ΑΣΦΑΛΕΙΑ ΠΛΗΡΟΦΟΡΙΑΚΩΝ ΣΥΣΤΗΜΑΤΩΝ ΚΑΙ ΚΡΙΣΙΜΩΝ ΥΠΟΔΟΜΩΝ

ΣΧΕΔΙΟ ΑΣΦΑΛΕΙΑΣ

ΟΝΟΜΑ ΕΡΓΑΣΙΑΣ: myHospital_Care

ΣΥΓΓΡΑΦΕΙΣ:
ΗΡΩ ΑΝΑΓΝΩΣΤΑΚΗ + 3140008
ΟΡΦΕΑΣ ΒΑΓΓΕΛΑΚΗΣ + 3140018
ΕΙΡΗΝΗ – ΡΑΦΑΕΛΛΑ ΓΑΖΕΠΙΔΟΥ + 3140262

ΕΡΓΑΣΙΑ ΧΕΙΜΕΡΙΝΟΥ ΕΞΑΜΗΝΟΥ 2017

ΠΕΡΙΕΧΟΜΕΝΑ

Α1. ΕΙΣΑΓΩΓΗ

Η τεχνολογία με την πάροδο του χρόνου συνεχώς εξελίσσεται και εισβάλλει ολοένα και περισσότερο στην καθημερινότητα μας. Συγκεκριμένα, επηρεάζει σε μεγάλο βαθμό τον τομέα και τις εξελίξεις της Ιατρικής.

Τα νοσοκομεία αποτελούν ένα από τα βασικότερα κομμάτια της ζωής μας, καθώς παρέχουν περίθαλψη στους ασθενείς που πάσχουν από διάφορες ασθένειες.

Αυτές οι ασθένειες προκαλούνται από τις κλιματικές αλλαγές, την κληρονομικότητα, τον τρόπο ζωής, την ψυχολογία του ανθρώπου κλπ.

Για αυτούς τους λόγους τα νοσοκομεία είναι απαραίτητο να παρακολουθούν καθημερινά τις δραστηριότητες τους και να καταγράφουν πλήρως τα προσωπικά στοιχεία των ασθενών.

Αυτό θα πραγματοποιηθεί με ένα λειτουργικό σύστημα που συνδέει όλες τις διασκορπισμένες δραστηριότητες του σε μία. Το λειτουργικό σύστημα αυτό θα οδηγήσει στην καλύτερη οργάνωση, ομαλή και επιτυχημένη λειτουργία των νοσοκομείων.

Συμπερασματικά, τα πληροφοριακά συστήματα αποτελούν μία γέφυρα μεταξύ του ανθρώπινου δυναμικού και των δεδομένων, διαδικασιών και τεχνολογιών πληροφορίας.

Α1.1 Περιγραφή Εργασίας

Ο σκοπός της εργασίας είναι η μελέτη της ασφάλειας της πληροφορίας, η ανάπτυξη και αξιολόγηση ενός ολοκληρωμένου πληροφοριακού συστήματος σε ένα νοσοκομείο.

Η παρούσα εργασία αναλύει την επικινδυνότητα του πληροφοριακού συστήματος του νοσοκομείου, έτσι ώστε να υπάρχει ομαλή λειτουργία και οργάνωση.

Δραστηριότητες όπως για παράδειγμα η αρχειοθέτηση των ασθενών, η εγγραφή του ιστορικού τους, η επεξεργασία των ευαίσθητων προσωπικών δεδομένων τους, ο τακτικός ηλεκτρονικός έλεγχος τόσο των εξετάσεων όσο και των φαρμάκων, η ενημέρωση των ασθενών και του προσωπικού των νοσοκομείων αποτελούν τις βασικότερες λειτουργίες του συστήματος αυτού.

Αυτό επιτυγχάνεται, με τη δημιουργία και το σχεδιασμό ενός πληροφοριακού συστήματος, το οποίο παρέχει λειτουργικά δεδομένα σε πραγματικό χρόνο έτσι ώστε οι υπεύθυνοι να μπορούν να διαχειρίζονται οτιδήποτε χρειάζονται ή είναι απαραίτητο.

Στόχος ή σκοπός του πληροφοριακού συστήματος, είναι η παροχή ποιοτικής φροντίδας ασθενών όσο το δυνατόν αποτελεσματικότερα.

Ο όρος ανάλυση της επικινδυνότητας αφορά την αναγνώριση, αποτίμηση, αντιμετώπιση της επικινδυνότητας με στόχο την ασφάλεια του συστήματος. Η ασφάλεια του πληροφοριακού συστήματος είναι πολύ σημαντική και απαραίτητη, καθώς βασίζεται στις έννοιες της εμπιστευτικότητας, ακεραιότητας και διαθεσιμότητας.

Συγκεκριμένα:

- **Εμπιστευτικότητα:** Η εμπιστευτικότητας ενός πληροφοριακού συστήματος εξασφαλίζει την απόκρυψη των ευαίσθητων πληροφοριών - δεδομένων των ασθενών από μη εξουσιοδοτημένους χρήστες.

- **Ακεραιότητα:** Η ακεραιότητα εξασφαλίζει την ακρίβεια και τη διατήρηση των ευαίσθητων πληροφοριών. Με άλλα λόγια, με την ακεραιότητα αποφεύγεται η τροποποίηση και επεξεργασία των πληροφοριών από μη εξουσιοδοτημένους χρήστες. Επιπλέον, οι χρήστες που δεν είναι εγγεγραμμένοι στο πληροφοριακό σύστημα δεν θα έχουν τη δυνατότητα να χρησιμοποιήσουν ή να εισέλθουν σε αυτό.
- **Διαθεσιμότητα:** Η διαθεσιμότητα εξασφαλίζει τη χρήση των ευαίσθητων πληροφοριών, του δικτύου, των υπολογιστών και γενικότερα του πληροφοριακού συστήματος οποιαδήποτε στιγμή.

Α1.2 Δομή παραδοτέου

Σκοπός αυτής της εργασίας είναι η ανάπτυξη και η αξιολόγηση του πληροφοριακού συστήματος του νοσοκομείου, καθώς παρουσιάζεται η ανάλυση ενός σχεδίου ασφαλείας .

Η μελέτη της εργασίας παρουσιάζεται αναλυτικά ως εξής:

- Στο **1ο κεφάλαιο**, γίνεται μία εισαγωγή για την σημαντικότητα της ύπαρξης ενός πληροφοριακού συστήματος σε ένα νοσοκομείο. Επιπλέον, αναλύεται το σύστημα βασισμένο σε ένα σχέδιο ασφάλειας.
- Στο **2ο κεφάλαιο**, αποτυπώνεται το πληροφοριακό σύστημα του νοσοκομείου. Σε αυτήν την περιγραφή αναλύονται ο εξοπλισμός, το δίκτυο, τα δεδομένα, οι διαδικασίες που αφορούν τους χρήστες και τους χειριστές του συστήματος, τα λογισμικά και οι εφαρμογές που χρησιμοποιούνται.
- Στο **3ο κεφάλαιο**, γίνεται η αποτίμηση των αγαθών του πληροφοριακού συστήματος του νοσοκομείου. Στο αρχείο excel που έχει παραδοθεί, παρουσιάζονται όλα τα αγαθά του συστήματος καθώς και οι λειτουργίες τους. Με βάση τις λειτουργίες του αγαθού, αναφέρεται και η ανάλογη ευπάθεια, απειλή και τα αποτελέσματα που δημιουργούνται. Οι ευπάθειες, οι απειλές και η πιθανότητα εμφάνισης των απειλών διαφέρει από αγαθό σε αγαθό και για αυτό το λόγο υπάρχει και διαφορετική αποτίμηση. Επιπλέον, περιγράφονται και πιο αναλυτικά τα αγαθά, οι απειλές, οι ευπάθειες του πληροφοριακού συστήματος και τα αποτελέσματα της αποτίμησης τους.
- Στο **4ο κεφάλαιο**, παρουσιάζονται τα μέτρα αντιμετώπισης ανάλογα με τις κατηγορίες που ανήκουν. Τα μέτρα αντιμετώπισης συμβάλλουν στην εξασφάλιση της ασφάλειας του πληροφοριακού συστήματος.
- Στο **5ο κεφάλαιο**, γίνεται η αποτίμηση των πιο σημαντικών αποτελεσμάτων που έχουν την υψηλότερη επικινδυνότητα.

Α2. ΜΕΘΟΔΟΛΟΓΙΑ ΜΕΛΕΤΗΣ ΑΣΦΑΛΕΙΑΣ

Για τη Διαχείριση Επικινδυνότητας του **myHospital_Care** 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.

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

- 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*

Α2.1 Περιγραφή Πληροφοριακού Συστήματος (ΠΣ) υπό έλεγχο

Στην ενότητα αυτή, καταγράφονται το υφιστάμενο πληροφοριακό σύστημα του **myHospital_Care**, τα οποία με το πέρας της μελέτης θα επικαιροποιηθούν, αναβαθμιστούν ή σε κάποιες περιπτώσεις αντικατασταθούν.

A2.1.1 Υλικός εξοπλισμός (hardware)

Οι προδιαγραφές των υλικών και του εξοπλισμού του πληροφοριακού συστήματος του νοσοκομείου παίζουν πολύ καθοριστικό ρόλο στην σύνθεση του. Ο όρος υλικό αναφέρεται σε όλες τις συσκευές που χρησιμοποιούν το σύστημα. Οι συσκευές αυτές μπορεί να είναι υπολογιστές, μονάδες αποθήκευσης πληροφοριών, δίκτυα κλπ.

Το πληροφοριακό σύστημα του νοσοκομείου αποτελείται από δύο server υπολογιστές, δύο εκτυπωτές, έξι υπολογιστές ή αλλιώς PC, δύο ηλεκτρικές συσκευές που έχουν καθοριστικό ρόλο στο δίκτυο των υπολογιστών και ονομάζονται switch, καθώς και δύο δρομολογητές ή router.

A2.1.2 Λογισμικό και εφαρμογές

Υπάρχουν διάφορες μορφές λογισμικού σε ένα οργανισμό και συγκεκριμένα σε ένα νοσοκομείο. Πέρα από το λογισμικό που αφορά το πληροφοριακό σύστημα, υπάρχει συνήθως και λογισμικό που αφορά την κοστολόγηση των φαρμάκων, την μισθοδοσία των υπαλλήλων κλπ.

Στην περίπτωση του πληροφοριακού συστήματος του νοσοκομείου, τα λογισμικά που χρησιμοποιούνται είναι τα εξής:

- IOS 12.4 Basic IP, το οποίο λειτουργεί στα Network Switch.
- IOS 15.5 Basic IP, το οποίο λειτουργεί στο router που συνδέεται με το Internet.
- IOS 15.5 Advanced IP Services το οποίο λειτουργεί στο router. Το router το συγκεκριμένο λειτουργεί και ως firewall.
- Windows XP, το οποίο λειτουργεί στους υπολογιστές που βρίσκονται στα Patient Room.
- Windows 7 Pro SP1, το οποίο το λειτουργεί στους υπολογιστές στα Secretary Room.

