Ανοικτό Πανεπιστήμιο Κύπρου

Σχολή Οικονομικών Επιστημών και Διοίκησης

Μεταπτυχιακό Πρόγραμμα Σπουδών

Διοίκηση, Τεχνολογία και Ποιότητα

Μεταπτυχιακή Διατριβή

Μελέτη Ασφάλειας της Πληροφορίας και Εφαρμογή του Προτύπου ISO/IEC27001:2013 στο Χώρο των Τηλεπικοινωνιακών Οργανισμών στην Ελλάδα

Σωτηριάδης Σταύρος

Επιβλέπουσα Καθηγήτρια

Δρ. Στυλιανή Σοφιανοπούλου

Μάιος 2018

Περίληψη

Η ασφάλεια των πληροφοριών είναι μία από τις βασικές ανησυχίες της σύγχρονης οργάνωσης. Ο όγκος και η αξία των δεδομένων που χρησιμοποιούνται στην καθημερινή επιχειρηματική δραστηριότητα αυξάνουν όλο και περισσότερο τον τρόπο λειτουργίας των οργανώσεων και την επιτυχία τους. Προκειμένου να προστατευθούν αυτές οι πληροφορίες - και να το προστατεύσουν - όλο και περισσότερες εταιρείες έχουν αποκτήσει πιστοποίηση ISO 27001.

Οι κύριοι παράγοντες για την ασφάλεια είναι αναμφισβήτητα η παγκοσμιοποίηση, οι κυβερνητικές οδηγίες, οι τρομοκρατικές δραστηριότητες και οι απειλές από τους χάκερ. Επιπλέον, οι οργανισμοί που αναζητούν ευκαιρίες για την οικοδόμηση αγορών παγκοσμίως θεωρούν όλο και περισσότερο το πρότυπο ISO 27001 ως προϋπόθεση για την επιχειρηματική τους δραστηριότητα. Η πιστοποίηση θεωρείται όλο και περισσότερο ως ισχυρή διαβεβαίωση της δέσμευσης να εκπληρώνονται οι υποχρεώσεις απέναντι σε πελάτες και επιχειρηματικούς εταίρους.

Αντιλαμβανόμαστε πως η επιδίωξη της σωστής πιστοποίησης για έναν οργανισμό μπορεί να είναι καθοριστική, κυρίως επειδή υπάρχουν τόσες πολλές παραλλαγές. Αυτές οι παραλλαγές μερικές φορές μετονομάζονται ή αντικαθίστανται από νεότερα πρότυπα, γεγονός που μπορεί να προκαλέσει κάποια σύγχυση. Σκοπός της παρούσας πτυχιακής εργασίας είναι μας βοηθήσει να κατανοήσουμε καλύτερα την πιστοποίηση ISO27001 μελετήσουμε της λειτουργείες της.

Abstract

Information security is one of the main concerns of the modern organization. The volume and value of data used in day-to-day business increasingly enhances the way organizations work and their success. In order to protect this information - and to protect it - more and more companies have obtained ISO 27001 certification.

The main factors for security are unquestionably globalization, government instructions, terrorist activities and threats from hackers. In addition, organizations looking for market-building opportunities worldwide are increasingly considering ISO 27001 as a prerequisite for their business. Certification is increasingly seen as a strong assurance of the commitment to meet obligations towards customers and business partners.

We understand that pursuing the right certification for an organization can be crucial, mainly because there are so many variations. These variations are sometimes renamed or replaced by newer standards, which may cause some confusion. The purpose of this thesis is to help us better understand ISO27001 certification to study its operations.

Ευχαριστίες

Ευχαριστώ ιδιαίτερα την επιβλέπουσα καθηγήτριά μου κα. Στυλιανή Σοφιανοπούλου για την υπομονή και την επιμονή της, καθώς επίσης και για την καθοδήγηση στην ολοκλήρωση της εκπόνησης της παρούσας μεταπτυχιακής διατριβής.

Τέλος, ευχαριστώ θερμά και την οικογένειά μου για την στήριξή τους σε όλη αυτή την πορεία μέχρι την ολοκλήρωσή της.

Πίνακας περιεχομένων

Κεφάλαιο 1

Εισαγωγή και Σκοπός

1. Βασικά στοιχεία μελέτης

1.1. Θεμελιώδεις έννοιες ασφάλειας

Η ασφάλεια των πληροφοριακών συστημάτων αποτελεί έναν κλάδο της Επιστήμης της Πληροφορικής. Βασική ασχολία του κλάδου αυτού είναι η προστασία των υπολογιστών, των δεδομένων που είναι αποθηκευμένα στους υπολογιστές και των δικτύων που συνδέουν τους υπολογιστές μεταξύ τους. Ένας ακόμα στόχος της ασφάλειας των πληροφοριακών συστημάτων είναι η αποτροπή της μη εξουσιοδοτημένης χρήσης των υπολογιστών και των δικτύων[1].

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

Καθημερινά είμαστε δέκτες πληροφοριών σχετικά με την διαρροή προσωπικών δεδομένων και στοιχείων επιχειρήσεων. Η οικονομική απώλεια τέτοιων στοιχείων αποτιμώνται σε εκατοντάδες δις USD μόνο για τις ΗΠΑ[2].

[1] Πανέτσος Σ., 2007
[2] Κατσίκας Σ., 2014

Στα πλαίσια του κλάδου της ασφάλειας των πληροφοριακών συστημάτων συμπεριλαμβάνεται η ψηφιακή εγκληματολογία και η εφαρμοσμένη κρυπτογραφία[3].

Στόχος της εργασίας είναι να προβάλλει το πρόβλημα της ασφάλειας των πληροφοριών, ιδιαίτερα στον ευαίσθητο τομέα των Τηλεπικοινωνιών. Το πρότυπο ISO/IEC 27001:2013 εστιάζει στις απαιτούμενες προδιαγραφές για τον σχεδιασμό, την υλοποίηση, τη λειτουργία, την παρακολούθηση, τον έλεγχο και τη συντήρηση ενός τεκμιριωμένου Συστήματος Διαχείρισης της Ασφάλειας των Πληροφοριών στο πλαίσιο ενός τηλεπικοινωνιακού οργανισμού[4].

1.2. Προϋποθέσεις ασφάλειας

Η ασφάλεια των πληροφοριακών συστημάτων στηρίζεται στους τρεις βασικούς πυλώνες στους οποίους στηρίζεται η σωστή λειτουργία ενός οποιουδήποτε πληροφοριακού συστήματος[5]. Οι τρεις αυτοί πυλώνες είναι:

[3] Κομνηνός Θ, Σπυράκης Π, 2002
[4] Κατσίκας Σ., 2014
[5] S. Powell, J.P. Shim, 2009

- **Ακεραιότητα (Integrity)**

Ως ακεραιότητα ορίζεται η διατήρηση των δεδομένων ενός πληροφοριακού συστήματος σε μια δεδομένη κατάσταση και η αποτροπή ανεπιθύμητων τροποποιήσεων, προσθηκών και αφαιρέσεων από άτομα τα οποία δεν είναι εξουσιοδοτημένα να προχωρήσουν στις παραπάνω ενέργειες[6].

Επίσης, στα πλαίσια της ακεραιότητας αποτρέπεται η πρόσβαση και η χρήση των ηλεκτρονικών υπολογιστών και των δικτύων του συστήματος από άτομα τα οποία δεν έχουν εξουσιοδότηση να κάνουν τη χρήση αυτή[7].

Ένα χαρακτηριστικό παράδειγμα της σημασίας της ακεραιότητας είναι η περίπτωση μιας ηλεκτρονικής εφημερίδας η οποία δημοσιεύει στην ιστοσελίδα της ένα άρθρο. Η διασφάλιση της ακεραιότητας αποτρέπει τον οποιοδήποτε που θα το ήθελε να επέμβει στο δημοσιοποιημένο άρθρο και να αλλοιώσει το κείμενο, εισάγοντας ανακριβείς πληροφορίες[8].

- **Διαθεσιμότητα (Availability)**

Ως διαθεσιμότητα των δεδομένων των ηλεκτρονικών υπολογιστών και των υπολογιστικών πόρων ορίζεται η διασφάλιση του ότι οι ηλεκτρονικοί υπολογιστές, τα δίκτυα και τα δεδομένα είναι διαθέσιμα στους χρήστες όποτε εκείνοι τα χρειάζονται[9].

Μια από τις συνηθέστερες απειλές των σύγχρονων πληροφοριακών συστημάτων είναι η επίθεση άρνησης υπηρεσιών (DOS attack). Σκοπός της άρνησης πληροφοριών είναι η προσωρινή ή και η μόνιμη τοποθέτηση των στοχευμένων πόρων εκτός λειτουργία[10]ς.

Η άρνηση πληροφοριών δεν γίνεται απαραίτητα στα πλαίσια μιας εχθρικής επίθεσης. Παράδειγμα αυτού αποτελεί το φαινόμενο Slashdot. Το Slashdot είναι η διαδικασία κατά την οποία μια ιστοσελίδα η οποία φιλοξενείται σε ένα διακομιστή με σύνδεση χαμηλής χωρητικότητας αναδημοσιεύεται σε ένα

[6] W. Stallings, 2003
[7] S. Powell, J.P. Shim, 2009
[8] W. Stallings, 2003
[9] W. Stallings, 2003
[10] S. Powell, J.P. Shim, 2009

δημοφιλή ιστότοπο. Συνέπεια αυτού είναι η υπερφόρτωση του δεύτερου ιστότοπου με τα ίδια αποτελέσματα της επίθεσης άρνησης πληροφοριών[11].

- **Εμπιστευτικότητα (Confidentiality)**

Ως εμπιστευτικότητα ορίζεται η διαδικασία κατά την οποία διασφαλίζεται ότι οι ευαίσθητες πληροφορίες δεν αποκαλύπτονται σε άτομα τα οποία δεν είναι εξουσιοδοτημένα[12].

Υπάρχουν πολλοί τρόποι διαρροής ευαίσθητων πληροφοριών, με συνηθέστερη την ψηφιακή υποκλοπή. Άλλος ένα συνήθης τρόπος υποκλοπής πληροφοριών μέσω της κλοπής φορητού εξοπλισμού. Σε μελέτη που πραγματοποιήθηκε το 2006 και συμμετείχαν 480 εταιρίες αναδείχθηκε το ότι το 80% των εταιριών αυτών έχουν αντιμετωπίσει στο παρελθόν προβλήματα με διαρροή πληροφοριών μέσω της κλοπής φορητού εξοπλισμού[13]

1.3. Ανάλυση επικινδυνότητας

Προκειμένου να έχουμε την αποτελεσματική διαμόρφωση της πολιτικής ασφάλειας των πληροφοριακών συστημάτων θα πρέπει αρχικά να πραγματοποιηθεί η αξιολόγηση του επιπέδου ασφαλείας των πληροφοριακών συστημάτων.

Υπάρχουν πολλοί τρόποι με τους οποίους μπορεί να γίνει η αξιολόγηση αυτή. Οι δύο από τους συνηθέστερους τρόπους είναι η εκπόνηση μελέτης ανάλυσης επικινδυνότητας (Risk Analysis) και η χρήση των προτύπων διαχείρισης της ασφάλειας[14].

Για να μπορέσουμε να κατανοήσουμε καλύτερα την ανάλυση της επικινδυνότητας, θα ορίσουμε τις βασικές έννοιες της ανάλυσης των κινδύνων.

[11] Κιουντούζης Ε, 2002
[12] Κιουντούζης Ε, 2002
[13] S. Powell, J.P. Shim, 2009
[14] Andrew S. Tanenbaum, 2003

- **Απειλή**

Ως απειλή ορίζεται ένα οποιοδήποτε μη επιθυμητό γεγονός το οποίο μπορεί να προκαλέσει τη μη διαθεσιμότητα ενός συστήματος και κάποιων υπηρεσιών. Η μη διαθεσιμότητα αυτή μπορεί να είναι είτε τυχαία είτε να είναι αποτέλεσμα της μετατροπής ή και της καταστροφής των δεδομένων και του συστήματος [15].

- **Ευπάθεια**

Ως ευπάθεια ορίζονται όλες οι αδυναμίες και οι σχεδιαστικές ατέλειες ενός πληροφοριακού συστήματος και κάποιας υποδομής. Αποτέλεσμα των αδυναμιών και των ατελειών αυτών είναι η παραβίαση της ασφάλειας και της ακεραιότητας του πληροφοριακού συστήματος. Θα μπορούσαμε να ορίσουμε την ευπάθεια με την παρακάτω συνάρτηση :

Ευπάθεια = Πιθανότητα να συμβεί μια απειλή x Πιθανότητα να είναι επιτυχής[16]

- **Κίνδυνος**

Ως κίνδυνος ορίζεται η πιθανότητα μιας απειλής να εκμεταλλευτεί μια συγκεκριμένη ευπάθεια. Μέσα από τον κίνδυνο εκφράζεται και το ενδεχόμενο της απώλειας[17].

- **Αντίμετρο**

Ως αντίμετρα ορίζονται όλα τα μέτρα τα οποία λαμβάνονται για να προστατεύονται τα πληροφοριακά συστήματα και να αντιμετωπίζονται με επιτυχία οι απειλές.

Στα πλαίσια του σχεδιασμού των αντίμετρων έχουμε την ανίχνευση, την πρόληψη και τη μείωση της απώλειας η οποία μπορεί να προκαλέσει την εμφάνισης μιας ή περισσότερων απειλών[18].

[15] Joseph Boyce, 2002
[16] Siponen M, 2000
[17] Siponen M, 2000
[18] Rash, Michael et al,2005

1.3.1. Οφέλη ανάλυσης της επικινδυνότητας

Στη συνέχεια καταγράφουμε επιγραμματικά τα οφέλη της ανάλυσης της επικινδυνότητας:

- Στόχευση της ασφάλειας των πληροφοριακών συστημάτων
- Κατανόηση και καλύτερη αντίληψη της σπουδαιότητας της ασφάλειας των πληροφοριακών συστημάτων
- Γενικότερη βελτίωση της ασφάλειας των πληροφοριακών συστημάτων
- Δικαιολόγηση των δαπανών που γίνονται για την ασφάλεια των πληροφοριακών συστημάτων [19]

1.3.2. Μέθοδοι ανάλυσης της επικινδυνότητας

Προκειμένου να αξιολογήσουμε και να αποτιμήσουμε σωστά τα επίπεδα ασφαλείας του εκάστοτε πληροφοριακού συστήματος, μπορούμε να εφαρμόσουμε κάποιες από τις τεχνικές ανάλυσης της επικινδυνότητας. Οι τεχνικές αυτές είναι πολλές, με τις πιο διαδεδομένες από αυτές να είναι η SBA (Security By Analysis), η MARION και η CRAMM (CCTA Risk Analysis and Management Method).

Κύριο χαρακτηριστικό και των τριών παραπάνω μεθόδων ανάλυσης της επικινδυνότητας είναι το ότι στηρίζονται σε μια πολιτική ασφαλείας η οποία ανταποκρίνεται πλήρως στις ανάγκες του κάθε οργανισμού για τον οποίο θέλουμε να ελέγξουμε την επικινδυνότητα. Επίσης, και οι τρεις αυτές μέθοδοι προσφέρουν ένα επίπεδο ασφάλειας αντίστοιχο των κινδύνων από τους οποίους προστατεύονται τα πληροφοριακά συστήματα[20].

Σημαντικό μειονέκτημα όλων των μεθόδων ανάλυσης της επικινδυνότητας είναι το ότι ενέχουν το στοιχείο του υποκειμενισμού. Τα αποτελέσματα της κάθε μελέτης για την επικινδυνότητα ενός πληροφοριακού συστήματος και η

[19] Rash, Michael et al,2005
[20] Andrew S. Tanenbaum, 2003

ανάλυση τους εξαρτώνται τόσο από τις γνώσεις όσο και από την εμπειρία του κάθε αναλυτή[21].

