ΑΣΦΆΛΕΙΑ ΠΛΗΡΟΦΟΡΙΑΚΩΝ ΣΥΣΤΗΜΑΤΩΝ ΚΑΙ ΚΡΙΣΙΜΩΝ ΥΠΟΔΟΜΩΝ

ΣΧΕΔΙΟ ΑΣΦΑΛΕΙΑΣ

ΣΥΓΓΡΑΦΕΙΣ: ΔΙΑΚΡΟΥΣΗ ΕΛΕΥΘΕΡΙΑ 3130056

ΜΠΕΝΟΣ ΑΝΑΣΤΑΣΙΟΣ 3130141

ΤΣΟΠΕΛΑΣ ΕΥΘΥΜΙΟΣ 3130210

ΕΡΓΑΣΙΑ ΧΕΙΜΕΡΙΝΟΥ ΕΞΑΜΗΝΟΥ 2017

Contents

Α1. ΕΙΣΑΓΩΓΗ

Η ασφάλεια πληροφοριακών συστημάτων, ασφάλεια υπολογιστικών συστημάτων ή ασφάλεια υπολογιστών, είναι ένα γνωστικό πεδίο της επιστήμης της πληροφορικής που ασχολείται με την προστασία των υπολογιστών, των δικτύων που τους διασυνδέουν και των δεδομένων σε αυτά τα συστήματα, αποτρέποντας τη μη εξουσιοδοτημένη πρόσβαση ή χρήση τους. Πρωταρχικό στόχο αποτελεί η ασφάλεια της πληροφορίας δηλαδή η προστασία και η τήρηση της εμπιστευτικότητας, ακεραιότητας και διαθεσιμότητας τους.

Η ασφάλεια πληροφοριακών συστημάτων δεν αποτελεί αμιγώς τεχνικό ζήτημα. Γενικά πρόκειται για τον περιορισμό της επικινδυνότητας στο πλέον αποδεκτό επίπεδο. Ωστόσο , η προστασία της πληροφορίας αποτελεί κάτι ανώτερο από την ωμή υπεράσπιση μηχανημάτων . Επικεντρώνεται στον άνθρωπο με σεβασμό και ευαισθησία προς την αξία της ιδιωτικότητας.

Α1.1 Περιγραφή Εργασίας

Η χρήση των Πληροφοριακών Συστημάτων συνεχώς αυξάνεται. Πλέον οι περισσότεροι οργανισμοί βασίζονται στην λειτουργία τους. Αχίλλειος πτέρνα αυτών είναι η ασφάλεια τους.

Η εργασία αυτή έχει ως στόχο να παρουσιάσει την διαδικασία risk analysis και risk assessment για το πληροφοριακό σύστημα ενός νοσοκομείου, που θεωρείται η πρότυπη μέθοδος ασφάλειας σύμφωνα με το ISO27k. Παρουσιάζεται το υφιστάμενο πληροφοριακό σύστημα και τα χαρακτηριστικά του όπως προκύπτουν από το δοθέν τοπολογικό σχέδιο. Εν συνεχεία,περιγράφονται αναλυτικά τα αγαθά που εντοπίστηκαν , οι ευπάθειες που τα συνοδεύουν καθώς και οι απειλές που προκύπτουν.

Ο σχεδιασμός ασφαλών πολιτικών στα πληροφοριακά συστήματα, συνδέεται άμεσα τόσο με τεχνικές, διαδικασίες και διοικητικά μέτρα όσο και με ηθικό-κοινωνικές αντιλήψεις, αρχές και παραδοχές, προφυλάσσοντας από κάθε είδους απειλή τυχαία ή σκόπιμη.

Παρουσιάζονται επίσης τα αποτελέσματα της προαναφερθείσας αποτίμησης σε ενδεικτικό πίνακα. Βάσει των ευπαθειών και των απειλών που εντοπίστηκαν, προτείνονται συγκεκριμένα μέτρα αντιμετώπισης.

Τέλος, παρουσιάζονται συνοπτικά τα κρισιμότερα αποτελέσματα της έρευνάς μας, λαμβάνοντας υπόψιν τον δείκτη επικινδυνότητας RPN, που προκύπτει απο το excel file που συνοδεύει την εργασία μας.

A1.1 Δομή παραδοτέου

Το παρόν παραδοτέο εκπονήθηκε στα πλαίσια του μαθήματος Ασφάλεια Πληροφοριακών Συστημάτων και μελετά το πληροφοριακό σύστημα ενός νοσοκομείου. Αποτελείται από πέντε κεφάλαια. Στο πρώτο κεφάλαιο παρουσιάζονται εισαγωγικά στοιχεία για το έργο. Στο δεύτερο κεφάλαιο περιγράφεται το πληροφοριακό σύστημα απαριθμώντας αναλυτικά τα αγαθά που το απαρτίζουν. Στο τρίτο κεφάλαιο παρουσιάζονται όλα αυτά τα βήματα που θεωρούνται απαραίτητα για την ανάλυση επικινδυνότητας. Στο τέταρτο κεφάλαιο προσεγγίζουμε προτεινόμενα μέτρα ασφάλειας εντάσσοντας τα σε έντεκα γενικές κατηγορίες. Εν τέλει, παραθέτουμε το 5% των ευρημάτων με την υψηλότερη επικινδυνότητα.

A2. ΜΕΘΟΔΟΛΟΓΙΑ ΜΕΛΕΤΗΣ ΑΣΦΑΛΕΙΑΣ

Για τη Διαχείριση Επικινδυνότητας του Νοσοκομείου 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*

Α1.1 Περιγραφή Πληροφοριακού Συστήματος (ΠΣ) υπό έλεγχο

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

Υλικός εξοπλισμός (hardware)

- Workstation
    - Asset Name : AMCWS001, AMCWS002 - 2 Workstations με λειτουργικό σύστημα Microsoft Windows 7 Pro SP1 που βρίσκονται στο registry και έχουν IPs 192.168.1.11 , 192.168.1.12. Μέσω ενός switch (AMCSW002) συνδέεται με τον server (AMCSRV001).
    - Asset Name : AMCWS003 - 1 Workstation με λειτουργικό σύστημα Microsoft Windows 7 Pro SP1 που βρίσκεται στη γραμματεία και έχει IP 192.168.1.13. Μέσω ενός switch (AMCSW002) συνδέεται με τον server (AMCSRV001).
    - Asset Name : AMCWS004, AMCWS005, AMCWS006 - 3 Workstations – Patient PC με λειτουργικό σύστημα Microsoft Windows XP που βρίσκονται στα FL1 Patient Rooms 1,2,3 και με IPs αντίστοιχα 192.168.1.14, 192.168.1.15, 192.168.1.16. Μέσω ενός switch (AMCSW001) συνδέεται με τον server (AMCSRV002).

