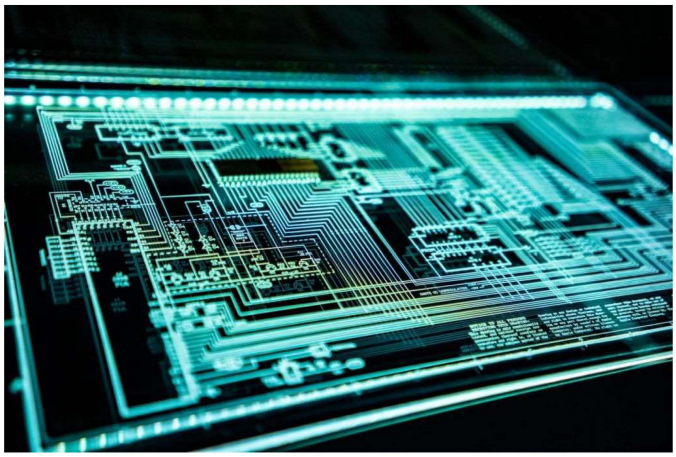
ΤΕΧΝΟΛΟΓΙΑ

Κυβερνοασφάλεια στην υγεία: η μεγάλη πρόκληση στη μετά-COVID εποχή

Σύμφωνα με στατιστικά στοιχεία του FBI, από τον Μάρτιο του 2020 στην Αμερική σημειώθηκε αύξηση κατά 400% (!) των καταγγελιών κυβερνοεπιθέσεων

17 Μαΐου 2021, 09:01



Γράφει: Βάσω Μιχοπούλου

Τον Σεπτέμβριο του 2020 εν μέσω πανδημίας αναφέρθηκε ο πρώτος θάνατος εξαιτίας κυβερνοεπίθεσης στο πανεπιστημιακό νοσοκομείο του Ντίσελντορφ, η οποία προκάλεσε μεγάλη αναστάτωση, όπως αναβολές χειρουργικών επεμβάσεων, προγραμματισμένων ιατρικών εξετάσεων ή χημειοθεραπειών. Εγκληματίες του κυβερνοχώρου αξιώνοντας λύτρα εισέβαλαν με το κακόβουλο λογισμικό ransomware σε 30 διακομιστές του νοσοκομείου, καταστρέφοντας υπολογιστικά συστήματα και αρχεία δεδομένων και αναγκάζοντας το προσωπικό να απομακρύνει ασθενείς που βρίσκονταν σε κατάσταση έκτακτης ανάγκης. Μια γυναίκα ασθενής που μεταφέρθηκε 35 χλμ. μακριά σε νοσοκομείο του Βούπερταλ, τελικά εξέπνευσε λόγω καθυστέρησης στην αντιμετώπιση της κατάστασής της. Σχεδόν έναν χρόνο νωρίτερα το Campbell County Health, ένας ιατρικός όμιλος με 20 κλινικές στην Πολιτεία Ουαόμινγκ των ΗΠΑ είχε πέσει επίσης θύμα κυβερνοεπίθεσης. Οι επιτιθέμενοι «κλείδωσαν» τους φακέλους των ασθενών και τις ιατρικές συσκευές απαιτώντας λύτρα. Οι εργαζόμενοι στον ιατρικό όμιλο αναγκάστηκαν να «παγώσουν» όλες τις ιατρικές υπηρεσίες και τις κλινικές πράξεις και να μεταφέρουν τους ασθενείς 500χλμ. μακριά, στη Νότια Ντακότα ή στο Ντένβερ που απέχει 350 χλμ.

