Ανοικτό Πανεπιστήμιο Κύπρου

Σχολή Θετικών και Εφαρμοσμένων Επιστημών

Μεταπτυχιακό Πρόγραμμα Σπουδών

Εφαρμοσμένη Πληροφορική της Υγείας και Τηλεϊατρική

Μεταπτυχιακή Διατριβή

Η Ευαισθητοποίηση των Επαγγελματιών Υγείας σε Σχέση με την Ασφάλεια στο Κυβερνοχώρο

Ευριπίδης Κνέκνας

Επιβλέπων Καθηγητής

Δρ. Θεοφάνης Φώτη

Λευκωσία

Μάιος 2021

Ανοικτό Πανεπιστήμιο Κύπρου

Σχολή Θετικών και Εφαρμοσμένων Επιστημών

Μεταπτυχιακό Πρόγραμμα Σπουδών

Εφαρμοσμένη Πληροφορική της Υγείας και Τηλεϊατρική

Μεταπτυχιακή Διατριβή

Η Ευαισθητοποίηση των Επαγγελματιών Υγείας σε Σχέση με την Ασφάλεια στο Κυβερνοχώρο

Ευριπίδης Κνέκνας

Επιβλέπων Καθηγητής

Δρ. Θεοφάνης Φώτη

Η παρούσα μεταπτυχιακή διατριβή υποβλήθηκε προς μερική εκπλήρωση των απαιτήσεων για απόκτηση μεταπτυχιακού τίτλου σπουδών στην Εφαρμοσμένη Πληροφορική της Υγείας και Τηλεϊατρική από τη Σχολή Θετικών και Εφαρμοσμένων Επιστημών του Ανοικτού Πανεπιστημίου Κύπρου.

Λευκωσία

Μάιος 2021

Περίληψη

Εισαγωγή: Η πληροφορία διαδραματίζει ένα πολύ σημαντικό ρόλο στη σύγχρονη υγειονομική περίθαλψη. Τα δεδομένα που συλλέγονται για την κατάσταση της υγείας του ασθενή, είναι συχνά ευαίσθητης φύσης και πρέπει να κρατούνται απόρρητα και να μην διατίθενται σε μη εξουσιοδοτημένα πρόσωπα. Τα θέματα ασφάλειας και εμπιστευτικότητας, αποτελούν κύριο μέλημα στο χώρο της υγείας. Στην Ευρώπη αλλά και σε πολλές άλλες χώρες, υπάρχουν οργανισμοί και κανόνες οι οποίοι επιβάλουν την προστασία των προσωπικών και ευαίσθητων δεδομένων. Για την ενίσχυση της ασφάλειας των νοσοκομείων από επιθέσεις στον κυβερνοχώρο, οι υπεύθυνοι χάραξης πολιτικής, πρέπει να εφαρμόσουν πολιτικές που θα αυξήσουν το επίπεδο και το στόχο των δυνατοτήτων ασφάλειας στον κυβερνοχώρο, και παράλληλα θα μειώσουν τη μεταβλητότητα της διαθεσιμότητας των πόρων σε ολόκληρο το σύστημα υγείας.

Σκοπός: Ο σκοπός της παρούσας κριτικής ανασκόπησης είναι να διερευνηθεί η ευαισθητοποίηση των επαγγελματιών υγείας σχετικά με την ασφάλεια στο κυβερνοχώρο.

Υλικό και μέθοδος: Εφαρμόστηκε κριτική ανασκόπηση της βιβλιογραφίας. Η ανεύρεση του υλικού έγινε με αναζήτηση της σχετικής ελληνικής και διεθνούς βιβλιογραφίας, χρησιμοποιώντας τη βάση δεδομένων GOOGLE SCHOLAR και PUBMED, με συγκεκριμένες λέξεις κλειδιά όπως *κυβερνοασφάλεια και υγεία, κυβερνοασφάλεια και επαγγελματίες υγείας, κυβερνοασφάλεια υγειονομικής περίθαλψης.* Τελικά συμπεριλήφθησαν επτά ερευνητικές μελέτες που πληρούσαν τα κριτήρια εισδοχής που τέθηκαν.

Αποτελέσματα: Μέσα από την αναζήτηση της βιβλιογραφίας διαπιστώθηκε ότι η ευαισθητοποίηση των επαγγελματιών υγείας, αποτελεί πρωταρχικό ρόλο στην υγειονομική περίθαλψη. Οι επαγγελματίες υγείας, εστιάζουν την σημαντικότητα της εκπαίδευσης στο τομέα της κυβερνοασφάλειας, αφού δεν έχουν τις απαραίτητες γνώσεις να αναγνωρίζουν τους κινδύνους, παρόλο που κάποιοι έχουν λάβει σχετική εκπαίδευση. Οι επικίνδυνες συμπεριφορές στον κυβερνοχώρο, ευνοούν τις παραβιάσεις των δεδομένων και τις ασφάλειας.

Συμπεράσματα: Ο μοναδικός τρόπος αντιμετώπισης της κυβερνοεπίθεσης, είναι η σωστή εκπαίδευση των επαγγελματιών υγείας και η χρηματοδότηση των εκπαιδευτικών προγραμμάτων. Οι οργανισμοί υγείας, οφείλουν να υιοθετήσουν πρότυπα ασφαλείας για να διασφαλιστούν τα δεδομένα που διαχειρίζονται οι λειτουργοί της υγειονομικής περίθαλψης. Είναι πολύ σημαντικό, να υπάρχει η γνώση ώστε να αντιμετωπιστεί έγκαιρα οποιαδήποτε ανεπιθύμητη επίθεση αφού οι επιπτώσεις που θα προκληθούν θα είναι ανεπανόρθωτες.

Abstract

Introduction: Data play an exceedingly significant role in contemporary health care. The collection of data concerning to a patient's health status is generally sensitive and must remain confidential and accessed strictly by authorised people only. Security and confidentiality issues constitute a fundamental concern in healthcare. European and many other countries incorporate organizations and regulations which enforce personal and sensitive data protection. In order to enhance hospital data security from cyber-attacks, policy makers must establish cyber-security policies which will improve cyber security capabilities, and additionally, eliminate any risk of variability of data throughout the entire health system.

Objective: The objective of this critical review is the investigation and exploration of the cyber security awareness among health professionals.

Method: A critical literature review was undertaken. The investigation of research papers comprised both Greek and international literature review, by using databases such as GOOGLE SCHOLAR and PUBMED, through certain key words like *cyber-security and health*, *cyber-security and health professionals*, *healthcare cybersecurity*. Finally, seven research papers were investigated conforming to the criteria which were established.

Findings of the study: In consequence of the examination of the literature review, the findings demonstrated that raising security awareness among health professionals constitutes a principal role in healthcare. Health professionals emphasise largely on the significance of cyber-security training, since they lack the necessary knowledge to identify risks, despite the fact that some have received previous relative training. Risky online behaviours might lead to data and security breaches.

Conclusion: In conclusion, the individual way to withstand cyber-attacks is the provision of adequate training for health professionals and funding of training programmes. Health organisations should adopt security standards to secure data which are administered by healthcare workers. It is of crucial importance, for the healthcare professionals, to have the appropriate knowledge required to achieve an immediate countering of any unpleasant cyber-attacks, taking into consideration that the effects will be irreversible.

Ευχαριστίες

Θα ήθελα να ευχαριστήσω τον επιβλέποντα καθηγητή μου, Δρ. Θεοφάνη Φώτη για τις συμβουλές και τις υποδείξεις του κατά την διάρκεια της εκπόνησης της μεταπτυχιακής μου εργασίας.

Επίσης ένα μεγάλο ευχαριστώ στην οικογένεια μου και ιδιαίτερα στην σύζυγο μου και στην κόρη μου, που μου έδωσαν τον χρόνο που απαιτείται για να επιτευχθεί η συγκεκριμένη έρευνα και που με στηρίζουν σε κάθε μου βήμα.

Στην Θεότη…

Περιεχόμενα

Εισαγωγή

Η πληροφορία διαδραματίζει ένα πολύ σημαντικό ρόλο στη σύγχρονη υγειονομική περίθαλψη. Τα πληροφοριακά συστήματα στα ιδρύματα υγειονομικής περίθαλψης, υποστηρίζουν ένα ευρύ φάσμα διαδικασιών. Οι πληροφορίες που ανακτώνται και παρέχονται από αυτά τα συστήματα, παίζουν καθοριστικό ρόλο για την κατάλληλη λειτουργία της υγειονομικής περίθαλψης. Τα δεδομένα που συλλέγονται για την κατάσταση της υγείας του ασθενή, είναι συχνά ευαίσθητης φύσης και πρέπει να κρατούνται απόρρητα και να μην διατίθενται σε μη εξουσιοδοτημένα πρόσωπα (Bakker, 2007).

Τα δεδομένα που παράγουν και στα οποία έχουν πρόσβαση οι επαγγελματίες υγείας, αποτελούνται από λέξεις, αριθμούς, σήματα, ήχους και εικόνες. Οι λειτουργίες που εκτελούνται για την ανάλυση των πληροφοριών και δεδομένων, ποικίλει, ανάλογα με το βαθμό εκλέπτυνσης των πληροφοριακών συστημάτων που είναι διαθέσιμα. Επομένως, οι πρακτικές εργασίας ποικίλουν, ώστε να ταιριάζουν με το εργασιακό περιβάλλον, με στόχο την μεγιστοποίηση των οφελών από τη χρήση των διαθέσιμων πληροφοριών. Τα δεδομένα υγείας χωρίζονται σε τέσσερις κατηγορίες, τα δημογραφικά δεδομένα, δεδομένα δραστηριοτήτων που αποτελούνται από κλινικά δεδομένα, δεδομένα πόρων και δεδομένα προμηθευτών υπηρεσιών υγείας. Είναι σαφές ότι τα δεδομένα υγείας είναι ιδιαίτερα σύνθετα και χρήζουν ανάλογης αντιμετώπισης (Hovenga & Sermeus, 2009).

Τα θέματα ασφάλειας και εμπιστευτικότητας, αποτελούν κύριο μέλημα στο χώρο της υγείας. Στην Ευρωπαϊκή Ένωση, υπάρχουν οργανισμοί και κανόνες οι οποίοι επιβάλουν την προστασία των προσωπικών και ευαίσθητων δεδομένων. Ήδη από τις 25 Μαΐου 2018, έχει τεθεί σε εφαρμογή ένα νέο σύνολο κανόνων προστασίας δεδομένων προσωπικού χαρακτήρα, με απώτερο στόχο, τον εκσυγχρονισμό του υφιστάμενου πλαισίου. Με τον νέο κανονισμό, οι οργανισμοί, οι εταιρείες αλλά και οι επαγγελματίες, έχουν διαφοροποιήσει τον τρόπο με τον οποίο συλλέγουν, διαχειρίζονται, επεξεργάζονται και αποθηκεύουν πληροφορίες που περιέχουν προσωπικά δεδομένα. Ταυτόχρονα, οι πολίτες αποκτούν νέα δικαιώματα και ενίσχυση της προστασίας των προσωπικών δεδομένων με επιβολή αυστηρών διοικητικών κυρώσεων (Εφημερίδα Ευρωπαϊκής Ένωσης, 2016).

Η Κύπρος από τον Αύγουστο του 2020, έχει εναρμονιστεί πλήρως την ευρωπαϊκή οδηγία 2016/1148 για την ασφάλεια των δικτύων και των συστημάτων πληροφοριών, μέσω του

Νόμου περί Ασφάλειας Δικτύων και Πληροφοριακών Συστημάτων (Νόμος 89 (I) / 2020). Ο κυπριακός νόμος δημιουργεί ένα πλαίσιο για την ασφάλεια δικτύων και συστημάτων πληροφοριών σε όλες τις κρίσιμες υποδομές πληροφοριών στην Κύπρο και ενισχύει τις υπάρχουσες δυνατότητες του κράτους του νησιού ώστε να χειρίζεται και να ανταποκρίνεται σε κυβερνοεπιθέσεις. Ο βασικός σκοπός της νομοθεσίας είναι να διασφαλίσει την κυπριακή υποδομή δικτύου έτσι ώστε να μπορεί να ανταποκριθεί σε κυβερνοεπιθέσεις και σε άλλες απειλές ως προς την ασφάλεια του κυβερνοχώρου (Εφημερίδα Ευρωπαϊκής Ένωσης, 2016).

Στις Ηνωμένες Πολιτείες Αμερικής (ΗΠΑ), το κανονιστικό πλαίσιο γύρω από τις προστατευμένες πληροφορίες της υγείας, έχει εξελιχθεί τις τελευταίες δυο δεκαετίες. Ο νόμος φορητότητας και λογοδοσίας για την ασφάλεια της υγείας (HIPPA), ψηφίστηκε το 1996 και επέβαλε την προστασία της χρήσης, της αποκάλυψης, της αποθήκευσης αλλά και της μετάδοσης των πληροφοριών για την υγεία. Ακολούθησε ο νόμος για την τεχνολογία πληροφοριών για την υγεία και την κλινική υγεία (HITECH) το 2009, ο οποίος αύξησε τις ποινές για τις παραβιάσεις προς την HIPAA. Επομένως, ενίσχυσε την κοινοποίηση ως προς την παραβίαση και ενθάρρυνε την ουσιαστική χρήση των ηλεκτρονικών αρχείων της υγείας (Argaw, 2020).

Η εφαρμογή των αυστηρών κανονισμών οι οποίοι θέτουν τεχνολογικές και οργανωτικές προκλήσεις για τα ιδρύματα υγείας, γίνονται για την προστασία των δεδομένων αλλά και για την κυβερνοασφάλεια των νοσοκομείων, καθώς και για την ασφάλεια των ασθενών.

Δεδομένου ότι τα ιατρικά δεδομένα έχουν εμπορική αξία, καθιστά την ασφάλεια ως κυρίαρχο χαρακτηριστικό των τελικών εφαρμογών. Οι επιθέσεις στον κυβερνοχώρο σε ιατρικούς χώρους, η πειρατεία των βάσεων δεδομένων και οι απαγωγές δεδομένων αποτελούν συχνό φαινόμενο, αφού ολοένα και αυξάνονται τα περιστατικά παραβιάσεων δεδομένων και υποκλοπής τους (Vayena, 2018) (Kostkova, 2015).

Η υγειονομική περίθαλψη είναι ένας ελκυστικός στόχος για αυτούς που διαπράττουν εγκλήματα στον κυβερνοχώρο, αφού υπάρχει πλούσια πηγή πολύτιμων δεδομένων και η ασφάλεια για παραβίαση είναι πολύ χαμηλή. Ως εκ τούτου, σε τέτοιες επιθέσεις, περιλαμβάνονται και επιθέσεις κατά των ιατρικών συσκευών, που μπορούν να αποβούν μοιραίες ακόμα και για τον ίδιο τον ασθενή (Coventry & Branley, 2018). Επιπρόσθετα, η ασφάλεια στον κυβερνοχώρο στα νοσοκομεία, πρέπει να λαμβάνει υπόψη τις χιλιάδες

αλληλοσυνδεόμενες ιατρικές συσκευές και τις συχνές ασυνεπείς επιχειρηματικές διαδικασίες. Οι συνδεδεμένες ιατρικές συσκευές εισάγουν πολλές ευπάθειες στην ασφάλεια στον κυβερνοχώρο ενός νοσοκομείου. Ωστόσο, αυτές οι συσκευές χρησιμοποιούνται σε όλο το νοσοκομείο και μπορούν ακόμη και να χρησιμοποιηθούν και εκτός του χώρου (Argaw et al, 2020).

Η επέμβαση στην ιδιωτική ζωή γίνεται σε συστηματική βάση από χάκερς, οι οποίοι στη συνέχεια πωλούν τα κλεμμένα αρχεία στην μαύρη αγορά. Τα αρχεία αυτά μπορεί να περιέχουν αρκετές πληροφορίες για να ανοίξουν τραπεζικούς λογαριασμούς, να λάβουν δάνεια ή να αποκτήσουν ταυτότητα και διαβατήριο (Mohammed et al, 2015) (Martin et al, 2017). Σαφώς το ισχυρότερο κίνητρο των χάκερ είναι το οικονομικό κέρδος. Τα δεδομένα της υγειονομικής περίθαλψης είναι πολύ πιο πολύτιμα από οποιαδήποτε άλλα δεδομένα. Οι εγκληματίες του κυβερνοχώρου, έχουν κερδίσει δισεκατομμύρια τα τελευταία χρόνια, καταθέτοντας ψευδείς ισχυρισμούς και διανέμοντας ναρκωτικά λόγω της συνταγογράφησης που επιτυγχάνουν και έτσι πωλούνται στην μαύρη αγορά (Coventry & Branley, 2018).

Οι παραβιάσεις έχουν ως αποτέλεσμα την οικονομική απώλεια, την δυσφήμηση και την μειωμένη αίσθηση ασφάλειας των ασθενών. Η συνεχής δημοσιότητα που σχετίζεται με μεγάλες παραβιάσεις δημιουργεί απώλεια ως προς την εμπιστοσύνη των ασθενών, η οποία έχει οδηγήσει σε λιγότερη προθυμία της κοινοποίησης των δεδομένων τους. Αυτό είναι ιδιαίτερα ανησυχητικό για ασθενείς οι οποίοι είναι στιγματισμένοι για την σεξουαλική ή ψυχική τους υγεία (Coventry & Branley, 2018).

Λόγω της πανδημίας που ταλανίζει ολόκληρο το πλανήτη, ο τομέας της υγείας έχει μετατοπίσει την εστίασή του από την ασφάλεια των συστημάτων και των πρακτικών του στο πρωταρχικό καθήκον της παροχής υγειονομικής περίθαλψης προκειμένου να σώσει ζωές, θέτοντας τον εαυτό τους σε μια ευάλωτη κατάσταση. Οι επιτιθέμενοι εκμεταλλεύονται την πανδημία COVID-19 και έχουν ξεκινήσει μια σειρά επιθέσεων στον κυβερνοχώρο εναντίον των οργανισμών της υγειονομικής περίθαλψης. Το έγκλημα στον κυβερνοχώρο προσαρμόζεται στις αλλαγές τις παγκόσμιας κατάστασης, πολύ γρήγορα. Στην αρχή της κλιμάκωσης της πανδημίας του COVID-19, οι κυβερνοεπιτιθέμενοι των κακόβουλων λογισμικών, εντόπιζαν τις αδυναμίες που υπήρχαν στα συστήματα υγείας και προσάρμοζαν τις επιθέσεις, εκμεταλλευόμενοι των αδυναμιών (He et al, 2021).

Τόσο η υγειονομική περίθαλψη όσο και οι ακαδημαϊκοί οργανισμοί οφείλουν να αξιολογήσουν άμεσα τους κινδύνους που ενέχει μια επίθεση στον κυβερνοχώρο στα πλαίσια της πανδημίας του COVID19 και να αναπτυχθεί ένα λεπτομερές σχέδιο αντιμετώπισης των συμβάντων, υπενθυμίζοντας ότι οι επιθέσεις είναι πιθανό να διακόψουν όλες τις πτυχές της έρευνας. Σε περίπτωση επίθεσης, οι οργανισμοί θα χρειαστούν ουσιαστική υποστήριξη για να ανταποκριθούν αποτελεσματικά, συμπεριλαμβανομένων των εγκληματολογικών υπηρεσιών και εμπειρογνωμοσύνης για παραβιάσεις δεδομένων (Muthuppalaniappan & Stevenson, 2021).

Οι ακόλουθες περιπτώσεις παραβίασης της κυβερνοασφάλειας αποτελούν παράδειγμα της ποικιλίας των επιθέσεων που αντιμετώπισε ο τομέας της υγειονομικής περίθαλψης σε διάφορα μέρη του κόσμου, τις συνέπειες αυτών των επιθέσεων και τα βήματα που έλαβαν οι οργανισμοί.

