ΕΘΝΙΚΗ ΣΧΟΛΗ ΔΗΜΟΣΙΑΣ ΔΙΟΙΚΗΣΗΣ

ΚΑΙ ΑΥΤΟΔΙΟΙΚΗΣΗΣ

ΚΖ΄ ΕΚΠΑΙΔΕΥΤΙΚΗ ΣΕΙΡΑ

ΤΕΛΙΚΗ ΕΡΓΑΣΙΑ

ΤΙΤΛΟΣ

ΣΥΓΧΡΟΝΕΣ ΑΠΕΙΛΕΣ ΚΑΤΑ ΤΗΣ ΑΣΦΑΛΕΙΑΣ ΚΑΙ ΠΡΟΣΤΑΣΙΑΣ ΤΗΣ ΙΔΙΩΤΙΚΟΤΗΤΑΣ ΣΤΟ ΧΩΡΟ ΤΗΣ ΥΓΕΙΑΣ

ΤΜΗΜΑ ΕΞΕΙΔΙΚΕΥΣΗΣ: ΔΙΟΙΚΗΣΗΣ ΥΠΗΡΕΣΙΩΝ ΥΓΕΙΑΣ

Επιβλέπων: Κωνσταντίνος Ράντος

Σπουδαστής: Λουκάς Τσικλητάρης

ΑΘΗΝΑ – 2022

ΕΘΝΙΚΗ ΣΧΟΛΗ ΔΗΜΟΣΙΑΣ ΔΙΟΙΚΗΣΗΣ
ΚΑΙ ΑΥΤΟΔΙΟΙΚΗΣΗΣ

ΚΖ΄ ΕΚΠΑΙΔΕΥΤΙΚΗ ΣΕΙΡΑ

ΤΕΛΙΚΗ ΕΡΓΑΣΙΑ

ΣΥΓΧΡΟΝΕΣ ΑΠΕΙΛΕΣ ΚΑΤΑ ΤΗΣ ΑΣΦΑΛΕΙΑΣ ΚΑΙ ΠΡΟΣΤΑΣΙΑΣ ΤΗΣ ΙΔΙΩΤΙΚΟΤΗΤΑΣ ΣΤΟ ΧΩΡΟ ΤΗΣ ΥΓΕΙΑΣ

Επιβλέπων:
Κωνσταντίνος Ράντος

Σπουδαστής:
Λουκάς Τσικλητάρης

ΑΘΗΝΑ – 2022

Δήλωση

«Δηλώνω ρητά ότι η παρούσα εργασία αποτελεί αποκλειστικά προϊόν προσωπικής εργασίας, δεν παραβιάζει καθ' οιονδήποτε τρόπο πνευματικά δικαιώματα τρίτων και δεν είναι προϊόν μερικής ή ολικής αντιγραφής».

Αθήνα, 19/05/2022

Υπογραφή

Λουκάς Τσικλητάρης

ΠΕΡΙΛΗΨΗ

Η παρούσα μελέτη πραγματεύεται το επίμαχο ζήτημα του προσδιορισμού των σύγχρονων απειλών κατά της ασφάλειας και της προστασίας της ιδιωτικότητας στο χώρο της υγείας. Η καταγραφή τους, καθώς και η αποτύπωση της αντιμετώπισής τους, συμβάλλουν αφενός στην ανάπτυξη μιας ολοκληρωμένης πολιτικής κυβερνοασφάλειας για τους φορείς παροχής υπηρεσιών υγείας, αφετέρου στην εξαγωγή κρίσιμων σχετικών συμπερασμάτων, που μπορούν να αξιοποιηθούν στο πλαίσιο του ελληνικού συστήματος υγείας (ΕΣΥ, ιδιωτικός τομέας) και της Δημόσιας Διοίκησης γενικότερα. Για την έρευνα πάνω στο θέμα χρησιμοποιήθηκαν δύο επιστημονικές μέθοδοι: Πρώτον, η βιβλιογραφική έρευνα και ανασκόπηση της εγχώριας και διεθνούς βιβλιογραφίας για το τι υπάρχει στο πεδίο των κυβερνοαπειλών στα συστήματα υγείας. Δεύτερον, η διεξαγωγή συνεντεύξεων μέσω ερωτηματολογίων ανοιχτού τύπου για την παροχή απόψεων και ποιοτικών στοιχείων από παράγοντες του ελληνικού συστήματος υγείας, ώστε να γίνει μία συνοπτική αποτίμηση της κατάστασης επιπέδων κυβερνοασφάλειας και του βαθμού της νομικής του συμμόρφωσης στην ισχύουσα νομοθεσία, με κυρίαρχο τον ΓΚΠΔ.

Στην εποχή εξάρτησης των συστημάτων υγείας από τις ΤΠΕ, οι σύγχρονες απειλές του κυβερνοχώρου μπορούν να οδηγήσουν στην παραβίαση τόσο της ασφάλειας της λειτουργίας τους, όσο και των ιατρικών δεδομένων (ιδιωτικότητας) στον Ηλεκτρονικό Φάκελο Υγείας των ασθενών. Οι συνέπειές τους κυμαίνονται σε ένα φάσμα, από οικονομικά επιβλαβείς, μέχρι ολέθριες με τη διακινδύνευση της ζωής των ασθενών, ακόμη και τον θάνατο. Μεταξύ άλλων, το ξέσπασμα της πανδημίας COVID-19 συμβαδίζει με την εκρηκτική αύξηση της συχνότητας και της πολυπλοκότητάς τους. Ωστόσο, για την επιτυχή αντιμετώπισή τους υπάρχει η κατάλληλη πολιτική ασφαλείας. Το ελληνικό σύστημα υγείας παρουσιάζει μεν ικανοποιητικά επίπεδα ασφαλείας των πληροφοριακών του συστημάτων, όπως επίσης επαρκή βαθμό νομικής συμμόρφωσης, αλλά υφίστανται ακόμη αρκετά περιθώρια βελτίωσης, που αφορούν κυρίως τα οργανωτικά μέτρα.

ΛΕΞΕΙΣ-ΚΛΕΙΔΙΑ: κυβερνοαπειλές–κυβερνοεπιθέσεις στα συστήματα υγείας, κυβερνοασφάλεια και προστασία ιατρικών δεδομένων, Ηλεκτρονικός Φάκελος Υγείας, ΕΣΥ, ΓΚΠΔ, πανδημία του κορωνοϊού (COVID-19).

ABSTRACT

The present study addresses the controversial issue of identifying contemporary threats to safety and privacy in the field of health. Their recording and the depiction of their tackling contributes, on the one hand, to the development of a complete cybersecurity policy for the health care providers, on the other, to the finding of relevant important conclusions, which can be used in the context of the Greek Health System (ESY, private sector) and the Public Administration in general. For the research on this topic two scientific methods were used: Firstly, the literature research and review in the domestic and international literature on what exists in the field of cyber threats in healthcare systems. Secondly, by conducting interviews through open-ended questionnaires, referring to officers in the Greek Health System, so as to provide opinions and quality data and to make a brief evaluation of the state of its cybersecurity levels and the degree of its legal compliance to current legislation, with GDPR as predominant.

In the age of healthcare systems dependence on ICT, modern cyber threats can lead to the violation of both the security of its operation and medical data (privacy) in the Electronic Health Record of patients. Their consequences range from costly to catastrophic, the risk of patients' lives, or even the cause of death. Amongst others, the outbreak of COVID-19 pandemic is accompanied by an explosive increase in their frequency and complexity. However, there is an appropriate security policy to tackle them successfully. The Greek Health System presents satisfactory levels of security of its information systems and a sufficient degree of legal compliance as well, but there is still much room for improvement, mainly concerning organizational measures.

KEYWORDS: cyberthreats-cyberattacks in healthcare systems, cybersecurity and protection of patients' medical-health data, Electronic Health Record, ESY, GDPR, COVID-19 pandemic.

ΠΡΟΛΟΓΟΣ - ΕΥΧΑΡΙΣΤΙΕΣ

Θα ήθελα να ευχαριστήσω προσωπικά τους εξής ανθρώπους, επειδή θεωρώ ότι, χωρίς την κρίσιμη συνεισφορά τους, η παρούσα εργασία δεν θα είχε υλοποιηθεί με την ίδια επιστημονική ορθότητα.

Ευχαριστώ τον επιβλέποντα καθηγητή μου, Κωνσταντίνο Ράντο, για την πρόταση του θέματος, την καθοδήγησή του και την αγαστή συνεργασία μας κατά τη διάρκεια εκπόνησης της εργασίας. Ακόμη, εκφράζω τις ευχαριστίες μου στον Προϊστάμενο της Διεύθυνσης Ηλεκτρονικής Διακυβέρνησης του Υπουργείου Υγείας, Αθανάσιο Κελεπούρη, για τις ιδιαιτέρως χρήσιμες πληροφορίες που μου παρείχε κατόπιν της επικοινωνίας μας, οι οποίες αποτέλεσαν αναπόσπαστο μέρος του υλικού στο οποίο βασίστηκα, όπως και στην Ευαγγελία Σιώζου, Προϊσταμένη του νοσοκομείου «Σωτηρία». Επιπλέον, ήταν πολύτιμη η συνεισφορά του DPO του Υπουργείου Υγείας, Δημητρίου Ζωγραφόπουλου, για τον ίδιο λόγο, καθώς επίσης γιατί μας δίδαξε το αντικείμενο των προσωπικών δεδομένων με τη μέγιστη σαφήνεια και επάρκεια, κάνοντας τους σπουδαστές να εκδηλώσουμε προσωπικό ενδιαφέρον πάνω σ’ αυτό.

Τέλος, ευχαριστώ τον Αντώνιο Κουφάκη, τον Ηλία Βασιλειάδη και τη Βάσια Νικολοπούλου για τις ωφέλιμες συμβουλές τους σχετικά με την επιλογή της κατάλληλης επιστημονικής μεθοδολογίας, τον τρόπο οργάνωσης της εργασίας και τη μεσολάβησή τους, ώστε να αποκτήσω πρόσβαση στις ανωτέρω σημαντικές πληροφορίες.

ΠΙΝΑΚΑΣ ΠΕΡΙΕΧΟΜΕΝΩΝ

ΠΙΝΑΚΑΣ ΣΧΗΜΑΤΩΝ ΚΑΙ ΓΡΑΦΗΜΑΤΩΝ

ΠΙΝΑΚΑΣ ΣΥΝΤΜΗΣΕΩΝ ΚΑΙ ΣΥΝΤΟΜΟΓΡΑΦΙΩΝ

Ελληνικές

ΑΔΑΕ: Αρχή Διασφάλισης Απορρήτου των Επικοινωνιών

ΑΠΔΠΧ: Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα

ΓΕΕΘΑ: Γενικό Επιτελείο Εθνικής Άμυνας

ΓΚΠΔ: Γενικός Κανονισμός Προστασίας Δεδομένων (GDPR)

ΔΙΔΗΕ: Διεύθυνση Δίωξης Ηλεκτρονικού Εγκλήματος

ΕΕ: Ευρωπαϊκή Ένωση

ΕΕΤΤ: Εθνική Επιτροπή Τηλεπικοινωνιών και Ταχυδρομείων

ΕΟΠΥΥ: Εθνικός Οργανισμός Παροχής Υπηρεσιών Υγείας

ΕΣΥ: Εθνικό Σύστημα Υγείας

ΕΥΠ: Εθνική Υπηρεσία Πληροφοριών

(Α) ΗΦΥ: (Ατομικός) Ηλεκτρονικός Φάκελος Υγείας

Ν.: Νόμος

ΝΠΔΔ: Νομικό Πρόσωπο Δημοσίου Δικαίου

ΝΠΙΔ: Νομικό Πρόσωπο Ιδιωτικού Δικαίου

ΠΔ: Προεδρικό Διάταγμα

π.δ: Προσωπικά Δεδομένα

ΠΦΥ: Πρωτοβάθμια Φροντίδα Υγείας

ΤΠΕ: Τεχνολογίες Πληροφορίας και Επικοινωνιών

ΥΑ: Υπουργική Απόφαση

ΥΠΕ: Υγειονομική Περιφέρεια

ΥΨΔ: Υπουργείο Ψηφιακής Διακυβέρνησης

Αγγλικές

CERT: Computer Emergency Response Team

CSIRT: Cybersecurity Incident Response Team

CISO: Chief Information Security Officer

DPO: Data Protection Officer

ENISA: European Union Agency for Cybersecurity

GDPR: General Data Protection Regulation

ISO: International Organization for Standardization

IoT: Internet of Things

LAN: Local Area Network

NHS: National Health System

NIS: Network Information Security

NIST: National Institute of Standards and Technology

1. Εισαγωγή

1.1. Περιγραφή του θέματος της εργασίας και της σημασίας του

Ο 21ος αιώνας έχει χαρακτηριστεί η «εποχή της πληροφορίας», διότι η διείσδυση των ΤΠΕ στην κοινωνικοοικονομική και προσωπική ζωή των ατόμων είναι τεράστια κι αυξάνεται ολοένα συνεχώς. Οι υπολογιστές, το Διαδίκτυο, οι έξυπνες συσκευές, με κυρίαρχα τα έξυπνα κινητά τηλέφωνα (smartphones), και τα πληροφοριακά συστήματα δικτύων και υποδομών έχουν καταστεί αναπόσπαστο τμήμα της καθημερινότητας, επιτελώντας πολλαπλούς σκοπούς σε ατομικό και συλλογικό επίπεδο: οικιακούς, βιομηχανικούς, εμπορικούς, εργασιακούς, εφοδιασμού, συντονισμού, παροχής δημοσίων και ιδιωτικών υπηρεσιών.

Πολλοί οργανισμοί, επιχειρήσεις και προηγμένα κράτη του κόσμου έχουν ήδη προχωρήσει σε μεγάλο βαθμό τον ψηφιακό τους μετασχηματισμό, εξυπηρετώντας τις πάσης φύσεως δραστηριότητές τους, αξιοποιώντας τα πλεονεκτήματα των πληροφοριακών συστημάτων (π.χ. ηλεκτρονική αρχειοθέτηση, e-shops). Όσοι δεν το έχουν πράξει ακόμη, δε, αναμένεται να ακολουθήσουν την ίδια πρακτική, προσαρμοζόμενοι στις ραγδαίες τεχνολογικές εξελίξεις, ώστε να αντλήσουν τα οφέλη της αυξημένης παραγωγικότητας κι αποτελεσματικότητας, της καλύτερης οργάνωσης, καθώς και της εξοικονόμησης χρόνου και κόστους, που αυτές μπορούν να προσφέρουν (Digital Information Statistics, 2022)[1].

Ωστόσο, η υψηλή αυτή τεχνολογική εξάρτηση από τα πληροφοριακά συστήματα, τα δίκτυα επικοινωνιών και εφοδιασμού συνεπάγεται αυτόματα έναν βαθμό κινδύνου, εξαιτίας των σύγχρονων απειλών του κυβερνοχώρου, των λεγόμενων κυβερνοαπειλών (Nepal, 2014). Το πιο σοβαρό είδος κυβερνοαπειλών εντοπίζεται στις κυβερνοεπιθέσεις με κακόβουλο λογισμικό, έννοιες που εξηγούνται διεξοδικά στη συνέχεια. Οι κυβερνοεπιθέσεις μπορούν να πλήξουν ατομικά ή μαζικά τους πολίτες είτε αποσπώντας τους κρίσιμα προσωπικά δεδομένα και πληροφορίες, ούτως ώστε οι επιτιθέμενοι (χάκερ) έπειτα

[1] Οι ψηφιακά μετασχηματισμένοι οργανισμοί προβλέπεται να συνεισφέρουν περισσότερο από το ήμισυ του παγκοσμίου ακαθάριστου εγχώριου προϊόντος (ΑΕΠ) έως το 2023, αντιπροσωπεύοντας το ποσό των 53,3 τρισεκατομμυρίων δολαρίων (IDC, 2020). Το 65% του παγκόσμιου ΑΕΠ προβλέπεται να ψηφιοποιηθεί μέχρι το 2022 (ΔΝΤ, 2020) (Digital Information Statistics, 2022)

να τα χρησιμοποιήσουν για ίδιο όφελος, είτε προκαλώντας εσκεμμένα ζημιές στα ψηφιακά τους συστήματα για την επίτευξη δόλιων αλλότριων σκοπών. Παρόμοιο πλήγμα μπορεί να δεχτούν μεγάλοι οργανισμοί όπως οι επιχειρήσεις, μέχρι οι κτηριακές, ενεργειακές ή δικτυακές υποδομές και εγκαταστάσεις ενός ολόκληρου κράτους. Κατ' αυτόν τον τρόπο, ενδέχεται να προκληθεί δυσλειτουργία, ακόμη και παράλυσή τους, με συνέπεια την ολοκληρωτική αδυναμία παροχής υπηρεσιών απέναντι στο κοινωνικό σύνολο, μία από τις στοιχειώδεις υποχρεώσεις των δημοσίων οργανισμών.

Οι συνέπειες των κυβερνοαπειλών μπορεί να αποβούν ολέθριες, ειδικότερα στο χώρο της υγείας, διότι η ομαλή λειτουργία του είναι πλέον άρρηκτα συνδεδεμένη με εκείνη των πληροφοριακών συστημάτων (Luna, 2015). Με τη λογική αυτή, γίνεται εύκολα κατανοητό ότι οι σύγχρονες απειλές κατά των πληροφοριακών συστημάτων της υγείας, συνιστούν απειλές και κινδύνους εναντίον των συστημάτων υγείας εν γένει. Έχουν άμεσο αντίκτυπο στις εγκαταστάσεις, στα δίκτυα υποδομών, στην εφοδιαστική αλυσίδα, στον εξοπλισμό και στο ανθρώπινο δυναμικό τους. Τελικά, η συνισταμένη των προηγούμενων παραγόντων, που σίγουρα πλήττονται με τον έναν ή τον άλλον τρόπο, επηρεάζει κατευθείαν την υγεία των πολιτών-ασθενών και τα ιατρικά τους δεδομένα, δύο πολύτιμα αγαθά που τα εμπιστεύονται στα συστήματα υγείας.

Παρά την εν λόγω ύψιστη κοινωνική και ανθρωπιστική σπουδαιότητά της, η υγεία είναι ο πιο ευάλωτος χώρος στις κυβερνοαπειλές κι ένας από τους ελκυστικότερους, πιο συχνά βαλλόμενους, από κυβερνοεπιθέσεις διαχρονικά (Perasklis, 2014) & (Luna, 2015). Συνεπώς, η λεπτομερής καταγραφή και προσδιορισμός των σύγχρονων απειλών στην υγεία καθίσταται κυριολεκτικά ζωτικής σημασίας. Είναι η βάση ώστε αργότερα να εξευρεθούν, να σχεδιαστούν και να υλοποιηθούν οι αρμόζουσες πολιτικές, μαζί με τα προληπτικά και κατασταλτικά μέτρα ασφαλείας, που θα τις αποτρέψουν ή, έστω, θα τις αντιμετωπίζουν με το μικρότερο δυνατό κόστος όταν εμφανιστούν.

Η εργασία πραγματεύεται το συγκεκριμένο επίμαχο ζήτημα, εξετάζοντάς το από δύο αλληλοσυνδεόμενες πλευρές. Η πρώτη καταγράφει και διερευνά τις σύγχρονες απειλές κατά της ασφάλειας των πληροφοριακών συστημάτων στην υγεία, αναφέροντας ταυτόχρονα εν συντομία τις πιθανές πραγματικές συνέπειές τους. Η δεύτερη κινείται σε μια προσέγγιση νοηματικής προέκτασης, όμως στοχευμένα κατά της προστασίας της ιδιωτικότητας των ασθενών. Έμφαση δίνεται στις συνηθέστερες και πιο σοβαρές κυβερνοαπει-

λές, που απαντώνται στη διεθνή και εγχώρια βιβλιογραφία, χωρίς αποκλειστικό περιορισμό σε αυτές.

Μάλιστα, η πανδημία του κορωνοϊού, από τις αρχές του 2020 έως σήμερα, επιβεβαιώνει τη διαπίστωση ότι η ένταση, η πολυπλοκότητα και η συχνότητα των κυβερνοεπιθέσεων στα συστήματα υγείας αυξήθηκε με πολύ υψηλούς ρυθμούς, κάτι που αναμένεται να συνεχιστεί, μιας κι αυτές εγκαθιδρύθηκαν μέσα στην πανδημία (Chua, 2021). Για τους λόγους αυτούς, το θέμα κρίνεται εξαιρετικά επίκαιρο και χρήσιμο, περιέχει ουσιώδες πληροφοριακό αντίκρισμα για τη δημόσια διοίκηση και, κυρίως, για τα συστήματα υγείας, όπου εντοπίζεται περαιτέρω πρακτικό όφελος, εκτός του όποιου επιστημονικού ενδιαφέροντος.

1.2. Σκοπός και στόχοι της εργασίας

Πρωτεύον σκοπός της εργασίας είναι η λεπτομερής καταγραφή και προσδιορισμός των σύγχρονων απειλών εναντίον των πληροφοριακών συστημάτων στον τομέα της υγείας. Στη βάση αυτή, εξάγεται ένας γνώμονας για τη μετέπειτα σχεδίαση και εφαρμογή των κατάλληλων πολιτικών ασφαλείας, των απαιτούμενων προληπτικών και κατασταλτικών μέτρων για τη θωράκιση των φορέων παροχής υπηρεσιών υγείας.

Εντασσόμενοι στο πνεύμα συμπλήρωσης του ευρύτερου σκοπού, οι στόχοι είναι ειδικότεροι και επιχειρείται να εκπληρώσουν τα εξής: την αποτύπωση του νομικού πλαισίου που διέπει την κυβερνοασφάλεια και τα ιατρικά δεδομένα των ασθενών, την περιγραφή της αποτελεσματικής πολιτικής ασφαλείας κατά των κυβερνοαπειλών αλλά και των οφελών της, τη συνοπτική αποτίμηση της κατάστασης των επιπέδων ασφαλείας του ελληνικού συστήματος υγείας και του βαθμού νομικής του συμμόρφωσης και τέλος την εξαγωγή σημαντικών συμπερασμάτων, τα οποία μπορούν να αξιοποιηθούν στο πλαίσιο του ΕΣΥ, του ελληνικού συστήματος υγείας και της δημόσιας διοίκησης γενικότερα. Τονίζεται πως η δομή ανάπτυξης του θέματος, η οποία εκτίθεται ακολούθως, εναρμονίζεται με την ανάγκη ικανοποίησης του πρωτεύοντος σκοπού και των επιμέρους στόχων του.

1.3. Μεθοδολογική προσέγγιση

Η μεθοδολογική προσέγγιση που ακολουθήθηκε είναι η βιβλιογραφική έρευνα και ανασκόπηση επικαιροποιημένων και σχετικών με το θέμα πηγών, οι οποίες είναι ελεύθερα διαθέσιμες στο Διαδίκτυο με αναζήτηση, με στόχο την έρευνα των στοιχείων που υπάρχουν στη διεθνή βιβλιογραφία επί του θέματος. Υλικό αντλήθηκε από βάσεις δεδομένων, ακαδημαϊκές εργασίες, επιστημονικές εκθέσεις, εγχειρίδια οδηγιών και καλών πρακτικών των αρμόδιων φορέων, ιστοσελίδες, ηλεκτρονικά περιοδικά και άρθρα του εγχωρίου και διεθνούς Τύπου. Οι πηγές εξετάστηκαν από πλευράς εγκυρότητας κι από επιστημονικής σκοπιάς, παραλείποντας τις όποιες υποκειμενικές κρίσεις.

Πέρα από την προηγούμενη μέθοδο, η οποία παρείχε σαφώς το περισσότερο υλικό, έγινε σύνθεση και ένταξη ποιοτικών στοιχείων και απόψεων, τα οποία αντλήθηκαν από ατομικές συνεντεύξεις, ώστε να συνδεθεί με την ελληνική δημόσια διοίκηση ο τρόπος αντιμετώπισης των απειλών αυτών. Πρόσωπα σε καίριες θέσεις του ελληνικού συστήματος υγείας απάντησαν γραπτώς σε διάφορα σχετικά ερωτήματα, μέσω προσωποποιημένων ερωτηματολογίων ανοιχτού τύπου, συμβάλλοντας έτσι στην εξαγωγή κρίσιμων συμπερασμάτων προς αξιοποίηση στον τομέα της υγείας, το ΕΣΥ και, γενικά, την ελληνική δημόσια διοίκηση.

1.4. Δομή της εργασίας

Αρχικά, παρατίθεται το εισαγωγικό κεφάλαιο, όπου περιγράφεται το θέμα και η σημασία του, αναφέρεται ο γενικός σκοπός και οι ειδικότεροι στόχοι της μελέτης κι έπειτα η επιλεχθείσα ερευνητική μεθοδολογία. Στη συνέχεια, έπεται το δεύτερο κεφάλαιο, όπου εξηγούνται οι βασικοί όροι και οι έννοιες, πάνω στις οποίες αναπτύσσεται το κυρίως θέμα, καθώς και η μεθοδολογική προσέγγιση. Κατόπιν, το τρίτο κεφάλαιο συνεχίζει με την ανάλυση του νομικού πλαισίου που διέπει την κυβερνοασφάλεια, τα δεδομένα υγείας των ασθενών και αναφέρει τους αρμόδιους φορείς που προβλέπονται για τον έλεγχο, την τήρηση και εφαρμογή του.

Στο τέταρτο κεφάλαιο, το οποίο αποτελεί τον κορμό της εργασίας, γίνεται η λεπτομερής καταγραφή και εξήγηση των σημαντικότερων σύγχρονων απειλών κατά της ασφάλειας και της προστασίας της ιδιωτικότητας στο χώρο της υγείας. Εξηγείται πότε θίγεται η

ασφάλεια εξαιτίας μιας απειλής, πότε η ιδιωτικότητα, πότε ενδεχομένως και οι δύο ταυτοχρόνως και ποιες οι επιπτώσεις τους. Στις ανωτέρω κρίσιμες παραμέτρους, δεν θα μπορούσε να μην ενταχθεί ο αντίκτυπος της –ακόμα εν εξελίξει– πανδημίας COVID-19. Στο πέμπτο κεφάλαιο γίνεται μία σύντομη περιγραφή κι αποτίμηση της κατάστασης των επιπέδων ασφαλείας του ελληνικού συστήματος υγείας, όπως επίσης του βαθμού της νομικής του συμμόρφωσης, σύμφωνα με την ισχύουσα νομοθεσία. Τέλος, στο τελικό κεφάλαιο διατυπώνονται οι συμπερασματικές παρατηρήσεις από τη μελέτη, ενώ ο επίλογος κλείνει με ένα γενικό σχολιασμό και διατυπώνει κάποιους προβληματισμούς για το «αύριο» του ελληνικού συστήματος υγείας στο φόντο των κυβερνοαπειλών και των μεταβαλλόμενων εξελίξεων.