1.4. Μέτρα ασφαλείας

Στα πλαίσια της πολιτικής ασφαλείας των πληροφοριακών συστημάτων έχουμε τα Αντίμετρα ή αλλιώς Μέτρα Ασφαλείας ή Μέτρα Προστασίας. Ως μέτρα ασφαλείας ορίζονται όλες οι τεχνικές, όλες οι διαδικασίες, όλες οι ενέργειες και όλες οι ηλεκτρονικές και μη συσκευές οι οποίες στόχο έχουν τον περιορισμό των ευπαθειών και των απειλών των πληροφοριακών συστημάτων[22].

Τα Αντίμετρα διακρίνονται σε τέσσερις κατηγορίες:

- Πρόληψη
- Διασφάλιση
- Ανίχνευση
- Επαναφορά[23]

Στα πλαίσια της πρόληψης εντάσσονται όλα τα αντίμετρα στόχος των οποίων είναι η μείωση των κινδύνων[24].

Στα πλαίσια της διασφάλισης εντάσσονται όλα τα εργαλεία, όλες οι στρατηγικές και όλοι οι έλεγχοι οι οποίοι στόχο έχουν τη συνεχή αποτελεσματικότητα των μέτρων ασφαλείας[25].

Στα πλαίσια της ανίχνευσης εντάσσονται όλα τα προγράμματα και όλες οι τεχνικές οι οποίες στόχο έχουν την έγκαιρη ανίχνευση των περιστατικών επικινδυνότητας, την αναχαίτιση των περιστατικών αυτών και την αντιμετώπισή τους[26].

Τέλος, στα πλαίσια της επαναφοράς, εντάσσονται όλες οι διαδικασίες που ως στόχο έχουν την όσο το δυνατόν αμεσότερη επαναφορά σε ασφαλή

[21] Andrew S. Tanenbaum, 2003
[22] K. Scasfone, P. Mell, 2007
[23] K. Scasfone, P. Mell, 2007
[24] K. Scasfone, P. Mell, 2007
[25] K. Scasfone, P. Mell, 2007
[26] K. Scasfone, P. Mell, 2007

περιβάλλοντα μετά από περιστατικό ρήξης ασφαλείας και μετά από την έρευνα των αιτιών που προκάλεσαν τη ρήξη αυτή[27].

Για να μπορέσει να εφαρμοστεί επιτυχώς η πολιτική ασφαλείας, θα πρέπει να περιλαμβάνονται συγκεκριμένες διαδικασίες στο σχέδιο ασφαλείας. Σύμφωνα με τις διαδικασίες αυτές θα πρέπει να υπάρχει μια συνεχής ροή ενημέρωσης και να γίνονται διαρκώς επισκοπήσεις του σχεδίου ασφαλείας και της εφαρμογής του.

Έτσι, το κάθε σχέδιο θα είναι πάντα εναρμονισμένο με τις τεχνολογικές εξελίξεις και θα ακολουθεί τις αλλαγές του οργανισμού στα πληροφοριακά συστήματα του οποίου εφαρμόζεται.

[27] K. Scasfone, P. Mell, 2007

Κεφάλαιο 2

Τηλεπικοινωνίες

2.1. Ορισμός

Ως τηλεπικοινωνίες ορίζονται όλες οι μορφές ενσύρματης και ασύρματης ηλεκτρομαγνητικής, ακουστικής, οπτικής και ηλεκτρικής επικοινωνίας που μπορεί να πραγματοποιηθεί ανάμεσα σε δύο ή περισσότερους ανθρώπους, ανεξάρτητα από την απόσταση που χωρίζει τους ανθρώπους αυτούς[28].

Στη σημερινή εποχή, οι τηλεπικοινωνίες περιλαμβάνουν, κατά κύριο λόγο, την αποστολή ηλεκτρομαγνητικών κυμάτων κι ηλεκτρικών σημάτων από διάφορες ηλεκτρονικές συσκευές όπως είναι το τηλέφωνο και ο ασύρματος.

Σε παλαιότερες εποχές, όταν η τεχνολογία δεν είχε αναπτυχθεί ακόμα η τηλεπικοινωνία γινόταν με τη χρήση ακουστικών σημάτων, σημάτων καπνού και άλλα[29].

2.2. Ιστορική αναδρομή

Η πρώτη μορφή τηλεπικοινωνιών ήταν η επικοινωνία με τη χρήση της φωτιάς. Στα ομηρικά κείμενα περιγράφεται ο τρόπος με τον οποίο οι Αχαιοί ανήγγειλαν στους Μυκηναίους την πτώση της Τροίας μετά τον Τρωικό πόλεμο χρησιμοποιώντας τις φρυκτωρίες, δηλαδή τις μεγάλες φωτιές στις κορυφές των βουνών. Η χρήση τη φωτιάς ως βασικό μέσο τηλεπικοινωνίας ήταν η επικρατέστερη μέχρι και τον 19ο αιώνα[30].

[28] ΕΕΚΤ, 2012
[29] Fjermestad, J., Romano, N, 2006
[30] Nicopolitidis P., Obaidat M. S., Papadimitriou G. I., Pomportsis A.S, 2006

Στον 21ο αιώνα, τον οποίο και διανύουμε, οι τηλεπικοινωνίες είναι διαδεδομένες, το ίδιο και οι συσκευές που χρησιμοποιούνται για την ύπαρξη των τηλεπικοινωνιών. Τέτοιες συσκευές είναι τα σταθερά τηλέφωνα, τα κινητά τηλέφωνα, τα ραδιοτηλέφωνα, οι ασύρματοι, οι συσκευές φαξ, η τηλεόραση και το ραδιόφωνο. Στις ημέρες μας το πλέον διαδεδομένο μέσο τηλεπικοινωνίας είναι το διαδίκτυο[31].

Για τη διασύνδεση των συσκευών αυτών είναι απαραίτητα κάποια δίκτυα, όπως τα δίκτυα υπολογιστών, τα δίκτυα κινητής τηλεφωνίας, τα δημόσια τηλεφωνικά δίκτυα, τα τηλεοπτικά δίκτυα και τα ραδιοφωνικά δίκτυα[32].

Ο σχηματισμός των δικτύων αυτών γίνεται μέσω τηλεπικοινωνιακών καναλιών. Τα κανάλια αυτά λειτουργούν ως φυσικές δίοδοι μέσα από τις οποίες μεταδίδονται τα κωδικοποιημένα σήματα σε σταθμούς που βρίσκονται στα άκρα των καναλιών αυτών. Οι σταθμοί αυτοί είναι οι συσκευές τις οποίες προαναφέραμε.

2.3. Κίνδυνοι που εντοπίζονται κατά την ανταλλαγή πληροφοριών μέσω των τηλεπικοινωνιών

Για να ταξινομηθεί μια πληροφορία θα πρέπει να ελεγχθεί η αξία της, οι νομικές της απαιτήσεις και η κρισιμότητά της στα πλαίσια του οργανισμού. Για μια σωστή ταξινόμηση θα πρέπει να λαμβάνονται υπόψη οι επιχειρηματικές ανάγκες για το διαμοιρασμό ή τον περιορισμό των πληροφοριών καθώς και ο επιχειρηματικός αντίκτυπος που σχετίζεται με τις πληροφορίες αυτές[33].

Στη συνέχεια θα παραθέσουμε τις αναλυτικές οδηγίες για την ταξινόμηση των πληροφοριών σε σχέση με την ευαισθησία τους. Παράλληλα θα καταγράψουμε και λεπτομέρειες για το πώς μπορούμε να χειριστούμε τις πληροφορίες που χρήζουν ιδιαίτερου χειρισμού.

Οι οδηγίες αυτές θα μπορούσαν να χρησιμοποιηθούν και ως πρότυπο και να εφαρμόζονται σε διάφορες περιπτώσεις, ανάλογα με την εκάστοτε περίσταση

[31] Nicopolitidis P., Obaidat M. S., Papadimitriou G. I., Pomportsis A.S, 2006
[32] Nicopolitidis P., Obaidat M. S., Papadimitriou G. I., Pomportsis A.S, 2006
[33] Hossein Bidgoli, 2006

και τη φύση των πληροφοριών που θέλουμε να ταξινομήσουμε. Βασικό στοιχείων των οδηγιών ταξινόμησης που θα παραθέσουμε είναι οι συμβάσεις για δύο ειδών ταξινομήσεις, για την αρχική ταξινόμηση και την ταξινόμηση σε βάθος χρόνου. Επίσης, η ταξινόμηση θα πρέπει πάντα να σχετίζεται με κάποια προκαθορισμένη πολιτική ελέγχου πρόσβασης στα πληροφοριακά συστήματα[34].

Προκειμένου να εξασφαλίσουμε την κατάλληλη ταξινόμηση των πληροφοριών θα πρέπει να κάνουμε ανά τακτά χρονικά διαστήματα ανασκόπηση του επιπέδου προστασίας των πληροφοριών και όταν διαπιστώνουμε ότι είναι απαραίτητη κάποια αλλαγή ή κάποια ενημέρωση, να ταξινομούμε άμεσα την πληροφορία σε άλλο επίπεδο[35].

Για να εκτιμήσουμε το επίπεδο της προστασίας θα πρέπει να αναλύσουμε την εμπιστευτικότητα, την ακεραιότητα και τη διαθεσιμότητα όλων των απαιτήσεων που λαμβάνονται υπόψη για την ταξινόμηση της πληροφορίας[36].

Τις περισσότερες φορές, όταν μια πληροφορία γίνεται δημόσια, δε θεωρείται πλέον ευαίσθητη ή/και κρίσιμη. Αυτό θα πρέπει πάντα να λαμβάνεται υπόψη καθώς αν γίνει λανθασμένη ταξινόμηση θα εφαρμοστούν και αχρείαστοι έλεγχοι με αποτέλεσμα να οδηγηθούμε σε αναίτια έξοδα[37].

Η σωστή ταξινόμηση της πληροφορίας θεωρείται θεμελιώδης, καθώς έτσι θα μπορέσουμε να καταλήξουμε σύντομα στο πως θα χειριστούμε και στο πως θα προστατεύσουμε την εκάστοτε πληροφορία[38].

Για να έχουμε τη σωστή ταξινόμηση της πληροφορίας είναι αναγκαίο να αναπτύξουμε μια σειρά από διαδικασίες. Μέσω των διαδικασιών αυτών αρχικά θα χαρακτηρίσουμε και εν συνεχεία θα διαχειριστούμε την κάθε πληροφορία. Τέλος, εξαιρετικά σημαντική κρίνεται η ονομασία των πληροφοριών, καθώς μέσα από το όνομα της εκάστοτε πληροφορίας μπορούμε να αντλήσουμε στοιχεία που θα μας οδηγήσουν στην ορθότερη ταξινόμηση της[39].

[34] Hossein Bidgoli, 2006
[35] Hossein Bidgoli, 2006
[36] Hossein Bidgoli, 2006
[37] Hossein Bidgoli, 2006
[38] Hossein Bidgoli, 2006
[39] Hossein Bidgoli, 2006

Κεφάλαιο 3

Ασφάλεια πληροφοριών και συστήματα διαχείρισης ασφαλείας των πληροφοριών

3.1. Εισαγωγή

Το 3ο κεφάλαιο της παρούσας εργασίας στηρίζεται στην απάντηση του ερωτήματος «Τί είναι η ασφάλεια των πληροφοριών;».

Ως ασφάλεια των πληροφοριών ορίζουμε τη διαδικασία μέσα από την οποία κρατάμε την πληροφορία ασφαλής προστατεύοντας την ιδιωτικότητά της, την ακεραιότητά της και τη διαθεσιμότητά της[40].

Οι πληροφορίες θεωρούνται πολύ σημαντικές από την απαρχή του ανθρώπινου είδους. Οι πρωτόγονοι άνθρωποι στηρίζονται σε πληροφορίες για το που θα βρουν τροφή και που και πως θα κατασκευάσουν τα καταλύματα τους[41].

Τον 20ο αιώνα τα περιουσιακά στοιχεία ενός οργανισμού ήταν φυσικά και αποδίδονταν με τη μορφή ιδιοκτησιακών τίτλων, κτιρίων, γραφείων, μετρητών, μετοχών και άλλων μεταβιβάσιμων τίτλων. Αντίστοιχα, οι κίνδυνοι και οι

[40] Andrew S. Tanenbaum, 2003
[41] Andrew S. Tanenbaum, 2003

ανησυχίες σχετικά με την ασφάλεια τους ήταν φυσικές. Οι οργανισμοί και οι περιουσίες τους προστατεύονταν με τη βοήθεια φυλάκων, θυρίδων, ενισχυμένων τοίχων και χρηματοκιβωτίων[42].

Στον 21ο αιώνα τα δεδομένα έχουν αλλάξει κατά πολύ. Τα περιουσιακά στοιχεία των οργανισμών δεν είναι πλέον μόνο φυσικά. Μέρος των περιουσιακών στοιχείων της κάθε επιχείρησης και του κάθε οργανισμού είναι πλέον η πνευματική ιδιοκτησία. Η πνευματική αυτή ιδιοκτησία εμφανίζεται με τη μορφή διάφορων ηλεκτρονικών μέσων, όπως τα αρχεία επεξεργασίας κειμένου, οι βάσεις δεδομένων και τα υπολογιστικά φύλλα. Άλλα περιουσιακά στοιχεία είναι τα αρχεία που υπάρχουν στους σκληρούς δίσκους του οργανισμού και οι συναλλαγές που εκτελούνται μέσα από ένα δίκτυο, είτε το δίκτυο αυτό είναι ενσύρματο, είτε ασύρματο. Πλέον, μεγάλο μέρος του πλούτου ενός οργανισμού αποτελείται από τα ψηφιακά αρχεία που διαθέτει ο οργανισμός αυτός[43].

Τα νέα στοιχεία πλούτου έχουν δημιουργήσει και νέες ανάγκες σχεδιασμού μέσων ασφαλείας του πλούτου αυτού. Βασικό στοιχεία στα νέα μέτρα ασφαλείας είναι ο έλεγχος ασφαλείας των πληροφοριών. Στην παραδοσιακή άποψη περί ασφάλειας των πληροφοριών περιλαμβάνονται τα τρία βασικότερα στοιχεία της ασφάλειας των πληροφοριών, τα οποία είναι γνωστά και ως η CIA της ασφάλειας των πληροφοριών:

- Εμπιστευτικότητα (Confidentiality)
- Ακεραιότητα (Integrity)
- Διαθεσιμότητα (Availability)[44]

3.2. Η ασφάλεια των πληροφοριών ως διαδικασία

Στα πλαίσια της αποτελεσματικής ασφάλειας των πληροφοριών εμπλέκονται τα προϊόντα ασφαλείας και προηγμένες πληροφορίες[45].

Τα κυριότερα από τα προϊόντα ασφαλείας είναι τα τείχη ασφαλείας, οι σαρωτές που εντοπίζουν όλες τις ευπάθειες των πληροφοριακών συστημάτων και οι

[42] Andrew S. Tanenbaum, 2003
[43] Arnason & Willett, 2007
[44] Andrew S. Tanenbaum, 2003
[45] Siponen M.,2000

διάφορες εφαρμογές που ανιχνεύουν και εντοπίζουν τις οποιοδήποτε εισβολές. Κανένα από τα παραπάνω μεμονωμένα δεν μπορεί να προσφέρει την απαραίτητη ασφάλεια των πληροφοριών[46].

Η ασφάλεια των πληροφοριών είναι μια ολόκληρη διαδικασία η οποία αποτελείται από πολλές και διαφορετικές μεταξύ τους διαδικασίες. Το σύνολο των διαδικασιών αυτών ως στόχο έχει το να διαχειριστεί και να προστατεύσει τα πληροφοριακά στοιχεία του οργανισμού. Επίσης, όταν αυτό κρίνεται απαραίτητο, οι διαδικασίες αυτές αναλαμβάνουν το να πάρουν τις αποφάσεις για τη μελλοντική υποδομή ασφαλείας των πληροφοριακών συστημάτων[47].

3.3. Η ασφάλεια των πληροφοριών ως συλλογική ευθύνη

Παρότι σε κάθε οργανισμό υπάρχει μια συγκεκριμένη ομάδα ανθρώπων και διαδικασιών που ασχολούνται αποκλειστικά με την ασφάλεια των πληροφοριακών συστημάτων και των πληροφοριών, γεγονός είναι πως σε καθημερινή βάση η ασφάλεια των πληροφοριών είναι συλλογική ευθύνη και αφορά όλους τους εμπλεκόμενους στον οργανισμό[48].

