ΑΚΡΙΒΕΣ ΑΝΤΙΓΡΑΦΟ

ΗΛΕΚΤΡΟΝΙΚΗ ΔΙΑΚΥΒΕΡΝΗΣΗ ΥΓΕΙΑΣ ΚΑΙ ΚΟΙΝΩΝΙΚΗΣ ΑΣΦΑΛΙΣΗΣ Μ.Α.Ε.

Δ/νση: Λυκούργου 10 -10551 Αθήνα
Αρ. Γ.Ε.ΜΗ.: 124503101000
info@idika.gr · www.idika.gr

Η.Δ.Υ.Κ.Α. Μ.Α.Ε.
Ημ/νία: 11/02/2026
Α. Π.: 1975
Απάντηση στο έγγραφο: 1854

ΓΕΝΙΚΗ ΔΙΕΥΘΥΝΣΗ ΨΗΦΙΑΚΩΝ ΥΠΟΔΟΜΩΝ
Πληροφορίες: Μ. Μιχαλόπουλος
Τηλέφωνο: 213-2168412
E-mail: Michalopoulos@idika.gr

ΓΕΝΙΚΗ ΔΙΕΥΘΥΝΣΗ ΗΛΕΚΤΡΟΝΙΚΗΣ ΥΓΕΙΑΣ
Πληροφορίες: Ιωαν. Σαλαγιάννη
Τηλέφωνο: 213-2168410
E-mail: isalagianni@idika.gr

ΓΡΑΦΕΙΟ ΑΣΦΑΛΕΙΑΣ ΣΥΣΤΗΜΑΤΩΝ ΠΛΗΡΟΦΟΡΙΚΗΣ & ΕΠΙΚΟΙΝΩΝΙΩΝ (Υ.Α.Σ.Π.Ε./CISO)
Πληροφορίες: Ασημ. Μπασδάνη
Τηλέφωνο:213-2168268
E-mail: a.basdani@idika.gr

Αθήνα, 10/02/2026

Προς: **ΥΠΟΥΡΓΕΙΟ ΨΗΦΙΑΚΗΣ ΔΙΑΚΥΒΕΡΝΗΣΗΣ**
ΥΠΗΡΕΣΙΑ ΣΥΝΤΟΝΙΣΜΟΥ
ΓΡΑΦΕΙΟ ΝΟΜΙΚΩΝ ΚΑΙ ΚΟΙΝΟΒΟΥΛΕΥΤΙΚΩΝ ΘΕΜΑΤΩΝ
e-mail: ke@mindigital.gr

Κοιν.:
- **ΓΡΑΦΕΙΟ ΥΠΟΥΡΓΟΥ ΨΗΦΙΑΚΗΣ ΔΙΑΚΥΒΕΡΝΗΣΗΣ**
  E-mail: minister@mindigital.gr
- **ΓΡΑΦΕΙΟ ΥΠΟΥΡΓΟΥ ΥΓΕΙΑΣ**
  E-mail: minister@moh.gov.gr
- **ΕΘΝΙΚΗ ΑΡΧΗ ΚΥΒΕΡΝΟΑΣΦΑΛΕΙΑΣ**
  E-mail: governor@cyber.gov.gr

Θέμα: ΕΞΑΙΡΕΤΙΚΑ ΕΠΕΙΓΟΝ: Κοινοβουλευτικός έλεγχος: Ερώτηση υπ' αρ. 2414/19.1.2026

Σχετικά :
1. Υπηρεσία Συντονισμού ΑΠ 5030 ΕΞ 2026/10-02-2026 (ΑΠ ΗΔΙΚΑ 1854/10-2-2026)
2. 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 των ερωτήσεων που τίθενται στο σχετικό (2) που διαβιβάζεται στην ΗΔΥΚΑ ΜΑΕ με το σχετικό (1), σας ενημερώνουμε για τα εξής τα εξής:

Η Η.Δ.Υ.Κ.Α. Μ.Α.Ε. αναγνωρίζοντας την κρισιμότητα των πληροφοριών και των πληροφοριακών συστημάτων στην εκτέλεση των επιχειρησιακών της λειτουργιών, για την επίτευξη υψηλού επιπέδου κυβερνοασφάλειας εφαρμόζει Πολιτικές και Διαδικασίες Ασφάλειας Πληροφοριών και ένα σύνολο από Τεχνικά και Οργανωτικά Μέτρα με στόχο:

