Συμβούλιο της Ευρωπαϊκής Ένωσης

Βρυξέλλες, 16 Ιανουαρίου 2025
(OR. en)

5426/25

CYBER 21
SAN 15

ΔΙΑΒΙΒΑΣΤΙΚΟ ΣΗΜΕΙΩΜΑ

Αποστολέας:	Για τη Γενική Γραμματέα της Ευρωπαϊκής Επιτροπής, η κα Martine DEPREZ, Διευθύντρια
Ημερομηνία Παραλαβής:	15 Ιανουαρίου 2025
Αποδέκτης:	κα Thérèse BLANCHET, Γενική Γραμματέας του Συμβουλίου της Ευρωπαϊκής Ένωσης
Αριθ. εγγρ. Επιτρ.:	COM(2025) 10 final
Θέμα:	ΑΝΑΚΟΙΝΩΣΗ ΤΗΣ ΕΠΙΤΡΟΠΗΣ ΠΡΟΣ ΤΟ ΕΥΡΩΠΑΪΚΟ ΚΟΙΝΟΒΟΥΛΙΟ, ΤΟ ΣΥΜΒΟΥΛΙΟ, ΤΗΝ ΕΥΡΩΠΑΪΚΗ ΟΙΚΟΝΟΜΙΚΗ ΚΑΙ ΚΟΙΝΩΝΙΚΗ ΕΠΙΤΡΟΠΗ ΚΑΙ ΤΗΝ ΕΠΙΤΡΟΠΗ ΤΩΝ ΠΕΡΙΦΕΡΕΙΩΝ Ευρωπαϊκό σχέδιο δράσης για την κυβερνοασφάλεια των νοσοκομείων και των παρόχων υγειονομικής περίθαλψης

Διαβιβάζεται συνημμένως στις αντιπροσωπίες το έγγραφο - COM(2025) 10 final.

συνημμ.: COM(2025) 10 final

ΕΥΡΩΠΑΪΚΗ
ΕΠΙΤΡΟΠΗ

Βρυξέλλες, 15.1.2025
COM(2025) 10 final

ΑΝΑΚΟΙΝΩΣΗ ΤΗΣ ΕΠΙΤΡΟΠΗΣ ΠΡΟΣ ΤΟ ΕΥΡΩΠΑΪΚΟ ΚΟΙΝΟΒΟΥΛΙΟ, ΤΟ ΣΥΜΒΟΥΛΙΟ, ΤΗΝ ΕΥΡΩΠΑΪΚΗ ΟΙΚΟΝΟΜΙΚΗ ΚΑΙ ΚΟΙΝΩΝΙΚΗ ΕΠΙΤΡΟΠΗ ΚΑΙ ΤΗΝ ΕΠΙΤΡΟΠΗ ΤΩΝ ΠΕΡΙΦΕΡΕΙΩΝ

Ευρωπαϊκό σχέδιο δράσης για την κυβερνοασφάλεια των νοσοκομείων και των παρόχων υγειονομικής περίθαλψης

1. Εισαγωγή

Το περιβάλλον ασφάλειας της ΕΕ μεταβάλλεται ραγδαία, με κλιμάκωση των υβριδικών επιθέσεων και των κυβερνοεπιθέσεων που αποσκοπούν στην αποσταθεροποίηση της κοινωνίας μας, επιδιώκοντας τον διχασμό και τη διάσπαση, αλλά και κέρδη από το κυβερνοέγκλημα. Ως εκ τούτου, η Ευρώπη πρέπει να ενισχύσει επειγόντως την ετοιμότητα και την ανθεκτικότητά της έναντι αυτής της νέας πραγματικότητας, σε όλους τους τομείς και σύμφωνα με την προσέγγιση σε επίπεδο «συνόλου της κοινωνίας» και «συνόλου της δημόσιας διοίκησης», σύμφωνα με την έκκληση που διατυπώθηκε στην έκθεση του ειδικού συμβούλου του προέδρου της Ευρωπαϊκής Επιτροπής, Sauli Niinistö.

Τα ασφαλή και ανθεκτικά συστήματα υγειονομικής περίθαλψης αποτελούν ακρογωνιαίο λίθο του κοινωνικού μοντέλου της ΕΕ. Ωστόσο, τα νοσοκομεία και τα συστήματα υγειονομικής περίθαλψης αντιμετωπίζουν εντεινόμενες απειλές, και ειδικότερα από συμμορίες λυτρισμικού που τα στοχεύουν για οικονομικό όφελος, λόγω της υψηλής αξίας που έχουν τα δεδομένα ασθενών, συμπεριλαμβανομένων των ηλεκτρονικών μητρώων υγείας. Ο τομέας της υγείας έχει πράγματι καταστεί ο κλάδος που δέχεται τις περισσότερες επιθέσεις στην ΕΕ κατά την τελευταία τετραετία, μεταξύ άλλων κατά τη διάρκεια της πανδημίας της COVID-19, όταν οι υποδομές υγείας βρέθηκαν όλο και περισσότερο στο στόχαστρο κυβερνοεπιθέσεων. Οι κυβερνοεπιθέσεις κατά νοσοκομείων και παρόχων υγειονομικής περίθαλψης προκαλούν άμεση ζημία στους ανθρώπους, καθώς καθυστερούν τις ιατρικές διαδικασίες, προκαλούν προβλήματα στα τμήματα επειγόντων περιστατικών και θα μπορούσαν, σε ακραίες περιπτώσεις, να οδηγήσουν σε απώλεια ανθρώπινων ζωών.

Το διακύβευμα είναι ακόμα μεγαλύτερο, δεδομένου ότι ο τομέας βρίσκεται σε στάδιο ψηφιακού μετασχηματισμού ζωτικής σημασίας. Η ψηφιακή υγεία και η χρήση και επαναχρησιμοποίηση δεδομένων υγείας μπορούν να δημιουργήσουν ευνοϊκές συνθήκες για μοντέλα περίθαλψης καλύτερα προσαρμοσμένα στις ανάγκες και τις προτιμήσεις των ατόμων και των ασθενών, προλαμβάνοντας την εκδήλωση νόσων ή καθιστώντας δυνατή την έγκαιρη θεραπεία. Η ενσωμάτωση ψηφιακών εργαλείων και λύσεων στις κλινικές διαδικασίες, καθώς και η χρήση και επαναχρησιμοποίηση δεδομένων υγείας μπορούν να τροφοδοτήσουν καλύτερες κλινικές αποφάσεις, να συμβάλουν στην αυτοματοποίηση της υγείας, καθώς και στην ταχύτερη και καλύτερη περίθαλψη των ασθενών. Τα ψηφιακά εργαλεία, η χρήση δεδομένων και τα ιατροτεχνολογικά προϊόντα —τα οποία συχνά συνδέονται με το διαδίκτυο και τροφοδοτούνται με τεχνητή νοημοσύνη (ΤΝ)— έχουν επίσης καθοριστική σημασία για την αντιμετώπιση προκλήσεων, όπως η έλλειψη επαγγελματιών του τομέα της υγείας.

Ταυτόχρονα, τα ψηφιακά εργαλεία διευρύνουν επίσης τους πιθανούς στόχους των κυβερνοεγκληματιών. Επιπλέον, ορισμένοι κρατικοί φορείς δεν διστάζουν να στοχεύσουν εγκαταστάσεις υγειονομικής περίθαλψης, όπως μαρτυρεί ο συνεχιζόμενος επιθετικός πόλεμος της Ρωσίας κατά της Ουκρανίας. Έτσι, ο τομέας μετατρέπεται σε πιθανό στόχο κυβερνοεπιθέσεων στο πλαίσιο μιας ευρύτερης υβριδικής εκστρατείας. Οι κυβερνοεπιθέσεις δεν θέτουν μόνο σε κίνδυνο την ασφάλεια των ασθενών, αλλά διαβρώνουν επίσης την εμπιστοσύνη του κοινού στις υποδομές υγείας και συνεπάγονται σημαντικό κόστος αποκατάστασης. Πέραν της προστασίας από κυβερνοεπιθέσεις, οι ανθεκτικές και ασφαλείς

ψηφιακές υποδομές είναι επίσης απαραίτητες για τη στήριξη της υλοποίησης και της πλήρους ανάπτυξης του ευρωπαϊκού χώρου δεδομένων για την υγεία[1] (EHDS).

Ως εκ τούτου, είναι καιρός να αναβαθμιστεί και να ενισχυθεί η κυβερνοασφάλεια και η ανθεκτικότητα των νοσοκομείων και των παρόχων υγειονομικής περίθαλψης της Ευρώπης, όπως τόνισε η πρόεδρος κ. φον ντερ Λάιεν στις πολιτικές κατευθύνσεις για την Επιτροπή 2024-2029[2]. Το παρόν σχέδιο δράσης ανταποκρίνεται στον επείγοντα χαρακτήρα της κατάστασης και στις μοναδικές απειλές που αντιμετωπίζει ο τομέας. Δεν υπάρχει κάποια απλή «μαγική» λύση για τις προκλήσεις της κυβερνοασφάλειας στον τομέα της υγειονομικής περίθαλψης. Αντιθέτως, το σχέδιο δράσης απαιτεί ενισχυμένη πρόληψη, ετοιμότητα και μια πιο συντονισμένη προσέγγιση της αλληλεγγύης, αξιοποιώντας παράλληλα την εμπειρογνωσία του ευρωπαϊκού κλάδου κυβερνοασφάλειας. Ως εκ τούτου, το σχέδιο δράσης αντικατοπτρίζει την προσέγγιση της ΕΕ για την ασφάλεια, η οποία θα αναπτυχθεί περαιτέρω και θα επισημοποιηθεί στην επικείμενη ευρωπαϊκή στρατηγική για την εσωτερική ασφάλεια, με τον καθορισμό μιας ολοκληρωμένης αντίδρασης για την αντιμετώπιση όλων των απειλών κατά της εσωτερικής ασφάλειας και την εστίαση στην ικανότητα πρόβλεψης των απειλών, πρόληψης των ζημιών και προστασίας των ανθρώπων, με ανάληψη δράσεων σε όλα τα επίπεδα βάσει της προσέγγισης για το σύνολο της κοινωνίας.

Ο τομέας της υγείας περιλαμβάνει ευρύ αριθμό φορέων και παραγόντων, στους οποίους συγκαταλέγονται νοσοκομεία, κλινικές, οίκοι ευγηρίας, κέντρα αποκατάστασης και διάφοροι πάροχοι υγειονομικής περίθαλψης, μαζί με τον φαρμακευτικό, τον ιατρικό κλάδο και τον κλάδο βιοτεχνολογίας, τους κατασκευαστές ιατροτεχνολογικών προϊόντων και τα ερευνητικά ιδρύματα υγείας. Το παρόν σχέδιο δράσης επικεντρώνεται κυρίως στην κυβερνοασφάλεια των νοσοκομείων και των παρόχων υγειονομικής περίθαλψης, οι οποίοι νοούνται ως κάθε φυσικό ή νομικό πρόσωπο ή άλλος φορέας που παρέχει νόμιμα υγειονομική περίθαλψη στο έδαφος κράτους μέλους[3]. Τα νοσοκομεία και οι πάροχοι υγειονομικής περίθαλψης αλληλεξαρτώνται από άλλους φορείς υγείας και αφορούν άμεσα τους πολίτες. Ταυτόχρονα, τα μέτρα για την ενίσχυση της κυβερνοασφάλειας των νοσοκομείων και των παρόχων υγειονομικής περίθαλψης θα πρέπει επίσης να αντιμετωπίζουν τους κινδύνους που επηρεάζουν την ευρύτερη αλυσίδα εφοδιασμού και το οικοσύστημα, οι οποίοι προκύπτουν για παράδειγμα από φορείς που χρησιμοποιούν δεδομένα υγείας για έρευνα και μηχανική μάθηση ή που παράγουν ιατροτεχνολογικά προϊόντα, και ειδικότερα ψηφιακά ιατροτεχνολογικά προϊόντα που συνδέονται με το διαδίκτυο ή άλλες συσκευές («διαδίκτυο των πραγμάτων»).

Ενώ η διασφάλιση των συστημάτων υγείας αποτελεί πρωτίστως εθνική αρμοδιότητα, η υγεία αποτελεί επίσης κρίσιμο τομέα στο πλαίσιο της οδηγίας σχετικά με μέτρα για υψηλό κοινό επίπεδο

[1] https://www.consilium.europa.eu/el/press/press-releases/2024/03/15/european-health-data-space-council-and-parliament-strike-provisional-deal/.

[2] https://commission.europa.eu/document/e6cd4328-673c-4e7a-8683-f63ffb2cf648_el.

[3] Άρθρο 3 στοιχείο ζ) της οδηγίας 2011/24/ΕΕ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου περί εφαρμογής των δικαιωμάτων των ασθενών στο πλαίσιο της διασυνοριακής υγειονομικής περίθαλψης, https://eur-lex.europa.eu/legal-content/EL/TXT/?uri=celex:32011L0024.

κυβερνοασφάλειας σε ολόκληρη την ΕΕ (NIS2)[4]. Οι κυβερνοεγκληματίες και άλλοι παράγοντες απειλών δραστηριοποιούνται σε διασυνοριακό επίπεδο, ενώ οι προκλήσεις που αντιμετωπίζουν οι οργανισμοί υγειονομικής περίθαλψης στον τομέα της κυβερνοασφάλειας είναι επίσης παρόμοιες σε όλα τα κράτη μέλη. Η συνεργασία σε ευρωπαϊκό επίπεδο είναι πολύτιμη για την ανταλλαγή και την αναβάθμιση των βέλτιστων πρακτικών σε επίπεδο ΕΕ και σε εθνικό επίπεδο. Ως εκ τούτου, το σχέδιο δράσης προτείνει τον συντονισμό και τη λήψη μέτρων σε επίπεδο ΕΕ, ενώ παράλληλα καλεί τα κράτη μέλη να αναλάβουν δράση προκειμένου να κάνουν τη διαφορά όσον αφορά την υγειονομική περίθαλψη και το ευρύτερο οικοσύστημα υγείας.

Το σχέδιο δράσης επικεντρώνεται πρωτίστως στην ανάπτυξη των ικανοτήτων του τομέα για την **πρόληψη** περιστατικών κυβερνοασφάλειας, καθώς η πρόληψη είναι πάντα καλύτερη από τη θεραπεία. Δεύτερον, το σχέδιο δράσης περιγράφει λεπτομερώς δράσεις για τη βελτίωση της ανταλλαγής πληροφοριών στον τομέα της κυβερνοασφάλειας και της ικανότητας **ανίχνευσης** κυβερνοαπειλών, καθιστώντας δυνατή την ταχύτερη αντίδραση. Τρίτον, προβλέπει μέτρα για την καλύτερη **αντίδραση** σε περιστατικά και την **ανάκαμψη** από αυτά. Τέλος, το σχέδιο δράσης προβλέπει τρόπους για την **αποτροπή** παραγόντων κυβερνοαπειλών από την πραγματοποίηση επιθέσεων κατά των συστημάτων υγείας στην Ευρώπη.

Το σχέδιο δράσης θα υλοποιηθεί σε συνεργασία με τους παρόχους υγειονομικής περίθαλψης και το ευρύτερο οικοσύστημα υγείας, τα κράτη μέλη και την κοινότητα κυβερνοασφάλειας. Η συνεργατική προσέγγιση έχει καθοριστική σημασία για τον περαιτέρω προσδιορισμό και τη βελτίωση των δράσεων με τον μεγαλύτερο αντίκτυπο, ώστε όλοι οι κρίσιμοι πάροχοι υγειονομικής περίθαλψης στην Ευρώπη να μπορούν να επωφεληθούν από αυτές. Ως εκ τούτου, η παρούσα ανακοίνωση θα συνοδευτεί από την έναρξη ολοκληρωμένης διαβούλευσης με τα ενδιαφερόμενα μέρη, τη βιομηχανία και τα κράτη μέλη. Η διεθνής συνεργασία είναι σημαντική για την κυβερνοασφάλεια λόγω του διασυνοριακού και διασυνδεδεμένου χαρακτήρα των κυβερνοαπειλών. Συγκρίσιμες απειλές κατά της κυβερνοασφάλειας παρουσιάζονται επίσης στις χώρες της διεύρυνσης και στις γειτονικές χώρες και σε άλλες στρατηγικές χώρες εταίρους της ΕΕ. Αυτό μπορεί να θέσει τελικά σε κίνδυνο την ασφάλεια των κρίσιμων υποδομών στην ΕΕ. Ως εκ τούτου, θα είναι σημαντικό να αντικατοπτρίζονται τα διδάγματα που αντλήθηκαν από την υλοποίηση του σχεδίου δράσης και στη συνεργασία της ΕΕ τόσο με τις χώρες της διεύρυνσης όσο και με άλλες χώρες εταίρους, υπό το πρίσμα των επιπέδων απειλής στα οποία εκτίθενται αντίστοιχα.