A2.1.3 Δίκτυο

Στο κτίριο του νοσοκομείου υπάρχουν 3 δωμάτια ή αλλιώς 3 Patient Room στον πρώτο όροφο, όπου το καθένα έχει και το δικό του υπολογιστή. Οι υπολογιστές είναι κατασκευασμένοι από την εταιρεία Hewlett Packard και συγκεκριμένα είναι το μοντέλο HP Compaq Elite 8300 MT. Ο ένας HP υπολογιστής, που βρίσκεται στο ένα Patient Room, έχει IP 192.168.1.14 και σειριακό αριθμό CZ00000004. Σε διπλανό δωμάτιο βρίσκεται ένας άλλος HP υπολογιστής, όπου έχει IP 192.168.1.15 και σειριακό αριθμό CZ00000005. Στο τρίτο και τελευταίο δωμάτιο που σε αυτόν τον όροφο, είναι ένας HP υπολογιστής, ο οποίος έχει IP 192.168.1.16 και σειριακό αριθμό CZ00000006. Οι HP υπολογιστές χρησιμοποιούνται για την καταγραφή και επεξεργασία των ευαίσθητων ιατρικών δεδομένων των ασθενών. Το λειτουργικό που τρέχουν είναι Microsoft Windows XP.

Αυτοί οι υπολογιστές δημιουργούν ένα υποδίκτυο μέσω μιας ηλεκτρικής συσκευής που ονομάζεται switch. Το switch βρίσκεται και αυτό στον πρώτο όροφο και ο κατασκευαστής του είναι η εταιρεία Cisco. Συγκεκριμένα, είναι το μοντέλο Cisco SF200-24P και τρέχει το λειτουργικό IOS 12.4 Basic IP. Έχει IP διεύθυνση την 192.168.1.6 και σειριακό αριθμό SV84573921.

Αυτό το υποδίκτυο συνδέεται με έναν HP υπολογιστή Server που βρίσκεται σε ξεχωριστό δωμάτιο στον πρώτο όροφο και τρέχει το λειτουργικό Microsoft Windows Server 2012 SP1. Ο server έχει κατασκευαστή την εταιρεία Hewlett Packard και το μοντέλο του είναι HP Proliant D 360 Gen 9. Επίσης, έχει IP διεύθυνση 192.168.1.3 και σειριακό αριθμό CZF1545832.

Στο ίδιο δωμάτιο με τον HP υπολογιστή Server της εταιρείας συνδέεται και ένας εκτυπωτής της εταιρείας Epson. Ο εκτυπωτής αυτός, είναι το μοντέλο Epson AcuLaser C2900N και έχει λογισμικό Firmware. Η IP διεύθυνση του εκτυπωτή είναι η 192.168.1.5 και ο σειριακός αριθμός είναι ZX38234448. Επιπλέον, το λογισμικό του εκτυπωτή έχει να αναβαθμιστεί από το 2003.

Συνεπώς, με την ύπαρξη του switch δημιουργείται ένα υποδίκτυο, το οποίο συνδέεται με ένα router/firewall της εταιρείας Cisco. Το μοντέλο του router/firewall είναι Cisco 800M Series ISR και το οποίο τρέχει λειτουργικό IOS 15.5 Advanced IP Services. Το

router/firewall,που αναφέρθηκε παραπάνω, βρίσκεται σε ένα ξεχωριστό δωμάτιο καθώς έχει IP 192.168.1.2 και σειριακό αριθμό SV23412386.

Σε άλλον όροφο του νοσοκομείου 3 δωμάτια ή 3 Secretary Room, όπου το καθένα έχει και από έναν υπολογιστή της εταιρείας Hewlett Packard. Οι HP υπολογιστές, είναι συγκεκριμένα το μοντέλο HP Compaq Elite 8300 MT και έχουν λειτουργικό τα Windows 7 Pro SP1 της Microsoft. Στο ένα δωμάτιο που είναι η Γραμματεία, ο HP υπολογιστής έχει IP διεύθυνση 192.168.1.11 και σειριακό αριθμό CZ00000003. Στο δωμάτιο που γίνονται οι εγγραφές των ασθενών, υπάρχει ένας HP υπολογιστής με IP 192.168.1.12 και σειριακό αριθμό CZ00000001. Στο επιπλέον δωμάτιο που γίνονται οι εγγραφές, ο HP υπολογιστής έχει IP192.168.1.13 και σειριακό αριθμό CZ00000002.

Αυτοί οι υπολογιστές που αναφέρθηκαν παραπάνω, συνδέονται με ένα switch, το οποίο τρέχει και αυτό λειτουργικό IOS 12.4 Basic IP. Το switch είναι κατασκευασμένο από την εταιρεία Cisco και το μοντέλο του είναι Cisco SF200-24P. Η IP του είναι η 192.168.1.7 και ο σειριακός αριθμός του είναι οι SV84573922.

Αυτό το υποδίκτυο συνδέεται με έναν HP υπολογιστή server της εταιρείας Hewlett Packard και το μοντέλο του είναι το Cisco SF200-24P, με σειριακό αριθμό SV84573922. Ο υπολογιστής Server βρίσκεται και αυτός σε ξεχωριστό δωμάτιο από τους HP υπολογιστές και τρέχει το λειτουργικό Microsoft Windows 2012 Server SP1. Επιπλέον, η IP διεύθυνση του είναι 192.168.1.7.

Στο ίδιο δωμάτιο με τον υπολογιστή Server υπάρχει ένας εκτυπωτής της εταιρείας EPSON. Το μοντέλο του είναι το Epson AcuLaser C2900N, με σειριακό αριθμό ZX38201747 και το λογισμικό του είναι το firmware και δεν έχει αναβαθμιστεί από το 2003. Ο εκτυπωτής αυτός έχει IP την 192.168.1.4.

Επίσης, αυτό το υποδίκτυο συνδέεται με το παραπάνω router/firewall. Το router/firewall συνδέεται με ένα router, σε άλλο δωμάτιο, καθώς είναι κατασκευασμένο από την εταιρεία Cisco, και συγκεκριμένα είναι το μοντέλο Cisco 800M Series ISR. Τρέχει το λειτουργικό IOS 15.5 Basic IP, έχει IP διεύθυνση την 192.168.1.1 και σειριακό αριθμό τον SV23412385. Τέλος, το router αυτό συνδέεται με το Internet.

A2.1.4 Δεδομένα

Τα δεδομένα που είναι απαραίτητα για την κατασκευή του πληροφοριακού συστήματος του νοσοκομείου είναι τα παρακάτω:

- Εικόνα, όπου μπορεί να είναι οι ακτινογραφίες, οι αξονικές ή μαγνητικές.
- Ήχος, όπου μπορεί να είναι η ηχογράφηση των καρδιακών παλμών ενός ασθενή.
- Κείμενο, όπου μπορεί να είναι αποτελέσματα μικροβιολογικών, αιματολογικών, καρδιακών εξετάσεων ενός ασθενή, τα στοιχεία των ασθενών.
- Κωδικοί, όπου οι χρήστες του συστήματος τους χρησιμοποιούν για την πρόσβαση τους στο πληροφοριακό σύστημα.
- Email, όπου αποτελεί ένα μέσο επικοινωνίας μεταξύ των χρηστών του πληροφοριακού συστήματος.

A2.1.5 Διαδικασίες

Οι διαδικασίες αφορούν τις οδηγίες για τους εμπλεκόμενους στο σύστημα και διακρίνονται σε:

- **Διαδικασίες για χρήστες.** Για παράδειγμα διαδικασίες για τους υπαλλήλους, που αφορούν την εισαγωγή, την επεξεργασία των δεδομένων τους, την έκδοση της μισθοδοσίας ή οποιασδήποτε άλλης πληροφορίας.
- **Διαδικασίες για χειριστές.** Οι διαδικασίες αυτές αφορούν την δημιουργία αντιγράφων ασφαλείας που σχετίζονται με τα ευαίσθητα δεδομένα των ασθενών, την ανάκτηση δεδομένων από το πληροφοριακό σύστημα, τον υπολογισμό στατιστικών στοιχείων, την κατασκευή γραφημάτων για απεικόνιση αποτελεσμάτων και την εισαγωγή νέων ασθενών.

Α3. ΑΠΟΤΙΜΗΣΗ ΠΣ ΚΑΙ ΕΓΚΑΤΑΣΤΑΣΕΩΝ ΝΟΣΟΚΟΜΕΙΟΥ

Στην ενότητα αυτή, καθορίζονται τα αγαθά του πληροφοριακού συστήματος του νοσοκομείου, τα οποία μπορεί να είναι ευπαθή σε κάποια ενέργεια, επίθεση ή απειλή. Κάθε αγαθό διαθέτει και τη δική του ευπάθεια, η οποία μπορεί να το καθιστά αδύναμο και συνεπώς να οδηγήσει σε βλάβες του συστήματος. Επιπλέον, παρουσιάζεται η αποτίμηση των αποτελεσμάτων σύμφωνα με την απώλεια της εμπιστευτικότητας, της διαθεσιμότητας και της ακεραιότητας.

Α3.1 Αγαθά που εντοπίστηκαν

Ο όρος αγαθά αναφέρεται στις οντότητες και στα αντικείμενα που αξίζουν να προστατευθούν, δηλαδή τα δεδομένα ή οι πληροφορίες που διακινούνται και αποθηκεύονται στο πληροφοριακό σύστημα του νοσοκομείου.

Στα αγαθά ανήκουν, επιπλέον, και οι υπολογιστικοί πόροι, δηλαδή ο εξοπλισμός του νοσοκομείου.

Τα δεδομένα και οι πληροφορίες του συστήματος του νοσοκομείου είναι τα εξής:

- ***Patient Data:*** Τα ευαίσθητα ιατρικά δεδομένα των ασθενών όπως το ιατρικό ιστορικό τους, τα στοιχεία τους, τα ραντεβού τους, τα αποτελέσματα των εξετάσεων κλπ.
- ***Personnel Data:*** Τα δεδομένα των υπαλλήλων του νοσοκομείου όπως τα στοιχεία τους , τα ωράρια εργασίας, η διεργασία πληρωμής κλπ.

Όσον αφορά τους υπολογιστικούς πόρους του πληροφοριακού συστήματος του νοσοκομείου, υπάρχουν τα εξής αγαθά που πρέπει να προστατευθούν γιατί το καθένα προσφέρει και από μία υπηρεσία:

- ***Patient PC:*** Οι 3 HP υπολογιστές, με λειτουργικό Microsoft Windows XP, βρίσκονται αντίστοιχα σε 3 διαφορετικά Patient Room. Συγκεκριμένα, οι HP υπολογιστές αξίζουν να προστατευθούν γιατί χρησιμοποιούνται για την καταγραφή και επεξεργασία των ιατρικών - ευαίσθητων δεδομένων των ασθενών.
- ***Workstation:*** Οι 2 HP υπολογιστές, με λειτουργικό Microsoft Windows 7 Pro SP1, βρίσκονται στα δωμάτια που αφορούν τις εγγραφές (Registry Workstation). Αξίζουν να προστατευθούν γιατί σε αυτούς γίνεται η επεξεργασία των στοιχείων των υπαλλήλων. Ο HP υπολογιστής, με λειτουργικό Microsoft Windows 7 Pro SP1, βρίσκεται στη Γραμματεία αξίζει να προστατευθεί γιατί σε αυτόν ρυθμίζονται τα ραντεβού των ασθενών.

- ***Server:*** Οι 2 HP υπολογιστές server, με λειτουργικό Microsoft Windows 2012 Server SP1, βρίσκονται σε διαφορετικά δωμάτια και παίζουν καθοριστικό ρόλο στο πληροφοριακό σύστημα του νοσοκομείου, καθώς εκεί αποθηκεύονται όλα τα δεδομένα που αφορούν τους ασθενείς και τους υπαλλήλους.

A3.2 Απειλές που εντοπίστηκαν

Ο όρος επικινδυνότητα αναφέρεται και στις απειλές που ενδέχεται να αντιμετωπίσει το πληροφοριακό σύστημα του νοσοκομείου.

Με τον όρο απειλή ορίζεται η πιθανή εκμετάλλευση μιας ευπάθειας ή μιας αδυναμίας του συστήματος με κίνδυνο τη μη εξουσιοδοτημένη πρόσβαση, την αποκάλυψη των ευαίσθητων πληροφοριών των ασθενών, τη χρήση, την κλοπή ή την καταστροφή των πόρων του συστήματος αυτού. Για κάθε αγαθό εντοπίστηκαν αρκετές απειλές.

