ΕΘΝΙΚΟ ΜΕΤΣΟΒΙΟ ΠΟΛΥΤΕΧΝΕΙΟ
ΣΧΟΛΗ ΗΛΕΚΤΡΟΛΟΓΩΝ ΜΗΧΑΝΙΚΩΝ ΚΑΙ Μ/Υ
ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΕΙΡΑΙΩΣ
ΣΧΟΛΗ ΝΑΥΤΙΛΙΑΣ ΚΑΙ ΒΙΟΜΗΧΑΝΙΑΣ
ΤΜΗΜΑΤΟΣ ΒΙΟΜΗΧΑΝΙΚΗΣ ΔΙΟΙΚΗΣΗΣ & ΤΕΧΝΟΛΟΓΙΑΣ
ΔΙΑΠΑΝΕΠΙΣΤΗΜΙΑΚΟ ΠΡΟΓΡΑΜΜΑ ΜΕΤΑΠΤΥΧΙΑΚΩΝ
ΣΠΟΥΔΩΝ «ΤΕΧΝΟ-ΟΙΚΟΝΟΜΙΚΑ ΣΥΣΤΗΜΑΤΑ»

ΑΝΑΛΥΣΗ ΚΑΙ ΔΙΑΧΕΙΡΙΣΗ ΕΠΙΚΙΝΔΥΝΟΤΗΤΑΣ ΣΤΗΝ ΑΣΦΑΛΕΙΑ ΠΛΗΡΟΦΟΡΙΑΚΩΝ ΣΥΣΤΗΜΑΤΩΝ

ΜΕΤΑΠΤΥΧΙΑΚΗ ΔΙΠΛΩΜΑΤΙΚΗ ΕΡΓΑΣΙΑ

Δέσποινα Α. Χατζηγεωργίου

Επιβλέπων: Γεώργιος Ματσόπουλος

Καθηγητής Ε.Μ.Π.

Αθήνα, Μάιος 2019

……

Δέσποινα Α. Χατζηγεωργίου.

Διπλωματούχος Ηλεκτρολόγος Μηχανικός και Μηχανικός Υπολογιστών Ε.Μ.Π.

ΠΕΡΙΛΗΨΗ

Τα πληροφοριακά συστήματα αποτελούν αναπόσπαστο κομμάτι της καθημερινής λειτουργίας των οργανισμών. Η διατάραξη ή η παραβίασή τους εγκυμονεί τον κίνδυνο της πρόκλησης σημαντικών υλικών, κοινωνικών και οικονομικών ζημιών. Είναι αναγκαία λοιπόν η εφαρμογή μέτρων για την πρόληψη και τον περιορισμό των κινδύνων που αντιμετωπίζουν τα πληροφοριακά συστήματα και τη διασφάλιση ενός υψηλού επιπέδου ασφαλείας. Ένας αναγνωρισμένος τρόπος για την ελάττωση και την αποφυγή των κινδύνων είναι η ανάλυση και η διαχείριση της επικινδυνότητας. Η ανάλυση και διαχείριση της επικινδυνότητας οδηγεί στον εντοπισμό και την αξιολόγηση των επιχειρησιακών κινδύνων και στον έλεγχο ή την εξάλειψη τους.

Στην παρούσα διπλωματική γίνεται μια παρουσίαση των κυριότερων προτύπων ασφάλειας πληροφοριών και περιγράφεται η οικογένεια ISO 27000. Ακολουθεί η ανάλυση των βασικών στοιχείων και απαιτήσεων του προτύπου ISO/IEC 27001, μέλους της οικογένειας ISO 27000, που αποτελεί ένα από τα πιο αναγνωρισμένα πρότυπα ασφαλείας. Στη συνέχεια περιγράφονται οι βασικές μεθοδολογίες ανάλυσης κινδύνου συμβατές με τις απαιτήσεις του ISO/IEC 27001 και γίνεται μια σύγκριση αυτών. Συγκεκριμένα περιγράφονται οι μεθοδολογίες Cramm, Magerit, Mehari, Ebios και IT-Grundschutz. Τέλος, πραγματοποιείται η μελέτη περίπτωσης ανάλυσης κινδύνου σε ένα μικρομεσαίο οργανισμό που δραστηριοποιείται στον τραπεζικό κλάδο. Γι’ αυτό τον οργανισμό αυτό υλοποιείται η ανάλυση της επικινδυνότητας με χρήση της μεθοδολογίας Magerit.

Λέξεις κλειδιά: Ασφάλεια Πληροφοριακών Συστημάτων, Κίνδυνος, Ανάλυση Επικινδυνότητας, Διαχείριση Επικινδυνότητας, ISO 27001

ABSTRACT

Information systems are vital for any business operation. Any disruption or violation can cause damage, social impact and financial loss. It is therefore necessary to implement measures to prevent and limit the risks and to ensure a high level of security. An internationally accepted way of reducing and avoiding risks is risk analysis and management. An organization that implements risk analysis and management can identify and evaluate the operational risks and achieve their control or elimination.

In this thesis the main standards of information security are presented and the ISO 27000 family of standards is described. Afterwards, the core elements and requirements of the ISO / IEC 27001 which is the best-known standard in the ISO/IEC 27000 family are analyzed. The basic methodologies of risk analysis compliant with the requirements of ISO / IEC 27001 are presented and a comparison of them is made. Specifically, the Cramm, the Magerit, the Mehari, the Ebios and the IT- Grundschutz methodologies are described. Finally, a risk analysis is carried out on an organization active in the banking sector using the MAGERIT methodology.

Keywords: Information Security, Risk, Risk Analysis, Risk Management, ISO/IEC 27001.

ΕΥΧΑΡΙΣΤΙΕΣ

Η παρούσα διπλωματική εργασία εκπονήθηκε στη σχολή Ηλεκτρολόγων Μηχανικών και Μηχανικών Υπολογιστών του Εθνικού Μετσόβιου Πολυτεχνείου το ακαδημαϊκό έτος 2018-2019, στα πλαίσια του μεταπτυχιακού προγράμματος «Τεχνοοικονομικά Συστήματα». Με την ολοκλήρωση της παρούσας διπλωματικής θα ήθελα να ευχαριστήσω ιδιαιτέρως τον Καθηγητή μου κ. Γεώργιο Ματσόπουλο για την εμπιστοσύνη που μου έδειξε αναθέτοντάς μου την διπλωματική εργασία καθώς και για την βοήθεια και την στήριξη που μου παρείχε κατά την εκπόνηση της. Τέλος, θα ήθελα να ευχαριστήσω την οικογένεια μου και όλους όσους με στήριξαν όχι μόνο κατά την εκπόνση της διπλωματικής αλλά καθ’ όλη την διάρκεια των σπουδών μου.

ΠΕΡΙΕΧΟΜΕΝΑ

ΛΙΣΤΑ ΕΙΚΟΝΩΝ

ΛΙΣΤΑ ΠΙΝΑΚΩΝ

1. ΕΙΣΑΓΩΓΗ

Πληροφοριακό σύστημα (Information Systems ή IS) είναι ένα σύνολο αλληλεπιδρώντων στοιχείων το οποίο συλλέγει, ανακτά, επεξεργάζεται και αποθηκεύει δεδομένα και παράγει πληροφορίες για έναν οργανισμό. Τα σύγχρονα πληροφοριακά συστήματα παρέχουν σημαντικές ηλεκτρονικές υπηρεσίες σε αδιάλειπτη βάση για τον ίδιο τον οργανισμό και για άλλους οργανισμούς. Η διακοπή της λειτουργίας , η παραβίαση ή η υποκλοπή δεδομένων μπορούν να επιφέρουν αρνητικές συνέπειες για σε κοινωνική και οικονομική βάση όπως βαρύτατες οικονομικές απώλειες, παραβιάσεις της ιδιωτικής ζωής, ακόμη και πτώση του οργανισμού. Οι κίνδυνοι δημιουργούνται από ηλεκτρονικούς πειρατές (hackers), κακόβουλο λογισμικό, ανταγωνιστές ακόμα και δυσαρεστημένους εργαζομένους. Κρίνεται λοιπόν αναγκαία η προστασία αυτών των συστημάτων από κάθε είδους απειλή και η εξασφάλιση ενός επιθυμητού επιπέδου ασφαλείας. Η ασφάλεια πληροφορικών συστημάτων (IS Security) είναι ένα οργανωμένο πλαίσιο από αρχές, διαδικασίες, τεχνικές και μέτρα που απαιτούνται για την προστασία του πληροφοριακού συστήματος. Στόχο έχει την προστασία του πληροφοριακού συστήματος από εσωτερικούς και εξωτερικούς κινδύνους που θα μπορούσαν να επηρεάσουν την ομαλή λειτουργία και τους στόχους του. Η ασφάλεια των πληροφοριακών συστημάτων στηρίζεται στην εξασφάλιση της ακεραιότητας, της διαθεσιμότητας και της εμπιστευτικότητας των δεδομένων ενός πληροφοριακού συστήματος χωρίς να παρακωλύεται η παραγωγικότητα και οι στόχοι του οργανισμού. Η πλέον διαδεδομένη μεθοδολογία για την εξασφάλιση της ασφάλειας πληροφοριακών συστημάτων είναι η Ανάλυση και Διαχείριση της Επικινδυνότητας.

1.1 ΑΝΑΛΥΣΗ ΕΠΙΚΙΝΔΥΝΟΤΗΤΑΣ

Με τον όρο Ανάλυση Κινδύνου (Risk Analysis) ορίζεται η διαδικασία εντοπισμού και αξιολόγησης των κινδύνων και των ευάλωτων σημείων ενός πληροφοριακού συστήματος και τον προσδιορισμό των επιμέρους κινδύνων που εάν εκδηλωθούν θα επιφέρουν αρνητικές συνέπειες στον οργανισμό. Σκοπός της Ανάλυσης Κινδύνου είναι ο εντοπισμός των κινδύνων και ο υπολογισμός της πιθανότητας εμφάνισης τους. Η διαδικασία ανάλυσης του κινδύνου λαμβάνει υπόψη τόσο την πιθανότητα πραγματοποίησης μια απειλής όσο και την επίπτωση που θα έχει εάν πραγματοποιηθεί. Η Ανάλυση του Κινδύνου αποτελεί το βασικότερο εργαλείο στην απόφαση αποδοχής του επίπεδου του κινδύνου ή της εφαρμογής κατάλληλων μέτρων για τη βελτίωση του επιπέδου του κινδύνου. Η Ανάλυση του κινδύνου μπορεί να γίνει με βάση την ποιοτική ή την ποσοτική προσέγγιση.

- Ποιοτική προσέγγιση. Η ποιοτική προσέγγιση βασίζεται σε υποκειμενικές εκτιμήσεις της αξίας των περιουσιακών στοιχείων, των απειλών, των αδυναμιών και του κινδύνου. Η προσέγγιση αυτή είναι εύκολα κατανοητή, απαιτεί λίγους ανθρώπινους και υλικούς πόρους και παρέχει μια καλή εικόνα του κινδύνου ασφαλείας. Από την άλλη μεριά, είναι υποκειμενικής φύσεως, βασίζεται στην εμπειρία των εμπλεκόμενων ατόμων και δεν γίνεται ιδιαίτερη προσπάθεια αποτίμησης της αξίας των αγαθών.

- Ποσοτική προσέγγιση. Η ποσοτική προσέγγιση βασίζεται στον υπολογισμό με συγκεκριμένους τύπους του κινδύνου ασφαλείας. Τα αποτελέσματα έχουν το κύρος της μαθηματικής απόδειξης και είναι αντικειμενικά. Η αξία των περιουσιακών στοιχείων και ο κίνδυνος εκφράζονται σε χρηματικά μεγέθη πράγμα που γίνεται αμέσως κατανοητό από τη Διοίκηση του οργανισμού. Από την άλλη μεριά είναι δύσκολος ο καθορισμός των μεταβλητών που χρησιμοποιούνται στους τύπους και ο υπολογισμός είναι περίπλοκος με αποτέλεσμα να χρειάζεται αρκετός χρόνος και κατάλληλα καταρτισμένα άτομα.

1.2 ΔΙΑΧΕΙΡΙΣΗ ΕΠΙΚΙΝΔΥΝΟΤΗΤΑΣ

Με τον όρο διαχείριση επικινδυνότητας (Risk Management) ορίζεται η διαδικασία αντιμετώπισης των κινδύνων που εντοπίστηκαν στη φάση της Ανάλυσης Κινδύνου σύμφωνα με τις αποφάσεις της Διοίκησης του οργανισμού. Μετά την ανάλυση επικινδυνότητας ακολουθεί η επιλογή κατάλληλων αντιμέτρων, ο καθορισμός της πολιτικής ασφαλείας, η σύνταξη του σχεδίου ασφαλείας και η εφαρμογή και παρακολούθηση του σχεδίου ασφαλείας.

Η επικινδυνότητα δεν μπορεί να μειωθεί σε μηδενικό επίπεδο. Αυτό συμβαίνει γιατί μηδενική επικινδυνότητα θα σήμαινε μηδενική αξία των περιουσιακών στοιχείων ή μηδενική πιθανότητα πραγματοποίησης μια απειλής. Συνεπώς, στόχος της διαχείρισης της επικινδυνότητας είναι η διατήρηση του επιπέδου του κινδύνου σε αποδεκτά επίπεδα. Η Διοίκηση του οργανισμού έχει την ευθύνη της υιοθέτησης της καλύτερης λύσης και μέτρων σε σχέση με το κόστος, τη μείωση του κινδύνου και την μικρότερη δυνατή επίδραση στους στόχους του οργανισμού.

Η διαχείριση της επικινδυνότητας μπορεί να γίνει με το μετριασμό της επικινδυνότητας την μεταβίβαση της επικινδυνότητας ,την αποδοχή της επικινδυνότητας ή την αποφυγή αυτής. Ο ***μετριασμός*** της επικινδυνότητας μπορεί να επιτευχθεί με τη μείωση της πιθανότητας εκδήλωσης απειλών, την αντιμετώπιση των αδυναμιών και τον περιορισμό των επιπτώσεων μια απειλής. Η ***μεταβίβαση*** της επικινδυνότητας είναι μια διαδικασία που επιτρέπει σε ένα άλλο μέρος να αποδεχθεί τον κίνδυνο. Ένα παράδειγμα αποτελεί η μεταβίβαση της επικινδυνότητας σε μια ασφαλιστική εταιρεία με την οποία δεν μειώνεται η πιθανότητα να συμβεί κάποιο ανεπιθύμητο γεγονός αλλά μετριάζονται οι συνέπειες για τον οργανισμό. Η ***αποδοχή*** της επικινδυνότητας είναι η λειτουργία του συστήματος με κάποιο γνωστό κίνδυνο. Ένας τέτοιος αποδεκτός κίνδυνος θα μπορούσε να είναι κάποιος που έχει υψηλό κόστος να περιοριστεί. Σε κάθε περίπτωση η απόφαση για την αποδοχή κάποιου κινδύνου θα πρέπει να παρθεί από τη Διοίκηση. Τέλος, η ***αποφυγή*** είναι η πρακτική αφαίρεσης των τρωτών σημείων του συστήματος ή και το ίδιο το σύστημα.

1.3 ΠΛΕΟΝΕΚΤΗΜΑΤΑ ΚΑΙ ΜΕΙΟΝΕΚΤΗΜΑΤΑ ΑΝΑΛΥΣΗΣ ΚΑΙ ΔΙΑΧΕΙΡΙΣΗΣ ΕΠΙΚΙΝΔΥΝΟΤΗΤΑΣ

Τα πλεονεκτήματα της Ανάλυσης και Διαχείρισης Επικινδυνότητας αναφέρονται παρακάτω:

1. Δίνει τη δυνατότητα της επικοινωνίας ανάμεσα στους ειδικούς της πληροφορικής και τη Διοίκηση του οργανισμού. Η ασφάλεια αποτιμάται σε όρους κόστους-ωφέλειας και αντιμετωπίζεται από τη Διοίκηση σαν μια επένδυση για τον οργανισμό.
2. Με την ανάλυση και διαχείριση της επικινδυνότητας αιτιολογείται το κόστος των αντιμέτρων που πρέπει να εφαρμοστούν.
3. Αποτελεί μια ευέλικτη μεθοδολογία που μπορεί να εφαρμοστεί με διάφορους τρόπους και σε συνδυασμό με άλλες μεθόδους.
4. Καλύπτει τις απαιτήσεις της ευρωπαϊκής και ελληνικής νομοθεσίας ως προς την ασφάλεια.
5. Βοηθά την καλύτερη κατανόηση του πληροφοριακού συστήματος αφού αποτελεί μέσο καταγραφής και ανάλυσης του.
6. Αποτελεί την πλέον διαδεδομένη μεθοδολογία με πληθώρα περιπτώσεων εφαρμογής.

Τα μειονεκτήματα της Ανάλυσης και Διαχείρισης της επικινδυνότητας παρουσιάζονται ως εξής:

1. Στηρίζεται σε ένα απλουστευμένο μοντέλο πληροφοριακού συστήματος και αγνοεί τα ιδιαίτερα χαρακτηριστικά του οργανισμού.
2. Εμπεριέχει σημαντική υποκειμενικότητα ως προς τον υπολογισμό της αξίας των αγαθών, των απειλών, των αδυναμιών, των επιπτώσεων και άρα τον υπολογισμό του κινδύνου. Συχνά συγκαλύπτεται με την χρήση αυστηρών μαθηματικών και πιθανοτικών μοντέλων.
3. Βασίζεται σε απλές στατιστικές μεθόδους για την πιθανότητα εμφάνισης μια απειλής κάτι το οποίο την καθιστά αμφισβητήσιμη από πολλούς ερευνητές.

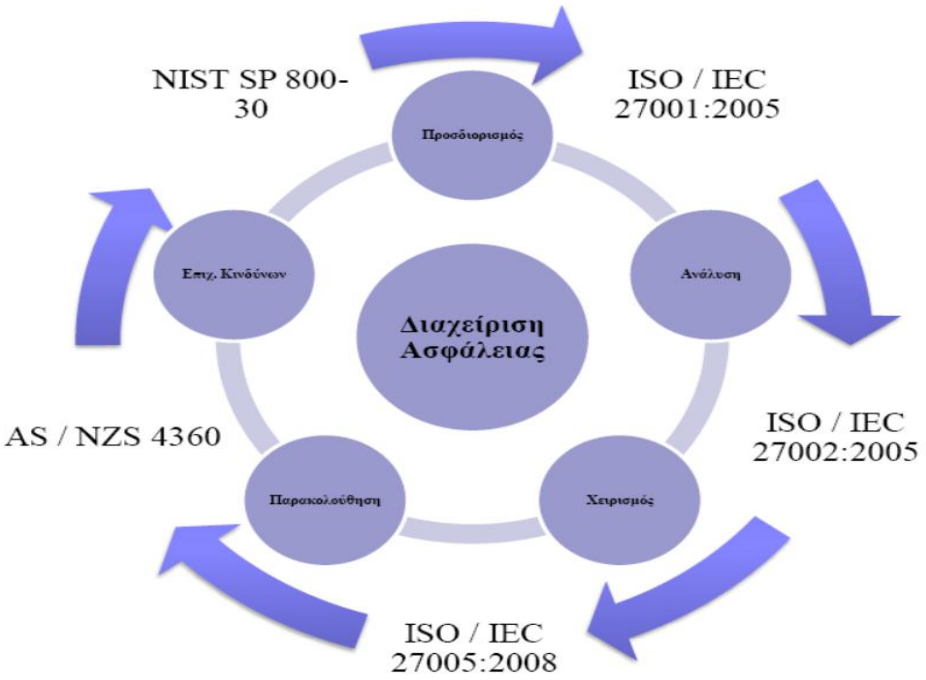
2. ΠΡΟΤΥΠΑ ΑΣΦΑΛΕΙΑΣ ΠΛΗΡΟΦΟΡΙΩΝ

2.1 ΕΙΣΑΓΩΓΗ

Η διαχείριση της ασφάλειας είναι μια διαδικασία που περιλαμβάνει την παρακολούθηση, ανάλυση και αντιμετώπιση των κινδύνων του κάθε οργανισμού. Αποσκοπεί στον περιορισμό της επικινδυνότητας σε ένα αποδεκτό επίπεδο. Στο κεφάλαιο αυτό περιγράφονται τα πιο σημαντικά διεθνή πρότυπα ασφαλείας. Αυτά είναι τα εξής:

[1] Το πρότυπο AS/NZS 4360
[2] Το πρότυπο NIST SP 800-30
[3] Το πρότυπο ISO/IEC 27001: 2005
[4] Το πρότυπο ISO/IEC 27002:2005
[5] Το πρότυπο ISO/IEC 27005: 2008

Τα πρότυπα [3],[4],[5] θα αναλυθούν στο 3^{ο} κεφάλαιο ενδελεχώς ως μέλη της οικογένειας ISO 27000.



ΕΙΚΟΝΑ 1: Βασικά πρότυπα διαχείρισης ασφάλειας

Πηγή: Risk assessment 2013- Δούσκας Θεόδωρος

2.2 ΠΡΟΤΥΠΑ ΑΣΦΑΛΕΙΑΣ

2.2.1 ΤΟ ΠΡΟΤΥΠΟ AS/NZS 4360

Το πρότυπο AS/NZS 4360 προτάθηκε από την Αυστραλία και τη Νέα Ζηλανδία το 1995. Παρέχει ένα γενικό οδηγό για τη Διαχείριση Κινδύνου σε υψηλό επίπεδο. Μπορεί να εφαρμοσθεί σε ένα ευρύ φάσμα συστημάτων, δραστηριοτήτων και οργανισμών. Δίνει μεγάλη έμφαση στον ακριβή προσδιορισμό του πλαισίου και είναι ευέλικτο. Από την άλλη μεριά δεν υποστηρίζεται από ένα πρακτικό εργαλείο και δεν επικεντρώνεται τόσο στην αντιμετώπιση του κινδύνου. Τα βασικά στάδια του προτύπου AS/NZS 4360 είναι τα εξής:

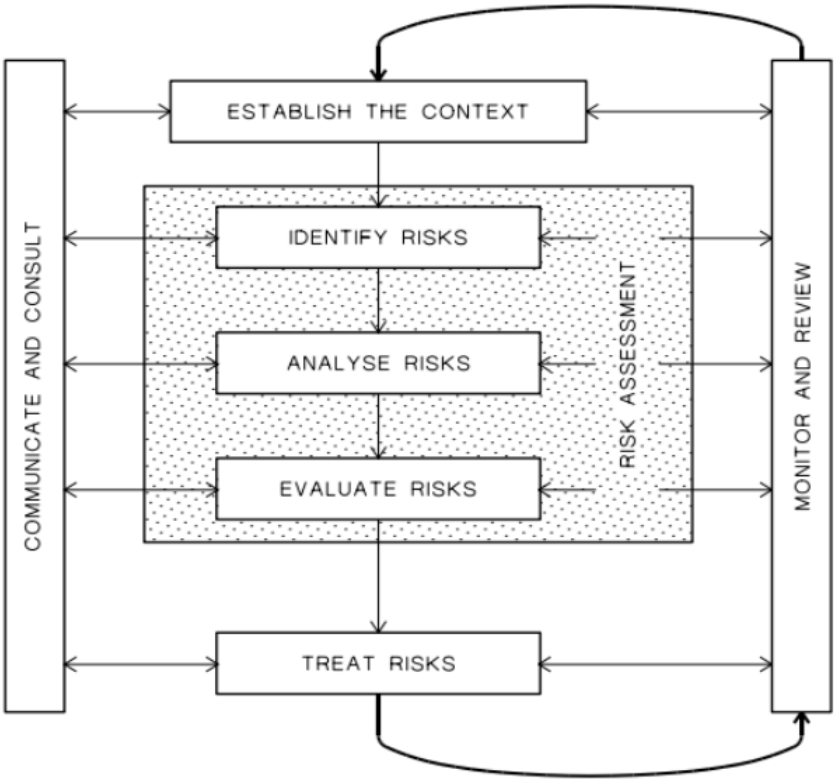
I. Καθορισμός του πλαισίου. Στο στάδιο αυτό καθορίζεται το εσωτερικό και εξωτερικό πλαίσιο του οργανισμού. Προσδιορίζονται τα κριτήρια σύμφωνα με τα οποία θα αξιολογηθεί ο κίνδυνος και οριοθετείται η όλη διαδικασία.
II. Προσδιορισμός των κινδύνων. Σε αυτό το στάδιο προσδιορίζονται το πως μπορούν να συμβούν οι κίνδυνοι και το ποιοι είναι αυτοί.
III. Ανάλυση των κινδύνων. Υπολογίζεται η πιθανότητα εμφάνισης των κινδύνων και οι επιπτώσεις που θα επιφέρουν. Ακόμα γίνεται μια αξιολόγηση των ήδη υπαρχόντων μέτρων ασφαλείας.
IV. Αξιολόγηση των κινδύνων. Με βάση τα αποτελέσματα της ανάλυσης των κινδύνων λαμβάνονται οι αποφάσεις σχετικά με το εάν επαρκούν τα μέτρα ασφαλείας και το ποιοι κίνδυνοι πρέπει να αντιμετωπιστούν.
V. Αντιμετώπιση των κινδύνων. Στο τελευταίο βήμα προσδιορίζονται οι τρόποι και τα μέτρα αντιμετώπισης των κινδύνων. Λαμβάνοντας υπόψιν το κόστος υλοποίησης και την αναγκαιότητα τους, αποφασίζεται ποια μέτρα θα εφαρμοστούν και καταστρώνεται ένα ολοκληρωμένο σχέδιο εφαρμογής τους.

Παράλληλα με τη διαδικασία της ανάλυσης και διαχείρισης κινδύνου που περιγράφηκε πρέπει να διενεργούνται και οι εξής δύο διαδικασίες:

I. Επικοινωνία και Συμβουλευτική.
Για τη λήψη των σωστών αποφάσεων και την ομαλή διενέργεια του εγχειρήματος είναι απαραίτητη η επικοινωνία με τα αρμόδια άτομα του οργανισμού καθ' όλη τη διάρκεια των σταδίων.

II. Παρακολούθηση και Αναθεώρηση. Σημαντική είναι η παρακολούθηση του έργου σε όλα τα στάδια για την βέλτιστη αντιμετώπιση των κινδύνων και την ανανέωση των πληροφοριών. Ακόμα αναγκαία είναι μια συνολική ανασκόπηση της διαδικασίας ανάλυσης και διαχείρισης επικινδυνότητας.

Στο παρακάτω σχήμα φαίνονται τα στάδια του προτύπου AS/NZS 4360:



ΕΙΚΟΝΑ 2: Το πρότυπο AS/NZS 4360

Πηγή: Project Risk Management for Sustainable Restoration of Immovable Cultural Heritage: Lessons from Construction Industry and Formulation of a Customized PRM Model

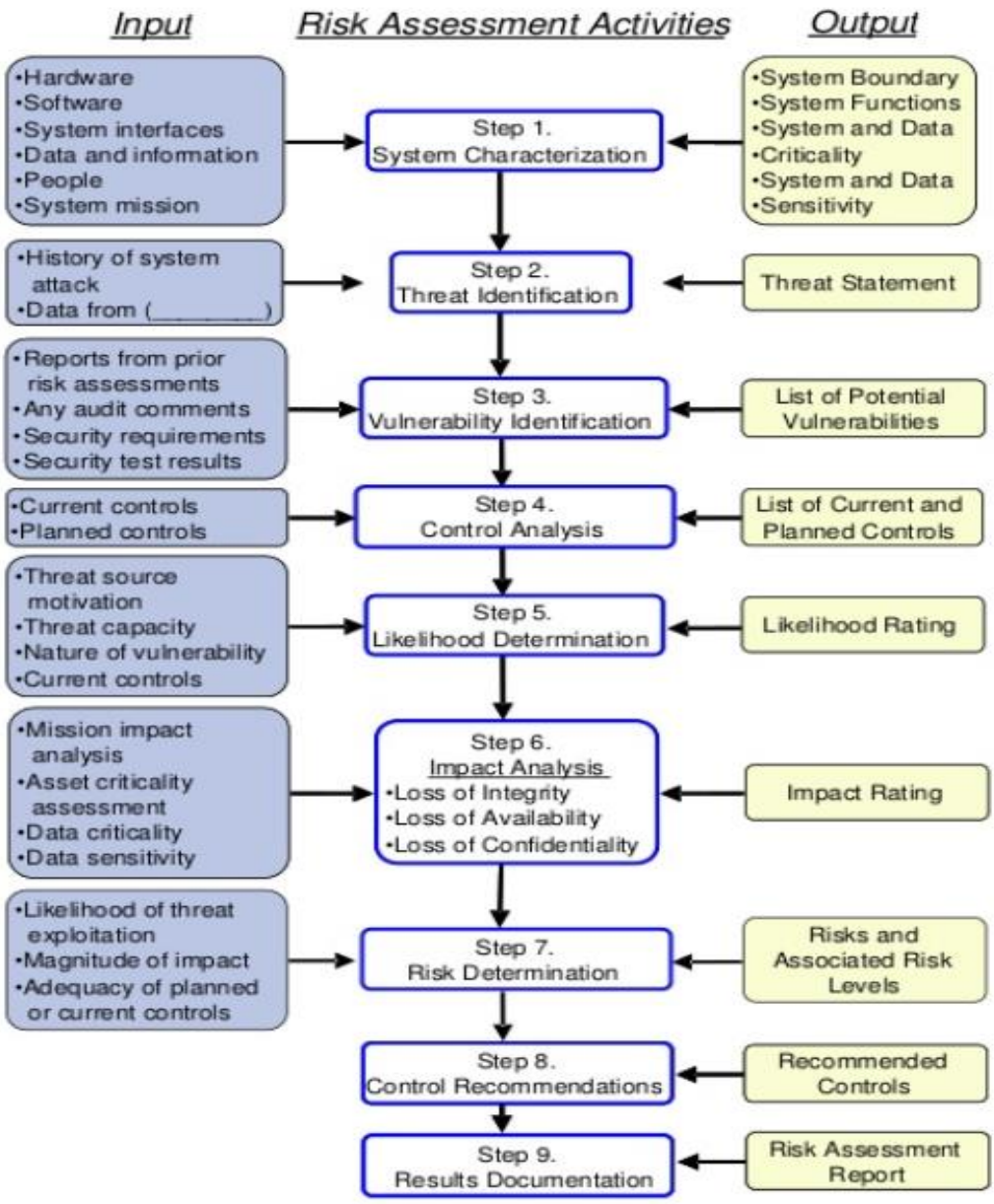
2.2.2 ΤΟ ΠΡΟΤΥΠΟ NIST SP 800-30

Το πρότυπο ασφαλείας NIST SP 800-30 εκδόθηκε το 2002 από το Εθνικό Ινστιτούτο Προτύπων και Τεχνολογίας Αμερικής και αποτελεί ένα δωρεάν πρότυπο διαχείρισης ασφαλείας. Η μέθοδος που προτείνει είναι κυρίως ποιοτική και περιλαμβάνει όλες τις διαδικασίες για την αποτελεσματική ανάλυση και διαχείριση των επιχειρηματικών κινδύνων. Απευθύνεται κυρίως σε εταιρείες μεγάλης κλίμακας και κυβερνητικούς οργανισμούς.
Το πρότυπο NIST SP 800-30 δεν συνοδεύεται από κάποιο εργαλείο μέτρησης της επικινδυνότητας. Επιπλέον, έχει υιοθετήσει τεχνικές και ερωτηματολόγια που απαιτούν τη συμμετοχή πολλών χρηστών αλλά δεν προάγει την συνεργασία για τον υπολογισμό των τελικών αποτελεσμάτων.

Το πρότυπο περιλαμβάνει τρία στάδια για τη διαχείριση της επικινδυνότητας:

I. Ανάλυση Επικινδυνότητας
   Στο στάδιο αυτό γίνεται ο προσδιορισμός των απειλών, των αδυναμιών και των κινδύνων καθώς και η ανάλυση των μέτρων προστασίας που θα μπορούσαν να εφαρμοστούν. Περιλαμβάνει εννέα βήματα:
   - Χαρακτηρισμό του συστήματος. Προσδιορίζονται τα αγαθά και ο στόχος της ανάλυσης επικινδυνότητας.
   - Αναγνώριση απειλών. Οι απειλές ταξινομούνται στις κατηγορίες –Φύση – Άνθρωποι – Περιβάλλον.
   - Αναγνώριση αδυναμιών.
   - Καταγραφή μέτρων ασφαλείας.
   - Καθορισμός πιθανότητας πραγμάτωσης. Προσδιορίζεται η πιθανότητα πραγματοποίησης ενός αρνητικού περιστατικού ασφαλείας.
   - Ανάλυση επιπτώσεων. Κατατάσσονται οι επιπτώσεις σε μια κλίμακα (Υψηλή, Μέτρια , Χαμηλή).
   - Καθορισμός επικινδυνότητας. Για τον υπολογισμό της επικινδυνότητας λαμβάνεται υπόψιν η πιθανότητα πραγμάτωσης μιας απειλής και η επίπτωση που θα επιφέρει η πραγμάτωση της.

- Προτεινόμενα μέτρα ασφαλείας. Αναλύονται τα μέτρα ασφαλείας ως προς την αποτελεσματικότητα τους, την νομική συμμόρφωση και τις αλλαγές που θα επιφέρουν στον οργανισμό.
- Δημιουργία αναφορών και τεκμηρίωσης.



