ΕΛΛΗΝΙΚΗ ΔΗΜΟΚΡΑΤΙΑ
ΥΠΟΥΡΓΕΙΟ ΑΝΑΠΤΥΞΗΣ
ΓΕΝΙΚΗ ΓΡΑΜΜΑΤΕΙΑ ΒΙΟΜΗΧΑΝΙΑΣ

ΥΠΟΥΡΓΕΙΟ ΟΙΚΟΝΟΜΙΑΣ & ΟΙΚΟΝΟΜΙΚΩΝ
ΥΠΟΥΡΓΕΙΟ ΕΣΩΤΕΡΙΚΩΝ, ΔΗΜΟΣΙΑΣ ΔΙΟΙΚΗΣΗΣ & ΑΠΟΚΕΝΤΡΩΣΗΣ
ΕΠΙΧΕΙΡΗΣΙΑΚΟ ΠΡΟΓΡΑΜΜΑ
"ΚΟΙΝΩΝΙΑ ΤΗΣ ΠΛΗΡΟΦΟΡΙΑΣ"

ΕΥΡΩΠΑΪΚΗ ΕΝΩΣΗ
ΕΥΡΩΠΑΪΚΟ ΤΑΜΕΙΟ
ΠΕΡΙΦΕΡΕΙΑΚΗΣ ΑΝΑΠΤΥΞΗΣ

GRNET
ΕΔΕΤ

ebusinessforum

Β κύκλος εργασιών
Ομάδα Εργασίας ΟΕ Β1

«ΑΣΦΑΛΕΙΑ ΠΛΗΡΟΦΟΡΙΑΚΩΝ & ΕΠΙΚΟΙΝΩΝΙΑΚΩΝ ΣΥΣΤΗΜΑΤΩΝ ΣΤΟ ΧΩΡΟ ΤΟΥ ΗΛΕΚΤΡΟΝΙΚΟΥ ΕΠΙΧΕΙΡΕΙΝ»

Συντονιστές: **Σωκράτης Κ. Κάτσικας, Αντιπρύτανης Πανεπιστημίου Αιγαίου**
Λίλιαν Μήτρου, Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα

Raporteur: **Στέφανος Γκρίτζαλης, Επίκουρος Καθηγητής Πανεπιστημίου Αιγαίου,**
Τμήμα Μηχανικών Πληροφοριακών & Επικοινωνιακών Συστημάτων

Αθήνα, Ιούλιος 2002

Ακολουθητέα Πρακτική

για αποτελεσματική Διαχείριση Ασφάλειας Πληροφοριών

(ISO 17799 Code of Practice for information security management)

Πίνακας Περιεχομένων

Περίληψη *7*

0. Εισαγωγή *8*

0.1 Τι είναι η Ασφάλεια Πληροφοριών; **8**

0.2 Σε τι χρειάζεται η Ασφάλεια Πληροφοριών **9**

0.3 Καταγραφή απαιτήσεων ασφάλειας **9**

0.4 Αποτίμηση κινδύνων ασφάλειας **10**

0.5 Επιλογή μηχανισμών **11**

0.6 Βασικοί μηχανισμοί ασφάλειας **12**

0.7 Βασικοί παράγοντες επιτυχίας **13**

1. Σκοπός *14*

2. Ορολογία *15*

2.1 Ασφάλεια πληροφοριών (Information Security) **15**

2.2 Αποτίμηση κινδύνου (Risk Assessment) **15**

2.3 Διαχείριση κινδύνου (Risk Management) **15**

3. Πολιτική ασφάλειας (Security Policy) *16*

3.1 Πολιτική ασφάλειας πληροφοριών **16**

3.1.1 Κείμενο της πολιτικής ασφάλειας 16

3.1.2 Έλεγχος και αξιολόγηση 17

4. Ασφάλεια του οργανισμού *18*

4.1 Υποδομή ασφάλειας πληροφοριών **18**

4.1.1 Ομάδα διαχείρισης της ασφάλειας 18

4.1.2 Συντονισμός ασφάλειας πληροφοριών 19

4.1.3 Καθορισμός καθηκόντων 19

4.1.4 Εξουσιοδότηση στις εγκαταστάσεις επεξεργασίας των πληροφοριών 20

4.1.5 Συνδρομή ειδικών εμπειρογνωμόνων 21

4.1.6 Συνεργασία ανάμεσα σε οργανισμούς 21

4.1.7 Ανεξάρτητος έλεγχος της ασφάλειας 22

4.2 Ασφάλεια προσπέλασης τρίτων μερών **22**

4.2.1 Καθορισμός των κινδύνων από την προσπέλαση τρίτων 23

4.2.2 Απαιτήσεις ασφάλειας σε συμβάσεις με τρίτους 24

4.3 Outsourcing **25**

4.3.1 Απαιτήσεις ασφάλειας σε συμβάσεις outsourcing 26

5. Ταξινόμηση πόρων και έλεγχος *27*

5.1 Υπευθυνότητα για πόρους **27**

5.1.1 Καταγραφή των πόρων 27

5.2 Κατηγοριοποίηση πληροφοριών **28**

5.2.1 Γενικές οδηγίες κατηγοριοποίησης 28

5.2.2 Χαρακτηρισμός και χειρισμός των πληροφοριών 29

6. Ασφάλεια προσωπικού *30*

6.1 Η ασφάλεια στα εργασιακά καθήκοντα **30**

6.1.1 Ευθύνες σχετικές με την ασφάλεια 30

6.1.2 Έλεγχος προσωπικού 30
6.1.3 Συμφωνίες τήρησης της εχεμύθειας 31
6.1.4 Όροι πρόσληψης και κανονισμοί εργασίας 32

6.2 Εκπαίδευση χρηστών 32
6.2.1 Εκπαίδευση στην ασφάλεια πληροφοριακών συστημάτων 32

6.3 Αντιμετώπιση περιστατικών 33
6.3.1 Αναφορά συμβάντων 33
6.3.2 Αναφορά αδυναμιών ασφάλειας 33
6.3.3 Αναφορά δυσλειτουργιών των εφαρμογών 34
6.3.4 Μαθαίνοντας από συμβάντα 34
6.3.5 Πειθαρχικές διαδικασίες 35

7. Φυσική και περιβαλλοντολογική ασφάλεια 36

7.1 Ασφαλείς περιοχές 36
7.1.1 Περίμετρος φυσικής ασφάλειας 36
7.1.2 Έλεγχος εισόδου 37
7.1.3 Ασφάλεια γραφείων, δωματίων και εγκαταστάσεων 38
7.1.4 Εργασία σε ασφαλείς περιοχές 39
7.1.5 Απομονωμένες περιοχές φορτοεκφόρτωσης 39

7.2 Ασφάλεια εξοπλισμού 40
7.2.1 Τοποθέτηση και προστασία εξοπλισμού 40
7.2.2 Παροχή ρεύματος 41
7.2.3 Ασφάλεια καλωδίωσης 42
7.2.4 Συντήρηση εξοπλισμού 42
7.2.5 Ασφάλεια εξοπλισμού εκτός των χώρων του οργανισμού 43
7.2.6 Ασφαλής καταστροφή ή επαναχρησιμοποίηση εξοπλισμού 44

7.3 Γενικοί μηχανισμοί προστασίας 44
7.3.1 Πολιτική προστασίας πληροφοριών στο γραφείο 44
7.3.2 Απομάκρυνση εξοπλισμού 45

8. Λειτουργίες του οργανισμού και επικοινωνίες 46

8.1 Διαδικασίες λειτουργίας και καθήκοντα 46
8.1.1 Καταγραφή διαδικασιών λειτουργίας 46
8.1.2 Έλεγχος αλλαγών 47
8.1.3 Διαδικασίες αντιμετώπισης συμβάντων 47
8.1.4 Διαχωρισμός καθηκόντων 48
8.1.5 Διαχωρισμός των εγκαταστάσεων δοκιμών και λειτουργιών 49
8.1.6 Διαχείριση από εξωτερικούς συνεργάτες 50

8.2 Σχεδιασμός και αποδοχή συστήματος 51
8.2.1 Σχεδιασμός χωρητικότητας 51
8.2.2 Αποδοχή συστήματος 51

8.3 Προστασία απέναντι σε κακόβουλο λογισμικό 52
8.3.1 Μηχανισμοί προστασίας 53

8.4 Καθημερινή λειτουργία 54
8.4.1 Εφεδρικό αντίγραφο ασφαλείας του συστήματος 54
8.4.2 Τήρηση αρχείων συστήματος 55
8.4.3 Καταγραφή σφαλμάτων 55

8.5 Διαχείριση δικτύου 56
8.5.1 Προστασία δικτύου 56

8.6 Διαχείριση αποθηκευτικών μέσων 57
8.6.1 Διαχείριση αποθηκευτικών μέσων που μπορεί να διαγραφεί το περιεχόμενο τους 57
8.6.2 Απόσυρση αποθηκευτικών μέσων 58
8.6.3 Χειρισμός πληροφοριών 59
8.6.4 Ασφάλεια των εγχειριδίων του συστήματος 59

8.7 Ανταλλαγή πληροφοριών και εφαρμογών 60
8.7.1 Συμφωνίες ανταλλαγής πληροφοριών και λογισμικού 60
8.7.2 Ασφάλεια των αποθηκευτικών μέσων κατά τη μεταφορά 61
8.7.3 Ασφάλεια ηλεκτρονικού εμπορίου 62
8.7.4 Ασφάλεια του ηλεκτρονικού ταχυδρομείου 64
8.7.5 Ασφάλεια των ηλεκτρονικών συστημάτων γραφείου 65
8.7.6 Δημόσια συστήματα 66
8.7.7 Άλλες μορφές ανταλλαγής πληροφοριών 67

9. Έλεγχος πρόσβασης (access control) 68

9.1 Επιχειρησιακές απαιτήσεις 68
9.1.1 Πολιτική ελέγχου πρόσβασης 68

9.2 Διαχείριση της πρόσβασης των χρηστών 69
9.2.1 Δήλωση χρηστών 70
9.2.2 Διαχείριση προνομιακών δικαιωμάτων 71
9.2.3 Διαχείριση συνθηματικών (password) 71
9.2.4 Έλεγχος δικαιωμάτων χρηστών 72

9.3 Ευθύνες χρηστών 73
9.3.1 Χρήση Συνθηματικών 73
9.3.2 Εξοπλισμός χωρίς επίβλεψη 74

9.4 Έλεγχος πρόσβασης δικτύου (network access control) 74
9.4.1 Πολιτική χρήσης των δικτυακών υπηρεσιών 75
9.4.2 Υποχρεωτικοί δίαυλοι επικοινωνίας 76
9.4.3 Αυθεντικοποίηση χρηστών για εξωτερικές συνδέσεις 77
9.4.4 Αυθεντικοποίηση κόμβων του δικτύου 77
9.4.5 Προστασία απομακρυσμένων διαγνωστικών θυρών 77
9.4.6 Διαχωρισμός στα δίκτυα 78
9.4.7 Έλεγχος δικτυακών συνδέσεων 78
9.4.8 Έλεγχος της δρομολόγησης (routing) 79
9.4.9 Ασφάλεια δικτυακών υπηρεσιών 79

9.5 Έλεγχος πρόσβασης στο λειτουργικό σύστημα 80
9.5.1 Αναγνώριση τερματικών 80
9.5.2 Διαδικασίες σύνδεσης στο σύστημα 81
9.5.3 Αυθεντικοποίηση χρηστών 82
9.5.4 Διαχείριση συνθηματικών 82
9.5.5 Χρήση εργαλείων συστήματος 83
9.5.6 Συναγερμός απειλής για την προστασία των χρηστών 84
9.5.7 Time-out τερματικών 84
9.5.8 Περιορισμός χρόνου σύνδεσης 85

9.6 Έλεγχος της πρόσβασης στις εφαρμογές 85
9.6.1 Περιορισμοί πρόσβασης στις πληροφορίες 86
9.6.2 Απομόνωση ευαίσθητων συστημάτων 87

9.7 Παρακολούθηση προσπέλασης και χρήσης συστήματος 87
9.7.1 Καταγραφή γεγονότων 87
9.7.2 Καταγραφή της χρήσης του συστήματος 89
9.7.3 Συγχρονισμός των συστημάτων 91

9.8 Τηλεεργασία και κινητή υπολογιστική 91
9.8.1 Κινητή υπολογιστική 91
9.8.2 Τηλεεργασία 92

10. Ανάπτυξη και συντήρηση συστημάτων 94

10.1 Απαιτήσεις ασφάλειας των συστημάτων 94
10.1.1 Ανάλυση απαιτήσεων ασφάλειας και προδιαγραφές 94

10.2 Ασφάλεια εφαρμογών 94

10.2.1 Έλεγχος εγκυρότητας δεδομένων 95
10.2.2 Έλεγχος της επεξεργασίας των δεδομένων 95
10.2.3 Αυθεντικοποίηση μηνυμάτων 97
10.2.4 Έλεγχος αποτελεσμάτων της επεξεργασίας 97

10.3 Μηχανισμοί κρυπτογραφίας 98
10.3.1 Πολιτική χρήσης κρυπτογραφίας 98
10.3.2 Κρυπτογραφία 98
10.3.3 Ψηφιακές υπογραφές 99
10.3.4 Υπηρεσίες μη αποποίησης 100
10.3.5 Διαχείριση κλειδιών 100

10.4 Ασφάλεια αρχείων συστήματος 103
10.4.1 Έλεγχος των εφαρμογών που λειτουργούν σε παραγωγή 103
10.4.2 Προστασία συστημάτων δοκιμών 104
10.4.3 Έλεγχος της πρόσβασης στον κώδικα των εφαρμογών 105

10.5 Ασφάλεια κατά την ανάπτυξη και την υποστήριξη των εφαρμογών 106
10.5.1 Διαδικασίες ελέγχου αλλαγών 106
10.5.2 Αναβαθμίσεις του λειτουργικού συστήματος 107
10.5.3 Περιορισμοί στη διενέργεια αλλαγών 108
10.5.4 Συγκαλυμμένα κανάλια επικοινωνίας και δούρειοι ίπποι 108
10.5.5 Outsourcing της ανάπτυξης εφαρμογών 109

11. Διαχείριση επιχειρησιακής συνέχειας 109

11.1 Παράμετροι της διαχείρισης της επιχειρησιακής συνέχειας 109
11.1.1 Διαδικασία διαχείρισης της επιχειρησιακής συνέχειας 110
11.1.2 Καθορισμός επιπτώσεων 111
11.1.3 Συγγραφή και υλοποίηση του σχεδίου επιχειρησιακής συνέχειας 111
11.1.4 Πλαίσιο σχεδιασμού 112
11.1.5 Δοκιμή, ενημέρωση και επανέλεγχος του σχεδίου 113

12. Έλεγχος συμμόρφωσης 116

12.1 Συμμόρφωση με τη σχετική νομοθεσία 116
12.1.1 Καθορισμός της σχετικής νομοθεσίας 116
12.1.2 Πνευματική ιδιοκτησία 116
12.1.3 Προστασία των αρχείων του οργανισμού 117
12.1.4 Προστασία δεδομένων και προστασία πληροφοριών προσωπικού χαρακτήρα 118
12.1.5 Πρόληψη κατάχρησης του πληροφοριακού συστήματος 119
12.1.6 Κανονισμοί χρήσης κρυπτογραφίας 120
12.1.7 Συλλογή αποδεικτικών στοιχείων 121

12.2 Έλεγχοι της πολιτικής ασφάλειας και τεχνική συμμόρφωση 122
12.2.1 Συμμόρφωση με την πολιτική ασφάλειας 122
12.2.2 Έλεγχος τεχνικής συμμόρφωσης 123

12.3 Ζητήματα ελέγχου συστημάτων 123
12.3.1 Μηχανισμοί ελέγχου συστημάτων 124
12.3.2 Προστασία εργαλείων ελέγχου συστημάτων 124

Βιβλιογραφικές Αναφορές 125

Περίληψη

Το παρόν κείμενο βασίζεται στο πρότυπο 17799 (2000.12.01) ISO/IEC (the International Organizational for Standardization / the International Electrotechnical Commission), το οποίο προετοιμάστηκε από το British Standards Institution (BS 7799) και υιοθετήθηκε από την Joint Technical Committee JTC 1 "Information Technology", παράλληλα με την αποδοχή του από εθνικές αρχές προτυποποίησης.

Αναφέρεται σε θέματα διαχείρισης ασφάλειας πληροφοριών (information security management) και έχει εφαρμογή και ιδιαίτερη σημασία στις απαιτούμενες δράσεις και ενέργειες επιχειρήσεων κάθε τύπου, οι οποίες δραστηριοποιούνται στο χώρο της ψηφιακής οικονομίας και του ηλεκτρονικού επιχειρείν.

Ιδιαίτερο ενδιαφέρον παρουσιάζει η δυνατότητα εφαρμογής του σε μικρές και μεσαίες επιχειρήσεις, αφού περιλαμβάνει, με πληρότητα, βασικούς κανόνες ακολουθητέας πρακτικής για επίτευξη αποτελεσματικής διαχείρισης της ασφάλειας των πληροφοριών, ανεξαρτήτως του τομέα δραστηριοποίησης της συγκεκριμένης επιχείρησης.

0. Εισαγωγή

0.1 Τι είναι η Ασφάλεια Πληροφοριών;

Η πληροφορία (information) είναι ένας πόρος, ένα περουσιακό στοιχείο, που όπως και όλα τα άλλα περιουσιακά στοιχεία έχει αξία για έναν οργανισμό και κατά συνέπεια χρειάζεται επαρκή προστασία. Η ασφάλεια των πληροφοριών (information security) τις προστατεύει από ένα σύνολο απειλών, ώστε να διασφαλίσει την επιχειρησιακή συνέχεια (business continuity), να ελαχιστοποιήσει τη ζημιά σε μια επιχείρηση και να μεγιστοποιήσει τις επιχειρηματικές ευκαιρίες και την απόδοση (return on investment – ROI).

Η πληροφορία μπορεί να εμφανιστεί υπό διάφορες μορφές. Μπορεί να γραφεί σε χαρτί, να αποθηκευθεί και να μεταδοθεί ηλεκτρονικά ή να αναφερθεί σε κάποια συζήτηση. Ασχέτως της μορφής ή του τρόπου αποθήκευσής της, η πληροφορία θα πρέπει πάντοτε να είναι επαρκώς προστατευμένη. Η ασφάλεια των πληροφοριών χαρακτηρίζεται ως η διαφύλαξη των ακόλουθων ιδιοτήτων - απαιτήσεων:

- Εμπιστευτικότητα (confidentiality): Διασφάλιση της προσπελασιμότητας της πληροφορίας μόνον από όσους έχουν τα απαραίτητα δικαιώματα.
- Ακεραιότητα (integrity): Διαφύλαξη της ακρίβειας και της πληρότητας της πληροφορίας και των μεθόδων επεξεργασίας αυτής.
- Διαθεσιμότητα (availability): Διασφάλιση της προσπελασιμότητας της πληροφορίας σε εξουσιοδοτημένους χρήστες όποτε απαιτείται.

Η ασφάλεια πληροφοριών επιτυγχάνεται με την υλοποίηση των κατάλληλων μηχανισμών ελέγχου, οι οποίοι μπορεί να είναι πολιτικές, πρακτικές, διαδικασίες, οργανωτικές δομές και λειτουργίες λογισμικού. Αυτοί οι μηχανισμοί ελέγχου είναι απαραίτητοι προκειμένου να διασφαλιστεί ότι ικανοποιούνται οι απαιτήσεις ασφάλειας του οργανισμού.

0.2 Σε τι χρειάζεται η Ασφάλεια Πληροφοριών

Οι πληροφορίες, καθώς και τα σχετικά συστήματα, δίκτυα και διαδικασίες αποτελούν σημαντικά περιουσιακά στοιχεία μιας επιχείρησης. Η εμπιστευτικότητα, η ακεραιότητα και η διαθεσιμότητα των πληροφοριών μπορούν να είναι ιδιαιτέρως σημαντικά για τη διατήρηση κάποιου ανταγωνιστικού πλεονεκτήματος, τη συμμόρφωση με τους νόμους, την εταιρική εικόνα, τα κέρδη και τα έσοδα μιας επιχείρησης.

Οι οργανισμοί και τα πληροφοριακά τους συστήματα συνεχώς αντιμετωπίζουν απειλές της ασφάλειας τους από ένα μεγάλο εύρος διαφορετικών πηγών, όπως ηλεκτρονική απάτη, βιομηχανική κατασκοπεία, βανδαλισμός, φυσικά φαινόμενα κλπ.. Επιπλέον, επιθέσεις με ιούς (viruses), hacking, cracking και επιθέσεις τύπου άρνησης παροχής υπηρεσιών (denial of service) έχουν πλέον γίνει συνήθεις και όλο πιο πολύπλοκες στην αντιμετώπισή τους. Καθώς οι επιχειρήσεις βασίζονται όλο και περισσότερο στα πληροφοριακά τους συστήματα, οι απειλές προς αυτά επηρεάζουν σημαντικά τις λειτουργίες των ίδιων των επιχειρήσεων. Η διασύνδεση ιδιωτικών και δημόσιων δικτύων και ο διαμοιρασμός πόρων δυσκολεύει ακόμη περισσότερο τον έλεγχο της πρόσβασης σε ένα σύστημα. Οι τάσεις επέκτασης κατανεμημένων περιβαλλόντων έχουν αποδυναμώσει την αποτελεσματικότητα του κεντρικού ελέγχου και διαχείρισης των συστημάτων.

Στην αρχική σχεδίαση πολλών πληροφοριακών συστημάτων δεν έχουν συμπεριληφθεί χαρακτηριστικά ασφάλειας. Η ασφάλεια που προσφέρουν είναι ελάχιστη και πρέπει να συμπληρωθεί από κατάλληλη διαχείριση και υλοποίηση επιμέρους διαδικασιών. Η επιλογή των κατάλληλων μηχανισμών ελέγχου, προϋποθέτει προσεκτικό και λεπτομερή σχεδιασμό. Η ασφάλεια των πληροφοριών απαιτεί τη συμμετοχή όλων των εργαζομένων του οργανισμού. Επιπλέον, μπορεί να χρειάζεται και η συμμετοχή των προμηθευτών, των πελατών ή ακόμη και η συνδρομή εξωτερικών εμπειρογνωμόνων συνεργατών εξειδικευμένων σε θέματα ασφάλειας. Οι μηχανισμοί ελέγχου ενσωματώνονται με το μικρότερο κόστος και αποδίδουν τα μέγιστα όταν περιλαμβάνονται στα αρχικά στάδια καταγραφής των απαιτήσεων και του σχεδιασμού.

0.3 Καταγραφή απαιτήσεων ασφάλειας

Πρωταρχική σημασία έχει η αναγνώριση εκ μέρους ενός οργανισμού των πραγματικών απαιτήσεων του σε θέματα ασφάλειας. Υπάρχουν τρεις κύριες πηγές για το σκοπό αυτόν:

- Η αποτίμηση των κινδύνων (risk assessment) που αντιμετωπίζει ο οργανισμός. Μέσω αυτής της διαδικασίας, αναγνωρίζονται οι πιθανές απειλές προς τους πόρους του οργανισμού. Επιπλέον εκτιμάται η ευπάθεια (vulnerability) του οργανισμού στις συγκεκριμένες απειλές, η πιθανότητα υλοποίησής τους, καθώς και το κόστος που θα έχουν για τον οργανισμό.

- Το νομικό πλαίσιο και οι συμβατικές υποχρεώσεις του οργανισμού απέναντι στο κράτος, το προσωπικό και τους συνεργάτες του.

- Το σύνολο των αρχών, των απαιτήσεων και των στόχων που ορίζει ο ίδιος ο οργανισμός σχετικά με την επεξεργασία των πληροφοριών που είναι απαραίτητες στη λειτουργία του.

0.4 Αποτίμηση κινδύνων ασφάλειας

Οι απαιτήσεις ασφάλειας του οργανισμού προκύπτουν ύστερα από μεθοδική καταγραφή των κινδύνων που αντιμετωπίζει ο οργανισμός. Το κόστος των μηχανισμών ασφάλειας θα πρέπει να δικαιολογείται από την πιθανή ζημιά στον οργανισμό στην περίπτωση που παραβιασθεί η ασφάλεια του. Τεχνικές αποτίμησης μπορούν να εφαρμοστούν στο σύνολο του οργανισμού ή μόνο σε επιμέρους τμήματά του, στα οποία έχουν καλύτερη πρακτική εφαρμογή και αποτελέσματα.

Η αποτίμηση κινδύνων είναι μια συστηματική εξέταση των ακόλουθων παραγόντων:

- Της ζημιάς που θα υποστεί ο οργανισμός στην περίπτωση που εμφανιστεί ένας κίνδυνος ασφάλειας, συμπεριλαμβανομένων των συνεπειών από την απώλεια της εμπιστευτικότητας, της ακεραιότητας ή της διαθεσιμότητας των πληροφοριών ή άλλων πόρων.

- Της ρεαλιστικής εκτίμησης της πιθανότητας να εμφανιστεί ένας τέτοιος κίνδυνος ασφάλειας σε σχέση με τους υπάρχοντες μηχανισμούς ελέγχου.

Τα αποτελέσματα αυτής της αποτίμησης καθορίζουν τις κατάλληλες ενέργειες και προτεραιότητες του οργανισμού, όπως και τους τρόπους υλοποίησης μηχανισμών ελέγχου της ασφάλειας απέναντι σε αυτούς τους κινδύνους. Η διαδικασία αποτίμησης των κινδύνων

και η επιλογή των κατάλληλων μηχανισμών ελέγχου και προστασίας μπορεί να επαναληφθεί πολλές φορές προκειμένου να καλύψει διαφορετικά τμήματα του οργανισμού ή διαφορετικά πληροφοριακά συστήματα.

Είναι απαραίτητος ο περιοδικός έλεγχος των κινδύνων ασφάλειας όπως και των μηχανισμών προστασίας προκειμένου να:

- προσαρμόζονται στις ανάγκες και τις προτεραιότητες του οργανισμού.
- επεκτείνονται στην προστασία από νέους κινδύνους.
- επιβεβαιώνουν την ορθή και αποτελεσματική λειτουργία των υπαρχόντων μηχανισμών προστασίας και ελέγχου.

Οι περιοδικοί έλεγχοι θα πρέπει να διεξάγονται σε διάφορα επίπεδα, ανάλογα με τα αποτελέσματα προηγούμενων ελέγχων και τις αλλαγές στο επίπεδο κινδύνου που είναι αποδεκτό για τον οργανισμό. Συχνά, η αποτίμηση κινδύνου γίνεται αρχικά σε ένα υψηλό επίπεδο για τον καθορισμό προτεραιοτήτων και στη συνέχεια σε πιο αναλυτικά επίπεδα για την καταγραφή και αντιμετώπιση συγκεκριμένων κινδύνων.

0.5 Επιλογή μηχανισμών

Εφόσον καθοριστούν οι απαιτήσεις ασφάλειας, μπορεί να γίνει η επιλογή των κατάλληλων μηχανισμών ελέγχου και προστασίας, οι οποίοι θα μειώσουν τον κίνδυνο σε αποδεκτά επίπεδα. Οι απαραίτητοι μηχανισμοί μπορούν να επιλεγούν από οποιοδήποτε σύνολο είναι κατάλληλο για τον οργανισμό. Υπάρχουν πολλοί διαφορετικοί τρόποι για τη διαχείριση κινδύνων. Πρέπει όμως να ληφθεί υπόψη ότι δεν είναι όλα τα μέσα το ίδιο κατάλληλα ή το ίδιο πρακτικά για όλους τους οργανισμούς.

Οι μηχανισμοί θα πρέπει να επιλεγούν με κριτήριο το κόστος υλοποίησής τους σε σχέση με τους κινδύνους που καλούνται να αντιμετωπίσουν και το κόστος των πιθανών επιπτώσεων των τελευταίων στον οργανισμό. Επίσης, θα πρέπει να συμπεριληφθούν και ποιοτικοί παράγοντες, όπως η απώλεια φήμης για τον οργανισμό. Κάποιοι από τους μηχανισμούς

ελέγχου και προστασίας μπορούν να θεωρηθούν ως βασικοί στην ασφάλεια πληροφοριών για κάθε είδους οργανισμό και περιγράφονται στην επόμενη παράγραφο.

0.6 Βασικοί μηχανισμοί ασφάλειας

Ένας αριθμός μηχανισμών ελέγχου και προστασίας θεωρούνται θεμελιώδεις και αποτελούν τη βάση για την ασφάλεια πληροφοριών. Βασίζονται είτε σε υποχρεωτικές νομικές διατάξεις, είτε έχουν καθιερωθεί ως κοινή πρακτική στην ασφάλεια.

Μηχανισμοί απαραίτητοι σε έναν οργανισμό και που βασίζονται στη νομοθεσία είναι:

- Διαφύλαξη των προσωπικών δεδομένων (παράγραφος 12.1.4)
- Διαφύλαξη των δεδομένων του οργανισμού (παράγραφος 12.1.3)
- Δικαιώματα πνευματικής ιδιοκτησίας (παράγραφος 12.1.2)

Μηχανισμοί που έχουν καθιερωθεί ως κοινή πρακτική είναι:

- Πολιτική ασφάλειας (παράγραφος 3.1)
- Καταμερισμός καθηκόντων σχετικών με την ασφάλεια (παράγραφος 4.1.3)
- Εκπαίδευση σε θέματα ασφάλειας (παράγραφος 6.2.1)
- Αναφορά συμβάντων (παράγραφος 6.3.1)
- Διαχείριση της επιχειρησιακής συνέχειας (παράγραφος 11.1)

Οι προαναφερθέντες μηχανισμοί μπορούν να χρησιμοποιηθούν σχεδόν σε κάθε οργανισμό. Όμως, αν και αποτελούν βασικά βήματα στην ασφάλεια, δεν πρέπει σε καμία περίπτωση να υποκαταστήσουν τη διενέργεια μελέτης αποτίμησης κινδύνων και προσεχτικής υλοποίησης των αποτελεσμάτων της τελευταίας.

0.7 Βασικοί παράγοντες επιτυχίας

Η εμπειρία δείχνει ότι οι ακόλουθοι παράγοντες έχουν ιδιαίτερη σημασία στην υλοποίηση της ασφάλειας πληροφοριών μέσα σε έναν οργανισμό:

- Πολιτική ασφάλειας, στόχοι και δραστηριότητες που αντικατροπτίζουν τους στόχους του οργανισμού.
- Εφαρμογή διαδικασιών ασφάλειας με τρόπο συμβατό με την κουλτούρα του οργανισμού.
- Ενεργή υποστήριξη από τη διοίκηση του οργανισμού.
- Κατανόηση των απαιτήσεων ασφάλειας, της αποτίμησης κινδύνων και της διαχείρισης τους.
- Κατανόηση από όλο το προσωπικό του οργανισμού της αναγκαιότητας ύπαρξης και λειτουργίας μηχανισμών ασφάλειας.
- Γνώση της πολιτικής ασφάλειας από όλο το προσωπικό και τους εξωτερικούς συνεργάτες.
- Εκπαίδευση και επιμόρφωση του προσωπικού.
- Ένα κατανοητό και ισορροπημένο σύστημα μέτρησης που να μπορεί να αξιολογήσει την απόδοση του συστήματος ασφάλειας των πληροφοριών και να προτείνει πιθανές βελτιώσεις.

1. Σκοπός

Το πρότυπο ISO 17799 παρέχει γενικές κατευθύνσεις για τη διαχείριση της ασφάλειας πληροφοριών. Απευθύνεται στους υπεύθυνους υλοποίησης της ασφάλειας σε έναν οργανισμό. Περιγράφει μια κοινή βάση για την ανάπτυξη επιπέδων ασφάλειας μέσα στον οργανισμό, την αποτελεσματική διαχείριση της ασφάλειας πληροφοριών και τη δημιουργία εμπιστοσύνης κατά τις συναλλαγές ανάμεσα σε οργανισμούς. Οι προτάσεις του προτύπου θα πρέπει να επιλεγούν και να χρησιμοποιηθούν σύμφωνα με τη σχετική νομοθεσία.

2. Ορολογία

Στο παρόν κείμενο χρησιμοποιείται η ακόλουθη ορολογία:

2.1 Ασφάλεια πληροφοριών (Information Security)

Ως ασφάλεια πληροφοριών χαρακτηρίζεται η προστασία και διατήρηση της εμπιστευτικότητας, της ακεραιότητας και της διαθεσιμότητας τους.

- **Εμπιστευτικότητα (Confidentiality):** Διασφάλιση ότι η πληροφορία μπορεί να προσπελασθεί μόνον από αυτούς που έχουν κατάλληλη εξουσιοδότηση.
- **Ακεραιότητα (Integrity):** Προστασία και διασφάλιση της ακρίβειας και της πληρότητας της πληροφορίας, όπως και των μεθόδων επεξεργασίας αυτής.
- **Διαθεσιμότητα (Availability):** Διασφάλιση ότι μόνον εξουσιοδοτημένοι χρήστες έχουν πρόσβαση στην πληροφορία και τους παρεμφερείς πόρους όταν απαιτείται.

2.2 Αποτίμηση κινδύνου (Risk Assessment)

Η αποτίμηση των κινδύνων, των αδυναμιών και των επιδράσεών τους στην πληροφορία και τη διαχείρισή της, όπως και της πιθανότητας πραγματοποίησής τους.

2.3 Διαχείριση κινδύνου (Risk Management)

Η αναγνώριση, ο έλεγχος και η ελαχιστοποίηση των κινδύνων ασφάλειας που μπορούν να επηρεάσουν τα πληροφοριακά συστήματα, με αποδεκτό κόστος.

3. Πολιτική ασφάλειας (Security Policy)

3.1 Πολιτική ασφάλειας πληροφοριών

Σκοπός της πολιτικής ασφάλειας πληροφοριών είναι η παροχή κατευθύνσεων και υποστήριξης για ζητήματα ασφάλειας πληροφοριών. Η διοίκηση του οργανισμού θα πρέπει να καθορίσει μια σαφή και ξεκάθαρη πολιτική, την οποία και θα υποστηρίζει έμπρακτα. Η πολιτική αυτή θα πρέπει να ρυθμίζει ζητήματα ασφάλειας σε όλα τα επίπεδα του οργανισμού.

3.1.1 Κείμενο της πολιτικής ασφάλειας

Το κείμενο της πολιτικής ασφάλειας θα πρέπει να γίνει αποδεκτό από τη διοίκηση του οργανισμού. Στη συνέχεια θα πρέπει να δημοσιοποιηθεί σε όλους τους υπαλλήλους. Θα πρέπει να αναφέρει τη δέσμευση της διοίκησης και τον τρόπο προσέγγισης του οργανισμού σε θέματα ασφάλειας. Θα πρέπει τουλάχιστον να περιλαμβάνει τα ακόλουθα:

- Τον ορισμό της ασφάλειας των πληροφοριών, το σκοπό της και τη σπουδαιότητά της ως μηχανισμού που επιτρέπει την ανταλλαγή πληροφοριών.
- Τους σκοπούς της διοίκησης και την υποστήριξή της αναφορικά με την ασφάλεια.
- Την επεξήγηση της πολιτικής ασφάλειας, των αρχών, των προτύπων και των απαιτήσεων που πρέπει να ικανοποιήσει ο οργανισμός, όπως σχετική νομοθεσία, προστασία από ιούς, επιπτώσεις μη συμμόρφωσης με την πολιτική ασφάλειας, διαχείριση επιχειρηματικής συνέχειας κλπ.
- Τον ορισμό γενικών και ειδικών καθηκόντων για τη διαχείριση της ασφάλειας και την αναφορά συμβάντων.
- Αναφορές σε άλλα κείμενα που μπορούν να υποστηρίξουν την πολιτική ασφάλειας, όπως περιγραφές συγκεκριμένων διαδικασιών και κανονισμών.

Η πολιτική ασφάλειας θα πρέπει να κοινοποιείται σε ολόκληρο τον οργανισμό, έχοντας κατά περίπτωση την κατάλληλη μορφή.

