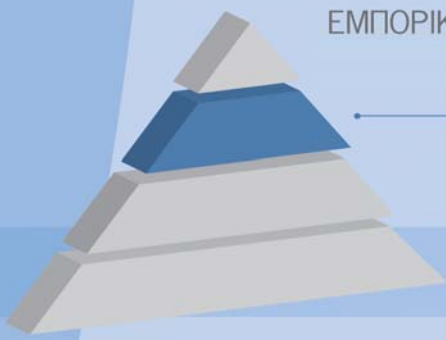




ΕΠΙΠΕΔΟ III - Διοίκηση εμπορικών τραπεζών

ΑΣΦΑΛΕΙΑ ΠΛΗΡΟΦΟΡΙΑΚΩΝ ΣΥΣΤΗΜΑΤΩΝ

Σεμινάριο εξειδικευμένων γνώσεων

23 – 25 Φεβρουαρίου 2012

Η σημασία της ασφάλειας των τραπεζικών δεδομένων είναι αδιαπραγμάτευτη. Οι τραπεζικοί οργανισμοί λαμβάνουν a priori όλα τα απαραίτητα μέτρα ώστε να εξασφαλίζεται η μέγιστη δυνατή ασφάλεια συναλλαγών και διαχείρισης τραπεζικών δεδομένων. Ωστόσο, ακόμα και οι πιο προηγμένες μέθοδοι μπορούν να αποδειχθούν κενές περιεχομένου, αν τα εμπλεκόμενα μέρη αγνοούν ή παραβλέπουν τους πιθανούς κινδύνους, καθώς και τις επιπτώσεις που συνεπάγεται η μη συμμόρφωση με τους κανόνες ασφάλειας. Κατά συνέπεια η συμμόρφωση με τις οδηγίες ασφάλειας, εκτός από ατομική υποχρέωση του κάθε εργαζόμενου, είναι διευθυντική απόφαση και ευθύνη.

Σκοπός:

Το σεμινάριο αποσκοπεί στο να ευαισθητοποιήσει τους συμμετέχοντες σχετικά με τα σύγχρονα προβλήματα στο χώρο της ασφάλειας δικτύων, υπολογιστών, και δεδομένων, και να τους εισαγάγει στις ενδεικνυόμενες στρατηγικές, μεθοδολογίες και πρότυπα αντιμετώπισής τους. Πιο συγκεκριμένα, το σεμινάριο περιλαμβάνει:

- Απαρίθμηση και ανάλυση των κινδύνων που αφορούν στη διαχείριση διαβαθμισμένης πληροφορίας και ανάπτυξη στρατηγικών σχετικά με την ασφάλεια των πληροφοριών
- Παρουσίαση των διαφόρων ειδών επιθέσεων που μπορεί να δεχθεί ένας τραπεζικός οργανισμός
- Παρουσίαση των προτύπων ασφάλειας
- Ανάλυση των σύγχρονων μηχανισμών ελέγχου και προστασίας ενός τραπεζικού οργανισμού μέσω επιτυχημένων πρακτικών ασφάλειας.

Έμφαση δίνεται στη μελέτη περιπτώσεων και την αντιμετώπιση πρακτικών θεμάτων.

Μαθησιακά αποτελέσματα:

Εξοικείωση με τις διάφορες μεθοδολογίες ασφάλειας πληροφοριακών συστημάτων και τους χειρισμούς πρόληψης περιστατικών ή περιορισμού των ζημιών στην εύρυθμη λειτουργία του οργανισμού.

Συμμετέχοντες:

Στελέχη που ασχολούνται με:

- τη διεύθυνση πληροφορικής και τη διεύθυνση ασφάλειας,
- τη διεύθυνση τμημάτων ή μονάδων του οργανισμού,
- τη διαχείριση ποιότητας και διαδικασιών,
- τον εσωτερικό έλεγχο.

Προαπαιτούμενα:

- Γνώση των βασικών λειτουργιών ενός υπολογιστή σε επίπεδο μέσου χρήστη,
- Αντίληψη, σε επίπεδο κοινού χρήστη, της λειτουργικότητας του διαδικτύου, καθώς και γενικότερα των δικτύων υπολογιστών.

Εισηγητές:

Δρ. Ζωή Αικατερινίδη, Σταύρος Σουρούτης, Παναγιώτης Κρομμυδάκης: Στελέχη Εταιρείας Προϊόντων, Λύσεων και Υπηρεσιών Πληροφορικής.

Διάρκεια: 24 ώρες.

Χρόνος διεξαγωγής: 23 – 25 Φεβρουαρίου 2012 (ώρες 8:30 – 16:30)

Δίδακτρα: 620 €.

Αριθμός συμμετεχόντων: Μέχρι 20, κατά προτεραιότητα δηλώσεων συμμετοχής.

Τόπος διεξαγωγής: Ελληνικό Τραπεζικό Ινστιτούτο, Σίνα 11, Αθήνα.

Για **δηλώσεις συμμετοχής**, συμπληρωματικές πληροφορίες, υποβολή προγράμματος στον ΟΑΕΔ παρακαλούμε τηλεφωνήστε στο 210 33.86.411 (κ. Τασάκος).

Ακύρωση εντός 5 εργάσιμων ημερών από την ημερομηνία έναρξης συνεπάγεται επιβάρυνση ίση με το 1/2 των διδάκτρων.