- Asset Name : AMCWS007 - 1 Workstation με λειτουργικό σύστημα Microsoft Windows XP που βρίσκεται στο pharmacy room και έχει IP 192.168.1.17. Συνδέεται με τον server (AMCSRV003).

- Server

  - Asset Name : AMCSRV001 - Server με λειτουργικό σύστημα Microsoft Windows 2012 Server SP1 που βρίσκεται στο data room με IP 192.168.1.2. Συνδέεται με τον printer (AMCPRN001), αλλά και τους υπόλοιπους δύο servers και με το δίκτυο μέσω του firewall/router (AMCRT002).

  - Asset Name : AMCSRV002 - Server με λειτουργικό σύστημα Microsoft Windows 2012 Server SP1 που βρίσκεται στο FL1 Data Room με IP 192.168.1.3. Συνδέεται με τον printer (AMCPRN002), αλλά και τους υπόλοιπους δύο servers και με το δίκτυο μέσω του firewall/router (AMCRT002).

  - Asset Name : AMCSRV003 - Server με λειτουργικό σύστημα Microsoft Windows 2012 Server SP1 που βρίσκεται στο Pharmacy Room με IP 192.168.1.8. Συνδέεται με τους υπόλοιπους δύο servers και με το δίκτυο μέσω του firewall/router (AMCRT002).

- Printer

  - Asset Name : AMCPRN001 - Printer με λειτουργικό σύστημα Firmware – last update 2003 που βρίσκεται στο registry με IP 192.168.1.4

  - Asset Name : AMCPRN002 - Printer με λειτουργικό σύστημα Firmware – last update 2003 που βρίσκεται στο FL1 Data Room με IP 192.168.1.5.

- Network Switch

  - Asset Name : AMCSW001 - Network Switch με λειτουργικό σύστημα IOS 12.4 Basic IP που βρίσκεται στο FL1 Data Room με IP 192.168.1.6

  - Asset Name : AMCSW002 - Network Switch με λειτουργικό σύστημα IOS 12.4 Basic IP που βρίσκεται στο registry με IP 192.168.1.7

- Router

  - Asset Name : AMCRT001 - Router με λειτουργικό σύστημα IOS 15.5 Basic IP που βρίσκεται στο Data Room με IP 192.168.1.1

  - Asset Name : AMCRT002 - Router / Firewall με λειτουργικό σύστημα IOS 15.5 Advanced IP Services που βρίσκεται στο Data Room με IP 192.168.1.2

Λογισμικό και εφαρμογές

- Software

- Asset Name :Windows XP – Microsoft που χρησιμοποιείται στα Workstation-Patient PCs
- Asset Name :Windows 7 Pro SP1 – Microsoft που χρησιμοποιείται στα Workstations
- Asset Name :Oracle Database – Oracle του μοντέλου Oracle SQL 9G που χρησιμοποιείται στους Servers AMCSRV001 , AMCSRV002.
- Asset Name :Hospital Website – JOOMLA μοντέλου JOOMLA με λειτουργικό σύστημα LINUX REDHAT που βρίσκεται στον server AMCSRV002 και έχει IP 1.2.3.4.5

Δίκτυο

Οι υπολογιστές του πληροφοριακού μας συστήματος συνδέονται μεταξύ τους μέσω Internet, όπως επίσης και με τον εξωτερικό κόσμο.

Δεδομένα

- Asset Name: Patient Data που είναι αποθηκευμένα στον AMCSRV001
- Asset Name: Employee Data που είναι αποθηκευμένα στον AMCSRV002
- Asset Name: Pharmacy Data που είναι αποθηκευμένα στον AMCSRV003
- Asset Name: Physical Copies of Data

Διαδικασίες

- Asset Name: Payment Process που γίνεται στο Workstation
- Asset Name: New Patient Register Process που γίνεται στα Workastation – Patient PCs

Α1. ΑΠΟΤΙΜΗΣΗ ΠΣ ΚΑΙ ΕΓΚΑΤΑΣΤΑΣΕΩΝ ΝΟΣΟΚΟΜΕΙΟΥ

Στο παρών κεφάλαιο αντικείμενο μελέτης μας αποτελεί το πληροφοριακό σύστημα σε βαθύτερο επίπεδο. Συγκεκριμένα περιγράφεται αναλυτικά η δομή του και παραθέτονται οι ευπάθειες και απειλές που αντιμετωπίζει. Ταυτόχρονα γίνεται αναλυτική αναφορά των αγαθών καθώς και του τρόπου που συνδέονται μεταξύ τους. Τέλος, εστιάζουμε στα αποτελέσματα της αποτίμησής μας.

A1.1 Αγαθά που εντοπίστηκαν

Είναι γνωστό ότι ως Αγαθό ορίζεται κάτι το οποίο αξίζει να προστατευθεί.

