ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΕΙΡΑΙΩΣ

ΤΜΗΜΑ ΨΗΦΙΑΚΩΝ ΣΥΣΤΗΜΑΤΩΝ

UNIVERSITY OF PIRAEUS

DEPARTMENT OF DIGITAL SYSTEMS

«ΔΙΑΧΕΙΡΙΣΗ ΚΙΝΔΥΝΟΥ ΣΕ ΣΥΣΤΗΜΑΤΑ ΠΛΗΡΟΦΟΡΙΚΗΣ»

Βαρβάρα Αλεξανδρή

Επιβλέπων Καθηγητής: Μαρίνος Θεμιστοκλέους

ΠΕΙΡΑΙΑΣ 2016

ΚΑΡΑΟΛΗ & ΔΗΜΗΤΡΙΟΥ 80
185 34 ΠΕΙΡΑΙΑΣ

TEL: 210-4142 235,426,373,
FAX: 210-4142376

80, KARAOLI & DIMITRIOU STR.
185 34 P1RAEUS - GREECE

Περιεχόμενα

Λίστα Εικόνων

Ευχαριστίες

Η συγκεκριμένη εργασία ξεκίνησε και τελείωσε μέσα στο ακαδημαϊκό έτος 2015 -2016 σύμφωνα με τον υπάρχον κανονισμό του μεταπτυχιακού προγράμματος σπουδών Τεχνοοικονομική Διοίκηση Ψηφιακών Συστημάτων του τμήματος Ψηφιακών Συστημάτων του Πανεπιστημίου Πειραιώς.

Αρχικά θα ήθελα να ευχαριστήσω τον καθηγητή κ. Θεμιστοκλέους για την ανάθεση της διπλωματικής εργασίας και τη δυνατότητα που μου δόθηκε να ασχοληθώ με έναν τόσο ενδιαφέρον τομέα. Οι χρήσιμες υποδείξεις και συμβουλές του ήταν αυτές που με βοήθησαν να φέρω εις πέρας αυτή την ερευνητική εργασία που για μένα ήταν κάτι εντελώς καινούριο. Τον ευχαριστώ θερμά για το χρόνο που μου αφιέρωσε, την καινούρια για μένα εμπειρία και γνώση πάνω στον τομέα της ερευνητικής διαδικασίας και όλη την υπομονή του.

Τέλος θα ήθελα να ευχαριστήσω την οικογένειά μου για τη στήριξη και την καθοδήγηση που μου παρείχαν καθ’ όλη τη διάρκεια των μεταπτυχιακών σπουδών μου.

Περίληψη

Η παρούσα διπλωματική εργασία, αναπτύσσεται στο πλαίσιο του προγράμματος μεταπτυχιακών σπουδών Τεχνοοικονομικής Διοίκησης Ψηφιακών Συστημάτων του τμήματος των Ψηφιακών Συστημάτων.

Η γενική μεθοδολογία της διαδικασίας της Διαχείρισης Κινδύνου αναπτύχθηκε με σκοπό να καθοδηγήσει το σχεδιασμό και τη διαχείριση της ασφάλειας ενός πληροφοριακού συστήματος στα πλαίσια μιας επιχείρησης. Αποτελείται από τρία βασικά επίπεδα: την Εκτίμηση Κινδύνου, την Αξιολόγηση Κινδύνου και το Σχέδιο Δράσης και Αντιμετώπισης Κινδύνου καθώς και τη φάση της Παρακολούθησης του Κινδύνου. Στόχος της εργασίας είναι η παρουσίαση και ανάλυση των κινδύνων που υπεισέρχονται στην ανάπτυξη και υλοποίηση ενός πληροφοριακού συστήματος και των τεχνικών προσδιορισμού και διαχείρισης κινδύνων.

Το προτεινόμενο μοντέλο για τη μελέτη περίπτωσης βασίζεται στη μέθοδο CRAMM, η οποία παρέχει ένα πλήρες εννοιολογικό πλαίσιο για τη διαχείριση των κινδύνων.

Λέξεις κλειδιά: Ασφάλεια Πληροφοριακών Συστημάτων, πληροφοριακό σύστημα ή ΠΣ, κίνδυνος, διαχείριση κινδύνου.

Abstract

This thesis, developed under the program graduate economic Management of Digital Systems Digital Systems Division.

The general methodology of the process of Risk Management was developed in order to guide the design and security management of an information system of an enterprise. It consists of three main areas: Risk Assessment, Risk Assessment and Risk Action and Contingency Plan and the phase of the Risk Monitoring. Work objective is the presentation and analysis of the risks involved in the development and implementation of an information system and identification techniques and risk management.

The proposed model for the case study based on CRAMM method, which provides a comprehensive conceptual framework for risk management

Keywords: Information Systems Security, IT system or CP, danger, risk management.

Εισαγωγή

Γενικά

Οι δημόσιες υπηρεσίες, οι τράπεζες, οι μεγάλοι οργανισμοί, οι επιχειρήσεις καθώς επίσης και οι ελεύθεροι επαγγελματίες, οι φοιτητές, οι μαθητές αντιμετωπίζουν συχνά την ανάγκη να διαχειριστούν μεγάλο όγκο πληροφοριών γρήγορα και αξιόπιστα. Σε αυτήν τη διαχείριση σημαντική βοήθεια μπορεί να δώσει η Τεχνολογία της Πληροφορικής. Για να διαχειριστούμε μεγάλα σύνολα πληροφοριών με την αξιοποίηση των σημαντικών δυνατοτήτων που μας προσφέρει η τεχνολογία της Πληροφορικής, αναπτύσσουμε Πληροφοριακά Συστήματα, με στόχο:

- τη βελτίωση της ποιότητας προϊόντων και υπηρεσιών
- την αύξηση της παραγωγικότητας
- την παραγωγή νέων προϊόντων και νέων υπηρεσιών.

Όταν τα πληροφοριακά συστήματα ή ΠΣ άρχισαν να διεισδύουν στις μεσαίες και μεγάλες επιχειρήσεις, τα άτομα που ήξεραν να τα χειρίζονται ήταν λίγα και με εξειδίκευση, ενώ τα φαινόμενα παραβίασης της ασφάλειας ήταν σχεδόν ανύπαρκτα. Η ίδια η πληροφορία δεν υπολογιζόταν ως σημαντικό περιουσιακό στοιχείο της επιχείρησης, ενώ οι διεργασίες που εφαρμόζονταν στο κομμάτι του μάνατζμεντ ήταν μια ατομική τέχνη προσωπικών επαφών και όχι μια παγκόσμια διεργασία συντονισμού.

