Αθήνα, 06/02/2026
Α. Π.: 4736 ΕΞ 2026
Απάντηση στο έγγραφο: 2623 ΕΞ 2026

ΕΛΛΗΝΙΚΗ ΔΗΜΟΚΡΑΤΙΑ
ΕΘΝΙΚΗ ΑΡΧΗ ΚΥΒΕΡΝΟΑΣΦΑΛΕΙΑΣ
ΓΕΝΙΚΗ ΔΙΕΥΘΥΝΣΗ ΕΠΙΤΕΛΙΚΟΥ ΣΧΕΔΙΑΣΜΟΥ
ΔΙΕΥΘΥΝΣΗ ΣΤΡΑΤΗΓΙΚΟΥ ΣΧΕΔΙΑΣΜΟΥ ΚΥΒΕΡΝΟΑΣΦΑΛΕΙΑΣ
ΤΜΗΜΑ ΚΑΝΟΝΙΣΤΙΚΗΣ ΣΥΜΜΟΡΦΩΣΗΣ
Δ/νση: Χανδρή 1 & Θεσσαλονίκης
Τ.Κ.: 18346, Μοσχάτο Αττικής
Πληροφορίες: Ι. Βοζώρης
Τηλ.: 210 480 2040
E-mail: i.vozoris@cyber.gov.gr

Προς: 1. Υπηρεσία Συντονισμού
2.Γραφείο Νομικών και Κοινοβουλευτικών Θεμάτων

Κοιν: Γραφείο Υπουργού

Θέμα: Απάντηση σε Ερώτηση στο πλαίσιο κοινοβουλευτικού ελέγχου

Σχετ.: **α.** Το υπ' αρ. πρωτ. 2623 ΕΞ 2026/23-01-2026 έγγραφο της Υπηρεσίας Συντονισμού

β. Η υπ' αρ. 2414/19.1.2026 Ερώτηση 10 βουλευτών της Κοινοβουλευτικής Ομάδας του Συνασπισμού Ριζοσπαστικής Αριστεράς με θέμα: «Θωράκιση των δημόσιων νοσοκομείων απέναντι σε κυβερνοεπιθέσεις και προστασία κρίσιμων συστημάτων υγείας»

Σε απάντηση του α' σχετικού, με το οποίο διαβιβάστηκε στην Υπηρεσία μας το ως άνω β' σχετικό, και στο πλαίσιο των αρμοδιοτήτων μας, σας ενημερώνουμε για τα εξής:

1. Θεσμικός ρόλος και αρμοδιότητες της ΕΑΚ

Η Εθνική Αρχή Κυβερνοασφάλειας (ν. 5086/2024, Α΄23) είναι αρμόδια για την οργάνωση, τον συντονισμό, την εφαρμογή και τον έλεγχο ενός ολοκληρωμένου πλαισίου (στρατηγικών, μέτρων και δράσεων) για την επίτευξη υψηλού επιπέδου κυβερνοασφάλειας στη χώρα, στα πεδία της πρόληψης, της προστασίας, της αποτροπής, του εντοπισμού, της αντιμετώπισης, της αποκατάστασης και της ανάκαμψης από κυβερνοεπιθέσεις. Ορίζεται δε, ως αρμόδια για τη χάραξη της ενιαίας πολιτικής κυβερνοασφάλειας στο πλαίσιο της ελληνικής και ενωσιακής νομοθεσίας για την κυβερνοασφάλεια και τις κρίσιμες υποδομές του δημόσιου και ιδιωτικού τομέα, όπως αυτές εκάστοτε ορίζονται νομοθετικά. Η Αρχή αναβαθμίστηκε

με τον ανωτέρω νόμο, ώστε να ενισχυθεί ο ρόλος και οι αρμοδιότητες της στο σύνολο των βασικών πυλώνων της δημόσιας πολιτικής κυβερνοασφάλειας, ήτοι:

