



ΕΛΛΗΝΙΚΗ ΔΗΜΟΚΡΑΤΙΑ
ΥΠΟΥΡΓΕΙΟ ΥΓΕΙΑΣ
ΓΡΑΦΕΙΟ ΓΕΝΙΚΟΥ ΓΡΑΜΜΑΤΕΑ
ΔΗΜΟΣΙΑΣ ΥΓΕΙΑΣ

Αθήνα, 3-8-2017
Α.Γ. 224

ΠΡΟΣ:

Πίνακα Αποδεκτών

Θέμα: Πρόσκληση σε ημερίδα για Κυβερνοασφάλεια στον τομέα της Υγείας από την ENISA

Το Γραφείο Γενικού Γραμματέα Δημόσιας Υγείας του Υπουργείου Υγείας σε συνεργασία με τον Ευρωπαϊκό Οργανισμό για την Ασφάλεια Δικτύων και Πληροφοριών (ENISA) και το Ίδρυμα Τεχνολογίας και Έρευνας (ΙΤΕ), προσκαλεί τα στελέχη Πληροφορικής των Νοσοκομείων και των ΥΠΕ την **Παρασκευή 15 Σεπτεμβρίου 2017 στις 10 π.μ.** σε ημερίδα με θέμα την «**Κυβερνοασφάλεια στον τομέα της Υγείας**». Η ημερίδα θα διεξαχθεί στην Αίθουσα Τελετών του Υπουργείου Υγείας, Αριστοτέλους 17, Ισόγειο.

Η ασφάλεια των δικτύων και των πληροφοριών αποτελούν αντικείμενο της Ευρωπαϊκής Οδηγίας που ψηφίστηκε τον Ιούλιο του 2016 από το Ευρωπαϊκό Κοινοβούλιο και το Συμβούλιο της Ευρώπης (Network and Information Security Directive EU 2016/1148). Η Οδηγία στοχεύει στη βελτίωση του επιπέδου κυβερνοασφάλειας στην Ένωση υιοθετώντας συγκεκριμένες υποχρεώσεις από τα Κράτη Μέλη.

Κατά τη διάρκεια της ημερίδας θα γίνει **παρουσίαση** της Ευρωπαϊκής Οδηγίας 2016/1148, καθώς και **συζήτηση** σχετικά με την εφαρμογή της συγκεκριμένης οδηγίας στο χώρο της Υγείας και **καταγραφή** της υφιστάμενης κατάστασης για περαιτέρω μελέτη από την ENISA και το Υπουργείο Υγείας ως κύριου εποπτεύοντος των φορέων φροντίδας υγείας.

Ενδεικτικό πρόγραμμα ημερίδας:

- **10.00 π.μ.:** Εναρκτήριο λόγος από τον αρμόδιο Γενικό Γραμματέα Δημόσιας Υγείας
- **10.15 π.μ.:** Παρουσίαση της Οδηγίας από ENISA
- **11.00 π.μ.:** Συζήτηση με τους φορείς
- **12.00 μ.μ.:** Διάλειμμα
- **12.15 μ.μ.:** Συζήτηση με τους φορείς
- **12.45 μ.μ.:** Παρουσίαση από Τμήμα Υποδομών Υπουργείου Υγείας σχετικά με ασφάλεια κεντρικών υποδομών Υπουργείου Υγείας
- **1.00 μ.μ.:** Παρουσίαση από ΙΤΕ σχετικά με ασφάλεια πληροφοριών στη Βιοϊατρική Έρευνα

Προς ενημέρωσή σας, αποστέλλεται συνημμένο έγγραφο σχετικά με το αντικείμενο της Ευρωπαϊκής Οδηγίας 2016/1148 και τα αναλυτικά θέματα που θα συζητηθούν, καθώς και κάποιο ενδεικτικό ερωτηματολόγιο στο οποίο θα κληθούν να απαντήσουν οι συμμετέχοντες και απαιτεί την προετοιμασία σας.

