Information Security Analyst

1. ΕΙΣΑΓΩΓΗ

Το Κέντρο Επιμόρφωσης και Δια Βίου Μάθησης (Κ.Ε.ΔΙ.ΒΙ.Μ.) του **Εθνικού και Καποδιστριακού Πανεπιστημίου Αθηνών (Ε.Κ.Π.Α.)** σας καλωσορίζει στο Πρόγραμμα Συμπληρωματικής εξ Αποστάσεως Εκπαίδευσης και συγκεκριμένα στο πρόγραμμα επαγγελματικής επιμόρφωσης και κατάρτισης με τίτλο **«Information Security Analyst»**.

Η ανάγκη συνεχούς επιμόρφωσης και πιστοποίησης επαγγελματικών δεξιοτήτων οδήγησε το **Πρόγραμμα Συμπληρωματικής εξ Αποστάσεως Εκπαίδευσης (E-Learning)** του Ε.Κ.Π.Α. στο σχεδιασμό των πρωτοποριακών αυτών Προγραμμάτων Επαγγελματικής Επιμόρφωσης και Κατάρτισης, με γνώμονα τη **διασύνδεση της θεωρητικής με την πρακτική γνώση**, αναπτύσσοντας κυρίως, την εφαρμοσμένη διάσταση των επιστημών στα αντίστοιχα επαγγελματικά πεδία.

Στη συνέχεια, σας παρουσιάζουμε αναλυτικά το πρόγραμμα σπουδών για το πρόγραμμα επαγγελματικής επιμόρφωσης και κατάρτισης: **«Information Security Analyst»**, τις προϋποθέσεις συμμετοχής σας σε αυτό, καθώς και όλες τις λεπτομέρειες που πιστεύουμε ότι είναι χρήσιμες, για να έχετε μια ολοκληρωμένη εικόνα του προγράμματος.

2. ΣΚΟΠΟΣ ΤΟΥ ΠΡΟΓΡΑΜΜΑΤΟΣ

Σκοπός του προγράμματος είναι η εκπαίδευση των συμμετεχόντων/ουσών στην ασφάλεια πληροφοριών και στην προστασία πληροφοριακών υποδομών από κυβερνοαπειλές. Το πρόγραμμα, εστιάζοντας στη σύνδεση θεωρίας και εφαρμογής, προετοιμάζει επαγγελματίες ικανούς να ανταποκριθούν στις αυξανόμενες απαιτήσεις του κλάδου, να διαχειρίζονται ρίσκα και να συμβάλλουν στη στρατηγική ενίσχυση της κυβερνοασφάλειας στους οργανισμούς τους.

Ειδικότερα, οι εκπαιδευόμενοι/ες θα εξοικειωθούν με κρίσιμους άξονες της κυβερνοασφάλειας, όπως η ταυτοποίηση και ο έλεγχος πρόσβασης, η ανάλυση ευπαθειών, η κρυπτογράφηση, η διαχείριση κλειδιών, καθώς και η ασφάλεια σε cloud και mobile περιβάλλοντα.

Παράλληλα, θα εκπαιδευτούν στη διαμόρφωση πολιτικών ασφάλειας, στη δημιουργία σχεδίων ανάκαμψης (Disaster Recovery Plans) και στην υλοποίηση προγραμμάτων ενημερότητας ασφαλείας. Ιδιαίτερη έμφαση δίνεται στην εφαρμογή εργαλείων ασφάλειας (firewalls, IDS/IPS, antivirus), στη διαχείριση περιστατικών και απειλών, καθώς και στη συμμόρφωση με διεθνή πρότυπα και κανονισμούς.

Με την ολοκλήρωση του προγράμματος, οι συμμετέχοντες/ουσες θα έχουν αποκτήσει τις απαιτούμενες τεχνικές δεξιότητες για την ανίχνευση και αντιμετώπιση απειλών, τη λήψη τεκμηριωμένων αποφάσεων και τη συμβολή στη δημιουργία ανθεκτικών πληροφοριακών περιβαλλόντων. Τέλος, θα είναι σε θέση να παρακολουθούν τεχνολογικές εξελίξεις, να εφαρμόζουν

βέλτιστες πρακτικές και να λειτουργούν με υψηλό επίπεδο επαγγελματισμού και ηθικής στον τομέα της κυβερνοασφάλειας.