Είναι πολύ σημαντικό, εκτός από την άρτια εφαρμογή των διαδικασιών ασφαλείας, να υπάρχει αξιοπιστία και στους εργαζομένους στον οργανισμό καθώς και σε όσους βρίσκονται καθημερινά στις εγκαταστάσεις του οργανισμού[49].

Για παράδειγμα, η ύπαρξη καρτών ασφαλείας για την είσοδο κάποιου στο χώρο, είναι μια άριστη μορφή ασφάλειας. Αν, ωστόσο, οι εργαζόμενοι χρησιμοποιώντας την κάρτα τους, επιτρέπουν και σε άλλους, μη έχοντας εργασία, να εισέλθουν στο χώρο, αυτόματα η ασφάλεια του οργανισμού γίνεται τρωτή. Ένα άλλο παράδειγμα είναι οι εργαζόμενοι οι οποίοι ενδέχεται να διαθέτουν λογισμικά με τα οποία μπορούν να παρακάμπτουν τα τείχη ασφαλείας, όσο ανθεκτικά και αν είναι αυτά[50].

[46] Siponen M.,2000
[47] Siponen M.,2000
[48] Rash, Michael et al,2005
[49] Rash, Michael et al,2005
[50] Rash, Michael et al,2005

Πολλά είναι τα παραδείγματα των οργανισμών που έχουν πέσει «θύματα» χάκερ όταν για λίγη ώρα έμειναν εκτεθειμένοι από ανυπαρξία του τείχους ασφαλείας. Η ελάχιστη ώρα που χρειάζεται για να γίνει μια αναβάθμιση του firewall είναι αρκετή για να εισβάλει στο σύστημα κάποιος χάκερ και να αποσπάσει τις πληροφορίες που θέλει. Για το λόγο αυτό και οι εφαρμογές ασφαλείας θα πρέπει να διαμορφώνονται με τέτοιο τρόπο ώστε να μην υπάρχουν κενά ασφαλείας[51].

Έρευνες έχουν δείξει ότι στόχος είναι κάθε επιχείρηση η οποία διατηρεί ευαίσθητες πληροφορίες. Το 60% των επιθέσεων σε εταιρείες και οργανισμούς γίνονται εσωτερικά από τους ίδιους τους υπαλλήλους της επιχείρησης.

[51] Rash, Michael et al,2005

Κεφάλαιο 4

Οικογένεια προτύπων συστημάτων ασφαλείας ISO/IEC 27000

4.1. Εισαγωγή

Όπως διαπιστώσαμε στο προηγούμενο κεφάλαιο, τα συστήματα ασφαλείας είναι ένα σημαντικό θεμέλιο της σωστής λειτουργίας των οργανισμών και των επιχειρήσεων.

Με την τεχνολογία να έχει αναπτυχθεί και τις περισσότερες επικοινωνίες ανάμεσα στους διάφορους τομείς ενός οργανισμού να γίνονται διαδικτυακά, η ασφάλεια των πληροφοριακών συστημάτων γίνεται όλο και πιο δύσκολη και αποτελεί απαιτητική εργασία[52].

Για να καταφέρουμε να μειώσουμε τους κινδύνους και να αποφύγουμε τις ζημίες που θα υπάρξουν στις επιχειρήσεις από κάποια επίθεση στα πληροφοριακά τους συστήματα θα πρέπει να εξασφαλίσουμε στο μέγιστο βαθμό την ασφάλεια των πληροφοριών[53]

Τα πρότυπα ISO 27000, ISO 27001 και ISO 27002 έχουν αναπτυχθεί για να παρέχουν προστασία στα πληροφοριακά συστήματα και στις πληροφορίες που μεταφέρονται μέσω των συστημάτων αυτών. Τα πρότυπα αυτά έχουν

[52] Hansen, M., 2016
[53] BSI, 2005

κατασκευαστεί με τέτοιο τρόπο ώστε να προσφέρουν όλους τους απαραίτητους, γενικούς και ειδικούς, ελέγχους καθώς και τις βάσεις για να πετύχουμε την άρτια ασφάλεια των πληροφοριών του οργανισμού[54].

Έτσι, το ISO 27001, λειτουργεί ως μέτρο πιστοποίησης του οργανισμού, βάσει των προτύπων ασφαλείας. Στα πλαίσια του ISO 27001 η ασφάλεια των πληροφοριών αντιμετωπίζεται ως το μέγιστο ζητούμενο[55].

Επίσης, μέσω του ISO 27001 μετράται η ασφάλεια των πληροφοριακών συστημάτων ενός οργανισμού και προάγεται η εμπιστοσύνη του καταναλωτικού κοινού στον εκάστοτε οργανισμό[56].

Τέλος, με το ISO 27001 το οποίο συμμορφώνεται με τα διεθνή πρότυπα περί ασφάλειας πληροφοριών, μειώνεται κατά πολύ ο κίνδυνος επιβολής κυρώσεων στους οργανισμούς. Επιπροσθέτως, ελαχιστοποιούνται οι περιπτώσεις χρηματικών αποζημιώσεων λόγω νομικών διαρροών[57]

Στη συνέχεια θα παρουσιάσουμε κάποια γενικά στοιχεία καθώς και την ιστορική αναδρομή των προτύπων ασφαλείας ISO 27000 έως ISO 27002[58].

4.2. Γενικά στοιχεία

Η κατασκευή των προτύπων ασφαλείας γίνεται μέσα από λεπτομερείς περιγραφές των χαρακτηριστικών ενός προϊόντος. Οι περιγραφές αυτές δίνονται από ειδικούς εμπειρογνώμονες και διάφορους επιστημονικούς φορείς[59].

Τα πρότυπα που έχουν δημιουργηθεί έχουν συγκεκριμένα χαρακτηριστικά τα οποία ανταποκρίνονται στην παρεχόμενη ασφάλεια, στην αξιοπιστία και στην ποιότητα, καθώς και στο ότι θα πρέπει να ισχύουν για μεγάλο χρονικό διάστημα[60].

[54] Danziger, J. N., & Andersen, K. V., 2002
[55] Danziger, J. N., & Andersen, K. V., 2002
[56] Pelnekar, 2011
[57] Pelnekar, 2011
[58] De Vivo, M., de Vivo, G. O., & Germinal, I., 1998
[59] Almarabeh, T., & AbuAli, A., 2010
[60] Almarabeh, T., & AbuAli, A., 2010

4.3. Ιστορική αναδρομή

4.3.1. Τέλη της δεκαετίας του '80: Ολλανδική Βασιλεία / Εγχειρίδιο Πολιτικής Ασφάλειας Πληροφοριών του ομίλου Shell

Ο όμιλος Shell έδωσε στη δημοσιότητα ένα εσωτερικό έγγραφο και το δώρισε στην κοινότητα. Πάνω στο έγγραφο αυτό στηρίχτηκε αρχικά το BS 7799 και αργότερα το ISO27K στο σύνολο του[61].

Το 1995 δημοσιεύεται για πρώτη φορά το BS 7799, στο οποίο δίνεται ιδιαίτερη έμφαση στη σημασία της ασφάλειας των πληροφοριακών συστημάτων. Βασική έλλειψη της δημοσίευσης εκείνης ήταν οι αναφορές στο διαδίκτυο, παρότι το ίντερνετ είχε ενταχθεί στις λειτουργίες των μεγάλων οργανισμών από τα τέλη της δεκαετίας του 1980 ήδη[62].

Η έλλειψη αυτή υπάρχει ακόμα και στο επικαιροποιημένο ISO27K, καθώς πολλές από τις διαδικασίες του δεν αναφέρονται σαφώς στο διαδίκτυο και στους κινδύνους αυτού στην προσπάθεια της διασφάλισης των πληροφοριών και των πληροφοριακών συστημάτων[63].

4.3.2. 1989: Κώδικας Πρακτικής Χρήσης του Υπουργείο Εμπορίου και Βιομηχανίας - Κέντρο Ασφάλειας Εμπορικών Υπολογιστών DTI CCSC (πρώτη δημοσίευση μετά την Shell)

Το Υπουργείο Εμπορίου και Βιομηχανίας και το Κέντρο Ασφαλείας Εμπορικών Υπολογιστών (Department of Trade and Industry's Commercial Computer Security Centre, DTI-CCSC) της Μεγάλης Βρετανίας ανέπτυξε και δημοσίευσε τον Κώδικα Πρακτικής Χρήσης (CCSC)με στόχο την ασφάλεια των πληροφοριών των οργανισμών που ήταν και μέλη του.

[61] ISO27K Forum, 2017
[62] ISO27K Forum, 2017
[63] ISO27K Forum, 2017

Ο Κώδικας Πρακτικής Χρήσης βασίστηκε στη δημοσίευση της εταιρείας Shell σχετικά με την ασφάλεια των πληροφοριών σε ένα μεγάλο οργανισμό[64].

4.3.3. 1993: BSI-DISC PD003 - Κώδικας Πρακτικής DTI για τη διαχείριση της ασφάλειας πληροφοριών - πρώτη δημόσια κυκλοφορία.

Όσο όλοι ανέμεναν την επίσημη κυκλοφορία του πρώτου βρετανικού προτύπου ασφαλείας, είχαμε την προέκδοση των κύριων μερών του BS 7799 από το Υπουργείο Εμπορίου και Βιομηχανίας του Ηνωμένου Βασιλείου. Η προέκδοση αυτή έγινε από το Βρετανικό Ινστιτούτο Προτύπων (British Standards Institute, BSI)[65].

Το σύνολο των μερών που πρωτοεκδόθηκαν ονομάστηκαν BSI-DISC PD003 (BSI – Παροχή Πληροφοριακών Λύσεων Προς Πελάτες - Δημόσιο Έγγραφο 003) και αποτελούσαν δωρεάν πληροφοριακό υλικό[66].

Σημαντικό ρόλο στην ανάπτυξη του PD003 έπαιξε ο Edward Humphreys, διευθυντής του Εθνικού Κέντρου Πληροφορικής του Ηνωμένου Βασιλείου (NCC), ο οποίος συνεργάστηκε με τους υπεύθυνους ασφαλείας μεγάλων εταιρειών όπως η BOC, τα Marks and Spencer, η την Shell και η British Telecom[67].

Πολλοί ήταν οι οργανισμοί οι οποίοι έσπευσαν να στηρίξουν το PD003, με σημαντικότερο το πρακτορείο ειδήσεων Reuters και τον βρετανικό τραπεζικό όμιλο TSB Bank[68].

Δύο χρόνια αργότερα κυκλοφόρησε από την BSI-DISC το PD005. Το PD005 ήταν μια περιληπτική έκδοση του PD003, η οποία δεν υπάρχει σε κανένα από τα αρχεία του ISO27K.

Το Υπουργείο Εμπορικών Επιχειρήσεων και Ρυθμιστικών Μεταρρυθμίσεων . (Department for Business Enterprise and Regulatory Reform, BERR) πήρε τη

[64] ISO27K Forum, 2017
[65] ISO27K Forum, 2017
[66] ISO27K Forum, 2017
[67] ISO27K Forum, 2017
[68] ISO27K Forum, 2017

θέση του Υπουργείου Εμπορίου και Βιομηχανίας (DTI) αλλά εξακολουθεί να στηρίζει τα πρότυπα ISO27K από ο 1995 έως και τις ημέρες μας.

4.3.4. BS7799:1995 – Αρχική Έκδοση ως Βρετανικό Πρότυπο

Το 1995 εκδίδεται από το Βρετανικό Ινστιτούτο Πιστοποίησης (British Standards Institute, BSI) το πρώτο Βρετανικό Πρότυπο Ασφαλείας το οποίο ονομάζεται BS7799:1995-«Κώδικας πρακτικής για διαχείριση ασφαλείας πληροφοριών (Code of Practice for Information Security Management)»[69].

4.3.5. BS 7799 Μέρος 1: 1998 – Μετονομασία

Το BS 7799 αρχικά μετονομάστηκε σε BS 7799 Μέρος I και αργότερα μετονομάστηκε σε ISO / IEC 27001, το 1998[70].

4.3.6. BS 7799 Μέρος 1: 1999 – Αναθεώρηση

Από το 1998 έως και το 1999 υπήρξε μια διαδικασία αναθεώρησης του BSI το οποίο και επανεκδόθηκε στα τέλη του 1999[71].

4.3.7. ISO / IEC 17799: 2000 - πρώτη έκδοση ISO / IEC του BS7799-1

Το έτος κατά το οποίο είχαμε την αναθεώρηση του BSI ήταν μια δύσκολη και απαιτητική περίοδος για την οικογένεια προτύπων ασφαλείας. Το 1999 αναθεωρείται και επανεκδίδεται το BS 7799, το οποίο ένα χρόνο μετά, τον Δεκέμβριο του 2000 ενσωματώνεται στο ISO / IEC και επαναδημοσιεύεται ως ISO / IEC 17799[72].

[69] Καρδάρη, 2011
[70] Middleton, M. R., 2007
[71] ISO27K Forum, 2017
[72] ISO27K Forum, 2017

Η επαναδημοσίευση αυτή δε βρήκε αρχικά σύμφωνα όλα τα μέλη του Διεθνούς Οργανισμού Τυποποίησης – ISO- αλλά τελικά αποδείχτηκε ένα κοινό σημείο εκκίνησης μέχρι να έρθει η περαιτέρω ανάπτυξη[73].

4.3.8. ISO / IEC 17799:2005

Πέντε χρόνια μετά την πρώτη δημοσίευση του ISO / IEC 17799:2000, η έκδοση επικαιροποιείται και επαναδημοσιεύεται. Πιο συγκεκριμένα, τον Ιούνιο του 2005 έχουμε τη δημοσίευση του ISO / IEC 17799:2005 στο οποίο περιλαμβάνονται όλες οι αναθεωρήσεις που είχαν γίνει κατά την προηγούμενη πενταετία καθώς και το σύνολο των συμβουλών για τη διαχείριση των κινδύνων ασφαλείας των πληροφοριακών συστημάτων[74].

4.3.9. ISO/IEC 27002:2005

Στα μέσα του 2007 το πρότυπο ISO / IEC 17799: 2005 μετονομάζεται σε ISO / IEC 27002: 2005 και γίνεται πλέον, και επίσημα, μέλος της οικογένειας των προτύπων ασφαλείας ISO / IEC 27000[75].

Ανάμεσα στα κείμενα των δύο προτύπων ασφαλείας δεν υπάρχει καμία διαφορά. Μάλιστα, για μεγάλο χρονικό διάστημα, σε όποιον ζητούσε το ISO / IEC 27002 παραδιδόταν το κείμενο του ISO / IEC 17799: 2005 μαζί με ένα φύλλο επικύρωσης στο οποίο καταγραφόταν η αλλαγή της ονομασίας[76].

4.3.10. ISO / IEC 27001:2013 και 27002:2013 - νέες εκδόσεις

Το 2013 έχουμε την αναδημοσίευση του αναθεωρημένου ISO / IEC 27001 και 27002. Ήταν μια διαδικασία η οποία καθυστέρησε πολύ να ολοκληρωθεί καθώς κατά τη διάρκεια της αντιμετωπίστηκαν σχεδόν ανυπέρβλητα προβλήματα.[77]

[73] ISO27K Forum, 2017
[74] ISO27K Forum, 2017
[75] ISO27K Forum, 2017
[76] ISO27K Forum, 2017
[77] ISO27K Forum, 2017

Η αναθεώρηση του 27001 ήταν αναγκαστική, καθώς το πρότυπο έπρεπε να ευθυγραμμιστεί με τα υπόλοιπα πρότυπα των συστημάτων διαχείρισης ISO[78]

[78] ISO27K Forum, 2017

Κεφάλαιο 5

ISO / IEC 27001:2013

5.1 Εισαγωγή

Το πρότυπο ISO / IEC 27000 είναι μια σειρά προτύπων τα οποία, όταν χρησιμοποιούνται μαζί, καθορίζουν την πλήρη υλοποίηση. Η σειρά εξακολουθεί να βρίσκεται σε εξέλιξη, ενώ τέσσερα από τα προτεινόμενα πρότυπα δημοσιεύονται αυτή τη στιγμή. Οι εργασίες προχωρούν στην ολοκλήρωση των υπολοίπων προτύπων ISO / IEC 27000 σύμφωνα με το ISO / IEC 27010. Αυτά καλύπτουν τις θεμελιώδεις απαιτήσεις ενός ISMS, εφαρμόζονται σε οποιοδήποτε τομέα και μπορούν να εφαρμοστούν σε κάθε οργανισμό ανεξάρτητα από το μέγεθος, τη δομή ή τον σκοπό . Οι αριθμοί ISO / IEC μετά από αυτό έχουν δεσμευτεί για συγκεκριμένες τομεακές κατευθυντήριες γραμμές εφαρμογής, οι περισσότερες από τις οποίες βρίσκονται ακόμη στο στάδιο προγραμματισμού ή προετοιμασίας. Το παράρτημα συνοψίζει την εξέλιξη της σειράς μέχρι σήμερα.

