Σχολή Οικονομικών Επιστημών και Διοίκησης Επιχειρήσεων

Τμήμα Διοικητικής Επιστήμης και Τεχνολογίας

Διπλωματική εργασία

Ασφάλεια πληροφοριακών συστημάτων υγείας

Ονοματεπώνυμο: Ελένη Βαγγέλη

Α.Μ: 1104162

Εποπτεύων καθηγητής: κ. Ιωάννης Σταματίου

ΑΘΗΝΑ 2024

ΕΥΧΑΡΙΣΤΙΕΣ

Θα ήθελα να ευχαριστήσω θερμά τον επιβλέποντα καθηγητή κ. Σταματίου Ιωάννη για την πολύτιμη βοήθειά του, την καθοδήγηση και άμεση απάντηση στις απορίες μου, κατά την διάρκεια της εκπόνησης της παρούσας διπλωματικής εργασίας.

ΠΙΝΑΚΑΣ ΠΕΡΙΕΧΟΜΕΝΩΝ

ΠΕΡΙΛΗΨΗ

Οι οργανισμοί σήμερα, αντιμετωπίζουν εκατοντάδες κινδύνους για τους οποίους πρέπει να προετοιμαστούν για να εξασφαλίσουν ένα ασφαλές περιβάλλον για τους πελάτες, τους υπαλλήλους και την επιχειρηματική τους συνέχεια. Αυτοί οι κίνδυνοι μπορεί να κυμαίνονται από την απειλή φυσικής εγκατάστασης, όπως πυρκαγιά ή απώλεια ισχύος, έως απειλή για την ασφάλεια των εργαζομένων.

Τα πληροφοριακά συστήματα, με την επιχειρηματική έννοια του όρου, είναι συμπληρωματικά δίκτυα και διασυνδεδεμένα στοιχεία που συγκεντρώνουν, διαχέουν και καθιστούν τα δεδομένα χρήσιμα για την ενίσχυση των διαδικασιών λήψης αποφάσεων της διοίκησης. Τα συστήματα πληροφοριών έχουν εξελιχθεί με την πάροδο του χρόνου, απαιτώντας επαναπροσδιορισμούς καθώς οι νέες τεχνολογίες (Web 2.0, για παράδειγμα) έχουν πολλαπλασιαστεί. Τα τελευταία 30 χρόνια, το έγκλημα στον κυβερνοχώρο και η κυβερνοτρομοκρατία έχουν εξελιχθεί από μια πιθανή ανησυχία σε κοινή απειλή. Οι κυβερνοαπειλές έγιναν ζήτημα εθνικής ασφάλειας μετά την 11η Σεπτεμβρίου. Μετά τις τρομοκρατικές επιθέσεις της 11ης Σεπτεμβρίου 2001, ο Πρόεδρος Μπους δημιούργησε το Γραφείο Ασφάλειας Κυβερνοχώρου.

Η διαχείριση κινδύνων στον κυβερνοχώρο στην υγειονομική περίθαλψη, δεν έχει μελετηθεί εκτενώς, αλλά τα δεδομένα από αυτή τη διατριβή υποδηλώνουν ότι ο τομέας δεν είναι ο πιο σημαντικός παράγοντας όσον αφορά τη διαχείριση του κινδύνου στον κυβερνοχώρο. Αντί να απαιτούνται συγκεκριμένες μέθοδοι για τη διαχείριση του κινδύνου στον κυβερνοχώρο, οι γενικές αρχές διαχείρισης κινδύνου μπορούν να χρησιμοποιηθούν αποτελεσματικά από τον τομέα της υγειονομικής περίθαλψης.

Τα ευρήματα υποδεικνύουν ότι ορισμένα χαρακτηριστικά που είναι κοινά μεταξύ των οργανισμών υγειονομικής περίθαλψης, όπως τα παλαιού τύπου συστήματα, θα πρέπει να λαμβάνονται υπόψη στη διαχείριση κινδύνων στον κυβερνοχώρο. Θα μπορούσε να υποστηριχθεί ότι ορισμένα χαρακτηριστικά ενός οργανισμού ή του επιχειρησιακού του περιβάλλοντος και όχι του τομέα, σχετίζονται περισσότερο με τους κινδύνους στον κυβερνοχώρο. Τέλος, μία από τις προκλήσεις στη διαχείριση κινδύνων στον κυβερνοχώρο της υγειονομικής περίθαλψης, περιλαμβάνει τον χρόνιο δημοσιονομικό περιορισμό, ο οποίος δεν είναι μοναδικός για την υγειονομική περίθαλψη.

Λέξεις- κλειδιά: κυβερνοασφάλεια, κυβερνοεπιθέσεις, πληροφοριακά συστήματα υγείας, κυβερνοχώρο, υγειονομική περίθαλψη

ABSTRACT

The organizations today face hundreds of risks for which they must prepare to ensure a secure environment for their customers, employees and business continuity. These risks can range from threatening a physical facility, such as a fire or power loss, to a threat to worker safety.

The information systems, in the business sense of the term, are complementary networks and interconnected elements that gather, disseminate and make data useful to enhance management decision-making processes. Information systems have evolved over time, requiring redefinitions as new technologies (Web 2.0, for example) have proliferated. Over the past 30 years, cybercrime and cyberterrorism have evolved from a potential concern to a common threat. Cyber threats became a national security issue after 9/11. After the terrorist attacks of September 11, 2001, President Bush created the Office of Cybersecurity.

The cyber risk management in healthcare has not been extensively studied, but the data from this thesis suggests that the domain is not the most important factor when it comes to cyber risk management. Rather than requiring specific methods to manage cyber risk, general risk management principles can be used effectively by the healthcare sector.

The findings suggest that certain characteristics common among healthcare organizations, such as legacy systems, should be considered in cyber risk management. It could be argued that certain characteristics of an organization or its business environment, rather than the sector, are more relevant to cyber risks. Finally, one of the challenges in

healthcare cyber risk management involves the chronic budget constraint, which is not unique to healthcare.

Key Words: cyber security, cyberattacks, health information systems (HIS), cyberspace, healthcare

ΕΙΣΑΓΩΓΗ

Αποτελεί γεγονός πως ο τομέας της ασφάλειας στον κυβερνοχώρο, για ιδιώτες αλλά και επιχειρήσεις, δημόσιες ή/και ιδιωτικές, αλλάζει συνεχώς με την εμφάνιση νέων απειλών. Ο τομέας της υγειονομικής περίθαλψης, παρέχει ωστόσο, κάποιες κρίσιμες για τη ζωή υπηρεσίες, καθώς οι επιτιθέμενοι στον κυβερνοχώρο, προσπαθούν να *εκμεταλλευτούν* τα τρωτά σημεία του (Ismailov, 2018).

Ο κλάδος της υγείας λοιπόν, είναι ένας από τους βασικούς στόχους της ασφάλειας στον κυβερνοχώρο, εκθέτοντας εκατομμύρια ανθρώπους διεθνώς, σε απειλές στον κυβερνοχώρο. Τα νοσοκομεία, οι γιατροί, οι ασφαλιστικές εταιρείες και ούτω καθεξής, είναι οι κύριοι στόχοι για τους επιτιθέμενους λόγω των Προστατευόμενων Πληροφοριών Υγείας που διατηρούν και του ζωτικού ρόλου που διαδραματίζουν στην κρίσιμη υποδομή της χώρας στην οποία βρίσκονται (Kieny et al., 2017).

Όταν συμβαίνει μια επίθεση στον κυβερνοχώρο, οι συνέπειες εκτείνονται πέρα από τις οικονομικές απώλειες και τη φήμη του κάθε οργανισμού. Οι προστατευόμενες πληροφορίες υγείας είναι πολύτιμες για τους χάκερ και σε αντίθεση με άλλες φόρμες δεδομένων, είναι μοναδικές για κάθε άτομο αφού δεν μπορούν να αντικατασταθούν, μετά από κάποια επίθεση (Kieny et al., 2017). Οι κυβερνοεπιθέσεις επίσης, μπορούν να κατακτήσουν συστήματα υπολογιστών και να περιορίσουν την πρόσβαση σε κρίσιμα δεδομένα, να απενεργοποιήσουν συστήματα και εξοπλισμό υγειονομικής περίθαλψης, ακόμη και να προσθέσουν βασικά σημαντικά στοιχεία σε αξονικές και μαγνητικές τομογραφίες. Παρά τους κανονισμούς που υφίστανται οι τομείς υγείας, η εφαρμογή των

μέτρων ασφαλείας εξακολουθεί να χρειάζεται βελτίωση (Ismailov, 2018).

Σε διεθνή βάση ωστόσο, σημειώνεται πως το 89% των οργανισμών υγειονομικής περίθαλψης, δέχθηκαν παραβιάσεις δεδομένων τα τελευταία δύο χρόνια και ο τομέας της υγείας ήταν ο κορυφαίος κλάδος για επιθέσεις στον κυβερνοχώρο και παραβιάσεις δεδομένων το έτος 2018. Η ίδια τάση συνεχίστηκε και το 2019. Όμως καθ' όλη τη διάρκεια του 2020 και της διάρκειας του κορωνοϊού, ο ψηφιακός μετασχηματισμός στον τομέα της υγειονομικής περίθαλψης και η πανδημία του ιού COVID-19, δημιουργεί έναν *επικίνδυνο* χώρο σε σχέση με την ασφάλεια στον κυβερνοχώρο. Τα δεδομένα που βασίζονται στο i-cloud αυξάνονται επίσης, καθώς γιατροί, διαχειριστές και ασθενείς υγείας, αναζητούν κάποια ασφαλή πρόσβαση σε εμπιστευτικές πληροφορίες με χαμηλότερο κόστος. Σύμφωνα με την ίδια πηγή, ο ιατρικός εξοπλισμός και η τηλεϊατρική εγκυμονούν κινδύνους για την ασφάλεια του Διαδικτύου των Πραγμάτων – IoT, αφού διευρύνουν περαιτέρω το τοπίο απειλών (Barnett, et al., 2013).

Βάσει των ανωτέρω λοιπόν, θα λέγαμε πως οι οργανισμοί σήμερα, αντιμετωπίζουν εκατοντάδες κινδύνους για τους οποίους πρέπει να προετοιμαστούν για να εξασφαλίσουν ένα ασφαλές περιβάλλον για τους πελάτες, τους υπαλλήλους και την επιχειρηματική τους συνέχεια. Αυτοί οι κίνδυνοι μπορεί να κυμαίνονται από την απειλή φυσικής εγκατάστασης, όπως πυρκαγιά ή απώλεια ισχύος, έως απειλή για την ασφάλεια των εργαζομένων (Ismailov, 2018).

Για να προετοιμαστούν καλύτερα για αυτές τις απειλές και να συντονίσουν μια πιο αποτελεσματική απόκριση στην όποια απειλή, οι οργανισμοί αναπτύσσουν διαδικασίες λειτουργίας έκτακτης ανάγκης. Το έγκλημα στον κυβερνοχώρο λοιπόν, είναι μια νέα και αναδυόμενη απειλή που πρέπει να λαμβάνεται υπόψη κατά την προετοιμασία των διαδικασιών λειτουργίας έκτακτης ανάγκης ενός ιδρύματος (Barnett, et al., 2013).

Ένας συγκεκριμένος κλάδος λοιπόν, που είναι ιδιαίτερα ευάλωτος στο έγκλημα στον κυβερνοχώρο, είναι ο κλάδος της υγειονομικής περίθαλψης λόγω της εξάρτησής του από ηλεκτρονικές πληροφορίες υγείας, καθώς και των απαρχαιωμένων συστημάτων ασφαλείας τους (Luna, et al., 2016). Σημειώνεται επίσης πως τα συντονισμένα ηλεκτρονικά ιατρικά αρχεία, η απεικόνιση, οι φαρμακευτικές υπηρεσίες, οι εργαστηριακές υπηρεσίες και ακόμη και οι συσκευές θεραπείας βασίζονται στην ηλεκτρονική σύνδεση και σε σχετικές απειλές στον κυβερνοχώρο.

Ωστόσο, μια ακόμη νεότερη απειλή για τους οργανισμούς υγειονομικής περίθαλψης, είναι οι επιθέσεις κακόβουλου λογισμικού, όπου οι εγκληματίες του κυβερνοχώρου μπορούν να κρυπτογραφήσουν τα αρχεία ενός οργανισμού, ουσιαστικά κλείνοντας αυτόν τον οργανισμό ηλεκτρονικά. Ξεκινώντας από το έτος 2016 για παράδειγμα, σημειώνεται πως υπήρξε μια σειρά από σημαντικές επιθέσεις ransomware σε νοσοκομεία σε όλες τις Ηνωμένες Πολιτείες (Kieny et al., 2017).

Τον Μάιο του έτους 2017, σημειώθηκε ένα ξέσπασμα περισσότερων από 75.000 επιθέσεων ransomware που στόχευσαν τουλάχιστον σε 99 χώρες σε όλο τον κόσμο, το οποίο οι ειδικοί αναφέρουν ένα από τα μεγαλύτερα περιστατικά ασφάλειας στον κυβερνοχώρο (Larson, 2017). Ως μέρος αυτής της επίθεσης, τουλάχιστον 36 οργανισμοί υγειονομικής περίθαλψης σε όλη τη Μεγάλη Βρετανία, αποκλείστηκαν από τα συστήματα υπολογιστών τους με αποτέλεσμα η Εθνική Υπηρεσία Υγείας να ακυρώσει τα ραντεβού των εξωτερικών ασθενών και να εκτρέψει αυτούς μακριά από τα τμήματα επειγόντων περιστατικών (Perlroth & Sanger, 2017). Τον Δεκέμβριο του έτους 2017, ένας σύμβουλος Εσωτερικής Ασφάλειας ανέφερε χαρακτηριστικά ότι αυτή η επίθεση και τα αποτελέσματά της, θέτουν άμεσα σε κίνδυνο τις ζωές των ανθρώπων (Chappell & Neuman, 2017).

Σημειώνεται επίσης πως όχι μόνο αυτή η απειλή θέτει σε κίνδυνο την υγεία των ασθενών, αλλά αυτές οι επιθέσεις κοστίζουν στο σύστημα υγειονομικής περίθαλψης των Ηνωμένων Πολιτειών ένα υπέρογκο χρηματικό ποσό. Μόνο το 2015, το FBI έλαβε 2.500 καταγγελίες για επιθέσεις ransomware σε όλες τις βιομηχανίες, οι οποίες στοίχισαν στα θύματα, 214 εκατομμύρια δολάρια (Radke, et al., 2016).

Επίσης μια δημοσίευση της Αμερικανικής Ένωσης Δημόσιας Υγείας, ανέφερε μια έκθεση τεχνολογίας που έγγραφε ότι το 2016, υπήρξαν 1.500 κυβερνοεπιθέσεις σε οργανισμούς που σχετίζονται με την υγεία και όπου εξέθεσαν προσωπικές πληροφορίες σε πάνω από 155 εκατομμύρια Αμερικανούς. Αυτή η δημοσίευση σημείωσε επίσης ότι το κόστος των παραβιάσεων δεδομένων υγειονομικής περίθαλψης, είναι η υψηλότερη σε όλους τους κλάδους (Krisberg, 2017).

Ωστόσο, πολύ λίγες μελέτες έως τις μέρες μας, έχουν εξετάσει τις επιθέσεις τύπου ransomware και πώς θα μπορούσαν ενδεχομένως να επηρεάσουν τους οργανισμούς υγειονομικής περίθαλψης. Μια συστηματική ανασκόπηση που δημοσιεύθηκε το έτος 2016, βρήκε μόνο 19 άρθρα που δημοσιεύτηκαν σε περιοδικά με κριτές μεταξύ 2008 και

2015 σχετικά με το θέμα των κυβερνοεπιθέσεων σε συστήματα υγείας, και η πλειονότητα από αυτά επικεντρώθηκε σε παραβιάσεις δεδομένων προστατευμένων πληροφοριών υγείας (Luna et al., 2016).

Είναι σημαντικό τέλος, να κατανοήσει κανείς τον κίνδυνο, τον μετριασμό και την ετοιμότητα αυτής της απειλής για την προστασία της ασφάλειας όσων βρίσκονται εντός και εκείνων που εξυπηρετούνται από ένα νοσοκομείο (Ayala, 2016). Υπάρχει ανάγκη λοιπόν να καταγραφούν οι υπάρχουσες απειλές στον κυβερνοχώρο που αντιμετωπίζουν τα νοσοκομεία και να διευρυνθούν οι γνώσεις τους σχετικά με την οργανωτική ετοιμότητα και τον μετριασμό αυτών των απειλών.

ΚΕΦΑΛΑΙΟ 1^{Ο} – ΕΝΝΟΙΑ ΚΑΙ ΧΑΡΑΚΤΗΡΙΣΤΙΚΑ ΤΗΣ ΛΕΙΤΟΥΡΓΙΑΣ ΤΩΝ ΠΛΗΡΟΦΟΡΙΑΚΩΝ ΣΥΣΤΗΜΑΤΩΝ ΚΑΘΩΣ ΚΑΙ ΠΡΟΣΤΑΣΙΑ ΑΠΟ ΚΥΒΕΡΝΟΕΠΙΘΕΣΕΙΣ ΣΤΟ ΤΟΜΕΑ ΤΗΣ ΥΓΕΙΑΣ

1.1 Η Έννοια και τα Χαρακτηριστικά Λειτουργίας των Πληροφοριακών Συστημάτων στις Επιχειρήσεις

Τα πληροφοριακά συστήματα, με την επιχειρηματική έννοια του όρου, είναι συμπληρωματικά δίκτυα και διασυνδεδεμένα στοιχεία που συγκεντρώνουν, διαχέουν και καθιστούν τα δεδομένα χρήσιμα για την ενίσχυση των διαδικασιών λήψης αποφάσεων της διοίκησης (Yu, Zhao & Song, 2021). Τα συστήματα πληροφοριών έχουν εξελιχθεί με την πάροδο του χρόνου, απαιτώντας επαναπροσδιορισμούς καθώς οι νέες τεχνολογίες (Web 2.0, για παράδειγμα) έχουν πολλαπλασιαστεί.

Ωστόσο, τα πληροφοριακά συστήματα δεν είναι μόνο τεχνολογικά. Εκτός από τα στοιχεία του υλικού, του λογισμικού και των δεδομένων, τα οποία από καιρό θεωρούνταν η βασική τεχνολογία των πληροφοριακών συστημάτων, έχει προταθεί να προστεθεί ένα άλλο στοιχείο: η επικοινωνία (Ransbotham, Kiron, & Prentice, 2016). Ένα πληροφοριακό σύστημα μπορεί να υπάρξει χωρίς την ικανότητα επικοινωνίας — οι πρώτοι προσωπικοί υπολογιστές ήταν αυτόνομες μηχανές που δεν είχαν πρόσβαση στο διαδίκτυο. Ωστόσο, στον σημερινό υπερσυνδεδεμένο κόσμο, είναι ένας εξαιρετικά σπάνιος υπολογιστής που δεν συνδέεται με άλλη συσκευή ή δίκτυο.

Για την ενοποίηση της επικοινωνίας, ο Bourgeois προτείνει την προσθήκη ατόμων και διεργασιών στο παραδοσιακό υλικό, λογισμικό και στοιχεία δεδομένων των συστημάτων πληροφοριών. Τα στελέχη επιχειρήσεων σχεδόν σε κάθε κλάδο έχουν ανακαλύψει ότι οι διαδικασίες που χρησιμοποιούν, ιδιαίτερα οι υπηρεσίες ανάλυσης cloud "ως υπηρεσία" και η ενεργή συμμετοχή πελατών που θέλουν να προσαρμόζουν περισσότερο τις εμπειρίες τους κάθε χρόνο είναι αδιαχώριστες από τα συστήματα πληροφοριών επιχειρήσεων (Sharma, Ali, & Husain, 2017). Μόλις ενσωματωθούν όλα τα στοιχεία, κάθε

πληροφοριακό σύστημα διαδραματίζει αρκετούς ρόλους για τις επιχειρήσεις με διάφορους βαθμούς σημασίας ανάλογα με τις ανάγκες μιας εταιρείας. Η Davoren αναλύει τις σχετικές σημαντικές λειτουργίες για τις επιχειρήσεις, ως εξής:

- ✓ **Αποθήκευση και ανάλυση πληροφοριών**: Προηγμένες και ολοκληρωμένες βάσεις δεδομένων, μερικές φορές βασισμένες σε υπηρεσίες ανάλυσης cloud, χρησιμοποιούνται για την αποθήκευση και ανάλυση πληροφοριών που σχετίζονται με επιχειρηματικές λειτουργίες, πελάτες, δεδομένα συναλλαγών και δραστηριότητα τόσο των εργαζομένων όσο και των πελατών. Τα αποτελέσματα αυτών των αναλύσεων παρέχουν πληροφορίες που μπορούν να βοηθήσουν τους υπεύθυνους λήψης αποφάσεων να λύσουν τρέχοντα και μελλοντικά ζητήματα.
- ✓ **Βοήθεια στη λήψη αποφάσεων**: Τα συστήματα πληροφοριών μπορούν να συγκρίνουν εσωτερικές αναλύσεις με εξωτερικές πηγές για να συγκρίνουν, για παράδειγμα, εσωτερικές πληροφορίες με πληροφορίες σχετικά με τη γενική κατάσταση της οικονομίας ή τις οικονομικές εκθέσεις των ανταγωνιστών. Οι υπεύθυνοι λήψης αποφάσεων χρησιμοποιούν αυτές τις γνώσεις για να επανεξετάσουν την επάρκεια και την ποιότητα των στρατηγικών τους αποφάσεων.
- ✓ **Βοήθεια στις επιχειρηματικές διαδικασίες**: Τα πληροφοριακά συστήματα χρησιμοποιούνται για την ανάπτυξη συστημάτων προστιθέμενης αξίας για επιχειρηματικές λειτουργίες. Οι επιχειρηματικές διαδικασίες μπορούν να απλοποιηθούν και οι περιττές δραστηριότητες μπορούν να εξορθολογιστούν μέσω της χρήσης πληροφοριακών συστημάτων προσαρμοσμένων σε κοινά επιχειρηματικά καθήκοντα, όπως η κατασκευή, η αλυσίδα εφοδιασμού και οι διαδικασίες των εργαζομένων.

Καθώς τα πληροφοριακά συστήματα εδραιώνονται όλο και περισσότερο στον κόσμο των επιχειρήσεων, τα διευθυντικά στελέχη και τα στελέχη των εταιρειών αναμένεται να εξοικειωθούν διεξοδικά με τα συστήματα πληροφοριών επιχειρήσεων και με το τι έχουν να προσφέρουν. Αντίστοιχα, πολλά μαθήματα MBA έχουν προσθέσει την τεχνολογία των πληροφοριών στο πρόγραμμα σπουδών τους.

1.2 Δυνατότητες των Πληροφοριακών Συστημάτων

Οι διευθυντές επιχειρηματικών τμημάτων που επωφελούνται από συστήματα πληροφοριών πρέπει να γνωρίζουν τις βασικές δυνατότητες της τεχνολογίας πληροφοριών, της ανάλυσης δεδομένων και των συστημάτων επιχειρηματικής ευφυΐας. Τα συστήματα πληροφοριών διαχείρισης χρησιμοποιούν όλες αυτές τις δυνατότητες με τρόπο προσαρμοσμένο στη λήψη διοικητικών και εκτελεστικών αποφάσεων. Ο Linton διαχωρίζει τις δυνατότητες του συστήματος πληροφοριών σε σχετικές κατηγορίες ως εξής (Yu, Zhao & Song, 2021):

✓ Πρόσβαση σε πληροφορίες: Οι διευθυντές πρέπει να έχουν εύκολη και γρήγορη πρόσβαση σε πληροφορίες, συμπεριλαμβανομένων των αρχείων πελατών, των δεδομένων πωλήσεων, της έρευνας αγοράς, των οικονομικών αρχείων, των δεδομένων κατασκευής και των αποθεμάτων και των αρχείων ανθρώπινου δυναμικού για να λαμβάνουν τεκμηριωμένες αποφάσεις.

✓ Συλλογή δεδομένων: Τα συστήματα πληροφοριών διαχείρισης συλλέγουν και συγκεντρώνουν δεδομένα τόσο από το εξωτερικό όσο και από το εσωτερικό ενός οργανισμού. Αυτά τα δεδομένα συγκεντρώνονται και στεγάζονται σε αποθήκες δεδομένων, οι οποίες στη συνέχεια δικτυώνονται μεταξύ τους για σκοπούς ανάλυσης.