- Διακυβέρνηση και στρατηγικός σχεδιασμός κυβερνοασφάλειας
- Νομοθετικός και ρυθμιστικός πυλώνας, καθώς και κανονιστική συμμόρφωση, μέσω ελεγκτικών μηχανισμών, προκειμένου να διασφαλίζεται η κανονιστική συμμόρφωση των οντοτήτων κρίσιμων υποδομών
- Επιχειρησιακός σχεδιασμός για την αντιμετώπιση περιστατικών μεγάλης κλίμακας και κρίσεων στον κυβερνοχώρο
- Τεχνικές λειτουργίες και δυνατότητες, με στόχο τον εντοπισμό και την παρακολούθηση απειλών και την αντιμετώπιση περιστατικών κυβερνοασφάλειας (μεταξύ των οποίων συγκαταλέγονται λειτουργίες CSIRT, SOC, cybersecurity lab).

2. Ενσωμάτωση της Οδηγίας 2022/2555 (Οδηγία NIS 2) και εθνικό κανονιστικό πλαίσιο

Η Εθνική Αρχή Κυβερνοασφάλειας, στο πλαίσιο της ενίσχυσης της ανθεκτικότητας των πληροφοριακών συστημάτων και της εναρμόνισης με τις ενωσιακές απαιτήσεις, έχει προχωρήσει στην ενσωμάτωση της Οδηγίας (ΕΕ) 2022/2555 (NIS 2) στο εθνικό δίκαιο με τον ν. 5160/2024 (Α΄ 195). Ο εν λόγω νόμος αποτελεί σημαντικό βήμα προς την κατεύθυνση της αναβάθμισης του επιπέδου κυβερνοασφάλειας στην Ελλάδα, με ευρύτερο πεδίο εφαρμογής, στο οποίο εντάσσεται, μεταξύ άλλων, η κεντρική κυβέρνηση και η περιφερειακή αυτοδιοίκηση, καθώς και επιβάλλοντας αυστηρότερες απαιτήσεις για την πρόληψη, την ανίχνευση και την απόκριση σε περιστατικά ασφάλειας. Στο πλαίσιο αυτό, η ΕΑΚ έχει αναλάβει τον κεντρικό ρόλο συντονισμού και εποπτείας της εφαρμογής των σχετικών διατάξεων, με στόχο την προστασία οντοτήτων του δημόσιου και ιδιωτικού τομέα οι οποίες εντάσσονται στο πεδίο εφαρμογής του ανωτέρω νόμου.

Ήδη, στο πλαίσιο αυτό, εκδόθηκε η Κοινή Υπουργική Απόφαση 1689/2025 (Β’ 2186), η οποία θεσπίζει το Εθνικό Πλαίσιο Απαιτήσεων Κυβερνοασφάλειας Βασικών και Σημαντικών Οντοτήτων, προσδιορίζοντας τις ελάχιστες απαιτήσεις συμμόρφωσης που καλούνται να εφαρμόσουν οι υπόχρεοι φορείς.

3. Ο τομέας της υγείας στο πεδίο εφαρμογής του ν. 5160/2024

Στο πεδίο εφαρμογής του ν. 5160/2024 εντάσσεται ρητά και ο τομέας της υγείας. Σύμφωνα με το άρθρο 4 και το Παράρτημα Ι του νόμου, τα δημόσια νοσοκομεία και οι δημόσιες δομές υγείας κατατάσσονται στις βασικές οντότητες υψηλής κρισιμότητας, υπαγόμενα σε ενισχυμένο κανονιστικό πλαίσιο υποχρεώσεων ως προς τη διαχείριση κινδύνων κυβερνοασφάλειας, την εφαρμογή τεχνικών και οργανωτικών μέτρων και την υποχρέωση κοινοποίησης περιστατικών προς την Εθνική Αρχή Κυβερνοασφάλειας (άρθρα 15 και 16).