Το Lukaskrankenhaus Neuss είναι ένα δημόσιο νοσοκομείο που ιδρύθηκε το 1911 στο Neuss της Γερμανίας με 537 κρεβάτια και 1400 υπαλλήλους. Τον Φεβρουάριο του 2016, οι εργαζόμενοι αντιμετώπισαν διάφορα μηνύματα σφάλματος από μια επίθεση ransomware που ξεκίνησε μέσω μιας τακτικής κοινωνικής μηχανικής. Σε απάντηση, το νοσοκομείο πήρε διακομιστές και συστήματα υπολογιστών εκτός σύνδεσης για να αξιολογήσει και να καθαρίσει μολυσμένα συστήματα. Εν τω μεταξύ, το προσωπικό κατέφυγε στη χρήση στυλό, χαρτί και φαξ για να συνεχίσει την εργασία του, αλλά χρειάστηκε να αναβάλει τις διαδικασίες υψηλού κινδύνου (Steffen, 2016).

Ενώ το νοσοκομείο δεν έλαβε κάποια απαίτηση να καταβάλει χρήματα, του δόθηκε μια διεύθυνση email για να επικοινωνήσει για περαιτέρω οδηγίες. Δεν έγινε καμία προσπάθεια επικοινωνίας με τους επιτιθέμενους όπως συνέστησαν οι τοπικές αρχές (Steffen, 2016). Το νοσοκομείο ανέφερε ότι το εφεδρικό του σύστημα διατηρήθηκε ενημερωμένο και χάθηκαν μόνο λίγες ώρες δεδομένων, αλλά μια καθυστέρηση χειρόγραφων εγγραφών από την στιγμή που τα συστήματα υπολογιστών ήταν εκτός σύνδεσης πρέπει τελικά να ενσωματωθούν με τον υπόλοιπο ηλεκτρονικό φάκελο (Steffen, 2016). Ο εκπρόσωπος του νοσοκομείου προέβλεψε ότι θα χρειαστούν λίγους μήνες προτού η ροή εργασίας τους επιστρέψει στο status quo (Zorz, 2016). Δεν υπήρχε ένδειξη ότι παραβιάστηκαν τα δεδομένα των ασθενών.

Η Περιφερειακή Αρχή Υγείας της Νοτιοανατολικής Νορβηγίας (Νοτιοανατολική RHF) είναι

ένας κρατικός οργανισμός ειδικευμένων νοσοκομείων και υπηρεσιών υγείας που δημιουργήθηκε το 2002 μαζί με τρεις άλλες περιφερειακές αρχές. Τον Ιανουάριο του 2018, το Νοτιοανατολικό RHF ανακοίνωσε ότι το PHI και τα αρχεία σχεδόν 2,9 εκατομμυρίων ανθρώπων (περισσότερο από το μισό του πληθυσμού της Νορβηγίας) είχαν παραβιαστεί (Khandelwal, 2018). Υποψιάζεται ότι μια εξελιγμένη εγκληματική ομάδα από ξένο κατάσκοπο ή κρατική υπηρεσία ηγήθηκε της επίθεσης με στόχο τόσο τα δεδομένα υγείας των ασθενών όσο και την αλληλεπίδραση της υπηρεσίας υγείας με τις ένοπλες δυνάμεις της Νορβηγίας (Hughes, 2018). Η ευπάθεια θεωρείται ότι προέρχεται από το παλαιό σύστημα, τα Windows XP (Hughes, 2018). Ενώ ο οργανισμός είχε ξεκινήσει μέτρα ασφαλείας για να μειώσει τους κινδύνους που ενέχουν τα Windows XP μαζί με ένα σχέδιο για την σταδιακή κατάργησή του, η επίθεση έλαβε χώρα πριν μπορέσουν να εφαρμόσουν τα μέτρα ασφαλείας (Irwin, 2018).

Ενώ αυτή η επίθεση δεν φαίνεται να δημιουργεί κινδύνους για την ασφάλεια των ασθενών ή καθυστερήσεις στις νοσοκομειακές επεμβάσεις, το γεγονός έθεσε ανησυχίες σχετικά με μελλοντικές επιθέσεις σε δεδομένα υγείας με σκοπό το πολιτικό κέρδος και χρησίμευσε ως έκκληση αφύπνισης για τον GDPR. Σύμφωνα με τον GDPR, ο οργανισμός θα έπρεπε να ειδοποιήσει τους πληγέντες εντός 72 ωρών, κάτι που δεν το έκανε (Warwick, 2018).

Το Περιφερειακό Νοσοκομείο Hancock είναι ένα μικρό μη κερδοσκοπικό νοσοκομείο (71 κλίνες) στο Greenfield της Ιντιάνα που ιδρύθηκε το 1951. Στις 11 Ιανουαρίου 2018, η Hancock Regional αντιμετώπισε μια επίθεση ransomware από το κακόβουλο λογισμικό SamSam (Secureworks, 2018). Η επίθεση στόχευσε έναν διακομιστή στο σύστημα εφεδρικών αντιγράφων ασφαλείας έκτακτης ανάγκης και εξαπλώθηκε μέσω της ηλεκτρονικής σύνδεσης μεταξύ του ιστότοπου δημιουργίας αντιγράφων ασφαλείας, που βρίσκεται μίλια από την κεντρική πανεπιστημιούπολη, και τη φάρμα διακομιστών στο νοσοκομείο (Long, 2018). Ανακαλύφθηκε αργότερα ότι οι χάκερ είχαν καταστρέψει μόνιμα στοιχεία των αρχείων αντιγράφων ασφαλείας από πολλά συστήματα, εκτός από τα αρχεία αντιγράφων ασφαλείας των ηλεκτρονικών ιατρικών αρχείων. Οι ερευνητές διαπίστωσαν ότι η επίθεση πραγματοποιήθηκε χρησιμοποιώντας το πρωτόκολλο απομακρυσμένης επιφάνειας εργασίας της Microsoft ως σημείο εισόδου στο διακομιστή και ότι οι εισβολείς είχαν θέσει σε κίνδυνο τον διαχειριστικό λογαριασμό ενός προμηθευτή υλικού για να ξεκινήσουν την επίθεση (Hughes, 2018).

Μετά την επίθεση, η ομάδα πληροφορικής του νοσοκομείου έκλεισε όλα τα συστήματα δικτύου και επιτραπέζιων υπολογιστών. Ωστόσο, οι νοσοκομειακές επεμβάσεις συνεχίστηκαν εντός των ορίων των διαδικασιών διακοπής λειτουργίας τους. Οι ασθενείς δεν εκτράπηκαν και το νοσοκομείο δεν έκλεισε. Οι χάκερς ζήτησαν τέσσερα Bitcoin (55.000 USD) για τα λύτρα και το νοσοκομείο πλήρωσε. Στη συνέχεια, το προσωπικό πληροφορικής πέρασε τις επόμενες τρεισήμισι μέρες αποκρυπτογραφώντας αρχεία και προσπαθώντας να λειτουργήσει κανονικά το σύστημα (Long, 2018). Δεν βρήκαν στοιχεία που να αποδεικνύουν ότι τα δεδομένα των ασθενών έχουν παραβιαστεί. Ο Διευθύνων Σύμβουλος, Steve Long, δήλωσε ότι η επίθεση βρέθηκε ότι ήταν μια προκαθορισμένη στοχευμένη επίθεση στη μονάδα υγειονομικής περίθαλψης, από μια περίπλοκη εγκληματική ομάδα και δημοσίευσε ένα άρθρο που εξηγούσε την απόφασή τους να πληρώσουν τα λύτρα (Long, 2018).

Η ευαισθητοποίηση των επαγγελματιών υγείας σχετικά με τις απειλές στον κυβερνοχώρο, τα τρωτά σημεία και οι επιπτώσεις που ακολουθούν, παίζουν καθοριστικό ρόλο για τα συστήματα της υγειονομικής περίθαλψης. Η ασφάλεια στον κυβερνοχώρο δεν μπορεί να είναι πλήρως αποτελεσματική, επομένως η απειλή στην υγειονομική περίθαλψη είναι αναπόφευκτη αφού αυτός ο τομέας στοχεύει συνήθως στο οικονομικό κέρδος. Η κυβερνοασφάλεια στοχεύει επίσης στην προστασία της εμπιστευτικότητας, της ακεραιότητας και της διαθεσιμότητας των πολύτιμων δεδομένων της υγειονομικής περίθαλψης. Απώτερος στόχος της ασφάλειας του κυβερνοχώρου θα πρέπει να είναι η ενίσχυση της ανθεκτικότητας. Μια απλή προσέγγιση για τη βελτίωση της ανθεκτικότητας όπως αναφέρει χαρακτηριστικά ο Martin et al, (2017), είναι η διατήρηση ασφαλούς ενημέρωσης και ανανέωσης των αντιγράφων ασφαλείας έτσι ώστε η επίθεση να μην οδηγήσει σε μόνιμη απώλεια των δεδομένων.

Η οδηγία για την ασφάλεια δικτύων και πληροφοριών (NISD) 2016/1148 / ΕΕ, η οποία τέθηκε σε ισχύ τον Μάιο του 2018, έχει ως στόχο την εφαρμογή των ελάχιστων απαιτήσεων ασφάλειας και την δημιουργία κοινοποιήσεων ασφάλειας στον κυβερνοχώρο τόσο για τους χειριστές των βασικών υπηρεσιών όσο και για τους παρόχους ψηφιακών υπηρεσιών. Οι πάροχοι υγειονομικής περίθαλψης και συγκεκριμένα οι εργαζόμενοι των νοσοκομείων, χαρακτηρίζονται ως «φορείς εκμετάλλευσης» των βασικών υπηρεσιών στα περισσότερα κράτη μέλη της Ευρωπαϊκής Ένωσης. Επομένως, αυτοί οι οργανισμοί πρέπει να λαμβάνουν υπόψη την οδηγία και την αντίστοιχη εθνική νομοθεσία κατά τη σύναψη ενός προϊόντος ή μιας υπηρεσίας. Η οδηγία υπερβαίνει την εφαρμογή των απαιτήσεων ασφαλείας, καθώς

παρέχει εξουσία στους ρυθμιστικούς φορείς να ελέγχουν τους χειριστές των βασικών υπηρεσιών για να διασφαλίσουν το επίπεδο ασφάλειας στον κυβερνοχώρο του οργανισμού και να είναι αποδεκτό σύμφωνα με τις διατάξεις της οδηγίας που διέπεται.

Επίσης, ο κανονισμός ιατρικών συσκευών (MDR) είναι ένας νέος κανονισμός που περιλαμβάνει συγκεκριμένες διατάξεις που σχετίζονται με την ασφάλεια πληροφορικής (υλικό, λογισμικό κ.λπ.) για όλες τις ιατρικές συσκευές. Οι Γενικές Απαιτήσεις Ασφάλειας και Απόδοσης που ορίζονται στο MDR (Medical Devices / SW) περιλαμβάνουν:
- Την αξιοπιστία και απόδοση σύμφωνα με την προβλεπόμενη χρήση.
- Τις αρχές του κύκλου ζωής ανάπτυξης, της διαχείρισης κινδύνων, της επαλήθευσης και της επικύρωσης.
- Τη χρήση λογισμικού σε συνδυασμό με πλατφόρμες φορητών υπολογιστών.
- Μέτρα ασφαλείας τεχνολογιών και πληροφοριών, συμπεριλαμβανομένης της προστασίας από μη εξουσιοδοτημένη πρόσβαση.

Στην ευρωπαϊκή πολιτική, προστίθεται και ο Γενικός Κανονισμός Προστασίας Δεδομένων (GDPR) ο οποίος ορίζει τους κανόνες για την επεξεργασία και την ελεύθερη κυκλοφορία των προσωπικών δεδομένων και ισχύει για όλους τους τομείς του δημόσιου και του ιδιωτικού τομέα. Ωστόσο, ορισμένες παρεκκλίσεις ορίζονται για δεδομένα που αφορούν την υγεία, με στόχο την προστασία των δικαιωμάτων των υποκειμένων δεδομένων και την εμπιστευτικότητα των προσωπικών τους δεδομένων για την υγεία και ταυτόχρονα της διατήρησης των πλεονεκτημάτων της επεξεργασίας δεδομένων για έρευνα. Ο GDPR θεωρεί ότι τα δεδομένα υγείας, είναι μια ειδική κατηγορία προσωπικών δεδομένων. Θεωρούνται ευαίσθητα δεδομένα και υπόκεινται σε συγκεκριμένες ορολογίες τόσο για τη θεραπεία όσο και για την πρόσβαση τρίτων (Χατζηπετρής, 2020).

Από τις 25 Μαΐου 2018, που τέθηκε σε εφαρμογή το νέο σύνολο κανόνων προστασίας δεδομένων προσωπικού χαρακτήρα, είχε ως στόχο, τον εκσυγχρονισμό του υφιστάμενου πλαισίου. Με τον κανονισμό αυτό, οι οργανισμοί, οι εταιρείες αλλά και οι επαγγελματίες, οφείλουν να διαφοροποιήσουν τον τρόπο με τον οποίο συλλέγουν, διαχειρίζονται, επεξεργάζονται και αποθηκεύουν πληροφορίες που περιέχουν προσωπικά δεδομένα. Ταυτόχρονα, οι πολίτες έχουν αποκτήσει νέα δικαιώματα ενισχύονταν την προστασία των προσωπικών δεδομένων με την επιβολή αυστηρών διοικητικών κυρώσεων.

Οι ιδιαιτερότητες που παρουσιάζει ο γενικός κανονισμός προστασίας των προσωπικών δεδομένων στην υγείας είναι η επεξεργασία των ευαίσθητων δεδομένων των ασθενών τα οποία είναι σε μεγάλη κλίμακα ενώ υπάρχουν και πολλές δραστηριότητες επεξεργασίας. Η επεξεργασία των δεδομένων εκτελείται από πολλούς εργαζόμενους και κατά συνέπεια υπάρχουν πολλοί δέκτες που λαμβάνουν αυτά τα δεδομένα. Με την υιοθέτηση του ISO 277700 περιλαμβάνεται η κρυπτογράφηση των δεδομένων προσωπικού χαρακτήρα με αποτέλεσμα την συμμόρφωση με το GDRP.

Επομένως με την οδηγία προστασίας δεδομένων της Ευρωπαϊκής ένωσης, οι φορείς επεξεργασίας δεδομένων προσωπικού χαρακτήρα πρέπει να συμμορφώνονται με τις υποχρεώσεις προστασίας των δεδομένων, όπου περιλαμβάνει τη διασφάλιση για δίκαιη και νόμιμη επεξεργασία των δεδομένων.

Για την ενίσχυση της ασφάλειας των νοσοκομείων από επιθέσεις στον κυβερνοχώρο, οι υπεύθυνοι χάραξης πολιτικής, πρέπει να εφαρμόσουν πολιτικές που όχι μόνο θα αυξήσουν το επίπεδο και το στόχο των δυνατοτήτων ασφάλειας στον κυβερνοχώρο, αλλά και να μειώσουν τη μεταβλητότητα της διαθεσιμότητας των πόρων σε ολόκληρο το σύστημα υγείας (Jalali & Kaiser, 2018). Ταυτόχρονα η ασφάλεια στο κυβερνοχώρο, θα επιτευχθεί με προγράμματα ευαισθητοποίησης και εκπαίδευσης του προσωπικού έτσι ώστε να είναι εύκολο να κατανοήσουν και να εφαρμόσουν τις πρακτικές για προστασία των δεδομένων (Kim, 2017). Συγκεκριμένες πρακτικές αποτελούν τα αντίγραφα ασφαλείας αφού διατηρείται η ανθεκτικότητα και η συνεχής ενημέρωση του λογισμικού. Η εμπιστευτικότητα επιτυγχάνεται με την ανωνυμοποίηση των δεδομένων δηλαδή, με την αφαίρεση αναγνωριστικών στοιχείων των ασθενών (Coventry & Branley, 2018).

Η αναγκαιότητα για την παρούσα μελέτη προκύπτει από το γεγονός ότι οι εγκληματίες του κυβερνοχώρου εκμεταλλεύονται όλο και περισσότερο τα λάθη των τελικών χρηστών παρά τα τρωτά σημεία του υλικού, του λογισμικού και του συστήματος. Οι χρήστες λόγω ελλιπής εκπαίδευσης κάνουν κλικ σε κακόβουλες ιστοσελίδες όπου γίνεται ηλεκτρονικό ψάρεμα πληροφοριών (phishing) με αποτέλεσμα να αποκαλύπτονται ευαίσθητες πληροφορίες. Η εκπαίδευση των χρηστών αποτελεί αναπόσπαστο κομμάτι του οργανισμού αφού η διαρροή των δεδομένων προέρχεται από την άγνωστη διαχείριση των κακόβουλων λογισμικών δηλαδή την διαχείριση ύποπτων email και κοινοποίησης των προσωπικών τους κωδικών.

Κρίνεται σημαντικό να οριστούν και να διαχειριστούν οι κίνδυνοι των τελικών χρηστών, έτσι ώστε οι οργανώσεις όπως τα νοσοκομεία, να μπορούν να υιοθετήσουν πρακτικές, με επίκεντρο των άνθρωπο, για την ασφάλεια του κυβερνοχώρου προκειμένου να προστατεύσουν αποτελεσματικότερα τους ασθενείς και τα δεδομένα. Επομένως το ζητούμενο ερευνητικό ερώτημα είναι, ποια είναι η ευαισθητοποίηση των επαγγελματιών υγείας σχετικά με την ασφάλεια στο κυβερνοχώρο;

2. Εννοιολογικοί προσδιορισμοί

2.1 Πληροφορίες

Η πληροφορίες ορίζονται τα δεδομένα στα οποία έχει προσδοθεί η σχετικότητα και ο σκοπός. Κύριο χαρακτηριστικό, είναι να υπάρχει νόημα, να είναι οργανωμένα ώστε να εξυπηρετούν ένα συγκεκριμένο σκοπό. Οι πληροφορίες, αφορούν την συλλογή δεδομένων με τις ενδεδειγμένες επεξηγήσεις, ερμηνείες καθώς και άλλες πληροφορίες που αφορούν συγκεκριμένο συμβάν, αντικείμενο ή διαδικασία (Κούμπουρος, 2015). Επομένως, οι πληροφορίες όπως αναφέρουν οι Hovenga & Sermeus (2009), γίνονται γνώση από την στιγμή που θα συντεθούν, έτσι ώστε οι δια-σχέσεις μεταξύ πληροφοριών από διάφορες πηγές να προσδιοριστούν και να τυποποιηθούν.

2.2 Δεδομένα

Ορίζονται ως το σύνολο των διακριτών αντικειμενικών στοιχείων τα οποία σχετίζονται με ένα γεγονός ή μια διαδικασία που από μόνα τους δεν έχουν ιδιαίτερη χρησιμότητα εάν δεν μετατραπούν σε πληροφορίες. Τα δεδομένα γίνονται πληροφορίες όταν συνδυάζονται, ερμηνεύονται, οργανώνονται και δομούνται μέσα σε κάποιο πλαίσιο για να αποδώσουν πρόσθετο νόημα (Hovenga & Sermeus 2009; Κούμπουρος, 2015).

Τα δεδομένα μετατρέπονται σε πληροφορίες κυρίως μέσα από πέντε βασικές διαδικασίες (Κούμπουρος, 2015):

- Συγκέντρωση: κάποια δεδομένα συνοψίζονται σε μια πιο περιεκτική μορφή, και έτσι απαλείφονται οι άχρηστες λεπτομέρειες.
- Συσχέτιση: ο σκοπός ή ο λόγος που γίνεται η συλλογή των δεδομένων είναι γνωστός ή κατανοητός από προηγουμένως.
- Υπολογισμός: Για να εξαχθούν χρήσιμες πληροφορίες, τα δεδομένα τυγχάνουν επεξεργασίας και αθροίζονται.
- Κατηγοριοποίηση: ταξινόμηση των δεδομένων σε συγκεκριμένους τύπους ή κατηγορίες.
- Διόρθωση: εξαλείφονται πιθανά σφάλματα.