✓ Συνεργασία: Μία από τις πιο χρήσιμες λειτουργίες των πληροφοριακών συστημάτων είναι η ευκολία με την οποία διαφορετικά τμήματα και κατανεμημένες ομάδες μπορούν να συνεργάζονται για αποφάσεις, λαμβάνοντας υπόψη τεράστιες ποσότητες δεδομένων από διάφορες πηγές, τμήματα ή ακόμα και κλάδους.

✓ Ερμηνεία: Μετά τη λήψη μιας απόφασης, τα πληροφοριακά συστήματα μπορούν να βοηθήσουν τους διαχειριστές να κατανοήσουν τις πιθανές επιπτώσεις αυτής της απόφασης ενημερώνοντας συνεχώς ακατέργαστα δεδομένα και προβλέποντας πιθανά μελλοντικά οφέλη ή προβλήματα.

✓ Παρουσίαση: Τα περισσότερα πληροφοριακά συστήματα, ειδικά εκείνα που προορίζονται για χρήση από διευθυντές, περιλαμβάνουν εργαλεία σχεδιασμένα για τη δημιουργία ευνόητων αναφορών για έλεγχο από διευθυντές υψηλότερου επιπέδου ή στελέχη C-suite.

✓ Οι διευθυντές μπορούν επίσης να επωφεληθούν από συστήματα πληροφοριών που έχουν σχεδιαστεί ειδικά για επιχειρηματικές λειτουργίες που επηρεάζουν το τμήμα ή τη θέση τους. Όλα τα συστήματα πληροφοριών μάρκετινγκ, τα υποσυστήματα προϊόντων, η πρόβλεψη πωλήσεων και τα συστήματα σχεδιασμού προϊόντων δημιουργούν πληροφορίες που είναι πολύτιμες για τους διευθυντές.

1.3 Ορισμός και Χαρακτηριστικά των Πληροφοριακών Συστημάτων Υγείας

Η εφαρμογή των πληροφοριακών συστημάτων υγείας (Health Information Systems) είναι πολύπλοκη, μη γραμμική και απρόβλεπτη. Ενδεχομένως, επειδή ο ίδιος ο οργανισμός υγειονομικής περίθαλψης είναι ένα πολύπλοκο κοινωνικοτεχνικό δίκτυο. Αυτό το χαρακτηριστικό του οργανισμού υγειονομικής περίθαλψης, παρουσιάζει δυσκολία στην ταξινόμηση της εφαρμογής των πληροφοριακών συστημάτων υγείας, ως επιτυχημένης.

Τα διάφορα ενδιαφερόμενα μέρη στον οργανισμό, μπορεί να ερμηνεύουν διαφορετικά την επιτυχή εφαρμογή. Εξάλλου, η επιτυχία είναι μια πολυδιάστατη έννοια που είναι δυναμική και κυμαινόμενη γιατί εξελίσσεται με την πάροδο του χρόνου. Η επιτυχία της εφαρμογής του συστήματος μπορεί να θεωρηθεί ως προς την αποτελεσματικότητα, την αποδοτικότητα, τις οργανωτικές στάσεις, τη δέσμευση στη συνεχή χρήση του και την ικανοποίηση των τελικών χρηστών· τόσο το προσωπικό όσο και οι πελάτες (Berg, 2001, Sligo et al., 2017).

Ο Berg (2001) προτείνει ότι η επιτυχία είναι υποκειμενική και ως εκ τούτου θα πρέπει να αξιολογηθεί λαμβάνοντας υπόψη σε ποιον απευθύνεται το ζήτημα της επιτυχίας της υλοποίησης. Ως εκ τούτου, μπορεί να φαίνεται περιττό να υποθέσουμε παράγοντες που οδηγούν στην επιτυχή εφαρμογή των πληροφοριακών συστημάτων (IS) στην υγειονομική περίθαλψη (Berg, 2001).

Ωστόσο, υπάρχουν κοινά χαρακτηριστικά που μοιράζονται τα συστήματα πληροφοριών υγείας, που θεωρούνται επιτυχημένα. Αυτά τα χαρακτηριστικά ή ιδέες, όπως προτείνονται από τον Berg, (2001) μπορούν να χρησιμοποιηθούν ως «βοηθήματα» για να βοηθήσουν άλλους οργανισμούς υγείας να εφαρμόσουν τα δικά τους πληροφοριακά συστήματα. Στις αναπτυσσόμενες χώρες, ο κίνδυνος τα συστήματα πληροφοριών υγείας να θεωρούνται αποτυχημένα εάν βασίζονται σε γνώσεις από τη βιβλιογραφία των συστημάτων πληροφοριών υγείας, είναι πολύ υψηλός.

Τα σχέδια συστημάτων πληροφοριών υγείας από τις δυτικές ή βιομηχανικές χώρες, έχουν κυριαρχήσει στον τομέα της υγείας στις αναπτυσσόμενες χώρες. Αυτό μπορεί να αποδοθεί στις οικονομίες της καινοτομίας, των επιχειρήσεων, των πολιτικών βοήθειας και των πολιτιστικών συμπεριφορών που υποδεικνύουν ότι η πλειονότητα των ερευνητών και εταιρειών ΤΠΕ, βρίσκονται στις βιομηχανικές χώρες.

Επιπλέον, οι βιομηχανικές χώρες έχουν επενδύσει πολλά σε νέα συστήματα πληροφοριών τα οποία εισάγουν στις αναπτυσσόμενες χώρες με τη μορφή βοήθειας (Heeks, 2002). Όσον αφορά τις πολιτιστικές συμπεριφορές, είναι η γενική συναίνεση στις αναπτυσσόμενες χώρες ότι τα προϊόντα που εισάγονται είναι ανώτερης ποιότητας (Heeks, 2002), επομένως από προεπιλογή, τα συστήματα πληροφοριών υγείας από τις βιομηχανικές χώρες θεωρούνται γενικά καλύτερα από αυτά που παράγονται τοπικά.

1.4 Επιτυχής Υλοποίηση των Πληροφοριακών Συστημάτων Υγείας

Σύμφωνα με τους Sligo et al. (2017), για την επιτυχή εφαρμογή ενός πληροφοριακού συστήματος υγείας, πρέπει να ξεκινήσει κανείς με σχεδιασμό, σχεδιασμό και πιλοτική εφαρμογή. Αυτό θα πρέπει να ακολουθείται από τη διακοπτόμενη χρήση του νέου συστήματος, την τροποποίηση, την αποδοχή ή την απόρριψη. Εάν γίνει αποδεκτό, τότε η χρήση του συστήματος συνεχίζεται μέχρι να γίνει μέρος των καθημερινών εργασιακών διαδικασιών του ιδρύματος, σε σημείο που να θεωρείται ρουτίνα.

Η επιτυχία γίνεται ένα επίπονο έργο όσο μεγαλύτερο είναι το εύρος της εφαρμογής των πληροφοριακών συστημάτων. Δεδομένου ότι ένας από τους στόχους των πληροφοριακών συστημάτων είναι να βελτιώσουν την οργανωτική λειτουργία μέσω αλλαγής και υποστήριξης, όσο μεγαλύτερος είναι ο βαθμός αλλαγής που εισάγει ένα πληροφοριακό σύστημα, τόσο πιο πιθανό είναι ότι θα υπάρξουν μεγάλες βελτιώσεις στη λειτουργία του οργανισμού.

Ωστόσο, αυτό μπορεί να διατρέχει τον κίνδυνο αποτυχίας της υλοποίησης των πληροφοριακών συστημάτων υγείας, λόγω του μεγέθους της αλλαγής που απαιτείται (Heeks, 2002, Sligo et al., 2017). Για την επιτυχή εφαρμογή συστημάτων πληροφοριών

υγείας, οι Sligo et al., (2017) ομαδοποιούν πιθανούς παράγοντες από τη διαθέσιμη βιβλιογραφία για το θέμα σε τρεις βασικούς τίτλους. δομικές / οργανωτικές, ανθρώπινες και τεχνικές. Δίνεται έμφαση στη διασύνδεση μεταξύ των τεχνικών και κοινωνικών (οργανωτικών και ανθρώπινων) πτυχών της εφαρμογής συστημάτων πληροφοριών υγείας (Evans et al., 2014, Sligo et al., 2017).

Οι δομικοί παράγοντες αφορούν τα πράγματα που απαιτούνται πριν και κατά την εφαρμογή των πληροφοριακών συστημάτων υγείας, όπως η παροχή πόρων (χρήματα και προσωπικό), σαφώς διατυπωμένοι στόχοι και προτεραιότητες, και καλές σχέσεις και επικοινωνία μεταξύ και μεταξύ της διοίκησης και του προσωπικού, για να αναφέρουμε μόνο μερικά. Όσον αφορά τους ανθρώπινους παράγοντες, χαρακτηριστικά όπως το προσωπικό με κάποια προηγούμενη εμπειρία τεχνολογίας, η αντίληψη της χρήσης της τεχνολογίας ως υποχρεωτική, εύκολη στη χρήση, κατανοητή και καλύτερη από τις προηγούμενες διαδικασίες εργασίας που είχαν, ήταν απαραίτητα για την επιτυχή εφαρμογή των πληροφοριακών συστημάτων υγείας.

Το προσωπικό πρέπει να εκπαιδευτεί επαρκώς και να του δοθεί επαρκής χρόνος για να εξοικειωθεί με τη νέα τεχνολογία, ώστε να την αποδεχτεί και να τη λειτουργήσει με μέγιστο όφελος. Υπάρχει επίσης η ανάγκη για «πρωταθλητές έργων», όπου αυτοί είναι ανώτεροι ηγέτες που λειτουργούν ως σύνδεσμοι μεταξύ της διοίκησης, του προσωπικού τεχνολογίας και άλλων μελών του προσωπικού για να διασφαλίσουν μια συνεχή ροή πληροφοριών για τη βελτίωση της διαδικασίας υλοποίησης.

Χαρακτηριστικά της τεχνικής φύσης που προωθούν την επιτυχή εφαρμογή των πληροφοριακών συστημάτων υγείας, περιλαμβάνουν την ικανότητα ενσωμάτωσης της νέας τεχνολογίας σε υπάρχοντα συστήματα και διαδικασίες εργασίας, το νέο πληροφοριακό σύστημα θα πρέπει να είναι φιλικό προς τον χρήστη. Δηλαδή, θα πρέπει να είναι εύκολο να κατανοηθεί και να λειτουργήσει, η πλοήγηση και οι εργασίες του συστήματος θα πρέπει να θυμούνται εύκολα και θα πρέπει να προσαρμόζονται εύκολα με μια ποιοτική διεπαφή σχεδιασμού που απαιτεί λίγη εκπαίδευση για τη χρήση του (Evans et al., 2014, Sligo et al. al., 2017).

Υπάρχει ωστόσο μικρή εμπειρία στη δημιουργία συστημάτων πληροφοριών υγείας, ιδιαίτερα συστημάτων ηλεκτρονικού ιατρικού φακέλου (EMR) για τις αναπτυσσόμενες

χώρες. Η ανάγκη αναφοράς συγκεντρωτικών στατιστικών για την κυβέρνηση ή τους οργανισμούς χρηματοδότησης ήταν ο στόχος για την ανάπτυξη και την εφαρμογή συστημάτων πληροφοριών υγειονομικής περίθαλψης στις περισσότερες αναπτυσσόμενες χώρες (Tomasi et al., 2004, Fraser et al., 2005).

Επιπλέον, υπάρχουν προκλήσεις και ζητήματα στην εφαρμογή ακόμη και όταν ο σχεδιασμός του συστήματος πληροφοριών υγείας βρίσκεται σε τοπικό (από σχεδιαστές σε αναπτυσσόμενες χώρες). Ένα κοινό ζήτημα εφαρμογής της πληροφορικής υγείας είναι η εστίαση στη λειτουργικότητα της νέας τεχνολογίας στο ευρύτερο οργανωτικό και διοικητικό πλαίσιο αντί στην κλινική πρακτική (Wagner-Menghin και Pokieser, 2016). Έτσι, η αλληλεπίδραση των εργαζομένων στον τομέα της υγείας με το HIS μπορεί να περιορίζεται στην εισαγωγή πληροφοριών στο σύστημα χωρίς να συνειδητοποιούν τα πλήρη πλεονεκτήματά του και ως εκ τούτου, δημιουργώντας μια αίσθηση παραμέλησης και δυσαρέσκειας στην εργασία (Nilsson, Eriksén and Borg, 2014). Μια ισχυρή πληροφοριακή υποδομή πριν από την εφαρμογή συστημάτων πληροφοριών υγείας παίζει καθοριστικό ρόλο στην επιτυχία της.

1.5 Κυβερνοεπιθέσεις σε Οργανισμούς Υγείας

Αποτελεί γεγονός πως η τεχνολογική καινοτομία είναι η κινητήρια δύναμη πίσω από την όποια προσφερόμενη βελτιωμένη υγειονομική περίθαλψη και την έκβαση της υγείας των ασθενών. Τα συστήματα πληροφοριών υγείας έχουν προσφέρει πολλά οφέλη για τους ασθενείς, τους παρόχους υγειονομικής περίθαλψης και άλλους ενδιαφερόμενους φορείς, ενώ συμβάλλουν στη διαχείριση του αυξανόμενου κόστους της υγειονομικής περίθαλψης.

Τα ηλεκτρονικά αρχεία υγείας επίσης, έχουν αυξήσει τη συνέχεια και την ασφάλεια της περίθαλψης των ασθενών, παρέχοντας κρίσιμες πληροφορίες. Οι ιατρικές συσκευές με δυνατότητα χρήσης Διαδικτύου και άλλα αυτοματοποιημένα συστήματα, έχουν επίσης πολλαπλασιάσει τον κλάδο της υγειονομικής περίθαλψης. Αν και αυτές οι εξελίξεις ήταν ευεργετήματα για την κοινωνία και τον τομέα της υγειονομικής περίθαλψης, συνοδεύονται από νέα είδη κινδύνων (Luna et al. 2015).

Οι κίνδυνοι στον κυβερνοχώρο, προκύπτουν από τη χρήση της πληροφορικής και

μπορούν να υπονομεύσουν την ακεραιότητα, τη διαθεσιμότητα ή το απόρρητο των υπηρεσιών ή των δεδομένων (Eling & Schnell 2016). Διάφορα είδη κινδύνων στον κυβερνοχώρο που αφορούν τον κλάδο της υγειονομικής περίθαλψης, έχουν σπάσει το εμπόδιο των πληροφοριών στην πρόσφατη ιστορία, λαμβάνοντας σημαντική δημοσιότητα και προσοχή. Δύο παραδείγματα από το καλοκαίρι του 2017, περιλαμβάνουν την επίθεση ransomware WannaCry που διέκοψε το NHS στο Ηνωμένο Βασίλειο, (BBC, 2017) και μια ανάκληση σχεδόν 500.000 βηματοδοτών από την FDA λόγω ευπάθειας κατά της πειρατείας στις Ηνωμένες Πολιτείες (FDA, 2017). Τα γεγονότα στον κυβερνοχώρο έχουν επίσης προκαλέσει προβλήματα μεταξύ των οργανισμών υγειονομικής περίθαλψης.

Τα γεγονότα που συμβαίνουν στον κυβερνοχώρο, όπου πλήττουν τους οργανισμούς υγειονομικής περίθαλψης, έχουν γίνει ολοένα και πιο κοινό φαινόμενο. Έρευνα για επιθέσεις στον κυβερνοχώρο στον κλάδο της υγειονομικής περίθαλψης δείχνει ότι πάνω από το 90% των παρόχων υγειονομικής περίθαλψης έχουν πέσει θύματα κυβερνοεπίθεσης. (Luna et al. 2016) Αρκετά κοινά χαρακτηριστικά των οργανισμών υγειονομικής περίθαλψης, συμπεριλαμβανομένων των αυστηρών οικονομικών περιορισμών και της ασθενέστερης υποδομής ασφάλειας στον κυβερνοχώρο, τους έχουν καταστήσει ιδιαίτερα ευάλωτους σε κινδύνους στον κυβερνοχώρο.

Οι κυβερνοεπιθέσεις στον τομέα της υγειονομικής περίθαλψης, οφείλονται σε ποικίλα κίνητρα, πολλά από τα οποία συνεπάγονται οικονομικό κέρδος με τον ένα ή τον άλλο τρόπο. (HCIC, 2017). Η κλοπή ιατρικών πληροφοριών έχει γίνει μια επικερδής επιχείρηση και ως εκ τούτου γίνεται ολοένα και πιο κοινή. Τα ιατρικά αρχεία αξίζουν περισσότερο από άλλα είδη πληροφοριών που παραδοσιακά στοχοποιούνται για κλοπή, όπως οι αριθμοί κοινωνικής ασφάλισης (Luna et al., 2016).

Οι κίνδυνοι στον κυβερνοχώρο μπορούν να οδηγήσουν σε ένα ευρύ φάσμα δυσμενών αποτελεσμάτων για όλα τα μέρη που εμπλέκονται στον τομέα της υγειονομικής περίθαλψης. Αυτά περιλαμβάνουν βλάβη σε ασθενείς, εκτός από οικονομικές απώλειες και πλήγμα στη φήμη των παρόχων υγειονομικής περίθαλψης. Αρκετές δικαιοδοσίες, συμπεριλαμβανομένης της Ε.Ε., έχουν εφαρμόσει κανονισμούς που αναγκάζουν τους παρόχους υγειονομικής περίθαλψης να εξετάσουν τους αυξανόμενους κινδύνους που συνδέονται με την ασφάλεια των πληροφοριών και το απόρρητο. Καθώς οι κυρώσεις για τη μη συμμόρφωση μπορεί να είναι σημαντικές, η

αποτελεσματική διαχείριση του κινδύνου στον κυβερνοχώρο έχει γίνει μια αυξανόμενη ανησυχία (Blanke & McGrady 2016).

Ως απάντηση στην αυξανόμενη σημασία των κινδύνων στον κυβερνοχώρο, έχουν χρησιμοποιηθεί νέες τεχνικές για τη διαχείρισή τους. Η αποτελεσματική διαχείριση κινδύνων στον κυβερνοχώρο έχει πολλά στοιχεία, συμπεριλαμβανομένης της ασφάλειας στον κυβερνοχώρο, της εκπαίδευσης των εργαζομένων και της ασφάλισης. Ενώ η διαχείριση κινδύνων θα είναι σε αντίθεση με την εντελώς αποτελεσματική, μπορεί να μειώσει την πιθανότητα και την έκβαση των κινδύνων στον κυβερνοχώρο. (Martin et al. 2017).

ΚΕΦΑΛΑΙΟ 2^{Ο} – Κίνδυνοι στο Τομέα της Υγειονομικής Περίθαλψης και των Πληροφοριακών Συστημάτων στον Κυβερνοχώρο Καθώς και Πλάνο Διαχείρισης Κρίσεων

2.1 Κίνδυνοι που Αναφέρονται στον Κυβερνοχώρο και Ειδικότερα στην Υγειονομική Περίθαλψη

Οι κίνδυνοι διαφόρων ειδών στον κυβερνοχώρο, έχουν αυξηθεί στον τομέα της υγειονομικής περίθαλψης τα τελευταία χρόνια. Μια σταθερή αύξηση σε αυτά τα συμβάντα, έχει αναφερθεί από ακαδημαϊκές πηγές καθώς και από ρυθμιστικούς φορείς. Το 2016, θεωρείται η χειρότερη χρονιά που έχει καταγραφεί για συμβάντα στον κυβερνοχώρο στον τομέα της υγειονομικής περίθαλψης όσον αφορά τις καταγεγραμμένες παραβιάσεις (HIPAA ,2017, Rubenfire, 2017)

Έχει αναφερθεί επίσης, ότι η απώλεια των ιατρικών πληροφοριών, ειδικότερα, θα συνεχίσει να αυξάνεται λόγω των οικονομικών της κινήτρων. Οι δύο πιο συνηθισμένοι λόγοι πίσω από τις σκόπιμες επιθέσεις στον κυβερνοχώρο, περιλαμβάνουν το οικονομικό κέρδος και τους δυσαρεστημένους εργαζόμενους. Οι ιατρικές πληροφορίες που λαμβάνονται παράνομα από τρίτα μέρη, μπορούν να πωληθούν, να χρησιμοποιηθούν για απάτη ταυτότητας, παράνομη ιατρική πρακτική ή ασφαλιστική απάτη. (Luna et al., 2016)

Οι πληροφορίες που διαχειρίζονται από οργανισμούς υγειονομικής περίθαλψης, μπορούν επίσης να χρησιμοποιηθούν για την πρόσβαση στα οικονομικά και τιμολογιακά δεδομένα των ασθενών ή για την παράνομη λήψη συνταγογραφούμενων φαρμάκων (World Medical Association, 2016). Έχουν επίσης καταγραφεί κυβερνοεπιθέσεις με πολιτικά ή ιδεολογικά κίνητρα (Lehto & Lehto, 2017). Άλλα πιθανά κίνητρα περιλαμβάνουν διακοπή της περίθαλψης ασθενών ή νοσοκομειακών συστημάτων, χειραγώγηση αποθεμάτων και παρεμβολές στην εφοδιαστική αλυσίδα (HCIC Task Force, 2017).

Οι επιθέσεις στον κυβερνοχώρο μπορεί να είναι μη στοχευμένες, αντί να σχεδιάζονται για κάποιο συγκεκριμένο θύμα. Αυτοί οι τύποι μη στοχευμένων επιθέσεων, θα έχουν αναπόφευκτο αντίκτυπο και στους οργανισμούς υγειονομικής περίθαλψης. Υπήρξε επίσης αύξηση στον αριθμό των στοχευμένων επιθέσεων ειδικά για παρόχους υγειονομικής περίθαλψης.

Οι Luna et al. (2016) αναφέρουν επίσης ότι αυτά τα γεγονότα μπορεί να είναι σκόπιμα και στρατηγικά σχεδιασμένα. Ο τραπεζικός και χρηματοοικονομικός τομέας ήταν παραδοσιακά στόχος επιθέσεων στον κυβερνοχώρο και οι κίνδυνοι στον κυβερνοχώρο εξακολουθούν να αποτελούν σημαντικό ζήτημα σε αυτόν τον τομέα. Σύμφωνα με τους Lehto και Lehto, (2017) υπήρξε μια αυξανόμενη στροφή προς τον τομέα της υγειονομικής περίθαλψης λόγω των τρωτών σημείων του και των δυνητικά υψηλότερων κερδών.

Μια έκθεση από τον οργανισμό Ponemon (2016a), αναφέρει ότι σχεδόν το 90% των παρόχων υγειονομικής περίθαλψης που συμμετείχαν στην έρευνα, είχαν αντιμετωπίσει παραβίαση δεδομένων τα τελευταία δύο χρόνια και οι μισοί από αυτούς τους οργανισμούς είχαν περισσότερες από πέντε παραβιάσεις κατά τη συγκεκριμένη χρονική περίοδο. Μια άλλη μελέτη διαπίστωσε ότι το 94% των παρόχων υγειονομικής περίθαλψης είχαν πέσει θύματα κυβερνοεπίθεσης (Luna et al. 2016). Μια μελέτη των Lehto και Lehto (2017) ανέλυσε 59 επιθέσεις στον κυβερνοχώρο στον τομέα της υγειονομικής περίθαλψης παγκοσμίως κατά τα έτη 2013-2017. Πολλές από τις περιπτώσεις στη μελέτη τους αφορούσαν προσωπικά στοιχεία εκατομμυρίων ατόμων, με μία περίπτωση να ανέρχεται συνολικά σε 80 εκατομμύρια άτομα.

Η επίθεση κακόβουλου λογισμικού WannaCry την άνοιξη του 2017, έγινε διεθνής πρωτοσέλιδο καθώς διέκοψε από την λειτουργία τους, εκατοντάδες χιλιάδες υπολογιστές

σε 150 χώρες, συμπεριλαμβανομένων 61 οργανισμών NHS στο Ηνωμένο Βασίλειο (BBC, 2017). Αυτή η επίθεση δεν στρεφόταν στον τομέα της υγειονομικής περίθαλψης, αλλά έθεσε σε κίνδυνο την ασφάλεια των ασθενών και επηρέασε την παροχή φροντίδας. Άλλες επιθέσεις έχουν ενορχηστρωθεί ειδικά για οργανισμούς υγειονομικής περίθαλψης.

