Κεφάλαιο 2

Διακυβέρνηση και Διοίκηση Ασφάλειας Πληροφοριών

Σπύρος Κοκολάκης

Τμήμα Μηχανικών Πληροφοριακών και Επικοινωνιακών Συστημάτων

Πολυτεχνική Σχολή
Πανεπιστήμιο Αιγαίου
Καρλόβασι, 83200 Σάμος
email: sak@aegean.gr

Περίληψη

Η ασφάλεια πληροφοριακών συστημάτων αποτελεί ένα διεπιστημονικό πεδίο, όπου μπορούμε να διακρίνουμε μία τεχνολογική και μία οργανωσιακή διάσταση, οι οποίες είναι εξίσου σημαντικές και αδιάρρηκτα αλληλένδετες μεταξύ τους. Θεωρώντας ότι κάθε πληροφοριακό σύστημα εντάσσεται σε έναν ή και περισσότερους οργανισμούς, δίνουμε έμφαση στη μελέτη της ασφάλειας πληροφοριακών συστημάτων εντός του οργανωσιακού πλαισίου. Εντάσσοντας, λοιπόν, την ασφάλεια πληροφοριακών συστημάτων στο οργανωσιακό πλαίσιο, αναγνωρίζουμε την ανάγκη για διακυβέρνηση (governance) και διοίκηση (management) της ασφάλειας πληροφοριών, δύο βασικές οργανωσιακές διεργασίες που αποτελούν το αντικείμενο του παρόντος Κεφαλαίου.

Στην εισαγωγή του Κεφαλαίου διακρίνουμε τις δύο έννοιες, διακυβέρνηση και διοίκηση και αναλύουμε το περιεχόμενό τους. Έπειτα, περιγράφουμε τους στόχους της διακυβέρνησης ασφάλειας πληροφοριών και τις δράσεις που περιλαμ-

βάνει. Στη συνέχεια, εισάγουμε την έννοια του Συστήματος Διαχείρισης Ασφάλειας Πληροφοριών και παρουσιάζουμε αναλυτικά τις συνιστώσες του και τους τομείς της ασφάλειας πληροφοριών που εντάσσονται στο πεδίο του. Ιδιαίτερη έμφαση δίνεται στη διαχείριση της επικινδυνότητας, στην οποία αφιερώνεται ξεχωριστή ενότητα. Το Κεφάλαιο ολοκληρώνεται με τη συνοπτική ανακεφαλαίωση και τις σχετικές βιβλιογραφικές αναφορές.

2.1. Εισαγωγή

Τόσο οι ερευνητές όσο και οι επαγγελματίες του χώρου της ασφάλειας πληροφοριών, αρκετά συχνά, τείνουν να δίνουν δυσανάλογη βαρύτητα στην τεχνική διάσταση της ασφάλειας πληροφοριών. Οπωσδήποτε η ανάπτυξη και εφαρμογή τεχνολογιών και εργαλείων προστασίας των ψηφιακών συστημάτων είναι εξαιρετικά σημαντική. Οι τεχνικές και τα εργαλεία προστασίας αποτελούν τη βάση κάθε συστήματος ασφάλειας πληροφοριών. Όμως, αν εξετάσουμε τις πιο συνήθεις περιπτώσεις παραβίασης της ασφάλειας των συστημάτων θα διαπιστώσουμε ότι οι κυριότερες αδυναμίες εντοπίζονται σε ζητήματα όπως η εκπαίδευση του προσωπικού, η εφαρμογή πολιτικών και διαδικασιών, ο έλεγχος της συμμόρφωσης με τις πολιτικές ασφάλειας πληροφοριών κ.ά. Αυτά τα ζητήματα χαρακτηρίζονται ως *οργανωσιακά*, με την έννοια ότι αφορούν στον οργανισμό που διαχειρίζεται τις πληροφορίες και στους ανθρώπους που εμπλέκονται στη χρήση και τη διαχείριση των σχετικών συστημάτων.

Μπορούμε, λοιπόν, να υιοθετήσουμε μία ευρύτερη θεώρηση, όπου η ασφάλεια πληροφοριών συνεπάγεται την προστασία των συστημάτων που διαχειρίζονται τις πληροφορίες, τα οποία αποκαλούμε *πληροφοριακά συστήματα (information systems)*, στο πλαίσιο ενός οργανισμού[1], που μπορεί να είναι ιδιωτική επιχείρηση, δημόσιος φορέας, ή ακόμη και ένας σύλλογος ή μια οργανωμένη ομάδα ανθρώπων. Σε αυτό το πλαίσιο, τα ζητήματα ασφάλειας πληροφοριών που μας απασχολούν περιλαμβάνουν τις πολιτικές του οργανισμού, τις διαδικασίες που ακολουθεί, τους ρόλους και τις αρμοδιότητες των στελεχών του, το νομικό και θεσμικό πλαίσιο στο οποίο λειτουργεί, τη συμπεριφορά των χρηστών κ.ά. Στην αντιμετώπιση αυτών των ζητημάτων απαιτείται η συμβολή πολλών επιστημών, όπως η διοίκηση επιχειρήσεων, η ψυχολογία, η νομική και οι επιστήμες των τεχνολογιών πληροφορικής και επικοινωνιών. Πρόκειται, δηλαδή, για ένα *διεπιστημονικό* αντικείμενο μελέτης και έρευνας.

[1] Χρησιμοποιούμε τον όρο ‘οργανισμός’ αντί του ορθότερου ‘οργάνωση’, καθώς ο πρώτος όρος έχει καθιερωθεί στην ελληνική βιβλιογραφία.

Σε κάθε οργανισμό, λοιπόν, που ενδιαφέρεται για την ασφάλεια των πληροφοριακών του συστημάτων προκύπτει η ανάγκη όχι απλά για την τεχνική αντιμετώπιση των προβλημάτων ασφάλειας, αλλά για την οργανωμένη *διακυβέρνηση και διοίκηση της ασφάλειας πληροφοριών*. Οι έννοιες της διακυβέρνησης (governance) και της διοίκησης (management) είναι συναφείς, αλλά έχουν διακριτό νόημα, όπως θα εξηγήσουμε στη συνέχεια.

Η διακυβέρνηση ασφάλειας πληροφοριών ορίζεται ως η επιχειρησιακή διεργασία (business process) της εγκαθίδρυσης και διατήρησης ενός πλαισίου (framework) και μιας διοικητικής δομής που διασφαλίζει ότι οι στρατηγικές ασφάλειας πληροφοριών υποστηρίζουν και εναρμονίζονται με τους στόχους του οργανισμού, αναθέτουν υπευθυνότητες και είναι συνεπείς με το νομικό και θεσμικό πλαίσιο, εφαρμόζοντας τις κατάλληλες πολιτικές και μέτρα, σε μια προσπάθεια να διαχειριστούν τους κινδύνους ασφάλειας [1].

Ο παραπάνω ορισμός προσδιορίζει ως *στόχο* της διακυβέρνησης ασφάλειας πληροφοριών τη διαχείριση των κινδύνων και ως *μέσο* τις στρατηγικές ασφάλειας πληροφοριών. Οι τελευταίες θα πρέπει να εναρμονίζονται με τους ευρύτερους στόχους του οργανισμού και να συμβάλλουν στην επίτευξη των οργανωσιακών στόχων. Επίσης, οι στρατηγικές αυτές θα πρέπει να λαμβάνουν υπόψη τις απαιτήσεις που προκύπτουν από το νομικό και θεσμικό πλαίσιο και να καθοδηγούν την εφαρμογή πολιτικών και μέτρων για τη συμμόρφωση με τις νομικές και θεσμικές απαιτήσεις. Βασικός άξονας της διακυβέρνησης είναι η ανάθεση υπευθυνοτήτων και, γενικότερα, η διαμόρφωση της κατάλληλης διοικητικής δομής που θα καθορίζει τους ρόλους που σχετίζονται με την ασφάλεια πληροφοριών και θα αντιστοιχεί σε κάθε ρόλο τις κατάλληλες αρμοδιότητες και υπευθυνότητες.

Ενώ η διακυβέρνηση ασφάλειας πληροφοριών ασχολείται με τη στρατηγική, δηλαδή με το τι πρέπει να γίνει, η *διοίκηση ασφάλειας πληροφοριών (information security management)* ασχολείται με το πώς θα υλοποιηθεί η στρατηγική. Η διοίκηση ασφάλειας πληροφοριών ορίζει τους στόχους ασφάλειας και διαμορφώνει πολιτικές, διαδικασίες και οδηγίες για την επίτευξη των στόχων. Επιπλέον, καθοδηγεί και επιβλέπει τη λήψη αποφάσεων που σχετίζονται με την ασφάλεια πληροφοριών σε όλα τα επίπεδα του οργανισμού, από το επίπεδο της καθημερινής λειτουργίας (π.χ. αποφάσεις για την εκχώρηση δικαιωμάτων πρόσβασης σε χρήστες) μέχρι το επίπεδο της ανώτερης διοίκησης (π.χ. αποφάσεις για την προμήθεια συστημάτων).

Στη συνέχεια θα παρουσιάσουμε αναλυτικά τη διακυβέρνηση και τη διοίκηση της ασφάλειας πληροφοριών και θα επικεντρωθούμε σε ορισμένες από τις πιοση-

μαντικές δράσεις που περιλαμβάνονται σε αυτές, όπως η διαχείριση επικινδυνότητας.