- Τη διασφάλιση της εμπιστευτικότητας, της ακεραιότητας και της διαθεσιμότητας των πληροφοριών που παράγονται, λαμβάνονται και διακινούνται στο πλαίσιο των υπηρεσιών ανάπτυξης, προμήθειας, διαχείρισης, διασύνδεσης και υποστήριξης συστημάτων και λογισμικού.
- Την εξασφάλιση της ορθής λειτουργίας και τη μεγιστοποίηση της αξιοπιστίας των πληροφοριακών συστημάτων.
- Την έγκαιρη αντιμετώπιση περιστατικών που είναι δυνατόν να θέσουν σε κίνδυνο τις επιχειρησιακές λειτουργίες της Εταιρείας.
- Την ικανοποίηση των νομοθετικών και κανονιστικών απαιτήσεων.
- Τη συνεχή βελτίωση του επιπέδου Ασφάλειας Πληροφοριών.

Πολιτικές Κυβερνοασφάλειας που Εφαρμόζονται Οριζόντια στην Η.Δ.Υ.Κ.Α. Μ.Α.Ε.

Η Η.Δ.Υ.Κ.Α. Μ.Α.Ε. εφαρμόζει σειρά πολιτικών και διαδικασιών για την αποτελεσματική προστασία των πληροφοριακών της συστημάτων, όπως:

- Πολιτική Ανάλυσης Κινδύνου Ασφάλειας Πληροφοριακών Συστημάτων: Εντοπισμός και αξιολόγηση των κινδύνων που απειλούν τα πληροφοριακά συστήματα.
- Πολιτική Διαχείρισης Περιστατικών Κυβερνοασφάλειας: Διαχείριση περιστατικών που αφορούν την ασφάλεια.
- Πολιτική Αντιγράφων Ασφάλειας: Δημιουργία και διαχείριση αντιγράφων ασφαλείας για την αποφυγή απώλειας δεδομένων.
- Πολιτική Ασφάλειας Εφοδιαστικής Αλυσίδας: Διασφάλιση της ασφάλειας των προμηθευτών και συνεργατών.
- Πολιτική Ασφάλειας στην Απόκτηση, Ανάπτυξη και Συντήρηση Πληροφοριακών Συστημάτων: Η ανάπτυξη και οι δοκιμές συστημάτων και εφαρμογών υλοποιούνται σε ξεχωριστό περιβάλλον το οποίο είναι απομονωμένο από το περιβάλλον παραγωγής, εξασφαλίζοντας με αυτό τον τρόπο την προστασία των επιχειρησιακών λειτουργιών της Εταιρείας.
- Πολιτική Διενέργειας Ελέγχων Κυβερνοασφάλειας: Ανάγκη συστηματικής εγκατάστασης των ενημερώσεων λογισμικού που εκδίδουν οι κατασκευαστές πληροφοριακών συστημάτων και υποδομών.
- Πολιτική Αξιολόγησης Αποτελεσματικότητας των Μέτρων Διαχείρισης Κινδύνων Κυβερνοασφάλειας: Παρακολούθηση και αξιολόγηση της αποτελεσματικότητας των εφαρμοζόμενων τεχνικών και οργανωτικών μέτρων. Εξασφαλίζει ότι τα μέτρα παραμένουν κατάλληλα και αποδοτικά σε σχέση με το εξελισσόμενο περιβάλλον απειλών.
- Πολιτική Εκπαίδευσης και Κατάρτισης στην Κυβερνοασφάλεια: Στοχεύει στην ενίσχυση της κουλτούρας ασφάλειας του προσωπικού μέσω τακτικών δράσεων εκπαίδευσης και ευαισθητοποίησης.
- Πολιτική Κρυπτογράφησης Δεδομένων και Επικοινωνιών: Προστασία των δεδομένων μέσω κρυπτογράφησης.
- Πολιτική Ασφάλειας Ανθρωπίνων Πόρων: Περιλαμβάνει ελέγχους, ρόλους, ευθύνες και δεσμεύσεις, ώστε να μειώνονται οι κίνδυνοι από ανθρώπινο παράγοντα.
- Πολιτική Ελέγχου Πρόσβασης: Καθορίζει τις αρχές χορήγησης, διαχείρισης και ανάκλησης δικαιωμάτων πρόσβασης σε συστήματα και δεδομένα, βάσει ρόλων και επιχειρησιακών αναγκών (least privilege). Διασφαλίζει ότι μόνο εξουσιοδοτημένα άτομα έχουν πρόσβαση σε κρίσιμους πόρους.