Το 2016, ένα νοσοκομείο στο Λος Άντζελες της Καλιφόρνια, εμποδίστηκε να αποκτήσει πρόσβαση σε ιατρικούς φακέλους ή να χρησιμοποιήσει ιατρικό εξοπλισμό έως ότου καταβληθούν λύτρα. Την ίδια χρονιά, ένα νοσοκομείο στην Αγγλία χρειάστηκε να μεταφέρει ασθενείς και να ακυρώσει τις επεμβάσεις λόγω ransomware. (Martin et al. 2017) Ένα άλλο σχέδιο περιελάμβανε το χακάρισμα μιας κλινικής πλαστικής χειρουργικής και τον εκβιασμό ασθενών διασημοτήτων με γυμνές φωτογραφίες (Lehto & Lehto 2017).

Τα προηγούμενα παραδείγματα οφείλονται σε οικονομικό κίνητρο, αλλά έχουν αναφερθεί και άλλα. Το 2016, η Υπηρεσία Αίματος του Αυστραλιανού Ερυθρού Σταυρού είχε «πέσει» θύμα υποκλοπών, πάνω από 1,28 εκατομμύρια αρχεία δεδομένων δωρητών. Οι πληροφορίες, πολλές από τις οποίες αφορούσαν επικίνδυνες συμπεριφορές δωρητών, δημοσιεύτηκαν σε δημόσιο ιστότοπο για να τονιστεί η ασθενής ασφάλεια. Άλλα παραδείγματα που έχουν δημοσιοποιηθεί έχουν ωθηθεί από πολιτικούς ή προπαγανδιστικούς σκοπούς, όπως η επίθεση του Ισλαμικού Κράτους στο NHS (Martin, et al. 2017).

Στις Ηνωμένες Πολιτείες για παράδειγμα, το Κογκρέσο ίδρυσε την Ειδική Ομάδα Ασφάλειας στον Κυβερνοχώρο της Βιομηχανίας Υγείας (HCIC) με τον Νόμο για την Ασφάλεια στον Κυβερνοχώρο του 2015. Το κίνητρο πίσω από αυτή τη νέα ομάδα εργασίας, είναι να αντιμετωπίσει τις αυξανόμενες απειλές στον κυβερνοχώρο που πρέπει να αντιμετωπίσει ο τομέας της υγειονομικής περίθαλψης.

Ενώ οι κίνδυνοι στον κυβερνοχώρο μπορεί να οδηγήσουν σε μεγάλη ποικιλία αρνητικών αποτελεσμάτων, συμπεριλαμβανομένης της κλοπής ταυτότητας και της απάτης, το πιο σημαντικό από αυτά σύμφωνα με την Ομάδα Εργασίας του HCIC είναι η διακοπή της φροντίδας των ασθενών. (HCIC Task Force, 2017). Η Ευρωπαϊκή Ρυθμιστική Αρχή Επικοινωνιών δημοσίευσε επίσης έναν οδηγό για την ασφάλεια στον κυβερνοχώρο στον τομέα της υγειονομικής περίθαλψης. Αυτή η έκθεση έχει σκοπό να ξεκινήσει έναν διάλογο για τους κυβερνοκινδύνους στη διαχείριση της υγειονομικής περίθαλψης και να τονίσει τη σημασία αυτών των κινδύνων στην υγειονομική περίθαλψη

(Viestintävirasto, 2016).

2.1.1 Εξοπλισμός της Υγειονομικής Περίθαλψης και τα Συστήματα Πληροφοριών

Τις τελευταίες δεκαετίες σημειώθηκαν πρόοδοι σε πολλά μέτωπα, οι οποίες αξιοποιήθηκαν για βελτιωμένη υγειονομική περίθαλψη και ιατρικό αποτέλεσμα για μια ποικιλία ασθενειών. Για παράδειγμα, το ταχέως μειούμενο ποσοστό θνησιμότητας από εγκεφαλικά επεισόδια οδήγησε σε βελτίωση της υγείας του πληθυσμού και έχει προκηρυχθεί ως ένα από τα δέκα κορυφαία επιτεύγματα δημόσιας υγείας. Αν και οι ακριβείς λόγοι δεν είναι σαφώς γνωστοί, αποδίδονται γενικά σε βελτιώσεις στους ακόλουθους τομείς: καλύτερη παρέμβαση για τον διαβήτη και την υπέρταση, μειωμένο κάπνισμα, καλύτεροι φαρμακολογικοί παράγοντες και τεχνολογικές εξελίξεις στα συστήματα φροντίδας και θεραπείας.

Η βελτιωμένη οργάνωση της παροχής φροντίδας από εγκεφαλικό επεισόδιο, μπορεί να είχε τη μεγαλύτερη επίδραση στη μείωση της θνησιμότητας από εγκεφαλικά επεισόδια (Lackland et al., 2014). Το λεγόμενο χρυσό πρότυπο της θεραπείας του εγκεφαλικού είναι η έγκαιρη χορήγηση φαρμάκων που διαλύουν θρόμβους. Στο Πανεπιστημιακό Νοσοκομείο του Τάμπερε, η έναρξη αυτής της θεραπείας διαρκεί κατά μέσο όρο 20 λεπτά και τέσσερις στους πέντε ασθενείς που λαμβάνουν θεραπεία θα επιστρέψουν σε μια ανεξάρτητη ζωή.

Τα συστήματα πληροφοριών υγείας έχουν αποφέρει σημαντικά οφέλη για τη βελτίωση της ποιότητας της περίθαλψης και της αποδοτικότητας του κόστους. Τα ηλεκτρονικά αρχεία υγείας (EHR) έχουν βοηθήσει στη διαχείριση χρόνιων παθήσεων και στην εντατική φροντίδα. Στην ιδανική περίπτωση, ένα σύστημα EHR θα περιέχει όλες τις πληροφορίες σχετικά με την υγεία ενός ατόμου κατά τη διάρκεια ολόκληρης της ζωής του. Αυτό περιλαμβάνει φάρμακα, εργαστηριακά αποτελέσματα, εικόνες, διάγνωση και μια πληθώρα άλλων προσωπικών πληροφοριών.

Η δημοτικότητα των εφαρμογών για κινητές συσκευές που σχετίζονται με την υγεία καθώς και των ιατρικών συσκευών αυξάνεται, πράγμα που σημαίνει ότι υπάρχουν περισσότερα πιθανά σημεία για αποτυχία ή είσοδο σε συστήματα που περιέχουν πληροφορίες υγείας. Οι κίνδυνοι στον κυβερνοχώρο διαφόρων ειδών μπορούν να εμποδίσουν την ασφάλεια των πληροφοριών και το απόρρητο των συστημάτων

πληροφοριών υγείας (Luna et al., 2016).

Οι Luna et al. (2016) εκτιμούν ότι περίπου το 95 % των επιλέξιμων νοσοκομείων χρησιμοποιούν EHR και άλλες τεχνολογίες πληροφοριών υγείας. Στη Φινλανδία για παράδειγμα, όλοι οι πάροχοι υγειονομικής περίθαλψης του δημόσιου τομέα και σχεδόν όλοι οι ιδιωτικοί οργανισμοί υγειονομικής περίθαλψης έχουν υιοθετήσει ηλεκτρονικά αρχεία υγείας. Η επικράτηση αυτού του τύπου τεχνολογίας είναι υψηλότερη στη Φινλανδία από ό,τι στα περισσότερα άλλα μέρη του κόσμου.

Εκτός από τα συστήματα πληροφοριών υγείας που χρησιμοποιούνται από τους παρόχους υγειονομικής περίθαλψης για την τήρηση αρχείων και την επικοινωνία μεταξύ τους, ο ρόλος του ασθενούς ως ενεργού συμμετέχοντος είναι μια αυξανόμενη τάση. Οι ασθενείς μπορούν να βλέπουν τις πληροφορίες τους, όπως στο Αποθετήριο Δεδομένων Ασθενούς και σε ορισμένες περιπτώσεις να ανεβάζουν τα δικά τους ιατρικά δεδομένα, όπως μετρήσεις αρτηριακής πίεσης στο σπίτι (Lääkäriliitto, 2016).

Τα EHR αντιπροσωπεύουν περίπου το 10% των πληροφοριακών συστημάτων ενός νοσοκομείου και αυτά συχνά θεωρούνται ως τα πιο κρίσιμα. Οι επιμέρους ειδικότητες και τμήματα, όπως η ιατρική απεικόνιση ή η αναισθησία, έχουν επίσης τα δικά τους συστήματα. Ένας πάροχος υγειονομικής περίθαλψης θα χρειαστεί επίσης εφαρμογές για διοικητικές εργασίες, τιμολόγηση, ανθρώπινους πόρους, επικοινωνίες, λογισμικό παραγωγικότητας και ασφάλεια, μεταξύ άλλων εργασιών. Ανάλογα με τον εν λόγω οργανισμό, αυτά μπορούν να προσθέσουν έως και 400-800 συστήματα συνολικά, με 500 συνδέσεις μεταξύ τους (Lehto & Lehto, 2017).

Ένα σύγχρονο νοσοκομείο βασίζεται σε μεγάλο βαθμό σε μια ποικιλία υποδομών και ιατρικών συσκευών που συνδέονται ολοένα και περισσότερο και διαθέτουν πρόσβαση στο διαδίκτυο. Αυτές περιλαμβάνουν αντλίες έγχυσης που χορηγούν φάρμακα, βηματοδότες και μηχανήματα αναισθησίας. Αυτές οι συσκευές διευκολύνουν την ομαλή και πιο αυτοματοποιημένη φροντίδα.

Μια ενημέρωση των πληροφοριών δοσολογίας φαρμάκου ενός ασθενούς στο EHR, μπορεί να προσαρμοστεί αυτόματα στην αντλία έγχυσης. Ένας ασθενής μπορεί να συνδεθεί με πολλές συσκευές και οθόνες ταυτόχρονα. Η ανάπτυξη αυτών των συνδεδεμένων ιατρικών συσκευών ήταν πολύ θετική για τη φροντίδα των ασθενών και ο επιπολασμός τους προβλέπεται να αυξηθεί σημαντικά στο μέλλον με νέες τεχνικές

προόδους. Οι ιατρικές συσκευές μπορούν να θεωρηθούν ως η πιο σημαντική πηγή κινδύνου στον κυβερνοχώρο στην υγειονομική περίθαλψη (Lehto & Lehto 2017).

Οι Luna et al. (2016) επισημαίνουν επίσης ότι οι ιατροτεχνολογικές συσκευές συμβάλλουν σε μεγάλο βαθμό σε παραβιάσεις δεδομένων υγειονομικής περίθαλψης. Έχουν εντοπιστεί εκατοντάδες κακόβουλες προσπάθειες, όπως ransomware σε εξοπλισμό ακτινολογίας. Αυτά τα έχουν προκαλέσει σημαντικό κόστος και αναστάτωση για τους παρόχους υγειονομικής περίθαλψης και τους ασθενείς. Ευτυχώς οι ασθενείς δεν έχουν τραυματιστεί. (Fox-Brewster 2017, Perakslis, 2014).

Οι ιατρικές συσκευές ενέχουν κινδύνους για την ασφάλεια των πληροφοριών και το απόρρητο, αλλά το πιο σημαντικό είναι ότι μπορούν να προκαλέσουν σωματικές επιπτώσεις, όπως τραυματισμό, ασθένεια ή θάνατο στον χρήστη τους. Τα χαρακτηριστικά ασφαλείας πρέπει να λαμβάνονται υπόψη κατά το σχεδιασμό και την κατασκευή αυτών των συσκευών, αλλά αυτό μπορεί να είναι δύσκολο λόγω της γρήγορης εξέλιξης εντός της τεχνολογίας (HCIC Task Force 2017).

Τα χαρακτηριστικά ασφαλείας των ιατρικών συσκευών, παραδοσιακά δεν ήταν στην πρώτη γραμμή κατά την ανάπτυξη και την απόκτησή τους (Lehto & Lehto 2017). Οι λεγόμενες συσκευές παλαιού τύπου αναφέρονται σε παλαιότερα κομμάτια εξοπλισμού. Αυτά τα μηχανήματα συγκεκριμένα δεν έχουν σχεδιαστεί με γνώμονα τα σύγχρονα ζητήματα ασφάλειας στον κυβερνοχώρο και σε πολλές περιπτώσεις δεν υποστηρίζονται πλέον με ενημερώσεις λογισμικού και είναι δύσκολο να αντικατασταθούν. Οι πάροχοι υγειονομικής περίθαλψης μπορούν επίσης να διαθέτουν πολύ σύγχρονα πληροφοριακά συστήματα και εξοπλισμό, με αποτέλεσμα μια περίπλοκη τεχνική υποδομή (Επιχείρηση HCIC 2017).

Αναπτύσσονται νέοι τύποι ιατροτεχνολογικών προϊόντων που χρησιμοποιούνται εκτός νοσοκομειακού περιβάλλοντος. Αν και αυτό είναι επωφελές για τους ασθενείς και τους παρόχους υγειονομικής περίθαλψής τους, σημαίνει ότι θα απαιτούνται ειδικές προφυλάξεις σχετικά με τη λειτουργία και την ασφάλεια των συσκευών και των δικτύων (Lehto & Lehto 2017). Μια αντλία ινσουλίνης μπορεί να συνδεθεί σε μια συσκευή παρακολούθησης γλυκόζης αίματος, η οποία μπορεί να παρακολουθηθεί στο αρχείο σακχάρου αίματος του ασθενούς. Αυτό είναι πολύ βολικό για τον ασθενή και ωφέλιμο και από κλινική άποψη. Η συνδεσιμότητα αυτών των εξαρτημάτων πρέπει να είναι αξιόπιστη, διαφορετικά μπορεί να βλάψει τους ασθενείς. Οδηγεί επίσης σε υψηλότερο

ποσοστό εξάρτησης από αυτήν την τεχνολογία. (Επιχείρηση HCIC, 2017).

Η χρήση κινητών συσκευών στην υγειονομική περίθαλψη βρίσκεται επίσης σε άνοδο. Οι φορητές συσκευές είναι πολύ βολικές και προσφέρουν πολλά οφέλη στους χρήστες τους. Αυτά τα πλεονεκτήματα είναι, ωστόσο, προβληματικά από την άποψη του κινδύνου. Οι φορητές συσκευές χάνονται ή κλέβονται εύκολα και μπορούν να χρησιμοποιηθούν σε ακατάλληλη τοποθεσία. Τα χαρακτηριστικά ασφαλείας τους δεν είναι τόσο πλήρως ανεπτυγμένα όσο τα παραδοσιακά αντίστοιχα. (Lehto & Lehto 2017)

2.2 Ευπάθειες στον Κυβερνοχώρο της Υγειονομικής Περίθαλψης

Ο πρωταρχικός στόχος του τομέα της υγειονομικής περίθαλψης και των παρόχων αυτής, αναφέρεται ως ιδιαίτερα επικεντρωμένος στον ασθενή. Οι πόροι συνήθως κατανέμονται με τρόπο που καθιστά δυνατή την παροχή βοήθειας στους περισσότερους ασθενείς. Ενώ οι πάροχοι υγειονομικής περίθαλψης έχουν άλλους στόχους, συμπεριλαμβανομένων των ζητημάτων ασφάλειας, συχνά μπορεί να δοθεί λιγότερη προτεραιότητα σε αυτούς στις καθημερινές λειτουργίες της εγκατάστασης. Οι προφυλάξεις που είναι απαραίτητες για τη διασφάλιση της ασφάλειας στον κυβερνοχώρο μπορούν να ερμηνευθούν ως εμπόδιο. Για παράδειγμα, οι σταθμοί εργασίας μπορούν να παραμείνουν ξεκλείδωτοι για να ανταποκρίνονται σε κλινικά ζητήματα όσο το δυνατόν γρηγορότερα.

Η πληκτρολόγηση ενός κωδικού πρόσβασης και η αναμονή για σύνδεση, μπορεί να διαρκέσει μερικά λεπτά, γεγονός που μπορεί να καθυστερήσει τον πρωταρχικό στόχο της φροντίδας των ασθενών. Οι χωρίς ασφάλεια σταθμοί εργασίας μπορούν να εξοικονομήσουν χρόνο, αλλά μπορεί επίσης να οδηγήσουν σε μη εξουσιοδοτημένη πρόσβαση ή αλλαγή πληροφοριών (HCIC, 2017).

Πολλοί πάροχοι υγειονομικής περίθαλψης είναι επίσης δημόσιοι φορείς. Πολλά από αυτά τα ιατρεία είναι ανοιχτά όλη την ημέρα, καθημερινά και υπάρχουν ελάχιστοι, αν υπάρχουν, περιορισμοί στο ποιος επιτρέπεται να εισέλθει. Ακόμη και για το προσωπικό, δεν είναι πάντα δυνατό να πούμε αν κάποιος δεν πρέπει να είναι εκεί. Το ίδιο το προσωπικό του νοσοκομείου αλλάζει επίσης σε αρκετά γρήγορη βάση. Το έκτακτο προσωπικό και οι εκ περιτροπής βάρδιες είναι επίσης συνηθισμένες (HCIC, 2017).

Οι οργανισμοί υγειονομικής περίθαλψης τείνουν επίσης να δαπανούν λιγότερους

πόρους για την ασφάλεια στον κυβερνοχώρο σε σύγκριση με άλλους τομείς. Σε άλλους τομείς, 5-15% πόροι πληροφορικής δαπανώνται για την ασφάλεια, ενώ το ποσοστό είναι 3% στην υγειονομική περίθαλψη (Lehto & Lehto 2017). Οι οργανισμοί υγειονομικής περίθαλψης έχουν βρεθεί ότι υστερούν σε σχέση με άλλους τομείς και σε άλλες πτυχές. Η ξεπερασμένη τεχνολογία και η έλλειψη διαδικασιών ασφάλειας πληροφοριών έχει βρεθεί ότι κυριαρχούν περισσότερο στην υγειονομική περίθαλψη (KPMG, 2015). Πολλά νοσοκομεία πρέπει επίσης να λειτουργούν υπό αυστηρούς δημοσιονομικούς περιορισμούς. Οι οικονομικοί λόγοι είναι επίσης ένας βασικός λόγος για τον μεγάλο αριθμό παλαιών συσκευών που χρησιμοποιούνται επί του παρόντος από την υγειονομική περίθαλψη με παρόχους, καθώς δεν είναι εφικτή η αντικατάσταση ακριβού εξοπλισμού λόγω ενημερωμένων λειτουργικών συστημάτων (HCIC, 2017).

Τείνει δε να υπάρχει μια υπόθεση ασφάλειας στον κυβερνοχώρο μεταξύ των παρόχων υγειονομικής περίθαλψης και των εργαζομένων (HCIC Task Force, 2017). Μια μελέτη που έγινε από το Sans Institute (2014) διαπίστωσε επίσης ότι φαίνεται να υπάρχει ένα χάσμα μεταξύ της αντιληπτής ασφάλειας και της πραγματικότητας, κάτι που υποδεικνύεται από υψηλό επίπεδο παραβιάσεων ασφάλειας. Οι οργανισμοί υγειονομικής περίθαλψης πρέπει να λάβουν ορισμένα μέτρα για να διασφαλίσουν τη συμμόρφωση, αλλά αυτό δεν σημαίνει απαραίτητα το ίδιο πράγμα με την ασφάλεια. Μια άλλη μελέτη του Sans Institute (2013) διαπίστωσε ότι η συμμόρφωση με τους κανονισμούς ήταν ο πιο σημαντικός μοχλός για την ασφάλεια στον τομέα της υγειονομικής περίθαλψης. Σε μια έκθεση της KPMG (2015) βρέθηκε επίσης ότι τα ρυθμιστικά ζητήματα αποτελούν το κύριο μέλημα για την ασφάλεια στον κυβερνοχώρο για τους παρόχους υγειονομικής περίθαλψης. Η χρήση των προτύπων που ορίζονται από το ρυθμιστικό πλαίσιο δεν επιτρέπεται είναι επαρκής για τη διατήρηση της ασφάλειας (Sans Institute, 2014).

2.3 Οι Κυβερνοεπιθέσεις στα Συστήματα Υγείας στην Ευρώπη και Σχετικές Επιπτώσεις

Αποτελεί γεγονός στις μέρες μας πως το ποσοστό των ηλικιωμένων στην Ευρώπη, αυξάνεται λόγω του χαμηλού αριθμού γεννήσεων και της αύξησης του προσδόκιμου ζωής (Barnett, et al., 2013). Σύμφωνα με την έκθεση «*Health redesign in Europe for 2020*», το κόστος της υγειονομικής περίθαλψης στην Ευρώπη, αυτή τη στιγμή, αυξάνεται συνεχώς.

Αυτά τα κόστη σε ορισμένες ευρωπαϊκές χώρες αποτελούν παράγοντες ανάπτυξης του ΑΕΠ και σε ορισμένες περιπτώσεις λόγο για την αύξηση των δημόσιων οικονομικών, που αντιπροσωπεύουν το 4% έως 12% του ΑΕΠ στα κράτη μέλη της ΕΕ (Ismailov, 2018).

Μια άλλη σημαντική πτυχή του τομέα της υγείας στην Ε.Ε., είναι ότι περίπου το 40% του πληθυσμού άνω των 15 ετών, δηλαδή πάνω από 100 εκατομμύρια πολίτες, αναφέρεται ότι πάσχει από χρόνια ασθένεια. Το ποσοστό αυτό αυξάνεται στο 66% για τον πληθυσμό που έχει συμπληρώσει την ηλικία συνταξιοδότησης με τουλάχιστον δύο χρόνια νοσήματα (Kieny et al., 2017). Ωστόσο, τα κράτη μέλη της Ε.Ε., αντιμετωπίζουν μια κατάσταση όπου έχει δαπανηθεί πάνω από το 70% του κόστους υγείας για χρόνιες ασθένειες, και το ποσοστό αυτό αναμένεται να αυξηθεί τα επόμενα χρόνια. Για το λόγο αυτό, τα κράτη μέλη της Ε.Ε., προσπαθούν να παρέχουν προσιτές, πιο αποτελεσματικές υπηρεσίες και πιο εξατομικευμένη φροντίδα στους πολίτες τους.

Για να επιτευχθούν λοιπόν τα παραπάνω, η εφαρμογή Τεχνολογιών Πληροφορικής και Επικοινωνιών αποτελεί σημαντικό πλεονέκτημα για τον κλάδο. Η χρήση της έννοιας της ηλεκτρονικής υγείας, διαδραματίζει βασικό ρόλο στη διατήρηση της ποιότητας των υπηρεσιών υγείας σε μια προσιτή σχέση κόστους-αποτελεσματικότητας (McCoy, Perlis, 2018).

Από την άποψη της ασφάλειας στον κυβερνοχώρο και ιδιαίτερα στα συστήματα υγεία, όλες αυτές οι τάσεις και οι τεχνολογικές εξελίξεις πρέπει να αναλύονται προσεκτικά από τους ειδικούς και τα ιδρύματα τα οποία παρέχουν υπηρεσίες υγείας. Οι οποιεσδήποτε διαδικτυακές επιθέσεις άλλωστε, εκθέτουν και συνάμα αυξάνουν την ευαισθησία των συστημάτων πληροφοριών και δεδομένων ασθενών μέσω σημάτων παρακολούθησης, κατάστασης υγείας και ιστορικού δεδομένων ασθενών σε ηλεκτρονική μορφή. Αυτές οι πληροφορίες θεωρούνται άκρως εμπιστευτικές και ευαίσθητες. Ως εκ τούτου, θα πρέπει να θεσπιστούν ισχυροί κανόνες και απαιτήσεις για τον έλεγχο ταυτότητας και να καταβάλλονται συνεχείς προσπάθειες για την προστασία των πληροφοριών, λαμβάνοντας υπόψη τις υπάρχουσες απειλές και τάσεις στις επιθέσεις στον κυβερνοχώρο (McCoy, Perlis, 2018).

Επίσης, σημειώνεται πως οι σχετικές επιθέσεις στον κυβερνοχώρο αυξάνονται συνεχώς. Εστιάζουν κυρίως στην κλοπή οικονομικών πληροφοριών, στοιχείων χρέωσης και αριθμών τραπεζικών λογαριασμών, χρησιμοποιώντας συσκευές με μη κρυπτογραφημένα δεδομένα, *ηλεκτρονικό ψάρεμα* (pishing) και ανεπιθύμητα μηνύματα

ηλεκτρονικού ταχυδρομείου. Η εξέλιξη της τεχνολογίας άλλωστε, οδήγησε σε προηγμένο *πόλεμο* στον κυβερνοχώρο με τη χρήση του SQL injection, Advance Persistence Threats (APT), επιθέσεις τύπου zero-day και διάφορα κακόβουλα προγράμματα (Barnett, et al., 2013).