Αυτές είναι οι σημαντικότερες:

AMCRT002

Το router AMCRT002 λειτουργεί και σαν firewall για το δίκτυο του νοσοκομείου. Το λειτουργικό σύστημα που χρησιμοποιεί είναι το IOS 15.5 Advanced IP Services το οποίο είναι ευάλωτο σε απειλές τύπου IP Spoofing, DDOS, Buffer Overflow. Επίσης η IP διεύθυνση του router είναι η 192.168.1.2 την οποία διεύθυνση έχει και ο server. Άρα υπάρχει conflict λόγο λανθασμένων ρυθμίσεων που δεν επιτρέπει την πρόσβαση στο δίκτυο στο router και τον server. Σαν κύρια απειλή επιλέχθηκε το IP Spoofing , αφού μια τέτοια επίθεση μπορεί να καταστήσει τις υπηρεσίες του νοσοκομείου μη διαθέσιμες καθώς μπορεί να τροποποιήσει ευαίσθητα δεδομένα οδηγώντας σε απάτη. Πρόκειται για γνωστή απειλή και μπορεί να αντιμετωπιστεί. ***(Impact: 8)***

- *IP Spoofing:* Προσπάθεια απόκρυψης της ταυτότητας του επιτιθέμενου μέσω της δημιουργίας πακέτων με ψεύτικη διεύθυνση προέλευσης.
- *DDOS:* Επίθεση που έχει ως στόχο να καταστήσει το θύμα ανίκανο να δεχτεί άλλες συνδέσεις μέσω αποστολής υπεράριθμων πακέτων από αυτά που μπορεί να δεχτεί.
- *Buffer Overflow:* Ο επιτιθέμενος εισβάλει στο σύστημα χωρίς να χρειάζεται να κάνει login, μέσω ενός προγράμματος που ήδη τρέχει στον υπολογιστή του θύματος και του δίνει να εκτελέσει ένα κομμάτι εντολών.

Patient data

Τα δεδομένα των ασθενών μπορούν να υποπέσουν σε επιθέσεις οι οποίες μπορούν να κλέψουν τα ευαίσθητα αυτά προσωπικά δεδομένα. Επίσης μπορούν να τα τροποιήσουν ή ακόμα να τα διαγράψουν από το σύστημα. Σαν κύρια απειλή επιλέχθηκε το γεγονός ότι τα δεδομένα των ασθενών μπορούν να υποκλαπούν. Μια τέτοια απειλή μπορεί να καταστήσει δυνατή την αποκάλυψη ή και τροποποίηση των ευαίσθητων δεδομένων των ασθενών . Πρόκειται για απειλή που δεν είναι γνωστή. ***(Impact: 10)***

Workstation

Οι υπολογιστές που λειτουργούν σαν workstations τρέχουν λειτουργικό σύστημα Microsoft Windows 7 SP1 γεγονός που τα κάνει ευπαθή σε επιθέσεις τύπου DDOS, Code Execution, Gain Privileges. Ως κύρια απειλή επιλέχθηκε η επίθεση DDOS. Αυτή η απειλή μπορεί να καταστήσει αδύνατη την πραγματοποίηση ηλεκτρονικών συναλλαγών με αποτέλεσμα την

δυσφήμιση του νοσοκομείου και την αγανάκτηση των πελατών. Πρόκειται για απειλή που δεν είναι γνωστή. ***(Impact: 10)***

- *DDOS:* Επίθεση που έχει ως στόχο να καταστήσει το θύμα ανίκανο να δεχτεί άλλες συνδέσεις μέσω αποστολής υπεράριθμων πακέτων από αυτά που μπορεί να δεχτεί.
- *Code Execution*: Σε αυτόν τον τύπο επίθεσης ο επιτιθέμενος έχει την δυνατότητα να εκτελέσει κώδικα της επιλογής του στο σύστημα του θύματος.
- *Gain Privileges*: Επίθεση κατά της οποία ο κακόβουλος χρήστης αποκτά δικαιώματα τα οποία δεν θα έπρεπε να διαθέτει άρα και πρόσβαση σε ευαίσθητα αρχεία και δεδομένα.

Patient PC

Οι υπολογιστές που λειτουργούν σαν patient pc τρέχουν λειτουργικό σύστημα Microsoft Windows XP γεγονός που τα κάνει ευπαθή σε επιθέσεις τύπου Code Execution, Gain Privileges, Buffer Overflow. Ως κύρια απειλή επιλέχθηκε το Code Execution. Μια τέτοια απειλή καθιστά τα δεδομένα μη διαθέσιμα καθώς δίνει τη δυνατότητα τροποποίησης και διαγραφής των ιατρικών ευαίσθητων δεδομένων. Η απειλή αυτή είναι γνωστή και μπορεί να ελεγχθεί. ***(Impact: 8)***

- *Code Execution*: Σε αυτόν τον τύπο επίθεσης ο επιτιθέμενος έχει την δυνατότητα να εκτελέσει κώδικα της επιλογής του στο σύστημα του θύματος.
- *Gain Privileges*: Επίθεση κατά της οποία ο κακόβουλος χρήστης αποκτά δικαιώματα τα οποία δεν θα έπρεπε να διαθέτει άρα και πρόσβαση σε ευαίσθητα αρχεία και δεδομένα.
- *Buffer Overflow*: Ο επιτιθέμενος εισβάλει στο συστήματα χωρίς να χρειάζεται να κάνει login, μέσω ενός προγράμματος που ήδη τρέχει στον υπολογιστή του θύματος και του δίνει να εκτελέσει ένα κομμάτι εντολών.

Server

Το νοσοκομείο διαθέτει δύο υπολογιστές που λειτουργούν σαν servers. Οι servers αυτοί τρέχουν Microsoft Windows 2012 Server SP1. Εντοπίσαμε ip conflict στο δίκτυο του νοσοκομείου μια και το router/firewall AMCRT002 έχει την ίδια ip me τον server AMCSRV001 192.168.1.2 άρα ο server δεν έχει πρόσβαση στο δίκτυο. Επίσης το λειτουργικό που τρέχουν οι server δεν έχει ενημερωθεί γεγονός που τα κάνει ευπαθή σε επιθέσεις Gain Privileges, Code Execution. Ως κύρια απειλή επιλέχθηκε η απόκτηση δικαιωμάτων (Gain Privileges). Μια τέτοια απειλή καθιστά τα δεδομένα μη διαθέσιμα αφού επιτρέπει την υποκλοπή ιατρικών ευαίσθητων πληροφοριών και την ανταλλαγή η μεταφορά τους. Πρόκειται για γνωστή απειλή που μπορεί να ελεγχθεί. ***(Impact: 8)***

- *Gain Privileges*: Επίθεση κατά της οποία ο κακόβουλος χρήστης αποκτά δικαιώματα τα οποία δεν θα έπρεπε να διαθέτει άρα και πρόσβαση σε ευαίσθητα αρχεία και δεδομένα.
- *Code Execution*: Σε αυτόν τον τύπο επίθεσης ο επιτιθέμενος έχει την δυνατότητα να εκτελέσει κώδικα της επιλογής του στο σύστημα του θύματος.

Printers

Υπάρχουν δυο εκτυπωτές στο δίκτυο όπου ο καθένας είναι συνδεδεμένος στον αντίστοιχο server. Το firmware των εκτυπωτών έχει να ενημερωθεί από το 2003 γεγονός που το κάνει εύκολο στόχο για κακόβουλες επιθέσεις που δίνουν την δυνατότητα στον επιτιθέμενο να έχει πρόσβαση στο δίκτυο του νοσοκομείου. Ως κύρια απειλή επιλέχθηκε η επίθεση κατά την οποία ο κακόβουλος χρήστης αποκτά πρόσβαση στο σύστημα. Αυτή η απειλή δίνει τη

δυνατότητα πρόσβασης σε όλο το πληροφοριακό σύστημα. Οι εκτυπωτές είναι διαθέσιμοι για χρήση αλλά παραβιάζεται η πολιτική του νοσοκομείου. ***(Impact: 7)***

Network Switch

Το δίκτυο του νοσοκομείου διαθέτει δυο switch τα οποία δημιουργούν δυο υποδίκτυα. Το λειτουργικό αυτών των switch είναι το IOS 12.4 Basic IP του οποίου η υποστήριξη και τα patches σταμάτησαν το 2016 γεγονός που το κάνει ευπαθές σε επιθέσεις. Κάποιες από αυτές είναι DDOS, Code Execution, Buffer Overflow. Ως κύρια απειλή επιλέχθηκε η DDOS επίθεση. Μια τέτοια επίθεση καθιστά αδύνατη την επικοινωνία μεταξύ του server και των υπολογιστικών πόρων. Έτσι το πρόβλημα είναι γνωστό αλλά δεν μπορεί να αντιμετωπιστεί. ***(Impact: 9)***

- *DDOS:* Επίθεση που έχει ως στόχο να καταστήσει το θύμα ανίκανο να δεχτεί άλλες συνδέσεις μέσω αποστολής υπεράριθμων πακέτων από αυτά που μπορεί να δεχτεί.
- *Code Execution*: Σε αυτόν τον τύπο επίθεσης ο επιτιθέμενος έχει την δυνατότητα να εκτελέσει κώδικα της επιλογής του στο σύστημα του θύματος.
- *Buffer Overflow*:. Ο επιτιθέμενος εισβάλει στο σύστημα χωρίς να χρειάζεται να κάνει login, μέσω ενός προγράμματος που ήδη τρέχει στον υπολογιστή του θύματος και του δίνει να εκτελέσει ένα κομμάτι εντολών.

AMCRT001

Το δίκτυο του νοσοκομείου διαθέτει ένα router μέσω του οποίου συνδέεται στο διαδίκτυο. Το λειτουργικό που τρέχει είναι το IOS 15.5 Basic IP. Το λειτουργικό αυτό δεν έχει ενημερωθεί γεγονός που κάνει το router ευάλωτο σε επιθέσεις τύπου DDOS, Buffer Overflow, Code Execution. Ως κύρια απειλή επιλέχθηκε η Gain privileges. Μια τέτοια απειλή μπορεί να καταστήσει τη συσκευή μη διαθέσιμη και να αποκόψει το δίκτυο του νοσοκομείου από το διαδίκτυο. Το πρόβλημα είναι γνωστό και μπορεί να ελεγχθεί. ***(Impact: 8)***

- *DDOS:* Επίθεση που έχει ως στόχο να καταστήσει το θύμα ανίκανο να δεχτεί άλλες συνδέσεις μέσω αποστολής υπεράριθμων πακέτων από αυτά που μπορεί να δεχτεί.
- *Buffer Overflow*: Ο επιτιθέμενος εισβάλει στο σύστημα χωρίς να χρειάζεται να κάνει login, μέσω ενός προγράμματος που ήδη τρέχει στον υπολογιστή του θύματος και του δίνει να εκτελέσει ένα κομμάτι εντολών.
- *Code Execution*: Σε αυτόν τον τύπο επίθεσης ο επιτιθέμενος έχει την δυνατότητα να εκτελέσει κώδικα της επιλογής του στο σύστημα του θύματος.