2. Βασικές έννοιες και θεωρητική προσέγγιση του θέματος

2.1. Υγεία και συστήματα υγείας

Ο ορισμός της έννοιας της υγείας δεν είναι τόσο απλός, όσο φαίνεται εκ πρώτης. Πολλοί και διάφοροι ορισμοί έχουν χρησιμοποιηθεί κατά καιρούς, ωστόσο ο επικρατέστερος διεθνώς θεωρείται αυτός του ΠΟΥ (ΠΟΥ, 1948), σύμφωνα με τον οποίο «υγεία είναι μία κατάσταση πλήρους σωματικής, πνευματικής και κοινωνικής ευημερίας και όχι μονάχα η απουσία ασθένειας ή και αναπηρίας». Υπό αυτό το πρίσμα, γίνεται σαφές ότι η προστασία και προαγωγή της υγείας των πολιτών, ως του πολυτιμότερου αγαθού, εκ μέρους του κράτους συνιστά διαχρονικά μία από τις πιο δύσκολα υλοποιήσιμες βασικές του υποχρεώσεις –και περισσότερο μάλιστα εν μέσω των διαρκώς μεταβαλλόμενων συνθηκών της σύγχρονης εποχής, όπως οι κοινωνικοοικονομικές, πολιτικές, τεχνολογικές, κλιματολογικές, γεωπολιτικές κλπ. Για την επίτευξη της ανωτέρω θεμελιώδους υποχρέωσης, τα θεσμικά οργανωμένα κοινωνικά κράτη (τα συντεταγμένα δημοκρατικά κράτη) έχουν αναπτύξει, ταυτόχρονα σχεδόν με την ίδρυσή τους, τους θεσμούς των συστημάτων κοινωνικής ασφάλισης και ιδίως της υγείας, προκειμένου να επιβιώσει ο κοινωνικός ιστός, ανεξαρτήτως των όποιων κοινωνικών ανισοτήτων. Όσον αφορά την Ελλάδα, το δικαίωμα στην υγεία κατοχυρώνεται στο Σύνταγμα[2], ως μία από τις ειδικότερες εκφάνσεις πρωταρχικής υποχρέωσης της Πολιτείας απέναντι στον σεβασμό και την προστασία της αξίας του ανθρώπου.

Ένα σύστημα υγείας, γνωστό επίσης ως σύστημα υγειονομικής περίθαλψης, είναι η οργάνωση ανθρώπων, θεσμών και πόρων που παρέχουν υπηρεσίες υγειονομικής περίθαλψης για την κάλυψη των αναγκών υγείας του πληθυσμού-στόχου (White, 2015). Υφίσταται ποικιλία συστημάτων υγείας ανά τον κόσμο, δημόσια, ιδιωτικά και μεικτά, με περίπου τόσες ιστορίες και οργανωτικές δομές όσα τα κράτη όπου αυτά υπάρχουν. Στην ουσία, τα κράτη πρέπει να σχεδιάζουν και να αναπτύσσουν τα συστήματα υγείας τους, με κριτήριο τις ανάγκες και τους πόρους τους. Πάρα ταύτα, κοινά στοιχεία σχεδόν όλων των συστημάτων αυτών είναι η ΠΦΥ και τα μέτρα δημόσιας υγείας που λαμβάνονται. Επιπλέον, κοινό στοιχείο τους είναι ότι απαρτίζονται από τρία μικρότερα υποσυστήματα, το

[2] Τα σχετικά άρθρα είναι τα 5 και 21.

υποσύστημα χρηματοδότησης, το υποσύστημα διεύθυνσης-συντονισμού και το υποσύστημα παραγωγής-διανομής, τα οποία τελούν μεταξύ τους σε σχέσεις αλληλεξάρτησης, και μαζί συναποτελούν τα συστήματα υγείας (Μπουρσανίδης, 2022).

2.2. Ψηφιακά - πληροφοριακά συστήματα στην υγεία

Στις μέρες μας, η πλειονότητα των ανθρώπων χρησιμοποιεί καθημερινά υπολογιστικά και πληροφοριακά συστήματα, με πιο χαρακτηριστικό παράδειγμα τον προσωπικό ή τον επαγγελματικό υπολογιστή, τα οποία συνδέονται στο Διαδίκτυο, για μια σειρά δραστηριοτήτων όπως η ενημέρωση, η επικοινωνία, η εργασία, οι συναλλαγές και η ψυχαγωγία.

Εντούτοις, δεν είναι απαραίτητο ότι η σημασία του όρου είναι εξίσου γνωστή και οικεία σε όλους. Προς συμπλήρωση του δημοφιλούς ορισμού που δόθηκε από τον Gabriele Piccoli το 2018 (Piccoli, 2018), πληροφοριακό-ψηφιακό σύστημα είναι ένα διατεταγμένο και αλληλεξαρτώμενο σύνολο διαδικασιών, ανθρωπίνου δυναμικού και αυτοματοποιημένων υπολογιστικών συστημάτων, που προορίζονται για τη συλλογή, αποθήκευση, επεξεργασία, ανάλυση και διανομή πληροφοριών. Από κοινωνιοτεχνική οπτική, τα συστήματα αυτά αποτελούνται από τέσσερα κύρια στοιχεία: διαδικασίες, ανθρώπους, ρόλους και τεχνολογία. Παρατηρούμε ότι οι πληροφορίες και τα δεδομένα κατέχουν κομβική σημασία στα ψηφιακά συστήματα, αποτελώντας το σημείο αναφοράς όλων των χρήσεων για τις οποίες προορίζονται.

Πλέον, τα ψηφιακά συστήματα είναι απαραίτητα μέσα, χάρη στα οποία αξιοποιείται ο ιατροτεχνολογικός εξοπλισμός, καθώς επίσης συντονίζεται, οργανώνεται και υλοποιείται η πρωταρχική λειτουργία των φορέων υγείας: η παροχή έγκαιρων, αποτελεσματικών και ποιοτικών υπηρεσιών υγείας σε όλους τους πολίτες χωρίς διακρίσεις. Συνεπώς, η εξάρτηση του χώρου της υγείας από την εύρυθμη λειτουργία των πληροφοριακών της συστημάτων είναι τεράστια. Τούτο διότι αυτός παρουσιάζει ιδιαιτερότητες, οι οποίες τον καθιστούν μοναδικό, συγκριτικά με οποιονδήποτε άλλο κλάδο της δημόσιας διοίκησης ή οικονομικής δραστηριότητας.

Πρώτον, παρέχει αδιάκοπες υπηρεσίες στον γενικό πληθυσμό, πολύ συχνά κατεπείγοντος χαρακτήρα, με πιο κλασική περίπτωση τα νοσοκομεία. Δεύτερον, απευθύνεται σε μία

ευαίσθητη ομάδα πολιτών, πρωτίστως στους ασθενείς και δευτερευόντως σε κάθε χρήστη των σχετικών υπηρεσιών συνολικότερα, δηλαδή όποιους κάνουν προληπτικό ιατρικό έλεγχο. Τρίτον, οι υπηρεσίες και τα φαρμακευτικά προϊόντα που παρέχονται και χορηγούνται στους ασθενείς ασκούν άμεση επίδραση στη ψυχοσωματική τους υγεία, με στόχο να θεραπεύσουν ή να μειώσουν την ένταση των νοσημάτων τους σε βαθμό διαχειρίσιμο και μη απειλητικό για εκείνους, προσδίδοντάς τους καλή ποιότητα ζωής. Τέταρτον, τα συστήματα υγείας επεξεργάζονται τεράστιο όγκο ευαίσθητων και ετερογενών π.δ και πληροφοριών (π.χ. ιατρικές εξετάσεις), των οποίων ο τύπος και το πλήθος μεταβάλλονται δυναμικά ανάλογα με το πέρασμα του χρόνου και την εξέλιξη της υγείας των ασθενών.

Κατά συνέπεια, τα δεδομένα αυτά πρέπει να παρακολουθούνται και να ενημερώνονται τακτικά, χρησιμεύοντας ως οδηγός για κάθε θεραπευτική ιατροφαρμακευτική παρέμβαση. Οι ανωτέρω παράγοντες ικανοποιούνται μέσω ολοκληρωμένων[3] ή και διαλειτουργικών[4] πληροφοριακών συστημάτων, διασυνδεδεμένων σε ένα ή παραπάνω δίκτυα ταυτόχρονα, είτε τοπικά εντός των νοσοκομείων (LAN), είτε ενδοδίκτυα (Intranet), είτε του Διαδικτύου –μέσω υπολογιστικών νεφών και του IoT (Laplante, 2019).

2.3. Ασφάλεια και ιδιωτικότητα: γενικά και στην υγεία

2.3.1. Βασικές απαιτήσεις ασφαλείας

Μέσω της ταξινόμησης, του συντονισμού και της χρήσης των πόρων ενός οργανισμού, ασκούνται οι διάφορες δραστηριότητές του, από τον εφοδιασμό, μέχρι τη διάθεση του προϊόντος ή της υπηρεσίας στον καταναλωτή-πελάτη, εάν πρόκειται για ΝΠΙΔ (ιδιωτικό φορέα) –και αντιστοίχως στον πολίτη, εάν πρόκειται για ΝΠΔΔ (δημόσιο φορέα). Άρα, είναι προφανές ότι τα ψηφιακά συστήματα των οργανισμών, κατά τη λειτουργία τους, πρέπει πάντα να είναι ασφαλή, διότι περιέχουν, φυλάσσουν και συντονίζουν όλους τους

[3] Η ολοκλήρωση ορίζεται ως η διαδικασία σύνδεσης διαφορετικών υπολογιστικών συστημάτων και εφαρμογών λογισμικού, φυσικά ή λειτουργικά, για να λειτουργήσει ως ένα συντονισμένο σύνολο (Georgia State University OECD, 2006).

[4] Η διαλειτουργικότητα είναι ικανότητα ενός συστήματος ή μιας διαδικασίας να μοιράζεται και να χρησιμοποιεί πληροφορία/ή και ενός άλλου συστήματος ή μιας άλλης διαδικασίας (Βάλσαμος, 2018).

πολύτιμους υλικούς και ψηφιακούς του πόρους (π.χ. ηλεκτρονικά αρχεία), οι οποίοι συναποτελούν τα περιουσιακά του στοιχεία. Από την άλλη, η ασφάλεια των ψηφιακών συστημάτων, επομένως και των πόρων-αγαθών του, προστατεύεται όταν τηρούνται οι τρεις βασικές απαιτήσεις ασφαλείας τους, οι οποίες είναι αναλυτικά οι ακόλουθες (Γκρίτζαλης, 2004) & (Εθνική Σχολή Δημόσιας Διοίκησης, 2021):

- Εμπιστευτικότητα (Confidentiality): Η διασφάλιση ότι μία πληροφορία ή ένας υπολογιστικός πόρος δεν γίνονται διαθέσιμα και δεν αποκαλύπτονται χωρίς την έγκριση του ιδιοκτήτη τους.
- Ακεραιότητα (Integrity): Η διασφάλιση της ακρίβειας και της πληρότητας των πληροφοριών, καθώς και η αποφυγή μη εξουσιοδοτημένης τροποποίησης μιας πληροφορίας.
- Διαθεσιμότητα (Availability): Η διασφάλιση ότι μια πληροφορία ή ένας υπολογιστικός πόρος βρίσκεται πάντα στη διάθεση ενός εξουσιοδοτημένου ατόμου όταν τη ζητήσει.

Κάτι που σταδιακά αλλάζει είναι ότι συμπληρωματικές απαιτήσεις ασφαλείας γίνονται, επίσης, αναγκαίες για την πλήρη διαφύλαξη της ασφάλειας των πληροφοριακών συστημάτων, καθώς η πολυπλοκότητα και η συχνότητα των κυβερνοαπειλών αυξάνονται συνεχώς. Οι επιπλέον απαιτήσεις ασφαλείας είναι:

- Αυθεντικοποίηση (Authentication): Είναι η διαδικασία πιστοποίησης και επιβεβαίωσης της ταυτότητας των χρηστών, η οποία σε κάθε περίπτωση βασίζεται στα διαπιστευτήρια που κατέχει ο χρήστης. Οι χρήστες μπορεί να είναι φυσικά πρόσωπα, υπηρεσίες, διαδικασίες ή υπολογιστές.
- Εξουσιοδότηση (Authorization): Είναι η διαδικασία που διέπει τα μέσα και τις λειτουργίες ελέγχου πρόσβασης σε πόρους από αυθεντικοποιημένους χρήστες. Οι πόροι περιλαμβάνουν αρχεία, βάσεις δεδομένων, πίνακες κλπ., σε συνδυασμό με πόρους συστήματος, όπως κλειδιά μητρώου και δεδομένα ρυθμίσεων.
- Μη αποποίηση της ευθύνης (Non-Repudiation): Είναι η αδυναμία αποποίησης της ευθύνης (άρνησης) για την εκτέλεση μιας ενέργειας, όπως την εκτέλεση μιας ηλεκτρονικής συναλλαγής.
- Ανθεκτικότητα (Resilience): Αναφέρεται στην ικανότητα ενός συστήματος να παράγει συνεχώς το επιδιωκόμενο αποτέλεσμα, παρά τα όποια αντίξοα περιστατικά.

Ειδικά για το χώρο της υγείας, λόγω των προαναφερθέντων ιδιαιτεροτήτων του, η διασφάλιση της ανθεκτικότητας είναι εξίσου κομβικής σημασίας, όχι μόνο συμβαδίζοντας με τις τάσεις που παρατηρούνται σε εθνικό, ευρωπαϊκό και διεθνές επίπεδο, αλλά κυρίως για το ότι τα συστήματα υγείας πρέπει να παρέχουν αδιάκοπα τις υπηρεσίες τους.

Η κυβερνοασφάλεια περιλαμβάνει εκείνες τις δραστηριότητες και τα μέτρα που απαιτούνται για την πλήρωση των απαιτήσεων ασφαλείας, ώστε τα ψηφιακά συστήματα και οι χρήστες τους να ανθίστανται στις κυβερνοαπειλές και τις κυβερνοεπιθέσεις.

Σχήμα 1: Οι απαιτήσεις ασφαλείας

Πηγή: ΕΣΔΔΑ, Κυβερνοασφάλεια στη δημόσια διοίκηση, 2021

2.3.2. Ιδιωτικότητα των ασθενών

Η ιδιωτικότητα των πολιτών, μία πτυχή της ατομικής ελευθερίας, είναι ένα από τα θεμελιώδη δικαιώματα που κατοχυρώνονται και προστατεύονται θεσμικά, στα σύγχρονα φιλελεύθερα κράτη δικαίου. Τα π.δ (δεδομένα προσωπικού χαρακτήρα) των ατόμων είναι ένα βασικό στοιχείο της ιδιωτικότητάς τους και η επεξεργασία τους διέπεται από συγκεκριμένες αρχές και επιτρέπεται σε ορισμένους φορείς, πάντα σύμφωνα με τις προϋποθέσεις του νόμου. Το Σύνταγμα, το εθνικό, το ενωσιακό και το διεθνές δίκαιο ρυθμίζουν το τοπίο των π.δ. Τα ιατρικά δεδομένα συνιστούν ειδική κατηγορία ευαίσθητων π.δ, η οποία

χρήζει ειδικής κι αυξημένης προστασίας από οποιαδήποτε παραβίαση, δηλαδή παράνομη αλλοίωση, τροποποίηση, διαγραφή, υποκλοπή ή διαρροή τους, εξαιτίας μη εξουσιοδοτημένης πρόσβασης σε αυτά.

Η προστασία αυτή, που συνεπάγεται υποχρεώσεις λήψης οργανωτικών, θεσμικών και τεχνικών μέτρων εκ μέρους των αποδεκτών των προσωπικών δεδομένων (των φορέων που δεσμεύονται με νομικές υποχρεώσεις για την προστασία τους), παρέχεται από το Σύνταγμα, το ιατρικό απόρρητο του Ν.3418/2005, τις διατάξεις του ΓΚΠΔ και του Ποινικού Κώδικα. Συγκεκριμένα, η ιδιωτικότητα των ασθενών και, γενικότερα, των χρηστών υπηρεσιών υγείας ταυτίζεται με τα ιατρικά δεδομένα και τις πληροφορίες τους, όπου κι αν αυτές καταχωρίζονται: σε φυσικό αρχείο, στον ΑΗΦΥ, στα ηλεκτρονικά αρχεία και τις βάσεις δεδομένων των ιδιωτών ιατρών, κλινικών, της ΠΦΥ, των διαγνωστικών κέντρων και των δημοσίων νοσοκομείων όπου νοσηλεύτηκαν ή εξετάστηκαν στο παρελθόν. Μεταξύ άλλων, τα δεδομένα στον ΗΦΥ περιέχουν δεδομένα, απλά και προσωπικά, όπως ονοματεπώνυμα, διευθύνσεις, τηλέφωνα, διευθύνσεις e-mail, ασφαλιστικά στοιχεία. Επειδή όμως η επεξεργασία των περισσοτέρων εξ αυτών των ιατρικών δεδομένων γίνεται μέσω των πληροφοριακών συστημάτων, οι κυβερνοαπειλές συγκαταλέγονται στους σοβαρότερους κινδύνους της παραβίασής τους. Ομοίως, περιστατικό παραβίασης ασφαλείας ή ιδιωτικότητας υφίσταται όταν πλήττεται –εσκεμμένα ή τυχαία– τουλάχιστον μία από τις αρχές της εμπιστευτικότητας, της ακεραιότητας ή της διαθεσιμότητας.

2.4. Κυβερνοαπειλές και κυβερνοεπιθέσεις

Η έννοια της κυβερνοαπειλής περιλαμβάνει όλες εκείνες τις απειλές και τους κινδύνους του κυβερνοχώρου, που αντιμετωπίζει δυνητικά ένα σύστημα ή δίκτυο πληροφοριών και που μπορούν να διαταράξουν ή να επιδράσουν δυσμενώς στη λειτουργία του. Το κακόβουλο λογισμικό (malware)[5] ανήκει στις πιο συχνές και σοβαρές κυβερνοαπειλές. Είναι οποιοδήποτε είδος λογισμικού, εσκεμμένα σχεδιασμένο να προκαλέσει δυσλειτουργία σε υπολογιστή, σέρβερ, διακομιστή ή δίκτυο, να παραβιάσει ιδιωτικές πληροφορίες, να αποκτήσει μη εξουσιοδοτημένη πρόσβαση σε πληροφορίες ή συστήματα, να στερήσει

[5] Ο όρος malware προέρχεται από τα αρχικά γράμματα του αγγλικών λέξεων malicious software. Για περισσότερα σχετικά, βλ. το κεφάλαιο 4.

τους χρήστες τους από την πρόσβαση στην πληροφορία και το οποίο παρεμβαίνει στην ασφάλεια και ιδιωτικότητα του υπολογιστή (Moir, 2009).

Οι κυβερνοεπιθέσεις συνιστούν τις πιο συνηθισμένες κυβερνοαπειλές, χωρίς ωστόσο αυτό να είναι εξαντλητικό, διότι οι κυβερνοαπειλές καταλαμβάνουν μεγαλύτερη έκταση. Για παράδειγμα, ένας κίνδυνος στα ψηφιακά συστήματα ενός νοσοκομείου, που μπορεί να προέλθει από την αμέλεια ή την άγνοια ενός εργαζόμενου περί της ορθής χρήσης του λογισμικού των δικτύων εφοδιασμού του, συνιστά μεν κυβερνοαπειλή και περιστατικό ασφαλείας, αλλά όχι κυβερνοεπίθεση για το νοσοκομείο.

Η κυβερνοεπίθεση-cyberattack διαφοροποιείται από την κυβερνοαπειλή ως προς το ότι είναι μία στενότερη έννοια, που ενέχει πολύ υψηλότερο κίνδυνο. Περιγράφει την κακόβουλη ενέργεια οποιωνδήποτε επιτιθέμενων (χάκερ) σε υπολογιστές, πληροφοριακά συστήματα, δίκτυα, υποδομές και εγκαταστάσεις, η οποία αποσκοπεί στην παραβίαση των απαιτήσεων ασφαλείας, ώστε από το αποτέλεσμά της να εξυπηρετηθεί προσωπικό όφελος είτε οικονομικό, είτε άλλου είδους. Κυρίως, δε, αποσκοπεί στην παραβίαση τουλάχιστον μίας εκ των τριών βασικών απαιτήσεων ασφαλείας, δηλαδή της ακεραιότητας, της εμπιστευτικότητας ή και της διαθεσιμότητας (Γκρίτζαλης, 2004). Ανάλογα με το πλαίσιο, οι επιθέσεις στον κυβερνοχώρο μπορεί να αποτελούν μέρος του κυβερνοπολέμου ή της κυβερνοτρομοκρατίας. Μια κυβερνοεπίθεση μπορεί να χρησιμοποιηθεί από κυρίαρχα κράτη, ιδιώτες, άτομα, ομάδες ή οργανισμούς, και μπορεί να προέρχεται από ανώνυμη πηγή (NIST, 2021).

3. Το σχετικό νομικό πλαίσιο σε εθνικό και ευρωπαϊκό επίπεδο

3.1. Η προ του ΓΚΠΔ εποχή

Πριν το 2016, το τοπίο προστασίας των π.δ ήταν, εν πολλοίς, θολό και προβληματικό. Οι έως τότε σχετικές νομικές ρυθμίσεις του εθνικού και ευρωπαϊκού δικαίου, κυρίως του Ν. 2472/1997 και της οδηγίας 95/46/ΕΚ, παρουσίαζαν προβλήματα ενιαίας εφαρμογής μεταξύ των κρατών μελών (Ζωγραφόπουλος, 2019). Εκτός αυτού, δεν συμβάδιζαν επαρκώς με την εκρηκτική πρόοδο των ΤΠΕ, του Διαδικτύου και των επιδράσεων αυτών στα προσωπικά δεδομένα. Τα π.δ στα ηλεκτρονικά είτε τα έντυπα αρχεία δημοσίων και ιδιωτικών φορέων αποθηκεύονταν, τροποποιούνταν και διανέμονταν, συχνά μάλιστα εν αγνοία και χωρίς τη συγκατάθεση των ατόμων και την τήρηση των απαραιτήτων μέτρων προστασίας.

Διευθύνσεις κατοικίας, ονοματεπώνυμα, ημερομηνίες γέννησης, τηλεφωνικοί αριθμοί, διευθύνσεις email, φωτογραφίες και βίντεο, ιατρικά δεδομένα, εμπορικές συναλλαγές είναι μόνο κάποια από τα παραδείγματα. Το αποτέλεσμα ήταν να προκύπτουν αρκετά εγχώρια και διεθνή περιστατικά παραβιάσεων π.δ (Todd, 2022), θίγοντας τη θεμελιώδη ατομική ελευθερία της ιδιωτικότητας, δίχως να επιβάλλονταν πάντα οι ανάλογες κυρώσεις στους υπευθύνους. Ωστόσο, αρκετά πρόστιμα επιβάλλονταν και πριν τη θέση σε ισχύ του ΓΚΠΔ (Ζωγραφόπουλος, 2019) & (Απόφαση 60/2011 της ΑΠΔΠΧ).

3.2. Η μετά τον ΓΚΠΔ εποχή (το ισχύον νομικό πλαίσιο)

3.2.1. Οι προβλέψεις του ΓΚΠΔ για τα προσωπικά δεδομένα και τα δεδομένα υγείας των ασθενών

Η κάλυψη των προηγούμενων επιτακτικών και επειγουσών αναγκών συνειδητοποιήθηκε κι έτσι το 2016 τέθηκε σε άμεση και οριζόντια ισχύ ο Κανονισμός (ΕΕ) 2016/679, γνωστός ως ΓΚΠΔ (GDPR). Καταργώντας και αντικαθιστώντας την προηγούμενη Οδηγία, ο ΓΚΠΔ εφαρμόζεται από το 2018 ενιαία σε όλα τα κράτη-μέλη της ΕΕ, με σκοπό την προστασία των φυσικών προσώπων έναντι της επεξεργασίας των δεδομένων προσωπικού χαρακτήρα και για την ελεύθερη κυκλοφορία των δεδομένων αυτών. Αποτελώντας έναν Κανονισμό-σταθμό στην ιστορία όχι μόνο της ΕΕ, αλλά και διεθνώς, λόγω της

πρωτοτυπίας των ρυθμίσεών του και του αυξημένου βαθμού προστασίας στα ατομικά δικαιώματα που παρέχει, ίδρυσε ουσιαστικά νέο αυτοτελή κλάδο δικαίου, το δίκαιο προστασίας π.δ. Οι διατάξεις του επαναπροσδιόρισαν τη σύγχρονη έννοια των π.δ, δημιούργησαν νέα ατομικά δικαιώματα για τα πρόσωπα, ίδρυσαν νέους αρμόδιους φορείς και Αρχές στα κράτη-μέλη, δεσμεύοντάς τα με υποχρεώσεις τήρησης συγκεκριμένων μέτρων ασφαλείας της επεξεργασίας τους και υποχρεώσεις μετά από ενδεχόμενα περιστατικά παραβίασης. Για την αδυναμία εκπλήρωσής τους προβλέφθηκαν αυστηρές ποινικές και διοικητικές κυρώσεις. Ακόμη, τέθηκαν αυστηρές αρχές, προϋποθέσεις και αποκλειστικοί σκοποί, η πλήρωση των οποίων είναι απαραίτητη για την επεξεργασία τους.

Στο άρθρο 4 του ΓΚΠΔ, ορίζεται ότι π.δ είναι κάθε πληροφορία που αφορά ταυτοποιημένο ή ταυτοποιήσιμο φυσικό πρόσωπο («υποκείμενο των δεδομένων»), ενώ δεδομένα υγείας είναι τα π.δ που σχετίζονται με τη σωματική ή ψυχική υγεία ενός φυσικού προσώπου, περιλαμβανομένης της παροχής υπηρεσιών υγειονομικής φροντίδας, και τα οποία αποκαλύπτουν πληροφορίες σχετικά με την κατάσταση της υγείας του. Επίσης, ορίζεται ότι παραβίασή τους είναι η παραβίαση της ασφάλειας των μέσων στα οποία αποθηκεύονται και η οποία οδηγεί σε τυχαία ή παράνομη καταστροφή, απώλεια, μεταβολή, άνευ άδειας κοινολόγηση ή πρόσβαση δεδομένων προσωπικού χαρακτήρα που διαβιβάστηκαν, αποθηκεύτηκαν ή υποβλήθηκαν κατ’ άλλο τρόπο σε επεξεργασία.