Η συμμόρφωση με τα πρότυπα ISO παρέχει στις εταιρείες πιστοποίηση που αποδεικνύει ότι η εταιρεία συμμορφώνεται με τις απαιτήσεις αυτού του καλά αναγνωρισμένου προτύπου. Παρέχει επίσης στους υπαλλήλους και στους πελάτες περισσότερη βεβαιότητα ότι τα δεδομένα τους είναι ασφαλή με την εταιρεία. Σε ορισμένες περιπτώσεις, οι εταιρείες ενδέχεται να απαιτούν πιστοποίηση ISO για την επιχειρηματική τους δραστηριότητα. Το πρότυπο ISO 27000 περιέχει πολλές χρήσιμες συστάσεις και οι εταιρείες ενθαρρύνονται να εξοικειωθούν με τις συστάσεις, ακόμη και αν δεν σχεδιάζουν να γίνουν πιστοποιημένοι. Η απόκτηση του προτύπου κοστίζει χρήματα για να αποκτήσει. Ωστόσο, οι εξειδικευμένοι επαγγελματίες συμμόρφωσης μπορούν να βοηθήσουν στην προετοιμασία για την προσπάθεια συμμόρφωσης.

Το ISO 27000 αποτελείται από έξι μέρη που περιγράφουν τις απαιτήσεις πιστοποίησης, κατευθυντήριες γραμμές για την επίτευξη των απαιτήσεων και κατευθυντήριες γραμμές για τους οργανισμούς διαπίστευσης. Το πρότυπο παρέχει πολλές χρήσιμες συστάσεις για εταιρείες που ζητούν πιστοποίηση καθώς και όσους ενδιαφέρονται μόνο για τη βελτίωση της ασφάλειάς τους. Παρόμοια με το πρότυπο ποιότητας ISO 9000, το ISO 27000 είναι προαιρετικό αλλά σύντομα μπορεί να είναι επιχειρηματική απαίτηση.

Τα βασικά έγγραφα της σειράς είναι το ISO / IEC 27001, το οποίο καθορίζει τις απαιτήσεις για ένα ISMS και ISO / IEC 27002, το οποίο καθορίζει κατευθυντήριες γραμμές και αρχές για την εφαρμογή. Αυτά τα πρότυπα βασίζονται στο μοντέλο Plan-Do-Check-Act (PDCA) για συνεχή έλεγχο και βελτίωση του ποιοτικού ελέγχου. Το ISMS μπορεί να ελεγχθεί σύμφωνα με το ISO / IEC 27001 και να πιστοποιηθεί για συμμόρφωση. Πιστοποίηση τρίτου μέρους διατίθεται από διάφορους διαπιστευμένους παρόχους και συνήθως διαρκεί 3 χρόνια. Η υποστήριξη για τη βελτίωση μιας εφαρμογής συνήθως παρέχεται καθ 'όλη την περίοδο πιστοποίησης.

Το 2013 έχουμε τη δημοσίευση της αναθεωρημένης έκδοσης του ISO 27001 με τον τίτλο «Τεχνολογία πληροφοριών - Τεχνικές ασφαλείας - Συστήματα διαχείρισης ασφάλειας πληροφοριών – Απαιτήσεις»[79].

Οι βασικές δομές του ISO / IEC 27001 αναθεωρούνται και έτσι το πρότυπο ασφαλείας επικαιροποιείται βάσει του παραρτήματος SL των οδηγιών ISO / IEC. Στόχος της επικαιροποίησης αυτής είναι η υιοθέτηση αυτού του τύπου ασφαλείας από όλα τα πρότυπα πριν την τελική τους αναθεώρηση.

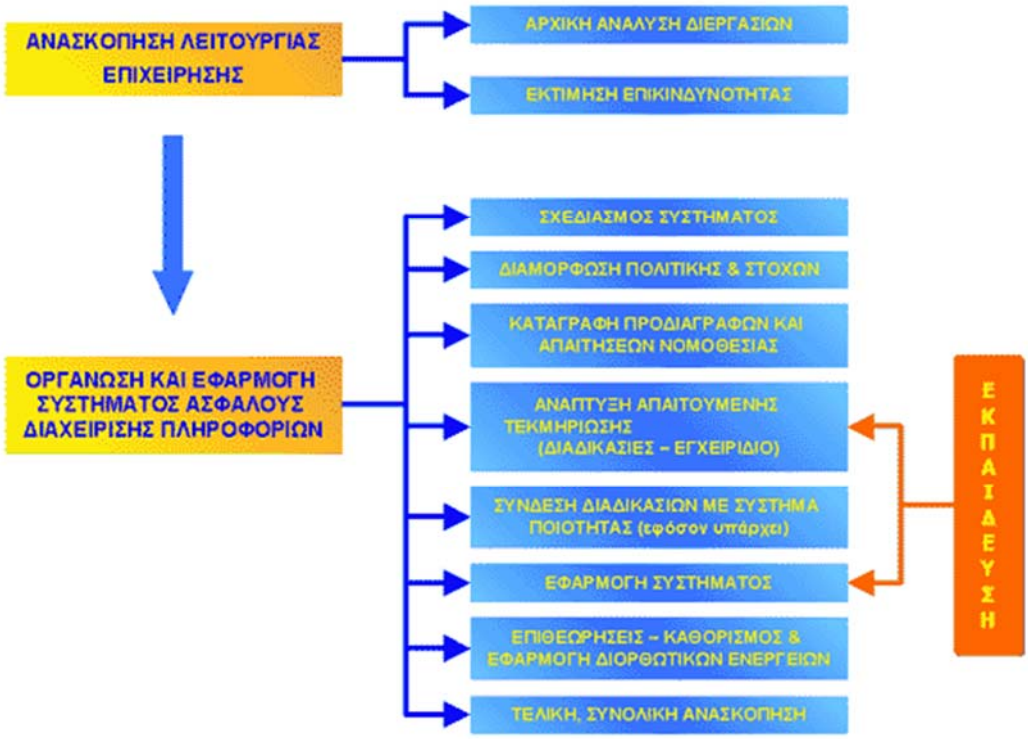
Στα πλαίσια της αναθεώρησης οι αριθμοί και οι τίτλοι των προτύπων ασφαλείας ISO παραμένουν ίδια και στην εισαγωγή καθώς και στις παραπομπές εισάγονται κάποιες συγκεκριμένες λεπτομερείς οδηγίες περί πειθαρχίας[80].

Το γεγονός αυτό προσφέρει συνοχή στους οργανισμούς που διαθέτουν ολοκληρωμένα συστήματα διαχείρισης της ασφάλειας των πληροφοριών στηριζόμενα σε πρότυπα όπως το ISO 9001[81].

[79] ISO/IEC 27000, 2016
[80] ISO/IEC 27000, 2016

5.2 Δομή του Προτύπου

Η μεθοδολογία που εφαρμόζεται για το σχεδιασμό και την εγκατάσταση συστημάτων σύμφωνα με το πρότυπο ISO 27001 αποτυπώνεται στο σχήμα, που ακολουθεί:



Το Το ISO / IEC 27001: 2013 αποτελείται από τις παρακάτω ενότητες:

- Εισαγωγή

Στην εισαγωγή του ISO / IEC 27001: 2013 γίνονται οι πρώτες αναφορές σχετικά με τις διαδικασίες ασφαλείας[82].

- Πεδίο εφαρμογής

[81] ISO/IEC 27000, 2016
[82] ISO/IEC 27000, 2016

Στο πεδίο εφαρμογής του ISO / IEC 27001: 2013 καθορίζονται οι γενικές απαιτήσεις του ISMS που υπάρχουν σε όλους τους οργανισμούς[83]

- Κανονιστικές αναφορές

Στις κανονιστικές αναφορές του ISO / IEC 27000 αναφέρονται όλες οι απαραίτητες πληροφορίες σχετικά με την οικογένεια προτύπων ασφαλείας

- Ορισμοί

Στο πεδίο των όρων και των ορισμών υπάρχει ένα επίσημο και περιεκτικό γλωσσάριο. Λίγο καιρό μετά αντικαταστάθηκε από το ISO / IEC 27000:2016[84]

- Πλαίσιο λειτουργίας του οργανισμού

Στο πλαίσιο λειτουργία του οργανισμού δίνονται όλες οι απαραίτητες διευκρινήσεις για να κατανοηθεί πλήρως το οργανωτικό πλαίσιο των αναγκών και των προσδοκιών από το πρόγραμμα ασφαλείας. Επίσης, στο πλαίσιο λειτουργίας του οργανισμού καθορίζεται και το πεδίο εφαρμογής του ΣΔΑΠ - ISMS[85].

- Ηγεσία

Στην ηγεσία ανήκει η ανώτατη διοίκηση του οργανισμού. Τα άτομα που έχουν ηγετικό ρόλο πρέπει να έχουν και ηγετικές θέσεις, να δεσμεύονται στο ΣΔΑΠ - ISMS, να παίρνουν πολιτικές αποφάσεις και να αναθέτουν τους ρόλους σχετικά με την ασφάλεια των πληροφοριών[86].

- Σχεδιασμός

Στα πλαίσια του σχεδιασμού εντάσσονται όλες οι διαδικασίες που σχετίζονται με την αναγνώριση των κινδύνων, την ανάλυση τους και το σχεδιασμό των κατάλληλων μέσων αντιμετώπισης των κινδύνων αυτών. Τέλος, όσοι

[83] ISO/IEC 27000, 2016
[84] ISO/IEC 27000, 2016
[85] ISO/IEC 27000, 2016
[86] ISO/IEC 27000, 2016

ασχολούνται με το σχεδιασμό έχουν ως αρμοδιότητα και την αποσαφήνιση των στόχων της ασφάλειας των πληροφοριών[87].

- Υποστήριξη

Προκειμένου να εφαρμοστούν τα σχέδια ασφάλειας των πληροφοριών και των πληροφοριακών συστημάτων θα πρέπει να είναι διαθέσιμοι οι απαραίτητοι πόροι. Επίσης, θα πρέπει να ετοιμαστούν και να ελεγχθούν τα απαραίτητα έγγραφα σχετικά με τις κινήσεις περί ασφάλειας των πληροφοριακών συστημάτων[88].

- Λειτουργία

Στα πλαίσια της λειτουργίας δίνονται όλες οι λεπτομέρειες σχετικά με την ταξινόμηση και την αντιμετώπιση των κινδύνων των πληροφοριακών συστημάτων. Επίσης, καταγράφονται οι λεπτομέρειες σχετικά με τη διαχείριση των αλλαγών που είναι απαραίτητες να γίνουν για να εξασφαλιστεί η μέγιστη δυνατή ασφάλεια των πληροφοριακών συστημάτων. Η κοινοποίηση των στοιχείων αυτών γίνεται με σκοπό να είναι εφικτοί όλοι οι απαραίτητοι έλεγχοι από τους ελεγκτές πιστοποίησης[89].

- Αξιολόγηση της απόδοσης

Στα πλαίσια της αξιολόγησης της απόδοσης έχουμε τις μετρήσεις, τις αναλύσεις και τις αξιολογήσεις των συστημάτων ασφαλείας. Παράλληλα, επανεξετάζονται οι διαδικασίες που ακολουθούνται κατά την εφαρμογή των ελέγχων ασφαλείας. Σκοπός της επανεξέτασης αυτής είναι η συνεχής βελτίωση των συστημάτων ασφαλείας [90].

- Βελτίωση

Στόχος της βελτίωσης είναι η αξιολόγηση των ευρημάτων που προκύπτουν κατά την αξιολόγηση της απόδοσης καθώς και οι αναθεωρήσεις, όταν αυτό κρίνεται απαραίτητο. Με τον τρόπο αυτό έχουμε συνεχείς βελτιώσεις στο ΣΔΑΠ – ISMS.

[87] ISO/IEC 27000, 2016
[88] ISO/IEC 27000, 2016
[89] ISO/IEC 27000, 2016
[90] ISO/IEC 27000, 2016

- Παράρτημα Α

Στο Α Παράρτημα έχουμε την καταγραφή όλων των ελέγχων και των στόχων αναφοράς. Μέσα στις καταγραφές του Παραρτήματος αναφέρεται ρητά ότι οι πιστοποιημένοι οργανισμοί έχουν τη δυνατότητα να αξιοποιήσουν το ISO / IEC 27002, ενώ παράλληλα τους δίνεται η δυνατότητα να κάνουν κάποιες αλλαγές ή κάποιες διορθώσεις ώστε να γίνει όσο το δυνατόν αποτελεσματικότερο για τον οργανισμό τους[91].

- Βιβλιογραφία

Στο τελευταίο μέρος του προτύπου αναγράφεται η βιβλιογραφία. Στη βιβλιογραφία περιλαμβάνονται και τα πέντε σχετικά πρότυπα ασφαλείας και το πρώτο μέρος από τις οδηγίες του ISO / IEC[92].

5.3.Μετρήσεις

Ο όρος «μετρήσει» δε χρησιμοποιείται ποτέ στην έκδοση του ISO / IEC 27001:2013. Παρόλα αυτά στη συγκεκριμένη έκδοση θεωρούνται απαραίτητες οι μετρήσεις με τις οποίες ελέγχεται η απόδοση και η αποτελεσματικότητα του προτύπου καθώς και τα στοιχεία ελέγχου ασφαλείας των οργανισμών που εφαρμόζουν το πρότυπο[93].

5.4. Γενικά επί της πιστοποίησης

Η πιστοποίηση βάσει του ISO / IEC 27001 είναι προαιρετική για τους οργανισμούς. Ωστόσο, όσο περνάει ο καιρός, τόσο οι προμηθευτές όσο και οι συνεργάτες των οργανισμών φαίνεται να ανησυχούν για την ασφάλεια των πληροφοριών τους και να απαιτούν αυτή την πιστοποίηση από τους οργανισμούς.

Η ευελιξία των ψηφιακών πληροφοριών μπορεί να θεωρηθεί ως μια μεγάλη δύναμη. Δεδομένου ότι το λογισμικό και το υλικό αναπτύσσονται, τα δεδομένα

[91] ISO/IEC 27000, 2016
[92] ISO/IEC 27000, 2016
[93] ISO/IEC 27000, 2016

μπορούν να δημιουργηθούν, να προσεγγιστούν, να επεξεργαστούν, να διακινηθούν και να μοιραστούν με μεγαλύτερη ευκολία. Το συμπέρασμα είναι ότι τα δεδομένα είναι ευάλωτα σε μη εξουσιοδοτημένη πρόσβαση, αλλοίωση ή χειραγώγηση, τα οποία χωρίς έλεγχο μπορούν εύκολα να μη εντοπιστούν και να υπονομεύσουν τον αυθεντικό χαρακτήρα τους. Η επιτυχής ψηφιακή επιδιόρθωση διασφαλίζει ότι τα δεδομένα διαχειρίζονται και προστατεύονται έτσι ώστε η εξουσία τους να διατηρείται και να διατηρείται καθ 'όλη τη διάρκεια του κύκλου ζωής του. Για να είναι αυθεντικά τα δεδομένα πρέπει να παραμένουν αυθεντικά, αξιόπιστα και χρησιμοποιήσιμα, διατηρώντας ταυτόχρονα την ακεραιότητά τους. Αυτά τα χαρακτηριστικά των δεδομένων μπορούν να διατηρηθούν μέσω της εφαρμογής ενός αποτελεσματικού Συστήματος Διαχείρισης της Ασφάλειας Πληροφοριών (ISMS). Οι πολιτικές, οι διαδικασίες, οι ανθρώπινοι και μηχανολογικοί πόροι που αποτελούν ένα ISMS θα πρέπει να διασφαλίζουν ότι η Τριάδα της CIA - εμπιστευτικότητα, ακεραιότητα και διαθεσιμότητα - διατηρείται σε επίπεδο σωματικής, προσωπικής και οργανωτικής οργάνωσης ενός οργανισμού. Η εμπιστευτικότητα εξασφαλίζει ότι τα δεδομένα είναι διαθέσιμα μόνο σε όσους έχουν εξουσιοδοτηθεί να έχουν πρόσβαση σε αυτά. Η ακεραιότητα διασφαλίζει ότι τα δεδομένα μπορούν να τροποποιηθούν μόνο από εξουσιοδοτημένα άτομα. Η διαθεσιμότητα απαιτεί από τα εξουσιοδοτημένα άτομα να έχουν πρόσβαση στα δεδομένα όταν χρειάζονται.