2.3 Τελικός χρήστης

Ο ορισμός τελικός χρήστης αφορά τον χρήστη για τον οποίο σχεδιάστηκε ένα σύστημα και θα είναι ο τελικός αποδέκτης των υπηρεσιών που εμπεριέχονται σε αυτό. Οι τελικοί χρήστες δεν είναι οι τεχνικοί που αναπτύσσουν, συντηρούν ή επιβλέπουν ένα σύστημα, αλλά ούτε και αυτοί που χρηματοδοτούν τη δημιουργία του (Μητάκος, 2015).

2.4 Κυβερνοχώρος

Ο κυβερνοχώρος είναι ένας παγκόσμιος και δυναμικός τομέας ο οποίος υπόκειται σε συνεχείς αλλαγές και χαρακτηρίζεται από τη συνδυασμένη χρήση ηλεκτρονίων και ηλεκτρομαγνητικού φάσματος. Σκοπός του είναι η δημιουργία, η αποθήκευση, η τροποποίηση, η ανταλλαγή, η κοινή χρήση και εξαγωγή, η χρήση και η εξάλειψη πληροφοριών.

Ο κυβερνοχώρος περιλαμβάνει (Mayer, 2014):

α) φυσικές υποδομές και συσκευές τηλεπικοινωνιών που επιτρέπουν τη σύνδεση τεχνολογικών δικτύων και συστημάτων επικοινωνιών, οι οποίες είναι κατανοητές με την ευρύτερη έννοια (smartphone / tablet, υπολογιστές, διακομιστές κ.λπ.).

β) συστήματα υπολογιστών και το σχετικό λογισμικό που εγγυώνται τη βασική λειτουργική λειτουργία και συνδεσιμότητα του τομέα.

γ) δίκτυα μεταξύ συστημάτων υπολογιστών.

δ) δίκτυα που συνδέουν συστήματα υπολογιστών.

ε) τους κόμβους πρόσβασης χρηστών και διαμεσολαβητών που δρομολογούν κόμβους.

2.5 Κυβερνοασφάλεια

Η κυβερνοασφάλεια είναι η οργάνωση και η συλλογή πόρων, των διαδικασιών και των

δομών που χρησιμοποιούνται για την προστασία του κυβερνοχώρου και των συστημάτων από περιστατικά του κυβερνοχώρου που δεν ευθυγραμμίζονται de jure από τα de facto δικαιώματα ιδιοκτησίας (Craigen et al, 2014).

Η αποδόμηση αυτού του ορισμού αναλύεται ως εξής (Craigen et al, 2014):

- «οργάνωση και συλλογή πόρων, διαδικασιών και δομών». Η συγκεκριμένη πτυχή καταγράφει τις πολλαπλές, συνυφασμένες διαστάσεις και την εγγενή πολυπλοκότητα της ασφάλειας στον κυβερνοχώρο, οι οποίες φαινομενικά περιλαμβάνουν τις αλληλεπιδράσεις μεταξύ ανθρώπων και συστημάτων.

- «χρησιμοποιείται για την προστασία του κυβερνοχώρου και των συστημάτων». Αυτή η πτυχή περιλαμβάνει την προστασία, με την ευρύτερη έννοια, από όλες τις απειλές, συμπεριλαμβανομένων των εκ προθέσεως, τυχαίων και φυσικών κινδύνων. Η προστασία ισχύει για περιουσιακά στοιχεία και πληροφορίες που αφορούν τον κυβερνοχώρο και τα συνδεδεμένα συστήματα.

- «Ότι δεν ευθυγραμμίζεται de jure από τα δικαιώματα ιδιοκτησίας de facto». Αυτή η πτυχή ενσωματώνει τις δύο ξεχωριστές έννοιες της ιδιοκτησίας και του ελέγχου που κυριαρχούν στη συζήτηση για την ασφάλεια στον κυβερνοχώρο και τα ψηφιακά περιουσιακά στοιχεία που εισάγονται στο πλαίσιο δικαιωμάτων ιδιοκτησίας, που περιλαμβάνουν πρόσβαση, εξαγωγή, συνεισφορά, αφαίρεση, διαχείριση, αποκλεισμό και αποξένωση. Κάθε γεγονός ή δραστηριότητα που δεν ευθυγραμμίζει τα πραγματικά (de facto) δικαιώματα ιδιοκτησίας από τα αντιληπτά (de jure) δικαιώματα ιδιοκτησίας, είτε από πρόθεση είτε από ατύχημα, είτε είναι γνωστά είτε άγνωστα, είναι ένα συμβάν ασφάλειας στον κυβερνοχώρο.

2.6 Κυβερνοεπίθεση

Η κυβερνοεπίθεση ορίζεται η σταδιακή και αργή αλλοίωση ή διάρρηξη ενός συστήματος ενδιαφέροντος – στόχου από τον επιτιθέμενο. Η κυβερνοεπίθεση ξεκινάει από έναν υπολογιστή εναντίον άλλου υπολογιστή ή ιστότοπου, με απώτερο στόχο να πληγεί η ακεραιότητα, η εμπιστευτικότητα ή η διαθεσιμότητα του στόχου και των πληροφοριών που

αποθηκεύονται σε αυτό (Κόλλια, 2017).

2.7 Τύποι κυβερνοεπιθέσεων

Οι απειλές στον κυβερνοχώρο, αποτελούν κακόβουλες ενέργειες είτε από ένα άτομο είτε από ένα οργανισμό, με απώτερο σκοπό την κλοπή δεδομένων και ζημιάς στον υπολογιστή, στα συστήματα και τα δίκτυα. Ενώ πολλοί τύποι επιθέσεων έχουν ήδη εντοπιστεί και καθοριστεί, οι πιο συνηθισμένοι αποτελούνται από:

- ιούς
- κακόβουλα λογισμικά
- ηλεκτρονικό ψάρεμα (phishing)
- άρνηση παροχής υπηρεσιών
- παραβιάσεις δεδομένων

Οι απώλειες που παρατηρούνται λόγω αυτών των κυβερνοεπιθέσεων, μπορούν να λάβουν πολλές μορφές και επηρεάζουν διάφορα τμήματα ενός οργανισμού. Για την αντιμετώπιση αυτών των επιθέσεων, είναι ζωτικής σημασίας για τους οργανισμούς και για τα άτομα του, να βελτιστοποιήσουν την επένδυση ή τις δαπάνες, που σχετίζονται με την ασφάλεια στον κυβερνοχώρο, με βάση τα διάφορα είδη πιθανών επιθέσεων (Roumani et al., 2016; Ahmed et al., 2020).

2.8 Πρότυπα και νομοθεσίες

Στην διεθνή πολιτική τα πρότυπα και οι νομοθεσίες είναι διαφορετικά σε σχέση με τα ευρωπαϊκά, χωρίς βέβαια να υπάρχουν σημαντικές διαφορές. Υπάρχουν οι κανόνες προστασίας προσωπικών δεδομένων και ασφάλεια του HIPPA, το πρόγραμμα κοινής διασφάλισης HITRUST και διάφορα πρότυπα για την επαρκή ασφάλεια των πληροφοριών.

Το HIPAA είναι το ακρωνύμιο του νόμου περί φορητότητας και λογοδοσίας για την ασφάλιση υγείας που ψηφίστηκε από το Κογκρέσο το 1996. Αυτή ήταν η αρχή της πίεσης της κυβέρνησης για μηχανογράφηση των αρχείων ασθενών και οδήγησε στους κανόνες προστασίας προσωπικών δεδομένων και ασφάλειας του HIPAA που διέπουν τον τρόπο με τον οποίο οι οντότητες ασφαλείς διαχειρίζονται τα δεδομένα ασθενών με τους οποίους συνεργάστηκαν. Οι κανόνες προστασίας προσωπικών δεδομένων και ασφάλειας του HIPAA

καθορίζουν ένα σύνολο προτύπων ασφαλείας που πρέπει να αντιμετωπίζονται από «καλυπτόμενες οντότητες», όπου κωδικοποιούνται σε τέσσερις κανόνες:

- Κανόνας απορρήτου του HIPAA
- Κανόνας ασφαλείας HIPAA
- Κανόνας επιβολής του HIPAA
- Κανόνας ειδοποίησης παραβίασης HIPAA.

Με απλά λόγια, το HIPAA παρέχει τη δυνατότητα μεταφοράς και συνέχισης ασφαλιστικής κάλυψης υγείας για εκατομμύρια Αμερικανούς εργαζομένους και τις οικογένειές τους όταν αλλάζουν ή χάνουν τη δουλειά τους, μειώνει την απάτη και την κακοποίηση της υγειονομικής περίθαλψης, επιβάλλει σε όλη τη βιομηχανία πρότυπα για πληροφορίες περί υγειονομικής περίθαλψης σχετικά με την ηλεκτρονική χρέωση και άλλες διαδικασίες και απαιτεί την προστασία και τον εμπιστευτικό χειρισμό προστατευόμενων πληροφοριών για την υγεία (California Department of Health Care Services).

Το HITRUST, αναπτύχθηκε σε συνεργασία με τους επαγγελματίες υγείας και της ασφάλειας των πληροφοριών. Το κοινό πλαίσιο ασφάλειας (Common Security Framework) είναι από τα πρώτα πλαίσια ασφάλειας που αναπτύχθηκαν τα οποία αφορούν πληροφορίες στο τομέα της υγείας. Το πρόγραμμα διασφάλισης HITRUST παρέχει μια απλοποιημένη αξιολόγηση της συμμόρφωσης και της υποβολής των εκθέσεων για HIPAA και HITECH συμπεριλαμβανομένων και των απαιτήσεων των συνεργατών αλλά και των επιχειρήσεων.

Το πρόγραμμα HITRUST CSF, βασίζεται σε ένα γενικό πλαίσιο προτύπων ασφαλείας (ISO, HIPAA, NIST και PCI) και παρέχει στους οργανισμούς υγειονομικής περίθαλψης και στους συνεργάτες τους, μια κοινή προσέγγιση για τη διαχείριση των αξιολογήσεων ασφαλείας που βελτιώνει την αποτελεσματικότητα ενώ ταυτόχρονα περιέχει δαπάνες που συνδέονται με πολλαπλές και ποικίλες απαιτήσεις διασφάλισης (https://hitrustalliance.net/).

Το Εθνικό Ινστιτούτο Προτύπων και Τεχνολογίας (NIST) ιδρύθηκε το 1901 και είναι μια ομοσπονδιακή υπηρεσία όπου έχει ως αποστολή την προώθηση της καινοτομίας και της βιομηχανικής ανταγωνιστικότητας στις ΗΠΑ (Michalsky, 2013). Το Ινστιτούτο είναι αρμόδιο για την ανάπτυξη των προτύπων και των κατευθυντήριων γραμμών, συμπεριλαμβανομένων και των ελάχιστων απαιτήσεων, που χρησιμοποιούνται από τις

ομοσπονδιακές υπηρεσίες για την παροχή επαρκούς ασφάλειας πληροφοριών αλλά και για την προστασία των πράξεων και των περιουσιακών στοιχείων μιας υπηρεσίας. Το Ινστιτούτο έχει αναπτύξει κατευθυντήριες γραμμές για τη βελτίωση της αποδοτικότητας και της αποτελεσματικότητας του σχεδιασμού, της εφαρμογής, της διαχείρισης και της λειτουργίας της τεχνολογίας και πληροφοριών (Scholl et al., 2008).

Το NIST παρέχει διάφορα έγγραφα τα οποία είναι ευρέως γνωστά για την ασφάλεια των δικτύων και των δεδομένων. Αν και προορίζονται συνήθως για ομοσπονδιακές υπηρεσίες των ΗΠΑ, χρησιμοποιούνται ευρέως και στον ιδιωτικό τομέα.

Τα τρία πιο δημοφιλή είναι το Πλαίσιο του NIST για τη βελτίωση της κρίσιμης υποδομής της κυβερνοασφάλειας, το NIST SP 800-53 και το NIST SP 800-171.

Λόγω των αυξανόμενων πιέσεων από απειλές, τόσο εξωτερικές όσο και εσωτερικές, οι οργανισμοί που είναι οι αρμόδιοι για την κρίσιμη υποδομή οφείλουν να έχουν μια συνεπή και επαναληπτική προσέγγιση για τον εντοπισμό, την αξιολόγηση και τη διαχείριση του κινδύνου ασφάλειας στον κυβερνοχώρο. Αυτή η προσέγγιση κρίνεται απαραίτητη, ανεξάρτητα από το μέγεθος του οργανισμού, την έκθεση σε απειλές ή την πολυπλοκότητα της κυβερνοασφάλειας.

Συγκεκριμένα, το πλαίσιο περιλαμβάνει μια μεθοδολογία για την προστασία της ιδιωτικής ζωής και των ατομικών ελευθεριών, ενώ μερικοί οργανισμοί υποδομής διεξάγουν δραστηριότητες για την κυβερνοασφάλεια. Πολλοί οργανισμοί έχουν ήδη θεσπίσει διαδικασίες για την αντιμετώπιση της ιδιωτικής ζωής αλλά και των πολιτικών ελευθεριών. Η μεθοδολογία έχει σχεδιαστεί για να συμπληρώνει τέτοιες διαδικασίες και να παρέχει καθοδήγηση για τη διευκόλυνση σε περιπτώσεις απορρήτου. Η ενσωμάτωση της ιδιωτικής ζωής και της ασφάλειας στον κυβερνοχώρο μπορεί να ωφελήσει τους οργανισμούς αφού με αυτό το τρόπο, αυξάνουν την εμπιστοσύνη των πελατών τους, επιτρέποντας μια πιο τυποποιημένη ανταλλαγή πληροφοριών και απλοποιώντας τις λειτουργίες σε όλα τα νομικά πλαίσια.

Το Πλαίσιο παραμένει αξιόπιστο και αποτελεσματικό αφού υποστηρίζει την τεχνική καινοτομία λόγω του ότι είναι τεχνολογικά ουδέτερο, ενώ ταυτόχρονα αναφέρεται σε μια ποικιλία υφιστάμενων προτύπων, οδηγιών και πρακτικών που εξελίσσονται με την

τεχνολογία (NIST,2018).

Η επιλογή και η εφαρμογή των ελέγχων ασφαλείας για τα συστήματα πληροφοριών είναι σημαντικά καθήκοντα σε ένα οργανισμό και μπορούν να έχουν σημαντικές επιπτώσεις στις επιχειρήσεις και στα προσωπικά στοιχεία που διαθέτουν οι οργανισμοί.

Το NIST 800-53 συμβάλει στη διαχείριση του κινδύνου της ασφάλειας πληροφοριών σε τρία διαφορετικά επίπεδα, το επίπεδο οργάνωσης, το επίπεδο αποστολής και επιχειρηματικής διαδικασίας και το επίπεδο συστήματος πληροφοριών. Οι έλεγχοι ασφαλείας που ορίζονται στους οργανισμούς για να ικανοποιηθούν οι απαιτήσεις ασφάλειας των πληροφοριών, πρέπει να χρησιμοποιούνται ως μέρος μιας καθορισμένης διαδικασίας διαχείρισης κινδύνου που να υποστηρίζει οργανωτικά προγράμματα ασφάλειας πληροφοριών.

Η ειδική έκδοση 800-53, παρέχει μια ολοκληρωμένη προσέγγιση στην ασφάλεια των πληροφοριών και τη διαχείριση κινδύνων, παρέχοντας έτσι στους οργανισμούς το εύρος και το βάθος στους ελέγχους ασφαλείας, όπου είναι απαραίτητο για την ουσιαστική ενίσχυση των συστημάτων πληροφοριών και των περιβαλλόντων στα οποία λειτουργούν αυτά τα συστήματα. Με αυτό το τρόπο τα συστήματα είναι πιο ανθεκτικά έναντι των κυβερνοεπιθέσεων και σε άλλες απειλές (NIST, 2020).
Το NIST SP 800-171, είναι μια ειδική έκδοση NIST όπου περιλαμβάνει κάποιες προτεινόμενες απαιτήσεις, για την προστασία του απορρήτου των ελεγχόμενων μη ταξινομημένων πληροφοριών (CUI). Οι ενδιαφερόμενοι πρέπει να εφαρμόσουν τις συνιστώμενες απαιτήσεις που περιλαμβάνονται στο NIST SP 800-171 ώστε να αποδείξουν την παροχή επαρκούς ασφάλειας και την προστασία των αμυντικών πληροφοριών που περιλαμβάνονται στα αμυντικά τους συμβόλαια (NIST 2017).

Ακόμη ένας διεθνής οργανισμός είναι το Center for Internet Security (CIS) ο οποίος είναι ένας μη κερδοσκοπικός οργανισμός που διατηρεί τους 20 κρίσιμους ελέγχους ασφαλείας (CSC, πρώην γνωστός ως SANS 20), με αναγνωρισμένες βέλτιστες πρακτικές για την ασφάλεια συστημάτων και δεδομένων πληροφορικής. Το CSC είναι μια λίστα πρακτικών ασφάλειας στον κυβερνοχώρο που αναστέλλει τις πιο κοινές επιθέσεις (www.cisecurity.org).

2.9 Εφαρμογές ανταλλαγής δεδομένων. Η περίπτωση του epSOS

Το πρόγραμμα epSOS είναι ένα πιλοτικό έργο μεγάλης κλίμακας όπου πραγματοποιείται σε διάφορες ευρωπαϊκές χώρες για να βοηθήσει τους Ευρωπαίους στον τομέα της υγείας. Το πρόγραμμα epSOS (Έξυπνες Ανοιχτές Ηλεκτρονικές Υπηρεσίες για τους Ευρωπαίους Ασθενείς), είναι ένα πανευρωπαϊκό έργο που άρχισε τον Ιούλιο του 2008. Επικεντρώνεται στην πρόσβαση των πολιτών σε υπηρεσίες της υγείας όταν βρίσκονται εκτός της χώρας διαμονής τους. Έτσι κάθε χώρα που λαμβάνει μέρος στο epSOS δίνει το δικαίωμα κάθε πολίτη της, να δικαιούται να κάνει χρήση των υπηρεσιών epSOS, στην περίπτωση που χρειάζεται ιατρική φροντίδα, ενώ βρίσκεται σε μια άλλη συμμετέχουσα χώρα του epSOS (epSOS, 2021).

Επομένως ο κύριος στόχος του epSOS είναι να αναπτύξει ένα πρακτικό πλαίσιο ηλεκτρονικής υγείας και κατάλληλες υποδομές που θα επιτρέπουν στα διάφορα μη εθνικά ευρωπαϊκά συστήματα υγειονομικής περίθαλψης, να έχουν ασφαλή πρόσβαση στις πληροφορίες αναφορικά με την υγεία του ασθενούς.

Το epSOS μετά από έρευνες έχει εντοπίσει δύο διαφορετικές υπηρεσίες ηλεκτρονικής υγείας για τις οποίες αναζητούνται διαλειτουργικές μέθοδοι στη διασυνοριακή επικοινωνία. Αυτές οι δύο υπηρεσίες είναι ο φάκελος ασθενούς και οι ηλεκτρονικές συνταγές (epSOS, 2021).
Μια σπουδαία επέκταση του προγράμματος epSOS είναι η αποτελεσματική εξυπηρέτηση των ασθενών. Όπως βλέπουμε στο πιο πάνω σχήμα, ένας ασθενής από την χώρα Α θα εξεταστεί από γιατρό στη χώρα Β. Ο γιατρός αυτής της χώρας ζητά από τον ασθενή μια σύνοψη από τη χώρα καταγωγής του, ώστε ο γιατρός να έχει μια πιο ακριβής και σαφής εικόνα για τον ασθενή αυτό. Ακολούθως μετά από τη θεραπεία του ασθενούς γίνετε μια περίληψη στη χώρα Β όπου θα μεταφραστεί και στη χώρα Α για την ένταξη της περίληψη του ασθενούς στη χώρα προέλευσης (χώρα Α). Ο ασθενής στη χώρα Α δεν θα ενημερώνεται αυτόματα, η διαδικασία ένταξης των νέων στοιχείων και ενημέρωσης του ασθενούς έγκειται στην αρμοδιότητα της χώρας καταγωγής του ασθενούς.