Employee Data

Τα δεδομένα των υπαλλήλων μπορούν να υποπέσουν σε επιθέσεις οι οποίες μπορούν να κλέψουν τα ευαίσθητα αυτά προσωπικά δεδομένα. Επίσης μπορούν να τα τροποιήσουν ή ακόμα να τα διαγράψουν από το σύστημα. Ως κύρια απειλή επιλέχθηκε η επίθεση κατά την οποία ο κακόβουλος χρήστης αποκτά πρόσβαση στα δεδομένα των υπαλλήλων του συστήματος καθιστώντας τα μη διαθέσιμα αφού μπορεί να έχουν τροποποιηθεί η διαγραφεί. Το πρόβλημα είναι γνωστό αλλά δεν μπορεί να ελεγχθεί. ***(Impact: 9)***

Windows XP

Είναι ένα παλαιό πλέον λειτουργικό σύστημα για το οποίο η υποστήριξη έχει σταματήσει γεγονός που το κάνει ευπαθές σε επιθέσεις. Κύρια απειλή σε αυτή την περίπτωση αποτελούν οι ιοί και τα κακόβουλα λογισμικά γενικά που καθιστούν τον υπολογιστή μη ασφαλή. Το πρόβλημα είναι γνωστό αλλά δεν μπορεί να ελεγχθεί. ***(Impact: 9)***

Windows 7 Pro SP1
Οι υπολογιστές που διαθέτουν Windows 7 Pro SP1 δεν έχουν κάνει τις τελευταίες ενημερώσεις γεγονός που τους καθιστά ευπαθείς σε επιθέσεις. Ως κύρια απειλή επιλέχθηκε η Gain Privileges. Μια τέτοια απειλή καθιστά δυνατή την απόκτηση πληροφοριών από τον κακόβουλο χρήστη. Ο υπολογιστής είναι διαθέσιμος αλλά έχουν παραβιαστεί οι διαδικασίες του. ***(Impact: 6)***

Oracle Database
Οι server του νοσοκομείου για να αποθηκεύουν τα δεδομένα που χρειάζεται το πληροφοριακό σύστημα του νοσοκομείου χρησιμοποιούν από μια Oracle Database ο καθένας. Οι βάσεις αυτές όμως δεν είναι κρυπτογραφημένες γεγονός που τις κάνει ευπαθής σε επιθέσεις. Επίσης δεν υπάρχει back up database σε περίπτωση καταστροφής της βάσης δεδομένων. Η κύρια απειλή για την βάση δεδομένων είναι η καταστροφή της που συνεπάγεται διαγραφή των ιατρικών δεδομένων (μη διαθέσιμη). Η απειλή είναι γνωστή και δεν μπορεί να αντιμετωπιστεί. ***(Impact: 8)***

Payment Process
Το νοσοκομείο χρησιμοποιεί αυτή την διαδικασία για να οριστικοποιήσει τις πληρωμές του προσωπικού. Η διαδικασία όμως αυτή είναι ευάλωτη διότι τρέχει στα Workstation PC τα οποία διαθέτουν για λειτουργικό σύστημα Windows 7 Pro SP1 χωρίς τις τελευταίες ενημερώσεις. Ως κύρια απειλή επιλέχθηκε η Gain Privileges. Αυτή η απειλή μπορεί να οδηγήσει σε διαγραφή των πληρωμών ή και υποκλοπή του IBAN. Διάφορες πληρωμές μπορούν να πραγματοποιηθούν αλλά παραβιάζονται οι πολιτικές συναλλαγής του νοσοκομείου. ***(Impact: 7)***

New Patient Register Process
Το νοσοκομείο χρησιμοποιεί αυτή την διαδικασία για να προσθέσει νέους ασθενείς στο σύστημα του αλλά και για να ενημερώνει το ιστορικό ασθενείας των υπάρχων ασθενών. Η διαδικασία όμως αυτή είναι ευάλωτη διότι τρέχει και στα Patient PC τα οποία διαθέτουν για λειτουργικό σύστημα Windows XP. Κυριότερη απειλή είναι απόκτηση πληροφοριών κατά την οποία μπορεί να υποκλαπούν ή διαγραφούν στοιχεία των ασθενών. Έτσι τα δεδομένα των ασθενών δεν είναι διαθέσιμα. Η απειλή είναι γνωστή αλλά δεν μπορεί να αντιμετωπιστεί. ***(Impact: 9)***

Hospital Website
Η ιστοσελίδα του νοσοκομείου υποστηρίζεται από το πρόγραμμα JOOMLA το οποίο έχεις γνωστές ευπάθειες όπως Code execution, SQL Injection, XSS. Ως κύρια απειλή επιλέχθηκε το Code Execution γιατί έτσι ο κακόβουλος χρήστης μπορεί να αποκτήσει πρόσβαση στο μηχάνημα και στη συνέχεια στα στοιχεία των υπαλλήλων. Το μηχάνημα μπορεί να σταματήσει να είναι διαθέσιμο. Πρόκειται για μια γνωστή απειλή που μπορεί να διορθωθεί. ***(Impact: 8)***

UPS
Το ρεύμα που παρέχεται στους Server περνά μέσα από UPS έτσι ώστε να διασφαλίζεται η σωστή λειτουργεία τους. Τα UPS όμως είναι ευπαθή σε φυσικές καταστροφές όπως πυρκαγιά ή πλημμύρα. Ως κύρια απειλή επιλέχθηκε η καταστροφή του όπου οδηγεί στη διακοπή της λειτουργίας του server και στην απώλεια των δεδομένων του. Είναι μια γνωστή απειλή που δεν μπορεί να αντιμετωπιστεί. ***(Impact: 9)***

Software Queue Management System

Μέσω αυτής της διεργασίας η Γραμματεία του νοσοκομείου διαμορφώνει τα ραντεβού των ασθενών. Η διαδικασία όμως αυτή είναι ευάλωτη διότι τρέχει στο Secretary PC το οποίο διαθέτει λειτουργικό σύστημα Windows 7 Pro SP1 χωρίς τις τελευταίες ενημερώσεις. Κυριότερη απειλή είναι η gain access διότι ο κακόβουλος χρήστης μπορεί να τροποποιήσει την ουρά προτεραιότητας παραβιάζοντας τους κανονισμούς της διαδικασίας. ***(Impact: 5)***

Human error
Ο ανθρώπινος παράγοντας αποτελεί απειλή για το πληροφοριακό σύστημα του νοσοκομείου μιας και υπάρχει περίπτωση οι χρήστες του συστήματος άθελα τους να δώσουν απόρρητες πληροφορίες. Πληροφορίες οι οποίες μπορούν να οδηγήσουν σε διείσδυση κακόβουλων χρηστών στο σύστημα του νοσοκομείου. Έτσι οι πληροφορίες μπορεί να πάψουν να είναι διαθέσιμες. Πρόκειται για ένα γνωστό πρόβλημα το οποίο μπορεί να αντιμετωπιστεί. ***(Impact: 8)***

A3.3 Ευπάθειες που εντοπίστηκαν

Οι ευπάθειες ενός πληροφοριακού συστήματος αφορούν τις αδυναμίες στη διαχείριση και στις ρυθμίσεις του συστήματος ή τα αδύναμα σημεία στο υποσύστημα της ασφάλειας.

Σύμφωνα με το σχέδιο του πληροφοριακού συστήματος του νοσοκομείου, έχουν εντοπιστεί οι εξής ευπάθειες:

AMCRT002
Το router AMCRT002 λειτουργεί σαν firewall για το δίκτυο του νοσοκομείου και έχει σαν στόχο να μπλοκάρει τα μη εξουσιοδοτημένα πακέτα και αιτήματα. Η ευπάθεια που εντοπίστηκε στο router είναι οι λάθος επιλογές στις ρυθμίσεις του που επιτρέπουν επιθέσεις της μορφής IP Spoofing. Επιπλέον το firewall έχει ίδια IP διεύθυνση με τον ένα server. Σύμφωνα με το αρχείο Asset Inventory και συγκεκριμένα με το Inventory ID φαίνεται να τοποθετήθηκε πρώτα ο server. Συνεπώς, η IP διεύθυνση του firewall θα πρέπει να αλλάξει και να πάρει μία διαφορετική IP (random), η οποία δεν χρησιμοποιείται από κάποιο άλλο αγαθό του πληροφοριακού συστήματος. Η ευπάθεια του firewall είναι μεσαίας επικινδυνότητας και εφαρμόζοντας μέτρα όπως η σωστή ρύθμιση της συσκευής μειώνεται περαιτέρω η επικινδυνότητα. ***(Vulnerability: 5)***

Patient data
Τα ευαίσθητα δεδομένα των ασθενών αποθηκεύονται στον server. Εντοπίστηκε ότι η βάση δεδομένων δεν είναι κρυπτογραφημένη γεγονός πού κάνει τα δεδομένα ευπαθή σε επιθέσεις που έχουν ως στόχο την υποκλοπή, τροποποίηση ή διαγραφή τους. Η ευπάθεια αυτή αποτελεί σοβαρό ζήτημα για την ασφάλεια του συστήματος. Μέτρα αντιμετώπισης της ευπάθειας έχουν σχεδιαστεί , όπως η κωδικοποίηση των δεδομένων της βάσης, αλλά δεν έχουν υλοποιηθεί ακόμα. ***(Vulnerability: 7)***

Workstation
Το νοσοκομείο διαθέτει 3 υπολογιστές που λειτουργούν σαν Workstations και τρέχουν λειτουργικό Windows 7 Pro SP1. Το λειτουργικό όμως αυτό δεν έχει κάνει τις τελευταίες ενημερώσεις εδώ και 6 μήνες γεγονός που αποτελεί ευπάθεια για την ασφάλεια του συστήματος. Η ευπάθεια αυτή αποτελεί ζήτημα μικρής ανησυχίας μιας και έχουν εφαρμοστεί άλλα μέτρα ασφαλείας, όπως το firewall ή αντιικά προγράμματα, τα οποία είναι αποτελεσματικά. ***(Vulnerability: 2)***

Patient PC

Οι υπολογιστές που λειτουργούν σαν patient pc τρέχουν λειτουργικό σύστημα Microsoft Windows XP ένα παλιό λειτουργικό σύστημα το οποίο πλέον δεν έχει υποστήριξη και ενημερώσεις από τον Απρίλιο του 2014. Η ευπάθεια αυτή αποτελεί ζήτημα μικρής ανησυχίας μιας και έχουν εφαρμοστεί άλλα μέτρα ασφαλείας, όπως το firewall ή αντιικά προγράμματα, τα οποία είναι αποτελεσματικά αλλά χρειάζονται και περαιτέρω μέτρα λόγο της παλαιότητας του λειτουργικού. ***(Vulnerability: 4)***

Server

Το νοσοκομείο διαθέτει δύο υπολογιστές που λειτουργούν σαν servers .Οι servers αυτοί τρέχουν Microsoft Windows 2012 Server SP1 και λειτουργούν σαν βάσεις δεδομένων για τα στοιχεία των ασθενών και των υπαλλήλων. Εντοπίστηκε ότι δεν έχουν γίνει οι νεότερες ενημερώσεις στο λειτουργικό σύστημα αλλά επίσης υπάρχει σύγκρουση στο δίκτυο μιας και έχει δοθεί η ίδια IP στον Server AMCSRV001 και στο router AMCRT002. Η ευπάθεια αυτή θεωρείται μεσαίας επικινδυνότητας και έχουν εφαρμοστεί κάποια μέτρα αντιμετώπισης που είναι αρκετά αποτελεσματικά όπως το firewall. ***(Vulnerability: 6)***

Printers

Το νοσοκομείο διαθέτει δύο εκτυπωτές των οποίων τα firmware ενημερώθηκαν τελευταία φορά το 2003. Γεγονός που κάνει τις συσκευές δεκτικές σε κακόβουλες επιθέσεις που μπορούν να έχουν σαν αποτέλεσμα την είσοδο κακόβουλων χρηστών στο δίκτυο. Η ευπάθεια αυτή θεωρείται μεσαίας επικινδυνότητας μιας και έχουν εφαρμοστεί κάποια μέτρα αντιμετώπισης που είναι αρκετά αποτελεσματικά όπως το firewall. ***(Vulnerability: 5)***