2. Πρόκληση για την κυβερνοασφάλεια των νοσοκομείων και των παρόχων υγειονομικής περίθαλψης

Κυβερνοαπειλές για τον τομέα της υγείας

Οι κυβερνοεπιθέσεις αυξάνονται σε παγκόσμιο επίπεδο και εντός της ΕΕ, διαμορφώνοντας ένα ολοένα και πιο σύνθετο και δυναμικό τοπίο απειλών. Οι εξελίξεις στον τομέα της ΤΝ παρέχουν στους

[4] Οδηγία (ΕΕ) 2022/2555 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 14ης Δεκεμβρίου 2022, σχετικά με μέτρα για υψηλό κοινό επίπεδο κυβερνοασφάλειας σε ολόκληρη την Ένωση (οδηγία NIS 2), https://eur-lex.europa.eu/eli/dir/2022/2555.

εγκληματίες και τους κακόβουλους παράγοντες ισχυρά εργαλεία για την αύξηση της ακρίβειας και του αντικτύπου των δραστηριοτήτων τους, ενώ, ταυτόχρονα, αναδιαμορφώνουν τις δυνατότητες κυβερνοάμυνας επιτρέποντας αυτοματοποιημένη δράση κατά των επιθέσεων σε πραγματικό χρόνο.

Το λυτρισμικό εξακολουθεί να αποτελεί κρίσιμη πρόκληση για την κυβερνοασφάλεια στην ΕΕ και σε παγκόσμιο επίπεδο, όπου σύμφωνα με μία έκθεση το παγκόσμιο ετήσιο κόστος εκτιμάται ότι θα υπερβεί τα 250 δισ. EUR έως το 2031[5]. Όταν επιτίθενται εγκληματίες λυτρισμικού, δεν κρυπτογραφούν μόνο τα δεδομένα των θυμάτων για λύτρα, αλλά διαρρέουν όλο και πιο συχνά ευαίσθητες πληροφορίες προκειμένου να ασκήσουν επιπλέον πίεση. Μια άλλη σημαντική πρόκληση είναι οι ευπάθειες του λογισμικού και του υλισμικού: σύμφωνα με τον Οργανισμό της Ευρωπαϊκής Ένωσης για την Κυβερνοασφάλεια (ENISA)[6], η υγειονομική περίθαλψη είναι ο τομέας που δήλωσε τα περισσότερα περιστατικά ασφάλειας σε σχέση με τέτοιες ευπάθειες[7]. Άλλες αυξανόμενες απειλές περιλαμβάνουν τις κατανεμημένες επιθέσεις άρνησης υπηρεσίας (DDoS), οι οποίες σχεδιάζονται με σκοπό να κατακλύσουν ένα στοχευμένο σύστημα με υπερβολική ροή κυκλοφορίας, καθιστώντας το μη προσβάσιμο στους νόμιμους χρήστες[8].

Ο τομέας της υγείας αντιμετωπίζει παρόμοιες τάσεις όσον αφορά τις απειλές για την κυβερνοασφάλεια, με έντονη έμφαση στις επιθέσεις λυτρισμικού. Σύμφωνα με τον ENISA, το λυτρισμικό αντιπροσώπευε το 54 % των περιστατικών κυβερνοασφάλειας που αναλύθηκαν στον τομέα της υγείας κατά την περίοδο 2021-2023. Το 83 % των επιθέσεων είχε οικονομικό κίνητρο, λόγω της υψηλής αξίας των δεδομένων υγειονομικής περίθαλψης, ενώ το 10 % των επιθέσεων είχε ιδεολογικό κίνητρο[9]. Ομοίως, σε έκθεση της Επιτροπής του 2024 διαπιστώθηκε ότι το 71 % των επιθέσεων με επιπτώσεις στην περίθαλψη των ασθενών, όπως η καθυστερημένη θεραπεία, η διάγνωση και η περιορισμένη πρόσβαση σε υπηρεσίες έκτακτης ανάγκης, ήταν επιθέσεις λυτρισμικού[10]. Οι επιθέσεις λυτρισμικού μπορούν να διαταράξουν ιδιαίτερα την παροχή υπηρεσιών υγειονομικής περίθαλψης, θέτοντας σε κίνδυνο την ασφάλεια των ασθενών. Επιπλέον, οι επιθέσεις λυτρισμικού συνδυάζονται πολλές φορές με παραβιάσεις των

[5] Cybersecurity Ventures (1 Ιουνίου 2024): Global Ransomware Damage Costs Predicted To Exceed $265 Billion By 2031 (Οι παγκόσμιες ζημιές από λυτρισμικό προβλέπεται να ξεπεράσουν τα 265 δισ. USD μέχρι το 2031). Διατίθεται στη διεύθυνση https://cybersecurityventures.com/global-ransomware-damage-costs-predicted-to-reach-250-billion-usd-by-2031/.

[6] Κανονισμός (ΕΕ) 2019/881 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 17ης Απριλίου 2019, σχετικά με τον ENISA («Οργανισμός της Ευρωπαϊκής Ένωσης για την Κυβερνοασφάλεια») και με την πιστοποίηση της κυβερνοασφάλειας στον τομέα της τεχνολογίας πληροφοριών και επικοινωνιών (πράξη για την κυβερνοασφάλεια), https://eur-lex.europa.eu/eli/reg/2019/881/oj/ell.

[7] ENISA Threat Landscape: Health Sector (Τοπίο απειλών για τον τομέα της υγείας) (Ιούλιος 2023).

[8] ENISA Threat Landscape 2024 (Τοπίο απειλών για το 2024).

[9] ENISA Threat Landscape: Health Sector (Τοπίο απειλών για τον τομέα της υγείας) (Ιούλιος 2023). Στην έκθεση αναλύθηκαν οι πάροχοι υγειονομικής περίθαλψης, καθώς και άλλοι τύποι οργανισμών, μεταξύ άλλων οι οργανισμοί που διεξάγουν έρευνα στον τομέα της υγείας, οι οντότητες που παρασκευάζουν ορισμένα προϊόντα που σχετίζονται με την υγεία, οι υγειονομικές αρχές, οι οργανισμοί ασφάλισης υγείας, καθώς και οι εγκαταστάσεις θεραπείας εσωτερικής διαμονής και οι πάροχοι κοινωνικών υπηρεσιών. Διατίθεται στη διεύθυνση https://www.enisa.europa.eu/publications/health-threat-landscape.

[10] Ευρωπαϊκή Επιτροπή: Κοινό Κέντρο Ερευνών, Reina, V. και Griesinger, C., Cyber security in the health and medicine sector – A study on available evidence of patient health consequences resulting from cyber incidents in healthcare settings (Κυβερνοασφάλεια στον τομέα της υγείας και της ιατρικής — Μελέτη σχετικά με τα διαθέσιμα στοιχεία για τις επιπτώσεις στην υγεία των ασθενών που προκύπτουν από κυβερνοπεριστατικά σε περιβάλλοντα υγειονομικής περίθαλψης), Υπηρεσία Εκδόσεων της ΕΕ, 2024, https://data.europa.eu/doi/10.2760/693487.

δεδομένων των ασθενών[11], τα οποία συχνά περιλαμβάνουν ευαίσθητα δεδομένα που σχετίζονται με την υγεία και παραβιάζουν το θεμελιώδες δικαίωμα των ανθρώπων στην προστασία των δεδομένων προσωπικού χαρακτήρα.

Ταυτόχρονα, με την αυξανόμενη ψηφιοποίηση της υγειονομικής περίθαλψης διευρύνεται η επιφάνεια έκθεσης σε πιθανές επιθέσεις. Σύμφωνα με την έκθεση για την κατάσταση της Ψηφιακής Δεκαετίας 2024, το 79 % των πολιτών της ΕΕ, κατά μέσο όρο, έχει διαδικτυακή πρόσβαση στα οικεία ηλεκτρονικά μητρώα υγείας στην πρωτοβάθμια περίθαλψη[12]. Τα ηλεκτρονικά μητρώα υγείας, τα συστήματα κλινικών πληροφοριών, τα συστήματα ροής εργασιών των νοσοκομείων, τα συστήματα ΤΠ για τον χειρισμό της επιστροφής δαπανών για θεραπευτικές αγωγές, τα συστήματα ιατρικής απεικόνισης και τα ιατροτεχνολογικά προϊόντα που χρησιμοποιούνται για διαγνωστικούς σκοπούς ή για την παρακολούθηση ασθενών αποτελούν όλα παραδείγματα ψηφιακών εργαλείων που μπορούν να διαδραματίσουν σημαντικό ρόλο στην ενίσχυση της αποδοτικότητας και των επιδόσεων του τομέα της υγείας, αλλά συνιστούν επίσης πιθανούς στόχους κυβερνοεπίθεσης. Συγκεκριμένες δραστηριότητες υγειονομικής περίθαλψης, όπως η εντατική θεραπεία και η ακτινολογική απεικόνιση, ή ιατρικοί τομείς όπως η ογκολογία και η καρδιολογία, που εξαρτώνται σε μεγάλο βαθμό από συσκευές που λειτουργούν ψηφιακά, διατρέχουν ιδιαίτερο κίνδυνο κυβερνοεπιθέσεων. Επιπλέον, τα προβλήματα στην αλυσίδα εφοδιασμού μπορεί να οδηγήσουν στην προμήθεια συσκευών με ανεπαρκή κυβερνοασφάλεια, επιδεινώνοντας τους υφιστάμενους γενικούς κινδύνους.

Για παράδειγμα, κατά τη διάρκεια της πανδημίας της COVID-19, μια επίθεση με λυτρισμικό παρέλυσε μεγάλα τμήματα του ιρλανδικού συστήματος υγειονομικής περίθαλψης, με αποτέλεσμα την ακύρωση τουλάχιστον ορισμένων υπηρεσιών σε 31 από τα 54 νοσοκομεία οξέων περιστατικών το πρωί της ημέρα που σημειώθηκε το περιστατικό[13]. Οι υπηρεσίες υγείας χρειάστηκε να επανέλθουν στη χρήση έντυπων αρχείων, με αποτέλεσμα να επιβραδυνθεί η αποτελεσματικότητα των εργασιών. Η επίθεση προήλθε από μήνυμα ηλεκτρονικού «ψαρέματος» που περιείχε κακόβουλο συνημμένο[14]. Το περιστατικό κατέδειξε τις πιθανότητες κυβερνοεπιθέσεων που εξαπλώνονται σε διάφορα συστήματα και, κατά συνέπεια, τη σημασία της προστασίας ολόκληρης της επιφάνειας έκθεσης σε πιθανές επιθέσεις ενός οργανισμού υγειονομικής περίθαλψης. Υπογράμμισε επίσης τη σημασία της διασφάλισης νοοτροπίας θεμελιώδους κυβερνοϋγιεινής και κυβερνοασφάλειας σε όλους τους οργανισμούς.

Επίπεδο ωριμότητας των νοσοκομείων και των παρόχων υγειονομικής περίθαλψης στον τομέα της κυβερνοασφάλειας

Το τοπίο της υγειονομικής περίθαλψης στην ΕΕ παρουσιάζει μεγάλες διαφορές, καθώς τα νοσοκομεία και άλλοι πάροχοι υγειονομικής περίθαλψης ποικίλλουν σημαντικά όσον αφορά την ιδιοκτησία, τη δομή και το μέγεθος μεταξύ των κρατών μελών. Σε ορισμένες περιπτώσεις, η διακυβέρνηση της υγειονομικής

[11] Σύμφωνα με το τοπίο απειλών του ENISA για τον τομέα της υγείας, στο 43 % των περιστατικών λυτρισμικού που αναλύθηκαν επιβεβαιώθηκε παραβίαση ή κλοπή δεδομένων.
[12] Έκθεση για την κατάσταση της Ψηφιακής Δεκαετίας 2024.
[13] Ιρλανδική αρχή υπηρεσιών υγείας (Health Service Executive) (2021): «Conti cyber attack on the HSE: Independent Post Incident Review».
[14] Ιρλανδική αρχή υπηρεσιών υγείας (Health Service Executive): «Cyber-attack and HSE response». Διατίθεται στη διεύθυνση https://www2.hse.ie/services/cyber-attack/what-happened/.

περίθαλψης μπορεί να βασίζεται σε συγκεντρωτική προσέγγιση σε εθνικό επίπεδο, ενώ σε άλλες σε περιφερειακό και τοπικό επίπεδο· οι πάροχοι υγειονομικής περίθαλψης μπορεί να είναι δημόσιας ή ιδιωτικής ιδιοκτησίας. Επιπλέον, διαφορές μπορεί να υπάρχουν επίσης εντός της ίδιας χώρας, για παράδειγμα όταν υφίστανται σημαντικές κοινωνικοοικονομικές και εδαφικές διαφορές μεταξύ των περιφερειών, με αποτέλεσμα να διαμορφώνεται μια σύνθετη εικόνα. Αυτό το πολύπλοκο τοπίο υγειονομικής περίθαλψης μπορεί να δοκιμαστεί από σημαντικές κρίσεις στον τομέα της υγείας, λόγω μεταδοτικών νόσων, όπως η πανδημία της COVID-19, αλλά και άλλων κινδύνων για την υγεία, που σχετίζονται, για παράδειγμα, με την κλιματική αλλαγή. Τέλος, παρατηρείται σημαντική μεταβλητότητα και κατακερματισμός στο επίπεδο ψηφιοποίησης και υιοθέτησης της τεχνολογίας από τους παρόχους υγειονομικής περίθαλψης. Ένα παράδειγμα αυτής της πολυπλοκότητας είναι ότι η μη διαθεσιμότητα υπηρεσιών που προκαλείται από περιστατικό κυβερνοασφάλειας μπορεί να οδηγήσει σε σοβαρή ζημία και βλάβη σε ασθενείς ακόμα και σε μικρής κλίμακας εγκαταστάσεις υγειονομικής περίθαλψης, συμπεριλαμβανομένων των κλινικών ή των ιατρικών υπηρεσιών έκτακτης ανάγκης που παρέχουν βασική υπηρεσία σε σχετικά μικρό αριθμό χρηστών.

Σύμφωνα με την έκθεση του ENISA του 2024 σχετικά με την κατάσταση της κυβερνοασφάλειας στην Ένωση[15], το επίπεδο ωριμότητας του τομέα της υγείας της ΕΕ στον τομέα της κυβερνοασφάλειας είναι μέτριο και παρατηρούνται μεγάλες διαφορές στο επίπεδο ωριμότητας στον τομέα της κυβερνοασφάλειας μεταξύ των φορέων υγειονομικής περίθαλψης σε ολόκληρη την Ευρώπη. Ελλείψεις παρατηρούνται σε βασικούς τομείς, όπως οι επαρκείς ανθρώπινοι πόροι, οι γνώσεις των οργανισμών σχετικά με τις αλυσίδες εφοδιασμού των τεχνολογιών των πληροφοριών και των επικοινωνιών (ΤΠΕ) που χρησιμοποιούν και η εγκατάσταση σύγχρονων χαρακτηριστικών ασφαλείας στα προϊόντα. Ο τομέας αντιμετωπίζει δυσκολίες με βασικά μέτρα κυβερνοϋγιεινής και θεμελιώδη μέτρα ασφάλειας, όπως καταδεικνύεται από το γεγονός ότι σχεδόν όλοι οι οργανισμοί υγείας που συμμετείχαν στην έρευνα αντιμετωπίζουν προκλήσεις όσον αφορά τη διενέργεια εκτιμήσεων κινδύνου για την κυβερνοασφάλεια, ενώ σχεδόν οι μισοί δεν έχουν διενεργήσει ποτέ ανάλυση κινδύνου[16].