ΕΙΚΟΝΑ 3: Στάδια ανάλυσης επικινδυνότητας κατά το NIST SP 800-30

Πηγή: common.wikimedia.org

II. Μετρίαση Κινδύνου

Από το προηγούμενο στάδιο ανάλυσης επικινδυνότητας έχουν προσδιοριστεί τα μέτρα ασφαλείας. Σε αυτό το στάδιο γίνεται η επιλογή των μέτρων που θα χρησιμοποιηθούν.

III. Αξιολόγηση και Αποτίμηση

Στο στάδιο αυτό αξιολογείται και παρακολουθείται το αποτέλεσμα της εφαρμογής των μέτρων ασφαλείας. Για την εξασφάλιση της ασφάλειας απαιτείται τακτική αξιολόγηση του σχεδίου ασφαλείας και αναβάθμιση του όπου κρίνεται αναγκαίο.

3. ΑΝΑΛΥΣΗ ΤΟΥ ISO

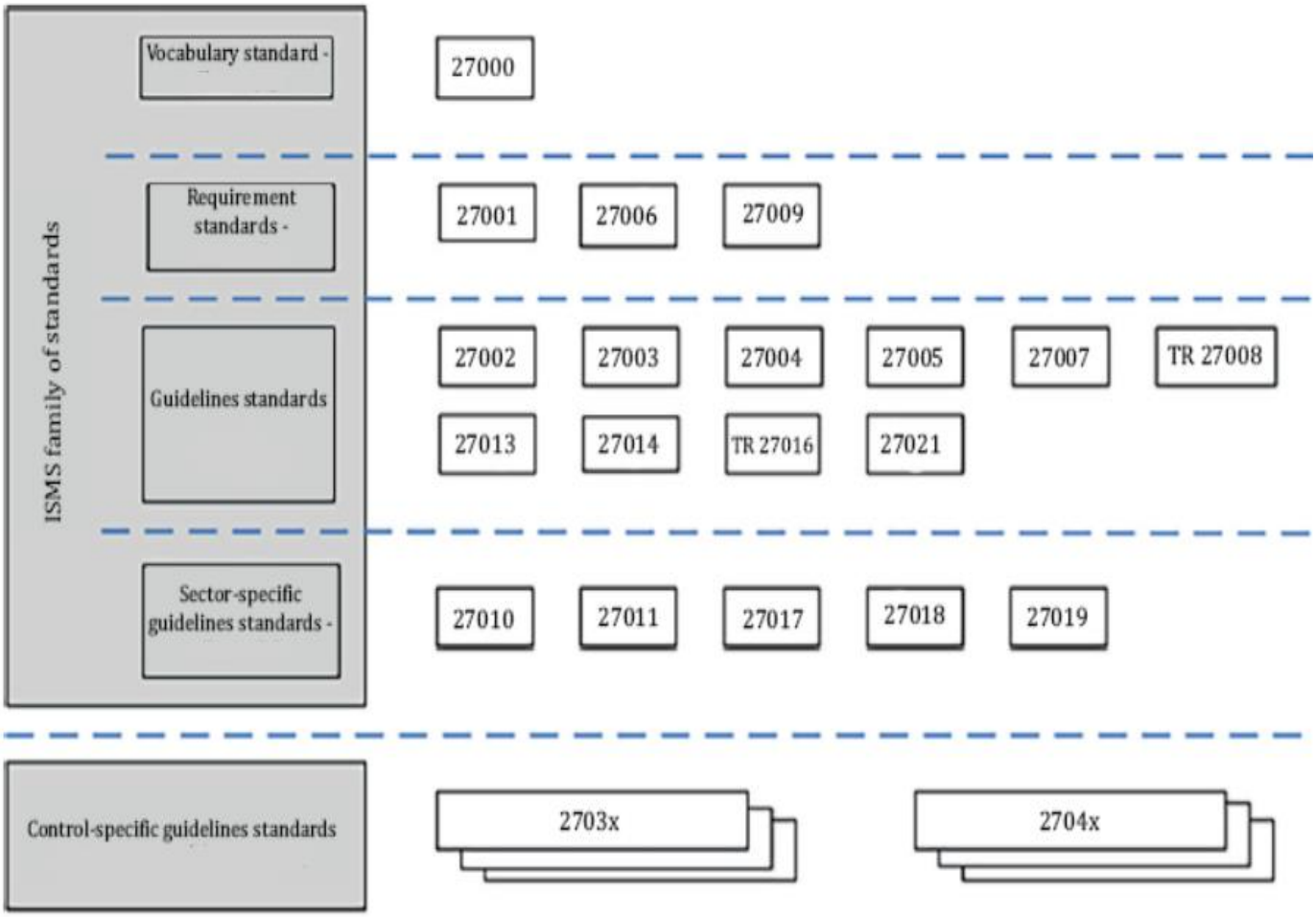
3.1 ΟΙΚΟΓΕΝΕΙΑ ISO 27000

Η σειρά προτύπων ISO 27000 αναπτύχθηκε από την κοινοπραξία δύο επιτροπών, του διεθνούς οργανισμού πιστοποίησης (International Organization for Standardization - ISO) και της διεθνούς ηλεκτροτεχνικής επιτροπής (International Electrotechnical Commission -IEC). Είναι επίσης γνωστή ως ISMS Family of Standards' ή ISO 27k. Χρησιμοποιώντας τη σειρά ISO 27k οι οργανισμοί μπορούν να αναπτύξουν ένα πλαίσιο για τη διαχείριση της ασφάλειας, να το υλοποιήσουν και να αξιολογήσουν τα αποτελέσματα του.

Η σειρά προτύπων ISO27K αποτελεί έναν οδηγό βέλτιστων πρακτικών για τη διαχείριση της ασφάλειας πληροφοριών και τη διαχείριση της σχετικής επικινδυνότητας ενός οργανισμού προτείνοντας κατάλληλα μέτρα. Μέχρι σήμερα 46 από τα πρότυπα της σειράς είναι διαθέσιμα και αρκετά βρίσκονται υπό ανάπτυξη.

Το ISO/IEC27001 είναι το κεντρικό πρότυπο της σειράς με το οποίο μπορεί ένας οργανισμός, εφόσον πληροί τις προϋποθέσεις, να πιστοποιηθεί από τρίτο ανεξάρτητο φορέα. Ο φορέας πιστοποίησης με τη σειρά του μπορεί να λάβει διαπίστευση, σύμφωνα με το πρότυπο ISO/IEC27006. Τα πρότυπα βρίσκουν εφαρμογή σε κάθε είδους και μεγέθους οργανισμούς. Παρέχουν ιδιωτικότητα, εμπιστευτικότητα και επιλύουν τεχνικά θέματα ασφαλείας. Όλοι οι οργανισμοί ενθαρρύνονται να αξιολογήσουν τους κινδύνους και να τους αντιμετωπίσουν με την ανάλογη καθοδήγηση. Λόγω του δυναμικού χαρακτήρα της ασφάλειας πληροφοριών, τα πρότυπα παρέχουν συνεχή ανατροφοδότηση και βελτιώσεις.

Στην παρακάτω εικόνα παρουσιάζεται η σχέση μεταξύ των κυριότερων προτύπων της οικογένειας ISO 27000:



ΕΙΚΟΝΑ 4: Σχέση προτύπων οικογένειας ISO 27000

Πηγή: ISO-IEC 27000 2018 5th edition

Στον παρακάτω πίνακα παρουσιάζονται τα δημοσιευμένα πρότυπα της οικογένειας 27000 που σχετίζονται με την ασφάλεια πληροφοριών.

	ΟΝΟΜΑ	ΑΝΤΙΚΕΙΜΕΝΟ
1	ISO/IEC 27000	Εισαγωγή και λεξιλόγιο όρων
2	ISO/IEC 27001	Απαιτήσεις υλοποίησης και συντήρησης Συστήματος Διαχείρισης Ασφάλειας Πληροφοριών
3	ISO/IEC 27002	Πρακτικές διαχείρισης της ασφάλειας και επιλογής μέτρων ασφάλειας
4	ISO/IEC 27003	Οδηγίες σχεδιασμού ενός Συστήματος Διαχείρισης Ασφάλειας ΠληροφοριώνISO
5	ISO/IEC 27004	Μετρικές εκτίμησης της αποτελεσματικότητας υλοποιημένου Συστήματος Διαχείρισης Ασφάλειας Πληροφοριών
6	ISO/IEC 27005	Οδηγίες διαχείρισης Επικινδυνότητας
7	ISO/IEC 27006	Οδηγίες ελέγχου και πιστοποίησης Συστήματος Διαχείρισης Ασφάλειας
8	ISO/IEC 27007	Οδηγίες ικανοτήτων ελεγκτών Συστημάτων Διαχείρισης Ασφάλειας Πληροφοριών
9	ISO/IEC 27008	Οδηγίες ελέγχου της υλοποίησης Συστήματος Διαχείρισης Ασφάλειας και Πληροφοριών
10	ISO/IEC 27009	Εσωτερικό έγγραφο για την επιτροπή που αναπτύσσει παραλλαγές συγκεκριμένων τομέων / βιομηχανιών ή κατευθυντήριες γραμμές εφαρμογής για τα πρότυπα ISO27K
11	ISO/IEC 27010	Οδηγίες για κοινότητες ανταλλαγής πληροφοριών
12	ISO/IEC 27011	Οδηγίες για τηλεπικοινωνιακούς οργανισμούς
13	ISO/IEC 27013	Οδηγίες υλοποίησης ISO/IEC 27001 και ISO/IEC 20000-1
14	ISO/IEC 27014	Έννοιες και αρχές διακυβέρνησης της ασφάλειας
15	ISO/IEC 27015	Οδηγίες για οργανισμούς παροχής χρηματοοικονομικών υπηρεσιών
16	ISO/IEC 27016	Οικονομικές επιπτώσεις αποφάσεων σχετικών με Διαχείριση Ασφάλειας Πληροφοριών
17	ISO/IEC 27017	Οδηγίες ελέγχου ασφαλείας βασισμένες στο ISO 27002 για υπηρεσίες υπολογιστικού νέφους (cloud services)
18	ISO/IEC 27018	Οδηγίες προστασίας Προσωπικών Αναγνωρίσιμων Πληροφοριών
19	ISO/IEC 27019	Οδηγίες για παρόχους Ηλεκτρικής Ενέργειας
20	ISO/IEC 27031	Περιγραφή εννοιών και αρχών επιχειρησιακής συνέχειας των Πληροφοριακών υποδομών
21	ISO/IEC 27032	Οδηγίες βελτίωσης της Κυβερνοασφάλειας
22	ISO/IEC 27033-1	Ασφάλεια δικτύων- Επισκόπηση και έννοιες
23	ISO/IEC 27033-2	Ασφάλεια δικτύων- οδηγίες για το σχεδιασμό και την υλοποίηση της ασφάλειας δικτύων
24	ISO/IEC 27033-3	Ασφάλεια δικτύων- Απειλές, τεχνικές σχεδιασμού και θέματα ελέγχου
25	ISO/IEC 27033-4	Ασφάλεια δικτύων- Ασφάλεια επικοινωνιών μεταξύ δικτύων με πύλες ασφαλείας

26	ISO/IEC 27033-5	Ασφάλεια δικτύων-- Ασφάλεια επικοινωνιών μεταξύ δικτύων μέσω VPN
27	ISO/IEC 27033-6	Ασφάλεια δικτύων- Εξασφάλιση πρόσβασης ασύρματου δικτύου IP
28	ISO/IEC 27034-1	Οδηγίες ενσωμάτωσης των μηχανισμών ασφάλειας στις επιχειρησιακές διεργασίες
29	ISO/IEC 27034-2	Οργανωτικό πλαίσιο
30	ISO/IEC 27034-6	Μελέτη περιπτώσεων
31	ISO/IEC 27035-1	Οδηγίες ανίχνευσης και αντιμετώπισης περιστατικών ασφάλειας
32	ISO/IEC 27035-2	Οδηγίες για το σχεδιασμό και την προετοιμασία για την αντιμετώπιση περιστατικών
33	ISO/IEC 27036-1	Ασφάλεια πληροφοριών για τις σχέσεις προμηθευτών-:Επισκόπηση
34	ISO/IEC 27036-2	Ασφάλεια πληροφοριών για τις σχέσεις προμηθευτών :Απαιτήσεις
35	ISO/IEC 27036-3	Ασφάλεια πληροφοριών για τις σχέσεις προμηθευτών :Οδηγίες για την ασφάλεια της αλυσίδας εφοδιασμού
36	ISO/IEC 27036-4	Ασφάλεια πληροφοριών για τις σχέσεις προμηθευτών :Οδηγίες για παρόχους υπηρεσιών cloud computing
37	ISO/IEC 27037	Οδηγίες διαχείρισης ψηφιακών τεκμηρίων
38	ISO/IEC 27038	Οδηγίες επιμέλειας ψηφιακών εγγράφων
39	ISO/IEC 27039	Πρόληψη εισβολής
40	ISO/IEC 27040	Ασφάλεια αποθεμάτων
41	ISO/IEC 27041	Ασφάλεια ερευνών
42	ISO/IEC 27042	Ανάλυση ψηφιακών αποδείξεων
43	ISO/IEC 27043	Διερεύνηση περιστατικών
44	ISO/IEC 27050-1	Ηλεκτρονικά ευρήματα
45	ISO/IEC 27050-2	Καθοδήγηση για τη διακυβέρνηση και τη διαχείριση της ηλεκτρονικών ευρημάτων
46	ISO/IEC 27799	Οδηγίες υλοποίησης του ISO/IEC 27002 σε οργανισμούς υγείας

ΠΙΝΑΚΑΣ 1: Τα πρότυπα της οικογένειας 27000

Πηγή : en.wikipedia.org/wiki/ISO/IEC_27000-series

3.2 ΤΟ ΠΡΟΤΥΠΟ ISO/IEC 27001:2005

3.2 1. ΓΕΝΙΚΑ ΣΤΟΙΧΕΙΑ

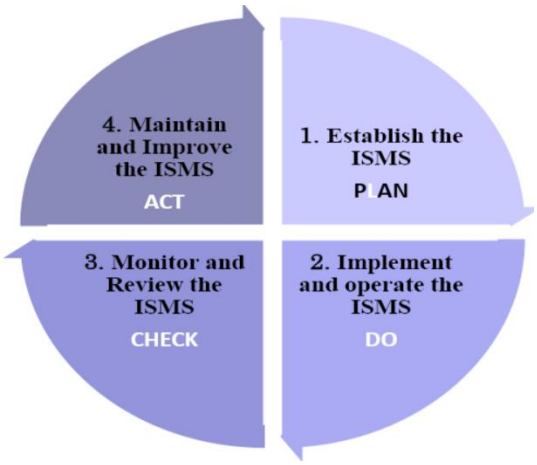
Το πρότυπο ISO/IEC 27001:2005 που εκδόθηκε τον Οκτώβριο του 2005 από την ISO και IEC αποτελεί βασικό μέλος της οικογένειας ISO 27000. Το πλήρες όνομα του είναι Information Technology – Security Techniques- Information security management systems requirements και εν συντομία ISO 27001. Αποτελεί ένα πρότυπο σύστημα διαχείρισης ασφάλειας πληροφοριών (ISMS).

Το πρότυπο ISO/IEC 27001 μπορεί να εφαρμοστεί σε επιχειρήσεις οποιουδήποτε επιχειρηματικού κλάδου και μεγέθους. Παρ' όλα αυτά καλύπτει κυρίως μεγάλης κλίμακας επιχειρήσεις καθώς είναι αρκετά πολύπλοκο για τις μικρές και μεσαίες επιχειρήσεις. Μια επιχείρηση ακολουθώντας το πρότυπο ISO/IEC 27001 μπορεί να μειώσει τον επιχειρηματικό κίνδυνο και να συμμορφωθεί με τα νομικά πλαίσια αλλά και να αυξήσει την ανταγωνιστικότητα της, να προβάλει την εμπορική της εικόνα και να κερδίσει την εμπιστοσύνη των πελατών.

Το ISO/IEC 27001:2005 αντικαταστάθηκε από το νέο πρότυπο ISO/IEC 27001:2013. Το ISO/IEC 27001:2013 δίνει μεγαλύτερη έμφαση στη μέτρηση και την αξιολόγηση της καλής λειτουργίας του οργανισμού, δεν τονίζεται ο κύκλος “Plan – Do – Check – Act” (ενότητα 3.2.2) και αναφέρεται στην εξωτερική ανάθεση των οργανισμών σε τρίτα μέρη που δεν περιλαμβάνεται στο ISO/IEC 27001:2005.

3.2.2 ΤΟ ΜΟΝΤΕΛΟ PDCA

Το ISO/IEC 27001:2005 ακολουθεί τη διαδικασία «Σχεδιάζω - Εκτελώ - Ελέγχω - Ενεργώ» (ΣΕΕΕ) «Plan - Do - Check - Act» (PDCA). Το μοντέλο PDCA παρουσιάζεται στην διπλανή εικόνα:



ΕΙΚΟΝΑ 5: Το μοντέλο PDCA

Πηγή: Risk assessment 2013- Δούσκας Θεόδωρος

1. Σχεδιάζω: Στο στάδιο αυτό καθορίζεται η πολιτική και οι στόχοι του συστήματος διαχείρισης πληροφοριών. Αναλύονται οι απαιτήσεις ασφάλειας των συστημάτων, των εφαρμογών, των υποδομών και των πληροφοριών του οργανισμού. Εντοπίζονται τα ευαίσθητα, από πλευράς ασφάλειας, σημεία ανάλογα με το βαθμό κρισιμότητας τους. Προσδιορίζονται οι διεργασίες και διαδικασίες που είναι απαραίτητες για την διαχείριση του κινδύνου και την εξασφάλιση της ασφάλειας σύμφωνα με την πολιτική του οργανισμού και τους στόχους των πελατών. Περιλαμβάνει την Διενέργεια Ανάλυσης και Διαχείρισης Κινδύνου (Risk Analysis and Risk Management), την Σύνταξη Πολιτικής Ασφάλειας (Security Policy), την Σύνταξη Σχεδίου Συνέχειας Λειτουργιών (Business Continuity Plan) και την Σύνταξη Σχεδίου Ανάκαμψης Συστημάτων Disaster Recovery Plan.

2. Εκτελώ: Σε αυτό το στάδιο υλοποιείται και τίθεται σε λειτουργία το σύστημα διαχείρισης ασφάλειας πληροφοριών. Προδιαγράφονται οι τεχνικές λύσεις που απαιτούνται για την υλοποίηση των απαιτήσεων ασφαλείας. Σχεδιάζεται η αρχιτεκτονική ασφαλείας του δικτύου και καθορίζονται τα σημεία ελέγχου εισόδου και εξόδου. Το δίκτυο διαχωρίζεται σε εικονικά ιδιωτικά δίκτυα (VPN) ή ανεξάρτητες ζώνες και καθορίζονται οι προδιαγραφές του δικτυακού εξοπλισμού

ασφαλείας (Firewall, Anti-virus, router, σημεία ασύρματης πρόσβασης κ.α.). Πραγματοποιείται η εγκατάσταση και η λειτουργία του απαιτούμενου εξοπλισμού ασφάλειας (υλικού και λογισμικού) και τέλος παραμετροποιούνται τα συστήματα και οι εφαρμογές (δημιουργία χρηστών, κωδικών πρόσβασής κ.α.).

3. Ελέγχω: Παρακολουθείται και αξιολογείται η επίδοση των διαδικασιών σε συνάρτηση με τους σκοπούς και την πολιτική του οργανισμού και παρουσιάζονται τα αποτελέσματα. Το στάδιο αυτό περιλαμβάνει την καθημερινή παρακολούθηση της ορθής λειτουργίας των συστημάτων από τα αρχεία καταγραφής λειτουργικών συστημάτων και εφαρμογών και τον έλεγχο των χρηστών και των δικαιωμάτων αυτών. Ακόμα πραγματοποιείται τακτική ενημέρωση των εφαρμογών και συστημάτων ασφάλειας (π.χ. κανόνων πρόσβασης του firewall, ενημέρωση του anti-virus). Παρακολουθούνται οι εξειδικευμένοι μηχανισμοί εντοπισμού πιθανών προβλημάτων και γίνονται έλεγχοι για την επιβεβαίωση της εφαρμογής των επιλεγμένων μέτρων και την αποτελεσματικότητας αυτών. Οι έλεγχοι αυτοί μπορεί να είναι εσωτερικοί (internal audits) ή εξωτερικοί έλεγχοι από ανεξάρτητους φορείς (external or independent audits) και μπορεί να στηρίζονται σε ερωτηματολόγια ελέγχου διαδικασιών, τεχνικούς ελέγχους κ.α.

4. Ενεργώ: Τέλος, με βάση τα αποτελέσματα του σταδίου «Ελέγχω» δημιουργείται η ανάγκη για αναθεώρηση. Ο έλεγχος της αναθεώρησης πρέπει να γίνεται ανεξάρτητα από το αν θα γίνουν ή όχι αλλαγές. Στόχος του σταδίου αυτού είναι η διατήρηση και βελτίωση του συστήματος με λήψη προληπτικών και διορθωτικών μέτρων.

3.2.3 ΟΙ ΤΟΜΕΙΣ ΤΟΥ ISO/IEC 27001

Το πρότυπο αυτό προσφέρει το γενικότερο πλαίσιο για την εφαρμογή επιμέρους πολιτικών ασφαλείας. Καθορίζει τις απαιτήσεις του συστήματος Διαχείρισης ασφάλειας πληροφοριών με στόχο τη διατήρηση της εμπιστευτικότητας, της ακεραιότητας και της διαθεσιμότητας της πληροφορίας. Το πρότυπο ISO/IEC 27001 διακρίνει την ασφάλεια σε δεκατέσσερεις βασικούς τομείς καθένας από τους οποίους προδιαγράφεται ενδελεχώς. Όσο περισσότερο η επιχείρηση πληροί αυτές τις προδιαγραφές τόσο πιο ασφαλής είναι.

Οι τομείς του ISO/IEC 27001 είναι:

	ΤΟΜΕΙΣ
1	ΠΟΛΙΤΙΚΗ ΑΣΦΑΛΕΙΑΣ
2	ΟΡΓΑΝΩΣΗ ΑΣΦΑΛΕΙΑΣ ΠΛΗΡΟΦΟΡΙΑΣ
3	ΑΣΦΑΛΕΙΑ ΔΙΑΧΕΙΡΙΣΗΣ ΠΟΡΩΝ
4	ΑΣΦΑΛΕΙΑ ΑΝΘΡΩΠΙΝΩΝ ΠΟΡΩΝ
5	ΦΥΣΙΚΗ ΑΣΦΑΛΕΙΑ ΧΩΡΩΝ
6	ΔΙΑΧΕΙΡΙΣΗ ΑΣΦΑΛΕΙΑΣ ΕΡΓΑΣΙΩΝ
7	ΔΙΑΧΕΙΡΙΣΗ ΑΣΦΑΛΕΙΑΣ ΕΠΙΚΟΙΝΩΝΙΩΝ
8	ΕΛΕΓΧΟΣ ΠΡΟΣΒΑΣΗΣ
9	ΑΠΟΚΤΗΣΗ, ΑΝΑΠΤΥΞΗ ΚΑΙ ΣΥΝΤΗΡΗΣΗ ΠΛΗΡΟΦΟΡΙΑΚΩΝ ΣΥΣΤΗΜΑΤΩΝ
10	ΚΡΥΠΤΟΓΡΑΦΗΣΗ
11	ΣΧΕΣΕΙΣ ΜΕ ΠΡΟΜΗΘΕΥΤΕΣ
12	ΔΙΑΧΕΙΡΙΣΗ ΠΕΡΙΣΤΑΤΙΚΩΝ ΑΣΦΑΛΕΙΑΣ
13	ΔΙΑΧΕΙΡΙΣΗ ΕΠΙΧΕΙΡΗΣΙΑΚΗΣ ΣΥΝΕΧΕΙΑΣ
14	ΣΥΜΜΟΡΦΩΣΗ

ΠΙΝΑΚΑΣ 2: Τομείς του ISO 27001

1. **Πολιτική Ασφαλείας**

   Ο σκοπός αυτού του τομέα είναι να παρέχει κατευθυντήριες γραμμές και υποστήριξη για την ασφάλεια των πληροφοριών σύμφωνα με τις επιχειρηματικές απαιτήσεις και τους σχετικούς νόμους και κανονισμούς. Το σύνολο των πολιτικών για την ασφάλεια των πληροφοριών πρέπει να προσδιοριστεί, να εγκριθεί από τη Διοίκηση, να δημοσιοποιηθεί και να γνωστοποιηθεί στους υπαλλήλους και τους εξωτερικούς συνεργάτες. Οι πολιτικές ασφάλειας θα επανεξεταστούν κατά το σχεδιασμό και μπορεί να προκύψουν σημαντικές αλλαγές προκειμένου να διασφαλιστεί η συνεχής καταλληλότητα, η επάρκεια και η αποτελεσματικότητα τους.

2. **Οργάνωση Ασφαλείας της Πληροφοριών**

   Στο στάδιο αυτό δημιουργείται το πλαίσιο διαχείρισης για την έναρξη της υλοποίησης και τον έλεγχο της λειτουργίας της ασφάλειας των πληροφοριών σε έναν οργανισμό.

   Εσωτερική Οργάνωση:

   Καθορίζονται οι ρόλοι και οι ευθύνες. Διαχωρίζονται τα καθήκοντα ώστε να μειωθεί η πιθανότητα για μη εξουσιοδοτημένη ή ακούσια τροποποίηση ή κατάχρηση των περιουσιακών στοιχείων του οργανισμού. Γίνεται η επικοινωνία με κατάλληλες ομάδες ειδικών. Η ασφάλεια πληροφορίας κατευθύνεται στη Διοίκηση Έργου.

   Εξωτερικοί κίνδυνοι(κινητές συσκευές και τηλε- εργασία):

   Θεσπίζεται η πολιτική και τα υποστηρικτικά μέτρα ασφαλείας για τη διαχείριση των κινδύνων που προκύπτουν με τη χρήση κινητών συσκευών. Ακόμη ορίζονται τα μέτρα που πρέπει να εφαρμοστούν για την προστασία της πληροφορίας που διαδίδεται και αποθηκεύεται κατά την εργασία από απόσταση.

3. **Διαχείριση περιουσιακών στοιχείων**

   Ευθύνη για τα περιουσιακά στοιχεία:

   Στο στάδιο αυτό προσδιορίζονται τα αγαθά που σχετίζονται με την ασφάλεια. Συντάσσεται και διατηρείται ένας κατάλογος αυτών των περιουσιακών στοιχείων.

Αναγνωρίζονται, καταγράφονται και υλοποιούνται οι κανόνες της επιτρεπτής χρήσης των αγαθών αυτών. Τέλος, κατά τη λήξη της εργασίας ενός εργαζομένου όλα τα αγαθά πρέπει να επιστρέφονται.

Διαβάθμιση πληροφορίας:

Η πληροφορίες ταξινομούνται ανάλογα με τις νομικές απαιτήσεις, την αξία, την κρισιμότητα και την ευαισθησία σε μη εξουσιοδοτημένη τροποποίηση ή παραβίαση. Ορίζονται διαδικασίες για την διαχείριση των αγαθών ανάλογα με την κατηγορία στην οποία κατατάχθηκαν από τον οργανισμό.

Χειρισμός Media:

Συγκεκριμένες διαδικασίες πρέπει να εφαρμοστούν για τη διαχείριση των αφαιρούμενων μέσων. Τα Μέσα Ενημέρωσης δεν πρέπει να έχουν πρόσβαση στον Οργανισμό, όταν δεν απαιτούνται πλέον, χρησιμοποιώντας τυπικές διαδικασίες.

4. Ασφάλεια Ανθρωπίνων Πόρων

Στόχος αυτού του τομέα είναι να εξασφαλίσει ότι οι υπάλληλοι και οι ανάδοχοι έργων κατανοούν τις ευθύνες τους και είναι κατάλληλοι για το ρόλο που έχουν αναλάβει.

Πριν την πρόσληψη:

Ελέγχεται το ιστορικό των εργαζομένων σύμφωνα με τους σχετικούς νόμους και κανονισμούς δεοντολογίας. Αυτό θα πρέπει να είναι ανάλογο με τις επιχειρηματικές απαιτήσεις και την κατηγορία των πληροφοριών στις οποίες θα έχουν πρόσβαση. Οι συμβάσεις με τους εργαζομένους και τους υπόλοιπους συμβαλλόμενους πρέπει να αναφέρουν ρητά της ευθύνες τους ως προς την ασφάλεια πληροφοριών.

Κατά τη διάρκεια της εργασίας:

Η Διοίκηση ζητά από τους εργαζομένους και τους συμβαλλόμενους να τηρούν τα μέτρα ασφάλειας πληροφοριών του οργανισμού. Όλοι οι εργαζόμενοι θα πρέπει να εκπαιδευτούν ως προς την ασφάλεια πληροφοριών σε σχέση με τη θέση τους και να επανεκπαιδεύονται σε τακτά χρονικά διαστήματα. Ακόμα πρέπει να

υπάρχει μια πειθαρχική διαδικασία στην οποία θα υποβάλλονται οι εργαζόμενοι που θα παραβιάζουν την ασφάλεια.

Λήξη εργασίας (παραίτηση ή απόλυση)

Αποσαφηνίζονται οι ευθύνες του εργαζομένου απέναντι στον οργανισμό κατά τη λήξη της εργασίας για την προστασία της ασφάλειας.

5. Φυσική Ασφάλεια Χώρων

Ασφαλισμένες περιοχές:

Οριοθετούνται οι περιοχές με ευαίσθητες ή κρίσιμες πληροφορίες. Οι περιοχές αυτές ασφαλείας παρακολουθούνται με κατάλληλα μέσα ελέγχου ώστε να διασφαλίζεται ότι μόνο τα εξουσιοδοτημένα άτομα θα έχουν πρόσβαση. Ακόμη, πρέπει να σχεδιαστούν και να εφαρμοστούν κάποια μέτρα για την προστασία των γραφείων και των χώρων. Απαραίτητη είναι και η εξασφάλιση της προστασίας από φυσικές καταστροφές και κακόβουλες επιθέσεις. Σε αυτό το στάδιο ορίζονται και οι διαδικασίες για την εργασία στις ασφαλισμένες περιοχές. Τέλος τα σημεία οπού και άτομα χωρίς άδεια μπορεί να παρευρεθούν (όπως τα σημεία φόρτωσης και παράδοσης) πρέπει να ελέγχονται και εάν είναι εφικτό να απομονώνονται από τις πληροφορίες.

Ασφάλεια εξοπλισμού:

Ο εξοπλισμός πρέπει να προστατεύεται για να μειωθούν οι κίνδυνοι από περιβαλλοντικές απειλές καθώς και οι κίνδυνοι από μη εξουσιοδοτημένη χρήση ή πρόσβαση. Ο εξοπλισμός θα πρέπει να προστατεύεται από διακοπές ρεύματος και αποτυχίες των υποστηρικτικών προγραμμάτων. Τα καλώδια τροφοδοσίας και επικοινωνιών που μεταφέρουν δεδομένα πρέπει να προστατεύονται από παρακολούθηση, παρεμβολή ή ζημία. Ο εξοπλισμός πρέπει να συντηρείται επαρκώς ώστε να διασφαλίζεται η διαθεσιμότητα και η ακεραιότητα του. Δεν θα πρέπει να μετακινείται χωρίς έγκριση. Επιπλέον, ο εξοπλισμός χωρίς επιτήρηση πρέπει να προστατεύεται. Τέλος, όλα τα είδη εξοπλισμού που περιέχουν μέσα αποθήκευσης πρέπει εξακριβώνεται ότι δεν έχουν πλέον ευαίσθητα δεδομένα και το λογισμικό πριν από επαναχρησιμοποιηθούν ή διατεθούν.

6. Διαχείριση Ασφαλείας Εργασιών

Επιχειρησιακές διαδικασίες και αρμοδιότητες:

Οι λειτουργικές εργασίες καταγράφονται και αρχειοθετούνται ώστε να είναι διαθέσιμες για τους χρήστες. Τυχόν αλλαγές στην οργάνωση, στις επιχειρηματικές διαδικασίες και στα συστήματα πληροφοριών πρέπει να ελέγχονται. Η χρήση πόρων παρακολουθείται και συντονίζονται μελλοντικές απαιτήσεις του συστήματος. Διαχωρίζονται τα στάδια της ανάπτυξης, των δοκιμών και της λειτουργίας ώστε να περιοριστεί η επίπτωση από μη εξουσιοδοτημένη πρόσβαση σε αυτά.

Προστασία από κακόβουλο λογισμικό και μεταφερόμενο κώδικα:

Πραγματοποιείται ανίχνευση, πρόληψη και αποκατάσταση κακόβουλων εισβολών.

Αρχειοθέτηση –Backup:

Σκοπός είναι η αποφυγή απώλειας δεδομένων. Δημιουργούνται αντίγραφα ασφαλείας για τις πληροφορίες, το λογισμικό και τις εικόνες του συστήματος σύμφωνα με την πολιτική της εταιρείας για την δημιουργία αντιγράφων.