Μελετώντας προσεκτικά το παρών πληροφοριακό σύστημα εντοπίσαμε πλήθος συσκευών επεξεργασίας και αποθήκευσης πληροφοριών όπως επίσης και βασικές συσκευές δικτύου. Αρχικά , διακρίναμε δύο Servers , οι οποίοι είναι υπεύθυνοι για την αποθήκευση και επεξεργασία ευαίσθητων δεδομένων του νοσοκομείου. Πιο συγκεκριμένα, ο πρώτος εξυπηρετητής (AMCSRV001) διαχειρίζεται πληροφορίες των ασθενών , των υπαλλήλων καθώς και τα στοιχεία ταυτοποίησης τους(Employee Data, Patient Information Data). Από την άλλη , ο δεύτερος εξυπηρετητής (AMCSRV002) προορίζεται για τις ιατρικές πληροφορίες των ασθενών(Patient Medical Data). Με δική μας πρωτοβουλία θεωρήσαμε ότι θα ήταν ορθό να προσθέσουμε και έναν τρίτο Server , προκειμένου να προσεγγίσουμε το ζήτημα πιο ρεαλιστικά. Ο τελευταίος εξυπηρετητής (AMCSRV003) είναι υπεύθυνος για την επιμέλεια και την καταγραφή των αποθεμάτων των φαρμακευτικών πόρων(Pharmacy Data) (Ιατρικά σκευάσματα,δισκία, σκόνη, ταμπλέτες, σταγόνες, υπόθετα, ενέσιμα, οροί, εμβόλια κτλπ). Είναι προφανές ότι και οι τρείς servers συνδέονται με αντίστοιχες βάσεις δεδομένων πληροφοριών(Oracle Database) ανάλογα με το σκοπό που προαναφέραμε.
Επιπροσθέτως, στο Πληροφοριακό Σύστημα συμμετέχουν επτα Η/Υ (workstations) εκ των οποίων τρεις από αυτούς(Workstation-Patient PC- AMCWS004, AMCWS005, AMCWS006) που χρησιμοποιούν λογισμικό Windows XP, συνδεδεμένοι με έναν μεταγωγέα (AMCSW001) , επικοινωνούν με τον server AMCSRV002. Οι υπόλοιποι τρείς (Workstation- AMCWS001, AMCWS002, AMCWS003) , που χρησιμοποιούν λογισμικό Windows 7 Pro SP1, του αρχικού σχήματος , συνδέονται και αυτοί με έτερο μεταγωγέα (AMCSW002) πρός τον AMCSRV001.Εν τέλει, ο Η/Υ (Workstation-Pharmacy PC - AMCWS007), που χρησιμοποιεί λογισμικό Windows XP , που προσθέσαμε επικοινωνεί με τον server AMCSRV003. Αριθμήσαμε επίσης δύο Printers (AMCPRN001, AMCPRN002) οι οποίοι είναι συνδεδεμένοι με τους αντίστοιχους servers(AMCSRV001, AMCSRV002). Παράλληλα, τα παραπάνω αγαθά συνδέονται στο ίδιο δίκτυο μέσω ενός router/firewall (AMCRT002) το οποίο ρυθμίζει τη κυκλοφορία δεδομένων μεταξύ του πληροφοριακού μας συστήματος και του βασικού δρομολογητή του παρόχου (AMCRT001). Ως αγαθό, θεωρήθηκε και η ιστοσελίδα που υποστηρίζει το νοσοκομείο και φιλοξενείται στον AMCSRV002. Τέλος , ειναι αδιαμφισβητητο οτι χρήζουν προστασίας τα proccesses που “τρέχουν” σε καθε workstation. Εν προκειμένω , η Payment Process και η New Patient Register process.

*Θεωρούμε ότι οι servers βρίσκονται σε κατάλληλα διαμορφομένα server rooms

A1.2 Απειλές που εντοπίστηκαν

Περιλαμβάνει όλες τις ενδεχόμενες ενέργειες οι οποίες αξιοποιώντας τις αδυναμίες του συστήματος, μπορούν να οδηγήσουν κάποιο από τα στοιχεία του Πληροφοριακού Συστήματος σε ανεπιθύμητες καταστάσεις.

Με βάση τις ευπάθειες που εντοπίσαμε προκύπτουν οι παρακάτω απειλές κατηγοριοποιημένες ανά αγαθό:

- **AMCWS001-007 (Workstations):** Η χρήση weak passwords κάνει ευπαθές το σύστημα σε εξαντλητική δοκιμή πιθανών κλειδιών (brute force attack). Επίσης, τα μη ενημερωμένα προγράμματα/εφαρμογές δίνουν τη δυνατότητα σε κακόβουλους χρήστες να γράψουν κώδικα malware εκμεταλλευόμενοι τις γνωστές ευπάθειες αυτών των εκδόσεων. Ακόμα μία συχνή απειλή που στοχεύει τα workstations είναι το buffer overflow που δίνει δικαιώματα στον επιτιθέμενο να τρέξει δικό του κακόβουλο κώδικα. Τέλος, το γεγονός οτι τα μηχανήματα είναι εκτεθειμένα, τα καθιστά ευάλωτα σε φυσικές φθορές αλλά και σε επιθέσεις USB Rubber Ducky.Το κύκλωμα USB μεταδίδει στον υπολογιστή τα δεδομένα που παρέχει ο memory controller και σ' αυτόν (στον controller) παραδίδονται τα δεδομένα που στέλνει ο υπολογιστής.
- **AMCSRV001-003 (Servers):** Το ακατάλληλο configuration και η απαρχαιωμένη έκδοση του λογισμικού οδηγούν σε εκμετάλλευση bugs του server απο τρίτους ώστε να αποκτήσουν μη εξουσιοδοτημένη πρόσβαση σε αρχεία και φακέλους.¨Όταν ο επιτιθέμενος αποκτήσει πρόσβαση, μπορεί να υποκλέψει ευαίσθητα δεδομένα, να εκτελέσει κώδικα στον server ή να εγκαταστήσει κακόβουλο λογισμικό. Επιθέσεις όπως Denial of Service Attacks, Domain Name System Hijacking, Sniffing, Phishing, Pharming, Defacement.

- **AMCPRN001-002(Printers):** Η παλαιά έκδοση του printer που χρησιμοποιείται επιτρέπει την εκμετάλευση γνωστών ευπαθειών της συγκεκριμένης έκδοσης που δεν έχουν γίνει patch/updates απο το 2003 με αποτέλεσμα ο επιτιθέμενος να αποκτήσει πρόσβαση τόσο στο μηχάνημα όσο και στο δίκτυο του νοσοκομείου. Κατ' επέκταση και στους servers στους οποίους είναι συνδεδεμένοι.
- **AMCSW001-002 (Network Switch):** Από τη στιγμή που οι μεταγωγείς είναι εκτεθειμένοι , βρίσκονται αντιμέτωποι με απειλές φυσικής φθοράς καθώς και μη εξουσιοδοτημένης σύνδεσης συσκευης τρίτων στο δίκτυο.
- **AMCRT001-002(Router - router/firewall):** Το ακατάλληλο configuration οδηγεί σε εκμετάλλευση απο τρίτους όπως spoofing δηλαδη δημιουργία πακέτων IP με ψεύτικη διεύθυνση προέλευσης ούτως ώστε να συγκαλυφθεί η ταυτότητα του αποστολέα του πακέτου και ο παραλήπτης να νομίζει ότι προήλθε από άλλον

υπολογιστή. Ταυτόχρονα οι ευπάθειες που παρουσιάζονται στην έκδοση 15.5 του συγκεκριμένου router είναι bugs τα οποία οι επιτιθέμενοι μπορούν να εκμεταλευτούν με πολλούς τρόπους. Ενδεικτικά, στέλνοντας ένα αυτοσχέδιο DHCP Version 4 (DHCPv4) πακέτο ώστε να μολύνει το σύστημα.