3.1.2 Έλεγχος και αξιολόγηση

Θα πρέπει να υπάρχει ένας υπεύθυνος για την πολιτική ασφάλειας, καθήκον του οποίου θα είναι ο περιοδικός έλεγχος και η αναπροσαρμογή της μέσω προκαθορισμένων διαδικασιών. Οι διαδικασίες αυτές θα πρέπει να διασφαλίζουν ότι οποιεσδήποτε αλλαγές γίνονται αντικατροπτίζουν μεταβολές που προκύπτουν από την αποτίμηση των κινδύνων που αντιμετωπίζει ο οργανισμός, όπως αλλαγές στη δομή του, ανακάλυψη νέων τρόπων επιθέσεων κλπ. Επίσης θα πρέπει να γίνεται περιοδικός έλεγχος σύμφωνα με τα ακόλουθα:

- Την αποτελεσματικότητα της πολιτικής σύμφωνα με καταγεγραμμένα περιστατικά ασφάλειας.
- Το κόστος των μηχανισμών προστασίας και τις επιπτώσεις τους στην λειτουργία του οργανισμού.
- Την εξέλιξη της τεχνολογίας.

4. Ασφάλεια του οργανισμού

4.1 Υποδομή ασφάλειας πληροφοριών

Η υποδομή της ασφάλειας πληροφοριών έχει ως αντικείμενο τη διαχείριση της ασφάλειας μέσα σε έναν οργανισμό. Θα πρέπει να δημιουργηθεί ένα πλαίσιο διαχείρισης προκειμένου να ελέγχεται η υλοποίηση της ασφάλειας των πληροφοριών μέσα στον οργανισμό. Θα πρέπει να υπάρχει έμπρακτο ενδιαφέρον και υποστήριξη από τη διοίκηση του οργανισμού για τη δημιουργία της πολιτικής ασφάλειας, τον καταμερισμό καθηκόντων και τη μεθοδική εφαρμογή της τελευταίας στον οργανισμό. Αν κριθεί αναγκαίο, θα πρέπει να ζητηθεί και η βοήθεια εμπειρογνωμόνων εκτός του οργανισμού, προκειμένου να μπορούν να ληφθούν υπόψη και οι εξελίξεις στο χώρο, αλλά και να αντιμετωπίζονται διάφορα συμβάντα. Θα πρέπει να επιδιωχθεί η συνεργασία διαφορετικών ομάδων, όπως οι χρήστες, οι προμηθευτές των τμημάτων του πληροφοριακού συστήματος, εμπειρογνώμονες ασφάλειας και η ίδια η διοίκηση του οργανισμού.

4.1.1 Ομάδα διαχείρισης της ασφάλειας

Η ασφάλεια πληροφοριών αποτελεί ευθύνη όλων των μελών της διοίκησης. Για αυτό το σκοπό θα πρέπει να συγκροτηθεί ειδική ομάδα εργασίας η οποία θα έχει ως σκοπό την προώθηση της ασφάλειας στον οργανισμό, με τη δέσμευση των κατάλληλων πόρων. Μια τυπική ομάδα εργασίας αναλαμβάνει τα ακόλουθα:

- Τον έλεγχο και την τελική έγκριση της πολιτικής ασφάλειας, όπως και τον καταμερισμό των σχετικών καθηκόντων.
- Τον έλεγχο σημαντικών αλλαγών και τις επιπτώσεις τους στην ασφάλεια του οργανισμού.
- Τον έλεγχο και την παρακολούθηση συμβάντων που σχετίζονται με την ασφάλεια.
- Την έγκριση πρωτοβουλιών για την ενίσχυση της ασφάλειας.

Ένα διοικητικό στέλεχος θα πρέπει να είναι υπεύθυνο για όλα τα ζητήματα ασφάλειας του οργανισμού.

4.1.2 Συντονισμός ασφάλειας πληροφοριών

Σε ένα μεγάλο οργανισμό θα πρέπει να υπάρχει μια ομάδα εργασίας που να περιλαμβάνει μέλη από όλα τα διαφορετικά τμήματα. Αυτή η ομάδα θα πρέπει να συντονίζει την υλοποίηση των μηχανισμών προστασίας. Μια τυπική τέτοια ομάδα έχει τις ακόλουθες αρμοδιότητες:

- Καθορίζει συγκεκριμένους ρόλους και καθήκοντα για την ασφάλεια του οργανισμού.
- Καθορίζει συγκεκριμένες διαδικασίες και μεθοδολογίες για την υλοποίηση της ασφάλειας, όπως αποτίμηση κινδύνου, διαβαθμίσεις ασφάλειας κλπ.
- Υποστηρίζει πρωτοβουλίες σχετικές με την ασφάλεια του οργανισμού.
- Διασφαλίζει ότι η ασφάλεια αποτελεί μέρος των δραστηριοτήτων του οργανισμού.
- Ελέγχει και κατευθύνει την υλοποίηση συγκεκριμένων μηχανισμών ασφάλειας για νέα συστήματα και υπηρεσίες.
- Εξετάζει τα συμβάντα σχετικά με την ασφάλεια.
- Υποστηρίζει ενεργά την εφαρμογή της ασφάλειας σε όλα τα τμήματα του οργανισμού.

4.1.3 Καθορισμός καθηκόντων

Τα καθήκοντα για την προστασία συγκεκριμένων στοιχείων του οργανισμού, όπως και τη διεκπεραίωση επίσης συγκεκριμένων διαδικασιών θα πρέπει να είναι σαφώς καθορισμένα.

Η πολιτική ασφάλειας θα πρέπει να παρέχει γενικές κατευθύνσεις για τον καθορισμό των ρόλων και των αρμοδιοτήτων στον οργανισμό. Όπου είναι απαραίτητο, η πολιτική ασφάλειας θα πρέπει να συμπληρώνεται από λεπτομερείς οδηγίες για συγκεκριμένα συστήματα, υπηρεσίες ή τοποθεσίες (sites). Θα πρέπει να περιγράφονται αναλυτικά ειδικές αρμοδιότητες

για δεδομένα και φυσικούς πόρους του οργανισμού, όπως το σχέδιο επιχειρησιακής συνέχειας.

Σε πολλούς οργανισμούς ένας υπεύθυνος ασφάλειας θα είναι ο κατάλληλος άνθρωπος να αναλάβει τον καθορισμό και την υλοποίηση της ασφάλειας, όπως και την επιλογή των μηχανισμών προστασίας και ελέγχου. Την ευθύνη για την καθημερινή ασφάλεια συγκεκριμένων στοιχείων του οργανισμού θα την έχουν επιλεγμένα στελέχη, τα οποία θα είναι οι τυπικοί ιδιοκτήτες τους.

Οι ιδιοκτήτες των στοιχείων του οργανισμού, μπορούν να μεταβιβάσουν τα καθήκοντά τους σε πιο εξειδικευμένα άτομα, αν και η τελική ευθύνη είναι πάντοτε δική τους. Τα καθήκοντα των στελεχών θα πρέπει να είναι σαφή και να περιλαμβάνουν τα ακόλουθα:

- Το σαφή συσχετισμό ανάμεσα σε διαδικασίες και πόρους του οργανισμού.
- Το υπεύθυνο στέλεχος για κάθε προστατευόμενο πόρο και την αναλυτική περιγραφή των καθηκόντων του και των ευθυνών του.
- Σαφώς καθορισμένα επίπεδα εξουσιοδότησης.

4.1.4 Εξουσιοδότηση στις εγκαταστάσεις επεξεργασίας των πληροφοριών

Θα πρέπει να υπάρχει μια διαδικασία εξουσιοδότησης για τις νέες εγκαταστάσεις επεξεργασίας των πληροφοριών. Συνιστώνται οι ακόλουθοι μηχανισμοί:

- Οι νέες εγκαταστάσεις θα πρέπει να έχουν τη σχετική έγκριση από τη διοίκηση, με την οποία καθορίζεται ο σκοπός και η χρήση τους. Θα πρέπει επίσης να υπάρχει και η έγκριση του τοπικού υπεύθυνου στελέχους, η οποία και θα επιβεβαιώνει την παρουσία όλων των απαραίτητων μηχανισμών ασφάλειας.
- Όπου κρίνεται απαραίτητο, υλικό και λογισμικό θα πρέπει να ελέγχονται για τη συμβατότητα τους με άλλα τμήματα του συστήματος.
- Η χρήση εγκαταστάσεων για την επεξεργασία προσωπικών δεδομένων θα πρέπει να έχει ιδιαίτερη εξουσιοδότηση.

- Η χρήση εγκαταστάσεων επεξεργασίας προσωπικών δεδομένων στο χώρο εργασίας, μπορεί να προκαλέσει νέους κινδύνους στο σύστημα. Κατά συνέπεια θα πρέπει να έχει την κατάλληλη εξουσιοδότηση.

Οι προαναφερόμενοι μηχανισμοί έχουν ιδιαίτερη σημασία σε περιβάλλον δικτύου.

4.1.5 Συνδρομή ειδικών εμπειρογνωμόνων

Η συνδρομή ειδικών εμπειρογνωμόνων σε θέματα ασφάλειας είναι πιθανό να απαιτείται σε πολλούς οργανισμούς. Στην ιδανική περίπτωση, ένας ειδικός εμπειρογνώμων θα υπάρχει στον ίδιο τον οργανισμό. Στην περίπτωση, όμως, που αυτό δεν είναι εφικτό, θα πρέπει να ζητηθεί η συνδρομή εξωτερικού συμβούλου, ειδικού σε θέματα ασφάλειας, ο οποίος θα καθοδηγήσει τον οργανισμό.

Οι εξειδικευμένοι σύμβουλοι ασφάλειας θα πρέπει να είναι σε θέση να βοηθήσουν τον οργανισμό σε κάθε ζήτημα ασφάλειας, βασιζόμενοι στην προσωπική τους εμπειρία ή στην εμπειρία τρίτων. Η ποιότητα των γνώσεών τους και η εμπειρία τους, επηρεάζουν άμεσα την αποτελεσματικότητα της ασφάλειας του οργανισμού. Για ακόμα καλύτερα αποτελέσματα θα πρέπει να έχουν απευθείας πρόσβαση στην διοίκηση του οργανισμού.

Η συνδρομή του συμβούλου ασφάλειας θα πρέπει να ζητείται όσο το δυνατόν πιο άμεσα, ειδικά όταν υπάρχει η υποψία παραβίασης της ασφάλειας του οργανισμού ή όταν έχει παρουσιασθεί κάποιος καινούριος κίνδυνος. Ο σύμβουλος ασφάλειας μπορεί να βοηθήσει τον οργανισμό στη διαδικασία της έρευνας που θα πρέπει να ακολουθήσει την καταγραφή κάποιου συμβάντος. Η συνδρομή του μπορεί να είναι καθαρά συμβουλευτικού χαρακτήρα ή πιο ενεργή, επιβλέποντας ή συμμετέχοντας ο ίδιος στην έρευνα.

4.1.6 Συνεργασία ανάμεσα σε οργανισμούς

Θα πρέπει να υπάρχουν οι κατάλληλοι σύνδεσμοι με τις αρχές, τηλεπικοινωνιακούς οργανισμούς και ISPs προκειμένου να εξασφαλισθεί η ανάληψη των κατάλληλων δράσεων στην περίπτωση ενός συμβάντος κατά της ασφάλειας του οργανισμού. Επιπλέον θα πρέπει να

εξετασθεί και το ενδεχόμενο της συμμετοχής του οργανισμού σε internet security groups, security mailing lists κ.α.

Η ανταλλαγή πληροφοριών σχετικών με την ασφάλεια του οργανισμού θα πρέπει να είναι περιορισμένη ώστε να μην περιέλθουν ευαίσθητες πληροφορίες σε μη εξουσιοδοτημένα άτομα.

4.1.7 Ανεξάρτητος έλεγχος της ασφάλειας

Το κείμενο της πολιτικής ασφάλειας καθορίζει την πολιτική και τις ευθύνες για την ασφάλεια των πληροφοριών. Η εφαρμογή του θα πρέπει να ελέγχεται ανεξάρτητα και συστηματικά, ώστε να επιβεβαιωθεί ότι οι πρακτικές που ακολουθεί ο οργανισμός είναι σύμφωνες με τις απαιτήσεις ασφάλειας του. Επιπλέον, η πολιτική ασφάλειας θα πρέπει να ελέγχεται για την αποτελεσματικότητα και τη σκοπιμότητα της.

Ένας τέτοιος έλεγχος μπορεί να γίνει από κάποιο στέλεχος ή μια ειδική ομάδα ελέγχου του οργανισμού, ή ακόμη από κάποιον εξωτερικό σύμβουλο.

4.2 Ασφάλεια προσπέλασης τρίτων μερών

Σκοπός είναι η ασφάλεια των εγκαταστάσεων επεξεργασίας πληροφοριών του οργανισμού, στις οποίες έχουν προσπέλαση τρίτοι. Η προσπέλαση από τρίτους στις εγκαταστάσεις του οργανισμού θα πρέπει να ελέγχεται. Όπου υπάρχει ανάγκη για τέτοιου είδους προσπέλαση θα πρέπει να διενεργείται αποτίμηση κινδύνου προκειμένου να καθοριστούν οι επιπτώσεις στην ασφάλεια του οργανισμού και να εγκατασταθούν οι απαραίτητοι μηχανισμοί ελέγχου και προστασίας, με τους οποίους θα πρέπει να συμφωνήσει και το εν λόγω τρίτο μέρος. Επίσης, θα πρέπει να προβλεφθούν και οι διαδικασίες μεταβίβασης των δικαιωμάτων προσπέλασης από το τρίτο μέρος σε κάποια άλλη οντότητα. Οι μηχανισμοί αυτοί μπορούν να χρησιμοποιηθούν και για την κάλυψη των αναγκών που προκύπτουν από το outsourcing λειτουργιών του ίδιου του οργανισμού.

4.2.1 Καθορισμός των κινδύνων από την προσπέλαση τρίτων

4.2.1.1 Είδη προσπέλασης

Το είδος της προσπέλασης που θα δοθεί σε κάποιον τρίτο έχει ιδιαίτερη σημασία. Οι κίνδυνοι που προκύπτουν από την προσπέλαση στο δίκτυο του οργανισμού είναι εντελώς διαφορετικοί από αυτούς της φυσικής προσπέλασης. Τα είδη της προσπέλασης τα οποία θα πρέπει να εξεταστούν είναι:

- Φυσική προσπέλαση σε διάφορους χώρους.
- Λογική προσπέλαση στα υπολογιστικά συστήματα του οργανισμού.

4.2.1.2 Λόγοι προσπέλασης

Η προσπέλαση από τρίτους μπορεί να είναι απαραίτητη για διάφορους λόγους. Για παράδειγμα, μπορεί κάποιο τρίτοι να παρέχουν υπηρεσίες στον οργανισμό και να χρειάζονται φυσική και λογική προσπέλαση. Τέτοιες περιπτώσεις είναι:

- Η τεχνική υποστήριξη σε υλικό και λογισμικό από τρίτους.
- Εμπορικοί συνεργάτες που χρειάζονται πρόσβαση στο πληροφοριακό σύστημα του οργανισμού.

Η ασφάλεια του οργανισμού μπορεί να τεθεί σε κίνδυνο όταν δε γίνεται σωστή αποτίμηση κινδύνου και δε λαμβάνονται σωστά μέτρα κατά την παροχή προσπέλασης σε τρίτους. Θα πρέπει να εξετάζεται τόσο ο τύπος της προσπέλασης που απαιτείται από το τρίτο μέρος και οι επιπτώσεις στη ασφάλεια του οργανισμού, όσο και οι μηχανισμοί ελέγχου και προστασίας που χρησιμοποιεί το ίδιο το τρίτο μέρος για τη δική του ασφάλεια.

4.2.1.3 Εξωτερικοί συνεργάτες on-site

Εξωτερικοί συνεργάτες οι οποίοι δουλεύουν στις εγκαταστάσεις του οργανισμού για συγκεκριμένο χρόνο, αποτελούν επίσης πιθανό κίνδυνο για την ασφάλεια. Τέτοιοι συνεργάτες μπορεί να είναι:

- Προσωπικό υποστήριξης του πληροφοριακού συστήματος του οργανισμού.
- Συνεργεία καθαρισμού, φύλαξης κλπ.
- Ειδικοί σύμβουλοι.

Είναι πολύ σημαντικό να καθοριστούν οι μηχανισμοί ελέγχου της προσπέλασης τρίτων στις εγκαταστάσεις του οργανισμού. Όλες οι απαιτήσεις που προκύπτουν από τέτοιου είδους προσπέλαση, θα πρέπει να καλύπτονται και από ειδικές συμβάσεις, όπως συμφωνίες μη αποκάλυψης στοιχείων κλπ. Επιπλέον, η προσπέλαση σε τρίτους δεν πρέπει να επιτρέπεται πριν την προετοιμασία του οργανισμού και την υπογραφή των απαραίτητων συμβάσεων.

4.2.2 Απαιτήσεις ασφάλειας σε συμβάσεις με τρίτους

Τα ζητήματα σχετικά με την προσπέλαση τρίτων θα πρέπει να ρυθμίζονται με ειδικές συμβάσεις, οι οποίες και θα διασφαλίζουν ότι οι τρόποι προσπέλασης είναι σύμφωνοι με την πολιτική ασφάλειας του οργανισμού. Οι συμβάσεις θα πρέπει να προβλέπουν και σχετικές αποζημιώσεις για τα δύο μέρη, ενώ μπορούν να περιλαμβάνουν τα ακόλουθα:

- Τη γενική πολιτική σχετικά με την ασφάλεια των πληροφοριών.
- Την προστασία των διάφορων πόρων, συμπεριλαμβανομένων των διαδικασιών μέσω των οποίων οι πόροι αυτοί θα προστατεύονται, των διαδικασιών με βάση τις οποίες θα ελέγχεται η ασφάλειά τους, των μηχανισμών ελέγχου και προστασίας, τους κανόνες διαθεσιμότητας και ακεραιότητας, όπως και περιορισμούς σχετικά με αντιγραφή πληροφοριών και την απαιτούμενη εχεμύθεια.
- Περιγραφή όλων των υπηρεσιών που θα είναι διαθέσιμες.
- Το απαιτούμενο επίπεδο ποιότητας των διαθέσιμων υπηρεσιών.

- Ζητήματα μεταφοράς προσωπικού.
- Ευθύνες των μερών της σύμβασης.
- Ευθύνες που απορρέουν από σχετική νομοθεσία.
- Ζητήματα πνευματικής ιδιοκτησίας.
- Μηχανισμούς ελέγχου προσπέλασης, πρόσωπα στα οποία θα επιτρέπεται η προσπέλαση, τα καθήκοντα και τις ευθύνες τους.
- Καθορισμό των μηχανισμών αξιολόγησης και ελέγχου των παρεχόμενων υπηρεσιών.
- Τα δικαιώματα παρακολούθησης των δραστηριοτήτων των χρηστών.
- Τα ζητήματα παρακολούθησης και επιβεβαίωσης όσων προβλέπονται στη σύμβαση.
- Τους μηχανισμούς επίλυσης προβλημάτων.
- Τις αρμοδιότητες για την εγκατάσταση και συντήρηση υλικού και λογισμικού.
- Ένα σαφή μηχανισμό αναφορών.
- Τους μηχανισμούς διαχείρισης των αλλαγών στον οργανισμό.
- Τους απαραίτητους μηχανισμούς φυσικής προστασίας.
- Την εκπαίδευση των χρηστών και των διαχειριστών του συστήματος.
- Τους μηχανισμούς προστασίας από κακόβουλο λογισμικό.
- Τις διαδικασίες χειρισμού, επίλυσης και αναφοράς συμβάντων.
- Τις σχέσεις των τρίτων μερών με υπεργολάβους.

4.3 Outsourcing

Σκοπός είναι η διατήρηση της ασφάλειας των πληροφοριών όταν η επεξεργασία τους έχει ανατεθεί σε έναν άλλο οργανισμό. Θα πρέπει να ληφθούν υπόψη τα ζητήματα που αφορούν

την ασφάλεια του δικτύου, του υλικού και του λογισμικού στα οποία θα έχει πρόσβαση ο τρίτος οργανισμός.

4.3.1 Απαιτήσεις ασφάλειας σε συμβάσεις outsourcing

Οι απαιτήσεις ασφάλειας ενός οργανισμού, ο οποίος αναθέτει τον έλεγχο μέρους ή και ολόκληρου του πληροφοριακού του συστήματος σε τρίτο οργανισμό, θα πρέπει να συμφωνηθούν με τη μορφή συμβάσεως ανάμεσα στα εμπλεκόμενα μέρη. Μια τέτοια σύμβαση θα πρέπει κατ' ελάχιστον να περιλαμβάνει:

- Τον τρόπο με τον οποίο θα ικανοποιούνται οι απαιτήσεις της σχετικής νομοθεσίας.
- Τον τρόπο με τον οποίο θα διασφαλιστεί η σωστή και σαφής κατανομή αρμοδιοτήτων σε όλα τα εμπλεκόμενα μέρη.
- Τον τρόπο διασφάλισης και ελέγχου της ακεραιότητας και της εμπιστευτικότητας των δεδομένων του οργανισμού.
- Τον τρόπο ελέγχου της πρόσβασης στα δεδομένα του οργανισμού.
- Τα επίπεδα φυσικής ασφάλειας.
- Τη διαθεσιμότητα των απαραίτητων υπηρεσιών σε περίπτωση ανάγκης.
- Τα δικαιώματα ελέγχου (audit).

Στη σύμβαση θα πρέπει να περιλαμβάνονται και όσα αναφέρονται στην παράγραφο 4.2.2. Η σύμβαση θα πρέπει να περιλαμβάνει ένα σχέδιο ασφάλειας στο οποίο θα συμφωνήσουν τα εμπλεκόμενα μέρη.

5. Ταξινόμηση πόρων και έλεγχος

5.1 Υπευθυνότητα για πόρους

Σκοπός είναι η κατάλληλη προστασία των πόρων του οργανισμού. Όλοι οι κύριοι πόροι, σχετικοί με τα δεδομένα του οργανισμού, θα πρέπει να έχουν έναν ορισμένο ιδιοκτήτη. Η υπευθυνότητα για τους πόρους του οργανισμού διασφαλίζει τη διατήρηση του κατάλληλου επιπέδου ασφάλειας. Θα πρέπει να καθοριστούν ιδιοκτήτες για όλα τα κύρια δεδομένα του οργανισμού, οι οποίοι θα είναι και υπεύθυνοι για την προστασία τους. Η ευθύνη της πρακτικής διασφάλισης των δεδομένων μπορεί να ανατεθεί σε κάποιον άλλον, αν και ο ιδιοκτήτης των δεδομένων έχει πάντα την τελική ευθύνη για την ασφάλειά τους.

5.1.1 Καταγραφή των πόρων

Η καταγραφή των πόρων βοηθά στη σωστή προστασία τους και μπορεί να απαιτείται και για άλλους λόγους, όπως συμμόρφωση με τη νομοθεσία, ασφάλεια προσωπικού κλπ. Η διαδικασία της καταγραφής των πόρων του οργανισμού είναι σημαντικό τμήμα της διαδικασίας διαχείρισης κινδύνου. Ο οργανισμός θα πρέπει να καθορίσει τους πόρους του και στη συνέχεια να προχωρήσει στην εκτίμησή τους, ποιοτικά αλλά και ποσοτικά. Στη συνέχεια μπορούν να καθοριστούν οι κατάλληλοι μηχανισμοί ασφάλειας ανάλογα με την αξία του κάθε πόρου. Για κάθε πόρο θα πρέπει να καθοριστεί ένας υπεύθυνος ιδιοκτήτης, καθώς επίσης και ένα επίπεδο ασφάλειας. Επιπλέον θα πρέπει να καταγραφεί και η τοποθεσία του. Παραδείγματα πόρων σχετικών με πληροφοριακά συστήματα είναι:

- Πληροφοριακοί πόροι: βάσεις δεδομένων, αρχεία δεδομένων, εκπαιδευτικό υλικό, περιγραφή διαδικασιών, σχέδια επιχειρησιακής συνέχειας, εγχειρίδια κλπ.
- Λογισμικό: εφαρμογές, εργαλεία ανάπτυξης, λειτουργικά συστήματα κλπ.
- Φυσικοί πόροι: υλικό υπολογιστών, εξοπλισμός τηλεπικοινωνιών, αποθηκευτικά μέσα κλπ.
- Υπηρεσίες: ηλεκτρισμός, κλιματισμός, υπηρεσίες επεξεργασίας δεδομένων κλπ.

5.2 Κατηγοριοποίηση πληροφοριών

Σκοπός της κατηγοριοποίησης είναι η εξασφάλιση ότι όλοι οι πληροφοριακοί πόροι του οργανισμού προστατεύονται κατάλληλα. Οι πληροφορίες θα πρέπει να κατατάσσονται σε κατηγορίες προκειμένου να φαίνεται η ανάγκη, ο βαθμός και η προτεραιότητα της προστασίας που χρειάζονται. Κάποια δεδομένα μπορεί να χρειάζονται ειδική μεταχείριση και επιπλέον μέτρα προστασίας. Ένα σύστημα κατηγοριοποίησης των πληροφοριών θα πρέπει να χρησιμοποιείται για τον καθορισμό των απαιτούμενων επιπέδων προστασίας, καθώς και για την επισήμανση τυχόν ανάγκης για ειδική μεταχείριση.

5.2.1 Γενικές οδηγίες κατηγοριοποίησης

Οι διάφορες κατηγορίες, καθώς και οι ανάλογοι μηχανισμοί προστασίας των πληροφοριών, θα πρέπει να περιλαμβάνουν και τις ανάγκες του οργανισμού για τη διακίνηση των πληροφοριών, καθώς και τις πιθανές επιπτώσεις που οφείλονται σε αυτές τις ανάγκες, όπως μη εξουσιοδοτημένη πρόσβαση σε πληροφορίες κλπ. Γενικά, η κατηγορία στην οποία κατατάσσεται κάποια πληροφορία, χρησιμεύει στον καθορισμό του τρόπου χειρισμού και προστασίας της πληροφορίας.

Οι πληροφορίες, όπως και τα αποτελέσματα της επεξεργασίας τους θα πρέπει να φέρουν ένα αναγνωριστικό σήμα (π.χ. μια ετικέτα) που να δηλώνει την αξία και το ευαίσθητο της πληροφορίας για τον οργανισμό. Συχνά, οι πληροφορίες παύουν να είναι κρίσιμης σημασίας μετά την πάροδο μιας χρονικής περιόδου. Θα πρέπει να ληφθεί υπόψη και αυτό το γεγονός, καθώς η υπερπροστασία της πληροφορίας μπορεί να επιφέρει άσκοπα έξοδα στον οργανισμό. Επίσης το σχήμα της κατηγοριοποίησης θα πρέπει να είναι αρκετά ευέλικτο ώστε να είναι δυνατή η αλλαγή του επιπέδου προστασίας των πληροφοριών στην πορεία του χρόνου (παράγραφος 9.1).

Προσοχή επίσης θα πρέπει να δοθεί στον αριθμό των κατηγοριών που θα χρησιμοποιηθούν, όπως και στα οφέλη από τη χρήση τους. Τα πολύπλοκα σχήματα τείνουν να μην είναι πρακτικά για έναν οργανισμό. Επίσης θα πρέπει να προβλεφθεί και ο τρόπος ερμηνείας των κατηγοριών που αναφέρονται στις πληροφορίες που προέρχονται από τρίτους οργανισμούς ώστε να χρησιμοποιούνται και να προστατεύονται κατάλληλα. Η ευθύνη της

κατηγοριοποίησης της κάθε πληροφορίας ανήκει στον καθορισμένο ιδιοκτήτη της. Αυτός θα πρέπει επίσης να ελέγχει περιοδικά την αναγκαιότητα κατηγοριοποίησης της συγκεκριμένης πληροφορίας στο επίπεδο όπου βρίσκεται.

5.2.2 Χαρακτηρισμός και χειρισμός των πληροφοριών

Είναι σημαντικό να καθοριστούν οι κατάλληλες διαδικασίες για το χαρακτηρισμό και τη διαχείριση των πληροφοριών σύμφωνα με το σύστημα κατηγοριοποίησης που έχει υιοθετηθεί από τον οργανισμό. Αυτές οι διαδικασίες θα πρέπει να καλύπτουν τόσο τους υλικούς όσο και τους ηλεκτρονικούς πληροφοριακούς πόρους του οργανισμού. Για κάθε κατηγορία θα πρέπει να καθοριστούν οι ανάλογες διαδικασίες χειρισμού της πληροφορίας, οι οποίες θα καλύπτουν τα ακόλουθα:

- Αντιγραφή
- Αποθήκευση
- Μετάδοση με φυσικό ή ηλεκτρονικό μέσο (π.χ. ταχυδρομείο, fax ή email)
- Μετάδοση μέσω ομιλίας (τηλεφωνικά ή δια ζώσης)
- Καταστροφή.

Τα παράγωγα της επεξεργασίας των πληροφοριών θα πρέπει να φέρουν την κατάλληλη επισήμανση της κατηγορίας τους, αντίστοιχη της κατηγορίας των πληροφοριών από τις οποίες προήλθαν. Τέτοια παράγωγα περιλαμβάνουν εκτυπώσεις, οθόνες προγραμμάτων, μαγνητικά μέσα αποθήκευσης, ηλεκτρονικά μηνύματα και μεταφορά αρχείων.

Οι κοινές ετικέτες αποτελούν γενικά το πιο κατάλληλο μέσο επισήμανσης του χαρακτήρα της πληροφορίας. Σε κάποιες περιπτώσεις όμως, όπως τα ηλεκτρονικά έγγραφα, θα πρέπει να χρησιμοποιούνται οι ανάλογες ηλεκτρονικές ετικέτες.

6. Ασφάλεια προσωπικού

6.1 Η ασφάλεια στα εργασιακά καθήκοντα

Σκοπός είναι η ελαχιστοποίηση των κινδύνων που μπορεί να προκληθούν από ανθρώπινο λάθος, κλοπή, απάτη ή κατάχρηση των εγκαταστάσεων του οργανισμού. Οι ευθύνες σχετικά με την ασφάλεια των πληροφοριών θα πρέπει να αναλύονται κατά τη διαδικασία πρόσληψης του προσωπικού. Επιπλέον θα πρέπει να αναφέρονται με σαφήνεια σε σχετικά συμβόλαια εργασίας, καθώς και να ελέγχεται η συμμόρφωση με αυτές κατά τη διάρκεια εργασίας του κάθε μέλους του προσωπικού. Οι υποψήφιοι υπάλληλοι θα πρέπει να ελέγχονται, ειδικά αυτοί που πρόκειται να έχουν ευαίσθητες θέσεις. Όλοι οι υπάλληλοι και οι συνεργάτες του οργανισμού θα πρέπει να υπογράφουν συμφωνητικό για τήρηση εχεμύθειας (non-disclosure agreement).

6.1.1 Ευθύνες σχετικές με την ασφάλεια

Οι ρόλοι και οι ευθύνες σχετικές με την ασφάλεια στον οργανισμό, θα πρέπει να επεξηγούνται αναλυτικά στην πολιτική ασφάλειας. Εκτός από τα γενικά καθήκοντα ασφάλειας, θα πρέπει να περιλαμβάνονται και τα ειδικά καθήκοντα, σχετικά με συγκεκριμένους πόρους ή την εκτέλεση ειδικών διαδικασιών.

6.1.2 Έλεγχος προσωπικού

Κατά την υποβολή αιτήσεων από τους υποψήφιους εργαζόμενους, ο οργανισμός θα πρέπει να ελέγχει και να επιβεβαιώνει τα όσα αναφέρονται σε αυτές. Θα πρέπει να ελέγχεται ότι:

- Υπάρχουν οι κατάλληλες συστάσεις.
- Τα στοιχεία που αναφέρονται στο βιογραφικό σημείωμα του υποψηφίου είναι ακριβή.
- Ο υποψήφιος κατέχει τους τίτλους που αναφέρει.
- Περιλαμβάνεται αποδεικτικό της ταυτότητας του υποψηφίου.

Στην περίπτωση που κάποιος υποψήφιος ή ένας εργαζόμενος πρόκειται να αναλάβει εξαιρετικά ευαίσθητα ή οικονομικά καθήκοντα, θα πρέπει – στα πλαίσια του νόμου - να διενεργείται και οικονομικός έλεγχος του συγκεκριμένου ατόμου. Επιπλέον, για μέλη του προσωπικού με σημαντικές θέσεις, θα πρέπει να επαναλαμβάνονται οι σχετικοί έλεγχοι σε τακτά χρονικά διαστήματα.

Παρόμοια διαδικασία επιλογής θα πρέπει να ακολουθείται και για το έκτακτο προσωπικό ή τους εξωτερικούς συνεργάτες. Στην περίπτωση που η επιλογή τους γίνεται με τη βοήθεια ειδικού γραφείου ευρέσεων προσωπικού, θα πρέπει να είναι ξεκάθαρες οι ευθύνες του γραφείου απέναντι στον οργανισμό.

Η διοίκηση του οργανισμού θα πρέπει επίσης να ελέγχει τους μηχανισμούς επίβλεψης για το νέο προσωπικό με πρόσβαση σε ευαίσθητα τμήματα του πληροφοριακού συστήματος. Περιοδικά θα πρέπει να γίνεται απευθείας έλεγχος από ανώτερα μέλη του προσωπικού. Θα πρέπει να ληφθεί υπόψη και το γεγονός ότι η εργασία των μελών του προσωπικού μπορεί να επηρεαστεί από διάφορα προβλήματα. Τέτοια προβλήματα μπορούν να οδηγήσουν σε λάθη, κλοπές ή άλλα προβλήματα ασφάλειας και θα πρέπει να αντιμετωπίζονται σύμφωνα με τη σχετική νομοθεσία.

6.1.3 Συμφωνίες τήρησης της εχεμύθειας

Οι συμφωνίες τήρησης της εχεμύθειας χρησιμοποιούνται για να επισημάνουν το απόρρητο των πληροφοριών. Τυπικά, το προσωπικό θα πρέπει να έχει υπογράψει τέτοιες συμφωνίες με τον οργανισμό. Σε περιπτώσεις μελών του προσωπικού ή εξωτερικών συνεργατών που δεν καλύπτονται από κάποια υπάρχουσα συμφωνία, θα πρέπει να καταρτίζεται ειδική σύμβαση πριν τους επιτραπεί η πρόσβαση στα δεδομένα και τις πληροφορίες του οργανισμού.

Οι υπάρχουσες συμφωνίες θα πρέπει να ελέγχονται περιοδικά και να αναπροσαρμόζονται σύμφωνα με τη σχετική νομοθεσία και τις ειδικές ανάγκες του οργανισμού, ειδικά όταν η σχέση συνεργασίας που καλύπτουν πλησιάζει στην ολοκλήρωση της.

6.1.4 Όροι πρόσληψης και κανονισμοί εργασίας

Οι όροι και οι κανονισμοί πρόσληψης και εργασίας θα πρέπει να περιέχουν και τις ευθύνες του υπαλλήλου για την ασφάλεια του οργανισμού. Σε ειδικές περιπτώσεις, οι ευθύνες αυτές θα πρέπει να συνεχίζονται για συγκεκριμένη χρονική περίοδο μετά τον τερματισμό της εργασίας. Θα πρέπει επίσης να ορίζονται και οι συνέπειες που θα υποστεί ο υπάλληλος αν παραβεί τους κανόνες ασφάλειας. Οι κανόνες ασφάλειας θα πρέπει να τηρούνται εντός και εκτός του οργανισμού, όπως και στην περίπτωση της τηλεεργασίας.

Οι νομικές ευθύνες του υπαλλήλου, όπως και τα δικαιώματά του, θα πρέπει να αναφέρονται με σαφήνεια στο συμβόλαιο εργασίας. Επιπλέον, σύμφωνα με το νόμο, θα πρέπει να λαμβάνεται μέριμνα και για την προστασία των προσωπικών δεδομένων του ίδιου του υπαλλήλου.