Η πανδημία που εξακολουθούμε να βιώνουμε απέδειξε την αξία των υπηρεσιών ηλεκτρονικής υγείας και επέβαλε εξ' ανάγκης την άρρηκτη διασύνδεσή μας με την τεχνολογία, επιβεβαιώνοντας ωστόσο, το πόσο ευάλωτοι είμαστε συλλογικά. Η πρόοδος στον τομέα της υγείας μέσω του δυναμικού περιβάλλοντος που διαμορφώνουν οι νέες τεχνολογίες στις απαρχές της 4ης Βιομηχανικής Επανάστασης, καλλιέργησε ευνοϊκές συνθήκες για την αύξηση των κυβερνοαπειλών. «Καθώς οι τεχνολογίες εξελίσσονται με ταχείς ρυθμούς, διαρκώς αποκαλύπτονται ευάλωτα σημεία και αναδύονται νέες απειλές. Οι διαδικτυακές επιθέσεις σε μονάδες υγείας σχεδιάζονται με στόχο να απαγορεύουν την πρόσβαση των εργαζομένων τους σε συστήματα κρίσιμης φροντίδας.

της παρενεργεια της προσφατης ταση για αυξηση της τηλεργασιας και τηλεϊατρικής λόγω της πανδημίας, οι παραβιάσεις συστημάτων που λειτουργούν πάνω από το υπολογιστικό νέφος αναμένεται να αυξηθούν», επισημαίνει ο Επικεφαλής του Κέντρου Εφαρμογών και Υπηρεσιών Ηλεκτρονικής Υγείας του Ινστιτούτου Πληροφορικής στο Ίδρυμα Τεχνολογίας και Έρευνας (ΙΤΕ), κ. Δημήτρης Κατεχάκης. Στη χώρα μας έχουν σημειωθεί κατά καιρούς μεμονωμένες και περιορισμένης έκτασης κυβερνοεπιθέσεις σε μονάδες υγείας, όπως η τελευταία στο νοσοκομείο Χανίων το 2017.

Υγεία, ένας ευάλωτος στόχος

Σύμφωνα με στατιστικά στοιχεία του FBI, από τον Μάρτιο του 2020 στην Αμερική σημειώθηκε αύξηση κατά 400% (!) των καταγγελιών κυβερνοεπιθέσεων. Ο Παγκόσμιος οργανισμός Υγείας και το Αμερικανικό υπουργείο Υγείας και Ανθρωπίνων Υπηρεσιών υπήρξαν οι πιο δημοφιλείς στόχοι των χάκερς που ενδιαφέρονταν να «λάβουν γνώση» σχετικά με την έρευνα που διενεργείτο για την Covid-19. Μάλιστα οι επιθέσεις πραγματοποιηθήκαν κυρίως με τη χρήση κακόβουλων μηνυμάτων ηλεκτρονικού ταχυδρομείου σχετικά με τον κορωνοϊό, προκειμένου να εξαπατήσουν άτομα να κάνουν κλικ σε επικίνδυνους συνδέσμους.

Στην ετήσια ενημερωτική έκθεση DBIR (Data Breach Investigations Report) της Verizon που είναι μια από τις πιο αξιόπιστες εταιρείες που δραστηριοποιούνται στον τομέα της ψηφιακής επικοινωνίας επιβεβαιώνεται πως το 2020 τα περιστατικά επιθέσεων αυξήθηκαν κατά 71% συγκριτικά με το 2019.

Αντίστοιχα, μια μελέτη της εταιρείας Bitglass που δραστηριοποιείται στο cloud security αναφέρει πως συνολικά στις ΗΠΑ μέσα στο 2020 περίπου 26 εκατομμύρια αρχεία ασθενών εκτέθηκαν σε μη εξουσιοδοτημένους χρήστες, από τα οποία τα 24,1 εκατομμύρια ανακτήθηκαν από επιθέσεις στον κυβερνοχώρο επηρεάζοντας περίπου 80 εκατομμύρια άτομα.