Στη δεκαετία του 1940 ερευνητές από όλους τους επιστημονικούς τομείς (τη φιλοσοφία, τα μαθηματικά, τη βιολογία κτλ.) άρχισαν να αναγνωρίζουν ότι κάθε αντικείμενο (οντότητα) μπορεί να θεωρηθεί ως μέρος ενός μεγαλύτερου όλου. Το γεγονός αυτό δε μειώνει τη σημασία της ατομικότητας μιας οντότητας, αλλά μετατοπίζει το ενδιαφέρον από το μέρος στο όλο. Η προσέγγιση αυτή θεμελίωσε ένα νέο τρόπο σκέψης που ονομάστηκε θεωρία συστημάτων. Ο τρόπος, αυτός, σκέψης έχει άμεση επίδραση στην αντίληψη που έχουμε για τον κόσμο. Νέοι κλάδοι των επιστημών αναπτύχθηκαν βασισμένοι στη θεωρία συστημάτων όπως η διοίκηση επιχειρήσεων, οι επιχειρησιακές έρευνες και η ανάλυση συστημάτων.

Στη σύγχρονη εποχή, συγκεκριμένα κατά τη διάρκεια της δεκαετίας του 1990 μέχρι και σήμερα, οι καινοτόμες τεχνολογίες οδήγησαν σε ευρεία χρήση των ηλεκτρονικών

υπολογιστών, συνεπώς ο αριθμός των παραβιάσεων της ασφάλειας ακολουθεί μια συνεχή εκθετική αύξηση. Η εύκολη πρόσβαση στις πληροφορίες, καθώς και οι ευκολίες που παρέχονται μέσω Διαδικτύου, έχουν οδηγήσει πολλές επιχειρήσεις να επενδύσουν στην ανάπτυξη και εφαρμογή ΠΣ και διαδικτυακών εφαρμογών. Παρόλο, όμως, που ένα αξιόπιστο πληροφοριακό σύστημα αποτελεί ένα από τα πιο πολύτιμα στοιχεία ενός οργανισμού, η χρήση της τεχνολογίας που δεν έχει υλοποιηθεί σωστά, παρουσιάζει τρωτά σημεία, δεν συντηρείται και δεν παρακολουθείται επαρκώς μπορεί να οδηγήσει σε σημαντικές απώλειες εσόδων, απόδοσης και φήμης. Μια τέτοια κατάσταση συνεπάγεται απώλεια κερδών για την επιχείρηση και η πιθανότητα να συμβεί ένα τέτοιο γεγονός είναι ευθέως ανάλογη με το εύρος και το χρόνο χρήσης του ΠΣ. Όσο πιο περίπλοκη είναι η τεχνολογία και όσο αυξάνει ο χρόνος χρήσης της σε μία εταιρεία, τόσο υψηλότερη είναι η πιθανότητα η εταιρεία αυτή, εάν δε λαμβάνονται τα κατάλληλα μέτρα, να υποστεί τις συνέπειες ενός περιστατικού ασφάλειας ΠΣ.

Η εισαγωγή των ΠΣ σε μια επιχείρηση έχει πολλαπλές επιδράσεις και στους εργαζομένους και στη ίδια την κοινωνία. Είναι λοιπόν, σαφές, ότι η μελέτη των ΠΣ απαιτεί μια δι-επιστημονική προσέγγιση. Σε κάθε ΠΣ, κατά τις διαδικασίες ανάπτυξης και συντήρησης του, θα πρέπει να πραγματοποιείται μια ανάλυση των κινδύνων με σκοπό την επιλογή των κατάλληλων μηχανισμών προστασίας που θα μειώσουν τους κινδύνους σε αποδεκτά για την επιχείρηση επίπεδα.

Σύμφωνα με την επίσημη επιστημονική βιβλιογραφία, ο όρος του «κινδύνου» είναι μια πολυδιάστατη έννοια στην οποία έχουν αποδοθεί μια πληθώρα από ορισμούς και ερμηνείες όπως θα δούμε και στα επόμενα κεφάλαια της εργασίας. Η διαχείριση του κινδύνου με την έννοια της πρόληψης καθ 'όλη τη διάρκεια του κύκλου ζωής ανάπτυξης ενός ΠΣ είναι σημαντική για την επιτυχία ενός έργου πληροφορικής.

Ένας γενικός ορισμός που συμπεριλαμβάνει το ουσιαστικό περιεχόμενο της έννοιας του κινδύνου σε σχέση με την επιχειρηματικότητα, που στη συγκεκριμένη περίπτωση μας απασχολεί, είναι ο ακόλουθος: Ο κίνδυνος εκφράζει την αβεβαιότητα για μελλοντικές καταστάσεις, εξελίξεις, των οποίων τα αποτελέσματα θα μπορούσαν να επηρεάσουν την επίτευξη των βραχυπρόθεσμων και μακροχρόνιων στόχων της επιχείρησης.

Αντικείμενο εργασίας

Αντικείμενο της παρούσας διπλωματικής εργασίας είναι η δόμηση μιας μεθοδολογίας Διαχείρισης Κινδύνου για έργα πληροφορικής και η εφαρμογή της μεθοδολογίας αυτής στην υλοποίηση ενός πραγματικού πληροφοριακού συστήματος. Το επιλεχθέν έργο είναι η ανάπτυξη ενός λογισμικού για τη Διαχείριση Στοιχείων Διαγωνισμών. Ο βασικός της στόχος είναι ο εντοπισμός των σύγχρονων τεχνικών και μεθοδολογιών διαχείρισης κινδύνου που απαιτούνται στην εκτέλεση έργων πληροφορικής μεγάλης κλίμακας και στην καταγραφή των κυριότερων βημάτων που εκτελούνται σε αυτές τις μεθόδους.

Δομή Μελέτης

Πιο συγκεκριμένα, η παρούσα εργασία αναπτύσσεται στα ακόλουθα κεφάλαια:

Η εισαγωγή αποτελεί το παρόν κεφάλαιο, στο οποίο παρουσιάζεται το πρόβλημα και στηρίζεται η ανάγκη ανάπτυξης μιας ολοκληρωμένης μεθοδολογίας διαχείρισης κινδύνων έργων και προγραμμάτων. Επίσης, αναλύεται πλήρως το αντικείμενο και ο στόχος της έρευνας.

Στο Κεφάλαιο 1 περιγράφονται οι βασικότερες έννοιες των Πληροφοριακών Συστημάτων και της Ασφάλειας αυτών που σχετίζεται με την ασφάλεια των συστημάτων, των δεδομένων και των δικτύων. Οι έννοιες αυτές θα χρησιμοποιηθούν στη συνέχεια προκειμένου να εντοπιστούν και να αναλυθούν οι κίνδυνοι που μπορούν να παρουσιαστούν σε συστήματα πληροφορικής.

Το Κεφάλαιο 2 περιγράφει τον ορισμό του κινδύνου, της διαχείρισης του κινδύνου, και μας εισάγει σε γενικές γραμμές στη μεθοδολογία ανάλυσής του.

Στο Κεφάλαιο 3 παρουσιάζεται αναλυτικά η διαδικασία της διαχείρισης του κινδύνου, εντοπίζονται οι επιμέρους παράμετροί της και αναλύονται λεπτομερώς οι φάσεις της μεθοδολογίας έτσι ώστε να καταστεί σαφής η σημαντικότητά της στο χώρο των επιχειρήσεων και στην υλοποίηση των έργων της πληροφορικής.

