ΜΗΤΡΟΠΟΛΙΤΙΚΟ ΚΟΛΛΕΓΙΟ

University of East London

SCHOOL OF ARCHITECTURE, COMPUTING & ENGINEERING

MSc Information Security & Digital Forensics

Εργασία του μαθήματος CN7014 – Security Management

Τίτλος εργασίας: Παρουσίαση μεθοδολογιών «Risk Assessment» και συμβολική υλοποίηση σχεδίου ασφαλείας

ΕΠΟΠΤΕΥΩΝ ΚΑΘΗΓΗΤΗΣ
ΑΡΟΥΚΑΤΟΣ ΝΙΚΟΛΑΟΣ

ΕΠΙΜΕΛΕΙΑ ΕΡΓΑΣΙΑΣ
U2121211

ΙΔΡΥΜΑ
ΜΗΤΡΟΠΟΛΙΤΙΚΟ ΚΟΛΛΕΓΙΟ CAMPUS ΑΜΑΡΟΥΣΙΟΥ

15 Ιανουαρίου 2023

Πίνακας περιεχομένων

Σκοπός της εργασίας είναι η παρουσίαση μιας ολοκληρωμένης πρότασης ενός σχεδίου ασφαλείας αναφορικά με ένα διαγνωστικό κέντρο που επεξεργάζεται προσωπικά και ευαίσθητα προσωπικά δεδομένα.

Έπειτα από προγραμματισμένη επίσκεψη στις εγκαταστάσεις του διαγνωστικού κέντρου, πραγματοποιήθηκε μια σειρά ενεργειών που περιλάμβανε: επιθεώρηση του χώρου και καταγραφή των περιουσιακών στοιχείων του κέντρου, εκτίμηση των κινδύνων που ελλοχεύουν, συνεντεύξεις με τα αρμόδια στελέχη, καθώς και συγγραφή της δήλωσης εφαρμογής και των πολιτικών ασφαλείας της επιχείρησης.

Αρχικά, κατά την επιθεώρηση του χώρου και την καταγραφή των περιουσιακών στοιχείων του κέντρου δημιουργήθηκε η υποδομή του πληροφοριακού συστήματος της επιχείρησης. Σε αυτήν περιλαμβάνονται: ένα σύστημα επικοινωνίας με υπηρεσίες «Cloud» για διεργασίες, όπως ταυτοποίηση και επικοινωνία, συσκευές δικτύου, απαραίτητες για την ασφάλεια των συνδέσεων (τοίχος προστασίας) και για την διασυνδεσιμότητα των συσκευών σε τοπικό επίπεδο (switches, router), όπως και ο χώρος φύλαξης και λειτουργίας (server room) των διακομιστών του Διαγνωστικού Κέντρου. Επίσης, στον χώρο των εγκαταστάσεων της δομής υφίσταται ένα πλήθος ιατρικών μηχανημάτων με δυνατότητα σύνδεσης στο διαδίκτυο, στους χώρους εργασίας (γραφεία) αντιστοιχεί από ένας επιτραπέζιος ηλεκτρονικός υπολογιστής και ένα τηλέφωνο IP (για επικοινωνία μέσω διαδικτύου) σε κάθε υπάλληλο, καθώς και υπάρχει πρόβλεψη για ασύρματη σύνδεση συσκευών κάνοντας χρήση ασύρματων σημείων πρόσβασης.

Έπειτα, μέσω των συνεντεύξεων, καθορίστηκε το πεδίο εφαρμογής του Συστήματος Διαχείρισης Ασφάλειας Πληροφοριών του Διαγνωστικού Κέντρου:

> *Το Διαγνωστικό Κέντρο παρέχει σε δύο ειδών ιατρικές υπηρεσίες: την κλινική παθολογία (π.χ. μικροβιολογία) και την ανατομική παθολογία (π.χ. κυτταρολογία). Οι υπηρεσίες αυτές προσφέρονται τόσο σε εσωτερικούς και εξωτερικούς ασθενείς νοσοκομείων, όσο και σε κλινικούς και άλλους μη νοσοκομειακούς ασθενείς. Συνεπώς, σκοπός του είναι η διασφάλιση της ασφάλειας των αγαθών του, στα οποία περιλαμβάνονται τα προσωπικά δεδομένα των υπαλλήλων και των ασθενών, τα ιατρικά δεδομένα των ασθενών, τα ιατρικά μηχανήματα και όλες τις υποδομές πληροφορικής συμπεριλαμβανομένων των λογισμικών που εκτελούνται. Ως μία επιχείρηση που δραστηριοποιείται μόνο δια ζώσης, οποιεσδήποτε διαδικασίες «απομακρυσμένης φύσεως» εξαιρούνται από το πεδίο εφαρμογής.*

Στη συνέχεια, αποσαφηνίστηκαν οι στόχοι του, μερικοί από τους οποίους είναι:

- Η προστασία της ψηφιακής διαχείρισης και επεξεργασίας των ιατρικών πληροφοριών από οποιαδήποτε μη εξουσιοδοτημένη πρόσβαση.
- Η διατήρηση της εμπιστευτικότητας, της ακεραιότητας και της διαθεσιμότητας των πληροφοριών.
- Η διασφάλιση της τήρησης των νομοκανονιστικών απαιτήσεων.
- Η αυτοματοποίηση χειρωνακτικών εργασιών, με σκοπό την γρηγορότερη επεξεργασία δεδομένων και κατά συνέπεια, την καλύτερη οικονομική και διοικητική οργάνωση.

Αφού εξασφαλίσθηκε η εξουσιοδότηση για την άντληση των απαιτούμενων στοιχείων, ακολούθησε η διαδικασία ανάλυσης και διαχείρισης επικινδυνότητας σύμφωνα με την μέθοδο «CRAMM» (CCTA Risk Analysis and Management Methodology). Η μέθοδος αυτή αποτελείται από τρία στάδια, τα οποία αναλύονται παρακάτω: 1. Προσδιορισμός και αξιολόγηση περιουσιακών στοιχείων (υλικολογισμικά αγαθά και δεδομένα), 2. Ανάλυση επικινδυνότητας και 3. Διαχείριση Επικινδυνότητας.

1. Προσδιορισμός και αξιολόγηση περιουσιακών στοιχείων

Σε αυτό το στάδιο δημιουργείται το μοντέλο του πληροφοριακού συστήματος, ταξινομώντας τα περιουσιακά στοιχεία σε κατηγορίες και προσδιορίζοντας τα και στη συνέχεια, πραγματοποιείται αποτίμηση τους. Στο αρχείο «Asset_Tracking.xlsx» περιέχεται η πλήρης λίστα περιουσιακών στοιχείων του διαγνωστικού κέντρου.

Προς διευκόλυνση των διαδικασιών του σταδίου προσδιορισμού και αξιολόγησης, τα περιουσιακά στοιχεία χωρίστηκαν στις εξής τρεις κατηγορίες:

- *Στοιχεία υλικού:* Περιλαμβάνει όλες τις συσκευές που αποτελούν το υπολογιστικό σύστημα του διαγνωστικού κέντρου.
- *Στοιχεία λογισμικού:* Περιλαμβάνει κάθε είδους λογισμικό που εκτελείται στα υλικά στοιχεία.
- *Στοιχεία δεδομένων:* Περιλαμβάνει όλους τους τύπους δεδομένων που επεξεργάζεται το διαγνωστικό κέντρο.

