ΕΘΝΙΚΟ ΚΑΙ ΚΑΠΟΔΙΣΤΡΙΑΚΟ ΠΑΝΕΠΙΣΤΗΜΙΟ ΑΘΗΝΩΝ

ΤΜΗΜΑ ΝΟΣΗΛΕΥΤΙΚΗΣ

ΔΙΑΠΑΝΕΠΙΣΤΗΜΙΑΚΟ ΔΙΑΤΜΗΜΑΤΙΚΟ

ΠΡΟΓΡΑΜΜΑ ΜΕΤΑΠΤΥΧΙΑΚΩΝ ΣΠΟΥΔΩΝ

ΕΙΔΙΚΕΥΣΗ: ΟΡΓΑΝΩΣΗ ΚΑΙ ΔΙΟΙΚΗΣΗ ΥΠΗΡΕΣΙΩΝ ΥΓΕΙΑΣ

# ΑΣΦΑΛΕΙΑ ΠΛΗΡΟΦΟΡΙΑΚΩΝ ΣΥΣΤΗΜΑΤΩΝ ΣΤΑ ΝΟΣΟΚΟΜΕΙΑ

**Μεταπτυχιακή Φοιτήτρια: Παπαϊωάννου Ευαγγελία**

ΝΟΣΗΛΕΥΤΡΙΑ ΠΕ

ΜΕΤΑΠΤΥΧΙΑΚΗ ΔΙΠΛΩΜΑΤΙΚΗ ΕΡΓΑΣΙΑ

Αθήνα, 2018

ΕΞΕΤΑΣΤΙΚΗ ΕΠΙΤΡΟΠΗ

1.ΚΑΘΗΓΗΤΗΣ ΓΡΗΓΟΡΙΟΣ ΧΟΝΔΡΟΚΟΥΚΗΣ (ΕΠΙΒΛΕΠΩΝ)

2.ΚΑΘΗΓΗΤΗΣ ΔΗΜΗΤΡΙΟΣ ΚΑΡΑΛΕΚΑΣ

3.ΕΠΙΚΟΥΡΟΣ ΚΑΘΗΓΗΤΗΣ ΙΩΑΝΝΗΣ ΓΙΑΝΝΑΤΣΗΣ

# ΕΥΧΑΡΙΣΤΙΕΣ

Η παρούσα διπλωματική εργασία εκπονήθηκε κατά τους μήνες Μάρτιο 2018 έως Σεπτέμβριο 2018 στα πλαίσια του μεταπτυχιακού προγράμματος «Οργάνωση και Διοίκηση Υπηρεσιών Υγείας». Για τη στήριξη και πολύτιμη βοήθειά του στην εκπόνηση της εργασίας μου θα ήθελα να ευχαριστήσω τον επιβλέποντα καθηγητή μου, κύριο Γρηγόρη Χονδροκούκη. Επίσης, θα ήθελα να ευχαριστήσω τους γονείς μου, Ιωάννη και Λεμονιά, για την συμπαράστασή τους και για ό,τι μου έχουν προσφέρει σε όλα τα χρόνια των σπουδών μου.

Παπαϊωάννου Ευαγγελία

Αθήνα, 2018

# Πίνακας περιεχομένων

# ΚΑΤΑΛΟΓΟΣ ΕΙΚΟΝΩΝ



# ΚΑΤΑΛΟΓΟΣ ΠΙΝΑΚΩΝ

## ΠΕΡΙΛΗΨΗ ΣΤΑ ΕΛΛΗΝΙΚΑ

Οι περισσότεροι οργανισμοί στις μέρες μας στηρίζουν τη λειτουργία τους στα Πληροφοριακά Συστήματα. Το ίδιο συμβαίνει και με τους οργανισμούς υγειονομικής περίθαλψης, όπως είναι τα νοσοκομεία, οι οποίοι αποθηκεύουν και επεξεργάζονται με τη βοήθεια των Πληροφοριακών Συστημάτων τόσο δεδομένα που αφορούν τη λειτουργία τους όσο και ιατρικές πληροφορίες. Αυτά τα στοιχεία είναι εμπιστευτικά και απόρρητα και πρέπει να προστατευθούν από εσωτερικούς και εξωτερικούς κινδύνους. Επομένως, κρίνεται ζωτικής σημασίας η διατήρηση της ασφάλειας των Πληροφοριακών Συστημάτων των νοσοκομείων. Σ΄ αυτήν την εργασία, αρχικά γίνεται μια μικρή εισαγωγή στα Πληροφοριακά Συστήματα και έπειτα στα Πληροφοριακά Συστήματα των νοσοκομείων. Στη συνέχεια, αναλύονται οι απειλές και οι κίνδυνοι που μπορούν να διαταράξουν τη φυσιολογική λειτουργία των Πληροφοριακών Συστημάτων των νοσοκομείων και να θέσουν σε κίνδυνο την προστασία των ηλεκτρονικών δεδομένων. Ακολουθεί ανάλυση της έννοια της ασφάλειας των Πληροφοριακών Συστημάτων των νοσοκομείων και στη συνέχεια παρατίθενται μέτρα προστασίας και πολιτικές ασφάλειας για τη διασφάλιση της προστασίας τους.

## ΠΕΡΙΛΗΨΗ ΣΤΑ ΑΓΓΛΙΚΑ

**NATIONAL AND KAPODISTRIAN UNIVERSITY OF ATHENS**

**FACULTY OF NURSING**

INTERUNIVERSITY POSTGRADUATE PROGRAM IN HEALTH CARE MANAGEMENT AND HEALTH CARE INFORMATICS

**SECURITY OF HOSPITAL INFORMATION SYSTEMS**

BY PAPAIOANNOU EVANGELIA

**SUMMARY**

Most organizations nowadays support their operation in Information Systems. The same applies to health care organizations, such as hospitals, which store and process both data about their operation and information about medical information with the help of information systems. These elements are confidential and must be protected from internal and external risks. Therefore, it is vital to maintain the safety of the Hospital Information Systems. In this work, there is initially a small introduction to Information Systems and then to the Information Systems of Hospitals. It then analyzes the threats and risks that can disrupt the normal operation of Hospital Information Systems and jeopardize the protection of electronic data. The following is an analysis of the concept of security of the Hospital Information Systems and then there are cited protection measures and security policies to ensure their protection.

# ΚΕΦΑΛΑΙΟ 1. ΕΙΣΑΓΩΓΗ

## 1.1.Σκοπός της εργασίας

Σκοπός της συγκεκριμένης εργασίας είναι να περιοριστούν οι κίνδυνοι που απειλούν τα Πληροφοριακά Συστήματα των νοσοκομείων και να εξασφαλιστεί η προστασία τους έναντι αυτών των κινδύνων.

## 1.2.Αντικείμενα της εργασίας

Για να επιτευχθεί ο σκοπός της εργασίας, αρχικά τονίζεται η σημασία της διασφάλισης της προστασίας των Πληροφοριακών Συστημάτων των νοσοκομείων. Στη συνέχεια, παρουσιάζεται ένα πλήθος μέτρων προστασίας για την εξασφάλιση της ακεραιότητας, εμπιστευτικότητας και διαθεσιμότητας των ιατρικών δεδομένων που αποθηκεύονται ή μεταφέρονται μέσω των Πληροφοριακών Συστημάτων στους χώρους υγείας.

Η εργασία πραγματοποιήθηκε με ανασκόπηση της βιβλιογραφίας τόσο σε βιβλία όσο και σε ηλεκτρονικές πηγές.

Οι λέξεις- κλειδιά που χρησιμοποιήθηκαν ήταν: πληροφοριακά συστήματα, πληροφοριακά συστήματα νοσοκομείων, κίνδυνοι, απειλές, εισβολείς, ασφάλεια, ακεραιότητα, εμπιστευτικότητα, διαθεσιμότητα, προστατευτικά μέτρα, πρωτόκολλα, πολιτική ασφάλειας, cybersecurity, health policy, patients' rights

## 1.3.Δομή της εργασίας

Στο Κεφάλαιο 1 αυτής της εργασίας γίνεται μια εισαγωγή στην εργασία, έτσι ώστε να παρουσιαστεί ο σκοπός, τα αντικείμενα και η δομή της εργασίας. Στο Κεφάλαιο 2 γίνεται μία «εισαγωγή στα Πληροφοριακά Συστήματα», όπου ορίζεται το πληροφοριακό σύστημα και αναλύονται τα συστατικά του. Στο Κεφάλαιο 3 γίνεται «εισαγωγή στα Πληροφοριακά Συστήματα των νοσοκομείων», με αναφορά στα υποσυστήματα των Πληροφοριακών Συστημάτων των νοσοκομείων, στους λόγους εισαγωγής πληροφοριακών συστημάτων στα νοσοκομεία και στα οφέλη εισαγωγής

πληροφοριακών συστημάτων στον τομέα της υγείας. Ακολουθεί το Κεφάλαιο 4 με τίτλο « Κίνδυνοι και απειλές» όπου αναφέρονται οι κατηγορίες κινδύνων και η διαδικασία αξιολόγησης των κινδύνων. Έπειτα, στο Κεφάλαιο 5 περιγράφεται μία σοβαρή κατηγορία απειλής, οι «Εισβολείς» με κύρια αναφορά στους λόγους επιθέσεων από εισβολείς, στον τρόπο ανίχνευσης μιας επίθεσης από εισβολείς αλλά και στο σωστό τρόπο χειρισμού αυτών των επιθέσεων. Στο Κεφάλαιο 6 με τίτλο «Βασικές έννοιες ασφάλειας Πληροφοριακών Συστημάτων», γίνεται ανάλυση του ορισμού της ασφάλειας, των βασικών εννοιών της ασφάλειας, των βασικών αρχών της ασφάλειας των Πληροφοριακών Συστημάτων, των υπηρεσιών ασφάλειας και των στόχων τους, αλλά και του ρόλου της ασφάλειας κατά τη διάρκεια όλης της ζωής του συστήματος. Στη συνέχεια, ακολουθεί το Κεφάλαιο 7 όπου αναφέρεται στην «Ασφάλεια των Πληροφοριακών Συστημάτων των Νοσοκομείων» με κύρια σημεία τις ιδιαιτερότητες που παρουσιάζουν τα Πληροφοριακά Συστήματα των Νοσοκομείων σε σχέση με την ασφάλεια, την αναγκαιότητα ύπαρξης στα Πληροφοριακά Συστήματα των Νοσοκομείων και τη διάκριση της ασφάλειας στο χώρο του νοσοκομείου. Στο Κεφάλαιο 8 με τίτλο «Πολιτική ασφάλειας στα Πληροφοριακά Συστήματα των νοσοκομείων» αναφέρεται ο ορισμός της πολιτικής ασφάλειας, η διαδικασία για την εφαρμογή μιας πολιτικής ασφάλειας στα νοσοκομεία και αναλύεται μια πολιτική ασφάλειας υψηλού επιπέδου (SEISMED). Τα «Μέτρα προστασίας των Πληροφοριακών Συστημάτων των νοσοκομείων» τόσο κατά τις καθημερινές διεργασίες όσο και σε περίπτωση έκτακτης ανάγκης αναλύονται στο Κεφάλαιο 9. Τέλος, στο Κεφάλαιο 10 αναφέρονται τα «Συμπεράσματα» της εργασίας.

# ΚΕΦΑΛΑΙΟ 2. ΕΙΣΑΓΩΓΗ ΣΤΑ ΠΛΗΡΟΦΟΡΙΑΚΑ ΣΥΣΤΗΜΑΤΑ

## 2.1. Εισαγωγή κεφαλαίου 2

Σ' αυτό το κεφάλαιο γίνεται μία εισαγωγή στα Πληροφοριακά Συστήματα. Στην υποενότητα 2.2 αναφέρεται ο ορισμός του πληροφοριακού συστήματος και στην υποενότητα 2.3 τα συστατικά του πληροφοριακού συστήματος.

## 2.2. Ορισμός Πληροφοριακού Συστήματος

«Πληροφοριακό σύστημα ονομάζεται ένα σύνολο διαδικασιών, ανθρώπινου δυναμικού και αυτοματοποιημένων υπολογιστικών συστημάτων, που προορίζονται για τη συλλογή, εγγραφή, ανάκτηση, επεξεργασία, αποθήκευση και ανάλυση πληροφοριών. Τα συστήματα αυτά μπορούν να περιλαμβάνουν λογισμικό, υλικό και τηλεπικοινωνιακό σκέλος.» (1)

## 2.3.Συστατικά Πληροφοριακού Συστήματος

Το πληροφοριακό σύστημα αποτελείται από πέντε συστατικά στοιχεία, τα οποία συνεργάζονται μεταξύ τους έτσι ώστε να επιτευχθεί ο στόχος του πληροφοριακού συστήματος. Τα πέντε, αυτά, συστατικά στοιχεία είναι:

1.οι άνθρωποι

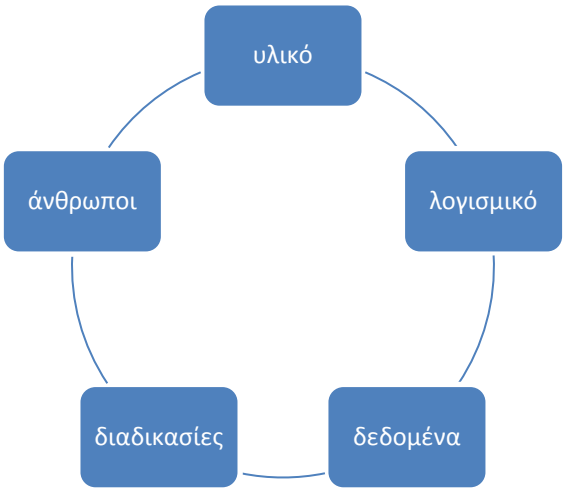
2.το υλικό (hardware)

3.οι διαδικασίες (procedures)

4.το λογισμικό ( software)

5.τα δεδομένα (data)

Εικόνα 1.Συστατικά Πληροφοριακού Συστήματος **(2)**




### 2.3.1. Υλικό

Το υλικό είναι ένα μέρος των πληροφοριακών συστημάτων που μπορούμε να αγγίξουμε. Περιλαμβάνει ψηφιακές συσκευές, όπως:

- επιτραπέζιους υπολογιστές
- φορητούς υπολογιστές
- κινητά τηλέφωνα
- συσκευές αποθήκευσης
- συσκευές εισόδου, όπως ποντίκια, πληκτρολόγια, σαρωτές
- συσκευές εξόδου, όπως εκτυπωτές και ηχεία

### 2.3.2. Λογισμικό

Το λογισμικό ορίζεται ως το σύνολο των οδηγιών που λένε στο υλικό τι πρέπει να κάνει. Δημιουργείται μέσω της διαδικασίας του προγραμματισμού. Χάρη στο λογισμικό, το υλικό γίνεται λειτουργικό.

Το λογισμικό μπορεί να χωριστεί σε δύο κατηγορίες: τα λειτουργικά συστήματα και το λογισμικό εφαρμογών.

**Λειτουργικά Συστήματα**

Τα λειτουργικά συστήματα διαχειρίζονται το υλικό και δημιουργούν την επαφή του με τον χρήστη. Οι βασικές τους λειτουργίες είναι:

- η διαχείριση των πόρων υλικού του υπολογιστή
- η παροχή των στοιχείων επαφής του χρήστη
- η παροχή μιας πλατφόρμας στους προγραμματιστές λογισμικού, έτσι ώστε να κατασκευάζουν εφαρμογές.

**Λογισμικό εφαρμογών**

Το λογισμικό εφαρμογών είναι η κατηγορία των προγραμμάτων που κάνουν επιτρέπουν στον χρήστη να επιτύχει έναν στόχο του. Το σύνολο των εφαρμογών λογισμικού που χρησιμοποιούνται στον εργασιακό χώρο και επιτρέπουν στους υπαλλήλους των γραφείων να ολοκληρώνουν την εργασία τους ονομάζεται «λογισμικό παραγωγικότητας». Κάποιες βασικές κατηγορίες του λογισμικού παραγωγικότητας είναι:

- η επεξεργασία λέξεων: Αυτή η κατηγορία προβλέπει τη δημιουργία γραπτών εγγράφων.
- το υπολογιστικό φύλλο: Βοηθάει στους αριθμητικούς υπολογισμούς και στην αριθμητική ανάλυση.
- η παρουσίαση: Βοηθάει στη δημιουργία διαφανειών παρουσίασης.
- άλλα είδη λογισμικού: Όπως είναι πακέτα ηλεκτρονικού ταχυδρομείου, εργαλεία συνεργασίας για τη συλλογή πληροφοριών και πακέτα βάσης δεδομένων.

### 2.3.3. Δεδομένα

Τα δεδομένα είναι τα ακατέργαστα κομμάτια των πληροφοριών που δεν έχουν κανένα πλαίσιο. Υπάρχουν δύο κατηγορίες δεδομένων, τα ποσοτικά δεδομένα και τα ποιοτικά δεδομένα. Τα ποσοτικά δεδομένα είναι αριθμητικά, αποτέλεσμα

μέτρησης ή κάποιου άλλου μαθηματικού υπολογισμού. Τα ποιοτικά δεδομένα είναι περιγραφικά.

**Τύποι δεδομένων**

Τα δεδομένα μπορούν να εμφανιστούν σε διάφορες μορφές, οι οποίες παρουσιάζονται παρακάτω:

- Κείμενο: Ως κείμενο εμφανίζονται συνήθως μη αριθμητικά δεδομένα, τα οποία αποτελούν λιγότερους από 256 χαρακτήρες.
- Αριθμός: Με τη μορφή αριθμού εμφανίζονται τα αριθμητικά δεδομένα.
- Ναι/όχι: Κατατάσσεται στα αριθμητικά δεδομένα και αποτυπώνεται με ένα byte. Συνήθως, χρησιμοποιείται το «0» για το «όχι» ή «ψεύτικο» και το 1 για το «ναι» ή «αληθινό».
- Ημερομηνία/ώρα: Θεωρείται αριθμητικό δεδομένο και ερμηνεύεται συνήθως ως αριθμός ή χρόνος.
- Νόμισμα: Αποτελεί μορφή αριθμητικών δεδομένων.
- Κείμενο παραγράφου: Επιτρέπει κείμενο το οποίο είναι μεγαλύτερο από 256 χαρακτήρες.
- Αντικείμενο: Αυτός ο τύπος δεδομένων επιτρέπει εισαγωγή στοιχείων που δεν μπορούν να εισαχθούν με το πληκτρολόγιο, όπως είναι οι εικόνες ή τα αρχεία μουσικής.

### 2.3.4 Διαδικασίες

Η διαδικασία είναι μία σειρά εργασιών που ολοκληρώνονται με σκοπό την επίτευξη του στόχου. Αντίστοιχα, σε μία επιχείρηση οι διαδικασίες έχουν στόχο την επίτευξη του στόχου της επιχείρησης. Επομένως, όσο καλύτερες είναι οι διαδικασίες, τόσο πιο αποτελεσματική είναι η επιχείρηση. Οι διαδικασίες μπορεί να είναι απλές ή περίπλοκες. Όταν μία διαδικασία είναι περίπλοκη, τότε πρέπει να τεκμηριώνεται. Ο απλούστερος τρόπος τεκμηρίωσης μιας διαδικασίας είναι η δημιουργία μιας λίστας, όπου θα καταγράφονται αναλυτικά όλα τα βήματα της διαδικασίας.

### 2.3.5 Άνθρωποι

Η τελευταία συνιστώσα του πληροφοριακού συστήματος είναι οι άνθρωποι. Μία ομάδα ανθρώπων διαδραματίζει σημαντικό ρόλο στο σχεδιασμό, την ανάπτυξη και την εγκαθίδρυση των πληροφοριακών συστημάτων. Μία άλλη ομάδα ατόμων ασχολείται με την καθημερινή λειτουργία και διοίκηση της πληροφορικής. Τέλος, υπάρχουν κάποια άτομα που αναλαμβάνουν τη διαχείριση των πληροφοριακών συστημάτων.

Η πρώτη ομάδα, η οποία αποτελεί τους δημιουργούς των πληροφοριακών συστημάτων, περιλαμβάνει τα παρακάτω επαγγέλματα:

- Αναλυτής συστημάτων: Ο αναλυτής θα πρέπει να έχει καλή γνώση της επιχείρησης και των επιχειρηματικών διαδικασιών που εμπλέκονται, καθώς και να έχει την ικανότητα να τεκμηριώνει αυτές τις διαδικασίες. Ο ρόλος του είναι να εντοπίσει τις επιχειρησιακές ανάγκες και να παρέχει τις λεπτομέρειες που απαιτούνται για να δημιουργηθεί ένα νέο ή να επανασχεδιασθεί ένα παλιό πληροφοριακό σύστημα, έτσι ώστε να καλυφθούν οι ανάγκες.
- Προγραμματιστής: Ο ρόλος του προγραμματιστή είναι να εκπληρώσει τις προδιαγραφές σχεδιασμού που έχουν δοθεί από τον αναλυτή συστημάτων.
- Μηχανικός υπολογιστών: Οι μηχανικοί υπολογιστών σχεδιάζουν τις συσκευές υπολογιστών που χρησιμοποιούμε καθημερινά.

Η δεύτερη ομάδα, η οποία ασχολείται με τη λειτουργία και διοίκηση των πληροφοριακών συστημάτων, αποτελείται από τα εξής επαγγέλματα:

- Χειριστής υπολογιστή: Ο ρόλος του είναι να επιβλέπει τους κεντρικούς υπολογιστές και τα κέντρα δεδομένων στους οργανισμούς. Στα καθήκοντά τους περιλαμβάνονται η ενημέρωση των λειτουργικών συστημάτων, η διασφάλιση διαθέσιμης μνήμης και χώρου αποθήκευσης και η επίβλεψη του φυσικού περιβάλλοντος του υπολογιστή.
- Διαχειριστής βάσης δεδομένων: Αυτό το άτομο διαχειρίζεται τις βάσεις δεδομένων. Δημιουργεί και διατηρεί, δηλαδή, βάσεις δεδομένων που χρησιμοποιούνται είτε ως μέρος των εφαρμογών είτε για την αποθήκη δεδομένων. Επίσης, συνεργάζεται με τον αναλυτή συστημάτων και τον

προγραμματιστή όταν κάποιο έργο απαιτεί πρόσβαση ή δημιουργία βάσης δεδομένων.

- Αναλυτής βοηθού γραφείου/ Αναλυτής υποστήριξης: Ο βοηθός γραφείου παρέχει πληροφορίες και υποστήριξη στους χρήστες υπολογιστών που δουλεύουν σ' έναν οργανισμό. Σε περίπτωση που ένας βοηθός γραφείου δεν μπορεί να αντιμετωπίσει ένα ζήτημα, συνεργάζεται με τον αναλυτή υποστήριξης για να ερευνήσουν και να επιλύσουν το πρόβλημα.
- Εκπαιδευτής πληροφορικής: Αυτό το άτομο παραδίδει μαθήματα για να μάθει στους χρήστες υπολογιστών συγκεκριμένες δεξιότητες πληροφορικής.

Η Τρίτη ομάδα, η οποία σχετίζεται με τη διαχείριση των πληροφοριακών συστημάτων, αποτελείται από τις παρακάτω ομάδες επαγγελμάτων:

- Επικεφαλής της πληροφορικής: Ο ρόλος αυτού του ατόμου είναι να ευθυγραμμίζει τα σχέδια και τις λειτουργίες των πληροφοριακών συστημάτων με τους στρατηγικούς στόχους του οργανισμού. Δηλαδή, κάποια από τα καθήκοντά του είναι ο προϋπολογισμός, ο στρατηγικός σχεδιασμός και οι αποφάσεις του προσωπικού για τη λειτουργία των πληροφοριακών συστημάτων. Επίσης, συνεργάζεται με τους ηγέτες των άλλων τμημάτων του οργανισμού για να εξασφαλιστεί η ομαλή επικοινωνία και ο προγραμματισμός.
- Λειτουργικός διαχειριστής: Καθώς η οργάνωση των πληροφοριακών συστημάτων γίνεται όλο και πιο μεγάλη και περίπλοκη, οι λειτουργίες τους ομαδοποιούνται και ελέγχονται από το λειτουργικό διαχειριστή.
- Διευθυντής έργων: Αυτό το άτομο είναι υπεύθυνο για την έγκαιρη τήρηση των έργων. Γι' αυτό το λόγο, συνεργάζεται με τους ενδιαφερόμενους του έργου έτσι ώστε να κρατάει την ομάδα οργανωμένη και να γνωστοποιεί τη θέση του έργου στη διοίκηση.
- Υπεύθυνος ασφάλειας πληροφοριών: Σκοπός του είναι να προστατέψει τις πληροφορίες από εσωτερικές και εξωτερικές απειλές. Για το λόγο αυτό, είναι υπεύθυνος για τον καθορισμό πολιτικής ασφάλειας των πληροφοριών και για τον έλεγχο εφαρμογής της. (2)

# ΚΕΦΑΛΑΙΟ 3. ΠΛΗΡΟΦΟΡΙΑΚΑ ΣΥΣΤΗΜΑΤΑ ΝΟΣΟΚΟΜΕΙΩΝ

## 3.1. Εισαγωγή κεφαλαίου 3

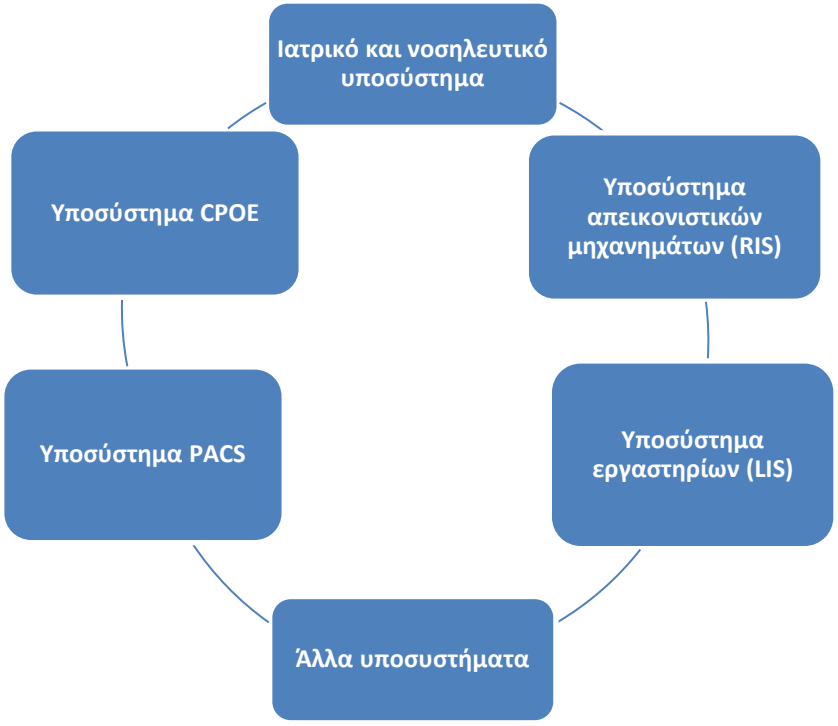
Η σύγχρονη υγειονομική περίθαλψη στηρίζεται στη μετάδοση της πληροφορίας μέσα σε ένα ίδρυμα αλλά και μεταξύ διαφορετικών ιδρυμάτων. Η μετάδοση της πληροφορίας γίνεται μέσω υπολογιστών που έχουν ως στόχο τη βελτίωση της παροχής πληροφοριών στο χώρο της υγείας. Οποιοδήποτε πρόβλημα στη λειτουργία αυτών των υπολογιστών θα μπορούσε να οδηγήσει σε διακοπή της μετάδοσης των πληροφοριών και κατ' επέκταση σε διατάραξη της λειτουργίας του ιδρύματος. Στην υποενότητα 3.2 αναφέρονται τα υποσυστήματα των Πληροφοριακών Συστημάτων των Νοσοκομείων, στην υποενότητα 3.3 οι λόγοι εισαγωγής και η αναγκαιότητα ύπαρξης των Πληροφοριακών Συστημάτων στα νοσοκομεία και στην υποενότητα 3.4 τα οφέλη που προκύπτουν από την εισαγωγή των Πληροφοριακών Συστημάτων στο χώρο της Υγείας.

## 3.2. Υποσυστήματα πληροφοριακών συστημάτων νοσοκομείων

Τα Πληροφοριακά Συστήματα Νοσοκομείων διακρίνονται στα παρακάτω υποσυστήματα:

1. Ιατρικό και Νοσηλευτικό υποσύστημα
2. Υποσύστημα εργαστηρίων (LIS)
3. Υποσύστημα απεικονιστικών μηχανημάτων (RIS)
4. Υποσύστημα PACS
5. Υποσύστημα CPOE
6. Διαχειριστικό υποσύστημα
7. Άλλα υποσυστήματα

Εικόνα 2. Υποσυστήματα Πληροφοριακών Συστημάτων Νοσοκομείων **(3)**




### 3.2.1. Ιατρικό και νοσηλευτικό υποσύστημα

Διαχειρίζεται τον ιατρικό φάκελο των ασθενών και τα ιατρικά και νοσηλευτικά πρωτόκολλα.

### 3.2.2. Υποσύστημα εργαστηρίων (LIS)

Διαχειρίζεται τα δεδομένα και τα αποτελέσματα που σχετίζονται με τους διάφορους αναλυτές που χρησιμοποιούνται στα νοσοκομεία.

### 3.2.3. Υποσύστημα απεικονιστικών μηχανημάτων (RIS)

Διαχειρίζεται τα ακτινοδιαγνωστικά μηχανήματα (π.χ. αξονικός/ μαγνητικός τομογράφος) και την εξαγωγή των αποτελεσμάτων των ακτινοδιαγνωστικών εξετάσεων.

### 3.2.4. Υποσύστημα PACS

Διαχειρίζεται τις εικόνες των ακτινοδιαγνωστικών εξετάσεων των ασθενών.

### 3.2.5. Υποσύστημα CPOE

Διαχειρίζεται την εισαγωγή ιατρικών εντολών.

### 3.2.6. Διαχειριστικό υποσύστημα

Μπορεί να ασχοληθεί με τη διαχείριση αποθηκών, υλικού, προσωπικού, παραγγελιών.

### 3.2.7. Άλλα υποσυστήματα

Ασχολείται με τη διαχείριση ειδικών αναγκών του νοσοκομείου, όπως με τη διαχείριση κίνησης ασθενοφόρου. (3)

## 3.3.Λόγοι εισαγωγής πληροφοριακών συστημάτων στα νοσοκομεία-Αναγκαιότητα ύπαρξης

Η αναγκαιότητα ύπαρξης ενός ολοκληρωμένου πληροφοριακού συστήματος στα νοσοκομεία είναι αποτέλεσμα τόσο της εξέλιξης της τεχνολογίας στο χώρο της υγείας όσο και των σύγχρονων απαιτήσεων των νοσοκομείων.

Η τεχνολογία, στις μέρες μας, συμβάλλει στην οργάνωση, διαχείριση και καταχώρηση των πληροφοριών και δεδομένων, έτσι ώστε να επιτυγχάνεται σωστή καταγραφή των εξελίξεων και προγραμματισμός.