Αυτή η περίπτωση εστιάζει στο να γίνετε γνωστό στους γιατρούς, της χώρα καταγωγής του ασθενούς, λεπτομέρειες σχετικά με τη θεραπεία ή διάγνωση του ασθενούς, ενώ ταξιδεύουν εκτός της χώρας καταγωγής τους. Αυτό είναι πολύ σπουδαίο για όλους, εφόσον αν θα κάνουν ένα ταξίδι και τους συμβεί το οτιδήποτε τότε ο γιατρός θα πάρει τις πληροφορίες που

χρειάζεται ώστε να έχει μια πιο ολοκληρωμένη εικόνα για τον ασθενή που βρίσκεται εκεί.

Ο κύριος στόχος του epSOS είναι να αποδείξει ότι είναι εφικτό για όλους τους πολίτες της Ευρωπαϊκής χώρας να μπορούν να απολαύσουν τα οφέλη των ηλεκτρονικών υπηρεσιών υγείας που λαμβάνουν στο σπίτι και όταν ταξιδεύουν στο εξωτερικό, χωρίς να θέτουν σε κίνδυνο τα δικαιώματά τους για την προστασία της ιδιωτικής τους ζωής και της εμπιστευτικότητας τους. Οι δύο αυτές υπηρεσίες epSOS που προσφέρονται σε πιλοτική βάση, έχουν δοκιμαστεί και έχουν ληφθεί τα κατάλληλα μέτρα διασφάλισης που απαιτούνται από την ευρωπαϊκή και την εθνική νομοθεσία.

Επιπλέον, εγγυάται στο επίπεδο της ασφάλειας και της προστασίας των πολιτών απέναντι στα δικαιώματα της ιδιωτικής τους ζωής, αλλά και έχει κριθεί σκόπιμο από όλες τις χώρες και περιφέρειες που συμμετέχουν σε αυτό το πρόγραμμα.

Το epSOS ακόμη είναι ένα έργο για τη διαλειτουργικότητα της ηλεκτρονικής υγείας που έχει σαν στόχο να κατασκευάσει και να αξιολογήσει μια υποδομή υπηρεσιών η οποία θα επιτρέπει τη διασυνοριακή διαλειτουργικότητα των συστημάτων ηλεκτρονικών μητρώων υγείας στην Ευρώπη, χωρίς να υπερβαίνει νομοθετικές ρυθμίσεις και ήδη υφιστάμενα εθνικά συστήματα (epSOS, 2021).

Το epSOS μετά από έρευνες έχει εντοπίσει δύο διαφορετικές υπηρεσίες ηλεκτρονικής υγείας για τις οποίες αναζητούνται διαλειτουργικές μέθοδοι στη διασυνοριακή επικοινωνία. Αυτές οι δύο υπηρεσίες είναι ο φάκελος ασθενούς και οι ηλεκτρονικές συνταγές. Σε αυτά στηρίζεται και το patient summary το οποίο χρησιμοποιείται για να αποθηκεύονται τα βασικά στοιχεία κάποιου ασθενή και συνεπώς και όλες οι πληροφορίες που αφορούν την υγεία του. Έτσι με αυτό τον τρόπο να υπάρχει καλύτερη αντιμετώπιση της υγείας του ασθενούς και να μπορεί οποιοσδήποτε επαγγελματίας της υγείας να μελετήσει το patient summary του ασθενή για να έχει μια ολοκληρωμένη εικόνα για το ιστορικό του και να καταλήξει σε πιο αποτελεσματική διάγνωση.

Επιπλέον το πρόγραμμα αυτό στηρίζεται στους ακόλουθους βασικούς άξονες:

- Υποστήριξη της κινητικότητας των ασθενών σε ολόκληρη την Ευρώπη. Μέσω του patient summary οι ευρωπαίοι πολίτες θα έχουν τη δυνατότητα να ταξιδεύουν με ασφάλεια σε όλη την Ευρώπη, αφού σε περίπτωση μιας απρογραμμάτιστης ή και προγραμματισμένης

περίθαλψης θα λαμβάνουν την καλύτερη δυνατή φροντίδα.

- Συνεπώς, με βάση το πιο πάνω χαρακτηριστικό το σύστημα οδηγεί και στην παροχή ασφαλέστερης υγειονομικής περίθαλψης. Ο γιατρός οποιασδήποτε χώρας στην Ευρωπαϊκή Ένωση μπορεί να προσφέρει την καλύτερη δυνατή φροντίδα σε κάθε Ευρωπαίο πολίτη αφού θα μπορεί να γνωρίζει τις σημαντικές πληροφορίες (π.χ. αλλεργίες) που χρειάζονται για την φροντίδα του.
- Προώθηση της συνεργασίας στον τομέα της υγείας μεταξύ των κρατών μελών της Ευρωπαϊκής Ένωσης. Οι πληροφορίες του ασθενή είναι προσβάσιμες και από άλλους γιατρούς άλλων χωρών της Ευρωπαϊκής Ένωσης με αποτέλεσμα να μπορεί να γίνει πιο εύκολα η ανταλλαγή απόψεων για κάποιο ιατρικό θέμα που αντιμετωπίζει κάποιος ασθενής.
- Αύξηση της αποτελεσματικότητας και της σχέσης κόστους- αποτελεσματικότητας της διασυνοριακής υγειονομικής περίθαλψης. Συμπίπτει με το προηγούμενο χαρακτηριστικό. Για παράδειγμα, ο ασθενής μπορεί να εξεταστεί στην χώρα του και τα αποτελέσματα των εξετάσεων του να διαγνωστούν από γιατρούς άλλων χωρών της Ευρωπαϊκής Ένωσης χωρίς να είναι απαραίτητο ο ασθενής να ταξιδέψει και να ξανά κάνει τις ίδιες εξετάσεις. Έτσι, μειώνεται το κόστος της διάγνωσης – θεραπείας του και παράλληλα βελτιστοποιείται η περίθαλψη του αφού η διάγνωση μπορεί να γίνει σε συνεργασία με πολλούς γιατρούς.

3. Μεθοδολογία

3.1 Συστηματική ανασκόπηση

Η συστηματική ανασκόπηση αποτελεί ανασκόπηση της βιβλιογραφίας όπου περιλαμβάνει μια συγκεκριμένη επιστημονική υπόθεση. Επομένως, επικεντρώνεται στην αναγνώριση, την εκτίμηση αλλά και στην επιλογή των βέλτιστων μεθοδολογικών σχεδιασμένων μελετών. Οι συστηματικές ανασκοπήσεις αποτελούν την πλέον αξιόπιστη πληροφορία σχετικά με την επιστημονική προσέγγιση και επομένως είναι απαραίτητο οι επιστήμονες υγείας και όχι μόνο, να γνωρίζουν τον τρόπο διεξαγωγής τους, καθώς και τον τρόπο ερμηνείας των αποτελεσμάτων τους (Γαλάνης, 2009).

Ο στόχος της συστηματικής ανασκόπησης είναι να προσδιορίσει όλα τα εμπειρικά στοιχεία που ταιριάζουν στα προκαθορισμένα κριτήρια ένταξης και να απαντήσουν σε μια συγκεκριμένη ερευνητική ερώτηση ή υπόθεση. Χρησιμοποιώντας ρητές και συστηματικές μεθόδους κατά τον έλεγχο άρθρων και όλων των διαθέσιμων αποδεικτικών στοιχείων, η προκατάληψη μπορεί να ελαχιστοποιηθεί, παρέχοντας έτσι αξιόπιστα ευρήματα από τα οποία μπορούν να εξαχθούν συμπεράσματα και να ληφθούν αποφάσεις (Snyder, 2019).

Υπάρχουν πολλά πλεονεκτήματα από τη εκπόνηση μιας συστηματικής ανασκόπησης. Μέσω αυτής, προσδιορίζεται εάν ένα αποτέλεσμα είναι σταθερό σε όλες τις μελέτες και ανακαλύπτεται ποιες μελλοντικές μελέτες απαιτείται να διεξαχθούν για να αποδειχθεί το αποτέλεσμα (Snyder, 2019).

3.2 Ημι-συστηματική ανασκόπηση

Η ημι-συστηματική ή αφηγηματική κριτική ανασκόπηση. αναφέρεται για θέματα που έχουν σχεδιαστεί διαφορετικά και έχουν μελετηθεί από διάφορες ομάδες ερευνητών σε διαφορετικούς κλάδους και εμποδίζουν την πλήρη συστηματική διαδικασία αναθεώρησης. Συγκεκριμένα, δεν είναι δυνατή η επανεξέταση κάθε άρθρου που θα μπορούσε να σχετίζεται με το θέμα, επομένως πρέπει να αναπτυχθεί μια διαφορετική στρατηγική. Υπάρχουν πολλά παραδείγματα άρθρων που χρησιμοποιούν αυτήν την προσέγγιση και δημοσιεύονται σε επιχειρηματικά πεδία. Εκτός από τον στόχο της επισκόπησης ενός θέματος, μια ημι-συστηματική ανασκόπηση συχνά εξετάζει πώς η έρευνα σε ένα επιλεγμένο πεδίο έχει προχωρήσει με την πάροδο του χρόνου ή πώς έχει αναπτυχθεί ένα θέμα σε όλες τις

ερευνητικές πτυχές. Γενικά, η ανασκόπηση επιδιώκει να εντοπίσει και να κατανοήσει όλες τις σχετικές ερευνητικές πτυχές που έχουν επιπτώσεις στο θέμα που μελετήθηκε και να τις συνθέσει χρησιμοποιώντας μετα-αφηγήσεις αντί να μετρήσει το μέγεθος του αποτελέσματος Επιπρόσθετα, ενώ καλύπτει μια ευρεία γκάμα από θέματα και διαφορετικούς τύπους μελετών, αυτή η προσέγγιση υποστηρίζει ότι η ερευνητική διαδικασία πρέπει να είναι διαφανής και πρέπει να έχει μια αναπτυγμένη ερευνητική στρατηγική ώστε να επιτρέπει στους αναγνώστες, να εκτιμήσουν εάν τα επιχειρήματα για τις αποφάσεις που πάρθηκαν, ήταν λογικά, τόσο για το επιλεγμένο θέμα όσο και από μια μεθοδολογική προοπτική (Snyder, 2019).

3.3 Ολοκληρωμένη ανασκόπηση

Σε σύγκριση με την ημι-δομημένη ανασκόπηση, η ολοκληρωμένη ανασκόπηση έχει συνήθως διαφορετικό σκοπό. Σκοπός της συγκεκριμένης ανασκόπησης είναι η αξιολόγηση, η κριτική και η σύνθεση της βιβλιογραφίας για ένα ερευνητικό θέμα, με ένα τρόπο ώστε να επιτρέπει την εμφάνιση των νέων θεωρητικών πλαισίων και προοπτικών. Οι περισσότερες ολοκληρωμένες ανασκοπήσεις, διεξάγονται για την αντιμετώπιση θεμάτων που έχουν μελετηθεί ξανά ή νέων αναδυόμενων θεμάτων. Στην περίπτωση των θεμάτων που μελετήθηκαν ξανά, ο σκοπός χρήσης της ολοκληρωμένης μεθόδου είναι η επισκόπηση της βάσης γνώσεων ή κριτική και ενδεχομένως εκ νέου εννοιολόγηση και επέκταση της θεωρητικής βάσης του συγκεκριμένου θέματος καθώς εξελίσσεται. Για πρόσφατα αναδυόμενα θέματα, ο σκοπός είναι να δημιουργηθούν αρχικές ή προκαταρκτικές αντιλήψεις και θεωρητικά μοντέλα, αντί να αναθεωρηθούν παλιά μοντέλα. Αυτός ο τύπος κριτικής απαιτεί συχνά μια πιο δημιουργική συλλογή δεδομένων, καθώς ο σκοπός συνήθως δεν καλύπτει όλα τα άρθρα που έχουν δημοσιευτεί ποτέ για το θέμα, επομένως συνδυάζει προοπτικές και ιδέες από διαφορετικά πεδία ή ερευνητικές παραδόσεις (Snyder, 2019).

3.4 Ανασκόπηση και ανάλυση παρούσας μελέτης

Στην παρούσα μελέτη, εφαρμόστηκε συστηματική ανασκόπηση της βιβλιογραφίας. Η ανεύρεση του υλικού έγινε με αναζήτηση της σχετικής ελληνικής και διεθνούς βιβλιογραφίας με τη χρήση της βάσης δεδομένων Google Scholar και Pubmed. Το Google Scholar, επιλέχθηκε γιατί βασίζεται πάνω σε διάφορα δίκτυα όπως τα BMJ, JAMA, Lancet, Science, Elsevier, Oxford, NEJM, CDC, τα οποία αποτελούν από μόνα τους πυλώνες αναζήτησης. Το

Pubmed, είναι μια δημόσια μηχανή αναζήτησης ιστού που αφορά ακαδημαϊκές δημοσιεύσεις και εργασίες.

Οι λέξεις κλειδιά που χρησιμοποιήθηκαν για την ανεύρεση του υλικού ήταν κυβερνοασφάλεια και υγεία (cybersecurity and health), κυβερνοασφάλεια και επαγγελματίες υγείας (cybersecurity and health care professionals), κυβερνοασφάλεια υγειονομικής περίθαλψης (healthcare cybersecurity), κυβερνοασφάλεια και ευαισθητοποίηση επαγγελματιών υγείας (cybersecurity and awareness of health professionals),.

Προκειμένου να αυξηθεί το αποτέλεσμα της αναζήτησης και ο αριθμός των μελετών, χρησιμοποιήθηκαν συνώνυμες φράσεις ή και συνδυασμός λέξεων με την χρήση των όρων «και», «ή», «όχι» (Μερκούρης, 2008).

Ο πιο κάτω πίνακας παρουσιάζει αναλυτικά τα αποτελέσματα στις μηχανές αναζήτησης με βάση τις λέξεις κλειδιά που χρησιμοποιήθηκαν συμπεριλαμβανομένων και των κριτηρίων που καθορίστηκαν.

Keywords	**Google Scholar**	**Pubmed**
Cybersecurity and health	16.600	372
Cybersecurity and health care professionals	5480	39
Healthcare cybersecurity	11.700	23

Ο καθορισμός των κριτηρίων εισαγωγής και αποκλεισμού της μελέτης αποτέλεσαν:

- ο τίτλος του επιστημονικού άρθρου, να ήταν συναφές με το θέμα που διερευνάται.
- η περίληψη να ήταν σαφές με το θέμα.
- η πρόσβαση σε ολόκληρο το άρθρο.
- τα άρθρα να ήταν γραμμένα στα ελληνικά ή αγγλικά.
- ο χρόνος δημοσίευσης των άρθρων, συμπεριλήφθηκαν αυτά που δημοσιεύτηκαν από το 2017 – 2021.

Επιπρόσθετα, το υλικό της συστηματικής ανασκόπησης αποτελούν και τα επιστημονικά περιοδικά, τα βιβλία της τελευταίας δεκαπενταετίας καθώς και οι περιλήψεις σε πρακτικά συνεδριών στο συγκεκριμένο θέμα. Στις περιπτώσεις που δεν ήταν δυνατή η πρόσβαση στο πλήρες κείμενο κάποιου άρθρου, εφαρμόστηκε επιπλέον αναζήτηση του τεύχους του επιστημονικού περιοδικού. Επίσης, οι βιβλιογραφικές παραπομπές των άρθρων και των ανασκοπήσεων που προέκυψαν από την αναζήτηση μελετήθηκαν μία προς μία για τον εντοπισμό περαιτέρω άρθρων.

Από την αρχική αναζήτηση, και βάσει των λέξεων-κλειδιών, προέκυψαν 124.858 μελέτες, από τις οποίες φιλτραρίστηκαν από την χρονολογία δημοσίευσης και απορρίφθηκαν οι 90,664 και παράλληλα απορρίφθηκαν επιπλέον 90,600 αφού ο τίτλος δεν σχετιζόταν με το περιεχόμενο της ανασκόπησης. Ακολούθως, από τις 64 μελέτες απορρίφθηκαν οι 50 επειδή το πλήρες κείμενο δεν ήταν διαθέσιμο. Έπειτα από μελέτη της περίληψης, εφαρμογή των κριτηρίων εισόδου και αποκλεισμού, καθώς και μελέτη ολόκληρου του κειμένου των άρθρων αξιολογήθηκαν οι υπόλοιπες 14 μελέτες, από τις οποίες προέκυψαν επτά που πληρούσαν τους σκοπούς της παρούσας ανασκόπησης, αφού αφορούσαν την υγειονομική περίθαλψη και τους επαγγελματίες υγείας.

4. Βιβλιογραφική ανασκόπηση

Ο σκοπός της παρούσας κριτικής ανασκόπησης είναι να αναλυθεί η ευαισθητοποίηση των επαγγελματιών υγείας σε σχέση με την ασφάλεια στο κυβερνοχώρο. Η βιβλιογραφία πλαισιώνεται από πέντε ενδιαφέρουσες έρευνες, οι οποίες διακρίνονται κάθε φορά από το δικό τους ξεχωριστό ερευνητικό πεδίο (Ondiege & Clarke, 2017; Fabisiak & Hyla, 2020; Stobert et al., 2020; Nunes et al., 2021; Giansanti & Monoscalco, 2021; Gordon et al., 2019; Priestman et al., 2019).

4.1 Ανάλυση ερευνών

Μια σημαντική ποσοτική – περιγραφική μελέτη είναι των Nunes et al. (2021) στην οποία αξιολογήθηκε το επίπεδο ευαισθητοποίησης των επαγγελματιών υγείας ως προς την ασφάλεια των πληροφοριών, αξιολογώντας τη στάση και τη συμπεριφορά τους στον κυβερνοχώρο. Η μελέτη πραγματοποιήθηκε στο Κεντρικό Νοσοκομείο Barreiro Montijo στην Πορτογαλία με δείγμα 56 επαγγελματίες της υγειονομικής περίθαλψης. Συγκεκριμένα, συμμετείχαν 10 Ιατροί, 19 Νοσηλευτές 18 ανώτεροι τεχνολόγοι ακτινοδιαγνωστικού, 2 ανώτεροι τεχνικοί, 5 βοηθητικοί λειτουργοί και 2 διοικητικοί/τεχνικοί λειτουργοί. Το ηλικιακό εύρος των συμμετεχόντων ήταν από 27 – 64 ετών και αφορούσε 40 γυναίκες και 16 άνδρες. Τα ερωτηματολόγια διατέθηκαν ψηφιακά, ώστε να συμπληρωθούν μέσω της διαδικτυακής πλατφόρμα ερευνών.

Οι κλίμακες που χρησιμοποιήθηκαν στην μελέτη ήταν η RScB και η ATC-IB. Η RScB αξιολογεί της συμπεριφορές που μπορεί να προκαλέσουν ανεπιθύμητες πρακτικές ασφάλειας στον κυβερνοχώρο. Η ATC-IB είναι μια κλίμακα τύπου Likert όπου αξιολογεί θετικά την ασφάλεια και το έγκλημα στον κυβερνοχώρο.