4. Εικόνα απειλών και περιστατικών στον τομέα υγείας

Ο τομέας της υγείας συγκαταλέγεται διεθνώς μεταξύ των πλέον στοχοποιημένων τομέων. Στην Ελλάδα παρατηρείται σημαντική αύξηση των αναφερόμενων στην ΕΑΚ κυβερνοπεριστατικών στον τομέα της υγείας το 2025, η οποία συνδέεται εν μέρει με την εφαρμογή του ν. 5160/2024 και το νομικά δεσμευτικό χαρακτήρα της αναφοράς των σημαντικών περιστατικών από τις υπόχρεες οντότητες προς την ΕΑΚ. Τα αναφερόμενα περιστατικά αφορούν κυρίως στην εκτέλεση κακόβουλου λογισμικού, τη διάδοση ransomware, την εκμετάλλευση ευπαθειών και την εφαρμογή τεχνικών phishing και social engineering, με αποτέλεσμα προσωρινές διακοπές στην επιχειρησιακή συνέχεια των πληττόμενων συστημάτων.

Όπως προκύπτει από στοιχεία που διαθέτει η υπηρεσία μας καταδεικνύεται έντονη αυξητική τάση στην εμφάνιση περιστατικών κυβερνοασφάλειας την τελευταία πενταετία με τον συνολικό αριθμό των περιστατικών που αναφέρονται στην ΕΑΚ να δεκαπλασιάζεται (2 το 2022 έναντι 19 το 2025) και τα σημαντικά περιστατικά να επταπλασιάζονται (1 έναντι 7), γεγονός που υποδηλώνει αυξημένη συχνότητα αλλά και βαρύτητα των συμβάντων. Επισημαίνεται ότι η σημαντική αύξηση της αναφοράς περιστατικών συμπίπτει με τη δημοσίευση και εφαρμογή του ν. 5160/2024, οποίος ενίσχυσε το πλαίσιο αναφοράς περιστατικών κυβερνοασφάλειας.

5. Εικόνα ωριμότητας και εργαλεία αποτίμησης

Η Εθνική Αρχή Κυβερνοασφάλειας, μέσω των δημόσια διαθέσιμων εργαλείων που έχει αναπτύξει για την ευαισθητοποίηση των φορέων στην ενίσχυση της κυβερνοανθεκτικότητάς τους και την υποστήριξη της κανονιστικής τους συμμόρφωσης, έχει συγκεντρώσει διαχρονικά πληθώρα δεδομένων και έχει σχηματίσει σαφή εικόνα για το επίπεδο ωριμότητας της κυβερνοασφάλειας κρίσιμων τομέων, όπως είναι αυτοί της ενέργειας, των μεταφορών, των τραπεζών και της υγείας, αξιοποιώντας μεταξύ άλλων και το εργαλείο αυτοαξιολόγησης της κυβερνοασφάλειας οργανισμών (self-assessment tool), που διατίθεται πλέον και ως διαδικτυακή εφαρμογή στον ιστότοπό της (www.cyber.gov.gr). Τα εν λόγω δεδομένα καταδεικνύουν την ανάγκη βελτίωσης του επιπέδου ωριμότητας του τομέα της υγείας σε ό,τι αφορά στη λήψη κατάλληλων μέτρων πρόληψης, προστασίας, καθώς και διαχείρισης περιστατικών κυβερνοασφάλειας. Τα ανωτέρω στοιχεία έχουν συμβάλλει ουσιαστικά στη διαμόρφωση της δημόσιας πολιτικής κυβερνοασφάλειας εκ μέρους της υπηρεσίας μας, όπως αυτή έχει αποτυπωθεί στην Εθνική Στρατηγική Κυβερνοασφάλειας 2026–2030, στις απαιτήσεις του ν. 5160/2024 και ιδίως στην κ.υ.α. 1689/2025 «Εθνικό Πλαίσιο Απαιτήσεων Κυβερνοασφάλειας», η οποία καθορίζει και εξειδικεύει τα μέτρα διαχείρισης των κινδύνων κυβερνοασφάλειας που υποχρεούνται να εφαρμόσουν οι οντότητες του πεδίου εφαρμογής του ν. 5160/2024, μεταξύ των οποίων και τα νοσοκομεία.