- Πολιτική Διαχείρισης Πόρων: Αφορά τη σωστή και ασφαλή διαχείριση των πληροφοριακών και τεχνολογικών πόρων.
- Πολιτική Φυσικής και Περιβαλλοντικής Ασφάλειας: Στοχεύει στην προστασία των υποδομών και του εξοπλισμού από φυσικούς και περιβαλλοντικούς κινδύνους.
- Πολιτική Ασφαλούς Διαμόρφωσης και Χρήσης Συσκευών Χρηστών: Διαχείριση των τελικών συσκευών των χρηστών (π.χ. υπολογιστές, κινητά).
- Πολιτική Ασφάλειας Δικτύων και Επικοινωνιών: Ρυθμίζει την προστασία των δικτυακών υποδομών και των επικοινωνιών, διασφαλίζοντας ότι τα συστήματα και οι εφαρμογές που απαιτείται να είναι προσβάσιμα από το διαδίκτυο τοποθετούνται σε ειδική ζώνη απομόνωσης Demilitarized Zone (DMZ). Η επικοινωνία τους με τις εσωτερικές πληροφοριακές υποδομές της Εταιρείας ελέγχεται ή αποκόπτεται μέσω συσκευών Firewall, με σκοπό την ενίσχυση της ασφάλειας.
- Πολιτική Διαβάθμισης και Χρήσης Πληροφοριακών Πόρων: Καθορίζει την κατηγοριοποίηση και διαβάθμιση των πληροφοριών ανάλογα με την κρισιμότητα και την ευαισθησία τους, καθώς και τους κανόνες ορθής χρήσης και διαχείρισής τους.
- Πολιτική Αφαιρούμενων Μέσων Αποθήκευσης: Αφορά τη χρήση αφαιρούμενων μέσων (USB, εξωτερικοί δίσκοι κ.λπ.) και θέτει περιορισμούς και ελέγχους για την αποτροπή απώλειας δεδομένων ή εισαγωγής κακόβουλου λογισμικού.

Συνεργασία με Εθνικούς και Διεθνείς Οργανισμούς Κυβερνοασφάλειας

Η Η.Δ.Υ.Κ.Α. Μ.Α.Ε. στο πλαίσιο ενίσχυσης της ετοιμότητας και της ανθεκτικότητας, συνεργάζεται στενά με την **ΕΑΚ (Εθνική Αρχή Κυβερνοασφάλειας)** και την **ENISA (Οργανισμός της Ευρωπαϊκής Ένωσης για την Κυβερνοασφάλεια)**, με σκοπό την παροχή υπηρεσιών κυβερνοασφάλειας. Στο πλαίσιο αυτής της συνεργασίας υλοποιούνται σημαντικά έργα, όπως:

1. **Αξιολογήσεις ευπαθειών και διενέργεια ελέγχου παρείσδυσης (Penetration Testing)**: Εφαρμογή ελέγχων ασφάλειας σε ολόκληρη την υποδομή της ΗΔΥΚΑ, τα domains και τα web applications.

2. **Ανάλυση Απειλών και Σενάρια Κινδύνων (Threat landscape and risk scenarios/assessment)**: Αξιολόγηση και αποτύπωση των απειλών και κινδύνων που ενδέχεται να επηρεάσουν τον Οργανισμό, καθώς και η κατανόηση και αποτύπωση του threat landscape του κλάδου της Υγείας σε εθνικό και ευρωπαϊκό επίπεδο.

3. **Παρακολούθηση Κινδύνων (**Risk Monitoring): Παρακολούθηση και ανάλυση για ενδεχόμενα περιστατικά ασφάλειας.

4. **Συμβουλές για Διαχείριση Περιστατικών**: Παροχή καθοδήγησης για την αντιμετώπιση και το συντονισμό περιστατικών κυβερνοασφάλειας.

5. **Εκπαίδευση και ασκήσεις (όπως** seminar, workshop, table-top, operational, technical) για όλο το προσωπικό της ΗΔΥΚΑ.