- **Windows XP, Windows 7 Pro SP1 (Software) :** Οι παλιότερες εκδόσεις των windows κάνουν το σύστημα ευάλωτο σε επιθέσεις, στοχευμένες στα bugs αυτών. Ενδεικτικά στην συγκεκριμένη έκδοση των windows 7, ο επιτιθέμενος μπορεί να αποκτήσει δικαιώματα σε ένα εκτελέσιμο αρχείο εκμεταλλευόμενος την ευπάθεια που υπάρχει στον TS WebProxy (https://www.cvedetails.com/vulnerability-list/vendor_id-26/product_id-17153/hasexp-1/Microsoft-Windows-7.html). Μια άλλη απειλή τόσο στα Windows 7 όσο και στα Windows XP είναι οι επιθέσεις man-in-the-middle attacks που προκαλούνται απο την αδυναμία τους να αναγνωρίσουν X.509 (certificates(http://www.itsecdb.com/oval/definition/oval/org.mitre.oval/def/26746/Alows-man-in-the-middle-attackers-to-spoof-servers-and-read-.html)
- **Oracle Database(Software):** Η έλλειψη κρυπτογραφίας στα ευαίσθητα δεδομένα έχει ως αποτέλεσμα την εύκολη εκμετάλλευση τους από επιτιθέμενους και την διέρρευση ευαίσθητων πληροφοριών.
- **Hospital Website (Software):** Εξαιτίας της ακατάλληλης συγγραφής κώδικα κατά τη δημιουργία του website το σύστημα μας γίνεται επιρρεπές σε επιθέσεις όπως sql injection .Επίθεση κατά την οποία ο κακόβουλος χρήστης δίνει σαν είσοδο SQL statements αντί για στοιχεία εισόδου, εν αγνοία του συστήματος.
- **New Patient Register Process(Process)**: Σε περίπτωση που ένας υπολογιστής παραμείνει συνδεδεμένος σε ένα λογαριασμό χρήστη, ένας επιτιθέμενος αποκτά εύκολα πρόσβαση στο συγκεκριμένο process.
- **Payment process (Process):** Εξαιτίας της έλλειψης κρυπτογραφίας τα δεδομένα μας σε περίπτωση υποκλοπής είναι ευάλωτα.

Γενικότερα , οι απειλές δεν εστιάζονται μόνο σε αξιοποίηση τεχνικών αδυναμιών του συστήματος. Είναι σύνηθες , πληροφοριακά συστήματα να βρίσκονται αντιμέτωπα με απειλές που προέρχονται από ανθρώπινη αφέλεια ή φυσικές καταστροφές (θεομηνίες). Πιο συγκεκριμένα, η έλλειψη γνώσεων των εργαζομένων σε θέματα ασφάλειας απειλεί καθημερινά το σύστημα μας, για παράδειγμα οι ανταλλαγές κωδικών μεταξύ των εργαζομένων με μη ασφαλές τρόπο. Όσον αφορά τις φυσικές καταστροφές ,οι πόροι μας είναι εκτεθειμένοι σε ζημίες που μπορούν να προκληθούν από φωτιές, πλημμύρες, σεισμούς, φθορές, αμέλεια κτλ. Τέλος από την στιγμή που όλα είναι στο ίδιο δίκτυο και ένας κακόβουλος χρήστης αποκτήσει πρόσβαση σε μία ή παραπάνω συσκευές του δικτύου είναι εύκολο να μεταπηδήσει μέσω αυτής στις υπόλοιπες.

A1.1 Ευπάθειες που εντοπίστηκαν

Ο ορισμός της ευπάθειας περιλαμβάνει όλα τα σημεία του φυσικού περιβάλλοντος , του υλικού , του λογισμικού ή των διαδικασιών, τα οποία ενδέχεται να προσδίδουν σε κάποιους την δυνατότητα να προβούν σε ενέργειες μή επιθυμητές απο αυτούς που ανέπτυξαν ή απο αυτούς που ελέγχουν το πληροφοριακό σύστημα.

- **AMCWS001-007 (Workstations) :** Θεωρούμε ως μια ευπάθεια την χρήση μη εξουσιοδοτημένων passwords..Ο κάθε υπάλληλος δύναται να ορίσει κωδικό της αρεσκείας του χωρίς να ελέγχεται ως προς την καταλληλότητα του. Στους συγκεκριμένους Η/Υ είναι εγκατεστημένα προγράμματα τα οποία δεν ενημερώνονται ανά τακτά χρονικά διαστήματα όπως θα έπρεπε. Επιπλέον , λόγω της θέσης που βρίσκονται είναι εύκολα προσβάσιμοι από τρίτους , με αποτέλεσμα να είναι εκτεθημένοι σε κακόβουλες ενέργειες.
- **AMCSRV001-003 (Servers):** Μία ευπάθεια που παρατηρείται και στους τρεις servers είναι το ακατάλληλο configuration που έχει γίνει. Επίσης η έκδοση του λογισμικού που χρησιμοποιείται είναι απαρχαιωμένη άρα και επιρρεπής σε απειλές για το πληροφοριακό μας σύστημα.
- **AMCPRN001-002(Printers):** Η ευπάθεια που αντιμετωπίζουμε στα δυο αυτά μηχανήματα έγκειται στο ότι έχουν να κάνουν update από το 2003, με αποτέλεσμα να μην έχουν ενημερωμένο λογισμικό και να είναι ευαίσθητα σε εξωτερικές απειλές. Απαράδεκτο θεωρείται το γεγονός ότι οι printers συνδέονται άμεσα με τους servers.
- **AMCSW001-002 (Network Switch):** Ευπάθεια αποτελεί το γεγονός ότι τα network switches είναι εύκολα προσβάσιμα από μη εξουσιοδοτημένα άτομα και το γεγονός ότι δεν εχει γίνει σωστό configuration τα καθιστά επικίνδυνα.
- **AMCRT001-002(Router - router/firewall):** Τα συγκεκριμένα router χρησιμοποιούν λογισμικό το οποίο έχει πολλές ευπάθειες, με σημαντικότερη από αυτές το Cisco Bug IDs: CSCsm45390, CSCuw77959 ,καθιστώντας τα ευάλωτα σε επιθέσεις.
- **Windows XP, Windows 7 Pro SP1 (Software) :** Από τη μια βρισκόμαστε αντιμέτωποι με την παλαιότητα του συγκεκριμένου “λειτουργικού” συστήματος (Windows XP) που το καθιστά ασύμβατο με τις νεότερες εκδόσεις των προγραμμάτων . Από την άλλη , τα μηχανήματα που “τρέχουν” Windows 7 δεν έχουν κάνει updates/patches τους τελευταίους 6 μήνες .