6. Παροχή συνδρομής: υποστηρικτικά εργαλεία συμμόρφωσης, ασκήσεις ετοιμότητας και εκπαίδευση

Η Εθνική Αρχή Κυβερνοασφάλειας, πέραν του κανονιστικού της ρόλου, παρέχει και υποστηρικτική συνδρομή στους φορείς για την ουσιαστική εφαρμογή των απαιτήσεων, μέσω καθοδήγησης και

πρακτικών εργαλείων, όπως το gap analysis tool και το cybersecurity handbook, τα οποία επίσης είναι διαθέσιμα στην ιστοσελίδα της, καθώς και μέσω θεσμοθετημένων συνεργειών με άλλους οργανισμούς.

Στο πλαίσιο ενίσχυσης της ετοιμότητας και της ανθεκτικότητας, η ΕΑΚ συνεργαζόμενη με τον ENISA υποστηρίζει και συντονίζει την υλοποίηση δράσεων, με σκοπό την επίτευξη παροχής υπηρεσιών κυβερνοασφάλειας υψηλού επιπέδου για την επαύξηση της προστασίας των κρίσιμων και ευαίσθητων υποδομών της Χώρας, όπως ορίζει η Οδηγία NIS 2, έχοντας τον τομέα της Υγείας, ως προτεραιότητα (ENISA Support Action).

Ήδη, τόσο η ίδια η ΗΔΙΚΑ αλλά κυρίως δεκαπέντε (15) μεγάλα νοσοκομειακά ιδρύματα της Ελλάδας έχουν επωφεληθεί από τις υπηρεσίες αυτές (όπως τα Λαϊκό, Ευαγγελισμός, Πάτρας, Αλεξανδρούπολης, Αττικόν, Παπανικολάου, Ιωαννίνων κ.α.) με υπηρεσίες όπως:

- Threat landscape and risk scenarios, όπου προσφέρεται η δυνατότητα διενέργειας πλήρους risk assessment.
- Testing: το οποίο περιλαμβάνει τη διενέργεια ελέγχου παρείσδυσης (penetration testing) σε υποδομή ενδιαφερόμενου Οργανισμού
- Πραγματοποίηση της άσκησης **DRY RUN** για την ενεργοποίηση του **Incident Response Retainer (IRR),** ως παρεχόμενη υπηρεσία από τον ENISA, με ρεαλιστική απεικόνιση της διαδικασίας ενεργοποίησης παροχής συνδρομής στην αντιμετώπιση περιστατικού (Incident Response) βάσει σεναρίου το οποίο αφορούσε την ανίχνευση και ανάλυση περιστατικού κυβερνοεπίθεσης ransomware στα δεδομένα και αρχεία καταγραφής (logs) του δικτύου και των συστημάτων ασφαλείας του νοσοκομείου Ευαγγελισμός.

Το γεγονός ότι τα ίδια τα νοσοκομεία προσδιόρισαν και ιεράρχησαν τις ανάγκες τους και επέλεξαν στοχευμένα τις αντίστοιχες υπηρεσίες, αναδεικνύει τον πρακτικό, επιχειρησιακό και ουσιαστικό χαρακτήρα της εν λόγω υποστήριξης.

Επίσης, πολλά δημόσια νοσοκομεία και φορείς υγείας συμμετείχαν στην πανευρωπαϊκή άσκηση Cyber Europe 2022, καθώς και στη διεθνή άσκηση που πραγματοποιήθηκε τον Φεβρουάριο του 2025 στο πλαίσιο της διεθνούς πρωτοβουλίας Counter Ransomware Initiative (CRI). Μέσω των ασκήσεων αυτών δοκιμάστηκαν στην πράξη οι δυνατότητες ανίχνευσης, απόκρισης και ανάκαμψης από σύνθετα σενάρια κυβερνοκρίσεων. Από τα συμπεράσματα των ασκήσεων προέκυψε ότι το πεδίο των κυβερνοαπειλών που αντιμετωπίζει ο τομέας στην Ελλάδα δεν διαφοροποιείται ουσιωδώς από αυτή άλλων ευρωπαϊκών χωρών, καθώς αναδεικνύονται κοινές προκλήσεις, όπως η ύπαρξη παρωχημένων πληροφοριακών συστημάτων και η ανάγκη ενίσχυσης της εκπαίδευσης και της ευαισθητοποίησης του προσωπικού σε θέματα κυβερνοασφάλειας.