6.2 Εκπαίδευση χρηστών

Σκοπός είναι η εξασφάλιση της ενημέρωσης των χρηστών για τους κινδύνους κατά της ασφάλειας των πληροφοριακών συστημάτων του οργανισμού και η διασφάλιση ότι είναι κατάλληλα προετοιμασμένοι για την εφαρμογή της πολιτικής ασφάλειας του οργανισμού στην καθημερινή τους εργασία. Οι χρήστες θα πρέπει να εκπαιδεύονται στις διαδικασίες ασφάλειας και τη σωστή χρήση του πληροφοριακού συστήματος ώστε να ελαχιστοποιηθούν οι πιθανοί κίνδυνοι κατά της ασφάλειας του οργανισμού.

6.2.1 Εκπαίδευση στην ασφάλεια πληροφοριακών συστημάτων

Όλοι οι υπάλληλοι του οργανισμού, και όπου απαραίτητο και εξωτερικοί συνεργάτες, θα πρέπει να εκπαιδεύονται κατάλληλα και να ενημερώνονται για την πολιτική ασφάλειας και τις όποιες αλλαγές γίνονται σε αυτήν. Θα πρέπει να γνωρίζουν τις διαδικασίες, τις νομικές ευθύνες, τους μηχανισμούς προστασίας και τη σωστή χρήση του πληροφοριακού συστήματος. Η εκπαίδευση θα πρέπει να γίνεται πριν δοθεί στους χρήστες πρόσβαση στο πληροφοριακό σύστημα του οργανισμού.

6.3 Αντιμετώπιση περιστατικών

Σκοπός είναι η ελαχιστοποίηση των επιπτώσεων από περιστατικά ασφάλειας, όπως και η παρακολούθηση και η απόκτηση εμπειρίας από αυτά. Τα συμβάντα σχετικά με την ασφάλεια του οργανισμού θα πρέπει να αναφέρονται άμεσα μέσα από κατάλληλους διαύλους επικοινωνίας του οργανισμού. Όλοι οι υπάλληλοι θα πρέπει να γνωρίζουν τις διαδικασίες αναφοράς συμβάντων (παραβίαση ασφάλειας, απειλή, αδυναμία ή λάθος λειτουργία) που μπορούν να έχουν επιπτώσεις στην ασφάλεια των πόρων του οργανισμού. Οι υπάλληλοι θα πρέπει να αναφέρουν άμεσα οτιδήποτε δουν ή τους κινήσει την υποψία στον κατάλληλο εκπρόσωπο του οργανισμού. Επιπλέον, ο οργανισμός θα πρέπει να έχει σε ισχύ τις κατάλληλες διαδικασίες για την αντιμετώπιση υπαλλήλων που παραβιάζουν την ασφάλεια του. Για την κατάλληλη αντιμετώπιση τέτοιων συμβάντων, θα πρέπει να συλλέγονται και όλα τα αποδεικτικά στοιχεία (παράγραφος 12.1.7).

6.3.1 Αναφορά συμβάντων

Τα συμβάντα που σχετίζονται με την ασφάλεια του οργανισμού θα πρέπει να αναφέρονται, το συντομότερο, μέσω των κατάλληλων διαύλων επικοινωνίας του οργανισμού. Θα πρέπει να υπάρχει συγκεκριμένη διαδικασία αναφοράς συμβάντων. Σε συνδυασμό με τις διαδικασίες αντιμετώπισης, θα είναι δυνατή η κατάστρωση ενός σχεδίου για την αντιμετώπιση ενός συμβάντος. Όλοι οι υπάλληλοι θα πρέπει να γνωρίζουν τις συγκεκριμένες διαδικασίες και θα πρέπει να τις χρησιμοποιούν άμεσα σε περίπτωση προβλήματος με την ασφάλεια. Επιπλέον θα πρέπει να γίνεται και ενημέρωση των χρηστών για τα αποτελέσματα των αναφορών τους, τις αιτίες των αναφερθέντων προβλημάτων και πως μπορούν να αποφευχθούν στο μέλλον (παράγραφος 12.1.7).

6.3.2 Αναφορά αδυναμιών ασφάλειας

Οι χρήστες του πληροφοριακού συστήματος θα πρέπει να αναφέρουν κάθε αδυναμία ή πιθανή απειλή του συστήματος την οποία παρατηρούν ή υποπτεύονται. Η αναφορά θα πρέπει να γίνεται απευθείας στη διοίκηση ή στον παροχέα της υπηρεσίας που χρησιμοποιούν. Οι χρήστες σε καμία περίπτωση δε θα πρέπει να επιδεικνύουν κάποια πιθανή αδυναμία του

συστήματος, γιατί κάτι τέτοιο μπορεί να ερμηνευθεί ως πιθανή υποβοήθηση εκδήλωσης επίθεση στο σύστημα.

6.3.3 Αναφορά δυσλειτουργιών των εφαρμογών

Θα πρέπει να υπάρχουν διαδικασίες για την αναφορά πιθανών δυσλειτουργιών των εφαρμογών που χρησιμοποιούνται στον οργανισμό. Μια τέτοια αναφορά μπορεί να περιλαμβάνει τα ακόλουθα:

- Τα συμπτώματα του προβλήματος και μηνύματα που πιθανόν παρουσιάζονται.
- Αν είναι δυνατόν, ο υπολογιστής θα πρέπει να απομονώνεται ή ακόμα και να διακόπτεται η λειτουργία του. Αν πρόκειται να εξεταστεί εξοπλισμός, θα πρέπει να αποσυνδέεται από το δίκτυο του οργανισμού. Επιπλέον, δισκέτες και CDs δε θα πρέπει να μεταφέρονται σε άλλους υπολογιστές.
- Το θέμα θα πρέπει να αναφέρεται αμέσως στον υπεύθυνο ασφάλειας του οργανισμού.

Οι χρήστες σε καμία περίπτωση δε θα πρέπει να επιχειρούν την απεγκατάσταση της προβληματικής εφαρμογής, εκτός αν έχουν απαραίτητη εξουσιοδότηση. Εξειδικευμένο προσωπικό θα πρέπει να αναλαμβάνει την αποκατάσταση της σωστής λειτουργίας.

6.3.4 Μαθαίνοντας από συμβάντα

Θα πρέπει να υπάρχουν μηχανισμοί μέσω των οποίων θα γίνεται η αποτίμηση και ο έλεγχος των διάφορων συμβάντων. Αυτή η πληροφορία θα πρέπει να χρησιμοποιείται για την αναγνώριση επαναλαμβανόμενων συμβάντων. Η παρουσία τους μπορεί να δείξει την αναγκαιότητα νέων μέσων προστασίας ή την αναπροσαρμογή της πολιτικής ασφάλειας του οργανισμού.

6.3.5 Πειθαρχικές διαδικασίες

Ο οργανισμός θα πρέπει να έχει και ένα σύνολο πειθαρχικών διαδικασιών μέσω των οποίων – σύμφωνα με το νόμο - θα τιμωρούνται οι υπάλληλοι που έχουν παραβιάσει τους κανονισμούς ασφάλειας. Θα πρέπει, όμως, ταυτόχρονα να διασφαλίζουν την ίση και δίκαιη μεταχείριση των υπαλλήλων που είναι ύποπτοι για τη διενέργεια σοβαρών πράξεων κατά της ασφάλειας του οργανισμού.

7. Φυσική και περιβαλλοντολογική ασφάλεια

7.1 Ασφαλείς περιοχές

Σκοπός είναι η αποτροπή μη εξουσιοδοτημένης πρόσβασης στις εγκαταστάσεις και το πληροφοριακό σύστημα του οργανισμού. Οι κρίσιμης σημασίας εγκαταστάσεις επεξεργασίας δεδομένων θα πρέπει να βρίσκονται σε ασφαλείς περιοχές, προστατευμένες από μια περίμετρο ασφάλειας και από τους κατάλληλους μηχανισμούς. Θα πρέπει να προστατεύονται φυσικά από μη εξουσιοδοτημένη πρόσβαση, παρεμβολές και καταστροφή. Η παρεχόμενη προστασία θα πρέπει να είναι ανάλογη των κινδύνων.

7.1.1 Περίμετρος φυσικής ασφάλειας

Η φυσική προστασία μπορεί να επιτευχθεί με τη δημιουργία φυσικών εμποδίων γύρω από τις εγκαταστάσεις του οργανισμού. Το καθένα από τα εμπόδια δημιουργεί και μια ζώνη περιμετρικής ασφάλειας, αυξάνοντας με αυτόν τον τρόπο τη συνολική ασφάλεια. Ο οργανισμός θα πρέπει να χρησιμοποιεί ζώνες ασφάλειας για την προστασία των χώρων που στεγάζουν το πληροφοριακό σύστημά του (παράγραφος 7.1.3). Η περίμετρος ασφάλειας λειτουργεί ως εμπόδιο, όπως ένας τοίχος, μια πόρτα με ηλεκτρονική κλειδαριά ή ένα γραφείο ελέγχου. Η τοποθέτηση και οι δυνατότητες του κάθε εμποδίου προκύπτουν από τη διαδικασία αποτίμησης κινδύνου.

Θα πρέπει να εξεταστούν οι ακόλουθες αρχές και μηχανισμοί:

- Η περίμετρος ασφάλειας θα πρέπει να είναι σαφώς καθορισμένη.
- Η περίμετρος ενός κτιρίου ή ενός site το οποίο στεγάζει τμήματα του πληροφοριακού συστήματος, θα πρέπει να είναι συμπαγής, δηλαδή να μην έχει κενά μέσω των οποίων θα είναι εύκολη κάποια παραβίαση. Οι εξωτερικοί τοίχοι θα πρέπει να είναι συμπαγείς και όλες οι εξωτερικές πόρτες θα πρέπει να είναι κατάλληλα προστατευμένες από μη εξουσιοδοτημένη προσπέλαση. Για αυτό το σκοπό μπορούν να χρησιμοποιηθούν συστήματα συναγερμού, μπάρες, ηλεκτρονικές κλειδαριές κλπ.

- Θα πρέπει να υπάρχει ένας μηχανισμός μέσω του οποίου θα ελέγχεται η φυσική πρόσβαση στο κτίριο. Αυτό μπορεί να γίνει με τη χρήση ενός γραφείου υποδοχής με φρουρούς. Η πρόσβαση στους διάφορους χώρους θα πρέπει να επιτρέπεται μόνο στο εξουσιοδοτημένο προσωπικό.

- Όπου κρίνεται απαραίτητο θα πρέπει να χρησιμοποιηθούν ειδικές μπάρες οι οποίες θα καλύπτουν όλο το χώρο από το πάτωμα έως και το ταβάνι. Με αυτόν τον τρόπο θα είναι δυνατός και ο έλεγχος φωτιάς ή πλημμύρας.

- Όλες οι πυρασφαλείς πόρτες της περιμέτρου θα πρέπει να έχουν συναγερμό και να κλείνουν εντελώς.

7.1.2 Έλεγχος εισόδου

Οι ασφαλείς περιοχές θα πρέπει να προστατεύονται από τους κατάλληλους μηχανισμούς, ώστε να επιτρέπεται η πρόσβαση μόνο σε εξουσιοδοτημένα άτομα. Θα πρέπει να εξεταστούν τα ακόλουθα:

- Οι επισκέπτες σε ασφαλείς περιοχές θα πρέπει να επιβλέπονται. Θα πρέπει να καταγράφεται η ακριβής ημερομηνία και ώρα εισόδου και εξόδου. Επιπλέον, θα πρέπει να τους επιτρέπεται η πρόσβαση μόνο όπου είναι απαραίτητο, ενώ θα πρέπει να τους παρέχονται οδηγίες σχετικά με τις απαιτήσεις ασφάλειας του χώρου και τις διαδικασίες που θα πρέπει να ακολουθήσουν σε περίπτωση ανάγκης.

- Η πρόσβαση σε ευαίσθητες πληροφορίες, όπως και στο πληροφοριακό σύστημα, θα πρέπει να ελέγχεται και να επιτρέπεται μόνο σε εξουσιοδοτημένο προσωπικό. Μηχανισμοί αυθεντικοποίησης (π.χ. αναγνώστες μαγνητικών καρτών και χρήση PIN) θα πρέπει να χρησιμοποιούνται για τον έλεγχο της πρόσβασης και την τήρηση σχετικών αρχείων. Θα πρέπει να προστατεύονται και τα αρχεία αυτά.

- Το προσωπικό θα πρέπει να φέρει σε εμφανές σημείο κάποιου είδους τεκμήριο ταυτοποίησης.

- Τα δικαιώματα προσπέλασης θα πρέπει να ελέγχονται ανά τακτά χρονικά διαστήματα.

7.1.3 Ασφάλεια γραφείων, δωματίων και εγκαταστάσεων

Μια ασφαλής περιοχή μπορεί να είναι ένα κλειδωμένο γραφείο ή πολλά δωμάτια μέσα σε μια περίμετρο ασφάλειας, τα οποία μπορούν να είναι κλειδωμένα ή να περιέχουν κλειδωμένα χρηματοκιβώτια ή φοριαμούς. Η επιλογή και ο σχεδιασμός μιας ασφαλούς περιοχής θα πρέπει να λαμβάνει υπόψη τα ενδεχόμενα φωτιάς, πλημμύρας, έκρηξης, ταραχών και άλλου είδους καταστροφές που μπορούν να προκληθούν από φυσικά πρόσωπα. Θα πρέπει επίσης να ικανοποιεί και τους σχετικούς κανονισμούς εργασιακής ασφάλειας και υγιεινής. Προσοχή θα πρέπει να δοθεί και στις ζημιές που μπορούν να προκληθούν από γειτονικούς χώρους, όπως διαρροή νερού από γειτονικό κτίσμα.

Θα πρέπει να εξεταστούν τα ακόλουθα:

- Το κοινό δε θα πρέπει να έχει πρόσβαση σε σημαντικού χαρακτήρα εγκαταστάσεις.
- Τα κτίρια δε θα πρέπει να φέρουν εξωτερικές ενδείξεις που να προδίδουν τη χρήση τους.
- Συμπληρωματικές υπηρεσίες και εξοπλισμός (π.χ. φωτοαντιγραφικά, συσκευές fax κλπ.), θα πρέπει επίσης να προστατεύονται κατάλληλα ώστε να μην μπορούν να χρησιμοποιηθούν για την υποκλοπή ή έκθεση πληροφοριών και δεδομένων.
- Πόρτες και παράθυρα θα πρέπει να είναι κλειδωμένα. Επιπλέον προστασία χρειάζονται τα εξωτερικά παράθυρα που βρίσκονται κοντά στο έδαφος.
- Θα πρέπει να λειτουργούν κατάλληλου τύπου μηχανισμοί ανίχνευσης εισβολέων, οι οποίοι θα πρέπει να ελέγχονται συχνά για την καλή τους λειτουργία. Η παρουσία ατόμου σε κανονικά κενούς χώρους θα πρέπει να ελέγχεται αμέσως.
- Οι χώροι που στεγάζουν το πληροφοριακό σύστημα του οργανισμού θα πρέπει να είναι ξεχωριστοί από τους χώρους που στεγάζουν εξοπλισμό τρίτων εξωτερικών συνεργατών.
- Το κοινό δε θα πρέπει να έχει πρόσβαση σε καταλόγους εσωτερικών τηλεφώνων ή χώρων.
- Επικίνδυνα υλικά θα πρέπει να φυλάσσονται μακριά από την ασφαλή περιοχή. Επιπλέον, όλα τα υλικά θα πρέπει να φυλάσσονται στην ασφαλή περιοχή μόνον όταν είναι απαραίτητο.

- Εφεδρικός εξοπλισμός και υλικά θα πρέπει να βρίσκονται σε απόσταση από το κύριο site και να προστατεύονται επαρκώς.

7.1.4 Εργασία σε ασφαλείς περιοχές

Μια ασφαλής περιοχή απαιτεί την ύπαρξη επιπλέον μηχανισμών ελέγχου και προστασίας, τόσο για το προσωπικό του οργανισμού όσο και για τους εξωτερικούς συνεργάτες. Θα πρέπει να εξεταστούν τα ακόλουθα:

- Το προσωπικό θα πρέπει να είναι ενήμερο για τις εργασίες τρίτων μέσα στην ασφαλή περιοχή.

- Οι εργασίες μέσα στην ασφαλή περιοχή θα πρέπει να επιβλέπονται, τόσο για λόγους ασφάλειας, όσο και για την πρόληψη ατυχημάτων.

- Οι κενοί χώροι μέσα στην ασφαλή περιοχή θα πρέπει να είναι κλειδωμένοι και να ελέγχονται περιοδικά.

- Οι εξωτερικοί συνεργάτες θα πρέπει να έχουν περιορισμένη πρόσβαση και μόνον όταν είναι απαραίτητο. Θα πρέπει να επιβλέπονται συνεχώς. Επιπλέον θα πρέπει να υπάρχουν ειδικά μέτρα προστασίας ανάμεσα σε περιοχές με διαφορετικά επίπεδα ασφάλειας μέσα στην προστατευόμενη περιοχή.

- Φωτογραφίες, βιντεοσκόπηση ή μαγνητοφώνηση θα πρέπει να απαγορεύονται μέσα στην προστατευόμενη περιοχή, εκτός και αν υπάρχει ειδική εξουσιοδότηση.

7.1.5 Απομονωμένες περιοχές φορτοεκφόρτωσης

Η παράδοση και η φορτοεκφόρτωση υλικών θα πρέπει να ελέγχεται και αν είναι δυνατό να γίνεται σε χώρους απομονωμένους από αυτούς που στεγάζουν τα πληροφοριακά συστήματα. Για τις απαιτήσεις ασφάλειας τέτοιων χώρων θα πρέπει να γίνεται αποτίμηση κινδύνου. Θα πρέπει να εξεταστούν τα ακόλουθα:

- Η προσπέλαση σε αποθηκευτικούς χώρους θα πρέπει να περιορίζεται σε εξουσιοδοτημένα πρόσωπα.

- Οι αποθηκευτικοί χώροι θα πρέπει να είναι έτσι σχεδιασμένοι ώστε μέσω αυτών να μην είναι δυνατή η πρόσβαση στο υπόλοιπο κτίριο.

- Οι εξωτερικές πόρτες των αποθηκευτικών χώρων θα πρέπει να είναι κλειστές προτού ανοίξουν οι εσωτερικές.

- Τα εισερχόμενα υλικά θα πρέπει να ελέγχονται πριν αποθηκευτούν ή πριν μετακινηθούν προς το χώρο στον οποίο θα χρησιμοποιηθούν.

- Τα εισερχόμενα υλικά θα πρέπει να καταγράφονται κατά την είσοδό τους στην ασφαλή περιοχή.

7.2 Ασφάλεια εξοπλισμού

Σκοπός είναι η πρόληψη απώλειας, ζημιών, έκθεσης των πόρων του οργανισμού και της διακοπής των επιχειρησιακών δραστηριοτήτων του οργανισμού. Ο εξοπλισμός θα πρέπει να προστατεύεται φυσικά από κινδύνους ασφάλειας και περιβαλλοντολογικές απειλές. Η προστασία του εξοπλισμού είναι απαραίτητη προκειμένου να ελαχιστοποιηθεί ο κίνδυνος μη εξουσιοδοτημένης προσπέλασης των δεδομένων, όπως και η προστασία απέναντι στο ενδεχόμενο απώλειας ή καταστροφής. Θα πρέπει επίσης να ληφθούν ειδικά μέτρα προστασίας σχετικά με την υποδομή καλωδίωσης και την παροχή ρεύματος.

7.2.1 Τοποθέτηση και προστασία εξοπλισμού

Ο εξοπλισμός θα πρέπει να τοποθετείται και να προστατεύεται έτσι ώστε να ελαχιστοποιηθούν οι περιβαλλοντολογικοί κίνδυνοι και η μη εξουσιοδοτημένη πρόσβαση. Θα πρέπει να εξεταστούν τα ακόλουθα:

- Ο εξοπλισμός θα πρέπει να είναι έτσι τοποθετημένος ώστε να χρειάζεται μόνον η απολύτως απαραίτητη πρόσβαση στο χώρο.

- Ο εξοπλισμός επεξεργασίας δεδομένων θα πρέπει να προστατεύεται από την κοινή θέα.

- Αντικείμενα που απαιτούν ειδική προστασία θα πρέπει να είναι απομονωμένα κατά το δυνατό.

- Θα πρέπει να υπάρχουν μέτρα προστασίας απέναντι σε κλοπή, φωτιά, εκρήξεις, καπνό, νερό, σκόνη, δονήσεις, χημικά, ηλεκτρομαγνητική ακτινοβολία και παρεμβολές στην παροχή ηλεκτρικής ενέργειας.

- Θα πρέπει να υπάρχουν περιορισμοί σχετικά με την κατανάλωση φαγητού και ποτού κοντά στους χώρους με εξοπλισμό.

- Θα πρέπει να παρακολουθούνται οι συνθήκες του περιβάλλοντος (θερμοκρασία και υγρασία).

- Θα πρέπει να χρησιμοποιούνται προστατευτικά (όπως καλύμματα πληκτρολογίων) όπου είναι απαραίτητο.

- Θα πρέπει να προστατεύεται επαρκώς ο χώρος ώστε να μη μεταδοθούν σε αυτόν προβλήματα από γειτονικούς χώρους.

7.2.2 Παροχή ρεύματος

Ο εξοπλισμός θα πρέπει να προστατεύεται από διακοπές ρεύματος ή οποιοδήποτε άλλο πρόβλημα στην παροχή. Οι υπάρχουσες επιλογές περιλαμβάνουν:

- Πολλαπλές παροχές ώστε να μην υπάρχει ένα κεντρικό σημείο που να μπορεί να δημιουργήσει πρόβλημα (single point of failure).

- Χρήση UPS (Uninterruptible Power Supply).

- Εφεδρική γεννήτρια ρεύματος.

Η χρήση UPS συνιστάται ιδιαίτερα για την υποστήριξη συστημάτων κρίσιμης σημασίας. Επιπλέον θα πρέπει να υπάρχουν σχέδια αντιμετώπισης ενδεχόμενης βλάβης του ίδιου του UPS. Παράλληλα θα πρέπει να γίνεται τακτικός έλεγχος της λειτουργίας των UPS για να επιβεβαιωθεί τόσο η σωστή λειτουργία τους, όσο και η ικανότητά τους να αντεπεξέλθουν στις απαιτήσεις του οργανισμού.

Η χρήση εφεδρικής γεννήτριας θα πρέπει να εξεταστεί στην περίπτωση που είναι απαραίτητη η λειτουργία του εξοπλισμού ακόμα και στην περίπτωση γενικευμένης διακοπής ρεύματος. Θα πρέπει να είναι πάντοτε εφοδιασμένη με καύσιμα και να συντηρείται σωστά.

Επιπλέον θα πρέπει να χρησιμοποιείται εφεδρικός φωτισμός σε όλες τις εξόδους και τους χώρους όπου στεγάζεται εξοπλισμός. Με αυτόν τον τρόπο θα είναι δυνατό το κλείσιμο των συστημάτων στην περίπτωση γενικευμένης διακοπής ρεύματος. Θα πρέπει επίσης όλοι οι χώροι να προστατεύονται από κεραυνούς.

7.2.3 Ασφάλεια καλωδίωσης

Τα καλώδια παροχής ρεύματος, τηλεπικοινωνιών και μεταφοράς δεδομένων θα πρέπει να προστατεύονται από καταστροφή και υποκλοπή. Θα πρέπει να εξεταστούν τα ακόλουθα:

- Οι παροχές ρεύματος και τηλεπικοινωνιών θα πρέπει να έρχονται στους προστατευόμενους χώρους υπόγεια ή αν αυτό δεν είναι δυνατό, να προστατεύονται κατάλληλα.
- Η δικτυακή καλωδίωση θα πρέπει να προστατεύεται από υποκλοπή και να μη διέρχεται από κανάλια όπου έχουν πρόσβαση τυχαία πρόσωπα.
- Οι καλωδιώσεις ρεύματος και δεδομένων πρέπει να είναι σε απόσταση μεταξύ τους ώστε να μην υπάρχουν παρεμβολές.
- Για κρίσιμης σημασίας συστήματα, μπορούν να ληφθούν επιπλέον μέτρα προστασίας όπως εναλλακτικά μέσα μετάδοσης και οπτικών ινών, εγκατάσταση θωρακισμένων κουτιών τερματισμού καλωδίωσης, περιοδικοί έλεγχοι για εντοπισμό συσκευών υποκλοπής κλπ.

7.2.4 Συντήρηση εξοπλισμού

Όλος ο εξοπλισμός θα πρέπει να συντηρείται κατάλληλα προκειμένου να διασφαλιστεί η απρόσκοπτη και αδιάλειπτη λειτουργία του. Θα πρέπει να εξεταστούν τα ακόλουθα

- Ο εξοπλισμός θα πρέπει να συντηρείται σύμφωνα με τις οδηγίες του κατασκευαστή.

- Μόνο εξουσιοδοτημένοι τεχνικοί θα πρέπει να συντηρούν και να επισκευάζουν τον εξοπλισμό.

- Θα πρέπει να τηρείται το ιστορικό συντήρησης και επισκευών.

- Θα πρέπει να υπάρχουν κατάλληλες διαδικασίες για την αποστολή του εξοπλισμού σε τρίτους προκειμένου να γίνει συντήρηση ή επισκευή.

7.2.5 Ασφάλεια εξοπλισμού εκτός των χώρων του οργανισμού

Η χρήση εξοπλισμού εκτός των χώρων του οργανισμού θα πρέπει να έχει προηγούμενη έγκριση από τη διοίκηση. Η παρεχόμενη ασφάλεια θα πρέπει να είναι ανάλογη με αυτή που έχει ο οργανισμός στους δικούς του χώρους. Η απαίτηση αυτή περιλαμβάνει κάθε είδους εξοπλισμό ο οποίος μεταφέρεται εκτός του οργανισμού για χρήση, συντήρηση ή επισκευή. Θα πρέπει να προσεχθούν τα ακόλουθα:

- Εξοπλισμός και αποθηκευτικά μέσα που μεταφέρονται εκτός των χώρων του οργανισμού, δεν πρέπει να εκτίθενται σε δημόσια μέρη. Οι φορητοί υπολογιστές θα πρέπει να μεταφέρονται με ειδική βαλίτσα, και κατά το δυνατόν να μη φαίνονται κατά το ταξίδι.

- Θα πρέπει να ακολουθούνται πιστά οι οδηγίες του κατασκευαστή για την προστασία του εξοπλισμού (π.χ. έκθεση σε ηλεκτρομαγνητική ακτινοβολία, συνθήκες μεταφοράς κλπ.).

- Θα πρέπει να γίνεται αποτίμηση κινδύνου για το προσωπικό που δουλεύει από το σπίτι του και να υπάρχουν και εκεί οι κατάλληλοι μηχανισμοί προστασίας.

- Θα πρέπει να ασφαλίζεται ο εξοπλισμός και το συμβόλαιο να καλύπτει και τη μεταφορά του εκτός του οργανισμού.

Διάφοροι κίνδυνοι, όπως υποκλοπή, είναι πολύ πιθανοί κατά τη μεταφορά του εξοπλισμού από μια τοποθεσία σε άλλη. Κατά συνέπεια θα πρέπει να λαμβάνονται όλα τα απαραίτητα μέτρα προστασίας (παράγραφος 9.8.1).

7.2.6 Ασφαλής καταστροφή ή επαναχρησιμοποίηση εξοπλισμού

Οι πληροφορίες μπορούν να εκτεθούν σε υποκλοπή όταν δε γίνεται σωστή καταστροφή ή επαναχρησιμοποίηση του εξοπλισμού (παράγραφος 8.6.2). Τα αποθηκευτικά μέσα που περιέχουν ευαίσθητες πληροφορίες θα πρέπει να καταστρέφονται φυσικά ή να επαναγράφονται με ειδικό τρόπο, αντί απλά να διαγράφονται.

Επιπλέον, όλα τα αποθηκευτικά μέσα θα πρέπει να ελέγχονται για την ύπαρξη ευαίσθητων πληροφοριών ή λογισμικού και να καταστρέφονται ή να διαγράφονται ανάλογα. Η διενέργεια αποτίμησης κινδύνου μπορεί να απαιτείται σε ειδικές περιπτώσεις προκειμένου να καθοριστεί αν τα υλικά αυτά θα πρέπει να πεταχτούν, να καταστραφούν ή να επισκευαστούν.

7.3 Γενικοί μηχανισμοί προστασίας

Σκοπός είναι η αποτροπή υποκλοπής ή και κλοπής των πληροφοριών ή τμήματος των εγκαταστάσεων του οργανισμού. Οι πληροφορίες και οι εγκαταστάσεις επεξεργασίας τους θα πρέπει να προστατεύονται από κλοπή, επέμβαση από μη εξουσιοδοτημένα πρόσωπα ή υποκλοπή. Διαδικασίες χειρισμού και αποθήκευσης εξετάζονται στην παράγραφο 8.6.3.

7.3.1 Πολιτική προστασίας πληροφοριών στο γραφείο

Ο οργανισμός θα πρέπει να ακολουθεί μια πολιτική προστασίας των πληροφοριών που μπορεί να είναι εκτεθειμένες στα γραφεία του προσωπικού. Η συγκεκριμένη πολιτική θα πρέπει να περιλαμβάνει τις κατηγορίες προστασίας των πληροφοριών (παράγραφος 5.2) και τους αντίστοιχους κινδύνους.

Οι πληροφορίες που είναι εκτεθειμένες στα γραφεία του προσωπικού μπορούν εκτός από το να κλαπούν, να καταστραφούν από φωτιά, πλημμύρα ή έκρηξη. Ο οργανισμός θα πρέπει να εξετάσει τα ακόλουθα:

- Όταν κρίνεται απαραίτητο, χαρτιά και αποθηκευτικά μέσα όταν δε χρησιμοποιούνται θα πρέπει να φυλάσσονται σε κατάλληλα ντουλάπια ή φοριαμούς, ειδικά μετά τη λήξη του ωραρίου εργασίας.

- Οτιδήποτε περιέχει ευαίσθητες πληροφορίες θα πρέπει να φυλάσσεται σε ειδικά ντουλάπια ή χρηματοκιβώτια ανθεκτικά στη φωτιά.

- Οι χρήστες δε θα πρέπει να αφήνουν τους υπολογιστές τους ή τα τερματικά τους συνδεδεμένα, ενώ ο εξοπλισμός θα πρέπει να προστατεύεται με ειδικές κλειδαριές όταν δε χρησιμοποιείται.

- Οι μηχανές telex, fax όπως και τα φωτοαντιγραφικά θα πρέπει να προστατεύονται.

- Οι εκτυπώσεις που περιέχουν ευαίσθητες πληροφορίες θα πρέπει να απομακρύνονται αμέσως από τους εκτυπωτές.

7.3.2 Απομάκρυνση εξοπλισμού

Εξοπλισμός, λογισμικό και πληροφορία σε κάθε μορφή δε θα πρέπει να απομακρύνεται από τις εγκαταστάσεις του οργανισμού χωρίς την κατάλληλη εξουσιοδότηση. Επιπλέον, θα πρέπει να καταγράφονται όλες οι μετακινήσεις των παραπάνω, ενώ σε τακτά χρονικά διαστήματα θα πρέπει να γίνονται απογραφές του εξοπλισμού.

8. Λειτουργίες του οργανισμού και επικοινωνίες

8.1 Διαδικασίες λειτουργίας και καθήκοντα

Σκοπός είναι η σωστή και ασφαλής λειτουργία του πληροφοριακού συστήματος του οργανισμού. Τα καθήκοντα και οι διαδικασίες για τη διαχείριση και τη λειτουργία του πληροφοριακού συστήματος θα πρέπει να είναι σαφώς καθορισμένα. Επιπλέον θα πρέπει να περιλαμβάνονται ειδικές διαδικασίες στην περίπτωση κάποιου συμβάντος που να απειλεί την ασφάλεια του συστήματος. Ο οργανισμός θα πρέπει να υιοθετήσει το διαχωρισμό των καθηκόντων όπου είναι δυνατό (παράγραφος 8.1.4), ώστε να ελαχιστοποιηθεί ο κίνδυνος κακής χρήσης του συστήματος, είτε από αμέλεια είτε από δόλο.

8.1.1 Καταγραφή διαδικασιών λειτουργίας

Οι διαδικασίες που σχετίζονται με τη λειτουργία του συστήματος και αναφέρονται στην πολιτική ασφάλειας του οργανισμού, θα πρέπει να είναι αναλυτικά καταγεγραμμένες. Θα πρέπει να θεωρούνται επίσημα έγγραφα του οργανισμού, ενώ οποιαδήποτε αλλαγή σε αυτά θα πρέπει να εγκρίνεται από τη διοίκηση.

Οι διαδικασίες αυτές θα πρέπει να περιγράφουν τις αναλυτικές οδηγίες εκτέλεσης όλων των εργασιών συμπεριλαμβανομένων των ακολούθων:

- διαχείριση και επεξεργασία πληροφοριών,
- χρονοδιαγράμματα εκτέλεσης εργασιών και ειδικά τη σχέση της κάθε εργασίας με άλλες, όπως και τους χρόνους ολοκλήρωσής της,
- οδηγίες για την αντιμετώπιση λαθών που μπορεί να προκύψουν κατά τη λειτουργία του συστήματος,
- συμβόλαια υποστήριξης για τον εξοπλισμό,
- οδηγίες χειρισμού ειδικού εξοπλισμού ή ευαίσθητων πληροφοριών,

- διαδικασίες επανεκκίνησης ή επαναφοράς του συστήματος στην περίπτωση κάποιου προβλήματος.

Θα πρέπει να είναι καταγεγραμμένες και οι διαδικασίες καθημερινής χρήσης του συστήματος, όπως εκκίνηση και τερματισμός λειτουργίας, τακτική συντήρηση, εφεδρική λήψη αντιγράφων κλπ.

8.1.2 Έλεγχος αλλαγών

Οι αλλαγές στο πληροφοριακό σύστημα του οργανισμού θα πρέπει να ελέγχονται, καθώς αποτελούν αρκετά συχνά αιτία προβλημάτων. Θα πρέπει να υπάρχουν επίσημες διαδικασίες και καθήκοντα, μέσω των οποίων θα ελέγχονται όλες οι αλλαγές σε εξοπλισμό, λογισμικό και διαδικασίες στο σύστημα. Θα πρέπει να τηρούνται αναλυτικά αρχεία με τις αλλαγές του συστήματος. Επειδή συχνά οι αλλαγές στον εξοπλισμό επηρεάζουν και τη λειτουργία των εφαρμογών, απαιτείται ιδιαίτερη προσοχή. Θα πρέπει να εξεταστούν οι ακόλουθοι μηχανισμοί:

- αναλυτική καταγραφή όλων των σημαντικών αλλαγών,
- έλεγχος των πιθανών συνεπειών τέτοιων αλλαγών,
- επίσημη διαδικασία έγκρισης των προτεινόμενων αλλαγών,
- κοινοποίηση όλων των σχετικών λεπτομερειών στα αρμόδια στελέχη του οργανισμού,
- διαδικασίες επαναφοράς του συστήματος στην περίπτωση ανεπιτυχών αλλαγών.

8.1.3 Διαδικασίες αντιμετώπισης συμβάντων

Ο οργανισμός θα πρέπει να ακολουθεί και συγκεκριμένες διαδικασίες αντιμετώπισης συμβάντων, ώστε να δρα έγκαιρα όταν απειλείται η ασφάλεια του συστήματος. Θα πρέπει να εξεταστούν τα ακόλουθα:

- Η ύπαρξη διαδικασιών για την αντιμετώπιση όλων των πιθανών απειλών κατά της ασφάλειας του συστήματος, όπως βλάβη, λάθη από ακατάλληλα δεδομένα, έκθεση της εμπιστευτικότητας, επιθέσεις τύπου άρνησης παροχής υπηρεσιών κλπ.

- Εκτός από την ύπαρξη σχεδίων για τη συνέχεια των λειτουργιών του οργανισμού σε περίπτωση καταστροφής, θα πρέπει να υπάρχουν διαδικασίες που να καλύπτουν την ανάλυση των αιτίων του προβλήματος που παρουσιάστηκε, τους τρόπους με τους οποίους μπορεί να αποτραπεί στο μέλλον το ίδιο πρόβλημα, συλλογή όλων των σχετικών στοιχείων, την επικοινωνία με όσους επηρεάζονται από το πρόβλημα και την αναφορά του προβλήματος στα κατάλληλα πρόσωπα ή αρχές.

