Κεφάλαιο 11. Διαχείριση Ασφάλειας

Σύνοψη
Η Ασφάλεια Πληροφοριών (Information Security) αποτελεί πλέον αντικείμενο μελέτης επιστημόνων και επαγγελματιών διαφόρων ειδικοτήτων. Επομένως, είναι απαραίτητο να οριστεί ένα πλαίσιο μέσα στο οποίο θα πραγματοποιούνται οι κατάλληλες διεργασίες ώστε να επιτυγχάνονται οι στόχοι της ασφάλειας πληροφοριών, σύμφωνα με τα όσα κάθε οργανισμός ορίζει. Συνήθως, οι διεργασίες αυτές οδηγούν στην ανάπτυξη μιας στρατηγικής ασφάλειας, η οποία περιλαμβάνει επιμέρους πολιτικές και επιπλέον εναρμονίζει τον οργανισμό με διεθνείς πρακτικές και πρότυπα. Επιπλέον, είναι απαραίτητο για την εύρυθμη λειτουργία του κάθε οργανισμού, να ορίζονται και να αξιοποιούνται μετρικές με τις οποίες μπορεί να υποστηρίζεται η ποσοτικοποίηση των μεγεθών, προκειμένου να παρέχεται με αυτόματο τρόπο η απάντηση στο βασικό ερώτημα που αφορά την επιτυχία ή την αστοχία των διεργασιών αυτών. Η διαχείριση της ασφάλειας ενσωματώνει στο αντικείμενο μελέτης της ασφάλειας πληροφοριών όλες εκείνες τις διεργασίες που πρέπει να πραγματοποιούνται ώστε να γίνεται εφικτή η απαραίτητη ποσοτικοποίηση των μεγεθών, που θα επιτρέπει κατόπιν στις διοικήσεις των οργανισμών να παίρνουν ορθές αποφάσεις και στους ειδικούς της ασφάλειας να αποτιμούν αξιόπιστα την επιτυχία ή την αποτυχία του συστήματος διαχείρισης ασφάλειας πληροφοριών που εφαρμόζουν στα πλαίσια του κάθε οργανισμού.

Προαπαιτούμενη γνώση
Για την κατανόηση του παρόντος κεφαλαίου απαιτείται γνώση των βασικών εννοιών και ζητημάτων ασφάλειας (Κεφ. 1).

11.1 Εισαγωγή

Το πρόβλημα της διαχείρισης της ασφάλειας πληροφοριών (information security management) αποτελεί ένα ιδιαίτερα σημαντικό ζήτημα για τα σύγχρονα πληροφοριακά συστήματα, καθώς επηρεάζει σε παγκόσμια κλίμακα το ηλεκτρονικό επιχειρείν και την ανάπτυξη εθνικών και διεθνών κρίσιμων υποδομών. Η αξιοποίηση όλο και πιο προηγμένων τεχνολογιών, όπως για παράδειγμα οι σύγχρονες βάσεις δεδομένων, τα δίκτυα και το Διαδίκτυο, προσφέρει σημαντικές δυνατότητες, αλλά αυξάνει ανάλογα και τα προβλήματα που αφορούν την προστασία της εμπιστευτικότητας, της ακεραιότητας και της διαθεσιμότητας των πληροφοριών.

Η ασφάλεια αποτελεί αναγκαία συνθήκη και είναι απαραίτητη, σε συνδυασμό με τις άλλες βασικές παραμέτρους λειτουργίας (ποιότητα, απόδοση, κ.ά.), για την εξασφάλιση της εύρυθμης λειτουργίας ενός οργανισμού. Αυτό είναι ιδιαίτερα σημαντικό σήμερα, όπου πολύ συχνά το σύνολο των παρεχόμενων υπηρεσιών ενός οργανισμού στηρίζεται στην πληροφορική (π.χ. πάνω από το 80% των υπηρεσιών μιας τράπεζας). Η ικανοποίηση των απαιτήσεων για την ασφάλεια των πληροφοριών (information security) είναι, συνεπώς, μια από τις βασικές προϋποθέσεις για την αποδοτική εισαγωγή και αξιοποίηση των τεχνολογιών πληροφορίας και επικοινωνιών (ΤΠΕ).

Ως Πληροφοριακό Σύστημα εννοούμε το οργανωμένο σύνολο από ανθρώπους, λογισμικό, υλικό, διαδικασίες, εγκαταστάσεις και δεδομένα. Τα στοιχεία αυτά βρίσκονται σε μια συνεχή αλληλεπίδραση μεταξύ τους, αλλά και με το περιβάλλον, με σκοπό την παραγωγή και διαχείριση της πληροφορίας. Η πληροφορία, στο πλαίσιο ενός οργανισμού, θεωρείται αγαθό με την έννοια ότι έχει αξία. Είναι πιθανό επίσης η πληροφορία να έχει και κόστος απόκτησης.

Οι σύγχρονοι οργανισμοί εξαρτώνται από πληροφοριακά αγαθά σε ότι αφορά την αποτελεσματικότητα και τη κερδοφορία των λειτουργιών τους και για αυτό χρειάζεται να προστατεύουν αυτά τα αγαθά. Η διασφάλιση (assurance) της εμπιστευτικότητας, της ακεραιότητας και της διαθεσιμότητας των πληροφοριών είναι σημαντική, ανεξάρτητα του κατά πόσον οι πληροφορίες αποτελούν αντικείμενο επεξεργασίας και διαχείρισης ή ανταλλάσσονται μεταξύ των συνεργαζόμενων οργανισμών. Στις μέρες μας, ο οικονομικός αλλά και εθνικός πλούτος εκφράζεται ολοένα και περισσότερο σε συνάρτηση με την πληροφορία. Η πληροφορία αποτελεί ένα σημαντικό δείκτη ανάπτυξης και επομένως είναι ανάγκη να προστατεύεται. Ακόμη, η σημασία

της πληροφορίας ξεφεύγει από τα στενά οικονομικά όρια και αγγίζει το ευρύτερο κοινωνικό σύνολο. Δεν είναι λίγα τα παραδείγματα όπου η πληροφορία αποτέλεσε ένα ισχυρό όργανο κοινωνικού ελέγχου. Επομένως, υπάρχουν και κοινωνικές προεκτάσεις της απόκτησης και κατοχής πληροφορίας.

Η εμπειρία έχει δείξει ότι οι ακόλουθοι παράγοντες έχουν ιδιαίτερη σημασία κατά την υλοποίηση της ασφάλειας πληροφοριών μέσα σε έναν οργανισμό:

- Η πολιτική ασφάλειας πληροφοριών, οι στόχοι και οι δραστηριότητες που αντικατοπτρίζουν τους στόχους του οργανισμού.

- Μια προσέγγιση και ένα πλαίσιο υλοποίησης, συντήρησης, επίβλεψης και βελτίωσης της ασφάλειας πληροφοριών με τρόπο συμβατό με την κουλτούρα του οργανισμού.

- Η ξεκάθαρη υποστήριξη και συμμετοχή από όλα τα επίπεδα της ιεραρχίας διοίκησης του οργανισμού.

- Μια καλή κατανόηση των απαιτήσεων ασφάλειας, με βάση τη μελέτη ανάλυσης και αποτίμησης της επικινδυνότητας.

- Η αποτελεσματική προώθηση των σκοπών της ασφάλειας πληροφοριών προς όλα τα στελέχη και τους εργαζόμενους, καθώς και τρίτα μέρη.

- Η αποκεντρωμένη καθοδήγηση σε θέματα ασφάλειας πληροφοριών και σχετικών προτύπων προς όλα τα στελέχη και τους εργαζόμενους, καθώς και τρίτα μέρη.

- Η παροχή οικονομικών πόρων για τις δραστηριότητες που αφορούν την ασφάλεια πληροφοριών.

- Η επίτευξη επαρκούς ευαισθητοποίησης και η παροχή κατάλληλης εκπαίδευσης και κατάρτισης.

- Η εφαρμογή αποτελεσματικών διαδικασιών διαχείρισης συμβάντων ασφάλειας πληροφοριών.

- Η υλοποίηση ενός συστήματος μέτρησης που να μπορεί να αξιολογήσει την απόδοση του συστήματος διαχείρισης της ασφάλειας πληροφοριών και να προτείνει προτάσεις για βελτιώσεις.

Οι μεμονωμένες λύσεις και μηχανισμοί ασφάλειας οι οποίοι εφαρμόζονται και χρησιμοποιούνται από τους οργανισμούς, προσφέρουν λύση στο πρόβλημα της ασφάλειας αλλά μόνο σε ότι αφορά το πεδίο στο οποίο εφαρμόζονται. Για παράδειγμα, ένα ανάχωμα προστασίας (firewall) μπορεί να προσφέρει ένα πρόσθετο βαθμό ασφάλειας στη δικτυακή υποδομή ενός οργανισμού ή ένας μηχανισμός ελέγχου πρόσβασης μπορεί να προσφέρει λύση στο πρόβλημα ελέγχου πρόσβασης σε ένα επιμέρους υπολογιστικό σύστημα. Ωστόσο, μια τέτοια πρακτική από μόνη της δεν προσφέρει συνήθως τη δυνατότητα αντιμετώπισης του προβλήματος της ασφάλειας πληροφοριών στην ολότητά του. Για το λόγο αυτό, είναι επιτακτική ανάγκη για τον ορισμό ενός πλαισίου, στη βάση του οποίου να αντιμετωπίζουμε με μια ολιστική προσέγγιση το πρόβλημα της ασφάλειας πληροφοριών. Συγκεκριμένα, ο πρώτος άξονας ενός τέτοιου πλαισίου θα μπορούσε να αφορά στο υπό εξέταση πληροφοριακό σύστημα (π.χ., δημόσιας διοίκησης, επιχειρησιακό πληροφοριακό σύστημα, κλπ.) και ο δεύτερος άξονας αφορά στις δράσεις οι οποίες πρέπει να πραγματοποιούνται. Στις δράσεις αυτές συμπεριλαμβάνονται θεσμικές ρυθμίσεις, οργανωσιακές ρυθμίσεις αλλά και κοινωνικές δράσεις.

Οι θεσμικές ρυθμίσεις κατηγοριοποιούνται σε κανονιστικές και νομικές. Ένα παράδειγμα κανονιστικής ρύθμισης αποτελούν τα πρότυπα (standards). Κανονιστική ρύθμιση αποτελούν επίσης και οι κώδικες δεοντολογίας οι οποίοι συμπληρώνουν την υπάρχουσα νομοθεσία. Μια διαφορετική κατηγοριοποίηση των θεσμικών ρυθμίσεων μπορεί να γίνεται σύμφωνα με το γεωγραφικό πεδίο εφαρμογής τους. Σε μια τέτοια περίπτωση, έχουμε διεθνείς, περιφερειακές, εθνικές και τοπικές θεσμικές ρυθμίσεις. Τέλος, οι θεσμικές ρυθμίσεις μπορούν να κατηγοριοποιούνται και σύμφωνα με το τομεακό πεδίο εφαρμογής τους. Αν μία θεσμική

ρύθμιση εφαρμόζεται σε παραπάνω από έναν τομέα (π.χ. υγεία, οικονομία κλπ.) τότε μιλάμε για μια οριζόντια θεσμική ρύθμιση. Αν η θεσμική ρύθμιση αφορά μόνον ένα τομέα, μιλάμε για μια κάθετη θεσμική ρύθμιση.

Οι οργανωσιακές ρυθμίσεις αφορούν εκείνα τα μέτρα οργάνωσης που κάθε επιχείρηση ή οργανισμός παίρνει προκειμένου να διασφαλίζει την ασφάλεια των πληροφοριών που διαχειρίζεται. Για παράδειγμα, μια στρατηγική και οι σχετικές πολιτικές, είναι ένα παράδειγμα οργανωσιακής ρύθμισης.

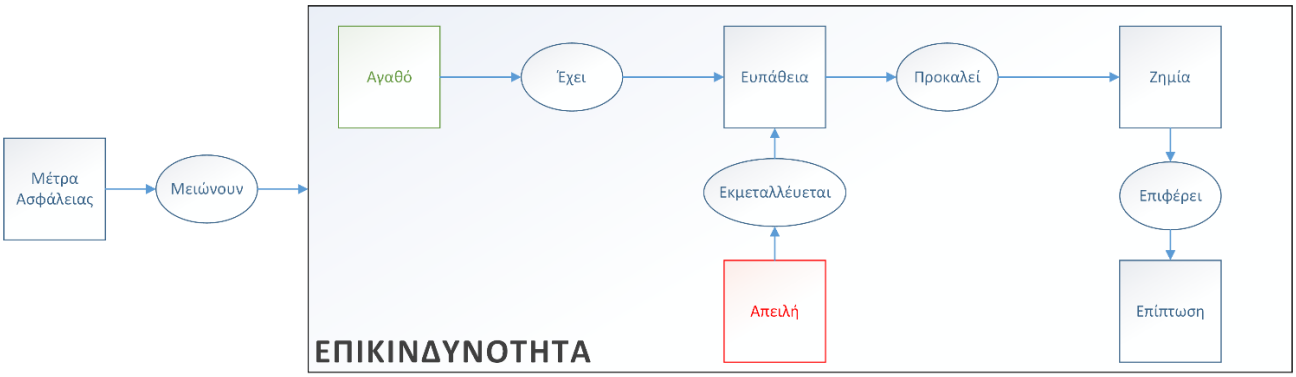
Ένα πρότυπο, όπως για παράδειγμα ένα τεχνικό πρότυπο (technical standard), είναι ένα σύνολο αποδεκτών κριτηρίων, μεθόδων και διεργασιών ή πρακτικών. Τα πρότυπα μπορεί να προκύπτουν από ενώσεις εταιρειών ή οργανισμών προτυποποίησης κατόπιν έρευνας και ευρύτερης συμφωνίας, οπότε τα de jure πρότυπα. Υπάρχουν όμως περιπτώσεις δημιουργίας προτύπων τα οποία απολαμβάνουν ευρείας αποδοχής, χωρίς να αποτελούν μέρος ενός τυπικού κανονιστικού πλαισίου. Κανείς δεν έχει τη νομική ή κανονιστική υποχρέωση να ακολουθήσει αυτά τα πρότυπα, τα οποία είναι γνωστά ως de facto πρότυπα, ενώ θεωρούνται ότι αποτελούν τα ισχυρότερα πρότυπα, καθώς επικράτησαν μετά από ανταγωνισμό στην πράξη.

Η διεργασία ανάπτυξης και υλοποίησης τεχνικών προτύπων ονομάζεται Προτυποποίηση. Συνεπώς, για να εξασφαλιστεί η συμμόρφωση ενός οργανισμού με συγκεκριμένες προδιαγραφές θα πρέπει να αυτός να αξιολογείται με σκοπό την απόκτηση του αντίστοιχου πιστοποιητικού συμμόρφωσης (πιστοποίηση). Η πιστοποίηση ορίζει τις διαδικασίες αξιολόγησης και ελέγχου ενός οργανισμού. Από τα πλέον διαδεδομένα πρότυπα ασφάλειας πληροφοριών είναι η σειρά προτύπων ISO/IEC 27000, καθώς και τα Common Criteria. Η εναρμόνιση ενός οργανισμού με κάποιο πρότυπο εξασφαλίζει την ύπαρξη συγκεκριμένων επιθυμητών χαρακτηριστικών σε προϊόντα ή υπηρεσίες. Επίσης, εξασφαλίζεται η συμβατότητα και η διαλειτουργικότητα μεταξύ διαφορετικών πληροφοριακών συστημάτων.