3. ΚΑΤΗΓΟΡΙΕΣ ΥΠΟΨΗΦΙΩΝ ΠΟΥ ΓΙΝΟΝΤΑΙ ΔΕΚΤΟΙ ΣΤΟ ΠΡΟΓΡΑΜΜΑ - ΤΡΟΠΟΣ ΕΝΤΑΞΗΣ

Αίτηση συμμετοχής μπορούν να υποβάλλουν:

- ► **απόφοιτοι Πανεπιστημίου/ΤΕΙ της ημεδαπής και της αλλοδαπής**
- ► **απόφοιτοι Δευτεροβάθμιας Εκπαίδευσης με συναφή στο αντικείμενο εργασιακή εμπειρία**

Αναλυτικότερα, το πρόγραμμα απευθύνεται σε:

- **Διαχειριστές Συστημάτων και Δικτύων και Ειδικούς Κυβερνοασφάλειας**, που επιδιώκουν να ενσωματώσουν αρχές ασφάλειας στην αρχιτεκτονική των πληροφοριακών συστημάτων και υποδομών τους και ασχολούνται με την πρόληψη επιθέσεων, την ασφάλεια εφαρμογών.
- **Στελέχη Βιομηχανικών Μονάδων και Εταιρειών Πληροφορικής**, που συμμετέχουν στη λειτουργία και ασφάλεια πληροφοριακών υποδομών
- **Υπάλληλους και Στελέχη Επιχειρήσεων και Οργανισμών**, που ασχολούνται με τον σχεδιασμό και τη διαχείριση ψηφιακών πόρων, την πολιτική ασφάλειας και την κανονιστική συμμόρφωση.
- **Οικονομολόγους, Χρηματοοικονομικούς Αναλυτές και Αναλυτές Κινδύνου**, που εργάζονται σε περιβάλλοντα υψηλής ψηφιακής εξάρτησης και επιθυμούν να κατανοήσουν τις βασικές αρχές της κυβερνοασφάλειας.

Η αίτηση συμμετοχής υποβάλλεται ηλεκτρονικά, μέσω της ιστοσελίδας:

https://elearningekpa.gr/

4. ΠΡΟΑΠΑΙΤΟΥΜΕΝΑ

Τα προαπαιτούμενα για την παρακολούθηση του Προγράμματος από τους εκπαιδευόμενους είναι:

- ► Πρόσβαση στο Διαδίκτυο
- ► Κατοχή προσωπικού e-mail
- ► Βασικές γνώσεις χειρισμού ηλεκτρονικών υπολογιστών

5. ΤΡΟΠΟΣ ΔΙΕΞΑΓΩΓΗΣ ΤΟΥ ΠΡΟΓΡΑΜΜΑΤΟΣ

Η διδασκαλία στα προγράμματα εξ αποστάσεως επαγγελματικής επιμόρφωσης και κατάρτισης του Κέντρου Επιμόρφωσης και Δια Βίου Μάθησης του ΕΚΠΑ διεξάγεται μέσω του διαδικτύου, προσφέροντας στον εκπαιδευόμενο «*αυτονομία*», δηλαδή δυνατότητα μελέτης ανεξαρτήτως περιοριστικών παραγόντων, όπως η υποχρέωση της φυσικής του παρουσίας σε συγκεκριμένο χώρο και χρόνο.

Το εκπαιδευτικό υλικό του προγράμματος διατίθεται σταδιακά, ανά διδακτική ενότητα, μέσω ειδικά διαμορφωμένων ηλεκτρονικών τάξεων. Κατά την εξέλιξη κάθε θεματικής ενότητας αναρτώνται σε σχετικό link οι απαραίτητες για την ομαλή διεξαγωγή της εκπαιδευτικής διαδικασίας ανακοινώσεις.

Ο εκπαιδευόμενος, αφού ολοκληρώσει τη μελέτη της εκάστοτε διδακτικής ενότητας, καλείται να υποβάλει ηλεκτρονικά, το αντίστοιχο τεστ αξιολόγησης. Τα τεστ μπορεί να περιλαμβάνουν ερωτήσεις αντιστοίχισης ορθών απαντήσεων, πολλαπλής επιλογής, αληθούς/ψευδούς δήλωσης, ή upload, όπου ο εκπαιδευόμενος θα πρέπει να διατυπώσει και να επισυνάψει την απάντησή του. Η θεματική ενότητα μπορεί να συνοδεύεται από τελική εργασία, η οποία διατίθεται κατά την ολοκλήρωση της θεματικής ενότητας (εφόσον το απαιτεί η φύση της θεματικής ενότητας) και αφορά το σύνολο της διδακτέας ύλης.

Παράλληλα, παρέχεται **πλήρης εκπαιδευτική υποστήριξη** δεδομένου ότι ο εκπαιδευόμενος μπορεί να απευθύνεται ηλεκτρονικά (για το διάστημα που διαρκεί το εκάστοτε μάθημα) στον ορισμένο εκπαιδευτή του, μέσω ενσωματωμένου στην πλατφόρμα ηλεκτρονικού συστήματος επικοινωνίας, για την άμεση επίλυση αποριών σχετιζόμενων με τις θεματικές ενότητες και τις ασκήσεις αξιολόγησης ή την τελική εργασία.