Διαχείριση υπηρεσιών προσφερόμενων από τρίτους

Παρακολούθηση:

Καταγραφή σε αρχεία των δραστηριοτήτων, των εξαιρέσεων, των λαθών και των γεγονότων. Τα αρχεία αυτά θα ανανεώνονται τακτικά και θα προστατεύονται από μη εξουσιοδοτημένη πρόσβαση. Επίσης, οι δραστηριότητες του διαχειριστή του συστήματος πρέπει να καταγράφονται.

Έλεγχος λογισμικού:

Η εγκατάσταση λογισμικού πρέπει να ελέγχεται από συγκεκριμένες διαδικασίες.

Ελεγκτικές διαδικασίες:

Διαδικασίες ελέγχου (audit) που απαιτούν την επαλήθευση των λειτουργικών συστημάτων πρέπει να οργανώνονται προσεκτικά για να μην παρεμποδίζονται οι επιχειρηματικές διαδικασίες.

7. Διαχείριση Ασφαλείας Επικοινωνιών

Διαχείριση ασφάλειας δικτύου:

Πραγματοποιείται έλεγχος του δικτύου για να προστατευτούν οι πληροφορίες του συστήματος και των εφαρμογών. Ομάδες υπηρεσιών πληροφοριών, χρήστες και συστήματα πληροφοριών πρέπει να διαχωρίζονται σε δίκτυα. Οι μηχανισμοί ασφαλείας των δικτύων πρέπει να προσδιορίζονται και να καταγράφονται επιμελώς.

Ανταλλαγή δεδομένων:

Σκοπός αυτού του σταδίου είναι να εξασφαλίσει ότι οι πληροφορίες μεταφέρονται με ασφάλεια μέσα στον οργανισμό αλλά και σε εξωτερικούς συνεργάτες. Ορίζονται οι πολιτικές ανταλλαγής δεδομένων, οι διαδικασίες και οι απαραίτητοι έλεγχοι για την ανταλλαγή δεδομένων με χρήση όλων των μέσων επικοινωνίας. Ακόμα συμφωνούνται οι κανόνες ανταλλαγής πληροφοριών με τρίτους και προστατεύονται οι ηλεκτρονικές επικοινωνίες. Πρέπει να προσδιορίζονται οι απαιτήσεις για εμπιστευτικότητα ή μη αποκάλυψη συμφωνιών, να αναθεωρούνται τακτικά και να τεκμηριώνονται σύμφωνα με τις ανάγκες του οργανισμού.

8. Έλεγχος Πρόσβασης

Απαιτήσεις ελέγχου πρόσβασης:

Εγκαθίσταται μια πολιτική ελέγχου της πρόσβασης, τεκμηριώνεται και αναθεωρείται σύμφωνα με τις απαιτήσεις ασφαλείας.

Διαχείριση πρόσβασης χρηστών:

Ορίζεται μια διαδικασία εγγραφής και διαγραφής των χρηστών και μια επίσημη διαδικασία για την ενεργοποίηση και απενεργοποίηση των δικαιωμάτων πρόσβασης για όλους τους τύπους χρηστών σε όλα τα συστήματα. Η χρήση προνομιακών δικαιωμάτων πρόσβασης πρέπει να ελέγχεται και να είναι περιορισμένη. Πρέπει να γίνεται επανεξέταση των δικαιωμάτων των χρηστών σε τακτά χρονικά διαστήματα. Τέλος, σε περίπτωση διακοπής της συνεργασίας τόσο με τους εργαζομένους όσο και με τρίτους όλες οι πληροφορίες και οι άδειες χρήσης πρέπει να απομακρύνονται από αυτούς.

Αρμοδιότητες χρηστών:

Η πρόσβαση των χρηστών στις πληροφορίες και στις εφαρμογές του συστήματος πρέπει να γίνεται σύμφωνα με την πολιτική πρόσβασης του οργανισμού.

Έλεγχος πρόσβασης στο δίκτυο:

Η πρόσβαση σε συγκεκριμένα δίκτυα και στις υπηρεσίες δικτύων θα γίνεται μόνο στους ειδικά εξουσιοδοτημένους χρήστες.

Έλεγχος πρόσβασης στο λειτουργικό σύστημα και σε εφαρμογές:

Η πρόσβαση στο λειτουργικό σύστημα και στις εφαρμογές πρέπει να είναι σύμφωνη με την πολιτική πρόσβασης του οργανισμού. Όπου απαιτείται μπορεί να ελέγχεται από ασφαλείς ειδικές διαδικασίες. Οι μηχανισμοί διαχείρισης κωδικών (passwords) πρέπει να είναι διαδραστικοί, να ζητούν τακτική ανανέωση των κωδικών και να εξασφαλίζουν την ισχυρότητα των κωδικών. Η πρόσβαση στον πηγαίο κώδικα πρέπει να είναι περιορισμένη.

9. Απόκτηση, Ανάπτυξη και Συντήρηση Πληροφοριακών Συστημάτων.

Απαιτήσεις ασφάλειας πληροφοριακών συστημάτων:

Οι απαιτήσεις ασφαλείας που έχουν ορισθεί θα πρέπει να περιλαμβάνονται στις απαιτήσεις για νέα συστήματα πληροφοριών και στις βελτιώσεις των υπαρχόντων.

Ορθή επεξεργασία στις εφαρμογές:

Οι πληροφορίες που εμπλέκονται σε υπηρεσίες εφαρμογών που μεταδίδονται σε δημόσια δίκτυα πρέπει να προστατεύονται από υποκλοπές, μη εξουσιοδοτημένη αποκάλυψη ή τροποποίηση. Οι πληροφορίες σε υπηρεσίες εφαρμογών θα πρέπει να προστατεύονται από ανεπιτυχή ή μη ολοκληρωμένη μετάδοση, λάθη δρομολόγησης, μη εξουσιοδοτημένη μεταβολή μηνύματος, μη εξουσιοδοτημένη αποκάλυψη, αλληλοεπικάλυψη ή επανάληψη μηνυμάτων.

Ασφάλεια αρχείων συστήματος

Ασφάλεια δεδομένων δοκιμών και ελέγχων

Ασφάλεια στις διαδικασίες ανάπτυξης και υποστήριξης:

Διαμορφώνονται οι κανόνες για την ανάπτυξη λογισμικού και των συστημάτων και εφαρμόζονται σε όλες τις υλοποιήσεις του οργανισμού. Αλλαγές στα συστήματα κατά τη διάρκεια της ανάπτυξης πρέπει να ελέγχονται από κατάλληλες διαδικασίες. Όταν γίνονται αλλαγές στα λειτουργικά οι κρίσιμες για την επιχείρηση εφαρμογές πρέπει να ελέγχονται ώστε να μην υπάρχει αρνητική επίπτωση στον οργανισμό. Ο οργανισμός πρέπει να παρέχει ασφαλή περιβάλλοντα ανάπτυξης για ολόκληρο τον κύκλο ανάπτυξης του συστήματος και να υποστηρίζει την πραγματοποίηση πλήθους δοκιμών αυτών. Τέλος, ο οργανισμός οφείλει να επιβλέπει την δραστηριότητα των συνεργατών.

Διαχείριση τεχνικών αδυναμιών

10. Κρυπτογράφηση

Ορίζεται η πολιτική στη χρήση της κρυπτογράφησης για την προστασία των πληροφοριών και οι όροι για τη χρήση και το χρόνο ζωής των κρυπτογραφικών κλειδιών.

11. Σχέσεις με προμηθευτές

Ασφάλεια των πληροφοριών που ανταλλάσσονται με τους προμηθευτές:

Συμφωνούνται οι απαιτήσεις ασφαλείας για τον περιορισμό του κινδύνου που σχετίζεται με την πρόσβαση του προμηθευτή στα περιουσιακά στοιχεία του οργανισμού. Οι σχετικές απαιτήσεις ασφαλείας πρέπει να συμφωνούνται με κάθε προμηθευτή ξεχωριστά ο οποίος μπορεί να έχει πρόσβαση, να αποθηκεύει, να επεξεργάζεται ή να παρέχει συστήματα πληροφορικής.

Ασφάλεια διανομής των υπηρεσιών των προμηθευτών:

Οι οργανισμοί πρέπει να παρακολουθούν και να ελέγχουν την διανομή των υπηρεσιών από τους προμηθευτές. Αλλαγές στον τρόπο διανομής των υπηρεσιών και βελτιώσεις πρέπει να γίνονται σύμφωνα με την κρισιμότητα των πληροφοριών, των συστημάτων και των διαδικασιών.

12. Διαχείριση Περιστατικών Ασφαλείας

Αναφορά περιστατικών και αδυναμιών ασφαλείας:

Τα περιστατικά ασφαλείας πρέπει να αναφέρονται γρήγορα μέσα από τα κανάλια διαχείρισης. Οι υπάλληλοι και οι συνεργάτες πρέπει να καταγράφουν και να ενημερώνουν για οποιαδήποτε αδυναμία ασφαλείας παρατηρήσουν. Τα γεγονότα αυτά θα αξιολογούνται και θα αποφασίζεται ποια από αυτά θα θεωρηθούν περιστατικά ασφαλείας.

Διαχείριση περιστατικών ασφαλείας και βελτίωση:

Τα περιστατικά ασφαλείας θα αντιμετωπίζονται όπως προδιαγράφεται στις τεκμηριωμένες διαδικασίες. Η γνώση που αποκτήθηκε κατά την ανάλυση και την αντιμετώπιση του περιστατικού θα χρησιμοποιηθεί για τη βελτίωση του συστήματος και την αποφυγή παρόμοιων περιστατικών στο μέλλον.

13. Διαχείριση Επιχειρησιακής Συνέχειας

Ο οργανισμός πρέπει να αποφασίσει για τις απαιτήσεις ασφαλείας και τη συνέχεια του συστήματος διαχείρισης ασφάλειας σε αντίξοες συνθήκες. Ο οργανισμός πρέπει να ορίσει , τεκμηριώσει, συντάξει, υλοποιήσει και διατηρήσει τις διαδικασίες και τους ελέγχους που θα εξασφαλίσουν την συνέχεια της ασφάλειας πληροφοριών κατά τη διάρκεια μιας δυσμενούς κατάστασης.

14. Συμμόρφωση

Συμμόρφωση με νομικές απαιτήσεις:

Όλες οι νομοθετικές απαιτήσεις και η προσέγγιση του οργανισμού σε αυτές πρέπει να διατυπώνονται ρητώς και να κρατούνται ενημερωμένες. Κατάλληλες διαδικασίες πρέπει να υλοποιούνται για να διασφαλίζονται οι απαιτήσεις ασφαλείας σχετικά με την πνευματική ιδιοκτησία και τη χρήση των ιδιόκτητων προϊόντων λογισμικού. Οι εγγραφές πρέπει να προστατεύονται από απώλεια, καταστροφή, μη εξουσιοδοτημένη χρήση ή αποκάλυψη. Οι προσωπικές πληροφορίες πρέπει να διασφαλίζονται σύμφωνα με τη σχετική νομοθεσία.

Συμμόρφωση με πολιτικές ασφαλείας:

Η προσέγγιση του οργανισμού για τη διαχείριση της ασφάλειας πληροφορίας πρέπει να επιθεωρείται και να αναθεωρείται εάν κριθεί σκόπιμο. Οι αρμόδιοι

πρέπει να επιθεωρούν την συμμόρφωση με τις πολιτικές και τις απαιτήσεις ασφαλείας στην περιοχή των αρμοδιοτήτων τους.

Τεχνική συμμόρφωση:

Σε τακτά χρονικά διαστήματα πρέπει να ελέγχεται η τεχνική συμμόρφωση των συστημάτων με τις πολιτικές ασφαλείας.

3.2.4 ΠΙΣΤΟΠΟΙΗΣΗ ΜΕ ΤΟ ISO/IEC 27001

Η πιστοποίηση με το πρότυπο ISO/IEC 27001 περιλαμβάνει 3 στάδια:

- Αρχικά, αναγνωρίζεται η ύπαρξη και η ορθότητα κρίσιμων εγγράφων όπως η πολιτική ασφαλείας του οργανισμού, η δήλωση εφαρμογής των συγκεκριμένων σημείων ελέγχου (Statement of Applicability- SoA) και το Σχέδιο Αντιμετώπισης του κινδύνου (Risk Treatment Plan- RTP).
- Στο δεύτερο στάδιο γίνεται ο έλεγχος για την ύπαρξη και τήρηση των μέτρων ασφαλείας που έχουν περιγραφεί στα έγγραφα του πρώτου σταδίου.
- Στο τρίτο στάδιο πραγματοποιείται μια επανεκτίμηση για να επιβεβαιωθεί ότι ο οργανισμός μετά την πιστοποίηση παραμένει σύμφωνος με το πρότυπο. Γίνονται τακτικές αναθεωρήσεις και επανεκτιμήσεις για τη διατήρηση της ασφάλειας του οργανισμού και την συμφωνία του με το πρότυπο.

3.3 ΤΟ ΠΡΟΤΥΠΟ ISO/IEC 27002:2005

Το πρότυπο ISO/IEC 27002:2005 περιλαμβάνει τις βασικές αρχές του ISO/IEC 17799:2005. Το πλήρες όνομα του είναι “Information Technology -Security Techniques – Code of practice for information security controls.”. Πρόκειται για ένα εμπορικό πρότυπο που παρέχει αναλυτικές προδιαγραφές για την έναρξη, την υλοποίηση, τη διατήρηση και τη βελτίωση της διαχείρισης της ασφάλειας των πληροφοριών σε έναν οργανισμό. Αποτελεί έναν οδηγό για την αξιολόγηση του επιπέδου ασφαλείας και την βελτίωση του το οποίο απευθύνεται σε άτομα με υψηλή τεχνογνωσία.

Το πρότυπο περιγράφει μια σειρά από δεκατέσσερις διατάξεις ασφαλείας. Για κάθε διάταξη υπάρχει μια σειρά από υποκατηγορίες για τις οποίες ορίζονται οι στόχοι και οι οδηγίες εφαρμογής τους. Το πρότυπο ορίζει μια διαδικασία τεσσάρων σταδίων την οποία πρέπει να ακολουθεί η εκτίμηση του κινδύνου. Αυτά τα στάδια είναι :

1. Προσδιορισμός, ποσοτικοποίηση του κινδύνου και καθορισμός των προτεραιοτήτων σύμφωνα με τους στόχους του οργανισμού.
2. Ανάλυση του κινδύνου με την εκτίμηση του μεγέθους των κινδύνων.
3. Αξιολόγηση του κινδύνου. Προσδιορισμός της σημαντικότητας των κινδύνων συγκρίνοντας τα εκτιμώμενα επίπεδα κινδύνου με τα καθορισμένα αποδεκτά.
4. Αντιμετώπιση κινδύνου. Ορίζονται τα κριτήρια αποδοχής του κινδύνου και ποιοι κίνδυνοι θα γίνουν αποδεκτοί. Για τους μη αποδεκτούς κινδύνους λαμβάνεται η απόφαση για τρόπο αντιμετώπισης τους.

Καλύπτει όλα τα είδη και μεγέθη οργανισμών και υλοποιείται από πληθώρα εργαλείων. Παρ' όλ' αυτά, το πρότυπο μειονεκτεί σε κάποια σημεία. Επικεντρώνεται στους ελέγχους και την αντιμετώπιση του κινδύνου δίνοντας λιγότερη σημασία στην αναγνώριση και την ανάλυση του κινδύνου. Γι΄αυτό το λόγο καλό είναι να συνδυάζεται με μια μέθοδο αποτίμησης της επικινδυνότητας.

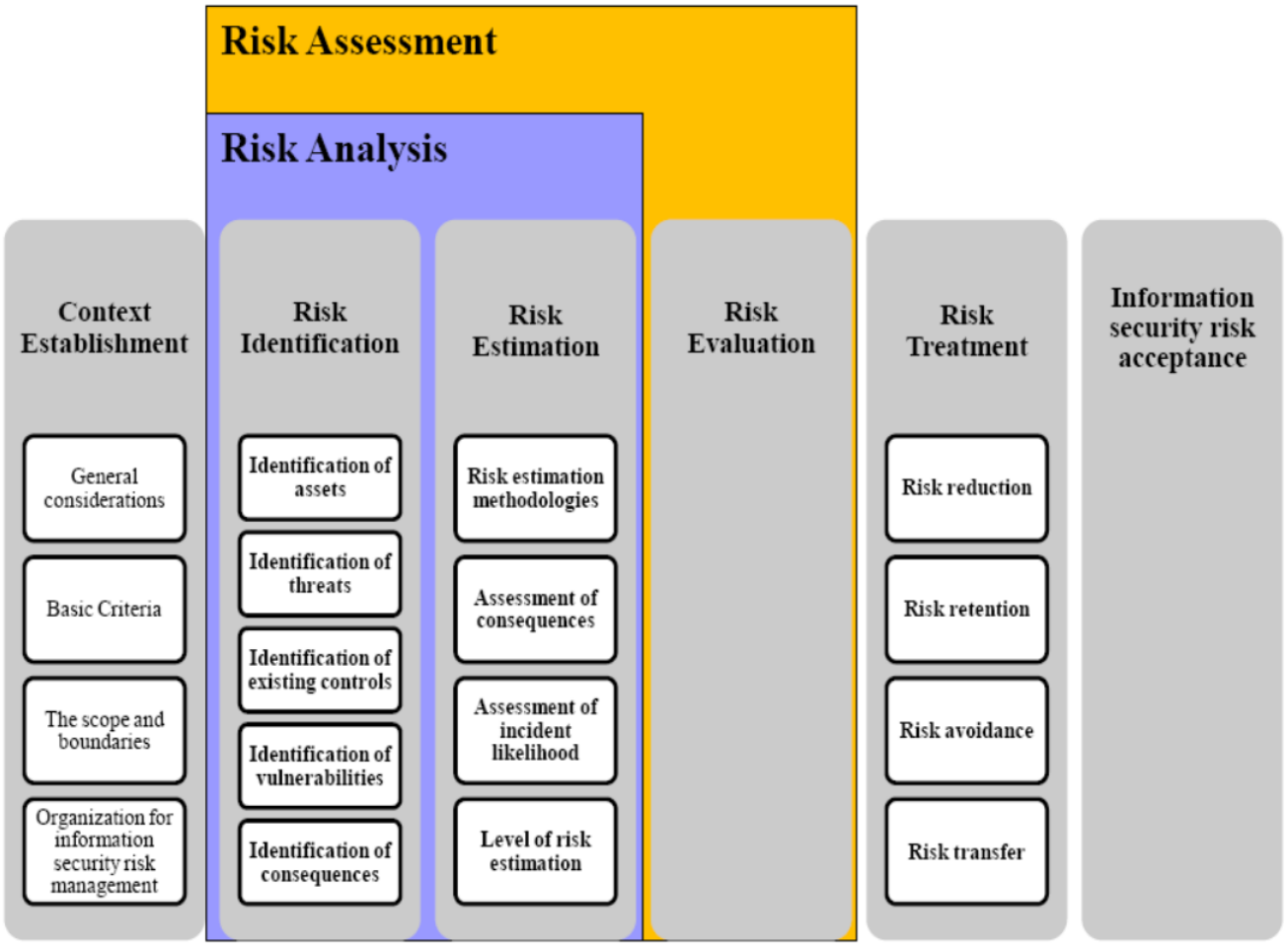
3.4 ΤΟ ΠΡΟΤΥΠΟ ISO/IEC 27005:2008

Το πλήρες όνομα του είναι “ Information technology — Security techniques — Information security risk management”. Το πρότυπο υποστηρίζει τις γενικές έννοιες που ορίζει το ISO 27001 και τις κύριες διαδικασίες και τους κανόνες του ISO 27002. Ορίζει τις αρχές , τους κανόνες και τις δραστηριότητες για την διαχείριση της επικινδυνότητας. Δεν αποτελεί μια ολοκληρωμένη μέθοδο ανάλυσης και διαχείρισης της επικινδυνότητας καθώς περιγράφει την αποτίμηση της επικινδυνότητας σε αφαιρετικό επίπεδο και εστιάζει στη διαχείριση των κινδύνων.

Η διαδικασία διαχείριση κινδύνου χωρίζεται στα παρακάτω στάδια:

1. Ανάλυση επικινδυνότητας (Risk analysis)
   Η ανάλυση επικινδυνότητας περιλαμβάνει τα παρακάτω δύο στάδια:
   - Αναγνώριση κινδύνου (Risk identification). Αναγνωρίζονται τα περιουσιακά στοιχεία, οι απειλές, οι αδυναμίες, οι υφιστάμενοι έλεγχοι και οι επιπτώσεις.
   - Υπολογισμός κινδύνου (Risk estimation). Υπολογίζεται το επίπεδο κινδύνου με ποιοτικό ή ποσοτικό τρόπο λαμβάνοντας υπόψιν τα στοιχεία από το στάδιο της αναγνώρισης κινδύνου.
2. Εκτίμηση επικινδυνότητας (Risk evaluation). Το επίπεδο κινδύνου που υπολογίστηκε συγκρίνεται με το αποδεκτό επίπεδο κινδύνου. Οι κίνδυνοι ιεραρχούνται με βάση την προτεραιότητα τους και παρουσιάζονται οι διαθέσιμες επιλογές για την αντιμετώπιση της επικινδυνότητας. Αξιολογούνται οι επιπτώσεις και η πιθανότητα εμφάνισης ενός περιστατικού ασφαλείας με την χρήση των οποίων υπολογίζεται το επίπεδο επικινδυνότητας.
3. Αντιμετώπιση επικινδυνότητας (Risk treatment). Λαμβάνονται μέτρα για την αντιμετώπιση της επικινδυνότητας και καταρτίζεται ένα σχέδιο αντιμετώπισης κινδύνου. Τα μέτρα αυτά αφορούν τη μείωση του κινδύνου (risk reduction),τη διατήρηση του κινδύνου (risk retention), την αποφυγή του κινδύνου (risk avoidance) και τη μεταφορά κινδύνου (risk transfer).

Στην παρακάτω εικόνα φαίνεται η διαδικασία διαχείρισης επικινδυνότητας σύμφωνα με το ISO 27005.



ΕΙΚΟΝΑ 6: Στάδια διαχείρισης κινδύνου σύμφωνα με ISO 27005

Risk assessment 2013- Δούσκας Θεόδωρος

Χρειάζεται να χρησιμοποιηθεί μαζί με μια εξωτερική μέθοδο αποτίμησης της επικινδυνότητας καθώς δεν εστιάζει στην ανάλυση της επικινδυνότητας. Το πρότυπο προτείνει τη χρήση ποιοτικών και ποσοτικών μεθόδων υπολογισμού του επιπέδου του κινδύνου χωρίς όμως να προσφέρει κάποια τεχνική για το σκοπό αυτό. Με τους κανόνες και τις οδηγίες του προτύπου 27005 συμμορφώνονται μεθοδολογίες όπως η MAGERI, MEHARI και EBIOS που θα αναλυθούν στο 4^{ο} κεφάλαιο.

4. ΜΕΘΟΔΟΛΟΓΙΕΣ ΑΝΑΛΥΣΗΣ ΚΑΙ ΔΙΑΧΕΙΡΙΣΗΣ ΕΠΙΚΙΝΔΥΝΟΤΗΤΑΣ ΣΥΜΒΑΤΕΣ ΜΕ ΤΙΣ ΑΠΑΙΤΗΣΕΙΣ ΤΟΥ ISO 27001

4.1 ΜΕΘΟΔΟΛΟΓΙΕΣ ΑΝΑΛΥΣΗΣ ΕΠΙΚΙΝΔΥΝΟΤΗΤΑΣ

4.1.1 CRAMM

Η μέθοδος CRAMM (CCTA Risk Analysis and Management Methodology) αποτελεί μια μέθοδο ποιοτικής ανάλυσης κινδύνων που αναπτύχθηκε το 1987 από την Κεντρική Υπηρεσία Υπολογιστών και Τηλεπικοινωνιών (Central Computer and Telecommunications Agency – CCTA) του Ηνωμένου Βασιλείου. Αναπτύχθηκε για να εφαρμοστεί σε οργανισμούς του δημόσιου τομέα του Ηνωμένου Βασιλείου. Η μέθοδος CRAMM έχει λάβει μεγάλη αναγνώριση και έχει χρησιμοποιηθεί σε εκατοντάδες μελέτες διεθνώς. Αποτελεί πρότυπη μέθοδο και κυρίως χρησιμοποιείται σε μεγάλης κλίμακας οργανισμούς και επιχειρήσεις κοινής ωφέλειας. Καλύπτει όλες τις συνιστώσες ασφαλείας όπως του τεχνικού παράγοντα, του προσωπικού, της φυσικής ασφάλειας κλπ. και συνοδεύεται από ένα αυτοματοποιημένο εργαλείο λογισμικού που υποστηρίζει όλα τα στάδια εφαρμογής της. Η μέθοδος CRAMM είναι η κύρια μέθοδος πιστοποίησης για τα πρότυπα ISO 27000, ενώ επικεντρώνεται στο ISO/IEC 27001:2005. Παράλληλα, καλύπτει τις απαιτήσεις της ευρωπαϊκής και της ελληνικής νομοθεσίας ως προς τη λήψη μέτρων προστασίας για τα συστήματα που επεξεργάζονται προσωπικά δεδομένα.

Η μέτρηση της επικινδυνότητας σε κλίμακα 1:7 γίνεται:

- Με αποτίμηση των περιουσιακών στοιχείων με βάση τις επιπτώσεις στον οργανισμό (κλίμακα 1:10).
- Με αξιολόγηση απειλών (κλίμακα 1:5)
- Με αξιολόγηση ευπαθειών (κλίμακα 1:3)

Η μέθοδος CRAMM αποτελείται από τα εξής στάδια:

1. Προσδιορισμός και αξιολόγηση αγαθών (identification and valuation of assets).
2. Ανάλυση επικινδυνότητας (risk analysis).
3. Διαχείριση επικινδυνότητας (risk management).

1. Προσδιορισμός και αξιολόγηση αγαθών

Το πρώτο στάδιο αναφέρεται στον προσδιορισμό και την αξιολόγηση των στοιχείων των πληροφοριακών συστημάτων που χρειάζονται προστασία. Περιλαμβάνει τα εξής βήματα:

I. Δημιουργία του μοντέλου του Πληροφοριακού συστήματος

Στο πρώτο βήμα προσδιορίζονται τα δεδομένα που επεξεργάζεται το πληροφοριακό σύστημα και ομαδοποιούνται. Προσδιορίζονται τα υλικά στοιχεία, οι χώροι και οι εγκαταστάσεις, το λογισμικό και το υλικό των πληροφοριακών συστημάτων. Δημιουργείται το μοντέλο που συσχετίζει τα παραπάνω, εισάγεται στο εργαλείο λογισμικού της CRAMM και ελέγχεται η συνέπεια του.

II. Αποτίμηση των στοιχείων του πληροφοριακού συστήματος

Κατά το δεύτερο βήμα γίνεται αποτίμηση των στοιχείων του πληροφοριακού συστήματος προκειμένου να προσδιοριστεί η σπουδαιότητα τους. Η αξία κάθε ομάδας στοιχείων αποτιμάται με βάση την επίπτωση (impact) που θα είχε η απώλεια της. Το μέγεθος της επίπτωσης υπολογίζεται αριθμητικά με κλίμακα 1 – 10. Ενδεικτικά παρατίθεται η κλίμακα επιπτώσεων:

Βαθμός	**Οικονομική Επίπτωση**
1	<= 1.000€
2	<= 10.000€
3	<= 30.000€
4	<= 100.000€
5	<= 300.000€
6	<= 1.000.000€
7	<= 3.000.000€
8	<= 10.000.000€
9	<= 30.000.000€
10	<= 100.000.000€

Κλίμακα Επιπτώσεων

Οι εξεταζόμενες περιπτώσεις είναι:

- Μη διαθεσιμότητα
- Καταστροφή
- Αποκάλυψη
- Μη εξουσιοδοτημένη μεταβολή
- Ηθελημένη μεταβολή
- Λάθη μετάδοσης δεδομένων

Για κάθε περίπτωση μελετάται το χειρότερο σενάριο και υπολογίζεται το μέγεθος της επίπτωσης. Η μέθοδος CRAMM παρέχει οδηγίες για τον υπολογισμό των επιπτώσεων των παρακάτω κατηγοριών:

- Σωματική ακεραιότητα και ζωή φυσικών προσώπων
- Δυσαρέσκεια από έκθεση προσωπικών πληροφοριών
- Νομικές επιπτώσεις
- Παρεμπόδιση δικαιοσύνης
- Οικονομικές απώλειες
- Διατάραξη δημόσιας τάξης
- Μη εφαρμογή πολιτικής οργανισμού
- Απώλεια εμπιστοσύνης του κοινού

Η αποτίμηση των πληροφοριακών συστημάτων στηρίζεται σε συνεντεύξεις χρηστών που εμπλέκονται με το πληροφοριακό σύστημα. Η μέθοδος CRAMM μέσω του αυτοματοποιημένου εργαλείου υπολογίζει την αξία των αγαθών αξιοποιώντας το μοντέλο του συστήματος.

III. Επιβεβαίωση και επικύρωση αποτίμησης

Στο τρίτο βήμα γίνεται η επιβεβαίωση και επικύρωση της αποτίμησης. Παρουσιάζονται στη διοίκηση τα αποτελέσματα του πρώτου σταδίου με τη μορφή αναφοράς και πραγματοποιείται η σύσκεψη επικύρωσης των αποτελεσμάτων.

2. Ανάλυση επικινδυνότητας (risk analysis)

Στο πρώτο στάδιο υπολογίστηκε η αξία των στοιχείων του πληροφοριακού συστήματος. Αυτός είναι ο ένας παράγοντας που συνθέτει την επικινδυνότητα. Οι άλλοι δύο είναι το επίπεδο απειλών και το επίπεδο των αδυναμιών του συστήματος οι οποίοι και υπολογίζονται στο δεύτερο στάδιο. Τα βήματα που ακολουθούνται είναι τα εξής:

I. Προσδιορισμός των απειλών που αφορούν το κάθε αγαθό

Με τη μέθοδο CRAMM συνδέεται κάθε αγαθό με συγκεκριμένες κατηγορίες απειλών. Η CRAMM παρέχει μία ενδεικτική λίστα απειλών καθώς και συστάσεις για το ποιες κατηγορίες στοιχείων ενός πληροφοριακού συστήματος μπορούν να αντιμετωπίσουν αυτή την απειλή. Το εργαλείο ζητά να συσχετιστεί κάθε αγαθό με μια κατηγορία απειλών.

II. Εκτίμηση απειλών και αδυναμιών

Για κάθε συνδυασμό αγαθού – απειλής εκτιμάται το μέγεθος της απειλής και η σοβαρότητα των αδυναμιών που θα μπορούσαν να οδηγήσουν στην πραγματοποίηση της απειλής. Στο βήμα αυτό συμπληρώνονται ερωτηματολόγια εκτίμησης απειλών και αδυναμιών. Η εκτίμηση των απειλών ορίζεται σε κλίμακα 1-5 (πολύ χαμηλό, χαμηλό, μέτριο, υψηλό, πολύ υψηλό) ενώ η εκτίμηση των αδυναμιών σε κλίμακα από 1-3 (χαμηλό, μέτριο, υψηλό) . Η αποτίμηση απειλών και αδυναμιών γίνεται αυτόματα από το εργαλείο λογισμικού και οι τιμές επιβεβαιώνονται ή/και διορθώνονται από τους αναλυτές.

ΒΑΘΜΟΣ ΑΠΕΙΛΗΣ	ΕΠΙΠΕΔΟ	ΠΕΡΙΓΡΑΦΗ
1	ΠΟΛΥ ΧΑΜΗΛΟ	Αναμένεται να συμβούν το πολύ μέχρι μια φορά κάθε δέκα χρόνια
2	ΧΑΜΗΛΟ	Αναμένεται να συμβούν κατά μέσο όρο μία φορά τα 3 χρόνια
3	ΜΕΤΡΙΟ	Αναμένεται να συμβούν κατά μέσο όρο μια φορά το χρόνο
4	ΥΨΗΛΟ	Αναμένεται να συμβούν κατά μέσο όρο μια φορά κάθε 4 μήνες
5	ΠΟΛΥ ΥΨΗΛΟ	Αναμένεται να συμβούν κατά μέσο όρο μία φορά το μήνα

Επίπεδο Απειλής (1-5)

ΒΑΘΜΟΣ ΑΔΥΝΑΜΙΑΣ	ΕΠΙΠΕΔΟ	ΠΕΡΙΓΡΑΦΗ
1	ΧΑΜΗΛΟ	Σε περίπτωση που συνέβαινε μια απειλή θα υπήρχε το πολύ 33% πιθανότητα να εκδηλωθεί το χειρότερο σενάριο συνεπειών με βάση την εκτίμηση συνέπειας που έχει πραγματοποιηθεί
2	ΜΕΤΡΙΟ	Σε περίπτωση που συνέβαινε μια απειλή θα υπήρχε από 33% μέχρι 66% πιθανότητα να εκδηλωθεί το χειρότερο σενάριο συνεπειών με βάση την εκτίμηση συνέπειας που έχει πραγματοποιηθεί
3	ΥΨΗΛΟ	Σε περίπτωση που συνέβαινε μια απειλή θα υπήρχε 66% πιθανότητα να εκδηλωθεί το χειρότερο σενάριο συνεπειών με βάση την εκτίμηση συνέπειας που έχει πραγματοποιηθεί

Επίπεδο Αδυναμίας (1-3)

III. Υπολογισμός της επικινδυνότητας για κάθε συνδυασμό αγαθό – απειλή – αδυναμία

Στο βήμα αυτό υπολογίζεται ο βαθμός επικινδυνότητας για κάθε συνδυασμό αγαθού-απειλής-αδυναμίας. Για κάθε συνδυασμό αγαθού- απειλής – αδυναμίας υπολογίζεται αυτόματα από το εργαλείο λογισμικού ο βαθμός επικινδυνότητας.
Ο υπολογισμός ορίζεται σε κλίμακα 1-7 και ο αναλυτής μπορεί να παρέμβει και να διορθώσει τις τιμές.