Network Switch

Το νοσοκομείο διαθέτει δυο switch. Το λειτουργικό αυτών των switch είναι το IOS 12.4 Basic IP του οποίου η υποστήριξη και τα patches σταμάτησαν το 2016. Το γεγονός αυτό δημιουργεί κενά στην ασφάλεια των συσκευών και τις κάνει ευπαθείς σε επιθέσεις. Η ευπάθεια αυτή είναι μεγάλης επικινδυνότητας μιας και επιθέσεις στα switch μπορούν να διακόψουν την λειτουργεία του δικτύου. Μέτρα για την αντιμετώπιση της ευπάθειας έχουν σχεδιαστεί, όπως η εγκατάσταση firewall και μπροστά από τα switch για να φιλτράρεται η κίνηση των δεδομένων, αλλά ακόμα δεν έχουν υλοποιηθεί. **(*Vulnerability: 7*)**

AMCRT001

Το δίκτυο του νοσοκομείου διαθέτει ένα router μέσω του οποίου συνδέεται στο διαδίκτυο. Το λειτουργικό που τρέχει είναι το IOS 15.5 Basic IP. Οι τελευταίες ενημερώσεις δεν έχουν πραγματοποιηθεί σε αυτή την συσκευή πράγμα που την καθιστά ευάλωτη σε επιθέσεις. Η ευπάθεια αυτή είναι μεγάλης επικινδυνότητας μίας και κακόβουλοι χρήστες μπορούν να αποκτήσουν πρόσβαση δίκτυο και στην συνέχεια να αποκτήσουν δικαιώματα και δυνατότητα υποκλοπής ευαίσθητων προσωπικών δεδομένων. Έχουν σχεδιαστεί μέτρα αντιμετώπισης αυτής της ευπάθειας αλλά δεν έχουν υλοποιηθεί ακόμα. **(*Vulnerability: 8)***

Employee Data

Τα δεδομένα των υπαλλήλων αφορούν ευαίσθητα στοιχεία όπως στοιχεία ταυτότητας, πληρωμές κλπ. Εντοπίστηκε ότι η βάση δεδομένων όπου φυλάσσονται αυτά τα δεδομένα δεν είναι κρυπτογραφημένη γεγονός που την κάνει ευπαθή σε υποκλοπές. Η ευπάθεια αυτή είναι μεγάλης επικινδυνότητας μιας και η υποκλοπή ευαίσθητων στοιχείων θα ήταν καταστροφική για το νοσοκομείο. Μέτρα αντιμετώπισης έχουν σχεδιαστεί, όπως η κρυπτογράφηση της βάσης δεδομένων, αλλά ακόμα δεν έχουν υλοποιηθεί. ***(Vulnerability: 8)***

Windows XP

Η υποστήριξη έχει σταματήσει για το λειτουργικό σύστημα Windows XP γεγονός που τα κάνει ευπαθή σε έναν μεγάλο όγκο επιθέσεων. Για το σύστημα του νοσοκομείου αυτό το γεγονός αποτελεί μια ευπάθεια μεγάλης επικινδυνότητας μιας και πολλά ευαίσθητα δεδομένα περνάνε μέσα από υπολογιστές που τρέχουν αυτό το λειτουργικό. Μέτρα έχουν σχεδιαστεί, όπως η αναβάθμιση του λειτουργικού σε νεότερη έκδοση, όμως ακόμα δεν έχουν υλοποιηθεί. ***(Vulnerability: 8)***

Windows 7 Pro SP1
Το νοσοκομείο διαθέτει υπολογιστές που τρέχουν Windows 7 Pro SP1 όμως δεν έχουν γίνει οι τελευταίες ενημερώσεις. Η ευπάθεια αυτή είναι μέτριας επικινδυνότητας άλλα έχουν υλοποιηθεί άλλα μέτρα για την αντιμετώπιση των απειλών, όπως αντιικά προγράμματα, που είναι αρκετά αποτελεσματικά. ***(Vulnerability: 6)***

Oracle Database
Τα δεδομένα που κινούνται μέσα στο νοσοκομείο αποθηκεύονται σε βάσεις δεδομένων Oracle Database. Η ευπάθεια που εντοπίστηκε είναι ότι δεν υπάρχουν backup βάσεις γεγονός που σε περίπτωση απώλειας της κύριας βάσης οδηγεί σε ολική καταστροφή. Η ευπάθεια αυτή είναι υψηλής επικινδυνότητας αλλά μέτρα έχουν σχεδιαστεί μα ακόμα δεν έχουν υλοποιηθεί ακόμα. ***(Vulnerability: 7)***

Payment Process
Το νοσοκομείο χρησιμοποιεί αυτή την διαδικασία για να οριστικοποιήσει τις πληρωμές του προσωπικού. Η διαδικασία όμως αυτή τρέχει στα Workstation PC τα οποία δεν έχουν ενημερωθεί. Η ευπάθεια αυτή είναι μέτριας επικινδυνότητας αλλά μέτρα έχουν παρθεί και είναι αρκετά αποτελεσματικά. ***(Vulnerability: 5)***

New Patient Register Process
Το νοσοκομείο χρησιμοποιεί αυτή την διαδικασία για να προσθέσει νέους ασθενείς στο σύστημα του αλλά και για να ενημερώνει το ιστορικό ασθενείας των υπάρχων ασθενών. Η διαδικασία όμως αυτή τρέχει στα Patient PC τα οποία τρέχουν παλαιό λειτουργικό σύστημα. Η ευπάθεια αυτή είναι μέτριας επικινδυνότητας αλλά μέτρα έχουν παρθεί και είναι αρκετά αποτελεσματικά. ***(Vulnerability: 5)***

Hospital Website
Η ιστοσελίδα του νοσοκομείου υποστηρίζεται από το πρόγραμμα JOOMLA το οποίο είναι open source και οι ευπάθειες του είναι γνωστές. Επίσης ο host της σελίδας είναι ο server AMCSRV002 ο ίδιος server που περιέχει τα δεδομένα των υπαλλήλων του νοσοκομείου. Άρα μια επίθεση στην ιστοσελίδα του νοσοκομείου μπορεί αρκετά εύκολα να δώσει πρόσβαση στα ευαίσθητα δεδομένα των υπαλλήλων. Η ευπάθεια αυτή είναι μεγάλης επικινδυνότητας αλλά έχουν σχεδιαστεί μέτρα αντιμετώπισης, όπως ή μεταφορά της ιστοσελίδα σε ένα άλλο μηχάνημα (dedicated server), αλλά δεν έχουν υλοποιηθεί ακόμα. ***(Vulnerability: 8)***

UPS
Το ρεύμα που παρέχεται στους Server περνά μέσα από UPS έτσι ώστε να διασφαλίζεται η σωστή λειτουργεία τους. Υπάρχει όμως η περίπτωση οι μπαταρίες του UPS να εξασθενίσουν και σε μία διακοπή του ρεύματος μπορεί να οδηγήσει σε διακοπή λειτουργίας του server και σε απώλεια δεδομένων. Η ευπάθεια αυτή είναι μεγάλης επικινδυνότητας αλλά έχουν σχεδιαστεί μέτρα αντιμετώπισης, όπως ή τακτική επίβλεψη των μηχανημάτων ανά δυο μήνες, αλλά δεν έχουν υλοποιηθεί ακόμα. ***(Vulnerability: 8)***

Software Queue Management System
Μέσω αυτής της διεργασίας η γραμματεία του νοσοκομείου διαμορφώνει τα ραντεβού των ασθενών. Η διαδικασία όμως αυτή τρέχει σε υπολογιστή με Windows 7 Pro SP1 που δεν έχει λάβει τις τελευταίες ενημερώσεις. Η ευπάθεια αυτή είναι μέτριας επικινδυνότητας άλλα έχουν υλοποιηθεί άλλα μέτρα για την αντιμετώπιση των απειλών, όπως αντιικά προγράμματα, που είναι αρκετά αποτελεσματικά. ***(Vulnerability: 5)***

Human error
Ο ανθρώπινος παράγοντας αποτελεί απειλή για το πληροφοριακό σύστημα του νοσοκομείου μιας και υπάρχει περίπτωση οι χρήστες του συστήματος άθελα τους να δώσουν απόρρητες πληροφορίες. Η ευπάθεια αυτή είναι μέτριας επικινδυνότητας άλλα έχουν υλοποιηθεί άλλα μέτρα για την αντιμετώπιση των απειλών, όπως ερωτήσεις ασφαλείας πέρα από το username και το password, που είναι αρκετά αποτελεσματικά. ***(Vulnerability: 6)***

Α3.4 Αποτελέσματα αποτίμησης

Στην εργασία παρουσιάζονται όλα τα αγαθά του πληροφοριακού συστήματος του νοσοκομείου και ο βαθμός επικινδυνότητας τους, καθώς είναι διαφορετικός σε κάθε αγαθό. Στον παρακάτω πίνακα γίνεται η αποτίμηση των αγαθών, όταν υπάρχει απώλεια της διαθεσιμότητας, της ακεραιότητας ή λάθη κατά την τηλεπικοινωνιακή μετάδοση.

Η *απώλεια διαθεσιμότητας* αναφέρεται στην απώλεια ενός κρίσιμου αγαθού του συστήματος του νοσοκομείου, η οποία μπορεί να προκαλέσει διαταραχές στην οργάνωση του νοσοκομείου. Η *απώλεια ακεραιότητας* αναφέρεται στην απώλεια των δεδομένων και των πληροφοριών. Οι μη εξουσιοδοτημένοι χρήστες παίζουν ουσιαστικό ρόλο στην διαταραχή της ακεραιότητας. Τα *λάθη που γίνονται κατά την τηλεπικοινωνιακή μετάδοση* μπορούν να πραγματοποιηθούν μέσω της πρόσβασης των μη εξουσιοδοτημένων χρηστών στο πληροφοριακό σύστημα του νοσοκομείου και να επιφέρουν βλάβες τόσο στο σύστημα όσο και γενικότερα στο νοσοκομείο.

Στο νοσοκομείο υπάρχουν αγαθά τα οποία είναι πάρα πολύ σημαντικά για τη λειτουργία του που αξίζουν να προστατευθούν, όπως για παράδειγμα τα ιατρικά ευαίσθητα δεδομένα των ασθενών και οι υπολογιστές Servers που διαχειρίζονται αυτά τα δεδομένα, η ιστοσελίδα του νοσοκομείου. Τα Windows XP είναι ένα αγαθό που πρέπει να αντικατασταθεί, καθώς η Microsoft έχει σταματήσει την υποστήριξη της και δεν υπάρχουν πλέον ενημερώσεις και patches. Στους υπολογιστές που χρησιμοποιούν τα Windows XP, πρέπει να εγκατασταθεί άλλο λειτουργικό. Με αυτόν τον τρόπο, δεν θα τους καθιστά ευάλωτους σε κινδύνους ασφαλείας και ιούς. Επιπλέον, η ιστοσελίδα του νοσοκομείου είναι open source και η πιθανότητα απώλειας δεδομένων είναι αυξημένη. Τέλος, η πιθανότητα να γίνει κάποιο ανθρώπινο λάθος είναι και αυτή αυξημένη, καθώς η απώλεια της διαθεσιμότητας, της ακεραιότητας, η αποκάλυψη και η τροποποίηση των δεδομένων μπορούν να γίνουν είτε σκόπιμα είτε τυχαία.