Μια άλλη σημαντική πρόκληση για την κυβερνοασφάλεια των νοσοκομείων είναι το σημείο τομής της τεχνολογίας των πληροφοριών (ΤΠ) και της επιχειρησιακής τεχνολογίας (ΕΤ), όπου πληρούνται διαφορετικές προτεραιότητες ασφάλειας όσον αφορά την εμπιστευτικότητα, τη διαθεσιμότητα και την αξιοπιστία, και όπου η παραβίαση στον έναν τομέα μπορεί να επηρεάσει τον άλλον. Στην έκθεση του ENISA του 2024 σχετικά με την κατάσταση της κυβερνοασφάλειας στην Ένωση τονίζεται περαιτέρω ότι ο τομέας της υγείας δεν αποδίδει επαρκώς όσον αφορά την εγγύηση της ασφάλειας των προϊόντων και των διαδικασιών ΤΠΕ που χρησιμοποιεί, λόγω της μεγάλης ποικιλίας φορέων, συσκευών και προϊόντων υγείας.

Η ποικιλομορφία αυτή, σε συνδυασμό με τα διάφορα επίπεδα ευαισθητοποίησης του προσωπικού και της διοίκησης των νοσοκομείων όσον αφορά την κυβερνοασφάλεια, δημιουργεί μια σύνθετη πρόκληση για τη διασφάλιση της κυβερνοασφάλειας των συστημάτων υγειονομικής περίθαλψης. Για παράδειγμα,

[15] ENISA: Έκθεση του 2024 σχετικά με την κατάσταση της κυβερνοασφάλειας στην Ένωση (Σεπτέμβριος 2024). Διατίθεται στη διεύθυνση https://www.enisa.europa.eu/publications/enisa-threat-landscape-2024.
[16] ENISA Threat Landscape: Health Sector (Τοπίο απειλών για τον τομέα της υγείας) (Ιούλιος 2023). Διατίθεται στη διεύθυνση https://www.enisa.europa.eu/publications/health-threat-landscape.

σύμφωνα με το Ευρωβαρόμετρο του 2024 για τις κυβερνοδεξιότητες, μόνο το 25 % των εταιρειών που συμμετείχαν στην έρευνα στον τομέα της υγείας, της εκπαίδευσης και της κοινωνικής πρόνοιας είχε παράσχει κατάρτιση ή ευαισθητοποίηση σχετικά με την κυβερνοασφάλεια κατά τους προηγούμενους 12 μήνες[17]. Απαιτείται δράση για την προώθηση μιας νοοτροπίας ευαισθητοποίησης όσον αφορά την κυβερνοασφάλεια μεταξύ των επαγγελματιών πρώτης γραμμής του τομέα της υγείας. Για παράδειγμα, οι εναλλαγές προσωπικού, η χρήση κοινόχρηστων σταθμών εργασίας, η ανεπαρκής διαχείριση ελέγχου της ταυτότητας και η χρήση αφαιρούμενων μέσων αποτελούν πρόσθετες πηγές ευπαθειών που επηρεάζουν την κυβερνοασφάλεια των παρόχων υγειονομικής περίθαλψης[18].

Σε πολλές περιπτώσεις, η ΤΠ και η ΕΤ ανατίθενται, τουλάχιστον εν μέρει, σε εξωτερικούς φορείς. Στο Ευρωβαρόμετρο του 2024 διαπιστώθηκε ότι το ποσοστό των εταιρειών που αναθέτουν σε εξωτερικούς φορείς τουλάχιστον ορισμένες πτυχές της κυβερνοασφάλειας είναι υψηλότερο στον τομέα της υγείας, της εκπαίδευσης και της κοινωνικής πρόνοιας, με το 57 % των εταιρειών που συμμετείχαν στην έρευνα να το πράττει[19]. Ομοίως, παρατηρείται έντονη τάση μετάβασης σε υπηρεσίες υπολογιστικού νέφους, η οποία οφείλεται στην ανάγκη για κλιμακούμενη αποθήκευση και διαχείριση δεδομένων, οικονομική αποδοτικότητα, βελτιωμένη συνεργασία και στήριξη για προηγμένες τεχνολογίες, όπως η ΤΝ και το διαδίκτυο των ιατρικών πραγμάτων. Το 2022 το 58 % των οργανισμών υγείας χρησιμοποιούσε ψηφιακή πλατφόρμα υγείας βασιζόμενη στο υπολογιστικό νέφος[20]. Ωστόσο, παρότι η εν λόγω μετάβαση μπορεί να επιφέρει σημαντική βελτίωση της αποτελεσματικότητας, ενέχει επίσης κινδύνους που απαιτούν τεκμηριωμένες αποφάσεις σχετικά με τις δημόσιες συμβάσεις και την ασφαλή παραμετροποίηση.

Πάνω από όλες αυτές τις προκλήσεις είναι το ζήτημα της ανάπτυξης ικανοτήτων και της χρηματοδότησης. Η χρηματοδότηση για την κυβερνοασφάλεια στον τομέα της υγείας είναι περιορισμένη και εξακολουθεί να αποτελεί παγκόσμια πρόκληση σε ολόκληρη την ΕΕ[21]. Επιπλέον, οι εν λόγω χρηματοδοτικές προκλήσεις προκύπτουν στο πλαίσιο της γήρανσης του πληθυσμού, η οποία αναμένεται να δημιουργήσει εκτεταμένες δημοσιονομικές πιέσεις στα συστήματα υγείας της Ευρώπης τις επόμενες δεκαετίες.

Η συνεχιζόμενη χρήση απαρχαιωμένων εργαλείων και παρωχημένων συστημάτων, οι περιορισμένοι πόροι για την πρόληψη ή την αντίδραση σε περιστατικά και τα κενά στην ωριμότητα στον τομέα της κυβερνοασφάλειας οφείλονται συχνά σε ελλείψεις χρηματοδότησης. Τα νοσοκομεία αντιμετωπίζουν τη συνεχή πρόκληση της εξισορρόπησης σύγχρονων, ασφαλών και ψηφιακών υποδομών με άλλες αναγκαίες επενδύσεις για τη βελτίωση της περίθαλψης των ασθενών, όπως η πρόσληψη ιατρών και άλλων επαγγελματιών του τομέα της υγείας, η εφαρμογή νέων διαγνωστικών και θεραπευτικών μεθόδων

[17]Εκτακτο Ευρωβαρόμετρο 547 για τις κυβερνοδεξιότητες (Μάιος 2024). Διατίθεται στη διεύθυνση https://europa.eu/eurobarometer/surveys/detail/3176.

[18]Panacea – People-centric cybersecurity in healthcare (2021): White Paper – Lessons learnt from PANACEA on the cyber-protection of hospitals and care centres.

[19] Έκτακτο Ευρωβαρόμετρο 547 για τις κυβερνοδεξιότητες (Μάιος 2024). Διατίθεται στη διεύθυνση https://europa.eu/eurobarometer/surveys/detail/3176.

[20] ENISA: NIS Investments Report 2022 (Έκθεση για τις επενδύσεις στην ασφάλεια δικτύων και πληροφοριών 2022) (Νοέμβριος 2022). Διατίθεται στη διεύθυνση https://www.enisa.europa.eu/publications/nis-investments-2022.

[21] Η οργάνωση και η παροχή υγειονομικών υπηρεσιών και ιατρικής περίθαλψης αποτελεί εθνική αρμοδιότητα σύμφωνα με το άρθρο 168 της Συνθήκης για τη λειτουργία της Ευρωπαϊκής Ένωσης, και η χρηματοδότηση των συστημάτων υγειονομικής περίθαλψης ποικίλλει μεταξύ των κρατών μελών.

και η απόκτηση συσκευών. Σύμφωνα με τον ENISA[22], ο τομέας της υγείας κατατάσσεται μόλις στην 7η θέση από τους 12 τομείς που μελετήθηκαν όσον αφορά το ποσοστό των δαπανών για την ασφάλεια των πληροφοριών επί των συνολικών δαπανών ΤΠ, με το 8,3 % να είναι η διάμεση τιμή στον τομέα της υγείας.

3. Ευρωπαϊκό Κέντρο Υποστήριξης της Κυβερνοασφάλειας για τα νοσοκομεία και τους παρόχους υγειονομικής περίθαλψης

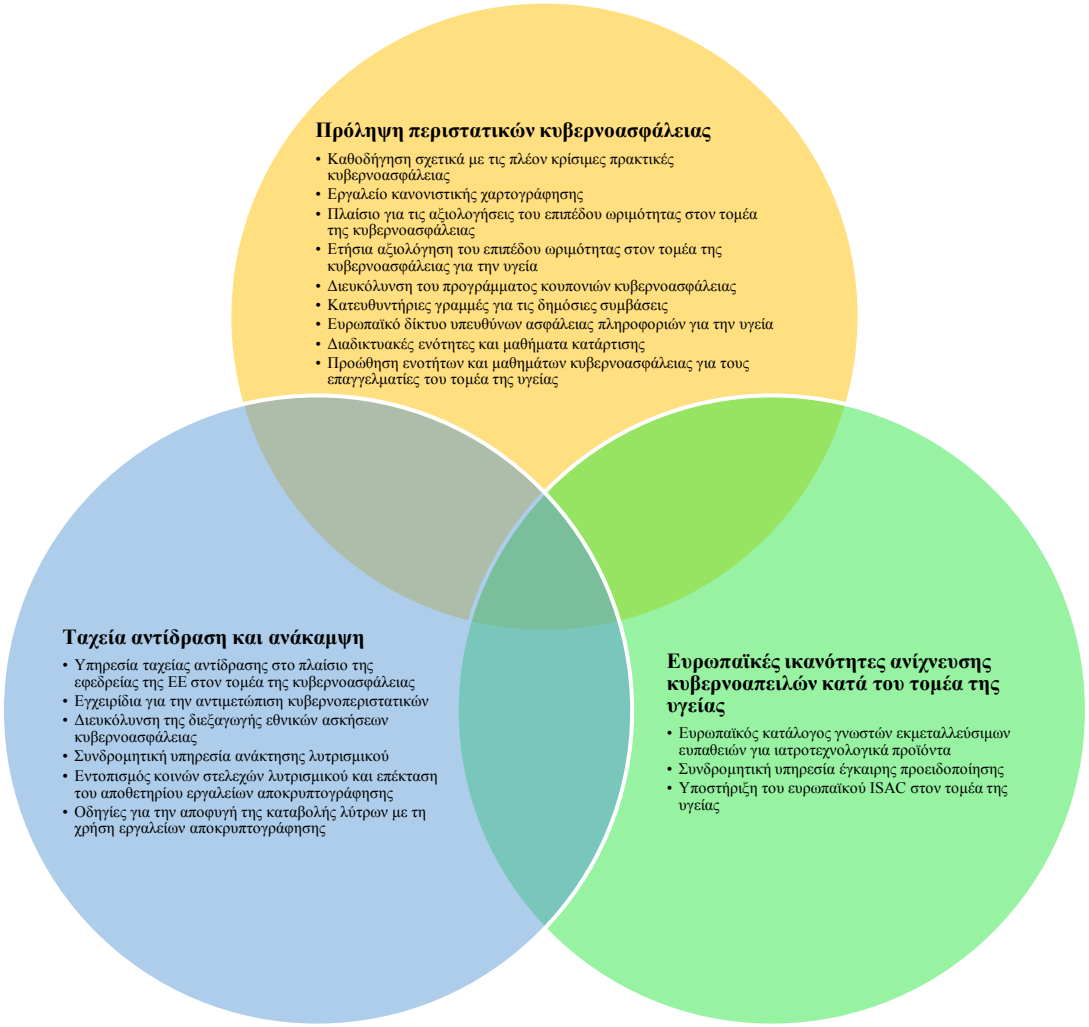
Το πλαίσιο κυβερνοασφάλειας της ΕΕ προσφέρει ευρύ φάσμα εργαλείων τα οποία θα πρέπει να αξιοποιηθούν για τη βελτίωση της ασφάλειας και της ανθεκτικότητας των νοσοκομείων και των παρόχων υγειονομικής περίθαλψης. Για την αντιμετώπιση των πολυάριθμων προκλήσεων που επισημαίνονται ανωτέρω, είναι αναγκαίο να αναπτυχθεί μια ενοποιημένη, στρατηγική προσέγγιση σε επίπεδο ΕΕ, η οποία θα συγκεντρώνει τους πόρους, την εμπειρογνωσία και τα εργαλεία που απαιτούνται για την αποτελεσματική αντιμετώπιση των κυβερνοαπειλών. Η ολοκληρωμένη επισκόπηση, καθώς και ο καλύτερος σχεδιασμός και συντονισμός είναι απαραίτητα στοιχεία για την στήριξη των παρόχων υγειονομικής περίθαλψης σε ολόκληρη την ΕΕ κατά την ενίσχυση της άμυνάς τους. Για να επιτευχθεί αυτό, ο ENISA είναι ο πλέον κατάλληλος φορέας για να δημιουργήσει, εντός του οργανισμού του, ένα ειδικό **Ευρωπαϊκό Κέντρο Υποστήριξης της Κυβερνοασφάλειας για τα νοσοκομεία και τους παρόχους υγειονομικής περίθαλψης**[23] στο πλαίσιο της εντολής του[24] για τη διασφάλιση και τη στήριξη των υποδομών ζωτικής σημασίας της ΕΕ.

Το Κέντρο Υποστήριξης θα πρέπει να **καταρτίσει σταδιακά έναν ολοκληρωμένο κατάλογο υπηρεσιών που θα καλύπτει τις ανάγκες των νοσοκομείων και των παρόχων υγειονομικής περίθαλψης**, στον οποίο θα περιγράφεται το φάσμα των διαθέσιμων υπηρεσιών ετοιμότητας, πρόληψης, ανίχνευσης και αντίδρασης. Σε συνεργασία με τις αρχές των κρατών μελών και με βάση τις εμπειρίες των νοσοκομείων και των παρόχων υγειονομικής περίθαλψης, το Κέντρο Υποστήριξης θα πρέπει να αναπτύξει ένα φιλικό προς τον χρήστη και εύκολα προσβάσιμο αποθετήριο όλων των διαθέσιμων μέσων σε ευρωπαϊκό, εθνικό και περιφερειακό επίπεδο. Κατά τη διεξαγωγή των δραστηριοτήτων του, θα πρέπει να διασφαλίζει τον κατάλληλο συντονισμό με τα κράτη μέλη και να στηρίζει την ιεράρχηση των προτεραιοτήτων και την υλοποίηση δράσεων, όπως απαιτείται σε πραγματικό χρόνο.

Ως σημαντικό δομικό στοιχείο για την ανάπτυξη του καταλόγου υπηρεσιών του Κέντρου Υποστήριξης, η Επιτροπή θα προτείνει τη δρομολόγηση πιλοτικών έργων σε ολόκληρη την ΕΕ για την ανάπτυξη βέλτιστων πρακτικών για την κυβερνοϋγιεινή και την εκτίμηση κινδύνων για την ασφάλεια, καθώς και για την αντιμετώπιση της ανάγκης συνεχούς παρακολούθησης της κυβερνοασφάλειας, συλλογής πληροφοριών για απειλές και αντίδρασης σε περιστατικά με τη χρήση προηγμένων λύσεων κυβερνοασφάλειας. Τα αποτελέσματα αυτών των πιλοτικών έργων, τα οποία θα χρηματοδοτηθούν από

[22] ENISA: NIS Investments Report 2022 (Έκθεση για τις επενδύσεις στην ασφάλεια δικτύων και πληροφοριών 2022) (Νοέμβριος 2022). Διατίθεται στη διεύθυνση https://www.enisa.europa.eu/publications/nis-investments-2022.
[23] Στο παρόν έγγραφο, ο όρος «Κέντρο Υποστήριξης» χρησιμοποιείται αδιακρίτως.
[24] Κανονισμός (ΕΕ) 2019/881 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 17ης Απριλίου 2019, σχετικά με τον ENISA («Οργανισμός της Ευρωπαϊκής Ένωσης για την Κυβερνοασφάλεια») και με την πιστοποίηση της κυβερνοασφάλειας στον τομέα της τεχνολογίας πληροφοριών και επικοινωνιών και για την κατάργηση του κανονισμού (ΕΕ) αριθ. 526/2013 (πράξη για την κυβερνοασφάλεια) (ΕΕ L 151 της 7.6.2019, σ. 15).