Στο κεφάλαιο 4 καταγράφονται μερικές από τις πιο γνωστές, σύμφωνα με τη βιβλιογραφία, πρακτικές που βασίζονται στην έννοια της διαχείρισης του κινδύνου και προτείνουν μια

δική τους μεθοδολογία μέσα από σειρά βημάτων για την επίλυση των προβλημάτων της ασφάλειας στα ΠΣ.

Το κεφάλαιο 5 αναφέρεται στη μελέτη περίπτωσης, παρουσιάζοντας ένα συγκεκριμένο ΠΣ μιας εταιρίας και τις επιμέρους λειτουργίες του. Στη συγκεκριμένη ενότητα εφαρμόζεται μία από τις μεθοδολογίες διαχείρισης κινδύνου του κεφαλαίου 4 στο επιλεγμένο σύστημα πληροφορικής, εντοπίζονται οι πιθανοί κίνδυνοι και προτείνονται λύσεις σχετικά με την επίλυσή τους.

Τέλος, το κεφάλαιο 6 παρουσιάζει τα συμπεράσματα που απορρέουν από την παρούσα μελέτη, καθώς και οι μελλοντικές επεκτάσεις της έρευνας που πραγματοποιήθηκε.

1. Πληροφοριακά Συστήματα

1.1. Εισαγωγικές έννοιες

Η έννοια του ΠΣ περιλαμβάνει όλα εκείνα τα τεχνικά συστατικά του Υπολογιστικού Συγκροτήματος[1], το περιβάλλον στο οποίο λειτουργεί το σύστημα, το σκοπό και επιπλέον τις πληροφορίες. Οι άνθρωποι μπορεί να θεωρηθεί ότι αποτελούν μέρος του ίδιου του ΠΣ γιατί είναι υπεύθυνοι για την μεταφορά της πληροφορίας στο Υπολογιστικό Σύστημα και εκτελούν λειτουργίες απαραίτητες για την πληρότητα και την ακρίβεια των πληροφοριών.

Οι σχετικές έννοιες που χρησιμοποιούνται ΠΣ σχετίζονται με έννοιες που θεωρούνται περισσότερο γνωστές από την Επιστήμη των Υπολογιστών, όπως αυτές του Λογισμικού, του Υλικού Ηλεκτρονικού Υπολογιστή κ.τ.λ.

Τα ΠΣ αποτελούν πλέον κύρια λειτουργία μιας επιχείρησης, δίνοντας έτσι στην ασφάλεια έναν κυρίαρχο ρόλο. Μέσω της ασφάλειας ΠΣ, η επιχείρηση προστατεύει τους υπολογιστικούς της πόρους και τα δεδομένα από μη εξουσιοδοτημένη ή κακόβουλη χρήση.

Η ασφάλεια των ΠΣ αποτελεί ένα γνωστικό πεδίο της επιστήμης της πληροφορικής και ασχολείται με τις επιμέρους παραμέτρους ανάπτυξης, διαχείρισης και αξιολόγησης ενός ασφαλούς ΠΣ μιας σύγχρονης επιχείρησης. Πιο συγκεκριμένα, η επιστήμη αυτή εφαρμόζει γνώσεις και δεξιότητες πάνω στις βασικές τεχνικές προστασίας καθώς και πρακτικές μεθόδους και εργαλεία που εφαρμόζονται στην αγορά για τη διαχείριση των κινδύνων ασφάλειας ΠΣ διαχείρισης.

1.2. Ορισμός ΠΣ

Τα ΠΣ έχουν σχέση με πάρα πολλές από τις ανθρώπινες δραστηριότητες και έχουν εξελιχθεί σε ένα βασικό εργαλείο διοίκησης. Η σπουδαιότητά τους συνεχώς αυξάνει με ραγδαίο ρυθμό τόσο σε ερευνητικό επίπεδο όσο και σε επίπεδο εφαρμογής, με αποτέλεσμα να

[1] Η έννοια του Υπολογιστικού Συστήματος περιλαμβάνει, εκτός από τα τεχνικά συστατικά του, το λειτουργικό περιβάλλον και το σκοπό για τον οποίο το Υπολογιστικό Σύστημα υπάρχει. Το λειτουργικό περιβάλλον περιλαμβάνει και τους ανθρώπους που είναι απαραίτητοι για τη λειτουργία των τεχνικών μερών του συστήματος και που θεωρούνται ως Υπολογιστικοί Πόροι. Ο σκοπός του Υπολογιστικού Συστήματος εκφράζεται μέσω του λογισμικού εφαρμογών.

διδάσκονται συστηματικά σε όλα τα Πανεπιστήμια παγκοσμίως. Ταυτόχρονα, τα ΠΣ αποτελούν βασικότατη πηγή πληροφόρησης ειδικά για τη λήψη αποφάσεων και σήμερα σχεδόν όλες οι μεγάλες εταιρείες έχουν στο οργανόγραμμά τους τη θέση του Γενικού Διευθυντή ΠΣ (CIO – Chief Information Officer), ο οποίος αποτελεί μέλος του Διοικητικού Συμβουλίου τους, μαζί με το Διευθύνοντα Σύμβουλο, το Γενικό Οικονομικό Διευθυντή, το Γενικό Διευθυντή Λειτουργίας και το Γενικό Τεχνικό Διευθυντή. Πολλές φορές ο Γενικός Τεχνικός Διευθυντής αναλαμβάνει ταυτοχρόνως τα καθήκοντα και τις αρμοδιότητες του Γενικού Διευθυντή ΠΣ.

Ένα ΠΣ είναι ένα οργανωμένο σύνολο των πέντε οντοτήτων (Άνθρωποι, Δεδομένα, Λογισμικό, Υλικό, Διαδικασίες) που όλες μαζί συνθέτουν ένα σύστημα, το οποίο δέχεται, αποθηκεύει, ανακτά, μετασχηματίζει, επεξεργάζεται και διανέμει πληροφορίες στους διάφορους χρήστες.

Τα ΠΣ συνδέονται και με άλλες επιστημονικές περιοχές, όπως του Ηλεκτρονικού Επιχειρείν, της Εικονικής Πραγματικότητας, της Θεωρίας Πιθανοτήτων, της Ανάλυσης Δεδομένων, της Επιχειρησιακής Έρευνας, της Μαθηματικής Στατιστικής και των Αλγορίθμων κ.λπ. Οι ανωτέρω τομείς έχουν πολύχρονη πορεία στην Επιστήμη, αλλά τα τελευταία χρόνια τα ΠΣ ακολούθησαν τη δική τους αυτόνομη πορεία. Τέλος, γενικότερα τα ΠΣ έχουν εφαρμογή και σε άλλες επιστήμες, όπως η Θεωρία Οργάνωσης και Διοίκησης.

1.3. Δομή ΠΣ

Στο πεδίο της Επιστήμης Υπολογιστών, ένα ΠΣ αποτελείται από τριών ειδών συνιστώσες:

1. τη Δομή (structure): Περιλαμβάνει τα μέσα αποθήκευσης (repositories) των δεδομένων είτε σε μόνιμη βάση είτε σε προσωρινή, όπως οι σκληροί δίσκοι, η μνήμη των υπολογιστών κ.λπ., καθώς και τις διεπαφές (interfaces), όπως τα πληκτρολόγια, οι εκτυπωτές, οι σαρωτές κ.λπ., μέσω των οποίων ανταλλάσσονται οι πληροφορίες μεταξύ ψηφιακού και μη-ψηφιακού κόσμου.

