Αναλυτική Περιγραφή

Το πρόγραμμα κατάρτισης προσφέρει τόσο θεωρητικές όσο και εφαρμοσμένες γνώσεις αναφορικά με την εξασφάλιση των πληροφοριών, δηλαδή την προστασία των δεδομένων ως προς την εμπιστευτικότητα, την ακεραιότητα και τη διαθεσιμότητά τους. Μέσα από το συγκεκριμένο πρόγραμμα αναλύεται η σωστή λειτουργία των υπολογιστικών συστημάτων και εφαρμογών, δηλαδή την προστασία από μη εξουσιοδοτημένες ενέργειες όπως αλλαγή δικαιωμάτων πρόσβασης, κακόβουλη εκτέλεση εντολών, τροποποίηση της διάρθρωσης του συστήματος, κακόβουλη ή λανθασμένη χρήση, διακοπή λειτουργίας, καθώς και τη φυσική προστασία των υπολογιστικών συστημάτων. Τέλος δίνεται έμφαση στην εύρυθμη λειτουργία των δικτύων και των υποδομών, δηλαδή την προστασία από μη εξουσιοδοτημένη λογική πρόσβαση σε ένα δίκτυο, παράκαμψη ή τροποποίηση των κανόνων δρομολόγησης στο δίκτυο, παρακολούθηση του μέσου επικοινωνίας, διακοπή της επικοινωνίας, φυσική προστασία των υποδομών επικοινωνίας κτλ.

Η ασφάλεια των πληροφοριών είναι ένα από τα πιο καυτά θέματα συζήτησης στην πληροφορική τα τελευταία χρόνια. Ο αυξανόμενος αριθμός επιθέσεων από εισβολείς και ιούς, καθώς και οι ιστορίες υψηλής προβολής με δεδομένα που έχουν υποστεί παραβίαση, έχουν προσελκύσει μεγάλη προσοχή στον κόσμο της τεχνολογίας πληροφοριών.

Τα στελέχη συχνά δεν κατανοούν σε βάθος την ασφάλεια των πληροφοριών, τους κινδύνους και τις τρέχουσες απειλές. Συνήθως έχουν μια ιδέα για δύο ή τρεις απειλές που τους απασχολούν γενικά σε προσωπικό επίπεδο και συχνά δεν θέλουν να εμβαθύνουν στις ιδιαιτερότητες του IT. Όταν εγκρίνουν τον προϋπολογισμό τους, είναι σημαντικό γι' αυτούς οι επενδύσεις σε νέο λογισμικό να είναι βέλτιστες από πλευράς κόστους και να έχουν θετικό αντίκτυπο στην επιχείρησή τους.

Μια συζήτηση με τους υπεύθυνους για την ασφάλεια των πληροφοριών έχει τα δικά της μοναδικά χαρακτηριστικά. Οι άνθρωποι συνήθως δεν δίνουν σημασία στην ασφάλεια εφόσον "όλα είναι εντάξει". Οι εταιρείες που έχουν βιώσει σημαντική απώλεια δεδομένων λόγω ιών κρυπτογράφησης δίνουν σημαντικά μεγαλύτερη προσοχή στην ασφάλεια από εκείνες που δεν έχουν αντιμετωπίσει ακόμη προβλήματα. Από την άλλη πλευρά, 100% ασφάλεια δεν υφίσταται. Όσο ένα σύστημα λειτουργεί, εκτίθεται σε κινδύνους. Καθήκον μας είναι να καταδείξουμε την ύπαρξη κινδύνων και να τους μειώσουμε σε αποδεκτό επίπεδο. Επειδή η μείωση του κινδύνου βασίζεται στην αγορά προϊόντων λογισμικού, είναι σημαντικό να βρεθεί η ισορροπία όπου είναι πιο επικερδές να πληρώνεις για την ασφάλεια από το να πληρώνεις για την απουσία της

Οι παραπάνω συνθήκες δημιουργούν νέες απαιτήσεις από τις επιχειρήσεις που δραστηριοποιούνται μέσα σε αυτό το περιβάλλον για υιοθέτηση νέων δεξιοτήτων από τη μεριά των εργαζομένων.