Ο τομέας της ηλεκτρονικής και των συστημάτων υγείας λοιπόν, δεν αποτελεί εξαίρεση. Η έλλειψη επενδύσεων στον τομέα της πληροφορικής από οργανισμούς υγειονομικής περίθαλψης καθώς και η έλλειψη ενημέρωσης για το έγκλημα στον κυβερνοχώρο, έχουν εκθέσει τις αδυναμίες των οργανισμών υγείας. Ο αντίκτυπος των επιθέσεων στον κυβερνοχώρο, στα νοσοκομεία και τα συστήματα υγειονομικής περίθαλψης εκτιμάται ότι κοστίζουν σχεδόν έξι δισεκατομμύρια ετησίως (Kieny et al., 2017).

Στο πλαίσιο αυτό, η BitSight διεξήγαγε μια διεθνή μελέτη για τους οργανισμούς υγειονομικής περίθαλψης. Ο στόχος της μελέτης ήταν να κατανοήσει καλύτερα πού ο τομέας της υγείας χρειάζεται μεγαλύτερη προσοχή διαχείρισης κινδύνων. Χρησιμοποιώντας δεδομένα που συλλέχθηκαν από την ομάδα Data Science της BitSight από την 1η Ιουνίου 2019 έως το 2022, εξετάστηκαν οι συνολικές αξιολογήσεις ασφάλειας των εταιρειών φροντίδας. καθώς και πιθανές ευπάθειες, όπως ευάλωτα συστήματα και προγράμματα, ανασφαλείς πύλες και παραδείγματα ήδη παραβιασμένων συστημάτων (McCoy, Perlis, 2018).

Τα αποτελέσματα ήταν ξεκάθαρα ως προς την ερμηνεία τους. Τα δεδομένα δείχνουν ότι οι οργανισμοί σε αυτόν τον τομέα, έχουν χώρο να βελτιώσουν τις συμπεριφορές ασφαλείας τους. Άλλωστε, μόνο το 50% των εταιρειών υγειονομικής περίθαλψης έχουν προηγμένες αξιολογήσεις - πράγμα που σημαίνει ότι έχουν μικρότερες πιθανότητες να παραβιάσουν την ασφάλεια (Ismailov, 2018).

2.4 Οι Κίνδυνοι της Παραβίασης Ασφάλειας στον Κυβερνοχώρο στον Τομέα της Υγείας

Σύμφωνα με τα όσα αναφέρθηκαν παραπάνω, θα λέγαμε πως τα διάφορα ιδρύματα και συστήματα υγείας, προσπαθούν συνεχώς να εφαρμόσουν τις πιο αποτελεσματικές πρακτικές για την ασφάλεια στον κυβερνοχώρο, καθώς ενδέχεται να διατρέχουν διάφορους κινδύνους (Kieny et al., 2017). Πρώτιστα σημειώνεται πως τα ιατρικά και προσωπικά δεδομένα των ασθενών, ενσωματώνονται στον ψηφιακό κόσμο, αφήνοντας ανοιχτό το ενδεχόμενο έκθεσής τους σε τρίτους.

Δεύτερον, οι κίνδυνοι για την υγεία από το έγκλημα και την ασφάλεια στον κυβερνοχώρο γίνονται όλο και πιο περίπλοκοι και τα δεδομένα ενδέχεται να κλαπούν ή ο οργανισμός να αναγκαστεί να πληρώσει ένα σημαντικό ποσό για την εκ νέου πρόσβαση σε αυτά (McCoy, Perlis, 2018). Για να αποφευχθεί λοιπόν η κλοπή δεδομένων ασθενών, θα πρέπει να ληφθούν υπόψη τέσσερις (4) κίνδυνοι για την ασφάλεια στον κυβερνοχώρο που αντιμετωπίζουν οι οργανισμοί υγείας, ως εξής (Barnett, et al., 2013):

Χρήση απαρχαιωμένου εξοπλισμού πληροφορικής

Οι πάροχοι υγειονομικής περίθαλψης συνεργάζονται με ένα ευρύ φάσμα φορέων, από ανθρώπινους πόρους έως παρόχους ιατροτεχνολογικών προϊόντων. Με αυτό το διαφοροποιημένο οικοσύστημα, είναι σημαντικό να λάβει κανείς υπόψη του ότι ορισμένα τρίτα μέρη ενδέχεται να έχουν πρόσβαση στο δίκτυό τους και σε εμπιστευτικά δεδομένα μέσω ξεπερασμένων τελικών συσκευών (όπως υπολογιστές, φορητοί υπολογιστές, tablet, κ.λπ.). Εάν δοθεί πρόσβαση στο δίκτυο σε μη εξουσιοδοτημένα άτομα και χρησιμοποιούν μη ενημερωμένο εξοπλισμό, γίνονται αιτία έκθεσης των δεδομένων του οργανισμού υγείας.

Χρήση σε απαρχαιωμένο Ιατρικό εξοπλισμό

Οι ιατρικές συσκευές μπορεί να μην είναι το κύριο μέλημα της ασφάλειας στον κυβερνοχώρο, αλλά η ασφάλειά τους είναι σημαντική για την ασφάλεια του οργανισμού συνολικά. Για παράδειγμα, ακόμα κι αν ένα παλαιότερο λειτουργικό σύστημα, όπως ένα μηχάνημα ακτινών Χ, δεν χρησιμοποιείται πλέον, ενδέχεται να εξακολουθούν να υπάρχουν ίχνη αυτού του συστήματος. Εάν γίνει παραβίαση με έναν ιό που ονομάζεται *σκουλήκι* σε αυτό το σύστημα, τότε ο ιός αυτός έχει τη δυνατότητα να θέσει ολόκληρο το δίκτυο σε κίνδυνο. Σήμερα, οι κατασκευαστές ιατρικών συσκευών, χρησιμοποιούν το κριτήριο ασφαλείας ως τρόπο διαφοροποίησης στην αγορά και σηματοδοτούν μια αλλαγή στον τρόπο με τον οποίο τρίτα μέρη εξετάζουν την ασφάλεια στον κυβερνοχώρο

στην υγειονομική περίθαλψη.

Ιός Ransomware

Ο ιός Ransomware αποτελεί έναν από τους πιο πιθανούς κινδύνους για την ασφάλεια των οργανισμών υγειονομικής περίθαλψης. Αυτό είναι ένα κοινό πρόβλημα στον κλάδο της υγειονομικής περίθαλψης, πιθανώς λόγω της ευαίσθητης φύσης των δεδομένων που χρησιμοποιούνται σε αυτόν τον τομέα. Η επιτυχία μιας επίθεσης ransomware εξαρτάται σχεδόν εξ ολοκλήρου από το πόσο απεγνωσμένα χρειάζονται τα δεδομένα. Έτσι, εάν ένα νοσοκομείο δεχτεί επίθεση και τα δεδομένα δεν είναι προσβάσιμα με οποιονδήποτε άλλο τρόπο, κάποιοι είναι πρόθυμοι να πληρώσουν για να αποκτήσουν πρόσβαση.

Ως αποτέλεσμα, είναι σημαντικό για τους οργανισμούς υγειονομικής περίθαλψης να παρακολουθούν συνεχώς τα τρίτα μέρη τους και να αξιολογούν εάν η πρόσβαση στο δίκτυό τους θα μπορούσε να οδηγήσει σε τρωτά σημεία (τα οποία, με τη σειρά τους, θα μπορούσαν να οδηγήσουν σε ransomware και άλλες επιθέσεις). Συνήθως για την αμοιβή για τη λήψη των δεδομένων, απαιτείται τουλάχιστον 300$.

Επίπτωση στη Φήμη του Οργανισμού

Θα πρέπει να ληφθεί υπόψη ότι αν ένα νοσοκομείο αποστείλει δείγματα ασθενών σε εργαστήριο για δοκιμή και εάν το εργαστήριο αντιμετωπίσει παραβίαση της ασφάλειας, οι ασθενείς, συμπεριλαμβανομένων των ονομάτων τους, των ιατρικών αρχείων, των αποτελεσμάτων των δοκιμών και άλλων πληροφοριών που είναι προσωπικά αναγνωρίσιμες - μπορεί να διατρέχουν κάποιο κίνδυνο. Εάν ο οργανισμός δεν παρακολουθεί ενεργά για να βεβαιωθεί ότι λαμβάνονται τα κατάλληλα μέτρα ασφαλείας, τα αρχεία ασθενών τοποθετούνται σε μια επικίνδυνη κατάσταση με κίνδυνο να βλάψουν τη φήμη του νοσοκομείου. Αυτό θα προκαλέσει επίσης επιχειρηματικές απώλειες για το νοσοκομείο. Ωστόσο, οι τέσσερις (4) κίνδυνοι που αναφέρονται παραπάνω, είναι μόνο μερικοί από τους λόγους για τους οποίους η διαχείριση κινδύνου που προέρχεται από παρόχους υπηρεσιών, κατέχει κεντρική θέση στις συζητήσεις σχετικά με την ασφάλεια στον κυβερνοχώρο στην υγειονομική περίθαλψη.

2.5 Καταγραφή Πόρων (Assets)

Έχοντας εξετάσει περιληπτικά το εξωτερικό περιβάλλον του νοσοκομείου και τα συστήματα φύλαξης και ασφαλείας που χρησιμοποιεί, η παρούσα εξέταση πλέον, αναφέρεται στο εσωτερικό περιβάλλον του νοσοκομείου και ειδικότερα στις υφιστάμενες πληροφοριακές διαδικασίες και υποδομές, όπως και στις δράσεις που θα πρέπει να επιτευχθούν για την βελτίωση του επιπέδου ασφαλείας τύπου ransomware στις υποδομές αυτές.

Είναι χρήσιμο στο πεδίο αυτό, να σημειωθεί πως το *ransomware* είναι ένα κακόβουλο λογισμικό που λειτουργεί, κρυπτογραφώντας δεδομένα που είναι αποθηκευμένα σε υπολογιστές ή στο ίδιο το δίκτυο (Hampton, 2010). Μια επίθεση τύπου ransomware είναι ένα κακόβουλο λογισμικό που εξαλείφει την πρόσβαση στα δεδομένα χρήστη, κρυπτογραφώντας τα με ένα κλειδί. Ο εισβολέας (hacker) είναι το μόνο άτομο που γνωρίζει το κλειδί, που σημαίνει ότι ο εισβολέας είναι το μόνο άτομο με πρόσβαση στα δεδομένα.

Ο σκοπός πίσω από αυτό το είδος επίθεσης είναι η πρόκληση πληρωμής λύτρων από τον κάτοχο των δεδομένων στον εισβολέα. Αυτός ο τύπος επίθεσης μπορεί να είναι αποτέλεσμα *ηλεκτρονικού ψαρέματος* (pishing). Οι αδυναμίες του συστήματος, όπως η έλλειψη δημιουργίας αντιγράφων ασφαλείας συστήματος, η έλλειψη δυνατοτήτων anti-phishing και η έλλειψη ασφάλειας δικτύου, ενδέχεται να οδηγήσουν σε σχετικές δυσμενείς συνέπειες (Serra, 2000).

Στο πλαίσιο αυτό, αναφέρονται οι πόροι του νοσοκομείου οι οποίοι σχετίζονται με ένα σύστημα το οποίο διαχειρίζεται τα δεδομένα που συλλέγονται και αποθηκεύονται στην εν λόγω μονάδα υγειονομικής περίθαλψης. Αυτό το σύστημα περιλαμβάνει καθημερινές καταγραφές, εισροές και δεδομένα για τα εσωτερικά και εξωτερικά ιατρεία του νοσοκομείου. Αυτό το σύστημα επίσης το οποίο είναι κοινό για όλες τις υπηρεσίες του νοσοκομείου, αποθηκεύει, διαχειρίζεται και αποστέλλει ηλεκτρονικά όλα τα ιατρικά αρχεία των ασθενών., μεταξύ των εργαζομένων στα διάφορα τμήματα του νοσοκομείου.

Ωστόσο, τα δεδομένα ασθενών είναι εξαιρετικά ευαίσθητα, επομένως το σύστημα πληροφοριών υγείας που χρησιμοποιείται, πρέπει να διασφαλίζει την ακρίβεια των δεδομένων που συλλέγονται και την εμπιστευτικότητα των ασθενών. Άλλες χρήσεις των δεδομένων ασθενών εκτός από τη θεραπεία τους, περιλαμβάνουν στοιχεία για την ιατρική έρευνα, τα δεδομένα χάραξης πολιτικής, την ανάλυση κύκλου εσόδων και τις πληροφορίες λήψης αποφάσεων. Το συγκεκριμένο σύστημα έχει μια τακτική πρόσβαση,

επεξεργασία ή αποθήκευση μεγάλου όγκου ευαίσθητων δεδομένων ασθενών. Ως αποτέλεσμα, η ασφάλεια του, είναι ζωτικής σημασίας.

Καταλήγοντας στα παραπάνω, θα λέγαμε πως το εν λόγω σύστημα, αναφέρεται ως ένα λογισμικό διαχείρισης καθημερινών δεδομένων και καταγραφών που βοηθά τις εγκαταστάσεις της υγειονομικής περίθαλψης και το προσωπικό του νοσοκομείου, ως προς τη διαχείριση των καθημερινών λειτουργιών της εγκατάστασης. Αυτό περιλαμβάνει τον προγραμματισμό των ασθενών και τη χρέωση των ιατρικών υπηρεσιών. Ανεξάρτητα από το μέγεθός του, από τους ιατρούς ενός ιατρείου μέχρι τα τεράστια πολυκεντρικά νοσοκομεία, όλοι οι πάροχοι υγειονομικής περίθαλψης χρησιμοποιούν το διαχείρισης καθημερινών δεδομένων. Ο στόχος είναι να αυτοματοποιηθούν οι διοικητικές εργασίες για τον εξορθολογισμό της ροής εργασιών της εγκατάστασης και η αύξηση των αλληλεπιδράσεων ασθενών-προσωπικού στο εν λόγω νοσοκομείο.

2.6 Η Αύξηση του Ηλεκτρονικού Εγκλήματος και της Τρομοκρατίας στο Διαδίκτυο

Σύμφωνα με όσα αναφέρθηκαν παραπάνω, θα λέγαμε πως τα τελευταία 30 χρόνια, το έγκλημα στον κυβερνοχώρο και η κυβερνοτρομοκρατία έχουν εξελιχθεί από μια πιθανή ανησυχία σε κοινή απειλή. Οι κυβερνοαπειλές έγιναν ζήτημα εθνικής ασφάλειας μετά την 11η Σεπτεμβρίου (Stohl, 2007). Μετά τις τρομοκρατικές επιθέσεις της 11ης Σεπτεμβρίου 2001, ο Πρόεδρος Μπους δημιούργησε το Γραφείο Ασφάλειας Κυβερνοχώρου (Weimann, 2005).

Σε αυτή τη θέση, το Γραφείο Ασφάλειας Κυβερνοχώρου συνέχισε να εγείρει το ζήτημα μιας πιθανής επίθεσης στο διαδίκτυο σε διάφορους στόχους των Ηνωμένων Πολιτειών (Stohl, 2007). Υπήρξε επίσης μια ειδική επιτροπή του Κογκρέσου που δημιουργήθηκε μετά την επίθεση της 11ης Σεπτεμβρίου 2001 για να εξετάσει τους κινδύνους τρομοκρατίας για τις Ηνωμένες Πολιτείες. Αυτή η επιτροπή ασχολήθηκε με την πιθανή χρήση μιας κυβερνοεπίθεσης σε συνδυασμό με μια τακτική τρομοκρατική επίθεση (Weimann, 2005).

Ωστόσο, συχνά, οι όροι που χρησιμοποιούνται για τον ορισμό των επιθέσεων στον κυβερνοχώρο, χρησιμοποιούνται εναλλακτικά όταν κατέχουν μια διαφορετική

σημασία. Ο Denning (2000) λοιπόν, ορίζει την κυβερνοτρομοκρατία ως «*τη σύγκλιση του κυβερνοχώρου και της τρομοκρατίας*». Αυτό σημαίνει ότι για να χαρακτηριστεί μια πράξη ως κυβερνοτρομοκρατία, πρέπει να έχει μια πτυχή στον κυβερνοχώρο, καθώς και να έχει το κίνητρο να δημιουργεί φόβο ή εξαναγκασμό σε μια κυβέρνηση ή έναν συγκεκριμένο πληθυσμό (Weimann, 2005).

Πιθανοί στόχοι για την κυβερνοτρομοκρατία υπάρχουν στην υποδομή των Ηνωμένων Πολιτειών και της Ευρώπης, συμπεριλαμβανομένου του χρηματοοικονομικού δικτύου των χωρών των ηπείρων αυτών, οποιουδήποτε τύπου ελέγχου κυκλοφορίας, συμπεριλαμβανομένων των αεροπορικών εταιρειών μεταφοράς και τρένων, των ηλεκτρικών δικτύων ή φραγμάτων και των μονάδων επεξεργασίας νερού (Squitieri, 2002).

Υπάρχουν επίσης φόβοι ότι οι τρομοκράτες θα μπορούσαν να χρησιμοποιήσουν μια κυβερνοεπίθεση σε συνδυασμό με μια *παραδοσιακή* τρομοκρατική επίθεση για να εμποδίσουν τις προσπάθειες διάσωσης που λαμβάνουν χώρα (Weimann, 2005, Squitieri, 2002). Υπάρχουν επίσης πτυχές της κυβερνοτρομοκρατίας που μπορεί να την κάνουν πιο *ελκυστική* για τους ίδιους τους τρομοκράτες σε σύγκριση με τις παραδοσιακές τρομοκρατικές επιθέσεις.

Σημειώνεται λοιπόν πως η κυβερνοτρομοκρατία διεξάγεται εξ αποστάσεως, καθιστώντας ευκολότερο για τους δράστες να παραμείνουν ανώνυμοι. Δεύτερον, οι επιθέσεις στον κυβερνοχώρο, είναι πολύ φθηνότερες από τις παραδοσιακές τρομοκρατικές επιθέσεις. Τέλος, η εμβέλεια και ο πιθανός αντίκτυπος που έχουν οι τρομοκράτες με τις επιθέσεις στον κυβερνοχώρο, είναι πολύ μεγαλύτερος από ό,τι με τις παραδοσιακές τρομοκρατικές επιθέσεις (Weimann, 2005).

Το έγκλημα στον κυβερνοχώρο λοιπόν, ορίζεται ως μια παράνομη πράξη στην οποία ένας υπολογιστής μπορεί να είναι το εργαλείο ή/και το θύμα για κάποιους άλλους (Dashora, 2011). Σύμφωνα με το FBI, δισεκατομμύρια δολάρια ξοδεύονται κάθε χρόνο για την επισκευή συστημάτων που έχουν πληγεί από το έγκλημα στον κυβερνοχώρο. Ένας από τους κύριους στόχους του εγκλήματος στον κυβερνοχώρο είναι τα δεδομένα, ιδιαίτερα τα αναγνωρίσιμα στοιχεία, συμπεριλαμβανομένων των ταυτοτήτων, των τραπεζικών λογαριασμών και των ηλεκτρονικών ιατρικών αρχείων (EMR).

Το 2016, υπολογίστηκε ότι η κλοπή ταυτότητας κοστίζει στις αμερικανικές

επιχειρήσεις πάνω από 50 δισεκατομμύρια δολάρια με επιπλέον 5 δισεκατομμύρια δολάρια σε δαπάνες σε ιδιώτες (Kshetri, 2019). Μια μελέτη του Ινστιτούτου Ponemon σημείωσε αύξηση 19% του εγκλήματος στον κυβερνοχώρο το 2015 (Gordon, 2016). Μαζί με την αυξανόμενη τάση των εγκλημάτων στον κυβερνοχώρο, αυτού του είδους οι επιθέσεις γίνονται πιο περίπλοκες και εκτεταμένες.

Μία από τις πιο διαβόητες επιθέσεις στον κυβερνοχώρο το 2016, ήταν η διαδικασία του hacking που έλαβε χώρα κατά τη διάρκεια των προεδρικών εκλογών στις ΗΠΑ. Ρώσοι χάκερ διέρρευσαν εμπιστευτικά email και έγγραφα τόσο από την Εθνική Επιτροπή των Δημοκρατικών όσο και από την Επιτροπή Εκστρατείας του Δημοκρατικού Κογκρέσου. Έγινε επίσης φανερό από τις εκλογές ότι η Ρωσία είχε ρόλο στην προσπάθεια να επηρεάσει ποιος έγινε Πρόεδρος των Ηνωμένων Πολιτειών (Lipton, Sanger, & Shane, 2016). Το 2016, ο Πρόεδρος Ομπάμα είπε ότι οι Ηνωμένες Πολιτείες έχουν τη δυνατότητα να είναι πιο ευάλωτες από άλλες χώρες σε κυβερνοεπιθέσεις λόγω του μεγάλου μεγέθους της οικονομίας των ΗΠΑ και λόγω του μεγάλου όγκου ψηφιοποίησης σε αυτή τη χώρα (Kelly, 2016).

Τον Μάρτιο του 2018 επίσης, το Υπουργείο Εσωτερικής Ασφάλειας και το Ομοσπονδιακό Γραφείο Ερευνών εξέδωσαν μια κοινή δήλωση σχετικά με τη ρωσική πειρατεία κρίσιμων υποδομών των Ηνωμένων Πολιτειών (Naylor, 2018). Ορισμένοι στόχοι ρωσικής *πειρατείας*, περιλαμβάνουν πυρηνικούς σταθμούς, τον τομέα της ηλεκτρικής ενέργειας και εμπορικές εγκαταστάσεις.

Η δήλωση αναφέρει ότι η Κοινότητα Πληροφοριών των ΗΠΑ, γνώριζε για ρωσικές εισβολές στις ΗΠΑ τουλάχιστον από τον Μάρτιο του 2016. Το καλοκαίρι του 2016, η Ρωσία ξεκίνησε μια «εκστρατεία εισβολής πολλών σταδίων» εναντίον των υπηρεσιών κοινής ωφέλειας των ΗΠΑ και το αποτέλεσμα αυτής της επίθεσης ήταν χάκερ απέκτησε πρόσβαση σε τουλάχιστον ένα σύστημα ελέγχου ενός σταθμού ηλεκτροπαραγωγής (Ismailov, 2018).

Το 2015, Ρώσοι χάκερ διέκοψαν την παροχή ρεύματος σε περισσότερους από 200.000 ανθρώπους στην Ουκρανία, όταν παραβίασαν ένα εργοστάσιο ηλεκτροπαραγωγής και τερμάτισαν τις υπηρεσίες (Naylor, 2018). Ένα άρθρο των New York Times ισχυρίζεται ότι η Ρωσία στοχεύει τις ΗΠΑ και την Ευρώπη σε ζωτικής σημασίας υποδομές, συμπεριλαμβανομένων των εγκαταστάσεων επεξεργασίας νερού, από το 2015. Αυτό το ίδιο άρθρο εξετάζει επίσης ισχυρισμούς από ιδιωτικές εταιρείες

ασφαλείας ότι αυτές οι συντονισμένες επιθέσεις λαμβάνουν χώρα από το 2013 (Perlroth & Sanger, 2018).

Ένα συγκεκριμένο έγκλημα στον κυβερνοχώρο λοιπόν, είναι μια επίθεση ransomware, η οποία έχει γίνει πολύ πιο συνηθισμένη εναντίον οργανισμών (Larson, 2017), αφού σημειώθηκε άλμα κατά 159% στις επιθέσεις ransomware από τον Μάρτιο έως τον Απρίλιο του 2016. Η κανονική αύξηση μεταξύ των μηνών ήταν προηγουμένως μόνο 9-20% (Lee, Μάιος 2016). Το FBI αναφέρει ότι το 2016, υπήρξαν 2.673 θύματα επιθέσεων ransomware σε όλες τις Ηνωμένες Πολιτείες.

Επίσης σημειώνεται πως δύο μεγάλες επιθέσεις ransomware, το WannaCry και το NotPetya, σημειώθηκαν μέσα σε ένα μήνα η μία από την άλλη, το καλοκαίρι του 2017 και είχαν επιπτώσεις σε όλο τον κόσμο. Η επίθεση WannaCry έλαβε χώρα τον Μάιο του 2017 και *μόλυνε* υπολογιστές σε 150 χώρες. Αυτή η επίθεση έχει από τότε συνδεθεί με τη Βόρεια Κορέα (Nakashima, 2018). Η άλλη μεγάλη επίθεση ήταν η επίθεση NotPetya, τον Ιούνιο του 2017, η οποία έκτοτε συνδέεται με τη Ρωσία (Nakashima, 2018).