Πολλές από τις προκλήσεις στην κυβερνοασφάλεια που αντιμετωπίζει σήμερα η βιομηχανία της υγείας συνδέονται με αδυναμίες που προυπήρχαν της πανδημίας, όπως ισχυρίζεται ο κ. Κατεχάκης: «Ο τομέας της υγείας αποτελεί έναν ευάλωτο στόχο κυβερνοεπιθέσεων γιατί οι ιατρικές συσκευές συνήθως κατασκευάζονται χωρίς ή με αδύναμη προστασία, γιατί οι επαγγελματίες υγείας δεν είναι επαρκώς εκπαιδευμένοι στους κινδύνους, γιατί ο τομέας είναι κατακερματισμένος και συνυπάρχουν πολλές και συχνές ανταλλαγές πολύμορφων δεδομένων μεταξύ παρόχων υπηρεσιών υγείας, γιατί εξακολουθεί να λειτουργεί ένας μεγάλος αριθμός τεχνολογικά ξεπερασμένων συστημάτων πληροφορικής, γιατί συνυπάρχουν διαφορετικές τεχνολογικές λύσεις, ενώ δεν υπάρχει ομοιόμορφη κουλτούρα προστασίας των δεδομένων».

Πληθώρα δε, μελετών κυβερνοασφάλειας συνηγορούν στο γεγονός πως πολλές φορές η «αχίλλειος πτέρνα» των συστημάτων είναι οι ίδιοι οι χρήστες τους. Πόσο μάλλον στον τομέα της υγείας όπου οι επαγγελματίες υγείας εστιάζουν το ενδιαφέρον τους στη ιατρική πρακτική δίνοντας έμφαση στον ασθενή και αφήνοντας σε δεύτερη μοίρα θέματα ασφάλειας και ιδιωτικότητας. «Δεν είναι λίγες οι φορές που χρήστες μοιράζονται τον ίδιο κωδικό για την πρόσβαση σε ιατρικά πληροφοριακά συστήματα. Παρότι έχουν γίνει διάφορες καμπάνιες ενημέρωσης και ευαισθητοποίησης είναι δύσκολο να αλλάξει η υπάρχουσα νοοτροπία. Απαιτείται χρόνος και ορθή προσέγγιση. Ο χρόνος μπορεί να είναι δυσεύρετος, αλλά η ορθή προσέγγιση είναι εφικτή!» αναφέρει χαρακτηριστικά ο Διευθυντής Ερευνών του Ινστιτούτου Πληροφορικής του ΙΤΕ, κ. Ευάγγελος Σακκαλής.

Οι κυβερνοεπιθέσεις σε παρόχους υγειονομικής περίθαλψης έχουν μετατραπεί σε μια βιομηχανία 13,2 δισεκατομμυρίων δολαρίων, με το μέσο κόστος παραβίασης δεδομένων ανά αρχείο να αγγίζει τα 499 δολάρια. Ο τομέας της υγείας χρειάζεται πλέον μεγαλύτερο χρόνο για την αποκατάσταση της κάθε παραβίασης (κατά μέσο 236 ημέρες), καθώς και για τον εντοπισμό αυτών των παραβιάσεων (κατά μέσο όρο 96 ημέρες). Οι καταβολές δε, των λύτρων από τα θύματα έχουν αποθρασύνει τους κυβερνοεγκληματίες. Ενδεικτικά πέρσι κυβερνοεγκληματίες απαίτησαν λύτρα σε bitcoin αξίας 14 εκατομμυρίων δολαρίων κατά τη διάρκεια μιας επίθεσης με ransomware που επηρέασε 110 γηροκομεία σε όλες τις ΗΠΑ.

Κυβερνοασφάλεια στη μετα-COVID εποχή με προϋποθέσεις

«Κάθε μέρα διαπιστώνονται και περισσότερο ευφάνταστοι τρόποι επιθέσεων οι οποίοι μπορούν να προκαλέσουν άρνηση υπηρεσίας, πειρατεία συνεδρίας, πλαστογράφηση, ηλεκτρονικό ψάρεμα, υποκλοπή δεδομένων, ενεργοποίηση κακόβουλων λογισμικών, κ.α. Φανταστείτε μία τέτοια επίθεση να γίνει σε λογισμικό που χρειάζεται να λειτουργεί για την υποστήριξη της ζωής ενός ασθενή (π.χ. σε ένα νοσοκομείο ή ακόμη και στο σπίτι του). Ακόμη περισσότερο επικίνδυνα σενάρια συμπεριλαμβάνουν τη χρήση μη αξιόπιστων λογισμικών (π.χ. αλγορίθμων τεχνητής νοημοσύνης) που θα μπορούσαν να οδηγήσουν στην εξαγωγή μίας λάθος διάγνωσης, ή τη χορήγηση μιας λανθασμένης θεραπείας, προκαλώντας με τον τρόπο αυτό βλάβη ή απώλεια ανθρώπινης ζωής», σχολιάζει ο κ. Κατεχάκης.