6. ΤΡΟΠΟΣ ΕΞΕΤΑΣΗΣ ΚΑΙ ΒΑΘΜΟΛΟΓΗΣΗΣ

Σε κάθε διδακτική ενότητα ο εκπαιδευόμενος θα πρέπει να επιλύει και να υποβάλλει ηλεκτρονικά το αντίστοιχο τεστ, τηρώντας το χρονοδιάγραμμα που έχει δοθεί από τον εκπαιδευτή του. Η κλίμακα βαθμολογίας κυμαίνεται από 0 έως 100%. Συνολικά, η βαθμολογία κάθε θεματικής ενότητας προκύπτει κατά το 60% από τις ασκήσεις αξιολόγησης και κατά το υπόλοιπο 40% από την τελική εργασία, η οποία εκπονείται στο τέλος του συγκεκριμένου μαθήματος και εφόσον το απαιτεί η φύση αυτού.

Η χορήγηση του **Πιστοποιητικού Συνεχιζόμενης Επαγγελματικής Κατάρτισης** πραγματοποιείται, όταν ο εκπαιδευόμενος λάβει σε όλα τα μαθήματα βαθμό μεγαλύτερο ή ίσο του 50%. Σε περίπτωση που η συνολική βαθμολογία ενός ή περισσοτέρων μαθημάτων δεν ξεπερνά το 50%, ο εκπαιδευόμενος έχει τη δυνατότητα επανεξέτασης των μαθημάτων αυτών μετά την ολοκλήρωση της

εκπαιδευτικής διαδικασίας του προγράμματος. Η βαθμολογία που θα συγκεντρώσει κατά τη διαδικασία επανεξέτασής του είναι και η οριστική για τα εν λόγω μαθήματα, με την προϋπόθεση ότι ξεπερνά εκείνη που συγκέντρωσε κατά την κανονική διάρκεια της εκπαιδευτικής διαδικασίας. Σε διαφορετική περίπτωση διατηρείται η αρχική βαθμολογία.

7. ΛΟΙΠΕΣ ΥΠΟΧΡΕΩΣΕΙΣ ΕΚΠΑΙΔΕΥΟΜΕΝΩΝ - ΠΡΟΫΠΟΘΕΣΕΙΣ ΧΟΡΗΓΗΣΗΣ ΠΙΣΤΟΠΟΙΗΤΙΚΟΥ

Πέρα από την **επιτυχή ολοκλήρωση** του προγράμματος για τη χορήγηση του Πιστοποιητικού απαιτούνται τα εξής:

► **Συμμετοχή του εκπαιδευόμενου στη διαδικασία Δειγματοληπτικού Ελέγχου Ταυτοποίησης**

Η διαδικασία Δειγματοληπτικού Ελέγχου Ταυτοποίησης Εκπαιδευόμενου στοχεύει στη διασφάλιση της ποιότητας των παρεχομένων εκπαιδευτικών υπηρεσιών. Συγκεκριμένα, εξουσιοδοτημένο στέλεχος του Κέντρου Επιμόρφωσης και Δια Βίου Μάθησης του ΕΚΠΑ, επικοινωνεί τηλεφωνικώς με ένα τυχαίο δείγμα εκπαιδευόμενων, προκειμένου να διαπιστωθεί εάν συμμετείχαν στις εκπαιδευτικές διαδικασίες του προγράμματος, εάν αντιμετώπισαν προβλήματα σε σχέση με το εκπαιδευτικό υλικό, την επικοινωνία με τον ορισμένο εκπαιδευτή τους, καθώς και με τη γενικότερη μαθησιακή διαδικασία. Η τηλεφωνική επικοινωνία διεξάγεται με την ολοκλήρωση του εκάστοτε προγράμματος, ενώ η μέση χρονική διάρκειά της συγκεκριμένης διαδικασίας είναι περίπου 2-3 λεπτά.

Σε περίπτωση μη συμμετοχής του εκπαιδευόμενου στη διαδικασία Δειγματοληπτικού Ελέγχου Ταυτοποίησης, εφόσον κληθεί, ή μη ταυτοποίησής του κατά τη διεξαγωγή της, δεν χορηγείται το πιστοποιητικό σπουδών, ακόμα και αν έχει ολοκληρώσει επιτυχώς την εξ αποστάσεως εκπαιδευτική διαδικασία.

► **Συμμετοχή του εκπαιδευόμενου στη διαδικασία Δειγματοληπτικού Ελέγχου Εγγράφων**

Ο δειγματοληπτικός έλεγχος εγγράφων διασφαλίζει την εγκυρότητα των στοιχείων που έχει δηλώσει ο εκπαιδευόμενος στην αίτηση συμμετοχής του στο Πρόγραμμα και βάσει των οποίων έχει αξιολογηθεί και εγκριθεί η αίτηση συμμετοχής του σε αυτό.