IV. Επιβεβαίωση και επικύρωση του βαθμού επικινδυνότητας
Στο στάδιο αυτό η ομάδα μελέτης καλείται να επιβεβαιώσει το βαθμό επικινδυνότητας. Γίνεται η παρουσίαση σε μορφή αναφοράς του βαθμού επικινδυνότητας. Σε κοινή σύσκεψη εργασίας της Διοίκησης και των αναλυτών επιβεβαιώνονται οι τιμές της επικινδυνότητας και αν κριθεί αναγκαίο οι αναλυτές μπορούν να υπολογίσουν εκ νέου την επικινδυνότητα.

3. Διαχείριση επικινδυνότητας (risk management)

Στο τρίτο στάδιο με βάση τα αποτελέσματα του δεύτερο σταδίου η μέθοδος CRAMM παράγει ένα σχέδιο ασφαλείας για τα πληροφοριακά συστήματα. Συγκεκριμένα τα βήματα που ακολουθούνται είναι:

I. Προσδιορισμός της λίστας των προτεινόμενων αντίμετρων

Με βάση τα αποτελέσματα της ανάλυσης επικινδυνότητας το εργαλείο λογισμικού παράγει αυτόματα μια λίστα προτεινόμενων αντίμετρων. Το λογισμικό της CRAMM διαθέτει μια βάση με τεχνικά, διοικητικά και οργανωτικά αντίμετρα. Τα αντίμετρα κατατάσσονται σε ομάδες ανάλογα με τα αγαθά που καλούνται να προστατέψουν και το είδος των απειλών που καλούνται να αντιμετωπίσουν. Από τα προτεινόμενα αντίμετρα πρέπει να γίνει

η επιλογή των μέτρων προς υλοποίηση. Στην επιλογή αυτή κύριο ρόλο έχουν οι αναλυτές. Η επιλογή βασίζεται στα παρακάτω κριτήρια:

- Επίδραση αντίμετρων στη λειτουργία του οργανισμού
- Διαθέσιμος προϋπολογισμός
- Κόστος εφαρμογής και διαχείρισης αντίμετρων (χρηματικό και σε ανθρώπινους πόρους)
- Άποψη της Διοίκησης και στόχοι του οργανισμού
- Ενδείξεις για μελλοντική ένταση ή ύφεση των απειλών
- Αποτελεσματικότητα αντιμέτρων

Οι κατηγορίες των αντίμετρων σε φθίνουσα σειρά αποτελεσματικότητας είναι:

- Μείωση των απειλών
- Μείωση των αδυναμιών
- Μείωση της επίπτωσης
- Ανίχνευση της παραβίασης
- Ανάκαμψη

Το λογισμικό της CRAMM περιέχει μία βάση με περισσότερα από 2.500 αντίμετρα. Το CRAMM εργαλείο επιλέγει αυτόματα τα αντίμετρα σύμφωνα με τα αποτελέσματα της ανάλυσης επικινδυνότητας. Η κατάσταση για ένα αντίμετρο μπορεί να είναι:

- Ήδη εγκατεστημένο (installed)
- Επιλεγμένο για εγκατάσταση (to be installed)
- Υπό υλοποίηση (implementing recommendation)
- Έχει υλοποιηθεί (implemented recommendation)
- Έχει ήδη καλυφθεί από άλλο αντίμετρο (already covered)
- Αναλαμβάνεται η επικινδυνότητα και δεν υλοποιείται (accept level of risk)
- Υπό συζήτηση (under discussion)
- Μη εφαρμόσιμο (not applicable)

II. Κατάρτιση σχεδίου / πλάνου ασφαλείας

Στο τελευταίο αυτό βήμα συντάσσεται το σχέδιο ασφαλείας το οποίο περιλαμβάνει:

- Το σχέδιο πολιτικής ασφαλείας (security policy)
- Τον κατάλογο των αντιμέτρων (countermeasures)
- Τη στρατηγική εφαρμογής (application strategy)

Το σχέδιο ασφαλείας κατατίθεται στη Διοίκηση και επικυρώνεται σε κοινή σύσκεψη.

Προϋποθέσεις για την επιτυχία της μεθόδου CRAMM είναι η συμμετοχή και η υποστήριξη της ανώτερης Διοίκησης, η συμμετοχή των στελεχών του οργανισμού, η σωστή επιλογή των καταλληλότερων στελεχών του οργανισμού για τις συνεντεύξεις και η σαφής οριοθέτηση της μελέτης.

Παρακάτω παρατίθενται τα πλεονεκτήματα και τα μειονεκτήματα της μεθόδου CRAMM.

ΠΛΕΟΝΕΚΤΗΜΑΤΑ ΤΗΣ ΜΕΘΟΔΟΥ CRAMM

1. Καλύπτει όλες τις φάσεις της ανάλυσης και διαχείρισης της επικινδυνότητας.
2. Καλύπτει όλες τις συνιστώσες ασφαλείας όπως τεχνικά θέματα, φυσική ασφάλεια, θέματα προσωπικού κ.α.
3. Έχει δοκιμαστεί σε διεθνές επίπεδο.
4. Συνοδεύεται από ειδικό εργαλείο λογισμικού.
5. Παρέχει πληθώρα αντιμέτρων.

ΜΕΙΟΝΕΚΤΗΜΑΤΑ ΤΗΣ ΜΕΘΟΔΟΥ CRAMM

1. Απαιτείται μεγάλη ανθρώπινη προσπάθεια και έχει υψηλό κόστος εφαρμογής.
2. Βασίζεται στη συνεργασία με τους χρήστες και τη Διοίκηση.
3. Εστιάζει μόνο στα δεδομένα και λαμβάνει υπόψιν τους ανθρώπους μόνο ως πηγές απειλών.
4. Γίνεται μια απλούστευση του πληροφοριακού συστήματος που παρουσιάζεται με ένα απλοϊκό μοντέλο.
5. Απαιτεί αρκετές φορές την επέμβαση του αναλυτή και την προσαρμογή των αποτελεσμάτων των αυτόματων υπολογισμών.
6. Το τελικό αποτέλεσμα στηρίζεται σε μεγάλο βαθμό σε υποκειμενικές εκτιμήσεις,
7. Τα αντίμετρα που ορίζονται είναι αρκετά γενικά. Απαιτείται η προσαρμογή τους στα ιδιαίτερα χαρακτηριστικά και τη φιλοσοφία του πληροφοριακού συστήματος που εξετάζεται.

4.1.2 ΜΕΘΟΔΟΛΟΓΙΑ MAGERIT

Η Μεθοδολογία MAGERIT είναι μια μεθοδολογία Ανάλυσης και Διαχείρισης Κινδύνου που αναπτύχθηκε το 1997 από το Ανώτατο Ισπανικό Συμβούλιο για την Ηλεκτρονική διακυβέρνηση (Consejo Superior de Administración Electrónica). Η MAGERIT έχει τους εξής στόχους [J.Kouns, 2010]:

- Να αναδείξει την ύπαρξη απειλών, κινδύνων και την ανάγκη έγκαιρης αντιμετώπισής τους.
- Να προσφέρει μια συστηματική μέθοδο ανάλυσης των κινδύνων.
- Να υποβοηθήσει στην περιγραφή και τον σχεδιασμό των μέτρων ελέγχου της επικινδυνότητας.
- Να προετοιμάσει τον Οργανισμό για τις διαδικασίες της Αξιολόγησης (valuating), του Ελέγχου(auditing) και της Πιστοποίησης(certifying).
- Να επιτύχει ομοιομορφία στις αναφορές που εμπεριέχουν τα ευρήματα και τα συμπεράσματα της ανάλυσης, προτείνοντας μια ενιαία δομή.

Η μέθοδος MAGERIT χρησιμοποιεί ένα εργαλείο λογισμικού που ονομάζεται EAR/Pilar. Με το εργαλείο αυτό παρακολουθείται η ορθή εφαρμογή της μεθόδου και συλλέγονται όλα τα στοιχεία κατά την εφαρμογής της μεθόδου. Το εργαλείο διατέθηκε στην αγορά το 2004 και υποστηρίζεται από τον A.L.H.J.Mañas. Είναι συμβατή με τα θεμελιώδη πρότυπα ασφάλειας της σειράς ISO/IEC 27000.

Η μέθοδος MAGERIT περιλαμβάνει τα παρακάτω τρία στάδια:

1. Προετοιμασία και προγραμματισμός έργου (Preparation & Planning of implementation)
2. Ανάλυση επικινδυνότητας (Risk analysis)
3. Διαχείριση επικινδυνότητας (Risk management)

1. **Προετοιμασία και προγραμματισμός έργου**

   Το πρώτο στάδιο αποτελείται από την προετοιμασία και τον προγραμματισμό του έργου και περιλαμβάνει τα εξής βήματα:

   I. Μελέτη σκοπιμότητας

   Στο βήμα αυτό διερευνώνται τα προβλήματα που αντιμετωπίζει ο οργανισμός και τα πιθανά οφέλη που θα επιφέρει η ανάλυση και διαχείριση της επικινδυνότητας. Τα παραπάνω περιγράφονται σε μια έκθεση που παρουσιάζεται στη Διοίκηση του οργανισμού η οποία εγκρίνει το έργο ή καθορίζει νέους στόχους.

   II. Καθορισμός πλαισίου αναφοράς

   Στο βήμα αυτό καθορίζεται το πλαίσιο αναφοράς του έργου. Γίνεται περιγραφή των στόχων του έργου, των πιθανών δυσκολιών, των περιορισμών που προκύπτουν αλλά και προσδιορισμός του κόστους για την υλοποίηση του έργου σε ανθρώπινους, χρηματικούς, υλικούς και χρονικούς πόρους.

   III. Προγραμματισμός έργου

   Στο τρίτο βήμα γίνεται ο προγραμματισμός του έργου. Προσδιορίζονται οι συνεντεύξεις που θα πραγματοποιηθούν για να δοθεί σαφή εικόνα του τρόπου λειτουργίας του οργανισμού. Καθορίζεται πως θα κατηγοριοποιηθεί αυτή η συλλεγόμενη πληροφορία. Προσδιορίζεται το ανθρώπινο δυναμικό που θα υλοποιήσει και διαχειριστεί το έργο και θέτονται τα καθήκοντα του. Το βήμα αυτό ολοκληρώνεται με την κατάρτιση του χρονοδιαγράμματος του έργου.

   IV. Έναρξη έργου

   Στο τελευταίο βήμα του πρώτου σταδίου ακολουθεί η έναρξη του έργου.

   Συντάσσονται τα ερωτηματολόγια για τη συλλογή πληροφοριών, προσδιορίζονται τα αγαθά που χρήζουν προστασίας και καθορίζονται οι απαραίτητοι πόροι για το έργο.

2. Ανάλυση επικινδυνότητας (Risk analysis)

I. Αναγνώριση και αποτίμηση αγαθών

Στο βήμα αυτό αναγνωρίζονται τα στοιχεία του πληροφοριακού συστήματος που έχουν αξία δηλαδή τα αγαθά. Τα αγαθά κατηγοριοποιούνται στις παρακάτω εννέα κατηγορίες (Magerit v2):

ΚΑΤΗΓΟΡΙΕΣ ΑΓΑΘΩΝ		
Υπηρεσίες (Services)	Εξοπλισμός (Computer equipment / Hardware)	Βοηθητικός Εξοπλισμός (Auxiliary equipment)
Δεδομένα/Πληροφορίες (Data/Information)	Δίκτυα Επικοινωνιών (Communication networks)	Εγκαταστάσεις Εξοπλισμού (Installation)
Εφαρμογές (Application/Software)	Φυσικά Μέσα Αποθήκευσης (Media)	Προσωπικό (Personel)

Μετά την κατηγοριοποίηση των αγαθών ακολουθεί η αποτίμηση τους βάσει του κόστους που θα επιφέρει στον οργανισμό η πιθανή καταστροφή κάθε αγαθού.

II. Χαρακτηρισμός και εκτίμηση απειλών

Στο βήμα αυτό προσδιορίζονται οι απειλές στις οποίες εκτίθενται τα αγαθά. Δεν επηρεάζουν όλες οι απειλές όλα τα αγαθά αλλά υπάρχει συσχέτιση της κατηγορίας του περιουσιακού στοιχείου και των απειλών αυτού. Οι απειλές χωρίζονται στις παρακάτω τέσσερις κατηγορίες:

ΚΑΤΗΓΟΡΙΕΣ ΑΠΕΙΛΩΝ
Φυσικές καταστροφές
Καταστροφές βιομηχανικής προέλευσης
Λάθη ή ακούσιες αποτυχίες
Ηθελημένες επιθέσεις

Ακόμα γίνεται υπολογισμός της συχνότητας εμφάνισης κάθε απειλής και εκτιμάται η υποτίμηση/υποβάθμιση της αξίας ενός αγαθού λόγω της απειλής. Η συχνότητα εμφάνισης της απειλής είναι πολύ σημαντικός παράγοντας καθώς μια απειλή μπορεί να έχει σοβαρές συνέπειες και να είναι αδύνατο να συμβεί ενώ μια άλλη απειλή μπορεί να έχει μικρότερες συνέπειες αλλά να συμβαίνει συχνά.

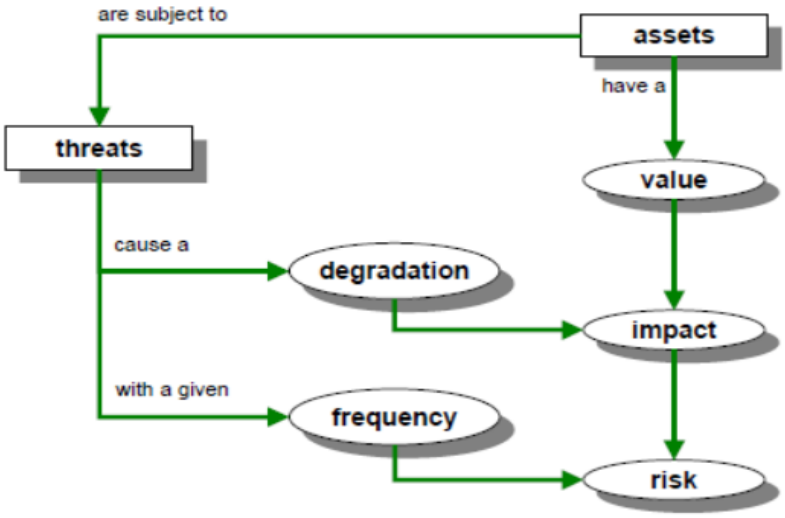
III. Χαρακτηρισμός αντιμέτρων

Προσδιορίζονται τα αντίμετρα και εκτιμάται το πόσο αποτελεσματικά είναι. Τα αντίμετρα είναι διαδικασίες ή μηχανισμοί που μειώνουν τον κίνδυνο των απειλών. Αντίμετρα μπορούν να αποτελέσουν διάφορα τεχνικά μέσα, προγράμματα, εξοπλισμός, η φυσική ασφάλεια κ.α.

IV. Εκτίμηση επικινδυνότητας

Εκτιμάται το αντίκτυπο δηλαδή η ζημία που προκλήθηκε σε κάποιο αγαθό από την εμφάνιση μιας απειλής. Καθώς έχει προσδιοριστεί ήδη η αξία των αγαθών και η υποβάθμιση λόγω των απειλών είναι εύκολος ο υπολογισμός της επίπτωσης. Τέλος, υπολογίζεται ο κίνδυνος ως η σταθμισμένη επίπτωση στο ρυθμό εμφάνισης της απειλής. Με τον κίνδυνο εκτιμάται η πιθανή βλάβη στο σύστημα και υπολογίζεται λαμβάνοντας υπόψη το αντίκτυπο και τη συχνότητα εμφάνισης ως εξής:

$$\boldsymbol{Κίνδυνος = Αντίκτυπο\ x\ Συχνότητα}$$



ΕΙΚΟΝΑ 7: Εκτίμηση κινδύνου με τη μέθοδο MAGERIT

Πηγή: BIBLIOTECA_PUBLICACIONES_MAGERIT_VOL_I_INGLES

3. Διαχείριση επικινδυνότητας (Risk management)

Το τρίτο και τελευταίο στάδιο χωρίζεται σε τρία επιμέρους βήματα:

I. Λήψη αποφάσεων

Στο βήμα αυτό ερμηνεύονται οι τιμές της επικινδυνότητας. Η επικινδυνότητα διακρίνεται σε μια κλίμακα (κρίσιμη – σοβαρή – αξιόλογη - αποδεκτή) και ταξινομούνται οι επιπτώσεις σε μορφή αναφοράς. Η Διοίκηση με βάση τα παραπάνω λαμβάνει αποφάσεις προκειμένου να αντιμετωπιστούν οι απειλές του συστήματος και να περιοριστούν οι επιπτώσεις του.

II. Προετοιμασία σχεδίου ασφαλείας

Στο βήμα αυτό γίνεται η δημιουργία του σχεδίου ασφάλειας του οργανισμού. Μεγαλύτερο ρόλο στην κατάρτιση του πλάνου ασφαλείας παίζουν τα σενάρια των οποίων η επικινδυνότητα είναι κρίσιμη ή σοβαρή. Είναι αναγκαίο να ληφθούν κάποια μέτρα για τη μείωση της επικινδυνότητας είτε με τη μείωση της υποβάθμισης του αγαθού είτε με τη μείωση της συχνότητας εμφάνισης της απειλής. Το πλάνο ασφαλείας θα περιλαμβάνει την εκτίμηση των πόρων,

το πλάνο λειτουργίας, το πλάνο συντήρησης, το πλάνο εκπαίδευσης και το πλάνο ελέγχου της αποτελεσματικότητας. Με τη δημιουργία του σχεδίου ασφαλείας και την εφαρμογή του ο οργανισμός θα μειώσει την επικινδυνότητα σε αποδεκτά επίπεδα και θα μπορεί να αντιμετωπίσει έκτακτες καταστάσεις. Το τελικό σχέδιο ασφαλείας θα περιλαμβάνει όλα τα επιμέρους σχέδια που δημιουργήθηκαν.

III. Υλοποίηση σχεδίου ασφαλείας

Στο τελευταίο αυτό βήμα πραγματοποιούνται όλες οι ενέργειες για την υλοποίηση των επιμέρους σχεδίων ασφαλείας και κατ΄επέκταση του συνολικού σχεδίου ασφαλείας για τον οργανισμό. Υλοποιούνται τα προκαθορισμένα αντίμετρα και ελέγχεται η αποτελεσματικότητα τους.

ΠΛΕΟΝΕΚΤΗΜΑΤΑ ΤΗΣ ΜΕΘΟΔΟΥ MAGERIT

1. Παρουσιάζει τη διαδικασία αξιολόγησης των κινδύνων και δίνει τη δυνατότητα ποιοτικής και ποσοτικής ανάλυσης.
2. Η μεθοδολογία αυτή βρίσκει εφαρμογή σε συστήματα πληροφορικής, τηλεματικής των μέσων ενημέρωσης και γενικότερα στην χρήση ηλεκτρονικών που παρουσιάζουν πολλούς κινδύνους.
3. Είναι συμβατό με τα ακόλουθα πρότυπα: ISO/IEC 13335:2004, ISO/IEC 17799:2005, ISO/IEC 15408:2005, ISO/IEC 27001:2005
4. Υπάρχει εξειδικευμένο εργαλείο συμβατό με τη μέθοδο
5. Μπορεί να εφαρμοστεί ξεχωριστά ως μέθοδος Αποτίμησης επικινδυνότητας αλλά μπορεί και να χρησιμοποιηθεί για να εφαρμοστεί ένα ολοκληρωμένο Σύστημα Διαχείρισης Ασφάλειας Πληροφοριών.
6. Παρέχει τη δυνατότητα ποσοτικοποίησης υπηρεσιών και πληροφοριών ορίζοντας τους συγκεκριμένες τιμές.

ΜΕΙΟΝΕΚΤΗΜΑΤΑ ΤΗΣ ΜΕΘΟΔΟΥ MAGERIT

1. Περιορισμένος αριθμός χρηστών ανά άδεια

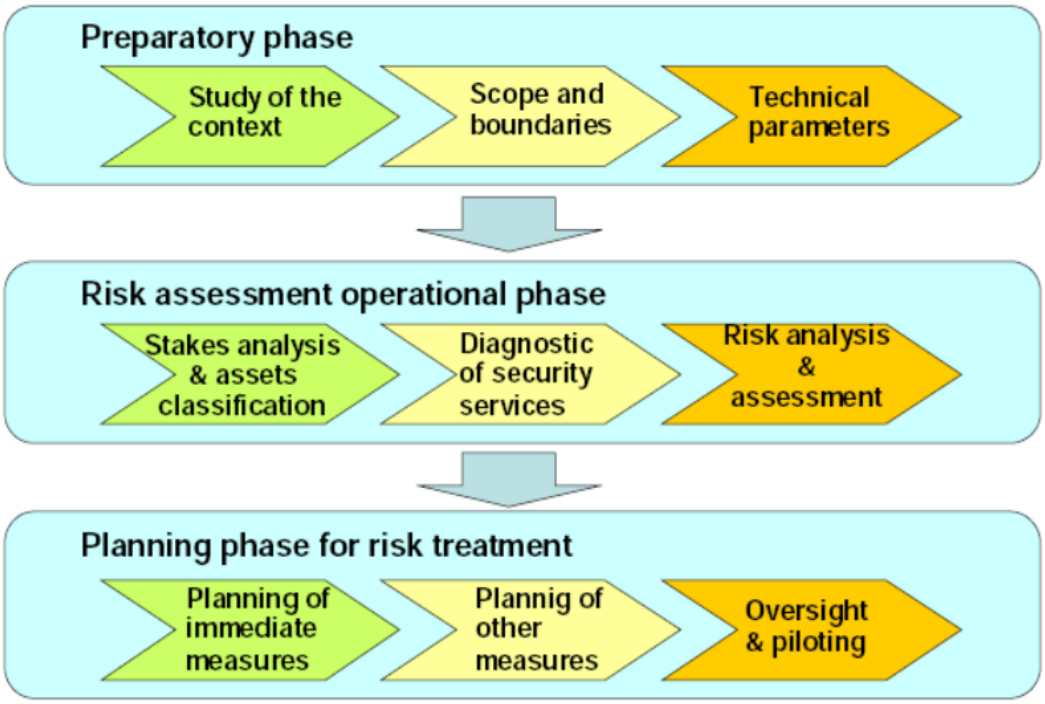
2. Χρήση μόνο με εργαλεία EAR/Pilar.
3. Απαιτούνται ειδικές γνώσεις για να πραγματοποιηθεί η υλοποίηση του εργαλείου και της μεθοδολογίας.

4.1.3 ΜΕΘΟΔΟΣ MEHARI

Η μέθοδος MEHARI (Methode Harmonisee d'Analyse de Risques) που αναπτύχθηκε από την CLUSIF το 1996 είναι μία μέθοδος αξιολόγησης κινδύνου συμβατή με το πρότυπο διαχείρισης κινδύνου ISO/IEC27005 και είναι κατάλληλη για τη διαδικασία ISMS που περιγράφεται στο πρότυπο ISO 27001. Στοχεύει στη διαχείριση της ασφάλειας των στοιχείων των πληροφοριακών συστημάτων και στη μείωση του κινδύνου. Χρησιμοποιείται κυρίως από διευθυντές λειτουργίας, CISO, CIO, ελεγκτές και διευθυντές διαχείρισης κινδύνων. Είναι εφαρμόσιμη σε όλα τα μεγέθη και τους τύπους οργανισμών. Το πεδίο εφαρμογής της MEHARI είναι ίδιο με της MAGERIT αλλά έχει μεγαλύτερη αποδοχή.

Η μέθοδος MEHARI περιλαμβάνει τα τρία παρακάτω στάδια:

1. Την προετοιμασία του έργου
2. Την αξιολόγηση της επικινδυνότητας
3. Την διαχείριση του κινδύνου.



ΕΙΚΟΝΑ 8: Οι τρεις φάσεις της μεθοδολογίας MEHARI

Πηγή: MEHARI-2010-Processing-Guide for risk analysis and management

1. Η προετοιμασία του έργου

Το πρώτο στάδιο χωρίζεται σε τρία επιμέρους βήματα. Ιδανικά τα βήματα αυτά πρέπει να γίνονται διαδοχικά. Είναι τα εξής:

I. Αξιολόγηση του πλαισίου

Στο βήμα αυτό ορίζονται το στρατηγικό, το τεχνικό και το οργανωτικό πλαίσιο. Συγκεκριμένα για τον ορισμό του στρατηγικού πλαισίου λαμβάνονται υπόψη η στρατηγική θέση του οργανισμού στην αγορά (για εμπορικούς οργανισμούς) ή η δομή στο πολιτικό προσκήνιο (για δημόσιους οργανισμούς). Επίσης για τον ορισμό του στρατηγικού πλαισίου προσμετρώνται οι περιορισμοί στη λειτουργία και τη δομή (νομικοί και ρυθμιστικοί περιορισμοί) και η πολιτική ασφαλείας του οργανισμού. Όσον αφορά τον ορισμό του τεχνικού πλαισίου, συγκεντρώνονται δεδομένα και τεχνικές πληροφορίες απαραίτητα για την ανάλυση και αντιμετώπιση του κινδύνου. Λαμβάνονται υπόψη η αρχιτεκτονική του πληροφοριακού συστήματος (δικτύων, εφαρμογών, συστήματος, συνολική επισκόπηση), τα σχέδια τεχνικής ανάπτυξης σε βραχυπρόθεσμη και

μακροπρόθεσμη βάση και η ζωτικής σημασίας τεχνικοί πάροχοι και προμηθευτές. Τέλος με τον ορισμό του οργανωτικού πλαισίου παρέχεται μια συνολική επισκόπηση όλης της δομής και του διαμοιρασμού των αρμοδιοτήτων όσον αφορά την ασφάλεια του πληροφοριακού συστήματος και την υλοποίηση των απαραίτητων ενεργειών.

II. Καθορισμός πεδίου και ορίων για την ανάλυση και την αντιμετώπιση του κινδύνου

Στο βήμα αυτό καθορίζονται τα τεχνικά και οργανωτικά όρια καθώς και η δομή εποπτείας όλου του εγχειρήματος. Για τον καθορισμό των τεχνικών ορίων λαμβάνονται υπόψη γεωγραφικά όρια, τα εμπλεκόμενα πληροφοριακά συστήματα και τα συστήματα πολυμέσων (digital, printed, voice and audio media). Όσον αφορά τα οργανωτικά όρια λαμβάνονται υπόψη οι δραστηριότητες του οργανισμού και τα είδη κινδύνου που μπορεί να αντιμετωπίσει. Τέλος, προσδιορίζεται μια γενική εποπτεία του εγχειρήματος από πλευράς συμμετεχόντων, προγράμματος συναντήσεων και τύπων παραδοτέων.

III. Καθορισμός των τεχνικών παραμέτρων ανάλυσης επικινδυνότητας.

Στο βήμα αυτό προσδιορίζονται οι τεχνικοί παράγοντες. Ο πρώτος είναι ένας πίνακας με τα όρια του αποδεκτού κινδύνου για ένα σενάριο και η ορολογία που σχετίζεται με την κάθε κατηγορία κινδύνου. Ο δεύτερος είναι ένας πίνακας πιθανοτήτων πραγματοποίησης των σεναρίων κινδύνου. Τέλος η τρίτη παράμετρος είναι ένας πίνακας που θα επιτρέπει τον υπολογισμό της υπολειπόμενης δυναμικότητας και των επιπτώσεων.

2. Η αξιολόγηση της επικινδυνότητας

Το δεύτερο στάδιο περιλαμβάνει τρία επιμέρους βήματα. Αυτά είναι:

I. Η ανάλυση και κατηγοριοποίηση των αγαθών

Σε αυτό το βήμα καθορίζεται μια κλίμακα δυσλειτουργίας για τις δραστηριότητες του οργανισμού που θα χρησιμοποιηθεί έπειτα στην κατηγοριοποίηση των αγαθών. Στη συνέχεια τα αγαθά ταξινομούνται σε κατηγορίες ανάλογα τη δραστηριότητα. Τα αγαθά θα πρέπει να κατηγοριοποιηθούν σύμφωνα με τους τρείς άξονες της Διαθεσιμότητας (Availability-A), Εμπιστευτικότητας (Confidentiality-C) και Ακεραιότητας (Integrity-I). Οι δύο πίνακες που δημιουργούνται δείχνουν τα επίπεδα της σοβαρότητας για τις τρεις ζημιές (μη διαθεσιμότητα, απώλεια εμπιστευτικότητας /ακεραιότητας) σε σχέση με τον τύπο του αγαθού και την αντίστοιχη δραστηριότητα του. Ο τρίτος πίνακας που δημιουργείται περιέχει την απαιτούμενη αποδοτικότητα της Διοίκησης.

Τέλος, δημιουργείται ένας πίνακας επιπτώσεων που περιλαμβάνει τις αποδιδόμενες τιμές επίπτωσης για τα σενάρια κινδύνου. Ο παρακάτω πίνακας παρουσιάζει την αντιστοίχιση του επιπέδου επικινδυνότητας όπως αυτό έχει οριστεί από την MEHARI με την εννοιολογική της περιγραφή:

Επίπεδο Επίπτωσης	**Περιγραφή**
1	Μικρή επίπτωση
2	Μέτρια επίπτωση
3	Μεγάλη επίπτωση
4	Κρίσιμη επίπτωση

Κλίμακα Επίπτωσης

II. Η αξιολόγηση της ποιότητας των υπηρεσιών ασφαλείας

Οι υπηρεσίες ασφάλειας περιέχουν διαφορετικούς τύπους εξοπλισμού και στρατηγικών υλοποίησης μέσα στον ίδιο οργανισμό. Αυτές οι διαφορές πρέπει να αξιολογηθούν κάθε μια ξεχωριστά. Σε αυτό το βήμα επιτυγχάνεται αρχικά ο διαχωρισμός των διαφορετικών μεταβλητών των υπηρεσιών ασφάλειας που απαιτούν αξιολόγηση. Στη συνέχεια, γίνεται μια αξιολόγηση της ποιότητας της κάθε μεταβλητής των υπηρεσιών ασφαλείας. Έτσι

δημιουργούνται τα διαγνωστικά αρχεία (κάθε ένα για κάθε τομέα ασφαλείας και κατηγορίας μεταβλητής). Η αξιολόγηση του κάθε τομέα γίνεται από τον αντίστοιχο προϊστάμενο και μεταβάλλεται λόγω διορθώσεων από τους υπεύθυνους των άλλων τμημάτων. Η τελική έγκριση γίνεται από τη Διοίκηση του οργανισμού.

III. Η ανάλυση κινδύνου.

Το βήμα αυτό είναι ιδιαίτερα σημαντικό. Περιλαμβάνει την επιλογή των σεναρίων κινδύνου που θα μπορούσαν να οδηγήσουν σε κρίσιμες καταστάσεις. Υλοποιείται μια λίστα σεναρίων τα οποία αναλύονται λεπτομερώς και εγκρίνονται από τη Διοίκηση του οργανισμού. Στη συνέχεια αξιολογείται η σοβαρότητα των σεναρίων αυτών σε σχέση με την ποιότητα των υπηρεσιών ασφαλείας και των παραγόντων μείωσης κινδύνου. Προϋπόθεση αυτού του βήματος είναι τα προηγούμενα βήματα να έχουν ολοκληρωθεί επιτυχώς. Η βάση που προκύπτει παρουσιάζεται στη Διοίκηση.

3. Η διαχείριση του κινδύνου.

Το τελευταίο στάδιο της διαχείρισης και αντιμετώπισης του κινδύνου περιλαμβάνει τα εξής βήματα:

I. Σχεδιασμό και οργάνωση των άμεσων μέτρων

Στο βήμα αυτό επιλέγονται τα σενάρια υψηλού κινδύνου για να αντιμετωπιστούν με προτεραιότητα. Η επιλογή κυρίως βασίζεται στο πιο υψηλό επίπεδο κινδύνου (το επίπεδο 4) αλλά μπορεί να βασιστεί και σε άλλα κριτήρια. Το αποτέλεσμα είναι μια λίστα κινδύνων που χρήζουν άμεσης αντιμετώπισης. Στη συνέχεια επιλέγονται τα άμεσα μέτρα που θα παρθούν ώστε να περιοριστεί ο κίνδυνος. Αυτά δεν θα οδηγήσουν στην ολοκληρωτική εξάλειψη του κινδύνου αλλά θα μειώσουν το επίπεδο του (από 4 σε 3 αρχικώς). Καταστρώνεται ένα σχέδιο ενεργειών για τη μείωση των μη ανεκτών κινδύνων. Αυτό μπορεί να περιλαμβάνει μέτρα για αποφυγή των

κινδύνων, μέτρα για μείωση του επιπέδου, υπολογισμό του κόστους, πρωταρχική έγκριση από τους υπεύθυνους και έγκριση από τη Διοίκηση.