- Η συλλογή στοιχείων σχετικών με το πρόβλημα, τόσο για ιδία χρήση από τον οργανισμό, όσο και για τη διεκδίκηση αποζημιώσεων από προμηθευτές ή την ενημέρωση των αρχών.

- Η αναλυτική καταγραφή των ενεργειών αποκατάστασης των λειτουργιών ύστερα από κάποιο πρόβλημα, όπως και τους απαραίτητους ελέγχους για τη σωστή αποκατάσταση όλων των λειτουργιών, καθώς και τις σχετικές αναφορές στη διοίκηση.

8.1.4 Διαχωρισμός καθηκόντων

Ο διαχωρισμός των καθηκόντων είναι μια μέθοδος για τη μείωση του κινδύνου κατάχρησης του συστήματος, είτε από αμέλεια είτε από δόλο. Ο διαχωρισμός των καθηκόντων διαχείρισης ή εκτέλεσης διάφορων επιχειρηματικών λειτουργιών είναι επίσης ένας μηχανισμός που θα πρέπει να εξεταστεί από τον οργανισμό προκειμένου να ελαχιστοποιηθούν οι πιθανότητες κατάχρησης ή μη εξουσιοδοτημένων αλλαγών στα δεδομένα ή τις υπηρεσίες.

Οι οργανισμοί με μικρό μέγεθος μπορεί να έχουν προβλήματα στην υλοποίηση μιας τέτοιας πρακτικής, αλλά όπου είναι δυνατό θα πρέπει να το ακολουθούν. Όπου είναι δύσκολος ο διαχωρισμός των καθηκόντων, θα πρέπει να υπάρχει επίβλεψη από τη διοίκηση, ενώ σε κάθε περίπτωση όλοι οι έλεγχοι θα πρέπει να γίνονται από άτομα που δεν παίρνουν μέρος στην εκτέλεση των υπό έλεγχο λειτουργιών.

Θα πρέπει να ληφθεί ειδική μέριμνα ώστε κανένας να μην μπορεί να διενεργήσει απάτη, μόνος του, χωρίς να γίνει αντιληπτός. Η εξουσιοδότηση κάποιας ενέργειας και η εκτέλεσή της θα πρέπει να γίνονται από διαφορετικά άτομα. Θα πρέπει να εξετασθούν τα ακόλουθα:

- Θα πρέπει να υπάρχει διαχωρισμός των καθηκόντων όπου είναι απαραίτητη η συνεργασία για τον εντοπισμό απάτης, όπως στην περίπτωση παραγγελίας και παραλαβής αγαθών.

- Αν υπάρχει κίνδυνος συγκάλυψης, θα πρέπει να υπάρχουν μηχανισμοί που να εμπλέκουν πολλά άτομα ώστε να μειωθεί ο κίνδυνος τέτοιων συνεργασιών .

8.1.5 Διαχωρισμός των εγκαταστάσεων δοκιμών και λειτουργιών

Ο διαχωρισμός της ανάπτυξης, των δοκιμών και της λειτουργίας του συστήματος είναι απαραίτητος για το διαχωρισμό των απαιτούμενων ρόλων. Θα πρέπει επίσης να υπάρχουν κανόνες με βάση τους οποίους θα καθίστανται πλήρως λειτουργικές οι εφαρμογές του συστήματος.

Η ανάπτυξη και οι δοκιμές εφαρμογών μπορούν να προκαλέσουν μεγάλα προβλήματα στο πληροφοριακό σύστημα του οργανισμού. Είναι λοιπόν απαραίτητη η ύπαρξη διαχωρισμού ανάμεσα στα περιβάλλοντα ανάπτυξης, δοκιμών και παραγωγής. Ο διαχωρισμός ανάμεσα στην ανάπτυξη και τις δοκιμές βοηθά στον αποτελεσματικότερο έλεγχο των εφαρμογών, αφού οι όποιες δοκιμές θα μπορούν να γίνουν σε ένα αρκετά σταθερό περιβάλλον.

Όταν το προσωπικό ανάπτυξης και δοκιμών έχει πρόσβαση στο περιβάλλον παραγωγής, είναι δυνατό να προκαλέσουν προβλήματα στην ομαλή λειτουργία του συστήματος. Τα προβλήματα αυτά μπορούν να φτάσουν μέχρι και τη διενέργεια απάτης ή την εισαγωγή κακόβουλων προγραμμάτων στο σύστημα. Μπορούν να αποτελέσουν απειλή και κατά της εμπιστευτικότητας των δεδομένων του οργανισμού.

Για την προστασία του συστήματος παραγωγής, ο οργανισμός θα πρέπει να εξετάσει τα ακόλουθα:

- Οι εφαρμογές που είναι σε φάση ανάπτυξης η δοκιμών θα πρέπει να τρέχουν σε ξεχωριστά συστήματα από αυτό των παραγωγικών λειτουργιών.

- Η ανάπτυξη και οι δοκιμές των εφαρμογών θα πρέπει να είναι όσο το δυνατό πιο πολύ διαχωρισμένες.

- Τα εργαλεία ανάπτυξης λογισμικού δε θα πρέπει να είναι προσπελάσιμα από τα παραγωγικά συστήματα.

- Θα πρέπει να υπάρχουν διαφορετικές διαδικασίες login στα συστήματα παραγωγής, τα συστήματα δοκιμών και τα συστήματα ανάπτυξης.

- Το προσωπικό ανάπτυξης θα πρέπει να έχει πρόσβαση μόνο στα απολύτως απαραίτητα μέρη των συστημάτων παραγωγής, στα οποία και θα πρέπει να υπάρχουν ειδικοί μηχανισμοί για λειτουργίες υποστήριξης.

8.1.6 Διαχείριση από εξωτερικούς συνεργάτες

Οι εξωτερικοί συνεργάτες που έχουν αναλάβει καθήκοντα διαχείρισης ή υποστήριξης του πληροφοριακού συστήματος του οργανισμού, μπορούν να προκαλέσουν απώλεια, υποκλοπή ή μη εξουσιοδοτημένη αλλαγή των δεδομένων. Θα πρέπει να γίνει αποτίμηση κινδύνου και στο συμβόλαιο ανάμεσα στον οργανισμό και τους εξωτερικού συνεργάτες να υπάρχουν όροι που να καθοδηγούν τους τελευταίους και να προστατεύουν τον οργανισμό. Θα πρέπει να εξεταστούν τα ακόλουθα:

- Ο καθορισμός των ευαίσθητων εφαρμογών που θα πρέπει να αναπτυχθούν από το προσωπικό του οργανισμού.

- Η ύπαρξη έγκρισης από τα κατάλληλα στελέχη του οργανισμού.

- Οι επιπλοκές στα σχέδια της συνέχειας των επιχειρησιακών λειτουργιών του οργανισμού.

- Τα πρότυπα ασφάλειας που θα ακολουθηθούν και οι διαδικασίες ελέγχου της συμμόρφωσης με αυτά.

- Ο καταμερισμός των καθηκόντων και των διαδικασιών που είναι απαραίτητες για την ασφάλεια του οργανισμού.

- Τα καθήκοντα και τις διαδικασίες για την αναφορά και το χειρισμό συμβάντων.

8.2 Σχεδιασμός και αποδοχή συστήματος

Σκοπός είναι η ελαχιστοποίηση των βλαβών του συστήματος. Ο προσεκτικός σχεδιασμός και η κατάλληλη προετοιμασία, είναι απαραίτητα στοιχεία για τη διαθεσιμότητα πόρων και χωρητικότητας στο πληροφοριακό σύστημα του οργανισμού. Θα πρέπει να γίνουν προβλέψεις των μελλοντικών απαιτήσεων από το σύστημα, ώστε να μειωθεί ο κίνδυνος υπερφόρτωσής του. Τα νέα συστήματα θα πρέπει να δοκιμάζονται με βάση τις καταγεγραμμένες λειτουργικές ανάγκες του οργανισμού, πριν γίνουν αποδεκτά από τον οργανισμό και τεθούν σε παραγωγική λειτουργία.

8.2.1 Σχεδιασμός χωρητικότητας

Η χωρητικότητα του συστήματος θα πρέπει να παρακολουθείται συστηματικά και με βάση τα στοιχεία που συγκεντρώνονται να γίνονται προβλέψεις για τις μελλοντικές ανάγκες του οργανισμού σε αποθηκευτικό χώρο και επεξεργαστική ισχύ. Ειδική προσοχή απαιτείται για τα mainframe συστήματα, λόγω του κόστους που απαιτείται για την οποιαδήποτε αναβάθμισή τους. Οι διαχειριστές τέτοιων συστημάτων θα πρέπει να παρακολουθούν τη χρήση των κύριων πόρων του συστήματος, όπως αποθηκευτικά μέσα, επεξεργαστές και συστήματα επικοινωνίας. Οι διαχειριστές θα πρέπει να αναγνωρίζουν τάσεις στη χρήση του συστήματος, σε σχέση πάντα με τις επιχειρησιακές ανάγκες του οργανισμού.

Στη συνέχεια, τα αρμόδια διοικητικά στελέχη του οργανισμού θα πρέπει να αξιολογούν αυτές τις πληροφορίες ώστε να προβλέπουν πιθανά προβλήματα, τα οποία μπορούν να έχουν επιπτώσεις στην ασφάλεια του συστήματος ή τις παρεχόμενες από αυτό υπηρεσίες. Επιπλέον, θα πρέπει να σχεδιάζουν τις κατάλληλες ενέργειες για την αντιμετώπιση των πιθανών προβλημάτων.

8.2.2 Αποδοχή συστήματος

Τα κριτήρια αποδοχής για τα νέα πληροφοριακά συστήματα, τις αναβαθμίσεις ή τις νέες εκδόσεις τους, θα πρέπει να είναι προκαθορισμένα και με βάση αυτά να γίνουν οι σχετικές δοκιμές. Η διοίκηση θα πρέπει να φροντίσει ώστε τα κριτήρια αποδοχής να είναι

καθορισμένα με σαφήνεια, καταγεγραμμένα, δοκιμασμένα και συμφωνημένα με τα εμπλεκόμενα μέρη. Θα πρέπει να εξεταστούν τα ακόλουθα:

- απαιτήσεις χωρητικότητας και απόδοσης
- διαδικασίες αντιμετώπισης προβλημάτων
- προετοιμασία και δοκιμή διαδικασιών ρουτίνας σε σχέση με τα καθορισμένα πρότυπα
- ύπαρξη των συμφωνημένων μηχανισμών ασφάλειας
- χειροκίνητες διαδικασίες
- διαδικασίες επιχειρηματικής συνέχειας, όπως απαιτούνται από την παράγραφο 11.1
- αποδείξεις ότι η λειτουργία του νέου συστήματος δε θα επηρεάσει αρνητικά τη λειτουργία των υπολοίπων
- αποδείξεις ότι το νέο σύστημα συμβαδίζει με τα πρότυπα ασφάλειας του οργανισμού
- εκπαίδευση στη χρήση του νέου συστήματος.

Στην περίπτωση σημαντικών αλλαγών στο πληροφοριακό σύστημα του οργανισμού, θα πρέπει να ζητείται και η συνδρομή των χρηστών σε όλα τα στάδια του σχεδιασμού και της υλοποίησης αυτών των αλλαγών. Με αυτόν τον τρόπο διασφαλίζεται η επάρκεια του προτεινόμενου συστήματος, τουλάχιστον σε επίπεδο σχεδιασμού, ενώ πρακτικά θα πρέπει να επιβεβαιωθεί από τις σχετικές δοκιμές.

8.3 Προστασία απέναντι σε κακόβουλο λογισμικό

Σκοπός είναι η προστασία της ακεραιότητας του συστήματος, όπως και των πληροφοριών. Χρειάζεται ειδική μέριμνα για τον εντοπισμό και την προστασία του πληροφοριακού συστήματος από κακόβουλο λογισμικό, όπως ιούς, worms, δούρειους ίππους και logic bombs. Οι χρήστες θα πρέπει να είναι ενήμεροι για τους κινδύνους που προκαλεί το κακόβουλο λογισμικό. Η διοίκηση θα πρέπει να χρησιμοποιήσει τους κατάλληλους

μηχανισμούς για τον εντοπισμό και την αποτροπή εισόδου στο σύστημα κακόβουλου λογισμικού. Ιδιαίτερης σημασίας είναι η προστασία των προσωπικών υπολογιστών από ιούς.

8.3.1 Μηχανισμοί προστασίας

Θα πρέπει να υλοποιηθούν οι κατάλληλοι μηχανισμοί για την αποτροπή και τον εντοπισμό κακόβουλου λογισμικού. Η προστασία απέναντι στο κακόβουλο λογισμικό θα πρέπει να βασίζεται στην ενημέρωση του προσωπικού για την ασφάλεια του οργανισμού, τα κατάλληλα δικαιώματα προσπέλασης και τους μηχανισμούς διαχείρισης αλλαγών στο σύστημα. Θα πρέπει να εξεταστούν οι ακόλουθοι μηχανισμοί:

- Μια επίσημη πολιτική που να επιβάλει την ύπαρξη των κατάλληλων αδειών χρήσης λογισμικού και να απαγορεύει τη χρήση μη εξουσιοδοτημένου λογισμικού (παράγραφος 12.1.2.2).

- Μια επίσημη πολιτική που να προστατεύει το πληροφοριακό σύστημα από λογισμικό και αρχεία που μπορούν να εισέλθουν στο σύστημα από κάποιο εξωτερικό δίκτυο ή μέσο αποθήκευσης (παράγραφος 10.5, ειδικά 10.5.4 και 10.5.5).

- Εγκατάσταση και τακτική ενημέρωση προγραμμάτων antivirus για τον έλεγχο προσωπικών υπολογιστών και αποθηκευτικών μέσων.

- Τακτικός έλεγχος του χρησιμοποιούμενου λογισμικού και των αρχείων του συστήματος. Οποιαδήποτε αλλαγή θα πρέπει να ερευνάται.

- Ο έλεγχος αρχείων και αποθηκευτικών μέσων για ιούς πριν από τη χρήση τους.

- Ο έλεγχος των εισερχόμενων ηλεκτρονικών μηνυμάτων για ιούς. Ο συγκεκριμένος έλεγχος μπορεί να γίνει σε διάφορα σημεία του συστήματος, όπως τους εξυπηρέτες ηλεκτρονικού ταχυδρομείου, τους προσωπικούς υπολογιστές κλπ.

- Την εκπαίδευση των χρηστών και ύπαρξη διαδικασιών για την αντιμετώπιση ιών.

- Την ύπαρξη σχεδίου επιχειρησιακής συνέχειας στην περίπτωση εκτεταμένων ζημιών στο σύστημα από ιούς.

- Την ύπαρξη διαδικασιών για τον έλεγχο της ακρίβειας της πληροφόρησης για ιούς και την αντιμετώπιση hoaxes.

Οι παραπάνω μηχανισμοί ελέγχου έχουν ιδιαίτερη σημασία για την προστασία εξυπηρετών αρχείων που εξυπηρετούν μεγάλο αριθμό σταθμών εργασίας.

8.4 Καθημερινή λειτουργία

Σκοπός είναι η διατήρηση της ακεραιότητας και της διαθεσιμότητας του πληροφοριακού συστήματος. Θα πρέπει να υπάρχουν διαδικασίες ρουτίνας για την καθημερινή λήψη εφεδρικών αντιγράφων του συστήματος, την καταγραφή γεγονότων και λαθών στο σύστημα, όπως και την παρακολούθηση του περιβαλλοντολογικών συνθηκών στους χώρους που στεγάζουν το πληροφοριακό σύστημα.

8.4.1 Εφεδρικό αντίγραφο ασφαλείας του συστήματος

Θα πρέπει να γίνεται τακτική λήψη εφεδρικών αντιγράφων του συστήματος, ειδικότερα των κρίσιμων αρχείων και προγραμμάτων. Θα πρέπει να υπάρχουν οι επαρκείς πόροι για τη λήψη εφεδρικών αντιγράφων του συστήματος, όπως και να γίνονται τακτικές δοκιμές ώστε να διασφαλίζεται η ικανοποίηση των αναγκών του οργανισμού (κεφάλαιο 11). Θα πρέπει να εξεταστούν οι ακόλουθοι μηχανισμοί:

- Ένα μέρος του εφεδρικού αντιγράφου και τα εγχειρίδια των διαδικασιών ανάκτησης θα πρέπει να φυλάσσονται σε ένα απομακρυσμένο σημείο, ώστε να αντιμετωπιστεί το ενδεχόμενο καταστροφής στο κύριο site του οργανισμού. Θα πρέπει να τηρούνται τουλάχιστον τρία διαφορετικά εφεδρικά αντίγραφα των κρίσιμων στοιχείων και εφαρμογών του οργανισμού.

- Τα αποθηκευτικά μέσα που περιέχουν εφεδρικά αντίγραφα, θα πρέπει να προστατεύονται σύμφωνα με τα πρότυπα ασφάλειας του οργανισμού, είτε φυλάσσονται σε απομακρυσμένο σημείο, είτε στους κύριους χώρους του οργανισμού.

- Θα πρέπει να γίνεται τακτικός έλεγχος των μέσων που χρησιμοποιούνται για εφεδρικά αντίγραφα.

- Οι διαδικασίες ανάκτησης θα πρέπει να δοκιμάζονται τακτικά για να ελεγχθεί η αποτελεσματικότητά τους σε σχέση με τις απαιτήσεις του οργανισμού.

Θα πρέπει επίσης να καθοριστεί η χρονική διάρκεια διατήρησης ενός εφεδρικού αντίγραφου.

8.4.2 Τήρηση αρχείων συστήματος

Το προσωπικό που διαχειρίζεται το πληροφοριακό σύστημα του οργανισμού θα πρέπει να τηρεί αρχεία με τις δραστηριότητες του. Τα αρχεία αυτά θα πρέπει να περιλαμβάνουν τα ακόλουθα:

- την ώρα έναρξης της λειτουργίας του συστήματος, όπως και του κλεισίματός του

- τα προβλήματα που παρουσιάστηκαν στο σύστημα και τις ενέργειες για την αντιμετώπισή τους

- επιβεβαίωση της σωστής διαχείρισης των δεδομένων και των αποτελεσμάτων της επεξεργασίας τους

- το όνομα του προσώπου που έκανε την καταχώρηση στο αρχείο.

Τα αρχεία λειτουργίας του συστήματος θα πρέπει να ελέγχονται σε τακτά χρονικά διαστήματα για τη συμμόρφωσή τους με τα πρότυπα του οργανισμού.

8.4.3 Καταγραφή σφαλμάτων

Τα σφάλματα που παρουσιάζονται στο σύστημα θα πρέπει να αναφέρονται και να αντιμετωπίζονται κατάλληλα. Τα σφάλματα που αναφέρονται από τους χρήστες θα πρέπει να

καταγράφονται. Θα πρέπει ακόμα να υπάρχουν συγκεκριμένοι τρόποι αντιμετώπισης των αναφερθέντων προβλημάτων:

- Έλεγχος των αρχείων καταγραφής των σφαλμάτων για να επιβεβαιωθεί η σωστή αντιμετώπισή τους.
- Έλεγχος των διαδικασιών αντιμετώπισης των σφαλμάτων για να επιβεβαιωθεί η συμμόρφωσή τους με τα πρότυπα ασφάλειας του οργανισμού.

8.5 Διαχείριση δικτύου

Σκοπός είναι η ασφάλεια των πληροφοριών που υπάρχουν στο δίκτυο του οργανισμού, καθώς και της δικτυακής υποδομής. Η διαχείριση της ασφάλειας του δικτύου απαιτεί ειδική προσοχή, καθώς επηρεάζει πολλά τμήματα του οργανισμού. Θα πρέπει επίσης να εξασφαλιστεί ότι ευαίσθητα δεδομένα δεν αποστέλλονται διαμέσου δημόσιων δικτύων.

8.5.1 Προστασία δικτύου

Για την προστασία του δικτύου του οργανισμού απαιτείται μια σειρά από μηχανισμούς ασφάλειας. Θα πρέπει να προστατευθούν τόσο τα δεδομένα που μεταδίδονται μέσω του δικτύου, όσο και οι δικτυακές συσκευές από μη εξουσιοδοτημένη πρόσβαση. Θα πρέπει να εξεταστούν τα ακόλουθα:

- Η ευθύνη για το δίκτυο, θα πρέπει να είναι ξεχωριστή από την ευθύνη για τα συστήματα.
- Θα πρέπει να είναι καθορισμένα τα καθήκοντα και οι ευθύνες για τη διαχείριση εξοπλισμού που βρίσκεται σε απομακρυσμένα σημεία.
- Όπου είναι αναγκαίο να μεταδοθούν ευαίσθητα δεδομένα μέσω δημόσιων δικτύων, θα πρέπει να λαμβάνεται ειδική μέριμνα για την προστασίας τους (παράγραφοι 9.4 και 10.3). Θα πρέπει επίσης να ληφθούν τα κατάλληλα μέτρα για τη διαθεσιμότητα των δικτυακών υπηρεσιών.

- Η διαχείριση των συστημάτων και του δικτύου θα πρέπει να διασφαλίζει τόσο την ασφάλεια του πληροφοριακού συστήματος, όσο και τη διαθεσιμότητα των παρεχόμενων υπηρεσιών για την κάλυψη των αναγκών του οργανισμού.

8.6 Διαχείριση αποθηκευτικών μέσων

Σκοπός είναι η αποτροπή ζημιών στους πόρους του οργανισμού και παρεμβολών στις λειτουργίες του οργανισμού. Τα διάφορα αποθηκευτικά μέσα (δίσκοι, ταινίες κλπ.), τα έγγραφα, τα εγχειρίδια του συστήματος θα πρέπει να προστατεύονται κατάλληλα από καταστροφή, κλοπή ή μη εξουσιοδοτημένη πρόσβαση.

8.6.1 Διαχείριση αποθηκευτικών μέσων που μπορεί να διαγραφεί το περιεχόμενο τους

Θα πρέπει να υπάρχουν οι κατάλληλες διαδικασίες για τη διαχείριση αποθηκευτικών μέσων που μπορεί να διαγραφεί το περιεχόμενο τους, όπως είναι οι ταινίες, οι δίσκοι και οι εκτυπώσεις. Θα πρέπει να εξεταστούν τα ακόλουθα:

- Τα αποθηκευτικά μέσα που δεν περιέχουν χρήσιμα πλέον δεδομένα θα πρέπει να διαγράφονται.

- Θα πρέπει να τηρείται αρχείο της μεταφοράς των αποθηκευτικών μέσων εκτός των χώρων του οργανισμού. Επιπλέον, θα πρέπει να υπάρχει η κατάλληλη εξουσιοδότηση για οποιαδήποτε τέτοια μεταφορά.

- Όλα τα αποθηκευτικά μέσα θα πρέπει να φυλάσσονται κατάλληλα, με ασφάλεια και σύμφωνα με τις οδηγίες του κατασκευαστή.

Όλες οι διαδικασίες και τα επίπεδα εξουσιοδότησης θα πρέπει να είναι καταγεγραμμένα με σαφήνεια.

8.6.2 Απόσυρση αποθηκευτικών μέσων

Τα διάφορα αποθηκευτικά μέσα, μετά την απόσυρση από τη λειτουργία τους θα πρέπει είτε να καταστρέφονται πλήρως, είτε να διαγράφονται όλα τα δεδομένα τους πριν επαναχρησιμοποιηθούν. Ευαίσθητες πληροφορίες του οργανισμού, είναι δυνατό να διαρρεύσουν λόγω έλλειψης προσοχής κατά την απόσυρση αποθηκευτικών μέσων. Θα πρέπει να δοθεί προσοχή στα ακόλουθα:

- Τα αποθηκευτικά μέσα που περιέχουν ευαίσθητες πληροφορίες θα πρέπει να φυλάσσονται κατά τη χρήση τους και να αποσύρονται ή να ανακυκλώνονται με ασφάλεια, όπως με τη χρήση καταστροφέων εγγράφων ή με ασφαλή διαγραφή δεδομένων από μαγνητικά μέσα πριν την επαναχρησιμοποίησή τους από τον οργανισμό.

- Ειδική μεταχείριση απαιτείται για τα διάφορα έγγραφα, αντίγραφα εγγράφων και εκτυπώσεις, τα μαγνητικά αποθηκευτικά μέσα (ταινίες, δισκέτες, δίσκους κλπ), τα οπτικά αποθηκευτικά μέσα (cd-roms κλπ.), τα φύλλα καρμπόν, τον κώδικα των εφαρμογών, τα δεδομένα που χρησιμοποιούνται από τις εφαρμογές και τα εγχειρίδια του συστήματος.

- Μπορεί να είναι ευκολότερη η συγκέντρωση όλων των αποθηκευτικών μέσων και η ασφαλής καταστροφή τους, αντί ο διαχωρισμός τους σε ευαίσθητα και μη.

- Υπάρχουν εταιρείες που προσφέρουν υπηρεσίες συλλογής και καταστροφής αντικειμένων. Θα πρέπει να δοθεί ιδιαίτερη προσοχή στην επιλογή μιας τέτοιας εταιρείας, η οποία θα πρέπει να έχει πείρα και επαρκή μέσα.

- Η καταστροφή και η απόσυρση ευαίσθητων αποθηκευτικών μέσων θα πρέπει να καταγράφεται και να τηρείται σχετικό αρχείο.

Όταν συγκεντρώνονται πολλά αποθηκευτικά μέσα για καταστροφή, θα πρέπει να δοθεί ιδιαίτερη προσοχή γιατί είναι πιθανό συσσωρευμένες μή ευαίσθητες πληροφορίες, να αποκαλύπτουν περισσότερα στοιχεία από μια μικρή ποσότητα ευαίσθητων πληροφοριών.

8.6.3 Χειρισμός πληροφοριών

Στον οργανισμό θα πρέπει να υπάρχουν συγκεκριμένες διαδικασίες για το χειρισμό και την αποθήκευση των πληροφοριών, προκειμένου να προστατεύονται από μη εξουσιοδοτημένη προσπέλαση ή ακόμα και κατάχρηση. Οι διαδικασίες αυτές θα πρέπει να βασίζονται στο σύστημα κατηγοριοποίησης των πληροφοριών του οργανισμού (παράγραφος 5.2) και να καλύπτουν έγγραφα, υπολογιστικά συστήματα, τηλεπικοινωνίες, ταχυδρομείο κλπ. Θα πρέπει να εξεταστούν τα ακόλουθα:

- Χειρισμός και κατηγοριοποίηση όλων των αποθηκευτικών μέσων (παράγραφος 8.7.2).
- Μηχανισμοί ελέγχου πρόσβασης στις πληροφορίες.
- Τήρηση αρχείου της προσπέλασης στις πληροφορίες.
- Έλεγχος της συνοχής ανάμεσα στην επεξεργασία των πληροφοριών και των αποτελεσμάτων αυτής.
- Προστασία των δεδομένων σε όλα τα στάδια της επεξεργασίας τους.
- Χρήση και αποθήκευση των διάφορων αποθηκευτικών μέσων σύμφωνα με τις προδιαγραφές του κατασκευαστή.
- Ελαχιστοποίηση της διανομής των δεδομένων.
- Επισήμανση όλων των αντιγράφων των δεδομένων για την αποτελεσματική προστασία τους.
- Περιοδικός έλεγχος του καταλόγου των εξουσιοδοτημένων χρηστών των δεδομένων.

8.6.4 Ασφάλεια των εγχειριδίων του συστήματος

Τα εγχειρίδια του συστήματος μπορεί να περιέχουν διάφορες ευαίσθητες πληροφορίες όπως δομές δεδομένων, διαδικασίες, περιγραφή των εφαρμογών κλπ. Θα πρέπει να ληφθούν τα ακόλουθα μέτρα για την προστασία των εγχειριδίων:

- Τα εγχειρίδια του συστήματος θα πρέπει να φυλάσσονται επαρκώς.

- Θα πρέπει να υπάρχει λίστα όσων έχουν πρόσβαση στα εγχειρίδια. Πρόσβαση θα πρέπει να δοθεί μόνο σε όσους είναι απολύτως απαραίτητο.

- Η ηλεκτρονική μορφή των εγχειριδίων θα πρέπει να προστατεύεται επαρκώς.

8.7 Ανταλλαγή πληροφοριών και εφαρμογών

Σκοπός είναι η προστασία των πληροφοριών που ανταλλάσσονται ανάμεσα σε δύο οργανισμούς από αλλαγές, κατάχρηση ή απώλεια. Η ανταλλαγή πληροφοριών και εφαρμογών ανάμεσα σε οργανισμούς θα πρέπει να ελέγχεται και να είναι σύμφωνη με τη σχετική νομοθεσία (κεφάλαιο 12). Θα πρέπει να υπάρχει ειδική συμφωνία ανάμεσα σε δύο οργανισμούς, με βάση την οποία θα γίνονται οι οποιεσδήποτε ανταλλαγές πληροφοριών. Θα πρέπει να προστατεύονται τόσο οι ίδιες οι πληροφορίες, όσο και τα μέσα που τις περιέχουν. Θα πρέπει επίσης να εξεταστούν οι συνέπειες της ηλεκτρονικής ανταλλαγής δεδομένων (EDI), του ηλεκτρονικού ταχυδρομείου (email) και του ηλεκτρονικού εμπορίου (e-commerce), όπως και οι απαραίτητοι μηχανισμοί προστασίας τους.

8.7.1 Συμφωνίες ανταλλαγής πληροφοριών και λογισμικού

Όταν είναι απαραίτητη η ανταλλαγή δεδομένων και λογισμικού ανάμεσα σε οργανισμούς, θα πρέπει να συνάπτονται μεταξύ τους ειδικές συμφωνίες. Οι συμφωνίες αυτές, οι οποίες μπορούν σε κάποιες περιπτώσεις να έχουν επίσημο χαρακτήρα με νομικό υπόβαθρο, θα πρέπει να αντανακλούν το ευαίσθητο των πληροφοριών που αφορούν. Τέτοιες συμφωνίες θα πρέπει να εξετάζουν τα ακόλουθα:

- Διοικητικές ευθύνες για τον έλεγχο και την καταγραφή της μετάδοσης και της λήψης των πληροφοριών.

- Διαδικασίες για την ενημέρωση του αποστολέα για τη μετάδοση και τη λήψη των πληροφοριών.

- Τις ελάχιστες τεχνικές προδιαγραφές για τη μετάδοση των πληροφοριών.

- Διαδικασίες για την ταυτοποίηση των μεταφορέων των πληροφοριών.

- Ευθύνες για την περίπτωση απώλειας δεδομένων.
- Τον καθορισμό κοινού συστήματος επισήμανσης και άμεσης αναγνώρισης των ευαίσθητων πληροφοριών.
- Θέματα ιδιοκτησίας των πληροφοριών, καθώς και προστασίας των πνευματικών δικαιωμάτων (παράγραφοι 12.1.2 και 12.1.4).
- Διαδικασίες και πρότυπα για την καταγραφή και την ανάγνωση των πληροφοριών.
- Ειδικές διαδικασίες για την προστασία κρίσιμων δεδομένων, όπως κρυπτογραφικά κλειδιά κλπ. (παράγραφος 10.3.5).

8.7.2 Ασφάλεια των αποθηκευτικών μέσων κατά τη μεταφορά

Οι πληροφορίες μπορούν να είναι ευάλωτες σε κάθε μορφής υποκλοπή, κατάχρηση ή μη εξουσιοδοτημένη παρέμβαση κατά τη μεταφορά τους. Για την προστασία των αποθηκευτικών μέσων κατά τη μεταφορά τους, θα πρέπει να εξεταστούν οι ακόλουθοι μηχανισμοί:

- Θα πρέπει να χρησιμοποιούνται αξιόπιστα μέσα και υπηρεσίες μεταφοράς. Θα μπορούσε για παράδειγμα να καταρτιστεί μια λίστα εταιρειών couriers που θα χρησιμοποιούνται για τη μεταφορά αποθηκευτικών μέσων ανάμεσα σε οργανισμούς, καθώς και οι διαδικασίες αναγνώρισης των μελών τους που εκτελούν τις μεταφορές.
- Τα αποθηκευτικά μέσα πριν από τη μεταφορά τους θα πρέπει να συσκευάζονται κατάλληλα και σύμφωνα με τις προδιαγραφές του κατασκευαστή, ώστε να προστατευθούν από το ενδεχόμενο φθοράς.
- Επιπλέον μηχανισμοί απαιτούνται για την προστασία των ευαίσθητων πληροφοριών. Τέτοιοι μηχανισμοί μπορούν να περιλαμβάνουν ειδικές θήκες που να κλειδώνουν, παράδοση χέρι με χέρι, χρήση ψηφιακών υπογραφών, κρυπτογραφίας κλπ. (παράγραφος 10.3).

8.7.3 Ασφάλεια ηλεκτρονικού εμπορίου

Το ηλεκτρονικό εμπόριο περιλαμβάνει τη χρήση EDI, ηλεκτρονικού ταχυδρομείου και μεταφορά δεδομένων μέσω δημόσιων δικτύων όπως το Internet. Το ηλεκτρονικό εμπόριο είναι ευάλωτο σε ένα πλήθος δικτυακών κινδύνων που μπορούν να προκαλέσουν μη εξουσιοδοτημένη πρόσβαση και επέμβαση στα μεταφερόμενα δεδομένα, ή και τη διάπραξη απάτης. Τα μέτρα ασφάλειας για την προστασία του ηλεκτρονικού εμπορίου θα πρέπει να περιλαμβάνουν τα ακόλουθα:

- Αυθεντικοποίηση (authentication), η οποία αφορά το επίπεδο εμπιστοσύνης που οι συναλλασσόμενοι απαιτούν σε σχέση με την ταυτότητα των εμπλεκόμενων μερών.

- Εξουσιοδότηση (authorization), που αφορά τα δικαιώματα καθορισμού των παραμέτρων των συναλλαγών (τιμοκατάλογοι, ψηφιακά έγγραφα κλπ.). Επίσης θα πρέπει οι συναλλασσόμενοι να γνωρίζουν ποιος έχει τέτοια δικαιώματα.

- Διαδικασίες προστασίας και τήρησης ειδικών συμφωνιών ή συμβολαίων ανάμεσα στους συναλλασσόμενους.

- Ακεραιότητα (integrity) του τιμοκαταλόγου που γνωστοποιείται στους αγοραστές, καθώς και προστασία ευαίσθητων πληροφοριών για ειδικές επιπλέον εκπτώσεις.

- Επεξεργασία των παραγγελιών με τέτοιον τρόπο που να προστατεύει τα χαρακτηριστικά της κάθε παραγγελίας (στοιχεία αγοραστή, αγαθά, τρόπο πληρωμής κλπ.).

- Διαδικασίες ελέγχου των πληροφοριών που παρέχει ο πελάτης για την πληρωμή των αγαθών.

- Καθορισμός του πλέον κατάλληλου τρόπου πληρωμής για την αποφυγή απάτης.

- Μηχανισμοί για την προστασία των στοιχείων της παραγγελίας αναφορικά με την ακεραιότητα και την εμπιστευτικότητα. Επιπλέον θα πρέπει να εξεταστούν τα κατάλληλα μέτρα προστασίας απέναντι στη διπλοεγγραφή ή την απώλεια των συναλλαγών.

- Καθορισμός των ευθυνών και ανάληψης κινδύνου για την περίπτωση απάτης.

Αρκετά από τα παραπάνω αντιμετωπίζονται με τη χρήση κρυπτογραφίας (παράγραφος 10.3), σε συνδυασμό πάντα με τη σχετική νομοθεσία (παράγραφος 12.1). Επιπλέον, το ηλεκτρονικό εμπόριο θα πρέπει να καλύπτεται από ειδική συμφωνία ανάμεσα στους συναλλασσόμενους. Σε αυτήν, θα πρέπει να ορίζονται οι όροι των συναλλαγών και αν κρίνεται απαραίτητο, το επίπεδο και η διαθεσιμότητα των παρεχόμενων υπηρεσιών. Τα δημόσια συστήματα ηλεκτρονικού εμπορίου θα πρέπει να έχουν στη διάθεση του κοινού, τους όρους συναλλαγών. Επίσης, ειδική προσοχή θα πρέπει να δοθεί στην προστασία των υπολογιστών που χρησιμοποιούνται για ηλεκτρονικό εμπόριο, όπως και των συνδέσεων που χρησιμοποιούν (παράγραφος 9.4.7).