το πρόγραμμα «Ψηφιακή Ευρώπη» που εκτελείται από το Ευρωπαϊκό Κέντρο Αρμοδιότητας για Θέματα Κυβερνοασφάλειας (ECCC), θα τροφοδοτήσουν περαιτέρω δράσεις σε επίπεδο ΕΕ, συμπεριλαμβανομένων των εργασιών του Κέντρου Υποστήριξης.



Σχήμα 1: Ιδέες για τον κατάλογο υπηρεσιών του Κέντρου Υποστήριξης των νοσοκομείων και των παρόχων υγειονομικής περίθαλψης

3.1. Πρόληψη περιστατικών κυβερνοασφάλειας

Απλές ενέργειες που αλλάζουν τις πιθανότητες

Βασικά μέτρα κυβερνοασφάλειας, όπως η διασφάλιση της επικαιροποίησης των συστημάτων, η διαχείριση εφεδρικών αντιγράφων και η εφαρμογή πολυπαραγοντικής επαλήθευσης της ταυτότητας

μπορούν, σύμφωνα με μία εκτίμηση, να προστατεύσουν τους οργανισμούς από έως και το 98 % των επιθέσεων[25]. Πολλά από τα πιο αποτελεσματικά μέτρα κυβερνοϋγιεινής και διαχείρισης κινδύνων είναι σχετικά απλά να υιοθετηθούν και, κατά συνέπεια, αποτελούν εφικτό στόχο για τη βελτίωση της κυβερνοασφάλειας. Ως εκ τούτου, ένας από τους βασικούς ρόλους του Κέντρου Υποστήριξης θα πρέπει να είναι **η ανάπτυξη σαφούς, στοχευμένης καθοδήγησης που θα επισημαίνει τις πλέον κρίσιμες πρακτικές κυβερνοασφάλειας και θα βοηθά τους παρόχους υγειονομικής περίθαλψης στην εφαρμογή τους**. Η υποστήριξη αυτή πρέπει να επεκταθεί πέραν των μεγάλων νοσοκομείων ώστε να περιλαμβάνει εξατομικευμένες συμβουλές για μικρότερες οντότητες, όπως τοπικά ιατρεία γενικών ιατρών και ειδικευμένες κλινικές, οι οποίες συχνά δεν διαθέτουν τους πόρους για τη σύσταση ειδικών ομάδων κυβερνοασφάλειας, αλλά παραμένουν εξίσου ευάλωτες σε επιθέσεις. Επιπλέον, είναι αναγκαίο να ληφθεί υπόψη η περιφερειακή σημασία συγκεκριμένων φορέων υγειονομικής περίθαλψης για τη διασφάλιση της περίθαλψης ασθενών, για παράδειγμα σε αραιοκατοικημένες περιοχές. Τα ερευνητικά ιδρύματα στον τομέα της υγείας που χειρίζονται μεγάλο όγκο ευαίσθητων δεδομένων προσωπικού χαρακτήρα θα μπορούσαν επίσης να επωφεληθούν από τη λήψη καθοδήγησης για βασικά μέτρα κυβερνοασφάλειας με σκοπό την ενίσχυση της ανθεκτικότητάς τους.

Οι οργανισμοί υγειονομικής περίθαλψης υπόκεινται επίσης σε σειρά υποχρεώσεων που σχετίζονται με την κυβερνοασφάλεια και απορρέουν από τη νομοθεσία της ΕΕ[26]. Παρότι οι υποχρεώσεις αυτές έχουν ζωτική σημασία για τη διασφάλιση υψηλής κοινής βάσης για την κυβερνοασφάλεια και την ασφάλεια των δεδομένων, είναι σημαντικό να διασφαλιστεί ότι η πλοήγηση στο κανονιστικό τοπίο δεν είναι αδικαιολόγητα δύσκολη και επαχθής. Η έντονη εστίαση στη συμμόρφωση δεν θα πρέπει να προσκρούει στον στόχο της προώθησης μιας ισχυρής νοοτροπίας κυβερνοασφάλειας. Ένα **εργαλείο κανονιστικής χαρτογράφησης με εύκολη πρόσβαση μπορεί να συμβάλει στην ελαχιστοποίηση της διοικητικής επιβάρυνσης για τις οντότητες που υπόκεινται σε πολλαπλά ρυθμιστικά μέσα**. Παράλληλα με την ανάπτυξη κατευθυντήριων γραμμών και εργαλείων, το Κέντρο Υποστήριξης θα πρέπει να συνεργαστεί στενά με την Επιτροπή και τα κράτη μέλη για την ανάπτυξη και τη διάδοση ενός τέτοιου εργαλείου το συντομότερο δυνατόν. Ως εκ τούτου, το Κέντρο Υποστήριξης θα διαδραματίσει σημαντικό ρόλο στο να

[25] Έκθεση της Microsoft για την ψηφιακή άμυνα 2022. Διατίθεται στη διεύθυνση https://www.microsoft.com/en-us/security/security-insider/intelligence-reports/microsoft-digital-defense-report-2022.

[26] Όπως η οδηγία NIS2, ο κανονισμός (ΕΕ) 2024/2847 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 23ης Οκτωβρίου 2024, σχετικά με οριζόντιες απαιτήσεις κυβερνοασφάλειας για προϊόντα με ψηφιακά στοιχεία (κανονισμός για την κυβερνοανθεκτικότητα), https://eur-lex.europa.eu/eli/reg/2024/2847/oj/ell, ο κανονισμός (ΕΕ) 2017/745 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 5ης Απριλίου 2017, για τα ιατροτεχνολογικά προϊόντα, https://eur-lex.europa.eu/eli/reg/2017/745/oj/ell (κανονισμός για τα ιατροτεχνολογικά προϊόντα), ο κανονισμός (ΕΕ) 2017/746 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 5ης Απριλίου 2017, για τα in vitro διαγνωστικά ιατροτεχνολογικά προϊόντα (κανονισμός για τα in vitro διαγνωστικά ιατροτεχνολογικά προϊόντα), https://eur-lex.europa.eu/eli/reg/2017/746/oj/ell, ο κανονισμός (ΕΕ) 2016/679 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 27ης Απριλίου 2016, για την προστασία των φυσικών προσώπων έναντι της επεξεργασίας των δεδομένων προσωπικού χαρακτήρα και για την ελεύθερη κυκλοφορία των δεδομένων αυτών (Γενικός Κανονισμός για την Προστασία Δεδομένων), https://eur-lex.europa.eu/legal-content/EL/TXT/?uri=CELEX:32016R0679, ο κανονισμός (ΕΕ) 2024/1689 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 13ης Ιουνίου 2024, για τη θέσπιση εναρμονισμένων κανόνων σχετικά με την τεχνητή νοημοσύνη, https://eur-lex.europa.eu/legal-content/EL/TXT/?uri=CELEX:32024R1689, η πρόταση κανονισμού του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου σχετικά με τον ευρωπαϊκό χώρο δεδομένων για την υγεία, [COM(2022) 197 final], https://eur-lex.europa.eu/legal-content/EL/TXT/?uri=celex:52022PC0197. Οι διαπραγματεύσεις ολοκληρώθηκαν με πολιτική συμφωνία την άνοιξη του 2024 και, μετά την οριστικοποίησή του, αναμένεται η δημοσίευσή του στην Επίσημη Εφημερίδα την άνοιξη του 2025.

καταστούν οι κανόνες κυβερνοασφάλειας απλοί ως προς την κατανόηση και την εφαρμογή, για παράδειγμα με την παροχή οδηγιών εφαρμογής[27] και, όταν απαιτείται, με την προώθηση σχετικών προτύπων.

Τα επικείμενα **ευρωπαϊκά πορτοφόλια ψηφιακής ταυτότητας** αποτελούν ένα ακόμα εργαλείο για τη διευκόλυνση της απλής εφαρμογής ορθών πρακτικών κυβερνοϋγιεινής. Η μείωση της εξάρτησης από μηχανισμούς μη ισχυρής ταυτοποίησης, όπως οι κωδικοί πρόσβασης, είναι απαραίτητη για τον μετριασμό των κινδύνων μη εξουσιοδοτημένης πρόσβασης σε δεδομένα υγείας. Η στροφή προς τις ασφαλείς λύσεις σύνδεσης που βασίζονται σε αξιόπιστη ταυτοποίηση έχει καθοριστική σημασία. Το πορτοφόλι ψηφιακής ταυτότητας της ΕΕ προσφέρει μια εναρμονισμένη προσέγγιση σε επίπεδο ΕΕ όσον αφορά την ηλεκτρονική ταυτοποίηση για τους επαγγελματίες του τομέα της υγείας, παρέχοντας αξιόπιστη και ενιαία λύση από το τέλος του 2026. Όλα τα επιγραμμικά συστήματα πληροφόρησης για την υγεία που απαιτούνται για την εφαρμογή αυστηρής επαλήθευσης ταυτότητας χρήστη θα υποχρεούνται να αποδέχονται το πορτοφόλι για σκοπούς ταυτοποίησης από το τέλος του 2027[28].

Ετοιμότητα και στοχευμένη υποστήριξη

Οι δοκιμές ετοιμότητας, που περιλαμβάνουν δράσεις όπως οι δοκιμές διείσδυσης, αποτελούν ακρογωνιαίο λίθο της αποτελεσματικής κυβερνοασφάλειας, και η Επιτροπή έχει ήδη διαθέσει στον ENISA χρηματοδότηση για πιλοτικές πρωτοβουλίες ετοιμότητας, από τις οποίες προέκυψε ότι ο τομέας της υγείας συγκαταλέγεται στους τομείς με τη μεγαλύτερη ζήτηση για δοκιμές και περαιτέρω αξιολογήσεις με σκοπό τον εντοπισμό κενών όσον αφορά την ωριμότητα στον τομέα της κυβερνοασφάλειας. Μετά την έναρξη ισχύος της πράξης για την αλληλεγγύη στον κυβερνοχώρο, οι προσπάθειες αυτές θα επεκταθούν σημαντικά, με το ECCC να αναλαμβάνει ηγετικό ρόλο. Για την αντιμετώπιση αυτής της ανάγκης, η Επιτροπή θα προτείνει, σε διαβούλευση με την ομάδα συνεργασίας για την ασφάλεια δικτύων και πληροφοριών (ομάδα συνεργασίας NIS), το EU-CyCLONe[29] και τον ENISA, να προσδιοριστεί η υγεία ως τομέας για τον οποίο μπορεί να παρασχεθεί στήριξη για **συντονισμένες δοκιμές ετοιμότητας** στο πλαίσιο της πράξης για την αλληλεγγύη στον κυβερνοχώρο. Επιπλέον, το Κέντρο Υποστήριξης θα πρέπει να αναπτύξει ένα **προσαρμοσμένο πλαίσιο για τις αξιολογήσεις του επιπέδου ωριμότητας στον τομέα της κυβερνοασφάλειας ειδικά για την υγειονομική περίθαλψη**. Οι εν λόγω αξιολογήσεις του επιπέδου ωριμότητας θα παρέχουν στις οντότητες αξιοποιήσιμες πληροφορίες σχετικά με τις ευπάθειές τους, ενώ παράλληλα θα τους επιτρέπουν να αποδεικνύουν την ετοιμότητά τους στον τομέα της κυβερνοασφάλειας σε ασθενείς και ενδιαφερόμενα μέρη, οικοδομώντας εμπιστοσύνη στις υπηρεσίες τους. Σε συγκεντρωτικό επίπεδο, το Κέντρο Υποστήριξης θα πρέπει να διενεργεί **ετήσια αξιολόγηση της ωριμότητας στον τομέα της κυβερνοασφάλειας για την υγεία**, η οποία θα παρέχει σαφή επισκόπηση της κυβερνοασφάλειας του τομέα της υγείας τόσο σε εθνικό όσο και σε ενωσιακό επίπεδο.

[27] Η εκπόνηση κατευθυντήριων γραμμών για την ερμηνεία του Γενικού Κανονισμού για την Προστασία Δεδομένων (ΓΚΠΔ) εμπίπτει στην αρμοδιότητα του Ευρωπαϊκού Συμβουλίου Προστασίας Δεδομένων (ΕΣΠΔ). Η εκπόνηση κατευθυντήριων γραμμών από τον ENISA θα πρέπει να σέβεται πλήρως τα προνόμια του ΕΣΠΔ.
[28] Άρθρο 5στ παράγραφοι 1 έως 2 του κανονισμού (ΕΕ) αριθ. 910/2014.
[29] Ευρωπαϊκό δίκτυο οργανισμών διασύνδεσης για τις κρίσεις στον κυβερνοχώρο.

Ο τομέας της υγείας βασίζεται σε μεγάλο βαθμό σε εξωτερικούς αναδόχους υπηρεσιών κυβερνοασφάλειας[30], κάτι που αναδεικνύει την ανάγκη για στοχευμένη στήριξη προκειμένου να ενισχυθούν οι αμυντικές γραμμές. Με βάση τις επιτυχημένες πρωτοβουλίες, όπως τα κουπόνια καινοτομίας της ΕΕ, **τα κράτη μέλη θα πρέπει να εξετάσουν στοχευμένα μέτρα, όπως τα κουπόνια κυβερνοασφάλειας για πολύ μικρά, μικρά και μεσαία νοσοκομεία και παρόχους υγειονομικής περίθαλψης**. Τα εν λόγω κουπόνια θα παρέχουν χρηματοδοτική συνδρομή για τη θέσπιση ειδικών μέτρων κυβερνοασφάλειας. Η ιεράρχηση της χορήγησης κουπονιών θα πρέπει να βασίζεται στα πορίσματα των δοκιμών ετοιμότητας και των αξιολογήσεων του επιπέδου ωριμότητας.

Η τοπική γνώση και το τοπικό πλαίσιο έχουν καίρια σημασία για την αποτελεσματική ανάπτυξη των κουπονιών ή άλλων προγραμμάτων στήριξης, διασφαλίζοντας τη συνάφεια και την προσβασιμότητα. Τα ταμεία της ΕΕ, όπως το Ευρωπαϊκό Ταμείο Περιφερειακής Ανάπτυξης, δραστηριοποιούνται ήδη στη στήριξη πρωτοβουλιών για την κυβερνοασφάλεια και την ψηφιακή υγεία και, ως εκ τούτου, θα μπορούσαν να χρησιμεύσουν ως μέσο ανάπτυξης στοχευμένων συστημάτων κουπονιών κυβερνοασφάλειας για τους παρόχους υγειονομικής περίθαλψης. Για την προώθηση αυτής της προσπάθειας, το Κέντρο Υποστήριξης θα συνεργαστεί με τα κράτη μέλη και τις αρχές των περιφερειακών προγραμμάτων με στόχο τη στήριξη της ανάπτυξης των εν λόγω περιφερειακών συστημάτων κουπονιών, με βάση τα διδάγματα που αντλήθηκαν από υφιστάμενα εθνικά έργα, καθώς και από δράσεις που χρηματοδοτούνται στο πλαίσιο του προγράμματος «Ψηφιακή Ευρώπη», ώστε να διασφαλιστεί η πρακτική και αποτελεσματική εφαρμογή.

Επιπλέον, από το 2014 τα προγράμματα «Ορίζων» διαδραμάτισαν καθοριστικό ρόλο στη χρηματοδότηση μιας σειράς ερευνητικών πρωτοβουλιών με επίκεντρο την ενίσχυση της ανθεκτικότητας των ιδρυμάτων υγειονομικής περίθαλψης, όπως τα νοσοκομεία, έναντι των κυβερνοαπειλών, και τον μετριασμό των κινδύνων που συνδέονται με την κατάχρηση αναδυόμενων τεχνολογιών. Τα αποτελέσματα που προέκυψαν περιλαμβάνουν μια σειρά εξειδικευμένων εργαλείων, πλαισίων και συστημάτων, όπως εργαλεία εκτίμησης κινδύνου, πλατφόρμες ανταλλαγής δεδομένων για τη διαφύλαξη της ιδιωτικής ζωής, κρυπτογραφικές λύσεις, προγράμματα κατάρτισης για την ευαισθητοποίηση στον τομέα της κυβερνοασφάλειας και συστήματα ανίχνευσης απειλών σε πραγματικό χρόνο. Ειδικότερα, οι λύσεις αυτές επικυρώθηκαν με αυστηρά κριτήρια μέσω πιλοτικών εφαρμογών σε πραγματικές συνθήκες σε περιβάλλοντα υγειονομικής περίθαλψης, διασφαλίζοντας την αποτελεσματικότητα και την πρακτική εφαρμογή τους όσον αφορά την προστασία από κυβερνοαπειλές.