Ο οργανισμός ISO εξήγαγε το 2015 μια έρευνα, σύμφωνα με την οποία σε ένα έτος εκδόθηκαν περισσότερα από 27.000 πιστοποιητικά ISO / IEC 27001 σε παγκόσμια κλίμακα. Σε σχέση με το 2014 καταγράφηκε μια αύξηση 20% και οι τάσεις μέχρι και το 2020 φαίνεται να είναι ανοδικές[94]

Σύμφωνα με δηλώσεις των οργανισμών που πήραν την πιστοποίηση ISO το έκαναν διότι με την πιστοποίηση αυτή απέδειξαν ότι είναι ποιοτικοί και αξιόπιστοι οργανισμοί.

Η αξιολόγηση των προτύπων ασφαλείας ISO είναι ανεξάρτητη και διέπεται από μεγάλη αυστηρότητα. Παράλληλα, κατά τη διάρκεια της αξιολόγησης, έχουμε τη λεπτομερή διατύπωση των διαδικασιών υλοποίησης των προγραμμάτων

[94] ISO/IEC 27000, 2016

ασφαλείας. Το γεγονός αυτό σημαίνει πως βελτιώνεται διαρκώς η παρεχόμενη ασφάλεια των πληροφοριών και αυξάνονται τα οφέλη από την πρόληψη και την αντιμετώπιση των κινδύνων[95].

Επίσης, η αξιολόγηση γίνεται πάντα με έγκριση από τα ανώτατα στελέχη του εκάστοτε οργανισμού και αυτό είναι άλλο ένα γεγονός που επιτείνει τη σημασία της ασφάλειας[96].

Ένα ISMS μπορεί να πιστοποιηθεί σύμφωνα με το πρότυπο ISO / IEC 27001 από διάφορους διαπιστευμένους καταχωρητές παγκοσμίως. Η πιστοποίηση από αναγνωρισμένες εθνικές παραλλαγές του ISO / IEC 27001 (π.χ. JIS Q 27001, η ιαπωνική έκδοση) από διαπιστευμένο οργανισμό πιστοποίησης είναι ισοδύναμη με την πιστοποίηση κατά ISO / IEC 27001.

Σε ορισμένες χώρες, οι οργανισμοί που επαληθεύουν τη συμμόρφωση των συστημάτων διαχείρισης με συγκεκριμένα πρότυπα ονομάζονται "φορείς πιστοποίησης", ενώ σε άλλες αναφέρονται συνήθως ως "οργανισμοί καταχώρισης", "φορείς αξιολόγησης και καταχώρησης", "φορείς πιστοποίησης / καταχώρησης" και μερικές φορές "καταχωρητές".

Η πιστοποίηση ISO / IEC 27001 [5], όπως και άλλες πιστοποιήσεις του συστήματος διαχείρισης ISO, περιλαμβάνει συνήθως μια διαδικασία εξωτερικού ελέγχου τριών σταδίων που ορίζεται από τα πρότυπα ISO / IEC 17021 [6] και ISO / IEC 27006 [7]:

Το στάδιο 1 είναι μια προκαταρκτική, ανεπίσημη αναθεώρηση του ISMS, για παράδειγμα, έλεγχος της ύπαρξης και της πληρότητας βασικών εγγράφων, όπως η πολιτική ασφάλειας της πληροφόρησης του οργανισμού, η δήλωση εφαρμογής (SoA) και το σχέδιο θεραπείας κινδύνου (RTP). Αυτό το στάδιο χρησιμεύει για την εξοικείωση των ελεγκτών με την οργάνωση και αντίστροφα.

Το στάδιο 2 είναι ένας πιο λεπτομερής και τυπικός έλεγχος συμμόρφωσης, ο οποίος ελέγχει ανεξάρτητα το ISMS σε σχέση με τις απαιτήσεις που ορίζονται στο ISO / IEC 27001. Οι ελεγκτές θα αναζητήσουν αποδεικτικά στοιχεία για να

[95] ISO/IEC 27000, 2016
[96] ISO/IEC 27000, 2016

επιβεβαιώσουν ότι το σύστημα διαχείρισης έχει σχεδιαστεί και εφαρμοστεί σωστά και είναι στην πραγματικότητα σε λειτουργία για παράδειγμα επιβεβαιώνοντας ότι μια επιτροπή ασφάλειας ή παρόμοιο διαχειριστικό όργανο συνεδριάζει τακτικά για να επιβλέπει το ISMS). Οι έλεγχοι πιστοποίησης διεξάγονται συνήθως από τους επικεφαλής ελεγκτές ISO / IEC 27001. Περνώντας αυτό το στάδιο, το ISMS πιστοποιείται σύμφωνα με το ISO / IEC 27001.

Η συνεχής παρακολούθηση περιλαμβάνει επιθεωρήσεις ή ελέγχους παρακολούθησης για να επιβεβαιωθεί ότι ο οργανισμός εξακολουθεί να συμμορφώνεται με το πρότυπο. Η συντήρηση πιστοποίησης απαιτεί περιοδικούς ελέγχους επαναξιολόγησης για να επιβεβαιωθεί ότι το ISMS συνεχίζει να λειτουργεί όπως καθορίζεται και προορίζεται. Αυτά θα πρέπει να γίνονται τουλάχιστον ετησίως, αλλά (σε συμφωνία με τη διοίκηση) συχνά διεξάγονται συχνότερα, ιδιαίτερα όταν το ISMS εξακολουθεί να ωριμάζει.

Το πιστοποιητικό ISO έχει πολλές δυνατότητας στον τομέα του marketing και μέσω αυτού ο οργανισμός που το εφαρμόζει φαίνεται ότι θεωρεί πολύ σημαντική τη διασφάλιση των πληροφοριών που έχει στην κατοχή του. Παρά τη δεδομένη αξία του ISO, ωστόσο, η σημασία της διασφάλισης που προσφέρει το πιστοποιητικό αυτό είναι άρρηκτα συνδεδεμένη με το ΣΔΑΠ – ISMS. Αυτό σημαίνει πως δεν μπορούμε και δεν πρέπει να εμπιστευόμαστε άκριτα το πιστοποιητικό, αφού η αξιοπιστία του εξαρτάται από την ασφάλεια των πληροφοριών [97].

5.5. Οργανωτικοί ρόλοι, ευθύνες και αρχές

Πρέπει να αντιληφθούμε ότι υπάρχει πολύ στενή σχέση μεταξύ της τεχνολογίας και της διοίκησης. Η ανώτατη διοίκηση εξασφαλίζει ότι ανατίθενται και ανακοινώνονται οι αρμοδιότητες και οι αρχές σχετικά με τους ρόλους που σχετίζονται με την ασφάλεια των πληροφοριών. Όπως ορίζεται από το πρότυπο η ανώτατη διοίκηση αναθέτει την ευθύνη για:

[97] ISO/IEC 27000, 2016

α) τη διασφάλιση της συμμόρφωσης του συστήματος διαχείρισης της ασφάλειας πληροφοριών με τις απαιτήσεις αυτού του διεθνούς προτύπου και

β) την υποβολή εκθέσεων σχετικά με την απόδοση του συστήματος διαχείρισης της ασφάλειας των πληροφοριών στην ανώτατη διοίκηση.

Το ISO / IEC 27000 καθορίζει τις απαιτήσεις για τη δημιουργία, τη διαχείριση, την τεκμηρίωση και τη συνεχή βελτίωση ενός ISMS χρησιμοποιώντας μια προσέγγιση διαχείρισης κινδύνου, η οποία πρέπει να προκαθορίζεται από έναν οργανισμό. Οι αναθέτοντες φορείς έχουν εντολή να εντοπίζουν, να αναλύουν και να αξιολογούν τους κινδύνους και να τις μειώνουν σε αποδεκτό επίπεδο. Τα ενδεχόμενα για τη θεραπεία αυτών των κινδύνων επιλέγονται από πάνω από 130 ελέγχους που ορίζονται από το πρότυπο. Αυτά καλύπτουν μια σειρά τομέων όπου η ασφάλεια της πληροφορίας μπορεί να διακυβευθεί και να επικεντρωθεί στην προετοιμασία των κατάλληλων πολιτικών και διαδικασιών και στην τεκμηρίωση των διαδικασιών. Οι έλεγχοι περιλαμβάνουν: πολιτική ασφάλειας. θέματα προσωπικού · ζητήματα εξοπλισμού · ελέγχους πρόσβασης τόσο στον εξοπλισμό πληροφορικής όσο και στα δεδομένα. συμμόρφωση με τις νομικές απαιτήσεις και πρότυπα · την απόκτηση, την ανάπτυξη και τη συντήρηση του συστήματος · και τη διαχείριση της συνέχειας των επιχειρήσεων. Οι έλεγχοι δεν είναι εξαντλητικοί και μπορεί να προσαρμοστούν ή να αναπτυχθούν επιπλέον για συγκεκριμένη υλοποίηση.

Το πρότυπο ορίζει επίσης ότι ένα συμμορφούμενο σύστημα ISMS: θα καταδείξει τη δέσμευση της διοίκησης μέσω της διάθεσης πόρων, του αρμόδιου προσωπικού και της κατάρτισης. υποβάλλονται σε αναθεωρήσεις εσωτερικού ελέγχου και διαχείρισης · και αναλαμβάνει να βελτιώνει συνεχώς την αποτελεσματικότητα.

Οι χαρτογραφήσεις σε σχέση με τα σχετικά πρότυπα διαχείρισης ISO 9001 και ISO 14001 παρέχονται, για να διασφαλιστεί η συνοχή της προσέγγισης σε όλες τις υλοποιήσεις.

Το ISO παρέχει οδηγίες πρακτικής εφαρμογής και περαιτέρω πληροφορίες για κάθε έλεγχο που εντοπίστηκε. Περιλαμβάνει καθοδήγηση σχετικά με τον τρόπο επιλογής κατάλληλων ελέγχων για μια εφαρμογή, συμπεριλαμβανομένων

εκείνων που είναι απαραίτητοι για τη συμμόρφωση με τη νομοθεσία και εκείνων που απαιτούνται για τη βέλτιστη πρακτική.

5.6. Σχεδιασμός και δράσεις για την αντιμετώπιση των κινδύνων και των ευκαιριών

Κατά τον σχεδιασμό του συστήματος διαχείρισης της ασφάλειας των πληροφοριών, ο οργανισμός εξετάζει τα ζητήματα και τις απαιτήσεις, προσδιορίζει τους κινδύνους και τις ευκαιρίες που πρέπει να αντιμετωπιστούν με σκοπό:

α) να εξασφαλίσει ότι το σύστημα διαχείρισης της ασφάλειας των πληροφοριών μπορεί να επιτύχει τα επιδιωκόμενα αποτελέσματα

β) να αποτρέπουν ή να μειώνουν τις ανεπιθύμητες ενέργειες και

γ) επίτευξη συνεχούς βελτίωσης.

δ) να δράσει σωστά ως προς την αντιμετώπιση αυτών των κινδύνων και ευκαιριών

Ο οργανισμός ορίζει και εφαρμόζει μια διαδικασία αξιολόγησης κινδύνου ασφάλειας πληροφοριών που:

α) θεσπίζει και διατηρεί κριτήρια κινδύνου ασφάλειας πληροφοριών που περιλαμβάνουν:

1) τα κριτήρια αποδοχής κινδύνου και

2) κριτήρια για την εκτίμηση των κινδύνων ασφάλειας πληροφοριών

β) διασφαλίζει ότι οι επανειλημμένες αξιολογήσεις κινδύνου ασφάλειας πληροφοριών παράγουν συνεπή, έγκυρα και συγκρίσιμα αποτελέσματα

γ) εντοπίζει τους κινδύνους ασφάλειας πληροφοριών:

1) εφαρμόζει τη διαδικασία αξιολόγησης κινδύνου ασφάλειας πληροφοριών για τον εντοπισμό των κινδύνων που σχετίζονται με την απώλεια εμπιστευτικότητας, ακεραιότητας και διαθεσιμότητας πληροφοριών στο πλαίσιο του συστήματος διαχείρισης της ασφάλειας πληροφοριών και

2) εντοπίζει τους ιδιοκτήτες κινδύνου

δ) αναλύει τους κινδύνους ασφάλειας πληροφοριών:

1) να αξιολογήσει τις πιθανές συνέπειες που θα προέκυπταν εάν οι κίνδυνοι υλοποιούνταν

2) να εκτιμήσει την ρεαλιστική πιθανότητα εμφάνισης των κινδύνων και

3) καθορίζουν τα επίπεδα κινδύνου

ε) αξιολογεί τους κινδύνους ασφάλειας πληροφοριών:

1) συγκρίνουν τα αποτελέσματα της ανάλυσης κινδύνου με τα κριτήρια κινδύνου και

2) να δοθεί προτεραιότητα στους κινδύνους που αναλύονται για τη θεραπεία κινδύνου.

Ο οργανισμός διατηρεί τεκμηριωμένες πληροφορίες σχετικά με τη διαδικασία αξιολόγησης του κινδύνου ασφάλειας πληροφοριών.

5.7. Διαχείριση κινδύνου ασφάλειας πληροφοριών

Ο οργανισμός καθορίζει και εφαρμόζει μια διαδικασία επεξεργασίας κινδύνου ασφάλειας πληροφοριών για:

α) να επιλέξουν τις κατάλληλες επιλογές αντιμετώπισης κινδύνου ασφάλειας πληροφοριών, λαμβάνοντας υπόψη τα αποτελέσματα της αξιολόγησης κινδύνου

β) καθορίζει όλους τους ελέγχους που είναι απαραίτητοι για την εφαρμογή της επιλογής επιλογής αντιμετώπισης κινδύνου ασφάλειας πληροφοριών

γ) να συγκριθούν οι ανωτέρω έλεγχοι και να επαληθευθεί ότι δεν έχουν παραλειφθεί οι αναγκαίοι έλεγχοι

δ) να καταρτίσει Δήλωση Εφαρμογής που να περιέχει τους αναγκαίους ελέγχους και αιτιολόγηση των εγκλεισμάτων, ανεξάρτητα από το εάν εφαρμόζονται ή όχι

ε) να διατυπώσει ένα σχέδιο θεραπείας κινδύνου ασφάλειας πληροφοριών

στ) να λαμβάνουν έγκριση από τους κατόχους κινδύνων για το σχέδιο θεραπείας κινδύνου ασφάλειας πληροφοριών και την αποδοχή των κινδύνων υπολειπόμενης ασφάλειας πληροφοριών.

Ο οργανισμός διατηρεί τεκμηριωμένες πληροφορίες σχετικά με τη διαδικασία διαχείρισης κινδύνου ασφάλειας πληροφοριών.

5.8. Επιχειρησιακός προγραμματισμός και έλεγχος

Ο οργανισμός σχεδιάζει, εφαρμόζει και ελέγχει τις διαδικασίες που απαιτούνται για την ικανοποίηση των απαιτήσεων ασφάλειας πληροφοριών και την υλοποίηση των δράσεων. Ο οργανισμός εφαρμόζει επίσης σχέδια για την επίτευξη των στόχων της ασφάλειας των πληροφοριών.