ΣΕΜΙΝΑΡΙΟ 9

ΑΣΦΑΛΕΙΑ ΠΛΗΡΟΦΟΡΙΑΚΩΝ ΣΥΣΤΗΜΑΤΩΝ

Θεματολογία

- Ασφάλεια των τραπεζικών πληροφοριακών υποδομών και συστημάτων (ασφάλεια δικτύων υπολογιστών, βάσεων δεδομένων, web εφαρμογών, κωδικοποιημένα (encrypted) επικοινωνία)
- Διαβάθμιση, ακεραιότητα και διαθεσιμότητα των ευαίσθητων τραπεζικών δεδομένων
- Προστασία και προσβασιμότητα των ευαίσθητων τραπεζικών δεδομένων
- Μηχανισμοί, διαδικασίες και συστήματα εξουσιοδότησης και ελέγχου ταυτοποίησης χρηστών (smart cards, βιομετρικά, identity and access management systems)
- Στρατηγικός και επιχειρησιακός σχεδιασμός της προστασίας των πληροφοριακών συστημάτων και των ευαίσθητων δεδομένων ενός τραπεζικού οργανισμού
- Αναγνώριση, εκτίμηση και διαχείριση κινδύνων σχετικών με την ασφάλεια των πληροφοριακών συστημάτων του οργανισμού
- Σχεδιασμός αντιμετώπισης περιστατικών ασφάλειας
- Σχεδιασμός αντιμετώπισης καταστροφικών συμβάντων
- Σχεδιασμός της επιχειρησιακής συνέχειας του οργανισμού
- Πιθανές απειλές και κακόβουλη εκμετάλλευση των αδυναμιών ενός συστήματος
- Κατηγοριοποίηση και ανάλυση των επιθέσεων ενάντια στα συστήματα ενός τραπεζικού οργανισμού
- Διεθνή πρότυπα και βέλτιστες πρακτικές στον τομέα της ασφάλειας πληροφοριών (ISO 27000, BS 25999)
- Ενημέρωση και εκπαίδευση των εργαζομένων στις διαδικασίες ασφάλειας και στα πρότυπα συμμόρφωσης του οργανισμού
- Διαδικασίες αυτοαξιολόγησης της ασφάλειας και συμμόρφωσης στα πρότυπα του τραπεζικού οργανισμού
- Εξωτερικοί έλεγχοι της ασφάλειας των πληροφοριακών συστημάτων, των διαδικασιών και της συμμόρφωσης στα πρότυπα του οργανισμού
- Σύγχρονες τεχνικές μέθοδοι αντιμετώπισης κινδύνων (μηχανισμοί περιορισμένης και ελεγχόμενης πρόσβασης (extranet) στα πληροφοριακά συστήματα του οργανισμού, τείχη προστασίας (firewalls), συστήματα ανίχνευσης (intrusion detection) και αποτροπής εισβολών (intrusion prevention)
- Το πρότυπο συμμόρφωσης PCI (Payment Card Industry)

ΑΣΦΑΛΕΙΑ ΠΛΗΡΟΦΟΡΙΑΚΩΝ ΣΥΣΤΗΜΑΤΩΝ

Η εκπαιδευτική διαδικασία συνιστά σχέση αμφίδρομης ουσιαστικής επικοινωνίας εκπαιδευτή και συμμετεχόντων. Η αποτελεσματικότητα της επικοινωνίας αυτής καθορίζεται σε μεγάλο βαθμό από το σχετικό με το σεμινάριο υπόβαθρο, τις ανάγκες και τις προσδοκίες των συμμετεχόντων.

Συγκεκριμένα, ζητήματα όπως η εργασιακή εμπειρία, το εκπαιδευτικό υπόβαθρο και τα ειδικότερα οφέλη που προσδοκούν οι συμμετέχοντες να αποκομίσουν από το εκπαιδευτικό πρόγραμμα συνιστούν καθοριστικούς παράγοντες, που πρέπει να συνεκτιμώνται για την αποτελεσματική προσαρμογή της μεθοδολογίας που θα χρησιμοποιήσει ο εισηγητής.

Τα παρακάτω στοιχεία είναι απολύτως εμπιστευτικά και θα χρησιμοποιηθούν μόνο από το ETI. Οι πληροφορίες αυτές θα βοηθήσουν τον εισηγητή να διαμορφώσει το κατάλληλο εκπαιδευτικό «μείγμα» που θα μεγιστοποιήσει το δικό σας όφελος.

ΠΡΟΦΙΛ ΕΚΠΑΙΔΕΥΟΜΕΝΟΥ	
Ονοματεπώνυμο:	Τράπεζα/εταιρεία:
	Μονάδα:
Σημερινά επαγγελματικά καθήκοντα (σύντομη περιγραφή):	
Χρόνια προϋπηρεσίας: Προηγούμενες θέσεις εργασίας (εντός ή εκτός τραπεζικού χώρου):	
Σπουδές – ειδικότητες:	
Θέματα σχετικά με το πρόγραμμα που γνωρίζετε με οποιονδήποτε τρόπο (π.χ. εμπειρία, εκπαίδευση, αναγνωστικά ενδιαφέροντα):	
Εκπαιδευτικά προγράμματα που έχετε παρακολουθήσει για το ίδιο ή παρεμφερές θέμα:	
Θεματικές ενότητες στις οποίες θα επιθυμούσατε να δώσει μεγαλύτερη έμφαση ο εισηγητής:	

**Παρακαλούμε στείλτε το συμπληρωμένο ερωτηματολόγιο μέχρι τις 16/2/2012
στο e-mail: ntassakos@hba.gr ή στο fax: 210-3646122**

Ευχαριστούμε για τη συμβολή σας στην αρτιότερη προετοιμασία του προγράμματος.

Τομέας Επικοινωνίας ETI