11.2 Εννοιολογική Θεμελίωση

Είναι αναγκαία η ύπαρξη ενός κοινού λεξιλογίου, αυστηρά καθορισμένου, έτσι ώστε να μπορέσουν δύο μέρη να επικοινωνήσουν αποτελεσματικά. Στο χώρο της Ασφάλειας Πληροφοριών, η ανάγκη αυτή είναι ακόμη επιτακτικότερη, καθώς τα μέρη τα οποία έρχονται σε επικοινωνία μπορεί να ανήκουν σε διαφορετικούς τομείς (π.χ. Πληροφορική, Οικονομικά, Διοίκηση κ.λπ.), ενώ λειτουργούν μέσα στον ίδιο οργανισμό για τον κοινό σκοπό. Έτσι, οι βασικές έννοιες που αφορούν στην Ασφάλεια Πληροφοριών (και κατ' επέκταση τη Διαχείριση της Ασφάλειας) θα πρέπει να είναι ξεκάθαρες για κάθε συμμετέχοντα στη διαδικασία λήψης αποφάσεων που αφορούν τον οργανισμό. Για το λόγο αυτό, είναι χρήσιμο να επαναλάβουμε ορισμένες βασικές έννοιες που παρουσιάσθηκαν στο πρώτο κεφάλαιο, μέσα από ένα διαφορετικό πρίσμα.

Στην παρακάτω Εικόνα 11.1, εμφανίζονται οι συσχετίσεις μεταξύ των όρων ασφάλειας πληροφοριών, οι οποίοι θα μας απασχολήσουν στη συνέχεια.



Εικόνα 11.1 *Συσχετίσεις μεταξύ όρων ασφάλειας πληροφοριών.*

Ένα αγαθό, όπως εμφανίζεται στην παραπάνω Εικόνα 11.1, έχει αξία για ένα οργανισμό και πρέπει να προστατευτεί. Αυτό είναι ιδιαίτερα σημαντικό στο διαρκώς διασυνδεόμενο επιχειρηματικό περιβάλλον, όπου οι πληροφορίες εκτίθενται σε ένα ολοένα αυξανόμενο αριθμό και με μια διερευνώμενη ποικιλία απειλών.

Η πληροφορία (ως αγαθό) μπορεί να εμφανιστεί υπό διάφορες μορφές. Μπορεί να γραφεί σε χαρτί, να αποθηκευτεί 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. Στο πλαίσιο της ασφάλειας πληροφοριών, επιδιώκεται η προστασία των πληροφοριών από μια ευρεία γκάμα απειλών, ώστε να διασφαλιστεί η επιχειρησιακή συνέχεια, να ελαχιστοποιηθεί η συνολική εναπομείνασα επικινδυνότητα και να μεγιστοποιηθούν οι αποδόσεις των επενδύσεων και οι επιχειρησιακές ευκαιρίες.

Η μείωση της συνολικής επικινδυνότητας επιτυγχάνεται με την υλοποίηση ενός κατάλληλου συνόλου (αντι)μέτρων (controls), που περιλαμβάνουν πολιτικές, πρακτικές, διαδικασίες, τεχνικές και λειτουργίες λογισμικού και υλικού. Αυτά τα μέτρα είναι απαραίτητα προκειμένου να διασφαλιστεί ότι επιτυγχάνονται οι επιμέρους στόχοι του οργανισμού που αφορούν την ασφάλεια πληροφοριών, σε συνδυασμό με άλλες πρακτικές διαχείρισης.

Η αξία ενός αγαθού αφορά τη σημαντικότητά του για την επίτευξη των στόχων του οργανισμού και εκφράζεται είτε με χρηματικούς ή άλλους όρους. Ένα υπολογιστικό σύστημα είναι δυνατό να παρουσιάζει ευπάθειες, δηλαδή αδυναμίες τις οποίες μπορεί να εκμεταλλευτεί μια απειλή (στο πλαίσιο μια επίθεσης) και να προκαλέσει ζημία. Η απειλή μπορεί να είναι φυσική, τεχνικής φύσης, ή ανθρώπινη, εκούσια ή ακούσια. Επίσης, μια απειλή μπορεί να είναι σκόπιμη ή τυχαία. Ως ζημία, θεωρούμε την επίπτωση που προκαλεί η μείωση της αξίας του αγαθού. Η επίπτωση αποτυπώνεται ως μια αλλαγή στο δυνητικό βαθμό επίτευξης των επιχειρησιακών στόχων του οργανισμού.

Τα πέντε αυτά στοιχεία (αγαθό, ευπάθεια, ζημία, απειλή και επίπτωση) ορίζουν την έννοια της επικινδυνότητας (risk). Με βάση την κατάλληλη αποτίμηση της επικινδυνότητας θα πρέπει να γίνεται επιλογή των κατάλληλων μέτρων προστασίας, που θα μετριάζουν την επικινδυνότητα.

Ο σχεδιασμός, η υλοποίηση, η συντήρηση και η βελτίωση της ασφάλειας πληροφοριών αποτελούν ουσιαστικούς παράγοντες για την επίτευξη ανταγωνιστικών χαρακτηριστικών, κερδοφορίας, επαρκούς συμμόρφωσης με τους νόμους και διαμόρφωσης κατάλληλης φήμης. Όμως, στον αρχικό σχεδιασμό των πληροφοριακών συστημάτων συνήθως δεν συμπεριλαμβάνονται εξ αρχής τα απαραίτητα χαρακτηριστικά ασφάλειας, με αποτέλεσμα το παρεχόμενο επίπεδο ασφάλειας να είναι ανεπαρκές και να χρειάζεται μια κατάλληλη διαχείριση και υλοποίηση επιμέρους διαδικασιών. Η επιλογή των κατάλληλων μέτρων ελέγχου, προϋποθέτει προσεκτικό και λεπτομερή σχεδιασμό, ενώ η ασφάλεια των πληροφοριών γενικότερα 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 συνεργατών, εξειδικευμένων σε θέματα ασφάλειας. Συνολικά, η Διαχείριση Ασφάλειας αποσκοπεί στη διαμόρφωση ενός οργανωμένου πλαισίου εννοιών, αρχών, πολιτικών, διαδικασιών και τεχνικών μέτρων που απαιτούνται προκειμένου να προστατευθούν τα αγαθά από σκόπιμες ή τυχαίες απειλές.

11.3 Συστήματα Διαχείρισης Ασφάλειας Πληροφοριών

Ορισμένοι βασικοί παράγοντες, στη βάση των οποίων ένας οργανισμός μπορεί να ορίζει το επιθυμητό επίπεδο ασφάλειας είναι οι εξής:

- Αποδεκτό επίπεδο ασφάλειας.
- Λειτουργικότητα του Πληροφοριακού Συστήματος που διαθέτει.
- Κόστος που επιθυμεί να επωμισθεί.

Ο σχεδιασμός της ασφάλειας πληροφοριών ενός οργανισμού είναι μια επιχειρησιακή διεργασία, η οποία αποσκοπεί στο να παρέχονται τα κατάλληλα εργαλεία λήψης αποφάσεων, προκειμένου να μπορεί η διοίκηση να ασκήσει αποτελεσματικά το ρόλο της. Υπό αυτή την έννοια, η ασφάλεια πληροφοριών δεν είναι ένα αμιγώς τεχνικό θέμα, αλλά συμπεριλαμβάνει ζητήματα και παραμέτρους από διάφορους χώρους (οικονομία, διοίκηση, κοινωνία κ.λπ.). Για να επιτευχθεί ένας αποδοτικός συντονισμός των ενεργειών προς αυτή τη κατεύθυνση, θα πρέπει να οριστούν οι στόχοι της ασφάλειας πληροφοριών, καθώς και οι διαδικασίες των οποίων η εξέλιξη αλλά και τα αποτελέσματα θα ελέγχονται διαρκώς, χρησιμοποιώντας ένα κατάλληλο σύστημα διαχείρισης της ασφάλειας. Επιπλέον, οι απαιτήσεις ασφάλειας θα πρέπει να προσδιορίζονται στη βάση μιας περιοδικά επαναλαμβανόμενης μελέτης για την ανάλυση και διαχείριση της επικινδυνότητας (Risk Management).

Ένα Σύστημα Διαχείρισης Ασφάλειας Πληροφοριών (Information Security Management System – ISMS) επικεντρώνεται κυρίως στις διαδικασίες που λαμβάνουν χώρα στο πλαίσιο ενός οργανισμού. Για τη

διαχείριση της Ασφάλειας Πληροφοριών υπάρχουν αρκετές διαφορετικές μεθοδολογίες οι οποίες χρησιμοποιούν ή στηρίζονται αποκλειστικά σε κάποιο από τα πολλά και διαφορετικά πρότυπα που έχουν αναπτυχθεί. Μερικές από τις γνωστότερες είναι οι παρακάτω:

- OCTAVE από τον οργανισμό CERT (Carnegie Mellon University).
- COBIT από τον οργανισμό ISACA. Βασίζεται στον κύκλο: **Govern → Direct → Control → Implement → Measure → Evaluate → Report**
- FIRM από το Information Security Forum
- Μεθοδολογία του οργανισμού NIST. Βασίζεται στον κύκλο: **System Characterization → Threat Identification → Vulnerability Identification → Control Analysis → Likelihood Determination → Impact Analysis → Risk Determination → Control Recommendations → Results Documentation**

Μια ιδιαίτερα διαδεδομένη μέθοδος για τον έλεγχο και τη βελτίωση αυτών των διαδικασιών κατά την ανάπτυξη ενός Συστήματος Διαχείρισης της Ασφάλειας Πληροφοριών (π.χ. σύμφωνα με το πρότυπο ISO/IEC 27001) είναι η μέθοδος Plan-Do-Check-Act (PDCA).

Η μέθοδος PDCA αποτελείται από τέσσερα επαναληπτικά βήματα ως εξής:

- **Σχεδιασμός (Plan):** Στο βήμα αυτό αναλύεται και μελετάται η ασφάλεια πληροφοριών στον οργανισμό, θέτονται οι στόχοι και ορίζονται οι τρόποι με τους οποίους θα επιτευχθούν οι στόχοι.
- **Υλοποίηση (Do)**: Εδώ υλοποιούνται τα μέτρα τα οποία ορίστηκαν κατά τη φάση του σχεδιασμού.
- **Έλεγχος (Check):** Πραγματοποιείται έλεγχος απόκλισης των αρχικών στόχων και των τελικών αποτελεσμάτων.
- **Δράση (Act):** Εφαρμόζονται ενέργειες διόρθωσης και βελτίωσης των μέτρων.

Μπορούμε να φανταστούμε το Σύστημα Διαχείρισης της Ασφάλειας Πληροφοριών ως μία ενιαία διεργασία η οποία δέχεται ως είσοδο τις απαιτήσεις ασφάλειας του οργανισμού και παρέχει ως έξοδο τη διαχείριση της ασφάλειας πληροφοριών.

Κατά τη φάση του σχεδιασμού, πραγματοποιείται ανάλυση και εκτίμηση της επικινδυνότητας για την ασφάλεια των πληροφοριών. Πιο συγκεκριμένα, διαμορφώνονται και πραγματοποιούνται μεταξύ άλλων τα εξής:

- Έγκριση από τη Διοίκηση του οργανισμού.
- Καθορισμός του πεδίου εφαρμογής (υπολογιστικά συστήματα, δεδομένα κλπ.).
- Μελέτη Ανάλυσης και Αποτίμησης Επικινδυνότητας.
- Καθορισμός απαιτήσεων ασφάλειας.
- Δημιουργία Πολιτικής Ασφάλειας.

Αξίζει εδώ να επισημανθεί ότι είναι πρωταρχικής σημασίας για έναν οργανισμό ο καθορισμός των απαιτήσεών του σε θέματα ασφάλειας. Μερικές βασικές πηγές άντλησης πληροφοριών για απαιτήσεις ασφάλειας είναι ο εξής:

- Η αποτίμηση της επικινδυνότητας (risk assessment) που αντιμετωπίζει ο οργανισμός. Μέσω αυτής της διαδικασίας, αναγνωρίζονται οι πιθανές απειλές προς τους πόρους του οργανισμού. Επιπλέον, εκτιμάται η συνολική ευπάθεια (vulnerability) του οργανισμού στις συγκεκριμένες

απειλές, η πιθανότητα υλοποιήσεών τους, καθώς και το κόστος που θα έχουν οι επιπτώσεις για τον οργανισμό από πιθανές επιθέσεις.

- Το νομικό και κανονιστικό πλαίσιο, καθώς 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 για τη λειτουργία του.

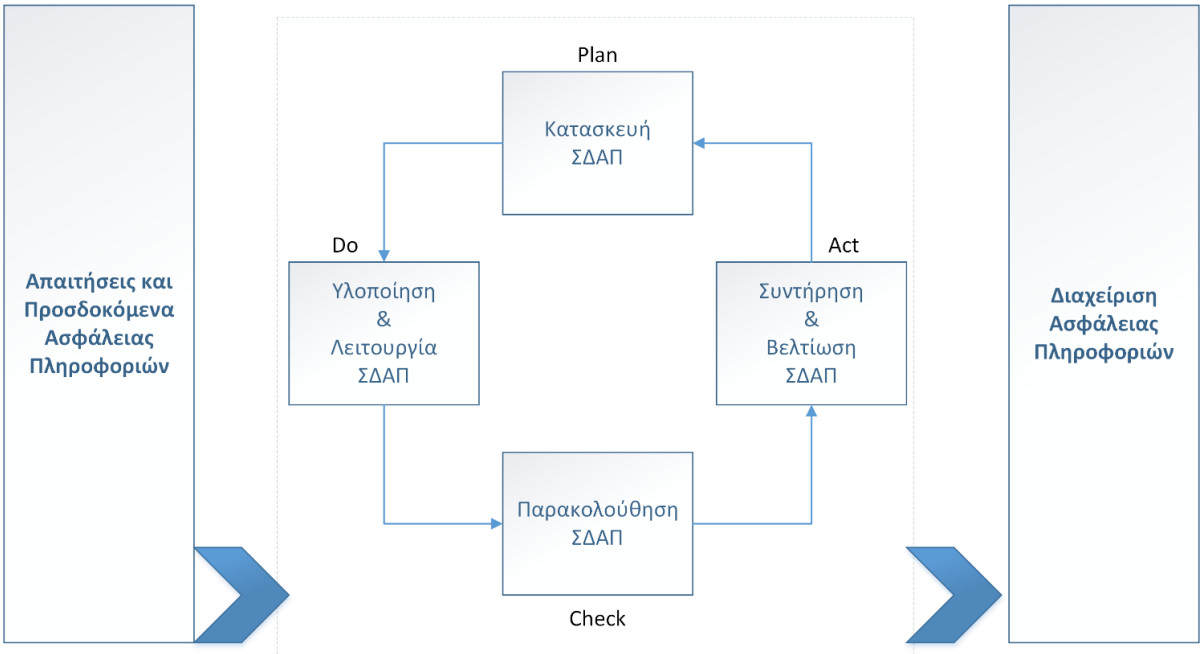
Στη φάση της υλοποίησης και με βάση τα αποτελέσματα της αποτίμησης, ακολουθεί νέα μελέτη που αποσκοπεί στη μείωση της επικινδυνότητας με την επιλογή και υλοποίηση των κατάλληλων μέτρων προστασίας. Αναλυτικότερα, διαμορφώνονται και υλοποιούνται μεταξύ άλλων τα εξής:

- Σχέδιο Διαχείρισης Επικινδυνότητας.
- Κατανομή ρόλων και αρμοδιοτήτων.
- Υλοποίηση μέτρων ασφάλειας.
- Δράσεις ενημέρωσης και κατάρτισης του προσωπικού.
- Υλοποίηση διαδικασιών έγκαιρης ανίχνευσης και αντιμετώπισης περιστατικών ασφάλειας.