Λόγω περιορισμένης χωρητικότητας, στην ημερίδα καλείται να παραστεί το πολύ **ένα στέλεχος Πληροφορικής** από κάθε Νοσοκομείο και ΥΠΕ. Επίσης, για την εύρυθμη διοργάνωση της ημερίδας τα στελέχη που θα συμμετέχουν θα πρέπει να καταχωρήσουν τα στοιχεία τους **το αργότερο μέχρι και τη Δευτέρα 4 Σεπτεμβρίου 2017** στην παρακάτω ηλεκτρονική φόρμα υποβολής:

https://ec.europa.eu/eusurvey/runner/NISD_Health_GR

Για οποιαδήποτε πληροφορία μπορείτε να απευθυνθείτε:

- Γρ. Γεν. Γραμματέα Δημόσιας Υγείας, Γ. Στεφανόπουλος, 2132161104, gstefanopoulos@moh.gov.gr
- Δ/νση Ηλεκτρονικής Διακυβέρνησης, Ευγενία Πολίτου, 2132161753, epolitou@moh.gov.gr

Παρακαλούνται οι ΥΠΕ να κοινοποιήσουν το παρόν στα νοσοκομεία ευθύνης τους.

ΣΥΝΗΜΜΕΝΑ: 2 σελίδες

ΚΟΙΝΟΠΟΙΗΣΗ:

- Γραφείο κ. Γεν. Γραμματέα Δημόσιας Υγείας
- Γραφείο Γεν. Διευθύντριας Ανθρωπίνων Πόρων και Διοικητικής Υποστήριξης
- Ίδρυμα Τεχνολογίας και Έρευνας (ΙΤΕ)
- Διεύθυνση Ηλεκτρονικής Διακυβέρνησης

Ο ΓΕΝΙΚΟΣ ΓΡΑΜΜΑΤΕΑΣ ΔΗΜΟΣΙΑΣ ΥΓΕΙΑΣ



ΠΙΝΑΚΑΣ ΑΠΟΔΕΚΤΩΝ	
1	1η Υ.Πε. ΑΤΤΙΚΗΣ, Ζαχάρωφ 3, Αμπελόκηποι Αθήνα, Τ.Κ. 11521, Γραφείο Διοικητή, Δ/νση Πληροφορικής
2	2η Υ.Πε. ΠΕΙΡΑΙΑ & ΑΙΓΑΙΟΥ, Θηβών 46-48, Πειραιάς, Τ.Κ. 18543, Γραφείο Διοικητή, Δ/νση Πληροφορικής
3	3η Υ.Πε. Κεντρικής και Δυτικής Μακεδονίας, Αριστοτέλους 16, Θεσ/κη Τ.Κ 54623, Γραφείο Διοικητή, Δ/νση Πληροφορικής
4	4η Υ.Πε. Ανατολικής Μακεδονίας & Θράκης, Αριστοτέλους 16, Θεσ/κη Τ.Κ 54623, Γραφείο Διοικητή, Δ/νση Πληροφορικής

5	5η Υ.Πε. Θεσσαλίας & Στερεάς Ελλάδας, Μεζούρλο , Λάρισα Τ.Κ. 41110, Γραφείο Διοικητή, Δ/νση Πληροφορικής
6	6η Υ.Πε. Πελοποννήσου, Ιονίων Νήσων, Ηπείρου και Δυτικής Ελλάδας, Υπάτης 1 & Ν.Ε.Ο. Πατρών-Αθηνών Πάτρα Τ.Κ. 26 441, Γραφείο Διοικητή, Δ/νση Πληροφορικής
7	7η Υ.Πε. Κρήτης, 3ο χιλ. Εθνικής Οδού Ηρακλείου - Μοιρών, Εσταυρωμένος, Ηράκλειο Κρήτης, Τ.Κ. 71500, Τ.Θ. 1285, Γραφείο Διοικητή, Δ/νση Πληροφορικής

