNDkhMrdQxxQZwcUyutlHc5AOYVm6GfntHZA5e7v8VehFqoVo1UOpoD3JIL4hL9Vrn4XwoiPkQhjUlAdg)

Router μοντέλου TP-LINK Archer C69 v1 με λειτουργικό TP-Link Proprietary software το οποίο βρίσκεται στο κεντρικό γραφείο με IP [192.186.1.44](http://192.186.1.44/?fbclid=IwAR09hh8Lj8IB1NxQnU-LXWAYnwJkN2HHEeloO5xW7Ccgm4oIcyLJm-TRRsk)

Router μοντέλου TP-LINK Archer C69 v1 με λειτουργικό TP-Link Proprietary software το οποίο βρίσκεται στην αίθουσα συνεδριάσεων με IP [192.186.1.45](http://192.186.1.45/?fbclid=IwAR37APX9JmzyiOsr9k_XYQ4rJvMs2WPY-ABXFaR3ypBu9-cbg7i1iMC26nY)

Router μοντέλου TP-LINK Archer C69 v1 με λειτουργικό TP-Link Proprietary software το οποίο βρίσκεται στη περιοχή των δωματίων με IP [192.186.1.47](https://l.facebook.com/l.php?u=http%3A%2F%2F192.186.1.47%2F%3Ffbclid%3DIwAR1tAeYzflD7vUnRcmhxNqUsgB46uO2sRBs8cTlB42zSPXAWMZq_OyckIpo&h=AT11qZsmuFne93lytqk8T0ZeQ_-X04zE2seFSt8U1PSuPQHoV9_T3Mnzdan_idQabf5aZDNDkhMrdQxxQZwcUyutlHc5AOYVm6GfntHZA5e7v8VehFqoVo1UOpoD3JIL4hL9Vrn4XwoiPkQhjUlAdg)

Network Hub μοντέλου LB-Link BL-S515 με LB-Link Proprietary software το οποίο βρίσκεται στο εστιατόριο με IP [192.186.1.14](http://192.186.1.14/?fbclid=IwAR3A3flinELabZkR0CyxElDF-K72Y986QZx821OB4mu89bsAaU9JsnieylQ)

Wireless Access Point μοντέλου Cisco Aironet 38021 Radio με λειτουργικό Cisco proprietary software το οποίο βρίσκεται στο εστιατόριο και έχει IP [192.168.1.10](http://192.168.1.10/?fbclid=IwAR3Jk7E8H2xbKX0Q0nZ8hnpLmWHUaObz2cR-jajXR77TNW9KK9dnQnxLoz8)

Wireless Access Point μοντέλου Cisco Aironet 38021 Radio με λειτουργικό Cisco proprietary software το οποίο βρίσκεται στην αίθουσα συνεδριάσεων και έχει IP 192.168.1.16

Wireless Access Point μοντέλου Cisco Aironet 38021 Radio με λειτουργικό Cisco proprietary software το οποίο βρίσκεται στο κεντρικό γραφείο και έχει IP 192.168.1.17

Wireless Access Point μοντέλου Cisco Aironet 38021 Radio με λειτουργικό Cisco proprietary software το οποίο βρίσκεται στη περιοχή των δωματίων και έχει IP 192.168.1.18

Fast Ethernet Switch μοντέλου FS108 32 Port Fast Ethernet Switch με λειτουργικό NETGEAR Proprietary software το οποίο βρίσκεται στη περιοχή των δωματίων με IP 192.198.1.11

Fast Ethernet Switch μοντέλου FS108 32 Port Fast Ethernet Switch με λειτουργικό NETGEAR Proprietary software το οποίο βρίσκεται στη περιοχή των δωματίων με IP [192.168.1.9](http://192.168.1.9/?fbclid=IwAR1I2bVM-6JG0YifeOlvyRuVdGYf6j0ZdIrYsx1nkxbHPtPgT27CF39Y424)

Public network Router μοντέλου FS110 Network Router με λειτουργικό NETGEAR proprietary softwarer

Εξυπηρετητής (Web Server) μοντέλου T2015 RAQ WEB με λειτουργικό Apache LDAP Studio 0.6.0 το οποίο βρίσκετε στο κεντρικό γραφείο με IP 192.168.1.94

Εξυπηρετητής (Web Server) μοντέλου QB Server Xpress Mail Xpress Console με λειτουργικό Ubuntu 12.04.5 LTS  το οποίο βρίσκεται στο κεντρικό γραφείο με IP 192.168.1.96

Συσκευή κλιματισμού (INDUSTRIAL air-condition) μοντέλου DEQ AFFINITY R410A το οποίο βρίσκεται στην οροφή.