Διασφάλιση των αλυσίδων εφοδιασμού στον τομέα της υγειονομικής περίθαλψης

Βασική πρόκληση για τους οργανισμούς υγειονομικής περίθαλψης συνιστά η διαχείριση πολύπλοκων αλυσίδων εφοδιασμού ΤΠΕ, οι οποίες περιλαμβάνουν μια σειρά προϊόντων, όπως τα συνδεδεμένα ιατροτεχνολογικά προϊόντα, τα συστήματα ηλεκτρονικών μητρώων υγείας και το υλισμικό γραφείου. Τα νοσοκομεία και οι πάροχοι υγειονομικής περίθαλψης χρειάζονται αξιόπιστα και ασφαλή συστήματα και υπηρεσίες ΤΠΕ για τις δραστηριότητές τους. Για να συμβάλει στην αντιμετώπιση των προκλήσεων

[30] Βλ. έκθεση του ENISA για τις επενδύσεις στην ασφάλεια δικτύων και πληροφοριών του 2023 (Νοέμβριος 2023), στην οποία τονίζεται η σημασία της εξωτερικής στήριξης για τον έλεγχο και τη συμμόρφωση στον τομέα της κυβερνοασφάλειας. Διατίθεται στη διεύθυνση https://www.enisa.europa.eu/publications/nis-investments-2023.

κυβερνοασφάλειας στον τομέα της υγείας, η ομάδα συνεργασίας NIS θα πρέπει να διενεργήσει **συντονισμένη εκτίμηση κινδύνου για την ασφάλεια, αξιολογώντας τόσο τους τεχνικούς όσο και τους στρατηγικούς κινδύνους που σχετίζονται με τις αλυσίδες εφοδιασμού ιατροτεχνολογικών προϊόντων και προτείνοντας μέτρα μετριασμού**[31]. Κατά περίπτωση, η ομάδα συνεργασίας NIS θα πρέπει να συνεργαστεί με το Συντονιστικό Όργανο Ιατροτεχνολογικών Προϊόντων.

Η πράξη για την κυβερνοανθεκτικότητα είναι ένα νέο, ολοκληρωμένο πλαίσιο που καθορίζει απαιτήσεις κυβερνοασφάλειας για τον προγραμματισμό, τον σχεδιασμό, την ανάπτυξη, καθώς και τον χειρισμό, τις διορθώσεις και την αναφορά ευπαθειών που αποτελούν αντικείμενο ενεργού εκμετάλλευσης όσον αφορά σχεδόν όλα τα προϊόντα υλισμικού και λογισμικού, σε κάθε στάδιο της αλυσίδας αξίας[32]. Τα ιατροτεχνολογικά προϊόντα αποτελούν είδος προϊόντος που χρησιμοποιείται σε έναν από τους πλέον ευαίσθητους τομείς της κοινωνίας μας. Οι απαιτήσεις κυβερνοασφάλειας για τα εν λόγω προϊόντα απορρέουν από τον προϋπάρχοντα κανονισμό για τα ιατροτεχνολογικά προϊόντα και τον κανονισμό για τα in vitro διαγνωστικά ιατροτεχνολογικά προϊόντα[33]. Στο πλαίσιο της υπό εξέλιξη αξιολόγησης των εν λόγω κανονισμών εξετάζονται οι δυνατότητες μεγαλύτερης συνεκτικότητας και συνεργειών μεταξύ των εν λόγω πλαισίων, προκειμένου να παρέχεται εγγυημένη απλούστευση και προηγμένη κυβερνοασφάλεια.

Επιπλέον, τα πορίσματα της εκτίμησης κινδύνου θα πρέπει να παρέχουν στους οργανισμούς υγειονομικής περίθαλψης στήριξη κατά την επανεξέταση των πρακτικών κυβερνοασφάλειας στην αλυσίδα εφοδιασμού τους, όπως απαιτείται βάσει της οδηγίας NIS2, και θα μπορούσαν να τροφοδοτήσουν την κατάρτιση νέων **κατευθυντήριων γραμμών για τις δημόσιες συμβάσεις**[34]. Οι εν λόγω κατευθυντήριες γραμμές, τις οποίες θα καταρτίσει ο ENISA μέσω του Κέντρου Υποστήριξης, θα πρέπει να αντικατοπτρίζουν τις πρόσφατες τάσεις, όπως η νεφοποίηση της αποθήκευσης δεδομένων ασθενών, συμπεριλαμβανομένης της ανάγκης ασφαλούς μετάβασης των ηλεκτρονικών δεδομένων υγείας σε περιβάλλοντα υπολογιστικού νέφους. Επιπλέον, οι νέες κατευθυντήριες γραμμές θα πρέπει να προσφέρουν στους οργανισμούς πρακτικά εργαλεία ώστε να παρακολουθούν τις αλυσίδες εφοδιασμού τους, συμπεριλαμβανομένων των παρόχων διαχειριζόμενων υπηρεσιών ασφάλειας, των εκθέσεων βεβαίωσης ή των εκτιμήσεων κινδύνου από τρίτους.

Όσον αφορά το υπολογιστικό νέφος, απαιτείται περαιτέρω δράση για την αντιμετώπιση των μοναδικών προκλήσεων της διαχείρισης ευαίσθητων δεδομένων υγειονομικής περίθαλψης, συμπεριλαμβανομένων των αυξημένων κινδύνων για την ασφάλεια, την ιδιωτικότητα και τη λειτουργία. Για την ενίσχυση των διασφαλίσεων, οι εμπειρογνώμονες συνιστούν να ενσωματωθεί στις υπηρεσίες υπολογιστικού νέφους η

[31] Σύμφωνα με το άρθρο 22 της οδηγίας NIS2.
[32] Σε πρώτο στάδιο, από την 1η Αυγούστου 2025 ευρείες κατηγορίες ραδιοεξοπλισμού, που δεν εμπίπτουν στο πεδίο εφαρμογής του κανονισμού για τα ιατροτεχνολογικά προϊόντα και του κανονισμού για τα in vitro διαγνωστικά ιατροτεχνολογικά προϊόντα, θα πρέπει να συμμορφώνονται με τις βασικές απαιτήσεις της οδηγίας για τον ραδιοεξοπλισμό οι οποίες σχετίζονται με την κυβερνοασφάλεια κατά τη διάθεσή τους στην ενιαία αγορά. Σε δεύτερο στάδιο, από τις 11 Δεκεμβρίου 2027 θα τεθεί σε εφαρμογή η πράξη για την κυβερνοανθεκτικότητα.
[33] Τον Δεκέμβριο του 2019 η ομάδα συνεργασίας για τα ιατροτεχνολογικά προϊόντα εξέδωσε έγγραφο καθοδήγησης σχετικά με την κυβερνοασφάλεια των ιατροτεχνολογικών προϊόντων, προκειμένου να στηρίξει τους κατασκευαστές στην εκπλήρωση των απαιτήσεων του παραρτήματος Ι των δύο κανονισμών: https://ec.europa.eu/docsroom/documents/41863.
[34] Με βάση τις κατευθυντήριες γραμμές του ENISA του 2020 για τις δημόσιες συμβάσεις στον τομέα της κυβερνοασφάλειας στα νοσοκομεία (Φεβρουάριος 2020). Διατίθεται στη διεύθυνση https://www.enisa.europa.eu/publications/good-practices-for-the-security-of-healthcare-services.

«ασφάλεια εξ ορισμού και εκ σχεδιασμού». Η προσέγγιση αυτή δίνει προτεραιότητα στις ασφαλείς υποδομές, στην προορατική διαχείριση της ευπάθειας και στον συνδυασμό κυβερνητικών και ιδιωτικών λύσεων υπολογιστικού νέφους. Η συνεχής παρακολούθηση και οι ειδικές ανά προμηθευτή βεβαιώσεις, όπως οι πιστοποιήσεις των παρόχων ασφάλειας και οι έλεγχοι συμμόρφωσης με εθνικά και διεθνή πρότυπα, έχουν επίσης καίρια σημασία για τη διασφάλιση αυστηρών πρακτικών ασφάλειας.

Όσον αφορά υπηρεσίες όπως η υποδομή ως υπηρεσία (IaaS), η πλατφόρμα ως υπηρεσία (PaaS) και το λογισμικό ως υπηρεσία (SaaS), η εφαρμογή της ασφάλειας είναι συχνά ευθύνη του πελάτη. Ωστόσο, πολλοί οργανισμοί υγειονομικής περίθαλψης δεν διαθέτουν τους πόρους ώστε να ανταποκριθούν ανεξάρτητα στις απαιτήσεις αυτές. Για την αντιμετώπιση αυτού του προβλήματος, **οι πάροχοι υπηρεσιών υπολογιστικού νέφους θα πρέπει να ενθαρρύνονται να εφαρμόζουν βασικά μέτρα ασφάλειας ως τυποποιημένο χαρακτηριστικό**. Τα μέτρα αυτά θα μειώνουν τον κίνδυνο εσφαλμένης παραμετροποίησης, θα διατηρούν τη συνεπή προστασία σε όλα τα περιβάλλοντα που τελούν υπό τη διαχείριση των πελατών και θα παρέχουν μεγαλύτερη διασφάλιση στους χρήστες. Η θέσπιση μιας βάσης ασφάλειας εξ ορισμού θα είχε ως στόχο να εξισορροπήσει την ισχυρή προστασία με την πρακτικότητα, διασφαλίζοντας τη χρηστικότητα για ένα ευρύ φάσμα οργανισμών υγειονομικής περίθαλψης. Η προσπάθεια αυτή συνεπάγεται τη στενή συνεργασία μεταξύ των παρόχων υπολογιστικού νέφους και του τομέα της υγείας, αξιοποιώντας βέλτιστες πρακτικές του κλάδου για τη δημιουργία αποτελεσματικών και κλιμακούμενων λύσεων.

Κατάρτιση και ανάπτυξη δεξιοτήτων

Η ύπαρξη εργατικού δυναμικού με περιζήτητες δεξιότητες είναι σημαντική για τη μακροπρόθεσμη βιώσιμη ανάπτυξη και ανταγωνιστικότητα στην Ευρώπη, καθώς και για τις υπηρεσίες υψηλής ποιότητας, συμπεριλαμβανομένων των υπηρεσιών υγειονομικής περίθαλψης. Η έλλειψη ειδικευμένων επαγγελματιών στον τομέα της κυβερνοασφάλειας αποτελεί σημαντική πρόκληση σε ολόκληρη την Ευρώπη, με το κενό να εκτιμάται στους 299 000 επαγγελματίες για την κάλυψη των αναγκών του εργατικού δυναμικού στην ΕΕ[35]. Σύμφωνα με το Ευρωβαρόμετρο του 2024 για τις κυβερνοδεξιότητες[36], το 81 % των εταιρειών θεωρούν ότι οι δυσκολίες στην πρόσληψη προσωπικού στον τομέα της κυβερνοασφάλειας αποτελούν βασικό κίνδυνο πιθανών κυβερνοεπιθέσεων. Στους τομείς της εκπαίδευσης, της υγείας και της κοινωνικής εργασίας, το 66 % των ρόλων στον τομέα της κυβερνοασφάλειας καλύπτεται από υπαλλήλους που μετατίθενται από θέσεις εκτός του τομέα της κυβερνοασφάλειας, κάτι που τονίζει την επείγουσα ανάγκη για επανειδίκευση και αναβάθμιση των δεξιοτήτων.

Για την αντιμετώπιση αυτής της πρόκλησης, το Κέντρο Υποστήριξης θα πρέπει να συνεργαστεί με την κοινοπραξία ευρωπαϊκής ψηφιακής υποδομής (EDIC) για τις μελλοντικές δεξιότητες κυβερνοασφάλειας όπως προβλέπεται στην ανακοίνωση της Επιτροπής σχετικά με την Ακαδημία Δεξιοτήτων

[35] The 2024 cybersecurity landscape: insights from the ISC2 cybersecurity workforce study | Digital Skills and Jobs Platform (Το τοπίο της κυβερνοασφάλειας 2024: στοιχεία από τη μελέτη της ISC2 για το εργατικό δυναμικό στον τομέα της κυβερνοασφάλειας | Πλατφόρμα ψηφιακών δεξιοτήτων και θέσεων εργασίας).

[36] Έκτακτο Ευρωβαρόμετρο 547 για τις κυβερνοδεξιότητες.

Κυβερνοασφάλειας[37]. Το έργο θα πρέπει να διευκολύνει τις ανταλλαγές πληροφοριών μεταξύ επαγγελματιών κυβερνοασφάλειας του τομέα της υγείας, όπως οι υπεύθυνοι ασφάλειας πληροφοριών (CISO). Μια πιθανή δράση είναι η δημιουργία ενός **ευρωπαϊκού δικτύου CISO στον τομέα της υγείας**, αρχής γενομένης από μια ομάδα εμπειρογνωμόνων για την ανταλλαγή και την ανάπτυξη βέλτιστων πρακτικών, στρατηγικών διατήρησης ταλέντων και λύσεων για την προσέλκυση επαγγελματιών κυβερνοασφάλειας στον τομέα της υγείας. Επιπλέον, στο πλαίσιο της Ακαδημίας Δεξιοτήτων Κυβερνοασφάλειας, θα πρέπει να αναπτυχθούν πόροι για την ενίσχυση του εργατικού δυναμικού στον τομέα της κυβερνοασφάλειας για τον τομέα της υγείας με τη στήριξη του κλάδου και της ακαδημαϊκής κοινότητας. Στο πλαίσιο αυτό, τα ενδιαφερόμενα μέρη του κλάδου θα πρέπει να ενθαρρύνονται να δεσμευτούν ότι θα στηρίξουν την ενίσχυση της κατάρτισης στον τομέα της κυβερνοασφάλειας.

Το ανθρώπινο σφάλμα εξακολουθεί να αποτελεί κύριο παράγοντα σε περιστατικά κυβερνοασφάλειας στον τομέα της υγειονομικής περίθαλψης, κάτι που υπογραμμίζει την επιτακτική ανάγκη ολοκληρωμένης κατάρτισης και ευαισθητοποίησης του προσωπικού στον τομέα της κυβερνοασφάλειας. Δεδομένης της συχνής χρήσης ψηφιακών εργαλείων από τους επαγγελματίες του τομέα της υγείας, είναι ζωτικής σημασίας να είναι εφοδιασμένοι με γνώσεις για τις ασφαλές πρακτικές. Οι στοχευμένες εκστρατείες κατάρτισης και ευαισθητοποίησης μπορούν να μειώσουν σημαντικά τους κινδύνους. Για την αντιμετώπιση αυτού του προβλήματος, το Κέντρο Υποστήριξης θα πρέπει να συνεργαστεί με επαγγελματίες και παρόχους υγειονομικής περίθαλψης, καθώς και με τους παρόχους εκπαίδευσης και κατάρτισης, τον κλάδο, την κοινοπραξία ευρωπαϊκής ψηφιακής υποδομής (EDIC) για τις δεξιότητες κυβερνοασφάλειας και με τις αρχές των κρατών μελών για τη δημιουργία και τη διάδοση **εκτεταμένων, εύκολα προσβάσιμων διαδικτυακών ενοτήτων και μαθημάτων κατάρτισης**.

Η ενσωμάτωση ενοτήτων ψηφιακής ικανότητας και κυβερνοασφάλειας στα εκπαιδευτικά προγράμματα έχει καίρια σημασία για τη δημιουργία ισχυρής βάσης κυβερνοασφάλειας στον τομέα της υγειονομικής περίθαλψης. Οι ενότητες αυτές θα πρέπει να αντιμετωπίζουν ειδικά τομεακά ζητήματα, όπως η προστασία των δεδομένων των ασθενών και οι ευπάθειες όσον αφορά την ασφάλεια των ιατροτεχνολογικών προϊόντων. Κατά την ανάπτυξη αυτών των πόρων θα πρέπει να λαμβάνονται υπόψη προηγούμενες δράσεις, όπως το έργο BeWell που χρηματοδοτείται στο πλαίσιο του προγράμματος Erasmus+[38] και το έργο PANACEA που χρηματοδοτείται στο πλαίσιο του προγράμματος «Ορίζων 2020»[39].