Κατά τον έλεγχο, πραγματοποιείται μια αξιολόγηση των αποτελεσμάτων σε σχέση με τους αρχικούς στόχους που είχαν τεθεί και διαμορφώνεται μια αναφορά αξιολόγησης προς τη διοίκηση του οργανισμού. Η διαδικασία του ελέγχου είναι επαναληπτική και πραγματοποιείται ανά τακτά χρονικά διαστήματα, συνήθως από το αρμόδιο τμήμα εσωτερικού ελέγχου του οργανισμού.

Τέλος, στο στάδιο της δράσης εκτελούνται όλες εκείνες οι απαραίτητες ενέργειες, οι οποίες κρίθηκε ότι απαιτούνται προκειμένου να βελτιωθεί η συνολική διεργασία της διαχείρισης της ασφάλειας πληροφοριών. Πραγματοποιείται ενημέρωση της διοίκησης και παράλληλα ελέγχεται και αξιολογείται και η ίδια η διαδικασία βελτίωσης των μέτρων προστασίας.

Το πρότυπο ISO/IEC 27001, συνδυάζοντας τα τέσσερα (4) βήματα της μεθοδολογίας PDCA, ορίζει το πλαίσιο της Διαχείρισης Ασφάλειας Πληροφοριών, όπως φαίνεται στην παρακάτω Εικόνα 11.2.



Εικόνα 11.2 *Διαχείριση Ασφάλειας Πληροφοριών κατά ISO/IEC 27001.*

Το πρότυπο BS 7799-1 του Βρετανικού οργανισμού προτυποποίησης υποβλήθηκε στον οργανισμό ISO/IEC και έγινε αποδεκτό το 2000. Το έτος 2002 μετονομάστηκε σε ISO/IEC 27002 ενώ το 2005 το βρετανικό πρότυπο BS 7799-2 έγινε δεκτό και μετονομάστηκε σε ISO/IEC 27001.

Η σειρά προτύπων ISO 27K είναι ένας οδηγός βέλτιστων πρακτικών για τη διαχείριση της ασφάλειας πληροφοριών και τη διαχείριση της σχετικής επικινδυνότητας που αντιμετωπίζει ένας οργανισμός. Προτείνει μέτρα ασφάλειας, ενώ μέχρι σήμερα η οικογένεια αριθμεί 23 μέλη. Το κεντρικό πρότυπο είναι το ISO/IEC 27001 με το οποίο μπορεί ένας οργανισμός να εναρμονιστεί και να λάβει πιστοποίηση από τρίτο ανεξάρτητο φορέα. Ο φορέας πιστοποίησης με τη σειρά του μπορεί να λάβει διαπίστευση, σύμφωνα με το πρότυπο ISO/IEC 27006.

Στον ακόλουθο πίνακα παρουσιάζεται μια σύντομη περιγραφή των προτύπων της οικογένειας ISO 27000:

Όνομα	**Αντικείμενο**
ISO/IEC 27000	Εισαγωγή και λεξιλόγιο όρων
ISO/IEC 27001	Απαιτήσεις υλοποίησης και συντήρησης Συστήματος Διαχείρισης Ασφάλειας Πληροφοριών
ISO/IEC 27002	Πρακτικές διαχείρισης της ασφάλειας και επιλογής μέτρων ασφάλειας
ISO/IEC 27003	Οδηγίες σχεδιασμού ενός Συστήματος Διαχείρισης Ασφάλειας Πληροφοριών
ISO/IEC 27004	Μετρικές εκτίμησης της αποτελεσματικότητας υλοποιημένου Συστήματος Διαχείρισης Ασφάλειας Πληροφοριών
ISO/IEC 27005	Οδηγίες διαχείρισης Επικινδυνότητας
ISO/IEC 27006	Οδηγίες ελέγχου και πιστοποίησης Συστήματος Διαχείρισης Ασφάλειας Πληροφοριών
ISO/IEC 27007	Οδηγίες ικανοτήτων ελεγκτών Συστημάτων Διαχείρισης Ασφάλειας Πληροφοριών
ISO/IEC 27008	Οδηγίες ελέγχου της υλοποίησης Συστήματος Διαχείρισης Ασφάλειας και Πληροφοριών
ISO/IEC 27010	Οδηγίες για κοινότητες ανταλλαγής πληροφοριών
ISO/IEC 27011	Οδηγίες για τηλεπικοινωνιακούς οργανισμούς
ISO/IEC 27013	Οδηγίες υλοποίησης ISO/IEC 27001 και ISO/IEC 20000-1
ISO/IEC 27014	Έννοιες και αρχές διακυβέρνησης της ασφάλειας
ISO/IEC 27015	Οδηγίες για οργανισμούς παροχής χρηματοοικονομικών υπηρεσιών
ISO/IEC 27016	Οικονομικές επιπτώσεις αποφάσεων σχετικών με Διαχείριση Ασφάλειας Πληροφοριών
ISO/IEC 27018	Οδηγίες προστασίας Προσωπικά Αναγνωρίσιμων Πληροφοριών
ISO/IEC 27019	Οδηγίες για παρόχους Ηλεκτρικής Ενέργειας
ISO/IEC 27031	Περιγραφή εννοιών και αρχών επιχειρησιακής συνέχειας των Πληροφοριακών υποδομών
ISO/IEC 27032	Οδηγίες βελτίωσης της Κυβερνοασφάλειας
ISO/IEC 27033	Οδηγίες ασφάλειας δικτύων
ISO/IEC 27034	Οδηγίες ενσωμάτωσης των μηχανισμών ασφάλειας στις επιχειρησιακές διεργασίες
ISO/IEC 27035	Οδηγίες ανίχνευσης και αντιμετώπισης περιστατικών ασφάλειας
ISO/IEC 27036	Οδηγίες για παρόχους υπηρεσιών cloud computing
ISO/IEC 27037	Οδηγίες διαχείρισης ψηφιακών τεκμηρίων
ISO/IEC 27038	Οδηγίες επιμέλειας ψηφιακών εγγράφων
ISO/IEC 27789	Οδηγίες για συστήματα Ηλεκτρονικού Φακέλου Υγείας
ISO/IEC 27790	Οδηγίες μετάδοσης, αποθήκευσης και αξιοποίησης ψηφιακών εγγράφων για οργανισμούς υγείας
ISO/IEC 27799	Οδηγίες υλοποίησης του ISO/IEC 27002 σε οργανισμούς υγείας

Πίνακας 11.1 *Πρότυπα ασφάλειας της οικογένειας ISO 27k.*

11.4 Ανάλυση, Αποτίμηση και Διαχείριση Επικινδυνότητας

Είδαμε σε προηγούμενη ενότητα ότι κατά τη διεργασία της Διαχείρισης Ασφάλειας Πληροφοριών είναι απαραίτητη η εκπόνηση μελέτης ανάλυσης και αποτίμησης επικινδυνότητας. Μια τέτοια μελέτη είναι απαραίτητη, καθώς θα μας δώσει απαντήσεις σε ερωτήματα όπως:

- Ποια αγαθά του ΠΣ μας πρέπει να προστατέψουμε;

- Τι απειλές υπάρχουν για τα αγαθά αυτά;
- Τι μέτρα προστασίας πρέπει να χρησιμοποιηθούν;

Ένας άλλος κύριος λόγος για τον οποίο είναι απαραίτητη η μελέτη ανάλυσης και αποτίμησης επικινδυνότητας είναι γιατί με αυτό τον τρόπο μπορούμε να ποσοτικοποιήσουμε το επίπεδο ασφάλειας που επιθυμούμε καθώς και να «μετρήσουμε» το βαθμό επίτευξης του στόχου της μείωσης επικινδυνότητας σε αποδεκτά επίπεδα. Από τη μια, οι απαιτήσεις ασφάλειας του οργανισμού προκύπτουν μετά από μια μεθοδική αποτίμηση της επικινδυνότητας που αντιμετωπίζει ο οργανισμός. Από την άλλη, το κόστος των μέτρων προστασίας θα πρέπει να εξισορροπείται από την πιθανή ζημιά στον οργανισμό σε περίπτωση που παραβιασθεί η ασφάλεια του πληροφοριακού συστήματός του. Τα αποτελέσματα της αποτίμησης επικινδυνότητας θα βοηθήθσουν στην καθοδήγηση και στη λήψη αποφάσεων για καθορισμό κατάλληλων διοικητικών ενεργειών και τον καθορισμό προτεραιοτήτων στην κατεύθυνση της διαχείρισης της ασφάλειας των πληροφοριών.

Η μελέτη ανάλυσης και αποτίμησης επικινδυνότητας είναι μια συστηματική διαδικασία και θα πρέπει να επαναλαμβάνεται σε περιοδική βάση προκειμένου να συμπεριλαμβάνονται οι οποιεσδήποτε αλλαγές στη λειτουργία του οργανισμού που πιθανώς να επηρεάζουν τα αποτελέσματα της μελέτης. Είναι απαραίτητος ο περιοδικός έλεγχος της επικινδυνότητας, όπως και της σωστής εφαρμογής των μέτρων προστασίας, προκειμένου αυτά να προσαρμόζονται στις ανάγκες και τις προτεραιότητες του οργανισμού, να επεκτείνονται για την προστασία από νέες απειλές και να επιβεβαιώνουν την ορθή και αποτελεσματική λειτουργία των υπαρχόντων μέτρων προστασίας.

Από τη στιγμή που θα καθοριστούν οι απαιτήσεις και οι απειλές ασφάλειας και θα έχουν παρθεί οι αποφάσεις για την αντιμετώπιση των απειλών, μπορεί να γίνει η επιλογή των κατάλληλων μέτρων προστασίας, τα οποία θα μειώσουν την επικινδυνότητα σε αποδεκτά επίπεδα. Τα μέτρα αυτά μπορούν να επιλεγούν από οποιοδήποτε σύνολο (π.χ. προτεινόμενο από κάποιο πρότυπο) μέτρων προστασίας είναι κατάλληλο για τον οργανισμό. Τα μέτρα θα πρέπει να επιλεγούν με κριτήριο το κόστος υλοποίησής τους σε σχέση με τις απειλές που καλούνται να αντιμετωπίσουν και το κόστος των πιθανών επιπτώσεων από πιθανές επιθέσεις στον οργανισμό. Επίσης, θα πρέπει να συμπεριληφθούν και ποιοτικοί παράγοντες, όπως η απώλεια φήμης για τον οργανισμό. Τέλος, τα μέτρα προστασίας θα πρέπει να είναι σύμφωνα με την εθνική και διεθνή νομολογία και τους κανονισμούς.

Υπάρχουν ορισμένα μέτρα προστασίας που θεωρούνται θεμελιώδη και αποτελούν τη βάση για την ασφάλεια πληροφοριών. Βασίζονται είτε σε υποχρεωτικές νομικές διατάξεις, είτε έχουν καθιερωθεί ως κοινή πρακτική στην ασφάλεια. Τέτοια μέτρα προστασίας μπορούν να αφορούν π.χ. την προστασία του προσωπικού απορρήτου, τη διαφύλαξη της ασφάλειας των δεδομένων του οργανισμού, την προστασία της πνευματικής ιδιοκτησίας, κ.ά.

Ορισμένα μέτρα προστασίας, πέρα από τα καθαρά τεχνικά, που θεωρούνται ότι αποτελούν κοινή πρακτική για την ασφάλεια πληροφοριών είναι:

- Το έγγραφο της πολιτικής ασφάλειας πληροφοριών.
- Ο επιμερισμός καθηκόντων σχετικών με την ασφάλεια πληροφοριών.
- Η ευαισθητοποίηση, η εκπαίδευση και η κατάρτιση σε θέματα ασφάλειας πληροφοριών.
- Η σωστή λειτουργία των εφαρμογών.
- Η διαχείριση των ευπαθειών.
- Η διαχείριση της επιχειρησιακής συνέχειας.
- Η διαχείριση των συμβάντων ασφάλειας και των συναφών βελτιώσεων που αφορούν την ασφάλεια πληροφοριών του οργανισμού.

Τα παραπάνω μέτρα μπορούν να χρησιμοποιηθούν σχεδόν σε κάθε οργανισμό. Ωστόσο, αν και αποτελούν βασικά βήματα εκκίνησης για την ασφάλεια πληροφοριών, δεν πρέπει σε καμιά περίπτωση να

υποκαταστήσουν τη διενέργεια της μελέτης ανάλυσης και αποτίμησης επικινδυνότητας και της προσεκτικής υλοποίησης των αποτελεσμάτων της.

Η έννοια της επικινδυνότητας έχει τις ρίζες της στην Οικονομική επιστήμη, όπου στόχος είναι η μείωσή της στις επιχειρηματικές επενδύσεις. Στην επιστήμη της Πληροφορικής και ειδικότερα στο πεδίο της Ασφάλειας Πληροφοριών, η επικινδυνότητα (R) εκφράζεται ως το γινόμενο της πιθανότητας (P) να συμβεί μια παραβίαση ασφάλειας επί το κόστος (C) της ζημίας που θα προκύψει από την παραβίαση. Σύμφωνα με το πρότυπο ISO/IEC 27005, επικινδυνότητα είναι «η επίδραση της αβεβαιότητας στους στόχους». Άρα, η επικινδυνότητα μπορεί να είναι ένα μέγεθος το οποίο μετριέται χρησιμοποιώντας τη θεωρία πιθανοτήτων (π.χ. κατά Bayes, όπου για ένα γεγονός μπορούμε να μετρήσουμε την πιθανότητα πραγματοποίησης του αν αναλύσουμε τους επιμέρους παράγοντες που το επηρεάζουν). Πιο συγκεκριμένα, η πιθανότητα να συμβεί ένα περιστατικό είναι συνάρτηση της πιθανότητας να εμφανιστεί μια απειλή και της πιθανότητας αυτή η απειλή να μπορέσει να εκμεταλλευτεί μια σχετική ευπάθεια του συστήματος.