Σύμφωνα με τον ίδιο, η αρχή της ανάπτυξης ασφαλών συστημάτων εξ' ορισμού και εκ του σχεδιασμού έχει έρθει για να μείνει. Ωστόσο, η κυβερνοασφάλεια και η προστασία της προσωπικής ζωής προϋποθέτουν οργανωτικά και τεχνολογικά στοιχεία που στοχεύσουν στην υλοποίηση αυτής της προστασίας, καθώς και αρχές προστασίας δεδομένων σε συστήματα και υπηρεσίες: «Αν και υπάρχει σχετική νομοθεσία για την προστασία των προσωπικών δεδομένων για τη διασφάλιση της ψηφιακής ιδιωτικής ζωής, εντός και εκτός της ΕΕ, αυτή από μόνη της δεν αρκεί. Χρειάζεται εκπαιδευμένο προσωπικό στη διαχείριση ποιότητας και σύστημα ασφαλούς διαχείρισης πληροφοριών με λύσεις που περιλαμβάνουν, μεταξύ άλλων, συναίνεση, ελαχιστοποίηση δεδομένων, κρυπτογράφηση και την πιθανή χρήση ψευδωνύμων».

Στο σημείο αυτό αξίζει να αναφερθεί πως από το 2004 λειτουργεί στην ΕΕ ο Οργανισμός της Ευρωπαϊκής Ένωσης για την Κυβερνοασφάλεια (ENISA), που είναι ένα ευρωπαϊκό κέντρο εμπειρογνωσίας για την ασφάλεια στον κυβερνοχώρο. Ο ρόλος του είναι να βοηθάει τα κράτη μέλη της ΕΕ να εξασφαλίσουν ένα υψηλό επιπέδου κυβερνοασφάλειας και να θωρακίσουν τις ψηφιακές τους υποδομές. Ο ENISA τον Ιανουάριο του 2021 δημοσίευσε μια έκθεση σχετικά με το Cloud Security for Healthcare Service, παρέχοντας στους οργανισμούς υγειονομικής περίθαλψης οδηγίες για την ασφάλεια στον κυβερνοχώρο που θα βοηθήσουν στην περαιτέρω ψηφιοποίηση με την υποστήριξη των υπηρεσιών νέφους. Σε ετήσια βάση εξάλλου, ο ENISA διοργανώνει διάσκεψη για την ασφάλεια της ηλεκτρονικής υγείας και του κυβερνοχώρου στον τομέα της υγείας.

Η στρατηγική υπεράσπισης όμως του κυβερνοχώρου κοστίζει και πιθανώς να μην διαθέτουν όλοι οι πάροχοι υγείας τις ίδιες δυνατότητες-πόρους για να υιοθετήσουν ένα σύστημα ασφαλείας. «Λόγω του χάσματος δεξιοτήτων σε θέματα κυβερνοασφάλειας είναι σαφές ότι εκείνοι που είναι λιγότερο

