ΕΛΛΗΝΙΚΗ ΔΗΜΟΚΡΑΤΙΑ
ΥΠΟΥΡΓΕΙΟ ΕΣΩΤΕΡΙΚΩΝ

εκδδα
ΕΘΝΙΚΟ ΚΕΝΤΡΟ ΔΗΜΟΣΙΑΣ ΔΙΟΙΚΗΣΗΣ ΚΑΙ ΑΥΤΟΔΙΟΙΚΗΣΗΣ

ΙΝΣΤΙΤΟΥΤΟ ΕΠΙΜΟΡΦΩΣΗΣ

Το **Ινστιτούτο Επιμόρφωσης (ΙΝ.ΕΠ.)** του **Εθνικού Κέντρου Δημόσιας Διοίκησης και Αυτοδιοίκησης (Ε.Κ.Δ.Δ.Α.)** διοργανώνει, κατά την τρέχουσα επιμορφωτική περίοδο σειρά πιστοποιημένων επιμορφωτικών προγραμμάτων που απευθύνονται στα στελέχη της Δημόσιας Διοίκησης και της Τοπικής Αυτοδιοίκησης, στο πλαίσιο του Εθνικού Σχεδίου Ανάκαμψης και Ανθεκτικότητας «Ελλάδα 2.0» με τη χρηματοδότηση της Ευρωπαϊκής Ένωσης – NextGenerationEU. Τα προγράμματα προέκυψαν μετά από ανίχνευση εκπαιδευτικών αναγκών, επεξεργασία σχεδίων ανάπτυξης δεξιοτήτων και αιτήματα των Φορέων, αποσκοπούν στην αποτελεσματική υποστήριξη της υλοποίησης των δημοσίων πολιτικών και εντάσσονται σε επτά θεματικούς τομείς.

Στο θεματικό τομέα **«Πληροφορική και Ψηφιακές Υπηρεσίες»**, διοργανώνεται επιμορφωτικό πρόγραμμα με τίτλο:

«Ασφάλεια πληροφοριακών συστημάτων: Βασικές Δεξιότητες»

Ομάδα Στόχος:. Το επιμορφωτικό πρόγραμμα απευθύνεται σε στελέχη της Δημόσιας Διοίκησης, της Τοπικής Αυτοδιοίκησης Α΄ και Β΄ βαθμού, σε στελέχη που προέρχονται από Νομικά Πρόσωπα Δημοσίου Δικαίου, κατηγορίας ΠΕ, ΤΕ, ΔΕ, με εμπειρία στη χρήση των Η/Υ και καθήκοντα που αφορούν σε διαχείριση Συστημάτων ή/και Δικτύων Πληροφορικής και Επικοινωνιών, σε ανάπτυξη Πληροφοριακών Συστημάτων και Εφαρμογών Πληροφορικής και Επικοινωνιών. Δεν προαπαιτείται γνωστικό υπόβαθρο σχετικό με την ασφάλεια πληροφοριακών συστημάτων. Επιθυμητό είναι να έχουν παρακολουθήσει επιμορφωτικό πρόγραμμα ευαισθητοποίησης σε θέματα ασφάλειας

Σκοπός του επιμορφωτικού προγράμματος είναι: (α) η ανάδειξη της ολιστικής προσέγγισης «ΑΝΘΡΩΠΟΙ-ΔΙΑΔΙΚΑΣΙΕΣ-ΤΕΧΝΟΛΟΓΙΑ» που πρέπει να διέπει την ασφάλεια πληροφοριών, (β) η ενημέρωση σχετικά με τα καθήκοντα και τις υποχρεώσεις που απορρέουν από το θεσμικό πλαίσιο σχετικά με την ασφάλεια πληροφοριακών συστημάτων, (γ) η εκπαίδευση σε πρότυπα και μεθοδολογίες ασφάλειας, (δ) η ανάδειξη και επίλυση θεμάτων ασφάλειας, μέσω μελέτης

αντιπροσωπευτικών περιπτώσεων (case studies), για τον έλεγχο και την αποτροπή ανεπιθύμητων καταστάσεων.

Χρονική Διάρκεια: 35 ώρες.

Θεματικές ενότητες:

ΘΕΜΑΤΙΚΕΣ ΕΝΟΤΗΤΕΣ	ΠΕΡΙΕΧΟΜΕΝΟ ΕΝΟΤΗΤΩΝ
Έναρξη, περιεχόμενο και στόχοι του προγράμματος	✓ **Σύντομη παρουσίαση του φορέα υλοποίησης του προγράμματος (ΙΝ.ΕΠ / Ε.Κ.Δ.Δ.Α).** ✓ **Σκοπιμότητα σχεδιασμού και υλοποίησης του επιμορφωτικού προγράμματος.** ✓ **Στόχοι, περιεχόμενο και διάρθρωση του επιμορφωτικού προγράμματος.**
Εισαγωγικές έννοιες / Βασικές αρχές ασφάλειας πληροφοριών	✓ **Ορισμός εννοιών (ενδεικτικά: ασφάλεια πληροφοριών, εμπιστευτικότητα, διαθεσιμότητα, ακεραιότητα, διακοπή παροχής υπηρεσίας, μη-εξουσιοδοτημένη χρήση / αποκάλυψη / αλλοίωση πληροφοριών, κλπ).** ✓ **Ιδιότητες της ασφάλειας πληροφοριών – Πλαίσιο Confidentiality-Integrity-Availability (και Authentication-Authorization-Non-repudiation)** ✓ **Χαρακτηριστικά ασφάλειας πληροφοριακών συστημάτων** ✓ **Συσχέτιση της ασφάλειας με τις εμπλεκόμενες οντότητες του περιβάλλοντος εργασίας: ΑΝΘΡΩΠΟΙ – ΔΙΑΔΙΚΑΣΙΕΣ-ΤΕΧΝΟΛΟΓΙΚΑ ΜΕΣΑ.** ✓ **Αλληλουχία ενεργειών για την επίτευξη ενός ασφαλούς περιβάλλοντος.**
Κανονιστικό & θεσμικό πλαίσιο	✓ **Βασικές έννοιες (ενδεικτικά: ευαίσθητα δεδομένα, δεδομένα προσωπικού χαρακτήρα, επεξεργασία δεδομένων, υπεύθυνος επεξεργασίας, κλπ).** ✓ **Υφιστάμενο κανονιστικό πλαίσιο Ν 2472/1997.** ✓ **Εμπλεκόμενες αρχές.** ✓ **Διαδικασίες γνωστοποίησης περιστατικού ασφάλειας** ✓ **Διαδικασίες γνωστοποίησης τήρησης αρχείου / επεξεργασίας προσωπικών δεδομένων.** ✓ **Νόμος 3471/2006 για την ανεπιθύμητη ηλεκτρονική επικοινωνία (spam).** ✓ **Νομοθετικό πλαίσιο για το έγκλημα στον Κυβερνοχώρο.** ✓ **Νέες θεσπίσεις: Γενικός κανονισμός για τα προσωπικά δεδομένα (ΕΕ 2016/679), Κανονισμός προστασίας κρίσιμων υποδομών (ΕΕ 2016/1148).**
Η «αλυσίδα» της ασφάλειας: Άνθρωποι – Διαδικασίες -Τεχνολογίες	✓ **Η αξία της ευαισθητοποίησης και της εκπαίδευσης του προσωπικού σε θέματα ασφάλειας.** ✓ **Ανάλυση των βασικών εννοιών καθώς και των εμπλεκόμενων οντοτήτων (ΑΝΘΡΩΠΟΙ-ΔΙΑΔΙΚΑΣΙΕΣ-**

	ΤΕΧΝΟΛΟΓΙΑ) στο σύγχρονο μοντέλο ασφάλειας πληροφοριών. ✓ **Βασικοί εννοιολογικοί ορισμοί (ενδεικτικά: Πολιτική ασφάλειας, διαδικασίες, «κουλτούρα» ασφάλειας, ανάλυση επικινδυνότητας, προτεραιοποιημένη risk-based αντιμετώπιση, κλπ)** ✓ **Εισαγωγή του μοντέλου διαχείρισης ασφάλειας.** ✓ **Ανάλυση μεθοδολογίας αντιμετώπισης περιστατικών ασφάλειας.** ✓ **Η αξία των διαδικασιών.** ✓ **Θέματα επιχειρησιακής συνέχειας.** ✓ **Ο «ρόλος» του ανθρώπου: «Αδύναμος» κρίκος ή η λύση του προβλήματος;**
Μελέτη περίπτωσης από τη Δημόσια Διοίκηση για τη Διαχείριση Περιστατικών Ασφάλειας	**Μελέτη περίπτωσης από τη Δημόσια Διοίκηση για τη Διαχείριση Περιστατικών Ασφάλειας.**
Ανάλυση κινδύνων - Κατηγορίες απειλών και επιθέσεων	✓ **Ορισμός εννοιών (ευπάθειας, απειλής, έκθεσης, επίπτωσης, επικινδυνότητας).** ✓ **Χαρακτηριστικά επιτιθέμενων – Μοντέλο οργάνωσης κυβερνοεπιθέσεων.** ✓ **Κατηγορίες απειλών** ✓ **Ανάλυση των σημαντικότερων κατηγοριών απειλών όπως: Trojans, Buffer overflow, Denial of Service – Distributed Denial of Service και χρησιμοποιούμενων τεχνικών.** ✓ **Απειλές επιπέδου εφαρμογών (π.χ. SQL injection) και υπηρεσιών δικτύου (π.χ. DNS poisoning, spear phising, pharming).**
Βασικές αρχές σχεδιασμού αντιμετώπισης απειλών	✓ **Αρχές σχεδιασμού συστημάτων με χαρακτηριστικά ασφάλειας.** ✓ **Παράδειγμα σχεδιασμού ασφάλειας σε βάθος – ασφάλειας πολλαπλών επιπέδων.** ✓ **Παράμετροι σχεδιασμού – η συμβολή των διαδικασιών και των ανθρώπων στην αξιοποίηση τεχνολογικών λύσεων.**
Τεχνολογικές προκλήσεις ασφάλειας στο σύγχρονο περιβάλλον	✓ **Σύγχρονες προκλήσεις.** ✓ **Ορισμοί εννοιών νεφοϋπολογιστικής.** ✓ **Οφέλη χρήσης νεφοϋπολογιστικής** ✓ **Σχετικοί κίνδυνοι και απειλές.** ✓ **Internet of Things** ✓ **Σχετικοί κίνδυνοι και απειλές.**
Αντιμετώπιση κινδύνων ασφάλειας πληροφοριών	✓ **Γιατί υπάρχουν «ευπάθειες»;** ✓ **Βασικές κατηγορίες ευπαθειών.** ✓ **Μέτρα αντιμετώπισης.**
Πρακτικά παραδείγματα επίθεσης	**Ενδεικτικά θα περιλαμβάνονται:** ✓ **Επίθεση buffer overflow.** ✓ **Επίθεση Denial of Service.**