Όσον αφορά τα σύγχρονα νοσοκομεία, οι απαιτήσεις που έχουν σχετίζονται με τον έλεγχο των δαπανών, τη διαμόρφωση ενός σχεδιασμένου και ορθολογικού προγραμματισμού για μελλοντικές ενέργειες και την αξιολόγηση της αποτελεσματικότητας των υφιστάμενων λειτουργιών. (4)

## 3.4. Οφέλη εισαγωγής πληροφοριακών συστημάτων στον τομέα της υγείας

Η εισαγωγή πληροφοριακών συστημάτων στον τομέα της υγείας βοηθάει τόσο στη βελτίωση του τρόπου λειτουργίας των μονάδων υγείας όσο και στη βελτίωση των παρεχόμενων υπηρεσιών. Πιο αναλυτικά, επιτυγχάνεται:

- Αναβάθμιση των παρεχόμενων υπηρεσιών για τους χρήστες των υπηρεσιών υγείας. Σ' αυτό συμβάλλουν:
  - Η εισαγωγή του ηλεκτρονικού φακέλου του ασθενούς.
  - Η δυνατότητα πρόσβασης σε παλαιότερα αρχεία του ασθενή και η αναδρομή στο ιστορικό του.
  - Η μείωση της γραφειοκρατίας.
  - Η ελαχιστοποίηση των λαθών.
  - Η βελτίωση της πληροφόρησης και η ταχύτητα εξυπηρέτησης των χρηστών υπηρεσιών υγείας.
- Περιορισμός των χειρόγραφων διαδικασιών και βελτίωση του εργασιακού περιβάλλοντος. Σ' αυτό συμβάλλουν:
  - Η αυτοματοποίηση των διαδικασιών.
  - Η διασύνδεση των επιμέρους συστημάτων σε ένα πλήρες σύστημα.
  - Η βελτίωση του εσωτερικού εργασιακού περιβάλλοντος.
  - Η αποτελεσματικότητα των καθημερινών διεργασιών.
  - Η ορθή αξιοποίηση του ανθρώπινου δυναμικού.
  - Η αξιοποίηση των σύγχρονων μορφών τεχνολογίας.
- Ελαχιστοποίηση του κόστους περίθαλψης του ασθενή. Σ' αυτό συμβάλλουν:
  - Ο έλεγχος των πόρων που χρησιμοποιούνται στα νοσοκομεία μέσω των συνεχών ελέγχων ανάλωσης υλικού και των αυτοματοποιημένων διαδικασιών.
  - Η αποφυγή άσκοπων ιατρικών πράξεων.
- Παροχή χρήσιμων πληροφοριών, όπως ο μέσος χρόνος νοσηλείας, η πληρότητα, το κόστος νοσηλείας ανά διάγνωση, στη διοίκηση του νοσοκομείου.
- Έλεγχος των διαφορετικών πολιτικών οργάνωσης της παροχής υγείας, κοστολόγησης και τιμολόγησης των υπηρεσιών της. (5)

# ΚΕΦΑΛΑΙΟ 4. ΚΙΝΔΥΝΟΙ ΚΑΙ ΑΠΕΙΛΕΣ

## 4.1. Εισαγωγή κεφαλαίου 4

Όταν χρησιμοποιούνται πληροφοριακά συστήματα στο χώρο του νοσοκομείου, ενέχουν κάποιοι κίνδυνοι τόσο για τον ίδιο τον εξοπλισμό των Πληροφοριακών Συστημάτων όσο και για τα ιατρικά δεδομένα που αποθηκεύονται σ' αυτά. Αυτό συμβαίνει κυρίως λόγω των πολλών χρηστών που έχουν πρόσβαση σε στοιχεία που επηρεάζουν τη λειτουργία, τη δομή, τις χρεώσεις και την απόδοση του δικτύου, αλλά και λόγω της γεωγραφικής θέσης που βρίσκονται αποθηκευμένα τα Πληροφοριακά Συστήματα. Υπάρχουν διάφορες κατηγορίες κινδύνων που σχετίζονται με τα Πληροφοριακά Συστήματα, οι οποίες αναφέρονται στην υποενότητα 4.2, καθώς και σωστή διαδικασία για την αξιολόγησή τους που αναλύεται στην υποενότητα 4.3.

## 4.2. Κατηγορίες κινδύνων

### 4.2.1. Φυσικές απειλές

Οι φυσικές απειλές, οι πλημμύρες και οι σεισμοί, σχετίζονται άμεσα με τις κτιριακές υποδομές των νοσοκομείων και έμμεσα με τα πληροφοριακά συστήματα που στεγάζονται σ' αυτά.

### 4.2.2. Ανθρώπινες απειλές

Οι άνθρωποι μπορεί να προκαλέσουν ζημιά στο λογισμικό των πληροφοριακών συστημάτων των νοσοκομείων είτε λόγω ανταγωνισμού είτε για προσωπικούς λόγους. Μπορεί να είναι είτε άτομα που δουλεύουν σε αντίπαλο οργανισμό είτε άτομα που αποτελούν προσωπικό του ίδιου νοσοκομείου.

### 4.2.3. Κίνδυνοι τεχνολογίας

Κάποιες φορές κρίνεται απαραίτητη η εισαγωγή νέων συστημάτων σ' έναν οργανισμό προκειμένου να επιτεύξει τους στόχους τους οποίους έχει θέσει. Οι

κίνδυνοι τεχνολογίας μπορεί να προκύψουν είτε από τη μη σωστή λειτουργία των νέων συστημάτων είτε από τον μη κατάλληλο εξοπλισμό τους.

### 4.2.4. Θεσμικό- Φυσικό περιβάλλον του έργου

«Θεσμικό περιβάλλον του έργου» ονομάζονται όλοι αυτοί οι θεσμοί που πρέπει να αναπτύξει και να εφαρμόσει το πληροφοριακό σύστημα του νοσοκομείου ώστε να πειθαρχεί με αυτούς. Οποιαδήποτε παρέκκλιση από αυτούς μπορεί να επιφέρει κυρώσεις, οι οποίες θα οδηγήσουν σε οικονομικές ζημίες ή χάσιμο χρόνου.

«Φυσικό περιβάλλον του έργου» ονομάζονται οι εγκαταστάσεις μέσα στις οποίες στεγάζονται τα πληροφοριακά συστήματα της οργανισμού. Εάν οι εγκαταστάσεις είναι παλιές, μπορεί να υπάρχει πρόβλημα στην παροχή ηλεκτρισμού, το οποίο μπορεί να επιφέρει ζημιά στο λογισμικό και στον εξοπλισμό των πληροφοριακών συστημάτων.

### 4.2.5. Επιχειρησιακοί κίνδυνοι

Οι επιχειρησιακοί κίνδυνοι αναφέρονται στους κινδύνους που σχετίζονται με την αδυναμία προσάρτησης της τεχνολογίας σ’ έναν οργανισμό. Αυτό έχει σαν αποτέλεσμα την αδυναμία λειτουργίας του πληροφοριακού συστήματος.

### 4.2.6. Κίνδυνοι οργάνωσης του έργου

Οι κίνδυνοι αυτοί αφορούν τα άτομα που ασχολούνται με το σχεδιασμό και την υλοποίηση του έργου. Εάν δεν υπάρχουν η κατάλληλη εκπαίδευση, οι γνώσεις και η σωστή λήψη αποφάσεων, είναι δυνατόν να επέλθουν οικονομικά προβλήματα και χρονικές καθυστερήσεις στον οργανισμό. (6)

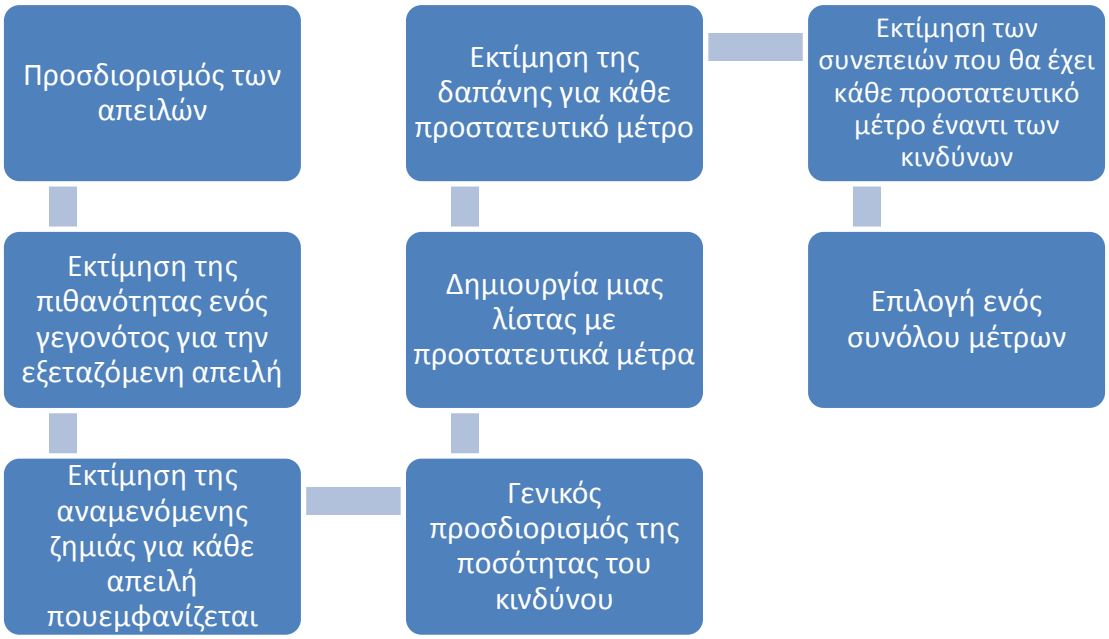
## 4.3. Αξιολόγηση κινδύνων

Η αξιολόγηση των παραπάνω κινδύνων περιλαμβάνει διάφορες φάσεις:

- Προσδιορισμός των απειλών: Θα πρέπει να υπάρχει μία λίστα με τις συχνότερες απειλές στα Πληροφοριακά Συστήματα. Όταν κάποιες απειλές δεν υπάρχουν στη συγκεκριμένη περίπτωση (π.χ. σεισμοί) μπορούν να διαγραφούν εντελώς από τη λίστα.

- Εκτίμηση της πιθανότητας ενός γεγονότος για την εξεταζόμενη απειλή: Όλες οι απειλές δεν εμφανίζονται με την ίδια συχνότητα. Άλλες απειλές είναι πιο συχνές και άλλες πιο σπάνιες. Για να μπορέσει να καθοριστεί η πιθανότητα εμφάνισης κάποιας απειλής, πρέπει να καθοριστούν συγκεκριμένες συχνότητες και να αντιστοιχηθούν στις απειλές.
- Εκτίμηση της αναμενόμενης ζημιάς για κάθε απειλή που εμφανίζεται.
- Γενικός προσδιορισμός της ποσότητας του κινδύνου σχετιζόμενης μιας απειλής με τον πολλαπλασιασμό της πιθανότητας και της αναμενόμενης ζημίας απ' αυτήν την απειλή.
- Δημιουργία μιας λίστας με προστατευτικά μέτρα.
- Εκτίμηση της δαπάνης για κάθε προστατευτικό μέτρο που περιλαμβάνεται στην παραπάνω λίστα. Οι δαπάνες μπορούν να σχετίζονται με τον επιπρόσθετο εξοπλισμό που θα χρησιμοποιηθεί για περαιτέρω προστασία, επιπρόσθετο λογισμικό, φυσικές παροχές, υπερωρίες των ατόμων που εργάζονται στο τμήμα της Πληροφορικής για να διασφαλίσουν την προστασία των συστημάτων .
- Εκτίμηση των συνεπειών που θα έχει κάθε προστατευτικό μέτρο έναντι των κινδύνων.
- Επιλογή ενός συνόλου μέτρων: Θα πρέπει να γίνει σωστός συνδυασμός προστατευτικών μέτρων, έτσι ώστε να μην επηρεάζονται αρνητικά όταν συνδυάζονται και να μην είναι δαπανηρά. (7)

Εικόνα 3. Διαδικασία αξιολόγησης κινδύνων **(7)**




# ΚΕΦΑΛΑΙΟ 5.ΕΙΣΒΟΛΕΙΣ

## 5.1. Εισαγωγή κεφαλαίου 5

Οι εισβολείς είναι άτομα, τα οποία επιθυμούν να αποκτήσουν πρόσβαση στα αρχεία των Πληροφοριακών Συστημάτων χωρίς να είναι εξουσιοδοτημένα. Σχεδιάζουν συχνά επιθέσεις στα Πληροφοριακά Συστήματα, γι' αυτό πρέπει τα συστήματα να παρακολουθούνται έτσι ώστε να ανιχνεύονται και να καταγράφονται όλες οι προσπάθειες για παραβίαση της ασφάλειας, είτε αυτές ήταν επιτυχείς είτε ανεπιτυχείς. Στην υποενότητα 5.2 αναφέρονται οι λόγοι που τα Πληροφοριακά Συστήματα δέχονται επιθέσεις από εισβολείς, στην υποενότητα 5.3 αναλύεται η αρχιτεκτονική του συστήματος ανίχνευσης εισβολών και στην υποενότητα 5.4 πώς γίνεται ο σωστός χειρισμός των εισβολών.

## 5.2. Λόγοι επιθέσεων από εισβολείς

Οι εισβολείς μπορούν να σχεδιάσουν επίθεση, κυρίως όταν:

- Οι ενέργειες και διεργασίες των χρηστών δεν είναι στατιστικά προβλέψιμες.
- Οι ενέργειες και διεργασίες των χρηστών περιλαμβάνουν ακολουθίες εντολών που να υπονομεύουν την πολιτική ασφαλείας του συστήματος.
- Οι ενέργειες των διεργασιών δε συμμορφώνονται με κάποιες συγκεκριμένες προδιαγραφές, οι οποίες περιγράφουν επιτρεπτές ενέργειες.

## 5.3. Αρχιτεκτονική Συστήματος Ανίχνευσης Εισβολών

Το σύστημα ανίχνευσης εισβολών μπορεί να θεωρηθεί και ως ένα σύστημα το οποίο παρακολουθεί και ελέγχει συνεχώς τα Πληροφοριακά Συστήματα. Αποτελείται από τρία μέρη:

- Τον αντιπρόσωπο (agent)
- Το διευθυντή (director)
- Τον αγγελιοφόρο (notifier)

Ο Αντιπρόσωπος:

Ο αντιπρόσωπος συλλέγει τα στοιχεία από ένα αρχείο καταγραφής, κάποια άλλη διεργασία ή ένα δίκτυο υπολογιστών. Αυτά τα στοιχεία τα στέλνει στο διευθυντή. Όμως, συνήθως πριν αποστείλει αυτά τα αρχεία στον διευθυντή, τα μορφοποιεί ως ένα βαθμό και αφαιρεί πληροφορίες που δε θεωρεί απαραίτητες. Αν ο διευθυντής κρίνει ότι οι πληροφορίες είναι ελλιπείς και χρειάζεται περισσότερες πληροφορίες από κάποια πηγή, τότε ο αντιπρόσωπος πρέπει να συλλέξει αυτά τα στοιχεία.

Ο διευθυντής:

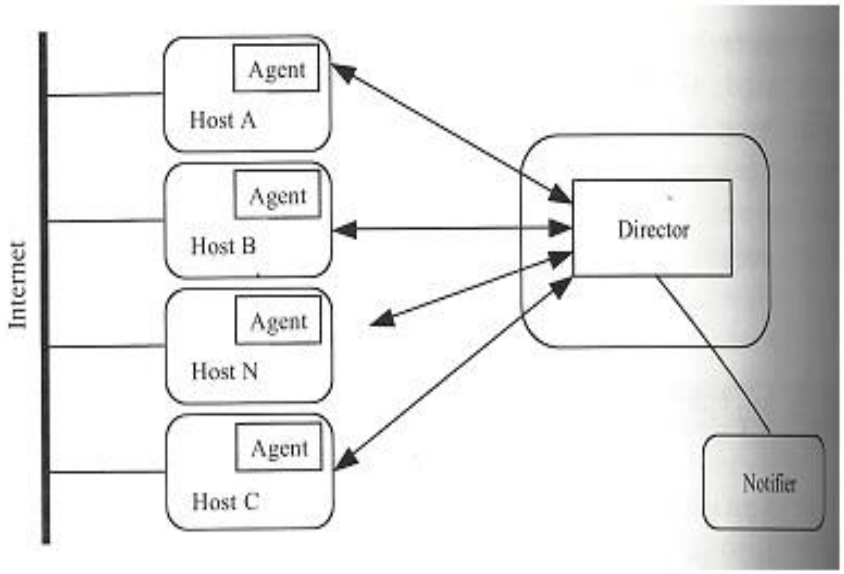
Ο διευθυντής λαμβάνει τα στοιχεία που έχει συλλέξει ο αντιπρόσωπος. Έπειτα, κρίνει ποιες πληροφορίες είναι περιττές ή αλληλεπικαλύπτονται και κάνει τις απαραίτητες μορφοποιήσεις. Έχει τη δυνατότητα, επίσης, με μία μηχανή ανάλυσης

να εξετάσει αν μια επίθεση από εισβολείς βρίσκεται σε εξέλιξη. Οι επιτιθέμενοι είναι δύσκολο να ξεφύγουν από το σύστημα ανίχνευσης εισβολών, καθώς δεν έχουν τις απαραίτητες γνώσεις.

Ο Αγγελιοφόρος:

Ο αγγελιοφόρος λαμβάνει τις πληροφορίες που του στέλνει ο διευθυντής. Έπειτα, επικοινωνεί με τους αρμόδιους φορείς για να τους ενημερώσει αν μία επίθεση βρίσκεται σε εξέλιξη ή εκτελεί από μόνος του κάποιες ενέργειες για να απαντήσει στην επίθεση. Αν το κρίνει απαραίτητο, μπορεί να ζητήσει από τους αντιπροσώπους να συλλέξουν επιπρόσθετα στοιχεία.

**Εικόνα 4. Αρχιτεκτονική ενός συστήματος ανίχνευσης εισβολών (8)**



## 5.4. Χειρισμός εισβολών

Όταν γίνεται μία εισβολή σε ένα Πληροφοριακό Σύστημα, τότε το σύστημα πρέπει να επανεξετάσει τη συμμόρφωσή του με την πολιτική ασφαλείας και να αντιμετωπίσει τους εισβολείς.. Συνήθως, ο χειρισμός των εισβολών λαμβάνει χώρα σε τρεις φάσεις:

- Η φάση του περιορισμού: Σε αυτή τη φάση, σκοπός είναι να προκληθεί όσο λιγότερη ζημιά γίνεται στο σύστημα. Ως «ζημιά» αναφέρεται οποιαδήποτε παρέκκλιση του συστήματος από την πολιτική ασφαλείας. Αυτό επιτυγχάνεται είτε μέσω του περιορισμού της πρόσβασης είτε μέσω παθητικής παρακολούθησης της επίθεσης. Με την παθητική παρακολούθηση της επίθεσης δεν υπάρχει παρέμβαση στην επίθεση. Οι παρακολουθητές απλώς παρατηρούν τα βήματα που ακολουθούν οι εισβολείς για να κάνουν την επίθεσή τους και βάσει αυτών μπορούν να συμπεράνουν το στόχο της επίθεσης. Όσον αφορά τον περιορισμό της πρόσβασης, σκοπός είναι να περιοριστεί η περιοχή προστασίας του επιτιθέμενου για να έχει λιγότερες πιθανότητες να επιτύχει το στόχο του. Όμως, οι υπεύθυνοι ασφαλείας μπορεί να μη γνωρίζουν τις πληροφορίες που θέλει να συλλέξει ο επιτιθέμενος και να γίνει λανθασμένος περιορισμός της πρόσβασης, με αποτέλεσμα οι πληροφορίες που χρειάζεται ο επιτιθέμενος να βρίσκονται μέσα στην περιοχή που έχει πρόσβαση.
- Η φάση της εξουδετέρωσης: Στη φάση της εξουδετέρωσης γίνεται πλήρης διακοπή της επίθεσης, είτε με πλήρη διακοπή της πρόσβασης στο σύστημα είτε με αναγκαστικό τερματισμό όλων των λειτουργιών που σχετίζονται με την επίθεση. Αυτή η φάση εμποδίζει την επανέναρξη παρόμοιων επιθέσεων.
- Η φάση της συνεχούς παρακολούθησης: Αυτή η φάση περιλαμβάνει μέτρα κατά του επιτιθέμενου αλλά εκτός του συστήματος. Συνήθως τίθενται κάποιοι νόμοι έναντι των επιτιθέμενων που ποικίλλουν από χώρα σε χώρα ή μέσα στην ίδια χώρα με την πάροδο του χρόνου. Στη φάση αυτή, χρησιμοποιούνται κυρίως δύο τεχνικές ανίχνευσης, η τεχνική αποτυπωμάτων και η εξέταση δημιουργίας μιας IP επικεφαλίδας. Με βάση την τεχνική αποτυπωμάτων, κάποιος υπεύθυνος ασφάλειας παρακολουθεί

τα βήματα που έχει ακολουθήσει κάποιος επιτιθέμενος μέχρι να φτάσει στον τελικό του στόχο. Συνήθως, οι επιτιθέμενοι περνούν από διάφορους υπολογιστές μέχρι να φτάσουν στο στόχο τους και ακολουθούν παρόμοιες συνδέσεις σ' όλες τις επιθέσεις τους. Έτσι, είναι εύκολο να βρεθεί η αλυσίδα των υπολογιστών που συμμετέχουν στις συνδέσεις. Όσον αφορά την τεχνική της δημιουργίας μιας IP επικεφαλίδας, επιλέγονται τα πακέτα που θα σημειωθούν και έπειτα τοποθετείται σήμανση σ' αυτά. Τα πακέτα επιλέγονται ή με κάποια δεδομένη πιθανότητα (πιθανολογική επιλογή) ή με βάση έναν αιτιοκρατικό μη τυχαίο αλγόριθμο (αιτιοκρατική επιλογή). Η σήμανση των πακέτων γίνεται ή εσωτερικά, δηλαδή στην επικεφαλίδα των πακέτων χωρίς σήμανση, ή με επέκταση, δηλαδή στην επεκταμένη επικεφαλίδα των πακέτων. (8)

# ΚΕΦΑΛΑΙΟ 6. ΒΑΣΙΚΕΣ ΕΝΝΟΙΕΣ ΑΣΦΑΛΕΙΑΣ ΠΛΗΡΟΦΟΡΙΑΚΩΝ ΣΥΣΤΗΜΑΤΩΝ

## 6.1.Εισαγωγή κεφαλαίου 6

Όπως προκύπτει από τα Κεφάλαια 4 και 5, τα Πληροφοριακά Συστήματα έρχονται καθημερινά σε επαφή με πολλούς κινδύνους, συμπεριλαμβανομένων των επιθέσεων από εισβολείς. Προκειμένου να μπορέσει να αναλυθεί η επικινδυνότητα των κινδύνων καθώς και να αναπτυχθούν μέτρα περιορισμού τους, πρέπει πρώτα να κατανοήσουμε την έννοια της ασφάλειας και το ρόλο που παίζει σ' ένα Πληροφοριακό Σύστημα. Στο κεφάλαιο αυτό, ορίζεται η ασφάλεια του Πληροφοριακού Συστήματος στην υποενότητα 6.2, αναφέρονται οι βασικές έννοιες της ασφάλειας στην υποενότητα 6.3, οι βασικές αρχές ασφάλειας των Πληροφοριακών Συστημάτων στην υποενότητα 6.4, οι κύριες ομάδες ασφάλειας και ο στόχος τους στην υποενότητα 6.5 και τέλος ο ρόλος της ασφάλειας κατά τη διάρκεια του κύκλου ζωής του συστήματος.

## 6.2. Ορισμός ασφάλειας Πληροφοριακών Συστημάτων

«Η ασφάλεια πληροφοριακών συστημάτων, ασφάλεια υπολογιστικών συστημάτων ή ασφάλεια υπολογιστών είναι ένα γνωστικό πεδίο της επιστήμης της πληροφορικής, και ειδικότερα του κλάδου των υπολογιστικών συστημάτων, 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.»

## 6.3. Έννοιες

Για να είναι ένα πληροφοριακό σύστημα ασφαλές, πρέπει να διακατέχεται από 3 αρχές:

- Εμπιστευτικότητα
- Ακεραιότητα
- Διαθεσιμότητα

### 6.3.1. Εμπιστευτικότητα

Η εμπιστευτικότητα είναι η αρχή, βάση της οποίας οι ευαίσθητες πληροφορίες δεν αποκαλύπτονται σε μη εξουσιοδοτημένα άτομα.

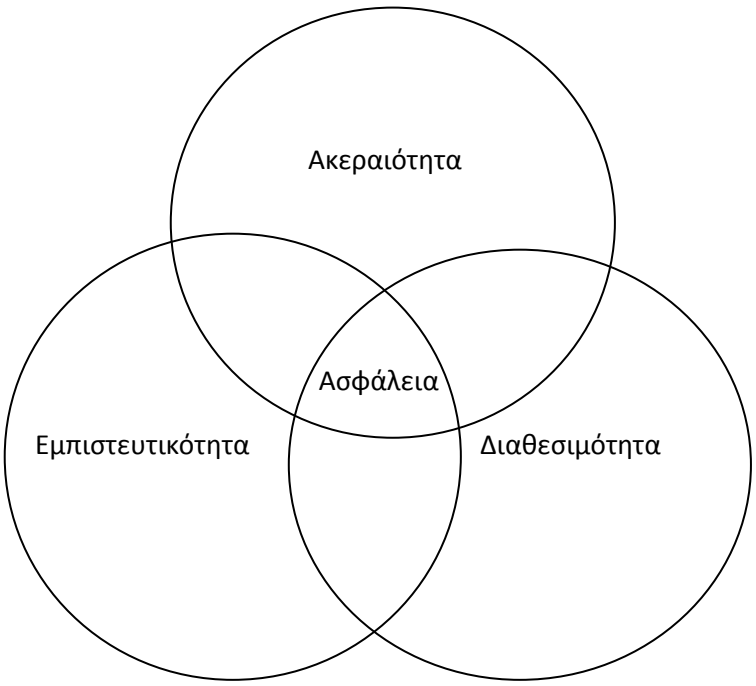
### 6.3.2. Ακεραιότητα

Η ακεραιότητα είναι η αρχή, βάση της οποίας τα δεδομένα ενός πληροφοριακού συστήματος παραμένουν αναλλοίωτα σε μία γνωστή μορφή, χωρίς τροποποιήσεις, προσθήκες ή αφαιρέσεις από μη εξουσιοδοτημένα άτομα. Επίσης, απαγορεύεται η πρόσβαση και η χρήση των υπολογιστών και δικτύων από τα μη εξουσιοδοτημένα άτομα.

### 6.3.3. Διαθεσιμότητα

Η διαθεσιμότητα είναι η αρχή, βάση της οποίας τα εξουσιοδοτημένα άτομα μπορούν να έχουν πρόσβαση στους υπολογιστές, τα δίκτυα και τα δεδομένα όποτε αυτά το θελήσουν. (9)

Εικόνα 5. Βασικές έννοιες ασφάλειας **(9)**




## 6.4. Βασικές αρχές ασφάλειας Πληροφοριακών Συστημάτων

- Αρχή 1: Η ασφάλεια είναι πρόβλημα του συστήματος και όχι του λογισμικού ή του υπολογιστή. Η συμπεριφορά του υπολογιστή μπορεί να είναι απόλυτα ασφαλής σ' ένα περιβάλλον, ενώ σε ένα διαφορετικό περιβάλλον όχι. Οι υπολογιστές δεν κινδυνεύουν άμεσα, αλλά μόνο όταν βρίσκονται σ' ένα περιβάλλον όπου εγκυμονούν κίνδυνοι και απροσδόκητες απώλειες. Επομένως, η ασφάλεια του Πληροφοριακού Συστήματος δημιουργείται και διασφαλίζεται σε επίπεδο συστήματος, και όχι λογισμικού ή υπολογιστή.
- Αρχή 2: Η ασφάλεια και η αξιοπιστία δεν είναι ταυτόσημες έννοιες, αλλά μπορεί να είναι και αντιφατικές. Αξιόπιστο λογισμικό καλείται το λογισμικό του οποίου η απόδοση παραμένει αμετάβλητη. Ένα αξιόπιστο λογισμικό δεν είναι απαραίτητα ασφαλές, και το ασφαλές λογισμικό δεν είναι πάντα αξιόπιστο. Κάποιες φορές, η αύξηση της αξιοπιστίας μπορεί να επιφέρει μείωση της ασφάλειας. Για παράδειγμα, εάν ο υπολογιστής εκτελεί μία διεργασία σε μη

ασφαλές περιβάλλον, τότε μπορεί να μεταβεί σε διακοπή της λειτουργίας του ή σε κάποιο λανθασμένο αποτέλεσμα.

- Αρχή 3: Η ασφάλεια πρέπει να ενσωματωθεί στο σύστημα από την αρχή. Δεν μπορεί να προστεθεί σ' ένα ολοκληρωμένο σύστημα.
- Αρχή 4: Η πρόληψη των ατυχημάτων και των απωλειών πρέπει να γίνεται με έλεγχο ολόκληρου του συστήματος και όχι μόνο μέρων του συστήματος.
- Αρχή 5: Τα ατυχήματα δεν οφείλονται μόνο σε μη σωστή λειτουργία του εξοπλισμού. Μπορεί να προκύψουν από δυσλειτουργικές αλληλεπιδράσεις, οι οποίες συμβαίνουν μεταξύ των διαφόρων εξαρτημάτων του εξοπλισμού.
- Αρχή 6: Τα ατυχήματα μπορούν να προληφθούν κάνοντας ανάλυση κινδύνου και δημιουργώντας μία πολιτική ασφάλειας έτσι ώστε να εξαλειφθούν ή να ελεγχθούν οι κίνδυνοι. (10)

## 6.5. Ομάδες υπηρεσιών ασφάλειας και ο στόχος τους

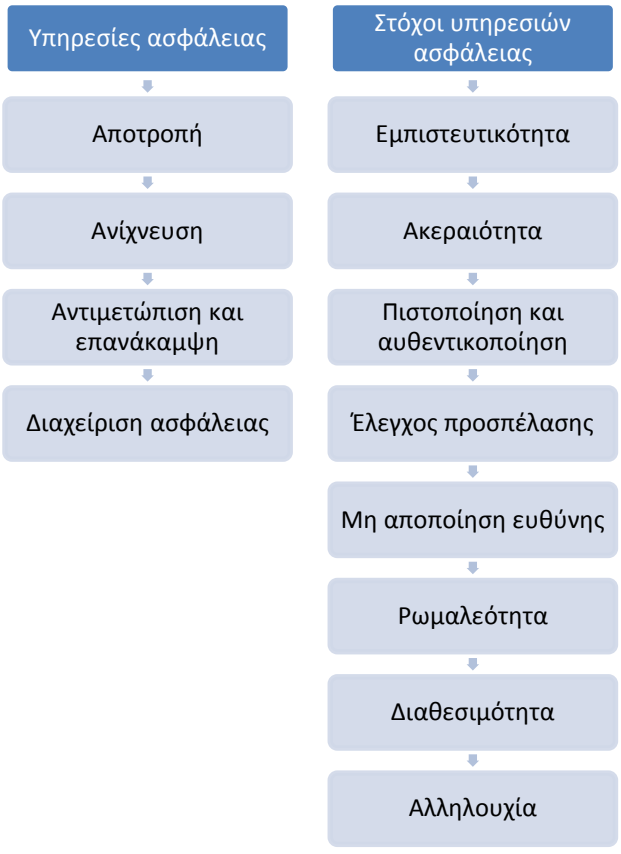
Σε κάθε σύστημα πρέπει να υπάρχουν ομάδες υπηρεσιών ασφάλειας, οι οποίες είναι οι ακόλουθες:

- Αποτροπή (prevention): Εμποδίζει την πρόσβαση στο σύστημα των μη εξουσιοδοτημένων χρηστών και περιλαμβάνει λειτουργίες ελέγχου προσπέλασης.
- Ανίχνευση (detection): Ασχολείται με την ανίχνευση πιθανής επίθεσης εισβολέων μέσω της παρατήρησης μιας ασυνήθιστης δραστηριότητας στο σύστημα ελέγχου και παρακολούθησης.
- Αντιμετώπιση και επανάκαμψη (containment and recovery): Ασχολείται με την αντιμετώπιση μιας εισβολής, επιδιόρθωση των ζημιών που έχουν προκληθεί απ' την εισβολή, καθώς και με την επανάκαμψη του συστήματος έπειτα από την εισβολή.
- Διαχείριση ασφάλειας (security administration): Ασχολείται με τη διαχείριση των πολιτικών ασφαλείας του συστήματος, δηλαδή με το σχεδιασμό και συντήρηση των κανόνων ασφαλείας.