2. τα Κανάλια Επικοινωνίας (communication channels): Περιλαμβάνει τα κανάλια επικοινωνίας που συνδέουν τα μέσα αποθήκευσης των δεδομένων, όπως τα καλώδια, τις

ασύρματες επίγειες ζεύξεις, τις δορυφορικές ζεύξεις κ.λπ. Το σύνολο των λογικών ή φυσικών καναλιών αποτελεί ένα δίκτυο.

3. την Έξοδο (behavior): Περιλαμβάνει τις υπηρεσίες, οι οποίες έχουν αξία για τους χρήστες ή για άλλες υπηρεσίες μέσω της ανταλλαγής μηνυμάτων καθώς και τα μηνύματα που σχετίζονται με τους χρήστες ή τις υπηρεσίες. Στη Γεωγραφία και τη Χαρτογραφία ένα Σύστημα Γεωγραφικών Πληροφοριών (GIS – Geographic Information System) χρησιμοποιείται για να ενοποιήσει, αποθηκεύσει, τροποποιήσει, αναλύσει, κατανείμει και παρουσιάσει γεωγραφικού περιεχομένου πληροφορίες.

Υπάρχουν πολλές εφαρμογές Συστημάτων Γεωγραφικών Πληροφοριών οι οποίες εκτείνονται μέχρι την Οικολογία και τη Γεωλογία κ.λπ. Στις Τηλεπικοινωνίες ο όρος ΠΣ αναφέρεται σε οποιοδήποτε τηλεπικοινωνιακό ή/και σχετικό με υπολογιστές εξοπλισμό ή σε διασυνδεδεμένα συστήματα ή υποσυστήματα εξοπλισμών που χρησιμοποιούνται για τη συλλογή, αποθήκευση, διαχείριση, διοίκηση, διακίνηση, έλεγχο, παρουσίαση, μεταγωγή, ανταλλαγή, εκπομπή ή λήψη φωνής ή/και δεδομένων (data).

1.4. Ασφάλεια Συστημάτων

Οι σημαντικότερες απειλές των ΠΣ και την ακεραιότητας των δεδομένων τους προέρχονται από πλημμελή εγκατάσταση και χρήση και από τη καταστροφική δράση των ιών. Με τις νέες, εξελιγμένες μεθόδους διάδοσης, ο χρόνος αντίδρασης των χρηστών και των διαχειριστών των συστημάτων έχει μειωθεί επικίνδυνα, ενώ η απειλή μπορεί να προέλθει από οπουδήποτε μέσα και έξω από το ΠΣ. Πιθανές είσοδοι κινδύνων θεωρούνται:

- ✓ Σταθμοί εργασίας
- ✓ Εξυπηρετητές του ΠΣ
- ✓ Πύλες Internet για διάφορες υπηρεσίες (WEB, e-mail, FTP κλπ.)

Οι λύσεις που προσφέρονται για την αντιμετώπιση των ιών (anti-virus S/W) λειτουργούν αποτελεσματικά σε μεμονωμένους εξυπηρετητές και σταθμούς εργασίας. Η εφαρμογή των λύσεων είναι εφικτή, αλλά μπορεί να αποδειχτεί μια πολύ δαπανηρή επένδυση αν δεν γίνει με το σωστό τρόπο. Μελέτες, που έχουν προτείνει μια συνολική, εξειδικευμένη λύση για

την αντιμετώπιση των απειλών που συνεπάγονται οι ιοί με το μικρότερο δυνατό κόστος και φυσικά με την μεγαλύτερη δυνατή εξασφάλιση της επένδυσης περιλαμβάνουν:

- ✓ Το είδος του λογισμικού και τις εργασίες που απαιτούνται ώστε όλοι οι σταθμοί εργασίας (ανεξάρτητα πλατφόρμας και λειτουργικού) να προστατεύονται από ιούς.
- ✓ Το λογισμικό και τις εργασίες για την προστασία των εξυπηρετητών (servers) και των Ιντερνέτ gateways (Proxy, e-mail κλπ.)
- ✓ Την παραμετροποίηση του λογισμικού στους εξυπηρετητές και τους σταθμούς εργασίας.
- ✓ Τον τρόπο ενημέρωσης όλης της εγκατάστασης με νέες εκδόσεις του λογισμικού.
- ✓ Τις μεθόδους και τις διαδικασίες που θα προστατεύσουν την πληροφοριακή υποδομή από νέους ιούς.

1.5. Ασφάλεια Δεδομένων

Οι αστοχίες στην λειτουργία ΠΣ, οι κακοί χειρισμοί χρηστών και η δράση ιών των ΠΣ, είναι μερικές από τις αιτίες που μπορούν να οδηγήσουν στην μερική ή συνολική καταστροφή των πολύτιμων δεδομένων που επεξεργάζεται κάθε ΠΣ.

Η λήψη αντιγράφων ασφαλείας (backup) είναι πλέον αναγκαία, ώστε να διασφαλιστούν τα δεδομένα της επιχείρησης και να επιτραπεί η ανασύσταση του ΠΣ (restore) όταν αυτό χρειαστεί. Οι μηχανικοί της εταιρείας μπορούν να αναλάβουν το σχεδιασμό και την υλοποίηση της υποδομής, όσο και τις διαδικασίες (backup plan) που θα εξασφαλίζουν την λήψη αντιγράφων ασφαλείας.

Ειδικότερα, οι μηχανικοί μιας επιχείρησης, μετά από εξέταση του ΠΣ, των δεδομένων και της λειτουργικής υποδομής της εταιρείας σε επίπεδο ανθρώπων και διαδικασιών, είναι σε θέση να δώσουν λύσεις που να περιλαμβάνουν:

1. Την τεκμηρίωση από την πλευρά των θεμάτων που εξετάστηκαν.
2. Το υλικό και το λογισμικό (H/W & S/W) που ανταποκρίνεται στις ανάγκες για την λήψη των αντιγράφων ασφαλείας.
3. Το είδος και την ποσότητα των δεδομένων που θα φυλάσσονται καθώς και τα αποθηκευτικά μέσα από τα οποία θα αντλούνται.

4. Τον προγραμματισμό και την μέθοδο (compress / uncompress, full / incremental / differential, offline / online).
5. Το σχεδιασμό της μεθόδου αρχειοθέτησης των tapes. Την περίοδο, τον τρόπο και τον τόπο φύλαξης τους.
6. Τον προϋπολογισμό της συνολικής λύσης για την απόκτηση και την λειτουργία του backup και του restore.
7. Τις προτεραιότητες και τα βήματα που θα πρέπει να ακολουθηθούν.