Τα ιατρικά δεδομένα, κατ’ αναλογία με τα άλλα είδη π.δ., πρέπει να προστατεύονται με τις προβλεπόμενες απαιτήσεις ασφαλείας, ασχέτως του εάν η επεξεργασία τους είναι αυτοματοποιημένη ή χειροκίνητη και του εάν αποθηκεύονται σε ηλεκτρονική ή έντυπη μορφή. Το άρθρο 32 προβλέπει τα εξής βασικά μέτρα προστασίας των π.δ:

- α) την ψευδωνυμοποίηση και την κρυπτογράφηση των δεδομένων προσωπικού χαρακτήρα.
- β) τη δυνατότητα διασφάλισης του απορρήτου, της ακεραιότητας, της διαθεσιμότητας και της αξιοπιστίας των συστημάτων και των υπηρεσιών επεξεργασίας σε συνεχή βάση.
- γ) τη δυνατότητα αποκατάστασης της διαθεσιμότητας και της πρόσβασης σε δεδομένα προσωπικού χαρακτήρα σε εύθετο χρόνο σε περίπτωση φυσικού ή τεχνικού συμβάντος.

- δ) διαδικασία για την τακτική δοκιμή, εκτίμηση και αξιολόγηση της αποτελεσματικότητας των τεχνικών και των οργανωτικών μέτρων για τη διασφάλιση της ασφάλειας της επεξεργασίας.

Της εφαρμογής των ανωτέρω θα πρέπει να προηγείται η εκτίμηση αντικτύπου (Business Impact Assessment) του άρθρου 33, για την εξακρίβωση των πόρων που χρήζουν προστασίας και των κινδύνων που θα συνεπαγόταν ένα περιστατικό παραβίασης, ιδίως όταν η επεξεργασία γίνεται με τη χρήση νέων τεχνολογιών. Επιπλέον, οι αποδέκτες των ιατρικών δεδομένων οφείλουν, σύμφωνα με το άρθρο 34, να ενημερώνουν τα υποκείμενα των ιατρικών δεδομένων για τυχόν παραβίαση. Βεβαίως, η ιδιαιτέρα ευαίσθητη φύση των ιατρικών δεδομένων, σε συνδυασμό με τον τεράστιο όγκο και τη σπουδαιότητά τους, όπως ήδη προαναφέρθηκε, καλό είναι να συνοδεύεται από τη λήψη περαιτέρω οργανωτικών και τεχνικών μέτρων εκ μέρους των αποδεκτών των συγκεκριμένων δεδομένων[6], τα οποία αναλύονται στο σχετικό κεφάλαιο. Όσον αφορά τα εφαρμοστικά μέτρα του ΓΚΠΔ, τις αρμοδιότητες της ΑΠΔΠΧ, καθώς και την ενσωμάτωση της σχετικής Οδηγίας 2016/680 στην εθνική έννομη τάξη, έγιναν με τον εκτελεστικό του ΓΚΠΔ Ν.4624/2019.

3.2.2. Ο θεσμός του DPO

Επίκεντρο του ΓΚΠΔ είναι ο θεσμός του Υπευθύνου Προστασίας Δεδομένων (DPO), στα άρθρα 37-39. Κατέχοντας συμβουλευτικό, άρα όχι αποφασιστικό ρόλο, αποτελεί τον βασικό παράγοντα που διευκολύνει τη συμμόρφωση του υπευθύνου και του εκτελούντος την επεξεργασία[7] με τις προβλεπόμενες απαιτήσεις ασφαλείας και που μεσολαβεί μεταξύ των άμεσα εμπλεκομένων, όπως τα υποκείμενα των δεδομένων και τις Ελεγκτικές Αρχές. Όμως, δεν φέρει ευθύνη για τυχόν παραβιάσεις των π.δ, σε αντίθεση με τον υπεύθυνο και τον εκτελούντα την επεξεργασία. Ο υπεύθυνος και εκτελών την επεξεργασία υποχρεούνται να ορίζουν DPO, οπότε κάθε μονάδα υγείας οφείλει να διαθέτει από έναν DPO.

[6] Η ομάδα εργασίας του άρθρου 29 έχει εκδώσει, σε συνεργασία με το δίκτυο ηλεκτρονικής υγείας των κρατών-μελών της ΕΕ την ακόλουθη οδηγία για τα μέτρα εφαρμογής του ΓΚΠΔ: (Clemens, 2018)

[7] Για την εξήγηση του «υπευθύνου επεξεργασίας» και του «εκτελούντος την επεξεργασία» βλ. άρθρα 24, 27 και 28 του ΓΚΠΔ.

3.2.3. Η Εγκύκλιος Οδηγία του Υπουργείου Υγείας

Το 2018, το Υπουργείο Υγείας εξέδωσε μία, πρωτοπόρα για τη δημόσια διοίκηση, Εγκύκλιο Οδηγία προς όλους τους φορείς υγείας, εποπτευόμενους και μη, ούτως ώστε να τους βοηθήσει στην προετοιμασία τους για τη συμμόρφωση προς τον ΓΚΠΔ (Υπουργείο Υγείας, 2018). Εκεί, μεταξύ άλλων, παρουσιάζονται οι βασικές έννοιες και αρχές του Κανονισμού, εξηγούνται οι απαιτούμενες ενέργειες συμμόρφωσης για τη λήψη και τήρηση μέτρων προστασίας των π.δ των ασθενών και παρατίθενται πρακτικά παραδείγματα για τη δέουσα επεξεργασία των π.δ ανάλογα την κάθε περίπτωση. Έκτοτε, η ενημέρωση κάθε φορέα υγείας περί του ΓΚΠΔ, των ιδιωτικών κλινικών, των διαγνωστικών κέντρων, των ιδιωτικών και δημόσιων μονάδων ΠΦΥ και των νοσοκομείων του ΕΣΥ, θεωρείται δεδομένη.

3.3. ENISA, Εθνική Αρχή Κυβερνοασφάλειας και άλλοι αρμόδιοι φορείς

Ο ENISA είναι ο Ευρωπαϊκός Οργανισμός Κυβερνοασφάλειας και λειτουργεί στην ΕΕ από το 2005, με έδρα την Αθήνα. Συνεργάζεται στενά με τα κράτη μέλη της ΕΕ και άλλους ενδιαφερόμενους φορείς για την παροχή συμβουλών και λύσεων, καθώς και για τη βελτίωση των δυνατοτήτων τους στον τομέα της κυβερνοασφάλειας. Επίσης, υποστηρίζει την ανάπτυξη μιας συνεργατικής αντίδρασης σε μεγάλης κλίμακας περιστατικά ή κρίσεις διασυνοριακής ασφαλείας στον κυβερνοχώρο κι από το 2019 καταρτίζει συστήματα πιστοποίησης κυβερνοασφάλειας (ENISA, 2022). Διαθέτει μεγάλο εύρος συμβουλευτικών και εκτελεστικών αρμοδιοτήτων επί της κυβερνοασφάλειας εντός της ΕΕ, οι οποίες, μαζί με λεπτομερείς ρυθμίσεις για την οργανωσιακή του δομή, την αποστολή και το ευρωπαϊκό πλαίσιο πιστοποίησης κυβερνοασφάλειας, καθορίζονται στον πρόσφατο Κανονισμό (ΕΕ) 2019/881. Έτσι, ο ENISA θα μπορούσε δικαίως να χαρακτηριστεί «το στρατηγείο κυβερνοασφάλειας της ΕΕ», φέροντας πρωταγωνιστικό ρόλο στην υποστήριξη των κρατών μελών ως προς την εφαρμογή της Οδηγίας NIS 2016/1148/ΕΕ, της πρώτης νομοθετικής πράξης σχετικά με τα μέτρα για την επίτευξη υψηλού κοινού επιπέδου ασφαλείας συστημάτων δικτύου και πληροφοριών σε ολόκληρη την ΕΕ.

Σε εθνικό επίπεδο, ένας από τους σημαντικότερους φορείς είναι η Γενική Διεύθυνση Κυβερνοασφάλειας του ΥΨΔ, η οποία ορίστηκε ως Εθνική Αρχή Κυβερνοασφάλειας με τον Ν.4577/2018, με τον οποίο ενσωματώθηκε στην ελληνική νομοθεσία η Οδηγία NIS. Η

Αρχή, που απαρτίζεται από ειδικό επιστημονικό προσωπικό, οργανώνει και εφαρμόζει τις δράσεις της Εθνικής Στρατηγικής Κυβερνοασφάλειας, η οποία εγκρίνεται με ΥΑ. Η πιο πρόσφατη –και ισχύουσα– στρατηγική είναι αυτή της περιόδου 2020-2025 (Υπουργός Επικρατείας, 2020). Επιπλέον, η Αρχή συντονίζει όλους τους συναρμόδιους για την κυβερνοασφάλεια φορείς στο δημόσιο και τον ιδιωτικό τομέα. Λόγω του ραγδαίου ψηφιακού μετασχηματισμού της ελληνικής δημόσιας διοίκησης και του ιδιωτικού τομέα, η Εθνική Στρατηγική Κυβερνοασφάλειας έχει αποκτήσει βαρύνουσα σημασία.

Άλλες αρμόδιες Αρχές και δημόσιοι φορείς για την προστασία των προσωπικών δεδομένων και την ασφάλεια των πληροφοριακών συστημάτων είναι:
(Α) Η ΑΔΑΕ για τη διασφάλιση του απορρήτου των επικοινωνιών, η οποία προβλέπεται στο άρθρο 19 του Συντάγματος και τη διέπει ο Ν.3115/2003.
(Β) Η ΕΕΤΤ (Ν. 4070/2012) για τις τηλεπικοινωνίες.
(Γ) Η ΔΙΔΗΕ, που λειτουργεί ως σημείο επαφής του κράτους σε 7ήμερη και 24ωρη βάση για ό,τι αφορά το ηλεκτρονικό έγκλημα, συμβουλές στους πληγέντες, εντοπισμό των υπόπτων και συλλογή αποδεικτικών στοιχείων.
(Δ) Η αρμόδια ομάδα απόκρισης CSIRT σε περιστατικά κυβερνοεπιθέσεων, θεσμός που εισήχθη με την οδηγία NIS, είναι η Διεύθυνση Κυβερνοχώρου της ΕΥΠ, η οποία συνιστά το εθνικό CERT/Εθνική Αρχή Αντιμετώπισης Ηλεκτρονικών Επιθέσεων.
(Ε) Ορισμένες αρμοδιότητες διαθέτει επίσης η Διεύθυνση Κυβερνοάμυνας του ΓΕΕΘΑ, που είναι αρμόδια για την αντιμετώπιση των επιθέσεων στο Υπουργείο Εθνικής Άμυνας και για όσες επιθέσεις δεν υπάγονται στην αρμοδιότητα του Εθνικού CERT της ΕΥΠ.

Επιπροσθέτως, ειδική μνεία πρέπει να γίνει στην ΑΠΔΠΧ, διότι είναι Ανεξάρτητη Αρχή με κομβικό ρόλο στο πεδίο προστασίας των π.δ των υποκειμένων –συμπεριλαμβανομένων και των ασθενών. Με τους νόμους 3471/2006 και 4624/2019, ορίζεται ότι η αποστολή της είναι η επίβλεψη της εφαρμογής του ΓΚΠΔ στην επικράτεια και η επιβολή κυρώσεων, σε περίπτωση που διαπιστωθεί παράβαση των υποχρεώσεων των αποδεκτών των π.δ, ιδιωτών ή Δημοσίου. Για παράδειγμα, μπορεί να επιβάλλει πρόστιμα και άλλα διοικητικά μέτρα, εάν διαπιστωθούν παραβάσεις κατά την εφαρμογή του ΓΚΠΔ. Επίσης, δέχεται τις καταγγελίες των φυσικών προσώπων για παραβάσεις, ενώ της γνωστοποιούνται υποχρεωτικά, αντιστοίχως, οποιαδήποτε περιστατικά παραβίασης π.δ των αποδεκτών κι έπειτα, κατά περίπτωση κι ανάλογα με τη βαρύτητα της παραβίασης και το είδος των δεδομένων, ενημερώνονται τα υποκείμενα των δεδομένων/φυσικά πρόσωπα.

3.4. Κανονισμός Ιατροτεχνολογικών Προϊόντων

Η φυσική ασφάλεια του ιατροτεχνολογικού εξοπλισμού που χρησιμοποιείται από το υγειονομικό προσωπικό είναι κρίσιμη ανά πάσα στιγμή, δεδομένου ότι επηρεάζει άμεσα πρωτίστως την υγεία των ασθενών και δευτερευόντως του υγειονομικού προσωπικού. Όμως, επειδή ο νοσοκομειακός αυτός εξοπλισμός είναι πλέον άρρηκτα διασυνδεδεμένος σε δίκτυα πληροφοριών και υποδομών, υπολογιστικά νέφη και στο IoT, έχοντας εγκατεστημένους συγκεκριμένους τύπους λογισμικών, είναι κυβερνοφυσικό συστήματα, η ψηφιακή ασφάλεια του οποίου καθίσταται εξίσου σημαντική. Ο συνδυασμός των παραμέτρων «ασφάλεια» και «κυβερνοφυσικά συστήματα» δίνει την «κυβερνοφυσική ασφάλεια», ήτοι την ασφάλεια των ηλεκτρονικών συσκευών και του εξοπλισμού που λειτουργούν μέσω του Διαδικτύου και του IoT (Pentek, 2016).

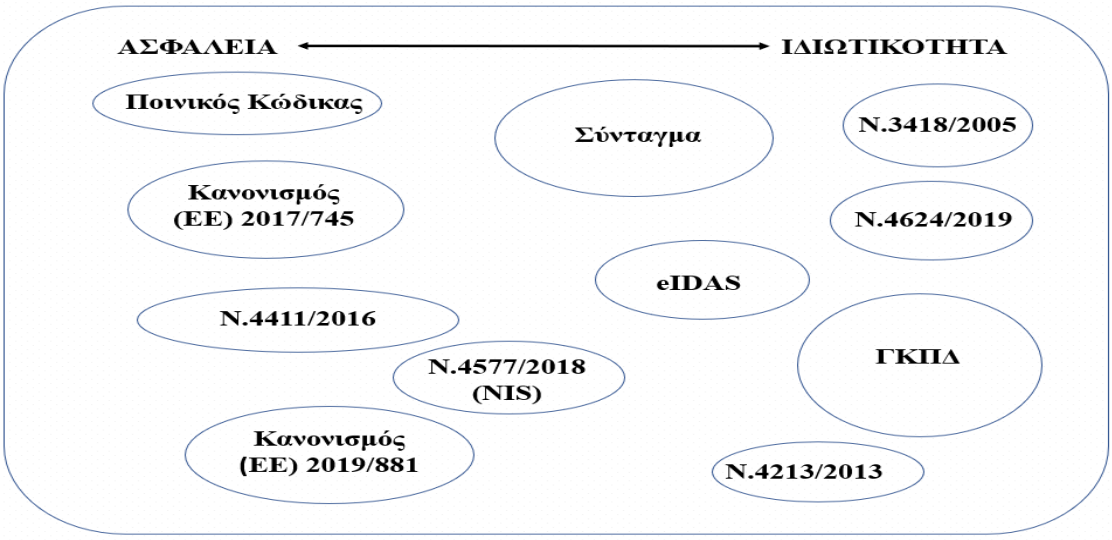
Ο Κανονισμός (ΕΕ) 2017/45 τέθηκε σε εφαρμογή το 2021 και προβλέπει την τήρηση αυστηρών προδιαγραφών ως προς την κυβερνοφυσική ασφάλεια από τους κατασκευαστές, τους προμηθευτές και τους εμπόρους, που διαθέτουν πάση φύσεως ιατροτεχνολογικά προϊόντα. Με σειρά ρυθμίσεων, θέτει ρητούς όρους που πρέπει να πληρούνται από τα ενδιαφερόμενα μέρη σχετικά με την ασφάλεια των προϊόντων, τον τρόπο ηλεκτρονικής καταχώρισής του σε βάσεις δεδομένων (άρθρο 29), αλλά και του λογισμικού που αυτά τρέχουν είτε κατά τη λειτουργία τους, είτε κατά την τροποποίηση και ενημέρωσή του. Μάλιστα, τα άρθρα 15 και 110 προβλέπουν ότι ορίζεται ειδικός αρμόδιος για την κανονιστική συμμόρφωση των προϊόντων και την επεξεργασία των π.δ που επεξεργάζονται μέσω των προϊόντων αυτών.

3.5. Λοιπές συναφείς νομοθετικές ρυθμίσεις

Το ηλεκτρονικό έγκλημα και η απάτη στον κυβερνοχώρο συνιστούν διακριτά ποινικά αδικήματα. Τιμωρούνται με την επιβολή χρηματικής ποινής ή φυλάκισης έως τρία έτη, αναλόγως της ζημιάς που προκλήθηκε σε ιδιώτες ή το Δημόσιο από τη διάπραξή τους. Με τον Ν.4411/2016, κυρώθηκε η Σύμβαση του Συμβουλίου της Ευρώπης για το έγκλημα στον κυβερνοχώρο, που διαπράττεται μέσω συστημάτων υπολογιστών, και μεταφέρθηκε η Οδηγία 2013/40/33 για τις επιθέσεις κατά συστημάτων πληροφοριών, με τις αντίστοιχες προσθήκες στα άρθρα του Ποινικού Κώδικα. Οι διατάξεις του ορίζουν ρητώς τα είδη του ηλεκτρονικού εγκλήματος και τις προβλεπόμενες ποινές, ώστε οι

παραβάτες να μη μένουν ατιμώρητοι. Προς αυτή την κατεύθυνση, η τροποποίηση του Ν.2225/1994 επιτρέπει την άρση του απορρήτου των επικοινωνιών και των ψηφιακών π.δ. Η άρση του ιατρικού απορρήτου επιτρέπεται κι από τον Κώδικα Ιατρικής Δεοντολογίας, Ν.3418/2005 (άρθρο 13), υπό συγκεκριμένες προϋποθέσεις και λόγους, εφόσον πρόκειται για ιατρικά δεδομένα. Η παράνομη πρόσβαση φυσικού ή νομικού προσώπου σε ψηφιακά π.δ., με σκοπό την αλλοίωση, υποκλοπή ή και διαγραφή τους, ανήκει στα εν λόγω αδικήματα. Επιβαρυντική περίσταση για την αυστηρότητα της ποινής είναι η παραβίαση ευαίσθητων π.δ σαν τα ιατρικά. Βαρύτερη ποινική μεταχείριση συνεπάγεται η παρακώληση λειτουργίας και οι κακόβουλες ενέργειες κατά πληροφοριακών συστημάτων και δικτύων υποδομών, μέσω των οποίων παρέχονται αγαθά και υπηρεσίες ζωτικής σημασίας για το κοινωνικό σύνολο, όπως η ηλεκτροδότηση, η ύδρευση, η τηλεφωνία, η εθνική άμυνα και, φυσικά, η υγεία.

Επιπλέον, ο Ν. 4213/2013 προσαρμόζει την εθνική νομοθεσία στην Οδηγία περί εφαρμογής των δικαιωμάτων των ασθενών στο πλαίσιο της διασυνοριακής υγειονομικής περίθαλψης, συμπεριλαμβανομένων των υπηρεσιών τηλεϊατρικής. Τέλος, ο Κανονισμός (ΕΕ) 910/2014-eIDAS θέτει κανόνες για την ηλεκτρονική ταυτοποίηση των ατόμων και την ασφάλεια όλων των ηλεκτρονικών συναλλαγών στην εσωτερική αγορά της ΕΕ είτε με το Δημόσιο, είτε με ιδιώτη, κανόνες που ισχύουν και στην υγεία-τηλεϊατρική. Ακολούθως, παρατίθεται το εξής σχήμα, προκειμένου να απεικονιστεί παραστατικά το ισχύον νομικό πλαίσιο ρύθμισης της κυβερνοασφάλειας των πληροφοριακών συστημάτων της υγείας και προστασίας ιδιωτικότητας των ασθενών, το οποίο εφαρμόζεται συνδυαστικά:



Σχήμα 2: Η νομοθεσία της ασφάλειας και της ιδιωτικότητας στο χώρο της υγείας –το νομικό πλαίσιο είναι ενιαίο και εφαρμόζεται συνδυαστικά, ad hoc.

4. Σύγχρονες απειλές κατά της ασφάλειας και προστασίας της ιδιωτικότητας στο χώρο της υγείας

Οι σύγχρονες απειλές στον κυβερνοχώρο αγγίζουν όλους τους κρατικούς και ιδιωτικούς οργανισμούς που χρησιμοποιούν πληροφοριακά συστήματα, διασυνδεδεμένα σε LAN, ενδοδίκτυα, δίκτυα υποδομών, υπολογιστικά νέφη και το IoT για την εξυπηρέτηση των δραστηριοτήτων τους. Υφίστανται πολλές και διαφορετικές κυβερνοαπειλές, η εξαντλητική περιγραφή των οποίων, προφανώς, υπερβαίνει τον σκοπό της παρούσας μελέτης.

Ωστόσο, ακολούθως εστιάζουμε στις πιο συχνές και σοβαρές απειλές που απασχόλησαν γενικότερα το πεδίο του κυβερνοχώρου, όπως διαμορφώθηκαν κατά τη διετία 2020-2021, σύμφωνα με τη σχετική έκθεση του ENISA (ENISA, Threat Landscape 2021, 2021) και το άρθρο της Chua (Chua, 2021). Η εξειδίκευση και έμφαση, όπου είναι δυνατόν, δίνεται στο χώρο της υγείας.

Η ταξινόμησή τους, βάσει της βιβλιογραφίας, γίνεται με κριτήριο την προέλευση της εκάστοτε απειλής, δηλαδή το εάν αυτή προέρχεται από το εξωτερικό ή το εσωτερικό περιβάλλον των συστημάτων υγείας. Βεβαίως, τα όρια της διάκρισης δεν είναι απόλυτα, αλλά σχετικοποιούνται, καθότι μια εσωτερική απειλή δύναται να καταλήξει εξωτερική, αποκτώντας πολύ ευρύτερες διαστάσεις από την αρχική, με ό,τι αυτό συνεπάγεται. Εξίσου πιθανό είναι το αντίστροφο σενάριο.

4.1. Σύγχρονες απειλές κατά της ασφάλειας και προστασίας της ιδιωτικότητας των ασθενών

4.1.1. Εξωτερικές απειλές

- Malware: Το malware είναι ιομορφικό λογισμικό διαφόρων τύπων και βαθμών επικινδυνότητας, το οποίο αποσκοπεί στην παραβίαση της ασφάλειας των πληροφοριακών συστημάτων. Συνιστά την υπ’ αριθμόν ένα απειλή του κυβερνοχώρου, δεδομένου ότι μπορεί να μολύνει πρωτογενώς ένα σύστημα ή δίκτυο, ενώ όλες οι άλλες κυβερνοαπειλές, με τις διαφορετικές μορφές και τρόπους δράσης τους, αποσκοπούν τελικά στη μόλυνση του θύματός τους με malware. Κάθε

κυβερνοεπίθεση, ενεργητική ή παθητική[8], χρησιμοποιεί κάποιο malware, προκειμένου έπειτα να εκπληρωθούν οι σκοποί των επιτιθέμενων-χάκερ. Στους κύριους τύπους του malware συγκαταλέγονται ο ιός (virus), ο δούρειος ίππος (trojan horse), το σκουλήκι-αναπαραγωγός (worm), οι κερκόπορτες (backdoors), η λογική βόμβα (logic bomb) και τα βακτήρια (bacteria)[9].

- Λυτρισμικό (ransomware): Το ransomware είναι ένα μοναδικό, ισχυρό είδος malware, που διαφέρει από τα υπόλοιπα ως προς το ότι προσπαθεί να μπλοκάρει την πρόσβαση στα δεδομένα ενός χρήστη, συνήθως κρυπτογραφώντας τα με ένα κλειδί γνωστό μόνο στον χάκερ που ανέπτυξε το malware, μέχρι να πληρωθούν λύτρα. Αφότου κρυπτογραφηθούν τα δεδομένα του χρήστη, το ransomware κατευθύνει τον χρήστη να πληρώσει τα λύτρα στον χάκερ (συνήθως σε κρυπτονομίσματα, όπως το Bitcoin), προκειμένου να λάβει ένα κλειδί αποκρυπτογράφησης. Ακόμη, μπορεί να αναπτυχθεί ransomware που καταστρέφει ή υποκλέπτει δεδομένα, ή να συνδυαστεί με άλλο malware για να πλήξει οποιαδήποτε βασική απαίτηση ασφαλείας των συστημάτων. Η πληρωμή των λύτρων δεν εγγυάται ότι ο χάκερ θα αποκρυπτογραφήσει ή θα ξεκλειδώσει κλεμμένα ή κλειδωμένα δεδομένα. Οι απειλές ransomware μπορεί να ενσωματώνουν τακτικές που είναι ίδιες ή πανομοιότυπες και σε άλλες απειλές. Οι επιθέσεις με λυτρισμικό έχουν αυξηθεί τόσο εκρηκτικά τα τελευταία χρόνια, έτσι ώστε το ransomware κατατάσσεται στην κορυφαία απειλή του κυβερνοχώρου για τη διετία του 2020-2021. Εν προκειμένω, νοσοκομεία δέχτηκαν πολλές επιθέσεις ransomware κι έτσι υποκλάπηκαν π.δ ασθενών και επλήγη το δίκτυο υποδομών τους (Weiner, 2021).
- Πειρατεία εξόρυξης κρυπτονομισμάτων (Cryptojacking): Το cryptojacking είναι ένα είδος κυβερνοεγκλήματος, που συνίσταται στην κρυφή εκμετάλλευση της υπολογιστικής ισχύος του θύματος από τους επιτιθέμενους, ούτως ώστε οι δεύτεροι να δημιουργούν κρυπτονομίσματα. Ο πολλαπλασμός των κρυπτονομισμάτων και η ολοένα αυξανόμενη απήχησή τους στο ευρύτερο κοινό έχει παρατηρηθεί

[8] Η ενεργητική επίθεση στοχεύει στο να παρέμβει και να τροποποιήσει τον τρόπο λειτουργίας του συστήματος. Αντιθέτως, η παθητική στοχεύει στη συλλογή και χρήση πληροφοριών, χωρίς να γίνει αντιληπτή και να επηρεάσει την ομαλή λειτουργία του (Εθνική Σχολή Δημόσιας Διοίκησης, 2021).

[9] Περαιτέρω ανάλυση για τον κάθε τύπο malware βλ. (Εθνική Σχολή Δημόσιας Διοίκησης, 2021)

ότι συσχετίζεται με την αύξηση των περιστατικών κυβερνοασφάλειας. Αν ένα νοσοκομείο χτυπηθεί από cryptojacking, η απόδοση των ψηφιακών δικτύων θα φθίνει, οπότε και του εξοπλισμού που συνδέεται με αυτά.