- **Oracle Database(Software):** Το σημαντικότερο πρόβλημα που εντοπίσαμε είναι το γεγονός ότι τα δεδομένα που είναι αποθηκευμένα, δεν είναι κρυπτογραφημένα όπως επιβάλλεται λόγω της σπουδαιότητάς τους ως ευαίσθητα δεδομένα.
- **Hospital Website (Software):**Εντοπίσαμε σφάλματα στον κώδικα του website καθιστώντας το τρωτό σε κυβερνοεπιθέσεις. Για παράδειγμα, ελλιπής έλεγχος στα δεδομένα εισόδου.
- **New patient register process(Process)**: Η ευπάθεια που αντιμετωπίζουμε εδώ έγκειται στην παράβλεψη ταυτοποίησης του χρήστη μετά από μία ήδη επιτυχημένη εγγραφή. (single sign on).
- **Payment process (Process):** Η έλλειψη κρυπτογραφίας των δεδομένων μας θέτει την διαδικασία σε κίνδυνο κλοπής αυτών.

Εν γένει, εκτος από τις προαναφερθέντες ευπάθειες βρισκόμαστε αντιμέτωποι με τις εξής παραλείψεις :

- Εκτεθειμένος εξοπλισμός (καλώδια και συσκευές.)
- Τα υπάρχοντα datarooms δεν πληρούν βασικές προυποθέσεις ασφάλειας.(Υπαρξη παραθύρων και γυψοσανίδων,έλλειψη κλιματισμού , πυρόσβεσης καθως και ανεπαρκείς κλειδαριές)
- Απουσία υπεύθυνου επεξεργασίας πληροφοριών

Τέλος, η σημαντικότερη ευπάθεια που εντοπίσαμε στο πληροφοριακό μας σύστημα αποτελεί το γεγονός ότι υπάρχει ένα και μόνο δίκτυο στο οποίο είναι συνδεδεμένες όλες οι συσκευές.

Αποτελέσματα αποτίμησης

Ολοκληρώνοντας την απαρίθμηση και την ανάλυση των αγαθών , ευπαθειών και απειλών είμαστε σε θέση να παράγουμε τον κάτωθι πίνακα ο οποίος αναπαριστά την σπουδαιότητα του κινδύνου που αφορά το εκάστοτε αγαθό κάτω από συγκεκριμένες καταστάσεις , σε κλίμακα από το 1 εώς και το 10. Συμπληρώνοντας τον πίνακα , παρατηρούμε ότι οι μεγαλύτεροι αριθμοί είναι συγκεντρωμένοι στα αγαθά που αποθηκεύονται και επεξεργάζονται τα ευαίσθητα δεδομένα, δηλαδή βάσεις δεδομένων καθώς και στα αγαθά που είναι υπεύθυνα για τη διαχείριση του δικτύου.Πιο συγκεκριμένα, έχουμε αξιολογήσει την μερική ή ολική απώλεια διαθεσιμότητας των εξυπηρετητών με **10** θεωρώντας ότι η έλλειψη τους καθιστά το πληροφοριακό σύστημα του νοσοκομείου ανίκανο να λειτουργήσει ομαλά. Πέραν αυτού, αξιοσημείωτη είναι και η βαθμολόγηση των routers , με 9, αλλά και των switches με 8, υποδεικνύοντας τη σπουδαιότητα του συγκεκριμένου αγαθού άρα και της απειλής που το συνοδεύει. Δεν πρέπει βέβαια να αμελούμε και τις απειλές των υπόλοιπων αγαθών οι οποίες μπορούν να εκθέσουν σημαντικά το σύστημα μας. Στην περίπτωση των workstations αξιολογούμε την απώλεια διαθεσιμότητας και εμπιστευτικότητας τους με 8 καθώς αποτελούν το βασικό πόρο επεξεργασίας των ευαίσθητων δεδομένων μας. Εν συνεχεία, αξιολογήσαμε με 9 τις διαδικασίες διότι σε περίπτωση ολικής καταστροφής το νοσοκομείο οδηγείται σε υπολειτουργία. Η ιστοσελίδα αν και μέτριας κατηγορίας απώλεια έχει αξιολογηθεί με 10 στα λάθη μεγάλης κλίμακας (sql injection) καθώς ο επιτιθέμενος μπορεί να αποκτήσει πρόσβαση σε ευαίσθητες πληροφορίες. Τέλος, οι printers αξιολογήθηκαν με την χαμηλότερη κλίμακα σε περίπτωση απώλειας εν αντιθέση με την βαθμολογία τους στην παρακολούθηση κίνησης (8) μέσω της οποίας ο κακόβουλος χρήστης είναι σε θέση να υποκλέψει ευαίσθητες πληροφορίες.

Εν γένει, οι βαθμολογίες του πίνακα είναι υψηλές γεγονός που υποδεικνύει την κρισιμότητα των υποδομών μας και της βαρύτητας των δεδομένων μας, όπως επίσης και την ανάγκη λήψης κατάλληλων μέτρων για την προστασία τους.

	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	καταστροφή Ολική	απώλεια Μερική	αλλοίωση Σκόπιμη	κλίμακας Λάθη μικρής	κλίμακας Λάθη μεγάλης	Εσωτερικούς	Υπηρεσιών Παρόχους	Εξωτερικούς	μηνυμάτων Επανάληψη	Αποστοίχηση αποστολέα	Αποστοίχηση παραλήπτη	ή παραλαβής αποστολής Άρνηση	λανθασμένων μηνυμάτων Παρεμβολή	δρομολόγηση Λανθασμένη	κίνησης Παρακολούθηση	Μη παράδοση	θέας μηνυμάτων Απώλεια ακολου-
AMCWS001-007 Windows XP, Windows 7 Pro SP1	3	4	5	5	7	8	8	6	5	7	4	7	5	3	9	6	8	8	7	7	8	9	7	7
AMCSRV001-003 Oracle Database	4	6	8	8	9	10	10	10	8	9	6	9	9	9	10	8	10	10	8	9	10	9	9	9
AMCPRN001-002	1	1	2	3	5	5	6	5	4	4	2	4	2	2	6	4	5	5	3	5	6	8	5	5
AMCSW001-002	2	3	4	4	6	7	7	7	5	6	3	6	2	2	8	6	7	7	7	7	8	8	8	8
AMCRT001-002	2	3	4	4	6	8	8	8	6	8	6	8	2	2	9	6	8	8	7	7	8	8	8	8

Hospital Website	1	1	1	2	5	5	6	7	5	7	4	10	1	2	8	6	3	3	7	7	5	6	6	6
New Patient Register process	3	4	5	5	8	8	9	9	7	7	4	7	6	6	8	6	8	8	6	7	7	7	7	7
Payment Process	3	4	5	5	8	8	9	9	7	8	4	7	7	7	8	7	8	8	7	8	8	8	8	8

Β2. ΠΡΟΤΕΙΝΟΜΕΝΑ ΜΕΤΡΑ ΑΣΦΑΛΕΙΑΣ

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

Α1. Προσωπικό – Προστασία Διαδικασιών Προσωπικού

Α2. Ταυτοποίηση και αυθεντικοποίηση

Α3. Έλεγχος προσπέλασης και χρήσης πόρων

Α4. Διαχείριση εμπιστευτικών δεδομένων

Α5. Προστασία από τη χρήση υπηρεσιών από τρίτους

Α6. Προστασία λογισμικού

Α7. Διαχείριση ασφάλειας δικτύου

Α8. Προστασία από ιομορφικό λογισμικό

Α9. Ασφαλής χρήση διαδικτυακών υπηρεσιών

Α10. Ασφάλεια εξοπλισμού

Α11. Φυσική ασφάλεια κτιριακής εγκατάστασης

Τα μέτρα έχουν εφαρμογή στο ΠΣ του Νοσοκομείου.