[37] Ανακοίνωση της Επιτροπής προς το Ευρωπαϊκό Κοινοβούλιο και το Συμβούλιο: Κάλυψη της έλλειψης ταλέντων στον τομέα της κυβερνοασφάλειας για την ενίσχυση της ανταγωνιστικότητας, της ανάπτυξης και της ανθεκτικότητας της ΕΕ («Η Ακαδημία Δεξιοτήτων Κυβερνοασφάλειας») [COM(2023) 207 final].

[38] BeWell – Blueprint alliance for a future health workforce strategy on digital and green skills (Έργο BeWell — Σχέδιο στρατηγικής για συμμαχία σχετικά με μια μελλοντική στρατηγική για το εργατικό δυναμικό στον τομέα της υγείας όσον αφορά τις ψηφιακές και πράσινες δεξιότητες). Διατίθεται στη διεύθυνση https://bewell-project.eu/.

[39] PANACEA – Protection and privAcy of hospital and health iNfrastructures with smArt Cyber sEcurity and cyber threat toolkit for data and people (Έργο PANACEA — Προστασία και ιδιωτικότητα των νοσοκομειακών υποδομών και των υποδομών υγείας με έξυπνη εργαλειοθήκη για την κυβερνοασφάλεια και τις κυβερνοαπειλές για τα δεδομένα και τους ανθρώπους). Διατίθεται στη διεύθυνση https://cordis.europa.eu/project/id/826293.

3.2.Ευρωπαϊκές ικανότητες ανίχνευσης κυβερνοαπειλών κατά του τομέα της υγείας

Η αποτελεσματική ανίχνευση κυβερνοαπειλών είναι απαραίτητη για την ταχεία αντιμετώπιση περιστατικών. Οι παράγοντες απειλών μπορούν να αξιοποιήσουν τεχνικές οι οποίες καθιστούν δύσκολη την ανίχνευση εισβολών, με αποτέλεσμα να επιτυγχάνουν παρατεταμένες περιόδους μη επιτρεπόμενης πρόσβασης σε ένα σύστημα[40]. Ως εκ τούτου, η βελτίωση των ικανοτήτων ανίχνευσης απειλών μπορεί να συμβάλει στην αναχαίτιση των κυβερνοεπιθέσεων κατά την πορεία τους. Για παράδειγμα, στην επίθεση με λυτρισμικό κατά του φινλανδικού παρόχου ψυχοθεραπευτικών υπηρεσιών Vastaamo, κατά τη διάρκεια της οποίας ο δράστης εκβίαζε ασθενείς των οποίων τα εμπιστευτικά αρχεία είχαν κλαπεί, η αρχική εισβολή σημειώθηκε το 2018, αλλά έγινε αντιληπτή από τον πάροχο μόλις το 2020[41].

Για τη βελτίωση της ανίχνευσης απειλών και της αντίληψης της κατάστασης σε ολόκληρη την ΕΕ είναι ουσιαστικής σημασίας να ανταλλάσσουμε πληροφορίες και να συνεργαζόμαστε με τρόπο αποτελεσματικό. Οι ομάδες αντιμετώπισης περιστατικών ασφάλειας σε υπολογιστές (CSIRT) διαδραματίζουν καθοριστικό ρόλο στη λήψη αναφορών περιστατικών, παρ' ολίγον περιστατικών και πιθανών απειλών, παρέχοντας καθοδήγηση σχετικά με τα μέτρα μετριασμού σε εθνικό επίπεδο. Ωστόσο, **τα κράτη μέλη ενθαρρύνονται θερμά να κοινοποιούν επίσης στο Κέντρο Υποστήριξης του ENISA όλες τις αναφορές κυβερνοπεριστατικών που λαμβάνουν από νοσοκομεία και παρόχους υγειονομικής περίθαλψης, ώστε να καταστεί δυνατή η αντίληψη της κατάστασης στην ΕΕ**. Ιδανικά, οι κοινοποιήσεις αυτές θα πρέπει να πρέπει να υποβάλλονται μαζί με έναν ουσιαστικό χαρακτηρισμό των διαφόρων σχετικών διαστάσεων ενός περιστατικού, συμπεριλαμβανομένων των γνωστών βαθύτερων ευπαθειών και των επιπτώσεων στις υπηρεσίες υγειονομικής περίθαλψης, καθώς και των ανεπιθύμητων συμβάντων σε ασθενείς. Επιπλέον, οι κατασκευαστές ιατροτεχνολογικών και in vitro διαγνωστικών ιατροτεχνολογικών προϊόντων ενθαρρύνονται να αναφέρουν οικειοθελώς, μέσω της ενιαίας πλατφόρμας αναφοράς που θα δημιουργηθεί και θα τελεί υπό τη διαχείριση του ENISA στο πλαίσιο της πράξης για την κυβερνοανθεκτικότητα, τις ευπάθειες που αποτελούν αντικείμενο ενεργού εκμετάλλευσης ή σοβαρά κυβερνοπεριστατικά που έχουν αντίκτυπο στην ασφάλεια των εν λόγω ιατροτεχνολογικών προϊόντων, καθώς και δυνητικά άλλες ευπάθειες, περιστατικά, παρ' ολίγον περιστατικά ή κυβερνοαπειλές που ενδέχεται να επηρεάσουν το προφίλ κινδύνου των εν λόγω ιατροτεχνολογικών προϊόντων.

Όταν οι πληροφορίες που περιέχονται στις αναφορές δεν είναι πλέον ευαίσθητες, το Κέντρο Υποστήριξης θα μπορούσε να δημιουργήσει έναν κατάλογο ευρωπαϊκών γνωστών εκμεταλλεύσιμων ευπαθειών (KEV) υπό την αιγίδα του ENIS για τα ιατροτεχνολογικά προϊόντα, τα συστήματα ηλεκτρονικών μητρώων υγείας και τους παρόχους εξοπλισμού ΤΠΕ και λογισμικού στον τομέα της υγείας. Για την αντιμετώπιση σημαντικών προκλήσεων όσον αφορά την ανίχνευση απειλών, το Κέντρο Υποστήριξης θα πρέπει να θεσπίσει **μια συνδρομητική υπηρεσία έγκαιρης προειδοποίησης σε επίπεδο ΕΕ για τον τομέα της υγείας, η οποία θα παρέχει προειδοποιήσεις σε σχεδόν πραγματικό χρόνο**. Η υπηρεσία αυτή θα βασίζεται σε επεξεργασμένα δεδομένα από τις CSIRT, τους φορείς

[40] ENISA Health Threat Landscape 2023 (Τοπίο απειλών κατά της υγείας για το 2023).
[41] Απόφαση 1150/161/2021 του Φινλανδού Διαμεσολαβητή Προστασίας Δεδομένων.

υγειονομικής περίθαλψης και τους κατασκευαστές, τις πληροφορίες ανοικτής πηγής (OSINT) και άλλους σχετικούς παράγοντες, όπως οι κυβερνοκόμβοι, τα κέντρα κοινοχρησίας και ανάλυσης πληροφοριών (ISAC) και οι αρχές επιβολής του νόμου. Η ενισχυμένη συνεργασία μεταξύ του ENISA και του Οργανισμού της Ευρωπαϊκής Ένωσης για τη Συνεργασία στον Τομέα της Επιβολής του Νόμου (Ευρωπόλ) —για παράδειγμα όσον αφορά τους τρόπους δράσης στο κυβερνοέγκλημα κατά του τομέα της υγείας— θα συμβάλει περαιτέρω στην αντίληψη της κατάστασης.

Τα ISAC λειτουργούν ως κεντρικοί πόροι για τη συλλογή πληροφοριών σχετικά με κυβερνοαπειλές, προάγοντας την αμφίδρομη ανταλλαγή πληροφοριών μεταξύ του δημόσιου και του ιδιωτικού τομέα και προωθώντας την οικοδόμηση εμπιστοσύνης. Το Κέντρο Υποστήριξης θα πρέπει να εντείνει τη στήριξη του **ευρωπαϊκού ISAC για την υγεία** με εργαλεία, ανταλλαγή πληροφοριών και τομεακές εκθέσεις για την αντίληψη της κατάστασης, καθώς και να προωθήσει μια αξιόπιστη κοινότητα για τακτική και στρατηγική συνεργασία. Τα κράτη μέλη θα πρέπει να ενθαρρύνουν την ανάπτυξη εθνικών ISAC για την υγεία[42]. Τα ISAC θα πρέπει επίσης να ενθαρρύνονται να φέρνουν σε επαφή τους παρόχους υγειονομικής περίθαλψης με τους κατασκευαστές προκειμένου να διαμορφώνεται κοινή κατανόηση των απειλών για την κυβερνοασφάλεια, μεταξύ άλλων στην αλυσίδα εφοδιασμού, και να διευκολύνουν τον διάλογο σχετικά με τον ασφαλή σχεδιασμό προϊόντων τα οποία λαμβάνουν πραγματικά υπόψη την απτή κατάσταση της ανάπτυξης.

3.3. Ταχεία αντίδραση και ανάκαμψη

Δεδομένης της υψηλής ευαισθησίας των δεδομένων υγείας των ασθενών και των δυνητικά καταστροφικών επιπτώσεων των κυβερνοεπιθέσεων στις υπηρεσίες υγειονομικής περίθαλψης, η ταχεία και αποτελεσματική αντίδραση σε περιστατικά κυβερνοασφάλειας είναι ζωτικής σημασίας για την εγγύηση της ασφάλειας των ασθενών. Όταν ένα νοσοκομείο ή ένας πάροχος υγειονομικής περίθαλψης αντιμετωπίζει μια κυβερνοεπίθεση, το πρώτο σημείο επαφής είναι η αρμόδια εθνική CSIRT[43]. Η CSIRT είναι υπεύθυνη για την παροχή έγκαιρης υποστήριξης, ιδανικά εντός 24 ωρών, για τη διαχείριση σημαντικών περιστατικών. Ωστόσο, εάν ένα περιστατικό υπερβαίνει την ικανότητα της CSIRT, θα πρέπει να διατίθεται στήριξη από την ΕΕ για τη διασφάλιση της ταχείας και αποτελεσματικής αντίδρασης.

Η εφεδρεία της ΕΕ στον τομέα της κυβερνοασφάλειας, η οποία συστάθηκε στο πλαίσιο της πράξης για την αλληλεγγύη στον κυβερνοχώρο, παρέχει υπηρεσίες αντιμετώπισης περιστατικών από αξιόπιστους παρόχους διαχειριζόμενων υπηρεσιών ασφάλειας ώστε να συνδράμει σε σημαντικά ή μεγάλης κλίμακας περιστατικά κυβερνοασφάλειας και προσπάθειες αρχικής ανάκαμψης. Η εφεδρεία αυτή έχει σχεδιαστεί για να συμπληρώνει τις προσπάθειες των CSIRT των κρατών μελών, παρέχοντάς τους τη δυνατότητα

[42] Για παράδειγμα, η Φινλανδία διαθέτει εθνικό ISAC για τον τομέα της κοινωνικής πρόνοιας και της υγειονομικής περίθαλψης. Βλ. Εθνικό Κέντρο Κυβερνοασφάλειας της Φινλανδίας: «ISAC information sharing groups» (Ομάδες ανταλλαγής πληροφοριών ISAC), διαθέσιμο στη διεύθυνση https://www.kyberturvallisuuskeskus.fi/en/our-services/situation-awareness-and-network-management/isac-information-sharing-groups.

[43] Το άρθρο 23 παράγραφος 1 της οδηγίας NIS2 ορίζει ότι οι βασικές και σημαντικές οντότητες πρέπει να κοινοποιούν σημαντικά περιστατικά στη σχετική CSIRT ή, κατά περίπτωση, στην αρμόδια αρχή.

να ζητούν πρόσθετη στήριξη σε περιπτώσεις που αφορούν κρίσιμους τομείς, όπως η υγεία. Για την ενίσχυση του εν λόγω συστήματος, **η Επιτροπή και ο ENISA θα πρέπει να διασφαλίσουν ότι η εφεδρεία περιλαμβάνει μια υπηρεσία ταχείας αντίδρασης ειδικά για τον τομέα της υγείας**. Συμπληρωματικά με άλλα υφιστάμενα πλαίσια, η υπηρεσία αυτή θα αποστέλλει εμπειρογνώμονες για τη διαχείριση σημαντικών ή μεγάλης κλίμακας περιστατικών κυβερνοασφάλειας στον τομέα της υγειονομικής περίθαλψης χωρίς καθυστέρηση, όταν η εθνική στήριξη δεν επαρκεί.

Για τη βελτίωση της αντίδρασης και της ανάκαμψης, το Κέντρο Υποστήριξης, σε συνεργασία με την ομάδα συνεργασίας NIS, το δίκτυο CSIRT και, κατά περίπτωση, την Ευρωπόλ, θα πρέπει να καταρτίσει **εγχειρίδια για την αντιμετώπιση κυβερνοπεριστατικών προσαρμοσμένα στην υγειονομική περίθαλψη**. Τα εν λόγω εγχειρίδια θα παρέχουν καθοδήγηση τόσο στις CSIRT όσο και στους οργανισμούς υγειονομικής περίθαλψης για την αντιμετώπιση συγκεκριμένων απειλών κυβερνοασφάλειας, συμπεριλαμβανομένου του λυτρισμικού. Δεδομένης της σημασίας που έχει η αποτελεσματική συνεργασία μεταξύ των CSIRT και των αρχών επιβολής του νόμου για την αντιμετώπιση και τη διερεύνηση περιστατικών κυβερνοασφάλειας ποινικού χαρακτήρα, τα εγχειρίδια θα πρέπει, μεταξύ άλλων πτυχών, να παρέχουν σαφή καθοδήγηση σχετικά με την αναφορά τέτοιων περιστατικών στις αρχές επιβολής του νόμου. Επιπλέον, το Κέντρο Υποστήριξης θα μπορούσε να **διευκολύνει την ευρεία διεξαγωγή εθνικών ασκήσεων κυβερνοασφάλειας, με βάση τις εμπειρίες από ασκήσεις όπως η άσκηση «Cyber Europe» 2022 του ENISA, για τη δοκιμή των εγχειριδίων και την ενίσχυση των πρωτοκόλλων αντιμετώπισης περιστατικών**.

Για την τεκμηρίωση των πολιτικών και την αξιολόγηση της αποτελεσματικότητας των μέτρων που λαμβάνονται κατά των επιθέσεων λυτρισμικού, είναι απαραίτητη η συλλογή περαιτέρω δεδομένων. Για τον σκοπό αυτόν, τα κράτη μέλη θα πρέπει να ζητούν από τις οντότητες που υπόκεινται στην οδηγία NIS2, συμπεριλαμβανομένων των οργανισμών υγειονομικής περίθαλψης, να αναφέρουν τυχόν πληρωμές λύτρων που έχουν καταβληθεί και πληρωμές λύτρων που προτίθενται να καταβάλουν, μαζί με άλλες πληροφορίες που παρέχουν κατά την αναφορά σημαντικών περιστατικών κυβερνοασφάλειας. Η εν λόγω υποβολή αναφορών υποστηρίζει την αποτελεσματική διερεύνηση περιστατικών λυτρισμικού, συμπεριλαμβανομένης της ιχνηλάτησης των πληρωμών σε πλατφόρμες ανταλλαγής κρυπτονομισμάτων με σκοπό την ταυτοποίηση των αποδεκτών.

Η ταχύτητα ανάκαμψης αποτελεί καθοριστικό παράγοντα για τη διατήρηση της ανθεκτικότητας και της εμπιστοσύνης του κοινού, ειδικότερα στον τομέα της υγειονομικής περίθαλψης, όπου ο χρόνος διακοπής της λειτουργίας μπορεί να διαταράξει την περίθαλψη των ασθενών. Για την αποτελεσματική ανάκαμψη από επιθέσεις λυτρισμικού, οι πάροχοι υγειονομικής περίθαλψης πρέπει να διαθέτουν ασφαλή, επικαιροποιημένα και απομονωμένα εφεδρικά αντίγραφα τα οποία μπορούν να αποκατασταθούν γρήγορα. Στο πλαίσιο του καταλόγου υπηρεσιών του, το Κέντρο Υποστήριξης θα μπορούσε να προσφέρει **μια συνδρομητική υπηρεσία ανάκτησης λυτρισμικού, βοηθώντας τα νοσοκομεία και τους παρόχους υγειονομικής περίθαλψης να καταρτίσουν εκ των προτέρων σχέδια ανάκαμψης**. Ο ENISA και η Ευρωπόλ θα πρέπει να συνεργαστούν για τον εντοπισμό των συνηθέστερων στελεχών λυτρισμικού που στοχεύουν οργανισμούς υγειονομικής περίθαλψης και **να επεκτείνουν το αποθετήριο εργαλείων αποκρυπτογράφησης** που διατίθεται μέσω του έργου «No More Ransom»[44]. Θα πρέπει

[44] https://www.nomoreransom.org/en/index.html.