Αναγνωρίζοντας την κεντρική σημασία της ευαισθητοποίησης και της εκπαίδευσης, η Εθνική Αρχή Κυβερνοασφάλειας, σε συνεργασία με το Εθνικό Κέντρο Δημόσιας Διοίκησης και Αυτοδιοίκησης, υλοποιεί ήδη τα τελευταία έτη ειδικά προγράμματα επιμόρφωσης των Υπευθύνων Ασφάλειας Συστημάτων Πληροφορικής και Επικοινωνιών (ΥΑΣΠΕ), καθώς και άλλων στελεχών του δημόσιου τομέα, στα οποία έχει συμμετάσχει πλήθος στελεχών προερχόμενων από νοσοκομεία από το σύνολο της επικράτειας.

Παράλληλα, υλοποιεί δράσεις ευαισθητοποίησης σε θέματα κοινωνικής μηχανικής και κυβερνο-υγιεινής, ιδίως ως προς την αναγνώριση επιθέσεων phishing.

Επιπλέον, στο πλαίσιο της συνεργασίας της Εθνικής Αρχής Κυβερνοασφάλειας με τον ENISA (ENISA Support Action), κατά την τρέχουσα περίοδο υλοποιούνται πολυάριθμες δράσεις για την ανάπτυξη εκστρατειών ευαισθητοποίησης (AR-in-a-Box) μέσω της μεθοδολογίας «εκπαίδευση των εκπαιδευτών» (train the trainers). Η εν λόγω πρωτοβουλία έχει ως στόχο την προώθηση των θεμελιωδών αρχών που ενισχύουν την κυβερνοανθεκτικότητα και διασφαλίζουν την αποτελεσματική διαχείριση και αντιμετώπιση των κυβερνοαπειλών, ώστε τα νοσοκομεία να μπορούν να αναπτύξουν στοχευμένες πρωτοβουλίες ευαισθητοποίησης, ενισχύοντας σταδιακά την κουλτούρα κυβερνοασφάλειας στο ανθρώπινο δυναμικό τους. Κύριοι συμμετέχοντες είναι εκπρόσωποι του τομέα της υγείας, μεταξύ των οποίων δημόσια νοσοκομεία, φορείς υγείας, φαρμακευτικές βιομηχανίες, επιχειρήσεις ιατροτεχνολογικού εξοπλισμού και άλλοι συναφείς φορείς (αναφέρονται ενδεικτικά: 77 νοσοκομεία, 20 μικρομεσαίες βιομηχανίες φαρμάκων και η 1^{Η} ΥΠΕ Αττικής).

Η συγκεκριμένη δράση αναμένεται να ενισχύσει την επαγρύπνηση του προσωπικού των συμμετεχόντων φορέων και να συμβάλει ουσιαστικά στη θωράκιση των πληροφοριακών συστημάτων υγείας. Σημειώνεται ότι οι υπηρεσίες παρέχονται από τον ENISA χωρίς καμία οικονομική επιβάρυνση για τους ωφελούμενους φορείς, εξασφαλίζοντας ότι οι δημόσιες δομές υγείας (νοσοκομεία, ΥΠΕ) μπορούν να διαθέσουν τους διαθέσιμους πόρους σε άλλες, άμεσες και κρίσιμες ανάγκες τους.