- Ηλεκτρονικό ψάρεμα-εξαπάτηση μέσω email (email phishing): Από τις πιο διαδεδομένες απειλές, το ηλεκτρονικό ψάρεμα είναι μια προσπάθεια εξαπάτησης κάποιου για να αποκαλύψει πληροφορίες μέσω email. Το εισερχόμενο email ηλεκτρονικού ψαρέματος περιλαμβάνει έναν ενεργό σύνδεσμο ή αρχείο (συχνά μια εικόνα ή ένα γραφικό). Το email φαίνεται να προέρχεται από νόμιμη πηγή, όπως από κάποιον φίλο, συνάδελφο, διευθυντή, εταιρεία ή ακόμα και τη διεύθυνση email του ίδιου του χρήστη. Κάνοντας κλικ για να ανοίξει ο σύνδεσμος ή το αρχείο, ο χρήστης οδηγείται σε έναν ιστότοπο, όπου μπορεί να του ζητηθούν ευαίσθητες πληροφορίες ή να μολυνθεί κατευθείαν ο υπολογιστής του. Η πρόσβαση στον σύνδεσμο ή το αρχείο μπορεί να έχει ως αποτέλεσμα την εγκατάσταση malware ή την παροχή πρόσβασης σε πληροφορίες, αποθηκευμένες στους συνδεδεμένους στο δίκτυο υπολογιστές. Πολύ συχνά χρησιμοποιούνται τα μέσα κοινωνικής δικτύωσης, το Facebook, το Twitter και το Instagram, για τέτοιες επιθέσεις κοινωνικής μηχανικής. Ένας άλλος τρόπος phishing, λιγότερο διαδεδομένος, που χρησιμοποιείται για εξαπάτηση από κακόβουλους χάκερ είναι να αφεθεί ένα μολυσμένο με malware USB stick ή CD σε κάποιον πολυσύχναστο χώρο του νοσοκομείου, όπως η αίθουσα αναμονής των επισκεπτών. Κάποιος εξουσιοδοτημένος χρήστης, που θα το βρει, ενδέχεται από περιέργεια να το συνδέσει στα ψηφιακά συστήματα για να δει το περιεχόμενό του κι έτσι να μολύνει, άθελά του, τον υπολογιστή, επεκτείνοντας τη μόλυνση σε όλο το δίκτυο.
- Άρνηση Υπηρεσίας (DoS) και Κατανεμημένη Άρνηση Υπηρεσίας (DDoS): Ανάμεσα στις απειλές της ασφάλειας ενός πληροφοριακού συστήματος, ξεχωρίζουν οι DoS και DDos επιθέσεις, οι οποίες στοχεύουν στην προσβολή της ακεραιότητας ή της διαθεσιμότητας, επιχειρώντας να θέσουν εκτός λειτουργίας το θύμα, προκαλώντας αδυναμία παροχής των υπηρεσιών του στους εξουσιοδοτημένους χρήστες του. Αυτό επιτυγχάνεται με την αποστολή υπεράριθμου πλήθους αιτημάτων εξυπηρέτησης, με συνέπεια να προκληθεί η υπερφόρτωση και η κατάρρευσή του δικτύου –η DoS επίθεση. Όταν η επίθεση γίνεται συντονισμένα από πολλές διαφορετικές τοποθεσίες του Διαδικτύου ως web based attack, π.χ. μέσω απομακρυσμένων ελεγχόμενων botnets (ρομπότ-λογισμικά), τότε πρόκειται για επίθεση DDoS, η οποία έχει τη δυνατότητα να επιφέρει τεράστιες ζημιές στα

συστήματα υγείας, διακόπτοντας τη διαθεσιμότητά του συνδεδεμένου εξοπλισμού τους και εξαντλώντας τους πόρους τους.

- Επίθεση στην εφοδιαστική αλυσίδα (supply chain attack): Οι κυβερνοεπιθέσεις στην εφοδιαστική αλυσίδα επιζητούν να βλάψουν έναν οργανισμό, στοχεύοντας λιγότερο ασφαλή μέρη της εφοδιαστικής αλυσίδας του, δηλαδή τα πάσης φύσεως εξαρτήματα, εξοπλισμό, software ή hardware, τα οποία προμηθεύεται από εξωτερικούς πελάτες και μετά τα συνδέει στα υπολογιστικά του δίκτυα. Επειδή τα περιφερειακά αυτά μέρη παραλαμβάνονται έτοιμα για χρήση και σύνδεση, αποτελούν μια εύκολη δίοδο για τους επιτιθέμενους, οι οποίοι τα μολύνουν εκ των προτέρων με malware ή hardware παρακολούθησης, γνωρίζοντας τη συγκεκριμένη ευπάθεια. Τέτοιες επιθέσεις μπορούν να αποβούν φοβερά επιβλαβείς για τους οργανισμούς, διότι νεκρώνουν το εφοδιαστικό τους δίκτυο, προκαλώντας την αδυναμία παροχής των υπηρεσιών τους, επειδή τους στερούν τις πρώτες ύλες. Ο αυξημένος κίνδυνος και η πολυπλοκότητά τους εντοπίζεται στο ότι παίρνουν διάφορες μορφές και χρησιμοποιούν ποικίλα μέσα: Για παράδειγμα, κλεμμένα πιστοποιητικά κωδικών ή υπογεγραμμένες κακόβουλες εφαρμογές που χρησιμοποιούν την ταυτότητα της εταιρείας προγραμματισμού, παραβιασμένο εξειδικευμένο κώδικα που αποστέλλεται σε στοιχεία υλικού ή λογισμικού, προεγκατεστημένο κακόβουλο λογισμικό σε συσκευές όπως κάμερες, USB, τηλέφωνα κ.λπ. (Microsoft, 2022). Ένα νοσοκομείο, για παράδειγμα, ίσως καταλήξει αποκομμένο από το δίκτυο αποθήκευσης και καταχώρισης του ιατροφαρμακευτικού υλικού του, επειδή συνέδεσε στον μαγνητικό τομογράφο ένα βοηθητικό εξωτερικό μηχάνημα, του οποίου το λογισμικό αποδείχτηκε τελικά μολυσμένο με malware. Η πιο γνωστή επίθεση στην εφοδιαστική αλυσίδα είναι αυτή που έγινε με το σκουλήκι Stuxnet, η οποία ευθύνεται για τη ματαίωση του πυρηνικού προγράμματος του Ιράν (Kushner, 2013)
- Επίθεση μέσω του IoT (IoT attack): Ο ιατρικός εξοπλισμός, οι ηλεκτρονικές έξυπνες συσκευές, η παροχή υπηρεσιών υγείας και τηλεϊατρικής εξαρτώνται ολοένα περισσότερο από το IoT, μέσω του οποίου γίνονται διαγνώσεις και παρακολουθούνται οι ζωτικές λειτουργικές των ασθενών. Με σύμβουλο τα στοιχεία αυτά, οι γιατροί προβαίνουν στις κατάλληλες θεραπευτικές παρεμβάσεις, πλέον ακόμη και εξ αποστάσεως. Το λογισμικό του υλικοτεχνικού αυτού εξοπλισμού ενημερώνεται πάλι μέσω του IoT κι έπειτα εγκαθίσταται στο υπολογιστικό δίκτυο του νοσοκομείου. Επιπρόσθετα, σε υπολογιστικά νέφη στο IoT, γίνεται ανάρτηση και

επεξεργασία ηλεκτρονικών αρχείων με ιατρικά δεδομένα ασθενών, συνθέτοντας μια αλυσίδα κρίσιμων αλληλεξαρτώμενων παραγόντων: των πληροφοριακών δικτύων, του ιατροφαρμακευτικού εξοπλισμού και των έξυπνων συσκευών που είναι διασυνδεδεμένα, διαλειτουργώντας μέσω του IoT ως κυβερνοφυσικά συστήματα. Οι IoT επιθέσεις, αξιοποιώντας το εύρος χρήσεων, τη διείσδυση του IoT στο χώρο της υγείας και των πιθανών ευπαθειών των κυβερνοφυσικών συστημάτων, είναι επιθέσεις κατά της κυβερνοφυσικής ασφάλειάς τους. Διαθέτουν τη δυνατότητα παραβίασης αυτής και, συνακόλουθα, της ιδιωτικότητας των ασθενών, χωρίς αυτό μάλιστα να μπορεί συχνά να γίνει αντιληπτό από το αρμόδιο προσωπικό, κάτι εξαιρετικά επικίνδυνο. Η IoT επίθεση λειτουργεί ως «πύλη» για την εξαπόλυση άλλων κυβερνοεπιθέσεων ή μπορεί να έχει προέλθει με αφετηρία αυτές. Έτσι, μία IoT επίθεση μπορεί να ξεκίνησε από το μολυσμένο με malware smartphone ή τάμπλετ ενός υπαλλήλου, ο οποίος συνδέθηκε στο ασύρματο δίκτυο (Wi-Fi) ενός νοσοκομείου, το οποίο διαλειτουργεί με το IoT. Η ανησυχία για επιθέσεις τέτοιου είδους, τα προσεχή χρόνια, είναι διάχυτη παγκοσμίως στις ιδιωτικές εταιρείες και τους δημόσιους οργανισμούς. Ομοίως με την εκρηκτική αύξηση των επιθέσεων στην εφοδιαστική αλυσίδα, υπό την επίδραση της πανδημίας του κορωνοϊού, οι IoT επιθέσεις αυξήθηκαν εκθετικά. Ως εκ τούτου, η πιθανότητα εμφάνισής τους καταλαμβάνει τις πρώτες θέσεις με τα μεγαλύτερα ποσοστά, σε σχέση με τις άλλες (INTERSOG, 2021) [10].

- Παραπληροφόρηση: Οι εκστρατείες παραπληροφόρησης είναι σε έξαρση, υποκινούμενες από την αυξανόμενη χρήση των μέσων κοινωνικής δικτύωσης και του ηλεκτρονικού Τύπου, καθώς κι ως αποτέλεσμα της αυξημένης διασύνδεσης των ανθρώπων στο Διαδίκτυο, λόγω των περιοριστικών μέτρων της πανδημίας του κορωνοϊού. Αυτή η ομάδα απειλών είναι η πρώτη φορά που εμφανίζεται στην έκθεση του ENISA, ωστόσο η βαρύτητά τους δεν είναι συνετό να υποτιμάται, επειδή αυτές χρησιμοποιούνται σε υβριδικές επιθέσεις.
- Άλλα αίτια, όπως ατυχήματα και φυσικές καταστροφές: Η συνεχής επιδείνωση της κλιματικής αλλαγής έχει δυστυχώς προσδώσει συνήθη χαρακτήρα σε ακραία καιρικά φαινόμενα. Πυρκαγιές, έντονες χιονοπτώσεις, θύελλες και πλημμύρες

[10] Το 2021, υπό την επίδραση της πανδημίας του κορωνοϊού, προέκυψαν παραπάνω από 1,5 δισεκατομμύρια παραβιάσεις IoT, οι περισσότερες εκ των οποίων χρησιμοποιούσαν το πρωτόκολλο απομακρυσμένης πρόσβασης telnet (INTERSOG, 2021).

συχνά προκαλούν φθορές έως και καταστροφές στις κτηριακές υποδομές των νοσοκομείων, με δυνητικό αντίκτυπο στα υπολογιστικά δίκτυά τους. Την ίδια απειλή συνιστούν τα ατυχήματα εντός των νοσοκομειακών εγκαταστάσεων από αμέλεια, φθορά, κακή συντήρηση του εξοπλισμού και των υποδομών κλπ.

4.1.2. Εσωτερικές απειλές

- Ανθρώπινα λάθη από άγνοια, ατυχή ή αμελή χρήση: Τα λάθη του ανθρώπινου παράγοντα από άγνοια, ατυχή ή αμελή χρήση είναι συνήθη σε κάθε περίσταση, επομένως αυτό ισχύει και αναφορικά με τα υπολογιστικά συστήματα ενός νοσοκομείου. Για παράδειγμα, η πλημμελής χρήση ενός υπολογιστή από κάποιον εργαζόμενό του, ανοίγοντας παραπλανητικά phishing emails, ή η αναβάθμιση του λογισμικού των ηλεκτρονικών συσκευών από φαινομενικά έγκυρη ιστοσελίδα, μπορούν να βλάψουν την ασφάλεια των πόρων του με απρόβλεπτα επακόλουθα.
- Κακόβουλη ενέργεια από το εσωτερικό: Η κακόβουλη ενέργεια μπορεί ενίοτε να προέλθει από το προσωπικό, τους συνεργάτες ή προμηθευτές ενός φορέα υγείας, επειδή από την ενέργειά τους περιμένουν να αποκομίσουν όφελος ή είναι για κάποιο λόγο δυσαρεστημένοι με τον εργοδότη τους (π.χ απολυμένο προσωπικό). Διάσημη περίπτωση τέτοιας ενέργειας είναι αυτή ενός πρώην συμβασιούχου φύλακα στο North Central Medical Plaza του Ντάλας, ο οποίος παραδέχτηκε, αναρτώντας μάλιστα βίντεο στην πλατφόρμα youtube, ότι χάκαρε τα συστήματα υπολογιστών του νοσοκομείου κατά τη βραδινή του βάρδια (Poulsen, 2011).
- Απώλεια ή κλοπή εξοπλισμού και διαπιστευτηρίων εξουσιοδοτημένων λογαριασμών χρηστών: Η απώλεια ή η κλοπή υλικοτεχνικού εξοπλισμού ενός νοσοκομείου και υλισμικού (hardware), που συνδέονται με το δίκτυό του, όπως cd, usb, λάπτοπ, ακόμη και των διαπιστευτήριων εξουσιοδότησης λογαριασμού (σελίδα χαρτί με όνομα χρήστη και κωδικό πρόσβασης) ενδέχεται να αφήσουν τους φορείς υγείας απροστάτευτους απέναντι σε όποιον κακόβουλο χρήστη τα βρει.
- Απουσία φύλαξης κρίσιμων υπολογιστικών δικτύων και υποδομών: Είναι σημαντικό οι πόροι των φορέων υγείας να φυλάσσονται αφενός από τεχνικής πλευράς, μέσω των ενδεδειγμένων μέτρων ασφαλείας, αφετέρου από φυσικής. Η τυχόν εύκολη πρόσβαση στους πόρους του νοσοκομείου από μη εξουσιοδοτημένο προσωπικό, σε μηχανήματα, ιατρικό εξοπλισμό και υπολογιστικά δίκτυα, είναι σίγουρα απειλή.

- Άγνοια, απουσία ενημέρωσης και εκπαίδευσης γύρω από τις κυβερνοαπειλές: Η άγνοια και η απουσία ενημέρωσης περί των κυβερνοαπειλών και των πρακτικών κυβερνοασφάλειας είναι από μόνες τους παράμετροι επικινδυνότητας. Οδηγούν σε αυξημένες πιθανότητες εμφάνισης των άλλων απειλών, φερ' ειπείν, ανθρώπινα λάθη κατά τη χρήση ενός υπολογιστή, μη φύλαξη των υπολογιστικών δικτύων και υποδομών, απώλεια διαπιστευτηρίων, εξαπάτηση από phishing κλπ.

Κατ' αντιστοιχία με τη σχετικότητα διάκρισης των απειλών σε εξωτερικές και εσωτερικές, επισημαίνεται ότι ισχύει το ίδιο για την ταξινόμηση κάθε ομάδας απειλών που παρουσιάστηκαν. Έτσι, επιτυχημένες επιθέσεις phishing μπορεί να οδηγήσουν στην εγκατάσταση ransomware σε έναν υπολογιστή, ενώ η μόλυνση με ransomware είναι δυνατόν να έχει προκύψει ως αποτέλεσμα πολλαπλών μολύνσεων με malware. Ένα άλλο χαρακτηριστικό παράδειγμα είναι οι IoT επιθέσεις, οι οποίες μπορούν κάλλιστα να πάρουν τελικά τη μορφή μιας επίθεσης στην εφοδιαστική αλυσίδα, DoS, DDoS επίθεσης ή ransomware.

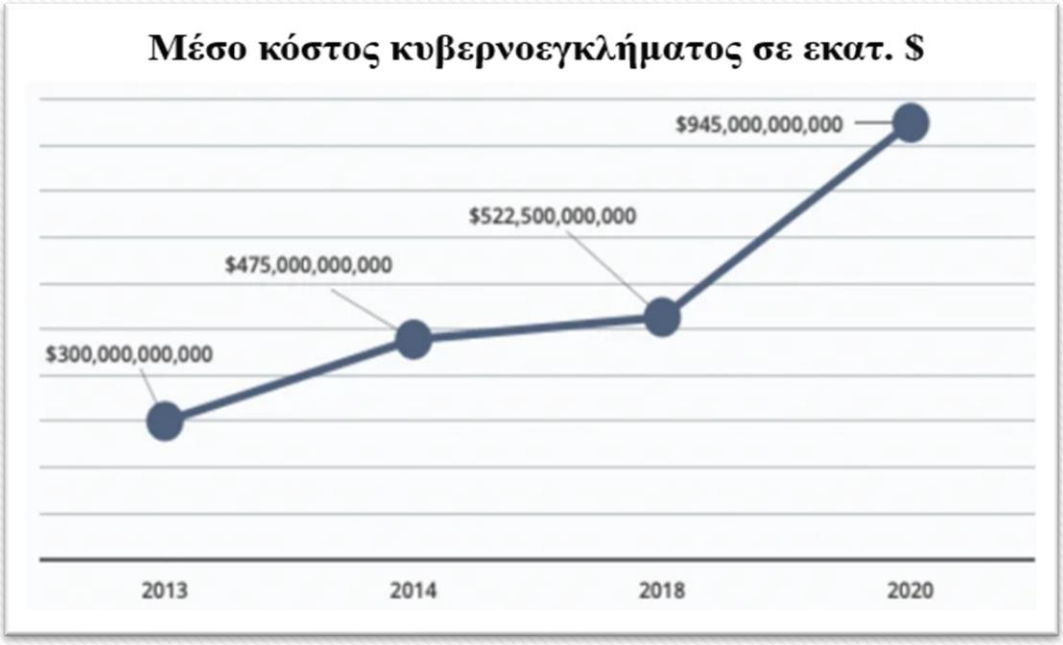
Στο δε περιστατικό παραβίασης της ασφάλειας των πληροφοριακών συστημάτων-δικτύων, μέσω οποιασδήποτε παραβίασης μιας εκ των τριών βασικών απαιτήσεων ασφαλείας, εύκολα επέρχεται η παραβίαση της εμπιστευτικότητάς τους. Από εκεί κι έπειτα, μια τέτοια μη εξουσιοδοτημένη ή παράνομη πρόσβαση αρκεί για να οδηγήσει στην παραβίαση των ηλεκτρονικών αρχείων και των βάσεων δεδομένων, δηλαδή παραβιάζεται η ιδιωτικότητα. Παρατηρείται, επομένως, ότι οι σύγχρονες απειλές κατά της ασφάλειας και προστασίας της ιδιωτικότητας στο χώρο της υγείας είναι μεταξύ τους αλληλένδετες και μπορούν να πλήξουν τόσο την ασφάλεια, όσο και την ιδιωτικότητα.

4.1.3. Συνέπειες – επιπτώσεις των σύγχρονων απειλών

Οποιαδήποτε παραβίαση της ασφάλειας των πληροφοριακών συστημάτων, των δικτύων και των βάσεων δεδομένων στην Υγεία συνεπάγεται ευρέως φάσματος και έντασης επιπτώσεις. Αναλόγως δε του είδους και των οριστικών αποτελεσμάτων της εκάστοτε απειλής, αυτές μπορεί να κυμαίνονται από ήπιες σε απλούς οικονομικούς όρους, μέχρι σοβαρότατες, με την υποκλοπή-διαρροή των π.δ των ασθενών και την άμεση διακινδύνευση της ζωής τους. Αναλυτικότερα, διαπιστώνονται οι κάτωθι δυνητικές επιπτώσεις από τις σύγχρονες απειλές ανά κατηγορία.

Οι οικονομικές-υλικές επιπτώσεις έχουν να κάνουν με τις υλικές φθορές που υφίσταται ο ιατρονοσηλευτικός εξοπλισμός, οι συσκευές, οι υπολογιστές και τα δίκτυα υποδομών των συστημάτων υγείας και της εμπλεκόμενης αγοράς (προμηθευτές, κατασκευαστές, φαρμακευτικές εταιρείες). Είναι το κόστος σε χρήμα που απαιτείται για την επιδιόρθωση ή τυχόν αντικατάσταση του εξοπλισμού και οι απώλειες σε χρήμα από τη διακοπή των εμπορικών συναλλαγών με τους φορείς υγείας εξαιτίας της επίθεσης.

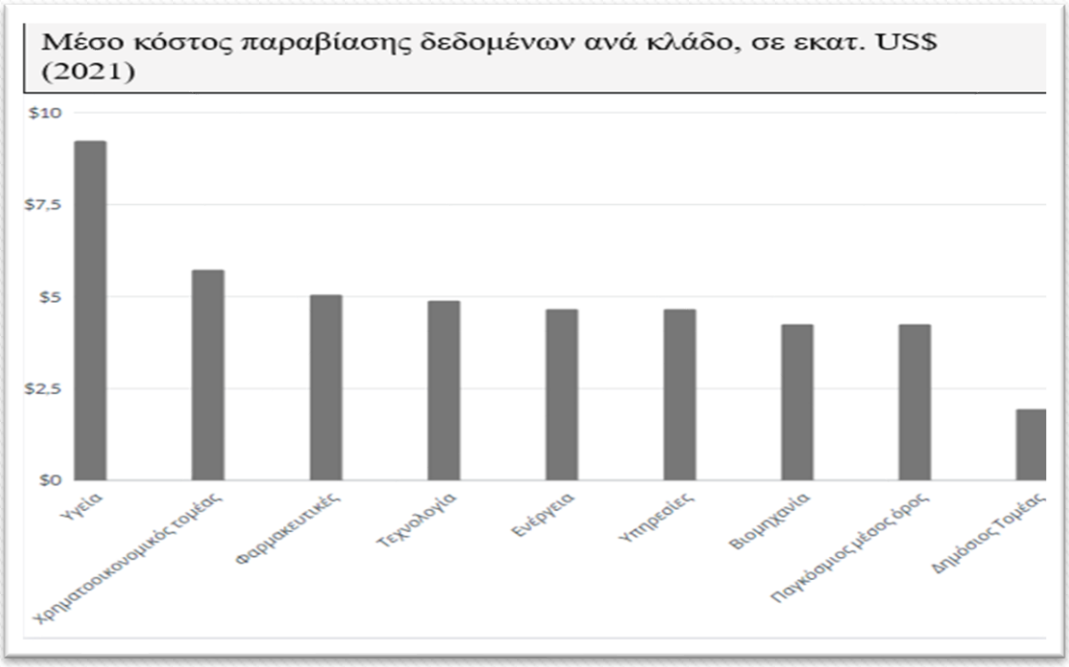
Πιο συγκεκριμένα, κάποια επιτυχημένη επίθεση στην εφοδιαστική αλυσίδα ενός νοσοκομείου, μία IoT attack, με ransomware, malware με κάποιον ιό ή σκουλήκι, είναι σίγουρο ότι θα επιφέρουν τουλάχιστον υλικές ζημιές, για την αποκατάσταση των οποίων θα χρειαστούν οικονομικοί πόροι (π.χ. επιδιόρθωση ενός μολυσμένου με malware αναλυτή αίματος ή αγορά νέου, αν δεν είναι δυνατή η επιδιόρθωσή του). Όταν ζημιώνεται δημόσιος φορέας υγείας, υπάρχει φθορά δημόσιας περιουσίας. Επίσης, στις οικονομικές επιπτώσεις υπάγονται οι χρηματικές ποινές, δηλαδή τα πρόστιμα, που επιβάλλονται στους υπευθύνους για την επεξεργασία των ιατρικών δεδομένων φορείς, λόγω της αδυναμίας προστασίας τους, σύμφωνα με τις διατάξεις του ΓΚΠΔ. Το μέγεθος των οικονομικών επιπτώσεων του κυβερνοεγκλήματος είναι τέτοιο, που υπολογίζεται ότι το κόστος του θα ανέλθει παγκοσμίως 10.5 τρισεκατ. δολάρια μέχρι το 2025 (Morgan, 2020).



Σχήμα 3: Το μέσο οικονομικό κόστος του κυβερνοεγκλήματος είναι σε διαρκή άνοδο, με το 2020, εν μέσω της πανδημίας του κορωνοϊού, να εκτινάσσεται σε 945 δις. δολάρια.

Πηγή: https://www.cobalt.io/blog/business-cost-of-cybercrime

Πέραν της συγκεκριμένης διάστασης, το οικονομικό κόστος παραβίασης των ιατρικών δεδομένων είναι πιο εκτεταμένο, διότι περιλαμβάνει επιπλέον το κόστος της αλλοίωσης, υποκλοπής και διαρροής των δεδομένων στο Διαδίκτυο από τους κυβερνοεγκληματίες. Τα παρανόμως κτηθέντα ιατρικά δεδομένα γίνονται αντικείμενο εμπορικών συναλλαγών, επειδή είχαν και έχουν τη μεγαλύτερη οικονομική αξία (Calyptix security, 2016) στο σκοτεινό Διαδίκτυο, φτάνοντας τα 499 δολάρια ανά παραβίαση το 2021 (Irwin, 2021), παράγοντας που οδήγησε άλλωστε στην κατακόρυφη αύξηση των παραβιάσεών τους εν μέσω της πανδημίας COVID-19 (Jercich, 2021). Το προηγούμενα γίνονται εμφανή στο κάτωθι γράφημα:



Σχήμα 4: Το μέσο κόστος παραβίασης δεδομένων στο χώρο της υγείας ανέρχεται σε 9,23 εκατ. δολάρια, το μεγαλύτερο με διαφορά συγκριτικά με τους άλλους τομείς παραγωγής και παροχής προϊόντων και υπηρεσιών.

Πηγή: https://www.hipaajournal.com/average-cost-of-a-healthcare-data-breach-9-42-million-2021/

Οι νομικές συνέπειες αφορούν τις ποινικές, διοικητικές και πειθαρχικές κυρώσεις, τις οποίες υφίστανται οι υπεύθυνοι ή οι εκτελώντες την επεξεργασία είτε αυτοί είναι ΝΠΔΔ, είτε ΝΠΙΔ που δραστηριοποιούνται στην Υγεία. Προκύπτουν μέσω της επιβολής ποινών από το Δικαστήριο της ΕΕ, τα εθνικά Δικαστήρια, τις κρατικές και ελεγκτικές Αρχές, όπως την ΑΠΔΠΧ, για την αδυναμία εκπλήρωσης των υποχρεώσεων απέναντι στην προστασία της ασφάλειας των πληροφοριακών συστημάτων, όπως αυτές προβλέπονται στην

ισχύουσα νομοθεσία, με συνέπεια την προσβολή της ιδιωτικότητας των χρηστών υπηρεσιών υγείας. Π.χ. Η μη ενημέρωση της ΑΠΔΠΧ ή και των υποκειμένων των δεδομένων για περιστατικό παραβίασης των δεδομένων τους επισύρει ποινή.