	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	Λάθη μεγάλης	Εσωτερικούς	Παρόχους Υπηρεσιών	Εξωτερικούς	Επανάληψη	Αποποίηση	Αποποίηση	Άρνηση αποστολής /παρεμβολή	Λανθασμένη δρομολόγηση	Παρακολούθηση	Μη παράδοση	Άπιστος- ακολου- θίας
Router/Firewall					1	2		4	3	4	3	5	2	2	3	4	4	4	4	4	5	4	5	5
Patient Data	1	2	3	4	5	7	8	9	7	8	7	8	6	7	8	7	7	7	7	8	9	7	7	7
Workstation					1	2		4	4	5	2	4	3	4	5	2	2	2	3	3	4	4	5	4
Patient PC		1	2	3	4	5		7	6	7	5	8	5	8	7	5	5	5	4	6	6	5	5	4
Server		1	2	3	5	6	8	9	6	8	5	8	6	7	8	7	7	7	7	8	8	6	7	6
Printer					1	2		3	2	3	3	5	2	3	5	3	3	3	3	3	4	3	4	4
Network Switch		1	2	3	5	7		7	3	3	3	4	2	5	5	4	4	4	4	3	5	5	6	5
Router					1	2		4	3	4	3	4	2	4	4	3	3	3	3	3	5	4	6	5
Employee Data		1	2	3	4	6		7	6	7	5	7	6	6	7	6	6	6	6	7	6	5	6	6
Windows XP	1	2	3	4	5	6	7	9	7	8	8	9	6	9	8	7	7	7	7	7	9	7	5	6
Windows 7 Pro SP1					1	2		4	3	4	4	5	2	3	5	2	2	2	2	3	5	4	5	3
Oracle Database					1	2		3	3	4	5	6	3	3	4	3	3	3	3	3	4	4	3	3
Payment Process					1	2	3	4	2	3	3	4	2	3	4	2	2	2	2	3	4	4	4	4
New Patient Register Process						1	2	3	1	2	3	4	2	3	3	3	3	3	3	3	4	4	2	2
Hospital Website		1	2	4	5	6		8	7	8	6	8	5	8	7	7	7	7	7	8	8	8	7	6
UPS					1	2		3	1	2	2	3	2	2	2	2	2	2	2	2	3	3	2	2
Software Queue Mana				1	2	3		5	3	4	4	6	3	4	5	3	3	3	3	3	3	3	3	3

gement System																									
Human Error	1	2	3	4	5	6	7	8	6	7	6	7	7	6	7	8	8	8	8	8	7	6	7	7	

B2. ΠΡΟΤΕΙΝΟΜΕΝΑ ΜΕΤΡΑ ΑΣΦΑΛΕΙΑΣ

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

A1. Προσωπικό – Προστασία Διαδικασιών Προσωπικού

A2. Ταυτοποίηση και αυθεντικοποίηση

A3. Έλεγχος προσπέλασης και χρήσης πόρων

A4. Διαχείριση εμπιστευτικών δεδομένων

A5. Προστασία από τη χρήση υπηρεσιών από τρίτους

A6. Προστασία λογισμικού

A7. Διαχείριση ασφάλειας δικτύου

A8. Προστασία από ιομορφικό λογισμικό

A9. Ασφαλής χρήση διαδικτυακών υπηρεσιών

A10. Ασφάλεια εξοπλισμού

A11. Φυσική ασφάλεια κτιριακής εγκατάστασης

Τα μέτρα έχουν εφαρμογή στο ΠΣ του **myHospital_Care**.

A1 ***Προσωπικό – Προστασία Διαδικασιών Προσωπικού***

Το πληροφοριακό σύστημα του νοσοκομείου παρουσιάζει αρκετές απειλές ως προς το προσωπικό και την προστασία διαδικασιών του προσωπικού ή των χρηστών του νοσοκομείου. Η ασφάλεια των δεδομένων βασίζεται στην ακεραιότητά τους και στην εμπιστευτικότητά τους και συνεπώς θα ήταν σημαντικό να υπάρχουν τα αντίστοιχα μέτρα αντιμετώπισης. Το προσωπικό βρίσκεται στη θέση να καταγράφουν και να επεξεργάζονται τα προσωπικά και ευαίσθητα δεδομένα των ασθενών. Ως προς τις διαδικασίες του προσωπικού υπάρχουν τα εξής μέτρα αντιμετώπισης:

1. Ενημέρωση των χρηστών για τον ορθό τρόπο λειτουργίας του συστήματος.
2. Ενημέρωση των χρηστών για οποιαδήποτε αλλαγή μέτρων ασφάλειας του συστήματος.
3. Ενημέρωση των χρηστών για τις έννοιες της ασφάλειας, όπως για παράδειγμα τις έννοιές της εμπιστευτικότητας, ακεραιότητας, διαθεσιμότητας με σκοπό να προστατέψουν τα ευαίσθητα δεδομένα των ασθενών.
4. Σωστή χρήση των αποθηκευτικών μέσων.

5. Παρακολούθηση σεμιναρίων για την ενημέρωση τους ως προς τα νέα προϊόντα ασφάλειας.
6. Σωστή διαχείριση περιστατικών παραβίασης προσωπικών δεδομένων των υπαλλήλων και των ασθενών.
7. Ύπαρξη ενός web portal για την περιγραφή των μέτρων ασφαλείας του νοσοκομείου.
8. Εξειδικευμένη εκπαίδευση στους χρήστες - υπαλλήλους που είναι αρμόδιοι στον τομέα της ασφάλειας του πληροφοριακού συστήματος του νοσοκομείου.
9. Παρακολούθηση σεμιναρίων και εκπαίδευση προσωπικού για την πιστοποίηση ως προς τη διαχείριση της ασφάλειας.
10. Ο σωστός τρόπος αποθήκευσης των προσωπικών - ευαίσθητων δεδομένων και η ύπαρξη αντιγράφων με back up είναι αναγκαία, διότι θα αποφεύγονται λάθη των χρηστών και θα προστατεύονται τα δεδομένα.

A2 *Ταυτοποίηση και αυθεντικοποίηση*

Η ταυτοποίηση και η αυθεντικοποίηση των χρηστών είναι πολύ σημαντική για την εμπιστευτικότητα του πληροφοριακού συστήματος του νοσοκομείου. Τα μέτρα αντιμετώπισης που αφορούν την ταυτοποίηση και την αυθεντικοποίηση είναι τα εξής:

1. Ύπαρξη διαφορετικού λογαριασμού, με διαφορετικό username και password για κάθε χρήστη του πληροφοριακού συστήματος.
2. Τα συνθηματικά, όπως για παράδειγμα, το username και password θα πρέπει να έχουν συγκεκριμένο μήκος και να περιέχουν πολλούς διαφορετικούς χαρακτήρες πχ θαυμαστικό (!), δίεση (#), αριθμούς κλπ.
3. Εάν τα συνθηματικά είναι αποθηκευμένα ηλεκτρονικά π.χ. σε e-mail, θα πρέπει να είναι σε μη αναγνώσιμη μορφή έτσι ώστε οι μη εξουσιοδοτημένοι χρήστες να μην μπορούν να ανακτήσουν τα στοιχεία των χρηστών.
4. Τα συνθηματικά των χρηστών θα πρέπει να αλλάζονται ανά τακτικά χρονικά διαστήματα π.χ. ανά 6 μήνες.
5. Οι χρήστες μετά την ολοκλήρωση της χρήσης του πληροφοριακού συστήματος θα ήταν απαραίτητο να κάνουν αποσύνδεση από το σύστημα αυτό έτσι ώστε οι μη εξουσιοδοτημένοι χρήστες να μην μπορούν να αποκτήσουν πρόσβαση.
6. Οι υπολογιστές και οι servers του πληροφοριακού συστήματος, αν χρησιμοποιούνται μετά από ένα συγκεκριμένο χρονικό διάστημα αδράνειας, θα πρέπει να ζητάνε ξανά το username και το password του χρήστη, αλλιώς να αποσυνδέονται. Με αυτόν τον τρόπο οι μη εξουσιοδοτημένοι χρήστες δεν θα έχουν τη δυνατότητα να εισβάλλουν στο πληροφοριακό σύστημα.
7. Όταν κάποιος εξουσιοδοτημένος ή μη εξουσιοδοτημένος χρήστης προσπαθεί συνεχόμενες φορές να μπει στο σύστημα με λανθασμένα συνθηματικά, θα πρέπει να αποδείξει την αυθεντικότητά του. Αυτό θα πραγματοποιηθεί απαντώντας συγκεκριμένες ερωτήσεις που αποδεικνύουν την εξουσιοδοτημένη χρήση του στο σύστημα.

A3 *Έλεγχος προσπέλασης και χρήσης πόρων*

Η πρόσβαση στο πληροφοριακό σύστημα είναι σημαντική καθώς δεν θα πρέπει να γίνεται από μη εξουσιοδοτημένους χρήστες. Οι μη εξουσιοδοτημένοι χρήστες δεν θα πρέπει να εισέρχονται σε συγκεκριμένα δωμάτια, όπως για παράδειγμα τα δωμάτια με τους

υπολογιστές Servers. Τα μέτρα αντιμετώπισης για τις απειλές που προκαλούνται από την πρόσβαση στο πληροφοριακό σύστημα και τη χρήση των πόρων είναι τα εξής:

1. Ανάθεση συγκεκριμένων ρόλων και καθηκόντων με σκοπό, μόνο οι εξουσιοδοτημένοι χρήστες να έχουν τη δυνατότητα πρόσβασης στους σημαντικούς υπολογιστικούς πόρους που διαχειρίζονται ευαίσθητα προσωπικά δεδομένα. Με αυτόν τον τρόπο, οι χρήστες του συστήματος θα έχουν συγκεκριμένα δικαιώματα πρόσβασης στο πληροφοριακό σύστημα.
2. Αναθεώρηση των εξουσιοδοτήσεων που αφορούν την πρόσβαση στο πληροφοριακό σύστημα και επανεξέταση ανά τακτικά χρονικά διαστήματα.
3. Η τήρηση του προσωπικού απορρήτου και των ευαίσθητων δεδομένων είναι σημαντική καθώς θα πρέπει να τη διαχειρίζονται οι κατάλληλοι εξουσιοδοτημένοι χρήστες. Οι τεχνικές γνώσεις των υπαλλήλων θα συμβάλλουν στην σωστή προστασία του απορρήτου.
4. Ύπαρξη κανόνων που αφορούν την ασφάλεια του πληροφοριακού συστήματος του νοσοκομείου. Σε περίπτωση απόλυσης ή παραίτησης κάποιου υπαλλήλου του νοσοκομείου, ο οποίος έχει εξουσιοδοτημένη πρόσβαση στο σύστημα, θα πρέπει να διαγράφουν τον προσωπικό τους λογαριασμό που περιέχει το username και το password.
5. Οι χρήστες που παύουν να έχουν εξουσιοδοτημένη πρόσβαση στο πληροφοριακό σύστημα θα πρέπει να παραδίδουν στους υπεύθυνους οποιοδήποτε υλικό ή ηλεκτρονικό εξοπλισμό που αφορά το σύστημα. Για παράδειγμα, αν γνωρίζουν τον κωδικό που αφορά την πρόσβαση στη βάση του υπολογιστή server, θα πρέπει οι υπάλληλοι να τον παραδίδουν στους υπεύθυνους, οι οποίοι θα πρέπει να τους αλλάζουν.