II. Σχεδιασμός μέτρων για συγκεκριμένους κινδύνους
Γίνεται μια αρχική επιλογή των κινδύνων για τους οποίους θα παρθούν αυτά τα μέτρα με βάση το επίπεδο κινδύνου ξεκινώντας από το επίπεδο 3. Επιπλέον για την επιλογή λαμβάνονται υπόψη πόσο γρήγορα μπορούν τα μέτρα να υλοποιηθούν, πόσο χρόνο απαιτούν, ποιο είναι το κόστος εφαρμογής τους, πόσοι ανθρώπινοι πόροι θα χρειασθούν και ποιες θα είναι οι θετικές ή αρνητικές επιπτώσεις. Ο σκοπός δεν είναι να αντιμετωπιστούν όλοι οι κίνδυνοι ταυτόχρονα αλλά να καταστρωθεί ένα σχέδιο -πιθανότατα πολυετές- για την σταδιακή αντιμετώπιση βάση προτεραιότητας.

III. Σφαιρική εποπτεία και πιλοτική εφαρμογή
Στο τελευταίο αυτό βήμα οργανώνεται η παρακολούθηση του εγχειρήματος. Η οργάνωση της εποπτείας προτείνεται από τον υπεύθυνο ασφαλείας (CISO), και επιλέγονται τα μέλη που θα παρακολουθούν το έργο. Απαραίτητη είναι η έγκριση της Διοίκησης. Επιλέγονται οι κατάλληλοι δείκτες, οι πίνακες ελέγχου και τα διαγράμματα που θα επιβεβαιώνουν την υλοποίηση των μέτρων, θα παρουσιάζουν την πρόοδο του έργου και την εξέλιξη των ρίσκων και θα καταδεικνύουν την ανάγκη για πρόσθετα ή διορθωτικά μέτρα.

ΠΛΕΟΝΕΚΤΗΜΑΤΑ ΤΗΣ ΜΕΘΟΔΟΥ MEHARI

- Η μέθοδος MEHARI είναι συμβατή με όλα τα πρότυπα ασφαλείας ISO. Υλοποιεί τα πρότυπα ISO/IEC 27001 και ISO/IEC IS 13335.
- Είναι η καλύτερη μέθοδος για την μελέτη ασφάλειας τραπεζικού πληροφοριακού συστήματος στην Ελλάδα.
- Περιέχει εκτεταμένη βάση γνώσεων σε μορφή Microsoft Excel
- Μπορεί να χρησιμοποιηθεί για την υλοποίηση ενός ολοκληρωμένου Συστήματος Διαχείρισης Ασφάλειας.

ΜΕΙΟΝΕΚΤΗΜΑΤΑ ΤΗΣ ΜΕΘΟΔΟΥ MEHARI

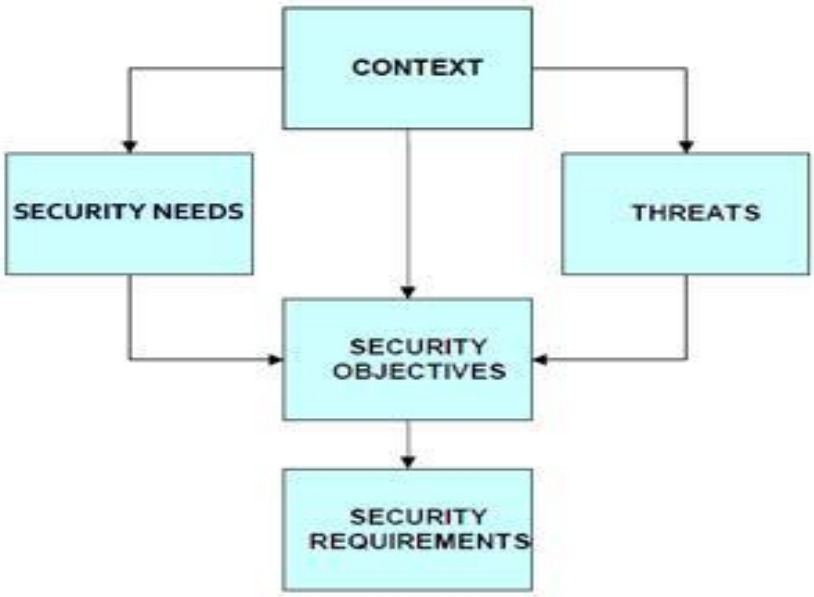
- Χρησιμοποιείται μόνο σε συνδυασμό με ειδικό λογισμικό ή υπολογιστικά φύλλα
- Για τον υπολογισμό της επικινδυνότητας μελετά τα αγαθά λαμβάνοντας υπόψιν την κατηγορία/είδος τους και υπολογίζει την επικινδυνότητα σύμφωνα με τις απειλές που πλήττουν την κάθε υποκατηγορία. Αυτό σε συνδυασμό με τις άκρως εκτενείς και λεπτομερείς βιβλιοθήκες απειλών την καθιστούν πολύπλοκη και δύσκολή στην μελέτη για μη έμπειρους χρήστες

4.1.4 ΜΕΘΟΔΟΛΟΓΙΑ EBIOS

Η μέθοδος EBIOS (Expression des Besoins et Identification des Objectifs de Securite – Έκφραση Αναγκών και Προσδιορισμός Στόχων Ασφαλείας) δημιουργήθηκε το 1995 από τη γραμματεία Εθνικής Άμυνας της Γαλλίας (Direction Centrale se la Securite des Systemes d' Information - DCSSI). Αποτελεί μια οργανωμένη μεθοδολογία για την αξιολόγηση και αντιμετώπιση κινδύνων ενός πληροφοριακού συστήματος. Η EBIOS συνάδει με τις απαιτήσεις και τις διαδικασίες μεγάλου εύρους διεθνών πρότυπων ασφαλείας όπως ISO/IEC 31000, ISO/IEC 27001, ISO/IEC 27005, ISO/IEC 13335, ISO/IEC 15408, ISO/IEC 17799. Καλύπτει επαρκώς τα βήματα για την αξιολόγηση και διαχείριση της επικινδυνότητας προσφέροντας μια υψηλού επιπέδου προσέγγιση των κινδύνων. Η μεθοδολογία συνδυάζει τα συνολικά δεδομένα με ένα αποτελεσματικό τρόπο βασιζόμενη σε μια ποιοτική προσέγγιση. Η μεθοδολογία EBIOS περιλαμβάνει 5 στάδια:

1. Προσδιορισμός του πλαισίου και των αλληλοεξαρτήσεων των αγαθών του
2. Προσδιορισμός των ανεπιθύμητων ενεργειών
3. Προσδιορισμός των πιθανών απειλών
4. Αξιολόγηση της επικινδυνότητας και επιλογή των μέτρων ασφαλείας
5. Ανασκόπηση της ασφάλειας

Σχηματικά φαίνονται παρακάτω:



ΕΙΚΟΝΑ 9: Υψηλού επιπέδου δομή της μεθοδολογίας EBIOS

Πηγή: Information Security Risk Assessment — A Practical Approach with a Mathematical Formulation of Risk - International Journal of Computer Applications

1. **Προσδιορισμός του πλαισίου και των αλληλοεξαρτήσεων των αγαθών του**
   Στο στάδιο αυτό συλλέγονται όλα τα απαραίτητα στοιχεία για την αξιολόγηση και διαχείριση των κινδύνων. Έχει στόχο την περιγραφή του συνόλου των παραμέτρων που θα χρησιμοποιηθούν στα επόμενα στάδια. Περιλαμβάνει τα εξής βήματα:

   I. Καθορισμός του πεδίου εφαρμογής της διαχείρισης του κινδύνου
   Στο βήμα αυτό πλαισιώνεται η ανάλυση του κινδύνου και περιγράφεται το γενικό πλαίσιο. Έπειτα καθορίζεται το πεδίο εφαρμογής της μελέτης και οι παράμετροι που θα εξεταστούν. Τέλος, εντοπίζονται οι πηγές των απειλών.

   II. Προετοιμασία των μετρήσεων
   Στο βήμα αυτό καθορίζονται οι απαιτήσεις ασφαλείας και τα κριτήρια διαχείρισης των κινδύνων. Ακόμα συντάσσονται οι κλίμακες των αναγκών , των επιπέδων δριμύτητας και πιθανοτήτων.

   III. Προσδιορισμός των περιουσιακών στοιχείων – αγαθών
   Γίνεται εντοπισμός των κρίσιμων περιουσιακών στοιχείων και των αλληλοεξαρτήσεων τους. Προσδιορίζονται οι ιδιοκτήτες των ακινήτων, οι κάτοχοι τους και η σχέση μεταξύ τους.

2. **Προσδιορισμός των ανεπιθύμητων ενεργειών**
   Το στάδιο αυτό έχει στόχο τον προσδιορισμό όλων των ανεπιθύμητων ενεργειών και επίφοβων εκδηλώσεων. Γίνεται καταγραφή όλων των ανεπιθύμητων ενεργειών και αξιολόγηση τους. Οι ανεπιθύμητες ενέργειες τοποθετούνται με βάση τη σοβαρότητα και την πιθανότητα τους να συμβούν.

3. **Προσδιορισμός των πιθανών απειλών**
   Αντιστοίχως με το δεύτερο στάδιο, στο τρίτο στάδιο καθορίζονται οι πιθανές απειλές. Καταγράφονται τα σενάρια απειλών και εκτιμώνται οι επιθυμητές τιμές για προστασία. Η καταγραφή των ανεπιθύμητων ενεργειών και απειλών βοηθά

στην εντοπισμό των μέτρων ασφαλείας και αφού εφαρμοστούν επαναπροσδιορίζονται ώστε να αξιολογηθεί η απόδοση των μέτρων.

4. **Αξιολόγηση της επικινδυνότητας και επιλογή των μέτρων ασφαλείας**
   Το βήμα αυτό περιλαμβάνει :

   I. Την αξιολόγηση των κινδύνων
   II. Τον προσδιορισμό των μέτρων ασφαλείας

   Με την μελέτη και συσχέτιση των ανεπιθύμητων ενεργειών και των σεναρίων απειλών προσδιορίζονται μόνο τα πραγματικά σενάρια κινδύνου στο πεδίο εφαρμογής της μελέτης. Στη συνέχεια επιλέγονται τα αντίμετρα για τα σενάρια κινδύνου, παρατηρείται η απόδοση των μέτρων και εκτιμώνται οι κίνδυνοι που εξακολουθούν να υπάρχουν.

5. **Ανασκόπηση της ασφάλειας**
   Στο τελευταίο στάδιο καθορίζεται η αντιμετώπιση των κινδύνων και παρακολουθείται η εφαρμογή και τα αποτελέσματα που επιφέρει. Ακολουθούν τα παρακάτω βήματα:

   I. Επισημοποίηση των μέτρων ασφαλείας
      Στο βήμα αυτό επιτυγχάνεται συναίνεση για τα μέτρα ασφαλείας που έχουν σχεδιαστεί προηγουμένως για την αντιμετώπιση του κινδύνου και συμφωνείται η χρησιμοποίηση τους. Επίσης αναλύονται οι εναπομείναντες κίνδυνοι και δηλώνεται συνολικά η εφαρμογή των μέτρων.

   II. Εφαρμογή των μέτρων ασφαλείας
      Στο τελευταίο βήμα καταστρώνεται ένα σχέδιο δράσης και παρακολουθείται η εφαρμογή αυτού. Ακόμα χορηγείται η σχετική έγκριση ασφάλειας.

ΠΛΕΟΝΕΚΤΗΜΑΤΑ ΤΗΣ ΜΕΘΟΔΟΛΟΓΙΑΣ EBIOS

- Η μεθοδολογία EBIOS είναι συμβατή με αρκετά πρότυπα ασφαλείας ISO όπως , ISO/IEC 27001/2005, ISO/IEC 27005/2008, ISO/IEC 27002/2005
- Είναι μια σχετικά εύκολη μεθοδολογία που μπορεί να βρει εφαρμογή σε μικρές και μεσαίες εταιρείες, κυβερνητικούς και μεγάλους οργανισμούς.
- Ακόμα μπορεί να χρησιμοποιηθεί σε ένα υποσύνολο ή μια διεργασία του οργανισμού όπως ένα σύστημα διασύνδεσης, μια εφαρμογή, ένα σύστημα υπολογιστή, ένα προϊόν ασφαλείας κ.α.
- Υποστηρίζεται από ένα εργαλείο ανοιχτού κώδικα το OpenEBIOS.
- Δεν απαιτείται ιδιαίτερη εμπειρία και εξειδίκευση για τη χρήση του εργαλείου.
- Είναι εύκολα στη χρήση πολλαπλών παραδοτέων, είναι γρήγορο και επαναχρησιμοποιήσιμο.

ΜΕΙΟΝΕΚΤΗΜΑΤΑ ΤΗΣ ΜΕΘΟΔΟΛΟΓΙΑΣ EBIOS

- Ένα μειονέκτημα αποτελεί η έλλειψη μιας προηγμένης υπολογιστικής τεχνικής για το συσχετισμό των αποτελεσμάτων.
- Δεν φτάνει σε τεχνικό επίπεδο

4.1.5 ΜΕΘΟΔΟΛΟΓΙΑ IT- Grundschutz

Η IT- Grundschutz ανακοινώθηκε το 1994 από το ομοσπονδιακό γραφείο για την ασφάλεια πληροφοριών στη Γερμανία (BSI –Bundesamt fur Sicherheit in der Informationstechnik) και είναι μια μεθοδολογία για την διαχείριση ασφάλειας πληροφοριακών συστημάτων. Είναι συμβατή με τα πρότυπα ISO/IEC 27001 και ISO/IEC 17779. Προσφέρει μια μεθοδολογία για τη δημιουργία ενός συστήματος διαχείρισης της ασφάλειας πληροφοριών αλλά και μια βάση για την αξιολόγηση των κινδύνων, την παρακολούθηση τους και την εφαρμογή κατάλληλων μέτρων.

Στο πλαίσιο της μεθοδολογίας IT- Grundschutz ακολουθούνται τα παρακάτω στάδια:

1. Κίνηση της διαδικασίας διαχείρισης ασφαλείας από τη Διοίκηση.
   Η Διοίκηση είναι ενημερωμένη για τους κινδύνους και της επιπτώσεις ανεπαρκούς ασφάλειας και αναλαμβάνει ευθύνη για την έναρξη των διαδικασιών διαχείριση της ασφάλειας. Ακολουθεί ο σχεδιασμός και προγραμματισμός της διαδικασίας διαχείρισης ασφάλειας και δημιουργείται η πολιτική για την ασφάλεια πληροφοριών. Μια ομάδα ανάπτυξης προσδιορίζει την πολιτική ασφαλείας η οποία εγκρίνεται από τη Διοίκηση. Στη συνέχεια δημιουργείται η κατάλληλη οργανωτική δομή για τη διαχείριση της ασφάλειας. Διαμοιράζονται τα καθήκοντα, προσδιορίζεται το ανθρώπινο δυναμικό που απαιτείται και ορίζονται οι ρόλοι τους. Γίνεται μια καταγραφή των απαιτούμενων οικονομικών πόρων και του χρονικού ορίζοντα του εγχειρήματος. Ο σκοπός της διασφάλισης των πληροφοριών εξηγείται στους εργαζομένους και ορίζεται ένα άτομο ως υπεύθυνος ασφαλείας στον οποίο και μπορούν να απευθυνθούν.

2. Δημιουργία του σχεδίου ασφαλείας.
   Καθορίζεται το πεδίο εφαρμογής της ασφάλειας και τεκμηριώνονται τα δομικά στοιχεία της ασφάλειας πληροφοριών. Παρακάτω παρουσιάζεται ένας κατάλογος των στοιχείων που απαιτούνται για την άσκηση των εργασιών που βρίσκονται στο πεδίο εφαρμογής ασφαλείας:

ΚΑΤΑΛΟΓΟΣ ΣΤΟΙΧΕΙΩΝ ΑΣΦΑΛΕΙΑΣ ΠΛΗΡΟΦΟΡΙΑΚΩΝ ΣΥΣΤΗΜΑΤΩΝ
Γενικές πτυχές (οργανισμός, προσωπικό, πολιτική εφεδρικών στοιχείων και υλικό προστασίας ιών των υπολογιστών)
Υποδομή (κτήρια, δωμάτιο κεντρικών υπολογιστών, και προστατευτικό δωμάτιο)
Πληροφοριακά Συστήματα (κεντρικοί υπολογιστές, πελάτες)
Δίκτυα & Εφαρμογές (ηλεκτρονικό ταχυδρομείο, κεντρικός υπολογιστής δικτύου και βάσεις δεδομένων)

Στη συνέχεια προσδιορίζονται οι κατηγορίες που απαιτούν προστασία:

ΚΑΤΗΓΟΡΙΕΣ ΑΠΑΙΤΗΣΕΩΝ ΠΡΟΣΤΑΣΙΑΣ
Παραβίαση των νόμων, των συμβάσεων ή των κανονισμών
Εξασθένιση του δικαιώματος στην εκπαιδευτική ατομική αποφασιστικότητα
Φυσική ζημιά
Εξασθένιση στην απόδοση καθηκόντων
Αρνητικά εσωτερικά ή εξωτερικά αποτελέσματα
Οικονομικές συνέπειες

Γίνεται επιλογή και προσαρμογή των μέτρων ασφαλείας και ακολουθεί ο έλεγχος της ασφάλειας όπου γίνεται σύγκριση με την πραγματική κατάσταση. Το στάδιο ολοκληρώνεται με την συμπληρωματική ανάλυση ασφάλειας.

3. Εφαρμογή του σχεδίου ασφαλείας

   Στο στάδιο αυτό γίνεται μια επισκόπηση των αποτελεσμάτων της εξέτασης και εντοπίζονται τυχόν περισσότερα μέτρα ασφαλείας που πρέπει να υλοποιηθούν. Εδραιώνονται λοιπόν τα μέτρα ασφαλείας που πρέπει να παρθούν. Στη συνέχεια υπολογίζεται το κόστος υλοποίησης και οι ανθρώπινοι πόροι που θα χρησιμοποιηθούν. Εάν ο προϋπολογισμός δεν επαρκεί καθορίζεται η σειρά προτεραιότητας για την εφαρμογή των μέτρων. Τέλος, ανατίθενται οι αρμοδιότητες και ορίζεται μέχρι πότε πρέπει να εφαρμοστούν τα μέτρα ασφαλείας.

4. Διατήρηση της ασφάλειας των πληροφοριών, παρακολούθηση, βελτίωση και πιστοποίηση τους.

   Ο στόχος είναι αφενός να επιτευχθεί το επιθυμητό επίπεδο ασφαλείας και αφετέρου να συντηρηθεί όσο γίνεται μεγαλύτερο χρονικό διάστημα. Απαιτείται λοιπόν τακτικός έλεγχος της διαδικασίας και της πολιτικής ασφάλειας και επιβεβαίωση ότι τα μέτρα έχουν εφαρμοστεί σωστά. Ακόμα εάν κριθεί αναγκαίο γίνεται βελτίωση της διαδικασίας και πιστοποίηση της (προαιρετικά).

Η ποιότητα της μεθοδολογίας IT- Grundschutz είναι στη δημιουργία των καταλόγων απειλών και προστασίας, οι οποίοι μπορούν να χρησιμοποιηθούν σε όλες τις άλλες μεθόδους. Η IT- Grundschutz παρέχει τους παρακάτω καταλόγους απειλών και μέτρων:

ΚΑΤΑΛΟΓΟΣ ΑΠΕΙΛΩΝ	ΚΑΤΑΛΟΓΟΣ ΜΕΤΡΩΝ
Ισχύς ανωτέρας βίας	Υποδομή
Επιχειρηματική ανεπάρκεια	Οργάνωση
Ανθρώπινο λάθος	Προσωπικό
Τεχνική βλάβη	Υλικό
Σκόπιμα μέτρα	Λογισμικό
	Επικοινωνία
	Ετοιμότητα έκτακτης ανάγκης

Ένας πολύ σημαντικός στόχος της μεθοδολογίας είναι η επαναχρησιμοποίηση γνωστών διαδικασιών για τη βελτίωση της ασφάλειας πληροφοριών. Παρέχει ένα ολοκληρωμένο σύστημα διαχείρισης ασφάλειας και πρέπει μόνο να προσαρμοσθεί στις συνθήκες του κάθε συγκεκριμένου οργανισμού. Απευθύνεται κυρίως στους υπεύθυνους ασφαλείας αλλά μπορεί να χρησιμοποιηθεί από οποιονδήποτε χρήση έχει βασικές γνώσεις ασφάλειας. Είναι κατάλληλη για όλους τους τύπους και τα μεγέθη οργανισμών. Το εργαλείο GSTOOL διατίθεται δωρεάν για τις δημόσιες αρχές ενώ υπάρχουν και εμπορικά εργαλεία για τους χρήστες (Gstool για εμπορικό σκοπό, HiSolutions AG HiScout SME, INFODAS GmbH –Save, inovationtec – IGSDoku, Kronsoft e.K – Secu-Max, Swiss Infosec AG- Baseline-Tool, WCK-PC-Checkheft)

4.2 ΣΥΓΚΡΙΣΗ ΜΕΘΟΔΟΛΟΓΙΩΝ ΑΝΑΛΥΣΗΣ ΚΙΝΔΥΝΟΥ ΣΥΜΒΑΤΕΣ ΜΕ ISO 27001

Μετά την περιγραφή των μεθοδολογιών ανάλυσης και διαχείρισης επικινδυνότητας συμβατών κατά ISO 27001 είναι σκόπιμη η σύγκριση αυτών. Στον παρακάτω πίνακα συνοψίζονται οι μεθοδολογίες που αναλύθηκαν κάτω από βασικά κριτήρια. Αυτά τα κριτήρια είναι:

- Το κόστος δηλαδή εάν η μεθοδολογία διατίθεται δωρεάν (βλέπε και επόμενο πίνακα με εργαλεία μεθοδολογιών).
- Η συνεργατικότητα δηλαδή η διευκόλυνση της εργασίας των χρηστών από κοινού για την υλοποίηση των σταδίων της ανάλυσης και διαχείρισης επικινδυνότητας.
- Η συμβατότητα με πρότυπα (βλέπε αναλυτικά σε επόμενο πίνακα).
- Το μέγεθος του οργανισμού στον οποίο απευθύνεται η μεθοδολογία (μικρομεσαίες επιχειρήσεις, μεγάλης κλίμακας, δημόσιες αρχές.
- Οι γλώσσες στις οποίες είναι διαθέσιμη η κάθε μεθοδολογία.
- Εάν είναι ποιοτική ή ποσοτική μέθοδος ανάλυσης. Αυτό εξαρτάται από τα αποτελέσματα που εξάγονται. Εάν ο κίνδυνος μετράται σε μια κλίμακα με αριθμούς η μέθοδος χαρακτηρίζεται ποσοτική ενώ εάν μετράται σε μια τακτική κλίμακα (υψηλό- μέτριο-χαμηλό) χαρακτηρίζεται ως ποιοτική.
- Εάν εστιάζει σε Ανάλυση Κινδύνου (Risk Analysis –RA) ή Διαχείριση Κινδύνου (Risk Management - RM)
- Το έτος της έκδοσης.
- Το επίπεδο ειδίκευσης που απαιτείται από τον χρήστη για την εφαρμογή της.

ΜΕΘΟΔΟΛΟΓΙΑ / **ΚΡΙΤΗΡΙΑ**		**CRAMM**	**MAGERIT**	**MEHARI**	**EBIOS**	**IT-Grundschutz**
ΚΟΣΤΟΣ		Εμπορικό	Δωρεάν	Δωρεάν	Δωρεάν	Δωρεάν
ΣΥΝΕΡΓΑΤΙΚΟΤΗΤΑ		ΟΧΙ	ΟΧΙ	ΟΧΙ	ΟΧΙ	ΟΧΙ
ΣΥΜΒΑΤΟΤΗΤΑ ΜΕ ΠΡΟΤΥΠΑ		ΝΑΙ	ΝΑΙ	ΝΑΙ	ΝΑΙ	ΝΑΙ
ΟΡΓΑΝΙΣΜΟΣ ΣΤΟΧΟΣ	ΜΙΚΡΟ-ΜΕΣΑΙΕΣ	ΟΧΙ	ΝΑΙ	ΟΧΙ	ΝΑΙ	ΝΑΙ
	ΜΕΓΑΛΗΣ ΚΛΙΜΑΚΑΣ		ΝΑΙ	ΝΑΙ	ΝΑΙ	ΝΑΙ
	ΔΗΜΟΣΙΩΝ ΑΡΧΩΝ		ΝΑΙ	ΝΑΙ	ΝΑΙ	ΝΑΙ
ΠΟΛΥΓΛΩΣ-ΣΙΚΟΤΗΤΑ		ΑΓΓΛΙΚΑ	ΑΓΓΛΙΚΑ ΙΣΠΑΝΙΚΑ	ΓΑΛΛΙΚΑ	ΝΑΙ	ΓΕΡΜΑΝΙΚΑ ΑΓΓΛΙΚΑ
ΠΟΙΟΤΙΚΗ/ ΠΟΣΟΤΙΚΗ		ΠΟΙΟΤΙΚΗ	ΠΟΙΟΤΙΚΗ &ΠΟΣΟΤΙΚΗ	ΠΟΙΟΤΙΚΗ	ΠΟΙΟΤΙΚΗ	ΠΟΙΟΤΙΚΗ
ΕΣΤΙΑΣΗ ΣΕ RA/RM		RA	RA	RM	RA	RM
ΕΤΟΣ ΕΚΔΟΣΗΣ		1987	1997	1996	1995	1994
ΕΠΙΠΕΔΟ ΧΡΗΣΤΗ		ΕΙΔΙΚΟ	ΒΑΣΙΚΟ	ΒΑΣΙΚΟ	ΒΑΣΙΚΟ	ΒΑΣΙΚΟ

ΠΙΝΑΚΑΣ 3: Βασικά χαρακτηριστικά μεθοδολογιών

Στον παρακάτω πίνακα παρουσιάζονται αναλυτικά τα πρότυπα με τα οποία είναι συμβατή κάθε μεθοδολογία που αναλύθηκε καθώς και το εργαλείο που τη συνοδεύει. Από τις μεθοδολογίες μόνο η CRAMM είναι καθαρά εμπορική και δεν διατίθεται δωρεάν. Το κόστος της μεθοδολογίας CRAMM κυμαίνεται από 800 μέχρι 3000€ ανάλογα την περίπτωση.

ΜΕΘΟΔΟΛΟΓΙΑ	**ΠΡΟΤΥΠΑ**	**ΕΡΓΑΛΕΙΟ**
CRAMM	ISO/IEC 27001:2005 ISO 27000 ISO/IEC 17799	Εμπορικό εργαλεία: CRAMM expert CRAMM express
MAGERIT	ISO/IEC 27001:2005 ISO/IEC 13335:2004 ISO/IEC 17799:2005 ISO/IEC 15408:2005	Μη εμπορικό εργαλείο: PILAR Εμπορικό εργαλείο: EAR
MEHARI	ISO/IEC 27001:2005 ISO/IEC IS 13335	Εμπορικό εργαλείοο: MEHARI 2010 basic tool Μη εμπορικό εργαλείο: RISICARE
EBIOS	ISO/IEC 27001 ISO/IEC 31000 ISO/IEC 27005 ISO/IEC 13335 ISO/IEC 15408 ISO/IEC 17799	Μη εμπορικό εργαλείο (δωρεάν): EBIOS
IT-Grundschutz	ISO/IEC 27001 ISO/IEC 17799	Μη εμπορικό εργαλείο (δωρεάν για δημόσιες αρχές): GSTOOL Εμπορικά εργαλεία: GSTOOl, HiScout SME, SAVe, IGSDoku, Secu-Max, Baseline-Tool, PC-Checkheft

ΠΙΝΑΚΑΣ 4: Συμβατά πρότυπα και εργαλεία μεθοδολογιών

Στοιχεία πίνακα από Ανάλυση και Διαχείριση επικινδυνότητας στα πληροφορικά συστήματα – Γεωργίου Σοφία

Σύμφωνα με τα χαρακτηριστικά της κάθε μεθόδου μπορεί να αποφασιστεί ποια μέθοδος είναι η βέλτιστη για την ανάλυση επικινδυνότητας. Αυτά τα συμπεράσματα μπορούν να χρησιμοποιηθούν για να γίνουν συστάσεις στις εταιρείες για την κατάλληλη επιλογή μεθοδολογίας. Για τον ορισμό του πίνακα απόφασης είναι αναγκαίο να ορισθούν τα παρακάτω κριτήρια επιλογής:

- ΜΜΕ: Αναφέρεται στο μέγεθος της εταιρείας. Κάθε εταιρεία που απασχολεί κάτω από 300 εργαζομένους θεωρείται ΜΜΕ (μικρομεσαία επιχείρηση)
- Διαθέσιμες ημέρες: Αναφέρεται στο χρονικό περιθώριο που είναι διαθέσιμο ή προτιμώμενο για την ολοκλήρωση του εγχειρήματος. Φυσικά και μέθοδοι που μπορούν να υλοποιηθούν σε 1 ημέρα μπορούν και σε 3 ημέρες.
- Διαθέσιμοι ειδικοί: Αναφέρεται στο εάν υπάρχουν ειδήμονες για την ασφάλεια πληροφοριακών συστημάτων και την ανάλυση ρίσκου που μπορούν να συμμετάσχουν στην αξιολόγηση κινδύνου.
- Κρίσιμη ως προς την ασφάλεια: Αναφέρεται στο εάν ο στόχος της αξιολόγησης είναι κρίσιμος για την ασφάλεια. Εάν είναι κρίσιμος, η ανάλυση πρέπει να καλύπτει όλα τα ενδεχόμενα ανεξαρτήτως πόσο σπάνια μπορούν να συμβούν.

Με βάση τα παραπάνω κριτήρια δημιουργούνται 24 κανόνες απαιτήσεων. Ανάλογα με το ποιος κανόνας είναι επιθυμητό να πληρείται επιλέγεται η καταλληλότερη μέθοδος. Για κάθε κανόνα μπορεί να είναι κατάλληλή περισσότερες από μια μέθοδοι. Το αποτέλεσμα της ανάλυσης επικινδυνότητας μπορεί να χρησιμοποιηθεί για έλεγχο, πιστοποίηση, νομική συμμόρφωση ή ακόμα για να ληφθούν αποφάσεις για την υιοθέτηση νέων τεχνολογιών.

	ΑΝΑΓΚΕΣ ΚΑΙ ΠΕΡΙΟΡΙΣΜΟΙ				**ΚΑΤΑΛΛΗΛΗ ΜΕΘΟΔΟΛΟΓΙΑ**				
ΑΠΑΙ-ΤΗΣΕΙΣ	**ΜΜΕ**	**ΗΜΕΡΕΣ ΔΙΑΘΕ-ΣΙΜΕΣ**	**ΣΥΜ-ΜΕΤΟΧΗ ΕΙΔΙΚΩΝ**	**ΚΡΙΣΙΜΟ ΓΙΑ ΑΣΦΑΛΕΙΑ**	**CRAMM**	**MAGERIT**	**MEHARI**	**EBIOS**	**IT-Grundschutz**
1	ΝΑΙ	<1	ΝΑΙ	ΝΑΙ					
2	ΝΑΙ	<1	ΝΑΙ	ΟΧΙ					
3	ΝΑΙ	<1	ΟΧΙ	ΝΑΙ					
4	ΝΑΙ	<1	ΟΧΙ	ΟΧΙ					
5	ΝΑΙ	1-3	ΝΑΙ	ΝΑΙ		**X**		**X**	**X**
6	ΝΑΙ	1-3	ΝΑΙ	ΟΧΙ		**X**		**X**	**X**
7	ΝΑΙ	1-3	ΟΧΙ	ΝΑΙ					
8	ΝΑΙ	1-3	ΟΧΙ	ΟΧΙ		**X**		**X**	
9	ΝΑΙ	>3	ΝΑΙ	ΝΑΙ		**X**		**X**	**X**
10	ΝΑΙ	>3	ΝΑΙ	ΟΧΙ		**X**		**X**	**X**
11	ΝΑΙ	>3	ΟΧΙ	ΝΑΙ		**X**		**X**	
12	ΝΑΙ	>3	ΟΧΙ	ΟΧΙ		**X**		**X**	
13	ΟΧΙ	<1	ΝΑΙ	ΝΑΙ					
14	ΟΧΙ	<1	ΝΑΙ	ΟΧΙ					
15	ΟΧΙ	<1	ΟΧΙ	ΝΑΙ					
16	ΟΧΙ	<1	ΟΧΙ	ΟΧΙ					
17	ΟΧΙ	1-3	ΝΑΙ	ΝΑΙ		**X**		**X**	**X**
18	ΟΧΙ	1-3	ΝΑΙ	ΟΧΙ		**X**	**X**	**X**	**X**
19	ΟΧΙ	1-3	ΟΧΙ	ΝΑΙ					
20	ΟΧΙ	1-3	ΟΧΙ	ΟΧΙ					
21	ΟΧΙ	>3	ΝΑΙ	ΝΑΙ	**X**	**X**		**X**	**X**
22	ΟΧΙ	>3	ΝΑΙ	ΟΧΙ		**X**	**X**	**X**	**X**
23	ΟΧΙ	>3	ΟΧΙ	ΝΑΙ		**X**		**X**	
24	ΟΧΙ	>3	ΟΧΙ	ΟΧΙ		**X**	**X**	**X**	

ΠΙΝΑΚΑΣ 5: Απόφαση επιλογής μεθοδολογίας

Στοιχεία πίνακα από "Current established Risk assessmet methodologies and tools- Dan Ionit"

Όσον αφορά τον υπολογισμό του κινδύνου οι παραπάνω μεθοδολογίες λαμβάνουν υπόψιν διαφορετικούς παράγοντες. Κάθε μεθοδολογία χρησιμοποιεί διαφορετικές φόρμουλες για τον υπολογισμό του κινδύνου αλλά σε μια μακροσκοπική βάση καταλήγουμε στα παρακάτω.