Σταθερά τηλέφωνα(VoIP) μοντέλου Cisco Unified IP Phone 7912G τα οποία βρίσκονται διάσπαρτα στα δωμάτια , γραφείο εστιατόριο, αίθουσα συνεδριάσεων με IP από 192.168.1.100 έως 192.168.1.200

Εκτυπωτές μοντέλου HP LaserJet Pro MFP M426fdw 16.0.18002.756-501 Driver-Product Software 16.0.18002.756-501 τα οποία βρίσκονται διάσπαρτα στα δωμάτια , γραφείο εστιατόριο, αίθουσα συνεδριάσεων με IP από 192.168.1.201 έως 192.168.1.211

### Λογισμικό και εφαρμογές

Windows 10 το οποίο βρίσκεται στο σταθερό υπολογιστή (workstation)

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

Microsoft Windows 2016 Server SP1 το οποίο βρίσκεται Database Server

D-Link proprietary software το οποίο βρίσκεται στους Manage Switches

TP-Link proprietary software το οποίο βρίσκεται στους Routers

Cisco proprietary software το οποίο βρίσκεται στους Wireless Access Points

LB-Link proprietary software το οποίο βρίσκεται στα Network Hubs

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

MAC-OS το οποίο βρίσκεται στα Laptops

My Sql το οποίο βρίσκεται στον Database Server

Microsoft Office (Υπόθεση) το οποίο βρίσκεται στο Workstation και στα Laptops

Chrome Browser(Υπόθεση) το οποίο βρίσκεται στο Workstation και στα Laptops

Avast free antivirus (Υπόθεση) το οποίο βρίσκεται στο Workstation και στα Laptops

Postfix  το οποίο βρίσκεται στον Mail Server

Ubuntu 12.04.5 LTS  το οποίο βρίσκεται στον Mail Server

Apache2 το οποίο βρίσκεται στον Web Server

PHP5 το οποίο βρίσκεται στον Web Server

Λογισμικό κρατήσεων το οποίο βρίσκεται στο Workstation

Λογισμικό Πληρωμών το οποίο βρίσκεται στο Workstation

### Δίκτυο

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

Managed Switch μοντέλου D-Link DGS-1100-10MPP με λειτουργικό D-Link proprietary sorftware ο οποίος βρίσκεται στη περιοχή δωματίων και έχει IP 192.168.1.34 [192.168.1.34](http://192.168.1.34/?fbclid=IwAR3BETAA7TAfx648FnN2VO_M-uYalXnkoQVtxLXjt2zGlildRJjVAalFbds)192.168.1.34192.168.1.34

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

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

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

Router μοντέλου TP-LINK Archer C69 v1 με λειτουργικό TP-Link Proprietary software το οποίο βρίσκεται στην αίθουσα συνεδριάσεων με IP 192.168.1.47 [192.186.1.45](http://192.186.1.45/?fbclid=IwAR37APX9JmzyiOsr9k_XYQ4rJvMs2WPY-ABXFaR3ypBu9-cbg7i1iMC26nY)  
  
Router μοντέλου TP-LINK Archer C69 v1 με λειτουργικό TP-Link Proprietary software το οποίο βρίσκεται στη περιοχή των δωματίων με IP 192.168.1.45

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

### Δεδομένα

Χάρτινα έγγραφα τα οποία βρίσκονται στο κεντρικό γραφείο.

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

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

Λογιστικά δεδομένα ξενοδοχείου τα οποία βρίσκονται στον DataBase Server

Δεδομένα λειτουργίας ξενοδοχείου τα οποία βρίσκονται στον DataBase Server

### Διαδικασίες

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

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

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

# ΑΠΟΤΙΜΗΣΗ ΠΣ ΚΑΙ ΕΓΚΑΤΑΣΤΑΣΕΩΝ **ΕΡΓΑΣΙΑΣ ΟΠΑ**

TODO

## Αγαθά που εντοπίστηκαν

Σταθεροί υπολογιστές (Workstation)

Φορητοί υπολογιστές (Laptops)

Εξυπηρετητής (Broadband access server)

Εξυπηρετητής (Database server)

Εξυπηρετητής (File server)

Εξυπηρετητής(Web Server)