1.1. Δημιουργία μοντέλου του πληροφοριακού συστήματος

1η Κατηγορία: Περιουσιακά Στοιχεία Υλικού

Τα περιουσιακά στοιχεία υλικού που χρησιμοποιούνται στο υπολογιστικό σύστημα του διαγνωστικού κέντρου είναι:

1. *Διακομιστής που κάνει χρήση του πρωτοκόλλου «LDAP» (Lightweight Directory Access Protocol):* Ο κύριος διακομιστής του διαγνωστικού κέντρου που περιέχει το σύνολο των αρχείων και δεδομένων της επιχείρησης, αναφορικά με τους υπαλλήλους, τους πελάτες-ασθενείς, τα συστήματα και της υπηρεσίες, και τα διανέμει εντός του εσωτερικού δικτύου. Κατά συνέπεια, σε αυτόν τον διακομιστή βρίσκονται όλες οι βάσεις δεδομένων του κέντρου.
2. *Τείχος προστασίας:* Η μέθοδος προστασίας της σύνδεσης των συστημάτων του κέντρου με το εξωτερικό δίκτυο και τις υπηρεσίες «Cloud», στις οποίες βασίζονται κρίσιμες ενέργειες για τη σωστή λειτουργία του.
3. *Διαδικτυακός εξοπλισμός:* Περιλαμβάνει συσκευές που είναι απαραίτητες για τη σύνδεση σε δίκτυο (εσωτερικό-εξωτερικό), όπως «Switch», «Router», απαραίτητη καλωδίωση για σύνδεση των Η/Υ (Ethernet) και σύνδεση με τον πάροχο υπηρεσιών διαδικτύου (ISP).
4. *Ιατρικά μηχανήματα:* Απαραίτητα συστήματα για την παραγωγή αποτελεσμάτων των εξετάσεων, που διαθέτουν λειτουργίες σύνδεσης στο διαδίκτυο.
5. *Μέσα αντιγράφων ασφαλείας:* Μαγνητικές ταινίες μεγάλης χωρητικότητας, στις οποίες δημιουργούνται και αποθηκεύονται, καθημερινά, αντίγραφα ασφαλείας των δεδομένων και των λογισμικών των ηλεκτρονικών υπολογιστών του κέντρου.
6. *Ηλεκτρονικοί υπολογιστές (Επιτραπέζιοι/Φορητοί):* Ολοκληρωμένα συστήματα εκτέλεσης λογισμικών, τα οποία διαθέτει κάθε υπάλληλος του διαγνωστικού κέντρου που είναι αρμόδιος για την επεξεργασία δεδομένων.
7. *Εκτυπωτές (Ενσύρματοι/Ασύρματοι):* Συστήματα εκτύπωσης όλων των ειδών των εγγράφων.
8. *Τηλέφωνα «IP»:* Συσκευές επικοινωνίας που βασίζονται στην αρχή μετάδοσης της φωνής μέσω διαδικτύου.

2η Κατηγορία: Περιουσιακά Στοιχεία Λογισμικού

Τα περιουσιακά στοιχεία λογισμικού που χρησιμοποιούνται στο υπολογιστικό σύστημα του διαγνωστικού κέντρου είναι:

1. *Λειτουργικό σύστημα:* Λογισμικό που είναι υπεύθυνο για τη δημιουργία περιβάλλοντος επικοινωνίας των χρηστών με τα συστήματα Η/Υ.
2. *Λογισμικό σύνδεσης με τις υπηρεσίες «Cloud»:* Απαραίτητο λογισμικό για τη σύνδεση των συστημάτων με τις υπηρεσίες Cloud, που απαιτούνται για τη λειτουργία του διαγνωστικού κέντρου.
3. *Λογισμικό ιατρικών αρχείων:* Λογισμικό υπεύθυνο για τη δημιουργία, διατήρηση και επεξεργασία των ιατρικών φακέλων των ασθενών.
4. *Λογισμικό δημιουργίας αρχείων καταγραφής:* Αποσκοπεί στη διατήρηση αρχείων καταγραφής (log files) των συμβάντων που παρουσιάζονται στα υπολογιστικά συστήματα.
5. *Λογισμικό διαχείρισης βάσεων δεδομένων:* Επιτρέπει στους αρμόδιους χρήστες των Η/Υ να προσπελαύνουν τα δεδομένα που ζητώνται ανά περίπτωση.

3η Κατηγορία: Περιουσιακά Στοιχεία Δεδομένων

Τα περιουσιακά στοιχεία δεδομένων που χρησιμοποιούνται στο υπολογιστικό σύστημα του διαγνωστικού κέντρου είναι:

1. *Προσωπικά δεδομένα υπαλλήλων/ασθενών.*
2. *Ιατρικά δεδομένα/Αποτελέσματα εξετάσεων.*
3. *Διαγνώσεις/Συνοδευτικές εκθέσεις.*
4. *Διοικητικά δεδομένα.*
5. *Οικονομικά/Εφοδιαστικά Δεδομένα.*
6. *Δεδομένα συστήματος (π.χ. αντίγραφα ασφαλείας).*

1.2. Αποτίμηση περιουσιακών στοιχείων

1η Κατηγορία: Περιουσιακά Στοιχεία Υλικού

Ο προσδιορισμός της αξίας των περιουσιακών στοιχείων υλικού συντείνουν στον καθορισμό των κινδύνων και την επακόλουθη επιλογή αντιμέτρων. Στον πίνακα που ακολουθεί, τα στοιχεία βαθμολογήθηκαν βάσει της παρακάτω κλίμακας:

- Βαθμός κλίμακας 1 → 0 έως και 999€
- Βαθμός κλίμακας 2 → 1.000€ έως και 9.999€
- Βαθμός κλίμακας 3 → 10.000€ έως και 29.999€

- Βαθμός κλίμακας 4 → 30.000€ έως και 99.999€
- Βαθμός κλίμακας 5 → 100.000€ έως και 300.000€

Υλικό	**Βαθμός**
Διακομιστής «LDAP»	4
Τείχος προστασίας	3
Διαδικτυακός εξοπλισμός	1
Ιατρικά μηχανήματα	5
Μέσα αντιγράφων ασφαλείας	2
Ηλεκτρονικοί υπολογιστές	2
Εκτυπωτές	2
Τηλέφωνα «IP»	1

Πίνακας 1 - Αποτίμηση περιουσιακών στοιχείων υλικού

2η Κατηγορία: Περιουσιακά Στοιχεία Λογισμικού

Ομοίως με τα περιουσιακά στοιχεία υλικού, ο προσδιορισμός της αξίας των στοιχείων λογισμικού συνεισφέρει στον υπολογισμό των κινδύνων και την επακόλουθη επιλογή αντιμέτρων, καθώς επίσης βαθμολογούνται με βάση την ίδια κλίματα.