2.2. Διακυβέρνηση ασφάλειας πληροφοριών

Στους βασικούς στόχους της διακυβέρνησης ασφάλειας πληροφοριών περιλαμβάνονται οι εξής:

- **Εναρμόνιση (alignment) με τη στρατηγική του οργανισμού.** Οι στρατηγικές, πολιτικές και δράσεις για την ασφάλεια πληροφοριών απαιτείται να εξυπηρετούν τους στρατηγικούς στόχους του οργανισμού. Η ασφάλεια πληροφοριών δε θα πρέπει να αποτελεί αυτοσκοπό. Αντιθέτως, θα πρέπει να καθορίζεται από τους οργανωσιακούς στόχους και να υποστηρίζει την επίτευξή τους. Ειδικότερα, η διακυβέρνηση ασφάλειας πληροφοριών περιορίζει την πιθανότητα να υπάρξουν περιστατικά ασφάλειας που θα εμποδίσουν την επίτευξη των οργανωσιακών στόχων. Η πιθανότητα αυτή δεν μπορεί να μηδενιστεί, αλλά μπορεί να περιοριστεί. Ο βαθμός στον οποίο θα περιοριστεί αποτελεί απόφαση της διοίκησης του οργανισμού και εντάσσεται στους στόχους της διακυβέρνησης ασφάλειας πληροφοριών.
- **Διαχείριση επικινδυνότητας (risk management).** Η βάση στην οποία οικοδομείται η ασφάλεια πληροφοριών είναι η διαχείριση της επικινδυνότητας, που συνεπάγεται τη μείωση της επικινδυνότητας σε επίπεδο που θεωρείται ανεκτό από τον οργανισμό. Επικινδυνότητα είναι το μέτρο της έκθεσης ενός οργανισμού σε κινδύνους. Είναι, δηλαδή, ένα μετρήσιμο μέγεθος. Κατά συνέπεια, στόχος της διακυβέρνησης ασφάλειας πληροφοριών είναι να θέσει ένα πλαίσιο για τη μέτρηση της επικινδυνότητας και τη διαχείρισή της.
- **Διαχείριση πόρων (resource management).** Η ασφάλεια πληροφοριών απαιτεί τη διάθεση πόρων, η οποίοι είναι ανθρώπινοι, υλικοί (εξοπλισμός, εγκαταστάσεις κ.λπ.) και οικονομικοί. Η διακυβέρνηση ασφάλειας πληροφοριών μεριμνά για τη διάθεση των απαιτούμενων πόρων, αλλά και για την εναρμόνιση του προϋπολογισμού που δεσμεύεται για την ασφάλεια πληροφοριών με τους οικονομικούς στόχους του οργανισμού.
- **Συνεισφορά αξίας (value delivery).** Οι επενδύσεις στην ασφάλεια πληροφοριών θα πρέπει να σχεδιάζονται και να υλοποιούνται με τρόπο που να διασφαλίζει ότι θα έχουν τη βέλτιστη απόδοση, δηλαδή θα έχουν τη μέγιστη συνεισφορά στην ασφάλεια πληροφοριών που αντιστοιχεί στους πόρους που επενδύονται.

- **Μέτρηση της απόδοσης (performance measurement).** Ο οργανισμός χρειάζεται μετρικές, με τις οποίες θα μπορεί να κρίνει αν επιτυγχάνονται οι στόχοι του οργανισμού σε σχέση με την ασφάλεια πληροφοριών.

Οι κυριότερες δράσεις της διακυβέρνησης ασφάλειας πληροφοριών περιλαμβάνουν:

- **Τον στρατηγικό σχεδιασμό.** Αφορά στην ανάπτυξη ενός στρατηγικού σχεδίου για την ασφάλεια πληροφοριών, το οποίο θα καθοδηγείται από τους στόχους που περιγράψαμε παραπάνω.
- **Τη διαμόρφωση της κατάλληλης οργανωσιακής δομής.** Όπου η οργανωσιακή δομή περιλαμβάνει την ένταξη της ασφάλειας πληροφοριών στον οργανόγραμμα του οργανισμού, τη συγκρότηση επιτροπών, οργάνων διοίκησης και θέσεων, όπου απαιτείται, και την καταγραφή και εφαρμογή κατάλληλων οργανωσιακών διαδικασιών.
- **Τον καθορισμό ρόλων και την απονομή αρμοδιοτήτων και υπευθυνοτήτων στον κάθε ρόλο.** Έχει ως στόχο να εξειδικεύσει και να καταστήσει λειτουργική την οργανωσιακή δομή.
- **Την ενσωμάτωση του συστήματος διαχείρισης ασφάλειας πληροφοριών στον οργανωσιακό αρχιτεκτονικό σχεδιασμό.** Η διοίκηση ασφάλειας πληροφοριών, την οποία θα αναλύσουμε στην επόμενη ενότητα, θα πρέπει να εντάσσεται στο αρχιτεκτονικό πλάνο του οργανισμού, δηλαδή στον υψηλού επιπέδου σχεδιασμό της διοίκησης του οργανισμού.
- **Την τεκμηρίωση των στόχων ασφάλειας στις πολιτικές του οργανισμού και την παροχή καθοδήγησης για την υλοποίησή τους.** Οι πολιτικές του οργανισμού, είτε αφορούν άμεσα την ασφάλεια πληροφοριών είτε απλώς την επηρεάζουν, θα πρέπει να είναι τεκμηριωμένες, δηλαδή να έχουν καταγραφεί με δομημένο και οργανωμένο τρόπο και να εδράζονται σε συγκεκριμένους στόχους. Η διακυβέρνηση ασφάλειας πληροφοριών μεριμνά, επιπλέον, για την παροχή κατάλληλης καθοδήγησης με σκοπό την εφαρμογή των πολιτικών ασφάλειας πληροφοριών. Η καθοδήγηση μπορεί να λάβει πολλές μορφές, όπως έκδοση οδηγιών (guidelines), εκπαίδευση, έλεγχο (audit) κ.ά.

2.3. Διοίκηση ασφάλειας πληροφοριών

2.3.1. Γενικά

Η πλέον ενδεδειγμένη προσέγγιση στη διοίκηση ασφάλειας πληροφοριών είναι ο σχεδιασμός και εφαρμογή ενός *Συστήματος Διαχείρισης Ασφάλειας Πληροφοριών – ΣΔΑΠ (Information Security Management System – ISMS)*. Ο Διεθνής Οργανισμός Τυποποίησης (International Organization for Standardization – ISO) σε συνεργασία με τη Διεθνή Επιτροπή Ηλεκτροτεχνίας (International Electrotechnical Commission – IEC) έχει εκδώσει ένα ειδικό πρότυπο που προδιαγράφει τις απαιτήσεις που θα πρέπει να ικανοποιεί ένα ΣΔΑΠ, το πρότυπο ISO/IEC 27001 [2]. Το ISO/IEC 27001 είναι ένα λεπτομερές πρότυπο και η εφαρμογή του πιστοποιείται έπειτα από έλεγχο που διεξάγουν αρμοδίως διαπιστευμένοι φορείς (accredited bodies).

Το ΣΔΑΠ δεν είναι απλώς ένα σύνολο κανόνων, διαδικασιών και μέτρων, αλλά αποτελεί ένα σύστημα, το οποίο ο οργανισμός σχεδιάζει, υλοποιεί, συντηρεί και βελτιώνει. Κατά συνέπεια, η επιτυχία του ΣΔΑΠ εξαρτάται σε μεγάλο βαθμό από τα ακόλουθα:

- Κατανόηση του οργανισμού και του περιβάλλοντός του.
- Κατανόηση των αναγκών και των απαιτήσεων των δικαιούχων (stakeholders), όπως είναι οι χρήστες, οι ιδιοκτήτες των πληροφοριών, η πολιτεία διαμέσου της νομοθεσίας και των θεσμικών οργάνων της κ.λπ.
- Άσκηση ηγεσίας και δέσμευση της ανώτερης διοίκησης του οργανισμού στους στόχους της ασφάλειας πληροφοριών.
- Σύνταξη και επικύρωση της πολιτικής ασφάλειας πληροφοριών (βλ. ενότητα 2.3.2), καθώς και προσδιορισμός ρόλων, αρμοδιοτήτων και υπευθυνοτήτων, σύμφωνα με το πλαίσιο που διαμορφώνει η διακυβέρνηση ασφάλειας πληροφοριών.
- Σχεδιασμός του ΣΔΑΠ με βάση τα αποτελέσματα της αποτίμησης της επικινδυνότητας (security risk assessment), δηλαδή της διαδικασίας με την οποία εντοπίζουμε, αναλύουμε και εκτιμούμε τη σοβαρότητα των κινδύνων που δυνητικά αντιμετωπίζει το πληροφοριακό σύστημα (βλ. ενότητα 2.4).
- Προσδιορισμός στόχων ασφάλειας, οι οποίοι θα πρέπει να είναι σαφείς, εφικτοί, επαρκείς και να απορρέουν από την πολιτική ασφάλειας πληροφοριών.

- Υποστήριξη του ΣΔΑΠ με πόρους ανθρώπινους, υλικούς και οικονομικούς, αλλά και με την ανάπτυξη των κατάλληλων δεξιοτήτων, την εκπαίδευση και ευαισθητοποίηση του προσωπικού και τις δράσεις επικοινωνίας.
- Τεκμηρίωση (documentation) του ΣΔΑΠ και των πληροφοριών που απαιτούνται για την εφαρμογή του και διαχείριση της τεκμηρίωσης (έλεγχος, ενημέρωση κ.λπ).
- Παρακολούθηση (monitoring), μέτρηση (measurement), ανάλυση (analysis), αξιολόγηση (evaluation) και αναθεώρηση (review), όταν απαιτείται, του ΣΔΑΠ, έτσι ώστε να βελτιώνεται διαρκώς και να καλύπτει τις μεταβαλλόμενες ανάγκες του οργανισμού.
- Εσωτερικός έλεγχος (internal audit) για τη διασφάλιση της αποτελεσματικής εφαρμογής του ΣΔΑΠ.

Το ΣΔΑΠ, σύμφωνα με το πρότυπο ISO/IEC 27001 απαιτείται να καλύπτει δεκατέσσερις βασικούς τομείς:

1. Πολιτικές ασφάλειας πληροφοριών (Information security policies).
2. Οργάνωση της ασφάλειας πληροφοριών (Organization of information security).
3. Ανθρώπινο δυναμικό (Human resource management).
4. Διαχείριση περιουσιακών στοιχείων (Asset management).
5. Έλεγχος πρόσβασης (Access control).
6. Κρυπτογραφία (Cryptography).
7. Φυσική και περιβαλλοντική ασφάλεια (Physical and environmental security).
8. Λειτουργική ασφάλεια (Operations security).
9. Ασφάλεια επικοινωνιών (Communications security).
10. Προμήθεια, ανάπτυξη και συντήρηση συστημάτων (System acquisition, development and maintenance).
11. Σχέσεις με προμηθευτές (Supplier relationships).
12. Διαχείριση επεισοδίων ασφάλειας πληροφοριών (Information security incident management).

13. Ασφάλεια πληροφοριών και επιχειρησιακή συνέχεια (Information security aspects of business continuity management).
14. Συμμόρφωση (Compliance).