1.6. Ασφάλεια Δικτύων

Η διαθεσιμότητα του συστήματος και των δεδομένων και η εμπιστευτικότητα της πληροφορίας, που συνήθως είναι πιο καταστροφική από την απώλεια, αποτελούν τους βασικότερους παράγοντες που δημιουργούν αυξημένες απαιτήσεις ασφάλειας ενός εταιρικού δικτύου. Με την πρόοδο της τεχνολογίας οι απειλές για τα σημαντικά δεδομένα των εταιρειών έχουν πολλαπλασιαστεί και μπορεί να προέρχονται είτε από το ενδοεταιρικό δίκτυο (χρήστες του εταιρικού ΠΣ), είτε από το διαδίκτυο (εξωτερικοί εισβολείς μέσω διαδικτυακών εφαρμογών/hackers - attackers). Μια ολοκληρωμένη μελέτη ασφάλειας δικτύου που στόχο έχει να παρέχει έλεγχο και προστασία στις καθημερινές συναλλαγές, καλύπτει αναγκαίες παραμέτρους όπως:

- ✓ Φυσική προστασία του δικτύου ώστε ο εξοπλισμός και οι συνδέσεις να μην είναι εκτεθειμένες.
- ✓ Κανόνες διαπίστευσης των χρηστών σε όλα τα επίπεδα.
- ✓ Έλεγχο στην προσπέλαση ώστε οι διαπιστευμένοι χρήστες να προσπελαύνουν μόνο την πληροφορία που τους αφορά.
- ✓ Εντοπισμό και εξουδετέρωση επιθέσεων, μεμονωμένων ή οργανωμένων, από το εσωτερικό δίκτυο ή το διαδίκτυο.
- ✓ Κρυπτογράφηση των δεδομένων για την εμπιστευτική διακίνηση της πληροφορίας στο δίκτυο.
- ✓ Διαχείριση όλων των δικτυακών λειτουργιών και συσκευών.

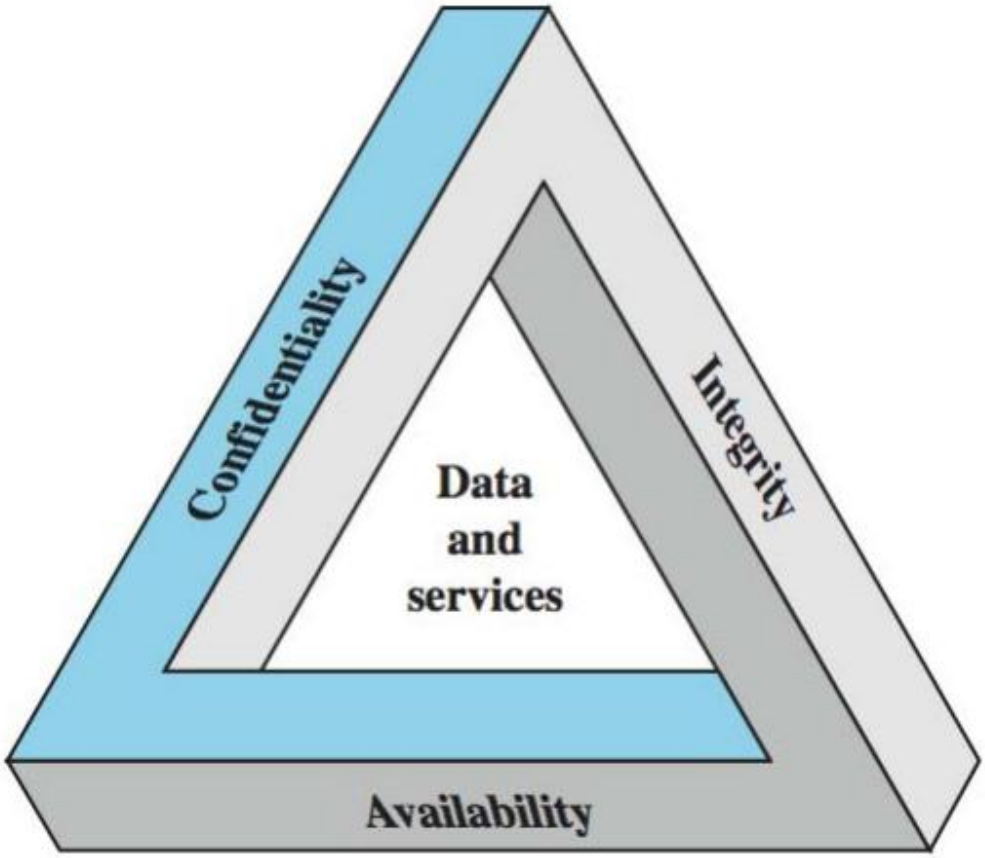
1.7. Εμπλεκόμενοι φορείς στην ανάπτυξη της ασφάλειας

Η ασφάλεια των ΠΣ μιας επιχείρησης για την ανάπτυξή μιας συγκεκριμένης πολιτικής βασίζεται στην καταγραφή των απαιτήσεων ασφαλείας, βάσει των οποίων διαμορφώνονται οι στόχοι της ασφάλειας και στον προσδιορισμό των τρόπων για την επίτευξη των στόχων αυτών. Οι εμπλεκόμενοι φορείς μπορεί να βρίσκονται εντός και εκτός του οργανισμού με την καλή επικοινωνία και συνεργασία των οποίων να αποτελεί βασική προϋπόθεση για την αποτελεσματική διαχείριση της ασφάλειας των ΠΣ. Οι συγκεκριμένες απαιτήσεις ασφάλειας μπορεί να προέρχονται από διαφορετικά είδη πηγών, όπως:

- Τη διοίκηση του οργανισμού που επιθυμεί την απρόσκοπτη χρήση των ΠΣ στις λειτουργίες του οργανισμού.
- Τους πελάτες του οργανισμού, εφόσον τα δεδομένα που τους αφορούν αποτελούν συνιστώσα του ΠΣ.
- Το νομικό και ρυθμιστικό πλαίσιο στο οποίο λειτουργεί η επιχείρηση.
- Τους χρήστες των ΠΣ.

1.8. Προϋποθέσεις ασφάλειας ΠΣ

Σύμφωνα με την πολιτική ασφαλείας (Security Policy), η ασφάλεια ενός ΠΣ μιας επιχείρησης βασίζεται σε τρεις κυρίαρχες ιδέες οι οποίες είναι απαραίτητες για την ορθή λειτουργία του ΠΣ, και είναι οι ακόλουθες:



Εικόνα 1: Προϋποθέσεις ασφάλειας πληροφοριακών συστημάτων

- ✓ Ακεραιότητα (Integrity): αναφέρεται στη διατήρηση των δεδομένων ενός ΠΣ σε μια γνωστή κατάσταση χωρίς ανεπιθύμητες τροποποιήσεις, αφαιρέσεις ή προσθήκες από μη εξουσιοδοτημένα άτομα. Επίσης αποτρέπει την πρόσβαση και χρήση των υπολογιστών και δικτύων του συστήματος από άτομα χωρίς άδεια. Σχετικά παραδείγματα αποτελούν:
  - Η Υπηρεσία Ακεραιότητας Σύνδεσης με αποκατάσταση (Connection Integrity Service With Recovery) η οποία εξασφαλίζει την ακεραιότητα και παρέχει παράλληλα δυνατότητα ανάκτησης των δεδομένων.
  - Η Υπηρεσία Ακεραιότητας Σύνδεσης Χωρίς Αποκατάσταση (Connection Integrity Service Without Recovery) η οποία περιλαμβάνει μόνο την ακεραιότητα των δεδομένων.
  - Η Υπηρεσία Ακεραιότητας Σύνδεσης Επιλεγμένου Πεδίου (Selected Field Connection Integrity Service) η οποία παρέχει ακεραιότητα μεμονωμένων πεδίων δεδομένων.