Λογισμικό	**Βαθμός**
Λειτουργικό σύστημα	1
Λογισμικό σύνδεσης με τις υπηρεσίες «Cloud»	3
Λογισμικό ιατρικών αρχείων	2
Λογισμικό δημιουργίας αρχείων καταγραφής	2
Λογισμικό διαχείρισης βάσεων δεδομένων	2

Πίνακας 2 - Αποτίμηση περιουσιακών στοιχείων λογισμικού

3η Κατηγορία: Περιουσιακά Στοιχεία Δεδομένων

Η αποτίμηση των περιουσιακών στοιχείων δεδομένων θεωρείται ένα από τα μείζονα στοιχεία για τον σχεδιασμό των απαιτήσεων ασφαλείας ενός οργανισμού. Η αξία κάθε αγαθού βασίζεται στις επιπτώσεις που παρουσιάζονται σε περίπτωση απώλειάς του και πιο συγκεκριμένα, σε περίπτωση καταστροφής, μη εξουσιοδοτημένης μεταβολής, αποκάλυψης ή μη-διαθεσιμότητας. Μέσω της μεθόδου CRAMM, εκτιμάται το δυσμενέστερο πιθανό σενάριο για κάθε περίπτωση ενώ, το μέγεθος της επίπτωσης εκτιμάται αριθμητικά με τιμές κλίμακας από 1 έως 10, όπου 1 είναι η χαμηλότερη τιμή και 10 η υψηλότερη.

	Μη-διαθεσιμότητα										**Κατα-στροφή**		**Αποκά-λυψη**		**Μεταβολή**		
Όνομα	15Λ	1Ω	3Ω	12Ω	1Μ	2Μ	1Ε	2Ε	1ΜΗ	2ΜΗ	ΜΚ	ΟΚ	ΑΕΝ	ΑΕΚ	ΜΚΕ	ΜΓΕ	ΕΜ
Προσωπικά δεδομένα υπαλλήλων/ασθενών	4	4	4	5	6	7	8	9	10	10	7	9	7	8	6	7	8
Ιατρικά δεδομένα/Αποτελέσματα εξετάσεων	6	7	8	9	10	10	10	10	10	10	8	10	8	9	8	9	10
Διαγνώσεις/Συνοδευτικές εκθέσεις	5	6	7	9	10	10	10	10	10	10	7	10	7	8	7	8	9
Διοικητικά δεδομένα	3	3	4	4	5	5	6	7	8	8	7	10	6	8	6	7	8
Οικονομικά/Εφοδιαστικά Δεδομένα	3	3	3	4	4	5	6	6	7	8	6	8	5	6	5	6	7
Δεδομένα συστήματος (π.χ. αντίγραφα ασφαλείας)	3	3	3	4	5	5	6	7	8	8	6	8	5	6	4	5	6

Πίνακας 3 - Αποτίμηση περιουσιακών στοιχείων δεδομένων

ΜΚ = Μερική Καταστροφή	ΜΚΕ = Μικρής Έκτασης Σφάλματα
ΟΚ = Ολική Καταστροφή	ΜΓΕ = Μεγάλης Έκτασης Σφάλματα
ΑΕΝ = Αποκάλυψη Εντός Οργανισμού	ΕΜ = Εκούσια Μεταβολή Δεδομένων
ΑΕΚ = Αποκάλυψη Εκτός Οργανισμού	

Πίνακας 4 - Υπόμνημα πίνακα αποτίμησης περιουσιακών στοιχείων δεδομένων

2. Ανάλυση επικινδυνότητας

Στο παρόν στάδιο υλοποιούνται οι διαδικασίες υπολογισμού του επιπέδου απειλών (threat level) και του επιπέδου αδυναμιών (vulnerability level) του πληροφοριακού συστήματος του διαγνωστικού κέντρου, όπως επίσης και του βαθμού επικινδυνότητας τους. Ομοίως με το πρώτο στάδιο, έτσι και σε αυτό, τα περιουσιακά στοιχεία χωρίστηκαν στις ίδιες τρεις κατηγορίες: 1. Περιουσιακά Στοιχεία Υλικού, 2. Περιουσιακά Στοιχεία Λογισμικού και 3. Περιουσιακά Στοιχεία Δεδομένων.

2.1. Προσδιορισμός απειλών ανά κατηγορία περιουσιακών στοιχείων

1η Κατηγορία: Απειλές Περιουσιακών Στοιχείων Υλικού

Οι απειλές που αφορούν τα περιουσιακά στοιχεία υλικού είναι οι εξής:

1. *Κακή χρήση των πόρων του συστήματος.*
2. *Κλοπή από «εσωτερικές» ή «εξωτερικές» οντότητες.*
3. *Εκ προθέσεως φθορά.*
4. *Διακοπή ρεύματος.*
5. *Σφάλματα συντήρησης.*
6. *Τεχνική βλάβη του εξυπηρετητή.*
7. *Τεχνική βλάβη των συσκευών αποθήκευσης/εκτύπωσης.*
8. *Τεχνική βλάβη των υπηρεσιών δικτύου.*

2η Κατηγορία: Απειλές Περιουσιακών Στοιχείων Λογισμικού

Οι απειλές που αφορούν τα περιουσιακά στοιχεία λογισμικού είναι οι εξής:

1. *Τεχνική βλάβη των υπηρεσιών δικτύου.*
2. *Τεχνική βλάβη του εξυπηρετητή.*
3. *Μη εξουσιοδοτημένη χρήση εφαρμογών.*
4. *Βλάβη λογισμικού εφαρμογών.*
5. *Σφάλματα Εργασιών.*
6. *Κακή χρήση των πόρων του συστήματος.*
7. *Εκτέλεση κακόβουλου κώδικα.*
8. *Εκτέλεση επιβλαβούς λογισμικού.*
9. *Σφάλματα χρηστών.*

3η Κατηγορία: Απειλές Περιουσιακών Στοιχείων Δεδομένων

Οι απειλές που αφορούν τα περιουσιακά στοιχεία δεδομένων είναι οι εξής:

1. *Υποκλοπή Επικοινωνιών.*
2. *Βλάβη Επικοινωνιών.*
3. *Λανθασμένη δρομολόγηση.*
4. *Χρήση ψεύτικης ταυτότητας χρήστη από «εσωτερικές» ή «εξωτερικές» οντότητες (Masquerade Attack).*
5. *Αποποίηση Ευθυνών.*
6. *Κλοπή από «εσωτερικές» ή «εξωτερικές» οντότητες.*
7. *Τεχνική βλάβη των συσκευών αποθήκευσης.*
8. *Τεχνική βλάβη του εξυπηρετητή.*
9. *Μη εξουσιοδοτημένη χρήση εφαρμογών.*
10. *Σφάλματα χρηστών.*

2.2. Κατηγοριοποίηση απειλών

Βάσει των προαναφερθέντων απειλών περιουσιακών στοιχείων, πραγματοποιείται η κατηγοριοποίησή τους σύμφωνα με το είδος τους ενώ, προστίθεται και η κατηγορία απειλών φυσικού περιβάλλοντος, καθώς αφορά το σύνολο των στοιχείων του πληροφοριακού συστήματος.