προετοιμασμένοι θα παραμείνουν περισσότερο ευάλωτοι. Η υλοποίηση συγκεκριμένων νομικών, οργανωτικών, αλλά και τεχνικών μέτρων ψηφιακής ασφάλειας απαιτεί προσεκτικό σχεδιασμό, μελέτη αντικτύπου και έχει κόστος. Για τους οργανισμούς υγειονομικής περίθαλψης θα απαιτηθεί πρόσθετη υποστήριξη, όπως και συγκεκριμένη καθοδήγηση, από εθνικές και κοινοτικές αρχές, βιομηχανικά πρότυπα για την ασφάλεια, σαφείς οδηγίες από τις Αρχές Προστασίας Δεδομένων καθώς και συνεργασία με παρόχους τεχνολογικών υπηρεσιών (π.χ. νέφους), αλλά και κατασκευαστές ιατρικών συσκευών. Είναι σαφές ότι θα απαιτηθεί η παροχή κινήτρων για επενδύσεις σε μέτρα κυβερνοασφάλειας», συμπληρώνει ο κ. Κατεχάκης.

Εν μέσω πανδημίας, τον Δεκέμβριο του 2020 στη χώρα μας δημοσιοποιήθηκε από το Υπουργείο Ψηφιακής Διακυβέρνησης η νέα εθνική Στρατηγική Κυβερνοασφάλειας, η οποία κινείται γύρω από 5 βασικούς πυλώνες και 15 ειδικούς στόχους, ανάμεσα στους οποίους είναι η προστασία της υποδομής κρίσιμων πληροφοριών, η θέσπιση βασικών μέτρων ασφάλειας, η καθιέρωση μηχανισμών αναφοράς συμβάντων, η ανάπτυξη ικανότητας αντιμετώπισης περιστατικών, η αύξηση της ευαισθητοποίησης των χρηστών και η προώθηση της έρευνας και ανάπτυξης. Η Βίβλος του ψηφιακού μετασχηματισμού 2020-2025 για τη χώρα μας προβλέπει, μεταξύ άλλων, οριζόντιο έργο για την εγκαθίδρυση πλατφόρμας διαμοιρασμού πληροφοριών που σχετίζονται με κυβερνοασφάλεια και κυβερνοαπειλές.

Μια PANACEA με ανθρωποκεντρική προσέγγιση

Από το 2019 «τρέχει» στην ΕΕ ένα σημαντικό ερευνητικό έργο, το PANACEA, στο οποίο επιστημονικά υπεύθυνος είναι ο Διευθυντής Ερευνών του Ινστιτούτου Πληροφορικής του ΙΤΕ, κ. Ευάγγελος Σακκαλής. Το έργο που αποτελεί μέρος του Ευρωπαϊκού Προγράμματος Πλαισίου για την Έρευνα και την Καινοτομία «Ορίζοντας 2020», χρηματοδοτήθηκε με 5 εκατομμύρια ευρώ και ολοκληρώνεται το 2021. «Το έργο, στο οποίο συμμετέχουν 15 επιστημονικοί εταίροι από 7 ευρωπαϊκές χώρες έχει ανθρωποκεντρική προσέγγιση, καθώς αφιερώνει μεγάλο του μέρος στη μελέτη και εκτίμηση της συμπεριφοράς διαφορετικών κατηγοριών επαγγελματιών υγείας (ιατρικό, νοσηλευτικό, τεχνικό, διοικητικό προσωπικό), ενώ προτείνει και αξιολογεί παρεμβάσεις ειδικά σχεδιασμένες στην εκάστοτε κουλτούρα, οι οποίες προϋποθέτουν τη συμμετοχή των επαγγελματιών για τη συνδιαμόρφωση αυτών», εξηγεί ο κ. Σακκαλής. Μέρος του Panacea αποτελεί η ανάπτυξη ενός “έξυπνου” συστήματος προσομοίωσης κυβερνοεπιθέσεων, το οποίο προσαρμόζεται στην εκάστοτε τοπολογία του νοσοκομειακού δικτύου και ελέγχεται όλο το 24ωρο προκειμένου να εντοπιστούν και ουσιαστικά να προβλεφθούν ελαττώματα ασφαλείας ή αδυναμίες που πρέπει να ενισχυθούν. Η πιλοτική του εφαρμογή περιλαμβάνει τρεις διαφορετικές δομές υγείας, συμπεριλαμβανομένου του μεγαλύτερου νοσοκομείου της Ρώμης, καθώς και μονάδων της Κρήτης.