Η ανάλυση και αποτίμηση επικινδυνότητας είναι απαραίτητο προαπαιτούμενο της διαχείρισης επικινδυνότητας. Με τη διαχείριση επικινδυνότητας στη συνέχεια επιδιώκεται:

- η μείωσή της, εφαρμόζοντας μέτρα προστασίας,
- η μεταφορά της προσλαμβάνοντας τρίτο οργανισμό π.χ. ασφαλιστικό,
- η με κάποιο τρόπο αποφυγή της,
- η αποδοχή της.

Η ανάλυση και εκτίμηση επικινδυνότητας αποτελούν τα αρχικά βήματα σε μια μεθοδολογία διαχείρισης της επικινδυνότητας. Οι οργανισμοί χρησιμοποιούν την ανάλυση και εκτίμηση επικινδυνότητας για να καθορίσουν την έκταση των πιθανών απειλών και τον κίνδυνο που σχετίζεται με ένα πληροφοριακό σύστημα. Για να μπορούμε να καθορίσουμε την πιθανότητα ενός μελλοντικού κακόβουλου γεγονότος, θα πρέπει να αναλύονται οι απειλές για ένα πληροφοριακό σύστημα σε συσχετισμό με την πιθανότητα εκμετάλλευσης ευπαθειών στο πληροφοριακό σύστημα. Η επίπτωση αναφέρεται στο μέγεθος της ζημιάς που θα μπορούσε να προκληθεί από την υλοποίηση (μέσω μιας επίθεσης) μιας απειλής, ως αποτέλεσμα της εκμετάλλευσης μιας ή περισσότερων ευπαθειών του συστήματος.

Το σχετικό πλαίσιο του οργανισμού NIST εμπεριέχει εννέα πρωτεύοντα στάδια:

- Χαρακτηρισμός Συστήματος.
- Αναγνώριση Απειλής.
- Αναγνώριση Ευπάθειας.
- Ανάλυση Μηχανισμών Ασφάλειας.
- Προσδιορισμός Πιθανότητας.
- Ανάλυση Επίπτωσης.
- Προσδιορισμός Επικινδυνότητας.
- Προτάσεις μηχανισμών Ελέγχου.
- Τεκμηρίωση Αποτελεσμάτων.

11.4.1 Χαρακτηρισμός συστήματος

Σε αυτό το βήμα, αναγνωρίζονται τα λογικά όρια του πληροφοριακού συστήματος. Οι πληροφορίες που συλλέγονται για το πληροφοριακό σύστημα αφορούν υλικό, λογισμικό, δικτυακές συνδέσεις, τα πρόσωπα που υποστηρίζουν και χρησιμοποιούν το πληροφοριακό σύστημα, την αποστολή του συστήματος καθώς και την ευαισθησία των δεδομένων του. Επίσης, συλλέγονται πληροφορίες σχετικά με τις λειτουργικές απαιτήσεις του πληροφοριακού συστήματος, τους χρήστες του, τις πολιτικές ασφαλείας, την αρχιτεκτονική του συστήματος ασφαλείας, την τρέχουσα τοπολογία δικτύου, τους διοικητικούς ελέγχους, τις ροές των πληροφοριών, τους τεχνικούς και λειτουργικούς ελέγχους, καθώς και το φυσικό περιβάλλον του πληροφοριακού συστήματος.

Για τη συλλογή των πληροφοριών χρησιμοποιούνται διάφορα εργαλεία όπως:

- Ερωτηματολόγιο, που θα πρέπει να διανέμεται στο προσωπικό που λειτουργεί ή υποστηρίζει το πληροφοριακό σύστημα. Το ερωτηματολόγιο θα μπορούσε επίσης να χρησιμοποιηθεί κατά τη διάρκεια συνεντεύξεων.

- Συνέντευξη με το διοικητικό προσωπικό.

- Εταιρικά έγγραφα, τα οποία περιγράφουν λεπτομερώς εσωτερικές διαδικασίες.

- Αυτοματοποιημένα εργαλεία συλλογής πληροφοριών.

11.4.2 Αναγνώριση απειλών

Ο σκοπός αυτού του βήματος είναι να αναγνωρίσει τις πιθανές απειλές που μπορεί να προκαλέσουν ρήγμα ασφάλειας στο πληροφοριακό μας σύστημα. Η κατηγοριοποίηση των απειλών σε φυσικές, ανθρώπινες και σκόπιμες ή τυχαίες μας βοηθάει να αντιληφθούμε το βαθμό σοβαρότητας ή το ενδεχόμενο εμφάνισης της απειλής.

11.4.3 Αναγνώριση ευπαθειών

Ο στόχος αυτού του βήματος είναι να καταγράψει μια λίστα από ευπάθειες του πληροφοριακού συστήματος, που θα μπορούσαν να γίνουν αντικείμενο εκμετάλλευσης από ενδεχόμενες απειλές. Η μεθοδολογία που θα ακολουθηθεί συνήθως ποικίλει και εξαρτάται από την φύση και κατάσταση του πληροφοριακού συστήματος. Αν το πληροφοριακό σύστημα δεν έχει σχεδιαστεί ακόμη, η αναζήτηση ευπαθειών θα πρέπει να επικεντρωθεί στις πολιτικές ασφάλειας του οργανισμού, στις σχεδιασμένες διαδικασίες ασφαλείας, καθώς και τις απαιτήσεις του συστήματος. Αν το σύστημα είναι ήδη σε λειτουργία, η αναγνώριση των ευπαθειών θα πρέπει να επεκταθεί ώστε να περιέχει περισσότερη εξειδικευμένη πληροφορία, όπως σχεδιασμένα χαρακτηριστικά ασφάλειας μέσα στα έγγραφα του σχεδίου ασφαλείας, καθώς και αποτελέσματα της αξιολόγησης της ασφάλειας του συστήματος.

11.4.4 Ανάλυση μηχανισμών ασφάλειας

Ο σκοπός αυτού του σταδίου είναι να αναλύσει τους μηχανισμούς ασφάλειας που ήδη εφαρμόζονται, ή σχεδιάζονται για εφαρμογή στον οργανισμό για να ελαττώσουν ή να εξαλείψουν την πιθανότητα εκμετάλλευσης ευπαθειών του συστήματος από διάφορες απειλές.

11.4.5 Προσδιορισμός πιθανότητας

Για τον υπολογισμό της πιθανότητας εμφάνισης ενός περιστατικού ασφάλειας, λαμβάνεται υπόψη το κίνητρο των απειλών και η ικανότητα των δυνητικά επιτιθέμενων, η φύση της ευπάθειας, η ύπαρξη και η αποτελεσματικότητα των υφιστάμενων μέτρων προστασίας.

Η πιθανότητα μπορεί να είναι:

- Υψηλή, όταν η απειλή έχει υψηλά κίνητρα, μεγάλη αποτελεσματικότητα και τα υφιστάμενα μέτρα προστασίας δεν επαρκούν.

- Μεσαία, όταν η απειλή έχει υψηλά κίνητρα και μεγάλη αποτελεσματικότητα, αλλά τα υφιστάμενα μέτρα προστασίας επαρκούν.

- Χαμηλή, όταν η απειλή δεν έχει υψηλά κίνητρα, δεν έχει αποτελεσματικότητα και τα υφιστάμενα μέτρα προστασίας επαρκούν.

11.4.6 Ανάλυση επίπτωσης

Η επίπτωση ενός γεγονότος ασφάλειας (π.χ. μιας επίθεσης) μπορεί να περιγραφεί με τους όρους απώλειας ή υποβάθμισης των τριών κύριων χαρακτηριστικών της ασφάλειας: ακεραιότητα, διαθεσιμότητα και εμπιστευτικότητα.

11.4.7 Προσδιορισμός επικινδυνότητας

Ο σκοπός αυτού του βήματος είναι να εκτιμήσει το επίπεδο επικινδυνότητας του πληροφοριακού συστήματος. Η επικινδυνότητα εκφράζεται ως το γινόμενο της πιθανότητας εκδήλωσης μιας απειλής επί την επίπτωση που μπορεί αυτή να επιφέρει.

Η κλίμακα της επικινδυνότητας, με τις αξιολογήσεις της σε υψηλή, μεσαία και χαμηλή, αναπαριστά τον βαθμό του επιπέδου του κινδύνου στον οποίο ένα πληροφοριακό σύστημα, μία εγκατάσταση ή διαδικασία μπορεί να εκτεθεί αν υπάρχει μία ευπάθεια. Η κλίμακα της επικινδυνότητας, επίσης, αναπαριστά δράσεις οι οποίες πρέπει να εκτελεστούν για κάθε επίπεδο κινδύνου, ως εξής:

- Υψηλή επικινδυνότητα: Άμεση ανάγκη για διορθωτικά μέσα.
- Μεσαία επικινδυνότητα: Ανάγκη για διορθωτικά μέσα σε εύλογο χρονικό διάστημα.
- Χαμηλή επικινδυνότητα: Αποδοχή της ή διορθωτικά μέσα.

11.4.8 Προτεινόμενα μέτρα προστασίας

Κατά τη διάρκεια αυτού του σταδίου, προτείνονται εκείνα τα μέτρα προστασίας, τα οποία μπορούν να περιορίσουν τις ευπάθειες ή να τις εκμηδενίσουν. Για το σκοπό αυτό, λαμβάνονται υπόψη η αποτελεσματικότητα των προτεινόμενων επιλογών, η νομοθεσία και οι οργανωσιακοί κανονισμοί, η πολιτική, οι λειτουργικές επιπτώσεις, καθώς και η αξιοπιστία των μηχανισμών εφαρμογής των μέτρων. Τα προτεινόμενα μέτρα προστασίας είναι το αποτέλεσμα της διαδικασίας εκτίμησης της επικινδυνότητας και αποσκοπούν στο μετριασμό της επικινδυνότητας.

11.4.9 Τεκμηρίωση αποτελεσμάτων

Όταν ολοκληρωθεί η εκτίμηση της επικινδυνότητας, θα πρέπει να ακολουθήσει καταγραφή των αποτελεσμάτων σε μία ολοκληρωμένη αναφορά. Η αναφορά της εκτίμησης επικινδυνότητας βοηθά τη διοίκηση του οργανισμού στο να λάβει αποφάσεις σχετικά με την πολιτική, καθώς και τις λειτουργικές και διοικητικές αλλαγές του πληροφοριακού συστήματος που απαιτούνται. Η αναφορά της εκτίμησης επικινδυνότητας θα πρέπει να παρουσιάζεται ως μία συστηματική και αναλυτική προσέγγιση στη διαδικασία διαχείρισης της επικινδυνότητας, έτσι ώστε η διοίκηση να κατανοεί τους κινδύνους και να προβαίνει στη λήψη των κατάλληλων μέτρων προστασίας ώστε να μειώνει την επικινδυνότητα.

11.5 Σχέδιο Ασφάλειας

Η Πολιτική Ασφάλειας ανήκει ως έννοια στο οργανωσιακό πλαίσιο της Ασφάλειας Πληροφοριών. Το οργανωσιακό πλαίσιο της Ασφάλειας Πληροφοριών ενός οργανισμού περιλαμβάνει έγγραφα για πολιτικές, κανόνες, διαδικασίες και οδηγίες. Το σύνολο αυτών των εγγράφων συνηθίζεται να λέγεται Σχέδιο Ασφάλειας.

Αυτό το πλαίσιο ασφάλειας αποτελεί κεντρικό σημείο αναφοράς για την επικοινωνία μεταξύ των εμπλεκομένων, έτσι ώστε να αναπτυχθεί μια κοινή αντίληψη για την ασφάλεια και να διευκολυνθεί η συνεργασία μεταξύ των εμπλεκομένων. Το γεγονός ότι υπάρχει αυτό το πλαίσιο ασφάλειας, εξυπηρετεί ουσιαστικά στην ανάπτυξη μιας σχέσης εμπιστοσύνης του οργανισμού με τους πελάτες και τους συνεργάτες του.

Μια πολιτική (policy) είναι μια τυπική, σύντομη και υψηλού επιπέδου δήλωση, που εκφράζει τις γενικές πεποιθήσεις, τους σκοπούς, τους στόχους και τις αποδεκτές διαδικασίες ενός οργανισμού σε μια

συγκεκριμένη θεματική περιοχή. Οι πολιτικές δεν ορίζουν ρητά τον τρόπο επίτευξης των στόχων, παρά μόνο ορίζουν τους στόχους. Για το λόγο αυτό, μια πολιτική συνοδεύεται από κανόνες και οδηγίες. Για έναν οργανισμό, η συμμόρφωση στην πολιτική είναι υποχρεωτική, ενώ η μη-συμμόρφωση αποτελεί πειθαρχικό παράπτωμα.

Στον επιχειρηματικό κόσμο συναντώνται διάφορα είδη πολιτικών ασφάλειας πληροφοριών. Στο υψηλότερο επίπεδο αφαίρεσης ανήκει η οργανωσιακή πολιτική ασφάλειας πληροφοριών, η οποία συνήθως περιέχει:

- Στόχους και σχέδια του οργανισμού σε σχέση με την ασφάλεια πληροφοριών.
- Ρόλους και καθήκοντα εμπλεκομένων.
- Ρητή δήλωση υποστήριξης της Διοίκησης ως προς τη συμμόρφωση με την πολιτική.
- Δέσμευση της διοίκησης για ενεργό συμμετοχή.
- Πλάνο ελέγχων των διαδικασιών.
- Πλάνο παροχής κατάλληλης κατάρτισης του προσωπικού.

Ένα παράδειγμα αυτού του πρώτου επιπέδου πολιτικής συναντάμε στο διαδικτυακό τόπο του Ελληνικού Ανοιχτού Πανεπιστημίου (http://noc.eap.gr/index.php/home/kentriki-politiki-asfaleias-pol20), που παρατίθεται στην Εικόνα 11.3.

Κεντρική Πολιτική Ασφαλείας Πληροφοριών - ΠΟΛ 20

Η Διοίκηση του **Ε.Α.Π. δεσμεύεται**, για την εφαρμογή και την συνεχή βελτίωση της αποτελεσματικότητας του Συστήματος Διαχείρισης Ασφάλειας Πληροφοριών, καθώς και για την διάθεση όλων των οικονομικών, τεχνικών και ανθρώπινων πόρων που απαιτούνται για τη λειτουργία του μέσω της Ανασκόπησης από τη Διοίκηση σε ετήσια βάση.

Μέτρο της επιτυχίας της Κεντρικής Πολιτικής Ασφάλειας Πληροφοριών αλλά και των επιμέρους Πολιτικών Ασφαλείας, είναι η επίτευξη συγκεκριμένων στόχων και η εμφύσηση εμπιστοσύνης σε κάθε συναλλασσόμενο για την ακεραιότητα, και ασφάλεια πληροφοριών.