Κατά τη διάρκεια ή μετά το πέρας του προγράμματος, πραγματοποιείται δειγματοληπτικός έλεγχος εγγράφων από τη Γραμματεία. Ο εκπαιδευόμενος θα πρέπει να είναι σε θέση να προσκομίσει τα απαραίτητα δικαιολογητικά τα οποία πιστοποιούν τα στοιχεία που έχει δηλώσει στην αίτηση συμμετοχής (Αντίγραφο Πτυχίου, Αντίγραφο Απολυτήριου Λυκείου, Βεβαίωση Εργασιακής Εμπειρίας, Γνώση Ξένων Γλωσσών κ.τ.λ.).

Σε περίπτωση μη συμμετοχής του εκπαιδευόμενου στη διαδικασία Δειγματοληπτικού Ελέγχου Εγγράφων, εφόσον κληθεί, ή μη ύπαρξης των δικαιολογητικών αυτών, δεν χορηγείται το πιστοποιητικό σπουδών, ακόμα και αν έχει ολοκληρώσει επιτυχώς την εξ αποστάσεως εκπαιδευτική διαδικασία.

► **Αποπληρωμή του συνόλου των διδάκτρων**

Ο εκπαιδευόμενος θα πρέπει να μην έχει οικονομικής φύσεως εκκρεμότητες. Σε περίπτωση που υπάρχουν τέτοιες, το πιστοποιητικό σπουδών διατηρείται στο αρχείο της Γραμματείας, μέχρι την ενημέρωση της για τη διευθέτηση της εκκρεμότητας.

Αναλυτική περιγραφή των παραπάνω υπάρχει στον Κανονισμό Σπουδών:
https://elearningekpa.gr/regulation

8. ΣΥΓΓΡΑΦΕΙΣ ΤΟΥ ΕΚΠΑΙΔΕΥΤΙΚΟΥ ΥΛΙΚΟΥ

Οι συγγραφείς του εκπαιδευτικού υλικού είναι μέλη ΔΕΠ του Εθνικού και Καποδιστριακού Πανεπιστημίου Αθηνών ή και ειδικοί εμπειρογνώμονες με ιδιαίτερη συγγραφική καταξίωση, οι οποίοι κατέχουν πολύ βασικό ρόλο στην υλοποίηση του προγράμματος.

9. ΠΩΣ ΔΙΑΜΟΡΦΩΝΕΤΑΙ Η ΥΛΗ ΤΟΥ ΠΡΟΓΡΑΜΜΑΤΟΣ

Το πρόγραμμα επαγγελματικής επιμόρφωσης και κατάρτισης περιλαμβάνει **8 θεματικές ενότητες (μαθήματα)**.

ΠΕΡΙΓΡΑΦΗ ΜΑΘΗΜΑΤΩΝ

Μάθημα - Το Επάγγελμα του Information Security Analyst

Διδακτική Ενότητα 1: Οι Τάσεις του Μέλλοντος και η Αγορά Εργασίας

Σκοπός της συγκεκριμένης διδακτικής ενότητας είναι η εισαγωγή στις βασικές έννοιες που αφορούν τις τεχνολογικές τάσεις του μέλλοντος και την εξέλιξη της αγοράς εργασίας, με ιδιαίτερη έμφαση στον ρόλο του Information Security Analyst. Παρέχεται το απαραίτητο πλαίσιο για την κατανόηση των δεξιοτήτων που απαιτούνται και των επαγγελματικών προοπτικών που διαμορφώνονται στη νέα ψηφιακή εποχή.

Διδακτική Ενότητα 2: Ο Ρόλος του Επαγγελματία στο Information Security

Σκοπός της συγκεκριμένης διδακτικής ενότητας είναι να αναδείξει τον κρίσιμο ρόλο του επαγγελματία στην Ασφάλεια Πληροφοριών, τόσο σε τεχνικό όσο και σε στρατηγικό επίπεδο. Παρουσιάζονται οι

βασικές αρμοδιότητες, οι απαιτούμενες δεξιότητες και οι προκλήσεις που καλείται να αντιμετωπίσει, καθώς και οι τρόποι με τους οποίους συμβάλλει ουσιαστικά στην προστασία ενός οργανισμού ή συστήματος.

Μάθημα - Ανάλυση Ασφαλείας στα Υπολογιστικά Συστήματα

Διδακτική Ενότητα 1: Αρχές Αρχιτεκτονικής Ασφαλείας Λογισμικών και Δικτυακών Συστημάτων

Σκοπός της συγκεκριμένης διδακτικής ενότητας είναι η παρουσίαση του πλήρους φάσματος των επιπέδων των δικτυακών υποδομών, από το φυσικό έως το επίπεδο εφαρμογών. Αναλύονται οι τεχνικές άμυνας, οι μέθοδοι κρυπτογράφησης, οι μηχανισμοί πιστοποίησης και οι πρακτικές ασφαλούς διαχείρισης που διασφαλίζουν την προστασία και την ακεραιότητα των συστημάτων.