Ο ιός NotPetya *μόλυνε* υπολογιστές στη Δανία, την Ινδία και τις Ηνωμένες Πολιτείες, αλλά τα περισσότερα από τα θύματά του εντοπίστηκαν στην Ουκρανία. Αυτός ο ιός αντιμετώπιζε έναν ιό ransomware ενώ στην πραγματικότητα διέγραφε οριστικά αρχεία. Μερικοί οργανισμοί που επλήγησαν, ήταν οι τράπεζες, εταιρείες ενέργειας, ένα αεροδρόμιο και κυβερνητικοί αξιωματούχοι. Μια αμερικανική εταιρεία που επηρεάστηκε επίσης, ήταν η φαρμακευτική εταιρεία, Merck. Οι εργαζόμενοι λέγεται ότι στάλθηκαν σπίτι από όλα τα εργοστάσια των ΗΠΑ, κατά τη διάρκεια αυτής της επίθεσης και μια έκθεση για τον αντίκτυπο της επίθεσης ανέφερε ότι τα έσοδα της Merck μειώθηκαν κατά 135 εκατομμύρια δολάρια λόγω χαμένων πωλήσεων (Davis, 2017).

Σύμφωνα τέλος με μια Έκθεση του Υπουργείου Δικαιοσύνης του 2016, κατά μέσο όρο το 2016 σημειώνονταν έως και 4.000 απόπειρες επίθεσης ransomware την ημέρα. Αυτό ήταν μια αύξηση κατά 300% από τον μέσο αριθμό ημερήσιων επιθέσεων που παρατηρήθηκαν το 2015. Το ransomware δεν αποτελεί πλέον απειλή για το μέλλον, αλλά μάλλον μια απειλή που όλοι οι οργανισμοί πρέπει να λάβουν σοβαρά υπόψη.

2.7 Στοιχεία τα Οποία Αναφέρονται στις Κυβερνοεπιθέσεις στα

Συστήματα Υγείας και Ενέργειες από Μέρους Αυτών για Πρόληψη και Προστασία

2.7.1 Ανάλυση Κινδύνων από Κυβερνοεπιθέσεις

Αναφερόμενος κανείς στην προστασία των συστημάτων υγείας από τις κυβερνοεπιθέσεις και τις δυσμενείς επιπτώσεις που δύναται να δημιουργηθούν, θα λέγαμε πως είναι απαραίτητες συγκεκριμένες κινήσεις και διεργασίες που θα πρέπει να εκτελεστούν με σκοπό την πρόληψη και προστασία από τις επιθέσεις αυτές. Στο πλαίσιο αυτό λοιπόν, αναφέρεται ως πρώτο βήμα η ανάλυση κινδύνων σε συγκεκριμένα πληροφοριακά συστήματα των συστημάτων υγείας και ιδιαίτερα των νοσοκομείων, όπου η ανάλυση αυτή οριοθετείτε στις απειλές οι οποίες έχουν ταξινομηθεί σε δύο κύριες κατηγορίες, δηλαδή τις εσωτερικές απειλές και εξωτερικές απειλές (Ismailov, 2018).

Μια εσωτερική απειλή σε συγκεκριμένα πληροφοριακά συστήματα των συστημάτων υγείας και ιδιαίτερα των νοσοκομείων, περιλαμβάνει διάφορους τύπους συμπεριφοράς εργαζομένων όπως την άγνοια, περιέργεια, απερισκεψία, ανεπαρκής συμπεριφορά, λήψη του κωδικού πρόσβασης κάποιου άλλου και παροχή κωδικό πρόσβασης σε άλλον υπάλληλο ή εξωτερικό επισκέπτη.

Μια εξωτερική απειλή στο πληροφοριακό σύστημα του νοσοκομείου, το οποίο περιλαμβάνει ιούς και επιθέσεις spyware, τους χάκερ και εισβολείς σε εγκαταστάσεις του συστήματος στο νοσοκομείο. Αναφέρεται επίσης η ενσωμάτωση κακόβουλου κώδικα λόγω της χρήσης ασύρματων και κινητών τεχνολογιών, η εισαγωγή επιβλαβούς λογισμικού, η εισβολή χάκερ λόγω μη ασφαλούς δικτύου, η απόκτηση πρόσβασης σε εμπιστευτικές πληροφορίες μέσω κοινωνικής αλληλεπίδρασης από τρίτους, η αποστολή εμπιστευτικών πληροφοριών σε λάθος παραλήπτη και η αποθήκευση δεδομένων ή διαβαθμισμένων πληροφοριών σε απροστάτευτες περιοχές από το προσωπικό (Kieny et al., 2017).

2.7.2 Πολιτικές Ασφαλείας Πληροφοριακών Συστημάτων στα Συστήματα Υγείας

Οι πολιτικές ασφαλείας σε συγκεκριμένα πληροφοριακά συστήματα των συστημάτων υγείας και ιδιαίτερα των νοσοκομείων, αναφέρονται σε έναν οδηγό ή εγχειρίδιο που καθορίζει τις διαδικασίες και τους κανόνες που έχουν σχεδιαστεί για να διατηρούν ασφαλής όλους τους χρήστες και τα δίκτυα σε έναν οργανισμό. Εξηγεί τα πρότυπα ασφάλειας πληροφορικής και προστασίας δεδομένων και καθορίζει τις ενέργειες που θα διατηρήσουν αυτά τα πρότυπα εντός του νοσοκομείου. Οι συγκεκριμένες πολιτικές ασφάλειας πληροφοριών, εστιάζουν καθαρά στο ψηφιακό τοπίο της λειτουργίας του συστήματος (Barnett, et al., 2013)

Όλες οι σύγχρονες εγκαταστάσεις και συστήματα υγειονομικής περίθαλψης θα πρέπει να χρησιμοποιούν μια ενσωματωμένη τεχνολογία σε όλο το μεγαλύτερο μέρος της λειτουργίας τους, που κυμαίνονται από λογαριασμούς email προσωπικού έως ασφαλή δεδομένα ασθενών. Μια πολιτική ασφάλειας πληροφοριών υγειονομικής περίθαλψης πρέπει να καλύπτει όλα αυτά, όπως τα ασφαλή δεδομένα, συστήματα, συσκευές, υποδομές, δεδομένα και όλους τους χρήστες (Serra, 2000).

Οι πολιτικές ασφαλείας σε συγκεκριμένα πληροφοριακά συστήματα των συστημάτων υγείας και ιδιαίτερα των νοσοκομείων, όπως επίσης και όταν η τεχνολογία δεν είχε αναπτυχθεί σε τόσο μεγάλο βαθμό όπως στις μέρες μας, είχαν ως σκοπό την καθιέρωση ενός σχεδίου για την ασφάλεια των πληροφοριών, την δημιουργία τεκμηρίωσης σχετικά με τα μέτρα ασφαλείας και τον έλεγχο πρόσβασης χρηστών, την χρήση εργαλείων για την ανίχνευση της κακής χρήσης δεδομένων ή των παραβιασμένων δικτύων ή συσκευών και για την ελαχιστοποίηση των επιπτώσεων, την προστασία των προσωπικών πληροφοριών των ασθενών, καθώς και των δεδομένων τους, συμπεριλαμβανομένων των αριθμών πιστωτικών καρτών αλλά και την κατάρτιση σχεδίων για την αντιμετώπιση των κινδύνων στον κυβερνοχώρο της υγειονομικής περίθαλψης (Kieny et al., 2017).

2.7.3 Διαδικασίες Ασφαλείας

Όσον αφορά τις διαδικασίες ασφαλείας σε συγκεκριμένα πληροφοριακά

συστήματα των συστημάτων υγείας και ιδιαίτερα των νοσοκομείων, θα λέγαμε πως αυτές θα πρέπει να αναφέρονται ως αυστηρές πολιτικές και διαδικασίες για να διατηρείται το δίκτυο του συστήματος ασφαλές, να διατηρείται επίσης ασφαλή η μετάδοση δεδομένων και να προστατεύονται τα εμπιστευτικά αρχεία των ασθενών. Η ανάπτυξη τέτοιων πολιτικών και διαδικασιών καθώς και η διεξαγωγή παρακολούθησης και ελέγχου σε πραγματικό χρόνο των πρακτικών ασφαλείας σε συγκεκριμένα πληροφοριακά συστήματα των συστημάτων υγείας και ιδιαίτερα των νοσοκομείων, θα μπορούσε να διασφαλίζει την ασφάλεια του περιβάλλοντος πληροφορικής του νοσοκομείου.

Είναι σημαντικό λοιπόν να κατανέμονται αποτελεσματικά οι πόροι και να διαχειρίζεται κανείς το περιβάλλον πληροφορικής προληπτικά, προκειμένου να περιορίζονται οι συνεχώς εξελισσόμενες απειλές και οι μεταβαλλόμενοι κανονισμοί. Αυτό το γεγονός μπορεί να επιτευχθεί με τη διαχείριση του αυστηρού ελέγχου πρόσβασης, του προσανατολισμού των εργαζομένων και των τακτικών εκπαιδεύσεων αλλά και της ταυτοποίησης του προσωπικού, των επισκεπτών και των ασθενών σύμφωνα με τους κανονισμούς του κλάδου (McCoy, Perlis, 2018).

2.7.4 Διαδικασίες Επαναφοράς Συστήματος

Ως προς τις διαδικασίες επαναφοράς του πληροφοριακού συστήματος σε συγκεκριμένα πληροφοριακά συστήματα των συστημάτων υγείας και ιδιαίτερα των νοσοκομείων, θα λέγαμε πως θα πρέπει να υπάρχουν συγκεκριμένες οδηγίες που ακολουθούνται κάθε φορά, και όχι μόνο όταν δημιουργηθεί ένα πρόβλημα, αφού οι χρήστες τους θα πρέπει να επικοινωνούν αμέσως με την εταιρεία παρασκευής και εμπορίας των συστημάτων αυτών, με σκοπό να επιλύσουν το συγκεκριμένο πρόβλημα παραβίασης και υποκλοπής δεδομένων (Barnett, et al., 2013).

Ωστόσο, παρά το ευρύ αυτό πεδίο εφαρμογής του συστήματος σε συγκεκριμένα πληροφοριακά συστήματα των συστημάτων υγείας και ιδιαίτερα των νοσοκομείων, κάθε έκτακτη ανάγκη θα πρέπει να αντιμετωπίζεται ως μοναδική και οι σχετικές διαφορές θα πρέπει να λαμβάνονται υπόψη κατά την εφαρμογή του οδηγού, με ιδιαίτερη προσοχή στο πλαίσιο, τη διάρκεια της μεταβατικής περιόδου, την προθυμία και την ικανότητα των χρηστών να επιλύσουν τα όποια προβλήματα στο σύστημα.

Για την περαιτέρω προσαρμογή του οδηγού σε συγκεκριμένα πλαίσια και τύπους έκτακτης ανάγκης λόγω επίθεσης τύπου ransomware, ενδέχεται να απαιτηθούν πρόσθετες εργασίες, όπως η ανάπτυξη τεχνικών κατευθυντήριων γραμμών και τυπικών διαδικασιών λειτουργίας για την τροποποίηση και προσαρμογή της υλοποίησης και της αλληλουχίας των δραστηριοτήτων προτεραιότητας στις διάφορες φάσεις της επαναφοράς του συστήματος μετά την επίθεση αυτού του τύπου (McCoy, Perlis, 2018).

2.7.5 Καθήκοντα Διαχειριστή Ασφαλείας Συστημάτων και Δικτύων

Ως προς τα καθήκοντα του διαχειριστή ασφαλείας συστημάτων και δικτύων εντός του νοσοκομείου και ως προς την προστασία στα πληροφοριακά συστήματα των συστημάτων υγείας και ιδιαίτερα των νοσοκομείων, αυτά αναφέρονται ως εξής

✓ Παροχή εκπαίδευσης για την ασφάλεια των πληροφοριών στο προσωπικό του οργανισμού

✓ Δημιουργία και διαχείριση στρατηγικών ασφαλείας στα τμήματα του νοσοκομείου

✓ Επιβλέπει τους ελέγχους ασφάλειας πληροφοριών, είτε από εξειδικευμένους οργανισμούς είτε από προσωπικό τρίτων

✓ Διαχειρίζεται τα μέλη της ομάδας ασφαλείας και όλο το άλλο προσωπικό ασφάλειας πληροφοριών

✓ Παροχή εκπαίδευσης στο προσωπικό ασφάλειας πληροφοριών κατά την επιβίβαση

✓ Αξιολογεί τον προϋπολογισμό του τμήματος και το κόστος που σχετίζεται με την

τεχνολογική εκπαίδευση των υφισταμένων του

✓ Αξιολογεί την τρέχουσα αρχιτεκτονική τεχνολογίας για τρωτά σημεία, αδυναμίες και για πιθανές αναβαθμίσεις ή βελτιώσεις

✓ Επιβλέπει την εφαρμογή και επίβλεψη τεχνολογικών αναβαθμίσεων, βελτιώσεων και σημαντικών αλλαγών στο περιβάλλον ασφάλειας πληροφοριών

✓ Χρησιμεύει ως σημείο επαφής για την ομάδα ασφάλειας πληροφοριών στα πληροφοριακά συστήματα των συστημάτων υγείας και ιδιαίτερα των νοσοκομείων

✓ Διαχειρίζεται και διαμορφώνει τα συστήματα φυσικής ασφάλειας, αποκατάστασης καταστροφών και δημιουργίας αντιγράφων ασφαλείας δεδομένων στο πληροφοριακό σύστημα

✓ Επικοινωνεί αποτελεσματικά τους στόχους ασφάλειας πληροφοριών και τα νέα προγράμματα με άλλους διευθυντές τμημάτων εντός του οργανισμού.

2.8 Πλάνο Διαχείρισης Κρίσεων Πριν, Κατά και Μετά την Ενδεχόμενη Κυβερνοεπίθεση σε Συστήματα Υγείας και Νοσοκομεία

2.8.1 Πριν τη Κρίση

Αναφερόμενοι σχετικά στο σχέδιο διαχείρισης σε συγκεκριμένα πληροφοριακά συστήματα των συστημάτων υγείας και ιδιαίτερα των νοσοκομείων αλλά και πριν ουσιαστικά «ξεσπάσει» μια κρίση με ένα περιστατικό επίθεσης ασφαλείας τύπου ransomware για παράδειγμα, θα πρέπει να προστατευθεί με κάθε τρόπο το σύστημα το οποίο διαχειρίζεται τα δεδομένα που συλλέγονται και αποθηκεύονται σε μια μονάδα υγειονομικής περίθαλψης. Αυτό το σύστημα περιλαμβάνει καθημερινές καταγραφές, εισροές και δεδομένα για τα εσωτερικά και εξωτερικά ιατρεία του νοσοκομείου. Επίσης το σύστημα είναι κοινό για όλες τις υπηρεσίες του νοσοκομείου, αποθηκεύει, διαχειρίζεται και αποστέλλει ηλεκτρονικά όλα τα ιατρικά αρχεία των ασθενών., μεταξύ των εργαζομένων στα διάφορα τμήματα του νοσοκομείου (Ismailov, 2018).

Το εν λόγω σύστημα ουσιαστικά, θα αναφέρεται ως ένα λογισμικό διαχείρισης καθημερινών δεδομένων και καταγραφών που βοηθά τις εγκαταστάσεις υγειονομικής περίθαλψης και το προσωπικό του κάθε νοσοκομείου, ως προς τη διαχείριση των καθημερινών λειτουργιών της εγκατάστασης. Αυτό θα περιλαμβάνει τον προγραμματισμό των ασθενών και τη χρέωση των ιατρικών υπηρεσιών. Δεδομένου ότι σε ένα συγκεκριμένο δίκτυο, καθένας μπορεί να έχει πρόσβαση στις προσωπικές πληροφορίες υγείας του ασθενούς και εκείνοι που χρησιμοποιούν το σύστημα, μπορούν να διαχειριστούν τη συνδυασμένη θεραπεία πιο εύκολα.

Στο πλαίσιο αυτό λοιπόν, το κενό απόκλισης στη λειτουργία του συστήματος, δεν θα πρέπει να αναφέρεται στο γεγονός πως στο σύστημα αυτό μπορεί να έχει πρόσβαση ο κάθε εργαζόμενος στο νοσοκομείο και όχι μόνο τα ανώτερα στελέχη των ιατρικών τμημάτων ή οι εργαζόμενοι που πραγματικά είναι ανάγκη να διαχειρίζονται αυτό. Επιπλέον, θα πρέπει να υπάρχουν στο εν λόγω σύστημα, ολοκληρωμένες δικλείδες ασφαλείας, με δύο ή τρία επίπεδα ασφαλείας και έως ο χρήστης να έχει πρόσβαση στο σύνολο των πληροφοριών. Αντιθέτως, το σύστημα δεν θα λειτουργεί μόνο με την εισαγωγή ενός κωδικού κοινού για όλους τους εργαζόμενους και την ελεύθερη επεξεργασία, εισαγωγή και εξαγωγή δεδομένων.

Οι πολιτικές ασφαλείας του συγκεκριμένου συστήματος, δεν θα αναφέρονται απλά σε έναν οδηγό ή εγχειρίδιο που καθορίζει τις διαδικασίες και τους κανόνες που έχουν σχεδιαστεί για να διατηρούν ασφαλή όλους τους χρήστες και τα δίκτυα σε έναν οργανισμό. Θα πρέπει να εξηγεί τα πρότυπα ασφάλειας πληροφορικής και προστασίας δεδομένων και καθορίζει τις ενέργειες που θα διατηρήσουν αυτά τα πρότυπα εντός του νοσοκομείου. Οι συγκεκριμένες πολιτικές ασφάλειας πληροφοριών, θα πρέπει να εστιάζουν καθαρά στο ψηφιακό τοπίο της λειτουργίας του συστήματος

Τέλος, όσον αφορά τις διαδικασίες ασφαλείας στο πληροφοριακό σύστημα που χρησιμοποιεί το κάθε νοσοκομείο, θα λέγαμε πως αυτές θα πρέπει να αναφέρονται ως αυστηρές πολιτικές και διαδικασίες για να διατηρείται το δίκτυο του συστήματος ασφαλές, να διατηρείται επίσης ασφαλή η μετάδοση δεδομένων και να προστατεύουν τα εμπιστευτικά αρχεία των ασθενών. Η ανάπτυξη τέτοιων πολιτικών και διαδικασιών και η διεξαγωγή παρακολούθησης και ελέγχου σε πραγματικό χρόνο των πρακτικών ασφαλείας στο κάθε νοσοκομείο, θα μπορούσε να διασφαλίζει την ασφάλεια του περιβάλλοντος πληροφορικής του νοσοκομείου (Kieny et al., 2017).

Ωστόσο αυτό που απορρέει από τα παραπάνω, είναι πως πριν από την κρίση δεν είχε προβλεφθεί από τους ιθύνοντες και τον υπεύθυνο ασφαλείας, πως κάποιος μπορεί να εισέλθει στο σύστημα και να «κλειδώσει» τη πρόσβαση για τους υπολοίπους χρήστες σε κάποια από τα τμήματα του νοσοκομείου και να ζητά λύτρα για αυτή την επίθεση.

2.8.2 Κατά τη Κρίση

Κατά την κρίση λοιπόν που έχει ξεσπάσει» με το περιστατικό επίθεσης ασφαλείας τύπου ransomware σε συγκεκριμένα πληροφοριακά συστήματα των συστημάτων υγείας και ιδιαίτερα των νοσοκομείων για παράδειγμα, θα πρέπει από μέρους του διαχειριστή ασφαλείας συστημάτων και δικτύων, να εφαρμοστούν οι οδηγίες που υπάρχουν στο εγχειρίδιο για όταν προκύψει ένα σημαντικό πρόβλημα στη λειτουργία του συστήματος και ταυτόχρονα να εξεταστούν αμέσως το ενδεχόμενο κατάργησης της δυνατότητας εκτύπωσης και αντιγραφής/επικόλλησης από εφαρμογές Ηλεκτρονικών Ιατρικών Αρχείων ή αλληλογραφία σε διαδικτυακή βάση από μέρους του ιδίου αλλά και των άλλων χρηστών του συστήματος (Kieny et al., 2017).

Η κρίση η οποία μπορεί να ξέσπασε στην εν λόγω περίπτωση και όπως δεν είχε προβλεφθεί παραπάνω από τους ιθύνοντες και τον υπεύθυνο ασφαλείας, αναφέρεται στο γεγονός πως ένα τρίτο άτομο εισήλθε στο σύστημα και «κλείδωσε» τη πρόσβαση για τους υπολοίπους χρήστες σε ορισμένα από τα τμήματα του νοσοκομείου, ζητώντας λύτρα για αυτή την επίθεση και κατόπιν να μπορέσει να ελευθερώσει το σύστημα και την πρόσβαση των χρηστών.

Για το σκοπό αυτό, ο υπεύθυνος ασφαλείας του συστήματος, θα πρέπει να εφαρμόσει βήματα που έχει διδαχθεί στο πρόγραμμα εκπαίδευσης για την ασφάλεια στον κυβερνοχώρο και άμεσα να έχει μια συνολική εικόνα του συστήματος και της λήψης μνήμης ενός δείγματος συσκευών που επηρεάζονται από την επίθεση στα διάφορα τμήματα του νοσοκομείου και να συλλέξει σχετικά αρχεία καταγραφής για επεξεργασία περαιτέρω στοιχείων. Κατόπιν, θα πρέπει να επικοινωνήσει με τους ειδικούς σχετικά με πιθανές διαθέσιμες αποκρυπτογραφήσεις και να ακολουθήσει τις οδηγίες τους για τη συγκεκριμένη επίθεση τύπου ransomware.

Τέλος, θα πρέπει να προσδιορίσει επακριβώς ποιες ηλεκτρονικές συσκευές επηρεάστηκαν από την επίθεση και να τις απομονώσει αμέσως στα σχετικά τμήματα του νοσοκομείου, όπως επίσης και να απενεργοποιήσει τα επηρεαζόμενα συστήματα για

έρευνα και σχετική ανάκτηση δεδομένων, όπως επίσης και να προσδιορίσει τυχόν συσχετισμένα συστήματα που μπορεί να είναι χρήσιμα για περαιτέρω ή συνεχή μη εξουσιοδοτημένη πρόσβαση.

2.8.3 Μετά τη Κρίση

Μετά την κρίση λοιπόν και εφόσον έχει ξεσπάσει» η κρίση με το περιστατικό επίθεσης ασφαλείας τύπου ransomware σε συγκεκριμένα πληροφοριακά συστήματα των συστημάτων υγείας και ιδιαίτερα των νοσοκομείων, ως παράδειγμα, θα πρέπει αμέσως ο διαχειριστής ασφαλείας συστημάτων και δικτύων, να προβεί στο «καθαρισμό» σε όλα τα συστήματα του δικτύου στο νοσοκομείο. Ωστόσο, θα πρέπει να έχει κατά νου πως υπάρχουν ορισμένα διαθέσιμα πακέτα λογισμικού που ισχυρίζονται ότι μπορούν να εξαλείψουν επιθέσεις τύπου ransomware από τα συστήματα ενός δικτύου, αλλά υπάρχουν δύο προβλήματα με αυτό το γεγονός. Το πρώτο είναι ότι δεν μπορεί κανείς να είναι σίγουρος ότι οποιοσδήποτε άλλος εκτός από τον εισβολέα θα μπορέσει να αφαιρέσει εντελώς το ransomware.

Το δεύτερο είναι ότι, ακόμα κι αν το σύστημα καθαριστεί επιτυχώς, ενδέχεται να μην έχει κανείς πρόσβαση στα δεδομένα του στο δίκτυο, Δυστυχώς, δεν υπάρχει ένα εργαλείο αποκρυπτογράφησης για κάθε τύπο ransomware και όσο νεότερο και πιο εξελιγμένο είναι το ransomware, τόσο περισσότερος χρόνος θα χρειαστεί οι ειδικοί για να αναπτύξουν ένα εργαλείο για την αποκωδικοποίηση των αρχείων (Barnett, et al., 2013).