Ημερίδα με θέμα την Κυβερνοασφάλεια στον τομέα της Υγείας

Τον τελευταίο καιρό το θέμα της κυβερνοασφάλειας βρίσκεται στο επίκεντρο καθώς οι επιθέσεις γίνονται συνεχώς πιο εξειδικευμένες άρα δυσκολότερα αντιμετωπίσιμες. Ο τομέας της υγείας έχει πληγεί επανειλημμένα από περιστατικά ασφάλειας:

- Επίθεση Άρνησης Υπηρεσίας (DDoS) στο εθνικό κεντρικό σύστημα πληροφοριών υγείας της Φιλανδίας προκάλεσε τη μη διαθεσιμότητά του για δύο μέρες με επιπτώσεις σε όλη τη χώρα
- Περιστατικά όπου νοσοκομεία πέφτουν θύματα ransomware (κρυπτογράφηση όλων των δεδομένων υγείας) υποχρεούμενα να πληρώσουν τεραστία ποσά για να απελευθερώσουν έχουν συμβεί στην Γερμανία, στην Ελλάδα και σε πολλά άλλα κράτη μέλη.
- Ιός πρόσβαλε τα ηλεκτρονικά συστήματα υγείας σε περιοχή της Αγγλίας και προκάλεσε ακυρώσεις εγχειρήσεων, ραντεβού ασθενών δημιουργώντας χάος σε πολλά νοσοκομεία της χώρας.

Συμπερασματικά, ο τομέας της υγείας είναι θύμα κυβερνοεπιθέσεων.

Τον Ιούλιο 2016 το Ευρωπαϊκό Κοινοβούλιο και το Συμβούλιο της Ευρώπης ψήφισαν την Ευρωπαϊκή Οδηγία για την ασφάλεια δικτύων και πληροφοριών (Network and Information Security Directive EU 2016/1148). Η Οδηγία στοχεύει στη βελτίωση του επιπέδου κυβερνοασφάλειας στην Ένωση εφαρμόζοντας συγκεκριμένες υποχρεώσεις για υιοθέτηση από τα Κράτη Μέλη.

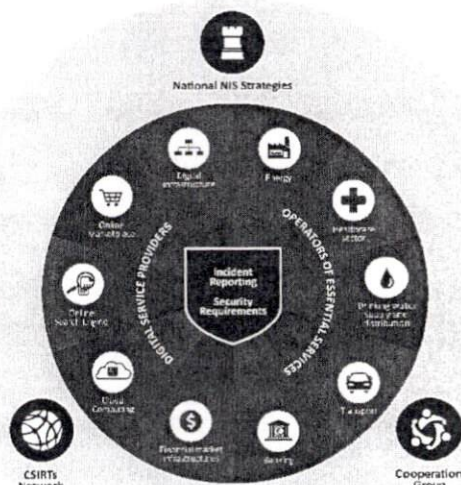
Η Οδηγία πρέπει να εφαρμοστεί στα Κράτη Μέλη εντός 21 μηνών από την ψήφισή της, μέσω εθνικής νομοθεσίας σε κάθε κράτος μέλος. Ο ENISA υποστηρίζει την Ευρωπαϊκή Επιτροπή και τα Κράτη Μέλη καθ' όλη τη διάρκεια της διαδικασίας αυτής.

Οι βασικοί πυλώνες της οδηγίας είναι η εφαρμογή μέτρων ασφαλείας στους φορείς εντός του πλαισίου και η αναφορά συμβάντων κυβερνοασφάλειας από τους ίδιους φορείς στις αρμόδιες εθνικές αρχές. Οι πάροχοι υπηρεσιών υγείας εμπίπτουν στο νομοθετικό πλαίσιο ως κρίσιμες πληροφοριακές υποδομές και υποχρεούνται να υλοποιήσουν τις συγκεκριμένες απαιτήσεις.