1η Κατηγορία: Φυσικό Περιβάλλον

1. *Απειλή από σεισμό.*
2. *Εκδήλωση πυρκαγιάς στις εγκαταστάσεις του διαγνωστικού κέντρου.*
3. *Διαρροή υδάτων λόγω κακής κατασκευής του δικτύου ή παλαιότητας των σωληνώσεων.*
4. *Αδυναμία ηλεκτροδότησης.*
5. *Παρεμβολή στις διαδικασίες μετάδοσης πληροφορίας και προσωπικών δεδομένων.*

2η Κατηγορία: Ανθρώπινος Παράγοντας

1. *Τροποποίηση, υποκλοπή ή καταστροφή πληροφοριών.*
2. *Παραποίηση ή κοινοποίηση περιεχομένου απόρρητων βάσεων δεδομένων.*
3. *Εξασφάλιση πρόσβασης σε κακόβουλους χρήστες.*

4. *Δολιοφθορά από δυσαρεστημένους υπαλλήλους.*

3η Κατηγορία: Τεχνολογικοί Κίνδυνοι

1. *Χρήση τεχνολογιών αβέβαιου μέλλοντος (πιθανόν να καταστούν μη λειτουργικές ή παρωχημένες).*
2. *Αδυναμία σύνδεσης όλων των μερών του πληροφοριακού συστήματος.*
3. *Ασυμβατότητα υπάρχοντος εξοπλισμού με εγκαθιστάμενο σύστημα νεότερης τεχνολογίας.*
4. *Εγκατάσταση ελαττωματικού εξοπλισμού.*

4η Κατηγορία: Επιχειρησιακοί Κίνδυνοι

1. *Αδυναμία χρήσης συστημάτων λόγω έλλειψης εκπαιδευμένου προσωπικού.*
2. *Καταστροφή περιουσιακών στοιχείων υλικού ή λογισμικού λόγω κακής χρήσης.*
3. *Λανθασμένη εγκατάσταση περιουσιακού στοιχείου υλικού ή λογισμικού εξαιτίας έλλειψης τεχνικών γνώσεων ή ανθρώπινου λάθους.*

2.3. Αποτίμηση απειλών κι ευπαθειών

Για να διεκπεραιωθεί υπολογισμός των απαιτήσεων ασφαλείας κρίνεται απαραίτητη η εκτίμηση του μεγέθους απειλής για κάθε συνδυασμό απειλής-περιουσιακού στοιχείου, όπως επίσης και της έκτασης των ευπαθειών που μπορούν να οδηγήσουν στην πραγματοποίηση της απειλής. Σύμφωνα με την μέθοδο CRAMM η εκτίμηση της απειλής ορίζεται σε κλίματα από 1 έως 5:

1. *Πολύ χαμηλή:* Ένα επεισόδιο αναμένεται να συμβεί, κατά μέσο όρο, μία φορά κάθε 5 χρόνια.
2. *Χαμηλή:* Ένα επεισόδιο αναμένεται να συμβεί, κατά μέσο όρο, μία φορά κάθε 3 χρόνια.
3. *Μέτρια:* Ένα επεισόδιο αναμένεται να συμβεί, κατά μέσο όρο, μία φορά κάθε χρόνο.
4. *Υψηλή:* Ένα επεισόδιο αναμένεται να συμβεί, κατά μέσο όρο, μία φορά κάθε 6 μήνες.
5. *Πολύ υψηλή:* Ένα επεισόδιο αναμένεται να συμβεί, κατά μέσο όρο, μία φορά κάθε μήνα.

Ενώ, η εκτίμηση της σοβαρότητας της ευπάθειας ορίζεται σε κλίμακα από 1 έως 3:

1. *Χαμηλή:* Μικρή πιθανότητα (έως 33%) να συμβεί το χείριστο σενάριο που αξιολογήθηκε κατά την αποτίμηση περιουσιακών στοιχείων.
2. *Μέτρια:* Μέτρια πιθανότητα (μεταξύ 33% και 66%) να συμβεί το χείριστο σενάριο που αξιολογήθηκε κατά την αποτίμηση περιουσιακών στοιχείων.
3. *Υψηλή:* Υψηλή πιθανότητα (άνω του 66%) να συμβεί το χείριστο σενάριο που αξιολογήθηκε κατά την αποτίμηση περιουσιακών στοιχείων.

Παρακάτω, επιλέχθηκαν ενδεικτικά τρεις απειλές, μία για κάθε κατηγορία περιουσιακού στοιχείου, ώστε να δομηθεί μια συνοπτική αναφορά σχετικά με το πόσο εκτεθειμένο είναι το πληροφοριακό σύστημα και τα δεδομένα του διαγνωστικού κέντρου στις απειλές αυτές:

- **Απειλή περιουσιακών στοιχείων υλικού**: Τεχνική βλάβη των υπηρεσιών δικτύου

Περιουσιακό Στοιχείο	**Επίπτωση**	**Απειλή**	**Ευπάθεια**
Διακομιστής «LDAP»	Μη-διαθεσιμότητα	Υψηλή	Υψηλή
Τείχος προστασίας	Μη-διαθεσιμότητα	Υψηλή	Υψηλή
Διαδικτυακός εξοπλισμός	Σφάλμα μετάδοσης δεδομένων	Υψηλή	Υψηλή
Ιατρικά μηχανήματα	Σφάλμα μετάδοσης δεδομένων	Υψηλή	Υψηλή
Μέσα αντιγράφων ασφαλείας	Σφάλμα μετάδοσης δεδομένων	Μέτρια	Μέτρια
Ηλεκτρονικοί υπολογιστές	Σφάλμα μετάδοσης δεδομένων	Πολύ χαμηλή	Χαμηλή
Εκτυπωτές	Σφάλμα μετάδοσης δεδομένων	Πολύ χαμηλή	Χαμηλή
Τηλέφωνα «IP»	Μη-διαθεσιμότητα	Χαμηλή	Υψηλή

Πίνακας 5 - Απειλή περιουσιακών στοιχείων υλικού: Τεχνική βλάβη των υπηρεσιών δικτύου

- **Απειλή περιουσιακών στοιχείων λογισμικού**: Εκτέλεση κακόβουλου κώδικα

Περιουσιακό Στοιχείο	Επίπτωση	Απειλή	Ευπάθεια
Λειτουργικό σύστημα	Μη διαθεσιμότητα ή/και Απώλεια δεδομένων	Μέτρια	Μέτρια
Λογισμικό σύνδεσης με τις υπηρεσίες «Cloud»	Μη-διαθεσιμότητα ή/και Σφάλμα μετάδοσης δεδομένων ή/και Αποκάλυψη	Υψηλή	Μέτρια
Λογισμικό ιατρικών αρχείων	Απώλεια δεδομένων ή/και Μεταβολή ή/και Αποκάλυψη	Πολύ υψηλή	Υψηλή
Λογισμικό δημιουργίας αρχείων καταγραφής	Απώλεια δεδομένων ή/και Μεταβολή	Μέτρια	Υψηλή
Λογισμικό διαχείρισης βάσεων δεδομένων	Απώλεια δεδομένων ή/και Μεταβολή ή/και Αποκάλυψη	Υψηλή	Υψηλή

Πίνακας 6 - Απειλή περιουσιακών στοιχείων λογισμικού: Εκτέλεση κακόβουλου κώδικα

- **Απειλή περιουσιακών στοιχείων δεδομένων**: Χρήση ψεύτικης ταυτότητας χρήστη από «εσωτερικές» ή «εξωτερικές» οντότητες (Masquerade Attack)