Διδακτική Ενότητα 2: Διαδικασίες Ταυτοποίησης Χρηστών και Διαχείριση Πρόσβασης

Σκοπός της συγκεκριμένης διδακτικής ενότητας είναι η κατανόηση των βασικών αρχών που διέπουν τη διαχείριση ταυτότητας, καθώς και η παρουσίαση των εργαλείων που χρησιμοποιούνται για τη διασφάλιση της ασφάλειας των προσβάσεων.

Διδακτική Ενότητα 3: Ανάλυση Κρυπτογραφίας και Διαχείριση Κλειδιών σε Υπολογιστικά Συστήματα

Σκοπός της συγκεκριμένης διδακτικής ενότητας είναι η ανάδειξη της σημασίας της ασφάλειας ως θεμελιώδους προϋπόθεσης για την ψηφιακή πρόοδο, παρέχοντας ταυτόχρονα τις βάσεις για περαιτέρω ενασχόληση και εμβάθυνση στο πεδίο της πληροφορικής ασφάλειας.

Διδακτική Ενότητα 4: Ασφάλεια Κινητών Συσκευών και Νέφους (Mobile and Cloud Security)

Σκοπός της συγκεκριμένης διδακτικής ενότητας είναι η παρουσίαση των βασικών εννοιών που συγκροτούν το φαινόμενο του υπολογιστικού νέφους. Αναλύονται οι κύριοι ορισμοί και τα χαρακτηριστικά που το διακρίνουν, τα μοντέλα παροχής υπηρεσιών (IaaS, PaaS, SaaS), καθώς και οι τύποι ανάπτυξης, όπως το δημόσιο, ιδιωτικό και υβριδικό νέφος.

Μάθημα - Επικοινωνία και Διαχείριση Χρόνου

Διδακτική Ενότητα 1: Έννοια και σημασία, είδη και βασικές αρχές επικοινωνίας

Σκοπός της συγκεκριμένης διδακτικής ενότητας είναι η κατανόηση της έννοιας και της σημασίας της επικοινωνίας, μέσα από την ανάλυση της διαδικασίας και των βασικών της στοιχείων.

Παρουσιάζονται οι κύριες μορφές επικοινωνίας, όπως διαμορφώνονται ανάλογα με τον τρόπο κωδικοποίησης, το κανάλι, τα εμπλεκόμενα μέρη, τον χρόνο και το ύφος, ενώ δίνεται έμφαση στις αρχές που διασφαλίζουν την αποτελεσματικότητά της με βάση το μοντέλο των 7Cs.

Διδακτική Ενότητα 2: Βασικές δεξιότητες επικοινωνίας και τρόποι ανάπτυξής τους

Σκοπός της συγκεκριμένης διδακτικής ενότητας είναι η παρουσίαση των βασικών δεξιοτήτων επικοινωνίας, με έμφαση στη λεκτική και μη λεκτική επικοινωνία καθώς και στην ενεργητική ακρόαση. Η ανάλυση συνοδεύεται από πρακτικές προσεγγίσεις και τεχνικές που συμβάλλουν στη συστηματική καλλιέργεια και βελτίωση των δεξιοτήτων αυτών.

Διδακτική Ενότητα 3: Επικοινωνία σε ομάδες

Σκοπός της συγκεκριμένης διδακτικής ενότητας είναι η ανάδειξη της σημασίας της αποτελεσματικής επικοινωνίας στο εσωτερικό μιας ομάδας αλλά και στις σχέσεις της με εξωτερικά ενδιαφερόμενα μέρη. Εξετάζονται τα συνηθέστερα εμπόδια που δυσχεραίνουν την επικοινωνία, οι συνέπειες της ανεπαρκούς ανταλλαγής πληροφοριών, καθώς και πρακτικές μέθοδοι υπέρβασής τους. Παράλληλα, παρουσιάζονται τρόποι βελτίωσης της επικοινωνίας και καλές πρακτικές που μπορούν να εφαρμοστούν τόσο στις προφορικές αλληλεπιδράσεις όσο και στη συνεργασία με stakeholders.

Διδακτική Ενότητα 4: Τεχνικές για τη διαχείριση χρόνου και την ιεράρχηση προτεραιοτήτων

Σκοπός της συγκεκριμένης διδακτικής ενότητας είναι η παρουσίαση της εφαρμογής του πλαισίου Scrum στον τομέα της ανάπτυξης λογισμικού, με έμφαση στην ιεράρχηση προτεραιοτήτων και τη διαχείριση χρόνου. Αναλύονται πρακτικές και τεχνικές όπως η MoSCoW, ο πίνακας Eisenhower και η μέθοδος RICE για την προτεραιοποίηση του product backlog, καθώς και οι τεχνικές Timeboxing, Pomodoro και Sprint Planning Poker για την αποτελεσματική διαχείριση χρόνου στο πλαίσιο του Scrum.