8.7.4 Ασφάλεια του ηλεκτρονικού ταχυδρομείου

8.7.4.1 Κίνδυνοι

Το ηλεκτρονικό ταχυδρομείο χρησιμοποιείται ευρέως για την επικοινωνία ανάμεσα στις επιχειρήσεις, αντικαθιστώντας τις παραδοσιακές μορφές επικοινωνίας όπως την αλληλογραφία και το telex. Το ηλεκτρονικό ταχυδρομείο διαφέρει σε σχέση με τις υπόλοιπες μορφές επικοινωνίας ως προς την ταχύτητά του, τη δομή των μηνυμάτων του και την τρωτότητά του απέναντι σε μη εξουσιοδοτημένες ενέργειες. Οι κίνδυνοι σε σχέση με την ασφάλειά του περιλαμβάνουν:

- Τη δυνατότητα μη εξουσιοδοτημένης πρόσβασης στα μηνύματα με σκοπό την ανάγνωση ή την αλλαγή των περιεχομένων τους.
- Τη διενέργεια λάθους κατά τη χρήση του όπως λανθασμένη διεύθυνση παραλήπτη, καθώς και τη γενικότερη διαθεσιμότητα και αξιοπιστία της υπηρεσίας.
- Τις επιπτώσεις στην επικοινωνία από την αλλαγή του μέσου, όπως ταχύτερη επικοινωνία ή μετατροπή της επίσημης επικοινωνίας ανάμεσα σε εταιρείες σε επικοινωνία ανάμεσα σε άτομα.
- Νομικά θέματα, όπως απόδειξη της ταυτότητας του αποστολέα, της ίδιας της αποστολής, αλλά και της λήψης του συστήματος.
- Θέματα από τη δυνατότητα που δίνεται σε τρίτους να αποκτήσουν πρόσβαση σε λίστες προσωπικού του οργανισμού.
- Έλεγχος της πρόσβασης των απομακρυσμένων χρηστών στο ηλεκτρονικό ταχυδρομείο.

8.7.4.2 Πολιτική ηλεκτρονικού ταχυδρομείου

Οι οργανισμοί θα πρέπει να υιοθετήσουν σαφή πολιτική για τη χρήση του ηλεκτρονικού ταχυδρομείου. Ενδεικτικά θα πρέπει να περιλαμβάνει τα ακόλουθα:

- Επιθέσεις κατά του ηλεκτρονικού ταχυδρομείου από ιούς ή από υποκλοπείς.
- Προστασία των συνημμένων αρχείων στα μηνύματα.

- Οδηγίες για το πότε να μη γίνεται χρήση του ηλεκτρονικού ταχυδρομείου.
- Ευθύνες των υπαλλήλων του οργανισμού ώστε να μην τον εκθέσουν μέσω της χρήσης του ηλεκτρονικού ταχυδρομείου (π.χ. με αποστολή υβριστικών μηνυμάτων κλπ.).
- Χρήση τεχνικών κρυπτογραφίας για την ακεραιότητα και την εμπιστευτικότητα των μηνυμάτων (παράγραφος 10.3).
- Διατήρηση μηνυμάτων που αν αποθηκευθούν μπορούν να χρησιμοποιηθούν σε περίπτωση αντιδικίας.
- Επιπλέον μηχανισμούς για τον έλεγχο μηνυμάτων για τα οποία δεν μπορεί να γίνει αυθεντικοποίηση.

8.7.5 Ασφάλεια των ηλεκτρονικών συστημάτων γραφείου

Η πολιτική ασφάλειας του οργανισμού θα πρέπει να έχει τέτοια μορφή ώστε να καλύπτει και τα ηλεκτρονικά συστήματα οργάνωσης γραφείου. Τα συστήματα αυτά προσφέρουν τη δυνατότητα ταχύτατης ανταλλαγής πληροφοριών μέσα στον οργανισμό, με χρήση υπολογιστών, τηλεπικοινωνιών, εγγράφων, τηλεφωνικών υπηρεσιών (τηλεφωνία, voice mail κλπ.), παραδοσιακού ταχυδρομείου και μηχανών γραφείου. Θα πρέπει να δοθεί ιδιαίτερη προσοχή στη διασύνδεση των παραπάνω, λαμβάνοντας υπόψη:

- Τις αδυναμίες των συστημάτων οργάνωσης γραφείων, όπως την καταγραφή των συνομιλιών.
- Πολιτικές για τη διαχείριση του τρόπου με τον οποίο οι πληροφορίες μοιράζονται ανάμεσα στα μέλη του οργανισμού (παράγραφος 9.1).
- Την εξαίρεση ευαίσθητων πληροφοριών εφόσον το σύστημα δεν μπορεί να τις προστατέψει επαρκώς.
- Τον περιορισμό της πρόσβασης σε στοιχεία συγκεκριμένων μελών (όπως τα μέλη μιας ομάδας εργασίας που εργάζεται πάνω σε κάποιο σημαντικό για τον οργανισμό έργο).

- Την καταλληλότητα του συστήματος να υποστηρίξει τις εφαρμογές που χρειάζεται ο οργανισμός.
- Τον έλεγχο όσων έχουν πρόσβαση στο σύστημα.
- Τον περιορισμό της χρήσης συγκεκριμένων τμημάτων του συστήματος από επίσης συγκεκριμένες κατηγορίες χρηστών.
- Την καταγραφή της κατάστασης των χρηστών σε σχέση με τον οργανισμό.
- Την πολιτική τήρησης αντιγράφων ασφάλειας.
- Τις απαιτήσεις αποκατάστασης του συστήματος.

8.7.6 Δημόσια συστήματα

Ειδική μεταχείριση απαιτείται για τις πληροφορίες που γίνονται διαθέσιμες στο κοινό. Οποιαδήποτε μη εξουσιοδοτημένη παρέμβαση σε αυτές, μπορεί να έχει άμεσο αντίκτυπο στην εικόνα του οργανισμού. Τα συστήματα στα οποία έχει προσπέλαση το κοινό (π.χ. Web servers) θα πρέπει να συμμορφώνονται με τη σχετική νομοθεσία, ενώ για τις πληροφορίες που προσφέρουν θα πρέπει να υπάρχει συγκεκριμένη διαδικασία στον οργανισμό, βάσει της οποίας θα χαρακτηρίζονται δημόσιες.

Το λογισμικό, καθώς και η κάθε μορφής πληροφορία που βρίσκεται σε ένα σύστημα προσπελάσιμο από το κοινό, απαιτεί ιδιαίτερη προστασία, όπως ψηφιακές υπογραφές (παράγραφος 10.3.3). Τέτοια συστήματα, ειδικά όσα επιτρέπουν την εισαγωγή δεδομένων από χρήστες, θα πρέπει να ελέγχονται προσεκτικά ώστε:

- Η συλλογή πληροφοριών να γίνεται σύμφωνα με τη σχετική νομοθεσία (παράγραφος 12.1.4).
- Η εισαγωγή και η επεξεργασία των δεδομένων στο σύστημα να γίνεται με ακρίβεια και σε αποδεκτό χρονικό διάστημα.
- Οι ευαίσθητες πληροφορίες να προστατεύονται επαρκώς.

- Η προσπέλαση στο σύστημα να μην μπορεί να χρησιμοποιηθεί για προσπέλαση στο υπόλοιπο δίκτυο του οργανισμού.

8.7.7 Άλλες μορφές ανταλλαγής πληροφοριών

Οι διαδικασίες και οι μηχανισμοί προστασίας που χρησιμοποιούνται από τον οργανισμό, θα πρέπει να καλύπτουν όλες τις μορφές επικοινωνίας όπως φωνή, fax και video. Οι πληροφορίες μπορούν να εκτεθούν σε τρίτους, είτε να προκληθούν προβλήματα στην παροχή των υπηρεσιών επικοινωνίας λόγω έλλειψης προσοχής, ενημέρωσης ή ελλιπών διαδικασιών κατά τη χρήση και τη μετάδοσή τους.

Ο οργανισμός θα πρέπει να έχει μια σαφή πολιτική για τη χρήση φωνητικής επικοινωνίας, fax και video που να περιλαμβάνει:

- Την ενημέρωση του προσωπικού για τους κινδύνους υποκλοπής των συνομιλιών.
- Οδηγίες για τη διενέργεια εμπιστευτικών συνομιλιών σε κατάλληλους χώρους.
- Οδηγίες για τη χρήση τηλεφωνητών, ειδικότερα για το γεγονός ότι σε καμία περίπτωση δεν πρέπει να αφήνεται κάποιο μήνυμα ευαίσθητου χαρακτήρα σε τηλεφωνητή αφού μπορεί να υποκλαπεί από τρίτους.
- Οδηγίες για τη χρήση fax και τους σχετικούς κινδύνους (όπως προγραμματισμός των συσκευών να στέλνουν τα κείμενα σε συγκεκριμένους αριθμούς, την κλήση λάθους αριθμού κλπ.).

9. Έλεγχος πρόσβασης (access control)

9.1 Επιχειρησιακές απαιτήσεις

Σκοπός είναι ο έλεγχος της πρόσβασης στις πληροφορίες του οργανισμού. Οι πληροφορίες καθώς και η πρόσβαση σε αυτές θα πρέπει να ελέγχονται με βάση τις επιχειρησιακές ανάγκες και της απαιτήσεις ασφάλειας του οργανισμού. Οδηγός θα πρέπει να είναι οι πολιτικές διάχυσης της πληροφορίας και εξουσιοδότησης.

9.1.1 Πολιτική ελέγχου πρόσβασης

9.1.1.1 Πολιτική και επιχειρησιακές ανάγκες

Οι ανάγκες του οργανισμού για τον έλεγχο της πρόσβασης για κάθε χρήστη ή ομάδες χρηστών, θα πρέπει να είναι καθορισμένη με σαφήνεια στο κείμενο της σχετικής πολιτικής. Οι χρήστες και οι παροχείς υπηρεσιών θα πρέπει να γνωρίζουν πως οι ανάγκες τους καλύπτονται από την πολιτική ελέγχου της πρόσβασης.

Η πολιτική θα πρέπει να περιλαμβάνει τα ακόλουθα:

- Απαιτήσεις ασφάλειας μεμονωμένων εφαρμογών.
- Καθορισμό όλων των πληροφοριών που σχετίζονται με κάποια εφαρμογή.
- Πολιτικές διάχυσης της πληροφορίας και εξουσιοδότησης, όπως για παράδειγμα τα επίπεδα ασφάλειας και την κατηγοριοποίηση των πληροφοριών.
- Συνοχή ανάμεσα στην πολιτική ελέγχου της πρόσβασης και τις πολιτικές κατηγοριοποίησης που ισχύουν σε διαφορετικά συστήματα και δίκτυα του οργανισμού.
- Σχετική νομοθεσία για την πρόσβαση στις πληροφορίες, την επεξεργασία και την προστασία τους.
- Τυπικά προφίλ χρηστών για κοινές κατηγορίες εργασιών στο σύστημα.

- Διαχείριση των δικαιωμάτων πρόσβασης σε κατανεμημένα δικτυακά περιβάλλοντα, καλύπτοντας όλους τους δυνατούς τρόπους σύνδεσης με το σύστημα.

9.1.1.2 Κανόνες ελέγχου πρόσβασης

Κατά τον καθορισμό τέτοιων κανόνων, θα πρέπει να δοθεί προσοχή στα ακόλουθα:

- Διαχωρισμός ανάμεσα σε υποχρεωτικούς και περιστασιακούς κανόνες.
- Καθορισμό κανόνων με βάση το σκεπτικό ότι αρχικά απαγορεύονται τα πάντα και στη συνέχεια επιτρέπονται μόνο όσα είναι απαραίτητα.
- Αλλαγές στις συνοδευτικές επισημάνσεις των πληροφοριών (παράγραφος 5.2) μόλις ο χρήστης ή το σύστημα προσπελάσουν τις πληροφορίες.
- Αλλαγές στα δικαιώματα των χρηστών, είτε αυτόματα από το σύστημα, είτε από κάποιο διαχειριστή.
- Διαχωρισμό των κανόνων σε αυτούς που χρειάζονται έγκριση από το διαχειριστή του συστήματος πριν να ισχύσουν και σε αυτούς για τους οποίους δεν απαιτείται κάτι τέτοιο.

9.2 Διαχείριση της πρόσβασης των χρηστών

Σκοπός είναι η προστασία του συστήματος από μή εξουσιοδοτημένη προσπέλαση. Θα πρέπει να υπάρχουν επίσημες και συγκεκριμένες διαδικασίες για τον έλεγχο της πρόσβασης των χρηστών στα διάφορα τμήματα του συστήματος και τις εφαρμογές. Οι διαδικασίες αυτές θα πρέπει να καλύπτουν ολόκληρο τον κύκλο της πρόσβασης των χρηστών, από την αρχική δήλωση του χρήστη στο σύστημα, μέχρι και τη διαγραφή του από αυτό. Ειδική προσοχή απαιτείται στον καθορισμό των δικαιωμάτων των χρηστών, ώστε να μην είναι δυνατό να παρακάμψουν τους μηχανισμούς ασφάλειας του συστήματος.

9.2.1 Δήλωση χρηστών

Ο οργανισμός θα πρέπει να χρησιμοποιεί μια συγκεκριμένη διαδικασία για την αρχική δήλωση των χρηστών στο σύστημα, όπως και τη διαγραφή τους από αυτό. Η διαδικασία αυτή θα πρέπει να περιλαμβάνει τα ακόλουθα:

- Χρήση μοναδικών ID χρηστών, τα οποία και θα καθιστούν υπεύθυνους τους χρήστες για τις πράξεις τους στο σύστημα.
- Έλεγχο της εξουσιοδότησης του χρήστη από τον ιδιοκτήτη του συστήματος για τη χρήση των παρεχόμενων υπηρεσιών. Σε κάποιες περιπτώσεις μπορεί να χρησιμοποιείται επιπλέον και ειδική εξουσιοδότηση της διοίκησης του οργανισμού.
- Έλεγχο ότι τα δικαιώματα που αποκτά ο χρήστης είναι σύμφωνα με τις απαιτήσεις της εργασίας του και επιπλέον δεν παρακάμπτουν την αρχή διαχωρισμού των καθηκόντων (παράγραφος 8.1.4).
- Τη γραπτή ενημέρωση των χρηστών για τα δικαιώματά τους στο σύστημα.
- Γραπτή δήλωση των χρηστών, μέσω της οποίας αποδέχονται τους όρους παροχής υπηρεσιών από το σύστημα.
- Εξασφάλιση ότι οι υπηρεσίες δεν παρέχονται πριν ολοκληρωθούν οι διαδικασίες εξουσιοδότησης των χρηστών.
- Τήρηση αρχείου όλων των χρηστών του συστήματος.
- Άμεση διαγραφή των χρηστών που αποχωρούν από τον οργανισμό.
- Περιοδικό έλεγχο για την ύπαρξη ανενεργών ή διπλών λογαριασμών χρηστών στο σύστημα.
- Εξασφάλιση ότι δεν μπορεί να αποδοθεί σε πολλούς χρήστες το ίδιο ID.

Επιπλέον μπορούν να συμπεριληφθούν ειδικοί όροι στα συμβόλαια απασχόλησης του προσωπικού, οι οποίοι να καλύπτουν το ενδεχόμενο μη εξουσιοδοτημένης χρήσης του συστήματος.

9.2.2 Διαχείριση προνομιακών δικαιωμάτων

Ο καθορισμός και η χρήση των προνομιακών δικαιωμάτων προσπέλασης (οποιοδήποτε σύνολο δικαιωμάτων ή χαρακτηριστικών σε ένα πολυχρηστικό σύστημα, τα οποία επιτρέπουν την παράκαμψη των μηχανισμών ελέγχου του συστήματος), θα πρέπει να είναι ελεγχόμενα και περιορισμένα. Ακατάλληλη χρήση προνομίων στο σύστημα είναι συχνά η κύρια αιτία εισβολής σε αυτό από μή εξουσιοδοτημένα άτομα.

Τα πολυχρηστικά συστήματα, τα οποία χρειάζονται προστασία απέναντι σε μη εξουσιοδοτημένη πρόσβαση, θα πρέπει να έχουν μια διαδικασία εξουσιοδότησης η οποία ελέγχει τα προνομιακά δικαιώματα. Θα πρέπει να εξεταστούν τα ακόλουθα:

- Τα προνομιακά δικαιώματα που συνδέονται με κάθε μέρος του συστήματος (εφαρμογές, λειτουργικό σύστημα κλπ.), όπως και οι χρήστες που πρέπει να τα χρησιμοποιούν, θα πρέπει να καθοριστούν επακριβώς.

- Τα προνομιακά δικαιώματα πρέπει να παρέχονται μόνο σε όσους χρήστες και για όσο χρονικό διάστημα είναι απολύτως απαραίτητο.

- Θα πρέπει να ακολουθείται κάποια διαδικασία καταγραφής των προνομιακών χρηστών του συστήματος, οι λογαριασμοί των οποίων θα ενεργοποιούνται στο σύστημα αφού ολοκληρωθεί η διαδικασία εξουσιοδότησης.

- Οι εφαρμογές του συστήματος θα πρέπει να λειτουργούν με τέτοιο τρόπο ώστε να μην απαιτούν προνομιακά δικαιώματα από τους χρήστες.

- Τα προνομιακά δικαιώματα θα πρέπει να δίνονται σε λογαριασμούς διαφορετικούς από αυτούς που χρησιμοποιούν οι χρήστες για τις συνηθισμένες εργασίες τους στο σύστημα.

9.2.3 Διαχείριση συνθηματικών (password)

Τα συνθηματικά είναι ο πλέον συνηθισμένος τρόπος για την επιβεβαίωση της ταυτότητας ενός χρήστη του συστήματος. Η διαχείριση των συνθηματικών θα πρέπει επίσης να βασίζεται σε συγκεκριμένες διαδικασίες, οι οποίες θα πρέπει να:

- Υποχρεώνουν τους χρήστες σε έγγραφη βεβαίωση για την τήρηση της μυστικότητας των συνθηματικών τους.

- Εξασφαλίζουν ότι για νέους χρήστες του συστήματος, όπως και στις περιπτώσεις που κάποιος χρήστης ξεχάσει το συνθηματικό του, θα πρέπει να του παρέχεται ένα προσωρινό συνθηματικό, το οποίο αμέσως μετά τη χρήση του θα πρέπει να αλλαχθεί.

- Εξασφαλίζουν ότι τα προσωρινά συνθηματικά θα παρέχονται στους χρήστες με κάποιον ασφαλή τρόπο, ενώ οι τελευταίοι θα πρέπει να επιβεβαιώνουν την παραλαβή.

Τα συνθηματικά δεν πρέπει ποτέ να αποθηκεύονται σε κάποιο υπολογιστικό σύστημα ή σε εκτεθειμένα σημεία. Αν κρίνεται απαραίτητο μπορούν να χρησιμοποιηθούν ειδικοί βιομετρικοί μηχανισμοί αυθεντικοποίησης χρηστών (δακτυλικά αποτυπώματα κλπ.) με ταυτόχρονη χρήση και ειδικών στοιχείων ασφάλειας, όπως έξυπνες κάρτες.

9.2.4 Έλεγχος δικαιωμάτων χρηστών

Προκειμένου να υπάρξει αποτελεσματικός έλεγχος στα δεδομένα και τις υπηρεσίες του συστήματος, η διοίκηση του οργανισμού θα πρέπει να καταρτίσει μια συγκεκριμένη διαδικασία για τον περιοδικό έλεγχο των δικαιωμάτων των χρηστών στο σύστημα. Με αυτόν τον τρόπο:

- Τα δικαιώματα των χρηστών ελέγχονται σε τακτά χρονικά διαστήματα (συνήθως συνίσταται μια περίοδος 6 μηνών) και μετά από κάθε αλλαγή (παράγραφος 9.2.1).

- Οι εξουσιοδοτήσεις για προνομιακά δικαιώματα θα πρέπει να ελέγχονται ανά μικρότερα χρονικά διαστήματα. Συνιστάται μια περίοδος 3 μηνών.

- Τα προνομιακά δικαιώματα θα πρέπει επίσης να ελέγχονται ανά τακτά χρονικά διαστήματα ώστε να μην είναι δυνατή η μη εξουσιοδοτημένη απόκτηση δικαιωμάτων.

9.3 Ευθύνες χρηστών

Σκοπός είναι η αποτροπή μή εξουσιοδοτημένης πρόσβασης στο σύστημα. Η συνεργασία των εξουσιοδοτημένων χρηστών του συστήματος είναι απαραίτητη για την ασφάλειά του. Οι χρήστες θα πρέπει να είναι ενήμεροι για τις ευθύνες τους σχετικά με τους χρησιμοποιούμενους μηχανισμούς ασφάλειας, ειδικότερα για τη χρήση συνθηματικών και την ασφάλεια του εξοπλισμού.

9.3.1 Χρήση Συνθηματικών

Οι χρήστες θα πρέπει να ακολουθούν τις συνιστώμενες πρακτικές ασφάλειας για τη χρήση συνθηματικών. Τα συνθηματικά αποτελούν το μέσο της εξακρίβωσης της ταυτότητας των χρηστών και κατά συνέπεια χρησιμοποιούνται για τον καθορισμό των δικαιωμάτων πρόσβασης στο σύστημα.

Οι χρήστες θα πρέπει να είναι είναι κατάλληλα ενημερωμένοι ώστε:

- Να κρατούν μυστικά τα συνθηματικά τους.
- Να αποφεύγουν να καταγράφουν τα συνθηματικά τους σε χαρτί, εκτός αν μπορούν να αποθηκευθούν με ασφάλεια.
- Να αλλάζουν τα συνθηματικά τους όποτε υπάρχει κάποια ένδειξη παραβίασης του συστήματος.
- Να επιλέγουν συνθηματικά με μήκος τουλάχιστον έξι χαρακτήρων, να είναι εύκολα απομνημονεύσιμα, να μη βασίζονται σε στοιχεία που μπορεί να μαντέψει κάποιος τρίτος (ονόματα, τηλέφωνα κλπ.) και να αποτελούνται από συνδυασμό αριθμών και χαρακτήρων.
- Να αλλάζουν τα συνθηματικά τους σε τακτά χρονικά διαστήματα ή μετά από κάποιο αριθμό χρήσεων και να μην ανακυκλώνουν τα ίδια συνθηματικά
- Να μη χρησιμοποιούν τα συνθηματικά μέσα σε αυτοματοποιημένες διαδικασίες εισόδου στο σύστημα (π.χ αποθηκευμένα συνθηματικά μέσα σε macros).
- Να μη μοιράζονται το ίδιο συνθηματικό με άλλους χρήστες.

Αν είναι απαραίτητο στους χρήστες να έχουν πρόσβαση σε πολλαπλές υπηρεσίες ή συστήματα με χρήση διαφορετικών συνθηματικών, θα πρέπει να διαλέγουν ένα ποιοτικό συνθηματικό σύμφωνα με τα παραπάνω. Το συγκεκριμένο συνθηματικό θα μπορεί να χρησιμοποιηθεί σε όλες τις απαραίτητες υπηρεσίες που παρέχουν ένα επαρκές επίπεδο προστασίας αποθηκευμένων συνθηματικών.

9.3.2 Εξοπλισμός χωρίς επίβλεψη

Οι χρήστες θα πρέπει να εξασφαλίζουν την επαρκή προστασία εξοπλισμού ο οποίος λειτουργεί χωρίς επίβλεψη. Οι σταθμοί εργασίας που λειτουργούν για μεγάλες χρονικές περιόδους χωρίς την επίβλεψη κάποιου χρήστη, μπορεί να χρειάζονται συγκεκριμένα μέτρα προστασίας από μή εξουσιοδοτημένη προσπέλαση. Όλοι οι χρήστες, όπως και οι εξωτερικοί συνεργάτες, θα πρέπει να είναι ενήμεροι για τις απαιτήσεις ασφάλειας εξοπλισμού που λειτουργεί χωρίς επίβλεψη, καθώς και για τις προσωπικές τους ευθύνες. Οι χρήστες θα πρέπει να είναι ενήμεροι ώστε:

- Να τερματίζουν τις συνδέσεις που δεν είναι απαραίτητες, εκτός και αν προστατεύονται κατάλληλα (π.χ. με χρήση συνθηματικών σε screen savers).
- Να αποσυνδέονται από το σύστημα όταν έχουν ολοκληρώσει την εργασία τους.
- Να ασφαλίζουν τους σταθμούς εργασίας με κατάλληλους μηχανισμούς (ειδικές κλειδαριές, συνθηματικά κλπ.) όταν δε χρησιμοποιούνται.

9.4 Έλεγχος πρόσβασης δικτύου (network access control)

Σκοπός είναι η προστασία των δικτυακών υπηρεσιών. Η προσπέλαση σε εσωτερικές αλλά και σε εξωτερικές δικτυακές υπηρεσίες θα πρέπει να είναι ελεγχόμενη. Αυτό είναι απαραίτητο προκειμένου να εξασφαλισθεί ότι οι χρήστες των δικτυακών υπηρεσιών δεν μπορούν να απειλήσουν την ασφάλεια αυτών των υπηρεσιών. Χρειάζεται να εξασφαλισθεί ότι:

- Υπάρχουν τα κατάλληλα σημεία διασύνδεσης ανάμεσα στο δίκτυο του οργανισμού και τα δίκτυα άλλων οργανισμών ή δημόσια δίκτυα.
- Υπάρχουν κατάλληλοι μηχανισμοί αυθεντικοποίησης για χρήστες και εξοπλισμό.
- Γίνεται έλεγχος της πρόσβασης των χρηστών στις προσφερόμενες υπηρεσίες.

9.4.1 Πολιτική χρήσης των δικτυακών υπηρεσιών

Ο οργανισμός μπορεί να επηρεασθεί από μη ασφαλείς συνδέσεις με δικτυακές υπηρεσίες. Οι χρήστες θα πρέπει να έχουν πρόσβαση μόνο στις απολύτως απαραίτητες υπηρεσίες δικτύου, για τις οποίες θα πρέπει να έχουν και τη σχετική εξουσιοδότηση. Μηχανισμοί ελέγχου είναι ιδιαίτερα απαραίτητοι για δικτυακές συνδέσεις με ευαίσθητες πληροφορίες ή κρίσιμης σημασίας εφαρμογές. Κατάλληλοι μηχανισμοί είναι επίσης απαραίτητοι στους χρήστες που είναι υποχρεωμένοι να εκτελούν τις εργασίες τους πάνω από δίκτυα τρίτων (άλλων οργανισμών ή το Internet).

Ο οργανισμός θα πρέπει να έχει συγκεκριμένη πολιτική για τη χρήση δικτυακών υπηρεσιών, η οποία θα πρέπει να περιλαμβάνει τα ακόλουθα:

- Τα δίκτυα και τις δικτυακές υπηρεσίες στα οποία θα επιτρέπεται η πρόσβαση.
- Διαδικασίες εξουσιοδότησης μέσω των οποίων θα καθορίζεται ποιος χρήστης έχει πρόσβαση σε ποια δίκτυα και σε ποιες υπηρεσίες.
- Διαδικασίες διαχείρισης και μηχανισμούς για την προστασία των δικτυακών συνδέσεων και των δικτυακών υπηρεσιών.

Η συγκεκριμένη πολιτική θα πρέπει να είναι συμβατή με τη γενικότερη πολιτική ελέγχου της πρόσβασης (παράγραφος 9.1).

9.4.2 Υποχρεωτικοί δίαυλοι επικοινωνίας

Ο δίαυλος επικοινωνίας από το τερματικό του χρήστη μέχρι την υπηρεσία που αυτός χρησιμοποιεί, μπορεί να χρειάζεται έλεγχο. Τα δίκτυα είναι σχεδιασμένα με τέτοιο τρόπο ώστε να παρέχουν την καλύτερη δυνατή απόκριση και δρομολόγηση των επικοινωνιών. Αυτά τα χαρακτηριστικά μπορούν να χρησιμοποιηθούν για τη μη εξουσιοδοτημένη πρόσβαση σε εφαρμογές ή άλλα τμήματα του συστήματος. Τέτοιοι κίνδυνοι μπορούν να αντιμετωπισθούν με τη χρήση μηχανισμών που επιβάλλουν συγκεκριμένο μονοπάτι δρομολόγησης ανάμεσα στο τερματικό του χρήστη και τις προσφερόμενες σε αυτόν υπηρεσίες.

Ο σκοπός ενός υποχρεωτικού διάυλου επικοινωνίας είναι να εμποδίσει κάποιο χρήστη να δρομολογήσει την επικοινωνία του τερματικού του εκτός των ορίων του συστήματος, παρακάμπτοντας έτσι τους μηχανισμούς ασφάλειας. Κάτι τέτοιο μπορεί να επιτευχθεί με τη χρήση κατάλληλων μηχανισμών σε διάφορα σημεία του δικτύου, ώστε η δρομολόγηση των επικοινωνιών να γίνεται μέσω προκαθορισμένων εναλλακτικών λύσεων. Παραδείγματα τέτοιων μηχανισμών είναι τα ακόλουθα:

- Χρήση μισθωμένων κυκλωμάτων επικοινωνίας.
- Αυτόματη σύνδεση θυρών με συγκεκριμένες εφαρμογές.
- Περιορισμός των επιλογών του χρήστη μέσα στα μενού των εφαρμογών που χρησιμοποιεί.
- Αποτροπή ανεξέλεγκτων περιαγωγών του δικτύου.
- Η επιβολή συγκεκριμένων εφαρμογών και συστημάτων στους εξωτερικούς χρήστες.
- Συνεχή έλεγχο των δικτυακών συνδέσεων (π.χ. με χρήση firewalls).
- Διαχωρισμός των χρηστών σε λογικά domains, ώστε να περιορίζεται η πρόσβασή τους στο δίκτυο.

Θα πρέπει και πάλι να δοθεί προσοχή ώστε να υπάρχει συμβατότητα με τη γενικότερη πολιτική ελέγχου της πρόσβασης (παράγραφος 9.1).

9.4.3 Αυθεντικοποίηση χρηστών για εξωτερικές συνδέσεις

Οι εξωτερικές συνδέσεις μπορούν να αποτελέσουν πύλη εισόδου σε μη εξουσιοδοτημένους χρήστες του πληροφοριακού συστήματος του οργανισμού. Κατά συνέπεια θα πρέπει να υπάρχει κάποιος μηχανισμός αυθεντικοποίησης απομακρυσμένων χρηστών. Υπάρχουν πολλοί τέτοιοι μηχανισμοί, οι οποίοι προσφέρουν διαφορετικό επίπεδο ασφάλειας. Είναι λοιπόν απαραίτητο να γίνει αποτίμηση κινδύνου πριν αποφασιστούν οι κατάλληλοι μηχανισμοί για τον οργανισμό.

Η αυθεντικοποίηση των απομακρυσμένων χρηστών μπορεί να γίνει με χρήση κρυπτογραφικών τεχνικών, ηλεκτρονικά διακριτικά (tokens) ή ειδικά πρωτόκολλα. Επίσης μπορούν να χρησιμοποιηθούν μισθωμένες γραμμές επικοινωνίας ή συστήματα ελέγχου της πηγής της σύνδεσης.

Διαδικασίες dial-back μπορούν να προστατέψουν τον οργανισμό από μή εξουσιοδοτημένες εισερχόμενες συνδέσεις. Η χρήση τέτοιων μηχανισμών προϋποθέτει την απενεργοποίηση διάφορων τηλεπικοινωνιακών διευκολύνσεων, όπως call-forwarding. Οι μηχανισμοί call-back θα πρέπει να δοκιμάζονται διεξοδικά πριν να χρησιμοποιηθούν από τον οργανισμό.

9.4.4 Αυθεντικοποίηση κόμβων του δικτύου

Μια διαδικασία αυτόματης σύνδεσης σε έναν απομακρυσμένο υπολογιστή, μπορεί να χρησιμοποιηθεί για τη μη εξουσιοδοτημένη πρόσβαση σε κάποια εφαρμογή του οργανισμού. Για αυτό το λόγο απαιτείται η αυθεντικοποίηση τέτοιων συνδέσεων, ειδικά όταν χρησιμοποιείται κάποιο δίκτυο εκτός του ελέγχου του οργανισμού. Κάποιοι μηχανισμοί αυθεντικοποίησης αναφέρονται στην προηγούμενη παράγραφο.

Η αυθεντικοποίηση κόμβων του δικτύου μπορεί να χρησιμοποιηθεί και ως εναλλακτικός τρόπος αυθεντικοποίησης ομάδων απομακρυσμένων χρηστών.

9.4.5 Προστασία απομακρυσμένων διαγνωστικών θυρών

Η πρόσβαση σε διαγνωστικές θύρες θα πρέπει να είναι αυστηρά ελεγχόμενη. Πολλά υπολογιστικά συστήματα διαθέτουν και μια σύνδεση για χρήση από το προσωπικό υποστήριξης. Αν αυτή η σύνδεση δεν προστατευθεί κατάλληλα, μπορεί να χρησιμοποιηθεί

για μή εξουσιοδοτημένη πρόσβαση στο σύστημα. Θα πρέπει λοιπόν να προστατεύονται από έναν κατάλληλο μηχανισμό ασφάλειας, ώστε να μπορούν να χρησιμοποιηθούν μόνο από εξουσιοδοτημένο προσωπικό.

9.4.6 Διαχωρισμός στα δίκτυα

Τα δίκτυα των υπολογιστών συνεχώς επεκτείνονται εκτός των ορίων του οργανισμού. Καθώς δημιουργούνται διάφορες επιχειρηματικές συνεργασίες, το δίκτυο θα πρέπει να προσφέρει τις αναγκαίες υπηρεσίες για κοινή πρόσβαση σε πληροφορίες από δύο ή περισσότερους οργανισμούς. Τέτοιου είδους προεκτάσεις μπορούν να αυξήσουν τον κίνδυνο μη εξουσιοδοτημένης πρόσβασης στα ήδη υπάρχοντα πληροφοριακά συστήματα, κάποια από τα οποία χρειάζονται ήδη προστασία από άλλους χρήστες του δικτύου λόγω του ευαίσθητου των πληροφοριών που επεξεργάζονται. Σε τέτοιες περιπτώσεις θα πρέπει να εξετάζεται το ενδεχόμενο χρήσης στο δίκτυο ειδικών μηχανισμών, οι οποίοι θα διαχωρίζουν κατηγορίες δικτυακών υπηρεσιών, συστημάτων ή χρηστών.

Μια κλασική μέθοδος ελέγχου της ασφάλειας σε ένα μεγάλο δίκτυο, είναι ο διαχωρισμός του σε πολλά λογικά πεδία (domains), με το καθένα από αυτά να προστατεύεται από μια περίμετρο ασφάλειας. Μια τέτοια περίμετρος μπορεί να δημιουργηθεί με τη χρήση ασφαλών πυλών (gateways), οι οποίες ελέγχουν την επικοινωνία ανάμεσα σε δύο πεδία. Μια τέτοια πύλη θα πρέπει να ελέγχει την επικοινωνία ανάμεσα στα πεδία (παράγραφοι 9.4.7 και 9.4.8) και να απαγορεύει τη μη εξουσιοδοτημένη πρόσβαση, σε αντιστοιχία με την πολιτική του οργανισμού (παράγραφος 9.1). Παράδειγμα μιας τέτοιας πύλης είναι η γνωστή ηλεκτρονική πύλη ασφαλείας (firewall).

Τα κριτήρια με βάση τα οποία θα γίνει ο διαχωρισμός των δικτύων σε πεδία, θα πρέπει να βασίζονται στην πολιτική ελέγχου της πρόσβασης που εφαρμόζει ο οργανισμός, τις ανάγκες επικοινωνίας, τα σχετικά κόστη και τις επιπτώσεις στην ταχύτητα του δικτύου.