Οι κοινωνικές συνέπειες είναι οι θέσεις εργασίας του υπευθύνου προσωπικού, που πιθανόν χάθηκαν εξαιτίας της παραβίασης, η δημιουργία κλίματος φόβου κι ανασφάλειας στους πολίτες ότι το σύστημα υγείας, από το οποίο εξαρτώνται, είναι εκτεθειμένο στους κινδύνους των κυβερνοαπειλών, αδυνατεί να τους εξυπηρετήσει και να προστατέψει τα π.δ τους.

Οι χειρότερες όλων των συνεπειών από τις κυβερνοαπειλές στον τομέα της υγείας είναι οι συνέπειες στον ανθρώπινο παράγοντα. Εκτός του ότι συνιστούν τα βαρύτερα κακουργήματα, οι επιθέσεις αυτές φέρουν τη μεγαλύτερη ηθικοκοινωνική απαξία, καθότι οι επιτιθέμενοι χρησιμοποιούν τις ανθρώπινες ζωές των ασθενών ως οχήματα επίτευξης των σκοπών τους. Κυβερνεπιθέσεις μέσω του IoT, στην εφοδιαστική αλυσίδα, επιθέσεις με ransomware και malware μπορούν να προκαλέσουν στους εξαρτώμενους από τα συστήματα υγείας ασθενείς μόνιμες οργανικές βλάβες, αναπηρίες, διακινδύνευση της ζωής τους, ακόμη και τον θάνατο. Κι αυτό διότι το χακάρισμα του ιατροτεχνολογικού εξοπλισμού, που συνδέεται σε κάποιο δίκτυο ή το IoT, είναι δυνατόν να επιφέρει από τη δυσλειτουργία μέχρι την παράλυση ενός νοσοκομείου, με θανάσιμα επακόλουθα στους ασθενείς. Για παράδειγμα, ενδέχεται να αποκτηθεί μη εξουσιοδοτημένη απομακρυσμένη πρόσβαση σε ένα ρομποτικό μηχάνημα χειρουργικών επεμβάσεων που λειτουργεί μέσω του IoT, να διακοπεί τελείως η λειτουργία ενός αναλυτή αίματος, μαγνητικού ή και αξονικού τομογράφου, καρδιογράφου, βηματοδότη, μιας συσκευής παροχής οξυγόνου, κλπ. Επιπλέον, η στέρηση της πρόσβασης του υγειονομικού προσωπικού στους ΑΗΦΥ των ασθενών, λόγω π.χ. κάποιας επίθεσης με ransomware, συνεπάγεται την αδυναμία των γιατρών και των νοσηλευτών να εξετάσουν κρίσιμα ιατρικά δεδομένα, τα οποία οφείλουν να λαμβάνουν υπόψη τους. Έτσι, δημιουργούνται σημαντικά εμπόδια στην ιατρική επιστήμη, με αποτέλεσμα μέχρι τη διακινδύνευση της ζωής των ασθενών. Μια άλλη συνέπεια, που δεν θα πρέπει να παραβλέπεται, η οποία έχει τονιστεί αρκετά υπό το πρίσμα της παραβίασης των ιατρικών δεδομένων, είναι η προσβολή της στοιχειώδους ατομικής ελευθερίας της ιδιωτικότητας των ατόμων. Μ’ άλλα λόγια, θίγεται η προσωπική ζωή και τα ατομικά δικαίωμα στην ελευθερία των ατόμων, όποτε παραβιάζονται τα ιατρικά τους δεδομένα.

Επίσης, στις διάφορες συνέπειες περιλαμβάνεται το πολιτικό κόστος για την εκάστοτε κυβέρνηση λόγω της δυσαρέσκειας –ακόμη και της οργής– των πολιτών ενός κράτους, γιατί αυτή απέτυχε να προστατεύσει έναν τόσο ευαίσθητο τομέα όπως η Υγεία, γιατί καταστράφηκε δημόσια περιουσία, χάθηκαν ανθρώπινες ζωές κλπ. Άρα, τελικά ίσως προκύπτει απώλεια λαϊκής εμπιστοσύνης προς την κυβέρνηση. Περιλαμβάνεται, τέλος, το χρονικό διάστημα που πρέπει να μεσολαβήσει έως ότου αποκατασταθεί, μερικώς ή πλήρως, η εύρυθμη λειτουργία των φορέων υγείας από μια κυβερνοεπίθεση, το οποίο μπορεί να είναι μακρό.

4.2. Σημαντικά συμβάντα κυβερνοεπιθέσεων σε συστήματα υγείας

Στο σημείο αυτό, για την επιβεβαίωση των προαναφερθέντων, είναι εποικοδομητική η συμπερίληψη πραγματικών κυβερνοεπιθέσεων, που έχουν λάβει χώρα κατά οργανισμών της δημόσιας διοίκησης και των συστημάτων υγείας. Μυριάδες κυβερνοεπιθέσεις έχουν συμβεί και συμβαίνουν στα νοσοκομεία διαφόρων χωρών του κόσμου, τα περισσότερα εξ αυτών στις ΗΠΑ (Ghafur & Grass, 2019) και των ευρωπαϊκών κρατών, προκαλώντας τους πολλές από τις επιπτώσεις που εκτέθηκαν, δηλαδή σοβαρές δυσλειτουργίες και ζημιές. Όμως, επιλέχθηκαν να αναλυθούν οι κάτωθι δύο, πασίγνωστες στα χρονικά για το πρωτοφανές της έκτασης και έντασης των συνεπειών τους στη γεωγραφική περιοχή της Ευρώπης, όπως και για τα διδάγματα κυβερνοασφάλειας, τα οποία αντλήθηκαν από την αντιμετώπισή τους.

4.2.1. Το WannaCry ransomware στο NHS της Αγγλίας

Τον Μάιο του 2017, έγινε παγκοσμίως αντιληπτό ότι μία κυβερνοεπίθεση πλανητικής εμβέλειας, εκμεταλλευόμενη μία ευπάθεια στο λογισμικό των Windows της Microsoft, είχε πλήξει με ransomware 250.000 υπολογιστές σε 150 χώρες του κόσμου. Αν και οι επιτιθέμενοι, κατ’ αρχήν, δεν στόχευαν κατευθείαν το NHS της Αγγλίας, καθότι θύματά της έπεσαν αρκετές εταιρείες και κράτη, ήταν αυτό που δέχτηκε μακράν το μεγαλύτερο πλήγμα (Ghafur & Grass, 2019). Υπολογίζεται ότι το 40% των υγειονομικών οργανισμών της Αγγλίας και το 60% των ψηφιακών συστημάτων της βιομηχανίας μολύνθηκαν με τον ιό του ransomware μέχρι το 2019 (Landi, 2019), από τους οποίους απαιτήθηκαν λύτρα. Τα αποτελέσματά τους ήταν η κρυπτογράφηση των ηλεκτρονικών τους αρχείων και δεδομένων, ο αποκλεισμός της πρόσβασης του ιατρονοσηλευτικού προσωπικού στους

ΑΗΦΥ των ασθενών, η διακοπή παροχής υπηρεσιών των μολυσμένων με το malware νοσοκομείων, εξαιτίας της διακοπής λειτουργίας του συνδεδεμένου στα δίκτυα εξοπλισμού, και η αναβολή των προγραμματισμένων επισκέψεων εξέτασης των ασθενών. Η απόκριση του NHS ήταν καλή και έγκαιρη, αποτρέποντας τα χειρότερα για την υγεία των εξαρτώμενων από το NHS ατόμων και προστατεύοντας τα ιατρικά δεδομένα των ασθενών, αφού δεν υπήρχαν αναφορές παραβίασης-διαρροής π.δ (Smart, 2018). Πάρα ταύτα, το ransomware WannaCry δεν παύει έως σήμερα να αποτελεί ένα πρωτόγνωρο περιστατικό ασφαλείας στα χρονικά των κυβερνοεπιθέσεων σε νοσοκομεία.

4.2.2. Το ransomware στο νοσοκομείο του Düsseldorf

Το Πανεπιστημιακό Νοσοκομείο του Düsseldorf στη Γερμανία έπεσε θύμα άλλης μιας επίθεσης με ransomware (Silomon, 2020). Εκτός των άλλων παρόμοιων προβλημάτων με το NHS, για πρώτη φορά στην ιστορία των κυβερνοεπιθέσεων στα συστήματα υγείας, η συγκεκριμένη επίθεση συσχετίζεται αιτιολογικά με τον θάνατο ασθενούς (Silomon, 2020). Η γυναίκα ήταν αδύνατο να λάβει την κατεπείγουσα ιατρική περίθαλψη που χρειαζόταν στο Düsseldorf, όπου είχε σπεύσει, κι έτσι μεταφέρθηκε στο κοντινότερο νοσοκομείο με μία ώρα καθυστέρηση, κάτι που τελικά αποδείχτηκε θανάσιμο για εκείνη. Αυτό οφείλεται στο γεγονός ότι ο ιατρικός εξοπλισμός, ο οποίος ήταν συνδεδεμένος με τα πληροφοριακά συστήματα και δίκτυα του νοσοκομείου, είχε τεθεί εκτός λειτουργίας, εξαιτίας του ransomware. Επίσης, η πρόσβαση στους ΑΗΦΥ και τα ιατρικά δεδομένα στα ηλεκτρονικά αρχεία ήταν αποκομμένη για το προσωπικό, για τον ίδιο λόγο –την παραβίαση της ασφάλειας από το ransomware. Τα email, οι τηλεπικοινωνίες και όλες οι ΤΠΕ του νοσοκομείου είχαν παραλύσει, ενώ η αποκατάστασή τους διήρκησε αρκετό διάστημα. Επομένως, αποδείχτηκε ότι η κυβερνοασφάλεια του νοσοκομείου δεν ήταν στο αυξημένο επίπεδο που θεωρούταν, ήταν διάτρητη (Silomon, 2020).

4.3. Ο αντίκτυπος της πανδημίας COVID-19 στις κυβερνοαπειλές στο χώρο της υγείας

Από το ξέσπασμα της πανδημίας του κορωνοϊού (COVID-19), πολλοί πάροχοι υπηρεσιών υγείας έχουν πέσει θύματα συντονισμένων και σύνθετων κυβερνοεπιθέσεων (Muthuppalaniappan & Stevenson, 2020). Με περισσότερο προσωπικό να εργάζεται εξ

αποστάσεως, τη λειτουργία μαζικών σημείων τεστ και εμβολιασμών και την εκρηκτική χρήση της τηλεϊατρικής, πολλά συστήματα υγείας παρακολούθησαν τις άμυνές τους ενάντια της έκθεσης των π.δ των ασθενών να καταρρέουν (Culbertson, 2021). Παράλληλα, δεχόντουσαν αιτήματα του Τύπου και του κοινού να μοιραστούν μαζί τους πληροφορίες σχετικές με την πανδημία.

Οι κυβερνοεγκληματίες επιχείρησαν να αποσπάσουν επιστημονικά στοιχεία, που σχετίζονται με ερευνητικές θεραπείες και ιατρικές στατιστικές, ή να παραβιάσουν τα ιατρικά δεδομένα που φυλάσσονται στα ηλεκτρονικά αρχεία. Κατά τη διάρκεια της έντονης, ούτως ή άλλως, αυτής περιόδου, επιχείρησαν να εκμεταλλευτούν οποιαδήποτε ευπάθεια των πληροφοριακών συστημάτων της υγείας, την ίδια ώρα που ο κλάδος πασχίζει να αντέξει την ασφυκτική πίεση των διογκωμένων αναγκών του πληθυσμού για ιατροφαρμακευτική περίθαλψη. Οι αυξημένες αυτές ανάγκες δεν αποδίδονται αλλού, παρά στον υψηλό αριθμό περιστατικών με βαρύτερη νόσηση από κορωνοϊό. Η παρατήρηση του εν λόγω αυξημένου δείκτη κυβερνοαπειλών, φτάνοντας +60% το 2020 συγκριτικά με το 2019 (Culbertson, 2021), σημαίνει ότι προστέθηκαν περαιτέρω περίπλοκα προβλήματα στους οργανισμούς υγείας, πέραν της διασφάλισης της επάρκειας κι αποτελεσματικότητας των υγειονομικών τους δυνατοτήτων. Τη μεγαλύτερη ποσοστιαία μεταβολή για τον τομέα της υγείας, κάνοντας πολύ έντονη την εμφάνισή τους για πρώτη φορά, μαζί με το malware και ransomware, σημείωσαν οι επιθέσεις στο IoT και οι επιθέσεις στην εφοδιαστική αλυσίδα (Deloitte, 2020)

Γίνεται εύκολα κατανοητό, λοιπόν, ότι οι κυβερνοαπειλές, που γεννήθηκαν λόγω της πανδημίας, έχουν επιφέρει περαιτέρω εκτεταμένη διαταραχή στην ήδη επιβαρυμένη βιομηχανία της υγείας. Μάλιστα, στόχους τους αποτελούν πλέον όχι μόνο τα νοσοκομεία, αλλά και πολλά από τα ακαδημαϊκά ιδρύματα που δραστηριοποιούνται στο χώρο (Muthuppalaniappan & Stevenson, 2020).

Προς ενίσχυση του επιχειρήματος, ούτε ο ΠΟΥ κατάφερε να μείνει απρόσβλητος από την έξαρση των κυβερνοεπιθέσεων, την ίδια περίοδο. Το 2020, στην καρδιά της πανδημίας, επίσημες αναφορές έκαναν λόγο για πενταπλασιασμό των κυβερνοεπιθέσεων από επιτήδειους κατά του ΠΟΥ ή το ευρύ κοινό, χρησιμοποιώντας το όνομα του Οργανισμού (ΠΟΥ, 2020). Άγνωστοι χάκερ παραβίασαν με phishing επίθεση τα ηλεκτρονικά διαπιστευτήρια (όνομα χρήστη, κωδικό πρόσβασης) αρκετών λογαριασμών του προσωπικού

του για να αποσπάσουν εμπιστευτικά αρχεία. Ακόμη, προσποιούμενοι στελέχη του ΠΟΥ, έστελναν από τους παραβιασμένους λογαριασμούς προσωποποιημένα phishing emails, προτρέποντας τους παραλήπτες τους να καταθέσουν δωρεές σε υποτιθέμενους τραπεζικούς λογαριασμούς του ΠΟΥ για την καταπολέμηση της πανδημίας, πίσω από τους οποίους φυσικά κρύβονταν εκείνοι. Ευτυχώς, η απάτη δεν έλαβε σημαντικές διαστάσεις, διότι τα σημαντικά αρχεία φυλάσσονταν σε πιο σύγχρονα, ασφαλέστερα λειτουργικά συστήματα και αντικαταστάθηκαν γρήγορα. Ωστόσο, τα πράγματα θα μπορούσαν να είχαν εξελιχθεί πολύ χειρότερα.

5. Αντιμετώπιση των σύγχρονων απειλών στην υγεία

Οι κυβερνοαπειλές κατά των ψηφιακών συστημάτων, δικτύων και υποδομών δεν είναι χωρίς αντίδοτο. Για τον περιορισμό και την εξάλειψη των σοβαρότατων επιπτώσεών τους, υφίστανται η δέουσα πολιτική ασφαλείας και τα ενδεδειγμένα μέτρα προστασίας, τα οποία αποσκοπούν κυρίως στην πρόληψη. Εφόσον όμως αυτό δεν καταστεί εφικτό, υπάρχει τρόπος της εκ των υστέρων κατασταλτικής αντιμετώπισης, ώστε ο οργανισμός να συνεχίσει τη λειτουργία του (ανθεκτικότητα), υφιστάμενος όσο το δυνατόν μικρότερες επιπτώσεις. Οι βασικές αρχές και τα πρότυπα κυβερνοασφαλείας, τα οποία πρέπει να εφαρμόζονται, είναι κοινά για όλους τους οργανισμούς, βέβαια κρίνεται απαραίτητη η προσαρμογή τους στα δεδομένα του εκάστοτε φορέα. Η ακόλουθη ανάλυση εντάσσεται στο πνεύμα αυτό. Παράλληλα, συγκεκριμενοποιείται στα συστήματα υγείας, επειδή, λόγω των ιδιαιτεροτήτων του χώρου, υπάρχει ανάγκη σχεδίασης και εφαρμογής ειδικότερων και επιπρόσθετων μέτρων προστασίας των αγαθών και των πόρων τους (εμπιστευτικότητα, ακεραιότητα, διαθεσιμότητα, ανθεκτικότητα).

5.1. Πολιτική ασφαλείας, μέτρα προστασίας και αντιμετώπισης

Η επίτευξη του παραπάνω κομβικού ζητουμένου σημαίνει ότι, πρωτίστως, έχει αναπτυχθεί μία ολοκληρωμένη πολιτική ασφαλείας, μαζί με ένα Σχέδιο Ασφαλείας. Η πολιτική ασφαλείας είναι ένα δεσμευτικό έγγραφο, εγκεκριμένο από την εκάστοτε Διοίκηση. Περιγράφει και καθορίζει με λεπτομέρεια τα τεχνικά, οργανωτικά και λοιπά μέτρα ασφαλείας που έχουν ληφθεί και πρόκειται να ενεργοποιηθούν, τις διαδικασίες που πρέπει να ακολουθηθούν, τους ρόλους και τα καθήκοντα του προσωπικού, στην περίπτωση που προκύψει έκτακτο περιστατικό ασφαλείας. Αντίγραφο του εγγράφου αυτού φυλάσσεται, δε, σε ειδικό προστατευμένο σημείο εντός των εγκαταστάσεων του οργανισμού, ώστε να είναι διαθέσιμο εάν χρειαστεί.

Αρχικά, προϋπόθεση για τον προσδιορισμό των μέτρων ασφαλείας είναι η εκπόνηση της ανάλυσης επικινδυνότητας (Risk Analysis) και της μελέτης επιχειρηματικών επιπτώσεων-αντικτύπου (Business Impact Assessment). Στόχος είναι να προσδιοριστεί το απαιτούμενο επίπεδο ασφαλείας, σε συνάρτηση με το αποδεκτό επίπεδο κινδύνου, δεδομένου ότι εφικτή είναι μόνο η ελαχιστοποίηση του κινδύνου και όχι η εξάλειψή του σε

πραγματικές συνθήκες (Εθνική Σχολή Δημόσιας Διοίκησης, 2021). Η ανάλυση επικινδυνότητας αποτυπώνει το είδος και την ένταση του κίνδυνου που διατρέχουν οι πόροι του οργανισμού, ενώ η μελέτη αντικτύπου προσδιορίζει τις πιθανές επιπτώσεις στους πόρους από μελλοντικές κυβερνοεπιθέσεις. Έπεται η επιλογή των κατάλληλων τεχνικών μέτρων, τα οποία περιλαμβάνουν την εγκατάσταση σύγχρονου υλικοτεχνικού εξοπλισμού ή την αναβάθμιση του υφιστάμενου, την κρυπτογράφηση των πληροφοριών που φυλάσσονται και ανταλλάσσονται μέσω των λειτουργικών συστημάτων του, την εγκατάσταση ενημερωμένων προγραμμάτων αντι-ιομορφικού λογισμικού σε κάθε υπολογιστή του δικτύου, την τήρηση αντιγράφων ασφαλείας των σημαντικών δεδομένων. Ο συνδυασμός της πολιτικής ασφαλείας με τα μέτρα ασφαλείας, ή αντίμετρα, αποτελεί το Σχέδιο Ασφαλείας των οργανισμών (Εθνική Σχολή Δημόσιας Διοίκησης, 2021).

Μονάχα η ύπαρξη των ανωτέρω τεχνικών μέτρων ασφαλείας δεν επαρκεί, για να αποτρέψει τον περιορισμό των βασικών απαιτήσεων ασφαλείας από ενδεχόμενες κακόβουλες ενέργειες (Εθνική Σχολή Δημόσιας Διοίκησης, 2021). Σε δεύτερο επίπεδο, δέουσα προσοχή θα πρέπει συμπληρωματικά να δίνεται στην τήρηση των κατάλληλων οργανωτικών-διαδικαστικών μέτρων, καθότι αυτά είναι εξίσου, αν όχι περισσότερο, σημαντικά με τα τεχνικά ως προς την ανάπτυξη μιας ολιστικής κι αποτελεσματικής πολιτικής ασφαλείας. Οι διαδικασίες περιλαμβάνουν αρκετά στοιχεία: ένα πρόγραμμα ευαισθητοποίησης, ενημέρωσης και επιμόρφωσης του προσωπικού, την επαρκή στελέχωση του φορέα με το κατάλληλο προσωπικό στη Μονάδα Πληροφορικής και την ανάθεση ρόλων κι αρμοδιοτήτων στα αντίστοιχα πρόσωπα.

Για τους μεγάλους οργανισμούς υγείας, όπως τα νοσοκομεία και τις ιδιωτικές κλινικές, εκτός από την αρμόδια Μονάδα Πληροφορικής, επιβάλλεται να υπάρχει η θέση Υπευθύνου Ασφαλείας (CISO), διαχειριστές πληροφοριακών συστημάτων, εθνικό CERT, αρμόδια CSIRT και DPO για τη στοχευμένη προστασία των ιατρικών δεδομένων. Μάλιστα, όπως τονίστηκε, τα αρχεία αυτά χρήζουν εξαιρετικά υψηλής προστασίας, διότι περιέχουν απόρρητα ιατρικά δεδομένα. Επομένως, επειδή η παραβίασή τους πρέπει οπωσδήποτε να αποτρέπεται, ή αν παραβιαστούν πρέπει να ανακτηθούν, πρέπει να τηρούνται αντίγραφα ασφαλείας τους, που να είναι ενημερωμένα. Συνολικά, σε διαδικασιακό, νομικό και τεχνολογικό επίπεδο, αν πληρούνται σωρευτικά οι ακόλουθες προδιαγραφές του Σχεδίου Ασφαλείας ως προς τις διαδικασίες και τα μέτρα ασφαλείας, τα συστήματα υγείας

πληρούν τις απαραίτητες κατηγορίες απαιτήσεων ασφαλείας, οπότε μπορούν να αξιολογηθούν ως «θωρακισμένα» (Εθνική Σχολή Δημόσιας Διοίκησης, 2021).

- Κανονιστική συμμόρφωση με την ισχύουσα νομοθεσία.
- Δημιουργία της δέουσας οργανωτικής δομής, με ορισμό ρόλων και εκχώρηση αρμοδιοτήτων, δίνοντας κυρίαρχο ρόλο στον CISO κι έπειτα στην Επιτροπή Εποπτείας κι Ελέγχου.
- Διαχείριση του προσωπικού με ευαισθητοποίηση και επιμόρφωση στα θέματα κυβερνοασφάλειας. Ένα παράδειγμα είναι τα διαπιστευτήρια των λογαριασμών εξουσιοδοτημένων χρηστών να μην αφήνονται εκτεθειμένα σε κοινή θέα (σελίδα χαρτί πάνω στο γραφείο).
- Διαχείριση της πολιτικής ασφαλείας, με τον συντονισμό των εμπλεκομένων και τακτικούς ελέγχους από τη Μονάδα Πληροφορικής, τον CISO και την Επιτροπή.
- Έλεγχος πρόσβασης στους εξουσιοδιοτημένους χρήστες, σύμφωνα με την αρχή του ελαχίστου προνομίου, όπου στον καθένα δίνεται πρόσβαση από τους διαχειριστές μόνο στους απαιτούμενους για την εκτέλεση των καθηκόντων του πόρους.
- Προσεκτική διαχείριση αλλαγών λογισμικού υπό την εποπτεία της μονάδας Πληροφορικής ή και του CISO και ξεχωριστή μέριμνα για τη δημιουργία αντιγράφων ασφαλείας των δεδομένων.
- Φυσική ασφάλεια της υλικοτεχνικής υποδομής, με την έννοια της φύλαξης των εγκαταστάσεων.
- Σχέδιο Συνέχισης Λειτουργίας για έκτακτα περιστατικά, για το οποίο γίνεται λόγος στη συνέχεια.

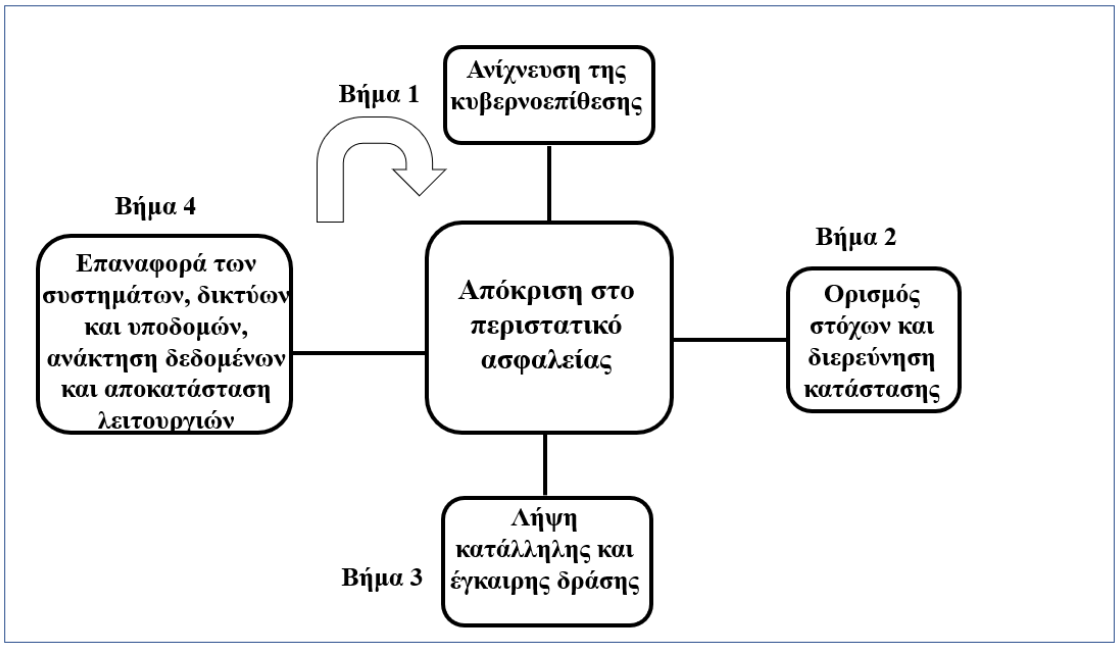
Επιπλέον δικλείδα ασφαλείας για τα συστήματα υγείας συνιστά η τήρηση ενός Συστήματος Διαχείρισης Ασφάλειας Πληροφοριών, με τρόπο ώστε αυτό να συμμορφώνεται με τα πρότυπα ISO 27000, 27001 & ειδικά το ISO 27799, το οποίο παρέχει περαιτέρω θωράκιση πληροφοριών, περιλαμβάνοντας αυστηρότερες προδιαγραφές (Tyalli & Pottas, 2010).