Περιουσιακό Στοιχείο	Επίπτωση	Απειλή	Ευπάθεια
Προσωπικά δεδομένα υπαλλήλων/ασθενών	Αποκάλυψη	Πολύ υψηλή	Μέτρια
Ιατρικά δεδομένα/Αποτελέσματα εξετάσεων	Αποκάλυψη ή/και Μεταβολή	Πολύ υψηλή	Μέτρια
Διαγνώσεις/Συνοδευτικές εκθέσεις	Αποκάλυψη ή/και Μεταβολή	Υψηλή	Μέτρια
Διοικητικά δεδομένα	Αποκάλυψη	Μέτρια	Υψηλή
Οικονομικά/Εφοδιαστικά Δεδομένα	Αποκάλυψη	Μέτρια	Υψηλή

Δεδομένα συστήματος (π.χ. αντίγραφα ασφαλείας)	Απώλεια δεδομένων	Μέτρια	Μέτρια

Πίνακας 7 - Απειλή περιουσιακών στοιχείων δεδομένων: Χρήση ψεύτικης ταυτότητας χρήστη από «εσωτερικές» ή «εξωτερικές» οντότητες (Masquerade Attack)

2.4. Υπολογισμός επικινδυνότητας

Επόμενο βήμα είναι η αποτίμηση της επικινδυνότητας για κάθε συνδυασμό Περιουσιακού Στοιχείου-Απειλής-Ευπάθειας. Σκοπός αυτής της διαδικασίας είναι η εξαγωγή ενός βαθμού, ο οποίος αντιστοιχεί στην αξία κάθε απειλής για τον οργανισμό, χωρίς όμως να συνυπολογίζει τυχόν αντίμετρα που ήδη εφαρμόζονται και ενδεχομένως να αντιμετωπίζουν την απειλή αυτή. Ο υπολογισμός του βαθμού επικινδυνότητας μέσω της μεθόδου CRAMM ακολουθεί μία κλίμακα από 1 έως 7, όπως φαίνεται στον παρακάτω πίνακα:

Threats		VL	VL	VL	L	L	L	M	M	M	H	H	H	VH	VH	VH
Vuln.		L	M	H	L	M	H	L	M	H	L	M	H	L	M	H
Assets/Value	1	1	1	1	1	1	1	1	1	2	1	2	2	2	2	3
	2	1	1	2	1	2	2	2	2	3	2	3	3	3	3	4
	3	1	2	2	2	2	2	2	3	3	3	3	4	3	4	4
	4	2	2	3	2	3	3	3	3	4	3	4	4	3	4	4
	5	2	3	3	3	3	4	3	4	4	4	4	4	4	4	5
	6	3	3	4	3	4	4	4	4	5	4	5	5	5	5	6
	7	3	4	4	4	4	5	4	5	5	5	5	6	5	6	6
	8	4	4	5	4	5	5	5	5	6	5	6	6	6	6	7
	9	4	5	5	5	5	6	5	6	6	6	6	7	6	7	7
	10	5	5	6	5	6	6	6	6	6	6	7	7	7	7	7

Πίνακας 8 - Πίνακας υπολογισμού επικινδυνότητας CRAMM (El Fray, 2012)

VL – Very Low	Πολύ Χαμηλό
L – Low	Χαμηλό
M – Medium	Μέτριο
H – High	Υψηλό
VH – Very High	Πολύ Υψηλό

Πίνακας 9 - Υπόμνημα πίνακα υπολογισμού κινδύνου CRAMM

Παρακάτω, ακολουθεί ο υπολογισμός επικινδυνότητας των ίδιων ενδεικτικών απειλών που επιλέχθηκαν προς αποτίμηση στο προηγούμενο στάδιο ενώ, στο αρχείο «Risk_Assessment.xlsx» εμπεριέχεται λεπτομερής λίστα εκτίμησης των κινδύνων που αφορούν τα περιουσιακά στοιχεία του διαγνωστικού κέντρου.

- **Υπολογισμός βαθμού επικινδυνότητας απειλής «Τεχνική βλάβη των υπηρεσιών δικτύου»**

Περιουσιακό Στοιχείο	Επίπτωση	Απειλή	Ευπάθεια	Β.Ε.
Διακομιστής «LDAP»	Μη-διαθεσιμότητα	Υψηλή	Υψηλή	6
Τείχος προστασίας	Μη-διαθεσιμότητα	Υψηλή	Υψηλή	5
Διαδικτυακός εξοπλισμός	Σφάλμα μετάδοσης δεδομένων	Υψηλή	Υψηλή	3
Ιατρικά μηχανήματα	Σφάλμα μετάδοσης δεδομένων	Υψηλή	Υψηλή	7
Μέσα αντιγράφων ασφαλείας	Σφάλμα μετάδοσης δεδομένων	Μέτρια	Μέτρια	4
Ηλεκτρονικοί υπολογιστές	Σφάλμα μετάδοσης δεδομένων	Πολύ χαμηλή	Χαμηλή	2
Εκτυπωτές	Σφάλμα μετάδοσης δεδομένων	Πολύ χαμηλή	Χαμηλή	2
Τηλέφωνα «IP»	Μη-διαθεσιμότητα	Χαμηλή	Υψηλή	2

Πίνακας 10 - Υπολογισμός βαθμού επικινδυνότητας απειλής «Τεχνική βλάβη των υπηρεσιών δικτύου»

- **Υπολογισμός βαθμού επικινδυνότητας απειλής «Εκτέλεση κακόβουλου κώδικα»**

Περιουσιακό Στοιχείο	Επίπτωση	Απειλή	Ευπάθεια	Β.Ε.
Λειτουργικό σύστημα	Μη διαθεσιμότητα ή/και Απώλεια δεδομένων	Μέτρια	Μέτρια	2
Λογισμικό σύνδεσης με τις υπηρεσίες «Cloud»	Μη-διαθεσιμότητα ή/και Σφάλμα μετάδοσης δεδομένων ή/και Αποκάλυψη	Υψηλή	Μέτρια	5
Λογισμικό ιατρικών αρχείων	Απώλεια δεδομένων ή/και Μεταβολή ή/και Αποκάλυψη	Πολύ υψηλή	Υψηλή	4

Λογισμικό δημιουργίας αρχείων καταγραφής	Απώλεια δεδομένων ή/και Μεταβολή	Μέτρια	Υψηλή	4
Λογισμικό διαχείρισης βάσεων δεδομένων	Απώλεια δεδομένων ή/και Μεταβολή ή/και Αποκάλυψη	Υψηλή	Υψηλή	4

Πίνακας 11 - Υπολογισμός βαθμού επικινδυνότητας απειλής «Εκτέλεση κακόβουλου κώδικα»

- **Υπολογισμός βαθμού επικινδυνότητας απειλής «Χρήση ψεύτικης ταυτότητας χρήστη από εσωτερικές ή εξωτερικές οντότητες (Masquerade Attack)»**

Περιουσιακό Στοιχείο	Επίπτωση	Απειλή	Ευπάθεια	Β.Ε.
Προσωπικά δεδομένα υπαλλήλων/ασθενών	Αποκάλυψη	Πολύ υψηλή	Μέτρια	6
Ιατρικά δεδομένα/Αποτελέσματα εξετάσεων	Αποκάλυψη ή/και Μεταβολή	Πολύ υψηλή	Μέτρια	7
Διαγνώσεις/Συνοδευτικές εκθέσεις	Αποκάλυψη ή/και Μεταβολή	Υψηλή	Μέτρια	6
Διοικητικά δεδομένα	Αποκάλυψη	Μέτρια	Υψηλή	6
Οικονομικά/Εφοδιαστικά Δεδομένα	Αποκάλυψη	Μέτρια	Υψηλή	5
Δεδομένα συστήματος (π.χ. αντίγραφα ασφαλείας)	Απώλεια δεδομένων	Μέτρια	Μέτρια	4