9.4.7 Έλεγχος δικτυακών συνδέσεων

Η πολιτική ελέγχου της πρόσβασης σε ένα δίκτυο, ιδιαίτερα αν αυτό εκτείνεται πέραν των ορίων του οργανισμού, μπορεί να απαιτεί τον έλεγχο και τον περιορισμό των συνδέσεων που

είναι διαθέσιμες στους χρήστες. Τέτοιοι μηχανισμοί μπορεί να περιλαμβάνουν δικτυακές πύλες που ελέγχουν τις επικοινωνίες με βάση προκαθορισμένα σύνολα κανόνων. Οι περιορισμοί που θα επιβάλλονται, θα πρέπει να είναι σύμφωνοι με την πολιτική του οργανισμού και τις απαιτήσεις των εφαρμογών που χρησιμοποιεί.

Παραδείγματα εφαρμογών στις οποίες θα πρέπει να επιβληθούν περιορισμοί είναι:

- Το ηλεκτρονικό ταχυδρομείο.
- Οι μεταφορές αρχείων (μονόδρομα και αμφίδρομα).
- Η διαδραστική (interactive) πρόσβαση.
- Η δικτυακή πρόσβαση με βάση την ώρα και την ημερομηνία.

9.4.8 Έλεγχος της δρομολόγησης (routing)

Ο έλεγχος της δρομολόγησης της μεταφοράς των δεδομένων είναι απαραίτητος στα δίκτυα, ειδικά σε αυτά που ξεπερνούν τα όρια του οργανισμού. Με αυτόν τον τρόπο προστατεύεται το πληροφοριακό σύστημα από μή εξουσιοδοτημένες συνδέσεις ή ροές δεδομένων, ιδιαίτερα όταν δίνεται πρόσβαση σε τρίτους, οι οποίοι δεν ανήκουν στο προσωπικό του οργανισμού.

Οι μηχανισμοί ελέγχου της δρομολόγησης θα πρέπει να επιβεβαιώνουν τόσο την πηγή, όσο και τον προορισμό μιας επικοινωνίας. Οι μηχανισμοί μετάφρασης των διευθύνσεων που χρησιμοποιεί ένα δίκτυο (Network Address Translation - NAT), είναι ιδιαίτερα χρήσιμοι για την απόκρυψη ενός δικτύου και τον περιορισμό των δυνατών δρομολογίων που γίνονται γνωστοί ανάμεσα σε δύο ή περισσότερα διαφορετικά δίκτυα. Το NAT ουσιαστικά αποκρύπτει τη δομή ενός δικτύου από το εξωτερικό περιβάλλον.

9.4.9 Ασφάλεια δικτυακών υπηρεσιών

Ένα μεγάλο εύρος δημόσιων και ιδιωτικών δικτυακών υπηρεσιών είναι διαθέσιμο στους χρήστες, με αρκετές από αυτές να προσθέτουν και αξία στη χρήση του δικτύου. Η κάθε υπηρεσία έχει τις δικές της απαιτήσεις ασφάλειας. Ο οργανισμός θα πρέπει να γνωρίζει όλες

τις παραμέτρους λειτουργίας μιας δικτυακής υπηρεσίας, ώστε να μπορέσει να λάβει κατάλληλα μέτρα για την προστασία της.

9.5 Έλεγχος πρόσβασης στο λειτουργικό σύστημα

Σκοπός είναι η αποτροπή της μη εξουσιοδοτημένης πρόσβασης στο σύστημα. Οι μηχανισμοί ασφάλειας που μπορεί να διαθέτει το σύστημα σε επίπεδο λειτουργικού συστήματος, θα πρέπει να χρησιμοποιούνται για τον περιορισμό της πρόσβασης στους διάφορους πόρους. Οι συγκεκριμένοι μηχανισμοί θα πρέπει να είναι σε θέση να:

- Αναγνωρίζουν και να επιβεβαιώνουν την ταυτότητα του χρήστη και αν είναι δυνατό και του τερματικού που αυτός χρησιμοποιεί.
- Καταγράφουν επιτυχείς και ανεπιτυχείς προσπάθειες πρόσβασης.
- Παρέχουν κατάλληλους μηχανισμούς για αυθεντικοποίηση, οι οποίοι θα πρέπει να είναι σύμφωνοι με την πολιτική του οργανισμού (παράγραφος 9.3.1).
- Περιορίζουν το χρόνο πρόσβασης των χρηστών αν αυτό κρίνεται απαραίτητο.

Επιπλέον μηχανισμοί ελέγχου μπορούν να χρησιμοποιούνται, εφόσον κρίνονται αναγκαίοι για την κάλυψη των αναγκών του οργανισμού.

9.5.1 Αναγνώριση τερματικών

Διαδικασίες αυτόματης αναγνώρισης των τερματικών μπορούν να χρησιμοποιηθούν για την αυθεντικοποίηση συνδέσεων σε συγκεκριμένα μέρη του συστήματος ή φορητό εξοπλισμό. Μπορούν να χρησιμοποιηθούν αν είναι αναγκαίο να διασφαλιστεί ότι η σύνδεση ξεκίνησε από κάποιο συγκεκριμένο σημείο. Ένα μέσο αναγνώρισης μπορεί να χρησιμοποιηθεί για τον καθορισμό των τερματικών από τα οποία μπορούν να γίνουν διάφορες ευαίσθητες εργασίες ή συναλλαγές. Θα πρέπει βέβαια να προστατεύεται κατάλληλα και το ίδιο το τερματικό ώστε να μην εκτεθεί η ταυτότητά του σε κίνδυνο. Για την αυθεντικοποίηση των χρηστών υπάρχουν πολλές διαθέσιμες τεχνικές (παράγραφος 9.4.3).

9.5.2 Διαδικασίες σύνδεσης στο σύστημα

Η πρόσβαση στις υπηρεσίες του πληροφοριακού συστήματος θα πρέπει να αποκτάται μέσω κάποιας ασφαλούς διαδικασίας εισόδου στο σύστημα (log-on). Μια τέτοια διαδικασία θα πρέπει να είναι έτσι σχεδιασμένη ώστε να ελαχιστοποιείται ο κίνδυνος μη εξουσιοδοτημένης πρόσβασης. Κατά συνέπεια θα πρέπει να αποκαλύπτει τις ελάχιστες δυνατές πληροφορίες για το σύστημα, ώστε να μη βοηθά τους μη εξουσιοδοτημένους χρήστες να ανακαλύψουν τη δομή του. Μια τέτοια διαδικασία θα πρέπει:

- Να μην εμφανίζει στην οθόνη διάφορα χαρακτηριστικά της ταυτότητας του χρήστη ή του συστήματος, έως ότου ολοκληρωθεί επιτυχώς.

- Να εμφανίζει προειδοποιητικά μηνύματα που να ενημερώνουν ότι η πρόσβαση επιτρέπεται μόνο στους εξουσιοδοτημένους χρήστες του συστήματος.

- Να μην εμφανίζει βοηθητικά μηνύματα που θα μπορούσαν να χρησιμοποιηθούν από μη εξουσιοδοτημένους χρήστες.

- Να επιβεβαιώνει τις απαιτούμενες πληροφορίες αφού εισαχθούν όλες στο σύστημα. Σε περίπτωση λάθους να μην ενημερώνει ποια πληροφορία απορρίφθηκε από το σύστημα.

- Να περιορίζει τον αριθμό των δυνατών προσπαθειών του χρήστη για να συνδεθεί. Παράλληλα, θα πρέπει να καταγράφει τις ανεπιτυχείς προσπάθειες, να επιβάλει ένα χρονικό όριο πριν επιτρέψει ξανά στο χρήστη να προσπαθήσει και να αποσυνδέει όλες τις πιθανές συνδέσεις επικοινωνίας.

- Να περιορίζει το χρόνο που έχει ο χρήστης στη διάθεσή του για να κάνει log-on.

- Μετά την επιτυχή ολοκλήρωση της διαδικασίας να εμφανίζει την ώρα και την ημερομηνία της τελευταίας επιτυχούς προσπάθειας του χρήστη και τις όποιες μη επιτυχείς προσπάθειες έγιναν στο μεταξύ.

9.5.3 Αυθεντικοποίηση χρηστών

Όλοι οι χρήστες του συστήματος (τεχνικό προσωπικό, διαχειριστές, προγραμματιστές, κοινοί χρήστες κλπ.), θα πρέπει να έχουν ένα μοναδικό αναγνωριστικό (user ID), για καθαρά προσωπική τους χρήση στο σύστημα. Με αυτόν τον τρόπο είναι δυνατός ο εντοπισμός του υπεύθυνου ατόμου για όλες τις δραστηριότητες που γίνονται στο πληροφοριακό σύστημα του οργανισμού. Επιπλέον, τα user IDs δεν πρέπει να φανερώνουν τα δικαιώματα του χρήστη στο σύστημα. Σε εξαιρετικές περιπτώσεις, και εφόσον κάτι τέτοιο είναι απαραίτητο για τον οργανισμό, μια ομάδα χρηστών μπορεί να μοιράζεται το ίδιο user ID για την εκτέλεση συγκεκριμένων εργασιών στο σύστημα. Σε μια τέτοια περίπτωση θα πρέπει να υπάρχει ειδική έγκριση από τη διοίκηση του οργανισμού, όπως επίσης και να χρησιμοποιηθεί κάποιος μηχανισμός που θα καθορίζει τις ευθύνες των μελών της ομάδας.

Υπάρχουν διάφορες διαδικασίες αυθεντικοποίησης που μπορούν να χρησιμοποιηθούν για την επιβεβαίωση της ταυτότητας ενός χρήστη. Τα συνθηματικά είναι ο πλέον συνηθισμένος τρόπος (παράγραφοι 9.3.1 και 9.5.4), ο οποίος βασίζεται στη χρήση ενός μυστικού, γνωστού μόνο στο χρήστη. Άλλοι μηχανισμοί αυθεντικοποίησης περιλαμβάνουν συνδυασμούς κρυπτογραφίας και πρωτοκόλλων εξακρίβωσης της ταυτότητας του χρήστη.

Διάφορα αντικείμενα, όπως έξυπνες κάρτες, τα οποία έχει στην κατοχή του ο χρήστης, μπορούν επίσης να χρησιμοποιηθούν για αυθεντικοποίηση στο σύστημα. Ένας άλλος τρόπος εξακρίβωσης της ταυτότητας, περιλαμβάνει την εξέταση διάφορων βιομετρικών χαρακτηριστικών του χρήστη, όπως είναι τα δακτυλικά αποτυπώματα. Ο συνδυασμός πολλαπλών τεχνολογιών εξακρίβωσης της ταυτότητας, έχει ως αποτέλεσμα ισχυρότερη αυθεντικοποίηση.

9.5.4 Διαχείριση συνθηματικών

Τα συνθηματικά είναι ο πιο διαδεδομένος τρόπος για την επιβεβαίωση της ταυτότητας ενός χρήστη. Ο οργανισμός θα πρέπει να διαθέτει ένα σύστημα διαχείρισης συνθηματικών, το οποίο να εξασφαλίζει τη χρήση ποιοτικών συνθηματικών από τους τελικούς χρήστες του πληροφοριακού συστήματος (παράγραφος 9.3.1).

Κάποιες εφαρμογές απαιτούν τη χρήση συνθηματικών, τα οποία έχουν δοθεί από μια ανεξάρτητη αρχή. Στις περισσότερες όμως περιπτώσεις επιλέγονται από τους ίδιους τους χρήστες. Ένα καλό σύστημα διαχείρισης συνθηματικών θα πρέπει να:

- Επιβάλει τη χρήση ατομικών συνθηματικών ώστε να μπορεί να γίνει συσχέτιση των εργασιών στο σύστημα με συγκεκριμένους χρήστες.
- Όπου είναι κατάλληλο, να επιτρέπεται στους χρήστες να επιλέγουν το προσωπικό τους συνθηματικό. Επιπλέον θα πρέπει να περιλαμβάνονται μηχανισμοί για τη διόρθωση εισαγωγής λανθασμένων στοιχείων από το χρήστη.
- Επιβάλει τη χρήση ποιοτικών συνθηματικών, κατάλληλων για την κάλυψη των αναγκών του οργανισμού.
- Επιβάλει την τακτική αλλαγή των συνθηματικών όπως περιγράφεται στην παράγραφο 9.3.1.
- Επιβάλει την αλλαγή των προσωρινών συνθηματικών κατά την πρώτη είσοδο του χρήστη στο σύστημα.
- Τηρεί ιστορικό των συνθηματικών που χρησιμοποιεί ο κάθε χρήστης για την αποτροπή ανακύκλωσης της χρήσης τους μέσα σε καθορισμένο χρονικό διάστημα.
- Μην εμφανίζει τα συνθηματικά στην οθόνη κατά την εισαγωγή τους.
- Φυλάσσει τα συνθηματικά ξεχωριστά από τα δεδομένα των εφαρμογών και με τρόπο ασφαλή, ενδεχομένως με χρήση μονόδρομης κρυπτογράφησης.
- Αλλάζει τα προκαθορισμένα συνθηματικά που χρησιμοποιούνται από τους κατασκευαστές κατά την εγκατάσταση εφαρμογών στο σύστημα.

9.5.5 Χρήση εργαλείων συστήματος

Τα περισσότερα υπολογιστικά συστήματα διαθέτουν ένα ή περισσότερα ειδικά εργαλεία (system utilities), τα οποία μπορούν να παρακάμπτουν μηχανισμούς ελέγχου του ίδιου του

συστήματος ή των εφαρμογών. Είναι απαραίτητο η χρήση τους να είναι περιορισμένη και αυστηρά ελεγχόμενη. Θα πρέπει να εξεταστούν οι ακόλουθοι μηχανισμοί:

- Η χρήση διαδικασιών αυθεντικοποίησης για τα εργαλεία του συστήματος.
- Διαχωρισμός των εργαλείων αυτών από τις υπόλοιπες εφαρμογές.
- Περιορισμός της χρήσης τους από ένα μικρό αριθμό έμπιστων χρηστών.
- Ειδική εξουσιοδότηση για τη χρήση τέτοιων εργαλείων.
- Περιορισμός της διαθεσιμότητας των εργαλείων συστήματος (π.χ. μόνο κατά τη διάρκεια απαραίτητων μεταβολών στο σύστημα).
- Καταγραφή της χρήσης των εργαλείων του συστήματος.
- Καθορισμός των επιπέδων εξουσιοδότησης για τη χρήση τους.
- Απομάκρυνση των μή απαραίτητων εργαλείων από το σύστημα.

9.5.6 Συναγερμός απειλής για την προστασία των χρηστών

Ο οργανισμός θα πρέπει να εξετάσει την εφαρμογή ενός ειδικού συναγερμού απειλής για την προστασία των χρηστών που μπορεί να ενεργούν κακόβουλα λόγω εξαναγκασμού. Η χρήση ενός τέτοιου μηχανισμού θα πρέπει να αποφασιστεί κατόπιν σχετικής αποτίμησης κινδύνου. Επιπλέον θα πρέπει να υπάρχουν προκαθορισμένες αρμοδιότητες και καθήκοντα για την αντίδραση του οργανισμού σε έναν τέτοιο συναγερμό.

9.5.7 Time-out τερματικών

Τα ανενεργά τερματικά, ειδικά αυτά που βρίσκονται τοποθετημένα σε περιοχές υψηλού κινδύνου, όπως δημόσιους χώρους, θα πρέπει να κλείνουν μετά από κάποιο χρονικό διάστημα. Με αυτόν τον τρόπο προστατεύεται το σύστημα του οργανισμού από μη εξουσιοδοτημένους χρήστες που μπορεί να προσπαθήσουν να χρησιμοποιήσουν ένα τέτοιο τερματικό. Θα πρέπει να τερματίζονται οι ενεργές συνδέσεις του τερματικού, οι εφαρμογές

που τρέχει και να καθαρίζει η οθόνη του από κάθε στοιχείο. Το χρονικό όριο για το οποίο ένα τερματικό θα μπορεί να παραμείνει ανενεργό, εξαρτάται άμεσα από τους κινδύνους του χώρου που βρίσκεται το τερματικό, όπως και από τη φύση των χρηστών του.

Για σταθμούς εργασίας μπορεί να χρησιμοποιηθεί ένας λιγότερο δραστικός μηχανισμός, ο οποίος θα καθαρίζει την οθόνη και θα κλειδώνει με κάποιο συνθηματικό τον υπολογιστή, αλλά δε θα τερματίζει της εφαρμογές ή τις συνδέσεις του.

9.5.8 Περιορισμός χρόνου σύνδεσης

Για εφαρμογές που χαρακτηρίζονται ευαίσθητες για τον οργανισμό, θα πρέπει να επιβάλλεται και ένα χρονικό όριο στη σύνδεση του χρήστη με αυτές. Με τον περιορισμό της χρονικής περιόδου κατά την οποία τα τερματικά μπορούν να έχουν πρόσβαση στις υπηρεσίες του συστήματος, περιορίζονται σημαντικά οι ευκαιρίες των μη εξουσιοδοτημένων χρηστών για να αποκτήσουν πρόσβαση στο σύστημα. Τέτοιοι μηχανισμοί είναι απαραίτητοι για όλες τις κρίσιμες εφαρμογές, ειδικά αυτές που έχουν τερματικά σε χώρους υψηλού κινδύνου.

Οι μηχανισμοί περιορισμού μπορούν να περιλαμβάνουν:

- Τη χρήση προκαθορισμένων χρονικών περιόδων μέσα στα πλαίσια των οποίων θα πρέπει να ολοκληρωθεί κάποια εργασία.

- Τον περιορισμό των δυνατοτήτων σύνδεσης στο σύστημα μόνο σε συγκεκριμένες ώρες (π.χ. κατά το ωράριο εργασίας).

9.6 Έλεγχος της πρόσβασης στις εφαρμογές

Σκοπός είναι η αποτροπή της μη εξουσιοδοτημένης πρόσβασης στις πληροφορίες που βρίσκονται στο σύστημα. Θα πρέπει να χρησιμοποιούνται ειδικοί μηχανισμοί για τον περιορισμό της πρόσβασης στις εφαρμογές του πληροφοριακού συστήματος. Επιπλέον, η λογική πρόσβαση σε προγράμματα και πληροφορίες θα πρέπει να δίνεται μόνο στους εξουσιοδοτημένους χρήστες. Οι εφαρμογές του συστήματος θα πρέπει να:

- Ελέγχουν την πρόσβαση του χρήστη σε διάφορες λειτουργίες και δεδομένα, σύμφωνα με την πολιτική του οργανισμού.

- Παρέχουν προστασία από μη εξουσιοδοτημένη πρόσβαση για χρήση λειτουργιών του λειτουργικού συστήματος, ικανών να παρακάμψουν τους μηχανισμούς ασφάλειας και ελέγχου.

- Προστατεύουν και την ασφάλεια άλλων συστημάτων, με τα οποία διαμοιράζονται δεδομένα.

- Παρέχουν πρόσβαση στα δεδομένα του συστήματος μόνο στους εξουσιοδοτημένους χρήστες ή ομάδες χρηστών.

9.6.1 Περιορισμοί πρόσβασης στις πληροφορίες

Τα δικαιώματα προσπέλασης των χρηστών των εφαρμογών του συστήματος, θα πρέπει να είναι σύμφωνα με την πολιτική ασφάλειας του οργανισμού. Θα πρέπει επίσης να λαμβάνονται υπόψη οι ανάγκες όλων των ομάδων των χρηστών του συστήματος (προσωπικό, εξωτερικοί συνεργάτες, προσωπικό υποστήριξης κλπ.), όπως και οι επιχειρησιακές ανάγκες του οργανισμού. Στην κατεύθυνση αυτή, μπορούν να χρησιμεύσουν οι ακόλουθοι μηχανισμοί:

- Η χρήση μενού επιλογών μέσω των οποίων θα ελέγχεται και θα κατευθύνεται η χρήση των εφαρμογών.

- Ο περιορισμός των γνώσεων των χρηστών για τις εφαρμογές του συστήματος, στα απολύτως απαραίτητα για την εργασία τους.

- Ο έλεγχος των δικαιωμάτων πρόσβασης των χρηστών.

- Η διασφάλιση του ότι τα παράγωγα εφαρμογών που χειρίζονται ευαίσθητα δεδομένα (εκτυπώσεις, αρχεία κλπ.) κατευθύνονται μόνο στα κατάλληλα προστατευμένα και διαβαθμισμένα τερματικά.

9.6.2 Απομόνωση ευαίσθητων συστημάτων

Τα ευαίσθητα συστήματα μπορεί να απαιτούν ένα ειδικό, απομονωμένο περιβάλλον λειτουργίας. Κάποια συστήματα μπορεί να απαιτούν ειδική μεταχείριση ώστε να αποφευχθεί το ενδεχόμενο απώλειας δεδομένων. Ο βαθμός ευαισθησίας του συστήματος μπορεί να ορίζει ότι οι εφαρμογές θα πρέπει να τρέχουν σε ένα ειδικό υπολογιστικό σύστημα, ότι θα πρέπει να μοιράζεται δεδομένα με άλλα έμπιστα συστήματα, ή να μην απαιτεί καμιά επιπλέον προστασία. Θα πρέπει να εξεταστούν τα ακόλουθα:

- Η ευαισθησία ενός συστήματος θα πρέπει να καθορίζεται από την ευαισθησία των εφαρμογών του.
- Όταν κάποια ευαίσθητη εφαρμογή πρέπει να εκτελεστεί σε περιβάλλον δικτύου, όλοι οι επιπλέον πόροι θα πρέπει να καθοριστούν και να συμφωνηθούν με τον ιδιοκτήτη της ευαίσθητης εφαρμογής.

9.7 Παρακολούθηση προσπέλασης και χρήσης συστήματος

Σκοπός είναι ο εντοπισμός μη εξουσιοδοτημένων ενεργειών. Τα υπολογιστικά συστήματα του οργανισμού θα πρέπει να παρακολουθούνται για τον εντοπισμό παραβιάσεων της πολιτικής ασφάλειας και την καταγραφή στοιχείων για μια τέτοια περίπτωση. Η παρακολούθηση του συστήματος μπορεί να χρησιμοποιηθεί και για την επιβεβαίωση της αποτελεσματικότητας των μηχανισμών προστασίας που χρησιμοποιούνται, καθώς και για τη συμμόρφωση με την πολιτική ασφάλειας του οργανισμού.

9.7.1 Καταγραφή γεγονότων

Στο σύστημα θα πρέπει να τηρούνται αρχεία που να καταγράφουν κάθε συμβάν σχετικό με την ασφάλεια του συστήματος. Τα αρχεία αυτά (audit logs) θα πρέπει να φυλάσσονται για συγκεκριμένο χρονικό διάστημα ώστε να είναι δυνατή η χρησιμοποίηση τους σε ενδεχόμενες έρευνες. Θα πρέπει να περιλαμβάνουν τα ακόλουθα:

- Την ταυτότητα των χρηστών (user IDs).
- Τον ακριβή χρόνο σύνδεσης και αποσύνδεσης του χρήστη.

- Το τερματικό το οποίο χρησιμοποιεί ο χρήστης.
- Τις επιτυχείς αλλά και τις ανεπιτυχείς προσπάθειες του χρήστη να προσπελάσει το σύστημα.
- Τις επιτυχείς και τις ανεπιτυχείς προσπάθειες του χρήστη να προσπελάσει δεδομένα του συστήματος.

Κάποια από τα αρχεία που τηρούνται στο σύστημα είναι δυνατό να διατηρούνται για αρκετό χρονικό διάστημα, σύμφωνα με τις ανάγκες του οργανισμού ή τη σχετική νομοθεσία (κεφάλαιο 12).

9.7.2 Καταγραφή της χρήσης του συστήματος

9.7.2.1 Διαδικασίες και περιοχές κινδύνου

Ο οργανισμός θα πρέπει να χρησιμοποιεί διαδικασίες μέσω των οποίων θα παρακολουθεί τη χρήση του υπολογιστικού συστήματος. Με αυτόν τον τρόπο διασφαλίζεται η εξουσιοδοτημένη χρήση του συστήματος από τα κατάλληλα πρόσωπα και για το σκοπό που τους είναι απαραίτητο. Η αυστηρότητα της παρακολούθησης, εξαρτάται από τις ανάγκες του οργανισμού και προκύπτει μετά από τη διενέργεια αποτίμησης κινδύνου. Θα πρέπει να παρακολουθούνται τα ακόλουθα:

- Η εξουσιοδοτημένη πρόσβαση (χρήστης, ώρα, τύπος πρόσβασης, πόροι που προσπελάσθηκαν, προγράμματα που χρησιμοποιήθηκαν).
- Η χρήση ειδικών προνομίων στο σύστημα (χρήση προνομιακών συνθηματικών χρηστών, έναρξη και τερματισμός λειτουργίας του συστήματος, χρήση εξωτερικών συσκευών).
- Οι προσπάθειες μη εξουσιοδοτημένης πρόσβασης (αποτυχημένες προσπάθειες, μηνύματα από ηλεκτρονικές πύλες ασφαλείας ή συστήματα ανίχνευσης επιθέσεων - intrusion detection).
- Μηνύματα του συστήματος (μηνύματα λάθους, μηνύματα δικτύου κλπ.).

9.7.2.2 Παράγοντες κινδύνου

Τα αρχεία (logs) που προκύπτουν από την παρακολούθηση του συστήματος θα πρέπει να ελέγχονται τακτικά. Η συχνότητα ελέγχου εξαρτάται από τους κινδύνους που αντιμετωπίζει το πληροφοριακό σύστημα του οργανισμού. Θα πρέπει να εξεταστούν οι ακόλουθοι παράγοντες κινδύνου:

- Η κρισιμότητα των εφαρμογών.
- Η αξία των δεδομένων για τον οργανισμό.
- Το ιστορικό προσπαθειών κατάχρησης του συστήματος ή μη εξουσιοδοτημένης πρόσβασης.

- Το εύρος της δικτύωσης του συστήματος, ειδικά όταν αυτή περιλαμβάνει δημόσια δίκτυα.

9.7.2.3 Καταγραφή και έλεγχος γεγονότων

Ο έλεγχος των αρχείων που προκύπτουν από την καταγραφή των διάφορων γεγονότων που σχετίζονται με τη λειτουργία του συστήματος, περιλαμβάνει τόσο την κατανόηση των ίδιων των κινδύνων που απειλούν το σύστημα, όσο και τον τρόπο με τον οποίο μπορούν να υλοποιηθούν. Παραδείγματα γεγονότων για τα οποία μπορεί να απαιτείται περαιτέρω έλεγχος δίνονται στην παράγραφο 9.7.1.

Τα αρχεία καταγραφής πολλές φορές περιέχουν πάρα πολλή πληροφορία, μεγάλο μέρος της οποίας είναι άσχετο με την ασφάλεια του συστήματος. Προκειμένου να διευκολυνθεί η διαδικασία εντοπισμού συμβάντων σχετικών με την ασφάλεια, θα πρέπει να εξεταστεί το ενδεχόμενο αυτόματης καταγραφής των σχετικών γεγονότων και σε ένα δεύτερο αρχείο. Το αρχείο αυτό θα μπορεί στη συνέχεια να επεξεργαστεί με τη χρήση ειδικών προγραμμάτων.

Επιθυμητό θα ήταν επίσης να διαχωριστούν οι ρόλοι αυτών που ελέγχουν τα αρχεία και αυτών των οποίων οι ενέργειες καταγράφονται. Ειδική προσοχή θα πρέπει να δοθεί στην ασφάλεια των ίδιων των αρχείων καταγραφής. Αν κάποιος μπορεί να επέμβει σε αυτά και να μεταβάλει τις πληροφορίες που περιέχουν, τότε ο οργανισμός μπορεί να έχει μια ψευδή αίσθηση ασφάλειας. Οι κίνδυνοι που απειλούν τα αρχεία καταγραφής περιλαμβάνουν:

- Την απενεργοποίηση των διαδικασιών καταγραφής.
- Την αλλαγή των τύπων των καταγεγραμμένων μηνυμάτων.
- Την επέμβαση στα περιεχόμενα των αρχείων.
- Την πλήρωση των μέσων αποθήκευσης των αρχείων καταγραφής (π.χ. σκληροί δίσκοι), με αποτέλεσμα να μην είναι δυνατή η περαιτέρω καταγραφή γεγονότων.

9.7.3 Συγχρονισμός των συστημάτων

Η σωστή ρύθμιση των ρολογιών των υπολογιστών είναι ιδιαίτερα σημαντική για την ακρίβεια των περιεχομένων των αρχείων καταγραφής, ειδικά όταν πρόκειται να χρησιμοποιηθούν ως αποδεικτικά στοιχεία σε κάποια έρευνα. Όταν κάποια συσκευή διαθέτει ρολόι πραγματικού χρόνου, αυτό θα πρέπει να ρυθμιστεί σύμφωνα με κάποιο συγκεκριμένο πρότυπο (π.χ. Universal Coordinated Time – UCT) ή την τοπική ώρα. Εφόσον κάποια τέτοια ρολόγια δεν είναι ιδιαίτερα ακριβή, θα πρέπει να υπάρχει κάποια διαδικασία ελέγχου και διόρθωσης της ώρας που δείχνουν.

9.8 Τηλεεργασία και κινητή υπολογιστική

Σκοπός είναι η προστασία του πληροφοριακού συστήματος του οργανισμού, όταν χρησιμοποιούνται τεχνικές και εξοπλισμός τηλεεργασίας ή κινητής υπολογιστικής (mobile computing). Η απαιτούμενη προστασία πρέπει να είναι ανάλογη των κινδύνων που απειλούν το σύστημα. Στην περίπτωση της κινητής υπολογιστικής θα πρέπει να εξεταστούν οι κίνδυνοι εργασίας σε ένα μη ελεγχόμενο και απροστάτευτο περιβάλλον. Στην περίπτωση της τηλεεργασίας, ο οργανισμός θα πρέπει να εφαρμόσει τους κατάλληλους μηχανισμούς προστασίας στην τοποθεσία από την όποια θα γίνεται τηλεεργασία.

9.8.1 Κινητή υπολογιστική

Κατά τη χρήση εξοπλισμού κινητής υπολογιστικής (φορητοί υπολογιστές, υπολογιστές χειρός, κινητά τηλέφωνα κλπ.) απαιτείται προσοχή ώστε να διασφαλιστεί η προστασία του πληροφοριακού συστήματος του οργανισμού. Θα πρέπει να υιοθετηθεί μια επίσημη πολιτική που να περιλαμβάνει την αντιμετώπιση των κινδύνων που σχετίζονται με την κινητή υπολογιστική, ειδικά σε περιβάλλον που δεν είναι προστατευμένο. Μια τέτοια πολιτική θα πρέπει να περιλαμβάνει μηχανισμούς φυσικής προστασίας, κρυπτογραφίας, προστασίας από ιούς, ελέγχου πρόσβασης και λήψης εφεδρικών αντιγράφων. Θα πρέπει επίσης να περιλαμβάνει οδηγίες για τη χρήση δημόσιων δικτύων και χρήσης του εξοπλισμού σε δημόσιους χώρους.

Ιδιαίτερη προσοχή θα πρέπει να δοθεί στη χρήση εξοπλισμού σε δημόσιους χώρους, συνεδριακούς χώρους και κάθε απροστάτευτο χώρο, εκτός των εγκαταστάσεων του

οργανισμού. Θα πρέπει να χρησιμοποιούνται οι κατάλληλοι μηχανισμοί προστασίας από μη εξουσιοδοτημένη πρόσβαση στον εξοπλισμό ή έκθεση των δεδομένων που περιέχονται σε αυτόν. Ένας συνηθισμένος μηχανισμός προστασίας είναι η χρήση τεχνικών κρυπτογραφίας (παράγραφος 10.3). Ένας άλλος σημαντικός κίνδυνος σε δημόσιους χώρους είναι η υποκλοπή από τρίτους που παρατηρούν τη χρήση του εξοπλισμού. Επιπλέον ο εξοπλισμός θα πρέπει να είναι κατάλληλα προστατευμένος από ιούς και να διαθέτει μηχανισμούς γρήγορης και εύκολης λήψης εφεδρικών αντιγράφων. Τα μέσα του τελευταίου θα πρέπει να προστατεύονται επαρκώς. Επίσης, η πρόσβαση στο πληροφοριακό σύστημα του οργανισμού μέσω δημόσιων δικτύων θα πρέπει να ελέγχεται με κατάλληλα μέσα αυθεντικοποίησης και ελέγχου πρόσβασης.

Ο εξοπλισμός κινητής υπολογιστικής είναι ιδιαίτερα ευάλωτος σε κλοπή. Θα πρέπει να προστατεύεται ανάλογα με ειδικές κλειδαριές και θήκες μεταφοράς, ειδικά όταν περιέχει ευαίσθητα για τον οργανισμό δεδομένα. Επίσης, το προσωπικό του οργανισμού θα πρέπει να είναι κατάλληλα ενημερωμένο και εκπαιδευμένο σχετικά με τους κινδύνους κινητής υπολογιστικής.

9.8.2 Τηλεεργασία

Η τηλεεργασία χρησιμοποιεί τεχνολογίες των τηλεπικοινωνιών προκειμένου το προσωπικό να μπορεί να εργάζεται από μια προκαθορισμένη τοποθεσία, εκτός των εγκαταστάσεων του οργανισμού. Η τοποθεσία αυτή θα πρέπει να προστατεύεται κατάλληλα απέναντι σε κλοπή εξοπλισμού και πληροφοριών, την κατάχρηση των εγκαταστάσεων, αλλά και τη μη εξουσιοδοτημένη πρόσβαση στα συστήματα του οργανισμού. Η τηλεεργασία θα πρέπει να έχει την έγκριση της διοίκησης, να ελέγχεται από αυτήν και προϋποθέτει την ύπαρξη των κατάλληλων συνθηκών για το συγκεκριμένο τρόπο εργασίας.

Ο οργανισμός θα πρέπει να έχει την κατάλληλη πολιτική, όπου με συγκεκριμένους μηχανισμούς, διαδικασίες και πρότυπα θα ελέγχει τα ζητήματα σχετικά με την τηλεεργασία. Η τηλεεργασία είναι αποδεκτή και χρήσιμη μόνον όταν είναι συμβατή και με την πολιτική ασφάλειας του οργανισμού. Θα πρέπει να εξετασθούν τα ακόλουθα:

- Η υπάρχουσα φυσική προστασία της τοποθεσίας από την οποία θα γίνεται η τηλεεργασία.

- Το προτεινόμενο περιβάλλον τηλεεργασίας.
- Οι απαιτήσεις ασφάλειας των τηλεπικοινωνιών, δεδομένων των αναγκών πρόσβασης στο σύστημα του οργανισμού και το ευαίσθητο των πληροφοριών.
- Ο κίνδυνος από τη μη εξουσιοδοτημένη πρόσβαση στους πόρους του συστήματος από άλλα άτομα που βρίσκονται στην ίδια τοποθεσία (π.χ. μέλη της οικογενείας υπαλλήλου που εργάζεται από το σπίτι του).

Οι μηχανισμοί ασφάλειας περιλαμβάνουν τα ακόλουθα:

- Τη παροχή του κατάλληλου εξοπλισμού για τις δραστηριότητες της τηλεεργασίας.
- Τον καθορισμό του ωραρίου εργασίας, του χρονικού διαστήματος κατά το οποίο είναι δυνατή η τηλεεργασία και την πρόσβαση στους απαιτούμενους πόρους του πληροφοριακού συστήματος του οργανισμού.
- Την παροχή του κατάλληλου τηλεπικοινωνιακού εξοπλισμού, συμπεριλαμβανομένων των μεθόδων διασφάλισης της απομακρυσμένης πρόσβασης στο σύστημα.
- Τη φυσική ασφάλεια.
- Τους κανόνες χρήσης του εξοπλισμού από τρίτους.
- Την παροχή τεχνικής υποστήριξης.
- Τις διαδικασίες λήψης εφεδρικών αντιγράφων ασφαλείας και επιχειρησιακής συνέχειας.
- Τις διαδικασίες ελέγχου και καταγραφής των ενεργειών στο σύστημα.
- Τις διαδικασίες επιστροφής του εξοπλισμού και ανάκλησης των δικαιωμάτων του χρήστη όταν παύσει η ανάγκη τηλεεργασίας.

