

Περιεχόμενα

Πρόλογος	15
ΚΕΦΑΛΑΙΟ 1: Εισαγωγή	19
1.1. Το πρόβλημα της ασφάλειας πληροφοριών	20
1.2. Η οικονομική σημασία της πληροφορίας	28
1.3. Η κοινωνική σημασία της πληροφορίας	32
1.4. Ένα πλαίσιο για την προστασία των πληροφοριών	34
1.5. Πρότυπα και προτυποποίηση, πιστοποίηση, διαπίστευση	39
1.6. Πληροφορίες ή δεδομένα;	41
1.7. Εννοιολογική θεμελίωση	43
Βιβλιογραφία	47
ΚΕΦΑΛΑΙΟ 2: Συστήματα διαχείρισης της ασφάλειας πληροφοριών	49
2.1. Συστήματα διαχείρισης της ασφάλειας πληροφοριών	51
2.2. Η σειρά προτύπων ISO27k	53
2.3. Το πρότυπο ISO 27001	61
2.4. Πώς αναπτύσσεται ένα ΣΔΑΠ	67
Βιβλιογραφία	89
ΚΕΦΑΛΑΙΟ 3: Ανάλυση, εκτίμηση και διαχείριση κινδύνων	93
3.1. Η έννοια του κινδύνου	95
3.2. Πώς εκφράζουμε και πώς μετράμε τον κίνδυνο	96
3.3. Η μεθοδολογία διαχείρισης κινδύνων	102
3.4. Μέθοδοι διαχείρισης κινδύνων	119

3.5. Πρότυπα για τη διαχείριση κινδύνου	129
Βιβλιογραφία	133
ΚΕΦΑΛΑΙΟ 4: Οργανωσιακό πλαίσιο ασφάλειας πληροφοριών ...	137
4.1. Το οργανωσιακό πλαίσιο ασφάλειας πληροφοριών	138
4.2. Οι πολιτικές ασφάλειας	141
4.3. Τα άλλα στοιχεία του πλαισίου	146
4.4. Τα επιθυμητά χαρακτηριστικά μιας πολιτικής ασφάλειας	147
4.5. Ο κύκλος ζωής μιας πολιτικής ασφάλειας	148
Βιβλιογραφία	154
ΚΕΦΑΛΑΙΟ 5: Επιχειρησιακή συνέχεια	155
5.1. Βασικές έννοιες	157
5.2. Η ανάγκη για επιχειρησιακή συνέχεια	158
5.3. Σχεδιασμός επιχειρησιακής συνέχειας	161
Βιβλιογραφία	166
ΚΕΦΑΛΑΙΟ 6: Διαχείριση περιστατικών ασφάλειας	167
6.1. Σκοπός και στόχοι της διεργασίας διαχείρισης περιστατικών	168
6.2. Παραδείγματα περιστατικών και των αιτιών τους	169
6.3. Η ομάδα αντιμετώπισης περιστατικών	173
6.4. Οι φάσεις της διεργασίας αντιμετώπισης περιστατικών	176
Βιβλιογραφία	188
ΚΕΦΑΛΑΙΟ 7: Ανάκαμψη από καταστροφή	189
7.1. Η διεργασία σχεδιασμού ανάκαμψης από καταστροφή	190
7.2. Δήλωση πολιτικής	192
7.3. Ανάλυση επιχειρησιακών επιπτώσεων	192
7.4. Εντοπισμός προληπτικών μέτρων ασφάλειας	197
7.5. Επιλογή στρατηγικών ανάκαμψης	198
7.6. Ανάπτυξη σχεδίου ανάκαμψης	205
7.7. Δοκιμές και εκπαίδευση	214
7.8. Συντήρηση και επικαιροποίηση του σχεδίου	216
7.9. Ο οικονομικός παράγοντας	217
Βιβλιογραφία	220