A4 ***Διαχείριση εμπιστευτικών δεδομένων***

Η προστασία των δεδομένων του πληροφοριακού συστήματος του νοσοκομείου είναι από τις σημαντικότερες λειτουργίες καθώς αφορούν τα ευαίσθητα δεδομένα των ασθενών και τα προσωπικά στοιχεία των υπαλλήλων. Τα μέτρα για τη σωστή διαχείριση των εμπιστευτικών δεδομένων είναι τα εξής:

1. Η κρυπτογράφηση με τη χρήση των κατάλληλων κλειδιών με συγκεκριμένο μέγεθος, θα προστατεύει τα ευαίσθητα δεδομένα των ασθενών.
2. Η χρήση συναρτήσεων κατακερματισμού συμβάλλει στην προστασία των δεδομένων του πληροφοριακού συστήματος.
3. Η χρήση σκληρού δίσκου, ο οποίος θα κρατάει back up καθημερινά με σκοπό να μην υπάρχει απώλεια των δεδομένων. Με αυτόν τον τρόπο, σε περίπτωση απώλειας ή καταστροφής οποιουδήποτε υπολογιστικού πόρου, δεν θα διαταράσσεται η διαθεσιμότητα και η ακεραιότητα των δεδομένων.
4. Τα αποθηκευτικά μέσα που περιέχουν αντίγραφα των δεδομένων θα πρέπει να κρυπτογραφούνται και αυτά.
5. Ο υλικός εξοπλισμός που αφορά τα αντίγραφα ασφάλειας των δεδομένων θα πρέπει να φυλάσσεται σε ξεχωριστό δωμάτιο από τους υπόλοιπους υπολογιστικούς πόρους.
6. Η ύπαρξη κατάλληλων προγραμμάτων που αφορούν την αντιμετώπιση των περιστατικών παραβίασης του συστήματος είναι σημαντική. Με αυτά τα προγράμματα, θα προστατεύονται τα δεδομένα από τις μη εξουσιοδοτημένες

προσβάσεις, τυχαίες διαγραφές των δεδομένων, των φυσικών καταστροφών των υπολογιστικών πόρων.

7. Οι υπολογιστές που περιέχουν τα ευαίσθητα δεν θα πρέπει να συνδέονται απευθείας στο Διαδίκτυο.
8. Τα αρχεία που περιέχουν προσωπικά – ευαίσθητα δεδομένα θα πρέπει να είναι τοποθετημένα σε έναν χώρο που δεν είναι εκτεθειμένος σε κοινή θέα.

A5 ***Προστασία από τη χρήση υπηρεσιών από τρίτους***

Ο κάθε υπάλληλος του νοσοκομείου έχει και μία διαφορετική αρμοδιότητα όσον αφορά το πληροφοριακό σύστημα. Η προστασία του πληροφοριακού συστήματος από τους μη εξουσιοδοτημένους χρήστες είναι αναγκαία καθώς αυτοί μπορούν να επιφέρουν πολλές αλλαγές στο σύστημα. Τα μέτρα αντιμετώπισης που προστατεύουν το σύστημα από τη χρήση υπηρεσιών από τρίτους είναι τα εξής:

1. Η ύπαρξη ενός καταλόγου με τα στοιχεία των υπαλλήλων και συγκεκριμένα των υπαλλήλων που διαχειρίζονται το πληροφοριακό σύστημα. Με αυτόν τον τρόπο χρήστες που δεν είναι καταγεγραμμένοι στον κατάλογο και δεν θα έχουν κάποιο λογαριασμό, δεν θα μπορούν να εισέλθουν στο σύστημα.
2. Η καταγραφή των ατόμων με τα στοιχεία τους, που εισέρχονται σε σημαντικούς χώρους που υπάρχει φυσικός εξοπλισμός είναι σημαντική. Με αυτόν τον τρόπο, οι μη εξουσιοδοτημένοι χρήστες δεν θα έχουν την δυνατότητα χρήσης των υπηρεσιών του πληροφοριακού συστήματος.
3. Σε περίπτωση ανάθεσης οποιασδήποτε υπηρεσίας του συστήματος από τους υπεύθυνους του νοσοκομείου σε κάποιον υπάλληλο, θα πρέπει η ανάθεση αυτή να γίνεται εγγράφως και μόνο με την εντολή των υπεύθυνων. Σε αυτό το έγγραφο, θα γράφονται τα προσωπικά δεδομένα των υπαλλήλων με σκοπό να είναι γνωστό ποιος έχει πρόσβαση στο σύστημα.
4. Καταγραφή των παραβιάσεων του πληροφοριακού συστήματος σε αρχείο, όπου θα αναφέρονται αναλυτικά οι ημερομηνίες και οι ώρες.
5. Σε περίπτωση απομακρυσμένης πρόσβασης στο πληροφοριακό σύστημα του νοσοκομείου πρέπει να γίνεται υπό την εποπτεία και έλεγχο των υπεύθυνων του νοσοκομείου και συγκεκριμένα του υπεύθυνου ασφάλειας, ο οποίος θα καταγράφει αυτήν την ενέργεια.

A6 ***Προστασία λογισμικού***

Η προστασία του λογισμικού είναι απαραίτητη καθώς σε αυτά βασίζεται η λειτουργία των υπολογιστικών πόρων. Τα μέτρα αντιμετώπισης για την προστασία του λογισμικού είναι τα εξής:

1. Το λογισμικό να είναι γνήσιο και να διαθέτει έγκυρη άδεια χρήσης έτσι ώστε να μπορούν οι υπολογιστές να λειτουργούν σωστά.
2. Το λογισμικό να προέρχεται από ελεγμένους και αξιόπιστους προμηθευτές.
3. Το λογισμικό να είναι εγκεκριμένο και καταγεγραμμένο, δηλαδή να υπάρχει αρχείο που να δηλώνει τι λογισμικό χρησιμοποιείται σε κάθε δωμάτιο που διαθέτει υπολογιστικό πόρο.
4. Το λογισμικό να είναι ενημερωμένο με τις τελευταίες εκδόσεις που έχει βγάλει η εταιρεία.

5. Το λογισμικό πρέπει να χρησιμοποιείται μόνο από τους εξουσιοδοτημένους χρήστες, καθώς οι μη εξουσιοδοτημένοι χρήστες μπορούν να προκαλέσουν βλάβες στο πληροφοριακό σύστημα του νοσοκομείου, π.χ. διαγραφή των προσωπικών – ευαίσθητων δεδομένων των ασθενών.
6. Οι εξουσιοδοτημένοι χρήστες θα ήταν σημαντικό να χρησιμοποιούν το λογισμικό των υπολογιστικών πόρων μόνο για το σκοπό και τις αρμοδιότητες που τους έχουν ανατεθεί.
7. Σε περίπτωση κάποιας ενημέρωσης ή αλλαγής του λογισμικού να γίνεται ο κατάλληλος έλεγχος για τυχόν εντοπισμό προγραμμάτων π.χ. κακόβουλων προγραμμάτων, που έχουν εγκατασταθεί εκτός των εγκεκριμένων διαδικασιών.
8. Η πραγματοποίηση περιοδικών ελέγχων για τυχόν παραβιάσεις από μη εξουσιοδοτημένους χρήστες είναι πολύ σημαντική για την προστασία του πληροφοριακού συστήματος του νοσοκομείου.

A7 ***Διαχείριση ασφάλειας δικτύου***

Η προστασία του δικτύου και συγκεκριμένα η προστασία της ασφάλειας του, είναι αναγκαία γιατί σε αυτό βασίζεται η λειτουργία του νοσοκομείου. Το δίκτυο χωρίζεται με βάση τα δωμάτια και τους υπολογιστικούς πόρους και η πρόσβαση σε αυτούς θα πρέπει να γίνεται μόνο από τους εξουσιοδοτημένους χρήστες. Τα μέτρα αντιμετώπισης είναι τα εξής:

1. Οι διαδικτυακοί διακομιστές και συγκεκριμένα οι web servers θα πρέπει να βρίσκονται σε διαφορετικό δίκτυο από τα υπόλοιπα εσωτερικά δίκτυα.
2. Οι διαδικτυακοί διακομιστές θα ήταν σημαντικό να εκτελούνται σε καθορισμένους υπολογιστές που δεν έχουν να εκτελέσουν κάποια άλλη λειτουργία ή εφαρμογές, όπως για παράδειγμα μία βάση δεδομένων.
3. Στους διαδικτυακούς διακομιστές θα ήταν αναγκαίο να υπάρχουν προγράμματα παραμετροποιημένα π.χ. script, τα οποία θα προστατεύουν το δίκτυο του νοσοκομείου από τους μη εξουσιοδοτημένους χρήστες.
4. Στους διαδικτυακούς διακομιστές, οι οποίοι θα είναι παραμετροποιημένοι, θα ήταν απαραίτητο να υπάρχουν αρχεία. Σε αυτά τα αρχεία θα καταγράφονται όλα τα συμβάντα που γίνονται για μεγάλο χρονικό διάστημα π.χ. για 12 μήνες.
5. Οι υπολογιστές που χρησιμοποιούνται σαν διακομιστές, δηλαδή servers, δεν θα πρέπει να χρησιμοποιούνται για άλλες αρμοδιότητες ή υπηρεσίες του νοσοκομείου.
6. Ο τακτικός έλεγχος των συσκευών που συνδέονται στο δίκτυο είναι απαραίτητος με σκοπό τη σωστή πρόσβαση και χρήση αυτών των συσκευών από τους εξουσιοδοτημένους χρήστες.
7. Η χρήση ασφαλών πρωτοκόλλων και των υπηρεσιών τους, που είναι κρυπτογραφημένα, όπως για παράδειγμα το πρωτόκολλο SSH, αποτελεί ένα από τα σημαντικότερα μέτρα αντιμετώπισης που θα είχαν ως στόχο την προστασία του δικτύου.
8. Οι συνδέσεις στο δίκτυο που ενεργοποιούνται μέσα από το firewall θα πρέπει να εγκρίνονται από τους υπεύθυνους του νοσοκομείου και συγκεκριμένα από τον υπεύθυνο ασφάλειας.

A8 ***Προστασία από ιομορφικό λογισμικό***

Το νοσοκομείο θα πρέπει να διαθέτει κατάλληλο λογισμικό για την προστασία από ιούς για όλες τις υπηρεσίες και εφαρμογές που προσφέρει στους χρήστες. Τα μέτρα για την αντιμετώπιση ιομορφικών λογισμικών είναι τα εξής:

1. Οι υπάλληλοι του νοσοκομείου και συγκεκριμένα οι υπεύθυνοι ασφάλειας του πληροφοριακού συστήματος του νοσοκομείου θα πρέπει να γνωρίζουν πως να χειρίζονται τις εφαρμογές κατά των κακόβουλων λογισμικών.
2. Η ενημέρωση των υπεύθυνων ασφάλειας του συστήματος για θέματα που αφορούν τα κακόβουλα λογισμικά είναι απαραίτητη.
3. Η χρήση αξιόπιστων προγραμμάτων antivirus, θα συμβάλλει θετικά στην προστασία των υπολογιστών, όπως για παράδειγμα των υπολογιστών που χρησιμοποιούν οι υπάλληλοι, των υπολογιστών server, στους οποίους αποθηκεύονται προσωπικά – ευαίσθητα δεδομένα των ασθενών.
4. Η χρήση προγραμμάτων τειχών ασφαλείας, δηλαδή firewalls, θα προστατέψει τα ευαίσθητα δεδομένα τόσο των ασθενών όσο και των χρηστών του πληροφοριακού συστήματος από κακόβουλα προγράμματα.
5. Η χρήση προγραμμάτων antivirus και firewalls θα πρέπει να διαθέτουν τις τελευταίες ενημερώσεις.
6. Ο τακτικός έλεγχος που αφορά την εγκατάσταση μη ελεγμένων προγραμμάτων ή προγραμμάτων από άγνωστες πηγές είναι σημαντικός.
7. Η χρήση συστημάτων ανίχνευσης εισβολών είναι αναγκαία γιατί χρησιμοποιούν αισθητήρες και καταγράφουν οποιαδήποτε ασυνέπεια των υπολογιστικών πόρων και εφαρμογών. Αυτό θα πραγματοποιηθεί με προγράμματα ή αρχεία που είναι παραμετροποιημένα.
8. Στο πληροφοριακό σύστημα, θα πρέπει να υπάρχουν παραμετροποιημένα προγράμματα που θα απαγορεύουν ή θα περιορίζουν την μεταφόρτωση εκτελέσιμου κώδικα. Με αυτόν τον τρόπο το σύστημα του νοσοκομείου δεν θα είναι εκτεθειμένο σε κακόβουλα προγράμματα ή στους μη εξουσιοδοτημένους χρήστες.
9. Οι χρήστες να χρησιμοποιούν τις εφαρμογές μόνο με βάση τα δικαιώματα πρόσβασης που έχουν.
10. Τα δωμάτια που περιέχουν σημαντικούς υπολογιστικούς πόρους, όπως για παράδειγμα τους υπολογιστές server και τα δωμάτια που επικοινωνούν με εξωτερικά πληροφοριακά συστήματα θα πρέπει να βρίσκονται σε δικτυακή απομόνωση γιατί περιέχουν ευαίσθητα δεδομένα.
11. Η χρήση εξωτερικών συσκευών, όπως για παράδειγμα USB ή σκληρός δίσκος θα πρέπει να ελέγχεται σε έναν υπολογιστή με ελεγχόμενο περιβάλλον.