10. Ανάπτυξη και συντήρηση συστημάτων

10.1 Απαιτήσεις ασφάλειας των συστημάτων

Σκοπός είναι η διασφάλιση ότι η ασφάλεια είναι υλοποιημένη μέσα στα πληροφοριακά συστήματα. Αυτό περιλαμβάνει την υποδομή, τις εφαρμογές του οργανισμού και τις εφαρμογές που αναπτύσσουν οι χρήστες. Ο τρόπος με τον οποίο παρέχεται υποστήριξη στο πληροφοριακό σύστημα του οργανισμού μπορεί να είναι ιδιαίτερα σημαντικός για την ασφάλεια. Οι απαιτήσεις ασφάλειας θα πρέπει να καθοριστούν και να συμφωνηθούν πριν από την ανάπτυξη των εφαρμογών. Το ίδιο θα πρέπει να γίνει και για τις διαδικασίες επαναφοράς του συστήματος σε κάποια προηγούμενη κατάσταση λειτουργίας (fall back).

10.1.1 Ανάλυση απαιτήσεων ασφάλειας και προδιαγραφές

Ο οργανισμός θα πρέπει να διατυπώνει επίσημα τις απαιτήσεις του σχετικά με την ανάπτυξη νέων συστημάτων ή την επέκταση των υπαρχόντων. Οι σχετικές προδιαγραφές θα πρέπει να περιλαμβάνουν την ενσωμάτωση αυτόματων μηχανισμών στο σύστημα, αλλά και τη χρήση χειροκίνητων μηχανισμών. Αντίστοιχες προδιαγραφές θα πρέπει να υπάρχουν για τη δοκιμή και αξιολόγηση εφαρμογών. Επιπλέον, αν η διοίκηση κρίνει σκόπιμο μπορεί να χρησιμοποιήσει πιστοποιημένα ή δοκιμασμένα από τρίτους προϊόντα.

Οι απαιτήσεις ασφάλειας και οι χρησιμοποιούμενοι μηχανισμοί προστασίας θα πρέπει να είναι ανάλογοι της αξίας για τον οργανισμό των πληροφοριών, καθώς και το πιθανό κόστος της απώλειας ή της έκθεσής τους. Αυτό μπορεί να διασφαλιστεί με τη χρήση τεχνικών αποτίμησης και διαχείρισης κινδύνου. Οι μηχανισμοί ελέγχου που συμπεριλαμβάνονται κατά τη σχεδίαση ενός συστήματος, έχουν σημαντικά χαμηλότερο κόστος υλοποίησης και λειτουργίας από τους μηχανισμούς που υλοποιούνται μετά την ολοκλήρωση του συστήματος.

10.2 Ασφάλεια εφαρμογών

Σκοπός είναι η αποτροπή κατάχρησης, απώλειας ή αλλαγής των δεδομένων στις εφαρμογές του συστήματος. Οι μηχανισμοί καταγραφής των ενεργειών στο σύστημα θα πρέπει να είναι

έτσι σχεδιασμένοι ώστε να καλύπτουν και τις εφαρμογές. Θα πρέπει επίσης να περιλαμβάνουν τον έλεγχο της εγκυρότητας των προς εισαγωγή δεδομένων, την επεξεργασία τους και τα αποτελέσματα της τελευταίας. Επιπλέον προστασία μπορεί να απαιτείται για τα συστήματα που επεξεργάζονται ευαίσθητα για τον οργανισμό δεδομένα.

10.2.1 Έλεγχος εγκυρότητας δεδομένων

Η εισαγωγή δεδομένων στις εφαρμογές θα πρέπει να ελέγχεται ώστε να είναι σωστή και να γίνεται με τον κατάλληλο τρόπο. Θα πρέπει να εξεταστούν οι ακόλουθοι μηχανισμοί:

- Διπλή εισαγωγή δεδομένων ώστε να εντοπισθούν μη αποδεκτές τιμές ή χαρακτήρες, ανεπαρκή δεδομένα, χαρακτήρες ελέγχου (control) κλπ.
- Περιοδικός έλεγχος των περιεχομένων των πεδίων-κλειδιών για να επιβεβαιωθεί η ορθότητά τους.
- Έλεγχος των προς εισαγωγή δεδομένων για να εντοπιστεί κάποια μή εξουσιοδοτημένη αλλαγή.
- Διαδικασίες για την αναφορά λαθών.
- Έλεγχο της αληθοφάνειας των δεδομένων.
- Καθορισμό των ευθυνών του προσωπικού που εισάγει τα δεδομένα στο σύστημα.

10.2.2 Έλεγχος της επεξεργασίας των δεδομένων

10.2.2.1 Περιοχές κινδύνου

Τα δεδομένα που έχουν εισαχθεί σωστά στο σύστημα μπορούν να παραποιηθούν από λάθη κατά την επεξεργασία τους ή από σκόπιμες ενέργειες. Στο σύστημα θα πρέπει να υπάρχουν ενσωματωμένες διαδικασίες για τον έλεγχο της εγκυρότητας των δεδομένων. Η σχεδίαση των εφαρμογών θα πρέπει να προβλέπει την προστασία των δεδομένων ώστε να ελαχιστοποιηθεί η πιθανότητα λάθους που μπορεί να οδηγήσει σε απώλεια της ακεραιότητας τους. Θα πρέπει να εξεταστούν τα ακόλουθα:

- Η θέση και η χρήση λειτουργιών των προγραμμάτων μέσω των οποίων μπορούν να γίνουν αλλαγές στα δεδομένα.

- Διαδικασίες που να διασφαλίζουν τη σωστή σειρά εκτέλεσης των εφαρμογών και των απαραίτητων βημάτων για την αποκατάσταση κάποιας βλάβης.

- Η χρήση των κατάλληλων προγραμμάτων για την αποκατάσταση των προβλημάτων που παρουσιάζονται στο σύστημα ώστε να διασφαλισθεί η σωστή επεξεργασία των δεδομένων.

10.2.2.2 Μηχανισμοί ελέγχου

Οι απαιτούμενοι μηχανισμοί ελέγχου εξαρτώνται από τη φύση των εφαρμογών και τις συνέπειες στον οργανισμό που απορρέουν από την απώλεια δεδομένων. Παραδείγματα ελέγχων είναι τα ακόλουθα:

- Η δυνατότητα rollback για δοσοληψίες που γίνονται στο σύστημα.

- Διαδικασίες ελέγχου της συνέχειας των δεδομένων (π.χ. έλεγχος κάποιου υπολοίπου σε σχέση με την τελευταία κίνηση).

- Έλεγχος των δεδομένων που δημιουργούνται από το ίδιο το σύστημα.

- Έλεγχος της ακεραιότητας των προγραμμάτων και των δεδομένων που μεταφέρονται ανάμεσα σε διαφορετικά συστήματα.

- Συνόψεις (hashes) εγγραφών και αρχείων.

- Έλεγχος ότι οι εφαρμογές τρέχουν τις κατάλληλες χρονικές περιόδους.

- Έλεγχος ότι οι εφαρμογές εκτελούνται με τη σωστή σειρά και ότι σε περίπτωση λάθους η επεξεργασία σταματά μέχρι να λυθεί το πρόβλημα που παρουσιάστηκε.

10.2.3 Αυθεντικοποίηση μηνυμάτων

Η αυθεντικοποίηση των μηνυμάτων (message authentication) είναι μια τεχνική που χρησιμοποιείται για τον εντοπισμό μη εξουσιοδοτημένων αλλαγών ή παρεμβάσεων στα περιεχόμενα των μηνυμάτων που μεταδίδονται ηλεκτρονικά στο σύστημα. Μπορεί να υλοποιηθεί με λογισμικό ή υλικό. Η αυθεντικοποίηση των μηνυμάτων είναι απαραίτητη όταν πρέπει να προστατευθεί η ακεραιότητα του περιεχομένου των μηνυμάτων (π.χ. ηλεκτρονική μεταφορά χρημάτων, συμβόλαια κλπ.). Θα πρέπει να διενεργηθεί αποτίμηση κινδύνου για να καθοριστεί η αναγκαιότητα της χρήσης της αυθεντικοποίησης, όσο και ο τρόπος υλοποίησης.

Η τεχνική αυτή δεν μπορεί να προστατεύσει το περιεχόμενο των μηνυμάτων από μη εξουσιοδοτημένη ανάγνωση. Για το σκοπό αυτό μπορούν να χρησιμοποιηθούν τεχνικές κρυπτογραφίας (παράγραφοι 10.3.2 και 10.3.3).

10.2.4 Έλεγχος αποτελεσμάτων της επεξεργασίας

Τα αποτελέσματα της επεξεργασίας των δεδομένων στο σύστημα θα πρέπει να ελέγχονται προκειμένου να διασφαλιστεί η ορθότητα της επεξεργασίας. Συνήθως τα πληροφοριακά συστήματα λειτουργούν με το σκεπτικό ότι εφόσον οι εφαρμογές έχουν δοκιμασθεί επιτυχώς, τα αποτελέσματα της επεξεργασίας θα είναι πάντοτε σωστά. Σε κάποιες περιπτώσεις όμως αυτό δεν ισχύει. Θα πρέπει να εξετασθούν τα ακόλουθα:

- Η αληθοφάνεια των αποτελεσμάτων
- Η εναρμόνιση της επεξεργασίας όλων των δεδομένων.
- Η παροχή επαρκούς πληροφορίας προκειμένου να επιβεβαιώνεται η ακρίβεια και η ορθότητα των πληροφοριών.
- Διαδικασίες για την αντιμετώπιση λαθών.
- Ο καθορισμός των ευθυνών του προσωπικού που σχετίζεται με τις διαδικασίες των αποτελεσμάτων της επεξεργασίας των δεδομένων.

10.3 Μηχανισμοί κρυπτογραφίας

Σκοπός είναι η προστασία της εμπιστευτικότητας, της ακεραιότητας και της αυθεντικότητας των δεδομένων. Τεχνικές κρυπτογραφίας θα πρέπει να χρησιμοποιούνται για την προστασία των πληροφοριών που θεωρείται ότι βρίσκονται σε κίνδυνο και που δεν μπορεί να αντιμετωπισθεί με άλλους μηχανισμούς προστασίας.

10.3.1 Πολιτική χρήσης κρυπτογραφίας

Η απόφαση για τη χρήση ή όχι τεχνικών κρυπτογράφησης θα πρέπει να είναι μέρος της γενικότερης διαδικασίας αποτίμησης κινδύνου και επιλογής μηχανισμών προστασίας. Η διενέργεια αποτίμησης κινδύνου οδηγεί στην επιλογή των κατάλληλων μηχανισμών που ικανοποιούν και τις επιχειρησιακές ανάγκες του οργανισμού.

Ο οργανισμός θα πρέπει να έχει κάποια πολιτική για τη χρήση κρυπτογραφίας. Μια τέτοια πολιτική πρέπει να μεγιστοποιεί τα οφέλη και να ελαχιστοποιεί τους κινδύνους από τη χρήση κρυπτογραφικών τεχνικών. Θα πρέπει να εξεταστούν τα ακόλουθα:

- Η θέση της διοίκησης σχετικά με τη χρήση κρυπτογραφίας στον οργανισμό, συμπεριλαμβανομένων των γενικών αρχών προστασίας των πληροφοριών του οργανισμού.

- Οι κατάλληλοι τρόποι διαχείρισης των κρυπτογραφικών κλειδιών, ειδικά για την αντιμετώπιση των προβλημάτων που προκύπτουν από την απώλειά τους.

- Οι απαραίτητοι ρόλοι και οι σχετικές ευθύνες για την εφαρμογή της πολιτικής, τη διαχείριση των κλειδιών, τον καθορισμό του κατάλληλου επιπέδου προστασίας και τους κατάλληλους μηχανισμούς σε σχέση με τις ανάγκες του οργανισμού.

10.3.2 Κρυπτογραφία

Η κρυπτογραφία είναι μια τεχνική που χρησιμοποιείται για την προστασία της εμπιστευτικότητας των πληροφοριών. Θα πρέπει να χρησιμοποιείται για την προστασία ευαίσθητων ή κρίσιμων πληροφοριών. Ανάλογα με το απαραίτητο επίπεδο προστασίας, θα

πρέπει να χρησιμοποιούνται και οι κατάλληλοι αλγόριθμοι κρυπτογράφησης με τα ανάλογου μήκους κλειδιά.

Η υλοποίηση της πολιτικής κρυπτογράφησης του οργανισμού, θα πρέπει να λαμβάνει υπόψη τη νομοθεσία που διέπει τη χρήση τεχνικών κρυπτογραφίας, ειδικά όταν απαιτείται η επικοινωνία ανάμεσα σε τοποθεσίες που βρίσκονται σε διαφορετικά κράτη. Προσοχή επίσης απαιτείται στους κανονισμούς εξαγωγής και εισαγωγής τεχνολογιών κρυπτογραφίας (παράγραφος 12.1.6).

Ο οργανισμός θα πρέπει να καταφεύγει στη συμβουλή εμπειρογνωμόνων για την επιλογή των κατάλληλων τεχνικών κρυπτογράφησης, τη διαχείριση των κλειδιών, αλλά και για τη συμμόρφωση με τη σχετική νομοθεσία.

10.3.3 Ψηφιακές υπογραφές

Οι ψηφιακές υπογραφές (digital signatures) είναι μία υπηρεσία διασφάλισης της αυθεντικότητας και της ακεραιότητας ηλεκτρονικών εγγράφων. Μπορούν, για παράδειγμα, να χρησιμοποιηθούν στο ηλεκτρονικό εμπόριο, όπου είναι αναγκαίο να εξακριβωθεί η ταυτότητα του αποστολέα ενός ηλεκτρονικού εγγράφου, καθώς και ότι τα περιεχόμενα του εγγράφου δεν έχουν μεταβληθεί. Οι ψηφιακές υπογραφές μπορούν να χρησιμοποιηθούν με κάθε τύπο ηλεκτρονικού εγγράφου (κείμενο, ηλεκτρονικό ταχυδρομείο κλπ). Βασίζονται στη χρήση ενός μοναδικού ζεύγους κρυπτογραφικών κλειδιών, όπου το ιδιωτικό κλειδί (private key) χρησιμοποιείται για τη δημιουργία της υπογραφής και το αντίστοιχο δημόσιο κλειδί (public key) για την επιβεβαίωση της υπογραφής.

Ιδιαίτερη προσοχή πρέπει να δοθεί στην προστασία του ιδιωτικού κλειδιού, καθώς όποιος έχει πρόσβαση σε αυτό μπορεί να υπογράψει ηλεκτρονικά έγγραφα, υποδυόμενος το νόμιμο κάτοχο του κλειδιού. Θα πρέπει επίσης να προστατευθεί και η ακεραιότητα του δημόσιου κλειδιού. Συνήθως αυτό επιτυγχάνεται με τη χρήση ψηφιακών πιστοποιητικών (digital certificates – παράγραφος 10.3.5).

Η επιλογή του αλγόριθμου και του μήκους των κλειδιών που χρησιμοποιούνται στις ψηφιακές υπογραφές είναι σημαντικές παράμετροι. Επιπλέον, τα κλειδιά που χρησιμοποιούνται για τις υπογραφές θα πρέπει να είναι διαφορετικά από αυτά που χρησιμοποιούνται για την κρυπτογράφηση των πληροφοριών.

Η χρήση ψηφιακών υπογραφών εξαρτάται άμεσα από την εγκυρότητα που τους αποδίδει η σχετική νομοθεσία. Σε κάποιες περιπτώσεις είναι απαραίτητη η σύναψη ειδικών συμφωνιών ανάμεσα σε οργανισμούς που χρησιμοποιούν τη συγκεκριμένη τεχνολογία για τις μεταξύ τους συναλλαγές. Είναι λοιπόν αναγκαία η νομική συμβουλή, πριν ο οργανισμός υιοθετήσει ψηφιακές υπογραφές στις συναλλαγές του.

10.3.4 Υπηρεσίες μη αποποίησης

Η χρήση ηλεκτρονικών συναλλαγών θα πρέπει να συνοδεύεται και από την ύπαρξη κάποιου τρόπου που να εμποδίζει τα συναλλασσόμενα μέρη να αποποιηθούν τις πράξεις τους (non-repudiation) που είναι σχετικές με κάποια συναλλαγή. Στην περίπτωση που, για παράδειγμα, κάποιος χρήστης ηλεκτρονικού εμπορίου αρνηθεί ότι απέστειλε μια παραγγελία, θα πρέπει να υπάρχει ένας μηχανισμός επίλυσης της διαφοράς. Τέτοιοι μηχανισμοί περιλαμβάνουν τη χρήση κρυπτογραφίας και ψηφιακών υπογραφών από τα συναλλασσόμενα μέρη.

10.3.5 Διαχείριση κλειδιών

10.3.5.1 Προστασία των κρυπτογραφικών κλειδιών

Η διαχείριση των κλειδιών που χρησιμοποιούνται στις τεχνικές κρυπτογραφίας είναι ζωτικής σημασίας. Πιθανή έκθεση ή απώλεια των κλειδιών, μπορεί να οδηγήσει σε έκθεση της εμπιστευτικότητας, της αυθεντικότητας ή της ακεραιότητας των πληροφοριών. Ο οργανισμός θα πρέπει να διαθέτει ένα σύστημα διαχείρισης για την υποστήριξη της χρήσης των δύο τύπων κρυπτογραφίας που είναι:

- Τεχνικές μυστικού κλειδιού (secret key), όπου τα μέλη που επικοινωνούν με τη χρήση κρυπτογραφίας διαμοιράζονται τη γνώση ενός μυστικού κλειδιού. Το συγκεκριμένο κλειδί χρησιμοποιείται για την κρυπτογράφηση και την αποκρυπτογράφηση των πληροφοριών. Θα πρέπει να ληφθούν μέτρα για την προστασία του, καθώς όποιος έχει πρόσβαση στο κλειδί, μπορεί να αποκτήσει πρόσβαση στις πληροφορίες ή να εισάγει άλλες πληροφορίες χωρίς εξουσιοδότηση.

- Τεχνικές δημόσιου κλειδιού (public key), όπου το κάθε συναλλασσόμενο μέλος έχει ένα ζεύγος κλειδιών στην κατοχή του. Το ένα κλειδί είναι ιδιωτικό (private) και πρέπει να

διατηρείται μυστικό. Το δεύτερο κλειδί είναι δημόσιο (public) και πρέπει να μπορεί να το γνωρίζει ο οποιοσδήποτε θέλει να επικοινωνήσει με το συγκεκριμένο μέλος. Οι τεχνικές δημόσιου κλειδιού μπορούν να χρησιμοποιηθούν τόσο για κρυπτογράφηση των πληροφοριών, όσο και για τη δημιουργία ψηφιακών υπογραφών.

Όλα τα κλειδιά θα πρέπει να προστατεύονται από μεταβολή ή καταστροφή, ενώ τα μυστικά και τα ιδιωτικά κλειδιά πρέπει επιπλέον να προστατεύονται από έκθεση σε μη εξουσιοδοτημένα άτομα. Για αυτό το σκοπό μπορούν επίσης να χρησιμοποιηθούν τεχνικές κρυπτογραφίας. Ο εξοπλισμός που χρησιμοποιείται για τη δημιουργία και την αποθήκευση των κλειδιών θα πρέπει να προστατεύεται και φυσικά.

10.3.5.2 Πρότυπα, διαδικασίες και μέθοδοι

Το σύστημα διαχείρισης κλειδιών θα πρέπει να βασίζεται σε κάποιο προσυμφωνημένο σύνολο από πρότυπα, διαδικασίες και μεθόδους για:

- Τη δημιουργία κλειδιών για διαφορετικές τεχνικές κρυπτογράφησης και διαφορετικές εφαρμογές.
- Τη δημιουργία και διάθεση ψηφιακών πιστοποιητικών (certificates).
- Τη διανομή των κλειδιών στους κατάλληλους χρήστες, καθώς και την ενεργοποίησή τους κατά την παραλαβή τους από τους χρήστες.
- Την ασφαλή αποθήκευση των κλειδιών και τον τρόπο με τον οποίο μπορούν οι νόμιμοι χρήστες να τα προσπελάσουν.
- Τον τρόπο αλλαγής ή ανανέωσης των κλειδιών, όπως και τη συχνότητα που θα πρέπει να γίνεται αυτό.
- Την αντιμετώπιση κλειδιών που έχουν εκτεθεί.
- Την ανάκληση και ακύρωση κλειδιών.
- Την ανάκτηση κλειδιών που έχουν καταστραφεί ή χαθεί, ως μέρος του σχεδίου επιχειρηματικής συνέχειας του οργανισμού.
- Την αρχειοθέτηση των κλειδιών.
- Την καταστροφή των κλειδιών.
- Την καταγραφή των ενεργειών που σχετίζονται με τη διαχείριση των κλειδιών.

Προκειμένου να ελαχιστοποιηθεί ο κίνδυνος έκθεσης τους, τα κλειδιά θα πρέπει να έχουν συγκεκριμένο χρόνο ισχύος, καθώς και συγκεκριμένο χρόνο ενεργοποίησης και απενεργοποίησης. Ο χρόνος ισχύος εξαρτάται από τους λόγους χρήσης κρυπτογραφίας και το σχετικό κίνδυνο από τον οποίο προστατεύει τον οργανισμό. Θα πρέπει ακόμα να υπάρχουν

ειδικές διαδικασίες για την πρόσβαση στα κλειδιά για νομικούς λόγους, όπως την αποκρυπτογράφηση κάποιου εγγράφου για χρήση του στο δικαστήριο.

Τα δημόσια κλειδιά πρέπει επίσης να προστατευθούν. Υπάρχει ο κίνδυνος παραβίασης ενός δημόσιου κλειδιού. Το πρόβλημα αντιμετωπίζεται με τη χρήση ψηφιακών πιστοποιητικών. Ένα τέτοιο πιστοποιητικό συνδυάζει με μοναδικό τρόπο το δημόσιο κλειδί με τις πληροφορίες του κατόχου του. Συνήθως αυτή η διαδικασία γίνεται από μια αρχή πιστοποίησης (certification authority), η οποία θα πρέπει να έχει τα κατάλληλα μέτρα προστασίας και να απολαμβάνει της εμπιστοσύνης των οργανισμών που θέλουν να χρησιμοποιήσουν ψηφιακά πιστοποιητικά.

Ο οργανισμός μπορεί να ζητήσει την παροχή υπηρεσιών κρυπτογραφίας από τρίτους, εξωτερικούς συνεργάτες. Σε μια τέτοια περίπτωση θα πρέπει να ληφθούν υπόψη το επίπεδο εξυπηρέτησης και η επίλυση προβλημάτων που μπορεί να προκύψουν κατά τη χρήση κρυπτογραφικών τεχνικών (παράγραφος 4.2.2).

10.4 Ασφάλεια αρχείων συστήματος

Σκοπός είναι η διασφάλιση ότι τα έργα πληροφορικής και οι εργασίες υποστήριξης γίνονται με ασφαλή τρόπο. Θα πρέπει να ελέγχεται η πρόσβαση στα αρχεία του συστήματος. Η ακεραιότητα του συστήματος είναι ευθύνη και των χρηστών, αλλά και των προγραμματιστών των εφαρμογών που χρησιμοποιεί οργανισμός.

10.4.1 Έλεγχος των εφαρμογών που λειτουργούν σε παραγωγή

Η εγκατάσταση εφαρμογών σε συστήματα παραγωγής θα πρέπει να είναι ελεγχόμενη. Προκειμένου να περιοριστεί ο κίνδυνος κάποιου προβλήματος θα πρέπει να εξεταστούν τα ακόλουθα:

- Η αναβάθμιση των εφαρμογών παραγωγής θα πρέπει να γίνεται από το εξουσιοδοτημένο προσωπικό και κατόπιν άδειας της διοίκησης (παράγραφος 10.4.3).
- Τα συστήματα παραγωγής θα πρέπει να περιέχουν μόνον εκτελέσιμο κώδικα.

- Ο εκτελέσιμος κώδικας θα πρέπει να δοκιμάζεται διεξοδικά πριν εγκατασταθεί σε σύστημα παραγωγής. Επιπλέον θα πρέπει να προηγηθεί όποια άλλη αναβάθμιση είναι απαραίτητη για τη σωστή λειτουργία του.

- Θα πρέπει να τηρείται αρχείο με όλες τις αναβαθμίσεις που έχουν γίνει στις εφαρμογές παραγωγής.

- Παλαιότερες εκδόσεις των προγραμμάτων θα πρέπει να φυλάσσονται ως μέτρο επιχειρησιακής συνέχειας του οργανισμού.

Εφαρμογές που αναπτύσσονται από εξωτερικούς προμηθευτές θα πρέπει να έχουν και την κατάλληλη υποστήριξη από αυτούς. Πριν αποφασισθεί οποιαδήποτε αναβάθμιση, θα πρέπει να εξεταστεί η ασφάλεια της νέας έκδοσης, π.χ. πιθανά προβλήματα, επιπλέον λειτουργικότητα από την τρέχουσα έκδοση κλπ. Διορθωτικές παρεμβάσεις στις εφαρμογές με χρήση συμπληρωματικού λογισμικού (patches) θα πρέπει να γίνεται εφόσον μπορούν να συνεισφέρουν στην αύξηση του παρεχόμενου επιπέδου ασφάλειας. Η πρόσβαση στους εξωτερικούς προμηθευτές θα πρέπει να παρέχεται μόνον όταν είναι αναγκαίο, να είναι ελεγχόμενη και να έχει την έγκριση της διοίκησης του οργανισμού.

10.4.2 Προστασία συστημάτων δοκιμών

Τα δεδομένα που προορίζονται για τις δοκιμές συστημάτων και εφαρμογών θα πρέπει να προστατεύονται επαρκώς, αφού συνήθως είναι παρεμφερή με τα δεδομένα παραγωγής. Η χρήση δεδομένων που περιέχουν προσωπικά στοιχεία πρέπει να αποφεύγεται. Εφόσον χρησιμοποιηθούν τέτοια δεδομένα, θα πρέπει πρώτα να αφαιρεθούν στοιχεία που να υποδεικνύουν συγκεκριμένα άτομα. Θα πρέπει να εξεταστεί η χρήση των ακόλουθων μηχανισμών όταν πρόκειται να χρησιμοποιηθούν πραγματικά δεδομένα για τη διενέργεια δοκιμών:

- Οι διαδικασίες ελέγχου πρόσβασης που ισχύουν για τα δεδομένα παραγωγής θα πρέπει να εφαρμόζονται και για τα δεδομένα δοκιμών.

- Θα πρέπει να υπάρχει ξεχωριστή εξουσιοδότηση κάθε φορά που πραγματικά δεδομένα αντιγράφονται σε συστήματα δοκιμών.
- Τα πραγματικά δεδομένα θα πρέπει να διαγράφονται από το σύστημα δοκιμών αμέσως μετά το πέρας της χρησιμότητάς τους.
- Η αντιγραφή και η χρήση δεδομένων παραγωγής θα πρέπει να καταγράφεται.

10.4.3 Έλεγχος της πρόσβασης στον κώδικα των εφαρμογών

Προκειμένου να ελαχιστοποιηθεί ο κίνδυνος μερικής ή ολικής καταστροφής των εφαρμογών, θα πρέπει να υπάρχει αυστηρός έλεγχος στην πρόσβαση του κώδικα των χρησιμοποιούμενων από τον οργανισμό προγραμμάτων (παράγραφος 8.3). Προτείνονται τα ακόλουθα:

- Ο κώδικας τον εφαρμογών δε θα πρέπει να υπάρχει στα συστήματα παραγωγής.
- Θα πρέπει να οριστεί ένας υπεύθυνος για τον πηγαίο κώδικα κάθε εφαρμογής.
- Το προσωπικό υποστήριξης δε θα πρέπει να έχει ελεύθερη πρόσβαση στον κώδικα των εφαρμογών.
- Ο κώδικας των εφαρμογών που είναι στη φάση της ανάπτυξης θα πρέπει να φυλάσσεται ξεχωριστά από τον κώδικα των εφαρμογών παραγωγής.
- Οποιαδήποτε αλλαγή στον πηγαίο κώδικα των εφαρμογών θα πρέπει να γίνεται σε συνεργασία με τον υπεύθυνο της εφαρμογής και κατόπιν ειδικής εξουσιοδότησης.
- Ο πηγαίος κώδικας θα πρέπει να είναι αποθηκευμένος σε ασφαλές περιβάλλον.
- Θα πρέπει να τηρείται αρχείο της προσπέλασης στον πηγαίο κώδικα των εφαρμογών.
- Οι παλαιότερες εκδόσεις του κώδικα θα πρέπει να αρχειοθετούνται και να καταγράφονται τα ακριβή στοιχεία τους.
- Η συντήρηση και η αντιγραφή του πηγαίου κώδικα θα πρέπει να ελέγχεται αυστηρά.

10.5 Ασφάλεια κατά την ανάπτυξη και την υποστήριξη των εφαρμογών

Σκοπός είναι η διατήρηση της ασφάλειας των εφαρμογών και των πληροφοριών. Οι υπεύθυνοι των εφαρμογών θα πρέπει να είναι υπεύθυνοι και για την ασφάλεια κατά το στάδιο της ανάπτυξης της εφαρμογής και της υποστήριξης. Θα πρέπει να διασφαλίσουν ότι οποιαδήποτε αλλαγή στο σύστημα θα ελέγχεται πριν πραγματοποιηθεί και ότι δεν έχει αρνητικές επιπτώσεις στην ασφάλεια του συστήματος.

10.5.1 Διαδικασίες ελέγχου αλλαγών

Ο οργανισμός θα πρέπει να χρησιμοποιεί ένα σύνολο διαδικασιών για τη διενέργεια οποιασδήποτε αλλαγής στις εφαρμογές του συστήματος. Έτσι μειώνεται ο κίνδυνος δημιουργίας προβλημάτων στο σύστημα. Οι προγραμματιστές που αναπτύσσουν κάποια εφαρμογή θα πρέπει να έχουν πρόσβαση μόνο στα τμήματα του κώδικα που είναι απαραίτητα για τη δουλειά τους και οποιαδήποτε αλλαγή σε αυτά θα πρέπει να είναι κατάλληλα εξουσιοδοτημένη, καθώς μπορεί να επηρεαστεί άμεσα το περιβάλλον παραγωγής. Οι διαδικασίες με βάση τις οποίες θα γίνονται οι αλλαγές στις εφαρμογές θα πρέπει να περιλαμβάνουν τα ακόλουθα:

- Την τήρηση αρχείων με τα συμφωνημένα επίπεδα εξουσιοδότησης.
- Την εξασφάλιση ότι οι αλλαγές γίνονται από εξουσιοδοτημένους χρήστες.
- Την εξασφάλιση ότι οι αλλαγές δεν επηρεάζουν το υπάρχον επίπεδο ασφάλειας.
- Τον καθορισμό των εφαρμογών και των συστημάτων για τα οποία απαιτείται κάποια αλλαγή.
- Την παροχή εξουσιοδότησης πριν γίνει κάποια αλλαγή.
- Τη σύμφωνη γνώμη των εξουσιοδοτημένων χρηστών πριν εφαρμοστούν οι αλλαγές.
- Τη εξασφάλιση ότι οι λειτουργίες του οργανισμού θα επηρεαστούν όσο το δυνατόν λιγότερο.
- Την ενημέρωση των εγχειριδίων του συστήματος και των εφαρμογών και την αρχειοθέτηση ή την καταστροφή των παλαιών εγχειριδίων.

- Τη χρήση μηχανισμού ελέγχου των εκδόσεων (version control) για όλες τις αλλαγές.
- Την αλλαγή των διαδικασιών που χρησιμοποιούν οι χρήστες εφόσον κρίνεται απαραίτητο.

Σε αρκετές περιπτώσεις, ο οργανισμός διαχωρίζει εντελώς το περιβάλλον δοκιμών από το περιβάλλον παραγωγής. Με αυτόν τον τρόπο έχει καλύτερο έλεγχο στις αλλαγές που γίνονται στο σύστημα και την προστασία των δεδομένων που χρησιμοποιούνται για δοκιμές.

10.5.2 Αναβαθμίσεις του λειτουργικού συστήματος

Περιοδικά είναι απαραίτητη η αναβάθμιση του λειτουργικού συστήματος που χρησιμοποιούν τα υπολογιστικά συστήματα του οργανισμού. Πριν όμως γίνει μια τέτοια αναβάθμιση θα πρέπει να ελεγχθεί κατά πόσο οι εφαρμογές του οργανισμού μπορούν να λειτουργήσουν με τη νέα έκδοση του λειτουργικού συστήματος. Αυτή η διαδικασία θα πρέπει να περιλαμβάνει τα ακόλουθα:

- Τον έλεγχο των εφαρμογών ώστε να διασφαλιστεί ότι δεν έχουν επηρεαστεί από τις αλλαγές του λειτουργικού συστήματος.
- Την εξασφάλιση οικονομικών πόρων για τις διαδικασίες που χρειάζονται για τη διενέργεια δοκιμών.
- Την έγκαιρη ενημέρωση για τις επικείμενες αλλαγές του λειτουργικού συστήματος ώστε να υπάρξει αρκετός χρόνος για τη δοκιμή των εφαρμογών στο καινούριο περιβάλλον.
- Τη διενέργεια των κατάλληλων αλλαγών του σχεδίου επιχειρησιακής συνέχειας του οργανισμού (κεφάλαιο 11).

10.5.3 Περιορισμοί στη διενέργεια αλλαγών

Οι αλλαγές στα έτοιμα προγράμματα εφαρμογών θα πρέπει να αποφεύγονται. Οι εφαρμογές θα πρέπει να χρησιμοποιούνται, κατά το δυνατόν, όπως παρέχονται από τον κατασκευαστή τους. Αν όμως είναι απαραίτητη κάποια αλλαγή θα πρέπει να εξεταστούν τα ακόλουθα:

- Οι επιπτώσεις στην ασφάλεια που προσφέρει η εφαρμογή.
- Αν απαιτείται άδεια του προμηθευτή.
- Η δυνατότητα του προμηθευτή να κάνει ο ίδιος τις επιθυμητές αλλαγές.
- Οι επιπτώσεις στη μελλοντική συντήρηση της εφαρμογής.

Εφόσον γίνουν κάποιες αλλαγές, η πρωτότυπη έκδοση της εφαρμογής θα πρέπει να διατηρείται. Οι αλλαγές θα πρέπει να γίνονται σε ένα αντίγραφο και να είναι πλήρως καταγεγραμμένες ώστε να εφαρμοσθούν ξανά αν είναι απαραίτητο σε κάποια αναβάθμιση της εφαρμογής.

10.5.4 Συγκαλυμμένα κανάλια επικοινωνίας και δούρειοι ίπποι

Ένα κρυφό συγκαλυμμένο κανάλι επικοινωνίας (covert channel) μπορεί να αποκαλύψει πληροφορίες με διάφορους και ασυνήθιστους τρόπους. Μπορεί να ενεργοποιηθεί από την πρόσβαση σε μια παράμετρο του συστήματος ή με παρεμβολή στο κανονικό κανάλι μετάδοσης των δεδομένων. Ένας δούρειος ίππος (trojan horse) είναι έτσι σχεδιασμένος ώστε να επηρεάζει το σύστημα με κάποιο μη εξουσιοδοτημένο τρόπο, ενώ ταυτόχρονα δεν προκαλεί την προσοχή των χρηστών ή παρουσιάζεται ως κανονική εφαρμογή του συστήματος. Τα κρυφά κανάλια επικοινωνίας, καθώς και οι δούρειοι ίπποι σπάνια αποτελούν τυχαίο γεγονός. Για την αντιμετώπισή τους θα πρέπει να εξεταστούν τα ακόλουθα:

- Η αγορά εφαρμογών να γίνεται μόνον από επώνυμες πηγές.
- Όταν είναι δυνατό, να αγοράζεται και ο πηγαίος κώδικας των εφαρμογών ώστε να ελέγχεται πριν από τη χρήση της εφαρμογής.

- Να ελέγχεται η κάθε μορφής πρόσβαση στον πηγαίο κώδικα των εφαρμογών που χρησιμοποιούνται στον οργανισμό.
- Να χρησιμοποιείται έμπιστο προσωπικό στα συστήματα με ιδιαίτερη σημασία για τον οργανισμό.
- Να χρησιμοποιούνται δοκιμασμένες εφαρμογές.