- Η Υπηρεσία Ακεραιότητας Άνευ Εγκατάστασης Σύνδεσης (Connectionless Integrity Service) η οποία παρέχει ακεραιότητα μεμονωμένων τμημάτων δεδομένων.
- Η Υπηρεσία Ακεραιότητας Επιλεγμένου Πεδίου Άνευ Εγκατάστασης Σύνδεσης (Selected Field Connectionless Integrity Service) η οποία παρέχει ακεραιότητα συγκεκριμένων πεδίων σε μεμονωμένα τμήματα δεδομένων.

✓ Διαθεσιμότητα (Availability): αναφέρεται στην εξασφάλιση ότι οι υπολογιστές, τα δίκτυα και τα δεδομένα είναι στη διάθεση των χρηστών όποτε απαιτείται η χρήση τους. Η πιο συνηθισμένη απειλή που αντιμετωπίζουν τα σύγχρονα ΠΣ είναι η επίθεση άρνησης υπηρεσιών (DOS attack), που έχει ως σκοπό να τεθούν εκτός λειτουργίας οι τιθέμενοι πόροι, είτε προσωρινά είτε μόνιμα.

✓ Εμπιστευτικότητα (Confidentiality): σημαίνει ότι ευαίσθητες πληροφορίες δεν πρέπει να αποκαλύπτονται σε μη εξουσιοδοτημένα άτομα. Η διαρροή ευαίσθητων πληροφοριών μπορεί να γίνει με πιο παραδοσιακές μεθόδους από την ψηφιακή υποκλοπή.

1.9. Αντιμετώπιση προβλημάτων ασφαλείας

Η αντιμετώπιση των προβλημάτων που σχετίζονται με την ασφάλεια των ΠΣ δεν είναι εύκολη υπόθεση. Η εισαγωγή ενός ΠΣ στο περιβάλλον μιας επιχείρησης μπορεί να έχει πολλά πλεονεκτήματα για τον οργανισμό, αυξάνοντας κατακόρυφα την παραγωγικότητα και το κέρδος, αλλά εισάγει νέους κινδύνους που αυξάνουν σε σημαντικό βαθμό την επικινδυνότητα. Για το λόγο αυτό πρέπει οπωσδήποτε να αναγνωριστούν οι πιθανοί κίνδυνοι και να δημιουργηθεί ένα κατάλληλο πλαίσιο ασφαλείας προκειμένου να αντιμετωπιστούν ανάλογα.

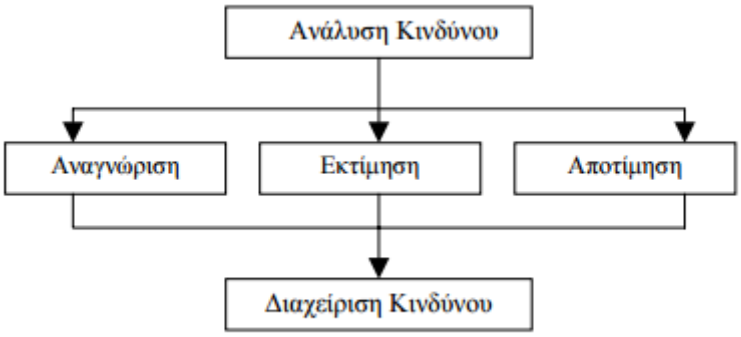
Το ζήτημα της ασφάλειας των ΠΣ απαιτεί μια συστηματική και ολοκληρωμένη αντιμετώπιση [1] γι’ αυτό και ο κλάδος της ασφάλειας ΠΣ έχει προσφέρει μια πληθώρα από εργαλεία, μεθόδους, έλεγχους και πολιτικές ασφαλείας για την αντιμετώπιση κάθε είδους προβλήματος. Γενικά, η ασφάλεια των ΠΣ περιλαμβάνει διαδικασίες διαχείρισης που σχετίζονται με:

- ✓ Τον προσδιορισμό των κινδύνων που αντιμετωπίζουν τα ΠΣ και των αναγκαίων μέτρων για την προστασία τους από τους κινδύνους αυτούς.
- ✓ Τον καθορισμό μιας πολιτικής ασφάλειας ΠΣ και τον προσδιορισμό των διαθέσιμων πόρων για την εφαρμογή ενός πλαισίου πολιτικής ασφάλειας.
- ✓ Τον καθορισμό των ρόλων, των αρμοδιοτήτων και την απόδοση υπευθυνοτήτων για τα ζητήματα της ασφάλειας των ΠΣ.
- ✓ Την ενημέρωση και ευαισθητοποίηση των χρηστών σε ζητήματα ασφάλειας και την εκπαίδευση και κατάρτισή τους στη χρήση και εφαρμογή των μέτρων προστασίας.
- ✓ Τον καθορισμό σχεδίων ανάνηψης και συνέχειας από την πραγματοποίηση περιστατικών ασφάλειας.
- ✓ Την αξιολόγηση όλων των διαδικασιών διαχείρισης της ασφάλειας των πληροφοριακών συστημάτων.

Οι προαναφερθείσες διαδικασίες δεν είναι εύκολο να ενσωματωθούν από έναν οργανισμό, αντιθέτως, ο διαφορετικός τρόπος λειτουργίας καθώς και η διαφορετική ανάθεση πόρων γύρω από τα θέματα της ασφάλειας, δημιουργούν εντελώς διαφορετικές συνθήκες, μοναδικές για κάθε επιχείρηση.

Την απάντηση στο πρόβλημα αυτό δίνει η ανάλυση κινδύνων (risk analysis) που έχει ως σκοπό την αξιολόγηση των περιουσιακών στοιχείων του οργανισμού και την αναγνώριση όλων των κινδύνων και των ευπαθειών που τα απειλούν. Πιο συγκεκριμένα η έννοια της ανάλυσης [2] αποτελεί μια διαδικασία τριών σταδίων (εικόνα 2):

- ✓ Αναγνώριση κινδύνου (risk identification)
- ✓ Εκτίμηση κινδύνου (risk estimation)
- ✓ Αποτίμηση κινδύνου (risk evaluation)



Εικόνα 2: Ανάλυση Κινδύνου

Στις ενότητες που ακολουθούν, αναλύεται η διαδικασία της διαχείρισης του κινδύνου που σχετίζεται με την ανθρώπινη συμπεριφορά η οποία περιλαμβάνει την εφαρμογή μέτρων πρόληψης, καθώς και τη μέτρηση της αποτελεσματικότητας των μέτρων αυτών μέσα στον οργανισμό.