Υπογραμμίζεται ότι, κατά τη διάρκεια των σταδίων ανάπτυξης οποιασδήποτε ολοκληρωμένης πολιτικής ασφαλείας, πρέπει να συνυπολογίζονται οι εξής παρατηρήσεις: Η σχεδίαση μιας πολιτικής ασφαλείας είναι ένα σύνθετο και πολυδιάστατο ζήτημα, που συνεπάγεται επενδυτικό, οικονομικό, υλικό, στελεχιακό, οργανωτικό κόστος και κόστος

εργατοωρών. Προηγουμένως, μία ανάλυση κόστους-οφέλους είναι χρήσιμη, προκειμένου να σταθμιστούν οι ωφέλειες από τη θωράκιση των συστημάτων συγκριτικά με το κόστος που απαιτείται για την υιοθέτηση των προτεινόμενων μέτρων. Πάντως, ισχύει ότι όσα περισσότερα μέτρα προτίθενται να εφαρμόσουν οι φορείς υγείας, τόσο μεγαλύτερη θα είναι η επιβάρυνση, αλλά ταυτόχρονα υψηλότερο το επίπεδο ασφαλείας. Αντιστρόφως, όσο λιγότερα μέτρα υιοθετηθούν, τόσο μικρότερο θα είναι το κόστος και το επίπεδο ασφαλείας. Η Διοίκηση πρέπει να κάνει στο προσωπικό σαφή τη δέσμευσή της για την ακέραια και ενιαία τήρηση της πολιτικής ασφαλείας και να καλλιεργήσει την κουλτούρα ότι αυτή αποτελεί ένα σημαντικό ζήτημα, ύψιστης προτεραιότητας, για όλους ανεξαιρέτως τους χρήστες των πληροφοριακών συστημάτων. Η σχεδίαση, χρηματοδότηση, οργάνωση, ο συντονισμός, η εφαρμογή κι ο έλεγχος μιας ολιστικής πολιτικής ασφαλείας είναι μια δυναμικώς μεταβαλλόμενη διαδικασία. Άρα, ως τέτοια, θα πρέπει να προσαρμόζεται και να επικαιροποιείται σύμφωνα με τις τεχνολογικές, θεσμικές, οργανωσιακές εξελίξεις και την τυχόν εμπειρία αντιμετώπισης προηγουμένων περιστατικών ασφαλείας (Εθνική Αρχή Κυβερνοασφάλειας, 2020). Ακολουθώντας την προσέγγιση αυτή, ο κύκλος ζωής της Στρατηγικής Κυβερνοασφάλειας αποτυπώνεται αφαιρετικά ως εξής:

Ανάπτυξη--------> Εφαρμογή---->Αξιολόγηση---->Διαχείριση.

Όπως προαναφέρθηκε, όποια πολιτική ασφαλείας και μέτρα προστασίας κι εάν έχουν αναπτυχθεί, κανένας οργανισμός δεν είναι απρόσβλητος στις κυβερνοεπιθέσεις, πόσο μάλλον με τη συχνότητα και την πολυπλοκότητα που αυτές εμφανίζονται μετά το ξέσπασμα της πανδημίας COVID-19. Όταν προκύψει κάποια περιστατικό παραβίασης των βασικών απαιτήσεων ασφαλείας, οι φορείς υγείας θα πρέπει να είναι προετοιμασμένοι να ανταποκριθούν επιτυχώς, συνεχίζοντας τη λειτουργία τους. Προτεραιότητά τους είναι η παροχή ζωτικών υπηρεσιών προς τους ασθενείς και η προστασία των ιατρικών δεδομένων, παρά τις όποιες ζημιές υποστούν τα υπολογιστικά τους συστήματα και δίκτυα (ανθεκτικότητα). Το Σχέδιο Συνέχισης Λειτουργίας αφορά ακριβώς αυτή τη βέλτιστη απόκριση και ενεργοποιείται σε έκτακτα περιστατικά. Στην ουσία, αποτελώντας κομμάτι του Σχεδίου Ασφαλείας, έρχεται να καλύψει τα όποια κενά του και προβλέπει τις ενέργειες στις οποίες θα προβεί το προσωπικό και τις οδηγίες που θα ακολουθήσει, για να συνεχίσει, π.χ. ένα νοσοκομείο, να λειτουργεί έστω μερικώς με εναλλακτικούς τρόπους (Εθνική Σχολή Δημόσιας Διοίκησης, 2021). Στόχος είναι ο περιορισμός των ζημιών και η αποκατάσταση της λειτουργίας των πληροφοριακών συστημάτων και δικτύων σε εύθετο χρόνο.



Σχήμα 5: Τα 5 καίρια βήματα που πρέπει να ακολουθηθούν ως απόκριση σε περιστατικό παραβίασης, κατά το CREST GB.

Πηγή: (Jason Creasey and Ian Glover, CREST GB, 2013)

Το επόμενο σχήμα απεικονίζει όλες τις προληπτικές και κατασταλτικές ενέργειες, που πρέπει να ακολουθούν οι –δημόσιοι και μη– οργανισμοί, κατά το NIST (2017), ώστε να φτάσουν στο μέγιστο εφικτό επίπεδο κυβερνοασφάλειας: την ολοκληρωμένη πολιτική ασφαλείας. Είναι γενικές κατευθυντήριες γραμμές και βοηθούν στον εντοπισμό και την κάλυψη των πιθανών ευπαθειών (Nieles, Dempsey, & Pilliteri, 2017) & (Bimco, Clia, 2017). Ασφαλώς, αφορούν και τους φορείς υγείας.

Σχήμα 6: Η ολοκληρωμένη πολιτική ασφαλείας είναι μία αλυσίδα επιμέρους, αλληλεξαρτώμενων παραγόντων.

5.1.2. Αντιμετώπιση επιθέσεων στην εφοδιαστική αλυσίδα και στο IoT

Η ομαλότητα εφοδιασμού των συστημάτων υγείας, της λειτουργίας του ιατρονοσηλευτικού εξοπλισμού και των έξυπνων συσκευών, που είναι διασυνδεμένες στο Διαδίκτυο, είναι επιβεβλημένο να διασφαλίζεται. Επομένως, είναι σαφές ότι, για τους λόγους που εκτέθηκαν, οι επιθέσεις στην εφοδιαστική αλυσίδα και στο IoT των συστημάτων υγείας χρήζουν ξεχωριστής αντιμετώπισης. Οι ενέργειες και τα προτεινόμενα μέτρα προς αυτή την κατεύθυνση, κάποια από τα οποία έχουν ήδη αναφερθεί, αποτελούν κομμάτι μιας ολιστικής πολιτικής ασφαλείας, όμως γίνεται ειδικότερη καταγραφή τους.

Αναφορικά με τις επιθέσεις στην εφοδιαστική αλυσίδα, οι ενδεδειγμένοι τρόποι αντιμετώπισής τους για τον περιορισμό του κινδύνου και των ευπαθειών είναι (Cybertalk, 2021):

1. Η αγορά προμηθειών μόνο από αξιόπιστους και γνωστούς προμηθευτές. Όποτε, δε, αγοράζεται εξοπλισμός από νέους προμηθευτές, πρέπει να διεξάγεται έλεγχός τους.
2. Η διενέργεια ανάλυσης επικινδυνότητας για να διευκρινιστεί αν και κατά πόσο οι προμηθευτές και συνεργάτες των φορέων υγείας συμμορφώνονται με πρότυπα κυβερνοασφάλειας.
3. Η εφαρμογή της αρχής του ελαχίστου προνομίου.
4. Τμηματοποίηση δικτύου, δηλαδή διαχωρισμός του πληροφοριακού δικτύου σε ζώνες και εξουσιοδότηση σε αυτό ανάλογα με τις επιχειρηματικές λειτουργίες που εξυπηρετούνται.
5. Καθιέρωση honeypots.[11]
6. Αυτοματοποιημένη πρόληψη απειλών μέσω ανάθεσης ή φύλαξης κρίσιμων δεδομένων σε Κέντρα Ασφαλείας Πληροφοριών.
7. Ευαισθητοποίηση σχετικά με την ασφάλεια

[11] Το honeypot είναι ένας μηχανισμός ασφαλείας υπολογιστή που έχει ρυθμιστεί για να ανιχνεύει, να εκτρέπει ή, κατά κάποιο τρόπο, να εξουδετερώνει τις προσπάθειες μη εξουσιοδοτημένης χρήσης συστημάτων πληροφοριών και λειτουργεί ως «δόλωμα» για τους υπόπτους. Βλ. (Mokube & Adams, 2007).

8. Καθορισμός πλάνου απόκρισης σε περιστατικά ασφαλείας, καθότι η πιθανότητα περιστατικού παραβίασης παραμένει ορατή, ανεξαρτήτως της πολιτικής ασφαλείας.

Κλειδί για την αντιμετώπιση των επιθέσεων μέσω του IoT είναι ο αποκλεισμός των σημείων εισόδων των χάκερ και η θωράκιση απέναντι στα botnets, τα οποία χρησιμοποιούνται κατά κόρον για τις επιθέσεις του συγκεκριμένου είδους (Austin, 2019). Για να συμβεί αυτό, πρέπει να αναπτυχθούν ορισμένα επιπλέον ειδικά μέτρα, πέραν των υπολοίπων, ενταγμένα στην πολιτική ασφαλείας του οργανισμού. Πρώτον, πρέπει το λογισμικό των πληροφοριακών συστημάτων και δικτύων, όπως επίσης των έξυπνων συσκευών, να είναι ενημερωμένο. Δεύτερον, ενδείκνυται να ρυθμιστούν εκ νέου οι κανόνες του τείχους προστασίας (firewall) των λειτουργικών συστημάτων, τροποποιώντας τις εργοστασιακές ρυθμίσεις, για να προσαρμοστούν στα δεδομένα του οργανισμού. Τρίτον, τα αποθηκευμένα δεδομένα και οι πληροφορίες που ανταλλάσσονται μεταξύ των χρηστών των δικτύων πρέπει να είναι κρυπτογραφημένες. Τέταρτον, σημαντική είναι η απενεργοποίηση του UPnP πρωτοκόλλου[12], το οποίο μπορεί να είναι βολικό και εύχρηστο, αλλά επιτρέπει στις αρρύθμιστες συσκευές, routers και υπολογιστές του δικτύου να εντοπίζονται από τρίτους, προκαλώντας ευπάθειες. Τέλος, θα πρέπει να εξεταστεί η δημιουργία δευτερευόντων δικτύων, δυνατότητα που παρέχεται από κάποια routers, για την αύξηση της ασφάλειας των LAN και της διαδικτυακής πρόσβασης.

5.2. Τα οφέλη της κυβερνοασφάλειας για την υγεία και τη δημόσια διοίκηση

Ο σχεδιασμός και η εφαρμογή μιας ολοκληρωμένης πολιτικής ασφαλείας, σε συνδυασμό με τα μέτρα προστασίας, δεν συνιστούν απλώς σωστές θεωρητικές αρχές θωράκισης των συστημάτων υγείας απέναντι στις σύγχρονες απειλές. Αντιθέτως, αποτελούν θεμελιώδη αμυντικά εργαλεία με πρακτικό αντίκρισμα, σε ό,τι αφορά τα προσφερόμενα οφέλη τους, όχι μόνο για τους φορείς υγείας, αλλά για τη δημόσια διοίκηση συνολικότερα, η οποία έχει την αρμοδιότητα διοίκησης του δημοσίου συστήματος υγείας και της εποπτείας του ιδιωτικού.

[12] Universal Plug and Play protocol

5.2.1. Οφέλη για το χώρο της υγείας

Ξεκινώντας από το χώρο της υγείας, διαπιστώνονται πέντε καίρια σημεία όπου η ολιστική πολιτική ασφαλείας αναμένεται να έχει θετική συνεισφορά (Cyberinsiders, 2022):

1. Μειωμένος κίνδυνος ιατρικών λαθών: Ο κίνδυνος του να προκύψουν ιατρικά λάθη θα μειωθεί, επειδή τα ιατρικά δεδομένα, τα οποία συμβουλεύεται το ιατρονοσηλευτικό προσωπικό, θα είναι προστατευμένα από την όποια παραβίασή τους. Εκτός αυτού, τα δεδομένα θα είναι ταχύτερα διαθέσιμα, γιατί η υιοθέτηση προτύπων κυβερνοασφάλειας αποδεδειγμένα βελτιώνει τη γενικότερη απόδοση των πληροφοριακών συστημάτων και δικτύων.
2. Αυξημένη ασφάλεια ιατρικών δεδομένων: Λαμβάνοντας υπόψη τις νομικές υποχρεώσεις των υγειονομικών οργανισμών έναντι της προστασίας των π.δ των ασθενών, ένα ακόμη όφελος, σχετιζόμενο με το προηγούμενο, θα είναι ο υψηλότερος βαθμός προστασίας των ιατρικών δεδομένων, όπου κι αν αυτά βρίσκονται: στους ΑΗΦΥ, στις βάσεις δεδομένων τους, στο IoT, στα αρχεία κάθε υπολογιστή. Κατ' αυτόν τον τρόπο, θα ελαττωθεί παράλληλα η πιθανότητα επιβολής των αυστηρών ποινών που προβλέπονται, γιατί οι κυβερνοεπιθέσεις δεν θα πλήττουν την ασφάλεια των ψηφιακών συστημάτων.
3. Ασφαλέστερη προσαρμογή στις τεχνολογικές εξελίξεις: Συνήθως, οι νοσοκομειακές μονάδες καθυστερούν την προσαρμογή κι αναβάθμιση του εξοπλισμού, των λογισμικών, των δικτύων και των υποδομών τους στις τεχνολογικές εξελίξεις. Μεταξύ άλλων, ένα αίτιο είναι ο φόβος τους για την ανακάλυψη κάποιας ευπάθειας από τις προηγμένες απειλές του κυβερνοχώρου. Έτσι, καταλήγουν να παρουσιάζουν υστερήσεις παραγωγικότητας, αποδοτικότητας κι αποτελεσματικότητας. Οι τεχνολογίες IoT μπορούν να βοηθήσουν στην επίλυση αυτών των προβλημάτων, ωστόσο προηγουμένως πρέπει να έχει εξασφαλιστεί η θωράκισή τους ενάντια στις σύγχρονες απειλές, όφελος που προβλέπεται ότι θα επιτευχθεί χάρη στην κυβερνοασφάλεια.
4. Ταχύτερη και πιο ποιοτική υγειονομική περίθαλψη: Η παραμικρή δυσλειτουργία των υπολογιστικών συστημάτων και δικτύων των φορέων υγείας μπορεί να οδηγήσει σε σημαντικές καθυστερήσεις και προβλήματα πρόσβασης του ιατρονοσηλευτικού προσωπικού στα ηλεκτρονικά δεδομένα των ασθενών, καθώς και στην παροχή ιατρικών υπηρεσιών εν γένει. Τούτο οφείλεται, όπως τονίστηκε, στην αυξημένη διασύνδεση και εξάρτηση από τις ΤΠΕ, δηλαδή τους υπολογιστές, το

Διαδίκτυο, τα υπολογιστικά νέφη και το IoT. Προφανώς, στο ατυχές συμβάν μιας κυβερνοεπίθεσης, το φαινόμενο αυτό θα επιδεινωθεί στο πολλαπλάσιο. Επομένως, το όφελος της πολιτικής ασφαλείας από την επιτυχή αντιμετώπιση των κυβερνοαπειλών είναι η παροχή ταχύτερων και ποιοτικότερων υπηρεσιών υγείας.

5. Ασφαλέστερη λειτουργία των ιατρικών συσκευών: Βεβαίως, η ασφαλέστερη λειτουργία του ιατρικού εξοπλισμού προηγείται του αποτελέσματος του προηγούμενου οφέλους και προκύπτει επίσης μέσω του εξάλειψης και του περιορισμού των επιπτώσεων των κυβερνοαπειλών. Το ιατρονοσηλευτικό προσωπικό θα είναι σίγουρο ότι θα έχει, ανά πάση στιγμή, στη διάθεσή του ακέραιες τις ιατρικές συσκευές που χρησιμοποιεί για ιατρικές πράξεις. Επιπλέον, θα υπάρχει ασφάλεια των συστημάτων και δικτύων, με τα οποία αυτές διαλειτουργούν κι από τα οποία αλληλεξαρτώνται.

5.2.2. Οφέλη για τη δημόσια διοίκηση

Εκτός από τα δημόσια συστήματα υγείας, όπου κατέχει τον κυρίαρχο ρόλο διοίκησης-χρηματοδότησης, μέσω της άσκησης κρατικής εξουσίας, η δημόσια διοίκηση έχει επίσης αρμοδιότητες καθορισμού του ρυθμιστικού πλαισίου και της εποπτείας των ιδιωτικών κλινικών, διαγνωστικών κέντρων, εργαστηρίων και της ιδιωτικής ΠΦΥ. Η κοινωνικοοικονομική και λειτουργική σπουδαιότητα θωράκισης του υγειονομικού μηχανισμού και της διασφάλισης της ανθεκτικότητάς του ενάντια στις σύγχρονες απειλές του κυβερνοχώρου συνεπάγεται ποικίλα οφέλη για ολόκληρη τη δημόσια διοίκηση. Συνεπώς, η σημασία σχεδίασης και εφαρμογής μιας ολιστικής πολιτικής ασφαλείας έγκειται στο ότι τα οφέλη της δεν περιορίζονται μονάχα στο χώρο της υγείας, αλλά μπορεί να διαχέονται εμμέσως σε κάθε οργανισμό του Δημοσίου (Εθνική Σχολή Δημόσιας Διοίκησης, 2021).

Πρώτον, η απρόσκοπτη λειτουργία των ψηφιακών συστημάτων, που υποστηρίζουν τις επιχειρησιακές διεργασίες του Δημοσίου, συμβάλλει στην επίτευξη των στόχων και στην εδραίωση του κύρους και της εμπιστοσύνης των πολιτών, οδηγώντας στην επίτευξη των επιχειρησιακών στόχων που έχουν τεθεί εκ των προτέρων.

Δεύτερον, η τήρηση προτύπων και μέτρων ασφαλείας, χάρη στην πολιτική ασφαλείας, αυξάνουν τον βαθμό νομικής συμμόρφωσης των οργανισμών, με βάση το ισχύον νομικό πλαίσιο, βελτιώνοντας την κανονιστική τους συμμόρφωση. Προηγήθηκε ήδη αναφορά

στις δεσμευτικές διατάξεις του ΓΚΠΔ ως προς την τήρηση συγκεκριμένων μέτρων ασφαλείας από τους αποδέκτες των δικαιωμάτων των προσωπικών και ευαίσθητων π.δ. Πέραν της συμμόρφωσης με τον ΓΚΠΔ, η απόδειξη ότι ακολουθούνται τα πρότυπα ISO 27000 ή και 27001 είναι υποχρεωτική για κάποιους φορείς, ώστε να αποκτήσουν την πιστοποίηση ασφαλείας των πληροφοριακών τους συστημάτων κατά ISO.

Τρίτον, καθιερώνεται μια συλλογική κουλτούρα ασφαλείας. Η πλειοψηφία των περιστατικών παραβιάσεων προέρχεται από ανθρώπινους δρώντες (Ponemon Institute, 2012) και, παρότι οι πρακτικές κυβερνοασφάλειας των οργανισμών είναι σχετικά συνήθεις, οι εργαζόμενοί τους τις αντιμετωπίζουν περισσότερο ως κατευθυντήριες γραμμές και λιγότερο ως κανόνες (ENISA, 2017). Η καθιέρωση κουλτούρας ασφαλείας βοηθά το προσωπικό να εκπαιδευτεί πάνω στην πολιτική ασφαλείας κι έτσι να αντιληφθεί τη σπουδαιότητά της στις πραγματικές της διαστάσεις κι όχι απλώς να ενημερωθεί περί αυτής εγκυκλοπαιδικά. Το προσωπικό και όλοι οι χρήστες των ψηφιακών συστημάτων επιμορφώνονται εις βάθος και αντιλαμβάνονται ότι η πολιτική ασφαλείας και προστασίας των π.δ είναι προτεραιότητα της Διοίκησης και ότι οι υπεύθυνοι θα υποστούν τις προβλεπόμενες κυρώσεις, εάν υπάρχει παραβίασή τους. Μαθαίνουν τις διαδικασίες, τις σωστές πρακτικές, τα μέτρα προστασίας των ψηφιακών συστημάτων και τα μεταφέρουν με τη σειρά τους στους συναδέλφους τους. Έτσι, δημιουργείται μία κοινή φιλοσοφία κυβερνοασφάλειας.

Τέταρτον, προσδιορίζεται με σαφήνεια η οργανωτική δομή των οργανισμών ως προς την κυβερνοασφάλεια. Αυτό σημαίνει ότι καθορίζονται οι ρόλοι, οι αρμοδιότητες, ο τρόπος δράσης και τα καθήκοντα του προσωπικού που επωμίζεται την ευθύνη της αντιμετώπισης και διαχείρισης των περιστατικών ασφαλείας. Η σχεδίαση και η εφαρμογή της ολιστικής πολιτικής ασφαλείας καθαυτές συνιστούν απαιτητικότατο εγχείρημα, για την υλοποίηση του οποίου ο οργανισμός επιβάλλεται να έχει νωρίτερα ολοκληρώσει τις προηγούμενες ενέργειες αλλά και να τις επικαιροποιεί τακτικά στο φως των νέων εξελίξεων.

Το πέμπτο και τελευταίο όφελος της πολιτικής ασφαλείας για τη δημόσια διοίκηση είναι η συμβολή της στη βελτίωση του προγραμματισμού. Ο προγραμματισμός επεκτείνει την οργάνωση και το συντονισμό των δημοσίων οργανισμών, συνυπολογίζοντας τους πόρους τους, πέρα από τα όρια της οργανωτικής δομής και της κουλτούρας ασφαλείας, που αφορούν κυρίως το προσωπικό. Οι πόροι περιλαμβάνουν το προσωπικό, τα λογισμικά, τις

υποδομές και τις εγκαταστάσεις. Ο προσανατολισμός τους γίνεται πλέον προς την προστασία της κυβερνοσφάλειας, αποτελώντας τα μέσα με τα οποία σχεδιάζεται και υλοποιείται το Σχέδιο Ασφαλείας του οργανισμού.

6. Η κατάσταση του ελληνικού συστήματος υγείας απέναντι στις σύγχρονες απειλές

Το παρόν κεφάλαιο πραγματεύεται τη συνοπτική αποτίμηση της συνολικότερης κατάστασης του ελληνικού συστήματος υγείας, δημοσίου και ιδιωτικού, απέναντι στις σύγχρονες απειλές. Δεν αποσκοπεί στην εμπεριστατωμένη ανάλυση (assessment) των τεχνικών χαρακτηριστικών του και της εξακρίβωσης του βαθμού προετοιμασίας του κατά των κυβερνοαπειλών, καθότι κάτι τέτοιο θα υπερέβαινε τα όρια της εργασίας. Για τη διερεύνηση απαντήσεων στο ανωτέρω επίμαχο ζήτημα έγινε συλλογή ποιοτικών στοιχείων κι απόψεων, μέσω ερωτηματολογίων ανοιχτού τύπου, τα οποία παρατίθενται αυτούσια στο παράρτημα. Παράγοντες του ΕΣΥ, που υπηρετούν σε διάφορες συναφείς καίριες θέσεις, όπως Προϊστάμενοι μονάδων Πληροφορικής νοσοκομείων, του Υπουργείου Υγείας και DPO, παρείχαν χρήσιμες πληροφορίες και κατέθεσαν τις προσωπικές τους απόψεις. Δίπλα στις διαπιστώσεις που προκύπτουν, παρατίθεται η αντίστοιχη αναφορά της πηγής.

Ομοίως, απάντησαν, με τη χρήση του ίδιου μεθοδολογικού εργαλείου, παράγοντες του ελληνικού ιδιωτικού συστήματος υγείας, οι οποίοι βρίσκονται σε κρίσιμες θέσεις: υπεύθυνοι μονάδας πληροφορικής ιδιωτικών κλινικών και διαγνωστικών κέντρων, DPO, προϊστάμενοι νομικών θεμάτων σε φαρμακευτικές εταιρείες. Ωστόσο, δεν αναφέρονται ονομαστικά, επειδή θέλησαν να διατηρηθεί η ανωνυμία τους.

6.1. Επίπεδα ασφαλείας του ΕΣΥ και βαθμός νομικής συμμόρφωσης

Το ΕΣΥ είναι το ελληνικό δημόσιο σύστημα υγείας και αποτελείται από 125 δημόσια νοσοκομεία, 201 Κέντρα Υγείας, 1.487 Περιφερειακά Ιατρεία, περίπου 200 πρώην Πολυϊατρεία του ΙΚΑ στις αστικές περιοχές, συγκροτώντας το Πρωτοβάθμιο Εθνικό Δίκτυο Υγείας, καθώς και 127 Τοπικές Μονάδες Υγείας σε αστικές περιοχές, που υπάγονται στις 7 ΥΠΕ (Ναυτεμπορική, 2020). Η κεντρική διοίκησή του ασκείται από το Υπουργείο Υγείας. Εξυπηρετώντας εκατομμύρια ασθενείς ανά την επικράτεια ετησίως, με απασχολούμενο προσωπικό περίπου 79.000 άτομα, είναι η ραχοκοκαλιά του ελληνικού συστήματος υγείας κι ένα από τα σημαντικότερα τμήματα της δημόσιας διοίκησης. Οι χρήστες των πληροφοριακών συστημάτων όλων αυτών των μονάδων υγείας μπορούν, ανάλογα με τα δικαιώματα χρήσης τους, να επεξεργάζονται τα π.δ των ασθενών, έχοντας

πρόσβαση στον ΑΗΦΥ. Ακόμα, ο ιατροτεχνολογικός εξοπλισμός και οι ηλεκτρονικές συσκευές που χρησιμοποιούνται από το προσωπικό στηρίζονται, σε μεγάλο βαθμό, στα πληροφοριακά συστήματα και δίκτυα του ΕΣΥ, ώστε να ικανοποιούνται οι ανάγκες υγείας του πληθυσμού. Γι' αυτό έχει βαρύνουσα σημασία η αξιολόγηση των επιπέδων κυβερνοασφάλειας και προστασίας της ιδιωτικότητας των ασθενών, όπως επίσης του βαθμού της νομικής του συμμόρφωσης.