Ο στόχος όλων των παραπάνω ομάδων ασφάλειας είναι να εξασφαλίσουν:

- Εμπιστευτικότητα των δεδομένων που αποθηκεύονται ή μεταδίδονται στα συστήματα
- Ακεραιότητα των δεδομένων που αποθηκεύονται ή μεταδίδονται στα συστήματα
- Πιστοποίηση και αυθεντικοποίηση
- Έλεγχο προσπέλασης στο δίκτυο και στο σύστημα γενικά
- Μη αποποίηση ευθύνης τόσο κατά την αποστολή όσο και κατά την παράδοση του μηνύματος
- Ρωμαλεότητα του συστήματος, δηλαδή την επανάκαμψη και εύρυθμη λειτουργία του συστήματος έπειτα από κάποια εισβολή
- Διαθεσιμότητα, δηλαδή το σύστημα να παραμένει σε ενεργή κατάσταση και να μην καταλήγει σε αδιέξοδα
- Αλληλουχία, δηλαδή ομαλή διαδοχή των μηνυμάτων και ενεργειών (8)

**Εικόνα 6. Ομάδες υπηρεσιών ασφάλειας και οι στόχοι τους (8)**



## 6.6. Η ασφάλεια κατά τον κύκλο ζωής του συστήματος

Όπως αναφέρθηκε και στις βασικές αρχές ασφάλειας Πληροφοριακών Συστημάτων, η ασφάλεια είναι μια έννοια που πρέπει να συμπεριληφθεί από την αρχή στο σύστημα και όχι να προστεθεί στη συνέχεια. Η προσθήκη της σ' ένα ολοκληρωμένο έργο είναι μια δαπανηρή διαδικασία και ενδέχεται να μη είναι αποτελεσματική. Προκειμένου να είναι αποτελεσματική, η ασφάλεια πρέπει να εξετάζεται σ' όλες τις φάσεις στον κύκλο ζωής του συστήματος. Οι δραστηριότητες που σχετίζονται με την ασφάλεια σε κάθε φάση στον κύκλο ζωής του συστήματος αναφέρονται στη συνέχεια.

- Κατά τη διάρκεια του σχεδιασμού του προγράμματος/ έργου:
    - Ανάπτυξη πολιτικών και διαδικασιών ασφάλειας και καθορισμός ενός σχεδίου ασφάλειας του συστήματος, το οποίο θα περιλαμβάνει τον τρόπο χειρισμού της ασφάλειας του λογισμικού.
    - Κατασκευή ενός συστήματος ασφάλειας, το οποίο θα περιέχει σαφώς προσδιορισμένες τις έννοιες της εξουσίας, της ευθύνης και της λογοδοσίας για ασφάλεια.
    - Καθορισμός κατάλληλων διαύλων επικοινωνίας για πληροφορίες που σχετίζονται με την ασφάλεια.
    - Δημιουργία ενός συστήματος παρακολούθησης του κινδύνου.
- Κατά την ανάπτυξη της έννοιας:
    - Προσδιορισμός των κινδύνων.
    - Ταξινόμηση των κινδύνων, συνήθως με κριτήριο τη σοβαρότητα.
    - Προσδιορισμός των απαιτήσεων και περιορισμών του συστήματος ασφάλειας, έτσι ώστε να επιτευχθεί η σωστή ανάπτυξη και λειτουργία του.
- Κατά τη διάρκεια σχεδιασμού του συστήματος:
    - Προσδιορισμός του τρόπου ανταπόκρισης του συστήματος σε επικίνδυνες καταστάσεις.
    - Εφόσον είναι δυνατόν, εξάλειψη των κινδύνων από το σχεδιασμό του συστήματος.
    - Εάν δεν μπορούν να εξαλειφθούν οι κίνδυνοι, έλεγχος αυτών.

- Προσδιορισμός και επίλυση συγκρούσεων μεταξύ των στόχων του σχεδιασμού, χρησιμοποιώντας την ασφάλεια ως κριτήριο για τη σωστή απόφαση.

- Όταν ολοκληρωθεί η ανάλυση και ο σχεδιασμός του συστήματος ασφάλειας:
    - Παρακολούθηση των ανεπίλυτων κινδύνων στα διάφορα στοιχεία του συστήματος, συμπεριλαμβανομένων του υλικού, του λογισμικού και των ανθρώπων.
- Κατά την εφαρμογή του συστήματος:
    - Σχεδιασμός ασφάλειας στα διάφορα συστατικά του συστήματος.
    - Επαλήθευση της ασφάλειας στο κατασκευασμένο σύστημα. Η επαλήθευση της ασφάλειας είναι ένα δύσκολο ζήτημα. Αυτό συμβαίνει διότι κάποιοι παράγοντες που είτε έχουν ξεχαστεί είτε έχουν παραλειφθεί κατά το σχεδιασμό του συστήματος, είναι πιθανό να παραλειφθούν και κατά τη διάρκεια της επαλήθευσης.
- Κατά την εφαρμογή:
    - Χρήση του αρχικού σχεδίου ασφάλειας που μελετήθηκε κατά την ανάπτυξη του συστήματος έτσι ώστε να δημιουργηθεί μία επίσημη πολιτική ασφάλειας για όλο το σύστημα.
- Κατά τη διάρκεια εργασιών και συντήρησης:
    - Αξιολόγηση όλων των προτεινόμενων αλλαγών όσον αφορά στην ασφάλεια, λαμβάνοντας υπόψιν όλες τις υποθέσεις και αναλύσεις κινδύνων που είχαν χρησιμοποιηθεί κατά τη φάση της ανάπτυξης.
    - Περιοδικοί έλεγχοι και παρακολούθηση της απόδοσης, καθώς οι αλλαγές δεν είναι πάντα προγραμματισμένες.

Τέλος, πρέπει να γίνεται ανάλυση περιστατικών και ατυχημάτων, έτσι ώστε να εντοπίζονται τα περιστατικά που σχετίζονται με την ασφάλεια. Η συχνή ανατροφοδότηση είναι απαραίτητη για να διασφαλίζει ότι η ανθρώπινη συμπεριφορά δεν αλλάζει με το χρόνο με τρόπο που θα μπορούσε να παραβιάσει το σύστημα ασφάλειας. (10)

# ΚΕΦΑΛΑΙΟ 7. ΑΣΦΑΛΕΙΑ ΠΛΗΡΟΦΟΡΙΑΚΩΝ ΣΥΣΤΗΜΑΤΩΝ ΤΩΝ ΝΟΣΟΚΟΜΕΙΩΝ

## 7.1.Εισαγωγή κεφαλαίου 7

Όπως αναφέρθηκε στα προηγούμενα κεφάλαια, η ασφάλεια των Πληροφοριακών Συστημάτων είναι απαραίτητη κατά τη διάρκεια όλου του κύκλου ζωής του συστήματος, έτσι ώστε να εξασφαλίζονται οι έννοιες της ακεραιότητας, διαθεσιμότητας και εμπιστευτικότητας των δεδομένων. Εξίσου σημαντική κρίνεται και η ύπαρξη ασφάλειας στα Πληροφοριακά Συστήματα των Νοσοκομείων. Καθημερινά διέρχονται πολλοί ασθενείς και άγνωστοι επισκέπτες και αποθηκεύονται πολλά ιατρικά αρχεία που περιλαμβάνουν προσωπικά δεδομένα των ασθενών, με αποτέλεσμα να κάνουν τα Πληροφοριακά Συστήματα των Νοσοκομείων ιδιαίτερα ευάλωτα στις επιθέσεις. Σ’ αυτό το κεφάλαιο, στην υποενότητα 7.2 αναφέρονται οι ιδιαιτερότητες που παρουσιάζουν τα Πληροφοριακά Συστήματα Νοσοκομείων ως προς την ασφάλεια, στην υποενότητα 7.3 τονίζεται η σημασία ύπαρξης ασφάλειας στα Πληροφοριακά Συστήματα στο χώρο του νοσοκομείου και στην υποενότητα 7.4 αναλύονται οι διακρίσεις της ασφάλειας των Πληροφοριακών Συστημάτων στο χώρο της υγείας.

## 7.2. Ιδιαιτερότητες που παρουσιάζουν τα Πληροφοριακά Συστήματα Νοσοκομείων σε σχέση με την ασφάλεια

Τα Πληροφοριακά Συστήματα Νοσοκομείων είναι ιδιαίτερα επιρρεπή στους εσωτερικούς και εξωτερικούς κινδύνους που εγκυμονούν για τους παρακάτω λόγους:

- Περιέχουν απόρρητα και εμπιστευτικά δεδομένα, τα οποία σχετίζονται με τα στοιχεία των ασθενών, το βιοτικό τους επίπεδο και τη θεραπεία τους. Όμως, η χρήση αυτών των δεδομένων για στατιστικούς λόγους μπορεί ξεφύγει από τους κανόνες ιδιωτικότητας.
- Τα ιατρικά δεδομένα είναι πολύ σημαντικά για τη θεραπεία και τη ζωή των ασθενών. Γι’ αυτό το λόγο, είναι κρίσιμη η διαφύλαξη της ακεραιότητάς

τους. Δεδομένου, όμως, του μεγάλου χρονικού διαστήματος που μπορεί να παραμείνουν τα ιατρικά δεδομένα σε μία μονάδα υγείας, η διαφύλαξη της ακεραιότητάς τους αποτελεί ένα πολύπλοκο ζήτημα.

- Το περιβάλλον ενός νοσοκομείου είναι ιδιαίτερα ανοιχτό και μη ελεγχόμενο. Καθημερινά εισέρχονται ασθενείς και συνοδοί τους, με αποτέλεσμα τα ιατρικά δεδομένα να μην μπορούν να προστατευθούν πλήρως.
- Τα ιατρικά δεδομένα επεξεργάζονται συνήθως διαδικτυακά. Για το λόγο αυτό, είναι απαραίτητη η ακεραιότητα των συστημάτων. Εάν τα συστήματα δεν πληρούν τις προϋποθέσεις, τότε τα δεδομένα είναι δυνατόν να τροποποιηθούν από μη εξουσιοδοτημένα άτομα.

## 7.3. Γιατί είναι σημαντική η ασφάλεια των Πληροφοριακών Συστημάτων των Νοσοκομείων;

Μέσω της ιδιωτικότητας και της ασφάλειας των Πληροφοριακών Συστημάτων των Νοσοκομείων αυξάνεται η εμπιστοσύνη των ασθενών και η ακεραιότητα των πληροφοριών. Προκειμένου οι ψηφιακές πληροφορίες για την υγεία να επιφέρουν καλύτερα αποτελέσματα, λιγότερα έξοδα θεραπείας και να οδηγήσουν σε ταχεία ανάρρωση των ασθενών, πρέπει οι πάροχοι υπηρεσιών υγείας και οι ασθενείς να εμπιστεύονται ότι οι ηλεκτρονικές πληροφορίες είναι ασφαλείς. Εάν οι ασθενείς δε θεωρούν ότι οι ψηφιακές πληροφορίες είναι εμπιστευτικές και ασφαλείς, ενδεχομένως να μη θελήσουν να ανταλλάξουν πληροφορίες με τους πάροχους υπηρεσιών υγείας. Όμως, αυτή η μη ανταλλαγή ιατρικών πληροφοριών θα μπορούσε να έχει απειλητικές συνέπειες για τη ζωή των ασθενών. Γι’ αυτό το λόγο, είναι πολύ σημαντικό να εξασφαλίσουμε ότι οι πληροφορίες και τα αρχεία των ασθενών είναι ασφαλή και απόρρητα. Μ’ αυτόν τον τρόπο, οι ασθενείς θα μπορέσουν να εμπιστευτούν το προσωπικό του νοσοκομείου ανταλλάσσοντας ιατρικές πληροφορίες, γεγονός που θα βοηθήσει τους ασθενείς να λάβουν πιο ενημερωμένες αποφάσεις. Επιπρόσθετα, όταν συμβούν παραβιάσεις των πληροφοριών σ’ ένα νοσοκομείο, αυτό μπορεί να έχει σοβαρές συνέπειες για την οικονομική κατάσταση και τη φήμη του νοσοκομείου αλλά και για τους ίδιους τους ασθενείς. Οι ελλιπείς πρακτικές ιδιωτικότητας και ασφάλειας αυξάνουν την

ευπάθεια των πληροφοριών των ασθενών στο Πληροφοριακό Νοσοκομειακό Σύστημα, αυξάνοντας τον κίνδυνο επιτυχημένης δράσης των εισβολέων στο σύστημα. (11)

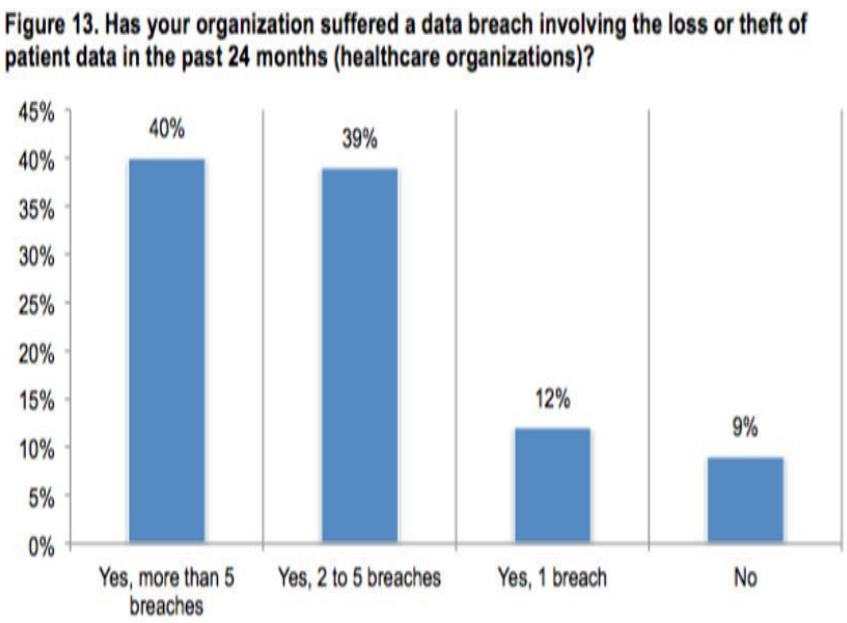
Η αναγκαιότητα ύπαρξης ασφάλειας των Πληροφοριακών Συστημάτων στο χώρο του Νοσοκομείου φαίνεται και από τα ακόλουθα στατιστικά στοιχεία, τα οποία αναδεικνύουν ότι τα Πληροφοριακά Συστήματα Νοσοκομείων απειλούνται συχνά από κινδύνους και απειλές.

Σύμφωνα με το Verizon 2016 Data Breach Investigations Report (DBIR), το οποίο εξέτασε περισσότερα από 100.000 περιστατικά, συμπεριλαμβάνοντας 2.260 αναλυμένες παραβιάσεις δεδομένων, που αφορούσαν εγκλήματα του κυβερνοχώρου, συλλέχτηκαν πληροφορίες που οδήγησαν στα εξής συμπεράσματα:

i. 89% των παραβιάσεων είχε οικονομικό ή κατασκοπευτικό κίνητρο
ii. 63% των επιβεβαιωμένων παραβιάσεων είχαν πολύ αδύναμο, προεπιλεγμένο ή κλεμμένο κωδικό πρόσβασης
iii. 30% των mails που ανοίχτηκαν το 2015 (τόσο τα συννημένα τους αρχεία όσο και οι σύνδεσμοι των mails) αποτελούν το κορυφαίο μέσο επίθεσης κακόβουλων προγραμμάτων.

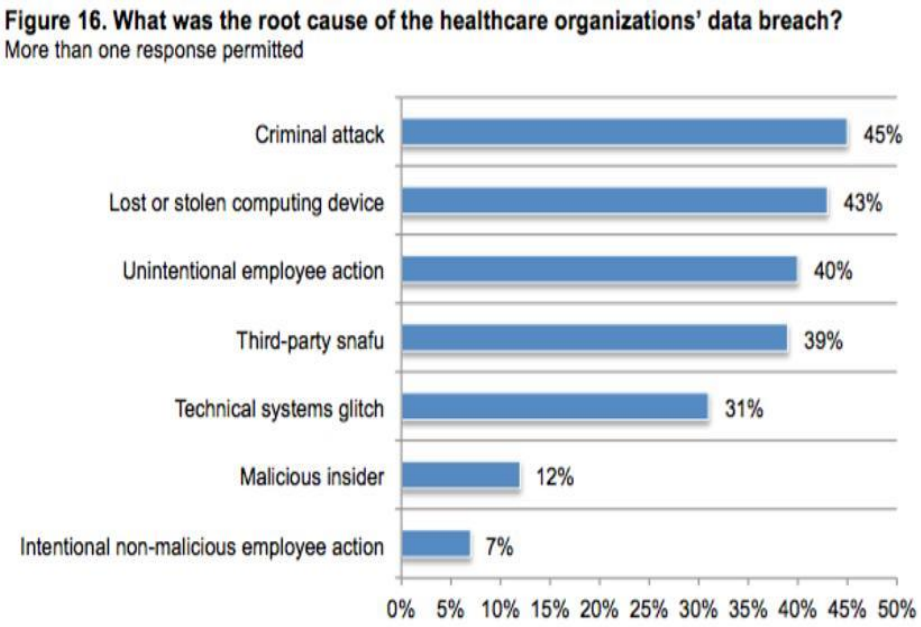
Συγκεκριμένα, όσον αφορά τους οργανισμούς υγειονομικής περίθαλψης, τα αποτελέσματα μιας έρευνας έδειξαν ότι το 91% των οργανισμών υγειονομικής περίθαλψης είχε μία τουλάχιστον παραβίαση δεδομένων που συμπεριλάμβανε απώλεια ή κλοπή των στοιχείων των ασθενών τα τελευταία 2 χρόνια.

**Πίνακας 1. Συχνότητα παραβίασης δεδομένων συμπεριλαμβανομένης απώλειας ή κλοπής των δεδομένων των ασθενών τα τελευταία 2 χρόνια (12)**




Η κύρια αιτία για την παραβίαση των δεδομένων των ασθενών ήταν εγκληματική επίθεση, ενώ άλλες σημαντικές αιτίες φαίνεται να ήταν η χαμένη ή κλεμμένη συσκευή υπολογιστή, η ακούσια δράση των εργαζομένων, η εμπλοκή τρίτων και η μικροβλάβη των τεχνικών συστημάτων. Σε μικρό ποσοστό, αιτίες για την παραβίαση των δεδομένων στους οργανισμούς υγειονομικής περίθαλψης ήταν οι κακόβουλοι γνώστες καθώς και η σκόπιμη μη κακόβουλη δράση των εργαζομένων. (12)

**Πίνακας 2. Ποια είναι η κύρια αιτία παραβίασης δεδομένων στους οργανισμούς υγειονομικής περίθαλψης (12)**




Μετά την εξαγωγή αυτών των συμπερασμάτων και της αμφισβήτησης των ασθενών, σκοπός των παρόχων υπηρεσιών υγείας είναι να κερδίσουν την εμπιστοσύνη των ασθενών. Αυτό μπορεί να γίνει εξασφαλίζοντας κάποιες απαραίτητες προϋποθέσεις:

- Πρέπει να διατηρούν με ασφάλεια και ακρίβεια τις πληροφορίες των ασθενών στα αρχεία τους.
- Πρέπει να εξασφαλίσουν ότι οι ασθενείς μπορούν να ζητήσουν πρόσβαση στο ιατρικό αρχείο τους και όταν το ζητήσουν θα πρέπει να πραγματοποιήσουν το αίτημά τους.
- Πρέπει να χειρίζονται προσεκτικά τις πληροφορίες των ασθενών προστατεύοντας το ιατρικό απόρρητο.
- Πρέπει να εξασφαλίζουν την πρόσβαση των εξουσιοδοτημένων χρηστών στις ιατρικές πληροφορίες όταν αυτό είναι απαραίτητο. (11)

## 7.4. Διάκριση ασφάλειας των Πληροφοριακών Συστημάτων στο χώρο της Υγείας

Για να γίνει εφικτή η ασφάλεια των Πληροφοριακών Συστημάτων στα νοσοκομεία και να ληφθούν σωστά μέτρα για τον περιορισμό των κινδύνων και των απειλών, πρέπει πρώτα να δούμε τις διάφορες κατηγορίες που διακρίνεται.

Η ασφάλεια των Πληροφοριακών Συστημάτων στο χώρο της Υγείας διακρίνεται:

1. στην ασφάλεια σε περίπτωση έκτακτης ανάγκης και
2. στην ασφάλεια στις καθημερινές διεργασίες.

### 7.4.1. Ασφάλεια σε περίπτωση έκτακτης ανάγκης

Ως έκτακτη ανάγκη θεωρούμε την κατάσταση κατά την οποία έχει επέλθει καταστροφή στο πληροφοριακό σύστημα, με αποτέλεσμα να μην μπορεί αυτό να λειτουργήσει άμεσα ή εντός κάποιων ωρών. Τέτοιες περιπτώσεις είναι οι καταστροφές από διακοπές ηλεκτρικής ενέργειας, προσωρινές βλάβες από πυρκαγιά ή πλημμύρα και η πτώση μέρους του εξοπλισμού και του κεντρικού υπολογιστή.

### 7.4.2. Ασφάλεια στις καθημερινές διεργασίες

Τα Πληροφοριακά Συστήματα πρέπει να είναι ασφαλή κατά τη καθημερινή τους χρήση. Κρίνεται, λοιπόν, απαραίτητη η ύπαρξη μιας πολιτικής ασφάλειας, η οποία θα:

- καλύπτει τα κτίρια, τις εγκαταστάσεις και το λογισμικό,
- μεριμνά για το ποιοι αναπτύσσουν τα Πληροφοριακά Συστήματα, πώς τα αναπτύσσουν και πώς τα χειρίζονται,
- ελέγχει ποιοι μπαίνουν σε ευαίσθητους χώρους και πώς διακινούνται οι εμπιστευτικές πληροφορίες εκτός δικτύων,
- επιβλέπει εάν διαφυλάσσονται τα δεδομένα και με ποιον τρόπο.

Η ασφάλεια στις καθημερινές διεργασίες μπορεί να διακριθεί σε 4 τύπους ασφάλειας:

- Φυσική ασφάλεια
- Λογική ασφάλεια
- Φυσική προστασία του δικτύου εγκατάστασης
- Ασφάλεια λοιπών δικτύων περιφερειακού και βοηθητικού εξοπλισμού.

### 7.4.2.1. Φυσική ασφάλεια

Η φυσική ασφάλεια των Πληροφοριακών Συστημάτων Νοσοκομείων περιλαμβάνει:

- Προστασία του χώρου του νοσοκομείου που βρίσκονται οι υπολογιστές
- Προστασία του υλικού (hardware) από οποιαδήποτε απειλή, βλάβη ή ανθρώπινη απροσεξία
- Προστασία των εφεδρικών αντιγράφων του συστήματος, των προγραμμάτων, των εφαρμογών και των δεδομένων
- Εγκατάσταση του συστήματος αδιάλειπτης λειτουργίας (U.P.S) και συστήματος πυρόσβεσης με αδρανές αέριο.

### 7.4.2.2. Λογική ασφάλεια

Η λογική ασφάλεια των Πληροφοριακών Συστημάτων των νοσοκομείων περιλαμβάνει:

- Προφύλαξη στο λογισμικό
- Προφύλαξη στα δεδομένα
- Λειτουργικά προγράμματα
- Προγράμματα εφαρμογών και πακέτα
- Προστασία λειτουργίας της μνήμης της κεντρικής μονάδας του επεξεργαστή (Κ.Μ.Ε)
- Προστασία αρχείων λειτουργικού συστήματος
- Προστασία βιβλιοθηκών εγκατάστασης
- Προστασία- έλεγχος προσπέλασης.

### 7.4.2.3. Φυσική προστασία του δικτύου εγκατάστασης

Η φυσική προστασία του δικτύου εγκατάστασης περιλαμβάνει:

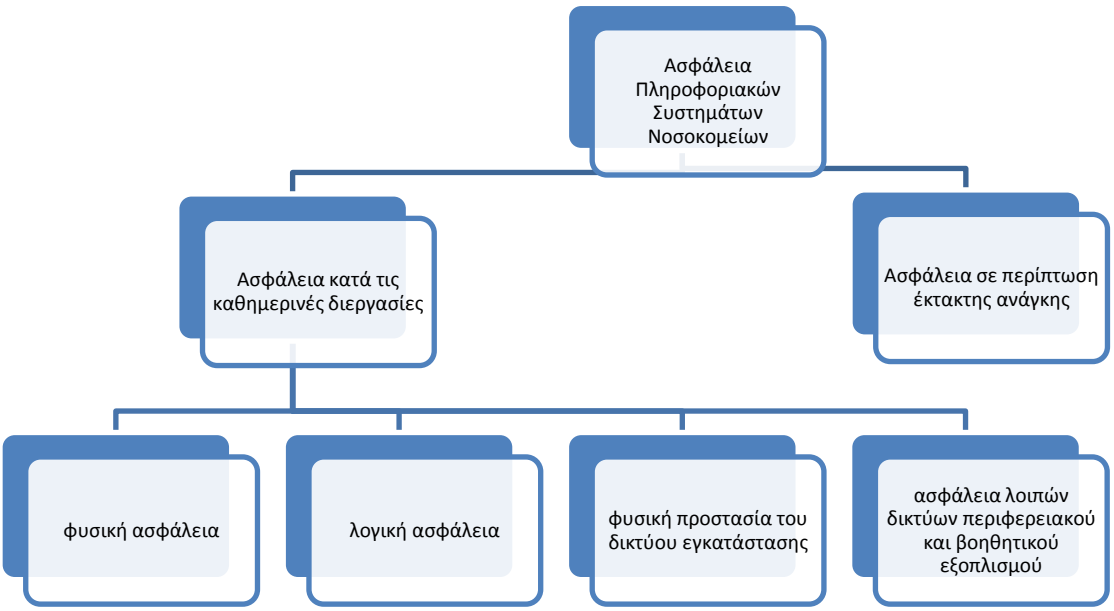
- Προστασία κατά τη μεταφορά δεδομένων
- Προστασία στις τηλεφωνικές γραμμές
- RESTART/RECOVERY διαδικασίες

### 7.4.2.4. Ασφάλεια λοιπών δικτύων περιφερειακού και βοηθητικού εξοπλισμού

Τα δίκτυα, τόσο του περιφερειακού όσο και του βοηθητικού εξοπλισμού, πρέπει να ελέγχονται και να πληρούν τις προδιαγραφές. Γι' αυτό, πρέπει να υπάρχει μια πολιτική ασφάλειας, η οποία να μεριμνά για:

- Την προστασία και τον έλεγχο του εξοπλισμού
- Την προστασία και τον έλεγχο του λογισμικού
- Την κατηγοριοποίηση του βαθμού ασφαλείας των δεδομένων
- Την κατηγοριοποίηση των προγραμμάτων που βρίσκονται εγκατεστημένα σ' αυτόν τον εξοπλισμό. (13)

**Εικόνα 7. Διάκριση ασφάλειας Πληροφοριακών Συστημάτων Νοσοκομείων (13)**



# ΚΕΦΑΛΑΙΟ 8. ΠΟΛΙΤΙΚΗ ΑΣΦΑΛΕΙΑΣ ΠΛΗΡΟΦΟΡΙΑΚΩΝ ΣΥΣΤΗΜΑΤΩΝ ΣΤΑ ΝΟΣΟΚΟΜΕΙΑ

## 8.1.Εισαγωγή κεφαλαίου 8

Για να υπάρξει ασφάλεια τόσο στις καθημερινές διεργασίες όσο και σε περίπτωση έκτακτης ανάγκης, πρέπει να δημιουργηθεί μία πολιτική ασφάλειας που θα περιλαμβάνει συγκεκριμένες οδηγίες για κάθε αρχή που αφορά τη χρήση των Πληροφοριακών Συστημάτων στα νοσοκομεία. Σ' αυτό το κεφάλαιο, ορίζεται η έννοια της πολιτικής ασφάλειας στην υποενότητα 8.2, περιγράφεται η διαδικασία για την εφαρμογή μιας πολιτικής ασφάλειας στο χώρο του νοσοκομείου στη υποενότητα 8.3 και αναλύεται η πολιτική ασφάλειας υψηλού επιπέδου SEISMED που χρησιμοποιείται στα νοσοκομεία στην υποενότητα 8.4.

## 8.2.Ορισμός πολιτικής ασφάλειας

Η πολιτική ασφάλειας είναι ένα έγγραφο, όπου αναφέρονται οδηγίες για κάθε γενική αρχή που αφορά τη χρήση τεχνολογιών πληροφορικής. Οι οδηγίες αυτές είναι συνήθως σταθερές, καθώς οι γενικές αρχές που αφορούν τη χρήση των Πληροφοριακών Συστημάτων μεταβάλλονται με πολύ αργό ρυθμό. Οι οδηγίες που αναφέρονται στην πολιτική ασφάλειας επικεντρώνονται στις διαδικασίες, στους κανόνες και στους ρόλους που σχετίζονται με την προστασία των Πληροφοριακών Συστημάτων στα νοσοκομεία και πρέπει να είναι γνωστές και να ακολουθούνται από όλα τα μέλη του προσωπικού που χειρίζονται αυτά τα συστήματα. Οι οδηγίες, αυτές, υλοποιούνται με την εφαρμογή συγκεκριμένων μέτρων προστασίας που αναλύονται στο Κεφάλαιο 9. Η πολιτική ασφάλειας μαζί με τα μέτρα προστασίας αποτελούν το Σχέδιο Ασφάλειας για τα Πληροφοριακά Συστήματα των νοσοκομείων. (7)

## 8.3. Διαδικασία για την εφαρμογή μιας πολιτικής ασφάλειας στο νοσοκομείο

Η διαδικασία για την εφαρμογή πολιτικής ασφάλειας στο νοσοκομείο περιλαμβάνει 7 βήματα:

- Επιλογή της ομάδας που σχετίζεται με την ασφάλεια των Πληροφοριακών Συστημάτων και εκπαίδευση της
- Ανακοίνωση της διαδικασίας, των ευρημάτων και των ενεργειών
- Επανεξέταση της ήδη υπάρχουσας ασφάλειας των Πληροφοριακών Συστημάτων των Νοσοκομείων
- Ανάπτυξη του σχεδίου δράσης
- Διαχείριση και μετριασμός των κινδύνων
- Προσδιορισμός της σημασίας ύπαρξης ασφάλειας
- Παρακολούθηση, έλεγχος και ενημέρωση της ασφάλειας σε συνεχή βάση

Α.Επιλογή της ομάδας που σχετίζεται με την ασφάλεια των Πληροφοριακών Συστημάτων και εκπαίδευση της:

Είναι σημαντικό να υπάρχει μία ομάδα και ένας ηγέτης αυτής της ομάδας, ο οποίος να τονίζει τη σημασίας προστασίας των πληροφοριών των ασθενών. Ο ηγέτης είναι υπεύθυνος για την οργάνωση ενός σχεδίου, όπου θα ενσωματώνεται η έννοια της ιδιωτικότητας και της ασφάλειας. Αυτό το βήμα περιλαμβάνει τα εξής:

- Ορισμός ενός υπεύθυνου ασφάλειας: Ο υπεύθυνος ασφάλειας θα είναι αρμόδιος για την ανάπτυξη και διατήρηση των πρακτικών ασφάλειας. Θα είναι, επίσης, υπεύθυνος για την προστασία των ηλεκτρονικών αρχείων των ασθενών από την πρόσβαση σ’ αυτά μη εξουσιοδοτημένων ατόμων και για τη διασφάλιση της ενημέρωσης των ασθενών.