Σύμφωνα με τον κ. Σακκαλή «ο χώρος της Υγείας συχνά περιλαμβάνει πεπαλαιωμένα αλλά πλήρως λειτουργικά ιατρικά συστήματα, όπως για παράδειγμα τα απεικονιστικά μηχανήματα που είναι υψηλού κόστους, τα οποία δεν παρέχουν σύγχρονες δικλείδες ασφαλείας και παραμένουν ευάλωτα σε επίδοξους χάκερ, ενώ απαιτούν και μια κοστοβόρα αναβάθμιση. Στην κατεύθυνση αυτή το έργο PANACEA προτείνει μια σειρά υπολογιστικών εργαλείων αλλά και εύχρηστων μηχανισμών πρόσβασης στα συστήματα αυτά βασισμένων σε βιομετρικά χαρακτηριστικά (όπως το σχήμα προσώπου, η φωνή κλπ.)».

Αναγνωρίζοντας την σημαντικότητα της έγκαιρης και αποτελεσματικής αντιμετώπισης των κυβερνο-επιθέσεων στον τομέα της Υγείας κρίθηκε επιτακτική η συνέργεια του P. ANACEA με πέντε ακόμη συναφή έργα, τα ASCLEPIOS, CUREX, FeatureCloud, SAFECARE and SPHINX, που εστιάζουν στην κυβερνοασφάλεια στον τομέα της υγείας, τα οποία χρηματοδοτούνται από την Ευρωπαϊκή επιτροπή στα πλαίσια του προγράμματος «Ορίζοντας 2020».

Στις 20 Απριλίου 2021 η ΕΕ έδωσε το «πράσινο» φως για τη σύσταση ενός Κέντρου Ικανοτήτων στον τομέα της κυβερνοασφάλειας που θα συγκεντρώσει επενδύσεις στην έρευνα, την τεχνολογία και τη βιομηχανική ανάπτυξη στον τομέα αυτό. Συγκεκριμένα, ο νέος φορέας, που θα έχει την έδρα του στο Βουκουρέστι της Ρουμανίας, αναλαμβάνει τη διοχέτευση της χρηματοδότησης που συνδέεται με την κυβερνοασφάλεια από τα προγράμματα «Ορίζοντας Ευρώπη» και «Ψηφιακή Ευρώπη». Το εν λόγω βιομηχανικό, τεχνολογικό και ερευνητικό Κέντρο Ικανοτήτων στον τομέα της κυβερνοασφάλειας θα συνεργάζεται με την ENISA και με ένα δίκτυο εθνικών κέντρων συντονισμού που θα ορίσουν τα κράτη μέλη και θα φέρνει σε επαφή τους κυριότερους ευρωπαϊκούς φορείς, όπως βιομηχανίες, πανεπιστημιακά και ερευνητικά ιδρύματα και άλλες συναφείς ενώσεις της κοινωνίας των πολιτών, για να σχηματίσουν μια κοινότητα ικανοτήτων στον τομέα της κυβερνοασφάλειας στην ΕΕ.

Ολοκληρώνοντας, αξίζει να αναφερθεί πως την ώρα που γραφόταν αυτό το άρθρο το σύστημα υγείας της Ιρλανδίας δεχόταν σημαντική κυβερνοεπίθεση με ransomware. Η Εκτελεστική Υπηρεσία Υγείας (Health Service Executive), η οποία είναι υπεύθυνη για την υγειονομική περίθαλψη και τις κοινωνικές υπηρεσίες σε όλη την Ιρλανδία, απενεργοποίησε προληπτικά όλα τα συστήματα πληροφορικής, προκαλώντας αναστάτωση στους ασθενείς με την ακύρωση προγραμματισμένων ραντεβού, προκειμένου να προστατεύσει το δίκτυο από την επίθεση και για να αξιολογήσει την κατάσταση.

Picture credits: Christos Tsoumplekas/FORTH