- Οι μεθοδολογίες CRAMM,MAGERIT και MEHARI χρησιμοποιούν την πιθανότητα να συμβεί μια απειλή, την αδυναμία σε αυτή την απειλή μιας ομάδας αγαθών και την επίπτωση που θα έχει αυτή η απειλή στην ομάδα αγαθών. Έτσι ο κίνδυνος δίνεται:

$$\text{Κίνδυνος} = \textit{Πιθανότητα}\ (\textit{Απειλής})\ x\ \textit{Αδυναμία}\ (\textit{Αγαθού στην απειλή})\ x\ \textit{Επίπτωση}\ (\textit{Απειλής σε αγαθό})$$

- Η μεθοδολογία EBIOS υπολογίζει το επίπεδο επικινδυνότητας βασιζόμενη στην επίπτωση μιας απειλής στις απαιτήσεις ασφαλείας του οργανισμού. Υπολογίζεται οι επίπτωση της κατηγορίας αγαθών και συνδυάζεται με την αδυναμίας στην απειλή της κατηγορίας αγαθών. Αυτή η προσέγγιση είναι ιδιαίτερα χρήσιμη για τις πιστοποιήσεις και για να προσδιοριστεί πόσο ο οργανισμός πληροί τις συστάσεις των καλύτερων πρακτικών. Έτσι ο κίνδυνος δίνεται ως εξής:

$$\text{Κίνδυνος} = \textit{Αδυναμία}\ (\textit{Αγαθού στην απειλή})\ x\ \textit{Επίπτωση}\ (\textit{Απειλής σε απαιτήσεις ασφάλειας})$$

- Η μεθοδολογία IT-Grundschutz υπολογίζει το επίπεδο κινδύνου βασιζόμενη στις αδυναμίες του συστήματος. Δεν λαμβάνεται υπόψιν κάποια συγκεκριμένη απειλή αλλά η συχνότητα των αρνητικών συμβάντων και η επίπτωση τους. Ο κίνδυνος υπολογίζεται ως εξής:

$$\text{Κίνδυνος} = \textit{Πιθανότητα}\ (\textit{Περιστατικού})\ x\ \textit{Επίπτωση}\ (\textit{Περιστατικού σε αγαθό})$$

5. ΜΕΛΕΤΗ ΠΕΡΙΠΤΩΣΗΣ – ΑΝΑΛΥΣΗ ΕΠΙΚΙΝΔΥΝΟΤΗΤΑΣ

5.1 ΠΕΡΙΓΡΑΦΗ

Η μελέτη περίπτωσης θα πραγματοποιηθεί για έναν μικρομεσαίο οργανισμό που δραστηριοποιείται στον τραπεζικό τομέα. Ο οργανισμός αυτός ασχολείται με τη διαχείριση συναλλαγών φορητών τερματικών συσκευών. Ο υπό μελέτη οργανισμός αποτελεί μέρος κρίσιμης υποδομής καθώς προσφέρει υπηρεσίες σε τράπεζες οι οποίες πρέπει να έχουν συνεχή και επαρκή έλεγχο στην τεχνολογία των πληροφοριών. Είναι ζωτικής σημασίας να διασφαλίζεται η ακεραιότητα των πληροφοριών, η διαθεσιμότητα, η ακρίβεια και η ασφάλεια στις τραπεζικές συναλλαγές. Τα περιουσιακά στοιχεία του οργανισμού χωρίζονται σε 8 ζώνες και είναι τα παρακάτω:

Zone 1	Active Directory Primary PC
	Active Directory Secondary PC
	ERP Database
	MTMS Database
Zone 2	MTMS COM
	Ingestate
Zone 3	Domain Controller 1
	Domain Controller
	Log and event manager (LEM)
	Windows updater
	MTMS Web UI
	FTPS Client
	VMware server
Zone 4	Antivirus server
Zone 5	Proxy server
Zone 6	Admins PCs

	Developers PCs
Zone 7	APV 1600 Node 1
	APV 1600 Node 2
Zone 8	Cisco 2960 Node 1
	Cisco 2960 Node 2
	Checkpoint 4406 Node 1
	Checkpoint 4406 Node 2

Στη ζώνη 1 βρίσκονται το Active Directory Primary, το Active Directory Secondary και οι βάσεις δεδομένων ERP DB και MTMS DB. Το Active Directory PC είναι ο server που είναι εγκατεστημένο το Active Directory. Ορίζει τους κανόνες ασφαλείας που χρησιμοποιούνται στον οργανισμό και υπάρχει Primary και Secondary για έκτακτες περιπτώσεις. Η βάση δεδομένων ERP DB (Enterprise Resource Planning) διευκολύνει την ροή πληροφοριών μεταξύ των επιχειρησιακών λειτουργιών του οργανισμού αλλά και μεταξύ του οργανισμού και τρίτων μερών. Η βάση δεδομένων MTMS DB έχει πολλαπλά επίπεδα και αποτυπώνει τις πληροφορίες των πελατών.

Στη ζώνη 2 βρίσκονται τα αγαθά που επικοινωνούν απευθείας με τις φορητές συσκευές τερματικών. Συγκεκριμένα ο MTMS COM είναι ένας server υπεύθυνος για την παρακολούθηση και τον έλεγχο της ομαλής επικοινωνίας του τερματικού είτε με το MTMS Web UI είτε με τη βάση MTMS DB. Το Ingestate είναι ένας server για τη διαχείριση του συνόλου των τερματικών και των εφαρμογών που φορτώνονται σε αυτά.

Στη ζώνη 3 περιλαμβάνονται οι ελεγκτές Domain Controller 1 και 2 που διαχειρίζονται την κίνηση του δικτύου. Ο LEM (log and event manager) είναι ένας server που κρατά διαγνωστικές πληροφορίες για όλο το δίκτυο για την ασφάλεια, τη συμμόρφωση και την αντιμετώπιση των προβλημάτων. Ο VMware server δημιουργεί όλα τα vms σε όλο το δίκτυο. Το MTMS Web UI είναι το web user interface του MTMS για τη διεπαφή των χρηστών του συστήματος με το MTMS. Το FTPS client είναι το λογισμικό που χρησιμοποιείται με σκοπό το την διεπαφή ενός χρήστη του συστήματος με τον FTPS server οπού τοποθετούνται τα αρχεία που παρέχει κάποιος πελάτης ή αυτά που πρέπει

να λάβει. Τέλος, το Windows Update είναι ένας server αναβαθμίσεων που συγκεντρώνει όλα τα updates, τα ελέγχει και τα προωθεί σε όλα το δίκτυο για εγκατάσταση.

Στη ζώνη 4 βρίσκεται ο Antivirus server που έχει εγκατεστημένο το πρόγραμμα antivirus για την προστασία του πληροφοριακού συστήματος από κακόβουλα λογισμικά ή ιούς.

Στη ζώνη 5 βρίσκεται ο Proxy server που είναι ο διαμεσολαβητής μεταξύ των διάφορων ζωνών τους συστήματος.

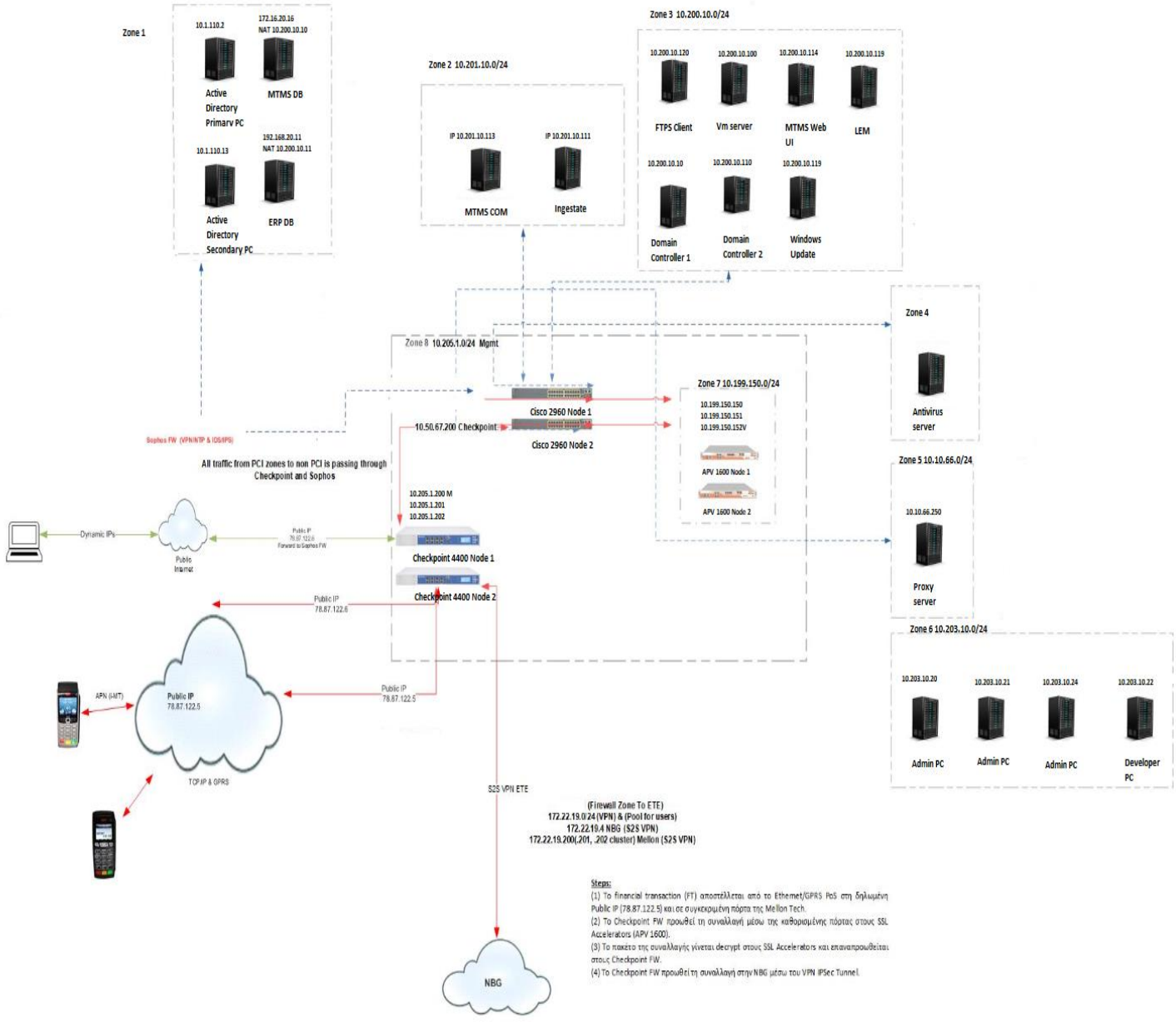
Στη ζώνη 6 βρίσκονται τα Admins PC και τα Developers PC. Τα Admins PC είναι υπεύθυνα για την διαχείριση όλων των servers ενώ τα developers PC χρησιμοποιούνται για την ανάπτυξη και τροποποίηση των εφαρμογών που εξελίσσονται στους servers.

Στη ζώνη 7 βρίσκονται τα APV 1600 Node 1 και APV 1600 Node 2. Το APV 1600 Node 1 (Application Delivery Controller) αποτελεί τον ελεγκτή/ κόμβο των εφαρμογών του συστήματος για τον έλεγχο της λειτουργίας των σημαντικών εφαρμογών του συστήματος. Το APV 1600 Node 2 αποτελεί τον ελεγκτή/ κόμβο των εφαρμογών του συστήματος για τον έλεγχο της λειτουργίας των δευτερευούσης σημασίας εφαρμογών του συστήματος.

Η ζώνη 8 περιλαμβάνει τη ζώνη 7 και τέσσερα επιπλέον αγαθά. Το Cisco 2960 Node 1 αποτελεί έναν κόμβο που δρομολογεί τις σημαντικές πληροφορίες μεταξύ των ζωνών του συστήματος ενώ το αγαθό Cisco 2960 Node 2 αποτελεί έναν κόμβο για τη δρομολόγηση των λιγότερο σημαντικών πληροφοριών μεταξύ των ζωνών του συστήματος. Το Checkpoint 4406 Node 1 αποτελείται από το μηχάνημα και την πλατφόρμα λογισμικού για τον έλεγχο της ασφάλειας επικοινωνιών μεταξύ των εφαρμογών του συστήματος ενώ το Checkpoint 4406 Node 2 εκτελεί την ίδια λειτουργία σε περίπτωση βλάβης του πρωτεύοντος.

Η ταξινόμηση των αγαθών σε ζώνες που δρουν ανεξάρτητα βοηθά στην προστασία του συνολικού συστήματος. Διασφαλίζεται έτσι ότι σε περίπτωση που προσβληθεί μια συγκεκριμένη ζώνη του συστήματος δεν επηρεάζονται τα άλλα αγαθά των υπόλοιπων ζωνών.

Στην παρακάτω εικόνα φαίνονται τα αγαθά του υπό μελέτη οργανισμού κατανεμημένα στις ζώνες 1-8.



ΕΙΚΟΝΑ 10: Τα αγαθά του υπό μελέτη οργανισμού κατανεμημένα σε ζώνες

5.2 ΑΝΑΛΥΣΗ ΕΠΙΚΙΝΔΥΝΟΤΗΤΑΣ ΜΕ ΧΡΗΣΗ ΤΟΥ ΕΡΓΑΛΕΙΟΥ PILAR

Για τη μελέτη του συγκεκριμένου οργανισμού επιλέχθηκε η μεθοδολογία MAGERIT. Για την υλοποίηση της προσομοίωσης της μεθοδολογίας χρησιμοποιήθηκε το εργαλείο PILAR (7.2.7 - 25.3.2019). Μέσω του εργαλείου πραγματοποιήθηκε η ανάλυση της επικινδυνότητας με τον τελικό προσδιορισμό του επιπέδου των κινδύνων.

Η MAGERIT ως μεθοδολογία στην φάση υπολογισμού της επικινδυνότητας μελετά τα αγαθά λαμβάνοντας υπόψιν τους τρεις (3) άξονες:

- Διαθεσιμότητα – Availability (A)
- Ακεραιότητα – Integrity (I)
- Εμπιστευτικότητα - Confidentiality(C)

Ως προς κάθε έναν από αυτούς γίνεται η αρχική εκτίμηση της αξίας των περιουσιακών στοιχείων, η εκτίμηση των απειλών, η εκτίμηση των επιπτώσεων και τελικά ο υπολογισμός της επικινδυνότητας. Συνεπώς η επικινδυνότητα που προκύπτει για κάθε απειλή κάθε αγαθού παρουσιάζεται και ως προς τους τρεις άξονες.

5.2.1 ΑΝΑΓΝΩΡΙΣΗ ΚΑΙ ΑΠΟΤΙΜΗΣΗ ΑΓΑΘΩΝ

Το πρώτο στάδιο στην ανάλυση επικινδυνότητας σύμφωνα με την μεθοδολογία MAGERIT είναι η αναγνώριση και η αποτίμηση της αξίας των περιουσιακών στοιχείων (assets). Το εργαλείο PILAR παρέχει τις κατηγορίες για την ταξινόμηση των αγαθών και πλήθος υποκατηγοριών. Τα περιουσιακά στοιχεία καταχωρήθηκαν στο εργαλείο PILAR ανά κατηγορία και προσδιορίστηκε η αξία τους. Για την αποτίμηση της αξίας των αγαθών διενεργήθηκαν συνεντεύξεις και συμπλήρωση συγκεκριμένων ερωτηματολογίων από τα άτομα που καταλαμβάνουν συγκεκριμένες θέσεις ευθύνης στο εξεταζόμενο οργανισμό. Τα περιουσιακά στοιχεία και η αξία που αποδόθηκε παρουσιάζονται στο διάγραμμα του **ΠΑΡΑΡΤΗΜΑΤΟΣ Β.**

5.2.2 ΧΑΡΑΚΤΗΡΙΣΜΟΣ ΚΑΙ ΕΚΤΙΜΗΣΗ ΑΠΕΙΛΩΝ

Το δεύτερο στάδιο στην ανάλυση επικινδυνότητας είναι ο χαρακτηρισμός και η εκτίμηση των απειλών (threats). Το εργαλείο αυτό ταξινομεί τις απειλές σε πέντε κατηγορίες. Στα πλαίσια της μελέτης του συγκεκριμένου οργανισμού χρησιμοποιούνται οι τρεις από αυτές:

[I] – Industrial (Βιομηχανικές)
[E] – Errors and unintentional failures (Λάθη και ακούσιες αποτυχίες)
[A] – Willful attacks (Ηθελημένες επιθέσεις)

Ανάλογα με την κατηγορία στην οποία καταχωρήθηκαν τα αγαθά, το εργαλείο προτείνει συγκεκριμένες απειλές για κάθε αγαθό. Για κάθε μια απειλή υπολογίζεται αυτόματα από το εργαλείο PILAR η πιθανότητα εμφάνισης και εκτιμάται η υποτίμηση/υποβάθμιση της αξίας ενός αγαθού λόγω της απειλής. Στο **ΠΑΡΑΡΤΗΜΑ Γ** παρουσιάζονται για κάθε αγαθό οι απειλές από τις οποίες κινδυνεύει , η συχνότητα εμφάνισης αυτών (κλίμακα 1 – 10) και η συνέπεια από την υποβάθμιση της αξίας τους (σε ποσοστό επί τοις εκατό % ως προς τους τρεις άξονες (Διαθεσιμότητα, Ακεραιότητα, Εμπιστευτικότητα).

5.2.3 ΕΚΤΙΜΗΣΗ ΕΠΙΠΤΩΣΕΩΝ

Στη συνέχεια ακολουθεί η εκτίμηση των επιπτώσεων (impact). Εκτιμάται δηλαδή η ζημία που προκλήθηκε σε κάποιο αγαθό από την εμφάνιση μιας απειλής. Καθώς έχει προσδιοριστεί ήδη η αξία των αγαθών και η υποβάθμιση λόγω των απειλών, είναι εύκολος ο υπολογισμός της επίπτωσης. Το εργαλείο PILAR υπολογίζει την επίπτωση για κάθε αγαθό ανά απειλή και ως προς τους τρεις άξονες (Διαθεσιμότητα, Ακεραιότητα, Εμπιστευτικότητα). Η κλίμακα του επιπέδου επίπτωσης από το εργαλείο PILAR είναι από 0 έως 10. Συγκεκριμένα η αντιστοίχιση του επιπέδου επίπτωσης όπως αυτό έχει

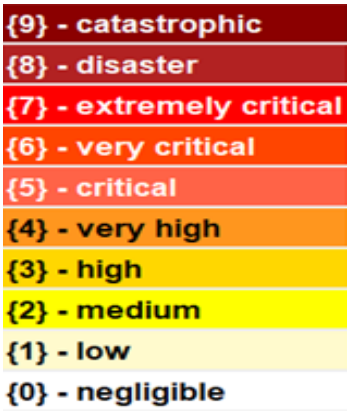
οριστεί από την MAGERIT και το εργαλείο PILAR με την εννοιολογική της περιγραφή είναι:

{0} Αμελητέα	{4} Μέτρια	{8} Πολύ μεγάλη επίπτωση
{1} Χαμηλή	{5} Επίπεδο 5	{9} Κρίσιμη επίπτωση
{2}Επίπεδο 2	{6} Επίπεδο 6	{10}Καταστροφική επίπτωση
{3} Επίπεδο 3	{7} Υψηλή	

Στο **ΠΑΡΑΡΤΗΜΑ Δ** παρουσιάζονται οι πίνακες με την εκτίμηση των επιπτώσεων για κάθε περιουσιακό στοιχείο ανά απειλή και ως προς τους τρεις άξονες (Διαθεσιμότητα, Ακεραιότητα, Εμπιστευτικότητα).

5.3.3 ΕΚΤΙΜΗΣΗ ΕΠΙΚΙΝΔΥΝΟΤΗΤΑΣ

Αυτό είναι το τελευταίο στάδιο στην ανάλυση της επικινδυνότητας σύμφωνα με τη μεθοδολογία MAGERIT στο οποίο πραγματοποιείται ο υπολογισμός του κινδύνου. Με τον κίνδυνο εκτιμάται η πιθανή βλάβη σε κάθε αγαθό από κάθε απειλή. Υπολογίζεται λαμβάνοντας υπόψη την επίπτωση από το προηγούμενο στάδιο και τη συχνότητα εμφάνισης. Σύμφωνα με τη μεθοδολογία MAGERIT και το εργαλείο PILAR το επίπεδο επικινδυνότητας εκτιμάται σε κλίμακα από μηδέν έως εννέα. Παρακάτω φαίνεται η αντιστοίχιση του επιπέδου επικινδυνότητας όπως αυτό έχει οριστεί από το εργαλείο PILAR με την εννοιολογική περιγραφή και σύμφωνα με τον χρωματικό κώδικα.



Στη συνέχεια παραθέτονται οι πίνακες επικινδυνότητας για κάθε αγαθό. Σε κάθε αγαθό εκτιμάται η επικινδυνότητα ως προς κάθε απειλή και ως προς τους τρεις άξονες (Διαθεσιμότητα - A, Ακεραιότητα - I, Εμπιστευτικότητα - C). Στην πρώτη στήλη παρουσιάζονται οι απειλές κάθε αγαθού κατηγοριοποιημένες στις 3 κατηγορίες απειλών [I* - Βιομηχανικές, E* Λάθη ή ακούσιες αποτυχίες, A* Ηθελημένες επιθέσεις]. Στην δεύτερη στήλη παρατίθεται ο κίνδυνος ως προς τον άξονα της Διαθεσιμότητας, στην τρίτη ως προς τον άξονα της Ακεραιότητας και στην τέταρτη ως προς τον άξονα της Εμπιστευτικότητας.

asset	[A]	[I]	[C]
[1.1] Active Directory Primary PC	{5.4}	{3.3}	{4.5}
⚠ [I.5] Hardware or software failure	{4.5}		
⚠ [E.23] Defects in hardware maintenance / upda	{3.3}		
⚠ [E.24] System failure due to exhaustion of res	{5.4}		
⚠ [E.25] Equipment loss	{5.1}		{4.5}
⚠ [A.11] Unauthorised access	{3.3}	{3.3}	{4.5}
⚠ [A.23] Hardware manipulation	{4.3}		{4.3}
⚠ [A.24] Denial of service	{5.3}		
⚠ [A.25] Theft	{4.8}		{4.3}
⚠ [A.26] Destructive attack	{5.1}		

ΠΙΝΑΚΑΣ 6: Risk - Active Directory Primary PC – MAGERIT

Το Active Directory Primary PC έχει κρίσιμο επίπεδο κινδύνου ως προς Αποτυχία συστήματος λόγω εξάντλησης πόρων [A], την Απώλεια εξοπλισμού [A], την Άρνηση υπηρεσίας [A] και τις Καταστροφικές επιθέσεις [A].

asset	[A]	[I]	[C]
[1.2] Active Directory Secondary PC	{3.7}	{2.1}	{4.5}
⚠ [I.5] Hardware or software failure	{2.8}		
⚠ [E.23] Defects in hardware maintenance / upda	{1.5}		
⚠ [E.24] System failure due to exhaustion of res	{3.7}		
⚠ [E.25] Equipment loss	{3.3}		{4.5}
⚠ [A.11] Unauthorised access	{1.5}	{2.1}	{4.5}
⚠ [A.23] Hardware manipulation	{2.5}		{4.3}
⚠ [A.24] Denial of service	{3.6}		
⚠ [A.25] Theft	{3.0}		{4.3}
⚠ [A.26] Destructive attack	{3.3}		

ΠΙΝΑΚΑΣ 7: Risk - Active Directory Secondary PC – MAGERIT

Το Active Directory Secondary PC εμφανίζει πολύ υψηλό κίνδυνο ως προς την Απώλεια εξοπλισμού [C], την Μη εξουσιοδοτημένη πρόσβαση [C], τον Χειρισμό του υλικού και την κλοπή [C].

asset	[A]	[I]	[C]
[1.3] ERP DB	{5.4}	{5.1}	{5.1}
⚠ [I.5] Hardware or software failure	{4.5}		
⚠ [E.23] Defects in hardware maintenance / upda	{3.3}		
⚠ [E.24] System failure due to exhaustion of res	{5.4}		
⚠ [E.25] Equipment loss	{5.1}		{5.1}
⚠ [A.6] Abuse of access privileges	{3.3}	{5.1}	{5.1}
⚠ [A.7] Misuse	{3.3}	{3.3}	{5.1}
⚠ [A.11] Unauthorised access		{5.1}	{5.1}
⚠ [A.24] Denial of service	{5.3}		
⚠ [A.25] Theft	{4.8}		{4.8}
⚠ [A.26] Destructive attack	{5.1}		

ΠΙΝΑΚΑΣ 8: Risk – ERP Database – MAGERIT

Η βάση δεδομένων ERP εμφανίζει κρίσιμο κίνδυνο ως προς την Αποτυχία συστήματος λόγω έλλειψης πόρων [A], την Απώλεια εξοπλισμού[A,C], την Κατάχρηση δικαιωμάτων πρόσβασης [I,C], την Μη εξουσιοδοτημένη πρόσβαση [I,C], την Κακή χρήση [C], την Άρνηση υπηρεσίας [A] και τις Καταστροφικές επιθέσεις [A].

asset	[A]	[I]	[C]
[1.4] MTMS DB	{4.2}	{5.1}	{5.1}
⚠ [I.5] Hardware or software failure	{3.4}		
⚠ [E.23] Defects in hardware maintenance / upda	{2.1}		
⚠ [E.24] System failure due to exhaustion of res	{4.2}		
⚠ [E.25] Equipment loss	{3.9}		{5.1}
⚠ [A.6] Abuse of access privileges	{2.1}	{5.1}	{5.1}
⚠ [A.7] Misuse	{2.1}	{3.3}	{5.1}
⚠ [A.11] Unauthorised access		{5.1}	{5.1}
⚠ [A.24] Denial of service	{4.2}		
⚠ [A.25] Theft	{3.6}		{4.8}
⚠ [A.26] Destructive attack	{3.9}		

ΠΙΝΑΚΑΣ 9: Risk – MTMS Database – MAGERIT

Η βάση δεδομένων MTMS DB παρουσιάζει κρίσιμο επίπεδο κινδύνου ως προς την Απώλεια εξοπλισμού [C], την Κατάχρηση δικαιωμάτων πρόσβασης [I,C] και την Μη εξουσιοδοτημένη πρόσβαση [I, C].

asset	[A]	[I]	[C]
[2.1] MTMS COM	{5.4}	{3.3}	{4.5}
⚠ [I.5] Hardware or software failure	{4.5}		
⚠ [E.23] Defects in hardware maintenance / upda	{3.3}		
⚠ [E.24] System failure due to exhaustion of res	{5.4}		
⚠ [E.25] Equipment loss	{5.1}		{4.5}
⚠ [A.11] Unauthorised access	{3.3}	{3.3}	{4.5}
⚠ [A.23] Hardware manipulation	{4.3}		{4.3}
⚠ [A.24] Denial of service	{5.3}		
⚠ [A.25] Theft	{4.8}		{4.3}
⚠ [A.26] Destructive attack	{5.1}		

ΠΙΝΑΚΑΣ 10: Risk – MTMS COM – MAGERIT

Ο server MTMS COM παρουσιάζει κρίσιμο επίπεδο κινδύνου ως προς την Αποτυχία συστήματος εξαιτίας εξάντλησης πόρων [A], την Απώλεια εξοπλισμού [A, C], την Άρνηση υπηρεσίας [A] και τις Καταστροφικές επιθέσεις [A]. Ακόμα παρουσιάζει πολύ υψηλό επίπεδο κινδύνου ως προς την Μη εξουσιοδοτημένη πρόσβαση [C], τον Χειρισμό του υλικού [C] και την Κλοπή [C].

asset	[A]	[I]	[C]
[2.2] Ingestate	{5.4}	{3.3}	{4.5}
⚠ [I.5] Hardware or software failure	{4.5}		
⚠ [E.23] Defects in hardware maintenance / upda	{3.3}		
⚠ [E.24] System failure due to exhaustion of res	{5.4}		
⚠ [E.25] Equipment loss	{5.1}		{4.5}
⚠ [A.11] Unauthorised access	{3.3}	{3.3}	{4.5}
⚠ [A.23] Hardware manipulation	{4.3}		{4.3}
⚠ [A.24] Denial of service	{5.3}		
⚠ [A.25] Theft	{4.8}		{4.3}
⚠ [A.26] Destructive attack	{5.1}		

ΠΙΝΑΚΑΣ 11: Risk - Ingestate – MAGERIT

Ο server Ingestate παρουσιάζει κρίσιμο βαθμό κινδύνου ως προς την Αποτυχία συστήματος εξαιτίας εξάντλησης πόρων [A], την Απώλεια εξοπλισμού [A, C], την Άρνηση υπηρεσίας [A] και τις Καταστροφικές επιθέσεις [A]. Ακόμα πολύ υψηλό κίνδυνο εμφανίζουν η Αποτυχία υλικού ή λογισμικού [A], η Μη εξουσιοδοτημένη πρόσβαση [C], ο Χειρισμός του υλικού [A, C] και η Κλοπή [A, C].

asset	[A]	[I]	[C]
[3.1] Domain Controller 1	{4.2}	{2.1}	{2.8}
⚠ [I.8] Communications services failure	{3.4}		
⚠ [E.2] System / Security administrator errors	{2.7}	{2.1}	{2.1}
⚠ [E.9] [Re-]routing errors			{1.5}
⚠ [E.10] Sequence errors		{1.5}	
⚠ [E.15] Accidental alteration of the information		{0.75}	
⚠ [E.19] Information leaks			{1.5}
⚠ [E.24] System failure due to exhaustion of res	{3.4}		
⚠ [A.5] Masquerading of identity		{1.5}	{2.8}
⚠ [A.7] Misuse	{2.1}	{1.5}	{1.5}
⚠ [A.9] [Re-]routing of messages			{1.5}
⚠ [A.10] Sequence alteration		{1.5}	
⚠ [A.11] Unauthorised access		{1.5}	{2.8}
⚠ [A.12] Traffic analysis			{0.86}
⚠ [A.14] Eavesdropping			{0.75}
⚠ [A.15] Deliberate alteration of information		{1.5}	
⚠ [A.18] Destruction of information	{3.4}		
⚠ [A.24] Denial of service	{4.2}		

ΠΙΝΑΚΑΣ 12: Risk – Domain Controller 1 – MAGERIT

Ο ελεγκτής Domain Controller 1 εμφανίζει πολύ υψηλό επίπεδο κινδύνου ως προς την Άρνηση υπηρεσίας [A].

asset	[A]	[I]	[C]
[3.2] Domain Controller 2	{3.7}	{2.1}	{2.8}
⚠ [I.8] Communications services failure	{2.8}		
⚠ [E.2] System / Security administrator errors	{2.1}	{2.1}	{2.1}
⚠ [E.9] [Re-]routing errors			{1.5}
⚠ [E.10] Sequence errors		{1.5}	
⚠ [E.15] Accidental alteration of the information		{0.75}	
⚠ [E.19] Information leaks			{1.5}
⚠ [E.24] System failure due to exhaustion of res	{2.8}		
⚠ [A.5] Masquerading of identity		{1.5}	{2.8}
⚠ [A.7] Misuse	{1.5}	{1.5}	{1.5}
⚠ [A.9] [Re-]routing of messages			{1.5}
⚠ [A.10] Sequence alteration		{1.5}	
⚠ [A.11] Unauthorised access		{1.5}	{2.8}
⚠ [A.12] Traffic analysis			{0.86}
⚠ [A.14] Eavesdropping			{0.75}
⚠ [A.15] Deliberate alteration of information		{1.5}	
⚠ [A.18] Destruction of information	{2.8}		
⚠ [A.24] Denial of service	{3.7}		

ΠΙΝΑΚΑΣ 13: Risk – Domain Controller 2 – MAGERIT

Ο δεύτερος ελεγκτής του δικτύου Domain Controller 2 εμφανίζει υψηλό επίπεδο κινδύνου ως προς την Άρνηση υπηρεσίας [A].