Ο σχεδιασμός και η εφαρμογή ενός ΣΔΑΠ σύμφωνα με τις προδιαγραφές του ISO/IEC 27001 αποτελεί μία από τις πιθανές επιλογές ενός οργανισμού. Εναλλακτικά, ένας οργανισμός θα μπορούσε να οργανώσει τη διοίκηση της ασφάλειας πληροφοριών με τον δικό του τρόπο, αναλόγως της τεχνογνωσίας που διαθέτει. Όμως, σε κάθε περίπτωση τα πρότυπα του ISO δίνουν ένα ολοκληρωμένο πλαίσιο για τη διοίκηση της ασφάλειας, που μπορεί να αποτελέσει έναν καλό οδηγό για κάθε προσπάθεια οργάνωσης της ασφάλειας πληροφοριών, είτε ο οργανισμός αποφασίσει να συμμορφωθεί με τα παραπάνω πρότυπα, είτε αποφασίσει να διαφοροποιηθεί.

2.3.2. Πολιτικές ασφάλειας πληροφοριών

Οι πολιτικές ασφάλειας πληροφοριών καθορίζουν τις αρχές και τους κανόνες που καθοδηγούν τις αποφάσεις που λαμβάνονται και τη συμπεριφορά των εμπλεκομένων στη λειτουργία των πληροφοριακών συστημάτων. Οι πολιτικές διακρίνονται ως προς το εύρος που καλύπτουν σε γενικές, θεματικές και αρθρωτές πολιτικές.

Οι γενικές ή αναλυτικές πολιτικές αναφέρονται σε όλες τις διαστάσεις ενός πληροφοριακού συστήματος ή ακόμη και σε πολλά πληροφοριακά συστήματα του ίδιου φορέα. Κατά συνέπεια, οι οδηγίες που περιλαμβάνουν είναι σε γενικό επίπεδο, δηλαδή σε υψηλό επίπεδο αφαίρεσης (level of abstraction), χωρίς λεπτομέρειες. Ένα βασικό μειονέκτημά τους είναι ότι απευθύνονται σε διαφορετικές κατηγορίες χρηστών, διαχειριστών κ.λπ., οι οποίοι θα πρέπει να ξεχωρίσουν ποιο μέρος της πολιτικής τούς αφορά και ποιο όχι.

Μία άλλη προσέγγιση είναι η αρθρωτή δόμηση των πολιτικών, όπου υπάρχει ένα βασικό ενιαίο κείμενο πολιτικής, το οποίο συνοδεύεται από ξεχωριστά παραρτήματα που αφορούν διαφορετικά συστήματα ή διαφορετικές κατηγορίες προσώπων. Αυτές οι πολιτικές είναι περισσότερο εύχρηστες και συνδυάζουν το γενικό πλαίσιο πολιτικής με τις περισσότερο λεπτομερείς ειδικές πολιτικές.

Θεματικές πολιτικές ονομάζουμε εκείνες που αφορούν ένα σύστημα ή μια εφαρμογή. Για παράδειγμα, μπορούμε να έχουμε πολιτικές ασφάλειας για τη χρήση του Διαδικτύου, για τον έλεγχο πρόσβασης (access control), για τη χρήση του ηλεκτρονικού ταχυδρομείου κ.ά. Το βασικό μειονέκτημά τους είναι ότι συχνά οδηγούν

σε μία αποσπασματική διαχείριση της ασφάλειας και μπορεί να μην είναι συνεπείς μεταξύ τους.

Σύμφωνα με τον ISO [3] οι θεματικές πολιτικές ασφάλειας μπορεί να αφορούν αντικείμενα, όπως:

- Πολιτική ελέγχου πρόσβασης.
- Πολιτική κατηγοριοποίησης και χειρισμού πληροφοριών.
- Πολιτική φυσικής και περιβαλλοντικής ασφάλειας.
- Πολιτική αντιγράφων ασφάλειας.
- Πολιτική μετάδοσης πληροφοριών.
- Πολιτική προστασίας από κακόβουλο λογισμικό.
- Πολιτική διαχείρισης τεχνικών ευπαθειών.
- Πολιτική κρυπτογραφικών μέσων.
- Πολιτική ασφάλειας επικοινωνιών.
- Πολιτική ιδιωτικότητας και προστασίας δεδομένων προσωπικού χαρακτήρα.
- Πολιτική σχέσεων με προμηθευτές.

Ειδικότερα όσον αφορά στους χρήστες των συστημάτων, ο ISO [3] διακρίνει τις εξής πολιτικές:

- Πολιτική αποδεκτής χρήσης.
- Πολιτική καθαρού γραφείου και καθαρής οθόνης.
- Πολιτική κινητών συσκευών και τηλεργασίας.
- Πολιτική περιορισμού της χρήσης και εγκατάστασης εφαρμογών.

Όποια μορφή πολιτικών και αν επιλέξουμε αυτές θα πρέπει να είναι σαφώς διατυπωμένες και να έχουν λάβει την έγκριση της ανώτερης διοίκησης του οργανισμού. Επιπλέον, θα πρέπει να αναθεωρούνται σε τακτά χρονικά διαστήματα ή όποτε συντελούνται σημαντικές αλλαγές στα πληροφοριακά συστήματα, έτσι ώστε να παραμένουν επίκαιρες. Επιπλέον της επικαιρότητας οι πολιτικές ασφάλειας θα πρέπει να είναι:

- εύκολα κατανοητές από όλους,
- ανεξάρτητες από την τεχνολογία, έτσι ώστε να μην απαιτείται συχνή αναθεώρησή τους,

- κατάλληλες για τον οργανισμό στον οποίο εφαρμόζονται, εφόσον έχουν λάβει υπόψη τα ιδιαίτερα χαρακτηριστικά του οργανισμού,
- εφαρμόσιμες και
- πλήρεις.

Ένα ζήτημα που απασχολεί τους συντάκτες των πολιτικών ασφάλειας είναι ο βαθμός λεπτομέρειας των πολιτικών. Μια πολιτική που περιλαμβάνει λεπτομερείς οδηγίες και κανόνες που καλύπτουν όλες τις πιθανές καταστάσεις είναι δύσχρηστη και απαιτεί συχνή επικαιροποίηση. Απ' την άλλη μεριά, μια γενική πολιτική, που κινείται σε υψηλό επίπεδο αφαίρεσης, πιθανόν να μην προσφέρει επαρκή καθοδήγηση και να επιτρέπει πολλαπλές ερμηνείες και διαφορετικούς τρόπους εφαρμογής.

2.3.3. Οργάνωση της ασφάλειας πληροφοριών

Η αποτελεσματική εφαρμογή ενός συστήματος διαχείρισης ασφάλειας πληροφοριών προϋποθέτει τη διαμόρφωση της κατάλληλης οργανωσιακής δομής. Βασικό στοιχείο αυτής της δομής αποτελεί ο καθορισμός ρόλων και η ανάθεση αρμοδιοτήτων και υπευθυνοτήτων. Αναλόγως με το είδος του ρόλου (π.χ. υπεύθυνος ασφάλειας πληροφοριών (information security officer), διαχειριστής δικτύου κ.λπ.) ανατίθενται υπευθυνότητες για τη λήψη αποφάσεων, την εκτέλεση εργασιών και διαδικασιών, την προστασία συγκεκριμένων συστημάτων ή κατηγοριών πληροφορίας κ.ά.

Μία βασική αρχή της οργάνωσης της ασφάλειας πληροφοριών είναι ο διαχωρισμός καθηκόντων (segregation of duties). Η εκτέλεση μιας εργασίας θα πρέπει να διαχωρίζεται από την έγκριση ή την εξουσιοδότηση για την έγκρισή της. Συνεπώς, η εκτέλεση και η εξουσιοδότηση θα πρέπει να ανατίθενται σε διαφορετικά πρόσωπα. Με αυτόν τον τρόπο αποφεύγουμε την κατάχρηση δικαιωμάτων, αλλά και την κακή χρήση (misuse) που μπορεί να είναι ακούσια. Στις περιπτώσεις που δεν είναι εφικτός ο διαχωρισμός καθηκόντων ή δεν είναι πρακτική η εφαρμογή του, ενδείκνυται να λαμβάνονται υποκατάστατα μέτρα, όπως παρακολούθηση (monitoring), καταγραφή και έλεγχος (audit) των ενεργειών που εκτελούνται σε ένα σύστημα.

Στα θέματα ασφάλειας οι οργανισμοί έχουν συχνά την τάση να γίνονται εσωστρεφείς. Είναι, όμως, σημαντικό να αναπτύσσουν σχέσεις συνεργασίας και επικοινωνίας με φορείς και αρχές, όπως η Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα, η Δίωξη Ηλεκτρονικού Εγκλήματος, η Αρχή Διασφάλισης Απορρήτου Επικοινωνιών κ.λπ., καθώς και με επαγγελματικές ενώσεις, εκπαιδευτικούς φορείς και οργανώσεις που ασχολούνται με ζητήματα ασφάλειας και ιδιωτικότη-

τας, ώστε να λαμβάνουν ενημέρωση για τις τεχνολογικές εξελίξεις και τις νέες απειλές, να εμπλουτίζουν τις γνώσεις τους κ.λπ.

Επιπλέον, η ασφάλεια θα πρέπει να εντάσσεται σε όλα τα έργα του οργανισμού είτε αυτά αφορούν άμεσα τα πληροφοριακά συστήματα (π.χ. ανάπτυξη νέων συστημάτων, επέκταση συστημάτων, προμήθεια και εγκατάσταση εξοπλισμού) είτε έχουν έμμεση σχέση (π.χ. ανάπτυξη νέων επιχειρησιακών διεργασιών, διαμόρφωση κτηριακών εγκαταστάσεων κ.ά.). Η ασφάλεια αφορά όλες τις φάσεις ενός έργου, από τον σχεδιασμό μέχρι και την υλοποίηση.

Σημαντικό ζήτημα είναι η τηλεργασία και η χρήση φορητών συσκευών. Νέες τάσεις όπως BYOD (Bring Your Own Device – Φέρε τη δική σου συσκευή), εργασία από το σπίτι, αλλά και η εκτεταμένη χρήση φορητών υπολογιστών, τάμπλετ και έξυπνων τηλεφώνων φέρνουν νέες προκλήσεις σε σχέση με την ασφάλεια πληροφοριών. Απαιτούνται, λοιπόν, ειδικές πολιτικές για τις περιπτώσεις αυτές, ώστε να αξιοποιηθούν οι δυνατότητες που προσφέρουν οι νέες τεχνολογίες και πρακτικές, χωρίς να τεθούν σε κίνδυνο τα υπολογιστικά συστήματα και τα πληροφοριακά αγαθά (information assets) του οργανισμού.