- Συζήτηση για τις απαιτήσεις σχετικά με την ασφάλεια με τον υπεύθυνο για την ανάπτυξη των Πληροφοριακών Συστημάτων: Πριν την ανάλυση κινδύνου, είναι απαραίτητη η συνεργασία με τον υπεύθυνο για την ανάπτυξη των Πληροφοριακών Συστημάτων, έτσι ώστε να εξετάσει εάν μπορεί να διασφαλίσει την προστασία των δεδομένων των ασθενών. Πριν την αγορά ενός Πληροφοριακού Συστήματος, το σύστημα πρέπει να ελεγχθεί ως προς το αν συμμορφώνεται με τις απαιτήσεις ασφάλειας και ιδιωτικότητας και ως προς τις δυνατότητες που προσφέρει. Κατά την εφαρμογή ενός Πληροφοριακού Συστήματος, πρέπει να αξιολογηθεί αν ανταποκρίνεται στις απαιτήσεις ασφάλειας που έχουν οριστεί από την αρχή. Εάν χρειάζονται επιπρόσθετες δυνατότητες και κάλυψη τυχόν ελλείψεων, πρέπει να γίνει η κατάλληλη διαχείριση από τον υπεύθυνο. Ο υπεύθυνος για την ανάπτυξη του συστήματος πρέπει να αναλάβει και την εκπαίδευση του προσωπικού ως προς τη λειτουργία του.
- Εξέταση του ενδεχομένου συνεργασίας με έναν πιστοποιημένο επαγγελματία, ο οποίος θα βοηθάει με την ανάλυση κινδύνου: Η ανάλυση του κινδύνου πρέπει να γίνεται με μία διαδικασία σύμφωνη με την πολιτική ασφάλειας, διαφορετικά δεν εξασφαλίζεται η προστασία των ηλεκτρονικών πληροφοριών. Η διαδικασία της ανάλυσης κινδύνου ίσως γίνει ταχύτερα και πιο αξιόπιστα αν γίνει από κάποιον πιστοποιημένο επαγγελματία απ’ ό,τι θα γινόταν αν την αναλάμβανε ένα μέλος του προσωπικού. Ο επαγγελματίας πρέπει να έχει ανάλογη πιστοποίηση και εμπειρία στην ανάλυση κινδύνου σε ιατρικές μονάδες καθώς και τα απαραίτητα προσόντα να προτείνει τρόπους μετριασμού των κινδύνων.
- Χρήση εργαλείων για προεπισκόπηση της ανάλυσης κινδύνου: Πρέπει να γίνεται χρήση των εργαλείων του υπεύθυνου ασφάλειας και του υπεύθυνου επαγγελματία για την ανάλυση κινδύνου προκειμένου να γίνονται γνωστές ελλείψεις που θέτουν σε κίνδυνο την ασφάλεια των ηλεκτρονικών πληροφοριών των ασθενών.

- Ανανέωση των γνώσεων σχετικά με τους κανόνες ασφάλειας: Ενημέρωση του προσωπικού σχετικά με τους κανόνες και τις απαιτήσεις απορρήτου και ασφάλειας.
- Προώθηση μιας στάσης προστασίας της ιδιωτικής ζωής των ασθενών και εξασφάλισης των πληροφοριών τους: Η προστασία της ιδιωτικής ζωής των ασθενών και η εξασφάλιση των πληροφοριών τους επιτυγχάνεται καλύτερα όταν στο νοσοκομείο τονίζεται συνεχώς η σημασία της εμπιστευτικότητας και της ασφάλειας. Γι' αυτό, πρέπει να υπάρχει η ανάλογη στήριξη του προσωπικού στην προσπάθειά τους να συμμορφωθούν και να εφαρμόσουν το ιατρικό απόρρητο.

Β. Ανακοίνωση της διαδικασίας, των ευρημάτων και των ενεργειών:

Αυτό το βήμα περιλαμβάνει στοιχεία σχετικά με το πώς έγινε η ανάλυση κινδύνου και πώς αντιμετωπίστηκαν οι κίνδυνοι που εντοπίστηκαν στην ανάλυση κινδύνου. Τα στοιχεία αυτά περιλαμβάνονται σ' ένα φάκελο τεκμηρίωσης, ο οποίος με την πάροδο του χρόνου θα βοηθήσει να γίνουν πιο αποτελεσματικές οι διαδικασίες ασφάλειας. Επιπλέον, τα μέλη του προσωπικού θα είναι σε θέση να αναφέρουν τα κύρια ευρήματα, αποφάσεις και ενέργειες. Τέλος, οι προηγούμενες εμπειρίες των μελών του προσωπικού θα βοηθήσουν στη διασφάλιση της μεγαλύτερης ακρίβειας των πληροφοριών.

Γ. Επανεξέταση της ήδη υπάρχουσας ασφάλειας των Πληροφοριακών Συστημάτων των Νοσοκομείων:

Η διαδικασία ανάλυσης κινδύνου αξιολογεί πιθανές απειλές και ευπάθειες όσον αφορά την εμπιστευτικότητα, διαθεσιμότητα και ακεραιότητα των Πληροφοριακών Συστημάτων. Τα ευρήματα που προκύπτουν απ' αυτή τη διαδικασία χρησιμοποιούνται για την εύρεση τρόπων μετριασμού των κινδύνων. Η πρώτη

ανάλυση κινδύνου που γίνεται πρέπει να είναι περιεκτική και να περιλαμβάνει όλους τους πιθανούς κινδύνους ασφάλειας. Πρέπει, λοιπόν, να:

- Προσδιορίζει πού υπάρχουν οι ηλεκτρονικές πληροφορίες, πώς δημιουργήθηκαν, πώς λήφθηκαν, πώς διατηρούνται και πώς μεταδίδονται, συμπεριλαμβανομένων των Πληροφοριακών Συστημάτων. Διαφορετικοί τύποι κινδύνων απειλούν τις ηλεκτρονικές πληροφορίες των ασθενών αν βρίσκονται σε ηλεκτρονικό φάκελο σ' ένα γραφείο και διαφορετικοί αν βρίσκονται σ' έναν ηλεκτρονικό φάκελο που φιλοξενείται στο διαδίκτυο.
    - Όταν οι ηλεκτρονικές πληροφορίες των ασθενών διατηρούνται σε ηλεκτρονικό φάκελο που βρίσκεται σε γραφείο, τότε η φυσική καταστροφή θα μπορούσε να βλάψει τη διαθεσιμότητά τους ή ακόμα και να τις καταστρέψει. Επίσης υπάρχει ο κίνδυνος τα χαρακτηριστικά ασφάλειας να μην είναι τόσο ενημερωμένα και εξειδικευμένα όσο θα ήταν αν ο ηλεκτρονικός φάκελος διατηρούταν στο διαδίκτυο. Τέλος, όταν γίνονται αλλαγές σχετικά με τις απαιτήσεις δημόσιας και ιδιωτικής ασφάλειας, πρέπει να υπάρχει ειδική διαμόρφωση του ηλεκτρονικού φακέλου και επεξεργασία τυχόν σφαλμάτων.
    - Όταν οι ηλεκτρονικές πληροφορίες των ασθενών βρίσκονται σε ηλεκτρονικό φάκελο που φιλοξενείται στο διαδίκτυο, τότε υπάρχει άμεση εξάρτηση από την αξιοπιστία της σύνδεσης στο διαδίκτυο. Τα δεδομένα μπορεί να αποθηκεύονται σε άλλη χώρα, όπου ενδέχεται να ισχύουν διαφορετικοί κανόνες και νόμοι ασφάλειας προσωπικών δεδομένων. Ακόμα, ο προγραμματιστής μπορεί με την πάροδο του χρόνου να ζητήσει επιπρόσθετα χρήματα για τη συμμόρφωση του φακέλου με τις απαιτήσεις που ορίζονται.
- Εντοπίζει πιθανές απειλές και ευάλωτα σημεία στις ηλεκτρονικές πληροφορίες των ασθενών. Οι πιθανές απειλές περιλαμβάνουν τις ανθρώπινες απειλές ( όπως επίθεση μέσω δικτύου από εισβολείς, σφάλμα μέλους τους προσωπικού, κλοπή), τις φυσικές απειλές ( όπως σεισμός, πυρκαγιά, τυφώνας) και τις περιβαλλοντικές απειλές (όπως ρύπανση ή

απώλεια ισχύος). Τα ευάλωτα σημεία είναι ελαττώματα ή αδυναμίες, που αν εκμεταλλευόντουσαν από απειλή, θα μπορούσαν να οδηγήσουν σε παραβίαση των κανόνων ασφάλειας.

- Προσδιορίζει τους κινδύνους και το επίπεδο που απειλούν την ακεραιότητα, διαθεσιμότητα και εμπιστευτικότητα των Πληροφοριακών Συστημάτων (υψηλό, μεσαίο, χαμηλό).

Δ. Ανάπτυξη του σχεδίου δράσης:

Με βάση τα αποτελέσματα που προέκυψαν από την ανάλυση κινδύνου, πρέπει να αναπτυχθεί ένα σχέδιο δράσης για το μετριασμό των προσδιορισμένων κινδύνων. Το σχέδιο δράσης θα πρέπει να επικεντρώνεται στις απειλές και ευπάθειες υψηλής προτεραιότητας και να είναι εφικτό και προσιτό για χρήση. Για να είναι αποτελεσματικό, πρέπει να αποτελείται από 5 συστατικά:

1. Διοικητικές διασφαλίσεις
2. Φυσικές διασφαλίσεις
3. Τεχνικές εγγυήσεις
4. Οργανωτικά πρότυπα
5. Πολιτικές και διαδικασίες

Αυτά τα συστατικά του σχεδίου δράσης αντιστοιχούν με συγκεκριμένα στοιχεία ασφάλειας, όπως παρουσιάζονται στον παρακάτω πίνακα.

**Πίνακας 3. Παραδείγματα ευπάθειας για κάθε συστατικό ασφάλειας και παραδείγματα στρατηγικής μετριασμού των προβλημάτων (11)**

| ΣΥΣΤΑΤΙΚΟ ΑΣΦΑΛΕΙΑΣ | ΠΑΡΑΔΕΙΓΜΑΤΑ ΕΥΠΑΘΕΙΑΣ | ΠΑΡΑΔΕΙΓΜΑΤΑ ΣΤΡΑΤΗΓΙΚΗΣ ΜΕΤΡΙΑΣΜΟΥ ΠΡΟΒΛΗΜΑΤΟΣ |
|---|---|---|
| Διοικητικές διασφαλίσεις | • Δεν ορίζεται υπεύθυνος ασφάλειας<br>• Το προσωπικό δεν έχει | • Ορισμός και ανακοίνωση του υπεύθυνου ασφάλειας |

| | | |
|---|---|---|
| | εκπαιδευτεί ή δε γνωρίζει θέματα ασφάλειας και ιδιωτικότητας<br>• Περιοδική αξιολόγηση ασφάλειας | • Η κατάρτιση του προσωπικού ξεκινάει με μίσθωση και συνεχίζεται σε τακτική βάση.<br>• Πραγματοποιείται ανάλυση κινδύνου σε τακτική βάση και όταν συμβαίνει κάποια αλλαγή στην καθημερινή πρακτική ή στην τεχνολογία. |
| Φυσικές διασφαλίσεις | • Η εγκατάσταση διαθέτει ανεπαρκείς κλειδαριές και άλλα εμπόδια στην πρόσβαση των δεδομένων των ασθενών.<br>• Οι υπολογιστές είναι εύκολα προσβάσιμοι στο κοινό.<br>• Οι φορητές συσκευές δεν παρακολουθούνται και δεν κλειδώνονται όταν δε χρησιμοποιούνται. | • Εγκατάσταση συστήματος συναγερμού.<br>• Κλείδωμα γραφείων.<br>• Οι οθόνες των υπολογιστών προστατεύονται από ξένους θεατές. |
| Τεχνικές εγγυήσεις | • Οι φτωχοί έλεγχοι επιτρέπουν την ακατάλληλη | • Εξασφάλιση ταυτότητας των χρηστών, κωδικών |

| | | |
|---|---|---|
| | πρόσβαση στις ηλεκτρονικές πληροφορίες των ασθενών.<br>• Τα αρχεία καταγραφής ελέγχου δε χρησιμοποιούνται συχνά για να παρακολουθούν τους χρήστες και τις δραστηριότητές τους.<br>• Δεν υπάρχουν μέτρα που να προστατεύουν τις ηλεκτρονικές πληροφορίες από ακατάλληλες αλλαγές.<br>• Δεν υπάρχει σχέδιο έκτακτης ανάγκης.<br>• Οι ηλεκτρονικές ανταλλαγές ιατρικών αρχείων δεν είναι κρυπτογραφημένες ή ασφαλείς. | πρόσβασης και πρόσβαση στα αρχεία μόνο εξουσιοδοτημένων χρηστών.<br>• Τακτικοί έλεγχοι πρόσβασης και αλλαγών σε αρχεία που αφορούν τις ηλεκτρονικές πληροφορίες των ασθενών.<br>• Εγκατάσταση λογισμικού για προστασία από εισβολείς και από κακόβουλο λογισμικό.<br>• Ανάπτυξη σχεδίου έκτακτης ανάγκης και δημιουργία αντιγράφων ασφάλειας.<br>• Κρυπτογράφηση δεδομένων |
| Οργανωτικά πρότυπα | • Δεν υπάρχει ειδοποίηση και ανάλογες πολιτικές για την παραβίαση δεδομένων.<br>• Οι συμφωνίες επιχειρηματικών | • Διεξαγωγή τακτικών αναθεωρήσεων των συμφωνιών και τακτική ενημέρωσή τους. |

| | | |
|---|---|---|
| | συνεργατών δεν έχουν ενημερωθεί εδώ και πολλά χρόνια. | |
| Πολιτικές και διαδικασίες | • Ενώ αγοράστηκαν πολιτικές και διαδικασίες για τη συμμόρφωση με τους κανόνες ασφάλειας, δεν τηρήθηκαν. | • Υλοποίηση γραπτών πολιτικών και διαδικασιών και κατάλληλη εκπαίδευση του προσωπικού.<br>• Μηνιαία αναθεώρηση των δραστηριοτήτων των χρηστών από την ομάδα ασφάλειας.<br>• Οι καθημερινές ενημερώσεις γίνονται για να τεκμηριώσουν τα μέτρα ασφάλειας. |

Πολλές φορές για να αντιμετωπιστεί μία μεμονωμένη ευπάθεια μπορεί να χρειαστεί ο συνδυασμός μέτρων προστασίας που αντιστοιχούν σε πολλαπλά συστατικά ασφάλειας, καθώς οι συνιστώσες ασφάλειας είναι αλληλένδετες. Αυτό συμβαίνει και κατά την ανάπτυξη σχεδίου έκτακτης δράσης.

Η διαδικασία που ακολουθείται για την ανάπτυξη σχεδίου δράσης είναι η εξής:

1. Ο υπεύθυνος ασφάλειας πρέπει να συγκαλέσει την ομάδα για να αναπτύξουν το σχέδιο δράσης ασφάλειας. Η αρχή γίνεται με τον εντοπισμό των απλούστερων δράσεων που θα οδηγήσουν στο μετριασμό των μεγαλύτερων κινδύνων.
2. Αν η ομάδα δεν ξέρει πώς πρέπει να εντάξει τους κανόνες και νόμους ασφάλειας προσωπικών δεδομένων στο σχέδιο δράσης, πρέπει να

συμβουλευτεί τον επαγγελματία ανάλυσης κινδύνου ή κάποιο νομικό σύμβουλο.

3. Όταν γραφτεί το σχέδιο δράσης, η ορισμένη ομάδα ασφάλειας θα πρέπει να συνεδριάζει περιοδικά για να συντονίζει τις ενέργειες, να επεξεργάζεται απροσδόκητα σφάλματα και να παρακολουθεί την πρόοδό της. Όταν πετυχαίνει τους στόχους της, η ομάδα ασφάλειας πρέπει να επιβραβεύεται. Πρέπει να γίνει κατανοητό ότι η εξάλειψη των κινδύνων δεν είναι δυνατή. Ωστόσο, με τη λήψη κατάλληλων μέτρων μπορούν να περιοριστούν.

Ε. Διαχείριση και μετριασμός των κινδύνων:

Η διαχείριση και ο μετριασμός των κινδύνων περιλαμβάνουν 4 βήματα:

I. Εφαρμογή του σχεδίου δράσης
II. Αποτροπή παραβιάσεων με την εκπαίδευση και κατάρτιση του προσωπικού
III. Επικοινωνία με τους ασθενείς
IV. Ενημέρωση των συμβολαίων με τους επιχειρηματικούς συνεργάτες

I. Εφαρμογή του σχεδίου δράσης:

Η εφαρμογή του σχεδίου δράσης περιλαμβάνει όλα τα στοιχεία που αναφέρθηκαν προηγουμένως σχετικά με τις διοικητικές διασφαλίσεις, φυσικές διασφαλίσεις, τεχνικές εγγυήσεις, οργανωτικά πρότυπα, πολιτικές και διαδικασίες. Όλα αυτά θα βοηθήσουν στον προσδιορισμό, αξιολόγηση και διαχείριση των κινδύνων με απώτερο στόχο την προστασία των ηλεκτρονικών αρχείων των ασθενών. Η εφαρμογή του σχεδίου δράσης περιλαμβάνει:

- ✓ Απαραίτητες ρυθμίσεις ασφάλειας των ηλεκτρονικών πληροφοριών στα Πληροφοριακά Συστήματα: Όταν ένα Πληροφοριακό Σύστημα είναι πιστοποιημένο, έχει ένα πακέτο βασικών λειτουργιών τεχνικής ασφάλειας που δίνει τη δυνατότητα επαλήθευσης των χρηστών με έγκυρους λογαριασμούς. Ωστόσο, το γεγονός ότι ένα Πληροφοριακό Σύστημα είναι πιστοποιημένο δε σημαίνει ότι είναι σύμφωνο με τους κανόνες ασφάλειας.

Επίσης, η πιστοποίηση δεν εγγυάται την απόδοση ή την αξιοπιστία των λειτουργιών ασφάλειας, καθώς οι λειτουργίες που είναι σημαντικές για τη συμμόρφωση με την προστασία προσωπικών δεδομένων μπορεί να είναι απενεργοποιημένες ή ρυθμισμένες σε χαμηλό επίπεδο. Επομένως, η ανάλυση κινδύνου πρέπει να εξετάσει διεξοδικά την επάρκεια των μέτρων προστασίας των ηλεκτρονικών πληροφοριών, καθώς τα Πληροφοριακά Συστήματα μεταδίδουν, αποθηκεύουν και επιτρέπουν τροποποιήσεις των ηλεκτρονικών πληροφοριών.

- ✓ Γραπτές πολιτικές και διαδικασίες: Οι γραπτές πολιτικές και διαδικασίες ορίζουν πώς πρέπει να είναι η λειτουργία σε καθημερινή βάση και πρέπει να περιλαμβάνουν τουλάχιστον τα παρακάτω:
    - Καθιέρωση πρωτοκόλλων για τα πέντε συστατικά ασφάλειας (διοικητικές διασφαλίσεις, φυσικές διασφαλίσεις, τεχνικές εγγυήσεις, οργανωτικά πρότυπα, πολιτικές και διαδικασίες).
    - Δέσμευση για κατάρτιση του νέου προσωπικού πάνω στους κανόνες ασφάλειας και για τακτική εκπαίδευση όλου του προσωπικού.
    - Καθιέρωση του τι πρέπει να γίνει όταν υποβαθμίζεται η ακεραιότητα, διαθεσιμότητα και εμπιστευτικότητα των ηλεκτρονικών πληροφοριών των ασθενών.
    - Καθιέρωση κυρώσεων και εφαρμογή τους για όποιον παραβιάζει τους κανόνες απορρήτου και ασφάλειας.
    - Οι πολιτικές και οι διαδικασίες πρέπει να περιλαμβάνουν λεπτομερώς όλα τα στοιχεία των Πληροφοριακών Συστημάτων, ξεκινώντας από τη χρήση καταγραφής των αρχείων ελέγχου καταγραφής και καταλήγοντας στην παρακολούθηση της πρόσβασης, χρήσης και διάθεσης των ηλεκτρονικών πληροφοριών.
    - Επισήμανση της ανάγκης για γραπτές συμφωνίες με τους επιχειρηματικούς συνεργάτες που αναφέρουν λεπτομερώς την ευθύνη τους να συμμορφώνονται με τους κανόνες ιδιωτικότητας και ασφάλειας.

II. Αποτροπή παραβιάσεων με την εκπαίδευση και κατάρτιση του προσωπικού:

Η κατάρτιση και εκπαίδευση του προσωπικού αποτελεί σημαντικό βήμα στη διαχείριση των κινδύνων. Απευθύνεται σ' όλα τα άτομα που ασχολούνται με τα Πληροφοριακά Συστήματα των Νοσοκομείων (εργαζόμενοι, εργολάβοι, εθελοντές, εκπαιδευόμενοι) και τα προετοιμάζει για:

- Τους ρόλους και τις ευθύνες τους σχετικά με τη διαφύλαξη των αρχείων των ασθενών
- Τη συμμόρφωσή τους με τους κανόνες και τις πολιτικές ασφάλειας
- Τις διαδικασίες που πρέπει να ακολουθούν για την παρακολούθηση τήρησης των κανόνων ασφάλειας
- Τα βήματα που πρέπει να ακολουθούν όταν παρατηρούνται παραβιάσεις.

Η εκπαίδευση και κατάρτιση του προσωπικού πρέπει να γίνεται τη στιγμή της πρόσληψης κάθε εργαζομένου. Από τη στιγμή της πρόσληψης και ύστερα, πρέπει να γίνεται μία φορά το χρόνο και κάθε φορά που αλλάζουν οι διαδικασίες, τα συστήματα, η τοποθεσία, η υποδομή. Είναι πολύ σημαντικό το προσωπικό να ξέρει να ανταποκρίνεται άμεσα σε συμβάντα που δε συμβαδίζουν με τους κανόνες ασφάλειας ( όπως μη εξουσιοδοτημένη πρόσβαση ή αποκάλυψη των ηλεκτρονικών πληροφοριών των ασθενών) καθώς θα μπορούσαν να είναι πιθανές παραβιάσεις. Επίσης, είναι απαραίτητη η καθιέρωση μιας στάσης που να:

- Τονίζει τη σημασία της εμπιστοσύνης μεταξύ ασθενών και παρόχων υπηρεσιών υγείας
- Υπενθυμίζει συνεχώς στο προσωπικό τη σημασία διαφύλαξης της εμπιστευτικότητας και ασφάλειας των ηλεκτρονικών αρχείων των ασθενών
- Εξασφαλίζει την ύπαρξη αντιγράφων των διαδικασιών και πολιτικών και τη συμμόρφωση σ' αυτές
- Απαντά στα ερωτήματα του προσωπικού
- Αξιολογεί τις υπηρεσίες που προσφέρει κάθε μέλος του προσωπικού και επιτρέπει την πρόσβαση μόνο στις ηλεκτρονικές πληροφορίες των ασθενών που είναι απαραίτητες για το έργο του.

III. Επικοινωνία με τους ασθενείς:

Οι ασθενείς μπορεί να ανησυχούν για την εμπιστευτικότητα και ασφάλεια των πληροφοριών τους. Γι' αυτό είναι απαραίτητη η παροχή πληροφοριών στους ασθενείς σχετικά με την ασφάλεια των Πληροφοριακών Συστημάτων που χρησιμοποιούνται και η επισήμανση των οφελών που μπορεί να έχουν τα Πληροφοριακά Συστήματα στη ζωή των ασθενών. Σε περίπτωση που γίνει κάποια παραβίαση των δεδομένων των ασθενών, το προσωπικό του νοσοκομείο πρέπει να φροντίσει να διατηρήσει καλές σχέσεις με τους ασθενείς και τους συνοδούς τους. Αυτό θα γίνει με την τήρηση ενός πολύπλευρου σχεδίου που θα ασχολείται με την επικοινωνία των ασθενών και συνοδών με τους παρόχους υγειονομικής περίθαλψης. Αυτό το σχέδιο θα:

- Ενημερώνει τους ασθενείς ότι πρωταρχικός στόχος του συστήματος είναι η διαφύλαξη της ακεραιότητας, διαθεσιμότητας και εμπιστευτικότητας των ηλεκτρονικών τους πληροφοριών.
- Σέβεται το δικαίωμα των ασθενών να ενημερώνονται σχετικά με την υγεία τους. Αυτό μπορεί να γίνει είτε με εξασφάλιση της πρόσβασης των ασθενών στα ηλεκτρονικά αρχεία είτε με παροχή ενός αντιγράφου του ηλεκτρονικού φακέλου στους ασθενείς.
- Εκπαιδεύει τους ασθενείς στο πώς χρησιμοποιούνται οι πληροφορίες τους και πού μεταδίδονται. Πολλές φορές μπορεί να χρειαστεί η εξουσιοδότηση ή συγκατάθεση των ασθενών για τη μετάδοση των πληροφοριών τους.
- Φροντίζει για την ενημέρωση των ασθενών όταν έχει συμβεί κάποια παραβίαση των προσωπικών τους δεδομένων.

Για να είναι επιτυχής η επικοινωνία μεταξύ ασθενών και παρόχων υπηρεσιών υγείας θα πρέπει να έχουν ληφθεί υπόψιν οι γλώσσες επικοινωνίας, οι διάφορες ανάγκες του πληθυσμού και τα επίπεδα εμπιστοσύνης των ασθενών. Σε περίπτωση που υπάρχει έλλειψη εμπιστοσύνης από κάποια ομάδα ασθενών, πρέπει να ληφθούν επιπρόσθετα μέτρα που θα τους καθησυχάζουν ότι οι προσωπικές τους πληροφορίες προστατεύονται.

Στο πλαίσιο της επικοινωνίας με τους ασθενείς περιλαμβάνεται και η ενημέρωση των ασθενών σχετικά με τα δικαιώματά τους. Με την πάροδο του χρόνου, όλο και περισσότεροι ασθενείς αναμένεται να ρωτούν τους παρόχους υγειονομικής περίθαλψης σχετικά με τον τρόπο που αποθηκεύονται οι προσωπικές τους ηλεκτρονικές πληροφορίες, να απαιτούν αλλαγές στα ηλεκτρονικά τους αρχεία και να ζητούν αντίγραφα των αρχείων τους. Συγκεκριμένα, τα δικαιώματα των ασθενών όσον αφορά τις ηλεκτρονικές τους πληροφορίες είναι τα εξής:

- Οι ασθενείς μπορούν να ζητήσουν αντίγραφα και πρόσβαση στις ηλεκτρονικές τους πληροφορίες είτε σε ηλεκτρονική είτε σε έντυπη μορφή.
- Οι ηλεκτρονικές πληροφορίες των ασθενών που διατηρούνται στους ηλεκτρονικούς τους φακέλους θα πρέπει να τίθενται στη διάθεση των ασθενών κατόπιν αιτήματός τους.
- Οι ασθενείς μπορούν να ζητήσουν διορθώσεις και τροποποιήσεις στις ηλεκτρονικές τους πληροφορίες που υπάρχουν στα αρχεία τους. Το δικαίωμα αυτό ονομάζεται « Δικαίωμα Τροποποίησης».
- Σύμφωνα με τον Κανόνα Προστασίας Προσωπικών Δεδομένων, ο ασθενής μπορεί να αιτηθεί τον περιορισμό της υποβολής των ηλεκτρονικών του πληροφοριών στο σχέδιο υγείας του όταν ο ασθενής έχει πληρώσει όλα τα έξοδα για την υγειονομική υπηρεσία που θα λάβει. Ο πάροχος υγειονομικής περίθαλψης οφείλει να ικανοποιήσει αυτό το αίτημα.

Επιπλέον, στο πλαίσιο της επικοινωνίας με τους ασθενείς περιλαμβάνεται και η ηλεκτρονική επικοινωνία. Εάν οι πάροχοι υπηρεσιών υγείας σκοπεύουν να επικοινωνούν με τους ασθενείς τους ηλεκτρονικά, μέσω ηλεκτρονικού ταχυδρομείου, γραπτών μηνυμάτων, κοινωνικών μέσων, τότε πρέπει να συμβαδίζουν με τον Κανόνα Ασφάλειας και να κάνουν χρήση κατάλληλων προτύπων έτσι ώστε να διατηρούνται ασφαλείς οι ηλεκτρονικές πληροφορίες των ασθενών. Η ανταλλαγή ηλεκτρονικών μηνυμάτων μεταξύ διαφόρων παρόχων υγειονομικής περίθαλψης ή μεταξύ παρόχου υγειονομικής περίθαλψης και ασθενών αποτελεί έναν κίνδυνο ασφάλειας για τις ηλεκτρονικές πληροφορίες, κυρίως όταν τα δεδομένα δεν είναι κρυπτογραφημένα.

IV. Ενημέρωση των συμβολαίων με τους επιχειρηματικούς συνεργάτες:

Οι συμφωνίες που γίνονται με τους επιχειρηματικούς συνεργάτες πρέπει να συμμορφώνονται με την προστασία απορρήτου, ασφάλειας και παραβίασης προσωπικών δεδομένων. Γι' αυτό, πρέπει να τηρούν τα παρακάτω κριτήρια:

- Πρέπει να συμμορφώνονται πλήρως με τους κανόνες ασφάλειας των ηλεκτρονικών πληροφοριών.
- Πρέπει να αναλαμβάνουν την εκπαίδευση του προσωπικού.
- Πρέπει να λαμβάνουν επιπρόσθετα μέτρα για τη διαφύλαξη των δικαιωμάτων των ασθενών και την αποφυγή παραβίασης προσωπικών δεδομένων.

ΣΤ. Προσδιορισμός της σημασίας ύπαρξης ασφάλειας:

Ο προσδιορισμός της σημασίας ύπαρξης ασφάλειας γίνεται με τα προγράμματα παροχής κινήτρων, τα οποία αποδεικνύουν την υιοθέτηση, εφαρμογή, αναβάθμιση και ουσιαστική χρήση των κανόνων ασφάλειας. Αυτά τα προγράμματα έχουν σχεδιαστεί για να υποστηρίξουν τους παρόχους υπηρεσιών υγείας σχετικά με τη μετάβαση της τεχνολογίας των ηλεκτρονικών πληροφοριών και να εγκαταστήσουν τη χρήση των ηλεκτρονικών αρχείων έτσι ώστε να βελτιώσουν την ποιότητα, ασφάλεια και αποτελεσματικότητα της υγειονομικής περίθαλψης των ασθενών. Οι πάροχοι υπηρεσιών υγείας μπορούν να εγγραφούν σ' αυτά τα προγράμματα όποτε θέλουν αλλά η βεβαίωση απαιτεί να έχουν συμμορφωθεί με τις απαιτήσεις κατάλληλης χρήσης για μία περίοδο αναφοράς. Επομένως, οι πάροχοι υγείας λαμβάνουν βεβαίωση ότι έχουν παρακολουθήσει ένα πρόγραμμα παροχής κινήτρων μόνο όταν έχουν πραγματοποιήσει ανάλυση κινδύνου ασφάλειας και έχουν καταγράψει τις προσπάθειές τους να διορθώσουν τυχόν ελλείψεις. Η λήψη αυτής της βεβαίωσης αποτελεί μία νομική δήλωση ότι οι πάροχοι έχουν εκπληρώσει συγκεκριμένα πρότυπα σχετικά με την προστασία ηλεκτρονικών πληροφοριών υγείας. Σε περίπτωση που κάποιος πάροχος λάβει βεβαίωση χωρίς να έχει συμμορφωθεί με τους κανόνες, θα μπορούσε να αυξήσει την ευθύνη της επιχείρησής του για παραβίαση του νόμου και υποβολής ψευδούς αξίωσης. Γι'

αυτό, πριν τη λήψη βεβαίωσης πρέπει να έχουν εφαρμοστεί πολλαπλά μέτρα ασφάλειας. Πρωταρχικός στόχος αυτών των προγραμμάτων είναι η μείωση των υψηλών κινδύνων.