Η κρυπτογράφηση περιλαμβάνει την εκτέλεση ενός κλειδιού αποκρυπτογράφησης και του αρχικού αρχείου μέσω μιας συνάρτησης μαζί για την ανάκτηση του αρχικού αρχείου. Ωστόσο, οι σύγχρονες επιθέσεις χρησιμοποιούν ένα μοναδικό κλειδί για κάθε θύμα, επομένως μπορεί να χρειαστούν χρόνια ακόμη και ένας ισχυρός υπερ-υπολογιστής για να βρει το σωστό κλειδί για ένα μεμονωμένο θύμα. Ακολούθως, ο διαχειριστής ασφαλείας συστημάτων και δικτύων στο νοσοκομείο, θα πρέπει να επιχειρήσει να επαναφέρει τα δεδομένα. Η δημιουργία αντιγράφων ασφαλείας δεδομένων θεωρείται παραδοσιακά ζήτημα συμμόρφωσης με τις τεχνολογίες πληροφορικής, που πραγματοποιείται για να επισημάνετε τα πλαίσια και να περάσουν από ελέγχους. Ωστόσο, θεωρείται όλο και περισσότερο ως θέμα ασφάλειας και για καλό λόγο (Kieny et al., 2017).

Η αποτροπή μιας κυβερνοεπίθεσης δεν είναι πάντα δυνατή, αλλά ο μετριασμός του αντίκτυπου είναι σίγουρα, γι' αυτό η δημιουργία αντιγράφων ασφαλείας πρέπει να θεωρείται ζήτημα ασφάλειας. Μόλις ένας οργανισμός υποστεί μια επίθεση τύπου ransomware, έρχεται αντιμέτωπος με ένα δίλημμα, να πληρώσει τα λύτρα, κάτι που δεν συνιστάται ποτέ, ή να προχωρήσει χωρίς τα δεδομένα. Εάν ο οργανισμός έχει μια κατάλληλη στρατηγική δημιουργίας αντιγράφων ασφαλείας για την αντιμετώπιση των επιθέσεων στον κυβερνοχώρο, μπορεί να ανακάμψει γρήγορα αποκτώντας πρόσβαση στα αντίγραφα ασφαλείας του και να αποφύγει δαπανηρές διακοπές λειτουργίας (Ismailov, 2018).

Ακολούθως, ο διαχειριστής ασφαλείας συστημάτων και δικτύων θα πρέπει να διατηρήσει κρυπτογραφημένα αντίγραφα ασφαλείας δεδομένων με στρατηγική δημιουργίας αντιγράφων ασφαλείας. Επίσης να δημιουργήσει, διατηρήσει και ασκήσει ένα σχέδιο αντιμετώπισης περιστατικών στον κυβερνοχώρο για να συμπεριλάβει μια στρατηγική επικοινωνίας κατά τη διάρκεια συμβάντων με άλλους υπευθύνους στο νοσοκομείο αλλά και στην εταιρεία που έχει αναλάβει την υποστήριξη του συστήματος στο νοσοκομείο.

Στο πλαίσιο αυτό, ο διαχειριστής ασφαλείας συστημάτων και δικτύων, θα πρέπει να επιδιορθώνει τακτικά και να διασφαλίζει ότι οι συσκευές έχουν διαμορφωθεί με ασφάλεια. Να εφαρμόζει την αρχή των ελάχιστων προνομίων σε όλα τα συστήματα και τις συσκευές αλλά και πρωτόκολλα ασφαλείας για να αποτρέψετε επιτυχημένες απόπειρες phishing. Επίσης να πραγματοποιεί έλεγχο της ταυτότητας των εισερχόμενων μηνυμάτων ηλεκτρονικού ταχυδρομείου για να αποτρέψει την καταστρατήγηση email καθώς και να εκτελεί ενός είδους διαχείριση κινδύνου για τρίτους προμηθευτές και διαχειριζόμενους παρόχους υπηρεσιών (επαλήθευση).

Πριν όμως εφαρμοσθούν τα παραπάνω, δεν θα πρέπει ο υπεύθυνος ασφαλείας να ξεχνά πως η πλήρης αποκατάσταση της λειτουργίας μετά από επίθεση με ransoware, χρειάζεται κατά μέσο όρο 23 μέρες για να επανέλθει στη κανονική του λειτουργία το σύστημα. Για το σκοπό αυτό, ο ίδιος επίσης θα πρέπει να προβεί στην εφαρμογή ενός προγράμματος εκπαίδευσης χρηστών στον τομέα της κυβερνοασφάλειας και σε τακτά χρονικά διαστήματα να εκτελεί επαναφορά δεδομένων με κρυπτογραφημένα αντίγραφα ασφαλείας με βάση την ιεράρχηση κρίσιμων υπηρεσιών.

Επίσης να προβαίνει στην συχνή έκδοση επαναφοράς κωδικού πρόσβασης για

όλα τα επηρεαζόμενα συστήματα και χρήστες και να ακολουθεί τις όποιες πρόσθετες τεχνικές οδηγίες από τους ειδικούς. Αντίστοιχα, να παρακολουθεί την κυκλοφορία του δικτύου και να εκτελεί σαρώσεις προστασίας από ιούς για να εντοπίσει τυχόν επίθεση. Τέλος, να αντιμετωπίζει τυχόν σχετικές ευπάθειες και κενά στην ασφάλεια. Μόνο έτσι αν εντοπιστεί μια απειλή, η λύση θα είναι να απομονωθεί το επηρεαζόμενο μηχάνημα, έτσι ώστε το κακόβουλο λογισμικό να μην μπορεί να εξαπλωθεί. Τέλος είναι σημαντικό να σημειωθεί πως το σχέδιο ασφαλείας θα πρέπει να αναθεωρείται κάθε έξι μήνες ή έναν χρόνο, με σκοπό την έγκαιρη και άμεση αντιμετώπιση προβλημάτων στο ηλεκτρονικό σύστημα του νοσοκομείου (Ismailov, 2018).

2.9 Έρευνες που Εντοπίζονται για τις Κυβερνοεπιθέσεις στα Συστήματα Υγείας

Σύμφωνα με τα όσα αναφέρθηκαν παραπάνω, θα λέγαμε πως η κυβερνοασφάλεια είναι ένα ερευνητικό θέμα που απασχολεί αρκετό καιρό τους ειδικούς καις ως προς τις αιτίες και αποτελεσματικούς τρόπους αντιμετώπισής του (Stohl, 2007, Weimann, 2005). Ωστόσο, αυτό το θέμα συζητήθηκε περισσότερο ως μια πιθανή ανησυχία που πρέπει να λαμβάνεται υπόψη κατά την ανάπτυξη σχεδίων ετοιμότητας για απειλές (Squitieri, 2002). Σχετικά τα πιο πρόσφατα χρόνια, όταν αυτές οι ανησυχίες άρχισαν να αναφέρονται εκτενώς, υπήρξε μια αύξηση στη βιβλιογραφία για την υγειονομική περίθαλψη (Dashora, 2011).

Σε μια αναζήτηση της βιβλιογραφίας από τους ερευνητές, αναφέρονται δύο συστηματικές ανασκοπήσεις που δημοσιεύθηκαν για αυτό το θέμα από το 2016, και οι δύο ολοκληρώθηκαν από το Πανεπιστήμιο του Τέξας (Kruse et al., 2017, Luna et al., 2016). Η πρώτη ανασκόπηση βρήκε 19 άρθρα που σχετίζονται με αυτό το θέμα της κυβερνοασφάλειας και της υγειονομικής περίθαλψης (Luna et al., 2016). Αυτή η ανασκόπηση εντόπισε διαφόρους τύπους απειλών, που συζητούνται στη βιβλιογραφία, συμπεριλαμβανομένων των παραβιάσεων δεδομένων, των εσωτερικών και εξωτερικών απειλών, των καταλήψεων και της τρομοκρατίας στον κυβερνοχώρο.

Οι ερευνητές σημείωσαν επίσης ότι οι παραβιάσεις δεδομένων ήταν η πιο κοινή απειλή στον κυβερνοχώρο για την υγειονομική περίθαλψη. Μόνο ένα από τα 19 άρθρα τους εξέταζε επιθέσεις άρνησης υπηρεσίας στην υγειονομική περίθαλψη, αλλά δεν έγινε αναφορά σε κακόβουλη ενέργεια τύπου ransomware σε αυτήν την ανασκόπηση. Η

δεύτερη ανασκόπηση επικεντρώθηκε περισσότερο στις σύγχρονες απειλές που αντιμετωπίζει η υγειονομική περίθαλψη στην ασφάλεια στον κυβερνοχώρο (Kruse et al., 2017).

Η αναθεώρηση αυτή συμπεριέλαβε ως κριτήριο αναζήτησης τον ιό «ransomware», το οποίο δεν συμπεριλήφθηκε στην πρώτη συστηματική αναθεώρηση. Αυτή η αναζήτηση ανέφερε 31 άρθρα που αναλύθηκαν σχετικά. Ένα από τα θέματα που είδαν οι συγγραφείς στην ανασκόπηση του άρθρου τους, ήταν ότι οι απειλές στον κυβερνοχώρο για τους οργανισμούς υγειονομικής περίθαλψης, αυξάνονται και υπάρχει συστηματική έλλειψη ετοιμότητας σε αυτόν τον κλάδο. Ένας από τους περιορισμούς αυτής της κριτικής που σημείωσαν οι συγγραφείς ήταν ότι πολλά από τα άρθρα που επιστράφηκαν, ήταν από πηγές ειδήσεων και όχι από δημοσιεύσεις. Το αποδίδουν αυτό στο γεγονός ότι η επίθεση στο διαδίκτυο τύπου ransomware είναι μια τόσο νέα απειλή για τους οργανισμούς υγειονομικής περίθαλψης.

Ένα άλλο θέμα που καλύπτεται στη βιβλιογραφία, είναι οι λύσεις τεχνολογίας πληροφοριών (IT) σε ζητήματα κυβερνοασφάλειας. Στη περίπτωση αυτή, τα άρθρα συζητούν πιθανά τελικά σημεία ή τρόπους εισόδου σε ένα σύστημα, καθώς και πιθανές λύσεις ή ενημερώσεις κώδικα για να εμποδίσουν οποιονδήποτε να εισέλθει σε ένα σύστημα. Ένα ερευνητικό άρθρο επεσήμανε επίσης ότι μεγάλο μέρος της βιβλιογραφίας καλύπτει το ρόλο της πληροφορικής κατά τη διάρκεια έκτακτων περιστατικών στον κυβερνοχώρο και πώς τα τμήματα πληροφορικής αναλαμβάνουν να επαναφέρουν τα συστήματα και να λειτουργούν μετά από μια επίθεση (Barnett et al., 2013).

Από την άποψη της δημόσιας υγείας και της ετοιμότητας για απειλές, η βιβλιογραφία προσδιορίζει τις απειλές στον κυβερνοχώρο ως πρόβλημα για τον κλάδο της υγειονομικής περίθαλψης, αλλά η έρευνα δεν εμβαθύνει πολύ στο θέμα. Ένα άρθρο που συνδέει τις απειλές στον κυβερνοχώρο απευθείας με τη δημόσια υγεία αναφέρει τις ακριβείς επιπτώσεις στη δημόσια υγεία, καθώς και πιθανές στρατηγικές μετριασμού έναντι αυτού του τύπου απειλών, λείπει από τη βιβλιογραφία (Barnett et al., 2013).

Αυτό το ερευνητικό έργο ελπίζει να προσδιορίσει καλύτερα την απειλή του ransomware κατά της υγειονομικής περίθαλψης, να εντοπίσει ορισμένες βέλτιστες πρακτικές οργανισμών που έχουν αντιμετωπίσει επιθέσεις και να εντοπίσει εμπόδια στην ετοιμότητα στον κυβερνοχώρο εντός των οργανισμών υγειονομικής περίθαλψης.

Απαιτείται μια πιο ισχυρή κατανόηση των απειλών στον κυβερνοχώρο κατά των νοσοκομείων για να βοηθήσει στον εντοπισμό περιοχών για δράση ετοιμότητας και θα καταστήσει τελικά δυνατή τη βελτίωση της ετοιμότητας στον τομέα της υγειονομικής περίθαλψης για την ασφάλεια στον κυβερνοχώρο. Ένα νοσοκομειακό περιβάλλον που είναι πιο ασφαλές έναντι των απειλών στον κυβερνοχώρο είναι ένα ασφαλέστερο περιβάλλον για τους ασθενείς, τους εργαζόμενους και την κοινότητα γενικότερα.

ΚΕΦΑΛΑΙΟ 3^{Ο} – Ορθή Διαχείριση Κυβερνοκινδύνων στο Τομέα της Υγείας

3.1 Ορθή Διαχείριση Κυβερνοκινδύνων στον Τομέα της Υγείας

Αποτελεί γεγονός πως διάφοροι τύποι κατευθυντήριων γραμμών διαχείρισης κινδύνων στον κυβερνοχώρο και λίστες ελέγχου, έχουν δημοσιευθεί στην ακαδημαϊκή βιβλιογραφία, καθώς και σε εκδόσεις του κλάδου και της κυβέρνησης (Blanke & McGrady 2016, KPMG 2015, HCIC Task Force, 2017). Αυτές οι διαφορετικές εκδόσεις έχουν υιοθετήσει μια ποικιλία προσεγγίσεων για τη διαχείριση των κινδύνων στον κυβερνοχώρο.

Στο ένα άκρο υπάρχουν αναλυτικές λίστες ελέγχου με αρκετά λεπτομερείς οδηγίες για τη μείωση των κινδύνων στον κυβερνοχώρο. Παραδείγματα από την άλλη ακραία έκκληση για πολυτομεακή συνεργασία έως τη διαχείριση κινδύνων και άλλες γενικές τακτικές. Αυτές οι διαφορετικές προσεγγίσεις δεν αναιρούν απαραίτητα την ανάγκη για άλλους τύπους καθοδήγησης, καθώς είναι τόσο αντιφατικές στη φύση τους.

Θα μπορούσε να υποστηριχθεί ότι σίγουρα υπάρχει ανάγκη αντιμετώπισης των κινδύνων στον κυβερνοχώρο σε πολλά επίπεδα και ότι οι διαφορετικές προσεγγίσεις στοχεύουν να κάνουν ακριβώς αυτό. Αυτό που γίνεται σαφές μετά τη σύγκριση διαφορετικών τύπων στρατηγικών διαχείρισης κινδύνου είναι η ανάγκη να ληφθούν υπόψη οι τεχνικοί και ανθρώπινοι παράγοντες που εμπλέκονται.

Ως επί το πλείστων, αυτές οι ειδικές οδηγίες για την υγειονομική περίθαλψη είναι πολύ παρόμοιες με τις γενικές εκδόσεις και θα μπορούσαν να εφαρμοστούν στους περισσότερους τύπους οργανισμών. Τούτου λεχθέντος, ορισμένα χαρακτηριστικά και ιδιαιτερότητες του κλάδου της υγειονομικής περίθαλψης θα πρέπει να ληφθούν υπόψη. Η ανάλυση κινδύνου περιλαμβάνει την ανάλυση των τρωτών σημείων και των κινδύνων, η οποία θα περιλαμβάνει ορισμένους από τους ειδικούς παράγοντες του κλάδου της υγειονομικής περίθαλψης.

Η έρευνα πραγματικών γεγονότων στον κυβερνοχώρο στον τομέα της υγειονομικής περίθαλψης είναι επίσης σημαντική για τη διαχείριση αυτών των κινδύνων. Η επίγνωση των πιθανών προβληματικών περιοχών μπορεί να οδηγήσει σε αυξημένη επαγρύπνηση και να βοηθήσει τη διοίκηση να ανταποκριθεί σε αυτούς τους τύπους

κινδύνων (Blanke και McGrady, 2016).

Ο οργανισμός KPMG (2015) έχει προτείνει διάφορα βήματα για τον μετριασμό των κινδύνων στον κυβερνοχώρο στον τομέα της υγειονομικής περίθαλψης, τα οποία θυμίζουν τις αρχές του ERM. Ο οργανισμός θα πρέπει να αναλυθεί από μια ευρεία προοπτική όσον αφορά τους κινδύνους στον κυβερνοχώρο. Οι οργανισμοί υγειονομικής περίθαλψης συνεργάζονται με διάφορες άλλες οντότητες εντός της αλυσίδας αξίας τους, οι οποίες πρέπει επίσης να ληφθούν υπόψη. Θα πρέπει να δεσμεύονται τρίτα μέρη για την κατανόηση και τον μετριασμό των πιθανών κινδύνων που συνδέονται με αυτά.

Η ευαισθητοποίηση για την ασφάλεια στον κυβερνοχώρο, θα πρέπει επίσης να αυξηθεί σε όλα τα επίπεδα ενός οργανισμού και όχι μόνο ως θέμα του τμήματος πληροφορικής. Θα πρέπει επίσης να υπάρχει μια συντονισμένη και καλά προετοιμασμένη ομάδα επιφορτισμένη με την ασφάλεια στον κυβερνοχώρο. Η ασφάλεια στον κυβερνοχώρο θα πρέπει επίσης να ενσωματωθεί στο σχεδιασμό της τεχνολογίας που χρησιμοποιείται στην υγειονομική περίθαλψη.

Οι Blanke και McGrady (2016) προτείνουν να ξεκινήσει κανείς με μια συνολική αξιολόγηση των τρεχουσών πρακτικών ασφαλείας και να διασφαλίσετε ότι συμμορφώνονται με τους κανονισμούς. Οι υπάρχουσες πρακτικές ασφαλείας θα πρέπει να συγκρίνονται με τα πρότυπα βέλτιστων πρακτικών για πιθανά κενά. Ολόκληροι οι οργανισμοί πρέπει να εκπαιδεύονται και να εκπαιδεύονται σε θέματα ασφάλειας, με ιδιαίτερη έμφαση στα πιο σχετικά θέματα.

Η εκπαίδευση πρέπει να επαυξηθεί με τακτικές υπενθυμίσεις για θέματα ασφάλειας στον κυβερνοχώρο. Οι Blanke και McGrady (2016) διαπίστωσαν ότι οι πιο συνηθισμένοι κίνδυνοι στον κυβερνοχώρο στην υγειονομική περίθαλψη σχετίζονται με φορητές συσκευές και κακόβουλα άτομα. Προτείνουν ότι η ασφάλεια και η εκπαίδευση στον κυβερνοχώρο θα πρέπει να επικεντρωθούν ιδιαίτερα σε αυτούς τους δύο προβληματικούς τομείς, καθώς τα γεγονότα στον κυβερνοχώρο συνήθως τα αφορούν.

Επίσης, η χρήση κινητών συσκευών έχει πολλαπλασιαστεί στον τομέα της υγειονομικής περίθαλψης και τα μέτρα που λαμβάνονται για τον περιορισμό των κινδύνων που συνδέονται με τη χρήση αυτών των συσκευών θα πρέπει να σχεδιάζονται σύμφωνα με τον σκοπό για τον οποίο χρησιμοποιούνται. Για παράδειγμα, εάν μια κινητή συσκευή χρησιμοποιείται για το χειρισμό εμπιστευτικών δεδομένων, θα χρειαστεί

κρυπτογράφηση. Η αυτόματη αποσύνδεση και οι προφυλάξεις οθόνης που προστατεύονται με κωδικό πρόσβασης μπορούν επίσης να χρησιμοποιηθούν για τον περιορισμό ορισμένων από τις συντομεύσεις ασφαλείας που ενδέχεται να ληφθούν σε μια ρύθμιση υγειονομικής περίθαλψης. (Blanke & McGrady 2016).

Επίσης οι Filkins et al. (2016) επισημαίνουν ότι αυτοί οι παραδοσιακοί τύποι μέτρων ασφαλείας, όπως οι περίπλοκοι κωδικοί πρόσβασης, καθίστανται ανεπαρκείς για το τρέχον περιβάλλον και ότι η ευαισθητοποίηση των χρηστών είναι ο πιο σημαντικός παράγοντας. Οι κωδικοί πρόσβασης, για παράδειγμα, είναι η πιο συχνά χρησιμοποιούμενη μέθοδος ασφαλούς ελέγχου ταυτότητας, παρόλο που έχει αποδειχθεί ότι είναι ο πιο αδύναμος κρίκος ασφάλειας για περισσότερα από είκοσι χρόνια.

Η διαχείριση κακόβουλων απειλών στον κυβερνοχώρο που σχετίζονται με εμπιστευτικές πληροφορίες είναι μια πρόκληση και θα πρέπει να λαμβάνεται υπόψη σε όλες τις φάσεις της απασχόλησης (Blanke & McGrady 2016). Το προφίλ προσωπικού του κλάδου της υγειονομικής περίθαλψης μπορεί να το κάνει αυτό δύσκολο, επειδή χρησιμοποιούνται πολλοί διαφορετικοί τύποι υπαλλήλων και εθελοντών (HCIC Task Force, 2017).

Η Task Force HCIC (2017) έχει καταλήξει σε έξι επιταγές για τη διαχείριση των κινδύνων στον κυβερνοχώρο στην υγειονομική περίθαλψη:

1. Οι προσδοκίες, η διακυβέρνηση και η ηγεσία του κλάδου της υγείας στον κυβερνοχώρο πρέπει να εξορθολογιστούν και να καθοριστούν.

2. Αναφέρεται σχετική ανθεκτικότητα

3. Θα πρέπει να αναπτυχθεί η ικανότητα του εργατικού δυναμικού της υγειονομικής περίθαλψης για τη διασφάλιση της ευαισθητοποίησης και των ικανοτήτων για την ασφάλεια στον κυβερνοχώρο. βιομηχανία. Αυτή η λίστα επιταγών συνοδεύεται από πολλές συστάσεις που καλύπτουν μια σειρά θεμάτων και των σχετικών μερών. Αυτή η κατευθυντήρια γραμμή μπορεί να θεωρηθεί ως μία από τις πιο ολιστικές και ευρύτερες εκδόσεις των διαθέσιμων δημοσιεύσεων.

Η Ομάδα Εργασίας HCIC (2017) έχει εργαστεί σε συνεργασία με εκπροσώπους από άλλες βιομηχανίες υποδομών ζωτικής σημασίας για να αποκτήσει καλύτερη κατανόηση των κινδύνων στον κυβερνοχώρο και να μάθει τις βέλτιστες πρακτικές. Ενώ

η υγειονομική περίθαλψη μοιράζεται ορισμένα κοινά χαρακτηριστικά σχετικά με αυτούς τους κινδύνους με βιομηχανίες όπως η χρηματοδότηση και η ενέργεια, αποκαλύφθηκαν επίσης ορισμένες μοναδικές πτυχές.

Αυτά πρέπει να λαμβάνονται υπόψη στις στρατηγικές διαχείρισης κινδύνων στον κυβερνοχώρο και να καθιστούν δύσκολη την υιοθέτηση βέλτιστων πρακτικών με την ακριβή τους μορφή από άλλους κλάδους. Τα βασικά ευρήματα περιλαμβάνουν τα ακόλουθα: οι οργανισμοί υγειονομικής περίθαλψης ποικίλλουν σημαντικά ως προς το μέγεθος και τους τύπους δραστηριοτήτων. Υπάρχει επίσης μεγάλη πίεση για ψηφιοποίηση των λειτουργιών, ενώ αναγκάζεται να βασιστεί σε παλαιού τύπου συστήματα. Οι απειλές τείνουν να γίνονται αντιληπτές με σημαντικές καθυστερήσεις.

Η υγειονομική περίθαλψη χρησιμοποιεί επίσης πολλά πολύ διασυνδεδεμένα συστήματα. Συγκρίνοντας διαφορετικούς κλάδους, είναι δυνατό να επισημανθούν οι μοναδικές πτυχές του καθενός. Αυτές οι πληροφορίες μπορεί να είναι χρήσιμες για την τροποποίηση και την εφαρμογή βέλτιστων πρακτικών. Οι Webb και Dayal (2017) υποστηρίζουν ότι η ευθύνη για τη διαχείριση των κινδύνων στον κυβερνοχώρο για την υγειονομική περίθαλψη μοιράζεται μεταξύ διαφόρων ενδιαφερομένων. Αυτή η άποψη έχει εκφράσει η Υπηρεσία Τροφίμων και Φαρμάκων των ΗΠΑ (FDA) και η Αυστραλιανή Υπηρεσία Θεραπευτικών Προϊόντων (TGA).

Ο μετριασμός αυτών των κινδύνων, είναι σημαντικός για όλους τους εμπλεκόμενους φορείς, συμπεριλαμβανομένων των ασθενών, των παρόχων και των κατασκευαστών. Η επιτυχής διαχείριση κινδύνων στον κυβερνοχώρο θα πρέπει να περιλαμβάνει όλους αυτούς τους ενδιαφερομένους, καθένας από τους οποίους εργάζεται με τις αντίστοιχες ικανότητές του σε μια συνεργασία.