Η κλίμακα RScB υποθέτει ότι οι τιμές βαθμολογίας μεταξύ 0 έως 120 και η υψηλότερες τιμές είναι ενδεικτικές της επικίνδυνης συμπεριφοράς στην ασφάλεια στον κυβερνοχώρο. Οι τιμές που ελήφθησαν από τους συμμετέχοντες κυμαίνονταν μεταξύ 0 και 64 με μέσο όρο 31,6 (14,2). Η κλίμακα ATC-IB έχει βαθμολογήσει τιμές μεταξύ 25 έως 100 και οι χαμηλότερες τιμές δείχνουν μια πιο επικίνδυνη συμπεριφορά στην ασφάλεια στον

κυβερνοχώρο. Οι τιμές που ελήφθησαν σε αυτό το δείγμα κυμαίνονταν μεταξύ 48 και 82 με μέση τιμή 66,4 (6,3).

Σύμφωνα με τα ευρήματα της μελέτης, επιβεβαιώνεται η σχέση μεταξύ της επικίνδυνης συμπεριφοράς ως προς την ασφάλεια στον κυβερνοχώρο και των στάσεων των εργαζομένων απέναντι στην ασφάλεια στον κυβερνοχώρο. Ταυτόχρονα, δημιουργείται η γέφυρα για τον ποσοτικό προσδιορισμό της κουλτούρας ασφάλειας των πληροφοριών που προωθεί το μοντέλο γνώση – στάση – συμπεριφορά. Η ικανότητα και οι ικανότητες των επαγγελματιών υγείας στον τομέα της ασφάλειας στον κυβερνοχώρο πρέπει να ποσοτικοποιηθούν, καθώς τα τεχνολογικά εξελιγμένα συστήματα χρειάζονται άτομα με γνώση ώστε να αποφευχθούν οι παραβιάσεις ασφαλείας, σύμφωνα με τα καθιερωμένα πρότυπα ασφαλείας.

Εξίσου σημαντική είναι και η έρευνα των Giansanti & Monoscalco (2021), στην οποία συμμετείχαν 57 καρδιολόγοι από όλο το κόσμο όπου απάντησαν ένα ερωτηματολόγιο σε ηλεκτρονική μορφή από το smartphone ή το tablet τους. Σκοπός της έρευνας ήταν να διερευνήσει την ασφάλεια στον κυβερνοχώρο στον χώρο της καρδιολογία, όπου αποτελεί ένα στρατηγικό πεδίο της υγειονομικής περίθαλψης. Η καρδιολογία χρησιμοποιεί εξαιρετικά φορετά ιατρικά βοηθήματα όπως βηματοδότες, εμφυτεύσιμους απινιδωτές και άλλες φορητές συσκευές. Ωστόσο, όλες αυτές οι τεχνολογίες δημιουργούν ένα εντελώς νέο σύνολο κινδύνων ασφάλειας στον κυβερνοχώρο που κάποτε ήταν αδιανόητο.

Ακόμη και τα ψηφιακά ηλεκτροκαδιογραφήματα μπορεί να υποστούν κυβερνοεπιθέσεις, αφού η εμφάνιση ενός ηλεκτροκαρδιογραφήματος υπό επίθεση στον κυβερνοχώρο μπορεί να δείξει αναληθή στοιχεία που να οδηγήσουν σε λανθασμένη θεραπεία. Επιπρόσθετα, οι βηματοδότες, οι οποίοι είναι πλέον ανοιχτοί σε συνδέσεις δικτύου, ώστε να επιτρέψουν τον απομακρυσμένο επαναπρογραμματισμό, μπορούν να υποβληθούν σε διάφορους τύπους επιθέσεων.

Σύμφωνα με τα αποτελέσματα της έρευνας, οι περισσότεροι ερωτηθέντες (93%) απάντησαν ότι παρά την ψηφιοποίηση του τομέα της υγείας η οποία έχει προκαλέσει προβλήματα ασφάλειας, τα οφέλη που έχει προσφέρει είναι υψηλότερα από τους πιθανούς κινδύνους.

Μόνο το 33% πιστεύει ότι οι πρωτοβουλίες που αποσκοπούν στην ασφάλεια στον κυβερνοχώρο είναι επαρκείς. Επιπρόσθετα, το 39% παρακολούθησε μαθήματα κατάρτισης ενώ το 74% υποστηρίζει την ένταξη συγκεκριμένων μαθημάτων για την ασφάλεια στο κυβερνοχώρο. Μέσα από την έρευνα, επισημάνθηκα σημαντικά ζητήματα που σχετίζονται με την αντίληψη της ασφάλειας στον κυβερνοχώρο στο τομέα της καρδιολογία και γίνεται αντιληπτή από τους εργαζόμενους του τομέα αυτού.

Στην έρευνα των Fabisiak & Hyla (2020), μελετήθηκε η ευαισθητοποίηση των επαγγελματιών υγείας της Πολωνίας σχετικά με την ασφάλεια στον κυβερνοχώρο. Η έρευνα πραγματοποιήθηκε το δεύτερο εξάμηνο του 2017. Στόχος της έρευνα ήταν να επαληθεύσει εάν οι λειτουργοί της υγειονομικής περίθαλψης (γιατροί, νοσηλευτές και βοηθοί εργαστηρίου) έχουν επαρκείς γνώσεις σχετικά με τις βασικές απειλές στον κυβερνοχώρο. Επιπρόσθετα στόχευε να διερευνήσει εάν υπάρχει επαρκής εκπαίδευση σύμφωνα με της απαιτήσεις του Γενικού Κανονισμού Προστασίας Δεδομένων (GDPR), των συστάσεων του Κέντρου Πληροφοριών των Συστημάτων Υγείας και με τους πολωνικούς κανονισμούς που αφορούν τα δικαιώματα των ασθενών. Το δείγμα της έρευνας, αποτελούσαν 300 λειτουργοί υγείας. Συγκεκριμένα 200 Ιατροί, 15 Νοσηλευτές & Μαίες, 51 Φυσιοθεραπευτές, 10 βοηθοί εργαστηρίου και 15 Medical Administrator.

Η έρευνα ήταν ανώνυμη και πραγματοποιήθηκε με ηλεκτρονική μορφή. Στάλθηκε στις διευθύνσεις των νοσοκομείων υγειονομικής περίθαλψης μαζί με μια συνοδευτική επιστολή για τον σκοπό της έρευνας. Η έρευνα περιελάμβανε 23 ερωτήσεις απλής και πολλαπλής επιλογής χωρισμένες σε τρία μέρη. Στο πρώτο μέρος περιλάμβανε ερωτήσεις για την χρήση των ηλεκτρονικών συστημάτων στον ιστότοπο της υγειονομικής περίθαλψης, στο δεύτερο μέρος περιλάμβανε ερωτήσεις σχετικά με τις γνώσεις και τις δεξιότητες τους, για την ασφάλεια στον κυβερνοχώρο και στο τρίτο μέρος περιείχε βασικά σενάρια επίθεσης στον κυβερνοχώρο.

Σύμφωνα με τα ευρήματα της μελέτης, το μέσο ποσοστό των σωστών απαντήσεων κυμαίνεται από 36-50% ανάλογα με την επαγγελματική ομάδα, όπου είναι πολύ χαμηλά από τα αναμενόμενα αποτελέσματα. Επιπλέον, το τρίτο μέρος περιείχε ερωτήσεις πολλαπλής

επιλογής που ήταν απλές ερωτήσεις που αφορούσε τις διαφορετικές κυβερνοεπιθέσεις. Η μέση βαθμολογία ήταν περίπου 10% χειρότερη στο τρίτο μέρος από ό, τι στο δεύτερο μέρος. Αυτό δείχνει ότι, ακόμη και όταν οι ερωτηθέντες έχουν γνώση, η χρήση αυτών των γνώσεων σε πραγματικά σενάρια είναι πολύ πιο δύσκολη. Υπάρχει επίσης μια σημαντική διαφορά στα αποτελέσματα μεταξύ των ιατρών και των λειτουργών διοίκησης του νοσοκομείου. Αυτό προκύπτει γιατί πιθανώς υπήρχε διαφορετική εκπαίδευση στο τομέα της ασφάλειας στον κυβερνοχώρο.

Τα αποτελέσματα παρουσιάζουν χαμηλό επίπεδο γνώσεων σε σχέση με την ασφάλεια των πληροφοριών. Αυτό μπορεί να οφείλεται στο γεγονός ότι πολλές πληροφορίες ως προς την ασφάλειας στον κυβερνοχώρο να είναι δύσκολο να της μάθουν κατά τη διάρκεια μερικών ημερών εκπαίδευσης. Εντούτοις, τα συνολικά αποτελέσματα είναι μη ικανοποιητικά αφού δείχνουν ότι πρέπει να εφαρμοστούν και να υλοποιηθούν αρκετές διαδικασίες όσον αφορά την εκπαίδευση, σε θέματα ασφάλειας αφού παράλληλα υπάρχει υψηλός κίνδυνος εκμετάλλευσης κυβερνοεπιθέσεων στους επαγγελματίες του ιατρικού τομέα.

Η μελέτη των Stobert et al. (2020), είχε σκοπό να μελετήσει τις πρακτικές που ακολουθούν οι επαγγελματίες υγείας των επειγόντων περιστατικών στα νοσοκομεία του Καναδά ως προς την κυβερνοασφάλεια. Η έρευνα διαφημίστηκε μέσω αλληλογραφίας καναδικών επαγγελματικών ιατρικών και νοσηλευτικών οργανισμών επείγουσας αντιμετώπισης. Ο σύνδεσμος που βρισκόταν ηλεκτρονικά η έρευνα, διανεμήθηκε και από νοσοκομεία που ήτα πρόθυμα να το πράξουν.

Το δείγμα της έρευνας αποτέλεσαν 347 επαγγελματίες υγείας εκ των οποίων 83% γιατροί, 16% νοσηλευτές και το υπόλοιπο ποσοστό, δεν αποκάλυψε την κατηγορία στην οποία άνηκε. Η συντριπτική πλειοψηφία των συμμετεχόντων εργάστηκε σε εκπαιδευτικά νοσοκομεία, εκ των οποίων το 55% σε αστικά νοσοκομεία και το 32% σε κοινοτικά εκπαιδευτικά νοσοκομεία.

Το εργαλείο της έρευνας αφορούσε ένα ερωτηματολόγιο με 28 ερωτήσεις, σχετικές με τις πρακτικές ασφάλειας στον κυβερνοχώρο στα Καναδικά Τμήματα Επειγόντων Περιστατικών

(ΤΕΠ). Η έρευνα περιελάμβανε γενικές ερωτήσεις σχετικά με τους κωδικούς πρόσβασης και τον έλεγχο ταυτότητας στο ΤΕΠ, τις πολιτικές ασφαλείας που χρησιμοποιούνται σε λογαριασμούς, συστήματα και συσκευές στο ΤΕΠ και στο νοσοκομείο, το επίπεδο σύνδεσης στο Διαδίκτυο στο ΤΕΠ και ερωτήσεις σχετικά με την εκπαίδευση και την ετοιμότητα ασφάλειας στον τομέα της πληροφορικής.

Σύμφωνα με τα αποτελέσματα της έρευνας, διαπιστώθηκε ότι οι ερωτηθέντες έχουν αυξημένα καθήκοντα ασφαλείας, όπως η διαχείριση πολλών κωδικών πρόσβασης, έλεγχος ταυτότητας και συχνές αλλαγές κωδικών πρόσβασης. Χρησιμοποιούν πολλαπλά συστήματα πληροφορικής για μια ποικιλία εργασιών, όπως προβολή δεδομένων των ασθενών, πρόσβαση σε ιατρικά αρχεία και διαχείριση της ροής των ασθενών. Περισσότεροι από τους μισούς ερωτηθέντες παραδέχτηκαν ότι χρησιμοποιούν το σύστημα με την σύνδεση άλλου ατόμου. Η συντριπτική πλειονότητα των ερωτηθέντων (95%) είχε 9 ή λιγότερους κωδικούς πρόσβασης. Οι περισσότεροι ερωτηθέντες είχαν τη δυνατότητα να επιλέξουν τους δικούς τους κωδικούς πρόσβασης (73%) και το 74% των ερωτηθέντων δήλωσαν ότι η επαναχρησιμοποίηση κωδικών επιτρέπεται από τα συστήματα πληροφορικής του νοσοκομείου τους.

Οι συμμετέχοντες ανέφεραν συχνότερα ότι έπρεπε να συνδεθούν για να δουν δεδομένα ασθενών, όπως ακτινοδιαγνωστικά (89%) και εργαστηριακά δεδομένα (88%), και για πρόσβαση σε ιατρικά αρχεία (84%). Επιπρόσθετα, οι ερωτηθέντες ήταν λιγότερο πιθανό να χρησιμοποιήσουν την προσωπική τους συσκευή για τη συλλογή (14%) ή τη μετάδοση (31%) πληροφοριών ασθενούς. Οι επαγγελματίες υγείας όταν χρησιμοποιούν τις προσωπικές τους συσκευές, εφαρμόζουν διάφορες στρατηγικές για την προστασία του απορρήτου των ασθενών τους. Κατά κύριο λόγο, οι ερωτηθέντες δήλωσαν ότι απέφυγαν να στείλουν πληροφορίες προσωπικής ταυτοποίησης (77%), αλλά επίσης δήλωσαν ότι βασίστηκαν σε στρατηγικές όπως η διαγραφή εικόνων (43%) και μηνυμάτων (38%). Το 23% είπε ότι προσπάθησαν να συνδυάσουν κανάλια εκτός ζώνης για να διαχωρίσουν τα αναγνωριστικά ασθενών από ιατρικά δεδομένα.

Όσον αφορά την εκπαίδευση, η πλειονότητα των ερωτηθέντων (75%) είχε λάβει τουλάχιστον κάποιο είδος επίσημης εκπαίδευσης από το νοσοκομείο τους, το οποίο σχετίζεται με την πληροφορική. Από τους ερωτηθέντες που είχαν λάβει εκπαίδευση, ήταν πιθανότερο να έχουν

εκπαιδευτεί στη χρήση πακέτων λογισμικού νοσοκομείου (75%) και να προστατεύουν τα δεδομένα των ασθενών (65%) ενώ λιγότεροι συμμετέχοντες (28%) δήλωσαν ότι είχαν λάβει εκπαίδευση συγκεκριμένη με την κυβερνοασφάλεια. Το 80% των νοσηλευτών ανέφεραν ότι είχαν λάβει επίσημη εκπαίδευση πληροφορικής, σε σύγκριση με το 74% των γιατρών. Ωστόσο, λιγότεροι νοσηλευτές (11%) ανέφεραν ότι έχουν λάβει εκπαίδευση ασφάλειας στον κυβερνοχώρο σε σχέση με τους γιατρούς (22%).

Μέσα από την έρευνα φάνηκε ότι οι γιατροί και οι νοσηλευτές χειρίζονται πολλά εργαλεία ασφαλείας σε μια μέση εργάσιμη ημέρα, τα οποία μπορεί να μειώσουν τις κύριες ιατρικές τους εργασίες. Επιπρόσθετα διαφάνηκαν παραβάσεις των πολιτικών ασφαλείας, όπως κοινόχρηστες συνδέσεις ή χρήση προσωπικών συσκευών για ιατρικές εργασίες. Τα ευρήματά υποστηρίζουν αυτό που φαίνεται στη βιβλιογραφία σχετικά με την ασφάλεια στον κυβερνοχώρο σε νοσοκομειακά περιβάλλοντα όπου υποδηλώνει ότι πολλά από τα θέματα που επηρεάζουν την ασφάλεια της πληροφορικής στα νοσοκομεία επηρεάζουν και τα ΤΕΠ.

Η μελέτη των Gordon et al. (2019) είχε σκοπό να κατανοήσει τον αντίκτυπο ενός προγράμματος κατάρτισης ηλεκτρονικού ψαρέματος στα ποσοστά κλικ ηλεκτρονικού ψαρέματος (phishing) για υπαλλήλους σε ένα μόνο, ανώνυμο ίδρυμα υγειονομικής περίθαλψης στις ΗΠΑ.

Στα πλαίσια της έρευνας ο πληθυσμός που συμμετείχε διαχωρίστηκε σε δύο ομάδες, στους παραβάτες και τους μη. Ως παραβάτες ορίστηκαν εκείνοι που είχαν κάνει κλικ σε τουλάχιστον 5 προσομοιωμένα ηλεκτρονικά μηνύματα ηλεκτρονικού "ψαρέματος" και οι μη παραβάτες ήταν εκείνοι που δεν είχαν. Οι ερευνητές υπολόγισαν τα ποσοστά κλικ και για τις δύο ομάδες πριν και μετά την εφαρμογή ενός υποχρεωτικού προγράμματος εκπαίδευσης.

Οι 5416 εργαζόμενοι που συμμετείχαν στην έρευνα, έλαβαν μέρος στις 20 συνολικά εκστρατείες κατά την περίοδο της παρέμβασης. Μέσα σε αυτά τα πλαίσια 772 εργαζόμενοι έκαναν κλικ σε τουλάχιστον 5 μηνύματα ηλεκτρονικού ταχυδρομείου και είχαν χαρακτηριστεί παραβάτες. Μόνο οι 975 (17,9%) του συνόλου των συμμετεχόντων έκανε κλικ σε 0 ηλεκτρονικά μηνύματα ηλεκτρονικού ψαρέματος (phishing) κατά τη διάρκεια της

έρευνας. 3565 εργαζόμενοι (65,3%) έκαναν κλικ σε τουλάχιστον 2 email. Υπήρξε μείωση στα ποσοστά κλικ για κάθε ομάδα στις 20 καμπάνιες. Το υποχρεωτικό πρόγραμμα εκπαίδευσης, που ξεκίνησε μετά την εκστρατεία 15, δεν είχε ουσιαστικό αντίκτυπο στα ποσοστά κλικ και οι παραβάτες παρέμειναν πιο πιθανό να κάνουν κλικ σε μια προσομοίωση ηλεκτρονικού ψαρέματος.

Από την έρευνα προέκυψε πως το ηλεκτρονικό ψάρεμα (phishing) είναι ένας κοινός φορέας απειλής κατά των υπαλλήλων του νοσοκομείου και ένας σημαντικός κίνδυνος ασφάλειας στον κυβερνοχώρο για τα συστήματα υγειονομικής περίθαλψης. Η εργασία έδειξε ότι, σύμφωνα με την προσομοίωση, τα ποσοστά κλικ των εργαζομένων μειώνονται με την επαναλαμβανόμενη προσομοίωση, αλλά ένα υποχρεωτικό πρόγραμμα εκπαίδευσης που απευθύνεται σε υπαλλήλους υψηλού κινδύνου δεν μείωσε ουσιαστικά τα ποσοστά κλικ αυτού του πληθυσμού.

Τα δεδομένα της υγειονομικής περίθαλψης έχουν σημαντική αξία ως πιθανός στόχος για τους χάκερ. Το ηλεκτρονικό ψάρεμα (phishing) είναι μια μέθοδο εκμετάλλευσης για κακόβουλους λόγους χρησιμοποιώντας στοχευμένες επικοινωνίες (email / μηνύματα). Η μελέτη των Priestman et al. (2019) περιγράφει μια εσωτερική αξιολόγηση που στοχεύει στο προσωπικό του νοσοκομείου και συνοψίζει τη βιβλιογραφία σχετικά με το ηλεκτρονικό ψάρεμα και την υγειονομική περίθαλψη.