Ζ. Παρακολούθηση, έλεγχος και ενημέρωση της ασφάλειας σε συνεχή βάση:

Άλλη μία απαίτηση του Κανόνα Ασφάλειας είναι να βρίσκονται σε εφαρμογή οι έλεγχοι και να έχουν τη δυνατότητα να ελέγχουν όταν χρειάζεται. Η έννοια του ελέγχου στους Κανόνες Ασφάλειας έχει δύο ερμηνείες.

Σε πρώτο πλαίσιο, ο έλεγχος σχετίζεται με την ασφάλεια και αποτελεσματικότητα της υποδομής της ασφάλειας και κάνει τις απαραίτητες αλλαγές όπου χρειάζονται. Ο υπεύθυνος ασφάλειας, ο διαχειριστής πληροφορικής και ο υπεύθυνος για την ανάπτυξη των ηλεκτρονικών αρχείων πρέπει να συνεργάζονται ώστε οι λειτουργίες ελέγχου να είναι ενεργοποιημένες και να γίνονται τροποποιήσεις ανάλογα με τις ανάγκες. Αυτοί σε συνεργασία με τους παρόχους υπηρεσιών υγείας:

- Αποφασίζουν αν θα διεξάγουν εσωτερικούς ελέγχους ή θα χρησιμοποιήσουν σύμβουλο για την ασφάλεια πληροφοριών ή θ κάνουν συνδυασμό και των δύο.
- Καθορίζουν τι θα ελεγχθεί και πώς θα γίνει η διαδικασία ελέγχου.
- Υποδεικνύουν συγκεκριμένους δείκτες και συγκεκριμένα σημάδια που δείχνουν ότι οι ηλεκτρονικές πληροφορίες των ασθενών ενδέχεται να έχουν υπονομευτεί και χρειάζεται περαιτέρω διερεύνηση.
- Καθιερώνουν ένα συγκεκριμένο χρονοδιάγραμμα για ελέγχους ρουτίνας και κατευθυντήριες οδηγίες για τυχαίους ελέγχους.

Στο δεύτερο πλαίσιο, ο έλεγχος είναι υπεύθυνος να εξετάσει το τι συνέβη. Αυτό σημαίνει ότι τα ηλεκτρονικά αρχεία πρέπει να δημιουργηθούν για να υπάρχει τεκμηρίωση σχετικά με το ποιος, τι, πότε, πώς έχει πρόσβαση στις ηλεκτρονικές

πληροφορίες των ασθενών. Αυτοί οι έλεγχοι απαιτούν τεχνικές δυνατότητες ασφάλειας, οι οποίες περιλαμβάνουν ελεγκτικά συμβάντα και αντίσταση σε οποιαδήποτε παραβίαση, αρχεία καταγραφής ελέγχου, ελέγχους πρόσβασης, εξουσιοδοτήσεις, αυτόματη απενεργοποίηση και πρόσβαση σε περίπτωση έκτακτης ανάγκης.

Σε αυτό το στάδιο, περιλαμβάνεται επίσης η σωστή διατήρηση των ιατρικών αρχείων. Σύμφωνα με το κρατικό δίκαιο, τα ιατρικά αρχεία πρέπει να διατηρούνται για συγκεκριμένο αριθμό ετών. Αυτό το χρονικό διάστημα αλλά και οι υποχρεώσεις των παρόχων υγειονομικής περίθαλψης τροποποιείται ανάλογα και με τους νόμους διατήρησης ιατρικών αρχείων του κράτους. Εάν γίνεται ηλεκτρονική ανταλλαγή προσωπικών δεδομένων, τότε θα πρέπει να επιστρέφονται ή να διατίθενται με ασφάλεια οι ηλεκτρονικές πληροφορίες που δημιουργούνται, λαμβάνονται, διατηρούνται ή μεταδίδονται. (11)

## 8.4.Πολιτική ασφάλειας υψηλού επιπέδου SEISMED

Το πρόγραμμα SEISMED ( Ασφαλές Περιβάλλον για τα Πληροφοριακά Συστήματα στην Ιατρική) είναι μία πολιτική ασφαλείας που εφαρμόζεται σε πολλά νοσοκομεία σ’ όλη την Ευρώπη. (7) Ο στόχος του προγράμματος SEISMED όταν δημιουργήθηκε ήταν να αναπτυχθεί ένα πλαίσιο, το οποίο θα αποτελείται από τεχνικές διαδικασίες και οργανωτικά μέτρα που μπορούν να χρησιμοποιηθούν για την αποτελεσματική εφαρμογή της ασφάλειας και προστασίας των δεδομένων σε αυτοματοποιημένα πληροφοριακά συστήματα νοσοκομείων σε όλη την Ευρώπη. Η πολιτική ασφάλειας υψηλού επιπέδου SEISMED απευθύνεται σε τρεις ομάδες ατόμων:

- Στη διοίκηση των μονάδων υγείας (όπως διοικητής νοσοκομείου κλπ)
- Στους χρήστες των Πληροφοριακών Συστημάτων των Νοσοκομείων (όπως ασθενείς, νοσηλευτές, ιατροί κλπ)

- Στο προσωπικό ασφάλειας και στο προσωπικό που ασχολείται με τα Πληροφοριακά Συστήματα των Νοσοκομείων (όπως διαχειριστές πληροφοριακού συστήματος, άτομα που σχετίζονται με την ανάπτυξη του λογισμικού κλπ)

Το πλαίσιο των κατευθυντήριων οδηγιών που αναπτύχθηκε ήταν αποτέλεσμα των παρακάτω:

- Του εντοπισμού των τρεχουσών πρακτικών ατόμων που εμπλέκονται στην υγειονομική περίθαλψη
- Της εξέτασης των ευρωπαϊκών νομοθεσιών που σχετίζονται με την προστασία και των κωδίκων δεοντολογίας
- Της λεπτομερούς ανάλυσης κινδύνου που έλαβε χώρα σε 4 οργανισμούς υγειονομικής περίθαλψης

Ως αποτέλεσμα των παραπάνω στοιχείων προέκυψε η δημιουργία του προγράμματος SEISMED που περιλάμβανε τις εξής κατευθυντήριες οδηγίες:

- Κώδικας δεοντολογίας για την Πληροφορική της Υγείας
- Πολιτική ασφάλειας υψηλού επιπέδου για τις μονάδες υγειονομικής περίθαλψης
- Πώς να πραγματοποιηθούν αξιολογήσεις κινδύνων για τα Πληροφοριακά Συστήματα που χρησιμοποιούνται σε μονάδες υγειονομικής περίθαλψης
- Πώς να συμπεριληφθεί η ασφάλεια στην ανάπτυξη, προμήθεια και υλοποίηση ενός συστήματος
- Πώς να ενσωματωθεί αναδρομικά η ασφάλεια στα ήδη υπάρχοντα Πληροφοριακά Συστήματα στο χώρο της υγείας
- Πώς να επιτευχθεί ασφάλεια στα συστήματα που χρησιμοποιούνται ήδη

- Συστάσεις για τη χρήση της κρυπτογραφίας μέσω της χρήσης ενός πρωτότυπου

Οι αρχές στις οποίες βασίζεται η πολιτική ασφάλειας υψηλού επιπέδου SEISMED αναλύονται παρακάτω:

- Κώδικας καλής πρακτικής, ο οποίος περιλαμβάνει καλές πρακτικές για την προστασία των ιατρικών δεδομένων και πρέπει να υπάρχει σε κάθε μονάδα υγειονομικής περίθαλψης.
- Συμβατικοί κανονισμοί, οι οποίοι περιγράφουν λεπτομερώς και εγγράφως τα καθήκοντα και τις ευθύνες κάθε μέλους του προσωπικού του νοσοκομείου που σχετίζεται με τις ιατρικές πληροφορίες των ασθενών.
- Αρχή προστασίας δεδομένων, η οποία πρέπει να καθιερωθεί σε κάθε μονάδα φροντίδας υγείας και σκοπό θα έχει να προστατεύει τα προσωπικά και απόρρητα ιατρικά δεδομένα και να ελέγχει αν εφαρμόζεται ο κώδικας καλής πρακτικής.
- Εκπαίδευση και ενημέρωση τόσο του προσωπικού του νοσοκομείου όσο και του δημοσίου κοινού σχετικά με τη σημασία της ύπαρξης ασφάλειας και εξασφάλισης της ιδιωτικότητας των πληροφοριών.
- Περιορισμένη κυκλοφορία δεδομένων, καθώς οι ιατρικές πληροφορίες αποτελούν ευαίσθητα και προσωπικά δεδομένα. Θα πρέπει να μεταδίδονται μόνο όταν είναι αναγκαίο και η μετάδοσή τους να βασίζεται στον κώδικα δεοντολογίας και σε άλλους κανόνες που διασφαλίζουν την προστασία και ιδιωτικότητάς τους.
- Δικαιώματα των ασθενών, τα οποία πρέπει να προστατεύονται στους χώρους παροχής υγειονομικής περίθαλψης.
- Ποιότητα των δεδομένων υγείας, δηλαδή επεξεργασία και αποθήκευση των δεδομένων υγείας με έναν τρόπο που να εξασφαλίζεται η ακεραιότητα και ακρίβειά τους.
- Ιατρική και επιδημιολογική έρευνα, δηλαδή συλλογή των ιατρικών στοιχείων των ασθενών για ερευνητικούς σκοπούς εφόσον οι ασθενείς έχουν δηλώσει τη συγκατάθεσή τους. Πρώτα, όμως, θα πρέπει να έχουν ενημερωθεί οι

ασθενείς σχετικά με το δικαίωμά τους να αρνηθούν τη μετάδοση των ιατρικών τους πληροφοριών, να αποκτήσουν πρόσβαση στα αρχεία τους, καθώς και να προτείνουν διορθώσεις σε αυτά.

- Κανονισμοί ασφάλειας, δηλαδή λήψη μέτρων για να αποφευχθεί η άρνηση των υπηρεσιών του συστήματος, η τυχαία ή σκόπιμη καταστροφή των δεδομένων, η πρόσβαση στα αρχεία μη εξουσιοδοτημένων χρηστών, η κοινοποίηση των ιατρικών αρχείων, η τυχαία ή σκόπιμη αλλαγή των δεδομένων και τέλος η δημιουργία δεδομένων από μη εξουσιοδοτημένα άτομα. (7)

# ΚΕΦΑΛΑΙΟ 9. ΜΕΤΡΑ ΠΡΟΣΤΑΣΙΑΣ ΠΛΗΡΟΦΟΡΙΑΚΩΝ ΣΥΣΤΗΜΑΤΩΝ ΝΟΣΟΚΟΜΕΙΩΝ

## 9.1.Εισαγωγή κεφαλαίου 9

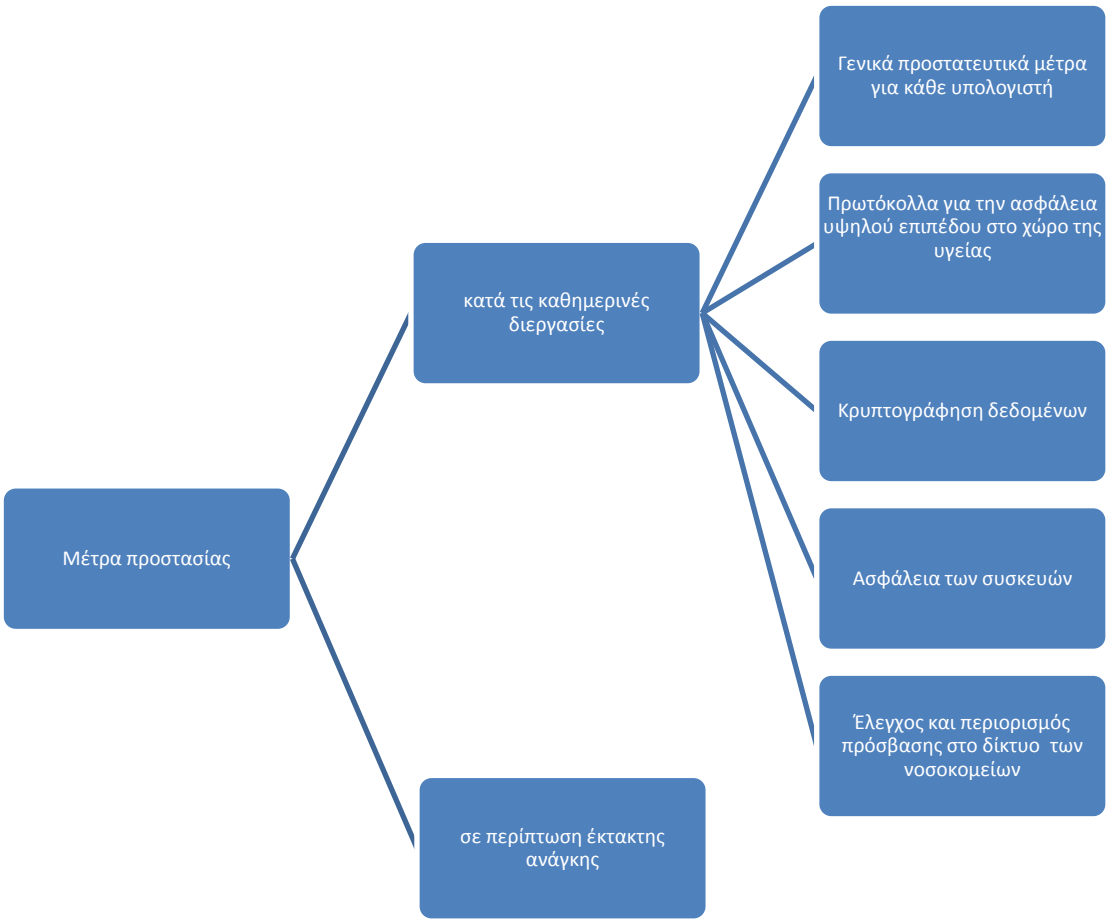
Ένα ολοκληρωμένο σχέδιο ασφάλειας των Πληροφοριακών Συστημάτων στα Νοσοκομεία απαρτίζεται από την εφαρμογή μιας πολιτικής ασφάλειας και τη λήψη μέτρων προστασίας. Στο κεφάλαιο 8 μελετήθηκε η εφαρμογή μιας πολιτικής ασφάλειας στο χώρο του νοσοκομείου. Σ’ αυτό το κεφάλαιο θα μελετηθεί η λήψη μέτρων προστασίας των Πληροφοριακών Συστημάτων στα Νοσοκομεία. Όπως αναλύθηκε στην υποενότητα 7.4 του κεφαλαίου 7, η ασφάλεια διακρίνεται στην ασφάλεια σε περίπτωση έκτακτης ανάγκης και στην ασφάλεια στις καθημερινές διεργασίες. Για να είναι λοιπόν επαρκής η λήψη μέτρων προστασίας, θα πρέπει να ληφθούν μέτρα τόσο κατά τις καθημερινές διεργασίες όσο και σε περίπτωση έκτακτης ανάγκης. Τα μέτρα προστασίας κατά τις καθημερινές διεργασίες αναλύονται στην υποενότητα 9.2 του κεφαλαίου, ενώ τα μέτρα προστασίας σε περίπτωση έκτακτης ανάγκης στην υποενότητα 9.3.

## 9.2.Μέτρα προστασίας κατά τις καθημερινές διεργασίες

Τα μέτρα προστασίας περιλαμβάνονται στην πολιτική ασφαλείας και σχετίζονται με την καθημερινή χρήση των Πληροφοριακών Συστημάτων στα νοσοκομεία είναι τα παρακάτω:

- Γενικά προστατευτικά μέτρα για κάθε υπολογιστή
- Έλεγχος και περιορισμός πρόσβασης στο δίκτυο των νοσοκομείων
- Ασφάλεια των συσκευών
- Κρυπτογράφηση δεδομένων
- Πρωτόκολλα για την ασφάλεια υψηλού επιπέδου στο χώρο της υγείας (7)

**Εικόνα 8.Διάκριση μέτρων προστασίας Πληροφοριακών Συστημάτων Νοσοκομείων (7)**



### 9.2.1. Γενικά προστατευτικά μέτρα για κάθε υπολογιστή

**Α. Επιλογή κατάλληλων κωδικών πρόσβασης (passwords)**

Για κάθε ίδρυμα υπηρεσιών υγείας κρίνεται επιτακτική η προστασία κάθε υπολογιστή τόσο από οποιονδήποτε προσπαθεί να αποκτήσει πρόσβαση σε αυτόν μη εξουσιοδοτημένα όσο κι από απειλές κι επιθέσεις μέσω του διαδικτύου. Οι κωδικοί πρόσβασης είναι η πρώτη γραμμή άμυνας για την αποτροπή μη εξουσιοδοτημένης πρόσβασης σε οποιονδήποτε υπολογιστή. Ανεξάρτητα από τον τύπο ή το λειτουργικό σύστημα, θα πρέπει να απαιτείται κωδικός πρόσβασης για να συνδεθεί ο χρήστης. Ακόμα και αν είναι ισχυρός ο κωδικός πρόσβασης, δε θα εμποδίσει τους εισβολείς να προσπαθήσουν να αποκτήσουν πρόσβαση. Μπορεί, όμως, να τους επιβραδύνει και να τους αποθαρρύνει. Επιπλέον, οι ισχυροί κωδικοί πρόσβασης, σε συνδυασμό με τους αποτελεσματικούς ελέγχους πρόσβασης, συμβάλλουν στη μείωση των περιπτώσεων κακής χρήσης των Πληροφοριακών Συστημάτων. Είναι, λοιπόν, πασιφανής η ανάγκη αυθεντικότητας του κάθε χρήστη κι ο πλέον συνηθισμένος μηχανισμός αυθεντικότητας είναι ο κωδικός πρόσβασης (password). (15)

Τα passwords είναι κωδικοποιημένες λέξεις που έχουν αμοιβαία συμφωνηθεί και θεωρούνται γνωστά μόνο στο χρήστη και στο σύστημα. Οι συνηθέστερες επιθέσεις στα passwords (password attacks) είναι δύο ειδών:

Α) Οι εξαντλητικές επιθέσεις (brute force attacks) κατά τις οποίες οι επιτιθέμενοι δοκιμάζουν όλα τα δυνατά passwords χτυπώντας όλους τους πιθανούς συνδυασμούς χαρακτήρων με δεδομένα ένα σετ χαρακτήρων (π.χ. abcd… ή ABCD… ή 1234 ή !@#$... κλπ. ) κι ένα μέγιστο αριθμό χαρακτήρων (password length).

Β) Οι επιθέσεις καταλόγου (dictionary attacks) οι οποίες λειτουργούν με το σκεπτικό ότι τα passwords αποτελούνται από λέξεις, ημερομηνίες ή/και αριθμούς που βρίσκονται σε κάποιο κατάλογο ή λίστα (π.χ αγγλικό λεξιλόγιο, τηλεφωνικός κατάλογος κλπ.)**.** Έτσι, οι επιθέσεις γίνονται χτυπώντας κατά σειρά όλα τα στοιχεία της επιλεχθείσας βάσης δεδομένων. (16)

Ένας ισχυρός κωδικός πρόσβασης είναι αυτός που δεν μπορεί εύκολα να προβλεφθεί. Επειδή οι εισβολείς χρησιμοποιούν αυτοματοποιημένες μεθόδους για να καταφέρουν να μαντέψουν έναν κωδικό πρόσβασης, πρέπει ο κωδικός πρόσβασης να αποτελείται από χαρακτηριστικά που δεν τον κάνουν ευάλωτο στους εισβολείς.

Επτά συμβουλές για την επιλογή κωδικών πρόσβασης είναι:

- Χρήση και άλλων χαρακτήρων εκτός από τα A-Z
- Επιλογή μεγάλων passwords (τουλάχιστον 8 χαρακτήρων)
- Αποφυγή πραγματικών ονομάτων ή λέξεων
- Επιλογή ενός απίθανου password
- Τακτική αλλαγή password
- Μην γράφετε το password
- Μην πείτε το password σε κανέναν άλλο .

Για κάθε οργανισμό, υπάρχει μια συγκεκριμένη πολιτική που καθορίζει τον τρόπο που πρέπει να είναι ο κωδικός πρόσβασης αλλά και τη συμπεριφορά των χρηστών των Πληροφοριακών Συστημάτων. Πιο αναλυτικά:

- Όλα τα μέλη του προσωπικού κατανοούν και συμφωνούν να συμμορφώνονται με τις πολιτικές του κωδικού πρόσβασης.
- Κάθε μέλος του προσωπικού έχει ένα μοναδικό όνομα χρήστη και ένα μοναδικό κωδικό πρόσβασης.
- Οι κωδικοί πρόσβασης δεν πρέπει να αποκαλύπτονται και να μοιράζονται με άλλους.
- Οι κωδικοί πρόσβασης δεν πρέπει να καταγράφονται και να εκτίθενται στην οθόνη του υπολογιστή.
- Οι κωδικοί πρόσβασης πρέπει να είναι δύσκολο να προβλεφθούν από τους άλλους, αλλά εύκολο να τους θυμηθούμε.
- Οι κωδικοί πρόσβασης πρέπει να αλλάζουν συχνά και να μην επαναχρησιμοποιούνται.

- Όλοι οι προεπιλεγμένοι κωδικοί πρόσβασης που συνοδεύουν ένα προϊόν πρέπει να αλλάζουν κατά τη διάρκεια εγκατάστασης του προϊόντος.

**Β. Χρήση τοίχου/αναχώματος προστασίας ( firewall)**

Ο κύριος τρόπος με τον οποίον οι εισβολείς θέτουν σε κίνδυνο τους υπολογιστές είναι μέσω των ιών, οι οποίοι τείνουν να εκμεταλλεύονται τις ευπάθειες των υπολογιστών. Ακόμα και οι υπολογιστές που είναι πλήρως ενημερωμένοι σε θέματα ασφάλειας και έχουν τις πιο πρόσφατες ενημερώσεις στο λειτουργικό σύστημα και τις εφαρμογές, μπορεί να διατρέχουν κίνδυνο εξαιτίας μη ανιχνεύσιμων ελαττωμάτων. Επιπλέον, οι υπολογιστές μπορούν εύκολα να μολυνθούν από φαινομενικά «αθώες» εξωτερικές πηγές, όπως είναι τα CDs, οι μονάδες flash, το ηλεκτρονικό ταχυδρομείο και οι λήψεις αρχείων από το διαδίκτυο.

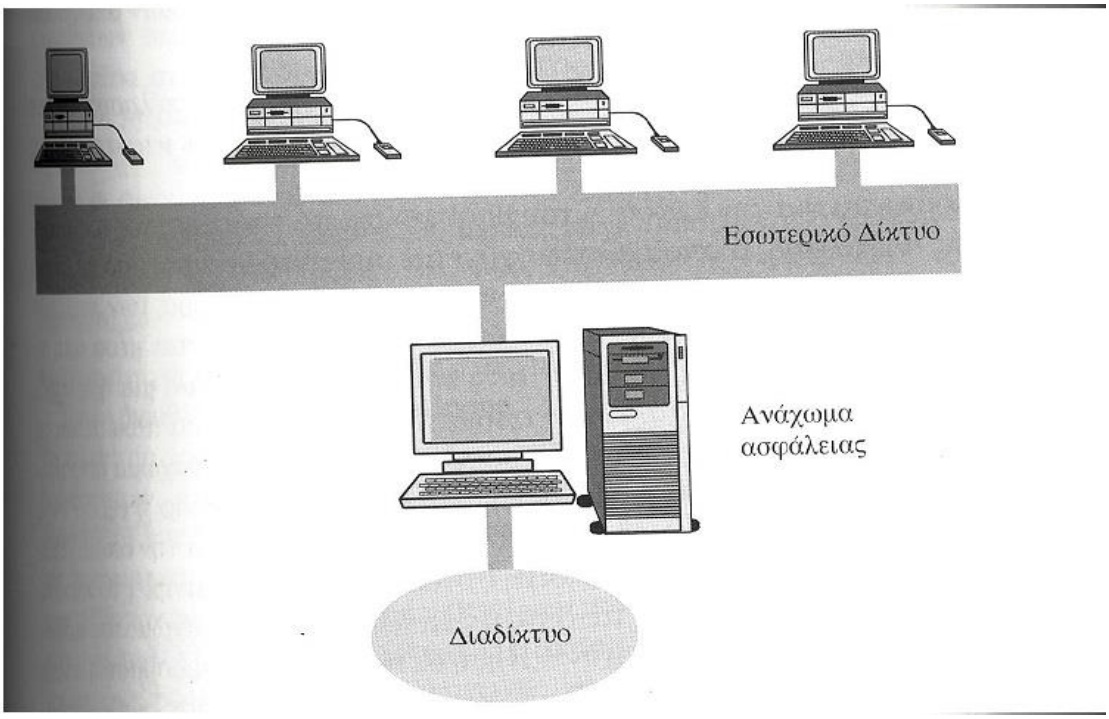
Σε πρώτη φάση είναι απαραίτητη η αποτροπή των εισβολέων, η οποία μπορεί να επιτευχθεί με τη χρήση ενός τοίχου προστασίας. (15 ) Ο τοίχος προστασίας είναι μία διάταξη εξειδικευμένων μηχανισμών ασφάλειας που ελέγχει την πρόσβαση και μετακίνηση των πληροφοριών ανάμεσα σε δύο δίκτυα, είτε τα εμπιστευόμαστε είτε όχι. Σκοπός του είναι να εφαρμόζει τους κανόνες που αναφέρονται στην πολιτική ασφάλειας. (7) Μπορεί να έχει τη μορφή ενός προϊόντος λογισμικού ή μιας συσκευής υλικού. Όποια μορφή και να έχει, σκοπός του είναι να ελέγξει όποια στοιχεία εισέρχονται από εξωτερικές πηγές (είτε από το διαδίκτυο είτε από τοπικές πηγές) και να κρίνει με βάση συγκεκριμένα κριτήρια αν τα στοιχεία επιτρέπεται να εισέρθουν στον υπολογιστή.

- Τοίχος προστασίας υλικού (hardware firewall): Οι μεγάλοι οργανισμοί, όπως είναι τα νοσοκομεία, πρέπει να χρησιμοποιούν τοίχο προστασίας υλικού. Ο τοίχος προστασίας υλικού βρίσκεται μεταξύ του τοπικού δικτύου και του διαδικτύου παρέχοντας κεντρική διαχείριση των ρυθμίσεων του τοίχου προστασίας και εξασφαλίζοντας ότι οι ρυθμίσεις του τοίχου προστασίας είναι ίδιες για όλους τους χρήστες. Μ’ αυτόν τον τρόπο, αυξάνεται η

ασφάλεια του τοπικού δικτύου. Σε περίπτωση που ένας οργανισμός χρησιμοποιεί τοίχο προστασίας υλικού, θα πρέπει να διαμορφώνεται, παρακολουθείται και συντηρείται από ειδικό.

- Τοίχος προστασίας λογισμικού (software firewall): Οι τοίχοι προστασίας λογισμικού έχουν προκαθοριστεί με κοινές ρυθμίσεις που είναι χρήσιμες σε πολλές περιπτώσεις. Περιλαμβάνουν, συνήθως, κάποια δημοφιλή λειτουργικά συστήματα και παρέχουν προστασία στο στάδιο της εγκατάστασης. (15)

**Εικόνα 9. Θέση ενός αναχώματος ασφάλειας (8)**



Πέρα από το γεγονός ότι ο τοίχος προστασίας αποτελεί την πρώτη γραμμή άμυνας έναντι των εισβολέων, ο τοίχος προστασίας έχει κι άλλες βασικές λειτουργίες, οι οποίες είναι:

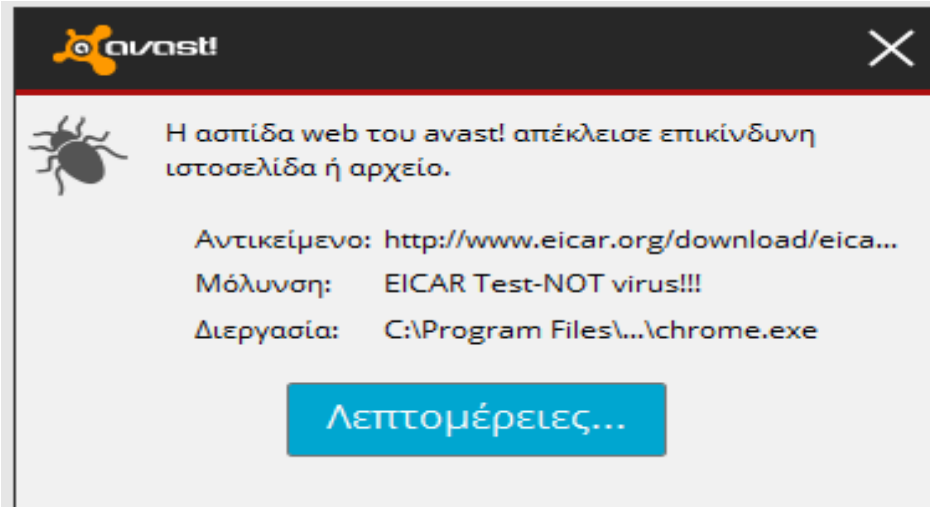
- Επιτρέπει στο διαχειριστή του συστήματος να ορίσει ένα σημείο ελέγχου, το οποίο θα ελέγχει αν ο χρήστης που θέλει να αποκτήσει πρόσβαση στο σύστημα είναι εξουσιοδοτημένος ή όχι.
- Εφαρμόζει έλεγχο προσπέλασης από και προς το δίκτυο σύμφωνα με το ποιον καθορίζει η πολιτική ασφάλειας ότι μπορεί να έχει πρόσβαση.
- Καταγράφει αποτελεσματικά τη δραστηριότητα στο σύστημα και στο δίκτυο, καθώς όλες οι κινήσεις διέρχονται από αυτό.
- Προστατεύει τα διαφορετικά δίκτυα ενός οργανισμό, καθώς τα διαχωρίζει μεταξύ τους. Έτσι, αν ένα δίκτυο έχει πρόβλημα, το πρόβλημα δε θα εξαπλωθεί και στα άλλα δίκτυα του ίδιου οργανισμού. (8) Για να λειτουργήσει σωστά ο τοίχος προστασίας, πρέπει να ακολουθούνται κάποια βασικά σημεία:
- Πρέπει να υπάρχουν πολιτικές που να προβλέπουν τη χρήση, διαμόρφωση και λειτουργία του τοίχου προστασίας και των αρχείων καταγραφής του τοίχου προστασίας.
- Όλοι οι υπολογιστές πρέπει να προστατεύονται από ένα σωστά διαμορφωμένο τοίχο προστασίας.
- Όλα τα μέλη του προσωπικού πρέπει να συμφωνήσουν ότι δε θα εμποδίσουν τη λειτουργία του τοίχου προστασίας. (15)

**Γ. Εγκατάσταση και συντήρηση της εφαρμογής Antivirus**

Όταν, όμως, δεν καταφέρει ο τοίχος προστασίας (firewall) να εμποδίσει τους εισβολείς, πρέπει να βρεθεί και να καταστραφεί το κακόβουλο λογισμικό που έχει ήδη εισέλθει. Για την εύρεση και καταστροφή του κακόβουλου λογισμικού, σε κάθε νοσοκομειακή μονάδα κάθε χρήστης οφείλει να έχει εγκατεστημένη μια εφαρμογή

η οποία ξεκινάει αυτόματα μαζί με τα Windows και παραμένει ενεργή για όση ώρα είναι ανοιχτός ο υπολογιστής. Μια τέτοια εφαρμογή είναι γνωστή ως «λογισμικό προστασίας από ιούς (Antivirus)» και έχει λειτουργία προστασίας σε πραγματικό χρόνο (real-time protection), ελέγχοντας άμεσα οποιοδήποτε αρχείο χρησιμοποιούνται. Σε κάθε antivirus είναι αποθηκευμένα τα χαρακτηριστικά του κώδικα εκατομμυρίων ιών κι άλλων κακόβουλων προγραμμάτων (trojans, mal-ware, worms κλπ.) που ονομάζονται «υπογραφές» ιών. Συνεπώς, όταν ελέγχει κάθε αρχείο το antivirus διαβάζει τον κώδικά του και τσεκάρει αν περιέχει ίχνη από τις ήδη γνωστές για εκείνο υπογραφές. Γι' αυτό και είναι σημαντικό να είναι συνδεδεμένο στο διαδίκτυο ώστε να κατεβάζει τις νεότερες ενημερώσεις ως προς τις υπογραφές ιών. Εάν δεν ενημερώνεται είναι θέμα χρόνου κάποιος ολοκαίνουριος ιός να περάσει στο σύστημά μας. (17)

**Εικόνα 10. Έλεγχος από το real time protection (17)**



Χωρίς το λογισμικό προστασίας από ιούς, τα δεδομένα είναι δυνατόν να κλαπούν, να καταστραφούν ή να υποβιβαστούν και ο έλεγχός τους να μεταβεί στα χέρια των επιτιθέμενων.