asset	[A]	[I]	[C]
[3.3] LEM	{3.7}	{1.5}	{2.8}
⚠ [I.5] Hardware or software failure	{2.8}		
⚠ [E.23] Defects in hardware maintenance / upda	{1.5}		
⚠ [E.24] System failure due to exhaustion of res	{3.7}		
⚠ [E.25] Equipment loss	{3.3}		{2.8}
⚠ [A.11] Unauthorised access	{1.5}	{1.5}	{2.8}
⚠ [A.23] Hardware manipulation	{2.5}		{2.5}
⚠ [A.24] Denial of service	{3.6}		
⚠ [A.25] Theft	{3.0}		{2.5}
⚠ [A.26] Destructive attack	{3.3}		

ΠΙΝΑΚΑΣ 14: Risk - LEM – MAGERIT

Ο διαχειριστής συμβάντων και ημερολογίου LEM εμφανίζει υψηλό επίπεδο κινδύνου ως προς την Αποτυχία του συστήματος λόγω εξάντλησης πόρων [A], την Απώλεια εξοπλισμού [A], την Κλοπή [A] και τις Καταστροφικές επιθέσεις [A].

asset	[A]	[I]	[C]
[3.4] Windows update	{1.9}	{0.75}	{1.0}
⚠ [I.5] Hardware or software failure	{1.0}		
⚠ [E.23] Defects in hardware maintenance / upda	{0.75}		
⚠ [E.24] System failure due to exhaustion of res	{1.9}		
⚠ [E.25] Equipment loss	{1.5}		{1.0}
⚠ [A.11] Unauthorised access	{0.75}	{0.75}	{1.0}
⚠ [A.23] Hardware manipulation	{0.94}		{0.94}
⚠ [A.24] Denial of service	{1.8}		
⚠ [A.25] Theft	{1.3}		{0.94}
⚠ [A.26] Destructive attack	{1.5}		

ΠΙΝΑΚΑΣ 15: Risk – Windows Update – MAGERIT

Ο server των αναβαθμίσεων Windows update παρουσιάζει αμελητέο έως χαμηλό επίπεδο κινδύνου ανά απειλή.

asset	[A]	[I]	[C]
[3.5] MTMS Web UI	{5.4}	{1.5}	{2.8}
⚠ [I.5] Hardware or software failure	{4.5}		
⚠ [E.23] Defects in hardware maintenance / upda	{3.3}		
⚠ [E.24] System failure due to exhaustion of res	{5.4}		
⚠ [E.25] Equipment loss	{5.1}		{2.8}
⚠ [A.11] Unauthorised access	{3.3}	{1.5}	{2.8}
⚠ [A.23] Hardware manipulation	{4.3}		{2.5}
⚠ [A.24] Denial of service	{5.3}		
⚠ [A.25] Theft	{4.8}		{2.5}
⚠ [A.26] Destructive attack	{5.1}		

ΠΙΝΑΚΑΣ 16: Risk – MTMS Web UI- MAGERIT

Ο server MTMS Web UI για την διεπαφή των χρηστών με το MTMS παρουσιάζει κρίσιμο επίπεδο κινδύνου ως προς την Αποτυχία του συστήματος λόγω εξάντληση πόρων [A], την Απώλεια εξοπλισμού [A], την Άρνηση υπηρεσίας [A] και τις Καταστροφικές επιθέσεις [A]. Ακόμα πολύ υψηλός κίνδυνος σχετίζεται με την Αποτυχία υλικού ή λογισμικού[A] και τον Χειρισμό του υλικού [A].

asset	[A]	[I]	[C]
[3.6] FTPS Client	{2.5}	{1.5}	{1.5}
[I.5] Hardware or software failure	{1.6}		
[E.23] Defects in hardware maintenance / upda	{0.87}		
[E.24] System failure due to exhaustion of res	{2.5}		
[E.25] Equipment loss	{2.1}		{1.5}
[A.6] Abuse of access privileges	{0.87}	{1.5}	{1.5}
[A.7] Misuse	{0.87}	{0.75}	{1.5}
[A.11] Unauthorised access		{1.5}	{1.5}
[A.24] Denial of service	{2.4}		
[A.25] Theft	{1.9}		{1.3}
[A.26] Destructive attack	{2.1}		

ΠΙΝΑΚΑΣ 17: Risk – FTPS Client- MAGERIT

Το αγαθό FTPS Client παρουσιάζει μέτριο επίπεδο κινδύνου ως προς την Αποτυχία του συστήματος λόγω εξάντλησης πόρων [A], την Απώλεια εξοπλισμού [A], την Άρνηση υπηρεσίας [A] και τις Καταστροφικές επιθέσεις [A].

asset	[A]	[I]	[C]
[3.7] Vmware server	{4.2}	{0.87}	{1.6}
[I.5] Hardware or software failure	{3.4}		
[E.23] Defects in hardware maintenance / upda	{2.1}		
[E.24] System failure due to exhaustion of res	{4.2}		
[E.25] Equipment loss	{3.9}		{1.6}
[A.11] Unauthorised access	{2.1}	{0.87}	{1.6}
[A.23] Hardware manipulation	{3.1}		{1.3}
[A.24] Denial of service	{4.2}		
[A.25] Theft	{3.6}		{1.3}
[A.26] Destructive attack	{3.9}		

ΠΙΝΑΚΑΣ 18: Risk – VMware server- MAGERIT

Ο server VMware παρουσιάζει πολύ υψηλό επίπεδο κινδύνου ως προς την προς την Αποτυχία του συστήματος λόγω εξάντλησης πόρων [A] και την Άρνηση υπηρεσίας [A].

asset	[A]	[I]	[C]
[4] Antivirus server	{2.5}	{0.87}	{1.6}
⚠ [I.5] Hardware or software failure	{1.6}		
⚠ [E.23] Defects in hardware maintenance / upda	{0.87}		
⚠ [E.24] System failure due to exhaustion of res	{2.5}		
⚠ [E.25] Equipment loss	{2.1}		{1.6}
⚠ [A.11] Unauthorised access	{0.87}	{0.87}	{1.6}
⚠ [A.23] Hardware manipulation	{1.3}		{1.3}
⚠ [A.24] Denial of service	{2.4}		
⚠ [A.25] Theft	{1.9}		{1.3}
⚠ [A.26] Destructive attack	{2.1}		

ΠΙΝΑΚΑΣ 19: Risk – Antivirus server- MAGERIT

Ο Antivirus server παρουσιάζει μέτριο επίπεδο κινδύνου ως προς την προς την Αποτυχία του συστήματος λόγω εξάντλησης πόρων [A], την Απώλεια εξοπλισμού [A], την Άρνηση υπηρεσίας [A] και τις Καταστροφικές επιθέσεις [A].

asset	[A]	[I]	[C]
[5] Proxy server	{4.2}	{2.1}	{2.8}
⚠ [I.5] Hardware or software failure	{3.4}		
⚠ [E.23] Defects in hardware maintenance / upda	{2.1}		
⚠ [E.24] System failure due to exhaustion of res	{4.2}		
⚠ [E.25] Equipment loss	{3.9}		{2.8}
⚠ [A.11] Unauthorised access	{2.1}	{2.1}	{2.8}
⚠ [A.23] Hardware manipulation	{3.1}		{2.5}
⚠ [A.24] Denial of service	{4.2}		
⚠ [A.25] Theft	{3.6}		{2.5}
⚠ [A.26] Destructive attack	{3.9}		

ΠΙΝΑΚΑΣ 20: Risk – Proxy server- MAGERIT

Ο Proxy server παρουσιάζει πολύ υψηλό επίπεδο κινδύνου ως προς την Αποτυχία του συστήματος λόγω εξάντλησης πόρων [A] και ως προς την Άρνηση υπηρεσίας [A].

asset	[A]	[I]	[C]
[6.1] Admin PC	{3.7}	{2.7}	{2.8}
⚠ [I.5] Hardware or software failure	{2.8}		
⚠ [E.23] Defects in hardware maintenance / upda	{1.5}		
⚠ [E.24] System failure due to exhaustion of reso	{3.7}		
⚠ [E.25] Equipment loss	{1.6}		{2.2}
⚠ [A.7] Misuse	{1.5}	{0.98}	{1.5}
⚠ [A.11] Unauthorised access	{1.5}	{2.7}	{2.8}
⚠ [A.23] Hardware manipulation	{2.5}		{2.5}
⚠ [A.24] Denial of service	{3.6}		
⚠ [A.25] Theft	{1.6}		{2.2}
⚠ [A.26] Destructive attack	{3.3}		

ΠΙΝΑΚΑΣ 21: Risk – Admins PCs MAGERIT

Το αγαθό Admins PCs παρουσιάζει υψηλό επίπεδο κινδύνου ως προς την Αποτυχία του συστήματος λόγω εξάντλησης πόρων [A], την Άρνηση υπηρεσίας [A] και τις Καταστροφικές επιθέσεις [A].

asset	[A]	[I]	[C]
[6.2] Developers PC	{3.7}	{2.7}	{2.8}
⚠ [I.5] Hardware or software failure	{2.8}		
⚠ [E.23] Defects in hardware maintenance / upda	{1.5}		
⚠ [E.24] System failure due to exhaustion of reso	{3.7}		
⚠ [E.25] Equipment loss	{1.6}		{2.2}
⚠ [A.7] Misuse	{1.5}	{0.98}	{1.5}
⚠ [A.11] Unauthorised access	{1.5}	{2.7}	{2.8}
⚠ [A.23] Hardware manipulation	{2.5}		{2.5}
⚠ [A.24] Denial of service	{3.6}		
⚠ [A.25] Theft	{1.6}		{2.2}
⚠ [A.26] Destructive attack	{3.3}		

ΠΙΝΑΚΑΣ 22: Risk – Developers PCs- MAGERIT

Το αγαθό Developers PCs παρουσιάζει υψηλό επίπεδο κινδύνου ως προς την Αποτυχία του συστήματος λόγω εξάντλησης πόρων [A], την Άρνηση υπηρεσίας [A] και τις Καταστροφικές επιθέσεις [A].

asset	[A]	[I]	[C]
[7.1] APV 1600 Node 1	{5.4}	{3.8}	{1.0}
[I.8] Communications services failure	{4.5}		
[E.2] System / Security administrator errors	{3.8}	{3.8}	{0.86}
[E.9] [Re-]routing errors			{0.75}
[E.10] Sequence errors		{3.3}	
[E.15] Accidental alteration of the information		{1.5}	
[E.19] Information leaks			{0.75}
[E.24] System failure due to exhaustion of reso	{4.5}		
[A.5] Masquerading of identity		{3.3}	{1.0}
[A.7] Misuse	{3.3}	{3.3}	{0.75}
[A.9] [Re-]routing of messages			{0.75}
[A.10] Sequence alteration		{3.3}	
[A.11] Unauthorised access		{3.3}	{1.0}
[A.12] Traffic analysis			{0.50}
[A.14] Eavesdropping			{0.40}
[A.15] Deliberate alteration of information		{3.3}	
[A.18] Destruction of information	{4.5}		
[A.24] Denial of service	{5.4}		

ΠΙΝΑΚΑΣ 23: Risk – APV 1600 Node 1- MAGERIT

Ο ελεγκτής/ κόμβος των εφαρμογών APV 1600 Node 1 για τον έλεγχο των σημαντικών εφαρμογών παρουσιάζει κρίσιμο επίπεδο κινδύνου ως προς την Άρνηση υπηρεσίας [A], και πολύ υψηλό ως προς την Αποτυχία των υπηρεσιών επικοινωνιών [A], την Καταστροφή πληροφοριών[A] και την Αποτυχία του συστήματος λόγω εξάντλησης πόρων [A].

asset	[A]	[I]	[C]
[7.2] APV 1600 Node 2	{3.7}	{2.1}	{1.0}
[I.8] Communications services failure	{2.8}		
[E.2] System / Security administrator errors	{2.1}	{2.1}	{0.86}
[E.9] [Re-]routing errors			{0.75}
[E.10] Sequence errors		{1.5}	
[E.15] Accidental alteration of the information		{0.75}	
[E.19] Information leaks			{0.75}
[E.24] System failure due to exhaustion of reso	{2.8}		
[A.5] Masquerading of identity		{1.5}	{1.0}
[A.7] Misuse	{1.5}	{1.5}	{0.75}
[A.9] [Re-]routing of messages			{0.75}
[A.10] Sequence alteration		{1.5}	
[A.11] Unauthorised access		{1.5}	{1.0}
[A.12] Traffic analysis			{0.50}
[A.14] Eavesdropping			{0.40}
[A.15] Deliberate alteration of information		{1.5}	
[A.18] Destruction of information	{2.8}		
[A.24] Denial of service	{3.7}		

ΠΙΝΑΚΑΣ 24 ΠΙΝΑΚΑΣ 25: Risk – APV 1600 Node 2- MAGERIT

Ο ελεγκτής/ κόμβος των εφαρμογών APV 1600 Node 2 για τον έλεγχο των δευτερευόντων εφαρμογών παρουσιάζει υψηλό επίπεδο ως προς την Άρνηση υπηρεσίας[A].

asset	[A]	[I]	[C]
[8.1] Cisco 2960 Node 1	{5.4}	{3.8}	{1.0}
[I.8] Communications services failure	{4.5}		
[E.2] System / Security administrator errors	{3.8}	{3.8}	{0.86}
[E.9] [Re-]routing errors			{0.75}
[E.10] Sequence errors		{3.3}	
[E.15] Accidental alteration of the information		{1.5}	
[E.19] Information leaks			{0.75}
[E.24] System failure due to exhaustion of reso	{4.5}		
[A.5] Masquerading of identity		{3.3}	{1.0}
[A.7] Misuse	{3.3}	{3.3}	{0.75}
[A.9] [Re-]routing of messages			{0.75}
[A.10] Sequence alteration		{3.3}	
[A.11] Unauthorised access		{3.3}	{1.0}
[A.12] Traffic analysis			{0.50}
[A.14] Eavesdropping			{0.40}
[A.15] Deliberate alteration of information		{3.3}	
[A.18] Destruction of information	{4.5}		
[A.24] Denial of service	{5.4}		

ΠΙΝΑΚΑΣ 26 ΠΙΝΑΚΑΣ 27: Risk – Cisco 2960 Node 1- MAGERIT

Ο κόμβος Το Cisco 2960 Node 1 που δρομολογεί τις σημαντικές πληροφορίες μεταξύ των ζωνών παρουσιάζει κρίσιμο επίπεδο κινδύνου ως προς την Άρνηση υπηρεσίας [A] και πολύ υψηλό επίπεδο ως προς Αποτυχία των υπηρεσιών επικοινωνιών [A], την Καταστροφή πληροφοριών[A] και την Αποτυχία του συστήματος λόγω εξάντλησης πόρων[A].

asset	[A]	[I]	[C]
[8.2] Cisco 2960 Node 2	{3.7}	{2.1}	{1.0}
[I.8] Communications services failure	{2.8}		
[E.2] System / Security administrator errors	{2.1}	{2.1}	{0.86}
[E.9] [Re-]routing errors			{0.75}
[E.10] Sequence errors		{1.5}	
[E.15] Accidental alteration of the information		{0.75}	
[E.19] Information leaks			{0.75}
[E.24] System failure due to exhaustion of reso	{2.8}		
[A.5] Masquerading of identity		{1.5}	{1.0}
[A.7] Misuse	{1.5}	{1.5}	{0.75}
[A.9] [Re-]routing of messages			{0.75}
[A.10] Sequence alteration		{1.5}	
[A.11] Unauthorised access		{1.5}	{1.0}
[A.12] Traffic analysis			{0.50}
[A.14] Eavesdropping			{0.40}
[A.15] Deliberate alteration of information		{1.5}	
[A.18] Destruction of information	{2.8}		
[A.24] Denial of service	{3.7}		

ΠΙΝΑΚΑΣ 28 ΠΙΝΑΚΑΣ 29 ΠΙΝΑΚΑΣ 30: Risk – Cisco 2960 Node 2- MAGERIT

Δ Ο κόμβος Το Cisco 2960 Node 1 που δρομολογεί τις σημαντικές πληροφορίες μεταξύ των ζωνών παρουσιάζει κρίσιμο επίπεδο κινδύνου ως προς την Άρνηση υπηρεσίας [A].

asset	[A]	[I]	[C]
[8.3] Checkpoint 4406 Node 1	{4.2}	{2.7}	{1.0}
[I.8] Communications services failure	{3.4}		
[E.2] System / Security administrator errors	{2.7}	{2.7}	{0.86}
[E.9] [Re-]routing errors			{0.75}
[E.10] Sequence errors		{2.1}	
[E.15] Accidental alteration of the information		{0.87}	
[E.19] Information leaks			{0.75}
[E.24] System failure due to exhaustion of reso	{3.4}		
[A.5] Masquerading of identity		{2.1}	{1.0}
[A.7] Misuse	{2.1}	{2.1}	{0.75}
[A.9] [Re-]routing of messages			{0.75}
[A.10] Sequence alteration		{2.1}	
[A.11] Unauthorised access		{2.1}	{1.0}
[A.12] Traffic analysis			{0.50}
[A.14] Eavesdropping			{0.40}
[A.15] Deliberate alteration of information		{2.1}	
[A.18] Destruction of information	{3.4}		
[A.24] Denial of service	{4.2}		

ΠΙΝΑΚΑΣ 31: Risk – Checkpoint 4406 Node 1- MAGERIT

Το Checkpoint 4406 Node 1 για τον έλεγχο της ασφάλειας επικοινωνιών μεταξύ των εφαρμογών του συστήματος παρουσιάζει υψηλό επίπεδο κινδύνου ως προς την Άρνηση Υπηρεσίας[A].

asset	[A]	[I]	[C]
[8.4] Checkpoint 4406 Node 2	{4.2}	{2.7}	{1.0}
[I.8] Communications services failure	{3.4}		
[E.2] System / Security administrator errors	{2.7}	{2.7}	{0.86}
[E.9] [Re-]routing errors			{0.75}
[E.10] Sequence errors		{2.1}	
[E.15] Accidental alteration of the information		{0.87}	
[E.19] Information leaks			{0.75}
[E.24] System failure due to exhaustion of reso	{3.4}		
[A.5] Masquerading of identity		{2.1}	{1.0}
[A.7] Misuse	{2.1}	{2.1}	{0.75}
[A.9] [Re-]routing of messages			{0.75}
[A.10] Sequence alteration		{2.1}	
[A.11] Unauthorised access		{2.1}	{1.0}
[A.12] Traffic analysis			{0.50}
[A.14] Eavesdropping			{0.40}
[A.15] Deliberate alteration of information		{2.1}	
[A.18] Destruction of information	{3.4}		
[A.24] Denial of service	{4.2}		

ΠΙΝΑΚΑΣ 32 ΠΙΝΑΚΑΣ 33 Risk – Checkpoint 4406 Node 2- MAGERIT

Ομοίως το Checkpoint 4406 Node 2 παρουσιάζει υψηλό επίπεδο κινδύνου ως προς την Άρνηση Υπηρεσίας[A].

5.3 ΑΠΟΤΕΛΕΣΜΑΤΑ

Η μεθοδολογία MAGERIT για τον υπολογισμό της επικινδυνότητας μελετά τα αγαθά λαμβάνοντας υπόψιν την τιμή της επίπτωσης κάθε αγαθού για κάθε απειλή ως προς και τους τρεις (3) άξονες (Διαθεσιμότητα, Ακεραιότητα, Εμπιστευτικότητα). Συνεπώς ,η επικινδυνότητα που προκύπτει αφορά κάθε αγαθό ως προς αυτούς τους τρεις άξονες. Μετά τη μελέτη των πινάκων με τα επίπεδα επικινδυνότητας προκύπτουν τα παρακάτω αποτελέσματα ως προς τον κάθε άξονα.

Ως προς τον άξονα της Διαθεσιμότητας [A] κρίσιμο επίπεδο επικινδυνότητας (επίπεδο 5) παρουσιάζουν τα αγαθά Active Directory Primary PC, ERP Database, MTMS COM, Ingestate, MTMS Web UI, APV 1600 Node 1 και Cisco 2960 Node 1. Ακόμη πολύ υψηλό επίπεδο επικινδυνότητας (επίπεδο 4) παρουσιάζουν τα αγαθά MTMS DB, Domain Controller 1, VMware server, Proxy server, Checkpoint 4406 Node 1, Checkpoint 4406 Node 2.

Ως προς τον άξονα της Ακεραιότητας [I] κρίσιμο επίπεδο επικινδυνότητας (επίπεδο 5) παρουσιάζουν τα αγαθά ERP Database και MTMS Database. Ακόμη υψηλό επίπεδο επικινδυνότητας (επίπεδο 3) παρουσιάζουν τα Active Directory Primary PC, Active Directory Secondary PC, MTMS COM, Ingestate, APV 1600 Node 1 και Cisco 2960 Node 1.

Ως προς τον άξονα της Εμπιστευτικότητας [C] κρίσιμο επίπεδο επικινδυνότητας (επίπεδο 5) παρουσιάζουν τα αγαθά ERP Database και MTMS Database. Ακόμη πολύ υψηλό επίπεδο επικινδυνότητας (επίπεδο 4) παρουσιάζουν τα Active Directory Primary PC, Active Directory Secondary PC, MTMS COM και Ingestate.

5. ΣΥΜΠΕΡΑΣΜΑΤΑ

Οι οργανισμοί χρησιμοποιούν την ανάλυση και τη διαχείριση της επικινδυνότητας για να προσδιορίσουν τις απειλές, να αξιολογήσουν τις επιπτώσεις και τους κινδύνους και να προσδιορίσουν και εφαρμόσουν τα κατάλληλα μέτρα ελέγχου και μείωσης των κινδύνων. Με την ανάλυση της επικινδυνότητας η επίτευξη της ασφάλειας δεν είναι πλέον μια γενική έννοια αλλά ορίζεται ως ο περιορισμός των προσδιορισμένων κινδύνων σε αποδεκτά επίπεδα.

Ο συγκεκριμένος οργανισμός επιλέχθηκε για την υλοποίηση της ανάλυσης επικινδυνότητας λόγω της υψηλού επιπέδου κρισιμότητας του. Από τη μελέτη του οργανισμού παρατηρήθηκε ότι αρκετά περιουσιακά στοιχεία έχουν υψηλό επίπεδο επικινδυνότητας. Το επίπεδο επικινδυνότητας υποδεικνύει ποια περιουσιακά στοιχεία πρέπει να προστατευθούν. Για το λόγο αυτό σκόπιμη είναι η αναγνώριση των κατάλληλων μέτρων που μπορούν να οδηγήσουν στην πρόληψη και τον περιορισμό των κινδύνων. Το εργαλείο PILAR εντοπίζει τους τομείς που απαιτούν τη λήψη μέτρων προστασίας και προσφέρει μια βιβλιοθήκη αντιμέτρων για τον περιορισμό των κινδύνων. Στη συγκεκριμένη περίπτωση τα κύρια μέτρα ασφαλείας αφορούν την προστασία του υλικού, την προστασία των επικοινωνιών, την ασφάλεια του εξοπλισμού, τα εργαλεία ασφαλείας και την διαχείριση των περιστατικών παραβίασης της ασφάλειας.

Συμπερασματικά, όταν η υλοποίηση της ανάλυσης και διαχείρισης επικινδυνότητας είναι επιτυχής μπορεί να αποτελέσει τη βάση της αποτελεσματικής ασφαλείας ενός πληροφοριακού συστήματος. Για να εξασφαλιστεί η μέγιστη αξία από την ανάλυση και διαχείριση του κινδύνου η διαδικασία πρέπει να είναι επαναλαμβανόμενη. Τα αγαθά θα επαναξιολογούνται και οι απειλές θα επαναπροσδιορίζονται μετά την μείωση των κινδύνων από τα μέτρα που ελήφθησαν. Με αυτόν τον τρόπο ο κίνδυνος θα περιοριστεί σε αποδεκτά ή ελάχιστα επίπεδα ανάλογα με τους οικονομικούς και ανθρώπινους πόρους που προτίθεται να δαπανήσει ο οργανισμός.

ΒΙΒΛΙΟΓΡΑΦΙΑ

[1] International standard ISO/IEC 27000: 2013 2th edition

[2] MAGERIT – version 2 Methodology for Information Systems Risk Analysis and Management Book I – The Method

[3] Mehari 2010 : Processing guide for risk analysis and management - Club de la securite de l' information francais

[4] Current Established Risk Assessment Methodologies and Tools - Dan Ionita

[5] A comparison of security safeguard selection methods –Thomas Neubauer

[6] Comparison of risk analysis methods: Mehari, Magerit, NIST800-30 and Microsoft's security management guide -2009 International conference on availability, reliability and security.

[7] A Comparative Study of Risk Assessment Methods, MEHARI & CRAMM with a New Formal Model of Risk Assessment (FoMRA) in Information Systems - Imed El Fray

[8] Information Security Risk Assesment- A Practical Approach with a mathematical formulation of risk- International Joyrnal of Computer Applicatios

[9] A Qualitative Risk Analysisand Management Tool – CRAMM - Zeki Yazar

[10] Σωκράτης Κ.Κάτσικας «Ανάλυση, Αποτίμηση και Διαχείριση Επικινδυνότητας Πληροφοριακών Συστημάτων»

[11] Σ.Κάτσικας, Δ. Γριτζαλης «Ασφάλεια Πληροφοριακών Συστημάτων»

[12] Συνεργατική πολυκριτηριακή διαχείριση ασφαλείας πληροφοριακών συστημάτων – Θεόδωρος Ν. Ντούσκας

[13] Ανάλυση και Διαχείριση επικινδυνότητας στα πληροφορικά συστήματα – Γεωργίου Σοφία

[14] Μελέτη μεθόδων ανάλυσης και διαχείρισης επικινδυνότητας και μελέτη μετάβασης από την μέθοδο CRAMM στην μέθοδο Magerit και στα αντίστοιχα εργαλεία - Αντωνίου Γιώργος

[15] Ασφάλεια πληροφοριακών συστημάτων και δικτύων, Γ. Πάγκαλος, Ι. Μαυρίδης «Πολιτικές και Μοντέλα Ασφαλείας ΠΣ»

[16] Διδακτικές σημειώσεις Ασφάλειας Δικτύων και Πληροφοριακών Συστημάτων-ΠΑΠΕΙ

[17] Διδακτικές σημειώσεις :Ανάλυση, Αποτίμηση και Διαχείριση Πληροφοριακών Συστημάτων – Σπύρος Κοκολάκης – Στέφανος Γκρίζαλης Πανεπιστήμιο Αιγαίου

ΠΗΓΕΣ ΑΠΟ ΤΟ ΔΙΑΔΙΚΤΥΟ

[1] https://www.enisa.europa.eu/

[2] https://www.plan42.com/index.php/en/it-security-management/it-grundschutz

[3] https://www.bsi.bund.de/EN/Topics/ITGrundschutz..html

[4] https://repository.kallipos.gr/bitstream/11419/1035/1/05_chapter_11.pdf

[5] http://www.greece.lrqa.com/standards-and-schemes/iso-iec27001

[6] https://en.wikipedia.org/wiki/ISO/IEC_27001

[7] https://en.wikipedia.org/wiki/ISO/IEC_27000-series

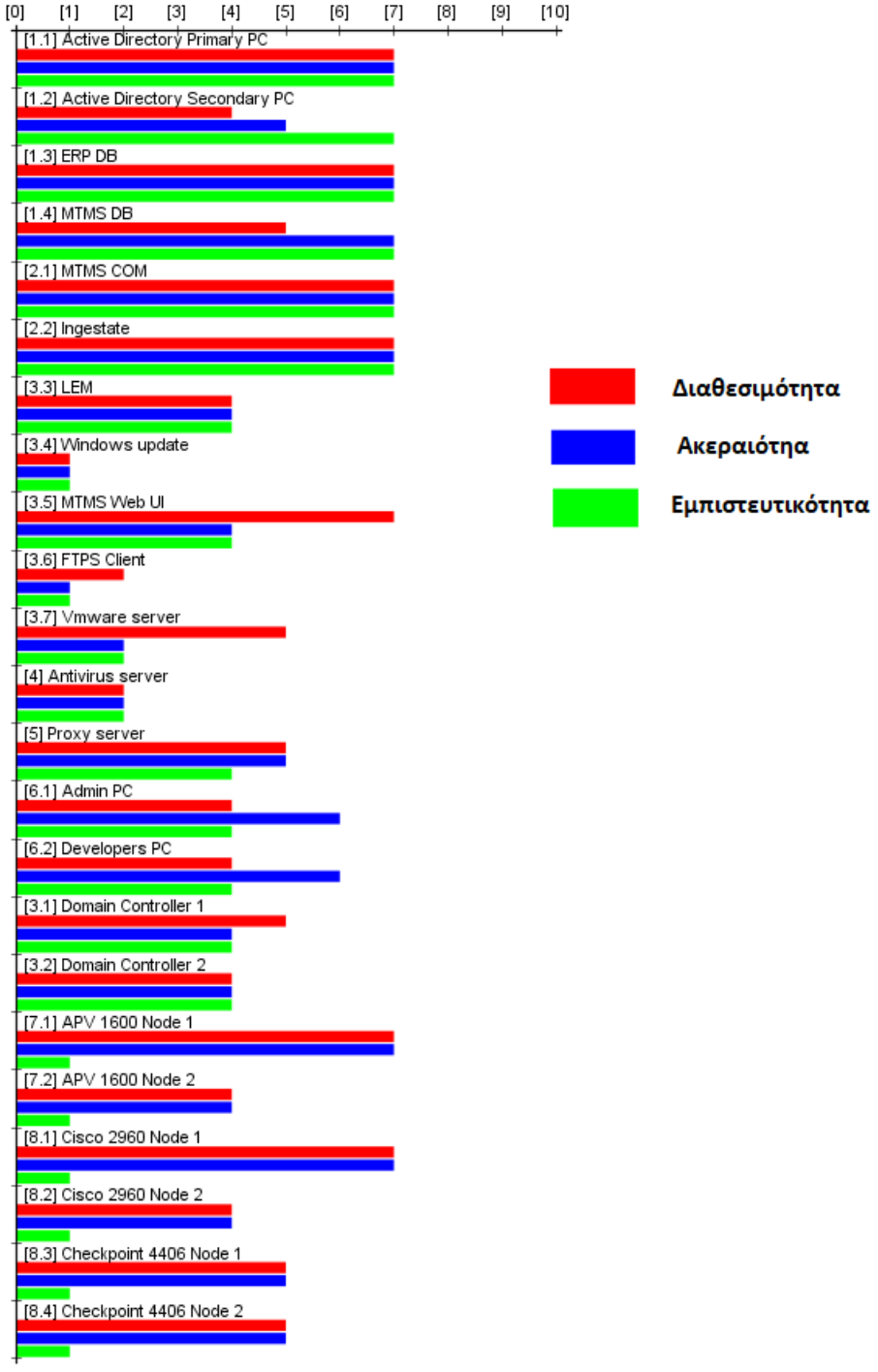
[8] http://www.itworks.lu/risk-analysis

[9] https://www.ar-tools.com/magerit/index.html

ΠΑΡΑΡΤΗΜΑ Α - ΒΑΣΙΚΕΣ ΕΝΝΟΙΕΣ

Αγαθά ή περιουσιακά στοιχεία (Assets)	Οτιδήποτε έχει αξία για τον οργανισμό (δεδομένα, πληροφορίες, υπολογιστικοί πόροι).
Απειλή (Threat)	Μια ενέργεια ή ένα γεγονός που μπορεί να προκαλέσει την απώλεια των χαρακτηριστικών ασφαλείας ενός πληροφοριακού συστήματος.
Επικινδυνότητα (Risk)	Συνάρτηση της αξίας του αγαθού, των απειλών, της σοβαρότητας των αδυναμιών. Είναι ο κίνδυνος να συμβεί ένα γεγονός που θα έχει αρνητική επίπτωση στον οργανισμό.
Εμπιστευτικότητα (Confidentiality)	Πρόσβαση στην πληροφορία μόνο όσων έχουν εξουσιοδότηση.
Ακεραιότητα (Integrity)	Διασφάλιση της ακρίβειας και της πληρότητας της πληροφορίας. Αποφυγή τροποποίησης από μη εξουσιοδοτημένα άτομα.
Διαθεσιμότητα (Availability)	Διάθεση της πληροφορίας σε εξουσιοδοτημένους χρήστες όπου αυτό απαιτείται.
Ζημιά (Damage)	Μερική ή ολική απώλεια της αξίας ενός αγαθού.
Παραβίαση (Breach)	Ένα γεγονός που προσβάλει την ακεραιότητα, τη διαθεσιμότητα, την εμπιστευτικότητα, την αυθεντικότητα ή την ακρίβεια/ πληρότητα της πληροφορίας.
Επίπτωση (Impact)	Η απώλεια μιας αξίας, η αύξηση του κόστους ή κάποια άλλη απώλεια που προκύπτει ως αποτέλεσμα μιας παραβίασης.
Αδυναμία (Vulnerability)	Ένα σημείο του πληροφοριακού συστήματος που μπορεί να επιτρέψει μια παραβίαση.
Περιστατικό (Incident)	Ένα γεγονός που θέτει σε κίνδυνο την ασφάλεια του ΠΣ.
Μέτρο ασφαλείας - Αντίμετρο (Countermeasures)	Ένα μέτρο με σκοπό να μειώσει την ευπάθεια ή αδυναμία του συστήματος , να μειώσει τις επιπτώσεις μιας παραβίασης ή και να αποτρέψει την ίδια την παραβίαση.
Πολιτική ασφαλείας (Security Policy)	Περιγραφή σε υψηλό επίπεδο των αρχών, των κανόνων, των διαδικασιών, των τεχνικών και των μέτρων που προφυλάσσουν από κάθε είδους απειλή τυχαία ή σκόπιμη.