7. Το σχέδιο δράσης της ΕΕ για την υγεία

Το Σχέδιο Δράσης της ΕΕ για την κυβερνοασφάλεια στον τομέα της υγείας προβλέπει μια συντονισμένη, στρατηγική προσέγγιση για την ενίσχυση της ανθεκτικότητας νοσοκομείων και παρόχων υγείας, με κεντρικό ρόλο του ENISA στη δημιουργία Ευρωπαϊκού Κέντρου Υποστήριξης που θα παρέχει υπηρεσίες πρόληψης, ανίχνευσης και απόκρισης, θα ενισχύει τη συνεργασία και την εκπαίδευση και θα υποστηρίζει τη συμμόρφωση με το κανονιστικό πλαίσιο. Παράλληλα, προωθείται η ενεργή συμμετοχή των κρατών-μελών μέσω εθνικών κέντρων, επενδύσεων, κοινών προμηθειών και αξιοποίησης ευρωπαϊκών χρηματοδοτήσεων (κυρίως μέσω των προγραμμάτων Digital Europe, Horizon), η ενίσχυση της ασφάλειας εφοδιαστικών αλυσίδων και cloud υποδομών, η ανάπτυξη δεξιοτήτων του ανθρώπινου δυναμικού, η ανταλλαγή πληροφοριών για απειλές, η ενίσχυση των μηχανισμών έγκαιρης προειδοποίησης και απόκρισης (CSIRTs, Cyber Reserve), καθώς και η προώθηση πρακτικών εργαλείων, ελέγχων ετοιμότητας και κατευθυντήριων γραμμών, με στόχο τη διαμόρφωση ενός ασφαλέστερου και πιο ώριμου ψηφιακού οικοσυστήματος υγείας σε ευρωπαϊκό επίπεδο.

8. Συμπέρασμα – Ολιστική προσέγγιση ανθεκτικότητας

Υπό το ανωτέρω πλαίσιο, και σε συνάρτηση με τις ευρωπαϊκές πρωτοβουλίες για τη συστηματική ενίσχυση της κυβερνοασφάλειας στον τομέα της υγείας, η αναβάθμιση των πληροφοριακών συστημάτων των δημόσιων νοσοκομείων δεν μπορεί να αντιμετωπίζεται ως μεμονωμένη τεχνολογική παρέμβαση. Αντιθέτως, απαιτείται να πλαισιώνεται από οργανωμένες και επαναλαμβανόμενες δράσεις εκπαίδευσης

και κατάρτισης του ανθρώπινου δυναμικού, ώστε οι τεχνολογικές επενδύσεις να καθίστανται λειτουργικά, οργανωτικά και επιχειρησιακά βιώσιμες. Η εκπαίδευση οφείλει να έχει περιοδικό χαρακτήρα και να απευθύνεται υποχρεωτικά τόσο στα μέλη της διοίκησης όσο και στο τεχνικό και λοιπό προσωπικό.

Το σύνολο των κανονιστικών απαιτήσεων, των ελέγχων ετοιμότητας, των ασκήσεων, των υποστηρικτικών εργαλείων και των εκπαιδευτικών δράσεων λειτουργεί συμπληρωματικά προς τις ενέργειες που αναλαμβάνουν οι ίδιοι οι φορείς υγείας, δεδομένου ότι είναι ίδιοι υπεύθυνοι για την ενίσχυση του επιπέδου κυβερνοασφάλειάς τους, ενισχύοντας σταδιακά και μεθοδικά τη συνολική τους ανθεκτικότητα έναντι των κυβερνοαπειλών, στο πλαίσιο μιας ευρύτερης εθνικής και ευρωπαϊκής προσέγγισης.

Ο Διοικητής

Μιχαήλ Μπλέτσας

Εσωτερική διανομή:

1. Γραφείο Διοικητή Εθνικής Αρχής Κυβερνοασφάλειας
2. Γενική Διεύθυνση Επιτελικού Σχεδιασμού
3. Γενική Διεύθυνση Επιχειρησιακού Σχεδιασμού