A. Θέση του ENISA

Με το θέμα της ασφάλειας των εθνικών συστημάτων υγείας ο ENISA άρχισε να ασχολείται το 2014 δημοσιεύοντας συστάσεις για καλές πρακτικές σε τεχνικά θέματα. Σε σχέση με την Ευρωπαϊκή οδηγία, ο ENISA είναι ο οργανισμός που υποστηρίζει την Ευρωπαϊκή επιτροπή και τα Κράτη Μέλη σε θέματα εφαρμογής του νόμου αυτού,

Network and Information Security Directive



προσφέροντας πληροφορίες και καλές πρακτικές ώστε η εφαρμογή να γίνει με εναρμονισμένο τρόπο σε όλα τα Κράτη Μέλη.

Ο ENISA στα πλαίσια ενημέρωσης για την εφαρμογή της Οδηγίας θα διοργανώσει ημερίδες συζητήσεων με τους εμπλεκόμενους φορείς σε πολλά Κράτη Μέλη. Σκοπός των ημερίδων είναι η ενημέρωση των φορέων και η συζήτηση μαζί τους σε θέματα σχετικά την εφαρμογής της συγκεκριμένη οδηγίας. Η δομή των συναντήσεων θα πρέπει να **προωθεί το διάλογο** ώστε να προσφέρει στον ENISA υλικό για περαιτέρω μελέτη.

B. Θέματα προς συζήτηση

- Ενημέρωση για την Ευρωπαϊκή Οδηγία
- Υποχρεώσεις για τους εμπλεκόμενους φορείς
- Εμπλεκόμενοι φορείς: κριτήρια και διαδικασία
- Ομάδες εργασίας στο πλαίσιο της Οδηγίας
- Κοινές πρακτικές
- Επόμενα βήματα

Γ. Σχετικές ερωτήσεις – υλικό για τους συμμετέχοντες

- Προσφέρετε υπηρεσίες υγείας στην Ελλάδα; Τι είδους υπηρεσίες (νοσοκομεία, άλλοι φορείς υγείας κτλ);
- Υπάρχει λίστα με τις υπηρεσίες, τα συστήματα, τις υποδομές και τα δεδομένα που διαχειρίζεστε/αποθηκεύετε στον φορέα υγείας;
- Έχετε διεξάγει σε αυτά τα συστήματα/ υποδομές/ δεδομένα ανάλυση του ρίσκου σε περίπτωση περιστατικών κυβερνοασφάλειας με επιπτώσεις στην διαθεσιμότητα των συστημάτων αυτών;
- Ποιες δυσκολίες αντιμετωπίζετε σε σχέση με την εφαρμογή μέτρων και την ασφάλεια πληροφοριακών συστημάτων στα συστήματα υγείας στα νοσοκομεία;
- Έχετε διαχωρίσει τους κρίσιμους από τους μη κρίσιμους πόρους (υπηρεσίες, δεδομένα, συστήματα, υποδομές);
- Παίρνετε μέτρα κυβερνοασφάλειας για να προστατέψετε αυτές τις υποδομές; Τι είδους μέτρα είναι αυτά (γενική λίστα);
- Ακολουθείτε κάποιο διεθνές/εθνικό πρότυπο για την προστασία των πόρων αυτών;
- Έχετε ζητήσει από τους προμηθευτές σας (προμηθευτές υπηρεσιών υγείας, συστημάτων υγείας κτλ) να λαμβάνουν μέτρα προστασίας για τις υπηρεσίες που σας προσφέρουν; Έχετε τρόπο να ελέγξετε αυτά τα μέτρα;
- Σε σχέση με την αναφορά περιστατικών υγείας, σε περίπτωση ενός περιστατικού κυβερνοασφάλειας με ποιόν οργανισμό θα επικοινωνήσετε;
- Έχετε εμπειρία από παρόμοια περιστατικά; Πως τα αντιμετωπίσατε εσωτερικά; Ενημερώσατε κάποια αρμόδια αρχή με πληροφορίες για το περιστατικό;
- Ποια είναι τα κριτήρια με βάση τα οποία ενημερώνετε τις αρχές για περιστατικά κυβερνοασφάλειας;
- Ποιες είναι οι δυσκολίες που αντιμετωπίζει ο τομέας της υγείας σε σχέση με την εφαρμογή αυτής της Οδηγίας;