ΠΑΡΑΡΤΗΜΑ Β - ΔΙΑΓΡΑΜΜΑ ΑΞΙΑΣ / ΠΕΡΙΟΥΣΙΑΚΟ ΣΤΟΙΧΕΙΟ



ΠΑΡΑΡΤΗΜΑ Γ- ΠΙΝΑΚΑΣ ΑΠΕΙΛΩΝ/ΠΕΡΙΟΥΣΙΑΚΟ ΣΤΟΙΧΕΙΟ

asset	c...	frequency	[A]	[I]	[C]
[1.1] Active Directory Primary PC			100%	10%	50%
⚠ [I.5] Hardware or software failure		1	50%		
⚠ [E.23] Defects in hardware maintenance / u		1	10%		
⚠ [E.24] System failure due to exhaustion of		10	50%		
⚠ [E.25] Equipment loss		1	100%		50%
⚠ [A.11] Unauthorised access		1	10%	10%	50%
⚠ [A.23] Hardware manipulation		0.5	50%		50%
⚠ [A.24] Denial of service		2	100%		
⚠ [A.25] Theft		0.5	100%		50%
⚠ [A.26] Destructive attack		1	100%		
[1.2] Active Directory Secondary PC			100%	10%	50%
⚠ [I.5] Hardware or software failure		1	50%		
⚠ [E.23] Defects in hardware maintenance / u		1	10%		
⚠ [E.24] System failure due to exhaustion of		10	50%		
⚠ [E.25] Equipment loss		1	100%		50%
⚠ [A.11] Unauthorised access		1	10%	10%	50%
⚠ [A.23] Hardware manipulation		0.5	50%		50%
⚠ [A.24] Denial of service		2	100%		
⚠ [A.25] Theft		0.5	100%		50%
⚠ [A.26] Destructive attack		1	100%		
[1.3] ERP DB			100%	100%	100%
⚠ [I.5] Hardware or software failure		1	50%		
⚠ [E.23] Defects in hardware maintenance / u		1	10%		
⚠ [E.24] System failure due to exhaustion of		10	50%		
⚠ [E.25] Equipment loss		1	100%		100%
⚠ [A.6] Abuse of access privileges		1	10%	100%	100%
⚠ [A.7] Misuse		1	10%	10%	100%
⚠ [A.11] Unauthorised access		1		100%	100%
⚠ [A.24] Denial of service		2	100%		
⚠ [A.25] Theft		0.5	100%		100%
⚠ [A.26] Destructive attack		1	100%		
[1.4] MTMS DB			100%	100%	100%
⚠ [I.5] Hardware or software failure		1	50%		
⚠ [E.23] Defects in hardware maintenance / u		1	10%		
⚠ [E.24] System failure due to exhaustion of		10	50%		
⚠ [E.25] Equipment loss		1	100%		100%
⚠ [A.6] Abuse of access privileges		1	10%	100%	100%
⚠ [A.7] Misuse		1	10%	10%	100%
⚠ [A.11] Unauthorised access		1		100%	100%
⚠ [A.24] Denial of service		2	100%		
⚠ [A.25] Theft		0.5	100%		100%
⚠ [A.26] Destructive attack		1	100%		
[2.1] MTMS COM			100%	10%	50%
⚠ [I.5] Hardware or software failure		1	50%		
⚠ [E.23] Defects in hardware maintenance / u		1	10%		
⚠ [E.24] System failure due to exhaustion of		10	50%		
⚠ [E.25] Equipment loss		1	100%		50%
⚠ [A.11] Unauthorised access		1	10%	10%	50%
⚠ [A.23] Hardware manipulation		0.5	50%		50%
⚠ [A.24] Denial of service		2	100%		
⚠ [A.25] Theft		0.5	100%		50%
⚠ [A.26] Destructive attack		1	100%		

asset	c...	frequency	[A]	[I]	[C]
[2.2] Ingestate			100%	10%	50%
[I.5] Hardware or software failure		1	50%		
[E.23] Defects in hardware maintenance / u		1	10%		
[E.24] System failure due to exhaustion of		10	50%		
[E.25] Equipment loss		1	100%		50%
[A.11] Unauthorised access		1	10%	10%	50%
[A.23] Hardware manipulation		0.5	50%		50%
[A.24] Denial of service		2	100%		
[A.25] Theft		0.5	100%		50%
[A.26] Destructive attack		1	100%		
[3.1] Domain Controller 1			50%	20%	50%
[I.8] Communications services failure		1	50%		
[E.2] System / Security administrator error		1	20%	20%	20%
[E.9] [Re-]routing errors		1			10%
[E.10] Sequence errors		1		10%	
[E.15] Accidental alteration of the informati		1		1%	
[E.19] Information leaks		1			10%
[E.24] System failure due to exhaustion of		1	50%		
[A.5] Masquerading of identity		1		10%	50%
[A.7] Misuse		1	10%	10%	10%
[A.9] [Re-]routing of messages		1			10%
[A.10] Sequence alteration		1		10%	
[A.11] Unauthorised access		1		10%	50%
[A.12] Traffic analysis		1			2%
[A.14] Eavesdropping		1			1%
[A.15] Deliberate alteration of information		1		10%	
[A.18] Destruction of information		1	50%		
[A.24] Denial of service		10	50%		
[3.2] Domain Controller 2			50%	20%	50%
[I.8] Communications services failure		1	50%		
[E.2] System / Security administrator error		1	20%	20%	20%
[E.9] [Re-]routing errors		1			10%
[E.10] Sequence errors		1		10%	
[E.15] Accidental alteration of the informati		1		1%	
[E.19] Information leaks		1			10%
[E.24] System failure due to exhaustion of		1	50%		
[A.5] Masquerading of identity		1		10%	50%
[A.7] Misuse		1	10%	10%	10%
[A.9] [Re-]routing of messages		1			10%
[A.10] Sequence alteration		1		10%	
[A.11] Unauthorised access		1		10%	50%
[A.12] Traffic analysis		1			2%
[A.14] Eavesdropping		1			1%
[A.15] Deliberate alteration of information		1		10%	
[A.18] Destruction of information		1	50%		
[A.24] Denial of service		10	50%		

asset		c...	frequency	[A]	[I]	[C]
[3.3] LEM				100%	10%	50%
[I.5] Hardware or software failure			1	50%		
[E.23] Defects in hardware maintenance / u			1	10%		
[E.24] System failure due to exhaustion of			10	50%		
[E.25] Equipment loss			1	100%		50%
[A.11] Unauthorised access			1	10%	10%	50%
[A.23] Hardware manipulation			0.5	50%		50%
[A.24] Denial of service			2	100%		
[A.25] Theft			0.5	100%		50%
[A.26] Destructive attack			1	100%		
[3.4] Windows update				100%	10%	50%
[I.5] Hardware or software failure			1	50%		
[E.23] Defects in hardware maintenance / u			1	10%		
[E.24] System failure due to exhaustion of			10	50%		
[E.25] Equipment loss			1	100%		50%
[A.11] Unauthorised access			1	10%	10%	50%
[A.23] Hardware manipulation			0.5	50%		50%
[A.24] Denial of service			2	100%		
[A.25] Theft			0.5	100%		50%
[A.26] Destructive attack			1	100%		
[3.5] MTMS Web UI				100%	10%	50%
[I.5] Hardware or software failure			1	50%		
[E.23] Defects in hardware maintenance / u			1	10%		
[E.24] System failure due to exhaustion of			10	50%		
[E.25] Equipment loss			1	100%		50%
[A.11] Unauthorised access			1	10%	10%	50%
[A.23] Hardware manipulation			0.5	50%		50%
[A.24] Denial of service			2	100%		
[A.25] Theft			0.5	100%		50%
[A.26] Destructive attack			1	100%		
[3.6] FTPS Client				100%	100%	100%
[I.5] Hardware or software failure			1	50%		
[E.23] Defects in hardware maintenance / u			1	10%		
[E.24] System failure due to exhaustion of			10	50%		
[E.25] Equipment loss			1	100%		100%
[A.6] Abuse of access privileges			1	10%	100%	100%
[A.7] Misuse			1	10%	10%	100%
[A.11] Unauthorised access			1		100%	100%
[A.24] Denial of service			2	100%		
[A.25] Theft			0.5	100%		100%
[A.26] Destructive attack			1	100%		
[3.7] Vmware server				100%	10%	50%
[I.5] Hardware or software failure			1	50%		
[E.23] Defects in hardware maintenance / u			1	10%		
[E.24] System failure due to exhaustion of			10	50%		
[E.25] Equipment loss			1	100%		50%
[A.11] Unauthorised access			1	10%	10%	50%
[A.23] Hardware manipulation			0.5	50%		50%
[A.24] Denial of service			2	100%		
[A.25] Theft			0.5	100%		50%
[A.26] Destructive attack			1	100%		

asset	c...	frequency	[A]	[I]	[C]
[4] Antivirus server			100%	10%	50%
[I.5] Hardware or software failure		1	50%		
[E.23] Defects in hardware maintenance / u		1	10%		
[E.24] System failure due to exhaustion of		10	50%		
[E.25] Equipment loss		1	100%		50%
[A.11] Unauthorised access		1	10%	10%	50%
[A.23] Hardware manipulation		0.5	50%		50%
[A.24] Denial of service		2	100%		
[A.25] Theft		0.5	100%		50%
[A.26] Destructive attack		1	100%		
[5] Proxy server			100%	10%	50%
[I.5] Hardware or software failure		1	50%		
[E.23] Defects in hardware maintenance / u		1	10%		
[E.24] System failure due to exhaustion of		10	50%		
[E.25] Equipment loss		1	100%		50%
[A.11] Unauthorised access		1	10%	10%	50%
[A.23] Hardware manipulation		0.5	50%		50%
[A.24] Denial of service		2	100%		
[A.25] Theft		0.5	100%		50%
[A.26] Destructive attack		1	100%		
[6.1] Admin PC			100%	10%	50%
[I.5] Hardware or software failure		1	50%		
[E.23] Defects in hardware maintenance / u		1	10%		
[E.24] System failure due to exhaustion of		10	50%		
[E.25] Equipment loss		5	5%		10%
[A.7] Misuse		1	10%	1%	10%
[A.11] Unauthorised access		1	10%	10%	50%
[A.23] Hardware manipulation		0.5	50%		50%
[A.24] Denial of service		2	100%		
[A.25] Theft		5	5%		10%
[A.26] Destructive attack		1	100%		
[6.2] Developers PC			100%	10%	50%
[I.5] Hardware or software failure		1	50%		
[E.23] Defects in hardware maintenance / u		1	10%		
[E.24] System failure due to exhaustion of		10	50%		
[E.25] Equipment loss		5	5%		10%
[A.7] Misuse		1	10%	1%	10%
[A.11] Unauthorised access		1	10%	10%	50%
[A.23] Hardware manipulation		0.5	50%		50%
[A.24] Denial of service		2	100%		
[A.25] Theft		5	5%		10%
[A.26] Destructive attack		1	100%		

asset		c...	frequency	[A]	[I]	[C]
[7.1] APV 1600 Node 1				50%	20%	50%
[I.8] Communications services failure			1	50%		
[E.2] System / Security administrator error			1	20%	20%	20%
[E.9] [Re-]routing errors			1			10%
[E.10] Sequence errors			1		10%	
[E.15] Accidental alteration of the informati			1		1%	
[E.19] Information leaks			1			10%
[E.24] System failure due to exhaustion of			1	50%		
[A.5] Masquerading of identity			1		10%	50%
[A.7] Misuse			1	10%	10%	10%
[A.9] [Re-]routing of messages			1			10%
[A.10] Sequence alteration			1		10%	
[A.11] Unauthorised access			1		10%	50%
[A.12] Traffic analysis			1			2%
[A.14] Eavesdropping			1			1%
[A.15] Deliberate alteration of information			1		10%	
[A.18] Destruction of information			1	50%		
[A.24] Denial of service			10	50%		
[7.2] APV 1600 Node 2				50%	20%	50%
[I.8] Communications services failure			1	50%		
[E.2] System / Security administrator error			1	20%	20%	20%
[E.9] [Re-]routing errors			1			10%
[E.10] Sequence errors			1		10%	
[E.15] Accidental alteration of the informati			1		1%	
[E.19] Information leaks			1			10%
[E.24] System failure due to exhaustion of			1	50%		
[A.5] Masquerading of identity			1		10%	50%
[A.7] Misuse			1	10%	10%	10%
[A.9] [Re-]routing of messages			1			10%
[A.10] Sequence alteration			1		10%	
[A.11] Unauthorised access			1		10%	50%
[A.12] Traffic analysis			1			2%
[A.15] Deliberate alteration of information			1		10%	
[A.18] Destruction of information			1	50%		
[A.24] Denial of service			10	50%		
[8.1] Cisco 2960 Node 1				50%	20%	50%
[I.8] Communications services failure			1	50%		
[E.2] System / Security administrator error			1	20%	20%	20%
[E.9] [Re-]routing errors			1			10%
[E.10] Sequence errors			1		10%	
[E.15] Accidental alteration of the informati			1		1%	
[E.19] Information leaks			1			10%
[E.24] System failure due to exhaustion of			1	50%		
[A.5] Masquerading of identity			1		10%	50%
[A.7] Misuse			1	10%	10%	10%
[A.9] [Re-]routing of messages			1			10%
[A.10] Sequence alteration			1		10%	
[A.11] Unauthorised access			1		10%	50%
[A.12] Traffic analysis			1			2%
[A.14] Eavesdropping			1			1%
[A.15] Deliberate alteration of information			1		10%	
[A.18] Destruction of information			1	50%		
[A.24] Denial of service			10	50%		

asset	c...	frequency	[A]	[I]	[C]
[8.2] Cisco 2960 Node 2			50%	20%	50%
[I.8] Communications services failure		1	50%		
[E.2] System / Security administrator error		1	20%	20%	20%
[E.9] [Re-]routing errors		1			10%
[E.10] Sequence errors		1		10%	
[E.15] Accidental alteration of the informati		1		1%	
[E.19] Information leaks		1			10%
[E.24] System failure due to exhaustion of		1	50%		
[A.5] Masquerading of identity		1		10%	50%
[A.7] Misuse		1	10%	10%	10%
[A.9] [Re-]routing of messages		1			10%
[A.10] Sequence alteration		1		10%	
[A.11] Unauthorised access		1		10%	50%
[A.12] Traffic analysis		1			2%
[A.14] Eavesdropping		1			1%
[A.15] Deliberate alteration of information		1		10%	
[A.18] Destruction of information		1	50%		
[A.24] Denial of service		10	50%		
[8.3] Checkpoint 4406 Node 1			50%	20%	50%
[I.8] Communications services failure		1	50%		
[E.2] System / Security administrator error		1	20%	20%	20%
[E.9] [Re-]routing errors		1			10%
[E.10] Sequence errors		1		10%	
[E.15] Accidental alteration of the informati		1		1%	
[E.19] Information leaks		1			10%
[E.24] System failure due to exhaustion of		1	50%		
[A.5] Masquerading of identity		1		10%	50%
[A.7] Misuse		1	10%	10%	10%
[A.9] [Re-]routing of messages		1			10%
[A.10] Sequence alteration		1		10%	
[A.11] Unauthorised access		1		10%	50%
[A.12] Traffic analysis		1			2%
[A.14] Eavesdropping		1			1%
[A.15] Deliberate alteration of information		1		10%	
[A.18] Destruction of information		1	50%		
[A.24] Denial of service		10	50%		
[8.4] Checkpoint 4406 Node 2			50%	20%	50%
[I.8] Communications services failure		1	50%		
[E.2] System / Security administrator error		1	20%	20%	20%
[E.9] [Re-]routing errors		1			10%
[E.10] Sequence errors		1		10%	
[E.15] Accidental alteration of the informati		1		1%	
[E.19] Information leaks		1			10%
[E.24] System failure due to exhaustion of		1	50%		
[A.5] Masquerading of identity		1		10%	50%
[A.7] Misuse		1	10%	10%	10%
[A.9] [Re-]routing of messages		1			10%
[A.10] Sequence alteration		1		10%	
[A.11] Unauthorised access		1		10%	50%
[A.12] Traffic analysis		1			2%
[A.14] Eavesdropping		1			1%
[A.15] Deliberate alteration of information		1		10%	
[A.18] Destruction of information		1	50%		
[A.24] Denial of service		10	50%		

ΠΑΡΑΡΤΗΜΑ Δ- ΠΙΝΑΚΑΣ ΕΠΙΠΤΩΣΗΣ/ ΠΕΡΙΟΥΣΙΚΟ ΣΤΟΙΧΕΙΟ

P impact

[10] Level 10
[9] Level 9
[8] Level 8
[7] High
[6] Level 6
[5] Level 5
[4] Medium
[3] Level 3
[2] Level 2
[1] Low
[0] Negligible

asset	[A]	[I]	[C]
[1.1] Active Directory Primary PC	[7]	[4]	[6]
[I.5] Hardware or software failure	[6]		
[E.23] Defects in hardware maintenance / upda	[4]		
[E.24] System failure due to exhaustion of reso	[6]		
[E.25] Equipment loss	[7]		[6]
[A.11] Unauthorised access	[4]	[4]	[6]
[A.23] Hardware manipulation	[6]		[6]
[A.24] Denial of service	[7]		
[A.25] Theft	[7]		[6]
[A.26] Destructive attack	[7]		
[1.2] Active Directory Secondary PC	[4]	[2]	[6]
[I.5] Hardware or software failure	[3]		
[E.23] Defects in hardware maintenance / upda	[1]		
[E.24] System failure due to exhaustion of reso	[3]		
[E.25] Equipment loss	[4]		[6]
[A.11] Unauthorised access	[1]	[2]	[6]
[A.23] Hardware manipulation	[3]		[6]
[A.24] Denial of service	[4]		
[A.25] Theft	[4]		[6]
[A.26] Destructive attack	[4]		
[1.3] ERP DB	[7]	[7]	[7]
[I.5] Hardware or software failure	[6]		
[E.23] Defects in hardware maintenance / upda	[4]		
[E.24] System failure due to exhaustion of reso	[6]		
[E.25] Equipment loss	[7]		[7]
[A.6] Abuse of access privileges	[4]	[7]	[7]
[A.7] Misuse	[4]	[4]	[7]
[A.11] Unauthorised access		[7]	[7]
[A.24] Denial of service	[7]		
[A.25] Theft	[7]		[7]
[A.26] Destructive attack	[7]		
[1.4] MTMS DB	[5]	[7]	[7]
[I.5] Hardware or software failure	[4]		
[E.23] Defects in hardware maintenance / upda	[2]		
[E.24] System failure due to exhaustion of reso	[4]		
[E.25] Equipment loss	[5]		[7]
[A.6] Abuse of access privileges	[2]	[7]	[7]
[A.7] Misuse	[2]	[4]	[7]
[A.11] Unauthorised access		[7]	[7]
[A.24] Denial of service	[5]		
[A.25] Theft	[5]		[7]
[A.26] Destructive attack	[5]		
[2.1] MTMS COM	[7]	[4]	[6]
[I.5] Hardware or software failure	[6]		
[E.23] Defects in hardware maintenance / upda	[4]		
[E.24] System failure due to exhaustion of reso	[6]		
[E.25] Equipment loss	[7]		[6]
[A.11] Unauthorised access	[4]	[4]	[6]
[A.23] Hardware manipulation	[6]		[6]
[A.24] Denial of service	[7]		
[A.25] Theft	[7]		[6]
[A.26] Destructive attack	[7]		

asset	[A]	[I]	[C]
[2.2] Ingestate	[7]	[4]	[6]
⚠ [I.5] Hardware or software failure	[6]		
⚠ [E.23] Defects in hardware maintenance / upda	[4]		
⚠ [E.24] System failure due to exhaustion of reso	[6]		
⚠ [E.25] Equipment loss	[7]		[6]
⚠ [A.11] Unauthorised access	[4]	[4]	[6]
⚠ [A.23] Hardware manipulation	[6]		[6]
⚠ [A.24] Denial of service	[7]		
⚠ [A.25] Theft	[7]		[6]
⚠ [A.26] Destructive attack	[7]		
[3.1] Domain Controller 1	[4]	[2]	[3]
⚠ [I.8] Communications services failure	[4]		
⚠ [E.2] System / Security administrator errors	[3]	[2]	[2]
⚠ [E.9] [Re-]routing errors			[1]
⚠ [E.10] Sequence errors		[1]	
⚠ [E.15] Accidental alteration of the information		[0]	
⚠ [E.19] Information leaks			[1]
⚠ [E.24] System failure due to exhaustion of reso	[4]		
⚠ [A.5] Masquerading of identity		[1]	[3]
⚠ [A.7] Misuse	[2]	[1]	[1]
⚠ [A.9] [Re-]routing of messages			[1]
⚠ [A.10] Sequence alteration		[1]	
⚠ [A.11] Unauthorised access		[1]	[3]
⚠ [A.12] Traffic analysis			[0]
⚠ [A.14] Eavesdropping			[0]
⚠ [A.15] Deliberate alteration of information		[1]	
⚠ [A.18] Destruction of information	[4]		
⚠ [A.24] Denial of service	[4]		
[3.2] Domain Controller 2	[3]	[2]	[3]
⚠ [I.8] Communications services failure	[3]		
⚠ [E.2] System / Security administrator errors	[2]	[2]	[2]
⚠ [E.9] [Re-]routing errors			[1]
⚠ [E.10] Sequence errors		[1]	
⚠ [E.15] Accidental alteration of the information		[0]	
⚠ [E.19] Information leaks			[1]
⚠ [E.24] System failure due to exhaustion of reso	[3]		
⚠ [A.5] Masquerading of identity		[1]	[3]
⚠ [A.7] Misuse	[1]	[1]	[1]
⚠ [A.9] [Re-]routing of messages			[1]
⚠ [A.10] Sequence alteration		[1]	
⚠ [A.11] Unauthorised access		[1]	[3]
[3.3] LEM	[4]	[1]	[3]
⚠ [I.5] Hardware or software failure	[3]		
⚠ [E.23] Defects in hardware maintenance / upda	[1]		
⚠ [E.24] System failure due to exhaustion of reso	[3]		
⚠ [E.25] Equipment loss	[4]		[3]
⚠ [A.11] Unauthorised access	[1]	[1]	[3]
⚠ [A.23] Hardware manipulation	[3]		[3]
⚠ [A.24] Denial of service	[4]		
⚠ [A.25] Theft	[4]		[3]
⚠ [A.26] Destructive attack	[4]		

asset	[A]	[I]	[C]
[3.4] Windows update	[1]	[0]	[0]
⚠ [I.5] Hardware or software failure	[0]		
⚠ [E.23] Defects in hardware maintenance / upda	[0]		
⚠ [E.24] System failure due to exhaustion of reso	[0]		
⚠ [E.25] Equipment loss	[1]		[0]
⚠ [A.11] Unauthorised access	[0]	[0]	[0]
⚠ [A.23] Hardware manipulation	[0]		[0]
⚠ [A.24] Denial of service	[1]		
⚠ [A.25] Theft	[1]		[0]
⚠ [A.26] Destructive attack	[1]		
[3.5] MTMS Web UI	[7]	[1]	[3]
⚠ [I.5] Hardware or software failure	[6]		
⚠ [E.23] Defects in hardware maintenance / upda	[4]		
⚠ [E.24] System failure due to exhaustion of reso	[6]		
⚠ [E.25] Equipment loss	[7]		[3]
⚠ [A.11] Unauthorised access	[4]	[1]	[3]
⚠ [A.23] Hardware manipulation	[6]		[3]
⚠ [A.24] Denial of service	[7]		
⚠ [A.25] Theft	[7]		[3]
⚠ [A.26] Destructive attack	[7]		
[3.6] FTPS Client	[2]	[1]	[1]
⚠ [I.5] Hardware or software failure	[1]		
⚠ [E.23] Defects in hardware maintenance / upda	[0]		
⚠ [E.24] System failure due to exhaustion of reso	[1]		
⚠ [E.25] Equipment loss	[2]		[1]
⚠ [A.6] Abuse of access privileges	[0]	[1]	[1]
⚠ [A.7] Misuse	[0]	[0]	[1]
⚠ [A.11] Unauthorised access		[1]	[1]
⚠ [A.24] Denial of service	[2]		
⚠ [A.25] Theft	[2]		[1]
⚠ [A.26] Destructive attack	[2]		
[3.7] Vmware server	[5]	[0]	[1]
⚠ [I.5] Hardware or software failure	[4]		
⚠ [E.23] Defects in hardware maintenance / upda	[2]		
⚠ [E.24] System failure due to exhaustion of reso	[4]		
⚠ [E.25] Equipment loss	[5]		[1]
⚠ [A.11] Unauthorised access	[2]	[0]	[1]
⚠ [A.23] Hardware manipulation	[4]		[1]
⚠ [A.24] Denial of service	[5]		
⚠ [A.25] Theft	[5]		[1]
⚠ [A.26] Destructive attack	[5]		
[4] Antivirus server	[2]	[0]	[1]
⚠ [I.5] Hardware or software failure	[1]		
⚠ [E.23] Defects in hardware maintenance / upda	[0]		
⚠ [E.24] System failure due to exhaustion of reso	[1]		
⚠ [E.25] Equipment loss	[2]		[1]
⚠ [A.11] Unauthorised access	[0]	[0]	[1]
⚠ [A.23] Hardware manipulation	[1]		[1]
⚠ [A.24] Denial of service	[2]		
⚠ [A.25] Theft	[2]		[1]
⚠ [A.26] Destructive attack	[2]		

asset	[A]	[I]	[C]
[5] Proxy server	[5]	[2]	[3]
[I.5] Hardware or software failure	[4]		
[E.23] Defects in hardware maintenance / upda	[2]		
[E.24] System failure due to exhaustion of reso	[4]		
[E.25] Equipment loss	[5]		[3]
[A.11] Unauthorised access	[2]	[2]	[3]
[A.23] Hardware manipulation	[4]		[3]
[A.24] Denial of service	[5]		
[A.25] Theft	[5]		[3]
[A.26] Destructive attack	[5]		
[6.1] Admin PC	[4]	[3]	[3]
[I.5] Hardware or software failure	[3]		
[E.23] Defects in hardware maintenance / upda	[1]		
[E.24] System failure due to exhaustion of reso	[3]		
[E.25] Equipment loss	[0]		[1]
[A.7] Misuse	[1]	[0]	[1]
[A.11] Unauthorised access	[1]	[3]	[3]
[A.23] Hardware manipulation	[3]		[3]
[A.24] Denial of service	[4]		
[A.25] Theft	[0]		[1]
[A.26] Destructive attack	[4]		
[6.2] Developers PC	[4]	[3]	[3]
[I.5] Hardware or software failure	[3]		
[E.23] Defects in hardware maintenance / upda	[1]		
[E.24] System failure due to exhaustion of reso	[3]		
[E.25] Equipment loss	[0]		[1]
[A.7] Misuse	[1]	[0]	[1]
[A.11] Unauthorised access	[1]	[3]	[3]
[A.23] Hardware manipulation	[3]		[3]
[A.24] Denial of service	[4]		
[A.25] Theft	[0]		[1]
[A.26] Destructive attack	[4]		
[7.1] APV 1600 Node 1	[6]	[5]	[0]
[I.8] Communications services failure	[6]		
[E.2] System / Security administrator errors	[5]	[5]	[0]
[E.9] [Re-]routing errors			[0]
[E.10] Sequence errors		[4]	
[E.15] Accidental alteration of the information		[1]	
[E.19] Information leaks			[0]
[E.24] System failure due to exhaustion of reso	[6]		
[A.5] Masquerading of identity		[4]	[0]
[A.7] Misuse	[4]	[4]	[0]
[A.9] [Re-]routing of messages			[0]
[A.10] Sequence alteration		[4]	
[A.11] Unauthorised access		[4]	[0]
[A.12] Traffic analysis			[0]
[A.14] Eavesdropping			[0]
[A.15] Deliberate alteration of information		[4]	
[A.18] Destruction of information	[6]		
[A.24] Denial of service	[6]		

asset	[A]	[I]	[C]
[7.2] APV 1600 Node 2	[3]	[2]	[0]
[I.8] Communications services failure	[3]		
[E.2] System / Security administrator errors	[2]	[2]	[0]
[E.9] [Re-]routing errors			[0]
[E.10] Sequence errors		[1]	
[E.15] Accidental alteration of the information		[0]	
[E.19] Information leaks			[0]
[E.24] System failure due to exhaustion of reso	[3]		
[A.5] Masquerading of identity		[1]	[0]
[A.7] Misuse	[1]	[1]	[0]
[A.9] [Re-]routing of messages			[0]
[A.10] Sequence alteration		[1]	
[A.11] Unauthorised access		[1]	[0]
[A.12] Traffic analysis			[0]
[A.14] Eavesdropping			[0]
[A.15] Deliberate alteration of information		[1]	
[A.18] Destruction of information	[3]		
[A.24] Denial of service	[3]		
[8.1] Cisco 2960 Node 1	[6]	[5]	[0]
[I.8] Communications services failure	[6]		
[E.2] System / Security administrator errors	[5]	[5]	[0]
[E.9] [Re-]routing errors			[0]
[E.10] Sequence errors		[4]	
[E.15] Accidental alteration of the information		[1]	
[E.19] Information leaks			[0]
[E.24] System failure due to exhaustion of reso	[6]		
[A.5] Masquerading of identity		[4]	[0]
[A.7] Misuse	[4]	[4]	[0]
[A.9] [Re-]routing of messages			[0]
[A.10] Sequence alteration		[4]	
[A.11] Unauthorised access		[4]	[0]
[A.12] Traffic analysis			[0]
[A.14] Eavesdropping			[0]
[A.15] Deliberate alteration of information		[4]	
[A.18] Destruction of information	[6]		
[A.24] Denial of service	[6]		
[8.2] Cisco 2960 Node 2	[3]	[2]	[0]
[I.8] Communications services failure	[3]		
[E.2] System / Security administrator errors	[2]	[2]	[0]
[E.9] [Re-]routing errors			[0]
[E.10] Sequence errors		[1]	
[E.15] Accidental alteration of the information		[0]	
[E.19] Information leaks			[0]
[E.24] System failure due to exhaustion of reso	[3]		
[A.5] Masquerading of identity		[1]	[0]
[A.7] Misuse	[1]	[1]	[0]
[A.9] [Re-]routing of messages			[0]
[A.10] Sequence alteration		[1]	
[A.11] Unauthorised access		[1]	[0]
[A.12] Traffic analysis			[0]
[A.14] Eavesdropping			[0]
[A.15] Deliberate alteration of information		[1]	
[A.18] Destruction of information	[3]		
[A.24] Denial of service	[3]		

asset	[A]	[I]	[C]
[8.3] Checkpoint 4406 Node 1	[4]	[3]	[0]
⚠ [I.8] Communications services failure	[4]		
⚠ [E.2] System / Security administrator errors	[3]	[3]	[0]
⚠ [E.9] [Re-]routing errors			[0]
⚠ [E.10] Sequence errors		[2]	
⚠ [E.15] Accidental alteration of the information		[0]	
⚠ [E.19] Information leaks			[0]
⚠ [E.24] System failure due to exhaustion of reso	[4]		
⚠ [A.5] Masquerading of identity		[2]	[0]
⚠ [A.7] Misuse	[2]	[2]	[0]
⚠ [A.9] [Re-]routing of messages			[0]
⚠ [A.10] Sequence alteration		[2]	
⚠ [A.11] Unauthorised access		[2]	[0]
⚠ [A.12] Traffic analysis			[0]
⚠ [A.14] Eavesdropping			[0]
⚠ [A.15] Deliberate alteration of information		[2]	
⚠ [A.18] Destruction of information	[4]		
⚠ [A.24] Denial of service	[4]		
[8.4] Checkpoint 4406 Node 2	[4]	[3]	[0]
⚠ [I.8] Communications services failure	[4]		
⚠ [E.2] System / Security administrator errors	[3]	[3]	[0]
⚠ [E.9] [Re-]routing errors			[0]
⚠ [E.10] Sequence errors		[2]	
⚠ [E.15] Accidental alteration of the information		[0]	
⚠ [E.19] Information leaks			[0]
⚠ [E.24] System failure due to exhaustion of reso	[4]		
⚠ [A.5] Masquerading of identity		[2]	[0]
⚠ [A.7] Misuse	[2]	[2]	[0]
⚠ [A.9] [Re-]routing of messages			[0]
⚠ [A.10] Sequence alteration		[2]	
⚠ [A.11] Unauthorised access		[2]	[0]
⚠ [A.12] Traffic analysis			[0]
⚠ [A.14] Eavesdropping			[0]
⚠ [A.15] Deliberate alteration of information		[2]	
⚠ [A.18] Destruction of information	[4]		
⚠ [A.24] Denial of service	[4]		