6. **Gap Analysis** για NIS2 και GDPR σε όλο τον Οργανισμό.

7. **Προτάσεις για βελτίωση της θωράκισης** σε δίκτυα, endpoints και servers.

8. **Προτάσεις για τη βελτίωση των πολιτικών ασφαλείας (security policies), των διαδικασιών και της διαχείρισης συμβάντων**, με στόχο την ενίσχυση της ανθεκτικότητας της Η.Δ.Υ.Κ.Α. Μ.Α.Ε. απέναντι σε απειλές.

Η ανωτέρω συνεργασία ενισχύει ουσιαστικά την επιχειρησιακή ετοιμότητα και την ανθεκτικότητα της Η.Δ.Υ.Κ.Α. Μ.Α.Ε., συμβάλλοντας τόσο στη συστηματική συμμόρφωση με τις απαιτήσεις της Οδηγίας

NIS2 όσο και στην αποτελεσματική υλοποίηση των διαδικασιών αυτοαξιολόγησης που προβλέπονται από την Εθνική Αρχή Κυβερνοασφάλειας. Παράλληλα, υποστηρίζει τη συνεχή βελτίωση των μηχανισμών πρόληψης, ανίχνευσης και απόκρισης σε περιστατικά κυβερνοασφάλειας, ενισχύοντας τη συνολική ικανότητα του Οργανισμού να διαχειρίζεται κινδύνους και να προστατεύει τις κρίσιμες πληροφορίες και τις υποδομές.

Εκπαίδευση και Ευαισθητοποίηση Προσωπικού της Η.Δ.Υ.Κ.Α. Μ.Α.Ε.

Ένα ακόμη σημαντικό έργο της Η.Δ.Υ.Κ.Α. Μ.Α.Ε. αποτελεί η **εκπαίδευση και κατάρτιση του προσωπικού της σε θέματα κυβερνοασφάλειας**. Η πιο πρόσφατη εκπαιδευτική δράση υλοποιήθηκε τον Δεκέμβριο του 2025 και σχεδιάστηκε σε συνεργασία με την Υ.Α.Σ.Π.Ε. και το Γραφείο Ασφάλειας Πληροφοριών, με στόχο την περαιτέρω ενίσχυση του επιπέδου ασφάλειας μέσω της ενημέρωσης και ευαισθητοποίησης των εργαζομένων σχετικά με σύγχρονες απειλές και ενδεδειγμένα μέτρα προστασίας. Η συγκεκριμένη πρωτοβουλία εντάσσεται στο πλαίσιο της διαρκούς καλλιέργειας κουλτούρας ασφάλειας πληροφοριών, απευθυνόμενη στο σύνολο του προσωπικού, ανεξαρτήτως ειδικότητας ή επιπέδου τεχνικών γνώσεων.
Η συνεχής και οριζόντια επιμόρφωση σε ζητήματα ασφάλειας αποσκοπεί πρωτίστως στην ενίσχυση του επιπέδου ενημέρωσης και ευαισθητοποίησης (awareness), καθώς και στην εμπέδωση της καθημερινής εφαρμογής των πολιτικών ασφάλειας από κάθε εργαζόμενο. Δεδομένου ότι ο ανθρώπινος παράγοντας αποτελεί κρίσιμο πυλώνα για την αποτελεσματική προστασία πληροφοριών και πληροφοριακών συστημάτων, η διαμόρφωση κοινής αντίληψης και υπεύθυνης συμπεριφοράς σε όλο τον οργανισμό είναι καθοριστικής σημασίας.

Συνεργασία με Επιχειρησιακό Κέντρο Ασφάλειας (SOC)

Η Η.Δ.Υ.Κ.Α. Μ.Α.Ε. συνεργάζεται με **Επιχειρησιακό Κέντρο Ασφάλειας (Security Operation Center - SOC)**, για τη συνεχιζόμενη παρακολούθηση των πληροφοριακών συστημάτων, όπως servers, endpoints και εξοπλισμό ασφάλειας. Η εταιρεία MSSP (Managed Security Services Provider) παρέχει Υπηρεσίες Διαχείρισης Ασφάλειας για τα πληροφοριακά συστήματα της Η.Δ.Υ.Κ.Α. Μ.Α.Ε., με σκοπό τον έγκαιρο και έγκυρο εντοπισμό των απειλών από κυβερνοεπιθέσεις, καθώς και την άμεση ενημέρωση για πιθανά συμβάντα ασφαλείας που σχετίζονται με αυτά και την έγκαιρη απόκριση αυτών.