2. Διαχείριση Κινδύνου ΠΣ

2.1. Η θεωρία του κινδύνου

Μια από τις πιο συνήθεις παραμέτρους της καθημερινής ζωής αποτελεί ο κίνδυνος και υφίσταται σε όλες εκείνες τις περιπτώσεις που δεν μπορεί να προβλεφθεί με βεβαιότητα το αποτέλεσμα μιας δραστηριότητας. Η έννοια του κινδύνου σε σχέση με μία συγκεκριμένη δραστηριότητα είναι η πιθανότητα εμφάνισης ενός μη επιθυμητού αποτελέσματος και μπορεί να οριστεί ως η έκθεση στην αβεβαιότητα [3].

Η έννοια της αβεβαιότητας με τη σειρά της είναι στενά συνδεδεμένη με την έννοια της μεταβλητότητας (variability) ή της αστάθειας (volatility). Οι κίνδυνοι από εσφαλμένες εκτιμήσεις έχουν συχνά ανεπιθύμητες συνέπειες για τις επιχειρήσεις (π.χ. κόστος), με αποτέλεσμα η διοίκηση να προβαίνει σε ενέργειες για τη διαχείριση των κινδύνων, που δε σχετίζονται με τη στρατηγική ή τους αρχικούς στόχους που έχουν τεθεί.

Ο κίνδυνος, συχνά, συνδέεται με τις παρακάτω έννοιες:

- ✓ Απειλή (threat): είναι οποιαδήποτε πράξη ή γεγονός που θα μπορούσε να παραβιάσει την ασφάλεια ενός συστήματος και να προκαλέσει ζημιά.
- ✓ Ευπάθεια (vulnerability): είναι μια αδυναμία του συστήματος, η ύπαρξη της οποίας μπορεί να επιτρέψει την πραγματοποίηση της απειλής.
- ✓ Επίπτωση (consequence): είναι το αποτέλεσμα της παραβίασης της ασφάλειας και η έκταση της ζημιάς που έχει προκληθεί.

Στις επιχειρήσεις ο κίνδυνος διαδραματίζει έναν κρίσιμο ρόλο για το λόγο ότι είναι εμφανής σε όλες τι δραστηριότητες, ανεξάρτητα από το σκοπό και από τη διάθρωση των λειτουργιών τους. Σχεδόν κάθε επιχειρηματική απόφαση απαιτεί από τη διοίκηση την εξισορρόπηση των κινδύνων, μια διαδικασία που είναι απαραίτητη για την επιτυχία μιας επιχείρησης. Μπορούμε να διακρίνουμε τρεις κατηγορίες επιχειρήσεων σύμφωνα με τον τρόπο τον οποίο συμπεριφέρονται στα πλαίσια της αβεβαιότητας που αντιμετωπίζουν, ως προς τις συνθήκες του περιβάλλοντος και τη διαμόρφωσης της πολιτικής που ακολουθούν [4]:

1. Επιχειρήσεις που έχουν την πεποίθηση ότι δεν μπορούν να αλλάξουν τον τρόπο διαμόρφωσης των μελλοντικών συνθηκών με αποτέλεσμα να αδυνατούν να λάβουν κάποιο μέτρο για την αντιμετώπιση της αβεβαιότητας.
2. Επιχειρήσεις που θεωρούν αδύνατη την τροποποίηση των μελλοντικών συνθηκών, αλλά υποστηρίζουν τη συνεχή προσαρμογή τους σε αυτές ως βασική μέθοδο εξασφάλισης της βιωσιμότητάς τους.
3. Επιχειρήσεις που υποστηρίζουν την ενεργή διαμόρφωση των μελλοντικών συνθηκών τους, βάση των παρόντων και των μελλοντικών δυνατοτήτων τους.

Ένας κίνδυνος μιας επιχείρησης μπορεί να συσχετιστεί με τις ακόλουθες έννοιες:[5]

- Αποτυχία**:** ανικανότητα έργου, υποέργου ή υπηρεσίας να ολοκληρώσει την απαιτούμενη λειτουργία του.
- Ασφάλεια ποιότητας: Πιθανότητα να μην ανταποκρίνεται το έργο στους σκοπούς για τους οποίους σχεδιάστηκε.
- Αξιοπιστία**:** Πιθανότητα το έργο να πραγματοποιήσει τους σκοπούς για τους οποίους σχεδιάστηκε, για συγκεκριμένο χρονικό διάστημα ή κάτω από συγκεκριμένες συνθήκες.
- Ασφάλεια εργασιών: Τεχνικές ελαχιστοποίησης της πιθανότητας να συμβεί ατύχημα ή περιορισμού των συνεπειών του ατυχήματος με σχεδιασμό και προληπτική συντήρηση.

- Αβεβαιότητα: Μέτρο των ορίων γνώσης σε τεχνικό τομέα. Τα τέσσερα κύρια στοιχεία της αβεβαιότητας είναι η στατιστική εμπιστοσύνη (μέτρο της ακρίβειας των δειγμάτων), η ανεκτικότητα (μέτρο της διαθέσιμης πληροφορίας), τα ημιτελή και ανακριβή δεδομένα εισόδου και η ασάφεια στη μοντελοποίηση του έργου.

2.2. Κίνδυνοι ΠΣ

Οι επιχειρήσεις έρχονται καθημερινά αντιμέτωπες με διάφορα ζητήματα τα οποία απειλούν τη λειτουργία των ΠΣ και την αξιοπιστία τους. Αυτό καθιστά επιτακτική την ανάγκη φύλαξης των υποδομών και του περιεχομένου τους έναντι οποιουδήποτε κινδύνου απειλεί τη ασφάλειά του και κατ’ επέκταση την ομαλή λειτουργία του οργανισμού.

Σε ότι αφορά ένα ΠΣ [6], ο κίνδυνος μπορεί να οριστεί ως «ένα αβέβαιο γεγονός ή κατάσταση που, σε περίπτωση που προκύψει, έχει θετική ή αρνητική συνέπεια σε κάποιο στόχο του έργου». Πιο συγκεκριμένα, ο κίνδυνος αποτελεί ένα γεγονός για το οποίο κανείς δεν μπορεί να είναι βέβαιος για το αν θα συμβεί ή όχι καθώς επίσης για το αν θα παρουσιάσει «θετική ή αρνητική» έκβαση.

Η διοίκηση μιας επιχείρησης είναι σημαντικό να εντοπίζει τους κινδύνους για τα ΠΣ, για τη μείωση ή διαχείριση αυτών των κινδύνων, και να αναπτύσσει ένα σχέδιο αντιμετώπισης σε περίπτωση κρίσης. Οι ιδιοκτήτες της επιχείρησης έχουν νομικές υποχρεώσεις σε σχέση με την προστασία της ιδιωτικής ζωής, των ηλεκτρονικών συναλλαγών, καθώς και την εκπαίδευση του προσωπικού σχετικά με τις στρατηγικές διαχείρισης κινδύνων ΠΣ.