Πίνακας 12 - Υπολογισμός βαθμού επικινδυνότητας απειλής «Χρήση ψεύτικης ταυτότητας χρήστη από εσωτερικές ή εξωτερικές οντότητες (Masquerade Attack)»

3. Διαχείριση επικινδυνότητας

Στο τελευταίο στάδιο την μεθόδου CRAMM συναντάται η διαχείριση επικινδυνότητας, η οποία αποτελείται από τον προσδιορισμό των προτεινόμενων αντιμέτρων που, σε συνδυασμό με το σχέδιο πολιτικών ασφαλείας, συντελούν το σχέδιο ασφαλείας του διαγνωστικού κέντρου. Σκοπός του παρόντος σταδίου είναι ο καθορισμός λύσεων μετριασμού των επιπτώσεων, χαρακτηριζόμενες από όσο το δυνατόν χαμηλότερο κόστος και λιγότερες απώλειες αναφορικά με το πληροφοριακό σύστημα.

Στο αρχείο «Risk_Assessment.xls» περιέχεται μια λεπτομερής λίστα που περιλαμβάνει εκτενέστερες πληροφορίες του σταδίου «2.4. Υπολογισμός επικινδυνότητας», όπως αναφέρθηκε και στο ίδιο το στάδιο (βλ. σελίδα 16), καθώς επίσης και τα παρακάτω γενικευμένα είδη απειλών με τα αντίστοιχα προτεινόμενα αντίμετρα τους.

Πιθανές απειλές	**Προτεινόμενα αντίμετρα**
Απειλή από σεισμό	Καμία δράση
Εκδήλωση πυρκαγιάς στις εγκαταστάσεις του διαγνωστικού κέντρου	Σύστημα ανίχνευσης πυρκαγιάς – πυρόσβεσης / Τήρηση κανόνων ασφαλείας από το προσωπικό
Διαρροή υδάτων λόγω κακής κατασκευής του δικτύου ή παλαιότητας των σωληνώσεων	Τεχνικός έλεγχος του χώρου εγκατάστασης του εκάστοτε συστήματος
Αδυναμία ηλεκτροδότησης	Τεχνικός έλεγχος του χώρου εγκατάστασης του εκάστοτε συστήματος και προώθηση του αποτελέσματος στην αρμόδια αρχή
Παρεμβολή στις διαδικασίες μετάδοσης πληροφορίας και προσωπικών δεδομένων	Εφαρμογή του νομικού πλαισίου που διέπει τη μετάδοση πληροφορίας και την τήρηση αρχείων προσωπικών και ιατρικών δεδομένων
Τροποποίηση, υποκλοπή ή καταστροφή πληροφοριών	Κρυπτογράφηση μεταδιδόμενων πληροφοριών / Καθημερινή δημιουργία αντιγράφων ασφαλείας των δεδομένων
Παραποίηση ή κοινοποίηση περιεχομένου απόρρητων βάσεων δεδομένων	Έλεγχος πρόσβασης χρηστών υπολογιστικών συστημάτων με βάση ρόλους και αρμοδιότητες

Εξασφάλιση πρόσβασης σε κακόβουλους χρήστες	Λογισμικά προστασίας από διαδικτυακές απειλές (Anti-Virus, Anti-Malware, Anti-Spyware κτλ.)
Δολιοφθορά από δυσαρεστημένους υπαλλήλους	Έλεγχος πρόσβασης υπαλλήλων σε υλικό, λογισμικό και χώρους εργασίας με βάση ρόλους και αρμοδιότητες
Χρήση τεχνολογιών αβέβαιου μέλλοντος (πιθανόν να καταστούν μη λειτουργικές ή παρωχημένες)	Προσεκτική και τεκμηριωμένη επιλογή του επιπέδου τεχνολογίας που θα χρησιμοποιηθεί
Αδυναμία σύνδεσης όλων των μερών του πληροφοριακού συστήματος	Τροποποίηση του αρχικού σχεδιασμού ώστε να προβλέπεται η δυνατότητα συνδεσιμότητας του συνόλου των τμημάτων του έργου
Ασυμβατότητα υπάρχοντος εξοπλισμού με εγκαθιστάμενο σύστημα νεότερης τεχνολογίας	Τροποποίηση του αρχικού σχεδιασμού ώστε να προβλέπεται η δυνατότητα συνδεσιμότητας του συνόλου των τμημάτων του έργου
Εγκατάσταση ελαττωματικού εξοπλισμού	Πρόβλεψη δυνατότητας άμεσης αντικατάστασης ελαττωματικού εξοπλισμού / Πρόβλεψη καθυστερήσεων αντικατάστασης ελαττωματικού εξοπλισμού στον αρχικό σχεδιασμό
Αδυναμία χρήσης συστημάτων λόγω έλλειψης εκπαιδευμένου προσωπικού	Εκπαίδευση του προσωπικού του διαγνωστικού κέντρου που θα χειρίζεται το εκάστοτε σύστημα
Καταστροφή περιουσιακών στοιχείων υλικού ή λογισμικού λόγω κακής χρήσης	Εκπαίδευση του προσωπικού του διαγνωστικού κέντρου που θα χειρίζεται το εκάστοτε σύστημα / Έλεγχος πρόσβασης υπαλλήλων σε ευπαθείς χώρους εργασίας με βάση ρόλους και αρμοδιότητες, όπου τυχόν αποκατάσταση ζημίας, απαιτεί ένα υψηλό κόστος
Λανθασμένη εγκατάσταση περιουσιακού στοιχείου υλικού ή λογισμικού εξαιτίας έλλειψης τεχνικών γνώσεων ή ανθρώπινου λάθους	Επικύρωση των γνώσεων του προσωπικού της υπεύθυνης, για την εγκατάσταση, εταιρίας

Πίνακας 13 - Αντιστοίχιση πιθανών απειλών με τα προτεινόμενα αντίμετρά τους

4. Δήλωση Εφαρμογής (Statement of Applicability – SOA)

Παράλληλα με τη διαδικασίας ανάλυσης και διαχείρισης επικινδυνότητας, διενεργείται και η συγγραφή της Δήλωσης Εφαρμογής. Πρώτο βήμα για την διεκπεραίωση της συγγραφής, αφού έχει ολοκληρωθεί το στάδιο της καταγραφής των περιουσιακών στοιχείων και η εκτίμηση των ευπαθειών του πληροφοριακού συστήματος, είναι η πρόταση των κατάλληλων αντιμέτρων (σε σύγκριση με τα ήδη εφαρμοσμένα) ενώ ταυτόχρονα, αποκλείονται τα μέτρα που δεν αποσκοπούν στη λειτουργία του συστήματος. Η διαδικασία αυτή ονομάζεται «Ανάλυση Απόστασης» (Gap Analysis) και περιγράφεται παρακάτω.

4.1. Gap Analysis

Η ανάλυση των μέτρων ασφαλείας που εφαρμόζονται ήδη πραγματώθηκε σύμφωνα με τους «ελέγχους» (Controls) που εμπεριέχονται στο «Παράρτημα Α» του προτύπου ISO/IEC 27001:2013.