ΚΕΦΑΛΑΙΟ 8: Η μέτρηση της ασφάλειας	223
8.1. Μετρήσεις και μετρικές	225
8.2. Η διεργασία μέτρησης της ασφάλειας	227
8.3. Ανάπτυξη μετρικών και μετρήσεων	228
8.4. Διενέργεια των μετρήσεων	241
8.5. Ανάλυση δεδομένων και παρουσίαση των αποτελεσμάτων των μετρήσεων	242
8.6. Αξιολόγηση και βελτίωση της διεργασίας μέτρησης της ασφάλειας	243
Βιβλιογραφία	244
 ΚΕΦΑΛΑΙΟ 9: Έλεγχος του ΣΔΑΠ	247
9.1. Αρχές της ελεγκτικής	249
9.2. Η ελεγκτική και το ΣΔΑΠ	250
9.3. Η διεργασία διαχείρισης του προγράμματος ελέγχων	252
9.4. Η διεργασία διεξαγωγής του ελέγχου	258
9.5. Η διεξαγωγή του ελέγχου	263
Βιβλιογραφία	266

Πρόλογος

Διδάσκω το μάθημα «Πολιτικές και διαχείριση ασφάλειας» στους φοιτητές του πέμπτου εξαμήνου σπουδών του Τμήματος Ψηφιακών Συστημάτων του Πανεπιστημίου Πειραιώς εδώ και οκτώ χρόνια. Αποφάσισα, ομολογουμένως με καθυστέρηση, να γράψω το βιβλίο αυτό αφενός –και κυρίως– για να υποστηρίξω τη διδασκαλία αυτού του μαθήματος και αφετέρου επειδή η υπάρχουσα ελληνική βιβλιογραφία σε θέματα ασφάλειας πληροφοριών αναφέρεται αποκλειστικά σε τεχνικά θέματα. Όμως, σύμφωνα και με τη φράση του Bruce Schneier που έβαλα ως προμετωπίδα, η ασφάλεια πληροφοριών δεν είναι τεχνικό θέμα. Θεώρησα λοιπόν χρήσιμο να αναδείξω τις μη τεχνικές διαστάσεις της.

Το βιβλίο είναι δομημένο σε εννέα κεφάλαια. Το πρώτο, όπως συμβαίνει με σχεδόν κάθε βιβλίο που προορίζεται για να υποστηρίξει την εκπαιδευτική διαδικασία, είναι εισαγωγικό. Το δεύτερο κεφάλαιο αναφέρεται στο βασικό θέμα του βιβλίου: στα Συστήματα Διαχείρισης της Ασφάλειας Πληροφοριών. Το τρίτο κεφάλαιο είναι αφιερωμένο σε ένα κεντρικό μέρος της όλης διεργασίας διαχείρισης της ασφάλειας πληροφοριών, την ανάλυση και διαχείριση κινδύνων. Το τέταρτο κεφάλαιο αναφέρεται στο πώς οργανώνεται το πλαίσιο της ασφάλειας πληροφοριών μέσα σε έναν οργανισμό. Στο σημείο αυτό αλλάζουμε λίγο σκοπιά: από εκεί που συζητούσαμε πώς προληπτικά θα μπορέσουμε να προστατεύσουμε τις πληροφορίες, θεωρούμε πλέον ότι οι προσπάθειές μας κάπως αστόχησαν και, επομένως, στόχος μας πλέον είναι να ελαχιστοποιήσουμε τις επιπτώσεις της αστοχίας. Έτσι, στο πέμπτο κεφάλαιο συζητάμε θέματα επιχειρησιακής συνέχειας, στο έκτο τη διαχείριση περιστατικών ασφάλειας και στο έβδομο τους τρόπους ανάκαμψης από καταστροφή. Στο

όγδοο κεφάλαιο ασχολούμαστε με το πώς μπορούμε να μετρήσουμε την ασφάλεια και, τέλος, στο ένατο κεφάλαιο πώς γίνεται ο έλεγχος και η πιστοποίηση ενός Συστήματος Διαχείρισης της Ασφάλειας Πληροφοριών.