Οι υπηρεσίες που παρέχονται περιλαμβάνουν:

- **Παρακολούθηση και ανάλυση περιστατικών ασφαλείας** σε πραγματικό χρόνο.
- **Ανίχνευση και απόκριση σε περιστατικά** με στόχο την άμεση επίλυση.
- **Cyber threat intelligence** για την παρακολούθηση και ανάλυση των νέων απειλών.
- **Proactive threat hunting**, με σκοπό την ενεργητική αναζήτηση και πρόληψη κινδύνων.
- **Διαχείριση περιστατικών κυβερνοασφάλειας**, διασφαλίζοντας την άμεση αντίδραση σε περίπτωση ενδεχόμενης παραβίασης της ασφάλειας.

Οι υπηρεσίες αυτές παρέχονται με βάση 24/7, είτε στα on-premises συστήματα είτε στο H-Cloud της Η.Δ.Υ.Κ.Α. Μ.Α.Ε., διασφαλίζοντας έτσι την αδιάλειπτη προστασία των πληροφοριακών συστημάτων και υποδομών της.

Ως εκ τούτων των παραπάνω τα νοσοκομεία που χρησιμοποιούν τα πληροφοριακά συστήματα της ΗΔΥΚΑ ΜΑΕ για τις επιχειρησιακές τους λειτουργίες καθίστανται καθόλα ασφαλή απέναντι σε κυβερνοεπιθέσεις.

Παράλληλα, υλοποιούμε με χρηματοδότηση του Ταμείου Ανάκαμψης και Ανθεκτικότητας το έργο «**Βελτίωση της Ψηφιακής Ετοιμότητας των Νοσοκομείων - Αναβάθμιση πληροφοριακών συστημάτων & υποδομών νοσοκομείων**», με στόχο την προώθηση της ψηφιακής ετοιμότητας στα ελληνικά νοσοκομεία, ώστε κάθε νοσοκομείο να είναι σε θέση να καλύψει το εθνικό επίπεδο αναφοράς ψηφιακής ετοιμότητας (National Digital Readiness Baseline), το οποίο θα περιλαμβάνει τη χρήση των κατάλληλων συστημάτων και υποδομών, ανάλογα με τη δυναμικότητα κάθε δομής, και θα επιτρέπει στους κλινικούς ιατρούς να μεταβούν από τους ένχαρτους φακέλους ασθενών σε πλήρη ψηφιακά αρχεία ασθενών.

Το έργο περιλαμβάνει τις εξής παρεμβάσεις:

- **Παρεμβάσεις που αφορούν σε λογισμικά εφαρμογών**
  - Υλοποίηση/προμήθεια λοιπών λογισμικών εφαρμογών για τις ανάγκες των μονάδων υγείας.

- **Παρεμβάσεις που αφορούν σε αναβάθμιση υλικοτεχνικών υποδομών**
  - Δικτυακές και υπολογιστικές υποδομές
  - Υποδομές ασφάλειας συστημάτων και δεδομένων
  - Εκσυγχρονισμός και αναβάθμιση της αρχιτεκτονικής ενσύρματων δικτύων (LAN)
  - Ασύρματα δίκτυο δεδομένων (WLAN)
  - Συστήματα ενοποιημένης IP επικοινωνίας
  - Τυποποιημένα λογισμικά υποδομών

Επίσης, προβλέπεται μια σειρά οριζόντιων παρεμβάσεων που αγγίζουν τόσο τη βασική επιχειρησιακή λειτουργία των νοσοκομείων όσο και τη λειτουργία τρίτων φορέων που συμμετέχουν στο οικοσύστημα της υγειονομικής περίθαλψης.
Επιπλέον, οι εμπλεκόμενοι φορείς θα μπορούν να διαλειτουργήσουν τον Εθνικό Ηλεκτρονικό Φάκελο Υγείας, με το Σύστημα Ηλεκτρονικής Συνταγογράφησης αλλά και οποιαδήποτε άλλη δομή του υπουργείου Υγείας.

Η Διευθύνουσα Σύμβουλος

Νίκη Τσούμα