Το ΕΣΥ υπόκειται οριζόντια στην ισχύουσα εθνική και ενωσιακή νομοθεσία που περιγράφηκε, σε ό,τι αφορά την ασφάλεια και την ιδιωτικότητα. Η δε νομική συμμόρφωση του Υπουργείου Υγείας κρίνεται εν γένει ικανοποιητική, αν και υπάρχουν αρκετά περιθώρια βελτίωσης (Ζωγραφόπουλος, 2022). Ήταν το πρώτο Υπουργείο που εξέδωσε εγκύκλιο οδηγία συμμόρφωσης των φορέων με τον ΓΚΠΔ και κάλυψε τη θέση του DPO. Η ίδια διαπίστωση δεν ισχύει απαραιτήτως για τα πολυάριθμα νοσοκομεία και τις λοιπές μονάδες ΠΦΥ του ΕΣΥ, διότι παρουσιάζεται ετερογένεια κι ανομοιομορφία μεταξύ τους (Ζωγραφόπουλος, 2022). Δηλαδή, λόγω των διαφορετικών διαρθρωτικών τους χαρακτηριστικών, κάποιοι φορείς διαθέτουν πληρέστερη πολιτικής ασφαλείας και συμμορφώνονται καλύτερα νομικά από άλλους. Γενικότερα, πάντως, τα επίπεδα νομικής συμμόρφωσης και κυβερνοασφάλειας του ΕΣΥ χαρακτηρίζονται επαρκή, παρουσιάζοντας συνεχείς τάσεις βελτίωσης, με τα μεγάλα πληροφοριακά συστήματα να προστατεύονται καλά.

Μία σειρά βασικών μέτρων ασφαλείας πληρείται, όπως η εξουσιοδότηση χρηστών σύμφωνα με την αρχή του ελαχίστου προνομίου, η μη απομακρυσμένη πρόσβαση, η λειτουργία και αναβάθμιση προγραμμάτων αντι-ιομορφικού λογισμικού, η ενημέρωση του προσωπικού για τους κινδύνους των κυβερνοαπειλών, η προσεκτική διαχείριση αλλαγών λογισμικού, η φυσική ασφάλεια κι ο περιοδικός έλεγχος ασφάλειας των συστημάτων (Σιώζου, 2022) & (Κελεπούρης, 2022). Τα μέτρα πρόληψης και προστασίας κατά των κυβερνοαπειλών του Εγχειριδίου Κυβερνοασφάλειας 2021 τηρούνται εν μέρει, ανάλογα το νοσοκομείο, καθότι αυτό εκδόθηκε πρόσφατα μες στην πανδημία, με συνέπεια η προσαρμογή να έχει καθυστερήσει, κάτι που σταδιακά αλλάζει (Σιώζου, 2022). Ενδεικτικό αυτού είναι το γεγονός ότι η στελέχωση της θέσης του CISO ξεκίνησε μόλις πρόσφατα στα περισσότερα νοσοκομεία. Οι προσπάθειες για την εναρμόνιση με την Εθνική Στρατηγική Κυβερνασφάλειας 2020-2025 εντείνονται, αλλά υπάρχει ακόμα απόσταση να διανυθεί. Τα βήματα που πρέπει να γίνουν αφορούν περισσότερο το οργανωτικό επίπεδο (Κελεπούρης, 2022) & (Σιώζου, 2022) και αναφέρονται στη συνέχεια στις προτάσεις.

Ο κυριότεροι παράγοντες στους οποίους αποδίδονται οι όποιες ανεπάρκειες είναι οργανωτικοί και οικονομικοί (Ζωγραφόπουλος, 2022) & (Κελεπούρης, 2022). Αφορούν τις ελλείψεις εξειδικευμένου προσωπικού, τις ατελείς προσπάθειες ευαισθητοποίησης και εκπαίδευσης του υπηρετούντος στο ΕΣΥ προσωπικού και την υποχρηματοδότηση. Οι ανάγκες αντιμετώπισης της πανδημίας COVID-19 χειροτέρευσαν το πρόβλημα, δεδομένου ότι απορρόφησαν πόρους, οι οποίοι προορίζονταν για την κάλυψη των κενών ασφαλείας και την εμβάθυνση της νομικής συμμόρφωσης (Ζωγραφόπουλος, 2022) & (Σιώζου, 2022).

Επιπρόσθετα, παρουσιάζεται υστέρηση ως προς την τήρηση διεθνώς αναγνωρισμένων προτύπων για τα συστήματα διαχείρισης ασφάλειας πληροφοριών. Πολλοί φορείς του ΕΣΥ δεν διαθέτουν πιστοποιήσεις κατά ISO 27000, 27001 και του 27799, που είναι το ειδικότερο. Αυτό σηματοδοτεί τη μη συμμόρφωσή τους με τα συγκεκριμένα πρότυπα και, ενδεχομένως, την ύπαρξη κάποιων κενών στην ακολουθούμενη πολιτική ασφαλείας, μιας και η απόκτηση των συγκεκριμένων πιστοποιήσεων οδηγεί, κατά κανόνα, σε υψηλότερη θωράκιση.

Περιστατικά παραβίασης π.δ κατά του ΕΣΥ έχουν λάβει χώρα στο παρελθόν, ευτυχώς χωρίς σοβαρό αντίκτυπο. Μεταξύ άλλων, από το 2018, υπήρχαν δύο περιστατικά παραβίασης στο Υπουργείο Υγείας, που αφορούσαν δεδομένα προσωπικού χαρακτήρα που κακώς αναρτήθηκαν στο Δι@υγεια. Ανακοινώθηκαν και στην ΑΠΔΠΧ, σύμφωνα με τα οριζόμενα στο ΓΚΠΔ, η οποία δεν έδωσε συνέχεια, κρίνοντας ότι καταβλήθηκαν οι δέουσες προσπάθειες για τον περιορισμό των συνεπειών τους. Ενημερώθηκαν, επίσης, τα υποκείμενα των δεδομένων (Ζωγραφόπουλος, 2022). Επίσης, άλλο ένα περιστατικό ασφαλείας συνέβη στις αρχές του 2022, όπου έγινε κυβερνοεπίθεση με λυτρισμικό στα νοσοκομεία «Σωτηρία» και «Ασκληπιείο Βούλας». Όπως προβλέπεται, για την αντιμετώπισή του ενεργοποιήθηκαν όλες οι αρμόδιες Αρχές, η Εθνική Αρχή Κυβερνοασφάλειας, το εθνικό CERT- ΕΥΠ και η ΔΙΔΗΕ, οι οποίες διαχειρίστηκαν τα περιστατικά έγκαιρα και αποτελεσματικά, αποτρέποντας την παραβίαση προσωπικών δεδομένων και την εμφάνιση δυσλειτουργιών στα νοσοκομεία. Τα παραπάνω αποδεικνύουν ότι το ΕΣΥ δεν παύει να συνιστά έναν πρόσφορο στόχο για τους επιτιθέμενους.

6.2. Επίπεδα ασφαλείας του ιδιωτικού τομέα υγείας και βαθμός νομικής συμμόρφωσης

Ο ελληνικός ιδιωτικός τομέας υγείας είναι ιδιαιτέρως αναπτυγμένος –σε μια χώρα στην οποία συνυπάρχει με το δημόσιο σύστημα υγείας. Αποτελείται από άνω των 180 ιδιωτικών κλινικών (Υπουργείο Υγείας, 2011), εκατοντάδων διαγνωστικών κέντρων, χιλιάδων ιδιωτών γιατρών, συμβεβλημένων και μη με τον ΕΟΠΥΥ. Διευρύνοντας το πεδίο ορισμού, μπορούν να συμπεριληφθούν επίσης τα φαρμακεία και οι φαρμακευτικές εταιρείες, ενώ το ποσοστό των αναγκών υγείας που καλύπτει όλος ο μηχανισμός, ανέρχεται σε 35,2% (OECD, 2021). Αυτές οι μονάδες υγείας, εξυπηρετώντας μεγάλο όγκο ασθενών, κάνουν επίσης χρήση ιατροτεχνολογικού εξοπλισμού κι έξυπνων συσκευών, έχοντας πρόσβαση στον ΑΗΦΥ για τους αναγκαίους σκοπούς, που ορίζονται στον ΓΚΠΔ, και επεξεργάζονται ιατρικά δεδομένα μέσω των πληροφοριακών συστημάτων και δικτύων τους, από τα οποία εξαρτώνται. Άρα, η αποτίμηση της κατάστασης των επιπέδων κυβερνοασφάλειας και προστασίας της ιδιωτικότητας των ασθενών, καθώς και η εκτίμηση του βαθμού της συμμόρφωσής τους στην ισχύουσα νομοθεσία, είναι αντίστοιχα αναγκαία με αυτή του ΕΣΥ.

Κατ’ αρχάς, το ιδιωτικό σύστημα υγείας υπόκειται στην ίδια νομοθεσία και τις ίδιες εποπτικές Αρχές με το ΕΣΥ, με ό,τι αυτό συνεπάγεται για την τήρηση των υποχρεώσεών του υπέρ της ασφάλειας των πληροφοριακών του συστημάτων και της ιδιωτικότητας των ασθενών. Έτσι, σε κάποιο περιστατικό παραβίασης των ηλεκτρονικών αρχείων μιας ιδιωτικής κλινικής, πρέπει να ενημερώνεται η ΑΠΔΠΧ κι έπειτα, κατά περίπτωση, τα υποκείμενα των δεδομένων (ασθενείς). Η νομική συμμόρφωση του ιδιωτικού συστήματος υγείας είναι, γενικά, μέτρια και βελτιώνεται σταθερά, ιδίως μετά τη θέση σε ισχύ του ΓΚΠΔ, όμως απέχει από το να χαρακτηριστεί πλήρης. Ένας λόγος είναι ότι δεν υπάρχει ο δέον αριθμός υπευθύνων επεξεργασίας και DPO, αναλογικά με το μεγάλο πλήθος και μέγεθος των φορέων. Οι ρόλοι αυτοί λειτουργούν αποκεντρωμένα, δίνοντας οδηγίες και κατευθύνσεις προς τα κατώτερα ιεραρχικά επίπεδα.

Ως προς την πολιτική ασφαλείας, εμφανίζεται η ίδια διαπίστωση με το ΕΣΥ. Οι συνεντευξιαζόμενοι τονίζουν τη σημαντική ετερογένεια και ανομοιομορφία στην πολιτική ασφαλείας και τα μέτρα προστασίας, που έχουν αναπτυχθεί στους φορείς, επειδή αυτό

εξαρτάται από την πολιτική της εκάστοτε Διοίκησης και το οικονομικό-επενδυτικό κόστος. Δηλαδή, ορισμένοι φορείς θέτουν σε υψηλότερη προτεραιότητα την πολιτική ασφαλείας, καταβάλλοντας πιο αυξημένο οικονομικό και στελεχιακό κόστος, ενώ άλλοι δεν της αποδίδουν την ίδια σημασία, με αποτέλεσμα να κινούνται σε χαμηλότερα επίπεδα ασφαλείας και να είναι περισσότερο εκτιθέμενοι απέναντι στις κυβερνοαπειλές. Βέβαια, βασικές πρακτικές ασφαλείας εφαρμόζονται στην πλειονότητα των φαρμακευτικών εταιρειών, των ιδιωτικών κλινικών και των διαγνωστικών κέντρων. Σ' αυτές ανήκουν τα επιμορφωτικά σεμινάρια του προσωπικού για την ιδιωτικότητα και τον ΓΚΠΔ, ο καθορισμός ρόλων, οδηγίες σε email για τις επιθέσεις phishing και ransomware, περιστασιακοί έλεγχοι ασφαλείας, εγκατάσταση και ενημέρωση προγραμμάτων αντι-ιομορφικού λογισμικού, η αρχή του ελάχιστου προνομίου στην πρόσβαση του ιατροτεχνολογικού εξοπλισμού και των υπολογιστικών δικτύων, η φυσική ασφάλεια, ο συντονισμός του προσωπικού υπό τις οδηγίες της μονάδας Πληροφορικής. Σημαντική υστέρηση παρουσιάζεται κι εδώ στην τήρηση αναγνωρισμένων διεθνών προτύπων για τη διαχείριση της ασφάλειας πληροφοριών, την πιστοποίηση κατά ISO 2700, 27001 και της πιο αυστηρής ISO 27799 για την υγεία. Πολλοί φορείς δεν διαθέτουν τις συγκεκριμένες πιστοποιήσεις, άρα δεν συμμορφώνονται με τα σχετικά πρότυπα ασφαλείας. Τέλος, αναφέρεται ότι μέχρι στιγμής περιστατικό παραβίασης με σημαντικό αντίκτυπο στην ασφάλεια διαγνωστικού κέντρου, ιδιωτικής κλινικής ή φαρμακευτικής εταιρείας δεν έχει προκύψει.

7. Συμπεράσματα, προτάσεις προς βελτίωση

Η ασφάλεια των πληροφοριακών συστημάτων πλήττεται, όταν πλήττεται τουλάχιστον μία από τις τρεις βασικές απαιτήσεις ασφαλείας τους, δηλαδή η ακεραιότητα, η εμπιστευτικότητα ή και η διαθεσιμότητα. Ειδικά για τα συστήματα υγείας, πολύ σημαντική είναι επιπλέον η διασφάλιση της ανθεκτικότητας.

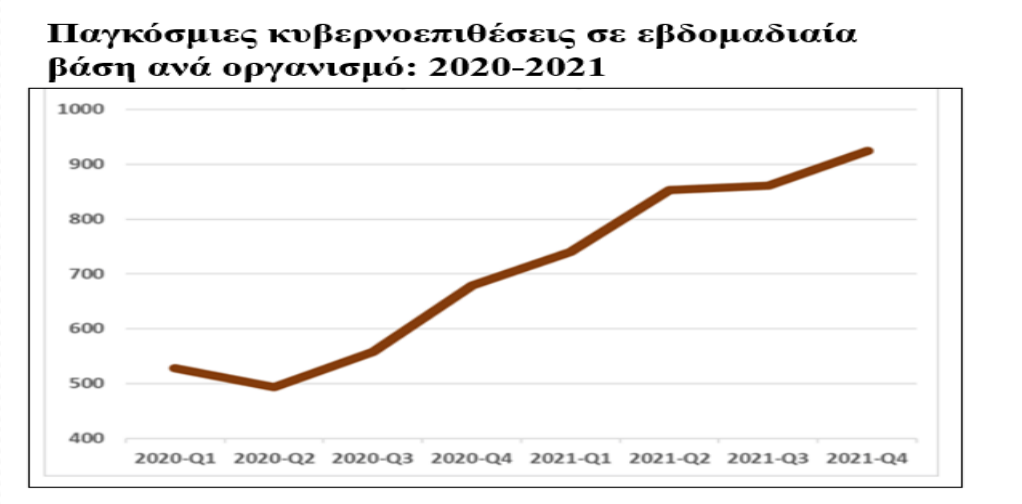
Πλέον είναι σε ισχύ η κατάλληλη νομοθεσία κατά του κυβερνοεγκλήματος σε εθνικό και ευρωπαϊκό επίπεδο, με κυρίαρχο τον ΓΚΠΔ, η οποία κατοχυρώνει θεσμικά τα π.δ των πολιτών-ασθενών και προστατεύει την ασφάλεια των ψηφιακών συστημάτων. Το νομικό πλαίσιο για την προστασία της ασφάλειας και της ιδιωτικότητας στην υγεία είναι ενιαίο, εφαρμόζεται κατά περίπτωση και δεσμεύει τους αποδέκτες των δεδομένων με υποχρεώσεις τήρησης συγκεκριμένων μέτρων ασφαλείας. Υπάρχουν αρμόδιοι δημόσιοι φορείς και Αρχές που ελέγχουν την τήρηση και εφαρμογή της σχετικής νομοθεσίας, επιβάλλουν κυρώσεις στους παραβάτες, ασκούν συμβουλευτικό ρόλο και βοηθούν στην αντιμετώπιση των κυβερνοαπειλών. Τα εθνικά και ευρωπαϊκά δικαστήρια, ο ENISA, η Εθνική Αρχή Κυβερνοασφάλειας, το εθνικό CERT-ΕΥΠ, η ΔΙΔΗΕ και η ΑΠΔΠΧ είναι οι σημαντικότεροι εξ αυτών.

Οι σύγχρονες απειλές κατά της ασφάλειας και προστασίας της ιδιωτικότητας αγγίζουν όλους τους οργανισμούς, δημόσιους και ιδιωτικούς, πλήττουν δε βαρύτερα το χώρο της υγείας. Η ταξινόμησή τους γίνεται σε εξωτερικές και εσωτερικές, σύμφωνα με την προέλευση της απειλής από το εξωτερικό ή το εσωτερικό περιβάλλον, χωρίς αυτό να είναι απόλυτο, καθότι υπάρχουν σχέσεις αλληλοεπηρεασμού τους. Οι κυριότερες περιλαμβάνουν το malware, το ransomware, τις επιθέσεις στην εφοδιαστική αλυσίδα, στο IoT, το phishing και τις επιθέσεις DoS και DDoS, ενώ οι εσωτερικές τις κακόβουλες ενέργειες από εργαζόμενους, τα ανθρώπινα λάθη από άγνοια, ατυχή χρήση ή αμέλεια και την απώλεια ή κλοπή των διαπιστευτηρίων εξουσιοδοτημένων λογαριασμών. Οι κυβερνοαπειλές αλληλοεπηρεάζονται και μπορούν να πλήξουν τόσο την ασφάλεια, όσο και την ιδιωτικότητα, δεδομένου ότι η παραβίαση μιας βασικής απαίτησης ασφαλείας εύκολα οδηγεί στην παραβίαση της εμπιστευτικότητας, άρα την παραβίαση των ιατρικών δεδομένων.

Οι επιπτώσεις των κυβερνοεπιθέσεων στα συστήματα υγείας, σε νοσοκομεία και ιδιωτικές κλινικές, είναι οι βαρύτερες από οποιονδήποτε άλλο τομέα της δημόσιας διοίκησης

ή οικονομικής δραστηριότητας, λόγω της ιδιαιτερότητάς τους και της τεράστιας εξάρτησης από τις ΤΠΕ (π.χ ηλεκτρονικά αρχεία, τηλεϊατρική, απομακρυσμένη παρακολούθηση των ασθενών). Κυβερνοεπιθέσεις στους φορείς υγείας μπορούν να οδηγήσουν σε βλάβες και δυσλειτουργίες στον ιατροτεχνολογικό εξοπλισμό, στις υποδομές και στην παραβίαση των ιατρικών δεδομένων των ασθενών. Εκτός από τις βαριές οικονομικές-υλικές επιπτώσεις, οι χειρότερες επιπτώσεις τους εστιάζονται στους ασθενείς, στους οποίους είναι δυνατόν να προκληθούν οργανικές βλάβες, αναπηρίες, διακινδύνευσης της ζωής τους μέχρι κι ο θάνατος. Τα πραγματικά συμβάντα κυβερνοεπιθέσεων με malware στο NHS της Αγγλίας και το νοσοκομείο του Düsseldorf επιβεβαιώνουν το προηγούμενο συμπέρασμα.

Εκτός των άλλων, η πανδημία του κορωνοϊού επέφερε τεράστιο αντίκτυπο στα συστήματα υγείας, σε ό,τι αφορά το τοπίο των κυβερνοαπειλών. Συγκεκριμένα, από το ξέσπασμά της κι έπειτα, παρατηρείται εκρηκτική αύξηση των κυβερνοεπιθέσεων. Αποτέλεσμα είναι οι μαζικές παραβιάσεις ιατρικών δεδομένων και η πρόκληση δυσλειτουργιών σε έναν ευαίσθητο χώρο που, ούτως ή άλλως, συνιστά διαχρονικά έναν από τους πιο ευάλωτους και ελκυστικότερους στις κακόβουλες ενέργειες των χάκερ. Κατά τη διάρκεια της τεταμένης αυτής περιόδου, προβλημάτισαν περισσότερο οι επιθέσεις με ransomware, malware, επιθέσεις στην εφοδιαστική αλυσίδα, phishing και μέσω του IoT, πράγμα αναμενόμενο λόγω της εξάρτησης από το Διαδίκτυο, τα υπολογιστικά νέφη και το IoT.



Σχήμα 7: Τη διετία 2020-2021 (στην πανδημία του κορωνοϊού), οι κυβερνοεπιθέσεις αυξήθηκαν κατακόρυφα παγκοσμίως σε όλους τους οργανισμούς –ειδικά στους φορείς υγείας.

Πηγή: https://blog.checkpoint.com/2022/01/10/check-point-research-cyber-attacks-increased-50-year-over-year/

Ωστόσο, οι κυβερνοαπειλές δεν είναι χωρίς αντίδοτο. Μπορούν να αντιμετωπιστούν με τα κατάλληλα προληπτικά και κατασταλτικά μέτρα ασφαλείας, τα οποία ταυτίζονται με την ανάπτυξη μιας ολοκληρωμένης πολιτικής ασφαλείας κι ενός Σχεδίου Ασφαλείας. Η διαδικασία αυτή συνεπάγεται ποικίλο κόστος, είναι σύνθετη και δυναμικώς μεταβαλλόμενη, πράγμα που σημαίνει ότι χρήζει τακτικής επικαιροποίησης, ελέγχων και διορθωτικών παρεμβάσεων, λαμβάνοντας υπόψη τα νέα δεδομένα, τις εξελίξεις και τις τυχόν εμπειρίες αντιμετώπισης προηγούμενων περιστατικών. Ακόμη κι αν εφαρμοστεί η πιο προηγμένη πολιτική ασφαλείας, η εξάλειψη του κινδύνου δεν είναι εφικτή, παρά μόνο η ελάττωσή του σε αποδεκτό βαθμό. Πάντως, στο απευκταίο ενδεχόμενο του πλήγματος ενός φορέα υγείας, πρέπει να ενεργοποιηθεί το Σχέδιο Ασφαλείας για έκτακτα περιστατικά ασφαλείας και, εάν αποτύχει, να ενεργοποιηθεί το Σχέδιο Συνέχισης Λειτουργίας, επειδή είναι ζωτικής σημασίας να εξακολουθήσει τη λειτουργία του, έστω μερική (ανθεκτικότητα). Τα οφέλη ενός υψηλού βαθμού θωράκισης των πληροφοριακών συστημάτων της υγείας είναι πολλαπλά και σημαντικά, δεν περιορίζονται μονάχα στον τομέα της υγείας, αλλά διαχέονται εμμέσως στο σύνολο της δημόσιας διοίκησης.

Ευτυχώς, οι κυβερνοεπιθέσεις που έχουν έως τώρα πλήξει το ελληνικό σύστημα υγείας δεν έχουν επιφέρει σοβαρό αντίκτυπο στην ομαλή λειτουργία του, στις υποδομές, τους ασθενείς και την προστασία της ιδιωτικότητάς τους. Τίποτα, όμως, δεν εγγυάται ότι θα εξακολουθεί να συμβαίνει το ίδιο στο εξής, γιατί η συχνότητα και η πολυπλοκότητα των κυβερνοαπειλών θα αυξάνονται περαιτέρω. Τόσο τα επίπεδα ασφαλείας των πληροφοριακών συστημάτων του ελληνικού χώρου της υγείας, όσο και ο βαθμός της νομικής του συμμόρφωσης, χαρακτηρίζονται μεν ικανοποιητικά προς το παρόν, αλλά με μεγάλα περιθώρια βελτίωσης. Κι αυτό διότι παρουσιάζονται διαφόρων ειδών υστερήσεις κι ανεπάρκειες, οι οποίες δημιουργούν ορισμένα κενά ασφαλείας, τα οποία έχουν να κάνουν με μια σειρά ποικίλων παραγόντων. Σ’ αυτούς εντάσσονται η υποχρηματοδότηση του ΕΣΥ, η μη συμμόρφωση πολλών φορέων υγείας στα διεθνώς αναγνωρισμένα πρότυπα κατά ISO για τα συστήματα διαχείρισης ασφάλειας πληροφοριών, καθώς και η μερική έλλειψη σύγχρονου εξοπλισμού. Πρωτίστως, οι ανεπάρκειες αφορούν καίρια οργανωτικά μέτρα, όπως τις ελλείψεις εξειδικευμένου προσωπικού στις κατάλληλες θέσεις, την ατελή εκπαίδευση-ευαισθητοποίηση του ήδη υπάρχοντος προσωπικού πάνω σε θέματα κυβερνοαπειλών, κυβερνοασφάλειας κλπ.

Υφίστανται συγκεκριμένες βελτιωτικές προτάσεις, που μπορούν να υιοθετηθούν από τη δημόσια διοίκηση, για τη μείωση της έντασης έως την πλήρη κάλυψη των κενών ασφαλείας. Κατ' αυτόν τον τρόπο, τα ψηφιακά συστήματα, τα δίκτυα και οι υποδομές του ελληνικού συστήματος υγείας, θα είναι περισσότερο θωρακισμένα ενάντια στις σύγχρονες απειλές του κυβερνοχώρου.

Η εξασφάλιση κονδυλίων-πόρων και η κατεύθυνσή τους προς της ενίσχυση της ανάπτυξης μιας ολοκληρωμένης πολιτικής ασφαλείας των φορέων υγείας, όπως και της αύξησης του βαθμού της νομικής του συμμόρφωσης, είναι σίγουρα μία λύση. Προϋπόθεση πραγματοποίησης είναι, πέραν της επίσπευσης των διοικητικών διαδικασιών, η ύπαρξη πολιτικής βούλησης, με τη θέση του ζητήματος σε υψηλότερη πολιτική προτεραιότητα, ασχέτως των λοιπών κρατικών αναγκών. Επιπλέον, χρήσιμη θα ήταν η αναβάθμιση του συμβουλευτικού και τεχνικού ρόλου της ΑΠΔΠΧ ως προς τα θέματα κυβερνοασφάλειας, γιατί στην πράξη φαίνεται να μην εμπλέκεται έως τώρα για λειτουργικούς λόγους. Η επόμενη πρόταση σχετίζεται με το ότι η πολιτική ασφαλείας θα πρέπει να μην είναι αποσπασματική, να λαμβάνεται υπόψη σε όλα τα στάδια λειτουργίας των οργανισμών και να επικαιροποιείται συνεχώς, ανάλογα με τις μεταβαλλόμενες τεχνολογικές, θεσμικές, οικονομικές και οργανωσιακές συνθήκες. Επίσης, επειδή οι σημαντικότερες ανεπάρκειες εντοπίζονται στα οργανωτικά μέτρα (Κελεπούρης, 2022) & (Ζωγραφόπουλος, 2022), συνιστάται η βελτίωσή τους μέσω της πρόσληψης του αναγκαίου εξειδικευμένου προσωπικού στις αρμόδιες μονάδες πληροφορικής, του ορισμού διακριτής θέσης CISO ειδικά για τα νοσοκομεία του ΕΣΥ και της ευαισθητοποίησης του προσωπικού και των λοιπών χρηστών των πληροφοριακών συστημάτων σε ζητήματα κυβερνοασφάλειας με πρόσθετη εκπαίδευση. Άλλη μια βασική πρόταση που προωθείται είναι η δημιουργία ενός Δικτύου Αντιμετώπισης και Συντονισμού, ειδικά για τον χώρο της Υγείας (Κελεπούρης, 2022). Τέλος, σημαντικότατη είναι η ευαισθητοποίηση των πολιτών πάνω στις κυβερνοαπειλές και στις πρακτικές ασφαλούς πρόσβασης-χρήσης του Διαδικτύου. Ζητούμενο είναι η ατομική προστασία των προσωπικών δεδομένων στο έξυπνο κινητό τηλέφωνο ή και τον υπολογιστή του κάθε πολίτη (Ζωγραφόπουλος, 2022), κάτι που επιτυγχάνεται με μαζικές καμπάνιες ενημέρωσης στον Τύπο.