Υπάρχουν κάποιοι τρόποι με τους οποίους οι χρήστες των Πληροφοριακών Συστημάτων μπορούν να αναγνωρίσουν στον υπολογιστή μία μόλυνση από ιό. Ορισμένα χαρακτηριστικά ενός «μολυσμένου» υπολογιστή αναφέρονται παρακάτω:

- Το σύστημα δε θα ξεκινήσει κανονικά. Χαρακτηριστικό παράδειγμα είναι η μπλε οθόνη θανάτου.
- Το σύστημα καταρρέει συνεχώς χωρίς προφανή λόγο.
- Τα προγράμματα περιήγησης στο διαδίκτυο μεταβαίνουν σε ανεπιθύμητες ιστοσελίδες.
- Το λογισμικό προστασίας από ιούς δε φαίνεται να λειτουργεί.
- Πολλές ανεπιθύμητες διαφημίσεις εμφανίζονται στην οθόνη.
- Ο χρήστης δεν μπορεί να ελέγξει το ποντίκι του υπολογιστή.

Στο νοσοκομείο, όπως και σε κάθε οργανισμό, πρέπει να υπάρχει μια πολιτική σχετικά με το λογισμικό προστασίας από ιούς, η οποία θα αναφέρει τα εξής:

- Όλα τα μέλη του προσωπικού κατανοούν και συμφωνούν ότι δε θα εμποδίσουν τη λειτουργία του λογισμικού προστασίας από ιούς.
- Όλα τα μέλη του προσωπικού πρέπει να γνωρίζουν πώς να αναγνωρίζουν πιθανές επιθέσεις ιών στους υπολογιστές τους.
- Όλα τα μέλη του προσωπικού πρέπει να γνωρίζουν τι πρέπει να κάνουν για να αποφύγουν τις επιθέσεις από ιούς (malware).
- Το λογισμικό προστασίας από ιούς εγκαθίστανται και λειτουργεί αποτελεσματικά σε κάθε υπολογιστή σύμφωνα με τις συστάσεις του κατασκευαστή.
- Το λογισμικό προστασίας από ιούς είναι πλήρως ενημερωμένο σύμφωνα με τα πρότυπα του κατασκευαστή.

- Οι συσκευές χειρός και οι φορητές συσκευές που υποστηρίζουν το λογισμικό προστασίας από ιούς, το έχουν εγκαταστημένο και σε λειτουργία.

### 9.2.2. Απαραίτητες ενέργειες κατά τη διάρκεια χρήσης των υπολογιστών

Τα Πληροφοριακά Συστήματα των Νοσοκομείων πρέπει να συντηρούνται κατάλληλα ώστε να συνεχίσουν να λειτουργούν σωστά και αξιόπιστα, με τρόπο που σέβεται τη σημασία και την ευαίσθητη φύση των πληροφοριών που αποθηκεύονται σ' αυτά.

- Διαχείριση διαμόρφωσης: Οι νέοι υπολογιστές και τα νέα πακέτα λογισμικού παραδίδονται με μία πολύπλοκη σειρά από επιλογές και με ελάχιστες οδηγίες σχετικά με τη διαχείρισή τους ώστε το σύστημα να είναι ασφαλές. Επομένως, είναι δύσκολο να γνωρίζει ο χρήστης του υπολογιστή ποιες επιλογές πρέπει να επιτρέψει και ποιες να απενεργοποιήσει. Κάποιες χρήσιμες συμβουλές είναι οι εξής:
    - Καταργήστε την εγκατάσταση οποιασδήποτε εφαρμογής λογισμικού δεν είναι απαραίτητη, όπως παιχνίδια ή μέσα κοινής χρήσης φωτογραφιών.
    - Εάν δεν είναι ξεκάθαρος ο σκοπός μιας εφαρμογής λογισμικού, δείτε την ιστοσελίδα του λογισμικού για να καταλάβετε το σκοπό και τις χρήσεις του.
    - Μη δέχεστε προεπιλεγμένες διαμορφώσεις για την εγκατάσταση του λογισμικού. Δείτε κάθε επιλογή, κατανοήστε τι σημαίνει η κάθε επιλογή και ζητήστε βοήθεια όταν χρειάζεστε.
    - Ενημερωθείτε εάν ο πωλητής του λογισμικού διατηρεί ανοικτή σύνδεση στο εγκατεστημένο λογισμικό για την παροχή ενημερώσεων και υποστήριξης. Εάν ναι, βεβαιωθείτε ότι υπάρχει ασφαλής σύνδεση μέσω του τοίχου προστασίας.

- Απενεργοποιήστε την απομακρυσμένη κοινή χρήση αρχείων και την απομακρυσμένη εκτύπωση, καθώς μη εξουσιοδοτημένα άτομα θα μπορούσαν να έχουν πρόσβαση σ' αυτά.

- Συντήρηση λογισμικού: Το μεγαλύτερο μέρος του λογισμικού χρειάζεται περιοδική ενημέρωση για να διατηρείται ασφαλές και να εμπλουτίζεται με κάποια χρήσιμα χαρακτηριστικά. Οι ενημερώσεις του λογισμικού μπορούν να γίνουν είτε αυτόματα από τους προμηθευτές είτε με αίτημα του πελάτη. Στις μεγαλύτερες επιχειρήσεις η ενημέρωση λογισμικού γίνεται συνήθως καθημερινά, ενώ στις πιο μικρές επιχειρήσεις μπορεί να γίνεται εβδομαδιαία. Ωστόσο, τόσο οι μεγάλες όσο και οι μικρές επιχειρήσεις πρέπει να ενημερώνουν το λογισμικό τους και να το διατηρούν ασφαλές.
- Συντήρηση λειτουργικού συστήματος: Με την πάροδο του χρόνου, ένα λειτουργικό σύστημα τείνει να συσσωρεύει ξεπερασμένες πληροφορίες και ρυθμίσεις, εκτός και εάν πραγματοποιείται τακτική συντήρηση. Γι' αυτό πρέπει να πραγματοποιούνται συχνοί έλεγχοι που θα σχετίζονται με τα παρακάτω:
    - Οι λογαριασμοί χρηστών για πρώην υπαλλήλους έχουν απενεργοποιηθεί κατάλληλα και έγκαιρα.
    - Οι υπολογιστές και άλλες συσκευές, όπως μηχάνημα αντιγραφής, στα οποία υπάρχουν αποθηκευμένα δεδομένα πρέπει να «καθαρίζονται» πριν από τη διάθεσή τους. Ακόμα και αν έχουν διαγραφεί όλα τα δεδομένα, αυτά μπορούν να ανακτηθούν με συγκεκριμένα εργαλεία. Για να αποφύγετε μία ακούσια παραβίαση δεδομένων, υπάρχουν κατευθυντήριες οδηγίες σχετικά με τη διάθεση μιας συσκευής.
    - Τα παλιά αρχεία δεδομένων αρχειοθετούνται για αποθήκευση εάν απαιτείται ή καθαρίζονται από το σύστημα αν δεν είναι πια απαραίτητα, σύμφωνα με τις ισχύουσες απαιτήσεις δεδομένων.
    - Το λογισμικό που δε χρειάζεται πια, πρέπει να είναι απεγκατεστημένο.

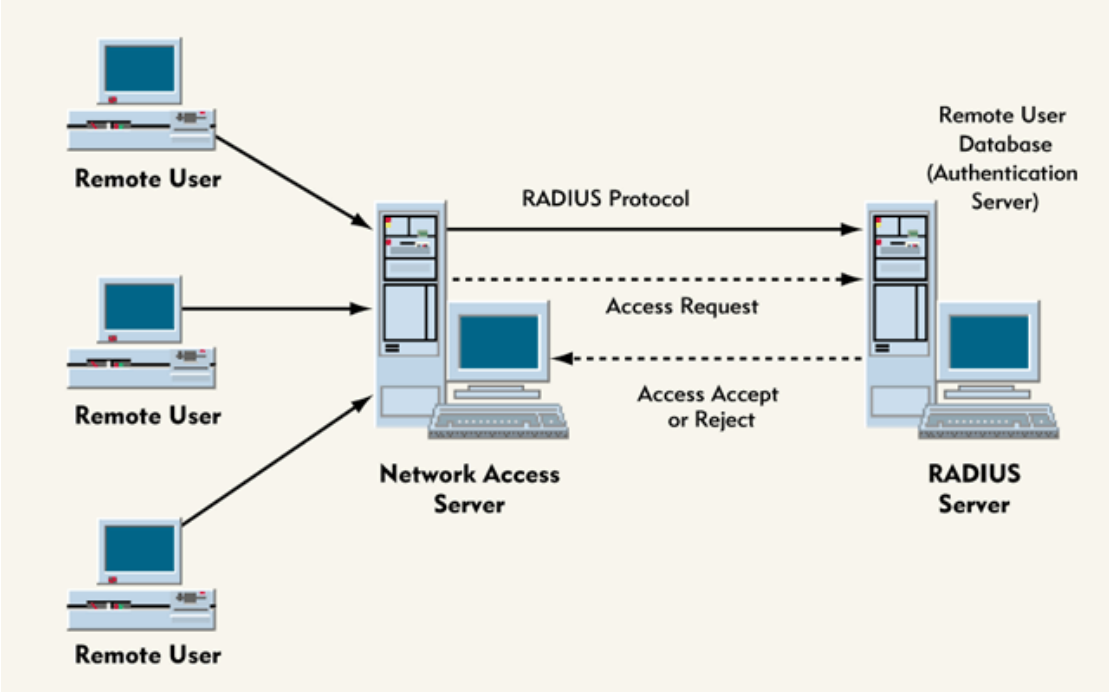
### 9.2.3. Έλεγχος και περιορισμός πρόσβασης στο δίκτυο των νοσοκομείων

Στις μέρες μας, με την εξέλιξη της τεχνολογίας είναι πολύ συχνή η κοινή χρήση αρχείων μεταξύ επαγγελματιών υγείας και η ανταλλαγή μηνυμάτων μέσω του ασύρματου δικτύου. Ωστόσο, λόγω της ευαισθησίας των πληροφοριών σχετικά με την υγειονομική περίθαλψη και του γεγονότος ότι προστατεύεται από τη νομοθεσία, πρέπει να χρησιμοποιηθούν εργαλεία που θα αποτρέψουν τρίτους να αποκτήσουν πρόσβαση σε ένα δίκτυο ιατρικής περίθαλψης. (15)

**Α. Έλεγχος της πρόσβασης στο δίκτυο των νοσοκομείων**

Ο Έλεγχος πρόσβασης στο δίκτυο ή NAC (Network Access Control) αποτελεί μία μέθοδο ενίσχυσης της ασφάλειας του δικτύου περιορίζοντας τη διαθεσιμότητα των πόρων του στο τελικό σημείο συσκευών που υπακούουν σε μια καθορισμένη πολιτική ασφάλειας. Αυτό επιτυγχάνεται με τον NAS (Network Access Server), ένα διακομιστή που εκτελεί τον έλεγχο της ταυτότητας και εξουσιοδότησης λειτουργιών για τους χρήστες με την επαλήθευση των διαπιστευτηρίων πρόσβασής τους. Εκτός από αυτές τις λειτουργίες, η μέθοδος NAC περιορίζει τα δεδομένα στα οποία κάθε συγκεκριμένος χρήστης μπορεί να έχει πρόσβαση, καθώς και την υλοποίηση αντι-απειλητικών εφαρμογών , όπως firewalls, λογισμικό προστασίας από ιούς και spyware- προγράμματα ανίχνευσης. Επίσης, η NAC ρυθμίζει και περιορίζει πράγματα που μεμονωμένοι συνδρομητές κάνουν τη στιγμή που είναι συνδεδεμένοι. Αρκετές δικτυώσεις και πωλητές πληροφορικής έχουν εισαχθεί σε προϊόντα της NAC. Η NAC είναι ιδανική για επιχειρήσεις και οργανισμούς, όπου το περιβάλλον του χρήστη μπορεί να ελέγχεται αυστηρά. Αν και ορισμένοι διαχειριστές αμφιβάλλουν για την πρακτικότητα της ανάπτυξης NAC σε δίκτυα με μεγάλο αριθμό διαφορετικών χρηστών και συσκευών, η φύση των οποίων αλλάζει συνεχώς (π.χ. στο δίκτυο για ένα μεγάλο πανεπιστήμιο με πολλαπλά τμήματα, πολυάριθμα σημεία πρόσβασης και χιλιάδες χρήστες με διάφορα υπόβαθρα και στόχους), είναι αλήθεια ότι είναι ιδανική για νοσοκομεία, κλινικές και για τις περισσότερες επιχειρήσεις και οργανισμούς. (18)

**Εικόνα 11. NAC – Έλεγχος πρόσβασης στο LAN του νοσοκομείου για κάθε απομακρυσμένο χρήστη (19)**




**Β. Περιορισμός της πρόσβασης τρίτων στο δίκτυο των νοσοκομείων**

Δεδομένου ότι οι ιατρικές πληροφορίες που ανταλλάσσονται μέσω του ασύρματου δικτύου είναι απόρρητες και προστατεύονται από το νόμο, κρίνεται σημαντικό να ασφαλιστεί το ασύρματο σήμα, ώστε να έχουν πρόσβαση στις πληροφορίες μόνο όσοι μπορούν να έχουν το σήμα. Ένας τρόπος ασφάλειας αποτελεί και η ρύθμιση των ασύρματων δρομολογητών (routers) να λειτουργούν μόνο σε κρυπτογραφημένη λειτουργία. Επίσης, για να διασφαλιστεί η προστασία του ασύρματου δικτύου, οι επισκέπτες στις μονάδες υγείας που φέρουν ηλεκτρονικές συσκευές δεν πρέπει να έχουν πρόσβαση στο δίκτυο του νοσοκομείου. Αυτό συμβαίνει καθώς είναι δύσκολο να ελεγχθούν αυτές οι συσκευές σχετικά με την ασφάλειά τους σε τόσο σύντομο χρονικό διάστημα που παραμένουν σε μία δομή

υγείας. Ένας τρόπος για να έχουν πρόσβαση στο δίκτυο οι επισκέπτες σ' ένα νοσοκομείο θα ήταν η εγκατάσταση ενός δικτύου που θα επιτρέπει την ασφαλή πρόσβαση. Όμως, η εγκατάσταση αυτού του δικτύου είναι δαπανηρή και χρονοβόρα διαδικασία με αποτέλεσμα η καλύτερη λύση σ' αυτήν την περίπτωση να είναι η απαγόρευση πρόσβασης στο διαδίκτυο.

Προκειμένου να επιτευχθεί ο έλεγχος και ο περιορισμός της πρόσβασης στο δίκτυο των νοσοκομείων, τα νοσοκομεία πρέπει να έχουν μία πολιτική που να αναφέρει τα παρακάτω:

- Όλα τα μέλη του προσωπικού πρέπει να κατανοούν και να συμφωνούν με τη συμμόρφωση στην πολιτική χρήσης του δικτύου.
- Η πρόσβαση στο δίκτυο περιορίζεται μόνο σε εξουσιοδοτημένους χρήστες και εξουσιοδοτημένες συσκευές.
- Οι συσκευές που φέρουν οι επισκέπτες σε μία μονάδα υγείας απαγορεύεται να έχουν πρόσβαση σε δίκτυα που περιέχουν εμπιστευτικές πληροφορίες για την υγεία (Protected Health Information).
- Τα ασύρματα δίκτυα πρέπει να χρησιμοποιούν την κατάλληλη κρυπτογράφηση.
- Οι υπολογιστές δεν πρέπει να περιέχουν εφαρμογές από ομότιμους χρήστες.
- Δεν πρέπει να χρησιμοποιούνται δημόσιες υπηρεσίες για ανταλλαγή άμεσων μηνυμάτων.
- Οι ιδιωτικές υπηρεσίες για ανταλλαγή άμεσων μηνυμάτων, όταν χρησιμοποιούνται, πρέπει να ασφαλίζονται καλά.

### 9.2.4. Ασφάλεια των συσκευών

Εκτός από τις πληροφορίες και τα αρχεία που σχετίζονται με την ιατρική περίθαλψη, οι συσκευές που χρησιμοποιούνται πρέπει να είναι ασφαλείς. Για το λόγο αυτό, πρέπει το σημείο που βρίσκονται να μην είναι προσβάσιμο από μη εξουσιοδοτημένους χρήστες, καθώς και να πληροί κάποια περιβαλλοντικά κριτήρια.

**Α. Ασφάλεια των συσκευών από την πρόσβαση μη εξουσιοδοτημένων χρηστών**

Οι συσκευές πρέπει, λοιπόν, να είναι ασφαλείς από τη μη εξουσιοδοτημένη πρόσβαση. Σύμφωνα με στοιχεία που αναφέρθηκαν από την Υπηρεσία Πολιτικών Δικαιωμάτων, πάνω από τις μισές περιπτώσεις απώλειας δεδομένων οφείλονται στην απώλεια των συσκευών είτε τυχαία είτε λόγω κλοπής. Προκειμένου να διασφαλιστεί η προστασία των συσκευών, πρέπει να υπάρχει μία πολιτική που να περιορίζει την πρόσβαση των μη εξουσιοδοτημένων ατόμων στα σημεία που βρίσκονται οι συσκευές και να αποτρέπει την απομάκρυνση των συσκευών από τα ασφαλή σημεία. Η καλύτερη λύση είναι η διατήρηση των συσκευών σε κλειδωμένους χώρους και η προσβασιμότητά τους μόνο στους εξουσιοδοτημένους χρήστες. (15)

**Β. Οργανωτικά και περιβαλλοντικά μέτρα του Computer Room**

Για όλα τα πληροφοριακά συστήματα νοσοκομείων υπάρχει η ανάγκη εξασφάλισης ενός ασφαλούς περιβάλλοντος κι ακόμα περισσότερο για το χώρο που στεγάζονται οι διακομιστές του νοσοκομειακού δικτύου, ο οποίος καλείται «computer room ή server room». Πρωταρχικά, η επιλογή του πού θα βρίσκεται στο κτίριο το computer room δε γίνεται να είναι τυχαία αλλά με βάση κάποια βασικά κριτήρια:

- Δεν πρέπει να βρίσκεται σε αίθουσα της οποίας ο ένας τοίχος είναι εξωτερικός του κτιρίου διότι οι εξωτερικοί τοίχοι μπορεί να έχουν υγρασία ή σωλήνες με νερό που θα μπορούσαν να σκάσουν και να μουσκέψουν τον εξοπλισμό.
- Αποφεύγοντας τους δύο πάνω ορόφους πρέπει να αποφεύγεται και το υπόγειο για πιθανές πλημμύρες αλλά και εξωτερικά παράθυρα για την αποφυγή ενδεχόμενων θραύσεων.
- Να είναι μακριά από σταθμούς παραγωγής ηλεκτρικής ενέργειας που μπορεί να προκαλέσουν παρεμβολές. (20)

Επίσης, είναι απαραίτητη η ύπαρξη τουλάχιστον μιας συσκευής UPS (Uninterruptible power supply), η οποία σε περίπτωση διακοπής του ηλεκτρικού ρεύματος παρέχει ηλεκτρικό ρεύμα μέχρι την έναρξη μιας βοηθητικής γεννήτριας ή

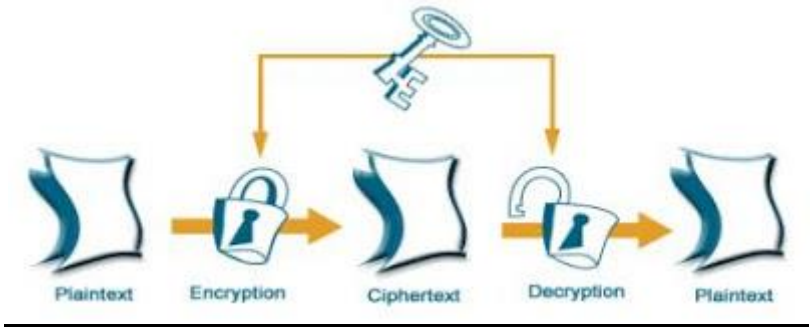
μέχρι να έρθει το ρεύμα ή μέχρι να τερματιστούν τα προγράμματα που ήταν σε λειτουργία. Η διαχείριση κατάλληλης θερμοκρασίας είναι ζωτικής σημασίας για το server room και τη σωστή λειτουργία του μιας και πρέπει να ψύχεται ο χώρος αυτός συνεχώς. Συστήματα μεταλλικών σχαρών (και τύπου πλέγματος πλέον) ώστε να διασφαλίζεται η σωστή διανομή των καλωδίων χαλκού και οπτικών ινών. Επίσης, συστήματα ελέγχου πρόσβασης (από πληκτρολόγια μέχρι αναγνώστες βιομετρικού αποτυπώματος και συστήματα κλειστού κυκλώματος παρακολούθησης) ώστε να ελέγχεται η είσοδος στο computer room και τέλος συστήματα πυρανίχνευσης και αυτόματοι πυροσβεστήρες τόσο στο server room αλλά και σε όλο το υπόλοιπο κτίριο ώστε να μην απειληθεί η ροή των εργασιών και κυρίως το προσωπικό σε περίπτωση πυρκαγιάς είναι μερικά μόνο από τα προστατευτικά και οργανωτικά μέτρα που απαιτούνται σε οποιαδήποτε νοσοκομειακή ή μη μονάδα που σχεδιάζεται και λειτουργεί σε οποιοδήποτε μέρος στον κόσμο. (21)

### 9.2.5. Κρυπτογράφηση δεδομένων

Κρυπτογράφηση (encryption) είναι η διαδικασία κωδικοποίησης μηνυμάτων και δεδομένων έτσι ώστε το νόημά τους να μην είναι προφανές. Είναι ουσιαστικά η μεταμφίεση πληροφοριών (κειμένων, αριθμών, αρχείων κλπ.) έτσι ώστε στα μάτια τρίτων να μη βγαίνει κανένα απολύτως νόημα. Την αρχική πληροφορία θα μπορεί να τη διαβάσει μόνο εκείνος (συνήθως ο παραλήπτης) που έχει το «κλειδί» της κρυπτογράφησης, το οποίο είτε είναι μυστικό και με το ίδιο μπορεί να αποκρυπτογραφηθεί η πληροφορία (συμμετρικοί αλγόριθμοι κρυπτογράφησης) είτε είναι δημόσιο. Στην περίπτωση αυτή, ο καθένας μπορεί να το γνωρίζει και να κάνει κρυπτογράφηση με αυτό. Εντούτοις, η αποκρυπτογράφηση γίνεται με διαφορετικό κλειδί το οποίο είναι ιδιωτικό και το έχει μονάχα εκείνος στον οποίο απευθύνεται το μήνυμα (ασύμμετροι αλγόριθμοι κρυπτογράφησης) . (22)

## Α. Συμμετρική Κρυπτογράφηση

Εικόνα 12. Συμμετρική Κρυπτογράφηση **(22)**




Η «συμμετρική κρυπτογράφηση» ονομάζεται αλλιώς και «κρυπτογραφία μυστικού κλειδιού» και περιλαμβάνει πέντε οντότητες όπως απεικονίζονται στο παραπάνω σχήμα.

- Αρχικό κείμενο (plaintext): Είναι το αρχικό κείμενο ή αρχικά δεδομένα που εισάγονται στον αλγόριθμο και επρόκειται να κρυπτογραφηθούν.
- Αλγόριθμος κρυπτογράφησης (encryption algorithm): Κάνει τις απαραίτητες τροποποιήσεις στο αρχικό κείμενο ώστε αυτό να μπορέσει να κρυπτογραφηθεί.
- Μυστικό κλειδί (secret key): Το μυστικό κλειδί εισάγεται στον αλγόριθμο κρυπτογράφησης και ευθύνεται για την πραγματοποίηση των τροποποιήσεων στο αρχικό κείμενο με ακρίβεια.
- Κρυπτογράφημα ή κρυπτογραφημένο μήνυμα (ciphertext): Είναι το τροποποιημένο μήνυμα που προκύπτει από τις τροποποιήσεις που κάνει ο αλγόριθμος κρυπτογράφησης στο αρχικό κείμενο με τη βοήθεια του μυστικού κλειδιού. Απ' το ίδιο αρχικό κείμενο μπορούν να προκύψουν διαφορετικά κρυπτογραφήματα εάν γίνει χρήση διαφορετικών μυστικών κλειδιών.

- Αλγόριθμος αποκρυπτογράφησης (decryption algorithm): Είναι ένας αλγόριθμος που αν χρησιμοποιήσει το κρυπτογράφημα και το μυστικό κλειδί που χρησιμοποιήθηκε μπορεί να παράγει το αρχικό κείμενο.

Για να πραγματοποιηθεί με ασφάλεια η συμμετρική κρυπτογράφηση πρέπει να ισχύουν τα εξής:

- Πρέπει να υπάρχει ένας ισχυρός αλγόριθμος κρυπτογράφησης. Αυτό σημαίνει ότι ακόμα και αν οι εισβολείς έχουν πρόσβαση σε κάποια κρυπτογραφήματα, δεν μπορούν να γνωρίζουν το μυστικό κλειδί και να συμπεράνουν το αρχικό κείμενο.
- Ο πομπός και ο δέκτης των μηνυμάτων πρέπει να έχουν αντίγραφα των μυστικών κλειδιών και να τα διαφυλάσσουν σε ασφαλές μέρος.

Επίσης, πρέπει να ισχύουν κάποιοι συγκεκριμένοι κανόνες, οι οποίοι είναι οι εξής:

a) Κρυπτογράφηση
b) Κρυπτανάλυση
c) Δομή κρυπτογραφίας του Feistel

a) <u>Κρυπτογράφηση</u>

Τα συστήματα κρυπτογράφησης ταξινομούνται με βάση τρία κριτήρια:

- Ανάλογα με τις διαδικασίες που χρησιμοποιούνται κατά την τροποποίηση του αρχικού κειμένου σε κρυπτογραφημένο μήνυμα: Ο μετασχηματισμός του αρχικού κειμένου σε κρυπτογράφημα μπορεί να γίνει βάση δύο αρχών, της αντικατάστασης και της μετάθεσης.
    - Αντικατάσταση: Κατά την αντικατάσταση, κάθε στοιχείο του αρχικού κειμένου, είτε αυτό είναι δυαδικό ψηφίο, είτε χαρακτήρας, είτε

συνδυασμός δυαδικών ψηφίων και χαρακτήρων αντικαθίσταται από ένα άλλο στοιχείο.

- Μετάθεση: Κατά τη μετάθεση, δεν υπάρχει αντικατάσταση των στοιχείων από άλλα καινούρια αλλά αναδιάταξη των στοιχείων του αρχικού κειμένου.

Το σημαντικό είναι να μην υπάρχει απώλεια οποιασδήποτε πληροφορίας, έτσι ώστε από το αρχικό κείμενο να μπορεί να προκύψει το κρυπτογραφημένο με τη διαδικασία της κρυπτογράφησης και από το κρυπτογραφημένο μήνυμα να μπορεί να προκύψει το αρχικό με τη διαδικασία της αποκρυπτογράφησης.

- Ανάλογα με τον αριθμό των κλειδιών που χρησιμοποιούνται: Αν ο πομπός και ο δέκτης χρησιμοποιούν το ίδιο κλειδί τότε η κρυπτογράφηση είναι συμμετρική, ενώ αν το κλειδί του πομπού και του δέκτη είναι διαφορετικά τότε η κρυπτογράφηση είναι ασύμμετρη.
- Ανάλογα με τον τρόπο επεξεργασίας του αρχικού κειμένου: Μπορεί να χρησιμοποιείται κωδικοποιητής τμημάτων ο οποίος από ένα τμήμα εισόδου παράγει ένα τμήμα εξόδου, ή κωδικοποιητής ροής ο οποίος για κάθε στοιχείο που εισέρχεται στο σύστημα παράγει ένα στοιχείο που εξέρχεται.

b) <u>Κρυπτανάλυση:</u>

Κρυπτανάλυση είναι η διαδικασία της προσπάθειας εύρεσης του αρχικού κειμένου και του μυστικού κλειδιού από μη εξουσιοδοτημένους χρήστες μέσω της διαδικασίας της αποκρυπτογράφησης.