Οι ερευνητές πραγματοποίησαν μια αξιολόγηση ως μέρος της δραστηριότητας ασφάλειας στον κυβερνοχώρο κατά τη διάρκεια μιας καθορισμένης περιόδου δοκιμής χρησιμοποιώντας πολλαπλές προσεγγίσεις συλλογής διαπιστευτηρίων μέσω email του προσωπικού. Επιπλέον μελέτησαν τη βιβλιογραφία που σχετίζεται με την ιατρική για να εντοπίσουν σχετικές δημοσιεύσεις που σχετίζονται με το ηλεκτρονικό “ψάρεμα”.
Κατά τη διάρκεια της δοκιμαστικής περιόδου ενός μηνός, ο οργανισμός έλαβε 858.200 email: 139.400 (16%) μάρκετινγκ, 18.871 (2%) αναγνωρίστηκαν ως πιθανές απειλές. Από 143 εκατομμύρια συναλλαγές στο Διαδίκτυο, περίπου 5 εκατομμύρια (3%) ήταν ύποπτες απειλές. 468 διευθύνσεις email υπαλλήλων εντοπίστηκαν από δημόσια δεδομένα και στοχεύθηκαν μέσω ηλεκτρονικού ψαρέματος χρησιμοποιώντας μια σειρά ωφέλιμων

φορτίων, συμπεριλαμβανομένων συνημμένων και κακόβουλων συνδέσμων. Ωστόσο, δεν ανακτήθηκαν διαπιστευτήρια ή δε λήφθηκαν κακόβουλα αρχεία. Αρκετοί υπάλληλοι του νοσοκομείου, ωστόσο, εντοπίστηκαν στα προφίλ κοινωνικών μέσων, συμπεριλαμβανομένων ορισμένων που έγιναν αποδέκτες αιτημάτων φιλίας από ψεύτικα προφίλ.

Οι οργανώσεις υγειονομικής περίθαλψης μετακινούνται όλο και περισσότερο σε ψηφιακά συστήματα, αλλά οι επαγγελματίες του τομέα της υγείας έχουν περιορισμένη επίγνωση των απειλών. Η αύξηση της έμφασης στην «κυβερνητική υγιεινή» και η διακυβέρνηση των πληροφοριών μέσω της υποχρεωτικής εκπαίδευσης αυξάνει την κατανόηση αυτών των κινδύνων. Παρόλο που δεν συλλέχθηκαν διαπιστευτήρια σε αυτήν τη μελέτη, καθώς έως και το 5% των ηλεκτρονικών μηνυμάτων / της διαδικτυακής κίνησης είναι ύποπτα, τονίζεται η ανάγκη για ισχυρά τείχη προστασίας, υποδομή ασφάλειας στον κυβερνοχώρο, πολιτικές πληροφορικής και, το πιο σημαντικό απ 'όλα, η εκπαίδευση προσωπικού.

Τα νοσοκομεία λαμβάνουν σημαντικό όγκο δυνητικά κακόβουλων μηνυμάτων ηλεκτρονικού ταχυδρομείου. Ενώ πολλοί υπάλληλοι φαίνεται να γνωρίζουν το ηλεκτρονικό ψάρεμα και να ανταποκρίνονται κατάλληλα, απαιτείται συνεχής εκπαίδευση σε όλο το φάσμα της ασφάλειας στον κυβερνοχώρο, με ιδιαίτερη έμφαση στην «διαρροή» πληροφοριών στα κοινωνικά μέσα.

Σημαντική μελέτη αποτελεί και αυτή των Ondiege & Clarke (2017), που είχε στόχο να προσδιορίσει την αντίληψη των επαγγελματιών υγείας σχετικά με την ασφάλεια των πληροφοριών καθώς και να αντιμετωπιστεί το ζήτημα των πλαστών συσκευών παρακολούθησης ασθενών.

Η μελέτη διεξήχθη σε τέσσερις χώρους υγειονομικής περίθαλψης του Λονδίνου, συμπεριλαμβανομένων τριών νοσοκομείων (Ealing Hospital, Royal Free Hospital και Hillingdon Hospital) και ενός κέντρου υγειονομικής περίθαλψης (Chorleywood Health Center). Η συλλογή δεδομένων προέκυψε από ημι-δομημένες συνεντεύξεις με σκοπό την διερεύνηση των αντιλήψεων των επαγγελματιών στον τομέα της υγείας έναντι της ασφάλειας πληροφοριών και των ζητημάτων ασφάλειας στην τηλε-υγεία. Το δείγμα αποτέλεσαν οκτώ επαγγελματίες υγείας που ασκούσαν την τηλεθεραπεία και αναγνωρίστηκαν ότι

δραστηριοποιούνται ενεργά στην τηλεθεραπεία. Οι συνεντεύξεις έγιναν τον Ιανουάριο του 2014 έως τον Φεβρουάριο του 2014.

Σύμφωνα με τα αποτελέσματα της μελέτης η αντίληψη των επαγγελματιών της υγειονομικής περίθαλψης έναντι της σημασίας της ασφάλειας, είναι πολύ χαμηλή και οι γνώσεις τους σχετικά με θέματα ασφάλειας είναι κακές. Όσον αφορά το επίπεδο γνώσεων των συμμετεχόντων σχετικά με τη φύση της ασφάλειας των πληροφοριών, δυο συμμετέχοντες δήλωσαν ότι είχαν κάποια γνώση ασφάλεια πληροφοριών, αλλά έξι από τους συμμετέχοντες παραδέχτηκαν ότι έχουν λίγη έως και καθόλου γνώση. Επιπρόσθετα, δυο άτομα περιέγραψαν σωστά τι είναι ο ιός υπολογιστή. Οι υπόλοιποι συμμετέχοντες βρίσκονταν σε πλήρη άγνοια για το τι είναι ο ιός των υπολογιστών.

Η μελέτη εντόπισε περαιτέρω απειλές για την εφαρμογή της τηλε-υγείας όπου περιλαμβάνουν πλαστές συσκευές παρακολούθησης των ασθενών. Κάθε συσκευή συνδέεται με τον ασθενή και έτσι το νοσοκομείο μπορεί να διασφαλίσει ότι οι συσκευές είναι καταχωρημένες επομένως οποιαδήποτε πλαστή συσκευή δεν θα πιστοποιηθεί και δεν θα επιτρέπεται η χρήση της.. Κανένας από τους ερωτηθέντες δεν μπορούσε να απαντήσει πως θα ξεχωρίσουν μια πλαστή συσκευή. Όλοι οι συμμετέχοντες γνώριζαν τα πλαστά προϊόντα, αλλά δεν γνώριζαν πώς να αναγνωρίσουν μια πλαστή συσκευή. Το πρόβλημα της πιστοποίησης της συσκευής δεν περιορίζεται στην τηλεϋγειονομική υγεία αλλά επηρεάζει ολόκληρη την υγεία βιομηχανία φροντίδας.

Η έρευνα συνιστά τη δημιουργία εργαστηρίων ευαισθητοποίησης που να μπορούν να χρησιμοποιηθούν για να εκπαιδεύσουν τους παρόχους υγειονομικής περίθαλψης για τη σημασία της ασφάλειας στο περιβάλλον της υγειονομικής περίθαλψης.

4.2 Αποτελέσματα ερευνών

Όπως έχει παρουσιαστεί από τις μελέτες, η ευαισθητοποίηση των επαγγελματιών υγείας, αποτελεί πρωταρχικό ρόλο στην υγειονομική περίθαλψη. Και στις τρεις μελέτες, οι επαγγελματίες υγείας, εστιάζουν την σημαντικότητα της εκπαίδευσης στο τομέα της κυβερνοασφάλειας, παρόλο που αρκετοί ερωτηθέντες είχαν εκπαιδευτεί σε θέματα

ασφαλείας στο κυβερνοχώρο και εντούτοις δεν ήταν καταρτισμένοι. Οι λάθος χειρισμοί και η άγνοια μπορεί να οδηγήσει σε ανεπιθύμητα αποτελέσματα στους οργανισμούς υγείας. Οι επαγγελματίες υγείας δεν είναι σε θέση να αναγνωρίσουν τους κινδύνους του κυβερνοχώρου με αποτέλεσμα οι επιθέσεις να μην αντιμετωπίζονται έγκαιρα. Παράλληλα, οι οργανισμοί δεν λαμβάνουν τα κατάλληλα μέτρα αντιμετώπισης με αποτέλεσμα οι επιθέσεις να αυξάνονται ολοένα και περισσότερο.

5. Συζήτηση

Η ύπαρξη μιας προσέγγισης για τον εντοπισμό βασικών τεχνολογικών κατασκευών και διαδικασιών για τη διασφάλιση της διαχείρισης της διαμόρφωσης μπορεί να βελτιώσει σημαντικά την ασφάλεια των συστημάτων. Θα πρέπει να αναπτυχθεί μια στρατηγική για να καταργηθούν ή να απενεργοποιηθούν περιττές λειτουργίες από τα συστήματα και να επιλύονται άμεσα τα θέματα που προκύπτουν. Σε αντίθετη περίπτωση, είναι πιθανό να προκληθεί αυξημένος κίνδυνος συμβιβασμού των συστημάτων και των πληροφοριών.

Οι συνδέσεις από δίκτυα στο διαδίκτυο άλλα και τα δίκτυα άλλων συνεργατών, εκθέτουν τα συστήματα και τις τεχνολογίες σε επιθέσεις. Με την δημιουργία και την εφαρμογή μερικών απλών πολιτικών και με τις κατάλληλες αρχιτεκτονικές και τεχνικές διαμορφώσεις, δίνεται η δυνατότητα να μειωθούν οι πιθανότητες επιτυχίας αυτών των επιθέσεων (ή πρόκλησης βλάβης στον οργανισμό). Τα δίκτυα του οργανισμού σίγουρα εκτείνονται σε πολλούς ιστότοπους και η χρήση υπηρεσιών κινητής ή απομακρυσμένης εργασίας και υπηρεσιών καθιστά δύσκολο τον καθορισμό ενός σταθερού ορίου δικτύου. Επομένως δεν πρέπει να γίνεται εστίαση μόνο σε φυσικές συνδέσεις αλλά εκεί που αποθηκεύονται και υποβάλλονται σε επεξεργασία τα δεδομένα.

Εάν στους χρήστες παρέχονται δικαιώματα στο σύστημα τα οποία είναι περιττά ή δικαιώματα πρόσβασης σε δεδομένα, τότε ο αντίκτυπος της κατάχρησης ή του συμβιβασμού αυτού του λογαριασμού χρηστών θα είναι πιο σοβαρός από ό, τι πρέπει. Σε όλους τους χρήστες θα πρέπει να παρέχεται ένα λογικό (αλλά ελάχιστο) επίπεδο προνομίων και δικαιωμάτων στο σύστημα μέχρι στο σημείο που απαιτεί ο ρόλος τους. Η χορήγηση υψηλών προνομίων στο σύστημα πρέπει να ελέγχεται και να διαχειρίζεται προσεκτικά. Σε παρόμοια συμπεράσματα κατέληξε και η έρευνα των Stobert et al. (2020).

Οι χρήστες μπορούν να διαδραματίσουν κρίσιμο ρόλο στην ασφάλεια του οργανισμού τους και ως εκ τούτου, είναι σημαντικό οι κανόνες ασφαλείας και η παρεχόμενη τεχνολογία να επιτρέπουν στους χρήστες να κάνουν τη δουλειά τους, καθώς και να συμβάλλουν στη διατήρηση της ασφάλειας του οργανισμού. Αυτό μπορεί να υποστηριχθεί από τη συστηματική υλοποίηση προγραμμάτων ευαισθητοποίησης και κατάρτισης που παρέχουν εμπειρογνωμοσύνη στον τομέα της ασφάλειας, καθώς και με τη συμβολή στη δημιουργία μιας νοοτροπίας που θα έχει συνείδηση της ασφάλειας. Η έρευνα των Fabisiak & Hyla

(2020) συμφωνεί με τις παραπάνω απόψεις καθώς κατέληξε στο συμπέρασμα ότι οι επαγγελματίες υγείας παρουσιάζουν χαμηλό επίπεδο γνώσεων σε σχέση με την ασφάλεια των πληροφοριών. Αυτό μπορεί να οφείλεται στο γεγονός ότι πολλές πληροφορίες ως προς την ασφάλειας στον κυβερνοχώρο να είναι δύσκολο να της μάθουν κατά τη διάρκεια μερικών ημερών εκπαίδευσης. Εντούτοις, τα συνολικά αποτελέσματα είναι μη ικανοποιητικά αφού δείχνουν ότι πρέπει να εφαρμοστούν και να υλοποιηθούν αρκετές διαδικασίες όσον αφορά την εκπαίδευση, σε θέματα ασφάλειας αφού παράλληλα υπάρχει υψηλός κίνδυνος εκμετάλλευσης κυβερνοεπιθέσεων στους επαγγελματίες του ιατρικού τομέα.

Σε παρόμοια συμπεράσματα κατέληξε και η μελέτη των Nunes et al. (2021), στα πλαίσια της οποίας επιβεβαιώνεται η σχέση μεταξύ της επικίνδυνης συμπεριφοράς ως προς την ασφάλεια στον κυβερνοχώρο και των στάσεων των εργαζομένων απέναντι στην ασφάλεια στον κυβερνοχώρο. Ταυτόχρονα, δημιουργείται η γέφυρα για τον ποσοτικό προσδιορισμό της κουλτούρας ασφάλειας των πληροφοριών που προωθεί το μοντέλο γνώση – στάση – συμπεριφορά. Η ικανότητα και οι ικανότητες των επαγγελματιών υγείας στον τομέα της ασφάλειας στον κυβερνοχώρο πρέπει να ποσοτικοποιηθούν, καθώς τα τεχνολογικά εξελιγμένα συστήματα χρειάζονται άτομα με γνώση ώστε να αποφευχθούν οι παραβιάσεις ασφαλείας, σύμφωνα με τα καθιερωμένα πρότυπα ασφαλείας.

Αναπόφευκτα, όλοι οι οργανισμοί θα αντιμετωπίσουν κάποια στιγμή περιστατικά ασφαλείας. Οι εργαζόμενοι στον τομέα της υγείας έχουν τη γνώμη πως το ζήτημα της ασφάλειας στον κυβερνοχώρο στον τομέα της υγείας είναι πολύ σημαντικό. Με αυτή την άποψη συμφωνούν και τα ευρήματα από την έρευνα των Giansanti & Monoscalco (2021).

Οι επενδύσεις στη θέσπιση αποτελεσματικών πολιτικών και διαδικασιών διαχείρισης συμβάντων συμβάλουν στη βελτίωση της ανθεκτικότητας, στην υποστήριξη της επιχειρησιακής συνέχειας, στη βελτίωση της εμπιστοσύνης των πελατών και των ενδιαφερόμενων και ενδεχομένως και στη μείωση τυχόν επιπτώσεων.

Το κακόβουλο λογισμικό είναι ένας όρος για την κάλυψη οποιουδήποτε κώδικα ή περιεχομένου που θα μπορούσε να έχει κακόβουλο, ανεπιθύμητο αντίκτυπο στα συστήματα. Οποιαδήποτε ανταλλαγή πληροφοριών, αυτόματα συμβάλει σε κάποιο κίνδυνο ανταλλαγής κακόβουλου λογισμικού, γεγονός που θα μπορούσε να επηρεάσει σοβαρά τα συστήματα και τις υπηρεσίες. Ο κίνδυνος μπορεί να μειωθεί με την ανάπτυξη και την

εφαρμογή κατάλληλων πολιτικών κατά του κακόβουλου λογισμικού στο πλαίσιο μιας συνολικής προσέγγισης.

Η παρακολούθηση του συστήματος παρέχει μια δυνατότητα όπου στοχεύει στον εντοπισμό πραγματικών ή τις απόπειρες των επιθέσεων, σε συστήματα και επιχειρηματικές υπηρεσίες. Η ορθή παρακολούθηση είναι απαραίτητη προκειμένου να αντιμετωπιστούν αποτελεσματικά οι επιθέσεις. Επιπλέον, η παρακολούθηση διασφαλίζει την καταλληλότητα των συστημάτων, εάν χρησιμοποιούνται σύμφωνα με τις οργανωτικές πολιτικές. Η παρακολούθηση αποτελεί συχνά, βασική ικανότητα η οποία απαιτείται για τη συμμόρφωση με τις νομικές ή τις κανονιστικές απαιτήσεις.

Σύμφωνα με τον Martin et al. (2017), εκτός από την ενίσχυση της ανθεκτικότητας, και της ασφαλής πρόσβασης. πρέπει να αναπτυχθούν κοινά πρότυπα ασφαλείας που έχουν σχέση με τον τομέα της υγειονομικής περίθαλψης. Οι οργανισμοί πρέπει να επινοήσουν ένα ολοκληρωμένο σχέδιο για την αντιμετώπιση των αναγκών της ασφάλειας τους.

Βάση της ευρωπαϊκής πολιτικής, η νομοθεσία διαδραματίζει σημαντικό ρόλο στον καθορισμό των απαιτήσεων της ασφάλειας στον κυβερνοχώρο αφού επιβάλλεται να περιγράφονται στις τεχνικές προδιαγραφές κατά την απόκτηση προϊόντων αλλά και υπηρεσιών στο οργανισμό ενός νοσοκομείου.

Οι οργανισμοί που επεξεργάζονται δεδομένα υγείας έχουν τις ακόλουθες υποχρεώσεις (ENISA 2020):

- να εφαρμόζουν τα κατάλληλα τεχνικά και οργανωτικά μέτρα για να εξασφαλίζεται η ασφάλεια των συστημάτων επεξεργασίας, των υπηρεσιών και των προσωπικών δεδομένων.

- να πραγματοποιούν εκτίμηση των επιπτώσεων όσον αφορά την προστασία των δεδομένων.

- να αναφέρουν παραβιάσεις δεδομένων που ενδέχεται να οδηγήσουν σε κίνδυνο για τα δικαιώματα και τις ελευθερίες των ατόμων εντός 72 ωρών από τη στιγμή που θα ενημερωθούν. Το άρθρο 4 παράγραφος 12 του GDPR, ορίζει την «παραβίαση προσωπικών δεδομένων» ως παραβίαση ασφάλειας που οδηγεί σε τυχαία ή παράνομη καταστροφή, απώλεια, αλλοίωση, μη εξουσιοδοτημένη αποκάλυψη ή πρόσβαση σε προσωπικά δεδομένα

που διαβιβάζονται, αποθηκεύονται ή υφίστανται επεξεργασία με άλλο τρόπο.

Οι Jumelle et al. (2014), αναφέρουν ότι τα επεξεργασμένα δεδομένα πρέπει να είναι επαρκή, συναφή και οπωσδήποτε πρέπει να υπάρχει σχέση με τους σκοπούς για τους οποίους έχουν συλλεχθεί, να είναι ακριβής, να μην φυλάσσονται περισσότερο από ό, τι είναι απαραίτητο και να ην μεταφέρονται πέρα από τα σύνορα των χωρών χωρίς επαρκή ασφάλεια και προστασία.

Η πολιτική επίδραση του Γενικού Κανονισμού Προστασίας Δεδομένων (GDPR) βρέθηκε αποτελεσματική στην πρόληψη μιας επιθετικής εξέλιξης του κύματος ψηφιοποίησης. Οι ψηφιακοί τομείς της δημόσιας υγείας σε ολόκληρη την Ευρωπαϊκή Ένωση έχουν εφαρμόσει δαπανηρές προσαρμογές ώστε να συμμορφωθούν με τον κανονισμό ο οποίος απαιτεί πολύ πιο αυστηρή προστασία για τα δεδομένα υγείας των ασθενών. Το πιο σημαντικό, είναι ότι καθιερώνει νέα πρότυπα προστασίας δεδομένων σχετικά με την υγεία και έτσι ενισχύει την υποχρέωση των υπευθύνων επεξεργασίας δεδομένων και των επεξεργαστών του τομέα της υγείας. Συγκεκριμένα ο GDPR θέτει τα υψηλότερα πρότυπα σχετικά με τα καθήκοντα ενημέρωσης και συναίνεσης (Yuan & Li, 2019).

Η ανάγκη για χρήση των ψηφιακών δεδομένων της υγείας, με το σεβασμό ταυτόχρονα των κανονισμών προστασίας δεδομένων και του απορρήτου και της εμπιστευτικότητας των ασθενών έχει επηρεάσει και την περίοδο που η παγκόσμια υγεία κλονίζεται με τον Covid-19.