Πρέπει να φυλάσσονται τεκμηριωμένες πληροφορίες στο βαθμό που απαιτείται για να έχει εμπιστοσύνη ότι οι διεργασίες έχουν διεξαχθεί όπως είχε προγραμματιστεί. Ο οργανισμός ελέγχει τις προγραμματισμένες αλλαγές και επανεξετάζει τις συνέπειες των ακούσιων αλλαγών, λαμβάνοντας μέτρα για την άμβλυνση τυχόν δυσμενών επιπτώσεων, ανάλογα με τις ανάγκες. Ο οργανισμός εξασφαλίζει ότι οι διεργασίες που ανατίθενται σε τρίτους καθορίζονται και ελέγχονται.

Είναι απαραίτητο να εκτελούνται αξιολογήσεις κινδύνου ασφάλειας πληροφοριών σε προγραμματισμένα χρονικά διαστήματα ή όταν προτείνονται ή λαμβάνουν χώρα σημαντικές αλλαγές λαμβάνοντας υπόψη τα κριτήρια. Ο

οργανισμός διατηρεί τεκμηριωμένη πληροφόρηση σχετικά με τα αποτελέσματα των αξιολογήσεων κινδύνου ασφάλειας πληροφοριών.

Τέλος εφαρμόζετε το σχέδιο θεραπείας κινδύνου πληροφόρησης. Ο οργανισμός διατηρεί τεκμηριωμένες πληροφορίες σχετικά με τα αποτελέσματα της αντιμετώπισης του κινδύνου ασφάλειας πληροφοριών.

5.9. Αξιολόγηση απόδοσης

Ο οργανισμός αξιολογεί τις επιδόσεις της ασφάλειας των πληροφοριών και την αποτελεσματικότητα του συστήματος διαχείρισης της ασφάλειας των πληροφοριών.

Η οργάνωση καθορίζει τι πρέπει να παρακολουθείται και να μετράται, συμπεριλαμβανομένων διαδικασιών και ελέγχων ασφάλειας της πληροφόρησης,τις μεθόδους παρακολούθησης, μέτρησης, ανάλυσης και αξιολόγησης, κατά περίπτωση, προκειμένου να εξασφαλιστούν έγκυρα αποτελέσματα όταν διενεργείται η παρακολούθηση και η μέτρηση το ποιος παρακολουθεί και μετρά όταν αναλύονται και αξιολογούνται τα αποτελέσματα από την παρακολούθηση και τη μέτρηση και τέλος το ποιος θα αναλύσει και θα αξιολογήσει αυτά τα αποτελέσματα.

Ο οργανισμός διατηρεί τις κατάλληλες τεκμηριωμένες πληροφορίες ως απόδειξη των αποτελεσμάτων παρακολούθησης και μέτρησης.

5.10. Βελτίωση - Μη συμμόρφωση και διορθωτικές ενέργειες

Σε περίπτωση μη συμμόρφωσης, ο οργανισμός πρέπει:

α) να αντιδράσει στη μη συμμόρφωση και, κατά περίπτωση:

1) να αναλάβει δράση για τον έλεγχο και τη διόρθωσή του

2) να ασχοληθεί με τις συνέπειες

β) να αξιολογήσει την ανάγκη για δράση για την εξάλειψη των αιτιών της μη συμμόρφωσης, προκειμένου να μην επαναληφθεί ή να συμβεί αλλού, με:

1) επανεξέταση της μη συμμόρφωσης

2) καθορισμός των αιτιών της μη συμμόρφωσης

3) προσδιορισμός εάν υπάρχουν παρόμοιες μη συμμορφώσεις ή θα μπορούσαν ενδεχομένως να συμβούν

γ) να εφαρμόσει κάθε απαραίτητη ενέργεια

δ) επανεξετάζει την αποτελεσματικότητα οποιωνδήποτε διορθωτικών μέτρων

ε) να πραγματοποιήσει αλλαγές στο σύστημα διαχείρισης της ασφάλειας των πληροφοριών, εάν είναι απαραίτητο.

Οι διορθωτικές ενέργειες πρέπει να είναι κατάλληλες για τις συνέπειες των μη συμμορφώσεων.

Ο οργανισμός διατηρεί τις τεκμηριωμένες πληροφορίες ως αποδεικτικά στοιχεία για:

στ) η φύση των μη συμμορφώσεων και οι τυχόν επακόλουθες ενέργειες που έχουν αναληφθεί, και

ζ) τα αποτελέσματα οποιασδήποτε διορθωτικής ενέργειας.

5.11. Τρωτά σημεία

Το θέμα ευπάθειας είναι ένα σημείο αδυναμίας ενός περιουσιακού στοιχείου ή μιας ομάδας περιουσιακών στοιχείων που μπορούν να αξιοποιηθούν από μία ή περισσότερες απειλές και τα αποτελέσματα ενδέχεται να θέσουν σε κίνδυνο την εμπιστευτικότητα, την ακεραιότητα ή / και τη διαθεσιμότητα των υπηρεσιών. Οι επιθέσεις είναι οι διαδικασίες εκμετάλλευσης μιας υπάρχουσας ευπάθειας. Οι επιθέσεις χωρίζονται σε δύο υποκατηγορίες με βάση την επίδρασή τους στις απαιτήσεις ασφάλειας, δηλαδή τις ενεργές και τις παθητικές επιθέσεις. Ονομάζονται ενεργά όταν οι επιθέσεις επηρεάζουν τις υπηρεσίες, θέτοντας σε κίνδυνο την ακεραιότητα ή τη διαθεσιμότητα και παθητικές όταν επηρεάζουν μόνο το εμπιστευτικό των πληροφοριών. Η ίδια η επίθεση αποτελεί απειλή για

το σύστημα πληροφοριών και κάθε απειλή έχει συγκεκριμένο κίνδυνο που βασίζεται στις ευπάθειες.[98]

Τα εξαρτήματα του hardware επηρεάζονται από υγρασία, σκόνη και ρύπανση, όπου η μη προστατευμένη αποθήκευση είναι μια άλλη ευπάθεια που πρέπει επίσης να ληφθεί υπόψη. Τα τρωτά σημεία του υλικού είναι σχετικά ευκολότερα ανιχνεύσιμα, αλλά η ζημιά μπορεί να είναι τεράστια και μη αναστρέψιμη. Μπορούμε να ελέγξουμε την ασφάλεια υλικού μέσω της παρακολούθησης και παρακολούθησης του υλικού, σε σχέση με την ασφάλεια του εξοπλισμού. Από την άλλη πλευρά, το λογισμικό είναι ευκολότερο να αξιοποιηθεί από τους εισβολείς λόγω ανεπαρκών δοκιμών και έλλειψης διαδρομής ελέγχου. Είναι δυνατό να χειριστούμε αυτές τις ευπάθειες κάνοντας εσωτερική / εξωτερική δοκιμή ευπάθειας, όπου μπορούμε να συνοψίσουμε μια λίστα προτεινόμενων διορθώσεων ή να χτίσουμε ένα ίχνος λογισμικού από την αρχή για να παρακολουθήσουμε τις ιδιότητες του λογισμικού ή να ελέγξουμε το τρέχον λογισμικό.

Τα πιο συχνά χρησιμοποιούμενα ευπάθειες από τους επιτιθέμενους είναι ευπάθειες δικτύου. Επειδή όλες οι εσωτερικές και εξωτερικές επικοινωνίες οποιασδήποτε εταιρείας βασίζονται σε ένα δίκτυο, οι μη προστατευόμενες γραμμές επικοινωνίας και ασφαλίζουν την αρχιτεκτονική του δικτύου είναι σοβαροί κίνδυνοι. Για να μειώσετε αυτήν την ευπάθεια, είναι σημαντικό να δημιουργήσετε με ασφάλεια την υποδομή δικτύου και να χρησιμοποιήσετε κατάλληλες μεθόδους καλωδίωσης με τον κατάλληλο τρόπο από την αρχή. Η χρήση ενός τείχους προστασίας είναι μια καλή ιδέα, αν και έχει τα δικά του προβλήματα.[99]

Οι κίνδυνοι του προσωπικού είναι πιο δύσκολο να διαχειριστούν, επειδή είναι αφηρημένοι. Οι κύριοι δείκτες κινδύνου αναφέρονται στους υποψήφιους που έχουν προσληφθεί και στους σημερινούς υπαλλήλους που δεν γνωρίζουν τη διαδικασία ασφάλειας. Ως απάντηση στην ευπάθεια των υπαλλήλων, οι

[98] Developing an ISO27001 Information Security Management System for an Educational Institute: Hashemite University as a Case Study

[99] Developing an ISO27001 Information Security Management System for an Educational Institute: Hashemite University as a Case Study

υπάλληλοι ελέγχου έχουν πρόσβαση στα συστήματα πληροφορικής, ορίζουν προνόμια πρόσβασης για όλους, εκπαιδεύουν τους υπαλλήλους για να αυξήσουν την ευαισθητοποίηση σχετικά με την ασφάλεια, συμπεριλαμβανομένης της δεοντολογίας και της χρήσης πολιτικών, καθώς και τα ξεχωριστά καθήκοντα των εργαζομένων, καθορίζοντας πρότυπα και κατευθυντήριες γραμμές για το προσωπικό ανάπτυξης του συστήματος.

Οι απροσδόκητες εξωτερικές απειλές, όπως η πλημμύρα και η αναξιόπιστη πηγή ενέργειας, είναι ευπάθειες ανάλογα με τον ιστότοπο. μια επιχείρηση θα πρέπει να συνειδητοποιήσει την εμφάνιση ενός κινδύνου, να θέσει τα απαραίτητα βήματα σχεδιασμού καταστροφών και να χρησιμοποιήσει γεννήτριες και εφεδρικά συστήματα ισχύος για να παρουσιάσει τα δεδομένα που χάθηκαν κατά την διακοπή ρεύματος. Η έλλειψη πολιτικών και διαδικασιών παρακολούθησης και ελέγχου προκαλεί οργανωτικές αδυναμίες. Για να τα μειώσει, ο οργανισμός θα πρέπει να κατασκευάσει προληπτικούς ελέγχους πληροφορικής. Πρέπει να γίνουν δοκιμές για την επιβεβαίωση και επικύρωση της ορθότητας των δεδομένων, του ελέγχου και της παρακολούθησης.

Υπό τον τεράστιο αριθμό επιθέσεων που μολύνουν πολλούς οργανισμούς και εταιρείες που προκλήθηκαν από την ύπαρξη τρωτών σημείων του συστήματος πληροφορικής, η αξιολόγηση ευπάθειας και η διείσδυση δοκιμών εντοπίστηκαν ως εργαλεία προσδιορισμού και ποσοτικοποίησης των σημείων αδυναμίας του συστήματος, προκειμένου να βελτιωθούν οι έλεγχοι ασφαλείας και οι υπηρεσίες που προστατεύουν πληροφοριών. Επίσης, κατανοούν καλύτερα τις αδυναμίες του υπάρχοντος συστήματος πληροφοριών. Η αξιολόγηση της ευπάθειας είναι η αξιολόγηση της υποδομής της τεχνολογίας της πληροφορίας του οργανισμού που τείνει να εντοπίσει την αδυναμία αυτών των συνιστωσών της υποδομής και τον τρόπο ελέγχου, προκειμένου να προστατευθεί από απειλές και επιθέσεις. Η αξιολόγηση ευπάθειας είναι μια σημαντική δραστηριότητα για την κατανόηση των περισσότερων από τις διάφορες ευπάθειες ενός συστήματος που μπορεί να θέσει σε κίνδυνο τα κρίσιμα πληροφοριακά του στοιχεία. Η δοκιμή διείσδυσης είναι η διαδικασία εκμετάλλευσης των εντοπισμένων σημείων αδυναμίας από έναν κακόβουλο χρήστη. Ο ελεγκτής πρέπει να συγκεντρώσει πληροφορίες, να

απαριθμήσει τις ευπάθειες, και τελικά να εκμεταλλευτεί τις δοσμένες αδυναμίες και να αποκτήσει πρόσβαση στο σύστημα.[100]

5.12. Πιστοποίηση έναντι συμμόρφωσης

Είναι δυνατό για μια οργάνωση να αναπτύξει το ISMS της μόνο σύμφωνα με το πρότυπο ISO 27000, διότι η αναγνωρισμένη καλή πρακτική είναι καθολικά εφαρμόσιμη. Επειδή δεν προοριζόταν να αποτελέσει τη βάση ενός συστήματος πιστοποίησης, ωστόσο, δεν διευκρινίζει τις απαιτήσεις συστήματος με τις οποίες ένα ISMS πρέπει να συμμορφώνεται, προκειμένου να πληροί τα κριτήρια πιστοποίησης.

Αυτές οι προδιαγραφές περιέχονται στο ISO 27001. Από τεχνική άποψη, αυτό σημαίνει ότι ένας οργανισμός που χρησιμοποιεί το ISO 27002 από μόνο του μπορεί να συμμορφωθεί με τις οδηγίες του κώδικα δεοντολογίας, αλλά δεν μπορεί να αποκτήσει έναν εξωτερικό φορέα για να επαληθεύσει ότι συμμορφώνεται με το πρότυπο. Ένας οργανισμός που χρησιμοποιεί το ISO 27001 και το ISO 27002 σε συνδυασμό μεταξύ τους μπορεί να σχεδιάσει ένα ISMS που είναι σύμφωνο με τις προδιαγραφές και το οποίο ακολουθεί την καθοδήγηση του κώδικα πρακτικής και ως εκ τούτου είναι ικανό να επιτύχει εξωτερική πιστοποίηση.[101]

Προκειμένου να επιτευχθεί διεθνώς αναγνωρισμένη πιστοποίηση, το ISMS πρέπει να ελεγχθεί από έναν οργανισμό που έχει εγκριθεί από τον αρμόδιο φορέα που συνδέεται με την EA και την IAF (στο Ηνωμένο Βασίλειο, αυτή είναι η υπηρεσία διαπίστευσης του Ηνωμένου Βασιλείου - UKAS). Επιπλέον, ο οργανισμός ελέγχου δεν μπορεί να είναι ο σύμβουλός σας - η συμμετοχή τους στο ISMS πρέπει να περιορίζεται στον έλεγχο τους.

[100] Developing an ISO27001 Information Security Management System for an Educational Institute: Hashemite University as a Case Study

[101] Information security & iso 27001, February 2013

5.13. Τεκμηρίωση συστήματος

Το πιο χρονοβόρο - και πιο κρίσιμο - μέρος του συνόλου του έργου είναι η ανάπτυξη της τεκμηρίωσης που καθορίζει τον τρόπο λειτουργίας του ISMS.

Υπάρχουν διάφορες προσεγγίσεις σε αυτό. Το βασικό επιχείρημα υπέρ του να το κάνετε μόνοι σας (εκτός από την αποφυγή ή τη μείωση του κόστους συμβουλευτικών υπηρεσιών) είναι ότι θα αναπτύξετε μέσα στον οργανισμό σας ένα πολύ μεγαλύτερο βάθος και συνειδητοποίηση του τρόπου ασφάλειας. Με την ανάπτυξη αυτής της εμπειρίας και εμπειρίας στο πλαίσιο του οργανισμού, οποιαδήποτε άλλα τέτοια έργα μπορούν να αντιμετωπιστούν πιο γρήγορα και με μεγαλύτερη εμπιστοσύνη.[102]

5.14. Σχέδια εκτίμησης κινδύνου και αντιμετώπισης κινδύνου

Ένα ISMS πρέπει να σχεδιάζεται για να ικανοποιεί τις ατομικές απαιτήσεις κάθε οργανισμού. Όχι μόνο κάθε οργανισμός έχει το δικό του επιχειρηματικό μοντέλο, τους στόχους, τα μοναδικά χαρακτηριστικά πώλησης και τον πολιτισμό, αλλά και τις διαφορετικές ορέξεις του για κινδύνους. Με άλλα λόγια, κάτι που μια οργάνωση θεωρεί ως μια απειλή που πρέπει να εκτρέψει, κάποιος άλλος θα μπορούσε να δει ως μια ευκαιρία που πρέπει να κατανοήσει.[103]

Ομοίως, ένας οργανισμός μπορεί να είναι λιγότερο προετοιμασμένος να επενδύσει σε άμυνες κατά ενός συγκεκριμένου κινδύνου από έναν άλλο. Για αυτούς και για άλλους λόγους, κάθε οργανισμός που εφαρμόζει ένα ISMS οφείλει να το πράξει ενάντια στα αποτελέσματα μιας εκτίμησης κινδύνου, της οποίας η μεθοδολογία, τα ευρήματα και οι συστάσεις έχουν εγκριθεί από το διοικητικό συμβούλιο.