Οι πιο συνήθεις τύποι επιθέσεων σε κρυπτογραφημένα μηνύματα είναι:

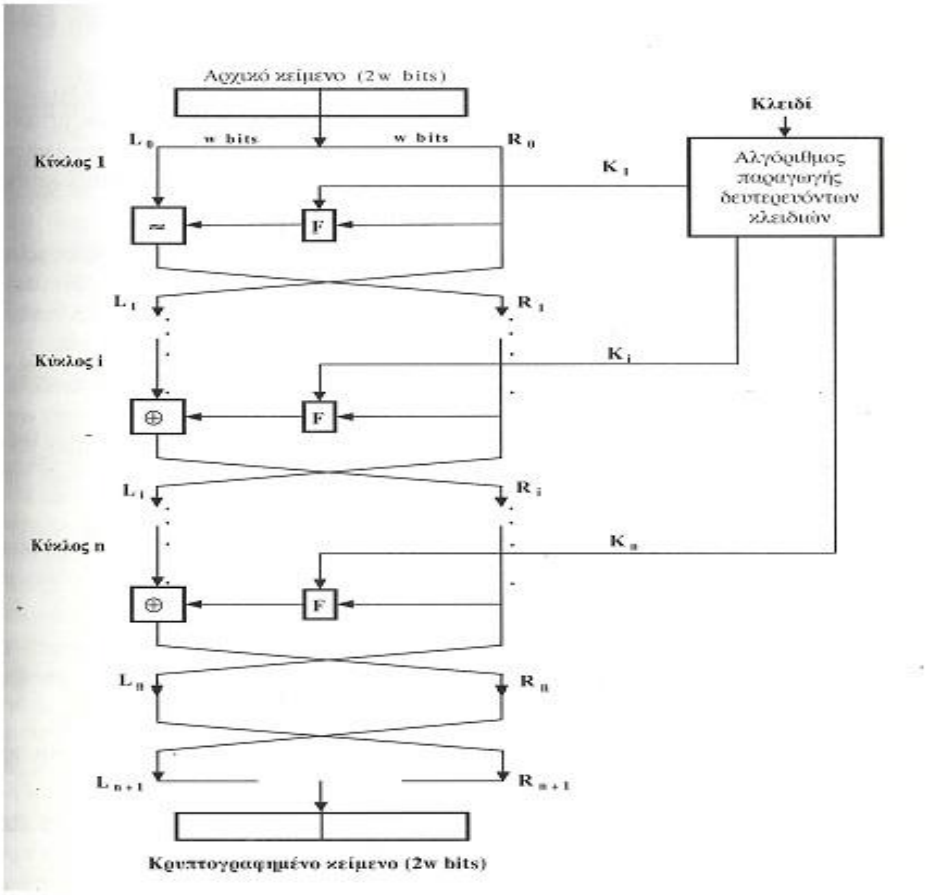
- Επίθεση κρυπτογραφήματος (ciphertext- only attack): Γίνεται αν ο κρυπταναλυτής γνωρίζει τον αλγόριθμο κρυπτογράφησης ή το κρυπτογράφημα. Είναι ένα εύκολο είδος επίθεσης, καθώς δε χρειάζεται μεγάλη ποσότητα πληροφοριών για να γίνει. Ο κρυπταναλυτής μπορεί να κάνει την επίθεσή του με δύο τρόπους, είτε καταγράφοντας δεδομένα του αρχικού μηνύματος και τα αντίστοιχα κρυπτογραφημένα μηνύματα, είτε γνωρίζοντας ποια συγκεκριμένα πρότυπα θα εμφανιστούν σε ένα μήνυμα. Και στις δύο αυτές περιπτώσεις, από τη στιγμή που ο κρυπταναλυτής γνωρίζει το αρχικό κείμενο, μπορεί να συμπεράνει ποιο είναι το μυστικό κλειδί.
- Επίθεση γνωστού αρχικού κειμένου (known- plaintext attack): Αυτό το είδος επίθεσης γίνεται αν ο αλγόριθμος κρυπτογράφησης ή το κρυπτογράφημα ή ζεύγη αρχικού και κρυπτογραφημένου κειμένου είναι γνωστά στον κρυπταναλυτή. Αν ο κρυπταναλυτής προσπαθεί να κρυπταναλύσει άγνωστο κείμενο, τότε μπορεί να μην καταλαβαίνει το περιεχόμενο του κειμένου. Αντίθετα, αν γνωρίζει κάποια τμήματα του κειμένου του κρυπταναλύει, τότε το μήνυμα μπορεί να θεωρηθεί γνωστό. Ειδικότερα, σε περίπτωση που ο κρυπταναλυτής επιλέγει συγκεκριμένα κομμάτια του κειμένου που είναι ήδη γνωστά σ’ αυτόν προς κρυπτογράφηση, τότε είναι πιο εύκολο για αυτόν να φτάσει στην εύρεση του μυστικού κλειδιού.
- Επίθεση επιλεγμένου κρυπτογραφήματος (chosen ciphertext attack): Είναι ένας τύπος επίθεσης που συμβαίνει όταν είναι γνωστά στον κρυπταναλυτή ο αλγόριθμος κρυπτογράφησης, το κρυπτογράφημα και ένα επιλεγμένο από τον κρυπταναλυτή κρυπτογράφημα μαζί με το αντίστοιχο αποκρυπτογραφημένο αρχικό κείμενο που παράχθηκε με το μυστικό κλειδί.
- Επίθεση επιλεγμένου κειμένου (chosen- text attack): Σ’ αυτήν την περίπτωση είναι γνωστά στον κρυπταναλυτή ο αλγόριθμος κρυπτογράφησης, το κρυπτογράφημα, ένα επιλεγμένο από τον κρυπταναλυτή κρυπτογράφημα μαζί με το αντίστοιχο αποκρυπτογραφημένο αρχικό κείμενο που παράχθηκε με το μυστικό κλειδί και ένα επιλεγμένο από τον κρυπταναλυτή μήνυμα

αρχικού κειμένου μαζί με το αντίστοιχο κρυπτογράφημα που παράχθηκε από το μυστικό κλειδί.

c) <u>Δομή κρυπτογραφίας του Feistel:</u>

Η δομή κρυπτογραφίας του Feistel παρουσιάζεται στο παρακάτω σχήμα. Σ' αυτό το δίκτυο που απεικονίζεται, υπάρχει ένα αρχικό κείμενο μήκους 2 λέξεων και ένα κλειδί K, τα οποία εισάγονται στον αλγόριθμο κρυπτογράφησης. Το αρχικό κείμενο διαιρείται σε δύο ίσα μέρη, $L_O$ και $R_O$. Τα $L_O$ και $R_O$ ακολουθούν n κύκλους επεξεργασίας μέχρι να κρυπτογραφηθούν πλήρως και να προκύψει ένα τελικό κρυπτογραφημένο κείμενο το οποίο θα έχει και αυτό μήκος δύο λέξεων. Κάθε κύκλος i έχει ως εισαγόμενα τμήματα τα $L_{i-1}$ και $R_{i-1}$ τα οποία παράγονται από τον προηγούμενο κύκλο και ως υποκλειδί το Ki που παράγεται από έναν αλγόριθμο παραγωγής δευτερευόντων κλειδιών. Σε κάθε κύκλο, στα δεδομένα της δεξιάς πλευράς εφαρμόζεται η συνάρτηση F και το αποτέλεσμα συνδυάζεται με τα δεδομένα της αριστερής πλευράς. Έτσι, προκύπτει μια αντικατάσταση στα δεδομένα της αριστερής πλευράς.

**Εικόνα 13. Δομή κρυπτογραφίας του Feistel (8)**



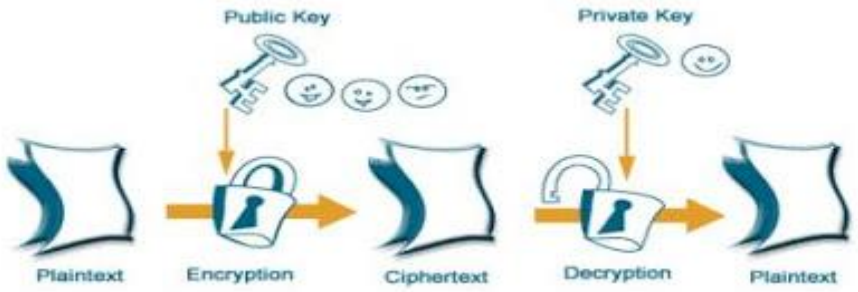

Για να πραγματοποιηθεί με ακρίβεια η κρυπογράφηση μέσω του δικτύου Feistel, πρέπει να επιλεχθούν με προσοχή τα πέντε παρακάτω χαρακτηριστικά:

- Το μέγεθος των τμημάτων (block size): Όσο μεγαλύτερο είναι το μέγεθος των τμημάτων, τόσο πιο ασφαλής είναι η κρυπτογράφηση και η αποκρυπτογράφηση. Όμως, μειώνεται η ταχύτητα πραγματοποίησης αυτών των διαδικασιών. Το πιο σύνηθες μέγεθος τμήματος στη διαδικασία της κρυπτογράφησης είναι τα 64 bit.

- Το μέγεθος του κλειδιού (key size): Όσο μεγαλύτερο είναι το μέγεθος του κλειδιού, τόσο πιο ασφαλής είναι η κρυπτογράφηση και η αποκρυπτογράφηση. Όμως, μειώνεται η ταχύτητα πραγματοποίησης αυτών των διαδικασιών. Το πιο σύνηθες μέγεθος κλειδιού είναι τα 128 bit.
- Ο αριθμός των κύκλων (number of rounds): Κάθε κύκλος από μόνος του δεν προσφέρει επαρκή ασφάλεια, ενώ η επανάληψη πολλών κύκλων προσφέρει αυξημένη ασφάλεια. Στο δίκτυο Feistel ο συνήθης αριθμός κύκλων είναι 16.
- Ο αλγόριθμος παραγωγής δευτερευόντων κλειδιών (subkey generation algorithm): Όσο πιο πολύπλοκος είναι ο αλγόριθμος, τόσο πιο δύσκολη είναι η κρυπτανάλυση.
- Η συνάρτηση κύκλου (round cycle): Όσο πιο πολύπλοκη είναι η συνάρτηση, τόσο πιο δύσκολη είναι η κρυπτανάλυση. (8)

**Β. Ασύμμετρη Κρυπτογράφηση**

**Εικόνα 14. Ασύμμετρη Κρυπτογράφηση (22)**




Το πρόβλημα με τη συμμετρική κρυπτογράφηση είναι ότι για να διαβάσει ο παραλήπτης το κρυπτογραφημένο μήνυμα που του αποστέλλεται πρέπει ο αποστολέας να στείλει και ένα αντίγραφο του κλειδιού, το οποίο αν το στείλει μέσω του διαδικτύου υπάρχει η πιθανότητα να το υποκλέψει κάποιος και να έχει πρόσβαση στα κρυπτογραφημένα δεδομένα. Αυτό αντιμετωπίζεται από την ασύμμετρη κρυπτογράφηση στην οποία οποιοδήποτε έγγραφο ή πληροφορία ανταλλάσσεται με τη χρήση ενός ζεύγους κλειδιών. Έτσι υπάρχει ένα δημόσιο κλειδί που γίνεται ελεύθερα διαθέσιμο σε οποιονδήποτε θέλει να στείλει μήνυμα και ένα

δεύτερο το οποίο είναι ιδιωτικό και το γνωρίζει μόνο ο παραλήπτης του μηνύματος. Συνεπώς, δεν υπάρχει ανησυχία σχετικά με τη μεταφορά των κλειδιών μέσω του διαδικτύου παρόλο που είναι δημόσια. Ωστόσο, το μειονέκτημα της ασύμμετρης κρυπτογράφησης είναι ότι είναι πιο αργή συγκριτικά με τη συμμετρική. (22)

Όπως και στη συμμετρική κρυπτογράφηση, έτσι και στην ασύμμετρη, ισχύει μία συγκεκριμένη δομή:

- Αρχικό κείμενο (plaintext): Είναι το αρχικό κείμενο ή αρχικά δεδομένα που εισάγονται στον αλγόριθμο και επρόκειται να κρυπτογραφηθούν.
- Αλγόριθμος κρυπτογράφησης (encryption algorithm): Κάνει τις απαραίτητες τροποποιήσεις στο αρχικό κείμενο ώστε αυτό να μπορέσει να κρυπτογραφηθεί.
- Ζεύγος δημοσίου (public) και ιδιωτικού (private) κλειδιού: Το δημόσιο κλειδί το έχει ο παραλήπτης και χρησιμοποιείται για κρυπτογράφηση, ενώ το ιδιωτικό κλειδί το έχει ο παραλήπτης και χρησιμοποιείται για αποκρυπτογράφηση. Το κρυπτογραφημένο μήνυμα προκύπτει με τη βοήθεια του αλγορίθμου κρυπτογράφησης και του ζεύγους δημόσιου και ιδιωτικού κλειδιού.
- Κρυπτογράφημα ή κρυπτογραφημένο μήνυμα (ciphertext): Είναι το μήνυμα που προκύπτει από τον μετασχηματισμό του αρχικού κειμένου, με τη βοήθεια του αλγορίθμου κρυπτογράφησης και του δημόσιου κλειδιού του παραλήπτη. Από το ίδιο αρχικό κείμενο, με δύο διαφορετικά δημόσια κλειδιά προκύπτουν δύο διαφορετικά κρυπτογραφημένα μηνύματα.
- Αλγόριθμος αποκρυπτογράφησης (decryption algorithm): Από τον αλγόριθμο αποκρυπτογράφησης και το ιδιωτικό κλειδί προκύπτει το αρχικό κείμενο.

Η ασύμμετρη κρυπτογράφηση χρησιμοποιείται κυρίως σε 3 περιπτώσεις:

a) Κρυπτογράφηση/ αποκρυπτογράφηση (encryption/ decryption)
b) Ψηφιακές υπογραφές (digital signatures)
c) Ψηφιακά πιστοποιητικά

a) Κρυπτογράφηση/ αποκρυπτογράφηση (encryption/ decryption):

Ο αποστολέας κρυπτογραφεί ένα κείμενο με το δημόσιο κλειδί και το στέλνει στον παραλήπτη, ο οποίος με το ιδιωτικό κλειδί το αποκρυπτογραφεί.

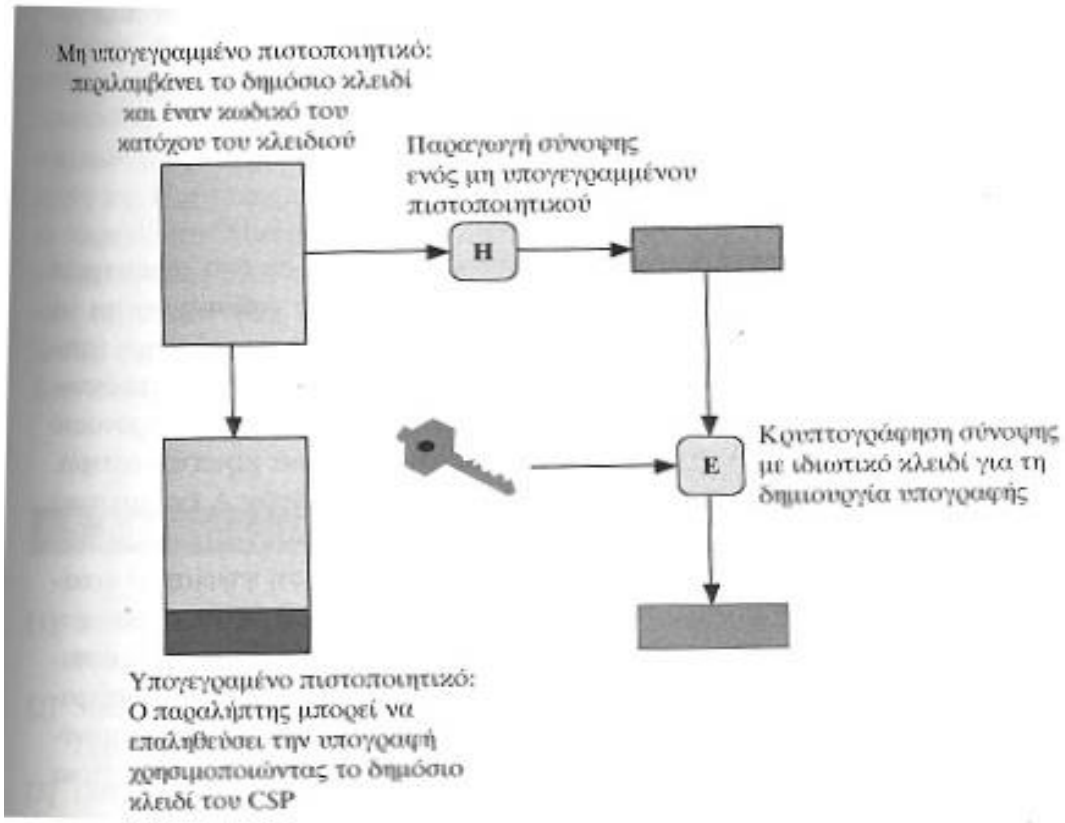
b) Ψηφιακές υπογραφές (digital signatures):

Η ψηφιακή υπογραφή μπαίνει στο μήνυμα από τον αποστολέα με το ιδιωτικό κλειδί που κατέχει. Έστω ότι είναι ένας αποστολέας Β και ένας παραλήπτης Α και ο αποστολέας Β θέλει να στείλει ένα μήνυμα στον Α. Ο Β κρυπτογραφεί το μήνυμα που θέλει να στείλει με το ιδιωτικό του κλειδί. Όταν ο Α παραλάβει το μήνυμα που έχει στείλει ο Β, τότε το αποκρυπτογραφεί με το δημόσιο κλειδί του Β, και έτσι συμπεραίνει ότι το αρχικό μήνυμα είχε κρυπτογραφηθεί από τον Β πριν την αποστολή του. Το κρυπτογραφημένο μήνυμα αποτελεί ψηφιακή υπογραφή, καθώς κανένας άλλος δεν μπορεί να δημιουργήσει κρυπτογραφημένο κείμενο που να αποκρυπτογραφείται με το δημόσιο κλειδί του Β, από τη στιγμή που κανένας άλλος δε γνωρίζει το ιδιωτικό κλειδί του Β. Επίσης, το γεγονός ότι κανένας άλλος δε γνωρίζει το ιδιωτικό κλειδί του Β εξασφαλίζει την αυθεντικοποίηση του αποστολέα και ακεραιότητα των δεδομένων, αλλά όχι την έννοια της εμπιστευτικότητας.

Το πρόβλημα που υπάρχει με τις ψηφιακές υπογραφές είναι ότι για λόγους ευκολίας το μήνυμα πρέπει να υπάρχει σε μη κρυπτογραφημένη μορφή. Όμως, επειδή μπορεί να υπάρξει αμφισβήτηση και διαφωνία σχετικά με το περιεχόμενο του μηνύματος, πρέπει να υπάρχει ένα αντίγραφο του μηνύματος σε κρυπτογραφημένη μορφή. Για καλύτερα αποτελέσματα, συνήθως κρυπτογραφείται ένα πολύ μικρό κείμενο του μηνύματος, το οποίο ονομάζεται αυθεντικοποιητής (authenticator). Το κείμενο δεν πρέπει να μπορεί να τροποποιείται αν δεν

τροποποιείται ο αυθεντικοποιητής. Ο αυθεντικοποιητής ονομάζεται και «ψηφιακή υπογραφή» αν κρυπτογραφηθεί με το ιδιωτικό κλειδί του αποστολέα. (8)

**Εικόνα 15. Ψηφιακή υπογραφή (8)**




c) <u>Ψηφιακά πιστοποιητικά:</u>

Το δημόσιο κλειδί που χρησιμοποιείται στην κρυπτογράφηση και αποκρυπτογράφηση πρέπει να είναι γνωστό σε όλους. Έτσι, αν υπάρχει ένας ευρέως αποδεκτός αλγόριθμος κρυπτογράφησης και αποκρυπτογράφησης, ο αποστολέας ενός μηνύματος μπορεί να στείλει το δημόσιο κλειδί του σε κάποιον άλλον ή να το μεταδώσει προς όλους, ώστε αυτοί να μπορέσουν να

αποκρυπτογραφήσουν το μήνυμα. Όμως, η αποστολή του μηνύματος που περιέχει το δημόσιο κλειδί μπορεί να επηρεάσει την ακεραιότητα του μηνύματος και την αυθεντικοποίηση του αποστολέα. Αυτό συμβαίνει γιατί μπορεί κάποιος άγνωστος να λάβει το δημόσιο κλειδί του αποστολέα και να το μεταδώσει προς τρίτους. Επίσης, μέχρι να αποκαλυφθεί το γεγονός ότι το δημόσιο κλειδί είναι στα χέρια κάποιου αγνώστου, αυτός ο άγνωστος θα έχει διαβάσει όλα τα κρυπτογραφημένα μηνύματα και θα μπορεί να υπογράφει και να αυθεντικοποιείται ως τον γνήσιο αποστολέα του αρχικού μηνύματος. Λύση σε αυτό το πρόβλημα αποτελεί η χρήση του ψηφιακού πιστοποιητικού, το οποίο περιλαμβάνει το δημόσιο κλειδί του χρήστη και έναν κωδικό (userID) του κατόχου του κλειδιού. Το δημόσιο κλειδί κι ο κωδικός είναι ψηφιακά υπογεγραμμένα από μια Έμπιστη Τρίτη Οντότητα (Trusted Third Party- TTP), η οποία συνήθως αποκαλείται Πάροχος Υπηρεσιών Πιστοποίησης (Certification Service Provider- CSP). Ο χρήστης δείχνει στον CSP το δημόσιο κλειδί του και λαμβάνει ένα πιστοποιητικό που περιέχει το κλειδί του. Έτσι, όποιος θέλει να λάβει το δημόσιο κλειδί του χρήστη για να αποκρυπτογραφήσει το μήνυμα, μπορεί να λάβει ένα ψηφιακό πιστοποιητικό και να είναι σίγουρος για την ορθότητά του. (8)

### 9.2.6. Πρωτόκολλα για την ασφάλεια υψηλού επιπέδου στο χώρο της υγείας

Τα ζητήματα της ασφάλειας και του απορρήτου θεωρούνται πολύ σημαντικά στην ανάπτυξη προτύπων στην Πληροφορική Υγείας. Όταν οι λειτουργίες επικοινωνίας είναι πολύπλοκες και χωρίζονται σε ανεξάρτητα στρώματα ή επίπεδα, τότε είναι χρήσιμη η στοίβα πρωτοκόλλων. Η στοίβα αυτή είναι μια συλλογή από πρωτόκολλα (σε κάθε στρώμα ή επίπεδο) με τα οποία πραγματοποιείται δικτυακή επικοινωνία. Τα χαμηλότερα στρώματα σχετίζονται με το υλικό (hardware) και τα υψηλότερα με το χρήστη. Ο αριθμός των διεργασιών που επιτελούνται σε κάθε επίπεδο εξαρτάται από το ποια στοίβα χρησιμοποιείται (π.χ. OSI, TCP/IP κλπ.). Το κατά πόσο εφαρμόζονται οι υπηρεσίες ασφαλείας δε συνδέεται με κάποιο συγκεκριμένο επίπεδο της στοίβας του προτύπου OSI αλλά με τα υποψήφια πρωτόκολλα

επικοινωνίας. Υπάρχουν τέσσερα επίπεδα πρωτοκόλλων ασφάλειας που διακρίνονται σε: α) πρωτόκολλα ασφάλειας επιπέδου πρόσβασης δικτύου, β) πρωτόκολλα ασφάλειας επιπέδου διαδικτύου, γ) πρωτόκολλα ασφάλειας επιπέδου μεταφοράς και δ) πρωτόκολλα ασφάλειας επιπέδου εφαρμογής. Με γνώμονα την επιλογή διαφορετικού σετ υπηρεσιών ασφαλείας κάθε πρωτόκολλο ασφαλείας μπορεί να περιγραφεί πλήρως. Στη συνέχεια αναφέρεται από ένα παράδειγμα πρωτοκόλλου για κάθε επίπεδο ασφάλειας. (23)

**Α. Πρωτόκολλα ασφάλειας επιπέδου πρόσβασης δικτύου**

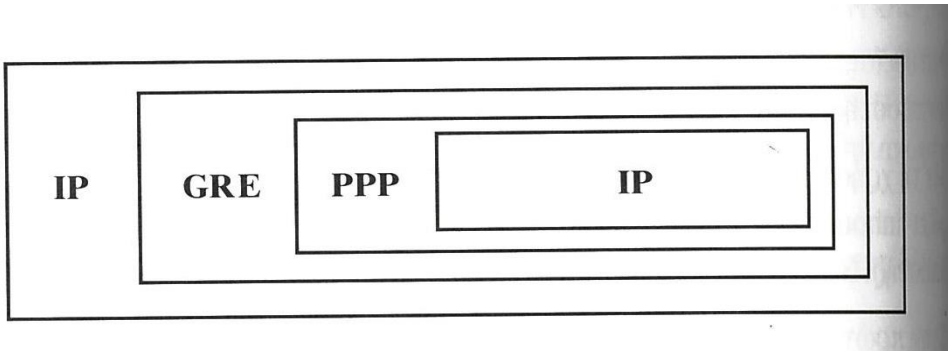
Τα πρωτόκολλα ασφάλειας επιπέδου πρόσβασης δικτύου χρησιμοποιούνται για την ασφαλή διαχείριση ζητημάτων που αφορούν τη δικτύωση της τοπικής περιοχής, τη σύνδεση του τηλεφώνου στο μοντέλο του Internet. Στις μέρες μας, για τη δικτύωση τοπικής περιοχής χρησιμοποιείται κυρίως το πρωτόκολλο Ethernet και για τη σύνδεση του τηλεφώνου στο δίκτυο το πρωτόκολλο PPP ( Point-to-Point Protocol). Ένα πρωτόκολλο αυτού του επιπέδου που χρησιμοποιείται για την ασφάλεια των Πληροφοριακών Συστημάτων είναι το «Πρωτόκολλο διέλευσης Σημείο-Προς- Σημείο PPTP». (8)

Το PPTP είναι ένα πρότυπο δικτύωσης για σύνδεση σε εικονικά ιδιωτικά δίκτυα ( virtual private networks- VPNs). Τα δίκτυα VPN είναι ασφαλή δίκτυα που μπορούν να αποκτήσουν πρόσβαση μέσω του Διαδικτύου, επιτρέποντας στους χρήστες να έχουν πρόσβαση σε ένα δίκτυο από μια απομακρυσμένη τοποθεσία. Αυτό είναι χρήσιμο για άτομα που χρειάζονται να συνδεθούν με ένα δίκτυο γραφείου από το σπίτι ή να έχουν πρόσβαση στον οικιακό τους υπολογιστή από άλλη τοποθεσία. Στην ονομασία του πρωτοκόλλου αναφέρεται ο όρος «Σημείο-Προς- Σημείο», δηλαδή το πρωτόκολλο αυτό επιτρέπει σε ένα σημείο ( στον υπολογιστή του χρήστη) να αποκτήσει πρόσβαση σε ένα άλλο συγκεκριμένο σημείο (απομακρυσμένο δίκτυο) μέσω της σύνδεσης στο διαδίκτυο. Ο όρος «διέλευση» που αναφέρεται στην ονομασία περιγράφει την ενσωμάτωση ενός πρωτοκόλλου σ' ένα άλλο πρωτόκολλο. Στο PPTP, το πρωτόκολλο Point- to- Point (PPP) είναι

ενσωματωμένο μέσα στο πρωτόκολλο TCP / IP (Transmission Control Protocol/ Internet Protocol), το οποίο παρέχει τη σύνδεση στο Internet. Επομένως, παρόλο που η σύνδεση δημιουργείται μέσω του διαδικτύου, η σύνδεση PPTP μιμείται μια άμεση σύνδεση μεταξύ των δύο θέσεων, επιτρέποντας μια ασφαλή σύνδεση. (24)

Ο τρόπος λειτουργίας του PPTP είναι ο εξής: Παίρνει κάποια πακέτα IP και τα μετατρέπει σε ένα νέο πακέτο IP, έτσι ώστε να μπορέσει να το μεταφέρει από ένα σημείο σε ένα άλλο σημείο. Τα αρχικά πακέτα IP πλαισιώνονται από το πρωτόκολλο PPP και στη συνέχεια ενθυλακώνονται χρησιμοποιώντας μια επικεφαλίδα Δρομολόγησης Γενικής Ενθυλάκωσης (Generic Routing Encapsulation- GRE). Έτσι, προκύπτει το τελικό πακέτο IP που είναι έτοιμο για μεταφορά μέσω του διαδικτύου. Ο τρόπος λειτουργίας αναπαριστάται στο παρακάτω σχήμα.

**Εικόνα 16. Το σχήμα ενθυλάκωσης PPTP (8)**




**Β. Πρωτόκολλα ασφάλειας επιπέδου Internet**

Όπως και τα πρωτόκολλα ασφάλειας επιπέδου πρόσβασης δικτύου, έτσι και τα πρωτόκολλα ασφάλειας επιπέδου Internet χρησιμοποιούν ως βασική τεχνική λειτουργίας τους την ενθυλάκωση. Ένα πρωτόκολλο ασφάλειας επιπέδου Internet που χρησιμοποιείται είναι το IP Security Protocol ( IPSP), το οποίο περιλαμβάνει μηχανισμούς αυθεντικοποίησης και κρυπτογράφησης ακόμα και χωρίς σύνδεση. Αυτοί οι δύο μηχανισμοί μπορούν να χρησιμοποιούνται ή ξεχωριστά ή σε συνδυασμό σύμφωνα με ένα συσχετισμό ασφάλειας (Security Association- SA). Ο

συσχετισμός ασφάλειας είναι μία συμφωνία που καθορίζει ποιοι μηχανισμοί ασφάλειας θα χρησιμοποιηθούν και τον τρόπο που θα χρησιμοποιηθούν. Όσον αφορά το πρωτόκολλο IPSP, υπάρχουν δύο μηχανισμοί ασφάλειας, ο μηχανισμός Authentication Header-AH και ο μηχανισμός Encapsulating Security Payload-ESP.

- Μηχανισμός Authentication Header-AH: Με το μηχανισμό της αυθεντικοποίησης, ο παραλήπτης του IP πακέτου είναι σε θέση να επιβεβαιώσει την οντότητα του δημιουργού και να εξετάσει αν έχει γίνει τροποποίηση του πακέτου κατά τη μεταφορά του. Όμως, αυτός ο μηχανισμός δε διασφαλίζει την εμπιστευτικότητα των δεδομένων. Η εμπιστευτικότητα των δεδομένων μπορεί να διασφαλιστεί από τον μηχανισμό Encapsulating Security Payload-ESP που αναλύεται στη συνέχεια.
- Μηχανισμός Encapsulating Security Payload-ESP: Με το μηχανισμό της κρυπτογράφησης, ο παραλήπτης του πακέτου μπορεί να αναγνώσει το πακέτο μόνο εάν είναι νόμιμος παραλήπτης. Επομένως, εξασφαλίζεται η εμπιστευτικότητα των δεδομένων μέσω της κρυπτογράφησης και της ενθυλάκωσης είτε του ωφέλιμου φορτίου του IP πακέτου είτε ολόκληρου του πακέτου. Αν αφορά ένα μέρος του πακέτου η κατάσταση λειτουργίας ονομάζεται «κατάσταση μεταγωγής- transport mode», ενώ αν αφορά ολόκληρο το πακέτο η κατάσταση λειτουργίας λέγεται « κατάσταση διόδου- tunnel mode».
    - κατάσταση μεταγωγής- transport mode: Ο αποστολέας επιλέγει από το πακέτο IP που θέλει να στείλει τα δεδομένα πρωτοκόλλου ανώτερου επιπέδου, τα ενθυλακώνει σε μία επικεφαλίδα ESP και στη συνέχεια τα κρυπτογραφεί. Τα δεδομένα πρωτοκόλλου ανώτερου επιπέδου που είναι ενθυλακωμένα στην επικεφαλίδα ESP ονομάζονται «ωφέλιμο φορτίο του IP πακέτου».
    - κατάσταση διόδου- tunnel mode: Αυτή η κατάσταση δεν απευθύνεται μόνο στα δεδομένα πρωτοκόλλου ανώτερου επιπέδου αλλά σε ολόκληρα τα πακέτα IP. Συνήθως χρησιμοποιείται κατάσταση διόδου μεταξύ δύο αναχωμάτων ασφάλειας, έτσι ώστε ο επιτιθέμενος ακόμα και αν βρει τις επικοινωνίες μεταξύ των

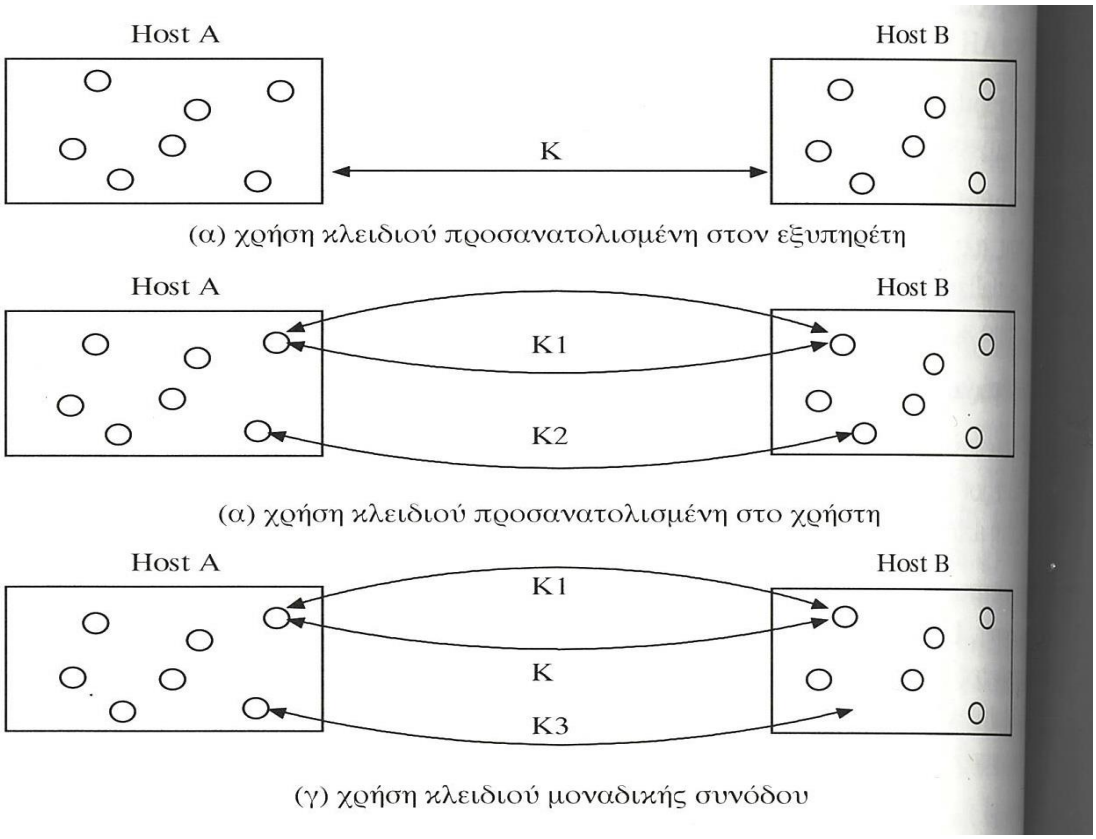
αναχωμάτων, να μην μπορεί να καταλάβει ποιος στέλνει και σε ποιον αυτά τα πακέτα δεδομένων.