10.5.5 Outsourcing της ανάπτυξης εφαρμογών

Στην περίπτωση που γίνεται outsourcing της ανάπτυξης των εφαρμογών του οργανισμού θα πρέπει να εξετάζονται τα ακόλουθα:

- Ζητήματα αδειών χρήσης, ιδιοκτησίας της εφαρμογής και πνευματικών δικαιωμάτων (παράγραφος 12.1.2).
- Πιστοποίηση της ποιότητας και της καταλληλότητας των εφαρμογών.
- Διαδικασίες που να αντιμετωπίζουν την περίπτωση αποτυχίας του τρίτου μέρους.
- Διαδικασίες ελέγχου των σταδίων ανάπτυξης της εφαρμογής και της απαιτούμενης ποιότητας.
- Δοκιμαστική λειτουργία της εφαρμογής πριν από την παραγωγική χρήση της.

11. Διαχείριση επιχειρησιακής συνέχειας

11.1 Παράμετροι της διαχείρισης της επιχειρησιακής συνέχειας

Σκοπός είναι η αποτροπή παρεμβολών στις επιχειρηματικές δραστηριότητες του οργανισμού και η προστασία των κρίσιμων διαδικασιών στην περίπτωση μερικών ή ολικών καταστροφών. Μια διαδικασία διαχείρισης της επιχειρησιακής συνέχειας του οργανισμού (business continuity management process) θα πρέπει να χρησιμοποιείται για τη μείωση σε κάποιο ανεκτό επίπεδο των επιπτώσεων από καταστροφές και συμβάντα σχετικά με την

ασφάλεια του οργανισμού. Τέτοιες καταστροφές μπορεί να είναι αποτέλεσμα φυσικών καταστροφών, αστοχίας υλικών ή σκόπιμων ενεργειών. Επιπλέον θα πρέπει να περιλαμβάνονται και μέτρα για την αποκατάσταση της φυσιολογικής λειτουργίας του οργανισμού.

Θα πρέπει να γίνει μια εκτίμηση των πιθανών επιπτώσεων στις λειτουργίες του οργανισμού ύστερα από κάποια μερική ή ολική καταστροφή. Ο σχεδιασμός για την αντιμετώπιση απρόοπτων γεγονότων θα πρέπει να εξασφαλίζει την αποκατάσταση των επηρεαζόμενων λειτουργιών μέσα σε ένα εφικτό και αποδεκτό χρονικό όριο. Τέτοια σχέδια θα πρέπει να είναι μέρος όλων των λειτουργιών διαχείρισης του οργανισμού. Επιπλέον θα πρέπει να χρησιμοποιούνται μηχανισμοί για την αναγνώριση και την πρόληψη κινδύνων.

11.1.1 Διαδικασία διαχείρισης της επιχειρησιακής συνέχειας

Ο οργανισμός θα πρέπει να χρησιμοποιεί μια συγκεκριμένη διαδικασία για το σχεδιασμό και την υλοποίηση της επιχειρησιακής συνέχειας. Θα πρέπει να βασίζεται στα ακόλουθα:

- Την κατανόηση των κινδύνων που ενδέχεται να απειλούν τον οργανισμό, την πιθανότητα να υλοποιηθούν και το κόστος που θα επιφέρουν. Θα πρέπει επίσης να καθοριστούν οι κρίσιμες λειτουργίες του οργανισμού και να κατηγοριοποιηθούν με βάση την προτεραιότητα τους για τον οργανισμό.

- Την κατανόηση των επιπτώσεων κάθε παρεμβολής στη φυσιολογική λειτουργία του οργανισμού. Θα πρέπει να υπάρχει κάποιο σχέδιο αντιμετώπισης τόσο των μικρών, όσο και των σοβαρών συμβάντων. Επίσης θα πρέπει να οριστούν οι στόχοι του πληροφοριακού συστήματος, σε σχέση με τις δραστηριότητες του οργανισμού.

- Την πιθανή σύναψη κατάλληλου ασφαλιστήριου συμβολαίου, το οποίο μπορεί να είναι μέρος του σχεδίου επιχειρησιακής συνέχειας.

- Την κατάστρωση μιας στρατηγικής επιχειρησιακής συνέχειας η οποία θα πρέπει να είναι σύμφωνη με τους στόχους και τις προτεραιότητες του οργανισμού.

- Την καταγραφή ενός σχεδίου επιχειρησιακής συνέχειας το οποίο θα υλοποιεί την παραπάνω στρατηγική.

- Τον τακτικό έλεγχο και την τακτική ενημέρωση του σχεδίου και των διαδικασιών που προβλέπονται σε αυτό.

- Την ενσωμάτωση του σχεδίου επιχειρησιακής συνέχειας σε όλες τις λειτουργίες του οργανισμού. Η ευθύνη της υλοποίησης του σχεδίου θα πρέπει να βρίσκεται μέσα στον οργανισμό (π.χ. στην επιτροπή ασφάλειας των πληροφοριών – παράγραφος 4.1.1).

11.1.2 Καθορισμός επιπτώσεων

Η επιχειρησιακή συνέχεια βασίζεται στην αναγνώριση των γεγονότων που μπορούν να προκαλέσουν παρεμβολές στην ομαλή λειτουργία του οργανισμού. Τέτοια γεγονότα είναι αστοχία υλικών, φυσικές καταστροφές κλπ. Στη συνέχεια θα πρέπει να διεξάγεται μια μελέτη αποτίμησης κινδύνου ώστε να καθοριστούν οι πιθανές επιπτώσεις από ένα τέτοιο γεγονός, τόσο αναφορικά με τις ζημιές που μπορεί να προκαλέσει, όσο και για την απαραίτητη χρονική περίοδο για την αποκατάσταση της ομαλής λειτουργίας του οργανισμού. Η όλη διαδικασία θα πρέπει να γίνεται με τη συμμετοχή των ιδιοκτητών των πόρων και των διαδικασιών του οργανισμού. Θα πρέπει επίσης να καλύπτει όλες τις λειτουργίες του οργανισμού και να μην εστιάζεται μόνο στο πληροφοριακό σύστημα.

Τα αποτελέσματα της αποτίμησης κινδύνου θα καθορίσουν και τη στρατηγική του οργανισμού στο ζήτημα της επιχειρησιακής συνέχειας. Το τελικό σχέδιο θα πρέπει να έχει την πλήρη υποστήριξη και αποδοχή της διοίκησης του οργανισμού.

11.1.3 Συγγραφή και υλοποίηση του σχεδίου επιχειρησιακής συνέχειας

Σκοπός του σχεδίου επιχειρησιακής συνέχειας είναι η διατήρηση και αποκατάσταση των λειτουργιών του οργανισμού, μέσα σε ένα αποδεκτό χρονικό διάστημα, ύστερα από κάποια παρεμβολή στις κρίσιμες λειτουργικές διαδικασίες. Κατά την ανάπτυξη ενός τέτοιου σχεδίου θα πρέπει να εξετάζονται τα ακόλουθα:

- Ο καθορισμός και η συμφωνία σε όλες τις διαδικασίες και η ευθύνη των εμπλεκομένων.

- Ο καθορισμός ρεαλιστικών χρόνων αποκατάστασης της ομαλής λειτουργίας του οργανισμού. Ειδική προσοχή χρειάζεται στην αναγνώριση εξωτερικών παραγόντων που μπορούν να επηρεάσουν τις διαδικασίες αποκατάστασης.

- Η πλήρης καταγραφή των συμφωνηθέντων διαδικασιών.

- Η κατάλληλη εκπαίδευση του προσωπικού στην υλοποίηση του σχεδίου.

- Η δοκιμή και η ενημέρωση του σχεδίου.

Η κατάστρωση του σχεδίου θα πρέπει να βασίζεται στους απολύτως απαραίτητους στόχους του οργανισμού, όπως την αποκατάσταση συγκεκριμένων υπηρεσιών σε εύλογο χρονικό διάστημα. Θα πρέπει να συμπεριληφθούν όλοι οι απαραίτητοι πόροι και όλες οι απαραίτητες διαδικασίες (προσωπικό, εξοπλισμός, συνεργασία με τρίτους κλπ.).

11.1.4 Πλαίσιο σχεδιασμού

Ο οργανισμός θα πρέπει να χρησιμοποιεί ένα ενιαίο πλαίσιο για την κατάστρωση του σχεδίου επιχειρησιακής συνέχειας, τον καθορισμό προτεραιοτήτων, τις δοκιμές και την τακτική ενημέρωση του σχεδίου. Θα πρέπει να αναφέρονται με σαφήνεια οι περιπτώσεις για τις οποίες ενεργοποιείται το σχέδιο (ή κάποιο μέρος του), καθώς και τους υπεύθυνους για την εκτέλεση του. Όταν υπάρξουν νέες απαιτήσεις από τον οργανισμό, το σχέδιο θα πρέπει να συμπληρώνεται κατάλληλα.

Το πλαίσιο ανάπτυξης του σχεδίου επιχειρησιακής συνέχειας θα πρέπει να εξετάζει τα ακόλουθα:

- Τις συνθήκες ενεργοποίησης του σχεδίου.

- Τις διαδικασίες που πρέπει να ακολουθηθούν όταν κινδυνεύουν ανθρώπινες ζωές και τον τρόπο επικοινωνίας με τις κατάλληλες δημόσιες αρχές.

- Τις διαδικασίες προσωρινής αποκατάστασης των λειτουργιών του οργανισμού, έως ότου ολοκληρωθεί η πλήρης αποκατάσταση (εφεδρικός εξοπλισμός ή τοποθεσίες, συνεργασία με τρίτους για την παροχή υπηρεσιών κλπ.).

- Τις διαδικασίες που απαιτούνται για την πλήρη αποκατάσταση των λειτουργιών του οργανισμού.

- Το χρονοδιάγραμμα συντήρησης του σχεδίου, το οποίο θα πρέπει να περιλαμβάνει τις απαραίτητες δοκιμές και ενημερώσεις.

- Την εκπαίδευση του προσωπικού στην αναγκαιότητα και την εκτέλεση του σχεδίου επιχειρησιακής συνέχειας.

- Τον καταμερισμό των ευθυνών για την εκτέλεση του σχεδίου.

Κάθε επιμέρους τμήμα του σχεδίου θα πρέπει να έχει ορισμένο «ιδιοκτήτη». Οι σχετικές διαδικασίες γίνονται με ευθύνη των ιδιοκτητών των εμπλεκόμενων πόρων και διαδικασιών. Η χρήση εξωτερικών προς τον οργανισμό πόρων ή υπηρεσιών, θα πρέπει να γίνεται με ευθύνη των συνεργατών που τα παρέχουν.

11.1.5 Δοκιμή, ενημέρωση και επανέλεγχος του σχεδίου

11.1.5.1 Δοκιμή του σχεδίου

Το σχέδιο επιχειρησιακής συνέχειας είναι πολύ πιθανό να αποτύχει κατά τη δοκιμή του. Αυτό συνήθως συμβαίνει λόγω λανθασμένων υποθέσεων, αλλαγών στον εξοπλισμό και το προσωπικό ή παραβλέψεων. Για αυτό το λόγο θα πρέπει να δοκιμάζεται σε τακτά χρονικά διαστήματα, σε όλες του τις διαστάσεις, προκειμένου να διασφαλιστεί η εγκυρότητα και η αποτελεσματικότητά του.

Κατά τη δοκιμή του σχεδίου, θα πρέπει να υπάρχει σαφές χρονοδιάγραμμα για κάθε τμήμα που θα εξεταστεί. Προτείνεται επίσης η συχνή δοκιμή των επιμέρους τμημάτων του σχεδίου. Υπάρχουν διάφορες τεχνικές με βάση τις οποίες μπορεί να γίνει η δοκιμή ενός σχεδίου. Θα πρέπει να περιλαμβάνουν τα ακόλουθα:

- Τον έλεγχο σε θεωρητικό επίπεδο διάφορων σεναρίων.
- Την προσομοίωση διάφορων γεγονότων, ειδικά κατά την εκπαίδευση του προσωπικού.
- Τον έλεγχο των δυνατοτήτων του εξοπλισμού να αντεπεξέλθει στις απαιτήσεις του σχεδίου.
- Τη δοκιμή του σχεδίου σε κάποιες εναλλακτικές εγκαταστάσεις ώστε να μη δημιουργούνται παρεμβολές στις λειτουργίες του οργανισμού.
- Τις δοκιμές των δυνατοτήτων των εξωτερικών συνεργατών να αντεπεξέλθουν στις απαιτήσεις του σχεδίου.
- Τη διενέργεια πλήρους υλοποίησης του σχεδίου ώστε να δοκιμαστεί η δυνατότητα όλων να ενεργήσουν όπως προβλέπεται.

Οι διάφορες τεχνικές μπορούν να χρησιμοποιηθούν από οποιονδήποτε οργανισμό και θα πρέπει να αντικατροπτίζουν τις ανάγκες συγκεκριμένου σχεδίου.

11.1.5.2 Ενημέρωση και επανέλεγχος του σχεδίου

Το σχέδιο επιχειρησιακής συνέχειας θα πρέπει να συντηρείται και να ενημερώνεται με χρήση τακτικών ελέγχων για τη διασφάλιση της αποτελεσματικότητάς του. Οι σχετικές διαδικασίες θα πρέπει να αποτελούν μέρος της γενικότερης διαχείρισης των αλλαγών μέσα στον οργανισμό, ώστε να αποδίδεται η ανάλογη αξία στα ζητήματα επιχειρησιακής συνέχειας. Επιπλέον, με αυτόν τον τρόπο οι όποιες αλλαγές στο σχέδιο θα επιβάλλονται και από τις αλλαγές που συντελούνται στις υπόλοιπες διαδικασίες του οργανισμού.

Αλλαγές στο σχέδιο μπορούν να προκληθούν από αλλαγές στα ακόλουθα:

- Το προσωπικό.
- Τις Διευθύνσεις, τηλέφωνα, πόρους του οργανισμού, τοποθεσία εγκαταστάσεων.
- Τη στρατηγική του οργανισμού.

- Τη νομοθεσία.
- Τους εξωτερικούς συνεργάτες, τους προμηθευτές ή τους σημαντικούς πελάτες.
- Τις διαδικασίες του οργανισμού.
- Τους κινδύνους (οικονομικούς και λειτουργικούς) που απειλούν τον οργανισμό.

12. Έλεγχος συμμόρφωσης

12.1 Συμμόρφωση με τη σχετική νομοθεσία

Σκοπός είναι η αποφυγή παραβίασης νόμων, ρυθμίσεων ή συμβάσεων. Ο σχεδιασμός, η λειτουργία και η διαχείριση ενός πληροφοριακού συστήματος είναι πιθανό να υπόκειται σε κάποιας μορφής νόμους ή συμβάσεις. Το νομικό τμήμα του οργανισμού θα πρέπει να φροντίζει για τη συμμόρφωση με τους διάφορους νόμους και ρυθμίσεις. Ιδιαίτερη προσοχή χρειάζεται όταν εμπλέκονται νομοθεσίες διαφορετικών χωρών (π.χ. κατά τη μεταφορά δεδομένων ανάμεσα σε χώρες).

12.1.1 Καθορισμός της σχετικής νομοθεσίας

Όλες οι υποχρεώσεις που απορρέουν από τη σχετική νομοθεσία θα πρέπει να είναι καταγεγραμμένες για κάθε σύστημα. Επιπλέον θα πρέπει να ορίζονται οι υπεύθυνοι και οι μηχανισμοί συμμόρφωσης.

12.1.2 Πνευματική ιδιοκτησία

12.1.2.1 Copyright

Ο οργανισμός θα πρέπει να λαμβάνει τα κατάλληλα μέτρα για τη συμμόρφωση με τις υποχρεώσεις που προκύπτουν από δικαιώματα δημιουργών, σχεδιαστών ή τη χρήση ονομάτων. Η παραβίαση τέτοιων δικαιωμάτων μπορεί να οδηγήσει σε νομικές κυρώσεις. Θα πρέπει να εξετασθούν οι δυνατότητες τήρησης αντιγράφων του λογισμικού που χρησιμοποιεί ο οργανισμός.

12.1.2.2 Copyright λογισμικού

Το λογισμικό παρέχεται συνήθως με βάση κάποια άδεια χρήσης, η οποία και περιορίζει την εγκατάσταση ή τη χρήση του λογισμικού σε συγκεκριμένους υπολογιστές ή από

συγκεκριμένο αριθμό χρηστών. Επιπλέον πιθανόν να περιορίζει και τη δυνατότητα τήρησης αντιγράφων του λογισμικού. Θα πρέπει να εξεταστούν τα ακόλουθα ζητήματα:

- Η δημιουργία μιας πολιτικής για τη συμμόρφωση με τα πνευματικά δικαιώματα που σχετίζονται με το χρησιμοποιούμενο από τον οργανισμό λογισμικό.
- Η δημιουργία συγκεκριμένης πολιτικής με βάση την οποία θα γίνεται η προμήθεια λογισμικού.
- Η εκπαίδευση και ενημέρωση του προσωπικού στα θέματα πνευματικής ιδιοκτησίας και τις επιπτώσεις τους για τον οργανισμό.
- Η δημιουργία και τήρηση αρχείου του χρησιμοποιούμενου λογισμικού.
- Η διατήρηση αποδείξεων για τη νόμιμη χρήση λογισμικού (άδειες χρήσης, πρωτότυπα του λογισμικού κλπ.).
- Η δημιουργία μιας διαδικασίας που να ελέγχει ότι δε χρησιμοποιείται στον οργανισμό παράνομα εγκατεστημένο λογισμικό.
- Η δημιουργία διαδικασίας για την απεγκατάσταση ή μεταφορά λογισμικού σε τρίτους.
- Η συμμόρφωση με τους όρους απόκτησης και χρήσης λογισμικού μέσω δημόσιων δικτύων.

12.1.3 Προστασία των αρχείων του οργανισμού

Όλα τα σημαντικά αρχεία του οργανισμού θα πρέπει να προστατεύονται απέναντι στο ενδεχόμενο μερικής ή ολικής καταστροφής ή νοθείας. Νομικές διατάξεις μπορεί να επιβάλουν τη τήρηση αρχείων για συγκεκριμένο χρονικό διάστημα. Τέτοια αρχεία μπορεί να χρησιμεύουν ως αποδεικτικά στοιχεία της νόμιμης λειτουργίας του οργανισμού. Η περίοδος διατήρησης των αρχείων συνήθως ορίζεται από τη νομοθεσία.

Τα αρχεία θα πρέπει να είναι κατανεμημένα σε κατηγορίες, π.χ. λογιστικά, διαδικασίες, logs κλπ. Για κάθε κατηγορία θα πρέπει να είναι καθορισμένη η χρονική περίοδος διατήρησης των αρχείων, καθώς και το μέσο φύλαξης. Στην περίπτωση που χρησιμοποιείται κρυπτογραφία

για κάποιο αρχείο, τα σχετικά κλειδιά θα πρέπει να φυλάσσονται ξεχωριστά και να είναι διαθέσιμα μόνο στους εξουσιοδοτημένους χρήστες.

Θα πρέπει να δοθεί προσοχή στο ενδεχόμενο φυσικής φθοράς του μέσου αποθήκευσης των αρχείων, το οποίο θα πρέπει να χρησιμοποιείται σύμφωνα με τις οδηγίες του κατασκευαστή. Για τα μαγνητικά μέσα αποθήκευσης θα πρέπει να υπάρχουν και διαδικασίες ελέγχου της σωστής λειτουργίας.

Το σύστημα αποθήκευσης των αρχείων θα πρέπει να μπορεί να αναγνωρίσει και να χειριστεί ανάλογα τις διάφορες κατηγορίες αρχείων καθόλο το χρονικό διάστημα τήρησής τους. Θα πρέπει επίσης να μπορεί να τα καταστρέψει κατάλληλα μετά το πέρας της αναγκαιότητας φύλαξής τους.

Ο οργανισμός θα πρέπει να ακολουθήσει τα ακόλουθα:

- Θα πρέπει να χρησιμοποιεί τις κατάλληλες διαδικασίες για την αποθήκευση, τη διαχείριση, τον έλεγχο και την καταστροφή των διάφορων τύπων αρχείων.
- Θα πρέπει να έχει καθορισμένο χρονοδιάγραμμα ελέγχου της καταλληλότητας των μέσων αποθήκευσης των αρχείων.
- Θα πρέπει να καθορίσει αναλυτικά τις πληροφορίες που θα αποθηκεύει.
- Θα πρέπει να χρησιμοποιεί τους κατάλληλους μηχανισμούς προστασίας των αρχείων.

12.1.4 Προστασία δεδομένων και προστασία πληροφοριών προσωπικού χαρακτήρα

Σε αρκετές χώρες υπάρχει ειδική νομοθεσία για την επεξεργασία και τη μετάδοση δεδομένων προσωπικού χαρακτήρα. Ως τέτοια, ορίζονται γενικά οι πληροφορίες για άτομα τα οποία μπορούν να αναγνωριστούν με βάση αυτές. Τέτοιοι νόμοι θέτουν περιορισμούς στη συλλογή, την επεξεργασία και τη διάχυση πληροφοριών, ειδικότερα ανάμεσα σε διαφορετικές χώρες.

Η συμμόρφωση με ανάλογη νομοθεσία απαιτεί έλεγχο από τη διοίκηση και τη δημιουργία των κατάλληλων δομών στον οργανισμό. Συνηθισμένη πρακτική είναι ο ορισμός ενός υπεύθυνου προστασίας των δεδομένων, ο οποίος συμβουλεύει τα μέλη του οργανισμού για τις ευθύνες τους, τις διαδικασίες και τον τρόπο διαχείρισης προσωπικών δεδομένων. Ο

υπεύθυνος προστασίας των δεδομένων θα πρέπει να είναι ενήμερος για όλα τα αρχεία προσωπικού χαρακτήρα που τηρούνται στον οργανισμό ώστε να διασφαλίσει τη συμμόρφωσή τους με την υπάρχουσα νομοθεσία.

12.1.5 Πρόληψη κατάχρησης του πληροφοριακού συστήματος

Το πληροφοριακό σύστημα του οργανισμού θα πρέπει να χρησιμοποιείται αποκλειστικά για τις λειτουργικές ανάγκες του οργανισμού. Η διοίκηση του οργανισμού θα πρέπει να εξουσιοδοτεί τους εμπλεκόμενους στη χρήση του. Οποιαδήποτε χρήση του συστήματος για σκοπούς που δεν έχουν σχέση με τον οργανισμό, χωρίς την προηγούμενη εξουσιοδότηση της διοίκησης, θα πρέπει να χαρακτηρίζεται ως κατάχρηση. Αν κάποια τέτοια δραστηριότητα γίνει αντιληπτή με οποιοδήποτε τρόπο, θα πρέπει να γνωστοποιηθεί στο κατάλληλο μέλος της διοίκησης, ο οποίος είναι υπεύθυνος για την επιβολή κατάλληλων κυρώσεων.

Η νομιμότητα της παρακολούθησης της χρήσης του συστήματος διαφέρει από χώρα σε χώρα και είναι δυνατό να απαιτεί την προηγούμενη ενημέρωση και τη σύμφωνη γνώμη των υπαλλήλων. Θα πρέπει το θέμα να διερευνηθεί από τους νομικούς συμβούλους του οργανισμού.

Αρκετές χώρες διαθέτουν ή πρόκειται να εφαρμόσουν νόμους για την αντιμετώπιση της κατάχρησης των υπολογιστικών συστημάτων, η οποία μπορεί να εκλαμβάνεται ως ποινικό αδίκημα. Για αυτό το λόγο, οι χρήστες του συστήματος πρέπει να είναι ενημερωμένοι για τις συνέπειες ενεργειών που συνιστούν κατάχρηση του συστήματος, καθώς και για τα δικαιώματα χρήσης που έχουν σε αυτό. Ο οργανισμός θα πρέπει να δίνει στο προσωπικό – χρήστες του συστήματος γραπτή εξουσιοδότηση με συγκεκριμένα δικαιώματα σε αυτό. Επιπλέον οι χρήστες θα πρέπει να υπογράφουν ότι έλαβαν γνώση των δικαιωμάτων τους.

Όλοι οι χρήστες του συστήματος, προσωπικό και εξωτερικοί συνεργάτες, θα πρέπει να ενημερώνονται για τις συνέπειες της κατάχρησής του. Κατά τη διαδικασία της σύνδεσης στο σύστημα θα πρέπει να εμφανίζεται σχετικό προειδοποιητικό μήνυμα. Ο χρήστης θα πρέπει να επιβεβαιώσει ότι έλαβε γνώση του μηνύματος πριν συνεχίσει την εργασία του στο πληροφοριακό σύστημα του οργανισμού.

12.1.6 Κανονισμοί χρήσης κρυπτογραφίας

Σε κάποιες χώρες υπάρχουν νόμοι που ελέγχουν την πρόσβαση ή τη χρήση τεχνικών κρυπτογραφίας. Τέτοιοι περιορισμοί περιλαμβάνουν τα ακόλουθα:

- Την εισαγωγή και την εξαγωγή εξοπλισμού και λογισμικού για τη διενέργεια κρυπτογράφησης.
- Την εισαγωγή και την εξαγωγή εξοπλισμού και λογισμικού που είναι σχεδιασμένα να προσφέρουν υπηρεσίες κρυπτογραφίας.
- Μηχανισμούς για την πρόσβαση των τοπικών αρχών στο περιεχόμενο κρυπτογραφημένων πληροφοριών.

Θα πρέπει να ζητείται η συμβουλή ειδικών για τη συμμόρφωση με τους σχετικούς νόμους. Το ίδιο θα πρέπει να γίνει στην περίπτωση που εμπλέκονται διαφορετικές χώρες (π.χ. κατά τη μεταφορά κρυπτογραφημένων πληροφοριών).

12.1.7 Συλλογή αποδεικτικών στοιχείων

12.1.7.1 Κανονισμοί

Για την υποστήριξη κάποιας διοικητικής ή δικαστικής ενέργειας είναι απαραίτητη η ύπαρξη επαρκών στοιχείων. Εφόσον η υπόθεση έχει αποκλειστικά εσωτερικό χαρακτήρα, η συλλογή αποδείξεων θα πρέπει να ρυθμίζεται από κανονισμούς του οργανισμού. Εφόσον εμπλέκονται νομικές διαδικασίες, τα αποδεικτικά στοιχεία θα πρέπει να είναι σύμφωνα με τους νόμους. Γενικά, τέτοιοι κανονισμοί περιλαμβάνουν:

- Τη δυνατότητα να γίνουν αποδεκτά τα στοιχεία στο δικαστήριο.
- Την ποιότητα και την αρτιότητα των στοιχείων.
- Απόδειξη ότι οι μηχανισμοί ελέγχου και συλλογής στοιχείων λειτουργούν κανονικά και ότι τα στοιχεία αποθηκεύτηκαν και επεξεργάστηκαν με αποδεκτούς τρόπους από το σύστημα.

12.1.7.2 Αποδεκτά στοιχεία

Προκειμένου τα αποδεικτικά στοιχεία να είναι αποδεκτά, ο οργανισμός θα πρέπει να διασφαλίσει ότι το πληροφοριακό σύστημα λειτουργεί σύμφωνα με όλους τους κανονισμούς συλλογής στοιχείων.

12.1.7.3 Ποιότητα και αρτιότητα στοιχείων

Για να επιτευχθεί η ποιότητα και η αρτιότητα των στοιχείων θα πρέπει να εξασφαλισθούν τα ακόλουθα:

- Για τα φυσικά έγγραφα θα πρέπει να φυλάσσεται το πρωτότυπο και να καταγράφεται ποιος το βρήκε, που το βρήκε και ποιος παρευρισκόταν κατά την ανακάλυψη. Θα πρέπει, επίσης, να διασφαλισθεί ότι τα έγγραφα δεν έχουν παραποιηθεί.
- Για τις πληροφορίες που περιέχονται σε ηλεκτρονική μορφή, θα πρέπει να προβλέπεται η φύλαξη των αποθηκευτικών μέσων ώστε να μην καταστραφούν τα στοιχεία. Στην

περίπτωση που γίνουν αντίγραφα, θα πρέπει να τηρηθεί αρχείο με όλες τις ενέργειες που ακολουθήθηκαν κατά την αντιγραφή. Επιπλέον, τουλάχιστον ένα αντίγραφο θα πρέπει να αποθηκευθεί με ιδιαίτερη προσοχή και ασφάλεια.

Όταν εντοπισθεί κάποια μη εξουσιοδοτημένη ενέργεια, μπορεί να μην είναι φανερό εξαρχής ότι το θέμα θα εξελιχθεί σε κάποια πιθανή δικαστική ενέργεια. Κατά συνέπεια, ο κίνδυνος καταστροφής στοιχείων από αμέλεια είναι πολύ μεγάλος πριν διαπιστωθεί η σοβαρότητα της κατάστασης. Για αυτό το σκοπό θα πρέπει να ζητείται η συμβουλή δικηγόρου ή της αστυνομίας όσο το δυνατό ταχύτερα.

12.2 Έλεγχοι της πολιτικής ασφάλειας και τεχνική συμμόρφωση

Σκοπός είναι η διασφάλιση της συμμόρφωσης των συστημάτων με την πολιτική ασφάλειας και τα πρότυπα του οργανισμού. Η ασφάλεια του υπολογιστικού συστήματος θα πρέπει να ελέγχεται τακτικά. Τέτοιοι έλεγχοι θα πρέπει να γίνονται με γνώμονα την πολιτική ασφάλειας του οργανισμού, τα υπάρχοντα πρότυπα ασφάλειας και τις τεχνολογικές εξελίξεις.

12.2.1 Συμμόρφωση με την πολιτική ασφάλειας

Τα μέλη της διοίκησης του οργανισμού θα πρέπει να επιβλέπουν τη σωστή εφαρμογή της πολιτικής ασφάλειας του οργανισμού στον τομέα ευθύνης τους. Επιπλέον, όλα τα μέρη του οργανισμού θα πρέπει να ελέγχονται περιοδικά για τη συμμόρφωσή τους με την πολιτική και τα πρότυπα ασφάλειας του οργανισμού. Θα πρέπει να συμπεριλαμβάνονται τα ακόλουθα:

- Τα πληροφοριακά συστήματα.
- Οι παροχείς των συστημάτων.
- Οι ορισμένοι ιδιοκτήτες των πόρων του συστήματος και των πληροφοριών.
- Οι χρήστες.
- Η διοίκηση του οργανισμού.

Οι ιδιοκτήτες των πληροφοριακών συστημάτων (παράγραφος 5.1) θα πρέπει να υποστηρίζουν τον τακτικό έλεγχο των συστημάτων τους.

12.2.2 Έλεγχος τεχνικής συμμόρφωσης

Τα πληροφοριακά συστήματα θα πρέπει να ελέγχονται τακτικά για τη συμμόρφωσή τους με τα πρότυπα υλοποίησης της ασφάλειας. Ο έλεγχος τεχνικής συμμόρφωσης περιλαμβάνει τον έλεγχο της σωστής λειτουργίας των μηχανισμών ελέγχου τόσο σε επίπεδο υλικού, όσο και σε επίπεδο λογισμικού. Για αυτό το σκοπό απαιτείται συμβουλή ειδικών εμπειρογνωμόνων. Θα πρέπει να γίνεται από κάποιον έμπειρο επιστήμονα, με τη χρήση κατάλληλων εργαλείων ή από κάποιο εξειδικευμένο πακέτο λογισμικού.

Οι έλεγχοι θα πρέπει να περιλαμβάνουν για παράδειγμα δοκιμές παραβίασης (penetration testing), που μπορούν να γίνουν από εξειδικευμένους εξωτερικούς συνεργάτες. Με αυτόν τον τρόπο είναι δυνατή η αναγνώριση των αδυναμιών του συστήματος. Απαιτείται όμως ιδιαίτερη προσοχή, γιατί κατά τη διάρκεια ενός τέτοιου ελέγχου μπορεί να παρουσιασθούν προβλήματα στη λειτουργία του συστήματος.

Σε κάθε περίπτωση, οποιοσδήποτε έλεγχος θα πρέπει να γίνεται υπό την επίβλεψη εξουσιοδοτημένου προσωπικού του οργανισμού.

12.3 Ζητήματα ελέγχου συστημάτων

Σκοπός είναι η μεγιστοποίηση της αποτελεσματικότητας της διαδικασίας ελέγχου του πληροφοριακού συστήματος, με ταυτόχρονη ελαχιστοποίηση των παρεμβολών από ή προς το σύστημα. Θα πρέπει να υπάρχουν μηχανισμοί προστασίας των συστημάτων και των εργαλείων ελέγχου κατά τη διάρκεια εκτέλεσης των ελέγχων. Θα πρέπει, επίσης, να υπάρχουν κάποιοι μηχανισμοί προστασίας απέναντι στην κακή χρήση των εργαλείων ελέγχου.

12.3.1 Μηχανισμοί ελέγχου συστημάτων

Η διενέργεια ελέγχων σε συστήματα παραγωγής θα πρέπει να είναι προσεκτικά σχεδιασμένη ώστε να ελαχιστοποιηθεί ο κίνδυνος παρεμβολών στην ομαλή λειτουργία του οργανισμού. Θα πρέπει να εξεταστούν τα ακόλουθα:

- Η διαδικασία ελέγχου θα πρέπει να συμπληρώνεται από ένα κατάλληλο σύστημα διαχείρισης.
- Ο σκοπός των ελέγχων θα πρέπει να είναι σαφής και προσυμφωνημένος.
- Οι διαδικασίες ελέγχου θα πρέπει να έχουν μόνο δικαιώματα ανάγνωσης σε λογισμικό και δεδομένα.
- Επιπλέον τύποι πρόσβασης θα πρέπει να επιτρέπονται μόνο σε απομονωμένα αντίγραφα αρχείων, τα οποία και θα πρέπει να καταστρέφονται μετά το πέρας των ελέγχων.
- Οι απαραίτητοι πόροι θα πρέπει να είναι σαφώς καθορισμένοι και διαθέσιμοι.
- Τυχόν επιπλέον ανάγκες για επεξεργασία δεδομένων θα πρέπει να είναι καθορισμένες και προσυμφωνημένες.
- Κάθε είδους πρόσβαση στο σύστημα θα πρέπει να παρακολουθείται και να καταγράφεται.
- Όλες οι σχετικές διαδικασίες, οι απαιτήσεις και ο καταμερισμός των ευθυνών θα πρέπει να είναι αναλυτικά καταγεγραμμένα.

12.3.2 Προστασία εργαλείων ελέγχου συστημάτων

Η πρόσβαση στα εργαλεία διενέργειας ελέγχων, όπως ειδικό λογισμικό ή αρχεία δεδομένων, θα πρέπει να προστατεύονται από λάθος χρήση, κατάχρηση ή έκθεση. Τέτοια εργαλεία θα πρέπει να φυλάσσονται ξεχωριστά από τα συστήματα παραγωγής και ανάπτυξης και ξεχωριστά από τα υπόλοιπα αρχεία του οργανισμού.

Βιβλιογραφικές Αναφορές

BS ISO/IEC 17799:2000 & BS 7799-1:2000, *Information technology – Code of practice for information security management*. British Standards Publishing Limited.

Tudor, Jan (2000), *Information Security Architecture: An Integrated Approach to Security in the Organization.* CRC Press.

Krause, Micki & Tipton, Harold F. (1999), *Information Security Management Handbook, 4th Edition.* CRC Press.

Peltier, Thomas R. (2001), *Information Security Risk Analysis.* Auerbach Publications.

Byrnes, Christian F. & Kutnick, Dale (2002), *Securing Business Information: Strategies to Protect the Enterprise and its Network.* Addison-Wesley Publications.

Krutz, Ronald L. & Vines, Russel (2001), *The CISSP Prep Guide.* Wiley & Sons.

Kovacich, Gerald L. (1998), *The Information Systems Security Officer's Guide: Establishing and Managing an Information Protection Program.* Butterworth – Heinemann.

Barman, Scott (2001), *Writing Information Security Policies.* New Riders Publishing.