Το αντικείμενο της Διαχείρισης Ασφάλειας Πληροφοριών δεν εξαντλείται με τα παραπάνω. Άφησα έξω από τη συζήτηση θέματα που σχετίζονται με τη νομοθεσία, με τα οικονομικά της ασφάλειας και με τη διακυβέρνηση της ασφάλειας. Ο βασικός λόγος αυτής της επιλογής πρέπει να αναζητηθεί στον κύριο στόχο αυτού του βιβλίου, που είναι να υποστηρίξει την εκπαιδευτική διαδικασία στην τριτοβάθμια εκπαίδευση στην Ελλάδα, στο αντικείμενο της ασφάλειας πληροφοριών. Το αντικείμενο αυτό εμπεριέχεται στα προγράμματα σπουδών σχεδόν όλων των τμημάτων πανεπιστημίων και ΤΕΙ που θεραπεύουν, με τον ένα ή τον άλλο τρόπο, την επιστήμη της πληροφορικής. Το πρόβλημα είναι ότι ελάχιστα από τα αντίστοιχα προγράμματα σπουδών εκθέτουν τους φοιτητές σε μη τεχνικά θέματα που άπτονται του πεδίου των επιστημών διοίκησης. Έτσι, λίγοι φοιτητές –και μελλοντικοί μηχανικοί ή επιστήμονες πληροφορικής– έχουν την ευκαιρία να αντιληφθούν τη στενή σχέση που (πρέπει να) υπάρχει μεταξύ τεχνολογίας και διοίκησης. Οι περισσότεροι, αν και μπορεί να είναι εξαιρετικά καταρτισμένοι σε τεχνικά θέματα, αποφεύγουν την ενασχόληση με αντικείμενα διοίκησης, που τα θεωρούν συνήθως «θεωρητικά» και, ως εκ τούτου, βαρετά και ενδεχομένως λιγότερο χρήσιμα. Το περιεχόμενο του βιβλίου αυτού έχει ήδη αρκετή απόσταση από την τεχνολογία: φανταστείτε να συμπεριλάμβανα και νομικά, οικονομικά και αμιγώς διοικητικά θέματα, όπως αυτά που συνειδητά παρέλειψα! Υπάρχει βέβαια και ένας δεύτερος λόγος: η διάρκεια του διδακτικού εξαμήνου. Εξηγούμαι: Τα συγκεκριμένα περιεχόμενα είναι δυνατόν (αν και δύσκολο) να καλυφθούν διδακτικά σε δεκατρείς τρίωρες εβδομαδιαίες διαλέξεις, όσο δηλαδή, θεωρητικά τουλάχιστον, διαρκεί ένα ακαδημαϊκό εξάμηνο στα ελληνικά ΑΕΙ.

Πριν σας παραδώσω το κείμενο, θέλω να ευχαριστήσω όλους όσοι συνέβαλαν στην προσπάθειά μου αυτή. Είναι δύσκολο να τους αναφέρω όλους ονομαστικά, γιατί η συγγραφή ενός βιβλίου έρχεται ως αποτέλεσμα μιας μακρόχρονης διαδικασίας διαμόρφωσης της γνώσης μου, της σκέψης μου αλλά και της γενικότερης προσωπικότητάς μου, διαδικασίας στην οποία έχουν συντελέσει –άλλος πολύ, άλλος λιγότερο– πάρα πολλοί: δάσκαλοί μου, συνάδελφοί μου και μαθητές μου. Τους ευχαριστώ, λοιπόν, όλους αυτούς. Ιδιαίτερες ευχαριστίες όμως οφείλω να απευθύνω στη συ-

νεργάτιδα και μαθήτριά μου, υποψήφια διδάκτορα του Τμήματος Ψηφιακών Συστημάτων, Ελένη Δάρρα, που ανέλαβε να μετατρέψει τις μουτζούρες που της έδωσα σε σχήματα για το βιβλίο. Τη γυναίκα μου, που ανέχεται τη μακρόχρονη ενασχόλησή μου με την επιστήμη σε βάρος του χρόνου που αφιερώνω σ' εκείνη και στα παιδιά μας, την ευχαριστώ κάθε μέρα –κι ας μην το ξέρει. Τον καλό μου φίλο και συνάδελφο Στέφανο Γκρίτζαλη, Καθηγητή και επί του παρόντος Πρύτανη του Πανεπιστημίου Αιγαίου, τον ευχαριστώ για τον εντοπισμό και διάθεση σε μένα βιβλιογραφίας απαραίτητης για την ολοκλήρωση του βιβλίου.

Με την ελπίδα ότι θα θελήσετε να μου γνωστοποιήσετε την όποια κριτική σας –θετική ή αρνητική, δεν έχει σημασία, αρκεί να είναι καλόπιστη– εύχομαι να κατάφερα να προσφέρω κάτι χρήσιμο στους φοιτητές μου και στους συναδέλφους μου.

Σωκράτης Κ. Κάτσικας
Αθήνα, Σεπτέμβρης 2014