Μάθημα - Επιθέσεις σε Web Servers

Διδακτική Ενότητα 1: Web Security Vulnerabilities

Σκοπός της συγκεκριμένης διδακτικής ενότητας είναι να εξεταστούν οι πιο κοινές ευπάθειες ασφαλείας του web. Περιλαμβάνονται η SQL Injection, το Cross Site Scripting ή XSS, το Broken Authentication και Session Management, τα Insecure Direct Object References, η Cross Site Request Forgery (CSRF), η Security Misconfiguration, η Insecure Cryptographic Storage, η Failure to Restrict URL Access, η Insufficient Transport Layer Protection και τα Unvalidated Redirects και Forwards.

Συγκεκριμένα, παρουσιάζονται οι ορισμοί αυτών των ευπαθειών, ο τρόπος που εκτελούνται με παραδείγματα, καθώς και οι συστάσεις για την προστασία από αυτές.

Διδακτική Ενότητα 2: Τύποι Επιθέσεων σε Web Servers

Σκοπός της συγκεκριμένης διδακτικής ενότητας είναι να παρουσιαστούν οι συνηθέστεροι web servers, να αναγνωριστούν οι τύποι επιθέσεων σε web servers, να περιγραφούν οι συνέπειες των επιτυχών επιθέσεων, να παρουσιαστούν ορισμένα κοινά εργαλεία επίθεσης σε web servers, καθώς και να αναφερθούν οι επιθέσεις SQL Injection, DoS (Denial of Service) και Sniffing μαζί με τους τύπους αυτών των επιθέσεων.

Διδακτική Ενότητα 3: Αντίμετρα για Επιθέσεις σε Web Server

Σκοπός της συγκεκριμένης διδακτικής ενότητας είναι να παρουσιαστούν οι τρόποι αποφυγής των επιθέσεων σε web servers και τα αντίμετρα για MAC flooding και sniffing. Επίσης, να αναδειχθούν μέθοδοι προστασίας του website έναντι hacks και συγκεκριμένων ευπαθειών/επιθέσεων — DoS, SQL Injection, Insecure Direct Object Reference, CSRF, Security Misconfiguration, Insecure Cryptographic Storage, Insufficient Transport Layer Protection και XSS — καθώς και τα αντίμετρα για την επίθεση session fixation.

Μάθημα - Πολιτικές Ασφάλειας Πληροφοριακών Συστημάτων

Διδακτική Ενότητα 1: Προσδιορισμός των Απειλών για την Ασφάλεια των Πληροφοριακών Συστημάτων

Σκοπός της συγκεκριμένης διδακτικής ενότητας είναι η παρουσίαση του τρόπου ανάλυσης επικινδυνότητας ενός πληροφοριακού συστήματος. Αρχικά θα παρουσιαστεί η μεθοδολογία ανάλυσης, εν συνεχεία θα αναλυθεί βήμα-βήμα η διαδικασία και τα βασικά φύλλα εργασίας (worksheets) της μεθοδολογίας Allegro, και τέλος θα χρησιμοποιηθεί η μέθοδος ανάλυσης επικινδυνότητας OCTAVE Allegro για την αξιολόγηση της ασφάλειας ενός υποθετικού πληροφοριακού συστήματος δημόσιου νοσοκομείου.

Διδακτική Ενότητα 2: Πολιτικές Ασφάλειας Πληροφοριακών Συστημάτων

Σκοπός της συγκεκριμένης διδακτικής ενότητας είναι η παρουσίαση μιας σύνοψης των βασικότερων κανόνων που διέπουν τις Πολιτικές Ασφάλειας των πληροφοριακών συστημάτων (ΠΣ).

Διδακτική Ενότητα 3: Disaster Recovery Plan

Σκοπός της συγκεκριμένης διδακτικής ενότητας είναι η παρουσίαση του Σχεδίου Ανάκαμψης από Καταστροφές (Disaster Recovery and Contingency Plan). Εξετάζονται ο κύριος στόχος του DRP, η

δημιουργία της Ομάδας Έκτακτης Ανάγκης (ΟΕΑ) και των απαραίτητων εγκαταστάσεων για περιπτώσεις έκτακτης ανάγκης, η στρατηγική των αντιγράφων ασφαλείας και του cloud mirroring, καθώς και οι διαδικασίες διαχείρισης κινδύνων. Παρουσιάζονται επίσης τα γεγονότα που οδηγούν στην ενεργοποίηση του σχεδίου, η διαδικασία επείγουσας ειδοποίησης, η κλιμάκωση και ενεργοποίηση του DRP, καθώς και η ενεργοποίηση της Ομάδας Έκτακτης Ανάγκης.