2.3.4. Ανθρώπινο δυναμικό

Ο ρόλος του ανθρώπινου δυναμικού στην ασφάλεια πληροφοριών είναι διττός. Απ' τη μια μεριά, οι άνθρωποι αποτελούν τον πλέον αδύναμο κρίκο κάθε συστήματος και πολλές απειλές προκύπτουν από αδυναμία, αμέλεια, ή από εσκεμμένες κακόβουλες ενέργειες χρηστών και διαχειριστών. Απ' την άλλη μεριά, το ανθρώπινο δυναμικό, εφόσον έχει τις κατάλληλες γνώσεις και δεξιότητες, καθώς και ενδιαφέρον και κίνητρο, μπορεί να συνεισφέρει σημαντικά στην προστασία συστημάτων και πληροφοριών.

Η διοίκηση του ανθρώπινου δυναμικού έχει ως αφετηρία τις διαδικασίες επιλογής προσωπικού, όπου είναι σημαντικό να επιλέγονται στελέχη με επαρκείς γνώσεις και δεξιότητες για τον ρόλο που θα αναλάβουν, καθώς και ακέραιο χαρακτήρα. Έπειτα, η σύμβαση εργασίας θα πρέπει να περιλαμβάνει όρους για την ασφάλεια πληροφοριών, την προστασία των προσωπικών δεδομένων και, γενικότερα, για τη συμμόρφωση με τις νομικές και κανονιστικές (regulatory) απαιτήσεις, όπως η προστασία δικαιωμάτων διανοητικής ιδιοκτησίας.

Ο έλεγχος και η επίβλεψη της συμμόρφωσης του προσωπικού με τις πολιτικές ασφάλειας αποτελεί υποχρέωση της διοίκησης του οργανισμού. Σε αυτές τις υποχρεώσεις εντάσσεται και η παροχή κινήτρων, καθώς και η εκπαίδευση, η επιμόρφωση και η ενημέρωση του προσωπικού. Ειδικότερα, η διοίκηση θα πρέπει να α-

ναπτύσσει και να εφαρμόζει ολοκληρωμένα προγράμματα εκπαίδευσης, επιμόρφωσης, ενημέρωσης και ευαισθητοποίησης του προσωπικού σε θέματα ασφάλειας πληροφοριών. Απ' την άλλη μεριά, η μη συμμόρφωση με τις πολιτικές ασφάλειας θα πρέπει να συνεπάγεται επιπτώσεις που θα αποτελούν αντικίνητρο για ενέργειες αντίθετες ή μη συμβατές με τις πολιτικές ασφάλειας.

Εξίσου σημαντικό ζήτημα αποτελεί η λήξη της συνεργασίας με ένα μέλος του προσωπικού ή έναν συνεργάτη του οργανισμού. Σε αυτές τις περιπτώσεις θα πρέπει να λαμβάνεται μέριμνα για την αφαίρεση δικαιωμάτων πρόσβασης σε συστήματα και πληροφορίες και για την τήρηση των υποχρεώσεων που αφορούν στην περίοδο μετά τη λήξη της συνεργασίας, όπως η μη αποκάλυψη εμπιστευτικών πληροφοριών.

2.3.5. Διαχείριση περιουσιακών στοιχείων

Η έννοια των περιουσιακών στοιχείων ή αγαθών (assets) αναφέρεται σε εκείνα τα στοιχεία του πληροφοριακού συστήματος που χρήζουν προστασίας, είτε πρόκειται για υλικό εξοπλισμό και λογισμικό είτε για πληροφορίες. Η διαχείριση των περιουσιακών στοιχείων συνεπάγεται την καταγραφή τους και την ανάθεση της ευθύνης για τη διαχείρισή τους στο κατάλληλο πρόσωπο ή οργανωτική δομή (π.χ. διεύθυνση πληροφορικής). Οι κανόνες αποδεκτής χρήσης των περιουσιακών στοιχείων αποτυπώνονται στις αντίστοιχες πολιτικές.

Η προστασία των πληροφοριών προϋποθέτει την κατάταξή τους σε κατηγορίες, ανάλογα με τον βαθμό ευαισθησίας τους. Ένας οργανισμός μπορεί να υιοθετήσει διάφορες κατηγοριοποιήσεις πληροφοριών, όπως η κατηγοριοποίηση σε *αυστηρώς εμπιστευτικές (strictly confidential), εμπιστευτικές (confidential)* και *μη κατηγοριοποιημένες (unclassified)* ή η κατηγοριοποίηση σε *εμπιστευτικές, περιορισμένης χρήσης, εσωτερικής χρήσης* και *δημόσιες*. Η κατάταξη γίνεται με κριτήρια όπως η αξία της πληροφορίας, η κρισιμότητά της για τη λειτουργία του οργανισμού, οι νομικές απαιτήσεις για την προστασία της κ.ά.

Τα μέσα όπου αποθηκεύονται οι πληροφορίες χρήζουν αντίστοιχης προστασίας κατά τη χρήση, την αποθήκευση και τη μεταφορά τους. Ιδιαίτερη προσοχή απαιτείται κατά την απόσυρσή τους, ώστε να διαγραφούν ασφαλώς τα δεδομένα που περιέχουν.

2.3.6. Έλεγχος πρόσβασης

Ο έλεγχος πρόσβασης αναφέρεται στις διαδικασίες με τις οποίες αποδίδονται δικαιώματα πρόσβασης σε πληροφορίες, εξοπλισμό και εγκαταστάσεις, καθώς και

στα μέτρα που λαμβάνονται για την προστασία από μη εξουσιοδοτημένη πρόσβαση. Ο έλεγχος πρόσβασης περιλαμβάνει τη φυσική πρόσβαση, δηλαδή την πρόσβαση σε εγκαταστάσεις και εξοπλισμό, καθώς και τη λογική πρόσβαση, δηλαδή την πρόσβαση σε πληροφορίες μέσω υπολογιστών και δικτύων.

Ειδικά όσον αφορά τους χρήστες, η διαχείριση των δικαιωμάτων πρόσβασης περιλαμβάνει διαδικασίες για την εγγραφή και τη διαγραφή χρηστών, την απόδοση δικαιωμάτων σε χρήστες, τον έλεγχο της χρήσης των δικαιωμάτων από τους χρήστες, την αναθεώρηση των δικαιωμάτων και την αφαίρεση ή την προσαρμογή τους. Αντιστοίχως, οι χρήστες θα πρέπει να γνωρίζουν ποιες είναι οι υποχρεώσεις τους, ειδικά σε σχέση με τη διαχείριση κωδικών πρόσβασης, καρτών πρόσβασης κ.λπ.

Ο έλεγχος πρόσβασης αποτελεί ένα από τα πιο σύνθετα αντικείμενα της διοίκησης ασφάλειας πληροφοριών, καθώς σχετίζεται με τη συμπεριφορά των χρηστών, το σχεδιασμό του λογισμικού που ελέγχει την πρόσβαση και την αλληλεπίδρασή τους. Η αποτελεσματικότητα του ελέγχου πρόσβασης εξαρτάται από τις σχετικές πολιτικές και διαδικασίες, τα τεχνικά μέτρα και την εκπαίδευση και ευαισθητοποίηση του προσωπικού.

2.3.7. Κρυπτογραφία

Κρυπτογραφικές τεχνικές χρησιμοποιούνται για τη διασφάλιση της εμπιστευτικότητας, της ακεραιότητας και της αυθεντικότητας των πληροφοριών. Ο βαθμός προστασίας που προσφέρει η κρυπτογραφία εξαρτάται από την επιλογή των κατάλληλων αλγορίθμων και εργαλείων και τη διαχείριση των κλειδιών. Κάθε οργανισμός που αξιοποιεί κρυπτογραφικές τεχνικές θα πρέπει να διαθέτει μία πολιτική για την επιλογή και τη χρήση κρυπτογραφικών αλγορίθμων και εργαλείων, όπως επίσης και πολιτικές και διαδικασίες για τη διαχείριση των κρυπτογραφικών κλειδιών.

2.3.8. Φυσική και περιβαλλοντική ασφάλεια

Η φυσική ασφάλεια αναφέρεται στην προστασία των χώρων, των εγκαταστάσεων και του εξοπλισμού των πληροφοριακών συστημάτων. Αρχικά, θα πρέπει να καθοριστούν οι ασφαλείς περιοχές και η περίμετρός τους. Ασφαλείς περιοχές μπορούν να χαρακτηριστούν ολόκληρα κτήρια, τμήματα των κτηριακών εγκαταστάσεων, ή ακόμη και ένα δωμάτιο ή ένας φωριαμός. Οι διαδικασίες και τα μέτρα φυσικής ασφάλειας εμποδίζουν την πρόσβαση από μη εξουσιοδοτημένα άτομα και ελέγχουν την πρόσβαση των εξουσιοδοτημένων ατόμων.

Επιπλέον των μεθόδων ελέγχου της φυσικής πρόσβασης, σημαντικά ζητήματα θεωρούνται η διαχείριση των επισκεπτών (π.χ. η καταγραφή εισόδου/εξόδου, η συνοδεία τους στους χώρους, η ενημέρωσή τους), ο διαχωρισμός των δημόσιων και των ελεγχόμενων χώρων, τα σημεία παράδοσης και φόρτωσης υλικών (π.χ. παράδοση προμηθειών, δεμάτων κ.λπ.) και οι διαδικασίες και κανόνες που οφείλουν να ακολουθούν όσοι εργάζονται σε ασφαλείς χώρους.

Ακόμη, οι εγκαταστάσεις αντιμετωπίζουν περιβαλλοντικές απειλές είτε από φυσικές καταστροφές (πυρκαγιές, πλημμύρες, σεισμοί κ.λπ.) είτε από ανθρωπογενείς καταστροφές (τρομοκρατικές ενέργειες, εκρήξεις, βανδαλισμοί, εξεγέρσεις κ.ά.).

Η προστασία του εξοπλισμού περιλαμβάνει την ασφαλή εγκατάστασή του, την υποστήριξη της λειτουργίας του (κλιματισμός, εξαερισμός, παροχή ηλεκτρικού ρεύματος κ.ά.), την προστασία των καλωδιώσεων, τη συντήρηση του εξοπλισμού, τη μεταφορά του, την απόσυρσή του και την επαναχρησιμοποίησή του.