Υπάρχουν αρκετές ανησυχίες όσον αφορά τον κανονισμό GDPR, με αποτέλεσμα οι οργανισμοί να αποφεύγουν τον κίνδυνο, και να αποτρέπεται η κοινή χρήση δεδομένων αν και ο κανονισμός επιτρέπει μια τέτοια κοινή χρήση. Οι οργανισμοί της υγειονομικής περίθαλψης που εστιάζουν στην ελαχιστοποίηση των ατομικών κινδύνων απειλούν να υπονομεύσουν τις ερευνητικές προσπάθειες κατά του COVID-19.

Το Ευρωπαϊκό Συμβούλιο Προστασίας Δεδομένων τόνισε τη σημασία της προστασίας των προσωπικών δεδομένων κατά τη διάρκεια της πανδημίας COVID-19. Ωστόσο, οι κανόνες προστασίας δεδομένων (όπως ο GDPR) δεν εμποδίζουν τα μέτρα που λαμβάνονται για την καταπολέμηση της πανδημίας του κορωνοϊού αφού επιτρέπεται η επεξεργασία ευαίσθητων προσωπικών δεδομένων (συμπεριλαμβανομένων γενετικών δεδομένων, βιομετρικών δεδομένων και δεδομένων που αφορούν την υγεία) εάν είναι απαραίτητο για λόγους

δημοσίου συμφέροντος στον τομέα της δημόσιας υγείας (McLennan et al., 2020).

Για την προστασία των συστημάτων πληροφοριών και γενικά των πληροφοριών, αναπτύχθηκαν τα πρότυπα ISO 27000, ISO 27001 και ISO 27002 όπου περιλαμβάνουν ειδικούς ελέγχους, στόχους ελέγχου, απαιτήσεις αλλά και κατευθυντήριες γραμμές, όπου οι εταιρίες και οι οργανισμοί μπορούν να επιτύχουν επαρκή ασφάλεια πληροφοριών.

Με αυτόν τον τρόπο, το ISO 27001 καθιστά δυνατή την πιστοποίηση του οργανισμού ή της εταιρίας, βάση με το πρότυπο, όπου η ασφάλεια των πληροφοριών μπορεί να τεκμηριωθεί ως αυστηρή εφαρμογή και διαχείριση σύμφωνα με ένα διεθνώς αναγνωρισμένο οργανωτικό πρότυπο (Disterer, 2013).

Με την πιστοποίηση κατά ISO 27001, μια εταιρεία επαληθεύει την εκπλήρωση γνωστών και αποδεκτών προτύπων ασφάλειας και προωθεί την εμπιστοσύνη των πελατών. Επομένως, η πιστοποίηση με ένα διεθνές πρότυπο μειώνει τον κίνδυνο προστίμων ή και αποζημιώσεων που έχουν ως αποτέλεσμα τις νομικές διαφορές, καθώς οι νομικές απαιτήσεις τείνουν να αντιμετωπίζονται με τη συμμόρφωση προς τα πρότυπα (Disterer, 2013).

Η εμπιστοσύνη και η ανησυχία σχετικά με την εμπιστευτικότητα και την ασφάλεια, αποτελούν μείζον ζητήματα που πρέπει να ληφθούν υπόψη στις τεχνολογίες και στις εφαρμογές της ηλεκτρονικής υγείας, και της τηλεϊατρικής. Επιπλέον, υπάρχει ο κίνδυνος οι ηλεκτρονικές υπηρεσίες υγειονομικής περίθαλψης και ιατρικής πληροφόρησης να είναι χαμηλής ποιότητας και υπερβολικά περίπλοκες.

Όπως χαρακτηριστικά αναφέρουν οι Coventry & Branley (2018), η ασφάλεια στον κυβερνοχώρο είναι ένα ουσιαστικό μέρος της διατήρησης της ασφάλειας, της ιδιωτικής ζωής και της εμπιστοσύνης των ασθενών. Η ασφάλεια του κυβερνοχώρου πρέπει να γίνει μέρος της κουλτούρας φροντίδας του ασθενούς, επομένως χρειάζεται να δαπανηθούν περισσότερα χρήματα ώστε να επιτευχθεί.

Η χρηματοδότηση για την ασφάλεια στον κυβερνοχώρο είναι ελλιπής. Ενώ οι οργανισμοί δαπανούν και χρηματοδοτούν για ένα ολοκληρωμένο λογισμικό, στην συνέχεια, δεν ξοδεύουν αρκετό χρόνο και χρήματα για να αναβαθμίζεται το λογισμικό και να ενημερώνεται ώστε να είναι ασφαλής τα συστήματα. Αυτό επιδεινώνεται από την έλλειψη εμπειρίας στον

κυβερνοχώρο και προκύπτει από μια γενική έλλειψη της τεχνολογίας αλλά και από το απαγορευτικό κόστος του προσωπικού ασφάλειας στον κυβερνοχώρο (Coventry & Branley, 2018).

Παρόμοια αποτελέσματα, παρουσιάζει και η μελέτη των Kruse et al. (2017), όπου επισημαίνει ότι μετά την εφαρμογή του λογισμικού, θα πρέπει να ενημερώνεται συνεχώς για να συμβαδίζει με τις πρόσφατες εξελίξεις και να εντοπίζονται τα κενά ασφαλείας που είναι εκτεθειμένα από τους εγκληματίες του κυβερνοχώρου. Οι οργανισμοί δαπανούν μεγάλα ποσά χρηματοδότησης για να γίνει πιο ολοκληρωμένο το λογισμικό, αλλά δεν ξοδεύουν αρκετό χρόνο ή χρήματα για τη διατήρηση ενός ενημερωμένου λογισμικού.

Οι υπηρεσίες της υγειονομικής περίθαλψης ξοδεύουν αρκετά μεγάλα κεφάλαια για να γίνουν πιο ολοκληρωμένες στην παροχή των υπηρεσιών της υγειονομικής περίθαλψης, εντούτοις, δεν δίνεται η απαραίτητη έμφαση στην πτυχή της ασφάλειας όσον αφορά τη συντήρηση, δηλαδή στην ενημέρωση του λογισμικού και στην ασφάλεια των συστημάτων. Σύμφωνα με τους He et al. (2021) αυτό οφείλεται λόγω της έλλειψης έμπειρων εμπειρογνωμόνων στον τομέα της ασφάλειας στον κυβερνοχώρο παρόλο που οργανισμοί υγειονομικής περίθαλψης με τις απαιτούμενες δεξιότητες και εμπειρία δεν αλλάζουν τις επιχειρηματικές τους δραστηριότητες και δεν αναλαμβάνονται τα επιτρεπόμενα επίπεδα ασφάλειας στον κυβερνοχώρο.

Σύμφωνα με τους Jalali & Kaiser (2018), ένας λόγος που οι επιθέσεις στην Εθνική Υπηρεσία Υγείας του Ηνωμένου Βασιλείου ήταν αυξημένες, ευθύνεται η έλλειψη πόρων αφού για τη συντήρηση του μεγάλου συστήματος η χρηματοδότηση μειώθηκε. Ακόμη και ένα νοσοκομείο με λιγότερους διαθέσιμους πόρους για την ασφάλεια στον κυβερνοχώρο είναι απειλή για το σύνολο της υποδομής της υγειονομικής περίθαλψης. Σύμφωνα με την μελέτη, η επίδραση της μεταβλητότητας στην διαθεσιμότητα των πόρων στις κυβερνοεπιθέσεις έχει αποδείξει ότι η μεγαλύτερη διαθεσιμότητα πόρων, μειώνει την πιθανότητα μιας επιτυχούς επίθεσης.

Η πρόοδος της τεχνολογίας στο σχεδιασμό των ιατρικών συσκευών, έχει αναπτύξει περισσότερες συσκευές με δυνατότητες στην διαχείριση πληροφοριών και ολοκλήρωσης του δικτύου των ασθενών. Οι ιατρικές συσκευές δέχονται απειλές από το κυβερνοχώρο, αφού έχουν τη δυνατότητα να θέσουν σε κίνδυνο την ακεραιότητα της τεχνολογίας των

πληροφοριών των νοσοκομείων (IT), τα δίκτυα και τη λειτουργία του ιατρικού εξοπλισμού (Coronado & Wong, 2014).

Το 2014, ταυτοποιήθηκαν περισσότερες από 300 ιατρικές συσκευές ότι διατρέχουν κίνδυνο. Οι χάκερ, έχουν δείξει πως μπορούν να έχουν πρόσβαση σε αντλίες ινσουλίνης και έχουν την δυνατότητα να χορηγήσουν μια θανατηφόρα δόση ινσουλίνης με ένα τηλεχειριστήριο. Οι κίνδυνοι αυτοί, είναι μεγαλύτεροι λόγω της ταχείας ανάπτυξης κινητών τεχνολογιών (Martin et al., 2017).

Σύμφωνα με τους Corando & Wong (2014), οι οργανισμοί θα πρέπει να εξεταστούν μερικά βασικά βήματα, όταν αρχίσει η εκπόνηση ενός σχεδίου για τη διαχείριση των κινδύνων στον κυβερνοχώρο. Ως πρώτο βήμα, θα πρέπει να προσδιοριστούν τα κύρια ενδιαφερόμενα μέρη σε μια εγκατάσταση και σαφώς να καθορίζουν την κατανομή της ασφάλειας του κυβερνοχώρου.

Δεδομένου ότι και οι ιατρικές συσκευές συνεχίζουν να προσφέρουν αυξημένες δυνατότητες συνδεσιμότητας και ολοκλήρωσης, οι κίνδυνοι ασφάλειας στον κυβερνοχώρο που συνδέονται με τις συσκευές θα πρέπει να αυξηθεί. Η διαχείριση των κινδύνων ασφάλειας στον κυβερνοχώρο είναι μια τεράστια ευθύνη, και όλοι οι εμπλεκόμενοι στην υγειονομική κοινότητα θα πρέπει να συνεργαστούν για την προστασία των εγκαταστάσεων ώστε να εξασφαλιστεί η βέλτιστη παροχή της φροντίδας του ασθενούς (Corando & Wong, 2014).

Όπως αναφέρει χαρακτηριστικά ο Kruse και συν. (2017), η έκθεση και η συχνότητα των επιθέσεων στον κυβερνοχώρο έχει αλλάξει, εντούτοις, τα κίνητρα και ο στόχος των εγκληματιών του κυβερνοχώρου παραμένουν τα ίδια. Οι ιατρικές πληροφορίες ενός ατόμου έχουν μεγαλύτερη αξία για τους εγκληματίες του κυβερνοχώρου σε σχέση με τα χρηματοπιστωτικά προσωπικά στοιχεία. Η πρόσβαση σε ιατρικές πληροφορίες επιτρέπει στους εγκληματίες του κυβερνοχώρου να διαπράξουν κλοπές της προσωπικής ταυτότητας, να προβούν σε ιατρική απάτη και σε εκβιασμό ενώ παράλληλα τους δίνεται η δυνατότητα να αποκτήσουν παράνομα ελεγχόμενες ουσίες.

Η εκτεταμένη κεντρική αποθήκευση των ιατρικών πληροφοριών σε αδύναμα συστήματα ασφαλείας πληροφορικής αλλά και η επέκταση της χρήσης της υγειονομικής περίθαλψης μέσω της τεχνολογίας, συμβάλλουν στην αύξηση των επιθέσεων στον κυβερνοχώρο στο

τομέα της υγείας.

Επομένως πρέπει να χρησιμοποιηθούν και άλλες τακτικές για τη μείωση της έκθεσης. Οι Argaw et al. (2020), τονίζουν ότι η σκόπιμη αλλαγή προεπιλεγμένων κωδικών πρόσβασης και η τακτική ενημέρωση των ρυθμίσεων ασφαλείας σε φορητούς υπολογιστές, διακομιστές και σταθμούς εργασίας, είναι πρακτικές που θα βοηθήσουν. Το λογισμικό προστασίας από ιούς είναι επίσης σημαντικό, όπως και η τακτική συντήρηση των αντιγράφων ασφαλείας (τα οποία θα πρέπει να αποθηκεύονται εκτός σύνδεσης). Το λογισμικό EDR μπορεί να βοηθήσει στον εντοπισμό παραβιάσεων ενός κακόβουλου λογισμικού και να αντιδράσει σωστά σε επιθέσεις.

Η χρησιμότητα και η ασφάλεια πρέπει να εξισορροπούνται με το απόρρητο και τη συμμόρφωση με τους κανονισμούς προστασίας δεδομένων, ειδικά σε περιβάλλοντα υψηλής κατανομής και συνεργασίας που απαιτούνται για την ιατρική ακρίβεια.

Η κυβερνοασφάλεια απαιτεί το υψηλότερο επίπεδο μέτρων ασφαλείας. Ωστόσο, δεδομένου ότι η αλάνθαστη ασφάλεια στον κυβερνοχώρο είναι ανύπαρκτη, κρίνεται απαραίτητη μια προσέγγιση βάσει κινδύνου μέσω της διαχείρισης του επιχειρηματικού κινδύνου. Ακόμη και με ποιοτικές υποδομές, τις βέλτιστες πρακτικές πληροφορικής, και με αυξημένα μέτρα ασφάλειας πληροφοριών, ο κίνδυνος της επίθεσης θα παραμείνει πάντοτε υψηλός (Argaw, 2020).

Η ασφάλεια στον κυβερνοχώρο δεν μπορεί ποτέ να είναι 100% αποτελεσματική, και η απειλή στην υγειονομική περίθαλψη είναι ένα αναπόφευκτη. Απώτερος στόχος της ασφάλειας του κυβερνοχώρου θα πρέπει να είναι η ενίσχυση της ανθεκτικότητας. Μια απλή προσέγγιση για τη βελτίωση της ανθεκτικότητας είναι η διατήρηση αντιγράφων ασφαλείας έτσι ώστε η επίθεση να μην οδηγήσει σε μόνιμη απώλεια δεδομένων.

Για να επιτευχθεί η ασφάλεια στον κυβερνοχώρο θα πρέπει να ενσωματωθεί από την αρχή, στο σχεδιασμό των νέων έργων πληροφορικής και παράλληλα θα πρέπει να είναι εγγενής σε όλα τα συστήματα υγειονομικής περίθαλψης (Martin et al, 2017).

Ο ιός COVID-19, δεν έχει αφήσει ανεπηρέαστο κανένα τομέα της υγειονομικής περίθαλψης. Παρόλο που ο τομέας της υγείας έχει καταβάλει υπεράνθρωπες προσπάθειες για την

αντιμετώπιση των τεχνολογικών προκλήσεων, με την εφαρμογή μέτρων ως προς την ευαισθητοποίηση της ασφάλειας και με την ανάπτυξη κατευθυντήριων οδηγιών για το COVID-19, απαιτούνται ακόμα, περισσότερες ερευνητικές προσπάθειες σε ορισμένους τομείς. Η έρευνα πρέπει να επικεντρωθεί στην διερεύνηση των βελτιωμένων τεχνικών ελέγχων μέσω της προσαρμογής των γενικών πρακτικών για την κυβερνοασφάλεια (π.χ. οδηγίες NIST).

Η βελτίωση της ανθεκτικότητας στον κυβερνοχώρο, επιτυγχάνεται με την οικοδόμηση μιας συντονισμένης προσπάθειας με τη συστηματική εκτίμηση των τρωτών σημείων της περίπλοκης αλυσίδας της υγειονομικής περίθαλψης. Η αντιμετώπιση των απειλών στον κυβερνοχώρο, επιτυγχάνεται με την μείωση των ανθρωπίνων περιστατικών ασφάλειας, διερευνώντας προσεγγίσεις για την μείωση των ανθρώπινων σφαλμάτων αλλά και μέσα από τις εκστρατείες ευαισθητοποίησης για την πανδημία.

Μέσω της ενίσχυση της στρατηγικής διαχείρισης της ασφάλειας στον κυβερνοχώρο, διερευνάται ο σχεδιασμός διαχείρισης κρίσεων, αναβαθμίζεται η ασφάλεια των κινδύνων που προκύπτουν και βελτιστοποιείται ο προϋπολογισμός για την ασφάλεια στον κυβερνοχώρο και την ανακατανομή των πόρων (He, et al, 2021).

Ο Kim (2017), υποστηρίζει ότι για την ευαισθητοποίηση της ασφάλειας στον κυβερνοχώρο και για την αποφυγή διαρροής δεδομένων, η εκπαίδευση της υγειονομικής κοινότητας περίθαλψης, κρίνεται αναγκαία. Η υιοθέτηση και εφαρμογή προγραμμάτων κατάρτισης, καθώς και το πρόγραμμα ασφάλειας των πληροφοριών στο σύνολό του, θα πρέπει να επαναξιολογηθούν μετά την εκπαίδευση, για να εντοπιστούν τυχόν κενά. Εάν υπάρχουν ελλείψεις, θα πρέπει να αναπτυχθεί ένα σχέδιο για την αντιμετώπισή τους, τόσο βραχυπρόθεσμα όσο και μακροπρόθεσμα. Αν και η συμμόρφωση είναι απαραίτητη, δεν ισούται με την ασφάλεια.

Κρίνεται αναγκαίο να καθοριστούν απαιτήσεις στην εκπαίδευση και στην πιστοποίηση ώστε να εφαρμοστεί και να αναπτυχθεί ένα επαγγελματικό εργατικό δυναμικό στον τομέα της ασφάλειας στον κυβερνοχώρο που παρέχει ένα επίπεδο διασφάλισης στους ασθενείς και στους εργοδότες. Για να καταστεί εφικτό, οι επαγγελματίες στον τομέα της ασφάλειας στον κυβερνοχώρο πρέπει να είναι σε θέση να προσαρμόσουν τα εργαλεία και τις πρακτικές για την προστασία των πληροφοριών, αλλά παράλληλα να μην εμποδίζουν τη διαθεσιμότητα για

όσους χρειάζονται τις πληροφορίες. Η παρεμπόδιση της διαθεσιμότητας δεν είναι απλώς ένα ζήτημα έκτακτης ανάγκης, αλλά μπορεί να είναι ένα ανεπιθύμητο συμβάν για την ασφάλεια των ασθενών. Αυτά τα γεγονότα , σύμφωνα με νόμους όπως το HIPAA μπορούν να οδηγήσουν σε αστικές και ποινικές κυρώσεις. Επομένως, απαιτείται μια εστιασμένη προσπάθεια εκπαίδευσης και αξιολόγηση της ικανότητας των επαγγελματιών στον τομέα της ασφάλειας στον κυβερνοχώρο (Murphy, 2015).

Δεδομένου ότι οι άνθρωποι είναι ο πιο αδύναμος κρίκος στην ασφάλεια στον κυβερνοχώρο, οι προσεγγίσεις των υπηρεσιών υγείας στην κυβερνοασφάλεια θα πρέπει να λαμβάνουν υπόψη την ανάγκη ευαισθητοποίησης όλων των χρηστών. Αυτό, φυσικά, δεν εγγυάται την ασφάλεια, αλλά είναι ένα βήμα προς τη σωστή κατεύθυνση. Οι τελικοί χρήστες, από τους κλινικούς ιατρούς έως το προσωπικό του προγραμματισμού, αλλά και από τους ασθενείς και τους φροντιστές που συνδέουν τις προσωπικές τους συσκευές με το νοσοκομειακό δίκτυο, μπορούν να απειλήσουν ακούσια ή σκόπιμα την ασφάλεια στον κυβερνοχώρο του κέντρου υγείας. Το ανθρώπινο σφάλμα ενέχει πολλούς κινδύνους και έτσι οι εκπαίδευση κρίνεται αναγκαία για όλους τους χρήστες.