Διδακτική Ενότητα 4: Προγράμματα Ενημερότητας Ασφάλειας

Σκοπός της συγκεκριμένης διδακτικής ενότητας είναι η αναλυτική παρουσίαση της έννοιας της ενημερότητας ασφάλειας και της σημασίας της για τους οργανισμούς. Παρουσιάζεται η μεθοδολογία ανάπτυξης Προγράμματος Ενημερότητας και Ευαισθητοποίησης χρηστών των Πληροφοριακών Συστημάτων σε θέματα Ασφάλειας και Προστασίας της Ιδιωτικότητας, με ιδιαίτερη έμφαση στις διεργασίες που πραγματοποιούνται στις τρεις φάσεις της μεθοδολογίας του E.N.I.S.A. Τέλος, εξετάζονται οι δράσεις που περιλαμβάνει ένα πρόγραμμα ενημερότητας (Information Security Awareness Program/ISAP) μέσα από ενδεικτικό παράδειγμα.

Μάθημα - Ανάλυση Ασφάλειας Δικτύων

Διδακτική Ενότητα 1: Αρχές Ασφάλειας Δικτύων και Πρωτόκολλα Επικοινωνίας

Σκοπός της συγκεκριμένης διδακτικής ενότητας είναι η παρουσίαση των αρχών ασφαλείας δικτύων και των βασικών πρωτοκόλλων επικοινωνίας, με έμφαση στις διαδικασίες ταυτοποίησης και ελέγχου πρόσβασης. Αναλύονται οι μέθοδοι σχεδιασμού και υλοποίησης ασφαλών δικτύων με τεχνολογίες όπως VPNs, κρυπτογράφηση και τμηματοποίηση, ενώ εξετάζονται τεχνικές έννοιες που αφορούν την ασφάλεια σε διαφορετικά επίπεδα εντός ενός οργανισμού.

Διδακτική Ενότητα 2: Firewalls and Routers

Σκοπός της συγκεκριμένης διδακτικής ενότητας είναι η παρουσίαση των βασικών συσκευών που χρησιμοποιούνται για την ασφάλεια των δικτυακών υποδομών, με έμφαση στους δρομολογητές και τα τείχη προστασίας.

Διδακτική Ενότητα 3: Σχεδιασμός Δικτύου Ασφαλείας και Διαχείριση Αδυναμιών (Secure Network Design and Vulnerability Management)

Σκοπός της συγκεκριμένης διδακτικής ενότητας είναι η παρουσίαση των βασικών αρχών που διέπουν τον σχεδιασμό ασφαλών δικτύων.

Διδακτική Ενότητα 4: Κατανόηση Απειλών στον Κυβερνοχώρο (Cyber Threats)

Σκοπός της συγκεκριμένης διδακτικής ενότητας είναι η παρουσίαση ενός ευρέος φάσματος κυβερνοαπειλών, όπως οι επιθέσεις DDoS, οι ευπάθειες λογισμικού και οι επιθέσεις κοινωνικής μηχανικής. Παράλληλα, αναλύονται οι κύριες απειλές στον κυβερνοχώρο και προτείνονται κατάλληλες λύσεις μετριασμού, ενώ εξετάζονται οι νέες τάσεις και τεχνολογίες στον τομέα της ασφάλειας δικτύων με στόχο τη συνεχή βελτίωση των υποδομών προστασίας.

Μάθημα - Η Δεξιότητα της Αναλυτικής και Κριτικής Σκέψης στον Εργασιακό Χώρο

Διδακτική Ενότητα 1: Εισαγωγή στην Αναλυτική και Κριτική Σκέψη και τη Σημασία τους στον Εργασιακό Χώρο

Σκοπός της συγκεκριμένης διδακτικής ενότητας είναι η ανάδειξη της σημασίας της κριτικής και αναλυτικής σκέψης στον εργασιακό χώρο. Παρουσιάζονται τα βασικά χαρακτηριστικά και στοιχεία που διέπουν καθεμία από αυτές, ώστε να καταστεί δυνατή η κατανόηση των διαφορών και των ομοιοτήτων τους και να αναγνωριστεί ο βαθμός εξοικείωσης με τα δύο αυτά είδη σκέψης.

Διδακτική Ενότητα 2: Μεθοδολογία Ανάπτυξης Κριτικής Σκέψης

Σκοπός της συγκεκριμένης διδακτικής ενότητας είναι η εισαγωγή στην κριτική σκέψη και η παρουσίαση του πεδίου εφαρμογής της. Αναδεικνύονται τα βασικά σημεία που πρέπει να ληφθούν υπόψη για την ανάπτυξή της, ενώ εξετάζονται τα ρητορικά τεχνάσματα και οι λογικές πλάνες που μπορούν να επηρεάσουν τη διαδικασία ορθολογικής σκέψης.