2.3.9. Λειτουργική ασφάλεια

Με τον όρο λειτουργική ασφάλεια (operations security) αναφερόμαστε στα ζητήματα ασφάλειας που σχετίζονται με τη λειτουργία του πληροφοριακού συστήματος, τις εργασίες που εκτελούνται σε αυτό και τις διαδικασίες που ακολουθούνται για τη διαχείριση της λειτουργίας του. Στους τομείς που απαιτούν ιδιαίτερη προσοχή, από άποψη ασφάλειας, περιλαμβάνονται οι παρακάτω:

- **Διαχείριση αλλαγών.** Οι αλλαγές σε όλα τα επίπεδα, από τον εξοπλισμό μέχρι τις επιχειρησιακές διεργασίες, θα πρέπει να εξετάζονται ως προς τις πιθανές επιπτώσεις που μπορεί να έχουν στην ασφάλεια των πληροφοριακών συστημάτων.
- **Διαχείριση επάρκειας πόρων.** Η απρόσκοπτη λειτουργία των συστημάτων σύμφωνα με τους στόχους διαθεσιμότητας (availability) που έχουν τεθεί εξαρτάται από την επάρκεια πόρων (resources), όπως οι δίσκοι αποθήκευσης, οι μνήμες και η επεξεργαστική ισχύς. Στόχος της διαχείρισης πόρων είναι, αφενός, η βελτιστοποίηση της χρήσης των πόρων ώστε να μην δαπανούνται πόροι άσκοπα και, αφετέρου, η έγκαιρη προμήθεια ή ανανέωση των πόρων. Για παράδειγμα, στο πλαίσιο της διαχείρισης της επάρκειας των πόρων σχεδιάζουμε τις βάσεις δεδομένων με τέτοιο τρόπο, ώστε να μην χρησιμοποιούν περισσότερο χώρο στους δίσκους απ' ότι απαιτείται και παρακολουθούμε τον απομένοντα χώρο στους δίσκους, έτσι ώστε να επεκτείνουμε τη χωρητικότητά τους πριν εξαντληθεί.

- **Διαχωρισμός των περιβαλλόντων ανάπτυξης, δοκιμής και λειτουργίας.** Πολύ συχνά παρατηρούμε όταν υλοποιούνται αλλαγές στο λογισμικό να εισάγονται αδυναμίες στην ασφάλειά του ή να εισάγονται σφάλματα που επηρεάζουν τη λειτουργία του πληροφοριακού συστήματος. Γι' αυτό, μία από τις αρχές που θεωρείται σημαντική για την ασφάλεια πληροφοριών είναι ο διαχωρισμός του περιβάλλοντος όπου γίνεται ανάπτυξη και συντήρηση του λογισμικού, του περιβάλλοντος όπου γίνονται δοκιμές και του περιβάλλοντος στο οποίο λειτουργεί παραγωγικά το λογισμικό.
- **Προστασία από κακόβουλο λογισμικό.** Η προστασία από κακόβουλο λογισμικό επιτυγχάνεται με τη χρήση κατάλληλων εργαλείων, αλλά και με την υιοθέτηση ορθών πρακτικών χρήσης των συστημάτων και ασφαλών διαδικασιών, όπως για παράδειγμα κατά την εγκατάσταση νέου λογισμικού.
- **Εφεδρικά αντίγραφα.** Οι διαδικασίες λήψης και διαχείρισης εφεδρικών αντιγράφων (backups) θα πρέπει να σχεδιάζονται με γνώμονα τον βαθμό ευαισθησίας των δεδομένων ως προς την ανάγκη προστασίας της διαθεσιμότητας, της εμπιστευτικότητας και της ακεραιότητάς τους.
- **Καταγραφή γεγονότων και παρακολούθηση.** Η καταγραφή των γεγονότων που συμβαίνουν σε ένα σύστημα αποτελεί προϋπόθεση για τον εντοπισμό απειλών (π.χ. μίας προσπάθειας κυβερνοεπίθεσης), τη διερεύνηση επεισοδίων ασφάλειας και τη λογοδοσία (accountability). Με τον όρο λογοδοσία εννοούμε τη συσχέτιση ενεργειών και αποφάσεων με τα πρόσωπα που τις έχουν πραγματοποιήσει και την απόδοση ευθυνών για αυτές.
- **Διαχείριση τεχνικών ευπαθειών.** Οι ευπάθειες (vulnerabilities) των συστημάτων θα πρέπει να εντοπίζονται (π.χ. μέσα από διαδικασίες ανίχνευσης ευπαθειών) και να αντιμετωπίζονται.

2.3.10. Ασφάλεια επικοινωνιών

Η ασφάλεια επικοινωνιών αφορά τόσο στην προστασία των δικτύων, όσο και στην προστασία των πληροφοριών κατά τη μεταφορά τους, ανεξαρτήτως του μέσου μεταφοράς (π.χ. δίσκοι, μνήμες USB κ.λπ.). Η προστασία των δικτύων περιλαμβάνει τα τεχνικά μέτρα προστασίας, αλλά και τον αρχιτεκτονικό σχεδιασμό των δικτύων (π.χ. διαχωρισμό του δικτύου σε υποδίκτυα).

Στη μεταφορά δεδομένων χρησιμοποιούμε, κυρίως, κρυπτογραφικές μεθόδους προστασίας δεδομένων. Παράλληλα, στις περιπτώσεις που η μεταφορά γίνεται από τρίτους φορείς ή που διαβιβάζουμε πληροφορίες σε συνεργάτες ή άλλους φορείς, θα πρέπει να εξετάσουμε εάν απαιτείται να υπάρξουν συμφωνίες (σύμβαση ή ιδιω-

τικό συμφωνητικό) με αυτούς τους φορείς που θα προβλέπει τις υποχρεώσεις τους. Για παράδειγμα, εάν για τη μεταφορά των εφεδρικών αντιγράφων δεδομένων σε ασφαλή χώρο χρησιμοποιούμε μία υπηρεσία μεταφοράς, τότε συνιστάται να έχουμε κρυπτογραφήσει τα εφεδρικά αντίγραφα και να έχουμε συμπεριλάβει στη σύμβαση με την εταιρεία που αναλαμβάνει τη μεταφορά όρους για την ειδική διαχείριση των εφεδρικών αντιγράφων.

2.3.11. Προμήθεια, ανάπτυξη και συντήρηση συστημάτων

Η ασφάλεια πληροφοριών θα πρέπει να εντάσσεται στον κύκλο ζωής των συστημάτων από τα αρχικά στάδια. Συνεπώς, η ανάλυση και ο σχεδιασμός των συστημάτων θα πρέπει να λαμβάνει υπόψη τα ζητήματα ασφάλειας, έτσι ώστε η ασφάλεια να αποτελεί εγγενές χαρακτηριστικό των συστημάτων (build-in) και όχι πρόσθετο (add-on). Στη συνέχεια, κατά την υλοποίηση θα πρέπει να καθοριστούν και να ακολουθούνται πρακτικές ασφαλούς ανάπτυξης και με την ολοκλήρωση της ανάπτυξης να ακολουθούν δοκιμές ασφάλειας (security testing).

Εξίσου σημαντική είναι και η συντήρηση των συστημάτων, με έμφαση στη διαχείριση των αλλαγών που γίνονται στα συστήματα και τον επανέλεγχο των συστημάτων μετά τις αλλαγές.

2.3.12. Σχέσεις με προμηθευτές

Οι προμηθευτές ενός οργανισμού αρκετά συχνά έχουν πρόσβαση σε πληροφορίες, σε συστήματα, σε εξοπλισμό και εγκαταστάσεις του οργανισμού και, κατά συνέπεια, η διαχείριση των σχέσεων με τους προμηθευτές είναι ιδιαιτέρως σημαντική για την ασφάλεια πληροφοριών. Συνεπώς, θα πρέπει να λαμβάνονται μέτρα ώστε η πρόσβαση των προμηθευτών σε εγκαταστάσεις, συστήματα, πληροφορίες να μην θέτει σε κίνδυνο την ασφάλεια των πληροφοριακών συστημάτων. Επίσης, σημαντικό ζήτημα αποτελεί η διασφάλιση ότι τα προϊόντα και οι υπηρεσίες που προσφέρουν οι προμηθευτές πληρούν τις προδιαγραφές ασφαλείας του οργανισμού.

2.3.13. Διαχείριση επεισοδίων ασφάλειας πληροφοριών

Η διαχείριση επεισοδίων ασφάλειας πληροφοριών αφορά στην έγκαιρη ανίχνευση απειλών, στην αντιμετώπισή τους και στην εκ των υστέρων ανάλυσή τους. Η διαχείριση των επεισοδίων ασφάλειας πληροφοριών περιλαμβάνει τα παρακάτω:

- **Ανάθεση υπευθυνοτήτων και καθορισμός διαδικασιών.** Ο καθορισμός συγκεκριμένων διαδικασιών για τη διαχείριση των επεισοδίων είναι εξαιρε-

τικά σημαντικός για την άμεση και αποτελεσματική αντιμετώπιση των επεισοδίων ασφάλειας.

- **Αναφορά συμβάντων ασφάλειας και ευπαθειών.** Η αναφορά συμβάντων από το προσωπικό και τους συνεργάτες του οργανισμού θα πρέπει να γίνεται μέσα από τα κατάλληλα κανάλια επικοινωνίας και θα πρέπει να είναι άμεση. Το ίδιο ισχύει για τις ευπάθειες (vulnerabilities) που πιθανόν να εντοπιστούν από μέλη του προσωπικού ή από συνεργάτες.
- **Αξιολόγηση και χαρακτηρισμός συμβάντων.** Κάθε αναφορά συμβάντος θα πρέπει να αξιολογείται και να λαμβάνεται απόφαση εάν θα πρέπει να χαρακτηριστεί ως συμβάν ασφάλειας και να αντιμετωπιστεί ως τέτοιο.
- **Απόκριση.** Η απόκριση στα επεισόδια ασφάλειας (security incident) θα πρέπει να γίνεται σύμφωνα με συγκεκριμένες, τεκμηριωμένες διαδικασίες.
- **Συλλογή δεδομένων.** Και για τη συλλογή δεδομένων που θα βοηθήσουν στην αξιολόγηση του περιστατικού, την αντιμετώπιση και τη διερεύνησή του απαιτούνται τεκμηριωμένες διαδικασίες.
- **Εκ των υστέρων ανάλυση και μάθηση.** Από κάθε σοβαρό περιστατικό ασφάλειας ο οργανισμός μπορεί να αντλήσει γνώση. Για να επιτευχθεί αυτός ο στόχος θα πρέπει να υπάρχουν μηχανισμοί που θα επιτρέπουν τη συλλογή δεδομένων, την ανάλυσή τους και την αξιοποίηση της γνώσης που προκύπτει από την ανάλυση.