Προσωπικό – Προστασία Διαδικασιών Προσωπικού

Το προσωπικό θα πρέπει να ενημερώνεται συχνά για την σπουδαιότητα της ασφάλειας και στη συνέχεια να λάβει την κατάλληλη πληροφόρηση σχετικά με το πώς θα διαχειρίζεται τους Η/Υ ορθά. Μια καλή τακτική αποτελεί η διοργάνωση σεμιναρίων και παρουσιάσεων από ειδικούς πάνω στα προαναφερθέντα . Ο εργαζόμενος , μετά την επιμόρφωση του, θα είναι σε θέση να κρίνει ποίες ενέργειες είναι θεμιτές κατά την χρήση Η/Υ. Για παράδειγμα, πρέπει να αναγνωρίζει και να αποφεύγει ύποπτα email και διαδικτυακές απάτες. Αυτό το μέτρο θα πλαισιώνεται από ένα σύνολο κανονισμών και διαδικασιών αυστηρά ορισμένων από την διοίκηση με σκοπό την αποφυγή περιστατικών που μπορούν να είναι επιβλαβή για το σύστημα. Ενδεικτικά, προτείνεται η απαγόρευση των social media , ιστοσελίδων που κρίνονται επικίνδυνες καθώς και οποιαδήποτε ενέργεια που κρίνεται άσχετη με το αντικείμενο εργασίας τους (π.χ. Downloads για προσωπική χρήση).Επιπλέον, ο υπάλληλος δεν θα πρέπει να αφήνει εκτεθειμένο τον χώρο εργασίας του ενώ θα πρέπει κατά την απομάκρυνσή του από αυτόν, να αποσυνδέεται από το δίκτυο με log out . Επιπροσθέτως ,απαγορεύεται ρητά η σύνδεση -μη εγκεκριμένης , καταγεγραμμένης συσκευής στο δίκτυο με μοναδική εξαίρεση ειδικές καταστάσεις που χρίζουν άμεσης αντιμετώπισης . Εν τέλει, προτείνουμε workplace reporting requirements για ηλεκτρονική παρενόχληση, διακρίσεις καθώς και αναφορά σχετικά με ηλεκτρονικές απάτες ή περιπτώσεις κακής πρόσβασης σε

ηλεκτρονικές πληροφορίες. Τα παραπάνω μέτρα στοχεύουν όχι μόνο στην ασφάλεια των workstations αλλά και ολόκληρου του πληροφοριακού συστήματος.

Ταυτοποίηση και αυθεντικοποίηση

Με βάση τις απειλές που εντοπίσαμε σχετικά με την ταυτοποίηση και αυθεντικοποίηση προτείνουμε την χρήση password generator για την παραγωγή 16ψήφιων κωδικών. Οι κωδικοί αυτοί θα αποθηκεύονται στη βάση δεδομένων ως hashes και όχι ως plain text έτσι ώστε σε περίπτωση κλοπής των κωδικών να μην είναι σε θέση να εξάγουν τον κωδικό. Σε συνδυασμό με τη χρήση one time password (two factor authentication) επιτυγχάνεται η αποφυγή επιθέσεων στοχευμένων στην αδυναμία των κωδικών όπως brute force attack. Κατά αυτόν τον τρόπο προστατεύεται αποτελεσματικά η πρόσβαση στους λογαριασμούς των υπαλλήλων στα workstations.

Επιπλέον ο κάθε εργαζόμενος φέρει συγκεκριμένα δικαιώματα(authentication privileges) τα οποία διαφοροποιούνται ανάλογα με την θέση που κατέχει στο νοσοκομείο. Πιο συγκεκριμένα τα δικαιώματα που του αναλογούν αντικατοπτρίζουν την ευθύνη της εργασίας του. Το συγκεκριμένο μέτρο απευθύνεται στην προστασία των δεδομένων(data, server) και του δικτύου.

Έλεγχος προσπέλασης και χρήσης πόρων

Στα μέτρα αυτά συμπεριλαμβάνονται όλες οι ενέργειες που έχουμε προτείνει ως απαραίτητες στην παράγραφο Α2 για την έγκυρη ταυτοποίηση και αυθεντικοποίηση. Επιπλέον πρέπει να εξασφαλίσουμε την σωστή εξουσιοδότηση στους χρήστες του πληροφοριακού συστήματος. Αυτό μπορεί να πραγματοποιηθεί μέσω μίας λίστας που είναι καταγεγραμμένοι όλοι οι χρήστες του συστήματος με τα δικαιώματα του καθενός. Τέλος, πρέπει να αποφυγούν τακτικές όπως single sign on και να απαιτείται Login σε κάθε είσοδο σε εφαρμογές/ ιστοσελίδες.

Διαχείριση εμπιστευτικών δεδομένων

Ένα από τα βασικότερα μέτρα προστασίας που προτείνουμε για την ασφάλεια των ευαίσθητων δεδομένων που μεταφέρονται στο δίκτυο μας είναι η ασφαλής επικοινωνία (secure communication). Πιο συγκεκριμένα αυτό επιτυγχάνεται μέσω encrypted network communication ή digital signature.

Λόγω της σπουδαιότητας της φύσης των δεδομένων κρίνεται απαραίτητη η προστασία της βάσης δεδομένων με διαδικασίες αποτελεσματικής κρυπτογράφησης, όπως επίσης και των διαδικασιών που κάνουν χρήση αυτών. Επιπλέον μέτρα για το σκοπό αυτό είναι η αλλαγή

των default settings(π.χ, username, password), η συχνή ενημέρωση των critical patches , αφαίρεση των άσκοπων public privileges. Επιπροσθέτως θα πρέπει να υπάρχει ένας backup server στον οποίο θα είναι αποθηκευμένα όλα τα δεδομένα σε περίπτωση απώλειας των αρχικών δεδομένων. Τα παραπάνω μέτρα αφορούν την προστασία της βάσης δεδομένων, του server και των δεδομένων .