Οι κατασκευαστές ιατροτεχνολογικών προϊόντων θα πρέπει να χρησιμοποιούν μια προσέγγιση κύκλου ζωής για την αξιολόγηση κινδύνου για τα προϊόντα τους. Οι εκτιμήσεις ασφαλείας και οι εκτιμήσεις κινδύνου θα πρέπει να διατηρούνται ενημερωμένες. Αυτές οι αρχές ισχύουν και για τους παρόχους υγειονομικής περίθαλψης. Ενώ οι κατασκευαστές και οι πάροχοι υπηρεσιών έχουν τη μεγαλύτερη υποχρέωση στη διαχείριση κινδύνου, οι τελικοί χρήστες θα πρέπει επίσης να διαδραματίσουν ρόλο. Αυτό περιλαμβάνει την εγκατάσταση ενημερώσεων κατά την κυκλοφορία τους. Η κυβέρνηση έχει επίσης το μερίδιο των ευθυνών της, όπως η κατάλληλη καθοδήγηση και ρύθμιση.

Μια πτυχή της διαχείρισης κινδύνων στον κυβερνοχώρο, είναι η προετοιμασία για τα χειρότερα σενάρια, έτσι ώστε ένας οργανισμός να είναι σε θέση να λειτουργεί εκτός σύνδεσης εάν συμβεί ένα σημαντικό συμβάν στον κυβερνοχώρο. Ορισμένοι έχουν λάβει μέτρα για να μειώσουν την εξάρτησή τους από τις διαδικτυακές λειτουργίες.

Ορισμένοι πάροχοι υγειονομικής περίθαλψης στη Γερμανία και τις ΗΠΑ, έχουν λάβει αυτήν την πορεία δράσης, όπου ορισμένα κρίσιμα συστήματα τίθενται εκτός σύνδεσης εάν δεν απαιτείται σύνδεση. Διατηρούνται επίσης μέθοδοι με στυλό και χαρτί των προηγούμενων ετών, προκειμένου να διασφαλιστεί ότι ο οργανισμός είναι σε θέση να λειτουργήσει ακόμη και αν δεν υπάρχουν διαθέσιμες ψηφιακές λειτουργίες. (Herbolzheimer, 2016).

Εταιρείες τεχνολογίας όπως η IBM έχουν επίσης αναπτύξει εργαλεία για τη διαχείριση των κινδύνων στον κυβερνοχώρο, τα οποία έχουν χρησιμοποιηθεί στον κλάδο της υγειονομικής περίθαλψης. Η πλατφόρμα γνωστικών υπολογιστών Watson έχει χρησιμοποιηθεί για την αξιολόγηση των απειλών ασφαλείας και την ανάλυση αναφορών φυσικής γλώσσας σε θέματα όπως η ευπάθεια λογισμικού. Αυτό το προϊόν φάσης βήτα έχει χρησιμοποιηθεί στο Ιατρικό Κέντρο του Πανεπιστημίου του Ρότσεστερ.

Η Watson μπορεί να χρησιμοποιήσει πολλούς τύπους πληροφοριών, συμπεριλαμβανομένων των εκθέσεων του FDA και του κατασκευαστή ιατρικών συσκευών, των ερευνητικών εργασιών και της ηλεκτρονικής γραφής, προκειμένου να προσφέρει πληροφορίες σχετικά με την ασφάλεια στον κυβερνοχώρο. Εφαρμογές προγνωστικής ανάλυσης έχουν επίσης αναπτυχθεί για τον τομέα της υγειονομικής περίθαλψης. Τα προϊόντα γνωστικών υπολογιστών αναπτύσσονται ακόμη, αλλά ελπίζουμε ότι θα βοηθήσουν στην ανάλυση των τεράστιων ποσοτήτων δεδομένων που αντιμετωπίζουν οι ειδικοί σε θέματα ασφάλειας και θα τους βοηθήσουν να λαμβάνουν πιο ενημερωμένες αποφάσεις. Αυτές οι νέες εφαρμογές μπορεί να είναι απαγορευτικά ακριβές, γεγονός που μπορεί να εμποδίσει την εγκατάστασή τους (Rubenfire, 2017).

Οι βιομηχανίες που αποθηκεύουν και βασίζονται σε μεγάλους όγκους προσωπικών δεδομένων, όπως η υγειονομική περίθαλψη, έχουν θεωρηθεί ως οι πιο πιθανοί υποψήφιοι για να αγοράσουν ασφάλιση κινδύνου στον κυβερνοχώρο (Allianz 2015, 25) Μια έρευνα του Ινστιτούτου Ponemon (2013, 13) διαπίστωσε ότι το 29 % των ερωτηθέντων στον κλάδο της υγειονομικής περίθαλψης και της φαρμακευτικής βιομηχανίας είχε προμηθευτεί ένα ασφαλιστήριο συμβόλαιο στον κυβερνοχώρο.

Αντιπροσώπευαν τον κλάδο με τα δεύτερα χαμηλότερα ποσοστά ασφάλισης στον κυβερνοχώρο. Για σύγκριση, τα υψηλότερα ποσοστά ήταν στην τεχνολογία και το λογισμικό (41%) και τα χαμηλότερα στον δημόσιο τομέα (19%). Παρόλο που οι οργανισμοί υγειονομικής περίθαλψης ήταν λιγότερο πιθανό να έχουν αγοράσει ένα ασφαλιστήριο συμβόλαιο στον κυβερνοχώρο, ήταν από τους πιο ικανοποιημένους με το προϊόν. Τα ποσοστά ασφάλισης στον κυβερνοχώρο που προτείνονται από το Ινστιτούτο Ponemon (2013) είναι πολύ διαφορετικά από τα ευρήματα του Willis (2013).

Αυτή η μελέτη διαπίστωσε ότι το 1% των οργανισμών υγειονομικής περίθαλψης ανέφερε ότι αγόρασε ασφάλεια στον κυβερνοχώρο. Ωστόσο, σχολιάζουν ότι αυτό το εύρημα προκαλεί έκπληξη, δεδομένης της εμπειρίας τους στην υγειονομική περίθαλψη ως ένας από τους μεγαλύτερους αγοραστές αυτών των ασφαλιστηρίων συμβολαίων. Οι συγγραφείς προτείνουν ότι αυτός ο χαμηλός αριθμός μπορεί να οφείλεται σε ελλιπή αναφορά. Ο ασφαλιστικός κλάδος έχει αναπτύξει ένα σειρά προϊόντων και υπηρεσιών ειδικά για οργανισμούς υγειονομικής περίθαλψης.

3.2 Μέτρα Προστασίας που Πρέπει να Εφαρμόζουν οι Φορείς Υγείας για την Προστασία από Κυβερνοεπιθέσεις

Σύμφωνα με τα όσα αναφέρθηκαν παραπάνω, θα λέγαμε πως οι φορείς στα συστήματα υγείας, θα πρέπει να εφαρμόζουν συγκεκριμένα μέτρα προστασίας από κυβερνοεπιθέσεις, ως εξής (Ismailov, 2018)

Ασφαλής Επίβλεψη Σημείων Πρόσβασης σε Ευαίσθητες Πληροφορίες

Τα σημεία πρόσβασης σε *ευαίσθητες* πληροφορίες αποτελούν πιθανή πηγή επιθέσεων στον κυβερνοχώρο. Εκμεταλλευόμενοι τα τρωτά σημεία τους, οι χάκερ μεταδίνουν έναν ιό για να επιβραδύνουν τη λειτουργία στο δίκτυο, να έχουν πρόσβαση σε κρίσιμες πληροφορίες υγείας ή να κάνουν το σύστημα πιο ευάλωτο στο μέλλον. Το κακόβουλο λογισμικό μπορεί να εισέλθει από οποιαδήποτε ευάλωτη τοποθεσία στο δίκτυο ή στο λειτουργικό σύστημα.

Ένας εργαζόμενος μπορεί εν αγνοία του να κάνει κλικ σε ένα αρχείο, να *κατεβάσει* μη εξουσιοδοτημένο λογισμικό ή να *ανεβάσει* ένα μολυσμένο έγγραφο. Επίσης, όταν δεν χρησιμοποιούνται ισχυροί ασφαλείς κωδικοί πρόσβασης, δημιουργείται ένα εύκολο σημείο πρόσβασης για τους χάκερ. Επιπλέον, το ιατρικό λογισμικό και οι διαδικτυακές εφαρμογές που χρησιμοποιούνται για την αποθήκευση δεδομένων ασθενών βρέθηκαν να περιέχουν πολυάριθμα τρωτά σημεία. Στατιστικά στοιχεία για την ασφάλεια στον κυβερνοχώρο του τομέα υγείας από το Kaspersky Security Bulletin αποκαλύπτει τρωτά σημεία σε σημεία πρόσβασης περίπου 1.500 συσκευών που χρησιμοποιούν οι επαγγελματίες υγείας για την επεξεργασία εικόνων ασθενών.

Απόκτηση Γνώσεων των Εργαζομένων για Αντιμετώπιση Ιών Τύπου Ransomware

Μια επίθεση ransomware είναι ένας συγκεκριμένος τύπος κακόβουλου λογισμικού που απειλεί να *μπλοκάρει* έναν υπολογιστή ή ένα ολόκληρο δίκτυο εάν δεν καταβληθεί ένα συγκεκριμένο χρηματικό ποσό. Η ανταμοιβή δεν είναι απαραίτητα υψηλός αριθμός. Ακόμη και η διεκδίκηση μερικών εκατοντάδων δολαρίων από μια επιχείρηση μπορεί να είναι εύκολο χρήμα για έναν χάκερ και πιο διαχειρίσιμο για άτομα ή εταιρείες για να αποκτήσουν ξανά πρόσβαση στους υπολογιστές τους. Για αυτό είναι απαραίτητο να αυξηθεί η γνώση του προσωπικού και των χρηστών του εξοπλισμού για να εντοπίσουν ransomware και να μάθουν πώς να ενεργούν εάν είναι στόχος μιας τέτοιας επίθεσης.

Δημιουργία Πολιτικής Διαχείρισης Ασφαλείας για Επιθέσεις Τύπου Ransomware

Ένας υπολογιστής με περιορισμένη πρόσβαση, δεν προκαλεί απαραίτητα μια βλάβη. Ωστόσο, ο κίνδυνος να μην είναι δυνατή η πρόσβαση στα αρχεία όπου είναι αποθηκευμένα τα δεδομένα, μπορεί να είναι επικίνδυνος για τη θεραπεία του ασθενούς. Όταν ένα τέτοιο συμβεί περιστατικό, οι εργαζόμενοι θα πρέπει να επικοινωνήσουν αμέσως με την IT. Αυτό θα πρέπει να είναι μέρος της εκπαίδευσης τους για την ασφάλεια. Θα πρέπει να ακολουθούν τις διαδικασίες του οργανισμού υγειονομικής περίθαλψης όταν βλέπουν ένα μήνυμα ransomware, αντί να προσπαθούν να επιλύσουν οι ίδιοι το πρόβλημα.

Ορθή Εκπαίδευση Εργαζομένων

Για να ελαχιστοποιηθεί το ανθρώπινο λάθος, οι διαχειριστές συστημάτων πρέπει να εκπαιδεύουν συνεχώς όλο το προσωπικό σε επικίνδυνες και «περίεργες» συμπεριφορές. Αυτό περιλαμβάνει διάφορα στοιχεία, από τη λήψη μη εξουσιοδοτημένου λογισμικού και τη δημιουργία αδύναμων κωδικών πρόσβασης έως την επίσκεψη σε ιστότοπους με κακόβουλο περιεχόμενο ή τη χρήση μολυσμένων συσκευών. Οι εργαζόμενοι πρέπει να εκπαιδεύονται για το πώς να αναγνωρίζουν κακόβουλα email, απειλές και παράνομους και ύποπτους ιστότοπους, προκειμένου να αποφύγουν επιθέσεις. Η εκπαίδευση θα πρέπει να διεξάγεται τακτικά ή εξατομικευμένη για διαφορετικές ομάδες εργαζομένων.

Δημιουργία και Ενημερώσεις στις Πολιτικές Διαχείρισης Κινδύνων Ασφαλείας

Οι εργαζόμενοι στα συστήματα υγείας θα πρέπει να έχουν διάφορα προνόμια πρόσβασης στο εταιρικό δίκτυο. Σε ένα νοσοκομείο, οι νοσηλευτές μπορεί να χρειαστεί να μοιραστούν πληροφορίες με το άλλο προσωπικό του τμήματός τους, αλλά δεν είναι απαραίτητο να το δουν άλλα τμήματα. Οι επισκέπτες γιατροί έχουν πρόσβαση μόνο στις πληροφορίες των ασθενών τους.

Τα προνόμια ασφαλείας πρέπει να παρακολουθούν για μη εξουσιοδοτημένη πρόσβαση ή προσπάθειες σε οποιοδήποτε επίπεδο. Στο πλαίσιο αυτό, η Digital Guardian προτείνει αρχικά εκπαίδευση, ακολουθούμενη από τον περιορισμό συγκεκριμένων εφαρμογών, περιοχών και δεδομένων υγειονομικής περίθαλψης ασθενών. Συνιστά επίσης να απαιτείται έλεγχος ταυτότητας πολλαπλών παραγόντων, κάτι που αποτελεί πρόσθετο επίπεδο προστασίας.

Οι ανησυχίες των ασθενών σχετικά με την ασφάλεια των δεδομένων στην υγειονομική περίθαλψη, θα πρέπει να λαμβάνονται υπόψη κατά τη δημιουργία πιο ασφαλών συστημάτων ή όταν τα πλαίσια ασφάλειας στον κυβερνοχώρο βελτιώνονται μετά την επίθεση σε νοσοκομείο. Οι ασθενείς δεν θέλουν να ανησυχούν για την ασφάλεια των δεδομένων, επομένως οι διαχειριστές συστημάτων πρέπει να επενδύσουν σε πρωτοβουλίες ασφάλειας (Kieny et al., 2017).

Προστασία στα Δεδομένα Υγείας σε «Έξυπνες» Συσκευές

Οι επιτραπέζιοι και φορητοί υπολογιστές, τα κινητά τηλέφωνα και όλες οι ιατρικές συσκευές, ειδικά αυτές που είναι συνδεδεμένες στο δίκτυο και θα πρέπει να παρακολουθούνται και να διαθέτουν προστασία από ιούς, *τείχος* προστασίας ή άλλη παρόμοια προστασία. Σήμερα, τα ιατρικά κέντρα διαθέτουν άλλες συνδεδεμένες ηλεκτρονικές συσκευές, όπως ιατρικές συσκευές, όπως οθόνες ινσουλίνης που συγχρονίζουν εξ αποστάσεως τις πληροφορίες των ασθενών απευθείας στο tablet ενός γιατρού ή μιας νοσοκόμας. Πολλές από αυτές τις διασυνδεδεμένες συσκευές μπορεί ενδεχομένως να παραβιαστούν, να καταστραφούν ή να απενεργοποιηθούν, τα οποία όλα μπορούν να επηρεάσουν την υγεία του ασθενούς.

Ενσωμάτωση Δεδομένων στο I-Cloud

Το I-Cloud παρέχει μια ασφαλή και ευέλικτη λύση για την αποθήκευση δεδομένων υγειονομικής περίθαλψης και παρέχει έναν τρόπο στους οργανισμούς να διαχειρίζονται τα δεδομένα τους. Οι λύσεις που βασίζονται στο i-cloud και η ανάκτηση σε περίπτωση επίθεσης, διασφαλίζουν ότι τα αρχεία ασθενών είναι προσβάσιμα ακόμη και σε περίπτωση παραβίασης ή διακοπής της όποιας εργασίας.

Σε συνδυασμό με την επιλογή ελέγχου εισαγωγής δεδομένων, παρέχεται το απαιτούμενο επίπεδο ασφάλειας. Με το i-cloud, ένας οργανισμός υγειονομικής περίθαλψης δεν χρειάζεται να επενδύσει πολλά σε κρίσιμες υποδομές αποθήκευσης δεδομένων. Η αποθήκευση cloud επιτρέπει σημαντική μείωση του κόστους πληροφορικής, καθώς δεν απαιτείται επένδυση σε εξοπλισμό. Το Cloud προσφέρει επίσης ένα σημαντικό επίπεδο ευελιξίας όταν αλλάζουν οι ανάγκες αποθήκευσης δεδομένων ενός ιδρύματος.

Επίλογος – Συμπεράσματα

Αποτελεί γεγονός πως οι οργανισμοί θα έχουν διαφορετικές στάσεις σχετικά με τον κίνδυνο, τον τρόπο αποδοχής του κινδύνου και τον τρόπο διαχείρισης του κινδύνου. Ακόμα κι αν δύο διαφορετικές οντότητες χρησιμοποιούν την ίδια διαδικασία διαχείρισης κινδύνου, τα τελικά αποτελέσματα δεν θα είναι τα ίδια, επειδή το πλαίσιο και το περιβάλλον ενός δεδομένου οργανισμού θα αντικατοπτρίζονται στον τρόπο με τον οποίο διεξάγεται η διαδικασία. Για παράδειγμα, μια διαδικασία διαχείρισης κινδύνου συνήθως περιλαμβάνει τον καθορισμό των στόχων.

Οι στόχοι διαχείρισης κινδύνου ενός νοσοκομείου, θα είναι διαφορετικοί από εκείνους ενός σταθμού ηλεκτροπαραγωγής. Το ίδιο μπορεί να ειπωθεί για την αξιολόγηση των κινδύνων, η οποία θα επηρεαστεί από τους τύπους των πράξεων που λαμβάνουν χώρα και από το πόσο σημαντικό είναι ένα συγκεκριμένο είδος κινδύνου σε αυτό το συγκεκριμένο πλαίσιο.

Υπάρχουν διαφορετικές διαστάσεις στην ασφάλεια των πληροφοριών, όλες οι οποίες μπορούν να θεωρηθούν πολύ απαραίτητες. Αλλά μπορεί να μην είναι δυνατό να τεθούν τα πάντα νούμερο ένα προτεραιότητα. Στην υγειονομική περίθαλψη, η ακρίβεια των πληροφοριών είναι ιδιαίτερα σημαντική. Οργανισμοί σε διαφορετικούς κλάδους μπορεί να έχουν κάποια άλλη πτυχή της ασφάλειας στον κυβερνοχώρο ως πρωταρχικής σημασίας.

Τα βασικά στοιχεία των κινδύνων στον κυβερνοχώρο και η διαχείρισή τους, φαίνεται να είναι τα ίδια σε διαφορετικούς κλάδους της βιομηχανίας. Αυτά πρέπει να χρησιμοποιηθούν με έναν συγκεκριμένο τρόπο οργάνωσης και όχι όπως είναι. Οι λειτουργίες και οι επικρατούσες συνθήκες θα πρέπει να λαμβάνονται υπόψη κατά τη διαχείριση του κινδύνου. Με την υγειονομική περίθαλψη, αυτά μπορεί να περιλαμβάνουν τη φύση 24-7 της παροχής υπηρεσιών και τα υπάρχοντα παλαιού τύπου συστήματα. Οι συνθήκες υπό τις οποίες λειτουργούν πολλοί οργανισμοί υγειονομικής περίθαλψης δεν

είναι πραγματικά μοναδικές για την υγειονομική περίθαλψη, καθώς αυτές μπορούν να φανούν εύκολα σε άλλους τομείς είναι καλές.

Αντί να έχει αντίκτυπο στις πραγματικές αρχές ή διαδικασίες που περιβάλλουν τη διαχείριση κινδύνου, το πλαίσιο της υγειονομικής περίθαλψης διαπιστώθηκε ότι αυξάνει την ανάγκη για διαχείριση κινδύνου. Οι οργανισμοί υγειονομικής περίθαλψης πρέπει να αντιμετωπίσουν τους κινδύνους στον κυβερνοχώρο, όπως και οι περισσότεροι άλλοι οργανισμοί. Τρεις λόγοι βρέθηκαν στα δεδομένα που υποστηρίζουν την ιδέα ότι η διαχείριση κινδύνων στον κυβερνοχώρο πρέπει να διαδραματίσει σημαντικό ρόλο στον τομέα της υγειονομικής περίθαλψης.

Πρώτον, οι επιπτώσεις της αποτυχίας διαχείρισης κινδύνων στον κυβερνοχώρο μπορεί να έχουν σημαντικές συνέπειες στους ασθενείς και τους ίδιους τους οργανισμούς. Τα συμβάντα στον κυβερνοχώρο μπορεί να καταστήσουν έναν οργανισμό υγειονομικής περίθαλψης ανίκανο να εκτελέσει το πρωταρχικό του καθήκον που είναι η παροχή υπηρεσιών υγειονομικής περίθαλψης ή να το καταστήσει πολύ πιο δύσκολο.

Η επίδραση αυτού του γεγονότος στους ασθενείς και στην κοινωνία γενικότερα, είναι προφανώς πολύ κακή. Πραγματοποιημένα συμβάντα στον κυβερνοχώρο μπορούν να οδηγήσουν σε μυριάδες αρνητικά αποτελέσματα και για τους παρόχους υγειονομικής περίθαλψης, όπως οικονομικές επιπτώσεις και απώλεια φήμης. Ιδιαίτερα στην εποχή της αυξημένης ελευθερίας των ασθενών να επιλέγουν τον πάροχο υγειονομικής περίθαλψης, η φήμη ενός νοσοκομείου είναι πολύ πολύτιμη.

Η διαχείριση κινδύνων στον κυβερνοχώρο στην υγειονομική περίθαλψη, δεν έχει μελετηθεί εκτενώς, αλλά τα δεδομένα από αυτή τη διατριβή υποδηλώνουν ότι ο τομέας δεν είναι ο πιο σημαντικός παράγοντας όσον αφορά τη διαχείριση του κινδύνου στον κυβερνοχώρο. Αντί να απαιτούνται συγκεκριμένες μέθοδοι για τη διαχείριση του κινδύνου στον κυβερνοχώρο, οι γενικές αρχές διαχείρισης κινδύνου μπορούν να χρησιμοποιηθούν αποτελεσματικά από τον τομέα της υγειονομικής περίθαλψης.

Τα ευρήματα υποδεικνύουν ότι ορισμένα χαρακτηριστικά που είναι κοινά μεταξύ των οργανισμών υγειονομικής περίθαλψης, όπως τα παλαιού τύπου συστήματα, θα πρέπει να λαμβάνονται υπόψη στη διαχείριση κινδύνων στον κυβερνοχώρο. Θα μπορούσε να υποστηριχθεί ότι ορισμένα χαρακτηριστικά ενός οργανισμού ή του επιχειρησιακού του περιβάλλοντος και όχι του τομέα, σχετίζονται περισσότερο με τους

κινδύνους στον κυβερνοχώρο.

Η ενασχόληση με παλαιού τύπου συστήματα και ταχέως εξελισσόμενη τεχνολογία δεν περιορίζεται στον τομέα της υγειονομικής περίθαλψης. Όλοι οι τύποι οργανισμών που αντιμετωπίζουν αυτές τις προκλήσεις θα πρέπει να αντιμετωπίσουν τους σχετικούς κινδύνους, αλλά η ακριβής φύση αυτών των κινδύνων και η σημασία τους θα διαφέρουν στους διάφορους κλάδους. Πολλοί τύποι υποδομών ζωτικής σημασίας, όπως οι σταθμοί ηλεκτροπαραγωγής και η παροχή νερού έχουν επίσης εξαρτήματα που μπορούν να ταξινομηθούν ως παλαιού τύπου συστήματα που βασίζονται όλο το εικοσιτετράωρο.

Όπως συμβαίνει με τους οργανισμούς υγειονομικής περίθαλψης, αυτά τα συστήματα πρέπει να μπορούν να λειτουργούν στο τρέχον περιβάλλον τους και η αποτυχία να το πράξουν θα προκαλούσε σημαντική ζημιά. Η σύγκριση της σημασίας της αξιόπιστης ενέργειας, του νερού και της υγειονομικής περίθαλψης είναι πέρα από το πεδίο εφαρμογής αυτής της διατριβής, αλλά περιττό να πούμε ότι είναι όλα σημαντικά για τη λειτουργία της σύγχρονης κοινωνίας.

