ΠΟΛΥΕΠΙΧΕΙΡΗΣΙΑΚΟ ΠΡΟΓΡΑΜΜΑ ΚΑΤΑΡΤΙΣΗΣ

ΥΠΕΥΘΥΝΟΣ ΑΣΦΑΛΕΙΑΣ ΠΛΗΡΟΦΟΡΙΩΝ (CISO – CHIEF INFORMATION SECURITY OFFICER) ΣΤΟ ΠΡΟΤΥΠΟ ISO 27001

Στοιχεία Διεξαγωγής

Ημερομηνίες & Ώρες Διεξαγωγής:
15/11/2023
17/11/2023

Διάρκεια Προγράμματος:
Σύνολο 14 ώρες
Τοποθεσία:
ΔΙΑ ΖΩΣΗΣ

Κόστος Συμμετοχής

Αρχικό Κόστος:
€418 + [VAT (€79.42)]

Κόστος με επιδότηση:
€180+ [VAT (€79.42)]

Κόστος για Μη Δικαιούχους ΑνΑΔ:
€368 [συμπεριλαμβανομένου του ΦΠΑ]
ΑΙΤΗΣΗ ΣΥΜΜΕΤΟΧΗΣ

ΤΟ ΠΡΟΓΡΑΜΜΑ ΕΧΕΙ ΕΓΚΡΙΘΕΙ ΑΠΟ ΤΗΝ ΑΝΑΔ ΚΥΠΡΟΥ.
Οι επιχειρήσεις που συμμετέχουν με εργοδοτούμενους τους οι οποίοι ικανοποιούν τα κριτήρια της Αρχής θα τύχουν της σχετικής επιχορήγησης.

Σκοπός του προγράμματος

Η αποτελεσματική αντιμετώπιση των προκλήσεων ασφάλειας των συστημάτων δικτύου και πληροφοριών απαιτεί μια σφαιρική προσέγγιση στο φορέα, που να καλύπτει ελάχιστες ικανές απαιτήσεις δημιουργίας και σχεδιασμού, την ανταλλαγή πληροφοριών, τη συνεργασία. Κομβικό ρόλο στη θωράκιση των φορέων έναντι αυτών των απειλών, υπηρετεί ο Υπεύθυνος Ασφάλειας Πληροφοριών (ή Chief Information Security Officer).

Η ένταση ανάγκης για ουσιαστική εκπαίδευση Υπεύθυνων Ασφάλειας Πληροφοριών αυξήθηκε τελευταία. Το Πρότυπο ISO 27001, επιβάλει σε φορείς που πιστοποιούνται με αυτό, να διαθέτουν Υπεύθυνο Ασφάλειας Πληροφοριών, ή CISO-Chief Information Security Officer κατά την ορολογία του Προτύπου. Η εφαρμογή συστημάτων συμμόρφωσης με το Πρότυπο ISO 27001, έχει αρχίσει να υλοποιείται από λίγους αλλά όχι αμελητέους σε ποσότητα φορείς στη χώρα. Στο επόμενο διάστημα ο αριθμός αυτός αναμένεται να αυξηθεί σημαντικά καθώς:

- Ενισχύεται το φαινόμενο «ντόμινο», όπου ένας φορέας Πιστοποιημένος με το Πρότυπο, «ωθεί» συνεργαζόμενους φορείς να Πιστοποιηθούν, ώστε να διασφαλίζει τις απαιτήσεις που προκύπτουν από σχετική πρόνοια του Προτύπου ως προς την Ασφάλεια Πληροφοριών σε Συνεργασίες με Τρίτους Φορείς.
- Το ίδιο φαινόμενο, παρουσιάζεται από φορείς που ακολουθούν (μη πιστοποιημένη αλλά υπαρκτή), συμμόρφωση με τον Κανονισμό Προστασίας Προσωπικών Δεδομένων, που πιέζει φορείς – συνεργάτες για Ασφάλεια Πληροφοριών, σύμφωνα με το Άρθρο 28 του Κανονισμού.
- Το συγχρηματοδοτούμενο «Σχέδιο Ψηφιακής Αναβάθμισης Επιχειρήσεων» του Υπουργείου Βιομηχανίας και Εμπορίου, καθορίζει ονομαστικά το Πρότυπο ISO 27001 και την Πιστοποίηση σύμφωνα με αυτό, στις επιδοτούμενες δράσεις. Πολλές επιχειρήσεις θα ενταχθούν στο σχέδιο αυτό και πολλές εξ αυτών, θα εντάξουν την Πιστοποίηση με το εν λόγω Πρότυπο στις δράσεις για τις οποίες θα επιδοτηθούν.
- Υπάρχει πλέον υποχρέωση των φορέων που παρέχουν κρίσιμες υπηρεσίες για τους πολίτες και φορέων εκμετάλλευσης κρίσιμων υποδομών [σύμφωνα με τις ανακοινώσεις της Αρχής Ψηφιακής Ασφάλειας (ΑΨΑ), ως εφαρμογή της Ευρωπαϊκής Οδηγίας γνωστής ως Οδηγία «NIS- Network and Information Systems»], να εφαρμόζουν όλες τις Αρχές Ασφάλειας Πληροφοριών

Contact Us

Mind The Gap Ltd

Tel: 25251435

Fax: 25251436

info@mindthegap.com.cy

www.mindthegap.com.cy

Με την ολοκλήρωση της Εκπαίδευσης οι Συμμετέχοντες θα λάβουν Πιστοποιητικό Παρακολούθησης.

και να τείνουν σε ασφαλείς διαδικτυακές υπηρεσίες (Κυβερνοασφάλεια). Ονομαστικά αναφέρεται στην Κανονιστική Διοικητική Πράξη 389/20 που εκδόθηκε σε εφαρμογή του Νόμου 89/I/2020, η υποχρέωση των φορέων να διαθέτουν Υπεύθυνο Ασφάλειας Πληροφοριών ή Υπεύθυνο Ασφάλειας Δικτύων και Πληροφοριών.

Τα παραπάνω, απαιτούν εξειδικευμένες γνώσεις από τα πρόσωπα που αναλαμβάνουν για λογαριασμό του φορέα τους αυτό το έργο (του Υπεύθυνου Ασφάλειας Πληροφοριών), κάτι που υπερβαίνει τα συνήθη έως τώρα καθήκοντά τους και απαιτεί εξειδικευμένη – συγκεκριμένη εκπαίδευση.

Η θεματολογία του σεμιναρίου είναι ιδανική για:

- Καθορισμένους από τον φορέα τους Υπεύθυνους Ασφάλειας Πληροφοριών (ο τίτλος μπορεί να διαφέρει, ειδικά σε φορείς που βρίσκονται σε διαδικασία Ανάπτυξης Συστημάτων Συμμόρφωσης με το Πρότυπο ISO 27001 ή/και τις κατευθύνσεις της Αρχής Ψηφιακής Ασφάλειας όπως εξειδικεύονται στην Κανονιστική Διοικητική Πράξη - ΚΔΠ 389/20, όπως ενδεικτικά: Υπεύθυνος Πληροφοριακής Υποδομής, Υπεύθυνος Ασφάλειας Δικτύων και Συστημάτων, Υπεύθυνος Ασφάλειας Δικτύων και Πληροφοριών, Υπεύθυνος Κυβερνοασφάλειας, CIO-Chief Information Officer, CTO – Chief Technology Officer, ICT Security Manager κλπ.), οι οποίοι επιθυμούν να εξειδικευτούν στο αντικείμενο που θα υπηρετήσουν.
- Διαχειριστές Πληροφοριακών Πόρων (IT Administrators), τους οποίους ο φορέας επιθυμεί να αναβαθμίσει σε Υπεύθυνους Ασφάλειας Πληροφοριών,
- Σύμβουλοι Επιχειρήσεων που αναπτύσσουν συστήματα συμμόρφωσης με το Πρότυπο ISO 27001 ή/και τις κατευθύνσεις της Αρχής Ψηφιακής Ασφάλειας,
- Εργαζόμενοι σε εταιρείες Πληροφορικής, που λειτουργούν ως εξωτερικοί συνεργάτες φορέων και θέλουν να προσφέρουν υπηρεσίες εξωτερικού Υπεύθυνου Ασφάλειας Πληροφοριών,
- Άνεργοι όπως προβλέπεται στον Οδηγό του Προγράμματος, εφόσον είναι απόφοιτοι Σχολών σχετικών με Πληροφορική ή/και Ψηφιακή Ασφάλεια ή/και Μηχανικοί Πολυτεχνικών Σχολών.