Το ISO 27000 απαιτεί την εκτίμηση του κινδύνου και, ενώ δεν προσδιορίζει μεθοδολογία, είναι πολύ σαφές ότι αυτή η αξιολόγηση κινδύνου πρέπει να βασίζεται στον εντοπισμό των απειλών και των τρωτών σημείων σε επίπεδο μεμονωμένων περιουσιακών στοιχείων και, από εκεί, την ανάλυση και την αξιολόγηση των κινδύνων.

[102] Information security & iso 27001, February 2013
[103] Information security & iso 27001, February 2013

Κεφάλαιο 6

Μεθοδολογία έρευνας

6.1. Μεθοδολογία και Σκοπός

Σκοπός της έρευνας είναι να διερευνηθεί η πρακτική εφαρμογή του ISO 27001:2013 σε εταιρίες και οργανισμούς που εφαρμόζουν τα πιστοποιημένα πρότυπα ασφαλείας και να μετρηθεί και η αποδοτικότητά τους.

Στόχοι της έρευνας είναι:

1) Να διαπιστωθούν οι βασικές στρατηγικές περιεχομένου που χρησιμοποιούνται από τις ελληνικές επιχειρήσεις και οργανισμούς τηλεπικοινωνιών.

2) Να μετρηθεί η αποδοτικότητα του συστήματος και η απόδοση μετά την εφαρμογή του.

Για να επιτευχθούν οι στόχοι της παρούσας εργασίας θα χρησιμοποιηθεί η μέθοδος της ανάλυσης απαντήσεων σε συγκεκριμένο πεδίο (ερωτηματολόγιο). Η ανάλυση ερωτηματολογίου χρησιμοποιεί το υλικό που χρησιμοποιούμε σε μορφή ποιοτικών και ποσοτικών δεδομένων. Μπορεί να ορισθεί ως ένα θεωρητικό πλαίσιο που διατυπώνεται από στόχους, τεχνικές, καθώς και πρότυπα ανάλυσης που έχουν ως χαρακτηριστικό την αντικειμενικότητα, τη συστηματικότητα και την ποιοτική περιγραφή ενός περιεχομένου.

Τα δεδομένα που συλλέγονται συνοψίζονται με αποτέλεσμα να συγκριθούν μεταξύ τους και να εξαχθούν μετρήσιμα συμπεράσματα.

6.2. Μεταβλητές έρευνας

Χρησιμοποιήθηκαν κλειστού τύπου ερωτήσεις. Οι ερωτήσεις κλειστού τύπου είναι εύκολες στην συμπλήρωση, δεν είναι ιδιαίτερα χρονοβόρες και παρέχουν την δυνατότητα αντικειμενικών απαντήσεων. Οι ερωτήσεις αυτές ουσιαστικά αποτελούν τις μεταβλητές της έρευνας.

Κεφάλαιο 7

Απαντήσεις σε ερωτηματολόγιο

Ερώτηση 1

Στη ερώτηση σχετικά με το αν ο οργανισμός διαθέτει κάποιο Διεθνές πρότυπο Ασφάλεια Πληροφοριών η απάντηση είναι καταφατικά θετική, γεγονός που αποδεικνύει την αναγκαιότητα υιοθέτησης των προτύπων από τις σύγχρονες επιχειρήσεις με σκοπό τη διασφάλιση της ποιότητας παρεχόμενων υπηρεσιών.

Ερώτηση 1α

Η θετική απάντηση στην παραπάνω ερώτηση επιβεβαιώνει την ανάγκη του οργανισμού να λειτουργεί με ασφάλεια σε θέματα διαχείρισης των πληροφοριών που διαχειρίζεται και να διασφαλίζει την επίσης την ασφάλεια των στοιχείων των πελατών της

Ερώτηση 2

Οι περισσότερες επιχειρήσεις μεγάλου μεγέθους που διαχειρίζονται μεγάλο όγκο δεδομένων, δημιουργούν δικά τους εσωτερικά τμήματα IT με σκοπό να ελαχιστοποιήσουν τον κίνδυνο τυχών διαρροών των προσωπικών δεδομένων και να εξασφαλίζουν την καλύτερη και πιο άμεση διαχείριση τους.

Ερώτηση 2α

Ανάλογα με το μέγεθος του οργανισμού αλλά και τον όγκο των δεδομένων που διαχειρίζεται διαμορφώνεται και η ανάγκη για την κάλυψη περισσότερων θέσεων εργασίας στο συγκεκριμένο τμήμα.

Ερώτηση 3

Από την απάντηση στο ερώτημα 3 προκύπτει πως η συγκεκριμένη επιχείρηση φροντίζει να σε πολύ μεγάλο βαθμό την ασφάλεια των δεδομένων και των πληροφοριών χρησιμοποιώντας όσον το δυνατών περισσότερα μέσα για την προστασία τους.

Ερώτηση 4

Το τμήμα εσωτερικού ελέγχου μιας επιχείρησης μπορεί να αποδειχθεί, αν και χρήσιμο, πολύ κοστο-βόρο και αυτό να δημιουργήσει προβλήματα στη βιωσιμότητα της. Για τον παραπάνω λόγο οι περισσότεροι οργανισμοί τείνουν να επιλέγουν εξωτερικούς συνεργάτες για να καλύπτουν τις υπηρεσίες του ελέγχου.

Ερώτηση 5

Πρόκειται για μια επιχείρηση που παρέχει διαδικτυακές εμπορικές υπηρεσίες, γεγονός που συνεπάγεται τη χρήση εργαλείων συλλογής πληροφοριών e-shop και online databases.

Ερώτηση 6

Η απάντηση αυτή διαμορφώνεται αυτόματα από την τήρηση του προτύπου ISO 27001 το οποίο ορίζει υποχρεωτική τη χρήση εργαλείων προφύλαξης δεδομένων από μη εξουσιοδοτημένους χρήστες.

Ερώτηση 7

Παρομοίως με την παραπάνω απάντηση πρέπει να υπάρχουν εργαλεία που αποτρέπουν και την εγκατάσταση λογισμικού από μη εξουσιοδοτημένους χρήστες.

Ερώτηση 8

Ο έλεγχος είναι ένα πολύ σημαντικό κομμάτι και ορίζεται απολύτως από το σύστημα ISO 27001:2013 ως προς την συχνότητα πραγματοποίησης και ως προς το βαθμό του.

Ερώτηση 9

Η χρήση λογισμικού R&D κρίνεται ως μη ασφαλής και εγκυμονεί κινδύνους. Καλό είναι να αποφεύγεται η χρήση τέτοιο είδους προγραμμάτων και εργαλείων.

Ερώτηση 10

Η χρήση μη εγκεκριμένων προγραμμάτων μπορεί να οδηγήσει σε απώλεια δεδομένων λόγο του κινδύνου εγκατάστασης κακόβουλου λογισμικού όπως επίσης ασταθούς λογισμικού με πολλά τρωτά σημεία.

Ερώτηση 11

Γίνεται πάντα επιθεώρηση του νέου λογισμικού πριν ο οργανισμός προχωρήσει στην εγκατάστασή του.

Ερώτηση 12

Η εταιρεία επιτρέπει στους υπαλλήλους της τη χρήση του προσωπικού τους ηλεκτρονικού ταχυδρομείου, αν και αυτό αποτελεί υψηλό παράγοντα κινδύνου όσων αφορά τη διαρροή πληροφοριών, η απόφαση κρίνεται κυρίως από την εμπιστοσύνη απέναντι στους εργαζομένους της.

Ερώτηση 13

Ορισμένοι υπάλληλοι έχουν πρόσβαση στους υπολογιστές του γραφείου απομακρυσμένα για να καλύπτουν κάποιες εργασιακές ανάγκες γεγονός ριψοκίνδυνο αλλά ταυτόχρονα και απαραίτητο για την ολοκλήρωση χρονοβόρων εργασιών που είναι αδύνατο να ολοκληρωθούν κατά τη διάρκεια της ημέρας.

Ερωτήσεις 14 & 15

Εφόσον καλύπτεται η προϋπόθεση της τήρησης των μέτρων ασφαλείας μέσω λογισμικού εξουσιοδότησης όπως απαντήθηκε παραπάνω, η πρόσβαση στο διαδίκτυο δεν αποτελεί πρόβλημα για το σύστημα ISO, ούτε προκαλεί κάποιο σημαντικό πρόβλημα σχετικά με την ασφάλεια των πληροφοριών.

Ερώτηση 15α

Το σύστημα αρχείων καταγραφής μέσω του firewall βοηθά στο πλήρη έλεγχο της χρήσης τους διαδικτύου δίνοντας στους υπαλλήλους την δυνατότητα να πλοηγούνται ελεύθερα και ταυτόχρονα στους ειδικούς ασφαλείας συστημάτων να έχουν καταγεγραμμένο τον πλήρη χάρτη διαδρομής-κινήσεων του κάθε χρήστη online.

Ερώτηση 16

Η χρήση των προσωπικών συσκευών στον εργασιακό χώρο απαγορεύεται αυστηρά από το πρότυπο ISO 27001.

Ερώτηση 17

Έχοντας τα αυτόματα αρχεία καταγραφής μέσω firewall άμεσα διαθέσιμα, η διαδικασία του ελέγχου απλοποιείται σημαντικά.

Ερώτηση 18

Οι Διαδικασίες Ανάλυσης και Διαχείρισης Περιστατικών και Προβλημάτων Ασφαλείας αποτελούν αναπόσπαστο κομμάτι του προτύπου ISO 27001:2013 και δεν μπορούν να λείπουν από έναν οργανισμό που το εφαρμόζει.

Ερωτήσεις 18α & 18β

Θα πρέπει να συνταχθεί σχεδιασμός αντιμετώπισης πιθανής καταστροφής. Ο λόγος μη ύπαρξης ενός σχεδίου δηλώνει πρόβλημα στην εφαρμογή του συστήματος ISO και μπορεί να φέρει τον οργανισμό σε πολύ δύσκολη θέση σε περίπτωση που συμβεί κάποια πιθανή απώλεια ή διαρροή πληροφοριών. Παρόλο που πραγματοποιούνται οι δοκιμαστικοί έλεγχοι ανά τακτά χρονικά διαστήματα, η πιθανότητα ύπαρξης προβλήματος είναι πολύ μεγάλη και πρέπει να ελαχιστοποιηθεί.

Ερωτήσεις 19 – 19α – 19β - 20 -20β - 21

Το πρότυπο ISO 27001:2013 καθορίζει τις απαιτήσεις για τη δημιουργία, την εφαρμογή, τη διατήρηση και τη συνεχή βελτίωση ενός συστήματος διαχείρισης της ασφάλειας των πληροφοριών στο πλαίσιο του οργανισμού. Αυτό περιλαμβάνει επίσης απαιτήσεις για την αξιολόγηση και την αντιμετώπιση των

κινδύνων ασφάλειας πληροφοριών που προσαρμόζονται στις ανάγκες του οργανισμού.

Σύμφωνα με τα παραπάνω το πρότυπο διασφαλίζει την ασφάλεια των πληροφοριών μειώνοντας σημαντικά τους κινδύνους, ελέγχοντας τα τρωτά σημεία ασφαλείας και όλα αυτά εξασφαλίζοντας το χαμηλότερο κόστος.

Παράλληλα διασφαλίζει στον οργανισμό ένα πολύ μεγάλο ανταγωνιστικό πλεονέκτημα διαβεβαιώνοντας στους πιθανούς πελάτες ή συμβαλλόμενους την υψηλή ασφάλεια των πληροφοριών και των ευαίσθητων προσωπικών δεδομένων τους.

Συμπεράσματα

Οι παραβιάσεις ασφαλείας έχουν αντιμετωπιστεί ως σημαντική απειλή για οργανισμούς σε όλο τον κόσμο. Οι οργανισμοί και οι κυβερνήσεις δαπανούν εκατομμύρια δολάρια ετησίως για να ανακάμψουν από τις αρνητικές επιπτώσεις των επιθέσεων στα πληροφοριακά τους στοιχεία. Πολλά στατιστικά στοιχεία έχουν δηλώσει ότι οι περισσότερες παραβιάσεις ασφαλείας που προκαλούνται από ένα πρόβλημα εσωτερικής οργάνωσης ή μπορούν να αποφευχθούν εξαλείφοντας ένα εσωτερικό πρόβλημα. Ως εκ τούτου, συστήματα διαχείρισης της ασφάλειας των πληροφοριών υιοθετούνται από πολλούς οργανισμούς προκειμένου να έχουν κατάλληλους ελέγχους για την εξάλειψη πιθανών εσωτερικών οργανωτικών προβλημάτων που ενδέχεται να προκαλέσουν κάποια σοβαρή παραβίαση της ασφάλειας.

Οι ευπάθειες μπορούν να κατηγοριοποιηθούν ως εξής:

• Ανεπαρκής ενημέρωση για την ασφάλεια των πληροφοριών για το προσωπικό του οργανισμού.

• Οι οργανισμοί δεν υιοθετούν σύστημα διαχείρισης της ασφάλειας των πληροφοριών για τον έλεγχο της διαδικασίας ασφαλείας των συστημάτων πληροφοριών.

Εφαρμόζοντας το διεθνές πρότυπο διαχείρισης πληροφοριών ISO27001:2013, το οποίο έχει τη δυνατότητα και παρέχει όλα τα απαραίτητα εργαλεία για να

εξαλείψει όλες τις ευπάθειες που εντοπίστηκαν κατά τη φάση αξιολόγησης των τρωτών σημείων. Κατά το σχεδιασμό της εφαρμογής του ISO27001, αναπτύσσοντας τους απαραίτητους ελέγχους, καθίσταται δυνατή την έναρξη των σταδίων εξάλειψης των εντοπισθέντων κινδύνων.

Οι εσωτερικοί ελεγκτές και οι ελεγκτικοί φορείς αντιλήφθηκαν, από νωρίς, τα οφέλη από την εφαρμογή του ISO 27001 καθώς προσφέρει μειωμένο κόστος για την επιχείρηση, αύξηση της αποτελεσματικότητας, απαιτεί λιγότερο χρόνο προετοιμασίας για έναν έλεγχο και εξοικονόμηση χρόνου.

Η εφαρμογή ή η πιστοποίηση του ISO / IEC 27000 μπορεί να αποφέρει ορισμένα οφέλη σε έναν οργανισμό:

Μετά από μια καθορισμένη δομημένη προσέγγιση, με διεθνή αναγνώριση, μπορεί να διασφαλίσει ότι ένα ISMS είναι κατάλληλο για αυτό το σκοπό.

Τα θέματα ασφάλειας των πληροφοριών και ο τρόπος μείωσης των σχετικών κινδύνων θα εντοπίζονται, θα παρακολουθούνται και θα βελτιώνονται με προγραμματισμένο τρόπο.

Οι κατάλληλες διαδικασίες και διαδικασίες για τη διαχείριση της ασφάλειας των πληροφοριών θα καθοριστούν, τεκμηριωθούν και ενσωματωθούν στην πράξη.

Η επίδειξη της οργανωτικής δέσμευσης για την ασφάλεια των πληροφοριών θα διασφαλίσει την επαρκή κατανομή των πόρων, τον προσδιορισμό των ρόλων και των ευθυνών και την κατάλληλη κατάρτιση.

Τα δεδομένα θα προστατεύονται από μη εξουσιοδοτημένη πρόσβαση, αποδεικνύοντας τον αυθεντικό χαρακτήρα τους, ενώ οι εξουσιοδοτημένοι χρήστες θα έχουν πρόσβαση στα δεδομένα όταν το απαιτούν

Η συνέχιση της επιχειρηματικής δραστηριότητας ενός οργανισμού θα διαχειριστεί αποτελεσματικά, βελτιώνοντας το προφίλ του και αυξάνοντας τις ευκαιρίες του

Τα δικαιώματα διανοητικής ιδιοκτησίας μπορούν να προστατευθούν.