Η διαχείριση κινδύνων στον κυβερνοχώρο, είναι σαν να στοχεύει κανείς σε έναν κινούμενο στόχο. Το πιο σύγχρονο σύστημα σήμερα θα γίνει ξεπερασμένο κάποια στιγμή στο μέλλον. Αυτή τη στιγμή, δεν έχουμε τρόπο να γνωρίζουμε τι είδους απρόβλεπτους κινδύνους στον κυβερνοχώρο θα έχουν αύριο οι σημερινές καινοτομίες. Ο εξοπλισμός υγειονομικής περίθαλψης και τα συστήματα πληροφοριών έχουν σχεδιαστεί με πολλούς στόχους κατά νου. Βασικό χαρακτηριστικό της τεχνολογικής ανάπτυξης σε αυτόν τον τομέα θα πρέπει να είναι η ανθεκτικότητα, ώστε να μπορεί να προσαρμοστεί στο μόνο σενάριο που μπορούμε να προβλέψουμε με ακρίβεια: τη συνεχή αλλαγή.

Μία από τις προκλήσεις στη διαχείριση κινδύνων στον κυβερνοχώρο της υγειονομικής περίθαλψης, περιλαμβάνει τον χρόνιο δημοσιονομικό περιορισμό, ο οποίος δεν είναι μοναδικός για την υγειονομική περίθαλψη. Με τις ανάγκες υγειονομικής περίθαλψης που προβλέπεται να αυξηθούν στο μέλλον, οι οικονομικοί παράγοντες ενδέχεται να γίνουν ακόμη πιο σημαντικοί.

Οι κίνδυνοι στην υγειονομική περίθαλψη έχουν επίσης προβλεφθεί να αυξηθούν τα επόμενα χρόνια. Εάν αυτά τα συμβάντα γίνουν πιο κοινά, πιθανότατα θα εγείρουν περισσότερη συζήτηση στον δημόσιο τομέα. Αυτή η συζήτηση και η προσοχή ενδέχεται

να επηρεάσουν τον τρόπο διαχείρισης των κινδύνων στον κυβερνοχώρο στην υγειονομική περίθαλψη και πώς αντιμετωπίζονται στην κοινωνία γενικότερα.

Η διαχείριση κινδύνων στον κυβερνοχώρο στο πλαίσιο της υγειονομικής περίθαλψης, ή οποιουδήποτε άλλου κλάδου για αυτό το θέμα, είναι ενδιαφέρουσα επειδή περιλαμβάνει ορισμένες ιδιότητες που μπορούν σχεδόν να θεωρηθούν ως αντίθετες με την πρώτη ματιά. Αυτά περιλαμβάνουν τη μη συνάφεια των εθνικών συνόρων και γλωσσών στον κόσμο του κυβερνοχώρου, ενώ έχουν μεγάλη επιρροή για οργανισμούς και άτομα που δραστηριοποιούνται σε αυτόν. Τα γεγονότα στον κυβερνοχώρο θα έχουν πιθανώς μια προέλευση από κάπου, αλλά αυτή η προέλευση μπορεί να είναι μια ασήμαντη πτυχή του ίδιου του γεγονότος. Φυσικά, η προέλευση ενός συμβάντος στον κυβερνοχώρο μπορεί να έχει επιπτώσεις, όπως πολιτικές προεκτάσεις, αλλά αυτό μπορεί να μην επηρεάζει απαραίτητα το ίδιο το γεγονός.

Οι εκτιμήσεις που σχετίζονται με τη γεωγραφία των κινδύνων στον κυβερνοχώρο ενδέχεται να έχουν δευτερεύουσα σημασία στη διαχείρισή τους. Ωστόσο, οι οργανισμοί υπάρχουν σε έναν κόσμο όπου τα ζητήματα που σχετίζονται με την εθνική καταγωγή είναι πολύ σχετικά, καθώς υπαγορεύουν ορισμένες από τις βασικές παραμέτρους λειτουργίας, όπως η ρύθμιση.

Μια άλλη ιδέα που φαίνεται να ενσωματώνει κάποιου είδους αντίθεση, είναι η ανθρώπινη και η τεχνολογική πτυχή των κινδύνων στον κυβερνοχώρο. Η διαίρεση των φαινομένων σε ανθρώπινα και τεχνολογικά αντίστοιχα μπορεί να είναι διαισθητική, αλλά η διεπαφή αυτών των στοιχείων μπορεί στην πραγματικότητα να είναι ακόμη πιο σημαντική.

Συγκεκριμένα παραδείγματα αυτού είναι οι τεχνικές διαχείρισης κινδύνων στον κυβερνοχώρο που επικεντρώνονται στη μείωση του κινδύνου μέσω του τρόπου με τον οποίο οι άνθρωποι χρησιμοποιούν διάφορες τεχνολογίες. Στην ιδανική περίπτωση, οι τεχνικές λύσεις για τη διαχείριση κινδύνων στον κυβερνοχώρο θα επωφελούνταν από την ανθρώπινη συμπεριφορά και τη γνώση, αντί να λειτουργούν εναντίον τους.

Η τρίτη και τελευταία ενδιαφέρουσα πτυχή των κινδύνων στον κυβερνοχώρο στην υγειονομική περίθαλψη (και γενικά) είναι η συγχώνευση του παλιού και του νέου. Σε ένα πλαίσιο υγειονομικής περίθαλψης, αυτό ενσωματώνεται από τον παλιό εξοπλισμό δεκαετιών που θα πρέπει να παραμείνει ως έχει, αλλά πρέπει με κάποιο τρόπο να

προσαρμοστεί για να αντιμετωπίσει το νέο του περιβάλλον. Οι οργανισμοί που υπάρχουν εδώ και πολύ καιρό υιοθετούν νέες διαδικασίες και τεχνολογίες με γρήγορους ρυθμούς. Μπορεί να μην είναι οικονομικά εφικτό ή λογικό να ενημερώνονται τα πάντα ταυτόχρονα, επομένως αυτός ο εκσυγχρονισμός θα πρέπει να λάβει υπόψη τα υπάρχοντα συστήματα και εξοπλισμό.

Βιβλιογραφία

Αγγλική Βιβλιογραφία

Ayala, L. (2016). Cybersecurity for hospitals and healthcare facilities: A guide to detection and prevention. Berkely: Apress.

Barbera, J.A., Yeatts, D.J., & Macintyre, A.G. (2009). Challenge of hospital preparedness: analysis and recommendations. Disaster Med Pub Health Prep, 3(S1), S74-82.

Barnett, D.J., Snell, T.K., Lord, R.K., Jenkins, C.J., Terbush, J.W., & Burke, T.A. (2013). Cyber security threats to public health. World Med Health Policy, 5(1), 37-46.

Becker's Hospital Review (2016, Jun 1) 93% of phishing emails contain ransomware. Becker's Hospital Review, Retrieved from https://www.beckershospitalreview.com/healthcare- information-technology/93-of-phishing-emails-contain-ransomware.html

Cagliuso, N. V. (2014a). Stakeholders' experiences with US hospital emergency preparedness: Part 1. J Bus Contin Emer Plan, 8(2), 156-168.

Chappell, B. and Neuman, S. (2017, Dec 19). U.S. says North Korea 'directly responsible' for wannacry ransomware attack. NPR. Retrieved from

https://www.npr.org/sections/thetwo- way/2017/12/19/571854614/u-s-says-north-korea-directly-responsible-for-wannacry- ransomware-attack

Chung, E. (2016, Mar 24). Ontario hospital website may have infected visitors with ransomware, security firm says. CBC News. Retrieved from http://www.cbc.ca/news/technology/norfolk- general-hospital-hack-1.3504229

Dashora, K. (2011). Cybercrime in the society: problems and preventions. J Alt Persp Soc Sci, 3(1), 240-259.

Davis, J. (2017, Oct 27). Petya cyberattack cost Merck $135 million in revenue. Healthcare IT News. Retrieved from http://www.healthcareitnews.com/news/petya-cyberattack-cost-merck- 135-million-revenue

Dembe, A.E., Erikson, J.B., Delbos, R.G., & Banks, S.M. (2005). The impact of overtime and long work hours on occupational injuries and illnesses: new evidence from the United States. Occup Environ Med, 62, 588-597.

Department of Health and Human Services. Top 10 tips for cybersecurity in health care. Retrieved from https://www.healthit.gov/sites/default/files/Top_10_Tips_for_Cybersecurity.pdf

Douglas, A. and Harrison, S. (2017After North Carolina county refuses to pay hacker ransom, attackers strike again. Government Technology, Retrieved from http://www.govtech.com/network/After-North-Carolina-County-Refuses-to-Pay-Hacker-Ransom- Attackers-Strike-Again.html

Gordon, P. (2016). Rise of the cyber criminals. Huffington Post. Retrieved from http://www.huffingtonpost.com/entry/rise-of-the-cyber-criminals_us_57bed90ae4b06384eb3e60b9

Hampton S., 2010. Security Systems Simplified Protecting your Home, Business and Car with state of the Art, Burglar Alarm

Höller, L., W., 2009, Smart city technologies. Future Internet Assembly 23-24

Healthcare IT News & HIMSS Analytics. Healthcare IT News and HIMSS Analytics quick HIT survey: Ransomware, 2016. Retrieved from https://healthmanagement.org/c/it/news/ransomware-attacks-hit-three-quarters-of-hospitals- without-them-knowing

Hightower, D. (2018, Feb 21). Davidson County, N.C., still reeling from ransomware attack. Government Technology, Retrieved from http://www.govtech.com/security/Davidson-County- NC-Still-Reeling-from-Ransomware-Attack.html

Ismailov G. 2018. Introduction to health vulnerability and risk analysis and mapping (VRAM). Copenhagen: WHO Regional Office for Europe.

Kelly, M.L. (2016, Dec 16). Obama: espionage is being 'turbocharged' by the internet. NPR. Retrieved from http://www.npr.org/sections/parallels/2016/12/16/505864712/obama-espionage- is-being-turbocharged-by-the-internet

Kruse, C.S., Frederick, B., Jacobson, T., & Monticone, D.K. (2017). Cybersecurity in healthcare: a systematic review of modern threats and trends. Technol Health Care, 25, 1-10.

Kshetri, N. (2009). Positive externality, increasing returns, and the rise in cybercrimes. Commun ACM, 52(12). 141-144.

Larson, S. (2017). Massive cyberattack targeting 99 countries causes sweeping havoc. CNN Tech, Retrieved from http://money.cnn.com/2017/05/12/technology/ransomware-attack-nsa-microsoft/index.html

Kieny MP, Bekedam H, Dovlo D, Fitzgerald J, Habicht J, Harrison G et al. 2017. Strengthening health systems for universal health coverage and sustainable development. Bull World Health Organ;95(7):537–9.

Lee, S. (2016). Ransomware attacks reached record high in April- and aren't slowing down: report. Newsweek. Retrieved from http://www.newsweek.com/ransomware-attacks-reached-record-high-april-and-not-slowing-down-report-455239)

Lee, S. (2016). Ransomware wreaking havoc in American and Canadian hospitals. Newsweek. Retrieved from http://www.newsweek.com/ransomware-wreaking-havoc-american- and-canadian-hospitals-439714

Lipton, E., Sanger, D.E., & Shane, S., (2016). The perfect weapon: how Russian cyberpower invaded the U.S. The New York Times. Retrieved from https://www.nytimes.com/2016/12/13/us/politics/russia-hack-election-dnc.html?rref=collection%2Fnewseventcollection%2Frussian-election-hacking&action=click&contentCollection=politics&region=rank&module=package&version=highli ghts&contentPlacement=1&pgtype=collection&_r=0

Luna, R., Rhine, E., Myhra, M., Sullivan, R., & Kruse, C.S. (2016). Cyber threats to health information systems: a systemic review. Technol Health Care, 24, 1-9.

Marx, D.A. & Slonim, A.D. (2003). Assessing patient safety risk before the injury occurs: an introduction to sociotechnical probabilistic risk modelling in health care. Qual Saf Health Care, 12(Supp II), ii33-38.

McCoy, T.H. Jr., Perlis, R.H. (2018). Temporal trends and characteristics of reportable health data breaches, 2010-2017. JAMA, 320(12), 1282-1284.

Nakashima, E. (2018) Russian military was behind 'NotPetya' cyberattack in Ukraine, CIA concludes. The Washington Post. Retrieved from https://www.washingtonpost.com/world/national-security/russian-military-was-behind-notpetya- cyberattack-in-ukraine-cia-concludes/2018/01/12/048d8506-f7ca-11e7-b34a-b85626af34ef_story.html?utm_term=. d3c66123570b

Naylor, B. (2018). Russia hacked the U.S. power grid- so what will the Trump administration do about it? NPR. Retrieved from https://www.npr.org/2018/03/23/596044821/russia-hacked-u-s-power-grid-so-what-will-the- trump-administration-do-about-it

Norman I., 2007. Integrated Security System Design

Nystedt, F. 2011. Verifying Fire Safety in Sprinklered Buildings. Lund: Department of Fire Safety Engineering and Systems safety. Lund University, Sweden.

Nyyssönen, T., Rajakko, J., & Rahkonen, O. K. 2005. On the reliability of fire detection and alarm systems. Espoo: VTT Information Service.

Perakslis, E.D. (2014). Cybersecurity in healthcare. N Engl J Med, 371 (5), 395-397.

Perlroth, N. & Sanger, D.E. (2018). Cyberattacks put Russian fingers on the switch at power plants, U.S. says. The New York Times. Retrieved from https://www.nytimes.com/2018/03/15/us/politics/russia-cyberattacks.html

Perlroth, N. & Sanger, D.E. (2017). Hackers hits dozens of countries exploiting stolen N.S.A. tool. The New York Times. Retrieved from https://www.nytimes.com/2017/05/12/world/europe/uk-national-health-service-cyberattack.html?_r=0

Radke, B.A., Waters, M.J., Cleary, J.C., Evans, D., & Kittle, C. (2016). Ransomware rises among hospitals. Lexology. Retrieved from http://www.lexology.com/library/detail.aspx?g=8f3d29a5-2f87-42b8-ada1-54a109e38b3f

Sauer, L.M., McCarthy, M.L., Knebel, A., & Brewster, P. (2009). Major influences on hospital emergency management and disaster preparedness. Disaster Med Pub Health Prep, 3(S1), S68-73.

Siwicki, B. (2017) Hackers hit 320% more healthcare providers in 2016 than in 2015, per HHS data. Healthcare IT News. Retrieved from https://www.healthcareitnews.com/news/hackers-hit-320-more-healthcare-providers-2016-2015- hhs-data

Squitieri, T. (2002). Cyberspace full of terror targets. USA Today. Retrieved from https://usatoday30.usatoday.com/tech/news/2002/05/06/cyber-terror.htm

Stohl, M. (2007), Cyber terrorism: a clear and present danger, the sum of all fears, breaking point or patriot games? Crime Law Soc Change, 46, 223-238.

The Joint Commission. (2017). Hospital accreditation. Retrieved from https://www.jointcommission.org/accreditation/hospitals.aspx

The Joint Commission E-dition. (2016). Hospitals: emergency management. Retrieved from https://www.jointcommission.org/standards_information/edition.aspx

The White House. (2013 Feb 12). Presidential policy directive—Critical infrastructure security and resilience. Retrieved from https://obamawhitehouse.archives.gov/the-press-office/2013/02/12/presidential-policy-directive-critical-infrastructure-security-and-resil

Weimann, G. (2005). Cyberterrorism: the sum of all fears? Stud Conflict Terrorism, 28, 129-149.

Zetter, K. (2016). Why hospitals are the perfect targets for ransomware. Wired. Retrieved from https://www.wired.com/2016/03/ransomware-why-hospitals-are-the-perfect- targets/

Αγγλική Διαδικτυακή Βιβλιογραφία

Baer, Walter & Parkinson, Andrew. 2007. Cyberinsurance in IT Security Management. IEEE Security and Privacy. 2016:5(3) DOI: 10.1109/MSP.2007.57

Bendovschi. Andreea. 2015. Cyber-Attacks – Trends, Patterns and Security Countermeasures. Procedia Economics and Finance, Vol. 28, 24-31

Berliner, Baruch. 1982. Limits of Insurability of Risks. Englewood Cliffs, NJ: Prentice Hall.

Berliner, Baruch. 1985. Large Risks and Limits of Insurability. The Geneva Papers on Risk and Insurance – Issues and Practice 10:4, 313-329

Blanke, Sandra & McGrady, Elizabeth. 2016. When it comes to securing patient health information from breaches, your best medicine is a dose of prevention: A cybersecurity risk assessment checklist. Journal of Healthcare Risk Management 36(1); 14-24

Biener, Christian, Eling, Martin & Wirfs, Jan Hendrik. 2015. Insurability of Cyber Risk: An Empirical Analysis. The Geneva Papers on Risk and Insurance - Issues and Practice 40:1, 131-158

Collum, Taleah & Menachemi, Nir. 2011. Benefits and drawback of electronic health record systems. Risk management and Healthcare Policy 2011:4 47-55

Eling, Martin & Schnell, Werner. 2016. What do we know about cyber risk and cyber insurance? The Journal of Risk Finance [1526-5943] v:2016 vsk/osa:17 iss:5 s:474

Filkins, Barbara, Kim, Young, Roberts, Bruce, Armstrong, Winston, Miller, Mark, Hultner, Michael, Castillo, Anthony, Ducom, Jean-Cristophe, Topol, Eric & Steinhubl, Steven. 2016. Privacy and security in the era of digital health: what should translational researchers know and do about it? American Journal of Translational Research 8(3); 1560-1580

Fraser, John & Simkins, Betty. 2010. Enterprise Risk Management-Today's Leading Research and Best Practices for Tomorrow's Executives. Hoboken, NJ: John Wiley & Sons Inc.

Galletta, Anne. 2012. Mastering the Semi-Structured Interview and Beyond: From Research Design to Analysis and Publication. New York: NYU Press

Guikema, Seth & Aven Terje. 2010. Assessing risk from intelligent attacks: a perspective on approaches. Reliability Engineering and System Safety 2010, 95:5, 478-483

Hathaway, Oona & Crootof, Rebecca. 2012. The Law of Cyber-Attack. Yale Law School Faculty Scholarship Series. Paper 3852

Holton, Glyn. 2004. Defining Risk. CFA Institute. Financial Analysts Journal, volume 60, 6

Jha, Ashish, DesRoches, Catherine, Campbell, Eric, Donelan, Karen, Rao, Sowmya, Ferris, Timothy, Shields, Alexandra, Rosenbaum, Sara & Blumenthal, David. 2009. Use of Electronic Health Records in US Hospitals. New England Journal of Medicine 2009; 360:1628-1638 April 16, 2009 DOI: 10.1056/NEJMsa0900592

Johnson, Kristin. 2016. Managing Cyber Risks. Georgia Law Review, 50:2, 547-592

Kendrick, Rupert. 2010. Cyber Risks for Business Professionals: a Management Guide. Cambridgeshire: IT Governance Publishing

Korpela, Karina. 2015. Improving Cyber Security Awareness and Training Programs with Data Analytics. Information Security Journal. 2015:24

Kshetri, Nir. 2010. The Global Cybercrime Industry: Economic, Institutional and Strategic Perspectives. Berlin: Springer

Lackland, Daniel, Roccella, Edward, Deutsch, Anne, Fornage, Myriam , George, Mary, Howard, George, Kissela, Brett, Kittner, Steven, Lichtman, Judith, Lisabeth, Lynda, Schwamm, Lee, Smith, Eric & Towfighi, Amytis. 2014. Factors Influencing the Decline in Stroke Mortality. Stroke. 2014; 45:315-353

Lam, James. 2014. Enterprise Risk Management: From Incentives to Controls. Hoboken, NJ: John Wiley & Sons Inc.

Limnéll, Jarno, Majewski, Klaus, & Salminen, Mirva. 2014. Kyberturvallisuus. Jyväskylä: Docendo

Luna, Raul, Rhine, Emily, Myhra, Matthew, Sullivan Ross & Kruse, Clemens. 2016. Cyber Threats to Health Information Systems: A Systematic Review. Technology and Health Care. 2016:24, 1-9

Lundqvist, Sara. 2014. An Exploratory Study of Enterprise Risk Management: Pillars of ERM. Journal Of Accounting, Auditing & Finance, 29(3), 393-429. doi:10.1177/0148558X14535780

Martin, Guy, Martin, Paul, Hankin, Chris, Darzi, Ara, & Kinross, James. 2017. Cyber Security and Healthcare: How Safe are we? British Medical Journal 2017;358:j3179

Moody, Micheal. 2010. Rating Agencies' Impact on Enterprise Risk Management. In: Fraser, John. & Simkins, Betty. 2010 Enterprise Risk Management-Today's Leading Research and Best Practices for Tomorrow's Executives. Hoboken, NJ: John Wiley & Sons Inc.

Mukhopadhyay, Arunabha, Chatterjee, Samir, Saha, Debashis, Mahanti, Ambuj & Sadhukhan, Samir. 2013. Cyber-risk decision models: To insure IT or not? Decision Support Systems, Volume 56, December 2013, 11-26

Nass, Sharyl, Levit, Laura & Gostin, Lawrence. 2009. Beyond the HIPAA Privacy Rule: Enhancing Privacy, Improving Health Through Research. Institute of Medicine. Washington DC: National Academies Press

Payne, Thomas. 2016. Teaching Old Law New Tricks: Applying and Adapting State Responsibility to Cyber Operations. Lewis and Clark Law Review 2016:20 (2), 683-715

Perakslis, Eric. 2014. Cybersecurity in Health Care. New England Journal of Medicine 371:395-397

Pfleeger, Shari & Caputo, Deanna. 2012. Leveraging Behavioral Science to Mitigate Cyber Security Risk. Computers and Security. 2012: 31(4)

Price, Jeffrey & Wear, Justin. 2015. Claims Made and Insurance Coverage Available for Losses Arising out of or Related to Electronic Data. Tort Trial & Insurance Practice Law Journal, vol. 51(1), 51-90

Rejda, George. 2013. Principles of Risk Management and Insurance. Pearson series in Finance

Romanosky, Sasha. 2016. Examining the Costs and Causes of Cyber Incidents. Journal of Cyber Security 2016: 2(2), 121-135

Rotenberg, Marc & Jacobs, David. 2013. Updating the Law of Information Privacy: The New Framework of the European Union. Harvard Journal of Law & Public Policy. 2013; 36(2):605-652

Rubenfire, Adam. 2017. A smarter anti-hacker defense. Modern Healthcare 47(4)

Saldana, Johnny. 2011. Fundamentals of Qualitative Research. USA: Oxford University Press

Schneier, Bruce. 2014. Carry on: Sound Advice from Schneier on Security. Indianapolis: John Wiley & Sons Inc.

Sheppard, Ben, Crannell, Mary, & Moulton, Jeff. 2013. Cyber first aid: proactive risk management and decision-making. Journal of Environmental Systems and Decisions 2013, 33:4, 530-535

Shackelford, Scott. 2012. Should your firm invest in cyber insurance? Business Horizons, 55(4), 349-356

Skipper, Harold. & Kwon, Jean. 2007. Risk Management and Insurance – Perspectives in a Global Economy. Malden: Blackwell Publishing

Sligo, Judith, Gault, Robin, Roberts, Vaughan & Villa, Luis. 2017. A literature review for large-scale health information system project planning,

implementation and evaluation. International Journal of Medical Informatics. 97; 86-97

Smith, Feff, Dinev, Tamara, & Xu, Heng. 2011. Information Privacy Research: An interdisciplinary review. MIS Quarterly, 35:4, 2011, 989-1015

Susilo, W., Rezaeibagha, F., Khin Than, W. 2015. A systematic literature review on security and privacy of electronic health record systems: technical perspectives. Health Information Management Journal, 44(3), 23-38. doi:10.12826/18333575.2015.0001

Ulsch, MacDonnel. 2014. Cyber Threat – How to Manage the Growing Risk of Cyber Attacks. Hoboken: John Wiley & Sons Inc.

Webb, Timothy & Dayal, Sumer. 2017. Building the wall: Addressing cyber security risks in medical devices in the U.S.A. and Australia. Computer Law & Security Review. 33(4); 559- 563

World Medical Association. 2016. WMA Statement on Cyber-Attacks on Health and Other Critical Infrastructure. 2016;62(4):145-146

Yener, Dener. 2010. Establishing ERM Systems in Emerging Countries. In: Fraser, J. & Simkins, B. 2010 Enterprise Risk Management-Today's Leading

Research and Best Practices for Tomorrows' Executives. Hoboken, NJ: John Wiley & Sons Inc.