Για τους λόγους αυτούς το Ε.Α.Π.:
- Αναπτύσσει και εφαρμόζει Πολιτικές και Διαδικασίες, που εξειδικεύουν την Κεντρική Πολιτική και διασφαλίζουν την ακεραιότητα πληροφοριών από εσωτερικούς και εξωτερικούς κινδύνους.
- Εμπνέει εμπιστοσύνη σε κάθε συναλλασσόμενο πως ενεργεί σύμφωνα με επικυρωμένα διεθνή πρότυπα, νόμους και κανονισμούς, καθώς και συμβατικές απαιτήσεις για την ασφάλεια πληροφοριακών συστημάτων.
- Προστατεύει τα περιουσιακά του στοιχεία και πληροφορίες από απειλές (εσωτερικές και εξωτερικές) και κινδύνους.
- Διασφαλίζει την ασφαλή διατήρηση εμπιστευτικών πληροφοριών και διαφυλάττει τη μη εξουσιοδοτημένη πρόσβαση.
- Βελτιώνει συνεχώς το Σύστημα Διαχείρισης Ασφάλειας Πληροφοριών με τη δημιουργία και την τακτική αναθεώρηση των μετρήσιμων στόχων ασφάλειας.
- Εφαρμόζει διαδικασίες για τον εντοπισμό και αξιολόγηση κινδύνων και των επιπτώσεών τους σε προστατευόμενες πληροφορίες.
- Προβαίνει σε όλες τις απαραίτητες ενέργειες, ώστε να επικοινωνει την Κεντρική αλλά και τις επιμέρους Πολιτικές Ασφαλείας σε κάθε συναλλασσόμενο.

Το **Ε.Α.Π.** διασφαλίζει ότι όλο του το στελεχιακό δυναμικό, καθώς και οι φοιτητές και προμηθευτές του, είναι ενήμεροι για την Κεντρική Πολιτική Ασφάλειας Πληροφοριών και πως οι εφαρμόσιμες επιμέρους Πολιτικές είναι εύκολα προσβάσιμες. Όλοι οι συναλλασσόμενοι με το **Ε.Α.Π.** θα πρέπει να συμβουλεύονται τις Πολιτικές Ασφάλειας Πληροφοριών του Ιδρύματος για κάθε τους ενέργεια που μπορεί να επηρεάσει την ασφάλεια και ακεραιότητα του **Συστήματος Διαχείρισης Ασφάλειας Πληροφοριών (Σ.Δ.Α.Π.)** και των Πληροφοριακών Συστημάτων του Ελληνικού Ανοιχτού Πανεπιστημίου **(Ε.Α.Π.)**.

Εικόνα 11.3 *Παράδειγμα οργανωσιακής πολιτικής ασφάλειας πληροφοριών.*

Στο αμέσως χαμηλότερο (δεύτερο) επίπεδο αφαίρεσης, κάθε επιμέρους πολιτική ασφάλειας πληροφοριών στοχεύει σε συγκεκριμένες ομάδες ανθρώπων μέσα στον οργανισμό και καλύπτει συγκεκριμένες θεματικές περιοχές. Τέτοιου είδους θεματικές πολιτικές ασφάλειας μπορεί να είναι η πολιτική ελέγχου πρόσβασης, η πολιτική ασφάλειας επικοινωνιών, η πολιτική κρυπτογραφικών τεχνικών, η πολιτική χρήσης ηλεκτρονικού ταχυδρομείου κ.ά. Μια πολιτική αυτού του επιπέδου, συνήθως, αναφέρεται στο θέμα το οποίο αφορά, στους στόχους, στους όρους και στις προϋποθέσεις που θέτει, στις κατηγορίες υπαλλήλων στους οποίους απευθύνεται, στους ρόλους και στα καθήκοντα

11.6 Το πρότυπο ISO/IEC 17799

Ένας ενδεδειγμένος τρόπος για την αξιολόγηση των πολιτικών και τεχνικών ασφάλειας ενός οργανισμού, είναι αυτός που χρησιμοποιεί ως βάση τις «βέλτιστες πρακτικές» (best practices), που προτάθηκαν αρχικά (2000) με τη μορφή του διεθνώς αναγνωρισμένου προτύπου ISO/IEC 17799 (International Organization for Standardization / International Electrotechnical Commission). Το πρότυπο ISO/IEC 17799 αποτέλεσε τον απόγονο του προτύπου BS 7799 (British Standards Institution) και είχε γίνει αποδεκτό από πολλές εθνικές αρχές προτυποποίησης, συμπεριλαμβανομένου του ΕΛΟΤ για την Ελλάδα. Το 2005 ενημερώθηκε (ISO/IEC 17799:2005) και το 2007 μετονομάσθηκε σε ISO/IEC 27002, συμμετέχοντας σε μια οικογένεια προτύπων, γνωστών ως η σειρά προτύπων ISO/IEC 27000.

Σκοπός της υιοθέτησης του προτύπου ISO/IEC 17799 από έναν οργανισμό, είναι να καθορισθεί ένας κοινός άξονας μελέτης και αντιμετώπισης των προβλημάτων ασφάλειας που αφορούν το πληροφοριακό σύστημά του. Σημαντικό πλεονέκτημα μιας τέτοιας προσέγγισης αποτελεί το γεγονός ότι τα αποτελέσματα της σχετικής μελέτης μπορούν να αποτελέσουν τη βάση για μια συνεχή και συντονισμένη προσπάθεια συμμόρφωσης (compliance) των πρακτικών και διαδικασιών ασφάλειας του οργανισμού με τα διεθνή και ευρωπαϊκά πρότυπα, προς την κατεύθυνση μιας ολιστικής διαχείρισης της ασφάλειας του πληροφοριακού συστήματος του οργανισμού.

Το πρότυπο ISO/IEC 17799 παρέχει γενικές κατευθύνσεις για τη διαχείριση της ασφάλειας πληροφοριών, στα πλαίσια βέλτιστων πρακτικών. Επιπλέον, περιγράφει μια κοινή βάση για την ανάπτυξη ασφάλειας μέσα στον οργανισμό, την αποτελεσματική διαχείριση της ασφάλειας πληροφοριών και τη δημιουργία εμπιστοσύνης κατά την πραγματοποίηση συναλλαγών με άλλους οργανισμούς. Οι προτάσεις του προτύπου θα πρέπει να υιοθετούνται και να εφαρμόζονται πάντα σε συμφωνία με την υφιστάμενη εθνική νομοθεσία.

Το πρότυπο ISO/IEC 17799 περιλαμβάνει 11 κύρια άρθρα (clauses) που συνολικά περιέχουν 39 βασικές κατηγορίες ασφάλειας (security categories), πέραν του ενός εισαγωγικού άρθρου που αφορά την αποτίμηση και μεταχείριση επικινδυνότητας. Τα κύρια άρθρα είναι τα εξής (σε παρένθεση το πλήθος των βασικών κατηγοριών ασφάλειας που περιέχονται σε καθένα από αυτά):

- Πολιτική Ασφάλειας - Security Policy.
- Οργάνωση Ασφάλειας Πληροφοριών - Organizing Information Security.
- Διαχείριση Αγαθών - Asset Management.
- Ασφάλεια Ανθρώπινων Πόρων - Human Resources Security.
- Φυσική και Περιβαλλοντική Ασφάλεια - Physical and Environmental Security.
- Διαχείριση Επικοινωνιών και Λειτουργιών - Communications and Operations Management .
- Έλεγχος Προσπέλασης - Access Control.
- Προμήθεια, Ανάπτυξη και Συντήρηση Πληροφοριακών Συστημάτων - Information Systems Acquisition, Development and Maintenance.
- Διαχείριση Συμβάντων Ασφάλειας Πληροφοριών - Information Security Incident Management.
- Διαχείριση Επιχειρησιακής Συνέχειας - Business Continuity Management.
- Συμμόρφωση – Compliance.

Η σειρά παράθεσης των παραπάνω άρθρων δεν αφορά την σπουδαιότητά τους, ενώ είναι στην ευχέρεια του κάθε οργανισμού να επιλέξει μεταξύ αυτών. Κάθε βασική κατηγορία ασφάλειας περιέχει:

- Ένα στόχο (objective), που δηλώνει το τι επιδιώκεται.
- Ένα ή περισσότερα μέτρα προστασίας (controls), που θα πρέπει να εφαρμοστούν για την επίτευξη του στόχου.

Η δομή της περιγραφής κάθε τέτοιου μέτρου είναι η ακόλουθη:

- Μέτρο (Control): μια επιμέρους δήλωση για την επίτευξη του στόχου.
- Οδηγίες υλοποίησης (Implementation guidance): περισσότερο λεπτομερής πληροφόρηση για την υποστήριξη της υλοποίησης προς την επίτευξη του στόχου.
- Άλλες πληροφορίες (Other information): επιπλέον πληροφόρηση, που πιθανώς αφορά π.χ. νομικά θέματα ή αναφορά σε άλλα πρότυπα.

11.6.1 Πολιτική ασφάλειας

Στόχος της πολιτικής ασφάλειας (security policy) 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. Προτεινόμενα μέτρα:

- Έγγραφο της πολιτικής ασφάλειας πληροφοριών.
- Αναθεώρηση της πολιτικής ασφάλειας πληροφοριών.

11.6.2 Οργάνωση της ασφάλειας πληροφοριών

11.6.2.1 Εσωτερική οργάνωση

Στόχος είναι η διαχείριση της ασφάλειας πληροφοριών 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 ενθαρρυνθεί μια προσέγγιση που θα βασίζεται στη συνεργασία διαφορετικών ειδικοτήτων και ομάδων, όπως οι χρήστες, οι προμηθευτές, οι ειδικοί της ασφάλειας, καθώς και η ίδια η διοίκηση του οργανισμού. Προτεινόμενα μέτρα αποτελούν τα ακόλουθα:

- Δέσμευση της διοίκησης για ασφάλεια των πληροφοριών.
- Συντονισμός για θέματα ασφάλειας πληροφοριών.
- Κατανομή αρμοδιοτήτων για την ασφάλεια πληροφοριών.
- Διαδικασία εξουσιοδοτήσεων για τα μέσα επεξεργασίας πληροφοριών.
- Συμφωνίες εμπιστευτικότητας.
- Επικοινωνία με τις αρχές.
- Επικοινωνία με ομάδες ειδικών ενδιαφερόντων (special interest groups – SIG).
- Ανεξάρτητη επιθεώρηση της ασφάλειας πληροφοριών, π.χ. από κάποιον εξωτερικό σύμβουλο.

11.6.2.2 Εξωτερικά μέρη

Στόχος είναι η διαφύλαξη της ασφάλειας των μέσων επεξεργασίας πληροφοριών του οργανισμού, στα οποία έχουν προσπέλαση τρίτα μέρη. Η προσπέλαση από τρίτους στις εγκαταστάσεις του οργανισμού θα πρέπει να ελέγχεται. Όπου υπάρχει ανάγκη για τέτοιου είδους προσπέλαση θα πρέπει να διενεργείται αποτίμηση επικινδυνότητας προκειμένου να καθοριστούν οι επιπτώσεις στην ασφάλεια του οργανισμού και να εγκατασταθούν τα απαραίτητα μέτρα προστασίας. Για τα μέτρα προστασίας θα πρέπει να έχει ενημερωθεί και να συμφωνεί εγγράφως κάθε τρίτο μέρος. Επίσης, θα πρέπει να προβλεφθούν και οι διαδικασίες μεταβίβασης των δικαιωμάτων προσπέλασης από τρίτα μέρη σε άλλες οντότητες. Αυτή η αντιμετώπιση θα πρέπει να αποτελεί μια βάση εφαρμογής και σε περιπτώσεις που αφορούν την εξωτερική προμήθεια (outsourcing) υπηρεσιών επεξεργασίας πληροφοριών. Προτεινόμενα μέτρα αποτελούν τα ακόλουθα:

- Καθορισμός επικινδυνότητας λόγω προσπέλασης τρίτων μερών .
- Ικανοποίηση απαιτήσεων ασφάλειας κατά τις συναλλαγές με τρίτα μέρη.
- Ικανοποίηση απαιτήσεων ασφάλειας κατά τις συμφωνίες με τρίτα μέρη.

11.6.3 Διαχείριση αγαθών

11.6.3.1 Απόδοση ευθυνών για αγαθά

Στόχος είναι η επίτευξη και διατήρηση κατάλληλης προστασίας των αγαθών του οργανισμού. Όλα τα κύρια πληροφοριακά αγαθά του οργανισμού θα πρέπει να έχουν έναν καθορισμένο 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. Προτεινόμενα μέτρα αποτελούν τα ακόλουθα:

- Απογραφή των πόρων.
- Ιδιοκτησία των πόρων.
- Αποδεκτή χρήση των πόρων.

11.6.3.2 Διαβάθμιση πληροφοριών

Στόχος είναι να εξασφαλισθεί 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. Θα πρέπει να χρησιμοποιείται ένα σύστημα διαβάθμισης των πληροφοριών για τον καθορισμό των απαιτούμενων επιπέδων προστασίας, καθώς και για την επισήμανση τυχόν ανάγκης για ειδική μεταχείριση. Προτεινόμενα μέτρα αποτελούν τα ακόλουθα:

- Οδηγίες διαβάθμισης.
- Σήμανση και χειρισμός των πληροφοριών.

11.6.4 Ασφάλεια ανθρώπινων πόρων

11.6.4.1 Πριν την πρόσληψη

Στόχος είναι να εξασφαλισθεί ότι οι εργαζόμενοι, οι εργολάβοι και τα τρίτα μέρη κατανοούν τις ευθύνες τους και ότι είναι κατάλληλοι για τους ρόλους τους οποίους προορίζονται να αναλάβουν, καθώς επίσης και να ελαχιστοποιηθούν οι κίνδυνοι που μπορεί να προκληθούν από κλοπή, ανθρώπινο λάθος, 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 καταλάβουν ευαίσθητες θέσεις. Όλοι οι υπάλληλοι και οι συνεργάτες του οργανισμού θα πρέπει να υπογράφουν συμφωνητικό για τήρηση εχεμύθειας. Προτεινόμενα μέτρα αποτελούν τα ακόλουθα:

- Ρόλοι και ευθύνες.
- Διαδικασία επιλογής προσωπικού.
- Όροι και συνθήκες πρόσληψης.

11.6.4.2 Μετά την πρόσληψη

Στόχος είναι να εξασφαλισθεί ότι οι εργαζόμενοι, οι εργολάβοι και τα τρίτα μέρη είναι ευαισθητοποιημένοι για τους κινδύνους και τα ζητήματα που αφορούν την ασφάλεια των πληροφοριών του οργανισμού, για τις ευθύνες και τις υποχρεώσεις τους, καθώς και ότι διαθέτουν τα κατάλληλα εφόδια ώστε να υποστηρίξουν την πολιτική ασφάλειας του οργανισμού κατά τη διάρκεια της κανονικής τους εργασίας και να μειώσουν τους κινδύνους από ανθρώπινα σφάλματα. Οι ευθύνες της διοίκησης θα πρέπει να καθορίζονται ώστε να δια-σφαλίζεται ότι η ασφάλεια εφαρμόζεται σε όλο το εύρος των ανθρώπινων δραστηριοτήτων μέσα στον οργανισμό.