Διδακτική Ενότητα 3: Μέθοδος Ανάλυσης Προβλημάτων (αναλυτική σκέψη)

Σκοπός της συγκεκριμένης διδακτικής ενότητας είναι η κατανόηση της διαδικασίας λήψης αποφάσεων. Παρουσιάζονται τα βασικά χαρακτηριστικά που τη διέπουν, αναλύονται ενδεικτικά μοντέλα λήψης αποφάσεων και εξετάζεται η σημασία της αβεβαιότητας ως καθοριστικού παράγοντα που επηρεάζει την αποτελεσματικότητας και την ορθότητα των επιλογών.

Διδακτική Ενότητα 4: Διαχείριση Πληροφοριών και Πηγών - Επίλυση Προβλημάτων

Σκοπός της συγκεκριμένης διδακτικής ενότητας είναι η παρουσίαση των τρόπων αξιολόγησης και διαχείρισης πληροφοριών, καθώς και η ανάλυση διαδικασιών εντοπισμού και προσδιορισμού προβλημάτων. Παράλληλα, αναδεικνύονται οι βασικές δεξιότητες που απαιτούνται για την αποτελεσματική επίλυσή τους.

Διδακτική Ενότητα 1: Εισαγωγή στην Ανάλυση Απειλών και τη Διαχείριση Ρίσκου

Σκοπός της συγκεκριμένης διδακτικής ενότητας είναι η κατανόηση της έννοιας του κινδύνου, των απειλών και της ευπάθειας σε διαφορετικά περιβάλλοντα, καθώς και η παρουσίαση των μεθοδολογιών αξιολόγησης ρίσκων και η αναφορά σε σχετικά πλαίσια και πρότυπα.

Διδακτική Ενότητα 2: Αρχές Εντοπισμού Ανάλυσης και Καταγραφής Απειλών (Incident Detection and Analysis)

Σκοπός της συγκεκριμένης διδακτικής ενότητας είναι η εισαγωγή στις θεμελιώδεις αρχές εντοπισμού, ανάλυσης και καταγραφής απειλών (Incident Detection and Analysis). Παρουσιάζονται τεχνικές αναγνώρισης κακόβουλων ενεργειών, μεθοδολογίες ανάλυσης και διαδικασίες συστηματικής καταγραφής περιστατικών, ενώ εξετάζονται σχετικά εργαλεία παρακολούθησης, βέλτιστες πρακτικές και πρότυπα αναφοράς. Στόχος είναι η καλλιέργεια δεξιοτήτων για αποτελεσματική απόκριση και διασφάλιση της ακεραιότητας των πληροφοριακών συστημάτων.

Διδακτική Ενότητα 3: Χειρισμός, Αποκατάσταση και Ανασκόπηση Απειλής (Incident Response, Recovery and Post-Incident Activities)

Σκοπός της συγκεκριμένης διδακτικής ενότητας είναι η παρουσίαση των αρχών και διαδικασιών χειρισμού, αποκατάστασης και ανασκόπησης απειλών (Incident Response, Recovery and Post-Incident Activities). Εξετάζονται τα στάδια από την άμεση απόκριση και τον περιορισμό ζημιών έως την πλήρη επαναφορά συστημάτων, καθώς και οι πρακτικές επικοινωνίας με τα ενδιαφερόμενα μέρη. Παράλληλα, παρουσιάζονται τεχνικές αξιολόγησης της ανταπόκρισης και ανασκόπησης με στόχο τη βελτίωση μελλοντικών πρακτικών ασφάλειας, ενισχύοντας την ικανότητα λήψης τεκμηριωμένων αποφάσεων και τη συνεχή αναβάθμιση της ασφάλειας πληροφοριών.

Διδακτική Ενότητα 4: Τεχνικές Αξιολόγησης Ρίσκου και Στρατηγικές Μετριασμού (Mitigation Strategy)

Σκοπός της συγκεκριμένης διδακτικής ενότητας είναι η παρουσίαση τεχνικών αξιολόγησης ρίσκου και στρατηγικών μετριασμού (Mitigation Strategy) σε περιβάλλοντα ασφάλειας πληροφοριών. Αναλύονται μέθοδοι αναγνώρισης, εκτίμησης και ιεράρχησης κινδύνων, καθώς και στρατηγικές εφαρμογής κατάλληλων ελέγχων με έμφαση στη συμμόρφωση με την ευρωπαϊκή νομοθεσία, όπως ο GDPR. Παρουσιάζονται πρότυπα και βέλτιστες πρακτικές που συμβάλλουν στη μείωση της πιθανότητας και του αντίκτυπου απειλών, με στόχο την καλλιέργεια δεξιοτήτων τεκμηριωμένης λήψης αποφάσεων και αποτελεσματικής προστασίας δεδομένων και συστημάτων.