2.3.14. Ασφάλεια πληροφοριών και επιχειρησιακή συνέχεια

Ο όρος επιχειρησιακή συνέχεια αναφέρεται στην επιχειρησιακή ικανότητα του οργανισμού να αντιμετωπίζει περιστατικά και διαταράξεις της λειτουργίας του, έτσι ώστε να έχει τη δυνατότητα να συνεχίζει τη λειτουργία του σε ένα προκαθορισμένο, αποδεκτό επίπεδο λειτουργικότητας. Το βασικό εργαλείο για την επιχειρησιακή συνέχεια είναι το *Σχέδιο Επιχειρησιακής Συνέχειας (Business Continuity Plan)*.

Η λειτουργία των πληροφοριακών συστημάτων αποτελεί ένα σημαντικό, αν και όχι το μοναδικό, στοιχείο της επιχειρησιακής συνέχειας. Γι' αυτό και στο πλαίσιο της διοίκησης ασφάλειας πληροφοριών δίνεται ιδιαίτερη βαρύτητα στην κατάρτιση σχεδίων επιχειρησιακής συνέχειας για τα πληροφοριακά συστήματα του οργανισμού. Παρά τα μέτρα ασφάλειας πληροφοριών που πιθανόν να εφαρμόζει ένας οργανισμός, θα πρέπει να θεωρείται πιθανό ένα περιστατικό ασφάλειας να έχει σοβαρές επιπτώσεις στη λειτουργία των πληροφοριακών συστημάτων. Στα επεισόδια ασφάλειας θα πρέπει να συμπεριλαμβάνονται και πιθανά καταστροφικά γεγο-

νότα, όπως φυσικές καταστροφές, ατυχήματα, τρομοκρατικές ενέργειες, κοινωνικές αναταράξεις, τεχνικές αστοχίες, κ.ά.

Η *διαχείριση της επιχειρησιακής συνέχειας (business continuity management)* περιλαμβάνει:

- τον καθορισμό των στόχων επιχειρησιακής συνέχειας που αφορά στόχους, όπως ο *μέγιστος ανεκτός χρόνος εκτός λειτουργίας* και ο *επιδιωκόμενος χρόνος ανάκαμψης*,
- την ανάλυση των κινδύνων και των πιθανών επιπτώσεών τους στον οργανισμό,
- την ανάπτυξη του σχεδίου επιχειρησιακής συνέχειας,
- τις δοκιμές και την εκπαίδευση στην εφαρμογή του σχεδίου επιχειρησιακής συνέχειας και
- την αξιολόγηση και επικαιροποίηση του σχεδίου.

Ένα υποσύνολο της επιχειρησιακής συνέχειας είναι η ανάκαμψη από καταστροφή (disaster recovery) και, αντιστοίχως, το σχέδιο ανάκαμψης από καταστροφή (Disaster Recovery Plan – DRP). Αφορά, συνήθως, μερικές ή ολοκληρωτικές καταστροφές της υποδομής των πληροφοριακών συστημάτων. Στόχος του είναι να διασφαλίσει την αποκατάσταση και συνέχιση λειτουργίας των πληροφοριακών συστημάτων, συχνά μέσω της μεταφοράς της λειτουργίας τους σε εφεδρικές εγκαταστάσεις.

Αξίζει να σημειώσουμε ότι τόσο το σχέδιο επιχειρησιακής συνέχειας, όσο και το σχέδιο ανάκαμψης από καταστροφή απαιτούν τη δέσμευση πλεοναζόντων πόρων, όπως, για παράδειγμα, εφεδρικούς εξυπηρετητές (servers), εφεδρικές δικτυακές συνδέσεις, ή εφεδρικές εγκαταστάσεις (backup site). Επειδή, όμως, το κόστος των πλεοναζόντων πόρων συνήθως είναι σημαντικό, θα πρέπει η αναγκαιότητά τους να τεκμηριώνεται επαρκώς και να απαντά στους στόχους συνέχειας του οργανισμού.

2.3.15. Συμμόρφωση

Τα σύγχρονα πληροφοριακά συστήματα λειτουργούν σε ένα σύνθετο νομικό και κανονιστικό πλαίσιο, το οποίο θέτει περιορισμούς στη λειτουργία των συστημάτων, υποχρεώσεις για τους οργανισμούς που τα διαχειρίζονται και απαιτήσεις για την ασφαλή λειτουργία τους. Οι κυριότεροι τομείς συμμόρφωσης περιλαμβάνουν την προστασία δεδομένων προσωπικού χαρακτήρα και την προστασία πνευματικών δικαιωμάτων. Ανάλογα με τον κλάδο στον οποίο δραστηριοποιείται ο ορ-

γανισμός απαιτείται η συμμόρφωση με ειδικότερες νομοθεσίες και ρυθμιστικά πλαίσια, όπως αυτά που αφορούν το ηλεκτρονικό εμπόριο, τις υπηρεσίες υγείας, τις τηλεπικοινωνίες, τις χρηματοπιστωτικές υπηρεσίες κ.ά.

Επιπλέον του νομικού και κανονιστικού πλαισίου, ο οργανισμός θα πρέπει να λάβει υπόψη του πιθανές δεσμεύσεις που προκύπτουν από συμβάσεις και συμφωνίες που έχει συνάψει με πελάτες και προμηθευτές και από τη συμμόρφωση με σχετικά πρότυπα, όπως τα πρότυπα ποιότητας (π.χ. ISO 9001) και ασφάλειας (π.χ. ISO/IEC 27001).

Ο οργανισμός και το προσωπικό του θα πρέπει να συμμορφώνεται με τις πολιτικές που έχει υιοθετήσει. Για τον σκοπό αυτό σχεδιάζονται και εκτελούνται έλεγχοι συμμόρφωσης με τις πολιτικές ασφάλειας πληροφοριών και έλεγχοι εφαρμογής των μέτρων ασφάλειας. Επιπλέον της ενίσχυσης της συμμόρφωσης, οι έλεγχοι αξιοποιούνται και για τη βελτίωση του συστήματος διαχείρισης ασφάλειας πληροφοριών. Όπως κάθε σύστημα, έτσι και το σύστημα διαχείρισης ασφάλειας πληροφοριών θα πρέπει να παρακολουθείται στη λειτουργία του, να αξιολογείται και να επικαιροποιείται με στόχο τη διαρκή βελτίωσή του.

2.3.16. Άλλες διαστάσεις της διοίκησης ασφάλειας πληροφοριών

Η προσέγγιση που παρουσιάσαμε παραπάνω βασίζεται στην εφαρμογή ενός συστήματος διαχείρισης ασφάλειας πληροφοριών. Αυτή, όμως, δεν είναι η μοναδική επιλογή που έχει ένας οργανισμός. Ένας οργανισμός μπορεί να ακολουθήσει εναλλακτικούς τρόπους οργάνωσης της διοίκησης της ασφάλειας πληροφοριών. Μία συνήθης προσέγγιση είναι αυτή που βασίζεται στην ανάπτυξη ενός Σχεδίου Ασφάλειας Πληροφοριών (information security plan).

Ένα σχέδιο ασφάλειας πληροφοριών περιλαμβάνει τις πολιτικές ασφάλειας, τα μέτρα προστασίας και τη στρατηγική για την εφαρμογή του. Η στρατηγική εφαρμογής αφορά στην εξεύρεση ή στη δέσμευση πόρων για την εφαρμογή του και στον καθορισμό προτεραιοτήτων, ειδικά στην περίπτωση της σταδιακής εφαρμογής του σχεδίου. Καθώς τα μέτρα προστασίας θα πρέπει να είναι ανάλογα των κινδύνων που αντιμετωπίζουν τα πληροφοριακά συστήματα, η ανάπτυξη του σχεδίου ασφάλειας συνιστάται να βασίζεται στην αποτίμηση επικινδυνότητας (risk assessment) που θα παρουσιάσουμε εκτενέστερα σε επόμενη ενότητα. Το σχέδιο ασφάλειας ακολουθεί και αυτό έναν κύκλο ζωής, που περιλαμβάνει τον σχεδιασμό, την ανάπτυξη, την εφαρμογή, την αξιολόγηση και την αναθεώρησή του.

Η διοίκηση της ασφάλειας απαιτεί καλή γνώση του τομέα της ασφάλειας πληροφοριών, απαιτεί όμως και γνώσεις και δεξιότητες διοίκησης. Η ηγεσία, η επικοι-

νωνία, η διαχείριση σχέσεων, η διαχείριση της αλλαγής και η αντιμετώπιση της αντίστασης στην αλλαγή είναι εξαιρετικά σημαντικές και διαδραματίζουν κεντρικό ρόλο στην επιτυχία του εγχειρήματος της διοίκησης της ασφάλειας πληροφοριών.