Θα πρέπει να παρέχεται προς όλους τους εργαζόμενους, τους εργολάβους και τους χρήστες από τρίτα μέρη ένα επαρκές επίπεδο ευαισθητοποίησης, εκπαίδευσης και κατάρτισης πάνω στις διαδικασίες ασφάλειας και τη σωστή χρήση των μέσων επεξεργασίας πληροφοριών ώστε να ελαχιστοποιούνται οι πιθανοί κίνδυνοι για την ασφάλεια. Ακόμη, θα πρέπει να εφαρμόζεται μια αυστηρά καθορισμένη πειθαρχική διαδικασία για το χειρισμό των ρηγμάτων ασφάλειας. Προτεινόμενα μέτρα αποτελούν τα ακόλουθα:

- Υποχρεώσεις της διοίκησης.
- Ευαισθητοποίηση, εκπαίδευση και κατάρτιση πάνω στην ασφάλεια πληροφοριών.
- Πειθαρχική διαδικασία.

11.6.4.3 Τερματισμός ή αλλαγή απασχόλησης

Στόχος είναι να εξασφαλισθεί ότι οι εργαζόμενοι, οι εργολάβοι και τα τρίτα μέρη αποχωρούν ή αλλάζουν απασχόληση με έναν προβλεπόμενο τρόπο. Θα πρέπει να έχουν κατανεμηθεί οι αρμοδιότητες για να εξασφαλισθεί ότι η λύση της σύμβασης ενός εργαζόμενου ή ενός χρήστη τρίτου μέρους είναι υπό έλεγχο και ότι η επιστροφή του εξοπλισμού, καθώς και η αφαίρεση των όποιων δικαιωμάτων πρόσβαση ολοκληρώνεται. Οι αλλαγές στις υποχρεώσεις και την απασχόληση μέσα στον οργανισμό θα πρέπει να ελέγχονται παρομοίως. Προτεινόμενα μέτρα αποτελούν τα ακόλουθα:

- Αρμοδιότητες για την περίπτωση τερματισμού απασχόλησης.
- Επιστροφή αγαθών.
- Αφαίρεση δικαιωμάτων πρόσβασης.

11.6.5 Φυσική και περιβαλλοντική ασφάλεια

11.6.5.1 Ασφαλείς περιοχές

Στόχος είναι η αποτροπή μη-εξουσιοδοτημένης φυσικής πρόσβασης, ζημιάς και παρέμβασης στις εγκαταστάσεις και το πληροφοριακό σύστημα του οργανισμού. Οι κρίσιμής 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. Προτεινόμενα μέτρα αποτελούν τα ακόλουθα:

- Περίμετρος φυσικής ασφάλειας.
- Μέτρα ελέγχου φυσικής πρόσβασης.
- Ασφάλεια γραφείων, δωματίων και μέσων.
- Προστασία από εξωτερικούς και περιβαλλοντικούς κινδύνους.
- Εργασία σε ασφαλείς περιοχές.
- Περιοχές φορτοεκφόρτωσης και δημόσιας πρόσβασης.

11.6.5.2 Ασφάλεια εξοπλισμού

Στόχος είναι η πρόληψη απώλειας, ζημιών, κλοπής ή διακύβευσης των αγαθών του οργανισμού και της διακοπής των επιχειρησιακών δραστηριοτήτων του. 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. Προτεινόμενα μέτρα:

- Τοποθέτηση και προστασία εξοπλισμού.
- Μέσα υποστήριξης.
- Ασφάλεια καλωδίωσης.
- Συντήρηση εξοπλισμού.
- Ασφάλεια εξοπλισμού εκτός των χώρων του οργανισμού.
- Ασφαλής καταστροφή ή επαναχρησιμοποίηση εξοπλισμού.
- Μετακίνηση αγαθών εκτός των χώρων του οργανισμού.

11.6.6 Διαχείριση επικοινωνιών και λειτουργιών

11.6.6.1 Λειτουργικές διαδικασίες και καθήκοντα

Στόχος 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 λειτουργικές οδηγίες και διαδικασίες αντιμετώπισης συμβάντων που απειλούν την ασφάλεια του συστήματος.

Θα πρέπει να εφαρμόζεται ο διαχωρισμός των καθηκόντων, όπου αυτό είναι δυνατό, ώστε να ελαχιστοποιηθεί ο κίνδυνος κακής χρήσης του συστήματος, είτε από αμέλεια είτε από δόλο. Προτεινόμενα μέτρα:

- Τεκμηριωμένες λειτουργικές διαδικασίες.
- Διαχείριση αλλαγών.
- Διαχωρισμός καθηκόντων.
- Διαχωρισμός μεταξύ των μέσων ανάπτυξης, δοκιμής και λειτουργίας.

11.6.6.2 Διαχείριση παροχής υπηρεσιών από τρίτα μέρη

Στόχος είναι η υλοποίηση και συντήρηση ενός κατάλληλου επιπέδου ασφάλειας κατά την παροχή υπηρεσιών στο πλαίσιο συμφωνιών με τρίτα μέρη.

Ο οργανισμός θα πρέπει να ελέγχει την υλοποίηση των συμφωνιών, να επιβλέπει τη συμμόρφωση με τα συμφωνηθέντα και να διαχειρίζεται κατάλληλα τις αλλαγές ώστε να εξασφαλίζεται ότι κατά την παροχή των υπηρεσιών ικανοποιούνται όλες οι απαιτήσεις που έχουν συμφωνηθεί με τα τρίτα μέρη. Προτεινόμενα μέτρα:

- Διαδικασίες παροχής υπηρεσιών.

- Επίβλεψη και αξιολόγηση των υπηρεσιών από τρίτα μέρη.
- Διαχείριση αλλαγών των υπηρεσιών από τρίτα μέρη.

11.6.6.3 Σχεδιασμός και αποδοχή συστήματος

Στόχος είναι η ελαχιστοποίηση των κινδύνων για βλάβες του συστήματος. Ο προσεκτικός σχεδιασμός και η κατάλληλη προετοιμασία, είναι απαραίτητα στοιχεία για τη διαθεσιμότητα πόρων και χωρητικότητας του πληροφοριακού συστήματος 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. Προτεινόμενα μέτρα:

- Διαχείριση δυνατοτήτων υπαρχόντων και μελλοντικών πόρων
- Αποδοχή συστήματος

11.6.6.4 Προστασία από κακόβουλο λογισμικό

Στόχος είναι η προστασία της ακεραιότητας του λογισμικού και των πληροφοριών. Χρειάζονται προληπτικά μέτρα για τον εντοπισμό και την προστασία του πληροφοριακού συστήματος από κακόβουλο λογισμικό και μη-εξουσιοδοτημένο κινητό κώδικα. Το λογισμικό και τα μέσα επεξεργασίας πληροφοριών είναι ευάλωτα σε εισβολές κακόβουλου κώδικα, όπως ιοί, σκουλήκια, Δούρειοι Ίπποι και λογικές βόμβες.

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 κώδικα. Προτεινόμενα μέτρα:

- Μέτρα προστασίας από κακόβουλο λογισμικό.

- Μέτρα προστασίας από κινητό κώδικα.

11.6.6.5 Λήψη εφεδρικού αντιγράφου ασφαλείας

Στόχος είναι η διατήρηση της ακεραιότητας και της διαθεσιμότητας των πληροφοριών και των μέσων επεξεργασίας. Θα πρέπει να υπάρχουν διαδικασίες ρουτίνας για την καθημερινή λήψη εφεδρικών αντιγράφων του συστήματος και τη διασφάλιση της επαναφοράς τους όποτε χρειαστεί. Προτεινόμενο μέτρο:

- Λήψη εφεδρικού αντιγράφου ασφαλείας των πληροφοριών.

11.6.6.6 Διαχείριση ασφάλειας δικτύου

Στόχος 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 δεν αποστέλλονται ευαίσθητα δεδομένα διαμέσου δημόσιων δικτύων. Προτεινόμενα μέτρα:

- Μέτρα προστασίας δικτύου.
- Ασφάλεια των δικτυακών υπηρεσιών.

11.6.6.7 Χειρισμός αποθηκευτικών μέσων

Στόχος 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. Προτεινόμενα μέτρα:

- Διαχείριση αποσπώμενων αποθηκευτικών μέσων.
- Απόσυρση αποθηκευτικών μέσων.
- Διαδικασίες χειρισμού πληροφοριών.
- Ασφάλεια τεκμηρίωσης συστήματος.

11.6.6.8 Ανταλλαγή πληροφοριών

Στόχος είναι η προστασία των πληροφοριών και του λογισμικού που ανταλλάσσονται μεταξύ του οργανισμού και μιας εξωτερικής οντότητας. Η ανταλλαγή πληροφοριών και εφαρμογών μεταξύ των οργανισμών θα πρέπει να βασίζεται σε μια αυστηρή πολιτική ανταλλαγών και να είναι σύμφωνη με τη σχετική νομοθεσία. Θα πρέπει να εφαρμόζονται διαδικασίες και πρότυπα για την προστασία των πληροφοριών και των φυσικών μέσων που περιέχουν πληροφορίες. Προτεινόμενα μέτρα:

- Διαδικασίες και πολιτικές ανταλλαγής πληροφοριών.
- Συμφωνίες ανταλλαγών.
- Ασφάλεια αποθηκευτικών μέσων κατά τη μεταφορά τους.
- Χρήση ηλεκτρονικού ταχυδρομείου.
- Επιχειρησιακά πληροφοριακά συστήματα.

11.6.6.9 Υπηρεσίες ηλεκτρονικού εμπορίου

Στόχος είναι να εξασφαλισθεί η ασφάλεια των υπηρεσιών ηλεκτρονικού εμπορίου και της χρήσης τους. Θα πρέπει να θεωρηθούν οι επιπτώσεις στην ασφάλεια, που σχετίζονται με τη χρήση των υπηρεσιών ηλεκτρονικού εμπορίου περιλαμβανομένων των άμεσων δοσοληψιών (online transactions) και των απαιτήσεων για μέτρα προστασίας. Θα πρέπει ακόμη να εξεταστεί η ακεραιότητα και η διαθεσιμότητα των ηλεκτρονικά δημοσιευόμενων πληροφοριών μέσω συστημάτων που είναι διαθέσιμα στο κοινό. Προτεινόμενα μέτρα:

- Διαδικασίες παροχής υπηρεσιών ηλεκτρονικού εμπορίου.
- Έλεγχος πρόσβασης στις δοσοληψίες,
- Έλεγχος πληροφοριών που είναι διαθέσιμες στο κοινό.

11.6.6.10 Επίβλεψη

Στόχος είναι να ανιχνευθούν δραστηριότητες μη εξουσιοδοτημένης επεξεργασίας πληροφοριών. Θα πρέπει να επιβλέπονται τα συστήματα και να καταγράφονται τα συμβάντα που αφορούν την ασφάλεια των πληροφοριών. Θα πρέπει να χρησιμοποιούνται καταγραφές λειτουργίας και σφαλμάτων για να εξασφαλισθεί ότι προσδιορίζονται τα προβλήματα που αντιμετωπίζουν τα πληροφοριακά συστήματα. Ο οργανισμός θα πρέπει να συμμορφώνεται με όλες τις εκ του νόμου απαιτήσεις που αφορούν τις ενέργειες επίβλεψης και καταγραφής. Η επίβλεψη των συστημάτων θα πρέπει να χρησιμοποιείται για να ελέγχεται η αποδοτικότητα των υιοθετημένων μέτρων και για να επιβεβαιώνεται η συμβατότητα με κάποιο μοντέλο πολιτικής πρόσβασης. Προτεινόμενα μέτρα:

- Καταγραφές ελέγχου.
- Επίβλεψη της χρήσης των συστημάτων.
- Προστασία των καταγεγραμμένων πληροφοριών.
- Καταγραφές διαχείρισης και λειτουργίας.
- Καταγραφές σφαλμάτων.
- Συγχρονισμός ρολογιών.

11.6.7 Έλεγχος πρόσβασης

11.6.7.1 Επιχειρησιακές απαιτήσεις για έλεγχο πρόσβασης

Στόχος είναι ο έλεγχος της πρόσβασης στις πληροφορίες του οργανισμού. Η πρόσβαση σε πληροφορίες και επιχειρησιακές διεργασίες θα πρέπει να ελέγχεται με βάση τις επιχειρησιακές ανάγκες και της απαιτήσεις ασφάλειας του οργανισμού, λαμβάνοντας υπόψη τις πολιτικές διάχυσης των πληροφοριών και των σχετικών εξουσιοδοτήσεων. Προτεινόμενο μέτρο:

- Πολιτική ελέγχου πρόσβασης

11.6.7.2 Διαχείριση πρόσβασης χρηστών

Στόχος είναι να εξασφαλισθεί η προσπέλαση από εξουσιοδοτημένους χρήστες και να προληφθεί η μη-εξουσιοδοτημένη πρόσβαση στα πληροφοριακά συστήματα. Θα πρέπει να υπάρχουν αυστηρές διαδικασίες για τον έλεγχο της πρόσβασης των χρηστών στα διάφορα πληροφοριακά συστήματα και τις υπηρεσίες. 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 μπορούν να παρακάμψουν τους μηχανισμούς ασφάλειας του συστήματος. Προτεινόμενα μέτρα:

- Διαδικασία εγγραφής χρηστών.
- Διαχείριση προνομίων χρηστών.
- Διαχείριση διαπιστευτηρίων (credentials) των χρηστών.
- Επιθεώρηση προνομίων των χρηστών.

11.6.7.3 Ευθύνες χρηστών

Στόχος είναι η αποτροπή της μη-εξουσιοδοτημένης πρόσβασης χρηστών στο σύστημα και η διακύβευση των πληροφοριών και των μέσων αποθήκευσης, διακίνησης και επεξεργασίας τους. Η συνεργασία των εξουσιοδοτημένων χρηστών του συστήματος είναι απαραίτητη για τη γενικότερη ασφάλειά του. Οι χρήστες θα πρέπει να είναι ενήμεροι για τις ευθύνες τους, σχετικά με τους χρησιμοποιούμενους μηχανισμούς ασφάλειας, ειδικότερα για τη χρήση διαπιστευτηρίων (π.χ. συνθηματικών) και την ασφάλεια του εξοπλισμού. Θα πρέπει να υλοποιηθεί μια πολιτική «καθαρού γραφείου» και «καθαρής οθόνης», ώστε να μειωθούν οι κίνδυνοι για καταστροφή εγγράφων, αποθηκευτικών μέσων και μέσων επεξεργασίας πληροφοριών. Προτεινόμενα μέτρα:

- Διαδικασία χρήσης διαπιστευτηρίων.
- Καταγραφή εξοπλισμού που δεν επιβλέπεται.
- Πολιτική καθαρού γραφείου και καθαρής οθόνης.

11.6.7.4 Έλεγχος πρόσβασης δικτύου

Στόχος είναι η αποτροπή μη-εξουσιοδοτημένης πρόσβασης στις δικτυακές υπηρεσίες. Η πρόσβαση 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. Για αυτό θα πρέπει να εξασφαλισθεί ότι:

- Υπάρχουν οι κατάλληλες διεπαφές (interfaces) μεταξύ του δικτύου του οργανισμού και των δικτύων άλλων οργανισμών ή δημόσιων δικτύων.

- Υπάρχουν κατάλληλοι μμηχανισμοί αυθεντικοποίησης χρηστών και εξοπλισμού.

- Επιβάλλεται ελεγχόμενη πρόσβαση των χρηστών στις προσφερόμενες υπηρεσίες.