Η ανεξάρτητη επαλήθευση της συμμόρφωσης με το πρότυπο μπορεί να διασφαλίσει ότι ένας οργανισμός δεν έχει παραμεληθεί όσον αφορά τους κατάλληλους νόμους για την προστασία της ιδιωτικής ζωής των προσωπικών δεδομένων. Στην Αγγλία και την Ουαλία το πρότυπο αναγνωρίζεται από τον Επίτροπο Πληροφοριών ως κατάλληλη πηγή συμβουλών για τη διασφάλιση της συμμόρφωσης με τον Νόμο περί Προστασίας Δεδομένων (1998).

Η διαχείριση του κινδύνου ασφάλειας των πληροφοριών είναι ένα πολύ σημαντικό μέρος της στρατηγικής διαχείρισης κάθε εταιρείας. Πρόκειται για τη διαδικασία με την οποία οι εταιρείες αντιμετωπίζουν μεθοδικά τους κινδύνους που συνδέονται με τις δραστηριότητες, τις υπηρεσίες και τις επιχειρηματικές τους διαδικασίες με κύριο στόχο την επίτευξη σταθερών οφελών. Το επίκεντρο της αποτελεσματικής διαχείρισης του κινδύνου ασφάλειας είναι ο εντοπισμός και η αντιμετώπιση των κινδύνων ασφάλειας των πληροφοριών. Στόχος του είναι να προσθέσει τη μέγιστη βιώσιμη αξία σε όλες τις επιχειρηματικές διαδικασίες και υπηρεσίες που παρέχει η εταιρεία στους πελάτες της. Αυξάνει την πιθανότητα επιτυχίας και μειώνει τόσο την πιθανότητα αποτυχίας όσο και την αβεβαιότητα για την επίτευξη των συνολικών επιχειρηματικών στόχων της εταιρείας.

Η διαχείριση των κινδύνων ασφάλειας των πληροφοριών επιτρέπει επίσης μια στρατηγική προσέγγιση στη διαχείριση της τεχνολογίας πληροφοριών και επικοινωνιών. Οποιεσδήποτε αλλαγές στο περιβάλλον των δεδομένων-πληροφοριών μπορούν να αξιολογηθούν προκειμένου να ληφθεί η απόφαση για την εναλλακτική λύση με το λιγότερο πιθανό κίνδυνο πριν από τη διάθεση κεφαλαίων σε οποιαδήποτε εναλλακτική λύση. Η διαχείριση κινδύνων ασφάλειας των προσωπικών δεδομένων πρέπει να είναι μια συνεχής και αναπτυσσόμενη διαδικασία. Θα πρέπει να αντιμετωπίσει μεθοδικά όλους τους κινδύνους που μπορεί να αντιμετωπίσει η εταιρεία, λαμβάνοντας υπόψη τις εμπειρίες του παρελθόντος (για παράδειγμα τυχόν συμβάντα ασφαλείας), την τρέχουσα κατάσταση και τις επικείμενες προκλήσεις, ειδικά στον τομέα της επέκτασης του χαρτοφυλακίου υπηρεσιών της εταιρείας.

Πρέπει να ενσωματωθεί στην κουλτούρα της επιχείρησης με μια αποτελεσματική πολιτική ασφάλειας όπως αυτή του ISO 27001:2013 και ένα πρόγραμμα υπό την ηγεσία της ανώτατης διοίκησης, καθώς η δέσμευση της

ανώτατης διοίκησης είναι ένας από τους βασικούς επιτυχείς παράγοντες για την αποτελεσματική διαχείριση του κινδύνου. Πρέπει να μεταφράσει τη στρατηγική σε στόχους τακτικής και λειτουργίας. Το πρότυπο ασφαλείας ISO 27001 υποστηρίζει τη αναλυτική παρακολούθηση και τη μέτρηση των επιδόσεων, προωθώντας έτσι τη λειτουργική αποδοτικότητα σε όλα τα επίπεδα.

Καταλήγοντας, η ασφάλεια πληροφοριών δεν είναι ένα καθαρά τεχνικό θέμα. Εάν θεωρείς ότι η τεχνολογία μπορεί να σου λύσει τα θέματα ασφαλείας, τότε δεν καταλαβαίνεις τόσο τα προβλήματα, όσο και την τεχνολογία (Bruce Schneier).

ΒΙΒΛΙΟΓΡΑΦΙΑ

ΕΕΚΤ- «Ο Κλάδος της Κινητής Τηλεφωνίας στις Νέες Συνθήκες», Οικονομικό Πανεπιστήμιο Αθηνών, Τμήμα Διοικητικής Επιστήμης και Τεχνολογίας, Σεπτέμβριος 2012.

Κατσίκας Σ., 'Διαχείριση της Ασφάλειας Πληροφοριών', Εκδόσεις Πεδίο, Αθήνα 2014.

Κιουντούζης Ε., 'Μεθοδολογίες ανάλυσης και σχεδιασμού πληροφοριακών συστημάτων', Β' Εκδόσεις Μπένου, Αθήνα 2002.

Κομνηνός , Θόδωρος Π. Σπυράκης , Παύλος Γ. , 'Ασφάλεια δικτύων & υπολογιστικών συστημάτων : αναχαιτίστε τους εισβολείς', 2002.

Πανέτσος Σ., 'Επικοινωνίες & Δίκτυα Υπολογιστών', εκδόσεις Τζιόλα, Θεσσαλονίκη 2007

Almarabeh, T., & AbuAli, A. (2010). A general framework for e-government: definition maturity challenges, opportunities, and success. European Journal of Scientific Research

Andrew S. Tanenbaum, 'Computer Networks', 4th Edition, Pearson Education Inc, 2003

Arnason, S. T., & Willett, K. D. (2007). How to achieve 27001 certification: An example of applied compliance management. CRC Press

BSI, I. (2005). Sicherheitsmanagement und IT-Grundschutz-BSI-Standards zur ITSicherheit.

Danziger, J. N., & Andersen, K. V. (2002). The Impacts of Information Technology on Public Administration: an Analysis of Empirical Research from the "Golden Age" of Transformation. International Journal of Public Administration [1]

De Vivo, M., de Vivo, G. O., & Germinal, I. (1998, April). Internet security attacks at the basic levels. ACM SIGOPS Operating Systems Review

Fjermestad, J., Romano, N., (2006), Electronic Customer Relationship Management, Εκδόσεις: M.E. Sharpe

Hansen, M. (2016). Data Protection by Design and by Default à la European General Data Protection Regulation. Privacy and Identity Management. Facing up to Next Steps

Hossein Bidgoli, 'Handbook of Information Security', John Wiley & Sons, California 2006.

ISO27K Forum. (2017). ISMS implementation and certification process flowchart v4. Ανάκτηση Φεβρουάριος 23, 2017, από Iso27001security.com: http://www.iso27001security.com/html/toolkit.html

ISO/IEC 27000. (2016). Information technology - Security techniques - Information security management systems - Overview and vocabulary. International Organization for Standardization.

Joseph Boyce, 'Information Assurance: Managing Organizational It Security Risks', ΗΠΑ, 2002.

K. Scasfone, P. Mell, "Guide to Intrusion Detection and Prevention Systems (IDPS)", National Institute of Standards and Technology,2007

Middleton, M. R. (2007). Approaches to evaluation of websites for public sector services. In Kommers, Piet, Eds. Proceedings IADIS Conference on e-Societ

Nicopolitidis P., Obaidat M. S., Papadimitriou G. I., Pomportsis A.S., Wireless Networks - Ασύρματα Δίκτυα», Εκδόσεις Κλειδάριθμος, Αθήνα (2006)

Rash, Michael et al, Intrusion Prevention and Active Response: Deployment Network and Host IPS, Syngress, 2005

S. Powell, J.P. Shim, "Wireless Technology Application, Management and Security", Springer, 2009

Siponen M., 'Policies for Construction of Information Systems Security Guidelines', Kluwer Academic Publishers, 2000

W. Stallings, "Network Security Essentials: Applications and Standards", 2nd edition, Prentice Hall, USA, 2003

Developing an ISO27001 Information Security Management System for an Educational Institute: Hashemite University as a Case Study, 2014

Παράρτημα Α

Ερωτηματολόγιο

Θα ήθελα να επισημάνω ότι το ερωτηματολόγιο απαντήθηκε από την πλειοψηφία των τηλεπικοινωνιακών παρόχων στην Ελλάδα, καλύπτοντας τις ανάγκες της διπλωματικής εργασίας.

Το παρόν ερωτηματολόγιο δημιουργήθηκε στα πλαίσια εκπόνησης μεταπτυχιακής διατριβής του τμήματος Διοίκηση, Τεχνολογία και Ποιότητα της Σχολής Οικονομικών Επιστημών και Διοίκησης του Ανοικτού Πανεπιστημίου Κύπρου. Πρόκειται για εργαλείο το οποίο θα χρησιμοποιηθεί για εκπαιδευτικούς σκοπούς στο πλαίσιο έρευνας εφαρμογής του Προτύπου ISO 27001:2013 στον χώρο των τηλεπικοινωνιών στην Ελλάδα.

Θα θέλαμε να σας ενημερώσουμε ότι σεβόμαστε απολύτως το χρόνο σας, και ότι το ερωτηματολόγιο έχει δομηθεί με τέτοιο τρόπο, ώστε η απάντησή του να μην απαιτεί υπερβολικό χρόνο από πλευράς σας.

Σκοπός της παρούσας έρευνας είναι η συλλογή πληροφοριών σχετικά με τη χρησιμότητα και την ανάγκη της εφαρμογής του ISO 27001:2013 στον χώρο των τηλεπικοινωνιών στην Ελλάδα.

Θα θέλαμε να σας ευχαριστήσουμε που δεχθήκατε να συμμετάσχετε στην έρευνα αυτή και θα το εκτιμούσαμε δεόντως εάν συμπληρώνατε όσο πιο ολοκληρωμένα γίνεται το ερωτηματολόγιο με όσο το δυνατόν μεγαλύτερη ακρίβεια και ειλικρίνεια.

Ερώτηση 1

Διαθέτετε κάποιο Διεθνές Πρότυπο Ασφάλειας Πληροφοριών;

Ερώτηση 1α

Εάν ναι, πιστεύετε ότι προσθέτει αξία στο Σύστημα Ασφάλειας του οργανισμού σας;

Ερώτηση 1β

Εάν όχι, σκοπεύετε να αποκτήσετε ένα τέτοιο Πρότυπο Ασφάλειας ή να εφαρμόσετε κάποιο χωρίς να έχει πιστοποίηση;

Ερώτηση 2

Έχετε εσωτερική ομάδα Πληροφορικής (τμήμα ΙΤ) ή έχετε αναθέσει αυτή την λειτουργία σε εξωτερική ομάδα/συνεργάτη;

Ερώτηση 2α

Εάν έχετε εσωτερικό τμήμα Πληροφορικής, από πόσα άτομα αποτελείται;

Ερώτηση 2β

Εάν έχετε εξωτερικό τμήμα Πληροφορικής, ποιά συμβατική δομή ακολουθείτε;

Ερώτηση 3

Διαθέτετε κάποιον Επικεφαλής τμήματος Ασφάλειας πληροφοριών (CISO – Chief Information Security Officer);

Ερώτηση 4

Διαθέτετε ομάδα εσωτερικού ελέγχου του Συστήματος Πληροφοριών στον οργανισμό σας;

Ερώτηση 5

Παρέχετε διαδικτυακές εμπορικές υπηρεσίες στους πελάτες σας;

Ερώτηση 6

Διαθέτετε κάποιον τρόπο ελέγχου αποφυγής μη εξουσιοδοτημένης πρόσβασης στα δεδομένα των πελατών σας;

Ερώτηση 7

Ελέγχετε τις τροποποιήσεις του συστήματος από τους υπαλλήλους σας; (πχ πρόληψη μη εξουσιοδοτημένης εγκατάστασης λογισμικού)

Ερώτηση 8

Πραγματοποιείτε ελέγχους του Συστήματος Πληροφοριών του οργανισμού σας για τρωτά σημεία ασφαλείας;

Ερώτηση 9

Επιτρέπετε τη χρήση λογισμικού το οποίο δεν έχει εκδοθεί επίσημα και βρίσκεται ακόμα στο στάδιο Έρευνας και Ανάπτυξης (R&D);

Ερώτηση 10

Πιστεύετε ότι η χρήση μη εγκεκριμένων προγραμμάτων καταλήγει σε απώλεια δεδομένων;

Ερώτηση 11

Η χρήση νέων συστημάτων λογισμικού επιθεωρούνται και εγκρίνονται από κάποιον επίσημα υπεύθυνο;

Ερώτηση 12

Επιτρέπετε στους υπαλλήλους σας τη χρήση του προσωπικού τους ηλεκτρονικού ταχυδρομείου από τους υπολογιστές του γραφείου;

Ερώτηση 13

Επιτρέπετε στους υπαλλήλους σας τη χρήση απομακρυσμένης πρόσβασης στον υπολογιστή του γραφείου;

Ερώτηση 14

Παρέχετε πρόσβαση στο διαδίκτυο στους υπαλλήλους σας;

Ερώτηση 15

Ελέγχετε την πρόσβαση στο διαδίκτυο των υπαλλήλων σας όταν χρησιμοποιούν το δίκτυο του οργανισμού σας;

Ερώτηση 15α

Εάν ναι πώς;

Ερώτηση 15β

Εάν όχι γιατί;

Ερώτηση 16

Επιτρέπετε τη χρήση BYOD (Bring Your Own Device);

Ερώτηση 16α

Έχετε εφαρμόσει κάποιο εργαλείο ελέγχου πρόσβασης στο δίκτυο του οργανισμού σας;

Ερώτηση 17

Διεξάγετε ελέγχους πρόσβασης στο δίκτυο του οργανισμού σας;

Ερώτηση 18

Διαθέτετε διαδικασίες Ανάλυσης και Διαχείρισης Περιστατικών και Προβλημάτων Ασφαλείας;

Ερώτηση 18α

Διαθέτετε κάποιο σχεδιασμό αντιμετώπισης πιθανής καταστροφής;

Ερώτηση 18β

Πραγματοποιείτε δοκιμαστικούς ελέγχους;

Ερώτηση 19

Θεωρείτε ότι η εφαρμογή του Προτύπου ISO 27001:2013 μείωσε τον επιχειρησιακό κίνδυνο και σας εξασφαλίζει μεγαλύτερη προστασία στα αρχεία και τα δεδομένα, αλλά και προσωπικές πληροφορίες του προσωπικού και των πελατών του οργανισμού σας;

Ερώτηση 19α

Θεωρείτε ότι η εφαρμογή του Προτύπου ISO 27001:2013 σας βοήθησε στον εντοπισμό και καταπολέμηση δυνητικών κινδύνων που απειλούν τις κρίσιμες πληροφορίες του οργανισμού σας, ενώ μείωσε την επίπτωση των περιστατικών/παραβιάσεων;

Ερώτηση 19β

Θεωρείτε ότι η εφαρμογή του Προτύπου ISO 27001:2013 ελαχιστοποίησε τις πιθανότητες παραβιάσεων των πληροφοριών ελέγχοντας τις πιθανές αδυναμίες και σας βοήθησε στον εντοπισμό νέων αναγκών ασφαλείας;

Ερώτηση 20

Θεωρείτε ότι η εφαρμογή του Προτύπου ISO 27001:2013 δημιούργησε ανταγωνιστικό πλεονέκτημα στην αγορά;

Ερώτηση 20α

Θεωρείτε ότι η εφαρμογή του Προτύπου ISO 27001:2013 στον οργανισμό σας βελτιώνει την αξιοπιστία και συμβάλλει στη ενίσχυση της σχέσης εμπιστοσύνης στους υφιστάμενους και δυνητικούς πελάτες σας, καθώς διασφαλίζει το απόρρητο των πληροφοριών;

Ερώτηση 21

Θεωρείτε ότι η εφαρμογή του ISO 27001:2013 συνέσφερε στην μείωση κόστους και γενικότερα προσέφερε όφελος στον οργανισμό σας;