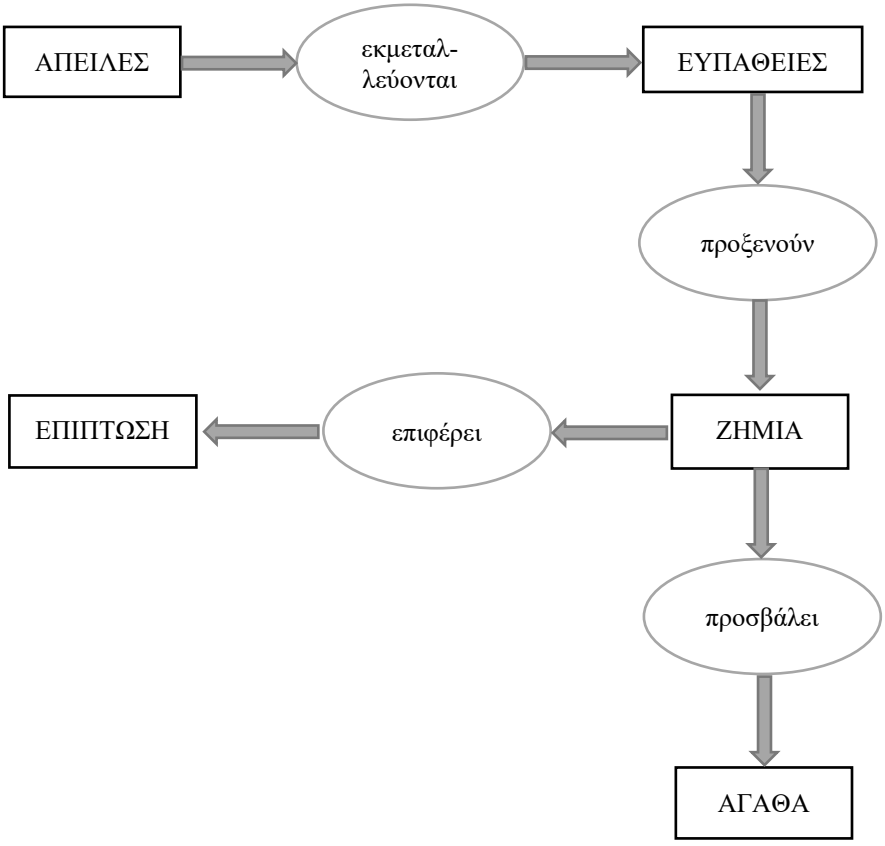
2.4. Διαχείριση επικινδυνότητας

2.4.1. Επικινδυνότητα και συναφείς έννοιες

Η διαχείριση της επικινδυνότητας (risk management) έχει ως στόχο τον περιορισμό και διατήρηση της επικινδυνότητας εντός του ορίου που θεωρείται αποδεκτό από τον οργανισμό. Περιλαμβάνει την αποτίμηση της επικινδυνότητας (risk assessment) και την αντιμετώπιση της επικινδυνότητας (risk treatment). Η αποτίμηση επικινδυνότητας περιλαμβάνει τρεις φάσεις. Η πρώτη φάση αφορά στην αναγνώριση της επικινδυνότητας (risk identification) όπου εντοπίζουμε και αναλύουμε τους παράγοντες που συμβάλλουν στην επικινδυνότητα του πληροφοριακού συστήματος. Η δεύτερη φάση αφορά στην ανάλυση επικινδυνότητας (risk analysis), όπου εκτιμάται το επίπεδο της επικινδυνότητας. Το επίπεδο της επικινδυνότητας συνήθως εκτιμάται σε ποσοτικούς όρους. Η τρίτη φάση αφορά στην εκτίμηση της επικινδυνότητας (risk evaluation), όπου συγκρίνουμε το επίπεδο της επικινδυνότητας με τα κριτήρια αποδοχής της επικινδυνότητας που έχει θέσει ο οργανισμός και καθορίζουμε τις προτεραιότητες αντιμετώπισης των κινδύνων.

Η αντιμετώπιση της επικινδυνότητας (risk treatment) αφορά στην επιλογή μέτρων προστασίας, τη σύνταξη πολιτικών ασφάλειας πληροφοριών και, γενικότερα, σε κάθε δράση που στοχεύει στη μείωση και διατήρηση της επικινδυνότητας εντός των ορίων που θέτει ο οργανισμός.

Η διαχείριση επικινδυνότητας απαντά στο ερώτημα της επιλογής μέτρων προστασίας που θα προσφέρουν προστασία ανάλογη των κινδύνων που απειλούν το πληροφοριακό σύστημα. Η αποτίμηση επικινδυνότητας αντιστρέφει το μοντέλο της αξιολόγησης επενδύσεων, όπου μία επένδυση θεωρείται συμφέρουσα αν το κόστος της (σε σταθερές τιμές) υπολείπεται του γινομένου του αναμενόμενου κέρδους επί την πιθανότητα επίτευξης αυτού του κέρδους. Εδώ, η επικινδυνότητα (Ε) ορίζεται ως το γινόμενο της πιθανότητας (Π) πραγματοποίησης ενός επεισοδίου ασφάλειας επί το κόστος (Κ) που θα επιφέρει το περιστατικό ασφάλειας, ήτοι: $Ε = Π \times Κ$ [4]. Αυτό, βέβαια, είναι το πιο απλό μοντέλο αποτίμησης επικινδυνότητας. Στην εξειδικευμένη βιβλιογραφία μπορεί κανείς να αναζητήσει πιο σύνθετα μοντέλα.



Σχήμα 2.1: *Οι έννοιες που συνθέτουν την επικινδυνότητα.*

Αναλυτικότερα, η πιθανότητα πραγματοποίησης ενός επεισοδίου εκτιμάται ως συνάρτηση της πιθανότητας εμφάνισης μίας απειλής (threat) και της σχετικής ευπάθειας – αδυναμίας (vulnerability) του συστήματος που δύναται να επιτρέψει στην απειλή να πραγματοποιηθεί. Αντίστοιχα, το κόστος από την πραγματοποίηση ενός επεισοδίου εκτιμάται με βάση την επίπτωση (impact) στον οργανισμό, που θα έχει η ζημιά που θα προκληθεί στα περιουσιακά στοιχεία – αγαθά (assets) του πληροφοριακού συστήματος (Σχήμα 2.1). Έτσι, τελικά, η επικινδυνότητα υπολογίζεται ως συνάρτηση τριών παραγόντων: (α) της αξίας των αγαθών, που προκύπτει από την αντίστοιχη επίπτωση της ζημιάς που θα υποστούν, (β) της πιθανότητας εμφάνισης των απειλών και (γ) του επιπέδου της ευπάθειας.

Το μοντέλο αυτό δίνει τη δυνατότητα αποτίμησης της επικινδυνότητας σε χρηματικούς όρους, έτσι ώστε να συγκριθεί με το κόστος των σχετικών αντιμέτρων. Συχνότερα, όμως, η αποτίμηση γίνεται σε απλή αριθμητική κλίμακα, καθώς οι επι-

πτώσεις από την απώλεια ορισμένων αγαθών (π.χ. απώλεια ανθρώπινης ζωής) είναι δύσκολο, αν όχι ανέφικτο, να αποτιμηθούν οικονομικά. Η αποτίμηση της επικινδυνότητας αποτελεί προϋπόθεση για τη διαχείρισή της, που είναι και ο αντικειμενικός στόχος της όλης προσπάθειας.

2.4.2. Η μεθοδολογία της διαχείρισης επικινδυνότητας πληροφοριακών συστημάτων

Η μεθοδολογία της διαχείρισης επικινδυνότητας υιοθετεί τις βασικές αρχές και το επιστημολογικό υπόβαθρο της στατιστικής επιστήμης και των πιθανοτήτων και κυρίως του κλάδου που αναφέρεται συνήθως ως στατιστική Bayes (Bayesian Statistics), από το όνομα του μαθηματικού Thomas Bayes (1702-1761) που διατύπωσε το ομώνυμο θεώρημα. Η περιγραφή του θεωρήματος βρίσκεται εκτός των στόχων του παρόντος βιβλίου.

Η στατιστική κατά Bayes θεμελιώνει την άποψη ότι η πιθανότητα να συμβεί ένα γεγονός στο μέλλον αποτελεί μετρήσιμο μέγεθος. Η πιθανότητα αυτή μπορεί να προσδιοριστεί αν αναλυθούν οι παράγοντες από τους οποίους εξαρτάται. Μπορούμε, για παράδειγμα, να υπολογίσουμε την πιθανότητα να κλαπούν τα απόρρητα δεδομένα που διατηρούμε στον υπολογιστή μας, ως συνάρτηση της πιθανότητας ένας επίδοξος εισβολέας να προσπαθήσει να "παρεισφρήσει" στον υπολογιστή μας και της πιθανότητας να το επιτύχει. Στη γλώσσα της αποτίμησης επικινδυνότητας, η πρώτη πιθανότητα μάς δίνει το μέγεθος της απειλής και η δεύτερη το μέγεθος της ευπάθειας του συστήματός μας.

Έτσι, η αποτίμηση επικινδυνότητας εκτιμά την πιθανότητα να συμβεί ένα περιστατικό ασφάλειας, αναλύοντας τους παράγοντες που συνδέονται με την πραγματοποίησή του, δηλαδή την απειλή και την ευπάθεια. Έπειτα, συνδυάζει την πιθανότητα αυτή με την επίπτωση που προκύπτει από την πραγματοποίηση του επεισοδίου, για να υπολογίσει την επικινδυνότητα του συστήματος.

Ο υπολογισμός της επικινδυνότητας μας δίνει τη δυνατότητα να εκτιμήσουμε την υφιστάμενη κατάσταση. Το ζητούμενο, όμως, είναι ο περιορισμός της επικινδυνότητας εντός αποδεκτών ορίων. Αυτό είναι το αντικείμενο της αντιμετώπισης της επικινδυνότητας (risk treatment). Προκύπτουν, όμως, τα εξής ερωτήματα: Σε ποιο βαθμό θα πρέπει να περιορίσουμε την επικινδυνότητα; Μπορούμε να τη μηδενίσουμε;

Μηδενική επικινδυνότητα έχουμε είτε όταν η αξία των αγαθών – περιουσιακών στοιχείων του συστήματος είναι ίση με το μηδέν, είτε όταν η πιθανότητα πραγματοποίησης ενός επεισοδίου ασφάλειας είναι ίση με το μηδέν. Αν κατά την αποτί-

μηση επικινδυνότητας εντοπίσουμε ότι κάποια στοιχεία του συστήματός μας έχουν ελάχιστη ή μηδενική αξία, τότε δε θα τα συμπεριλάβουμε στην αντιμετώπιση της επικινδυνότητας, καθώς η λήψη μέτρων προστασίας αυτών των στοιχείων στερείται νοήματος.

Όσον αφορά το δεύτερο σκέλος, δηλαδή την πιθανότητα να συμβεί ένα περιστατικό ασφάλειας, ο μηδενισμός της πιθανότητας αυτής – δηλ. η επίτευξη απόλυτης ασφάλειας – δεν είναι εφικτός για πολλούς λόγους, μεταξύ των οποίων οι εξής:

- Οι απειλές που αντιμετωπίζει ένα ανοικτό σύστημα που λειτουργεί σε ένα δυναμικό περιβάλλον, όπως είναι, κατά κανόνα, τα σύγχρονα πληροφοριακά συστήματα, είναι δυναμικές – δηλαδή χαρακτηρίζονται από συνεχή μεταβλητότητα – και οι αιτίες που τις προκαλούν είναι εξαιρετικά σύνθετες.
- Η ανθρώπινη συμπεριφορά, η οποία είναι δύσκολο να προβλεφθεί και να μοντελοποιηθεί, παίζει ιδιαίτερα σημαντικό ρόλο στην ασφάλεια των πληροφοριακών συστημάτων.
- Οι πόροι που διαθέτει ένας οργανισμός είναι πεπερασμένοι.