Προτεινόμενα μέτρα:

- Πολιτική χρήσης των δικτυακών υπηρεσιών.
- Αυθεντικοποίηση χρηστών για εξωτερικές συνδέσεις.
- Διαδικασία αναγνώρισης δικτυακού εξοπλισμού.
- Προστασία θυρών απομακρυσμένης διάγνωσης και διαμόρφωσης.
- Διαχωρισμός μεταξύ δικτύων.
- Έλεγχος δικτυακών συνδέσεων.
- Έλεγχος δρομολόγησης δικτύου.

11.6.7.5 Έλεγχος πρόσβασης σε λειτουργικά συστήματα

Στόχος είναι η αποτροπή μη-εξουσιοδοτημένης πρόσβασης σε λειτουργικά συστήματα. Θα πρέπει να χρησιμοποιούνται μέσα ασφάλειας για τον περιορισμό της άμεσης πρόσβασης (π.χ. στη γραμμή εντολών) του λειτουργικού συστήματος σε εξουσιοδοτημένους χρήστες. Αυτά τα μέσα θα πρέπει να είναι σε θέση να:

- Αυθεντικοποιούν τους εξουσιοδοτημένους χρήστες, με βάση την καθορισμένη πολιτική ελέγχου πρόσβασης.

- Καταγράφουν τις επιτυχείς και τις ανεπιτυχείς προσπάθειες αυθεντικοποίησης από το σύστημα.

- Καταγράφουν τη χρήση των ειδικών προνομίων συστήματος.

- Ενεργοποιούν συναγερμούς όταν παραβιάζονται οι πολιτικές ασφάλειας συστήματος.

- Παρέχουν κατάλληλα μέσα αυθεντικοποίησης.

- Περιορίζουν τους χρόνους και τόπους σύνδεσης των χρηστών, όπου αυτό κρίνεται απαραίτητο.

Προτεινόμενα μέτρα:

- Διαδικασίες ασφαλούς σύνδεσης στο σύστημα.
- Αναγνώριση και αυθεντικοποίηση χρηστών.
- Σύστημα διαχείρισης συνθηματικών.
- Χρήση εργαλείων συστήματος.
- Περιορισμός χρόνου και τόπου σύνδεσης.

11.6.7.6 Έλεγχος πρόσβασης σε πληροφορίες και εφαρμογές

Σκοπός είναι η αποτροπή της μη-εξουσιοδοτημένης πρόσβασης στις πληροφορίες που χρησιμοποιούνται από τις διάφορες εφαρμογές. Θα πρέπει να χρησιμοποιούνται ειδικά μέσα ασφάλειας για τον περιορισμό της πρόσβασης στις εφαρμογές. Η λογική πρόσβαση σε λογισμικό και πληροφορίες εφαρμογών θα πρέπει να περιορίζεται μόνο στους εξουσιοδοτημένους χρήστες. Οι εφαρμογές θα πρέπει να:

- ελέγχουν την πρόσβαση των χρηστών σε διάφορες πληροφορίες και λειτουργίες των εφαρμογών, σύμφωνα με την καθορισμένη πολιτική ελέγχου πρόσβασης του οργανισμού,

- παρέχουν προστασία από μη-εξουσιοδοτημένη προσπέλαση μέσω οποιασδήποτε υπηρεσίας, λογισμικού λειτουργικού συστήματος και κακόβουλου λογισμικού, που είναι ικανά να παρακάμψουν τα μέτρα προστασίας του συστήματος,

- μην διακυβεύουν την ασφάλεια άλλων συστημάτων, με τα οποία διαμοιράζονται πόρους.

Προτεινόμενα μέτρα:

- Περιορισμός προσπέλασης πληροφοριών.

- Απομόνωση ευαίσθητων συστημάτων.

11.6.7.7 Τηλεργασία και κινητή υπολογιστική

Σκοπός είναι η εξασφάλιση της ασφάλειας των πληροφοριών, όταν χρησιμοποιούνται μέσα κινητής υπολογιστικής και τηλεργασίας. Η απαιτούμενη προστασία θα πρέπει να είναι ανάλογη των κινδύνων που εισάγουν αυτοί οι τρόποι εργασίας. Στην περίπτωση της κινητής υπολογιστικής θα πρέπει να εξεταστούν οι κίνδυνοι λόγω εργασίας σε ένα απροστάτευτο περιβάλλον και να εφαρμοσθούν κατάλληλα μέτρα προστασίας. Στην περίπτωση της τηλεργασίας, ο οργανισμός θα πρέπει να εφαρμόσει κατάλληλα μέτρα προστασίας στην τοποθεσία από την όποια θα γίνεται τηλεργασία και να εξασφαλίσει ότι έχουν γίνει οι κατάλληλες διευθετήσεις για αυτό τον τρόπο εργασίας. Προτεινόμενα μέτρα:

- Διαδικασία κινητής υπολογιστική
- Μέτρα προστασίας των επικοινωνιών.
- Διαδικασία τηλεργασίας.

11.6.8 Προμήθεια, ανάπτυξη και συντήρηση πληροφοριακών συστημάτων

11.6.8.1 Απαιτήσεις ασφάλειας πληροφοριακών συστημάτων

Η ασφάλεια αποτελεί αναπόσπαστο μέρος των πληροφοριακών συστημάτων. Τα πληροφοριακά συστήματα περιλαμβάνουν τα λειτουργικά συστήματα, την υποδομή, τις επιχειρησιακές εφαρμογές, τα πακέτα εφαρμογών (off-the-shelf), τις υπηρεσίες και τις εφαρμογές που αναπτύσσουν οι χρήστες. Ο σχεδιασμός και η υλοποίηση των επιχειρησιακών διεργασιών που υποστηρίζουν τις εφαρμογές ή τις υπηρεσίες του οργανισμού μπορεί να είναι ιδιαίτερα σημαντικό ζήτημα για την ασφάλεια. Οι απαιτήσεις ασφάλειας θα πρέπει να καθορίζονται και να συμφωνούνται πριν από την ανάπτυξη και την υλοποίηση των πληροφοριακών συστημάτων. Όλες οι απαιτήσεις ασφάλειας θα πρέπει να προσδιορίζονται κατά τη φάση καθορισμού των απαιτήσεων στο πλαίσιο ενός έργου, ενώ θα πρέπει επίσης να προσαρμόζονται, να συμφωνούνται και να τεκμηριώνονται στο πλαίσιο του συνολικού επιχειρησιακού σχεδίου που αφορά το πληροφοριακό σύστημα. Προτεινόμενα μέτρο:

- Ανάλυση και προδιαγραφή απαιτήσεων ασφάλειας.

11.6.8.2 Ορθή επεξεργασία από τις εφαρμογές

Σκοπός είναι η πρόληψη λαθών, απώλειας ή μη-εξουσιοδοτημένης μετατροπής των δεδομένων από τις εφαρμογές. θα πρέπει να σχεδιάζονται κατάλληλοι μηχανισμοί καταγραφής των ενεργειών στις εφαρμογές, προκειμένου να διασφαλίζεται η ορθότητα της επεξεργασίας. Θα πρέπει επίσης να περιλαμβάνουν τον έλεγχο της εγκυρότητας των προς εισαγωγή δεδομένων, την εσωτερική επεξεργασία τους. καθώς και τον έλεγχο των δεδομένων εξόδου. Επιπρόσθετα μέτρα προστασίας πιθανόν να απαιτούνται για συστήματα που επεξεργάζονται, ή προκαλούν επιπτώσεις σε ευαίσθητες ή κρίσιμες πληροφορίες. Η λήψη αυτών των μέτρων θα πρέπει να αποφασίζεται με βάση τις απαιτήσεις ασφάλειας και την εκτίμηση της επικινδυνότητας. Προτεινόμενα μέτρα:

- Επικύρωση εισαγόμενων δεδομένων.
- Έλεγχος εσωτερικής επεξεργασίας.
- Ακεραιότητα μηνυμάτων.
- Επικύρωση εξαγόμενων δεδομένων.

11.6.8.3 Κρυπτογραφικά μέτρα προστασίας

Σκοπός είναι η προστασία της εμπιστευτικότητας, της ακεραιότητας και της αυθεντικότητας των πληροφοριών με κρυπτογραφικά μέσα. Για το σκοπό αυτό θα πρέπει να αναπτυχθεί μια πολιτική χρήσης κρυπτογραφικών μέτρων προστασίας. Ακόμη, θα πρέπει να εφαρμόζονται κατάλληλες διαδικασίες διαχείρισης κλειδιών για την υποστήριξη των διάφορων κρυπτογραφικών τεχνικών. Προτεινόμενα μέτρα:

- Πολιτική χρήσης των κρυπτογραφικών μέτρων προστασίας.
- Διαχείριση κλειδιών.

11.6.8.4 Ασφάλεια αρχείων συστήματος

Σκοπός είναι η εξασφάλιση της ασφάλειας των αρχείων συστήματος. Θα πρέπει να ελέγχεται η πρόσβαση στα αρχεία του συστήματος και στον πηγαίο κώδικα των προγραμμάτων, ενώ οι δραστηριότητες διενέργειας και υποστήριξης έργων πληροφορικής θα πρέπει να πραγματοποιούνται με ασφαλή τρόπο. Θα πρέπει επίσης να υπάρχει φροντίδα για την αποφυγή έκθεσης ευαίσθητων δεδομένων σε περιβάλλοντα δοκιμών. Προτεινόμενα μέτρα:

- Έλεγχος λογισμικού συστήματος.
- Προστασία των δεδομένων δοκιμών των συστημάτων.
- Έλεγχος πρόσβασης στον πηγαίο κώδικα προγραμμάτων.

11.6.8.5 Ασφάλεια στις διαδικασίες ανάπτυξης και υποστήριξης

Σκοπός είναι η διαφύλαξη της ασφάλειας του λογισμικού και των πληροφοριών των συστημάτων εφαρμογών. Τα περιβάλλοντα ανάπτυξης και υποστήριξης θα πρέπει να είναι αυστηρά ελεγχόμενα. Οι υπεύθυνοι για τα συστήματα εφαρμογών θα πρέπει να είναι υπεύθυνοι και για την ασφάλεια των περιβαλλόντων ανάπτυξης και υποστήριξής τους. Θα πρέπει να διασφαλίσουν ότι οποιαδήποτε αλλαγή στο σύστημα ελέγχεται πριν πραγματοποιηθεί και ότι δεν έχει αρνητικές επιπτώσεις στην ασφάλεια είτε του συστήματος είτε του λειτουργικού περιβάλλοντος. Προτεινόμενα μέτρα:

- Διαδικασίες ελέγχου αλλαγών.
- Τεχνική επιθεώρηση των εφαρμογών μετά από αλλαγές στο λειτουργικό σύστημα.
- Περιορισμοί στις αλλαγές των πακέτων λογισμικού.
- Διαρροή πληροφοριών.
- Ανάπτυξη λογισμικού από τρίτους (outsourced).

11.6.8.6 Διαχείριση τεχνικών ευπαθειών

Σκοπός είναι η μείωση της επικινδυνότητας που απορρέει από την αξιοποίηση δημοσίως γνωστών τεχνικών ευπαθειών. Η διαχείριση τεχνικών ευπαθειών θα πρέπει να υλοποιείται με τρόπο αποτελεσματικό, συστηματικό και επαναλαμβανόμενο, καθώς και με μετρήσεις που λαμβάνονται προκειμένου να επιβεβαιώνεται η

αποτελεσματικότητά της. Τα παραπάνω θα πρέπει να αφορούν τα λειτουργικά συστήματα και κάθε άλλη εφαρμογή σε χρήση. Προτεινόμενο μέτρο:

- Έλεγχος τεχνικών ευπαθειών

11.6.9 Συμβάντα ασφάλειας

11.6.9.1 Αναφορά συμβάντων και ευπαθειών ασφάλειας

Σκοπός είναι η διασφάλιση του ότι τα συμβάντα και οι ευπάθειες ασφάλειας πληροφοριών γνωστοποιούνται με τρόπο που επιτρέπει την έγκαιρη λήψη κατάλληλων ενεργειών. Για αυτό, θα πρέπει να έχουν καθορισθεί και εφαρμοσθεί επίσημες διαδικασίες αναφοράς συμβάντων και κλιμάκωσης ενεργειών. Όλοι οι εργαζόμενοι, οι συμβαλλόμενοι και οι χρήστες τρίτων μερών θα πρέπει να προσδίδουν την απαραίτητη προσοχή στις διαδικασίες αναφοράς διαφόρων τύπων συμβάντων και ευπαθειών που πιθανώς να έχουν επίπτωση στην ασφάλεια των αγαθών του οργανισμού. Επιπλέον, θα πρέπει να είναι υποχρεωμένοι να αναφέρουν οποιαδήποτε συμβάντα και ευπάθειες για την ασφάλεια πληροφοριών το συντομότερο δυνατόν στο προκαθορισμένο σημείο επικοινωνίας. Προτεινόμενα μέτρα:

- Αναφορά συμβάντων ασφάλειας.
- Αναφορά ευπαθειών ασφάλειας.

11.6.9.2 Διαχείριση συμβάντων ασφάλειας

Σκοπός είναι η διασφάλιση της εφαρμογής μιας συνεπούς και αποτελεσματικής προσέγγισης για τη διαχείριση των συμβάντων ασφάλειας πληροφοριών. Θα πρέπει να έχουν καθορισθεί και να εφαρμόζονται κατάλληλες αρμοδιότητες και διαδικασίες διαχείρισης συμβάντων ασφάλειας πληροφοριών, κατά τρόπο αποτελεσματικό, από τη στιγμή της αναφοράς τους. Θα πρέπει να εφαρμόζεται μια διαδικασία συνεχούς βελτίωσης ως αποτέλεσμα της επιθεώρησης, εκτίμησης και συνολικής διαχείρισης των συμβάντων ασφάλειας πληροφοριών. Όπου απαιτείται, θα πρέπει να συλλέγονται αποδείξεις για να διασφαλίζεται η συμμόρφωση με τις απαιτήσεις του νόμου. Προτεινόμενα μέτρα:

- Αρμοδιότητες και διαδικασίες.
- Μαθαίνοντας από τα συμβάντα ασφάλειας πληροφοριών.
- Συλλογή αποδείξεων (forensics).

11.6.10 Διαχείριση επιχειρησιακής συνέχειας

Σκοπός είναι η αντίδραση σε περίπτωση διακοπών στις επιχειρησιακές δραστηριότητες του οργανισμού και η προστασία των κρίσιμων διαδικασιών από τις επιπτώσεις σημαντικών αστοχιών των πληροφοριακών συστημάτων ή καταστροφών και η διασφάλιση της έγκαιρης ανάκτησής τους.

Θα πρέπει να έχει υλοποιηθεί μια διαδικασία διαχείρισης της επιχειρησιακής συνέχειας (business continuity management) του οργανισμού προκειμένου να μειωθούν οι επιπτώσεις στον οργανισμό και να ανακτηθούν τα απολεσθέντα αγαθά του οργανισμού (π.χ. ως αποτέλεσμα φυσικών καταστροφών, δυστυχημάτων, αστοχιών εξοπλισμού και εσκεμμένων πράξεων) σε ένα ανεκτό επίπεδο, μέσω συνδυασμένων μέτρων πρόληψης και ανάκτησης. Σε αυτή τη διαδικασία θα πρέπει να ορίζονται οι κρίσιμες επιχειρησιακές διαδικασίες και να ενοποιούνται οι απαιτήσεις διαχείρισης ασφάλειας πληροφοριών με άλλες απαιτήσεις συνέχειας που αφορούν λειτουργίες, προσωπικό, υλικά, μεταφορές και υπηρεσίες.