Εξυπηρετητής(Mail Server)

Routers

Switches

Hubs

WiFi

Ethernet's

Χάρτινα έγγραφα

Δεδομένα πελατών ξενοδοχείου

Δεδομένα υπαλλήλων ξενοδοχείου

Δεδομένα προμηθειών

Λογιστικά δεδομένα

Προσωπικό ξενοδοχείου

Πελάτες

Δωμάτια

Back ups

Διαδικασίες πληρωμής

Διαδικασίες κρατήσεων

Διαδικασίες παραγγελίας προμηθειών

Τοπολογία δικτύου

Υπάρχοντα μετρά ασφάλειας

Εκτυπωτές

Κτιριακή εγκατάσταση

## Απειλές που εντοπίστηκαν

Απόκτηση πρόσβασης ως admin λόγο(remote code execution Windows 10 με Microsoft Windows PDF βιβλιοθήκη).

* Εμπιστευτικότητα :προσπέλαση πληροφοριών χρηστών , κρατήσεων παραγγελιών
* Ακεραιότητα: τροποποίηση διαδικασιών πληρωμής,κρατήσεων,παραγγελιών
* Διαθεσιμότητα: denial of service

Απόκτηση πρόσβασης λόγο(memory coraption [CVE-2015-7104](https://www.cvedetails.com/cve/CVE-2015-7104/) Apple Safari Multiple Memory Corruptio Vulnerabilities).

* Εμπιστευτικότητα :προσπέλαση πληροφοριών
* Ακεραιότητα: τροποποίηση αρχείον αλλά χωρίς τον πλήρη ελέγχο του μηχανήματος
* Διαθεσιμότητα: denial of service

Εξυπηρετητής (Broadband access server) (Execute CodeOverflow  [CVE-2018-8136](https://www.cvedetails.com/cve/CVE-2018-8136/))

* Εμπιστευτικότητα :προσπέλαση όλων των πληροφοριών
* Ακεραιότητα: Έκθεση ολου του συστήματος σε απειλές
* Διαθεσιμότητα: denial of service επιτηθέμενος μπορεί να βγάλει το σύστημα μη λειτουργισμό.

Εξυπηρετητής ( File server) (Execute CodeOverflow  [CVE-2018-8136](https://www.cvedetails.com/cve/CVE-2018-8136/))

* Εμπιστευτικότητα :προσπέλαση όλων των πληροφοριών
* Ακεραιότητα: Έκθεση ολου του συστήματος σε απειλές
* Διαθεσιμότητα: denial of service επιτηθέμενος μπορεί να βγάλει το σύστημα μη λειτουργισμό.

Εξυπηρετητής ( Database server) (Execute Code Overflow  [CVE-2018-8136](https://www.cvedetails.com/cve/CVE-2018-8136/))

* Εμπιστευτικότητα :προσπέλαση όλων των πληροφοριών
* Ακεραιότητα: Έκθεση ολου του συστήματος σε απειλές
* Διαθεσιμότητα: denial of service επιτηθέμενος μπορεί να βγάλει το σύστημα μη λειτουργισμό.

Fortinet (firewall)

* Εμπιστευτικότητα :προσπέλαση μεγάλου μέρους πληροφοριών
* Ακεραιότητα: τροποποίηση αρχείον αλλά χωρίς τον πλήρη ελέγχο του μηχανήματος
* Διαθεσιμότητα: μειωμένη επίδοση συστήματος .

Πλαστογραφία : προσωποποίηση τεχνικού ανελκυστήρα πρόσβαση σε χώρους 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

ακούσια ζημία από προσωπικό σε μηχανήματα

πολύωρη πτώση ρεύματος

αποτυχία Hardware

malware Introduction of damaging or disruptive s/w

κλοπή προσοπηκών δεδομενων από δομάτια

## Ευπάθειες που εντοπίστηκαν

TODO

Windows 10 με Microsoft Windows PDF βιβλιοθήκη. Η συγκεκριμένη βιβλιοθήκη διαχειρίζεται λάθος μνήμη (remote code execution)

Έλλειψη λογισμικού προστασίας Anti Virus.

Έλλειψη πολιτικής αναβάθμισης συστημάτων.

Μη τήρηση πολίτικης ασφαλείας.

Mac os μη αναβαθμισμένο λειτουργικό σύστημα και εφαρμογές.

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

sql injection

doss

sensitivi data exposure

elici ids

## 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)

https://www.cvedetails.com/

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