Όπως επισημάνθηκε στις συνεντεύξεις που πραγματοποιήθηκαν κατά την επίσκεψη στις εγκαταστάσεις του Διαγνωστικού Κέντρου, πρόκειται για έναν νεοσύστατο οργανισμό, κάτι που συνεπάγεται με ένα ελλιπές, όσον αφορά στην ασφάλεια, πληροφοριακό σύστημα. Πιο συγκεκριμένα, οι μηχανισμοί ασφαλείας που εφαρμόζονται ήδη από το Διαγνωστικό Κέντρο είναι οι εξής:

- **A.11** - Φυσική και περιβαλλοντική ασφάλεια (Εκτός των A.11.1.5 και A.11.2.6)
- **A.15** - Σχέσεις με προμηθευτές
- **A.17** - Πτυχές της ασφάλειας πληροφοριών στη διαχείριση της επιχειρησιακής συνέχειας

Για το ολοκληρωμένο πλάνο ασφαλείας της επιχείρησης, κρίθηκαν απαραίτητοι προς υλοποίηση οι παρακάτω έλεγχοι:

- **A.5** - Πολιτικές για την ασφάλεια πληροφοριών
- **A.6** - Οργάνωση της ασφάλειας πληροφοριών (Εκτός των A.6.1.4 και A.6.2.2)
- **A.7** - Ασφάλεια ανθρωπίνου δυναμικού
- **A.8** - Διαχείριση παγίων
- **A.9** - Έλεγχος πρόσβασης

- **A.10** - Κρυπτογράφηση
- **A.12** - Ασφάλεια λειτουργιών (Εκτός του A.12.1.4)
- **A.13** - Ασφάλεια επικοινωνιών
- **A.14** - Απόκτηση, ανάπτυξη και συντήρηση συστήματος (Εκτός των A.14.2 και A.14.3)
- **A.16** - Διαχείριση περιστατικών στην ασφάλεια πληροφοριών
- **A.18** – Συμμόρφωση (Εκτός του A.18.1.5)

Τέλος, οι έλεγχοι που δε θα εφαρμοστούν στο παρόν πληροφοριακό σύστημα είναι οι εξής:

- **A.6.1.4** - Επαφές με ομάδες ειδικού ενδιαφέροντος

Ο λόγος που εξαιρείται αυτός ο έλεγχος είναι: Δεν υφίστανται επαφές με ομάδες ειδικού ενδιαφέροντος.

- **A.6.2.2** – Τηλεργασία

Ο λόγος που εξαιρείται αυτός ο έλεγχος είναι: Η επιχείρηση δραστηριοποιείται μόνο δια ζώσης.

- **A.11.1.5** - Εργασία σε ασφαλείς τομείς

Ο λόγος που εξαιρείται αυτός ο έλεγχος είναι: Δεν υπάρχει πρόβλεψη για εργασία σε ασφαλείς τομείς.

- **A.11.2.6** - Ασφάλεια εξοπλισμού και παγίων εκτός εγκαταστάσεων

Ο λόγος που εξαιρείται αυτός ο έλεγχος είναι: Δεν προβλέπεται εργασία εκτός της δομής του Διαγνωστικού Κέντρου.

- **A.12.1.4** - Διαχωρισμός περιβάλλοντος ανάπτυξης, δοκιμών και λειτουργικού περιβάλλοντος

Ο λόγος που εξαιρείται αυτός ο έλεγχος είναι: Δεν εφαρμόζονται περιβάλλοντα ανάπτυξης και δοκιμών στις δραστηριότητες του Διαγνωστικού Κέντρου.

- **A.14.2** - Ασφάλεια στις διαδικασίες ανάπτυξης και υποστήριξης

  Ο λόγος που εξαιρείται αυτός ο έλεγχος είναι: Δεν εφαρμόζεται στις δραστηριότητες και την υποδομή του Διαγνωστικού Κέντρου.

- **A.14.3** - Δεδομένα δοκιμών

  Ο λόγος που εξαιρείται αυτός ο έλεγχος είναι: Δεν εφαρμόζεται στις δραστηριότητες και την υποδομή του Διαγνωστικού Κέντρου.

- **A.18.1.5** - Κανονισμός κρυπτογραφικών ελέγχων
  Ο λόγος που εξαιρείται αυτός ο έλεγχος είναι: Δεν υφίσταται νομοθεσία ή κανονισμός που να επιβάλλει την κρυπτογράφηση των δεδομένων του Διαγνωστικού κέντρου. Ωστόσο, το Διαγνωστικό Κέντρο, για λόγους ασφαλείας, εφαρμόζει πολιτική κρυπτογράφησης των περιουσιακών στοιχείων που θεωρεί κρίσιμα, όπως προσωπικά και ιατρικά δεδομένα.

4.2. Συγγραφή της Δήλωσης

Αφού διεκπεραιώθηκε το στάδιο της Ανάλυσης Απόστασης, ακολουθεί η συγγραφή της Δήλωσης Εφαρμογής. Για τις ανάγκες εξοικονόμησης χώρου, δεν θα συμπεριληφθεί στο παρόν έγγραφο, αλλά σε ένα ανεξάρτητο αρχείο με όνομα «Statement_of_Applicability.xlsx». Στο αρχείο αυτό, αναλύονται όλοι οι έλεγχοι, οι λόγοι επιλογής ή εξαίρεσής τους και η περιγραφή της υλοποίησής τους.

5. Πολιτική Ασφαλείας

Στο παρόν κεφάλαιο επιλέγεται προς ανάλυση μία εκ των πολιτικών ασφαλείας πληροφοριών που παρουσιάζονται στο έγγραφο «Information_Security_Policy.docx». Εν γένει, το σύνολο των πολιτικών αυτών ωφελεί τις οντότητες καθορίζοντας ένα πλαίσιο που θα διασφαλίζει την εφαρμογή κατάλληλων μέτρων για την προστασία της εμπιστευτικότητας, της ακεραιότητας και της διαθεσιμότητας των δεδομένων και εγγυάται πως το προσωπικό κατανοεί το ρόλο και τις ευθύνες τους, έχει επαρκή γνώση της πολιτικής ασφάλειας, των διαδικασιών και των πρακτικών και να γνωρίζει πώς να προστατεύει τις πληροφορίες που διαχειρίζεται.

Παρακάτω πραγματοποιείται ανάλυση της πολιτικής ασφαλείας υπ' αριθμόν 7 «Διαχείριση περιστατικού κυβερνοασφάλειας».

5.1. Σκοπός

Σκοπός της πολιτικής «Διαχείριση περιστατικού κυβερνοασφάλειας» είναι η παροχή ενός πλαισίου διασφάλισης ότι πιθανά περιστατικά κυβερνοασφάλειας αντιμετωπίζονται με αποτελεσματικό και συνεπή τρόπο. Επίσης, καθορίζει τους ρόλους και τις ευθύνες των συμμετεχόντων, οι οποίοι έπειτα από την ολοκλήρωση της διαδικασίας εκπαίδευσης που αναφέρεται στην πολιτική υπ' αριθμόν 6 «Ασφάλεια Προσωπικού» του εγγράφου πολιτικής ασφαλείας, καθίστανται υπεύθυνοι για την υλοποίηση των μέτρων αντιμετώπισης περιστατικών ασφάλειας πληροφοριών στο Διαγνωστικό Κέντρο.