Πρακτικά παραδείγματα εφαρμογής τεχνολογιών ασφάλειας	**Πρακτικά παραδείγματα εφαρμογής τεχνολογιών ασφάλειας. Βασικοί μηχανισμοί προστασίας συστημάτων (ενδεικτικά: Encryption, VLAN/Network segmentation, IPSec, VPN, SSL, Anti-X, Firewalls, IDS/IPS, κλπ).** **Θεωρητική προσέγγιση και πρακτικά παραδείγματα αναφορικά με:** ✓ **Firewalls** o **Τεχνολογίες** o **Αρχιτεκτονικές,** o **Ποια θέματα αντιμετωπίζουν (και ποια όχι).** o **Μεθοδολογία παραμετροποίησης** ✓ **Ασφαλής πρόσβαση στους εξυπηρετητές.** ✓ **Διαδικασίες ελαχιστοποίησης «έκθεσης» (hardening) συστημάτων.** ✓ **Εντοπισμός σφαλμάτων παραμετροποίησης**
Μελέτη περίπτωσης: Περιστατικό ασφάλειας οργανισμού	**Μελέτη περίπτωσης: Περιστατικό ασφάλειας οργανισμού. Το σενάριο της άσκησης περιλαμβάνει:** ✓ **Περιγραφή τεχνολογικού περιβάλλοντος** ✓ **Περιγραφή τεχνικών και οργανωτικών μέτρων ασφάλειας** ✓ **Περιγραφή περιστατικού ασφάλειας.** **Οι εκπαιδευόμενοι καλούνται να:** ✓ **Αξιολογήσουν το επίπεδο ασφάλειας** ✓ **Εντοπίσουν την / τις αιτία /αιτίες που οδήγησαν στο περιστατικό.** ✓ **Προτείνουν μέτρα βελτίωσης**
Μελέτη περίπτωσης: Ανάλυση κακόβουλου λογισμικού	✓ **Αλληλουχία συμβάντων που οδήγησαν στην εκδήλωση της «επίθεσης».** ✓ **Ανάλυσης της «επίθεσης». Έκταση / συνέπειες.** ✓ **Τεχνική ανάλυση κακόβουλου λογισμικού. Μηχανισμός προσβολής, διαδικασίες αντιμετώπισης.** ✓ **Αξιολόγηση ενδεδειγμένων τεχνικών και οργανωτικών μέτρων αποτροπής ανάλογων περιστατικών.**
Μελέτη περίπτωσης: Αντιμετώπιση περιστατικού παραβίασης προσωπικών δεδομένων	**Στην προαιρετική αυτή θεματική ενότητα γίνεται μελέτη περίπτωσης αντιμετώπισης περιστατικού διαρροής προσωπικών δεδομένων, με έμφαση:** ✓ **στις διαδικασίες που πρέπει να ακολουθηθούν για την ενημέρωση των εμπλεκομένων** ✓ **την αντιμετώπιση του περιστατικού** ✓ **την ανάλυση-διερεύνησή του εξετάζοντας τα σχετικά αρχεία καταγραφής.** **Η προσαρμογή της υποενότητας πραγματοποιείται αναλόγως της προέλευσης, των αναγκών και του ενδιαφέροντος των εκπαιδευόμενων.**
Αξιολόγηση γνώσεων και δεξιοτήτων εκπαιδευομένων	**Εξέταση.**

Προκειμένου οι συμμετέχοντες/χουσες να λάβουν Βεβαίωση Πιστοποίησης θα πρέπει να έχουν παρακολουθήσει ανελλιπώς το πρόγραμμα και να έχουν ολοκληρώσει επιτυχώς την προβλεπόμενη διαδικασία αξιολόγησης γνώσεων και δεξιοτήτων.

Η ανωτέρω δράση υλοποιείται στο πλαίσιο του Εθνικού Σχεδίου Ανάκαμψης και Ανθεκτικότητας «Ελλάδα 2.0» με τη χρηματοδότηση της Ευρωπαϊκής Ένωσης – NextGenerationEU.