Αρχικά επιχειρείται μια παρουσίαση των βασικών εννοιών της Ασφάλειας Πληροφοριών και Συστημάτων Πληροφορικής. Επιπλέον, αναλύουμε τις βασικές έννοιες που απαιτείται να γνωρίζει ο αναγνώστης προκειμένου να κατανοήσει την ύλη του υπόλοιπου τεύχους, όπως η έννοια της πληροφορίας και του πληροφοριακού συστήματος και παρουσιάζουμε τα τεχνολογικά μέρη που το συνθέτουν και τις προκλήσεις που αντιμετωπίζει η ανάπτυξη και η λειτουργία των πληροφοριακών συστημάτων.

Μέσα από ειδικό κεφάλαιο παρουσιάζονται οι πιθανοί κίνδυνοι ασφαλείας που μπορεί να παρουσιαστούν στα συστήματα πληροφορικής. Η ενασχόληση με οποιαδήποτε επιστημονική περιοχή απαιτεί την κατανόηση των βασικών εννοιών της περιοχής. Για να συμβεί αυτό, απαιτείται η καθιέρωση ενός επαρκώς αποδεκτού συνόλου όρων, που θα μας επιτρέψει την αποτελεσματική και σαφή επικοινωνία. Σκοπός του κεφαλαίου αυτού είναι να ξεκαθαρίσει βασικές έννοιές σχετικές με το αντικείμενο μμελέτης μας δίνοντας αυστηρούς (πια) ορισμούς.

Οι επόμενες ενότητες είναι αφιερωμένες σε υποκείμενα και αντικείμενα, δύο έννοιες βασικές για τη συζήτηση στις επόμενες ενότητες, σε διαφορετικές πολιτικές ελέγχου προσπέλασης, στα φορμαλιστικά μμοντέλα περιγραφής πολιτικών ελέγχου προσπέλασης και στους διάφορους μμηχανισμούς υλοποίησης πολιτικών ελέγχου προσπέλασης. Το κεφάλαιο αυτό έχει ως στόχο επίσης να μας εισαγάγει στις βασικές έννοιες της Κρυπτογραφίας και, στη συνέχεια, να συζητήσουμε τους λόγους που καθιστούν αναγκαίες τις κρυπτογραφικές τεχνικές στην προστασία και ασφάλεια συστημάτων υπολογιστών.

Στην τελευταία ενότητα αναλύεται η Ασφάλεια Εφαρμογών, Συστημάτων & Δεδομένων. Η ραγδαία ανάπτυξη της τεχνολογίας έχει προκαλέσει τόσο θετικές όσο και αρνητικές επιπτώσεις. Με την ανάπτυξη της παραγωγικής διαδικασίας, εισάγονται νέα συστήματα και τεχνικές καθώς και ύλες που ναι μεν βοηθάνε στην ανάπτυξη της παραγωγής αλλά και της ποιότητας των παραγόμενων προϊόντων, αλλά από την άλλη μεριά αποτελεί μεγαλύτερο κίνδυνο όσον αφορά την υγεία και ασφάλεια των εργαζομένων. Για τον λόγο αυτό, η προστασία των εργαζομένων κατά την εργασία αποτελεί ένα βασικό λόγο αναθεώρησης των ήδη υπάρχοντών μέτρων στην επιχείρηση, καθώς οι εργαζόμενοι αποτελούν έναν από τους βασικότερους παράγοντες μέσα στην μονάδα. Μια ολοκληρωμένη εκτίμηση επαγγελματικού κινδύνου στην επιχείρηση, καθώς και ένα πλήρες σχέδιο ορθής διαχείρισης και αντιμετώπισης των κινδύνων αυτών, είναι αναγκαία σε μια επιχείρηση η οποία εκτός από την επιτυχία στην παραγωγή αλλά και στις πωλήσεις στοχεύει στη

δημιουργία καλής εικόνας τόσο στο εσωτερικό όσο και στο εξωτερικό περιβάλλον. Η μελέτη όλων των εν δυνάμει κινδύνων αποτελεί μια δύσκολη και χρονοβόρα διαδικασία καθώς πρέπει να μελετηθεί κάθε στοιχείο που μπορεί να αποτελέσει κίνδυνο για τους εργαζομένους.