5.2. Πεδίο Εφαρμογής

Η εν λόγω πολιτική, καθώς και όλες οι πολιτικές που αναφέρονται στο παρόν κεφάλαιο, ισχύουν για όλες τις οντότητες που χρησιμοποιούν, έχουν πρόσβαση ή μεταχειρίζονται με έτερο τρόπο, τοπικά ή απομακρυσμένα, τους πόρους πληροφορικής του Διαγνωστικού Κέντρου.

5.3. Ρόλοι και Ευθύνες

- Οι οντότητες πρέπει να διαθέτουν σχέδιο αντιμετώπισης συμβάντων και συνεπή πρότυπα για την αποτελεσματική αντιμετώπιση περιστατικών που θέτουν σε κίνδυνο την ασφάλεια των πληροφοριών και των συστημάτων.

- Όλα τα παρατηρούμενα ή εικαζόμενα συμβάντα ή αδυναμίες που αφορούν την ασφάλεια των πληροφοριών πρέπει να αναφέρονται στον Υπεύθυνο Συστήματος Ασφάλειας Πληροφοριών το συντομότερο δυνατόν

5.4. Ορισμοί

- **Συμβάν:** Ένα συμβάν είναι ένα περιστατικό που πραγματικά ή δυνητικά θέτει σε κίνδυνο την εμπιστευτικότητα, την ακεραιότητα ή τη διαθεσιμότητα ενός συστήματος πληροφοριών ή των πληροφοριών που επεξεργάζεται, αποθηκεύει ή μεταδίδει (Fordham University, n.d.).
- **Πόροι Πληροφορικής:** Οι Πόροι Πληροφορικής περιλαμβάνουν συστήματα υπολογιστών, δικτύωσης, επικοινωνιών, εφαρμογών και τηλεπικοινωνιών, υποδομή, υλικό, λογισμικό, δεδομένα, βάσεις δεδομένων, προσωπικό, διαδικασίες και φυσικές εγκαταστάσεις (Fordham University, n.d.).

5.5. Επιμέλεια

Η διοίκηση του Διαγνωστικού Κέντρου είναι υπεύθυνη για την εφαρμογή, επιμέλεια και αναθεώρηση της παρούσας πολιτικής.

5.6. Πολιτικές με άμεση σχέση

Η παρούσα πολιτική εξαρτάται άμεσα με τις διαδικασίες εκπαίδευσης που αναφέρονται στην πολιτική υπ' αριθμόν 6 «Ασφάλεια Προσωπικού» του εγγράφου πολιτικής ασφαλείας του Διαγνωστικού Κέντρου.

5.7. Συμμόρφωση

Η μη συμμόρφωση με την εν λόγω πολιτική μπορεί να οδηγήσει σε πειθαρχικά μέτρα για τους υπαλλήλους, μέχρι και τον τερματισμό της σύμβασης εργασίας.

5.8. Ιστορικό αναθεωρήσεων

Έκδοση	Ημερομηνία Τροποποίησης	Περιγραφή
1.0	10 Ιανουαρίου 2023	Αρχική Έκδοση σύμφωνα με απαιτήσεις ISO/IEC 27001:2013

Πίνακας 14 - Ιστορικό αναθεωρήσεων πολιτικής Διαχείρισης περιστατικού κυβερνοασφάλειας

6. Συμπεράσματα

Στα παραπάνω κεφάλαια παρουσιάστηκαν τα βήματα προς την υλοποίηση μιας ολοκληρωμένης πρότασης σχεδίου ασφαλείας ενός διαγνωστικού κέντρου που επεξεργάζεται και διατηρεί προσωπικά και ευαίσθητα προσωπικά δεδομένα προσωπικού και ασθενών.

Προτού ξεκινήσει η διαδικασία, βασική προϋπόθεση ήταν η άντληση πληροφοριών σχετικά με τα αντικείμενα που εμπλέκονταν άμεσα με το σχέδιο ασφαλείας. Αφού προηγήθηκε η επιθεώρηση του χώρου εργασίας, καταγράφηκαν τα περιουσιακά στοιχεία και η δομή των συστημάτων της επιχείρησης. Αμέσως μετά, το αρμόδιο προσωπικό κλήθηκε σε μία σειρά συνεντεύξεων με σκοπό τον καθορισμό του πεδίου εφαρμογής και των στόχων του συστήματος ασφάλειας πληροφοριών, όπως και των πιθανών κινδύνων που απειλούν το διαγνωστικό κέντρο.

Η μεθοδολογία ανάλυσης κινδύνων, στην οποία βασίστηκε η διεκπεραίωση του σχεδίου, αξιοποιεί τα κύρια χαρακτηριστικά της «CRAMM» και αποτελείται από την αναγνώριση των περιουσιακών στοιχείων, των απειλών και των ευπαθειών του πληροφοριακού συστήματος. Προϊόν αυτής της ανάλυσης ήταν ο εντοπισμός των πιο επιζήμιων απειλών και η πρόταση αντιμέτρων, προκειμένου να μετριαστούν οι ευπάθειες, επιδιώκοντας την ομαλή λειτουργία των συστημάτων και κατ' επέκταση, του διαγνωστικού κέντρου.

Στη συνέχεια, για τις ανάγκες συγγραφής της Δήλωσης Εφαρμογής πραγματοποιήθηκε σύγκριση των μέτρων που απαιτείται να εφαρμοστούν στο πληροφοριακό σύστημα, με τα μέτρα που ήδη βρίσκονταν σε εφαρμογή. Έπειτα, σειρά είχε η σύνταξη της Δήλωσης με γνώμονα τους «ελέγχους» που συμπεριλαμβάνονται στο «Παράρτημα Α» (Annex A) του προτύπου ISO/IEC 27001:2013.

Τέλος, με την σύνταξη του εγγράφου πολιτικών ασφαλείας του πληροφοριακού συστήματος ολοκληρώθηκε η διαδικασία υλοποίησης του σχεδίου ασφαλείας του διαγνωστικού κέντρου.

Από όλα τα παραπάνω γίνεται εύκολα αντιληπτό πως λόγω της πολυπλοκότητας των πληροφοριακών συστημάτων, η διαδικασία ανάλυσης κινδύνων είναι μια ακολουθία ενεργειών καίριας σημασίας για μια ολοκληρωμένη πρόταση σχεδίου ασφαλείας, που πρέπει να εφαρμόζονται παράλληλα σε όλα τα στάδια σχεδιασμού και ανάπτυξης πληροφοριακών συστημάτων.

Παράρτημα

1. Βιβλιογραφικές Αναφορές

El Fray, I. (2012). A Comparative Study of Risk Assessment Methods, MEHARI & CRAMM with a New Formal Model of Risk Assessment (FoMRA) in Information Systems. Computer Information Systems and Industrial Management, pp.428–442. doi:10.1007/978-3-642-33260-9_37.

Fordham University (n.d.). Information Security Incident Response Policy | Fordham. [online] Available at: https://www.fordham.edu/information-technology/it-security--assurance/it-policies-procedures-and-guidelines/information-security-incident-response-policy/ [Accessed 10 Jan. 2023].

2. Κατάλογος Πινάκων