Στόχοι του προγράμματος

Με την ολοκλήρωση του προγράμματος οι συμμετέχοντες θα είναι σε θέση να:

- Να διατυπώνουν το πότε απαιτείται διερεύνηση περιστατικού ασφάλειας πληροφοριών
- Να ταξινομούν τα βήματα διερεύνησης περιστατικού ασφάλειας πληροφοριών
- Να περιγράφουν το ρόλο τους στη φάση Πιστοποίησης του φορέα (πριν, κατά και μετά τον έλεγχο του φορέα)
- Να περιγράφουν τις υποχρεώσεις του φορέα προς την Αρχή Ψηφιακής Ασφάλειας (ΑΨΑ)
- Να εκτελούν τους απαραίτητους ελέγχους δραστηριοτήτων του IT Administrator
- Να επιλέγουν κατάλληλες μεθόδους ανίχνευσης και πρόληψης εισβολών για επίτευξη κυβερνοασφάλειας

- Να συνεργάζονται με τις οργανωτικές μονάδες στη συλλογή αποδεικτικών στοιχείων για τον έλεγχο του Φορέα Πιστοποίησης

Προφίλ Εισηγητή

Ο εισηγητής Δημητρίου Κυριάκος, είναι εγκεκριμένος Εκπαιδευτής Επαγγελματικής Κατάρτισης, με μακρόχρονη εμπειρία στην εκπαίδευση Ενηλίκων σε διάφορες Ευρωπαϊκές Χώρες. Διαθέτει εξειδικευμένες γνώσεις στην Προστασία Προσωπικών Δεδομένων και στην Ασφάλεια των Πληροφοριών και έχει βοηθήσει συμβουλευτικά πάρα πολλές επιχειρήσεις στην συμμόρφωση τους με τον Κανονισμό GDPR.

Θεματολόγιο

- Εισαγωγική Ενότητα
- Ενότητα 1: Βασικές γνώσεις και Ορολογία, Αρχές Νομιμότητας Επεξεργασιών και Νόμιμες Βάσεις
- Ενότητα 2: Κατανόηση ορισμών και βασικών εννοιών
- Ενότητα 3: Οι βασικές και Συμπληρωματικές Αρχές της Ασφάλειας Πληροφοριών
- Ενότητα 4: Τα Στοιχεία Ενεργητικού (Asset) στην Ασφάλεια Πληροφοριών και ο έλεγχός τους
- Ενότητα 5: Ο έλεγχος και η Συμβουλευτική του ΥΑΠ στο ανθρώπινο δυναμικό
- Ενότητα 6: Τα αρχεία ενεργειών (log files - Ιχνηλασιμότητα) και ο κεντρικός τους ρόλος στην Ασφάλεια Πληροφοριών
- Ενότητα 7: Ο έλεγχος του IT Administrator, ως βασικό στοιχείο καθηκόντων του Υπεύθυνου Ασφάλειας Πληροφοριών
- Ενότητα 8: Ο Ρόλος του Υπεύθυνου Ασφάλειας Πληροφοριών (ΥΑΠ) στην Επιχειρησιακή Συνέχεια
- Ενότητα 9: Ο Ρόλος του Υπεύθυνου Ασφάλειας Πληροφοριών (ΥΑΠ) στη Διαχείριση Περιστατικών Ασφαλείας (Incident management)
- Ενότητα 10: Η Πιστοποίηση της Ασφάλειας Πληροφοριών
- Ενότητα 11: Ο Υπεύθυνος Ασφάλειας Πληροφοριών στην Κυβερνοασφάλεια
- Ενότητα 12: Ολοκλήρωση προγράμματος