Εντούτοις, θα πρέπει να παρθούν τα κατάλληλα μέτρα για την φυσική ασφάλεια τόσο των φακέλων που περιέχουν προσωπικά δεδομένα όσο και των φορητών αποθηκευτικών μέσων. Είναι προφανές ότι δεν θα πρέπει να αφήνονται εκτεθειμένα , χωρίς επίβλεψη ,πάνω σε γραφεία αλλά σε συγκεκριμένους ασφαλείς και προκαθορισμένους χώρους. Από την άλλη θα πρέπει να καταγράφεται η μεταφορά των φυσικών φακέλων σε διαφορετικά γραφεία ή οργανωτικές μονάδες. Τα παραπάνω μέτρα αφορούν τα ευαίσθητα προσωπικά δεδομένα (data).

Προστασία από τη χρήση υπηρεσιών από τρίτους

Ενα απο τα βασικότερα αγαθά τα οποία πρέπει να προστατέψουμε απο τρίτους είναι τα workstations ,λαμβάνοντας κάποια απο τα μέτρα τα οποία αναφέραμε στις παραγράφους A1,A10. Ενδεικτικά, θα πρέπει σε περίπτωση αδρανοποίησης να αναπτυχθούν διαδικασίες αυτόματης αποσύνδεσης, μετά από λίγα λεπτά,και προφύλαξης της οθόνης- για την απενεργοποίηση της οποίας θα απαιτείται χρήση συνθηματικού.

Καθοριστικής σημασίας για την διαφύλαξη των αγαθών απο τρίτους είναι η ασφάλεια του δικτύου , η οποία θα αναλυθεί εκτενέστερα στη παράγραφο A7.

Εν συνεχεία, στην κατηγορία αυτή ανήκει και η δημιουργία, ειδικά ασφαλισμένου/προστατευμένου, server room που θα περιέχει τις κρίσιμες υποδομές του δικτύου του Νοσοκομείου(εκτενέστερη αναφορά στο A10).

Προστασία λογισμικού

Οι εφαρμογές που χρησιμοποιούνται, στο Νοσοκομείο, για την επεξεργασία προσωπικών πληροφοριών θα πρέπει να πληρούν και να είναι σύμφωνες με το άρθρο 4 του ν. 2472/1997 και να ακολουθούν την αρχή της ελαχιστοποίησης των δεδομένων. Επίσης, τα λειτουργικά αρχεία των συστημάτων, τα δεδομένα ελέγχου συστημάτων καθώς και ο πηγαίος κώδικας των προγραμμάτων πρέπει να ελέγχονται και να προστατεύονται από μη εξουσιοδοτημένη πρόσβαση ή τροποποίηση. Απαραίτητη κρίνεται η αντικατάσταση των default κωδικών/ρυθμίσεων κατά την εγκατάσταση νέων προγραμμάτων/ μηχανημάτων.

Για ασφαλέστερη χρήση των Η/Υ συνιστούμε την εγκατάσταση αξιόπιστων antivirus προγραμμάτων.

Προτείνουμε την τακτική εγκατάσταση patches προκειμένου να επιδιορθωνουμε bugs του λογισμικου. Πέραν αυτού , απαραίτητη θεωρείται η αντικατάσταση του παρόντος λειτουργικού συστήματος (Windows xp) με νεότερο.

Διαχείριση ασφάλειας δικτύου

Ένα από τα πρώτα και σημαντικότερα μέτρα που προτείνουμε είναι η δημιουργία διαφορετικών υποδικτύων με χρήση subnet mask για την απομόνωση και προστασία των κρίσιμων υποδομών του δικτύου μας. Η τακτική αυτή οδηγεί στην ανεξαρτησία τους , δηλαδή στην χείριστη περίπτωση που ένας κακόβουλος χρήστης αποκτήσει πρόσβαση σε μία συσκευή υποδικτύου δεν απειλεί άμεσα τις υπόλοιπες συσκευές εκτός αυτού . Εν παραλλήλω, κρίνεται απαραίτητη η ύπαρξη υπεύθυνου επεξεργασίας που θα είναι υπόλογος για την ασφάλεια του πληροφοριακού μας συστήματος.

Τα network switches/routers θα έχουν καταλόγους με τις authorized συσκευές(ACL). Πρέπει να απαιτούν την σύνδεση του χρήστη με username/password ώστε στη περίπτωση σύνδεσης unauthorized συσκευής να μην επιτρέπουν την πρόσβαση στο δίκτυο και να καταγράφεται η προσπάθεια σύνδεσής τους. Καθοριστικής σημασίας είναι η αλλαγή default settings / passwords. Διατηρώντας τους κωδικούς ενημερωμένους και εγκαθιστώντας τα νεότερα firmware είναι μικρές ενέργειες που μπορούν να βελτιώσουν αισθητά την ασφάλεια του δικτύου. Από την άλλη επιδιώκουμε την αποσύνδεση των printers από τους servers προτιμώντας την άμεση σύνδεση τους στους Η/Υ μέσω USB.

Επιβάλλεται η ανανέωση και η συντήρηση του firewall όπως επίσης και η χρήση encrypted network communication ώστε να ελέγχεται και να προστατεύεται η κίνηση των πακέτων των δεδομένων μας στο δίκτυο.

Εν τέλει θα πρέπει πάντοτε να ανατρέχουμε (συμβουλευόμαστε) στο χάρτη δικτύου προκειμένου να είμαστε υπεύθυνοι και να έχουμε πλήρη εικόνα του δικτύου μας.

Προστασία από ιομορφικό λογισμικό

Καθοριστικό ρόλο στην προστασία του πληροφοριακού μας συστήματος έχει το firewall. Κρίνουμε άμεση την αντικατάσταση του από νεώτερη έκδοση η οποία θα είναι ικανή να φιλτράρει αποτελεσματικά την κίνηση του δικτύου μπλοκάροντας παράλληλα την πρόσβαση σε ύποπτες ιστοσελίδες (application layer). Εν συνεχεία, όπως έχει προαναφερθεί επενδύουμε στην ενημέρωση και συχνή πληροφόρηση των υπαλλήλων με σκοπό την ανάπτυξη της κριτικής τους ικανότητας καθώς και της τεχνολογικής τους

εξοικείωσης. Έτσι θα βρίσκονται σε θέση , να αναγνωρίζουν ηλεκτρονικές απάτες καθώς και άλλες ύποπτες τακτικές και να τις αναφέρουν άμεσα μέσω του workplace reporting system που παρουσιάσαμε στο Α1.Ταυτόχρονα, θα πρέπει να καθιερωθούν συγκεκριμένες μέρες του μήνα όπου θα πραγματοποιούνται computer scans , από συγκεκριμένο προσωπικό, με σκοπό τον εντοπισμό και την εξόντωση ύποπτων αρχείων και προγραμμάτων.Από την άλλη, θα πραγματοποιείται , ανά τακτά χρονικά διαστήματα, έλεγχος για διαθέσιμες ενημερώσεις (updates, patches) που είναι απαραίτητο να μην παραλείπονται . Αυτονόητη θεωρείται η ελεγχόμενη εκκίνηση των εκάστοτε προγραμμάτων (disable autorun) . Ολοκληρώνοντας , θα πρέπει να ορισθεί συγκεκριμένο antivirus και spyware που θα ταιριάζει στις ανάγκες του νοσοκομείου.