Οι συνέπειες των καταστροφών, αστοχιών ασφάλειας, απωλειών υπηρεσιών και διαθεσιμότητας υπηρεσιών θα πρέπει να γίνουν αντικείμενο μιας ανάλυσης επιχειρησιακών επιπτώσεων (business impact analysis – BIA). Ακόμη, θα πρέπει να αναπτυχθούν και να υλοποιηθούν σχέδια επιχειρησιακής συνέχειας (business continuity plans) προκειμένου να διασφαλισθεί η έγκαιρη ανάκτηση των βασικών λειτουργιών. Η

ασφάλεια πληροφοριών θα πρέπει να αποτελεί αναπόσπαστο μέρος της συνολικής διαδικασίας επιχειρησιακής συνέχειας, καθώς και άλλων διαδικασιών διαχείρισης μέσα στον οργανισμό. Η διαχείριση της επιχειρησιακής συνέχειας θα πρέπει να περιλαμβάνει μέτρα για τον καθορισμό και τη μείωση επικινδυνότητας, πέραν της γενικής διαδικασίας εκτίμησης επικινδυνότητας, για τον περιορισμό των συνεπειών από καταστροφικά συμβάντα και για τη διασφάλιση της άμεσης διαθεσιμότητας των πληροφοριών που είναι απαραίτητες για τις επιχειρησιακές λειτουργίες. Προτεινόμενα μέτρα:

- Εισαγωγή της ασφάλειας πληροφοριών στη διαδικασία διαχείρισης επιχειρησιακής συνέχειας.
- Σχεδιασμός επιχειρησιακής συνέχειας και εκτίμηση επικινδυνότητας.
- Υλοποίηση σχεδίων επιχειρησιακής συνέχειας σε συνδυασμό με τη διαχείριση ασφάλειας των πληροφοριών.
- Δοκιμή, συντήρηση και επανεκτίμηση των σχεδίων επιχειρησιακής συνέχειας.

11.6.11 Συμμόρφωση

11.6.11.1 Συμμόρφωση με τις απαιτήσεις του νόμου

Σκοπός είναι η αποφυγή παραβιάσεων οποιουδήποτε νόμου, ρυθμίσεων, κανονισμών ή συμβατικών υποχρεώσεων, καθώς και κάθε είδους απαιτήσεων ασφάλειας. Ο σχεδιασμός, η λειτουργία, η χρήση και η διαχείριση πληροφοριακών συστημάτων είναι πιθανό να υπόκειται σε κάποιας μορφής νόμους, ρυθμίσεις, κανονισμούς ή συμβατικές υποχρεώσεις ασφάλειας. Το νομικό τμήμα του οργανισμού θα πρέπει να παρέχει συμβουλές 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). Προτεινόμενα μέτρα:

- Καθορισμός της εφαρμοζόμενης νομοθεσίας.
- Δικαιώματα πνευματικής ιδιοκτησίας.
- Προστασία των αρχείων δεδομένων του οργανισμού.
- Προστασία του απόρρητου των προσωπικών πληροφοριών.
- Πρόληψη κακής χρήσης των μέσων αποθήκευσης, διακίνησης και επεξεργασίας πληροφοριών.
- Νομοταγής χρήση των κρυπτογραφικών μέσων.

11.6.11.2 Συμμόρφωση με πολιτικές ασφάλειας, πρότυπα και τεχνικές

Σκοπός είναι η διασφάλιση της συμμόρφωσης των συστημάτων με πολιτικές ασφάλειας του οργανισμού και πρότυπα. Θα πρέπει να εξετάζεται σε τακτικά χρονικά διαστήματα η ασφάλεια των πληροφοριακών συστημάτων. Οι εξετάσεις αυτές θα πρέπει να γίνονται σε αντιπαράθεση με τις κατάλληλες πολιτικές ασφάλειας. Ακόμη, τα πληροφοριακά συστήματα θα πρέπει να επιθεωρούνται για να ελέγχεται η συμμόρφωσή τους με εφαρμοζόμενα πρότυπα υλοποίησης μηχανισμών ασφάλειας και τεκμηριωμένα μέτρα προστασίας. Προτεινόμενα μέτρα:

- Συμμόρφωση με πολιτικές ασφάλειας και πρότυπα.
- Έλεγχος τεχνικής συμμόρφωσης.
- Καθορισμός της εφαρμοζόμενης νομοθεσίας.

11.6.11.3 Ζητήματα επιθεώρησης πληροφοριακών συστημάτων

Σκοπός είναι η μεγιστοποίηση της αποτελεσματικότητας της διαδικασίας επιθεώρησης, καθώς και η ελαχιστοποίηση των παρεμβολών που μπορεί να προκαλέσει στη λειτουργία των πληροφοριακών συστημάτων.

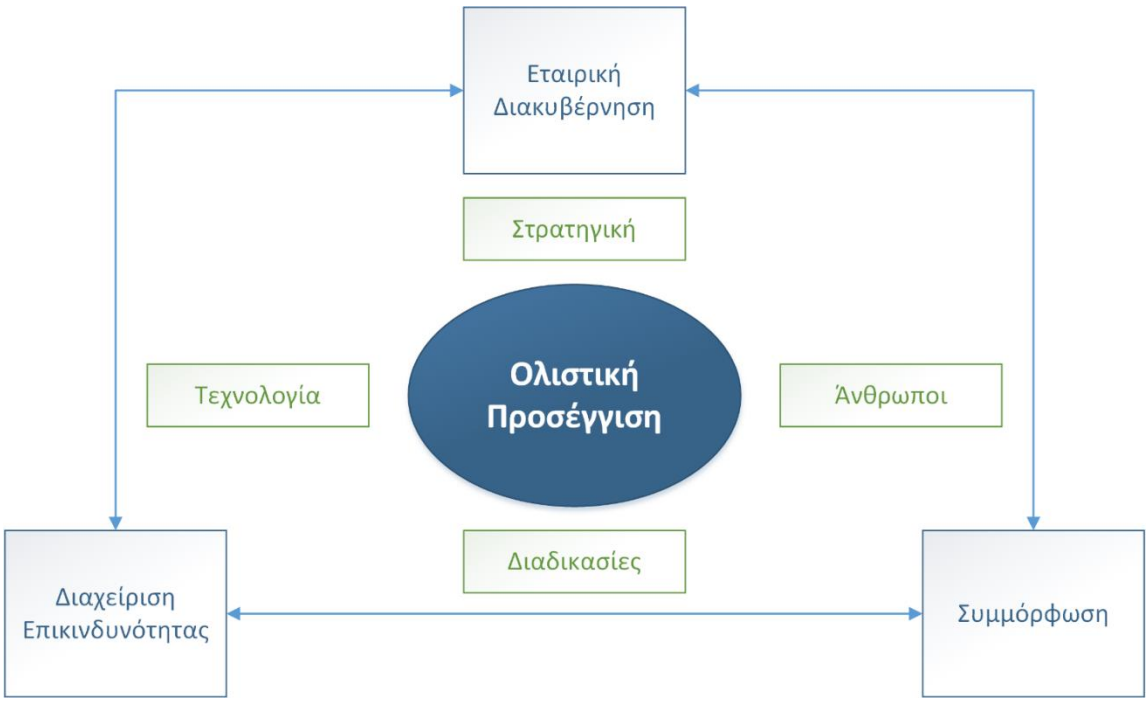
Θα πρέπει να λαμβάνονται μέτρα προστασίας για την προφύλαξη των παραγωγικών συστημάτων και των εργαλείων επιθεώρησης κατά τη διάρκεια των επιθεωρήσεων πληροφοριακών συστημάτων. Επιπλέον, απαιτείται κατάλληλη προστασία για την προφύλαξη της ακεραιότητας και την αποφυγή κατάχρησης των εργαλείων επιθεώρησης. Προτεινόμενα μέτρα:

- Μέτρα επιθεώρησης πληροφοριακών συστημάτων.
- Προστασία των εργαλείων επιθεώρησης πληροφοριακών συστημάτων.
- Συμμόρφωση με πολιτικές ασφάλειας και πρότυπα.

11.7 Διακυβέρνηση – Επικινδυνότητα - Συμμόρφωση

Στις μέρες μας έχει γίνει κατανοητό από τους οργανισμούς ότι οι άξονες Διακυβέρνηση – Επικινδυνότητα – Συμμόρφωση αλληλοσυμπληρώνονται και πρέπει να αντιμετωπίζονται ενιαία. Στη διεθνή βιβλιογραφία αυτοί οι τρεις άξονες αναφέρονται με το ακρωνύμιο GRC (Governance – Risk – Compliance).

Η αντιμετώπιση των εννοιών της εταιρικής διακυβέρνησης, της διαχείρισης επικινδυνότητας και της κανονιστικής συμμόρφωσης ως ένα ενιαίο σύνολο, αποτελεί πλέον απαίτηση στο σύγχρονο επιχειρηματικό περιβάλλον. Οι Racz, Weippl και Seufert διατύπωσαν τον ακόλουθο ορισμό για το τρίπτυχο GRC: «είναι μία ολοκληρωμένη, ολιστική προσέγγιση σε επίπεδο εταιρικής διακυβέρνησης, επικινδυνότητας και συμμόρφωσης που εξασφαλίζει ότι ολόκληρος ο οργανισμός δρα ηθικά και σύμφωνα με το αποδεκτό επίπεδο ανάληψης επικινδυνότητας, τις εσωτερικές πολιτικές και τους εξωτερικούς κανονισμούς, δια μέσου της ευθυγράμμισης των στρατηγικών, των διαδικασιών, της τεχνολογίας και των ανθρώπων, βελτιώνοντας έτσι την αποδοτικότητα και την αποτελεσματικότητα της επιχείρησης.». Από τον παραπάνω ορισμό προκύπτει το πλαίσιο αναφοράς ενιαίας διαχείρισης GRC, που αποτυπώνεται στην ακόλουθη Εικόνα 11.4.



Εικόνα 11.4 *Πλαίσιο αναφοράς GRC.*

Υπάρχουν ολοκληρωμένες λύσεις και εξειδικευμένο λογισμικό GRC, που ικανοποιεί την ανάγκη αυτοματοποίησης των σχετικών ελέγχων. Η αυτοματοποίηση των διαδικασιών διευκολύνει τη συμμόρφωση των σύγχρονων επιχειρήσεων με το εκάστοτε ρυθμιστικό πλαίσιο, τη διενέργεια εσωτερικών ελέγχων, την αποτελεσματικότητα των ελέγχων, ενώ ταυτόχρονα καθιστά ευκολότερο τον εντοπισμό των απειλών.

Βιβλιογραφία

Blyth, M. (2008). Risk and security management: protecting people and sites worldwide. Hoboken, N.J: John Wiley & Sons.

Dhillon, G. (Ed.). (2001). Information security management: global challenges in the new millennium. Hershey, PA: Idea Group Pub.

Fay, J. (2011). Contemporary security management (3rd ed). Burlington, MA: Butterworth-Heinemann.

Initiative, J. T. F. T. (2011). SP 800-39. Managing Information Security Risk: Organization, Mission, and Information System View. Gaithersburg, MD, United States: National Institute of Standards & Technology.

ISO/IEC 17799:2005 - Information technology -- Security techniques -- Code of practice for information security management. (n.d.). Retrieved 30 September 2015, from

NIST Computer Security Resource Center. (n.d.). Retrieved 30 September 2015, from http://csrc.nist.gov/

Ortmeier, P. J. (2002). Security management: an introduction. Upper Saddle River, NJ: Prentice Hall.

Pfleeger, C. P., & Pfleeger, S. L. (2002). Security in Computing (3rd ed.). Prentice Hall Professional Technical Reference.

Racz, N., Panitz, J., Amberg, M., Weippl, E., & Seufert, A. (2010). Governance, risk & compliance (grc) status quo and software use: Results from a survey among large enterprises. Governance, 1, 1–2010.

Sennewald, C. A. (2011). Effective security management (5th ed). Burlington, MA: Butterworth-Heinemann.

Stoneburner, G., Goguen, A. Y., & Feringa, A. (2002). SP 800-30. Risk Management Guide for Information Technology Systems. Gaithersburg, MD, United States: National Institute of Standards & Technology.

Tarantino, A. (Ed.). (2008). Governance, risk, and compliance handbook: technology, finance, environmental, and international guidance and best practices. Hoboken, N.J: John Wiley & Sons.

Tipton, H. F., & Nozaki, M. K. (Eds.). (2007). Information security management handbook (6th ed). Boca Raton: Auerbach Publications.

Κριτήρια αξιολόγησης

Απαντήστε στις ακόλουθες ερωτήσεις. Η κάθε ερώτηση μπορεί να έχει μοναδική ή περισσότερες απαντήσεις.

1. Ποιο από τα παρακάτω ανήκει σε ένα Πληροφοριακό Σύστημα:
α) άνθρωποι
β) λογισμικό
γ) υλικό
δ) όλα τα παραπάνω

2. Μια απειλή:
α) προκαλεί πάντα επιπτώσεις.
β) μπορεί να εκμεταλλευτεί μια ευπάθεια.
γ) προκαλεί πάντα ζημιά.
δ) ανιχνεύεται σε ένα αγαθό.

3. Η ονομασία PDCA σημαίνει:

α) Plan - Do - Check -Act
β) Plan - Design - Check - Act
γ) People - Do - Check - Act
δ) Plan - Direct - Computer - Action

4. Η οικογένεια προτύπων ISO/IEC 27K στηρίχτηκε στη συλλογή προτύπων:
α) DIN.
β) BSI.
γ) BS.
δ) IEC.

5. Ποιο είναι το κεντρικό πρότυπο της οικογένειας προτύπων 27K;
α) 27000
β) 27001
γ) 27100
δ) 27010

6. Τι σημαίνουν τα αρχικά ΣΔΑΠ;
α) Σωστή Διαχείριση Ασφάλειας Πληροφοριών
β) Σύστημα Διαχείρισης Ασφάλειας Πληροφοριών
γ) Σωστή Διαχείριση Ασφάλειας Πληροφορικής
δ) κανένα από τα παραπάνω

7. Ποια από τις παρακάτω είναι μεθοδολογία εκτίμησης επικινδυνότητας;
α) COBIT
β) OCTAVE
γ) FRIM
δ) FIRM

8. Πόσα στάδια έχει η μεθοδολογία NIST;
α) 6
β) 7
γ) 8
δ) 9

9. Ποιος όρος δεν ανήκει στο GRC;
α) Governance
β) Government
γ) Risk
δ) Compliance

10. Ποιο πρότυπο της οικογένειας ISO/IEC 27K χρησιμοποιείται κατά τη διαδικασία διαπίστευσης;
α) 27001
β) 27006
γ) 27600
δ) κανένα από τα παραπάνω