επίσης να αναπτύξουν και να προωθήσουν προσβάσιμες οδηγίες για να βοηθήσουν τους παρόχους υγειονομικής περίθαλψης να αποφεύγουν την πληρωμή λύτρων χρησιμοποιώντας εργαλεία αποκρυπτογράφησης.

Η **διεθνής πρωτοβουλία για την καταπολέμηση του λυτρισμικού**[45] αποτελεί πολύτιμο χώρο για την ανταλλαγή απόψεων σχετικά με συγκεκριμένα περιστατικά λυτρισμικού, καθώς και για την ανάπτυξη των ικανοτήτων των χωρών μελών της με σκοπό την ενίσχυση των πλαισίων κυβερνοασφάλειας και των ικανοτήτων διερεύνησης κατά των παραγόντων λυτρισμικού. Η Επιτροπή, σε συνεργασία με την ύπατη εκπρόσωπο, θα συνεχίσει να προωθεί τη συνεργασία στο πλαίσιο της πρωτοβουλίας «Counter Ransomware», μεταξύ άλλων κατά των απειλών λυτρισμικού για τον τομέα της υγείας. Επιπλέον, η Επιτροπή θα επιδιώξει συνεργασία στο πλαίσιο της **ομάδας εργασίας της G7 για την κυβερνοασφάλεια**, με σκοπό την ενίσχυση της κυβερνοασφάλειας του τομέα της υγείας. Ειδικότερα, η ομάδα εργασίας θα μπορούσε να εξετάσει δυνατότητες στήριξης του τομέα της υγείας έναντι απειλών όπως το λυτρισμικό, με βάση διάφορους προβληματισμούς, όπως αυτοί που διατυπώνονται στην κοινή δήλωση σχετικά με τις επιθέσεις λυτρισμικού κατά εγκαταστάσεων υγειονομικής περίθαλψης της 8ης Νοεμβρίου 2024, η οποία παρουσιάστηκε στο πλαίσιο του Συμβουλίου Ασφαλείας των Ηνωμένων Εθνών[46].

4. Εθνικές δράσεις

Οι δυνατότητες του παρόντος σχεδίου δράσης για τη βελτίωση της κυβερνοασφάλειας στον τομέα της υγείας στηρίζονται στην ενεργό συμμετοχή και δέσμευση των κρατών μελών. Για την επιτυχή υλοποίηση του σχεδίου δράσης, τα κράτη μέλη θα μπορούσαν να ορίσουν **εθνικά κέντρα υποστήριξης της κυβερνοασφάλειας ειδικά για τα νοσοκομεία και τους παρόχους υγειονομικής περίθαλψης**. Τα κέντρα αυτά θα λειτουργούν ως τα βασικά σημεία επαφής για τον τομέα της υγείας σε εθνικό επίπεδο, σε στενή συνεργασία με το Κέντρο Υποστήριξης του ENISA. Όπου είναι εφικτό και σκόπιμο, τα κράτη μέλη θα πρέπει να ορίζουν ως εθνικά κέντρα υποστήριξης της κυβερνοασφάλειας υφιστάμενους φορείς, όπως εθνικές CSIRT για την υγεία ή αρμόδιες αρχές.

Τα κράτη μέλη ενθαρρύνονται επίσης να καταρτίσουν **εθνικά σχέδια δράσης με επίκεντρο την κυβερνοασφάλεια στον τομέα της υγείας**. Τα σχέδια αυτά θα περιγράφουν τους ειδικούς κινδύνους κυβερνοασφάλειας που αντιμετωπίζουν τα συστήματα υγειονομικής περίθαλψης και τις εθνικές δράσεις που αναλαμβάνονται για την αντιμετώπισή τους, διασφαλίζοντας παράλληλα την αποτελεσματική χρήση των πόρων και των πρακτικών σε ευρωπαϊκό επίπεδο. Το Κέντρο Υποστήριξης του ENISA μπορεί να συνδράμει στη διαμόρφωση αυτών των σχεδίων, λαμβάνοντας υπόψη τα ήδη υφιστάμενα

[45] https://www.counter-ransomware.org/.
[46] https://usun.usmission.gov/joint-statement-on-ransomware-attacks-against-healthcare-facilities/.

εθνικά σχέδια και συντονίζοντας τις προσπάθειες προκειμένου να διασφαλιστεί ότι οι πόροι και οι στρατηγικές των επιμέρους κρατών μελών αλληλοσυμπληρώνονται.

Ένα ακόμα βασικό σημείο εστίασης για τα κράτη μέλη είναι η διευκόλυνση της κατανομής των πόρων μεταξύ των παρόχων υγειονομικής περίθαλψης, η οποία θα μπορούσε να επιτευχθεί μέσω **κοινής προμήθειας ή συγκέντρωσης πόρων** σε εθνικό, περιφερειακό ή ακόμα και σε ευρωπαϊκό επίπεδο. Η προσέγγιση αυτή θα μειώσει την οικονομική επιβάρυνση των επιμέρους οντοτήτων, αυξάνοντας παράλληλα τη διαπραγματευτική τους ισχύ με τους παρόχους υπηρεσιών κυβερνοασφάλειας.

Για παράδειγμα, στο πλαίσιο του γαλλικού προγράμματος CaRE[47] έχει θεσπιστεί σειρά μέτρων σε εθνικό και περιφερειακό επίπεδο για την αντιμετώπιση των προκλήσεων όσον αφορά τους πόρους: μέσω ενός κυβερνοκαταλόγου παρέχεται επισκόπηση των λύσεων και των πακέτων στον κυβερνοχώρο που διατίθενται στα νοσοκομεία μέσω του εθνικού οργανισμού κυβερνοασφάλειας, του οργανισμού ψηφιακής υγείας, των περιφερειακών οργανισμών, των εθνικών οργανισμών προμηθειών, καθώς και εμπορικών λύσεων. Αυτό συμπληρώνεται από πρόσθετη χρηματοδότηση για τους περιφερειακούς οργανισμούς ώστε να προσφέρουν κοινούς πόρους.

Τα κράτη μέλη θα πρέπει επίσης να αντιμετωπίσουν τα ανεπαρκή επίπεδα επενδύσεων στην κυβερνοασφάλεια στον τομέα της υγείας. Για να εξασφαλιστεί επαρκής χρηματοδότηση, θα πρέπει να καθορίσουν **μη δεσμευτικούς δείκτες αναφοράς και να παρακολουθούν τους στόχους χρηματοδότησης που αποσκοπούν ειδικά στην κυβερνοασφάλεια**, διασφαλίζοντας παράλληλα ότι οι εν λόγω επενδύσεις δεν υπονομεύουν τη βασική περίθαλψη των ασθενών. Οι εν λόγω στόχοι χρηματοδότησης θα πρέπει επίσης να αποσκοπούν στην ενσωμάτωση ζητημάτων ασφάλειας σε όλες τις ψηφιακές επενδύσεις στον τομέα. Τα κράτη μέλη μπορούν να ανταλλάσσουν βέλτιστες πρακτικές και συμβουλές σχετικά με τους στόχους αυτούς μέσω πλατφορμών όπως το δίκτυο eHealth[48].

5. Συνεργασία δημόσιου και ιδιωτικού τομέα

Η συνεργασία δημόσιου και ιδιωτικού τομέα και η διαβούλευση με παρόχους υγειονομικής περίθαλψης, άλλες οντότητες του τομέα της υγείας, καθώς και με σχετικούς παράγοντες του κλάδου της κυβερνοασφάλειας έχει ουσιαστική σημασία για την επιτυχή υλοποίηση του σχεδίου δράσης. Για να τροφοδοτήσει περαιτέρω το έργο του Κέντρου Υποστήριξης, **η Επιτροπή, με την υποστήριξη του ENISA, θα συστήσει κοινή συμβουλευτική επιτροπή για την κυβερνοασφάλεια στον τομέα της υγείας** με υψηλού επιπέδου εκπροσώπους και των δύο τομέων, δηλαδή της υγειονομικής περίθαλψης και της κυβερνοασφάλειας, η οποία θα μπορεί να συμβουλεύει την Επιτροπή και το Κέντρο Υποστήριξης σχετικά με αποτελεσματικές δράσεις και να συζητά την περαιτέρω ανάπτυξη συμπράξεων δημόσιου και ιδιωτικού τομέα στον τομέα αυτόν. Η επιτροπή θα συσταθεί με βάση τις υφιστάμενες

[47] Γαλλικός Οργανισμός Ψηφιακής Υγείας: Cybersécurité acceleration et Résilience des Établissements (CaRE). Διατίθεται στη διεύθυνση https://esante.gouv.fr/strategie-nationale/cybersecurite.

[48] Το δίκτυο eHealth είναι ένα εθελοντικό δίκτυο των αρμόδιων για την ηλεκτρονική υγεία εθνικών αρχών που ορίζουν τα κράτη μέλη και έχει θεσπιστεί βάσει του άρθρου 14 της οδηγίας 2011/24/ΕΕ.

προσπάθειες για συμπράξεις δημόσιου και ιδιωτικού τομέα, συμπεριλαμβανομένου του ευρωπαϊκού ISAC στον τομέα της υγείας.

Επιπλέον, η Επιτροπή θα προκηρύξει **πρόσκληση για δράση** των εταιρειών, των ιδρυμάτων, των εκπαιδευτικών φορέων και των ενδιαφερόμενων μερών του κλάδου στον τομέα της κυβερνοασφάλειας, **ώστε να αναλάβουν δράσεις για την αντιμετώπιση των προκλήσεων στον τομέα της υγείας**. Με βάση την πείρα της Ακαδημίας Δεξιοτήτων Κυβερνοασφάλειας, οι δεσμεύσεις αυτές θα μπορούσαν να αφορούν, για παράδειγμα, δεσμεύσεις στο πλαίσιο της Ακαδημίας Δεξιοτήτων Κυβερνοασφάλειας για τη συμπερίληψη της παροχής μαθημάτων κατάρτισης και υλικού με έμφαση στον τομέα της υγείας για τους επαγγελματίες στον τομέα της κυβερνοασφάλειας[49]. Άλλες δεσμεύσεις θα μπορούσαν επίσης να αφορούν δραστηριότητες ευαισθητοποίησης ή την παροχή διαχειριζόμενων υπηρεσιών ασφάλειας σε ιδιαιτέρως ευάλωτες οντότητες, δωρεάν ή με μειωμένο κόστος, προκειμένου να αυξηθεί η ετοιμότητά τους και η ανθεκτικότητά τους στον τομέα της κυβερνοασφάλειας. Επιπλέον, οι δεσμεύσεις θα μπορούσαν να συνίστανται στην ανταλλαγή πληροφοριών σχετικά με κυβερνοαπειλές με το Κέντρο Υποστήριξης του ENISA. Το Κέντρο Υποστήριξης θα πρέπει να τηρεί επισκόπηση των δεσμεύσεων που αναλήφθηκαν στο πλαίσιο της πρόσκλησης για ανάληψη δράσης, με στόχο τη διασφάλιση της συνοχής και της συμπληρωματικότητάς τους.

6. Αποτροπή παραγόντων κυβερνοαπειλών

Οι εσωτερικές και εξωτερικές πολιτικές της ΕΕ για την κυβερνοασφάλεια θα πρέπει να στηρίζουν τον στόχο της αποτροπής των παραγόντων κυβερνοαπειλών από την πραγματοποίηση επιθέσεων στα ευρωπαϊκά συστήματα υγειονομικής περίθαλψης. Οι κυβερνοεπιθέσεις κατά των οργανισμών υγειονομικής περίθαλψης αποτελούν ιδιαίτερα απαράδεκτο είδος κακόβουλης δραστηριότητας στον κυβερνοχώρο, δεδομένης της ικανότητάς τους να απειλήσουν την ασφάλεια των ασθενών και τις ανθρώπινες ζωές. Ως εκ τούτου, θα πρέπει να χρησιμοποιηθεί η πλήρης δύναμη των αποτρεπτικών ικανοτήτων της ΕΕ στον τομέα της κυβερνοασφάλειας και της επιβολής του νόμου για να υπονομεύσει το συνολικό επιχειρηματικό μοντέλο των παραγόντων απειλής που βάζουν στο στόχαστρο τον τομέα της υγείας και να τους στερήσει τα εύκολα κέρδη. Αυτό θα περιλαμβάνει την προώθηση διασυνοριακών ερευνών μέσω της ενισχυμένης ανταλλαγής δεικτών παραβίασης και άλλων σχετικών δεδομένων, καθώς και την αυξημένη εστίαση σε στόχους υψηλής αξίας και σε βασικούς παράγοντες διευκόλυνσης του εγκλήματος, όπως οι απροσπέλαστες υπηρεσίες φιλοξενίας (bulletproof hosting) ή οι υπηρεσίες ανάμειξης κρυπτονομισμάτων.

Η **εργαλειοθήκη για τη διπλωματία στον κυβερνοχώρο** προσφέρει ένα πλαίσιο για την πρόληψη, την αποτροπή και την αντιμετώπιση κυβερνοεπιθέσεων κατά της ΕΕ, των κρατών μελών και των εταίρων. Η Ύπατη Εκπρόσωπος θα συνεχίσει να χρησιμοποιεί το υφιστάμενο πλαίσιο κυβερνοκυρώσεων για την αντιμετώπιση απειλών που βάζουν στο στόχαστρο τα συστήματα υγείας.

Η λογοδοσία των εγκληματιών για τις ενέργειές τους αποτελεί σημαντικό αποτρεπτικό παράγοντα. Ως εκ τούτου, τα κράτη μέλη θα πρέπει να διασφαλίσουν ότι η επιβολή του νόμου ενσωματώνεται πλήρως

[49] Cyber Skills Academy: Get Involved | Digital Skills and Jobs Platform (Ακαδημία Δεξιοτήτων Κυβερνοασφάλειας: Ενεργοποιηθείτε | Πλατφόρμα ψηφιακών δεξιοτήτων και θέσεων εργασίας).

στα οικεία εθνικά σχέδια δράσης. Ειδικότερα, θα πρέπει να αξιοποιήσουν πλήρως τις διατάξεις της οδηγίας για τις επιθέσεις κατά συστημάτων πληροφοριών[50] και της Σύμβασης της Βουδαπέστης του Συμβουλίου της Ευρώπης για το έγκλημα στον κυβερνοχώρο με σκοπό την αποτροπή επιθέσεων, την προσαγωγή των εγκληματιών στη δικαιοσύνη και την εξάρθρωση εγκληματικών υποδομών που ευνοούν τις επιθέσεις[51]. Η επιτυχής εφαρμογή αυτών των εργαλείων θα πρέπει να διασφαλίζει ότι οι εγκληματικές και κακόβουλες ενέργειες κατά της υγειονομικής περίθαλψης τιμωρούνται.

7. Υλοποίηση και παρακολούθηση του σχεδίου δράσης

Σε ολόκληρο το σχέδιο δράσης, προβλέπονται ορισμένα καθήκοντα για τη δημιουργία Κέντρου Υποστήριξης στο πλαίσιο του ENISA. Με τον τρόπο αυτόν διασφαλίζεται η ολιστική και συνεκτική υλοποίηση του σχεδίου δράσης, ενώ παράλληλα αποφεύγεται η δημιουργία νέων οντοτήτων που οδηγούν σε πιθανές αλληλεπικαλύψεις και γενικά έξοδα. Η Επιτροπή προτίθεται να εξασφαλίσει τους κατάλληλους πόρους για το Κέντρο Υποστήριξης.