Για να προσφέρουν σχετικές και αποτελεσματικές εκπαιδεύσεις, οι εγκαταστάσεις υγείας θα πρέπει συχνά να αξιολογούν και να εντοπίζουν κενά που υπάρχουν στη γνώση ως προς την κυβερνοασφάλεια. Είναι σημαντικό για τους τελικούς χρήστες να συνειδητοποιήσουν τους κινδύνους που προκαλούν μέσω ακούσιων ενεργειών. Για παράδειγμα, πρέπει να γνωρίζουν ότι η αποθήκευση δεδομένων στις κινητές του συσκευές, ενδέχεται να θέσουν σε κίνδυνο το απόρρητο και την ακεραιότητα των δεδομένων ενώ ταυτόχρονα η χρήση των συνδεδεμένων συσκευών ή αφαιρούμενων συσκευών αποθήκευσης μπορεί να αυξήσει τον κίνδυνο ενός κακόβουλου λογισμικού. Οι τελικοί χρήστες είναι πιθανοί στόχοι, επομένως τα εκπαιδευτικά προγράμματα θα πρέπει να τονίζουν την σωστή διαχείριση των μη αναγνωρισμένων e-mail και την τακτική του ηλεκτρονικού ψαρέματος (Argaw et al., 2020).

6. Συμπεράσματα

Η αλματώδης ανάπτυξη της τεχνολογίας αλλά και της ιατρικής επιστήμης, σηματοδοτούν μια νέα πορεία στο χώρο της παροχής υπηρεσιών υγείας. Το αυξημένο μορφωτικό και βιοτικό επίπεδο ωθεί την κοινωνία να αναζητά υπηρεσίες υγείας υψηλής ποιότητας και ασφάλειας. Η ένταξη της τεχνολογίας στις υπηρεσίες υγείας, αποσκοπεί στην βελτίωση της υγείας αφού μειώνει το κόστος των υπηρεσιών υγείας, μειώνονται τα λάθη και οι παραλείψεις ενώ ταυτόχρονα, οι πολίτες απολαμβάνουν σύγχρονες υπηρεσίες.

Η καινοτομία στην ψηφιακή υγεία είναι ότι αντιμετωπίζει πολλές ηθικές και πολιτικές προκλήσεις. Τα δεδομένα είναι υψίστης σημασίας για την ψηφιακή υγεία και η πρόσβαση σε επαρκείς ποσότητες δεδομένων είναι μια βασική προϋπόθεση για την ανάπτυξη καινοτόμων διαγνωστικών, θεραπευτικών και εργαλείων παρακολούθησης.

Δεδομένου ότι τα ιατρικά δεδομένα έχουν εμπορική αξία, καθιστά την ασφάλεια ως κυρίαρχο χαρακτηριστικό των τελικών εφαρμογών. Οι επιθέσεις στον κυβερνοχώρο σε ιατρικούς χώρους, η πειρατεία των βάσεων δεδομένων και οι απαγωγές δεδομένων αποτελούν συχνό φαινόμενο, αφού ολοένα και αυξάνονται τα περιστατικά παραβιάσεων δεδομένων και υποκλοπής τους. Τα θέματα ασφάλειας και εμπιστευτικότητας, αποτελούν κύριο μέλημα στο χώρο της υγείας. Στην Ευρώπη αλλά και σε πολλές άλλες χώρες, υπάρχουν οργανισμοί και κανόνες οι οποίοι επιβάλουν την προστασία των προσωπικών και ευαίσθητων δεδομένων.

Οι επαγγελματίες υγείας, αποτελούν την ραχοκοκαλιά των συστημάτων υγείας κάθε οργανισμού και οφείλουν να εναρμονίζονται με του κανονισμούς και τις προκλήσεις που προκύπτουν σε θέματα ασφάλειας. Από τα αποτελέσματα των ερευνών διαπιστώθηκε ότι οι επαγγελματίες υγείας, δεν έχουν την απαραίτητη γνώση να αντιμετωπίσουν τις κυβερνοεπιθέσεις που προκύπτουν. Παρόλο που αρκετοί έτυχαν εκπαίδευσης σε θέματα ασφαλείας, εντούτοις, δεν είναι ακόμη σε θέση να αναγνωρίζουν και να αντιμετωπίζουν πιθανές επιθέσεις. Αυτό βέβαια πιθανόν να οφείλεται και στην ελλιπή εκπαίδευση του προσωπικού από τους εργοδότες. Οι οργανισμοί υγείας οφείλουν να δώσουν περισσότερη έμφαση στα θέματα ασφαλείας αφού τα δεδομένα των ασθενών είναι ευαίσθητα και οφείλουν της ανάλογης αντιμετώπισης. Μπορεί η τεχνολογία να έχει βοηθήσει τον άνθρωπο σε πολλούς τομείς, παρόλα’ αυτά, πρέπει να γίνεται σωστός χειρισμός από τους λειτουργούς υγείας και παράλληλα να προωθείτε η ανάλογη εκπαίδευση τους.

Η οικονομική ενίσχυση στα προγράμματα εκπαίδευσης του προσωπικού αλλά και η χρηματοδότηση σε πλήρως εξοπλισμένα συστήματα ασφάλειας, θα πρέπει να βρίσκονται σε πρώτη προτεραιότητα από τους διοικητικούς διευθυντές. Η επαρκής ασφάλεια των οργανισμών με διάφορα πρότυπα και πλαίσια, μειώνει το κίνδυνο των κυβερνοεπιθέσεων και διασφαλίζονται τα δεδομένα, με αποτέλεσμα να αυξάνεται η εμπιστευτικότητα και η αξιοπιστία του οργανισμού.

Ακόμα και με την πανδημία που ταλανίζει ολόκληρο τον πλανήτη, δόθηκε η ευκαιρία στους εγκληματίες του κυβερνοχώρου, να εισβάλουν σε δεδομένα, αφού οι εργαζόμενοι δίνουν την μάχη με τον κορωνοϊό χωρίς να υπολογίζουν τους κινδύνους. Οι οργανισμοί, οφείλουν να παρέχουν δικλείδες ασφαλείας ώστε να διασφαλίζουν τους λειτουργούς της υγειονομικής περίθαλψης και παράλληλα και τους ασθενείς.

Στην Κύπρο, έχουν γίνει κάποια μικρά βήματα ως προς την διασφάλιση των δεδομένων των ασθενών. Ως μέλος τη Ευρωπαϊκής Ένωσης, η χώρα έχει εναρμονιστεί με τον Γενικό Κανονισμό Προσωπικών Δεδομένων οποίος προνοεί κυρώσεις σε περίπτωση παραβίασης του. Τόσο τα ιδιωτικά ιδρύματα όσο και τα δημόσια νοσηλευτήρια, με την εφαρμογή του Γενικού Σχεδίου Υγείας, έχουν αρχίσει δειλά – δειλά να χρησιμοποιούν ηλεκτρονικά δεδομένα των ασθενών, πράγμα που αποτελεί άλμα για τα κυπριακά δεδομένα. Η πραγματοποίηση μιας έρευνας μελλοντικά, για την ευαισθητοποίηση των κύπριων επαγγελματιών υγείας, θα κατέγραφε ενδιαφέρον δεδομένα τα οποία θα άξιζαν ανάλυσης.

Βιβλιογραφία

Ελληνόγλωσση

Bakker, A. (2007) Προστασία δεδομένων και εμπιστευτικότητα. Στο Mantas, J. & Hasman, A. (επιστημονική επιμέλεια) *Πληροφορική της Υγείας*, Εκδόσεις Π.Χ. Πασχαλίδης, Αθήνα.

Hovenga, E., Sermeus, W. (2007) Μέθοδοι ανάλυσης δεδομένων. Στο Mantas, J. & Hasman, A. (επιστημονική επιμέλεια) *Πληροφορική της Υγείας*, Εκδόσεις Π.Χ. Πασχαλίδης, Αθήνα.

Γαλάνης, Π. (2009) Συστηματική ανασκόπηση και μετα-ανάλυση. *Αρχεία Ελληνικής Ιατρικής*, 26(6):826-841. Διαθέσιμο: https://www.mednet.gr/archives/2009-6/pdf/826.pdf

Διαδικτυακό τόπος: https://hitrustalliance.net/

Επίσημη Εφημερίδα της Ευρωπαϊκής Ένωσης (2016) Οδηγία (ΕΕ) 2016/1148 του ευρωπαϊκού κοινοβουλίου και του συμβουλίου.

Κόλλια, Μ. (2017) Μοντέλα Επιθέσεων, Μετρικές και Προτεινόμενη Ιεράρχιση Μετρικών Κυβερνοασφάλειας. Μεταπτυχιακή εργασία, Πανεπιστήμιο Πατρών, Ελλάδα. Διαθέσιμο στο: https://nemertes.lis.upatras.gr/jspui/bitstream/10889/10360/3/Nemertes_Kollia(com).pdf

Κούμπουρος, Ι. (2015) Τεχνολογίες πληροφορίας και επικοινωνιών στην Υγεία. Ηλεκτρονικό βιβλίο.

Μερκούρης, Α. (2008). *Μεθοδολογία Νοσηλευτικής Έρευνας. Έλλην*: Αθήνα.

Μητάκος, Θ (2015) Οι χρήστες των πληροφοριακών συστημάτων διοίκησης. Ηλεκτρονικό Βιβλίο.

Χατζηπετρής, Α. (2020) Ο Γενικός Κανονισμός Προσωπικών Δεδομένων στο χώρο της υγείας: Διερεύνηση και αξιολόγηση του επιπέδου ενσωμάτωσης του κανονισμού στους οργανισμούς υγείας στην Κύπρο. Μεταπτυχιακή διατριβή, Ανοικτό Πανεπιστήμιο Κύπρου.

Ξενόγλωσση

Ahmed, M., Maglaras, L., Ferrag, M. (2020) Entrepreneurial Development and Innovation in Family Businesses and SMEs. Chapter 5th, Cyber Threats in the Healthcare Sector and Countermeasures. *Business Science Reference.*

Argaw, S., Troncoso-Pastoriza, J., Lacey, D., Florin, M., Calcavecchia, F., Anderson, D., Burleson, W., Voge, J.M., Leary, C., Chauvin, B., Flahault, A. (2020) Cybersecurity of Hospitals: discussing the challenges and working towards mitigating the risks. *BMC Medical Informatics and Decision Making,* 20:146.

California Department of Health Care Services (2019) Health Insurance Portability & Accountability Act. Διαθέσιμο στο: https://www.dhcs.ca.gov/formsandpubs/laws/hipaa/Pages/1.00WhatisHIPAA.aspx

Center for Internet Security. The 20 CIS Controls & Resources. Διαθέσιμο: https://www.cisecurity.org/controls/cis-controls-list/

Coronado, A., Wong, T. (2014) Healthcare Cybersecurity Risk management: Keys to an effective plan. Managing Risk. *Horizons*.

Coventry, L., Branley, D. (2018) Cybersecurity in healthcare: A narrative review of trends, threats and ways forward. *Maturitas*, 113, p.p. 48–52.

Craigen, D., Diakun-Thibault, N., Purse, R (2014) Defining Cybersecurity. Technology Innovation Management Review.

Disterer, G. (2013) ISO/IEC 27000, 27001 and 27002 for Information Security Management. *Journal of Information Security*, 4, p.p. 92-100. Διαθέσιμο στο: https://serwiss.bib.hs-hannover.de/frontdoor/deliver/index/docId/938/file/ISOIEC_27000_27001_and_27002_for_Information_Security_Management.pdf

ENISA (2020) Procurement Guidelines for Cybersecurity in hospitals. Good practices for the security of Healthcare services. European Union Agency for Cybersecurity. Διαθέσιμο στο: https://ec.europa.eu/futurium/en/system/files/ged/procurement_guidelines_for_cybersecurity_in_hospitals.pdf

epSOS (2021). European Patients – Smart Open Services, Making Healthcare Better. Διαθέσιμο: http://www.epsos.eu/.

Fabisiak, L., Hyla, T. (2020) Measuring cyber security awareness within groups of medical professionals in Poland. *53rd Hawaii International Conference on System Sciences.* Διαθέσιμο: https://scholarspace.manoa.hawaii.edu/bitstream/10125/64215/0383.pdf

Giansanti, D., Monoscalco, L. (2021) The cyber risk in cardiology: towards an investigation on the self perception among the cardiologists. *mHealth*, 7:28. Διαθέσιμο στο: https://www.ncbi.nlm.nih.gov/pmc/articles/PMC8063011/pdf/mh-07-2020.01.08.pdf

Gordon, W.J., Wright, A., Glynn, R.J., Kadakia, J., Mazzone, C., Leinbach, E., Landman, A. (2019). Evaluation of a mandatory phishing training program for high-risk employees at a US healthcare system. *Journal of the American Medical Informatics Association*, *26*(6), 547–552.

He, Y., Aliyu, A., Evans, M., Luo, C. (2021) Health Care Cybersecurity Challenges and Solutions Under the Climate of COVID-19: Scoping Review. *Journal Medical Internet Research*, 23(4):e21747. Διαθέσιμο: https://www.jmir.org/2021/4/e21747/.

Hughes, O. (2018). Norway healthcare cyber-attack could be biggest of its kind. Digital Health. Διαθέσιμο: https://www.digitalhealth.net/2018/01/norway-healthcare-cyber-attack-could-be-biggest/.

Hughes, O. (2018). Hancock regional hospital back online after paying hackers $55,000. Digital Health. Διαθέσιμο: https://www.digitalhealth.net/2018/01/hancock-regional-hospital-back-online/.

Jalali, M., Kaiser, P. J. (2018) Cybersecurity in Hospitals: A Systematic, Organizational Perspective. *Journal of Medical Internet Research*, 20(5).

Jumelle, A., Ispas, I., Thuemmler, Ch., Mival, O., Kosta, E., Casla, P., Azúa, S., González-Pinto, A. (2014) Ethical Assessment in E-Health. 16th International Conference on e-Health Networking, Applications and Services Healthcom.

Irwin, L. (2018). Breach at Norway's largest healthcare authority was a disaster waiting to happen. IT Governance Blog. Διαθέσιμο: https://www.itgovernance.eu/blog/en/breach-at-norways-largest-healthcare-authority-was-a-disaster-waiting-to-happen/.

Khandelwal, S. (2018). Nearly half of the Norway population exposed in HealthCare data breach. The Hacker News. Διαθέσιμο: https://thehackernews.com/2018/01/healthcare-data-breach.html.

Kim, L. (2017) Cybersecurity awareness: Protecting data and patients. Tech Notes, *Nursing 2017*, V. 47:6.

Kostkova, P. (2015) Grand Challenges in Digital Health. Front Public Health, 3:134.

Kruse, C.S., Frederick, B., Jacobson, T., Monticone, D. K. (2017) Cybersecurity in healthcare: A systematic review of modern threats and trends. *Technology and Health Care*, 25, p.p. 1–10.

Long, S. (2018). The cyber attack - from the POV of the CEO - Hancock regional hospital. Hancock Health. Διαθέσιμο: https://www.hancockregionalhospital.org/2018/01/cyber-attack-pov-ceo/.

Martin, G., Martin, P., Hankin, Ch., Darzi, A. (2017) Cybersecurity and healthcare: how safe are we? British Medical Journal.

Mayer, M., Martino, L., Mazurier, P., Tzvetkova, G. (2014) How would you define Cyberspace? Experimental online laboratory.

McLennan, S., Celi, L.A., Buyx, A. (2020) COVID-19: Putting the General Data Protection Regulation to the Test. *JMIR Public Health Surveill*, 6(2): e19279. Διαθέσιμο στο: https://www.ncbi.nlm.nih.gov/pmc/articles/PMC7265798/#

Mohammed, D., Mariani, R., Mohammed, Sh. (2015) Cybersecurity Challenges and Compliance Issues within the U.S. Healthcare Sector. *International Journal of Business and Social Research*, V. 05:2.

Muthuppalaniappan, M., Stevenson, K. (2021) Healthcare cyber-attacks and the COVID-19 pandemic: an urgent threat to global health. *International Journal for Quality in Health Care*, 33:1. Διαθέσιμο στο: https://academic.oup.com/intqhc/article/33/1/mzaa117/5912483?login=true

National Cyber Security Center (2019) 10 steps to cyber security. Διαθέσιμο στο: https://www.ncsc.gov.uk/collection/10-steps-to-cyber-security/introduction-to-cyber-security/executive-summary

National Institute of Standards and Technology. (2017) Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations. Revision 1. Διαθέσιμο στο: https://csrc.nist.gov/CSRC/media/Publications/sp/800-171/rev-1/archive/2016-12-20/documents/sp800-171r1-20161220.pdf

National Institute of Standards and Technology. (2018) Framework for Improving Critical Infrastructure Cybersecurity. Version 1.1. Διαθέσιμο στο: https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf

National Institute of Standards and Technology. (2020) Security and Privacy Controls for Federal Information Systems and Organizations. Revision 4. Διαθέσιμο στο: https://nvlpubs.nist.gov/nistpubs/specialpublications/nist.sp.800-53r4.pdf

Nune, P., Antunes, M., Silva, C. (2021) Evaluating cybersecurity attitudes and behaviors in Portuguese healthcare institutions. *Procedia Computer Science*, 11, p.p. 173-181. Διαθέσιμο: https://www.sciencedirect.com/science/article/pii/S1877050921001563

Ondiege, B., Clarke, M. (2017) Health care professionals' perception of security of personal health devices. *Dove press*, 4:35-42.

Priestman, W., Anstis, T., Sebire, I.G. et al. (2019). Phishing in healthcare organisations: threats, mitigation and approaches. *BMJ Health Care Inform, 26*.

Roumani, M., Fung, C., Rai, S., Xie, H (2016) Value Analysis of Cyber Security Based on Attack Types. *ITMSOC Transactions on Innovation & Business Engineering* 01, p.p. 34–39. Διαθέσιμο: https://researchrepository.murdoch.edu.au/id/eprint/34865/1/ValueAnalysis-Paper.pdf

Scholl, M., Stine, K., Hash, J., Bowen, P., Johnson, A., Smithm C, Steinberg, D. (2008) An Introductory Resource Guide for Implementing the Health Insurance Portability and Accountability Act (HIPAA) Security Rule. Computer Security Resource Center. Διαθέσιμο: https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-66r1.pdf.

Secureworks (2018). Secureworks Counter Threat Unit Threat Intelligence. SamSam Ransomware campaigns. Secureworks. Διαθέσιμο: https://www.secureworks.com/research/samsam-ransomware-campaigns.

Steffen, S. (2016). Hackers hold German hospital data hostage. DW. Διαθέσιμο: http://www.dw.com/en/hackers-hold-german-hospital-data-hostage/a-19076030.

Stobert, E., Barrera, D., Hemier, V., Kokkak. D. (2020) Understanding Cybersecurity Practices in Emergency Departments. Paper from Conference on Human Factors in Computing Systems, Honolulu, HI, USA.

Warwick, A. (2018). Norwegian healthcare breach alert failed GDPR requirements. Computer Weekly. Διαθέσιμο: http://www.computerweekly.com/news/252433538/Norwegian-healthcare-breach-alert-failed-GDPR-requirements.

Vayena, E., Haeusermann, T., Adjekum, A., Blasimme, A. (2018) Digital Health meeting the ethical and policy challenges. Swiss Medical Weekly.

Yuan, B., Li, J. (2019) The Policy Effect of the General Data Protection Regulation (GDPR) on the Digital Public Health Sector in the European Union: An Empirical Investigation. *International Journal of Environmental Research and Public Health,* 16(6), 1070. Διαθέσιμο στο: https://www.mdpi.com/1660-4601/16/6/1070/htm.

Zorz, Z. (2016). Crypto ransomware hits German hospitals. Help Net Security. Διαθέσιμο: https://www.helpnetsecurity.com/2016/02/26/crypto-ransomware-hits-german-hospitals/.