Παράλληλα, οι απειλές που αντιμετωπίζει ένα πληροφοριακό σύστημα χαρακτηρίζονται από ποικιλία, συμπλοκότητα και συνεχή μεταβλητότητα. Για παράδειγμα, υπάρχουν φυσικές απειλές (πχ. πυρκαγιά, σεισμός κ.λπ.), απειλές μη-εξουσιοδοτημένης πρόσβασης, τεχνικές αστοχίες, λάθη διαχείρισης κ.λπ. Καθώς το τεχνολογικό και κοινωνικό περιβάλλον εξελίσσεται διαρκώς και με ταχύ ρυθμό, έτσι και οι απειλές μεταβάλλονται και εξελίσσονται.

Το κόστος των μέτρων προστασίας δεν μπορεί να αγνοηθεί. Το κόστος αυτό δεν αφορά μόνο στην προμήθεια και εγκατάσταση μηχανισμών και εργαλείων προστασίας. Συμπεριλαμβάνει το κόστος από την απασχόληση πολύτιμων ανθρώπινων πόρων, το κόστος για εκπαίδευση και ενημέρωση των χρηστών, καθώς και για τη διεκπεραίωση εργασιών και διαδικασιών που αφορούν στην ασφάλεια.

Κατά συνέπεια, εφόσον ο μηδενισμός της επικινδυνότητας δεν είναι εφικτός, το ενδιαφέρον εστιάζεται στον περιορισμό της επικινδυνότητας σε αποδεκτά επίπεδα. Η απόφαση αυτή δεν είναι ποτέ μονοσήμαντη, αλλά εξαρτάται αφενός από το κόστος και αφετέρου από την αποτελεσματικότητα των μέτρων προστασίας που απαιτούνται για τη μείωση της επικινδυνότητας.

Όταν η λήψη μέτρων για τη μείωση της επικινδυνότητας δεν κρίνεται συμφέρουσα, τότε υπάρχουν άλλες δύο εναλλακτικές επιλογές: η μεταβίβαση της επικινδυνότητας και η αποδοχή της επικινδυνότητας. Στην πρώτη περίπτωση η επικινδυνότητα μεταβιβάζεται σε τρίτους, συνήθως με την καταβολή του αντίστοιχου τιμή-

ματος. Χαρακτηριστική περίπτωση μεταβίβασης επικινδυνότητας αποτελεί η ασφάλιση (insurance), όπου η επικινδυνότητα μεταβιβάζεται στην ασφαλιστική εταιρεία, στην οποία καταβάλλεται το αντίστοιχο αντίτιμο ως δίκαιο ασφάλιστρο.

Η δεύτερη επιλογή αφορά στην αποδοχή της επικινδυνότητας. Σε αυτήν την περίπτωση ο οργανισμός αποδέχεται συνειδητά τις επιπτώσεις που ενδέχεται να υποστεί εάν συμβεί μία παραβίαση της ασφάλειας του πληροφοριακού συστήματος. Επιλέγει, όμως, να μην υλοποιήσει τα μέτρα προστασίας που απαιτούνται για να μειωθεί περαιτέρω η σχετική επικινδυνότητα. Υπάρχουν αρκετές περιπτώσεις που συνειδητά επιλέγεται η αποδοχή της επικινδυνότητας, όπως, για παράδειγμα, περιπτώσεις όπου τα μέτρα προστασίας αντιβαίνουν στην πολιτική και την κουλτούρα του οργανισμού.

Αναλυτικές προδιαγραφές για τη διαχείριση της επικινδυνότητας περιέχονται στο πρότυπο ISO/IEC 27005, "Information Technology – Security Techniques – Information security risk management" [5]. Η εφαρμογή, όμως, της διαχείρισης επικινδυνότητας απαιτεί περαιτέρω εξειδίκευση, δηλαδή απαιτεί τη διαμόρφωση μιας συγκεκριμένης μεθόδου εφαρμογής, με καλώς προσδιορισμένα βήματα και ενέργειες. Μπορεί κανείς να υιοθετήσει μία από τις πολλές δεκάδες μεθόδους (π.χ. OCTAVE, MEHARI κ.ά.) πολλές εκ των οποίων υποστηρίζονται από εργαλεία λογισμικού ή να διαμορφώσει τη δική του μέθοδο.

2.4.3. Πλεονεκτήματα και μειονεκτήματα

Στα πλεονεκτήματα της διαχείρισης επικινδυνότητας περιλαμβάνονται τα παρακάτω:

- Δίνει τη δυνατότητα αιτιολόγησης του κόστους των μέτρων προστασίας.
- Αποτελεί ένα εργαλείο επικοινωνίας ανάμεσα στους ειδικούς των τεχνολογιών πληροφορικής και επικοινωνιών και τη διοίκηση των οργανισμών, καθώς επιτρέπει την έκφραση του προβλήματος της ασφάλειας σε γλώσσα κατανοητή από τη διοίκηση, αντιμετωπίζοντας την ασφάλεια ως 'επένδυση' που αποτιμάται με όρους κόστους/οφέλους.
- Είναι αρκετά ευέλικτη, ώστε να μπορεί να ενταχθεί σε διάφορα επιστημολογικά πλαίσια και να εφαρμόζεται είτε αυτούσια, είτε σε συνδυασμό με άλλες μεθοδολογίες.
- Ανταποκρίνεται στις απαιτήσεις της ευρωπαϊκής νομοθεσίας, που απαιτούν από τα πληροφοριακά συστήματα που επεξεργάζονται προσωπικά δεδομένα, τη λήψη μέτρων προστασίας, έτσι ώστε να εξασφαλίζεται επίπεδο α-

σφάλειας ανάλογο προς τους κινδύνους που συνεπάγεται η επεξεργασία και η φύση των δεδομένων.

Επιπλέον, όμως, η μεθοδολογία αυτή παρουσιάζει σημαντικά μειονεκτήματα, όπως τα παρακάτω:

- Στηρίζεται σε ένα απλοϊκό μοντέλο του πληροφοριακού συστήματος και αγνοεί τα ιδιαίτερα χαρακτηριστικά του οργανισμού στον οποίο ανήκει το σύστημα.
- Εμπεριέχει σημαντική υποκειμενικότητα στις εκτιμήσεις τόσο της αξίας των αγαθών, όσο και στην αποτίμηση απειλών και ευπάθειας. Η υποκειμενικότητα αυτή συχνά συγκαλύπτεται πίσω από την αυστηρότητα των μαθηματικών-πιθανοτικών μοντέλων, στα οποία στηρίζεται, τη συστηματικότητα των περισσότερων μεθόδων διαχείρισης επικινδυνότητας και την 'αντικειμενικότητα' των εργαλείων που υποστηρίζουν τις σχετικές μεθόδους.
- Βασίζεται σε απλές στατιστικές μεθόδους για τον υπολογισμό της πιθανότητας εμφάνισης μιας απειλής. Η εγκυρότητα της εφαρμογής των μεθόδων αυτών στον τομέα της ασφάλειας πληροφοριακών συστημάτων έχει αμφισβητηθεί από πολλούς ερευνητές.

2.5. Σύνοψη

Κάθε οργανισμός που διαχειρίζεται πληροφορίες που έχουν αξία γι' αυτόν έχει την ανάγκη να προστατεύσει αυτές τις πληροφορίες με τεχνικά και οργανωσιακά μέτρα ασφάλειας. Η επιτυχία, όμως, της προστασίας των πληροφοριών και των συστημάτων του οργανισμού εξαρτάται από τη διακυβέρνηση και τη διοίκηση της ασφάλειας πληροφοριών. Στο πλαίσιο της διακυβέρνησης ασφάλειας πληροφοριών αναπτύσσεται ο στρατηγικός σχεδιασμός για την ασφάλεια πληροφοριών, διαμορφώνεται η κατάλληλη οργανωτική δομή, καθορίζονται ρόλοι και απονέμονται αρμοδιότητες και υπευθυνότητες, διασφαλίζεται η ενσωμάτωση του συστήματος διοίκησης ασφάλειας πληροφοριών στον οργανωσιακό σχεδιασμό, επιλέγονται και τεκμηριώνονται οι στόχοι της ασφάλειας πληροφοριών και εποπτεύεται η επίτευξή τους.

Η διοίκηση της ασφάλειας πληροφοριών αφορά στις πολιτικές, τις διαδικασίες και τις οδηγίες για την προστασία των πληροφοριών και των συστημάτων, εντός του πλαισίου που διαμορφώνει η διακυβέρνηση ασφάλειας πληροφοριών. Τα διεθνή πρότυπα συνιστούν σχεδιασμό και εφαρμογή ενός συστήματος διαχείρισης ασφάλειας πληροφοριών που να καλύπτει όλους τους βασικούς τομείς της ασφά-

λειας πληροφοριών. Τόσο η διακυβέρνηση όσο και η διοίκηση της ασφάλειας πληροφοριών βασίζονται στη διαχείριση της επικινδυνότητας που διασφαλίζει ότι οι πολιτικές και τα μέτρα προστασίας που λαμβάνονται είναι ανάλογα των κινδύνων που αντιμετωπίζουν τα πληροφοριακά συστήματα του οργανισμού.

Σε κάθε περίπτωση, πέρα από την εφαρμογή των κατάλληλων μεθοδολογιών και προτύπων, η διακυβέρνηση και η διοίκηση της ασφάλειας πληροφοριών απαιτούν γνώσεις και δεξιότητες διοίκησης. Η ηγεσία, η επικοινωνία, η διαχείριση σχέσεων, η διαχείριση της αλλαγής και η αντιμετώπιση της αντίστασης στην αλλαγή είναι εξαιρετικά σημαντικές για την επιτυχία κάθε προσπάθειας προστασίας των πληροφοριών και των συστημάτων ενός οργανισμού.

Βιβλιογραφικές Αναφορές

[1] P. Bowen, J. Hash, M. Wilson, *Information Security Handbook: A Guide for Managers*, NIST SP 800-100, NIST, 2006.

[2] *Information technology – Security techniques – Information security management systems – Requirements*, ISO/IEC 27001:2013, ISO, Geneva, Switzerland, Oct. 2013.

[3] *Information technology – Security techniques – Code of practice for information security controls*, ISO/IEC 27002:2013, ISO, Geneva, Switzerland, Oct. 2013.

[4] R. Baskerville, "Information Systems Security Design Methods: Implications for Information Systems Development", *ACM Computing Surveys*, vol. 25, no. 4, pp. 375-414, 1993.

[5] *Information technology – Security techniques – Information security risk management*, ISO/IEC 27005:2018, ISO, Geneva, Switzerland, Jul. 2018.