8. Επίλογος

Η υγεία είναι το υπέρτατο αγαθό. Η πανδημία COVID-19 κατέδειξε παγκοσμίως την τεράστια κοινωνική σπουδαιότητα των συστημάτων υγείας για την προστασία της, αναδεικνύοντας τη δημόσια διοίκηση ως πρωταγωνιστικό δρώντα διασφάλισης της ομαλούς λειτουργίας τους. Ωστόσο, παράλληλα με την πανδημία COVID-19, εξαιτίας της μόλυνσης της ανθρωπότητας από τον κορωνοϊό, κινδυνεύει να ξεσπάσει μια άλλη πανδημία στον κυβερνοχώρο με απρόβλεπτες επιπτώσεις και διάρκεια, που πυροδοτείται εν μέρει από την αρχική, λόγω της μεγάλης εξάρτησης από τις ΤΠΕ και των συνεπαγόμενων κινδύνων της: η πανδημία των κυβερνοαπειλών και των κυβερνοεπιθέσεων με τη μόλυνση των πληροφοριακών συστημάτων, δικτύων και υποδομών από κακόβουλο λογισμικό. Θύματά της μπορεί να πέσουν άτομα, οργανισμοί, επιχειρήσεις, μέχρι ολόκληρες χώρες, καθότι οι επιτιθέμενοι δεν πληρώνουν σημαντικό κόστος για να τις εξαπολύσουν, καταφέρνουν συχνά να μη γίνονται αντιληπτοί και να μην υφίστανται κυρώσεις, εκμεταλλευόμενοι τις τεχνολογίες του Διαδικτύου.

Απ’ όλους τους τομείς κρατικής πολιτικής και οικονομικής δραστηριότητας που είναι δυνατόν να πληγούν, ο χώρος της υγείας είναι από τους πιο ευάλωτους και ελκυστικότερους. Κι αυτό διότι μπορεί να υποστεί τις χειρότερες επιπτώσεις από την παραβίαση της ασφάλειας των ψηφιακών του συστημάτων, σε πολλαπλά επίπεδα, όπως ενδεικτικά την παραβίαση της ιδιωτικότητας των ασθενών και τη διακινδύνευση της ζωής τους. Επομένως, οι κυβερνοαπειλές στους δημόσιους και ιδιωτικούς φορείς υγείας πρέπει να αντιμετωπίζονται αμέσως και αποτελεσματικά, ώστε να συνεχίζει να εξυπηρετείται η πρωταρχική λειτουργία τους, η παροχή έγκαιρων και ποιοτικών υπηρεσιών υγείας σε όλους ανεξαιρέτως τους πολίτες, ανεξαρτήτως των αυξανόμενων σύγχρονων απειλών. Η ικανοποίηση αυτού του θεμελιώδους σκοπού, εν μέσω μάλιστα των ταχέως μεταβαλλόμενων εγχωρίων και διεθνών συνθηκών, συνιστά μία εκ των σοβαρότερων προκλήσεων, την οποία καλείται να αντιμετωπίσει το κράτος στο εγγύς και απώτερο μέλλον.

9. Πηγές και βιβλιογραφικές αναφορές

Αγγλικές

1. Austin, K. (2019). How to mitigate the IoT attacks that are increasing at 217.5%. TechTarget.
   Ανάκτηση από https://www.techtarget.com/iotagenda/blog/IoT-Agenda/How-to-mitigate-the-IoT-attacks-that-are-increasing-at-2175

2. Bimco, Clia. (2017). The guidelines on cybersecurity onboard ships, Version 2. Bimco, Clia.

3. Chua, J. (2021). Cybersecurity in the healthcare industry. *Physician Leadership Journal*.

4. Clemens, M.-A. (2018). Agreement between National Authorities or National Organisations responsible for National Contact Points for eHealth on the Criteria required for the participation in. ARTICLE 29 Data Protection Working Party.

5. Culbertson, N. (2021). Increased Cyberattacks On Healthcare Institutions Shows The Need For Greater Cybersecurity. *Forbes*. Ανάκτηση από https://www.forbes.com/sites/forbestechcouncil/2021/06/07/increased-cyberattacks-on-healthcare-institutions-shows-the-need-for-greater-cybersecurity/?sh=4258cc385650

6. Deloitte. (2020). *The rise of cyberthreats to supply chains amid COVID-19.* Deloitte.

7. Digital Information Statistics. (2022). (F. Online, Συντάκτης) Ανάκτηση από https://financesonline.com/digital-transformation-statistics/

8. ENISA. (2021). *Threat Landscape 2021.* Athens: ENISA.

9. Georgia State University OECD. (2006). *CIS 8020 Systems Integration.*

10. Ghafur, S., & Grass, E. (2019). The challenges of cybersecurity in health care: the UK National Health Service as a case study. Ανάκτηση από https://www.thelancet.com/journals/landig/article/PIIS2589-7500(19)30005-6/fulltext

11. INTERSOG. (2021). IoT Security Statistics: 6 Facts. Ανάκτηση από https://intersog.com/blog/iot-security-statistics/

12. Irwin, L. (2021). What is the cost of a healthcare data breach in the US. It governance. Ανάκτηση από https://www.itgovernanceusa.com/blog/what-is-the-cost-of-a-health-care-data-breach-in-the-us

13. Jason Creasey and Ian Glover, CREST GB. (2013). Cyber Security Incident Response Guide, Version 1. London.

14. Kushner, D. (2013). The real story of Stuxnet. *IEEE*.

15. Landi, H. (2019). 40% of healthcare organizations hit by WannaCry in past 6 months. *Fierce Healthcare*. Ανάκτηση από https://www.fiercehealthcare.com/tech/lingering-impacts-from-wannacry-40-healthcare-organizations-suffered-from-attack-past-6-months

16. Laplante, P. A. (2019). Building Caring Healthcare Systems in the Internet of Things. *PubMed Central*. Ανάκτηση από https://www.ncbi.nlm.nih.gov/pmc/articles/PMC6506834/

17. Luna, M. (2015). *Cyber Threats to Health Information Systems: A systematic review*. Texas State University.

18. Microsoft. (2022). Supply chain attacks. Ανάκτηση από https://docs.microsoft.com/en-us/microsoft-365/security/intelligence/supply-chain-malware?view=o365-worldwide

19. Moir, R. (2009). Defining malware. Ανάκτηση από https://docs.microsoft.com/en-us/previous-versions/tn-archive/dd632948(v=technet.10)?redirectedfrom=MSDN

20. Morgan, S. (2020). Cybercrime To Cost The World $10.5 Trillion Annually By 2025. Cybercrime Magazine. Ανάκτηση από https://cybersecurityventures.com/hackerpocalypse-cybercrime-report-2016/

21. Nepal, J.-J. (2014). A survey of emerging threats in cyber security. *Journal of Computer and System Sciences*. Ανάκτηση από https://www.sciencedirect.com/journal/journal-of-computer-and-system-sciences

22. Nieles, M., Dempsey, K., & Pilliteri, V. (2017). *An introduction to information security.* NIST.

23. NIST. (2021). Glossary: Cyber Attack. Ανάκτηση από https://csrc.nist.gov/glossary/term/cyber_attack

24. Pentek, H. &. (2016). Design Principles for Industrie 4.0 Scenarios. IEEE. Ανάκτηση από https://ieeexplore.ieee.org/document/7427673?arnumber=7427673&newsearch=true&queryText=industrie%204.0%20design%20principles

25. Perasklis, E. (2014). Cybersecurity in healthcare. *Perspective*.

26. Piccoli, G. (2018). *Information Systems for managers.* Prospect Press.

27. Poulsen, K. (2011). Leader of Hacker Gang Sentenced to 9 Years For Hospital Malware. Ανάκτηση από https://www.wired.com/2011/03/ghostexodus-2/

28. Silomon, J. (2020). The Düsseldorf Cyber Incident. IFSH. Ανάκτηση από https://ifsh.de/en/news-detail/the-duesseldorf-cyber-incident

29. Smart, W. (2018). Lessons learned review of the WannaCry Ransomware Cyber Attack. NHS. Ανάκτηση από https://www.england.nhs.uk/wp-content/uploads/2018/02/lessons-learned-review-wannacry-ransomware-cyber-attack-cio-review.pdf

30. Todd, D. (2022). *Top 10 Data Breaches of All Time*. Ανάκτηση από secureworld: https://www.secureworld.io/industry-news/top-10-data-breaches-of-all-time

31. Tyalli, S., & Pottas, D. (2010). *Information Security Management Systems.* Port Elizabeth: School of ICT.

32. Weiner, S. (2021). The growing threat of ransomware attacks on hospitals. AAMC. Ανάκτηση από https://www.aamc.org/news-insights/growing-threat-ransomware-attacks-hospitals

33. White, F. (2015). Primary Health Care and Public Health: Foundations of Universal Health Systems. Ανάκτηση από https://www.ncbi.nlm.nih.gov/pmc/articles/PMC5588212/

Ελληνικές

1. Βάλσαμος, Π. (2018). *Συστήματα Πληροφορικής Υπηρεσιών Υγείας, εκπαιδευτικές σημειώσεις.* Αθήνα: Εθνική Σχολή Δημόσιας Διοίκησης και Αυτοδιοίκησης.
2. Γκρίτζαλης, Δ. (2004). *Ασφάλεια Πληροφοριακών Συστημάτων.* Αθήνα: Νέων Τεχνολογιών.
3. Εθνική Σχολή Δημόσιας Διοίκησης. (2021). Κυβερνοασφάλεια στη Δημόσια Διοίκηση. Αθήνα: Εθνικό Κέντρο Δημόσιας Διοίκησης.
4. Ζωγραφόπουλος, Δ. (2019). GDPR οκτώ μήνες μετά. (Γ. Φετουκάκης, Δημοσιογράφος) Ανάκτηση από https://netweek.gr/gdpr-okto-mines-meta/
5. Ζωγραφόπουλος, Δ. (2022, Μάιος). Συνέντευξη του DPO του Υπουργείου Υγείας. (Λ. Τσικλητάρης, Δημοσιογράφος)
6. Κελεπούρης, Α. (2022, Μάιος). Συνέντευξη του προϊσταμένου της Διεύθυνσης Ηλεκτρονικής Διακυβέρνησης του Υπουργείου Υγείας. (Λ. Τσικλητάρης, Δημοσιογράφος)
7. Μπουρσανίδης. (2022). *Συστήματα και πολιτικές υγείας, εκπαιδευτικές σημειώσεις.* Αθήνα: Εθνική Σχολή Δημόσιας Διοίκησης κα Αυτοδιοίκησης.
8. ΠΟΥ. (1948). Καταστατικός Χάρτης.
9. Σιώζου, Ε. (2022, Μάιος). Συνέντευξη της προϊσταμένης της διεύθυνσης πληροφορικής του νοσοκομείου "Σωτηρία". (Λ. Τσικλητάρης, Δημοσιογράφος)
10. Υπουργείο Υγείας. (2018). Εγκύκλιος: Προετοιμάστε το Φορέα σας για τη συμμόρφωση προς τον ΓΚΠΔ -Οδηγός Προετοιμασίας. Αθήνα.

Εθνική Νομοθεσία

1. Σύνταγμα της Ελλάδας (1986-2001-2008-2019)
2. Ν. 2225/1994 «Για την προστασία της ελευθερίας της ανταπόκρισης και επικοινωνίας και άλλες διατάξεις».
3. Ν. 2472/1997 «Προστασία του ατόμου από την επεξεργασία δεδομένων προσωπικού χαρακτήρα».
4. Ν. 3115/2003 «Αρχή Διασφάλισης του Απορρήτου των Επικοινωνιών».
5. Ν. 3418/2005 «Κώδικας Ιατρικής Δεοντολογίας».
6. Ν.3471/2006 «Προστασία δεδομένων προσωπικού χαρακτήρα και της ιδιωτικής ζωής στον τομέα των ηλεκτρονικών επικοινωνιών και τροποποίηση του ν.2472/1997».
7. Ν.4070.2012 «Ρυθμίσεις Ηλεκτρονικών Επικοινωνιών, Μεταφορών, Δημοσίων Έργων και άλλες διατάξεις».
8. Ν. 4213/2013 «Προσαρμογή της εθνικής νομοθεσίας στις διατάξεις της Οδηγίας 2011/24/ΕΕ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου της 9ης Μαρτίου 2011 περί εφαρμογής των δικαιωμάτων των ασθενών στο πλαίσιο της διασυνοριακής υγειονομικής περίθαλψης (L 88/45/ 4.4.2011) και άλλες διατάξεις».
9. Ν. 4411/2016 «Κύρωση της Σύμβασης του Συμβουλίου της Ευρώπης για το έγκλημα στον Κυβερνοχώρο και του Προσθέτου Πρωτοκόλλου της, σχετικά με την ποινικοποίηση πράξεων ρατσιστικής και ξενοφοβικής φύσης, που διαπράττονται μέσω Συστημάτων Υπολογιστών Μεταφορά στο ελληνικό δίκαιο της Οδηγίας 2013/40/ΕΕ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου για τις επιθέσεις κατά συστημάτων πληροφοριών και την αντικατάσταση της απόφασης – πλαισίου 2005/222/ΔΕΥ του Συμβουλίου, ρυθμίσεις σωφρονιστικής και αντεγκληματικής πολιτικής και άλλες διατάξεις».
10. Ν.4577/2018 «Ενσωμάτωση στην ελληνική νομοθεσία της Οδηγίας 2016/1148/ΕΕ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου σχετικά με μέτρα για υψηλό κοινό επίπεδο ασφάλειας συστημάτων δικτύου και πληροφοριών σε ολόκληρη την Ένωση και άλλες διατάξεις».
11. Ν.4619/2019 «Κύρωση του Ποινικού Κώδικα».
12. Ν.4624/2019 «Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα, μέτρα εφαρμογής του Κανονισμού (ΕΕ) 2016/679 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου της 27ης Απριλίου 2016 για την προστασία των φυσικών

προσώπων έναντι της επεξεργασίας δεδομένων προσωπικού χαρακτήρα και ενσωμάτωση στην εθνική νομοθεσία της Οδηγίας (ΕΕ) 2016/680 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου της 27ης Απριλίου 2016 και άλλες διατάξεις».

13. Π.Δ 178/2014 «Οργάνωση Υπηρεσιών Ελληνικής Αστυνομίας».
14. Π.Δ 40/2020 «Οργανισμός του Υπουργείου Ψηφιακής Διακυβέρνησης».
15. ΥΑ 34368/2020 «Έγκριση της Εθνικής Στρατηγικής Κυβερνοασφάλειας 2020 – 2025» ΑΔΑ 6ΙΒΕ46ΜΤΛΠ-ΦΜ5. Υπουργός Επικρατείας.

Ευρωπαϊκή Νομοθεσία

1. Κανονισμός (ΕΕ) 910/2014 «Σχετικά με την ηλεκτρονική ταυτοποίηση και τις υπηρεσίες εμπιστοσύνης για τις ηλεκτρονικές συναλλαγές στην εσωτερική αγορά και την κατάργηση της οδηγίας 1999/93/ΕΚ».
2. Κανονισμός (ΕΕ) 2016/679 «Για την προστασία των φυσικών προσώπων έναντι της επεξεργασίας των δεδομένων προσωπικού χαρακτήρα και για την ελεύθερη κυκλοφορία των δεδομένων αυτών και την κατάργηση της οδηγίας 95/46/ΕΚ (Γενικός Κανονισμός για την Προστασία Δεδομένων)».
3. Κανονισμός (ΕΕ) 2017/745 «Για τα ιατροτεχνολογικά προϊόντα, για την τροποποίηση της οδηγίας 2001/83/ΕΚ, του κανονισμού (ΕΚ) αριθ. 178/2002 και του κανονισμού (ΕΚ) αριθ. 1223/2009 και για την κατάργηση των οδηγιών του Συμβουλίου 90/385/ΕΟΚ και 93/42/ΕΟΚ».
4. Κανονισμός (ΕΕ) 2019/881 «(Οργανισμός της Ευρωπαϊκής Ένωσης για την Κυβερνοασφάλεια) και με την πιστοποίηση της κυβερνοασφάλειας στον τομέα της τεχνολογίας πληροφοριών και επικοινωνιών και για την κατάργηση του κανονισμού (ΕΕ) αριθ. 526/2013 (πράξη για την κυβερνοασφάλεια)».
5. Οδηγία (ΕΕ) 2016/1148 (NIS) «σχετικά με μέτρα για υψηλό κοινό επίπεδο ασφάλειας συστημάτων δικτύου και πληροφοριών σε ολόκληρη την Ένωση».

Παράρτημα

Ερωτηματολόγια

Ερωτηματολόγιο 1: DPO του Υπουργείου Υγείας.

1. Τι είδους προσωπικά δεδομένα επεξεργάζεται το Υπουργείο Υγείας;

2. Έχει πρόσβαση το Υπουργείο Υγείας στα ιατρικά δεδομένα των ασθενών, τα οποία βρίσκονται στον ΑΗΦΥ, όπως έχουν τα νοσοκομεία; Αν ναι, για ποιες υπηρεσίες του και υπό ποιες προϋποθέσεις;

3. Σύμφωνα με τις προβλέψεις του ΓΚΠΔ, ποια η σχέση του Υπουργείου Υγείας ως προς την επεξεργασία των δεδομένων υγείας των ασθενών με τους εποπτευόμενους απ' αυτό φορείς, όπως ο ΕΟΠΥΥ;

4. Οι ιδιωτικές κλινικές ή τα διαγνωστικά κέντρα έχουν πρόσβαση στον ΑΗΦΥ; Υπό ποιες προϋποθέσεις;

5. Πώς θα χαρακτηρίζατε τον βαθμό συμμόρφωσης του Υπουργείου Υγείας (και των εποπτευόμενων φορέων του) με τα μέτρα ασφάλειας και προστασίας των ευαίσθητων προσωπικών δεδομένων που προβλέπονται στο ισχύον νομικό πλαίσιο κυβερνοασφάλειας και προστασίας της ιδιωτικότητας των ασθενών (ΓΚΠΔ, Ν.4624/2019, Ν. 4577/2018). Αν η συμμόρφωση δεν είναι πολύ ικανοποιητική, ποιοι παράγοντες θεωρείτε ότι ευθύνονται;

6. Υπάρχουν κάποιες επιπλέον δικλείδες ασφαλείας που θα έπρεπε να τηρούνται εκ μέρους του Υπουργείου; Αν ναι, ποιες είναι αυτές, ώστε να βελτιωθεί το επίπεδο ασφαλείας και προστασίας της ιδιωτικότητας των ασθενών;

7. Οι ερωτήσεις (5) και (6) για τα νοσοκομεία του ΕΣΥ

8. Γνωρίζετε αν έχει συμβεί κάποια παραβίαση ή απόπειρα παραβίασης των ευαίσθητων προσωπικών δεδομένων των ασθενών στο Υπουργείο Υγείας, σε κάποιο

εποπτευόμενο φορέα του ή νοσοκομείο; Τι αποτελέσματα προκάλεσε; Πώς αντιμετώπισε το περιστατικό ο οργανισμός;

9. Πόσο κατάλληλα προετοιμασμένο είναι το Υπουργείο Υγείας, οι εποπτευόμενοι φορείς και το ΕΣΥ γενικότερα (με βάση τη γνώση ή και την προσωπική σας εκτίμηση) για να αντιμετωπίσει κυβερνοεπιθέσεις, που στοχεύουν στην παραβίαση-υποκλοπή των δεδομένων υγείας των ασθενών;

10. Διαδραματίζει κάποιο συμβουλευτικό ή τεχνικό ρόλο η ΑΠΔΠΧ ως προς την ασφάλεια των πληροφοριακών συστημάτων των δημόσιων και ιδιωτικών φορέων παροχής υπηρεσιών υγείας; Πώς ασκεί πρακτικά αυτόν τον ρόλο;

11. Υπάρχει νομολογία ή γνωστή απόφαση της ΑΠΔΠΧ με την οποία επιβάλλονται ποινικές-διοικητικές κυρώσεις (π.χ χρηματικό πρόστιμο) σε δημόσιο ή ιδιωτικό φορέα υγείας, εξαιτίας περιστατικού παραβίασης-διαρροής ευαίσθητων προσωπικών δεδομένων;

12. Πόσο απαιτητική είναι η ιδιότητα του DPO του Υπουργείου Υγείας και γιατί;

Ερωτηματολόγιο 2: Προϊστάμενος Διεύθυνσης Ηλεκτρονικής Διακυβέρνησης του Υπουργείου Υγείας.

1. Πόσο κατάλληλα προετοιμασμένο είναι, κατά την άποψή σας, το Υπουργείο Υγείας, οι εποπτευόμενοι φορείς του και το ΕΣΥ γενικότερα (με βάση τη γνώση ή και την προσωπική σας εκτίμηση) για την επιτυχή αντιμετώπιση κυβερνοεπιθέσεων; Σε ποιους παράγοντες θα αποδίδατε το συγκεκριμένο επίπεδο προετοιμασίας;

2. Πώς κρίνετε τον βαθμό συμμόρφωσης του Υπουργείου στο ισχύον νομικό πλαίσιο κυβερνοασφάλειας και προστασίας των δεδομένων υγείας των ασθενών; (GDPR, N.4577/2018, κλπ.). Αν κρίνετε ότι παρουσιάζεται υστέρηση, γιατί θεωρείται ότι δεν υπάρχει ακόμη πλήρης συμμόρφωση;

3. Υπάρχουν κάποιες επιπλέον δικλείδες ασφαλείας που θα έπρεπε να τηρούνται; Αν ναι, ποιες είναι αυτές, ώστε να βελτιωθεί το επίπεδο ασφαλείας των ψηφιακών συστημάτων του Υπουργείου;

4. Γνωρίζετε αν έχει συμβεί κάποια παραβίαση ή απόπειρα παραβίασης ευαίσθητων προσωπικών δεδομένων στο Υπουργείο Υγείας, σε κάποιο εποπτευόμενο φορέα του ή νοσοκομείο; Τι αποτελέσματα προκάλεσε; Ο οργανισμός το αντιμετώπισε με επιτυχία;

5. Ως Προϊστάμενος της Διεύθυνσης Ηλεκτρονικής Διακυβέρνησης, έχετε κάποιες επιπλέον προτάσεις προς υιοθέτηση από το Υπουργείο Υγείας ή τα νοσοκομεία του ΕΣΥ, σε οργανωτικό ή και τεχνικό επίπεδο, προκειμένου να είναι περισσότερα θωρακισμένα απέναντι στις σύγχρονες κυβερνοαπειλές, συγκριτικά με την παρούσα κατάσταση;

6. Πόσο απαιτητική είναι η θέση του Προϊσταμένου της Διεύθυνσης Ηλεκτρονικής Διακυβέρνησης και γιατί;

Ερωτηματολόγια 3 και 4: Υπεύθυνη Μονάδας Πληροφορικής του νοσοκομείου Σωτηρία και της ιδιωτικής κλινικής Ψ.

1. Υπάρχει η θέση του υπευθύνου ασφαλείας πληροφοριακών συστημάτων στο νοσοκομείο/ιδιωτική κλινική; Αν όχι, ποιος αρμόδιος αναλαμβάνει αυτόν τον ρόλο;

2. Υπάρχει πολιτική ασφαλείας των ψηφιακών συστημάτων;

3. Τι πρότυπα-πρακτικές εφαρμόζει το νοσοκομείο/ιδιωτική κλινική, ώστε να κρατά σε αποδεκτό επίπεδο τον κίνδυνο των κυβερνοαπειλών;

4. Γίνεται περιοδικός έλεγχος της πολιτικής ασφαλείας, κι αν ναι, υπό ποια μορφή;

5. Το νοσοκομείο/κλινική εφαρμόζει τα μέτρα του εγχειριδίου κυβερνοασφάλειας 2021 και σε ποιον βαθμό;

6. Συνέβη ποτέ κάποια κυβερνοεπίθεση στο νοσοκομείο/κλινική; Κι αν ναι, πού αποσκοπούσε και πώς αντιμετωπίστηκε;

7. Πώς θα χαρακτηρίζατε τον βαθμό συμμόρφωσης στα μέτρα ασφάλειας και προστασίας των ευαίσθητων προσωπικών δεδομένων που προβλέπονται στο ισχύον νομικό πλαίσιο κυβερνοασφάλειας και προστασίας της ιδιωτικότητας των ασθενών (ΓΚΠΔ, Ν.4624/2019, Ν. 4577/2018, Ν.4727/2020).

8. Πώς προβλέπεται ότι θα αντιμετωπίσει το νοσοκομείο/κλινική τα περιστατικά ασφαλείας-κυβερνοεπιθέσεις κατά των ψηφιακών συστημάτων; Ποιες υπηρεσίες-φορείς θα ενεργοποιηθούν σε μια τέτοια περίπτωση;

9. Πόσο θωρακισμένο κρίνετε ότι είναι το νοσοκομείο/κλινική απέναντι στις κυβερνοαπειλές; Υπάρχουν κάποια επιπλέον οργανωτικά και τεχνικά μέτρα ασφαλείας που θα μπορούσαν να υιοθετηθούν, ώστε να βελτιωθεί η προστασία των ψηφιακών συστημάτων;

10. Μπορείτε να εκτιμήσετε, κατά την άποψη και την εμπειρία σας, την κατάσταση των επιπέδων ασφαλείας των νοσοκομείων του ΕΣΥ;

11. Πόσο απασχολούν το νοσοκομείο και το προσωπικό του νοσοκομείου οι κυβερνοαπειλές; Είναι προετοιμασμένο το προσωπικό γι' αυτές;

Εθνική Σχολή Δημόσιας Διοίκησης και Αυτοδιοίκησης (Ε.Σ.Δ.Δ.Α.)
Πειραιώς 211, ΤΚ 177 78, Ταύρος
τηλ: 2131306349 , fax: 2131306479
www.ekdd.gr