Ασφαλής χρήση διαδικτυακών υπηρεσιών

Όπως έχουμε αναφέρει σε προηγούμενες ενότητες η εκπαίδευση των υπαλλήλων είναι πρωταρχικής σημασία για την ασφαλή χρήση των διαδικτυακών υπηρεσιών. Εγκατάσταση προγραμμάτων antivirus και spyware σε συνδυασμό με το κατάλληλο firewall είναι ικανά να προστατεύσουν αποτελεσματικά τα μηχανήματα μας απο διαδικτυακές επιθέσεις.

Ασφάλεια εξοπλισμού

Επιδιώκουμε την δημιουργία κοινού server room το οποίο θα φιλοξενεί τους 3 servers και τα router και θα είναι εξοπλισμένο με όλα τα απαραίτητα μέτρα προστασίας. Απαιτείται μία και μοναδική είσοδος, χωρίς παράθυρα, με ελεγχόμενη - καταγραφόμενη πρόσβαση μέσω digital code door lock . Ιδανικά το δωμάτιο αυτό θα πρέπει να είναι δύσκολα προσβάσιμο, σε όροφο που έχει πρόσβαση μόνο το προσωπικό του νοσοκομείου. Κατά τον σχεδιασμό πρέπει να ληφθεί μέριμνα ώστε να διασφαλιστεί ότι τα τοιχώματα του δωματίου είναι ενισχυμένα. Επιπροσθέτως, θα πρέπει να επιβεβαιωθεί ότι οι διαδρομές σωλήνων νερού και ηλεκτροφόρων καλωδίων δεν τρέχουν δίπλα στο server room . Για να διασφαλιστεί η αυτονομία του θα πρέπει να συνδέεται με μια εφεδρική γεννήτρια, η οποία σε περίπτωση διακοπής ρεύματος θα ενεργοποιηθεί Εν συνεχεία, η θερμοκρασία του server room θα πρέπει να διατηρείται σταθερή σε χαμηλές τιμές για την αποφυγή υπερθέρμανσης και αυτό επιτυγχάνεται με κατάλληλες μονάδες air-condition που θα προστεθούν .Θα υπάρχει κατάλληλο πυροσβεστικό σύστημα cdt extinguishing το οποίο είναι ικανό να εξουδετερώσει άμεσα ενδεχόμενη πυρκαγιά προστατεύοντας παράλληλα τα μηχανήματα. Για την αντιμετώπιση των σεισμών θα γίνει κατάλληλη εγκατάσταση ειδικών σκελετών από επαγγελματίες.

Εκτός απο τα μέτρα που αφορούν την προστασία του server room προτείνεται η λήψη μέτρων σχετικών με τα workstations και τα switches . Ενδεικτικά θα πρέπει ο χώρος που βρίσκονται να απομονωθεί με κατάλληλη κατασκευή, η οποία θα δίνει την αίσθηση της

ιδιωτικότητας προστατεύοντας τον εξοπλισμό από κοινή θέα, συμπεριλαμβανομένων και των καλωδίων.

Φυσική ασφάλεια κτιριακής εγκατάστασης

Οφείλουμε να προστατεύσουμε τις εγκαταστάσεις μας από φυσικές καταστροφές. Αρχικά, είναι απαραίτητη η τοποθέτηση θυρών πυρασφάλειας σε όλες τις εισόδους. Επιπλέον σε κάθε δωμάτιο και διάδρομο θα πρέπει να υπάρχει πυροσβεστήρας εύκολα προσβάσιμος όπως και σύστημα εντοπισμού καπνού. Χρήσιμη θεωρείται και η προσθήκη συστήματος ανίχνευσης υγρασίας και πλημμύρας. Τέλος, θα πρέπει να ληφθούν τα απαραίτητα μέτρα προστασίας σε περίπτωση σεισμού όπως: ασφάλιση των υπολογιστών και τοποθέτηση της κεντρικής μονάδας στο έδαφος, ασφάλιση ραφιών και βιβλιοθηκών και γενικότερα οποιουδήποτε επίπλου ξεπερνά το ύψος του γραφείου και τοποθέτηση επικίνδυνων υλικών σε ασφαλές μέρος.

Εν κατακλείδι, σε περίπτωση τροποίησης του υπάρχοντος τοπολογικού δικτύου (πρόσθεση και αφαίρεση συσκευών) κρίνεται απαραίτητη η δημιουργία νέου σχεδίου ασφάλειας.

A1. ΣΥΝΟΨΗ ΠΙΟ ΚΡΙΣΙΜΩΝ ΑΠΟΤΕΛΕΣΜΑΤΩΝ

Υπάρχουν πολλά high risk αγαθά τα οποία καλούμαστε να αντιμετωπίσουμε, επομένως θα τα παραθέσουμε με σειρά προτεραιότητας όπως έχει προκύψει από τον δείκτη RPN.

Αρχικά , η μεγαλύτερη απειλή που εντοπίσαμε, με δείκτη 490, είναι η έλλειψη κρυπτογραφίας στη βάση δεδομένων (server) αφού εκεί φυλάσσονται τα ευαίσθητα δεδομένα του νοσοκομείου. Δεύτερο στη κατάταξη βρίσκονται τα workstations καθώς και ο server με αντίστοιχες απειλές το DDOS attack και Ddos/sniffing με δείκτη 441. Εν συνεχεία , ακολουθεί το website το οποίο απειλείται με επίθεση SQL injection , η οποία έμμεσα διακιινδυνεύει το Database με δείκτη 392.

Έπεται , μια άλλη σύνηθης απειλή , το buffer overflow, που στοχεύει τα workstations και έχει δείκτη 294. Με αξιολόγηση 252 ακολουθούν τα routers και system softoware με αντίστοιχες απειλές DHCPv4 και Man in the middle attack. Εν τέλει , παραθέτουμε τις απειλές που φέρουν τον μικρότερο δείκτη RPN , όντας ουραγοί στο πίνακα μας: Exposed switches , not updated printers, exposed workstations , weak passwords και ipspoofing on routers.