Μόλις τεθεί σε λειτουργία το Κέντρο Υποστήριξης, ο ENISA, σε διαβούλευση με την Επιτροπή, θα πρέπει να παρέχει τακτικά επικαιροποιήσεις των εργασιών του Κέντρου Υποστήριξης στο διοικητικό συμβούλιο του ENISA, καθώς και στα σχετικά δίκτυα των κρατών μελών, και ειδικότερα στην ομάδα συνεργασίας NIS, στο δίκτυο CSIRT, στο δίκτυο eHealth και, κατά περίπτωση, στο συμβούλιο του ευρωπαϊκού χώρου δεδομένων για την υγεία. Επιπλέον, ο ENISA θα πρέπει να ανταλλάσσει συνεχώς πληροφορίες με τη συμβουλευτική επιτροπή για την κυβερνοασφάλεια στον τομέα της υγείας του δημόσιου και του ιδιωτικού τομέα σχετικά με την υλοποίηση των δράσεων που παρέχονται από το Κέντρο Υποστήριξης.

Οι τακτικές εκθέσεις του ENISA, όπως η έκθεση σχετικά με την κατάσταση της κυβερνοασφάλειας στην Ένωση, η οποία παρέχει συγκεντρωτική αξιολόγηση του επιπέδου ωριμότητας των ικανοτήτων και των πόρων κυβερνοασφάλειας σε ολόκληρη την ΕΕ, μεταξύ άλλων στον τομέα της υγείας, θα πρέπει να χρησιμεύουν ως ευκαιρίες για τη δημοσίευση σχετικών δεδομένων, υποστηρίζοντας την παρακολούθηση του σχεδίου δράσης. Επιπλέον, ο ενωσιακός δείκτης κυβερνοασφάλειας του ENISA[52] μπορεί να παρέχει ποσοτικά και ποιοτικά δεδομένα, τα οποία χρησιμεύουν ως βάση τεκμηρίωσης για την αξιολόγηση της κρισιμότητας και του επιπέδου ωριμότητας του τομέα της υγείας.

8. Επόμενα βήματα

[50] Οδηγία 2013/40/ΕΕ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 12ης Αυγούστου 2013, για τις επιθέσεις κατά συστημάτων πληροφοριών και την αντικατάσταση της απόφασης-πλαισίου 2005/222/ΔΕΥ του Συμβουλίου: https://eur-lex.europa.eu/eli/dir/2013/40/oj/ell.

[51] Σύμβαση για το έγκλημα στον κυβερνοχώρο (Σύμβαση της Βουδαπέστης, ETS αριθ. 185) και τα πρωτόκολλά της: https://www.coe.int/en/web/cybercrime/the-budapest-convention.

[52] ENISA, EU Cybersecurity Index, Framework and Methodological Note (Ενωσιακός δείκτης, πλαίσιο και μεθοδολογικό σημείωμα κυβερνοασφάλειας) (2024). Διατίθεται στη διεύθυνση https://www.enisa.europa.eu/sites/default/files/2024-12/eu_csi_methodological_note_v1-0.pdf.

Η παρούσα ανακοίνωση ορίζει ένα φιλόδοξο θεματολόγιο για έναν τομέα υγείας με μεγαλύτερη κυβερνοασφάλεια στην ΕΕ. Με την προτεινόμενη ανάπτυξη του Κέντρου Υποστήριξης της Κυβερνοασφάλειας για τα νοσοκομεία και τους παρόχους υγειονομικής περίθαλψης στον πυρήνα του ENISA, το σχέδιο δράσης καθορίζει μια πορεία για τη δημιουργία συνεκτικής και κοινής ευρωπαϊκής προσέγγισης για την αντιμετώπιση της πρόκλησης της κυβερνοασφάλειας στον εν λόγω τομέα.

Η παρούσα ανακοίνωση θα πρέπει να αντιμετωπιστεί ως σημείο εκκίνησης της διαδικασίας για τη βελτίωση της κυβερνοασφάλειας στον τομέα της υγειονομικής περίθαλψης. Ως εκ τούτου, η έγκριση του σχεδίου δράσης θα συνοδευτεί από την έναρξη διεξοδικών διαβουλεύσεων με τα ενδιαφερόμενα μέρη και τη συνέχιση της ανταλλαγής απόψεων με τα κράτη μέλη και τα σχετικά δίκτυα για τη συλλογή πληροφοριών. Με βάση τα αποτελέσματα των διαβουλεύσεων, η Επιτροπή προτίθεται να υποβάλει συστάσεις το τέταρτο τρίμηνο του 2025 για την περαιτέρω βελτίωση του σχεδίου δράσης.

Η Επιτροπή καλεί τα κράτη μέλη και όλα τα ενδιαφερόμενα μέρη να συνεργαστούν για την επίτευξη των φιλόδοξων στόχων του σχεδίου δράσης.

ΠΑΡΑΡΤΗΜΑ — Επισκόπηση των προτεινόμενων δράσεων

Η Επιτροπή:

Κέντρο Υποστήριξης της Κυβερνοασφάλειας του ENISA για τα νοσοκομεία και τους παρόχους υγειονομικής περίθαλψης	
Εξασφάλιση κατάλληλων πόρων για το Κέντρο Υποστήριξης της Κυβερνοασφάλειας Συνεργασία με το ECCC για τη δρομολόγηση πιλοτικών έργων με σκοπό την ανάπτυξη βέλτιστων πρακτικών για την κυβερνοϋγιεινή και την εκτίμηση κινδύνων για την ασφάλεια και την αντιμετώπιση της ανάγκης συνεχούς παρακολούθησης της κυβερνοασφάλειας, της συλλογής πληροφοριών για απειλές και της αντιμετώπισης περιστατικών με τη χρήση προηγμένων λύσεων κυβερνοασφάλειας, για την ανάπτυξη του καταλόγου υπηρεσιών του Ευρωπαϊκού Κέντρου Υποστήριξης της Κυβερνοασφάλειας	2025
Πρόληψη περιστατικών κυβερνοασφάλειας	
Σε διαβούλευση με την ομάδα συνεργασίας NIS, το EU-CyCLONe και τον ENISA, διερεύνηση του προσδιορισμού της υγείας ως τομέα για τον οποίο μπορεί να παρασχεθεί στήριξη για συντονισμένες δοκιμές ετοιμότητας στο πλαίσιο της πράξης για την αλληλεγγύη στον κυβερνοχώρο	1ο τρίμηνο του 2025
Ταχεία αντίδραση και ανάκαμψη	
Από κοινού με τον ENISA, διασφάλιση ότι η εφεδρεία της ΕΕ στον τομέα της κυβερνοασφάλειας περιλαμβάνει υπηρεσία ταχείας αντίδρασης ειδικά για τον τομέα της υγείας	4ο τρίμηνο του 2025
Συνεργασία δημόσιου και ιδιωτικού τομέα	
Με την υποστήριξη του ENISA, σύσταση κοινής συμβουλευτικής επιτροπής για την κυβερνοασφάλεια στον τομέα της υγείας	1ο τρίμηνο του 2025
Προκήρυξη πρόσκλησης για δράση των εταιρειών, των ιδρυμάτων, των εκπαιδευτικών φορέων και των ενδιαφερόμενων μερών του κλάδου στον τομέα της κυβερνοασφάλειας, ώστε να αναλάβουν δράσεις για	2ο τρίμηνο του 2025

την αντιμετώπιση των προκλήσεων στον τομέα της υγείας	
Αποτροπή παραγόντων κυβερνοαπειλών	
Από κοινού με την Ύπατη Εκπρόσωπο, διερεύνηση της χρήσης της εργαλειοθήκης για τη διπλωματία στον κυβερνοχώρο με σκοπό την πρόληψη, την αποθάρρυνση, την αποτροπή και την αντιμετώπιση κακόβουλων δραστηριοτήτων κατά των συστημάτων υγείας	2025
Προώθηση της διεθνούς συνεργασίας κατά των παραγόντων λυτρισμικού, ιδίως στο πλαίσιο της διεθνούς πρωτοβουλίας για την καταπολέμηση του λυτρισμικού, σε συνεργασία με την Ύπατη Εκπρόσωπο	2025-2026
Επιδίωξη συνεργασίας στο πλαίσιο της ομάδας εργασίας της G7 για την κυβερνοασφάλεια, με σκοπό την ενίσχυση της κυβερνοασφάλειας του τομέα της υγείας	2025-2026
Επόμενα βήματα	
Έναρξη διεξοδικών διαβουλεύσεων με τα ενδιαφερόμενα μέρη	1ο τρίμηνο του 2025
Έκδοση συστάσεων για περαιτέρω βελτίωση του σχεδίου δράσης	4ο τρίμηνο του 2025

ENISA:

Ενωσιακό Κέντρο Υποστήριξης της Κυβερνοασφάλειας για τα νοσοκομεία και τους παρόχους υγειονομικής περίθαλψης	
Έναρξη εργασιών για τη δημιουργία Ευρωπαϊκού Κέντρου Υποστήριξης της Κυβερνοασφάλειας για τα νοσοκομεία και τους παρόχους υγειονομικής περίθαλψης	2ο τρίμηνο του 2025
Κατάρτιση ολοκληρωμένου καταλόγου υπηρεσιών που θα παρέχεται από το Κέντρο Υποστήριξης της Κυβερνοασφάλειας	Από το 4ο τρίμηνο του 2025
Πρόληψη περιστατικών κυβερνοασφάλειας	
Έκδοση κατευθυντήριων γραμμών για την ανάδειξη των πλέον κρίσιμων πρακτικών κυβερνοασφάλειας	3ο τρίμηνο του 2025

και στήριξη των παρόχων υγειονομικής περίθαλψης κατά την εφαρμογή τους	
Σε στενή συνεργασία με την Επιτροπή και τα κράτη μέλη, ανάπτυξη εργαλείου κανονιστικής χαρτογράφησης	1ο τρίμηνο του 2025
Ανάπτυξη πλαισίου για τις αξιολογήσεις του επιπέδου ωριμότητας στον τομέα της κυβερνοασφάλειας ειδικά για την υγειονομική περίθαλψη	3ο τρίμηνο του 2025
Διενέργεια ετήσιας αξιολόγησης του επιπέδου ωριμότητας στον τομέα της κυβερνοασφάλειας για την υγεία	2025-2026
Συνεργασία με τα κράτη μέλη και τις αρχές περιφερειακών προγραμμάτων για τη δημιουργία πρότυπων προγραμμάτων κουπονιών κυβερνοασφάλειας	2025-2026
Κατάρτιση νέων κατευθυντήριων γραμμών για τις δημόσιες συμβάσεις στον τομέα της κυβερνοασφάλειας των νοσοκομείων και των παρόχων υγειονομικής περίθαλψης	3ο τρίμηνο του 2025
Δημιουργία ενός ευρωπαϊκού δικτύου CISO στον τομέα της υγείας	1ο τρίμηνο του 2026
Σχεδιασμός και προώθηση ενοτήτων και μαθημάτων κατάρτισης για τους επαγγελματίες του τομέα της υγείας	1ο τρίμηνο του 2026
Ευρωπαϊκές ικανότητες ανίχνευσης κυβερνοαπειλών κατά του τομέα της υγείας	
Δημιουργία ευρωπαϊκού καταλόγου γνωστών εκμεταλλεύσιμων ευπαθειών για ιατροτεχνολογικά προϊόντα, συστήματα ηλεκτρονικών μητρώων υγείας και παρόχους εξοπλισμού και λογισμικού ΤΠΕ στον τομέα της υγείας	4ο τρίμηνο του 2025
Θέσπιση πανευρωπαϊκής συνδρομητικής υπηρεσίας έγκαιρης προειδοποίησης για τον τομέα της υγείας	Από το 2026
Υποστήριξη του ευρωπαϊκού ISAC στον τομέα της υγείας με εργαλεία και ανταλλαγή πληροφοριών	2025-2026
Ταχεία αντίδραση και ανάκαμψη	
Από κοινού με την Επιτροπή, διασφάλιση ότι η εφεδρεία της ΕΕ στον τομέα της κυβερνοασφάλειας	4ο τρίμηνο του 2025

περιλαμβάνει υπηρεσία ταχείας αντίδρασης ειδικά για τον τομέα της υγείας	
Σε συνεργασία με το δίκτυο CSIRT, κατάρτιση εγχειριδίων για την αντιμετώπιση κυβερνοπεριστατικών τα οποία είναι προσαρμοσμένα στην υγειονομική περίθαλψη	3ο τρίμηνο του 2025
Διευκόλυνση της ευρείας διεξαγωγής εθνικών ασκήσεων κυβερνοασφάλειας για τη δοκιμή των εγχειριδίων και την ενίσχυση των πρωτοκόλλων αντιμετώπισης περιστατικών	Από το 4ο τρίμηνο 2025
Παροχή συνδρομητικής υπηρεσίας ανάκτησης λυτρισμικού	Από το 2026
Από κοινού με την Ευρωπόλ, προσδιορισμός των συνηθέστερων στελεχών λυτρισμικού που στοχεύουν οργανισμούς υγειονομικής περίθαλψης και επέκταση του αποθετηρίου εργαλείων αποκρυπτογράφησης μέσω του έργου No More Ransom.	4ο τρίμηνο του 2025
Από κοινού με την Ευρωπόλ, ανάπτυξη προσβάσιμων οδηγιών που θα βοηθούν τους παρόχους υγειονομικής περίθαλψης να αποφεύγουν την πληρωμή λύτρων	3ο τρίμηνο του 2025
Εθνικές δράσεις	
Παροχή βοήθειας στα κράτη μέλη για την ανάπτυξη εθνικών σχεδίων δράσης	2025
Συντονισμός των προσπαθειών προκειμένου να εξασφαλιστεί ότι οι πόροι και οι στρατηγικές των επιμέρους κρατών μελών αλληλοσυμπληρώνονται	2025-2026
Υλοποίηση και παρακολούθηση του σχεδίου δράσης	
Σε διαβούλευση με την Επιτροπή, παροχή τακτικών επικαιροποιήσεων των εργασιών του Κέντρου Υποστήριξης της Κυβερνοασφάλειας στα σχετικά δίκτυα των κρατών μελών	2025-2026
Συνεχής ανταλλαγή απόψεων με τη συμβουλευτική επιτροπή για την κυβερνοασφάλεια στον τομέα της υγείας	2025-2026

Κράτη μέλη:

Ευρωπαϊκές ικανότητες ανίχνευσης κυβερνοαπειλών κατά του τομέα της υγείας

Κοινοποίηση αναφορών περιστατικών από νοσοκομεία και παρόχους υγειονομικής περίθαλψης στο πλαίσιο της οδηγίας NIS2 στο Ευρωπαϊκό Κέντρο Υποστήριξης της Κυβερνοασφάλειας	Από το 4ο τρίμηνο 2025
Ενθάρρυνση της ανάπτυξης εθνικών ISAC για την υγεία	2025-2026
Πρόληψη περιστατικών κυβερνοασφάλειας	
Στο πλαίσιο της ομάδας συνεργασίας NIS, διενέργεια συντονισμένης εκτίμησης κινδύνων για την ασφάλεια, αξιολογώντας τόσο τους τεχνικούς όσο και τους στρατηγικούς κινδύνους που σχετίζονται με τις αλυσίδες εφοδιασμού ιατροτεχνολογικών προϊόντων	4ο τρίμηνο του 2025
Ταχεία αντίδραση και ανάκαμψη	
Διεξαγωγή εθνικών ασκήσεων κυβερνοασφάλειας για τη δοκιμή των εγχειριδίων και την ενίσχυση των πρωτοκόλλων αντιμετώπισης περιστατικών	Από το 2026
Εθνικές δράσεις	
Ορισμός εθνικών κέντρων υποστήριξης της κυβερνοασφάλειας για τα νοσοκομεία και τους παρόχους υγειονομικής περίθαλψης	2ο τρίμηνο του 2025
Διαμόρφωση εθνικών σχεδίων δράσης με επίκεντρο την κυβερνοασφάλεια στον τομέα της υγείας	4ο τρίμηνο του 2025
Διευκόλυνση της κατανομής πόρων μεταξύ των παρόχων υγειονομικής περίθαλψης	2025-2026
Καθορισμός μη δεσμευτικών δεικτών αναφοράς και παρακολούθηση των στόχων χρηματοδότησης που αποσκοπούν ειδικά στην κυβερνοασφάλεια	4ο τρίμηνο του 2025
Αίτημα προς τους οργανισμούς υγειονομικής περίθαλψης και άλλες οντότητες που υπόκεινται στην οδηγία NIS2 να αναφέρουν τις προθέσεις τους να πληρώνουν λύτρα	4ο τρίμηνο του 2025