Κατά τις παραπάνω διαδικασίες της αυθεντικοποίησης και της κρυπτογράφησης χρησιμοποιούνται κάποια κλειδιά. Ανάλογα με την πολυπλοκότητα αυτών των κλειδιών, ο συσχετισμός ασφάλειας καθορίζει τρεις τρόπους χρήσης κλειδιού για αυθεντικοποίηση και κρυπτογράφηση.

- Χρήση κλειδιού προσανατολισμένη στον εξυπηρέτη: Όλοι οι χρήστες ανήκουν σε έναν εξυπηρέτη (host A) και γνωρίζουν το ίδιο κλειδί (K), με το οποίο ανταλλάσσουν δεδομένα με τους χρήστες άλλου εξυπηρέτη (host B).
- Χρήση κλειδιού προσανατολισμένη στο χρήστη: Κάθε χρήστης ενός εξυπηρέτη (host A) έχει ένα ή περισσότερα μοναδικά κλειδιά για τη μεταφορά των δεδομένων σε έναν άλλον εξυπηρέτη (host B). Ένας χρήστης του εξυπηρέτη Α που θέλει να επικοινωνήσει με ένα χρήστη του εξυπηρέτη Β χρησιμοποιεί για την επικοινωνία τους ένα μοναδικό κλειδί. Αυτό το κλειδί το χρησιμοποιούν κάθε φορά που θέλουν να επικοινωνήσουν.
- Χρήση κλειδιού μοναδικής συνόδου: Κάθε χρήστης του εξυπηρέτη Α που θέλει να επικοινωνήσει με ένα χρήστη του εξυπηρέτη Β χρησιμοποιεί για την επικοινωνία τους ένα συγκεκριμένο κλειδί. Όταν θελήσουν να επικοινωνήσουν ξανά, το κλειδί θα είναι διαφορετικό από αυτό της προηγούμενης φοράς.

Οι διαφορετικές προσεγγίσεις χρήσης κλειδιού με βάση το συσχετισμό ασφάλειας αναπαριστώνται στο παρακάτω σχήμα. (8)

**Εικόνα 17. Τρεις προσεγγίσεις χρήσης κλειδιού για IPSP (8)**




**Γ. Πρωτόκολλα ασφάλειας επιπέδου μεταφοράς:**

Ένα πρωτόκολλο ασφάλειας επιπέδου μεταφοράς που χρησιμοποιείται για την ασφαλή μεταφορά των δεδομένων στο διαδίκτυο είναι το «Πρωτόκολλο Secure Sockets Layer-SSL». Το πρωτόκολλο αυτό επιτρέπει την ασφαλή μεταφορά δεδομένων μεταξύ ενός server και ενός browser με τη χρήση κλειδιών κρυπτογράφησης και την πιστοποίηση του server προτού ανταλλαχθούν δεδομένα από εφαρμογές υψηλότερων στρωμάτων. Διατηρεί την ασφάλεια και την ακεραιότητα του καναλιού μετάδοσης χρησιμοποιώντας την κρυπτογράφηση, την πιστοποίηση και κωδικούς. Αν δε χρησιμοποιείται αυτό το πρωτόκολλο, θα είναι πολύ εύκολο για τους εισβολείς να αποκτήσουν πρόσβαση στα δεδομένα που

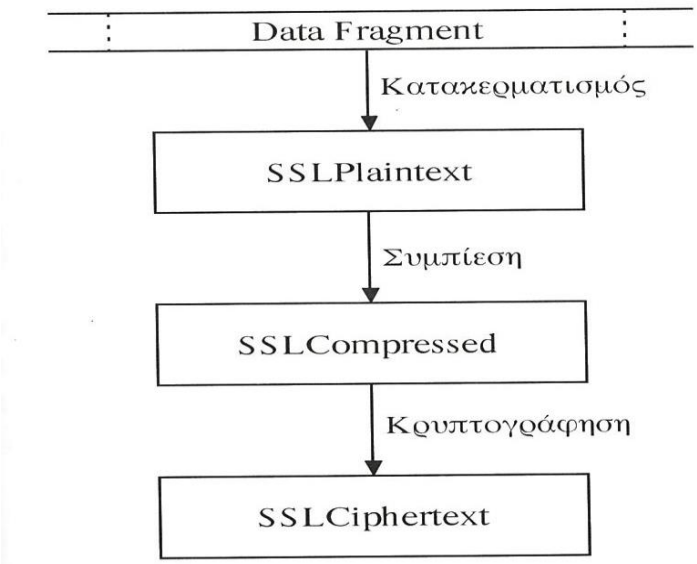
μεταφέρονται, στον server και στον browser. Οι βασικές υπηρεσίες ασφάλειας πάνω στις οποίες στηρίζεται το SSL είναι:

- Αυθεντικοποίηση του server και του browser μέσω κρυπτογραφίας του δημόσιου κλειδιού
- Εμπιστευτικότητα των δεδομένων μέσω της κρυπτογράφησης της σύνδεσης μετά από μία αρχική χειραψία και τον καθορισμό ενός κλειδιού συνόδου
- Ακεραιότητα των δεδομένων μέσω της αυθεντικοποίησης των μηνυμάτων και τον έλεγχο της ακεραιότητάς τους από τους MAC κωδικούς (Message Authentication Code). Οι MAC κωδικοί ελέγχουν την ακεραιότητα και αυθεντικοποίηση των δεδομένων που μεταφέρονται με τη χρήση ενός κοινού μυστικού κλειδιού, ενός αριθμού των 32 bits και του περιεχομένου των μηνυμάτων.

Το SSL αποτελείται από τα δύο πρωτόκολλα, το SSL Record Protocol και το SSL Handshake Protocol.

- SSL Record Protocol: Λαμβάνει δεδομένα από πρωτόκολλα υψηλότερων επιπέδων και στη συνέχεια κάνει κατακερματισμό, συμπίεση, αυθεντικοποίηση και κρυπτογράφηση αυτών των δεδομένων, όπως περιγράφεται στο παρακάτω σχήμα.

**Εικόνα 18.Τα βήματα του SSL record protocol (8)**



Το SSL Record Protocol λαμβάνει δεδομένα από πρωτόκολλα, όπως το:

- Πρωτόκολλο προειδοποίησης (SSL Alert Protocol): Μεταφέρει προειδοποιήσεις, οι οποίες αποτελούνται από ένα επίπεδο προειδοποίησης και μία περιγραφή της προειδοποίησης, με το SSL Record Protocol.
- Πρωτόκολλο Αλλαγής Προδιαγραφών Κρυπτογραφίας ( SSL Change Cipher Spec Protocol): Χρησιμοποιείται όταν πρέπει να γίνει αλλαγή μιας προδιαγραφής κρυπτογραφίας με μια άλλη.
- Πρωτόκολλο χειραψίας (SSL Handshake Protocol): Είναι το κύριο πρωτόκολλο που δίνει δεδομένα στο SSL Record Protocol και αναλύεται στη συνέχεια.

➢ SSL Handshake Protocol: Αυτό το πρωτόκολλο στέλνει δεδομένα στο SSL Record Protocol, το οποίο με τη σειρά του κάνει κατακερματισμό, συμπίεση, αυθεντικοποίηση και κρυπτογράφηση αυτών των δεδομένων. (8,25)

**Δ. Πρωτόκολλα ασφάλειας επιπέδου εφαρμογής:**

Αυτό το είδος πρωτοκόλλων είναι ιδιαίτερα χρήσιμο, καθώς η ασφάλεια διαμορφώνεται και οριοθετείται με βάση τα χαρακτηριστικά κάθε εφαρμογής. Τα πρωτόκολλα ασφάλειας επιπέδου εφαρμογής περιλαμβάνουν τόσο πρωτόκολλα εφαρμογής βελτιωμένα ως προς την ασφάλεια όσο και συστήματα αυθεντικοποίησης και διανομής κλειδιών. Στην πρώτη περίπτωση, οι υπηρεσίες ασφάλειας αναπτύσσονται μέσα σε κάθε εφαρμογή ανάλογα με τις απαιτήσεις της κάθε εφαρμογής, ενώ στη δεύτερη περίπτωση υπάρχει ένα γενικό πλαίσιο ασφάλειας το οποίο προσαρμόζεται σε κάθε εφαρμογή. Μία εφαρμογή που πρέπει να έχει πρωτόκολλο ασφάλειας για να παρέχει ενισχυμένη προστασία έναντι των απειλών είναι το διαδίκτυο. Με τη χρήση ειδικών πρωτοκόλλων ελέγχεται η πρόσβαση στις ιστοσελίδες και εξασφαλίζεται η διαθεσιμότητα, ακεραιότητα και εμπιστευτικότητα των δεδομένων. Ένα τέτοιο πρωτόκολλο που χρησιμοποιείται για την παροχή υπηρεσιών ασφάλειας κατά τις δοσοληψίες στον παγκόσμιο ιστό είναι το Secure HTTP (S-HTTP). Σε σχέση με το πρωτόκολλο HTTP, το S-HTTP προσφέρει βελτιωμένες υπηρεσίες κρυπτογράφησης για τα δεδομένα που υπάρχουν στο

διαδίκτυο. Οι εξυπηρέτες και οι εξυπηρετούμενοι έχουν τη δυνατότητα να προσαρμόζουν τις τεχνικές ασφάλειας που θα χρησιμοποιήσουν κατά την ανταλλαγή δεδομένων στο διαδίκτυο ανάλογα με τις δυνατότητές τους. Αυτό σημαίνει ότι οι συναλλαγές ιστού μπορούν να πραγματοποιηθούν ακόμα και αν οι εξυπηρέτες και οι εξυπηρετούμενοι δε διαθέτουν πιστοποιητικά δημόσιων κλειδιών, κάνοντας χρήση άλλων μεθόδων ασφάλειας. Το πρωτόκολλο S-HTTP παρέχει τρεις τεχνικές ασφάλειας, οι οποίες μπορούν να χρησιμοποιηθούν ή κάθε μία μόνη της ή σε συνδυασμό.

1. Ψηφιακή υπογραφή: Όταν χρησιμοποιείται αυτή η τεχνική ασφάλειας, ή ο αποστολέας των μηνυμάτων επισυνάπτει στα μηνύματα πιστοποιητικό ασφάλειας ή ο παραλήπτης πρέπει να έχει ένα δικό του πιστοποιητικό ασφάλειας για να μπορέσει να έχει πρόσβαση στα απεσταλμένα αρχεία.
2. Αυθεντικοποίηση μηνύματος: Η αυθεντικοποίηση των μηνυμάτων εξασφαλίζεται με την ψηφιακή υπογραφή. Αν η διαδικασία της ψηφιακής υπογραφής όμως δεν είναι κατανοητή στο χρήστη, ο χρήστης μπορεί να χρησιμοποιήσει μονόδρομη συνάρτηση σύνοψης με χρήση διαμοιραζόμενου μυστικού κλειδιού. Από αυτήν τη συνάρτηση εξάγεται ένας κωδικός MAC (Message Authentication Code) που είναι υπεύθυνος για την αυθεντικοποίηση των δεδομένων.
3. Κρυπτογράφηση μηνύματος: Η κρυπτογράφηση των δεδομένων γίνεται με δύο τρόπους:
    - Με πιστοποιητικά δημόσιων κλειδιών, όπου ο αποστολέας του μηνύματος κρυπτογραφεί το κλειδί ανταλλαγής των μηνυμάτων με το δημόσιο κλειδί του παραλήπτη.
    - Χωρίς πιστοποιητικά δημόσιων κλειδιών, όπου η συναλλαγή των μηνυμάτων γίνεται με εξωτερικό κλειδί. Οι πληροφορίες και προδιαγραφές του εξωτερικού κλειδιού αναφέρονται στις επικεφαλίδες του S-HTTP. (8)

## 9.3. Σχέδιο ασφάλειας σε περίπτωση έκτακτης ανάγκης

Σε περίπτωση που συμβούν καταστροφές, όπως πυρκαγιά, πλημμύρα ή καταστροφικές ανθρώπινες ενέργειες, τα αρχεία υγειονομικής περίθαλψης και άλλα σημαντικά στοιχεία πρέπει να προστατευθούν και να μη χαθούν. Σ' αυτή την περίπτωση, υπάρχουν δύο πράγματα που πρέπει να γίνουν:

- Δημιουργία αντιγράφων ασφάλειας: Στις μεγάλες επιχειρήσεις η δημιουργία αντιγράφων ασφάλειας αποτελεί καθημερινή διεργασία. Ωστόσο, τα μέλη του προσωπικού είναι συνήθως εξοικειωμένα με τους υπολογιστές που χρησιμοποιούν στο σπίτι και δε λαμβάνουν σοβαρά υπόψιν τη δημιουργία αντιγράφων ασφάλειας μέχρι να συμβεί η καταστροφή. Είναι λοιπόν απαραίτητο, από την πρώτη μέρα που αρχίζει να λειτουργεί ένα Πληροφοριακό Σύστημα, οι πληροφορίες του να υποστηρίζονται τακτικά και αξιόπιστα. Σε περίπτωση έκτακτης ανάγκης, είναι σημαντικό το αντίγραφο ασφάλειας να ανακτήσει τα δεδομένα γρήγορα και με ακρίβεια. Για να είμαστε σίγουροι ότι το αντίγραφο ασφάλειας θα μπορέσει να ανταποκριθεί σε μία τέτοια περίπτωση, χρειάζεται τακτικό έλεγχο της λειτουργίας του. Επίσης, το αντίγραφο ασφάλειας πρέπει να αποθηκευτεί σε τέτοιο σημείο που να μην καταστραφεί από την ίδια καταστροφή που πλήττει το κύριο σύστημα. Αυτό σημαίνει ότι μπορεί να χρειαστεί να δημιουργηθούν αντίγραφα ασφάλειας πολλά μίλια μακριά από το νοσοκομείο για να μπορέσουν να διατηρηθούν ασφαλή. Ακόμα, κάποιοι τύποι μέσων δημιουργίας αντιγράφων ασφάλειας, όπως η μαγνητική ταινία και οι αφαιρούμενοι σκληροί δίσκοι, είναι επαναχρησιμοποιούμενοι. Αυτό σημαίνει ότι μπορεί να αλλοιωθούν με την πάροδο του χρόνου και με επαναλαμβανόμενα αντίγραφα ασφάλειας. Για το λόγο αυτό, χρειάζονται συχνοί έλεγχοι.
- Προγραμματισμός ανάκτησης: Σε περίπτωση έκτακτης ανάγκης, οι οργανισμοί υγειονομικής περίθαλψης μπορεί να κληθούν να παρέχουν γρήγορα ιατρικές πληροφορίες και αρχεία. Για αυτό, θα πρέπει να υπάρχει μία σαφής διαδικασία ανάκτησης που θα πρέπει να ακολουθηθεί. Ο οργανισμός πρέπει να είναι προετοιμασμένος να έχει πρόσβαση στα

αντίγραφα ασφάλειας και να ανακτήσει τη λειτουργικότητά τους, το οποίο απαιτεί γνώσεις σχετικά με το ποια αρχεία ανακτήθηκαν, πότε ανακτήθηκαν, πού είναι αποθηκευμένα τα αντίγραφα ασφάλειας και τι είδους εξοπλισμός χρειάζεται για να τα ανακτήσει.

Για να είναι αποτελεσματικά τα αντίγραφα ασφάλειας και να μπορέσει να λειτουργήσει το σχέδιο ανάκτησης, υπάρχουν κάποιοι κανόνες:

- Υπάρχει συγκεκριμένη πολιτική που καθορίζει πώς πρέπει να είναι τα αντίγραφα ασφάλειας και ο προγραμματισμός ανάκτησης.
- Όλα τα μέλη του προσωπικού πρέπει να είναι ενημερωμένα για το σχέδιο ασφάλειας και για τα καθήκοντά τους σε περίπτωση έκτακτης ανάγκης.
- Θα πρέπει να υπάρχει ένα αντίγραφο του σχεδίου ανάκτησης σε αξιόπιστο μέρος εκτός του οργανισμού.
- Πρέπει να δημιουργούνται οπωσδήποτε αντίγραφα ασφάλειας για τα αρχεία μεγάλης σημασίας.
- Το πρόγραμμα δημιουργίας αντιγράφων ασφάλειας είναι έγκαιρο και ελέγχεται τακτικά.
- Κάθε εκτέλεση των αντιγράφων ασφάλειας ελέγχεται για την ικανότητά του να επαναφέρει τα δεδομένα με ακρίβεια.
- Τα μέσα δημιουργίας αντιγράφων ασφάλειας είναι φυσικά προστατευμένα.
- Τα αντίγραφα ασφάλειας που είναι αποθηκευμένα εκτός του οργανισμού είναι κρυπτογραφημένα.
- Τα μέσα δημιουργίας αντιγράφων ασφάλειας καθίστανται δυσανάγνωστα πριν από τη διάθεσή τους.
- Τα πολλαπλά αντίγραφα ασφάλειας διατηρούνται ως αποτυχημένα. (15)

## ΚΕΦΑΛΑΙΟ 10. ΣΥΜΠΕΡΑΣΜΑΤΑ

Στα Πληροφοριακά Συστήματα που χρησιμοποιούνται στους χώρους της σύγχρονης υγειονομικής περίθαλψης, γίνεται συχνά αποθήκευση των ιατρικών πληροφοριών των ασθενών αλλά και ανταλλαγή αυτών των πληροφοριών μεταξύ διαφόρων παρόχων υπηρεσιών υγείας. Επίσης, αποθηκεύονται και μεταδίδονται δεδομένα που σχετίζονται με τα στοιχεία του νοσοκομείου και του προσωπικού που εργάζεται σε αυτό. Όλα αυτά τα στοιχεία πρέπει να διατηρούνται ασφαλή στα Πληροφοριακά Συστήματα των Νοσοκομείων, καθώς ενέχουν πολλοί κίνδυνοι στις μονάδες υγείας. Τέτοιοι κίνδυνοι είναι οι φυσικές απειλές, οι ανθρώπινες απειλές, οι κίνδυνοι τεχνολογίας, το θεσμικό και φυσικό περιβάλλον του έργου, οι επιχειρησιακοί κίνδυνοι και οι κίνδυνοι οργάνωσης έργου. Για τους αναφερθέντες κινδύνους, πρέπει να γίνεται σωστή αξιολόγηση έτσι ώστε να μπορέσουν να περιοριστούν. Πρέπει, δηλαδή, να εκτιμηθεί η ζημιά που μπορεί να προκαλέσει κάθε μία από αυτές τις απειλές και να προταθούν προστατευτικά μέτρα. Για κάθε προστατευτικό μέτρο, πρέπει να προβλεφθεί η δαπάνη που ενδεχομένως να στοιχίσει η λήψη του, καθώς και οι συνέπειες που θα έχει έναντι κάθε απειλής. Στο τέλος της αξιολόγησης των κινδύνων, επιλέγονται ποια προστατευτικά μέτρα ή συνδυασμός προστατευτικών μέτρων θα ληφθούν. Τα προστατευτικά μέτρα που λαμβάνονται έχουν ως στόχο να παρέχουν ασφάλεια στα Πληροφοριακά Συστήματα των νοσοκομείων, και κατά τη διάρκεια των καθημερινών διεργασιών και σε περίπτωση έκτακτης ανάγκης. Αυτά τα μέτρα περιλαμβάνουν γενικά προστατευτικά μέτρα για κάθε υπολογιστή, έλεγχο και περιορισμό της πρόσβασης στο δίκτυο των νοσοκομείων, ασφάλεια των συσκευών, κρυπτογράφηση δεδομένων και πρωτόκολλα για την ασφάλεια υψηλού επιπέδου στο χώρο της υγείας. Σε συνδυασμό με την εφαρμογή μιας πολιτικής ασφάλειας αποτελούν το σχέδιο δράσης ασφάλειας του νοσοκομείου.

## ΒΙΒΛΙΟΓΡΑΦΙΑ

(1)Πληροφοριακά Συστήματα. Βικιπαίδεια [Online]. 2018 March 21 [cited 2018 September 16]; Available from:

URL:
https://el.wikipedia.org/wiki/%CE%A0%CE%BB%CE%B7%CF%81%CE%BF%CF%86%CE%BF%CF%81%CE%B9%CE%B1%CE%BA%CE%AC_%CF%83%CF%85%CF%83%CF%84%CE%AE%CE%BC%CE%B1%CF%84%CE%B1

(2) Bourgeois D. Information Systems for Business and Beyond. Pressbooks [Online]. 2014 February [cited 2018 September 16]; Available from:
URL:

https://bus206.pressbooks.com

(3) Ολοκληρωμένο πληροφοριακό σύστημα νοσοκομείου. Βικιπαίδεια [Online]. 2017 December 09 [cited 2018 September 16]; Available from:
URL:

https://el.wikipedia.org/wiki/%CE%9F%CE%BB%CE%BF%CE%BA%CE%BB%CE%B7%CF%81%CF%89%CE%BC%CE%AD%CE%BD%CE%BF_%CF%80%CE%BB%CE%B7%CF%81%CE%BF%CF%86%CE%BF%CF%81%CE%B9%CE%B1%CE%BA%CF%8C_%CF%83%CF%8D%CF%83%CF%84%CE%B7%CE%BC%CE%B1_%CE%BD%CE%BF%CF%83%CE%BF%CE%BA%CE%BF%CE%BC%CE%B5%CE%AF%CE%BF%CF%85

(4) Μάρκοβιτς Ι, Μοναστηρίδου Σ. Η Διαχείριση Αλλαγών στην Υγεία: Η Περίπτωση της Εισαγωγής Ολοκληρωμένου Πληροφοριακού Συστήματος σε Δημόσιο Νοσοκομείο. Νοσηλευτική [Online]. 2011 July 25 [cited 2018 September 16]; Available from:
URL:

http://hjn.gr/wp-content/uploads/2014/10/get_pdf-53.pdf

(5) Βαγγελάτος Α, Σαριβουγιούκας Ι. Πληροφοριακό Σύστημα Νοσοκομείου: Απαραίτητη υποδομή στο σύγχρονο Νοσοκομείο. Ιατρολέξη [Online]. 2001 [cited 2018 September 16]; Available from:
URL:

http://www.iatrolexi.gr/vagelat/Iatriki_2001.pdf

(6) Προκόπος Γ. Ανάλυση Κινδύνων και Συστήματα Διαχείρισης Ασφαλείας Πληροφοριακών Συστημάτων σε Μεγάλους Οργανισμούς. Τ.Ε.Ι. ΠΕΛΟΠΟΝΝΗΣΟΥ [Online]. 2014 November [cited 2018 September 16]; Available from:
URL:

http://nestor.teipel.gr/xmlui/bitstream/handle/123456789/13433/STE_MHP_00188_Medium.pdf?sequence=1

(7) Mantas J, Hasman A. Πληροφορική της Υγείας. Αθήνα: Ιατρικές Εκδόσεις Π.Χ. Πασχαλίδης, 2007.

(8) Γκρίτζαλης Στ, Γκρίτζαλη Δ, Κάτσικας Σ. Ασφάλεια Δικτύων Υπολογιστών: Τεχνολογίες και Υπηρεσίες σε περιβάλλοντα Ηλεκτρονικού Επιχειρείν και Ηλεκτρονικής Διακυβέρνησης. Αθήνα: Εκδόσεις Παπασωτηρίου, 2003.

(9)Ασφάλεια πληροφοριακών συστημάτων. Βικιπαίδεια [Online] . 2017 May 06 [cited 2018 September 16]; Available from:
URL:

https://el.wikipedia.org/wiki/%CE%91%CF%83%CF%86%CE%AC%CE%BB%CE%B5%CE%B9%CE%B1_%CF%80%CE%BB%CE%B7%CF%81%CE%BF%CF%86%CE%BF%CF%81%CE%B9%CE%B1%CE%BA%CF%8E%CE%BD_%CF%83%CF%85%CF%83%CF%84%CE%B7%CE%BC%CE%AC%CF%84%CF%89%CE%BD

(10) Wears R, Leveson N. "Safeware": Safety-Critical Computing and Health Care Information Technology. NCBI [Online]. [cited 2018 September 16]; Available from:
URL:

https://www.ncbi.nlm.nih.gov/books/NBK43774/pdf/Bookshelf_NBK43774.pdf

(11) Guide to Privacy and Security of Electronic Health Information. The office of the National Coordinator for Health Information Technology [Online]. 2015 April [cited 2018 September 16]; Available from:
URL:

file:///C:/Users/USER/Downloads/privacy-and-security-guide.pdf

(12) Shin L. Why Medical Identity Theft Is Rising And How To Protect Yourself. Forbes [Online]. 2015 May 29 [cited 2018 September 16]; Available from:

URL:

https://www.forbes.com/sites/laurashin/2015/05/29/why-medical-identity-theft-is-rising-and-how-to-protect-yourself/#10a51e303608

(13) Βάγια Α, Βασιλείου Α. Ασφάλεια και έλεγχος νοσοκομειακών πληροφοριακών συστημάτων. ΤΕΙ Καλαμάτας Τμήμα εκδόσεων βιβλιοθήκης [Online]. [cited 2018 September 16]; Available from:
URL:

http://nestor.teipel.gr/xmlui/bitstream/handle/123456789/12292/SDO_DMYP_00250_Medium.pdf?sequence=1

(14) Data Security for Health Care. The SEISMED Consortium [Online]. 1996 [cited 2018 September 16]; Available from:
URL:

https://books.google.gr/books?hl=el&lr=&id=QiuzOJlT5GAC&oi=fnd&pg=PA4&dq=%CF%80%CE%BF%CE%BB%CE%B9%CF%84%CE%B9%CE%BA%CE%B7+%CE%B1%CF%83%CF%86%CE%B1%CE%BB%CE%B5%CE%B9%CE%B1%CF%82+seismed&ots=TiRy04ADPi&sig=pabBvbICfSZg3vWuLSV_hSm_ov4&redir_esc=y#v=onepage&q=%CF%80%CE%BF%CE%BB%CE%B9%CF%84%CE%B9%CE%BA%CE%B7%20%CE%B1%CF%83%CF%86%CE%B1%CE%BB%CE%B5%CE%B9%CE%B1%CF%82%20seismed&f=false

(15) Top 10 Tips for Cybersecurity in Health Care. Department of health and human services USA [Online]. [cited 2018 September 16]; Available from:
URL:

https://www.healthit.gov/sites/default/files/Top_10_Tips_for_Cybersecurity.pdf

(16) Grimes R. Types of password attacks. ITProToday [Online] ,2006 January 30 [cited 2018 September 16]; Available from:
URL:

https://www.itprotoday.com/security/types-password-attacks

(17) Κυρίτσης Α. Πώς λειτουργεί το Antivirus. PC STEPS [Online]. 2014 July 23 [cited 2018 September 16]; Available from:
URL:

https://www.pcsteps.gr/1391-%CF%80%CF%8E%CF%82-%CE%BB%CE%B5%CE%B9%CF%84%CE%BF%CF%85%CF%81%CE%B3%CE%B5%CE%AF-%CF%84%CE%BF-antivirus/

(18) Rouse M. Network Access Control (NAC). TechTarget [Online]. [cited 2018 September 16]; Available from:
URL:

https://searchnetworking.techtarget.com/definition/network-access-control

(19) Walton Ch. Novell's Border Manager Authentication Service: Arm Your Network for Remote Users. MICROFOCUS [Online]. 1998 December 01 [cited 2018 September 16]; Available from:
URL:

https://support.novell.com/techcenter/articles/nc1998_12b.html

(20) Server room. Wikipedia [Online]. 2018 August 02 [cited 2018 September 16]; Available from:
URL:

https://en.wikipedia.org/wiki/Server_room

(21) Data Center Server Room. Legrand [Online]. 2011 [cited 2018 September 16]; Available from:
URL:

https://www.legrand.gr/solutions/data-center/server-room.html

(22) Κυρίτσης Α. Κρυπτογράφηση δεδομένων- Τι είναι και πώς λειτουργεί. PC STEPS [Online]. 2016 January 21 [cited 2018 September 16]; Available from:
URL:

https://www.pcsteps.gr/16634-%CE%BA%CF%81%CF%85%CF%80%CF%84%CE%BF%CE%B3%CF%81%CE%AC%CF%86%CE%B7%CF%83%CE%B7-%CE%B4%CE%B5%CE%B4%CE%BF%CE%BC%CE%AD%CE%BD%CF%89%CE%BD

(23) Allaërt FA, Blober B, Louwerse K, Barber B. Security standards for healthcare information systems: a perspective from the EU ISIS MEDSEC Project. Amsterdam (AMS): IOS Press; 2002. p. 160-161. 164-166.

(24) PPTP Definition. Tech Terms [Online]. 2018 [cited 2018 September 16]; Available from:
URL:

https://techterms.com/definition/pptp

(25) Derian M. Websites & HTTPS - Συνδεθείτε ασφαλώς μέσω του πρωτοκόλλου ασφαλείας SSL. Wedia [Online]. 2015 September 15 [cited 2018 September 16]; Available from:
URL:

https://blog.wedia.gr/websites-https-protokolo-ssl