A9 ***Ασφαλής χρήση διαδικτυακών υπηρεσιών***

Η σύνδεση στο διαδίκτυο από τους υπολογιστές και τις συσκευές του νοσοκομείου θα πρέπει να ακολουθεί μια συγκεκριμένη πολιτική προκειμένου να υπάρχει η απαραίτητη προστασία. Τα μέτρα αντιμετώπισης που συμβάλλουν στην ασφαλή χρήση των διαδικτυακών υπηρεσιών είναι τα εξής:

1. Ο τακτικός έλεγχος σύνδεσης των υπολογιστών που περιέχουν ευαίσθητα δεδομένα με το διαδίκτυο είναι αναγκαίος.
2. Ο καθορισμός των διαδικτυακών υπηρεσιών κρίνεται σημαντικός διότι οι χρήστες του πληροφοριακού συστήματος θα γνωρίζουν ποιες υπηρεσίες είναι επιτρεπτές και ποιες απαγορευμένες.

3. Οι υπολογιστικοί πόροι που συνδέονται στο διαδίκτυο θα πρέπει να περιέχουν προγράμματα antivirus, firewalls και συστήματα ανίχνευσης κακόβουλων προγραμμάτων ή επιθέσεων.
4. Η ενημέρωση του λογισμικού των υπολογιστών του νοσοκομείου που συνδέονται με το διαδίκτυο πρέπει να είναι έγκαιρη.
5. Οι χρήστες του πληροφοριακού συστήματος του νοσοκομείου θα πρέπει να έχουν συγκεκριμένα δικαιώματα χρήσης του διαδικτύου.

A10 ***Ασφάλεια εξοπλισμού***

Η ασφάλεια των χώρων και των υποδομών του νοσοκομείου έχουν ως κύριο στόχο την αποτροπή της μη εξουσιοδοτημένης πρόσβασης στους χώρους όπου είναι εγκατεστημένα τα πληροφοριακά συστήματα και της καταστροφής των αγαθών τους. Η πρόσβαση σε κρίσιμους χώρους όπως για παράδειγμα η πρόσβαση στο Computer Room έχει ως στόχο στην προστασία των προσωπικών – ευαίσθητων δεδομένων των χρηστών των πληροφοριακών συστημάτων. Τα μέτρα αντιμετώπισης είναι τα εξής:

1. Ο εξοπλισμός του νοσοκομείου που μεταφέρεται εκτός κτιρίου, όπως για παράδειγμα η μεταφορά του σκληρού δίσκου ή οποιουδήποτε υπολογιστή, θα πρέπει να πραγματοποιείται μόνο κατ' εντολή και την έγκριση του υπεύθυνου ασφάλειας. Επίσης, τέτοιου είδους ενέργειας θα καταγράφονται σε αρχείο από τον υπεύθυνο ασφάλειας.
2. Η εγκατάσταση αντικλεπτικού συστήματος συναγερμού θα συμβάλλει στην προφύλαξη τόσο των υπολογιστικών πόρων όσο και των δεδομένων του πληροφοριακού συστήματος του νοσοκομείου από κλοπή.
3. Ο τακτικός έλεγχος πρόσβασης στα συστήματα που βρίσκονται σε κρίσιμους χώρους, όπως για παράδειγμα στους χώρους που βρίσκονται οι servers είναι απαραίτητος διότι με αυτόν τον τρόπο προστατεύεται το πληροφοριακό σύστημα του νοσοκομείου.
4. Η εγκατάσταση κλειστού κυκλώματος τηλεόρασης, θα παρέχει τη δυνατότητα κεντρικής εποπτείας και καταγραφής των δραστηριοτήτων που λαμβάνουν χώρα σε μια εγκατάσταση του νοσοκομείου.
5. Η επικοινωνία μεταξύ των υπολογιστών θα ήταν σημαντικό να πραγματοποιείται μέσω κάποιου καναλιού επικοινωνίας που είναι κρυπτογραφημένο.
6. Οι συσκευές που περιέχουν προσωπικά - ευαίσθητα π.χ. εκτυπωτές, υπολογιστές δεν θα πρέπει να βρίσκονται εκτεθειμένα σε κοινή θέα.
7. Η ύπαρξη επιπλέον εξοπλισμού σε περίπτωση βλάβης ή φυσικής καταστροφής είναι σημαντική.
8. Η ύπαρξη υπεύθυνου συντήρησης είναι απαραίτητη γιατί θα επιδιορθώνει τυχόν βλάβες του εξοπλισμού του νοσοκομείου.
9. Η τοποθέτηση πορτών και παράθυρων ασφαλείας στους κρίσιμους χώρους, όπως είναι τα Server Room, είναι αναγκαία διότι έτσι θα είναι αδύνατο να πραγματοποιηθεί υποκλοπή.

A11 ***Φυσική ασφάλεια κτιριακής εγκατάστασης***

Η φυσική ασφάλεια τόσο του κτιρίου του νοσοκομείου, όσο και των υπολογιστικών κρίσιμων χώρων είναι απαραίτητη. Τα μέτρα αντιμετώπισης για την προστασίας της ασφάλειας του είναι τα εξής:

1. Η τοποθέτηση συναγερμών στο κτίριο του νοσοκομείου αλλά και στους κρίσιμους χώρους είναι απαραίτητη διότι έτσι θα αποφεύγονται οι υποκλοπές.
2. Το νοσοκομείο θα πρέπει να είναι κατασκευασμένο σωστά και να παρέχει αντισεισμική προστασία. Με άλλα λόγια, σε περίπτωση να μην υπάρχουν βλάβες ή καταστροφές τόσο της κτιριακής εγκατάστασης όσο και των υπολογιστικών πόρων.
3. Η πυροπροστασία είναι αναγκαία σε περίπτωση κάποιας πυρκαγιάς.
4. Οι εξοπλισμοί του νοσοκομείου θα πρέπει να βρίσκονται σε χώρους που δεν υπάρχουν υδροσωληνώσεις.
5. Η απαγόρευση καπνίσματος στις εγκαταστάσεις του νοσοκομείου που υπάρχουν εξοπλισμοί, είναι απολύτως απαραίτητη.
6. Οι εξοπλισμοί δεν θα πρέπει να είναι τοποθετημένοι δίπλα από εύφλεκτα υλικά.
7. Η ύπαρξη και χρήση κλιματισμού, θα συμβάλλει στη διατήρηση της ενδεικνυόμενης θερμοκρασίας του εξοπλισμού.
8. Η χρήση ανιχνευτών υγρασίας θα έχει ως στόχο την προστασία του εξοπλισμού από τυχόν φυσικές καταστροφές.
9. Η χρήση κατάλληλου μηχανισμού εισόδου στους κρίσιμους χώρους του νοσοκομείου να πραγματοποιείται μόνο από έναν εξουσιοδοτημένο χρήστη κάθε φορά.
10. Η ύπαρξη υπεύθυνου συντήρησης είναι σημαντική σε περίπτωση φυσικής καταστροφής ή βλάβης.
11. Στους κρίσιμους χώρους θα πρέπει βρίσκονται συσκευές UPS, οι οποίες παρέχουν ρεύμα και προστατεύουν τους υπολογιστικούς πόρους, όπως για παράδειγμα τους server από τη διακοπή ρεύματος. Σε αυτήν την περίπτωση δεν θα χάνονται τα προσωπικά – ευαίσθητα δεδομένα.
12. Στο νοσοκομείο θα πρέπει να υπάρχουν γεννήτριες ρεύματος, με σκοπό την παροχή ρεύματος σε περίπτωση διακοπής ρεύματος.
13. Η ύπαρξη υπεύθυνων που έχουν την κατάλληλη εκπαίδευση και γνώσεις ως προς τις κτιριακές επιδιορθώσεις.

Α4.ΣΥΝΟΨΗ ΠΙΟ ΚΡΙΣΙΜΩΝ ΑΠΟΤΕΛΕΣΜΑΤΩΝ

Στην εργασία παρουσιάζονται όλα τα αγαθά του πληροφοριακού συστήματος του νοσοκομείου. Σύμφωνα με το excel αρχείο, παρουσιάζονται όλα τα αγαθά του συστήματος και οι αντίστοιχες ευπάθειες, απειλές και αποτελέσματα.

Τα 3 αγαθά που παρουσιάζουν την υψηλότερη επικινδυνότητα είναι τα εξής:

- Windows XP, καθώς δεν μπορούν να προστατέψουν τους υπολογιστές που χρησιμοποιούνται στα Patient Room από τους ιούς. ***(RPN: 720)***
- Hospital Website, επειδή είναι open source και οι μη εξουσιοδοτημένοι χρήστες μπορούν εύκολα να υποκλέψουν ή να τροποποιήσουν ή να διαγράψουν τα ιατρικά ευαίσθητα δεδομένα. ***(RPN: 512)***
- Patient Data, είναι από τα σημαντικότερα αγαθά του πληροφοριακού συστήματος του νοσοκομείου καθώς αναφέρονται σε ευαίσθητα δεδομένα των ασθενών. ***(RPN: 490)***

Α5. ΠΗΓΕΣ

Οι πηγές που χρησιμοποιήθηκαν για την εργασία είναι οι εξής:

1. https://support.microsoft.com/el-gr/help/14223/windows-xp-end-of-support
2. https://www.infosec.aueb.gr/Courses/lectures/iss/Advanced%20Risk%20Assessment_RA_Controls_Processes-Stergiopoulos2016.pdf
3. https://www.infosec.aueb.gr/Courses/lectures/iss/AUEB_Risk_Management_v1.8.pdf
4. http://www.cvedetails.com
5. https://www.cnet.com/news/why-windows-xp-users-are-more-vulnerable-to-security-threats/
6. http://nestor.teipel.gr/xmlui/bitstream/handle/123456789/12292/SDO_DMYP_00250_Medium.pdf?sequence=1
7. http://nestor.teipel.gr/xmlui/bitstream/handle/123456789/13433/STE_MHP_00188_Medium.pdf?sequence=1
8. http://www.alphr.com/security/1000131/the-windows-7-and-8-vulnerability-you-need-to-know-about
9. http://newtech-pub.com/wp-content/uploads/2013/10/kef-asf.plhr_.sust_.pdf
10. http://www.icte.uowm.gr/uploads/thesis/dipl_ergasia_am14.pdf
11. http://slideplayer.gr/slide/2019439/