Ο κίνδυνος στον οποίο εκτίθεται ένα ΠΣ είναι συνάρτηση της αξίας των περιουσιακών στοιχείων, των ευπαθειών του, των πιθανών απειλών και της φύσης του καθώς και των επιπτώσεων που μπορεί να προκύψουν. Ένας κίνδυνος ΠΣ περιλαμβάνει το υλικό και την αποτυχία λογισμικού, ανθρώπινο λάθος, spam, ιούς και κακόβουλες επιθέσεις, καθώς και φυσικές καταστροφές όπως πυρκαγιές, πλημμύρες ή κυκλώνες. Πιο συγκεκριμένα, περιλαμβάνει:

- ✓ αστοχία υλικού και λογισμικού: όπως απώλεια ισχύος ή καταστροφή δεδομένων.
- ✓ malware: κακόβουλο λογισμικό σχεδιασμένο για να διακόψει τη λειτουργία του υπολογιστή.
- ✓ ιούς: κώδικα κακόβουλο πρόγραμμα υπολογιστή, το οποίο μπορεί να αντιγραφεί χωρίς παρέμβαση του χρήστη. Ο αρχικός ιός μπορεί να τροποποιήσει τα αντίγραφά του ή τα ίδια τα αντίγραφα μπορούν να υποστούν από μόνα τους τροποποίηση, όπως συμβαίνει σε έναν μεταμορφικό ιό.
- ✓ spam, phishing: ανεπιθύμητα μηνύματα ηλεκτρονικού ταχυδρομείου που επιδιώκουν να ξεγελάσουν τους ανθρώπους ώστε να αποκαλύψουν προσωπικά στοιχεία κλπ.
- ✓ ανθρώπινο λάθος: εσφαλμένη επεξεργασία των δεδομένων, απρόσεκτη διάθεση των δεδομένων, ή τυχαίο άνοιγμα μολυσμένων συνημμένων αρχείων ηλεκτρονικού ταχυδρομείου.

Πιο εξειδικευμένες και στοχευμένες ενέργειες ηλεκτρονικών εγκληματικών πράξεων εις βάρος των ΠΣ και των δεδομένων περιλαμβάνουν:

- ✓ Χάκερ: άτομα που παραβιάζουν παράνομα συστήματα ηλεκτρονικών υπολογιστών
- ✓ Απάτες: χρήση υπολογιστικών συστημάτων για την αλλοίωση της πληροφορίας για το παράνομο όφελος
- ✓ Κλοπές κωδικών πρόσβασης: αποτελούν συχνά στόχο για τους κακόβουλους χάκερ
- ✓ denial-of-service: online επιθέσεις που εμποδίζουν την πρόσβαση σε ιστοσελίδες για εξουσιοδοτημένους χρήστες
- ✓ παραβιάσεις ασφάλειας: περιλαμβάνουν κυρίως online εισβολές
- ✓ ανεντιμότητα σε προσωπικό επίπεδο: κλοπή δεδομένων ή ευαίσθητών πληροφοριών, όπως στοιχεία πελατών.

Όλοι οι παραπάνω κίνδυνοι ΠΣ μπορούν να ομαδοποιηθούν σε τέσσερα βασικά είδη απειλών που σχετίζονται με την ασφάλεια των ΠΣ, και είναι:

- Διακοπή (Interruption): Τα αντικείμενα του συστήματος χάνονται, δεν είναι διαθέσιμα ή δεν μπορούν να χρησιμοποιηθούν.
- Παρεμπόδιση (Interception): Μια μη εξουσιοδοτημένη ομάδα (π.χ. άτομα, προγράμματα ή ακόμα και παρέμβαση ενός άλλου ΠΣ) έχει αποκτήσει το δικαίωμα πρόσβασης σε ένα αντικείμενο.
- Τροποποίηση (Modification). Αναφέρεται σε μια μη εξουσιοδοτημένη ομάδα που όχι μόνο επιδιώκει να προσπελάσει τα δεδομένα ενός συστήματος αλλά στοχεύει και να τα τροποποιήσει.
- Πλαστοποίηση (fabricate). Μια μη εξουσιοδοτημένη ομάδα μπορεί να κατασκευάσει πλαστά αντικείμενα σε ένα Π.Σ. Ο εισβολέας έχει τη δυνατότητα να προσθέσει εγγραφές σε μια υπάρχουσα βάση δεδομένων. Μερικές φορές, αυτές οι προσθέσεις ανιχνεύονται σαν πλαστές, αλλά εάν έχουν γίνει περίτεχνα τότε είναι αδιαχώριστες από τα πραγματικά αντικείμενα του συστήματος.

2.3. Διαχείριση Κινδύνου ΠΣ

Μολονότι ένα αξιόπιστο ΠΣ αποτελεί ένα από τα πιο σημαντικά περιουσιακά στοιχεία ενός οργανισμού, η χρήση τεχνολογίας που δεν έχει υλοποιηθεί με σωστό τρόπο, παρουσιάζει

τρωτά σημεία, δεν συντηρείται και δεν παρακολουθείται επαρκώς μπορεί να οδηγήσει σε σημαντικές απώλειες κερδών, απόδοσης και φήμης. Η πιθανότητα να συμβεί ένα μη επιθυμητό γεγονός είναι ευθέως ανάλογη με το εύρος και το χρόνο χρήσης του ΠΣ. Για το λόγο αυτό, εάν δεν ληφθούν τα κατάλληλα μέτρα, όσο πιο πολύπλοκη είναι η τεχνολογία που εφαρμόζεται και όσο αυξάνει ο χρόνος χρήσης της σε μία επιχείρηση, τόσο υψηλότερη είναι η πιθανότητα η επιχείρηση αυτή να υποστεί τις συνέπειες ενός περιστατικού ασφάλειας ΠΣ.

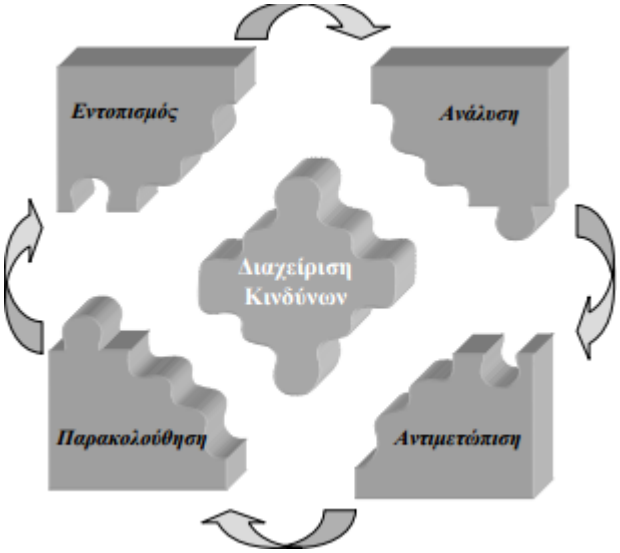
Η Διαχείριση Κινδύνων (Risk Management) σύμφωνα με τη γενική της μορφή μπορεί να οριστεί ως «μία διαδικασία που εφαρμόζεται από τη διοίκηση και το υπόλοιπο προσωπικό μίας επιχείρησης κατά τον σχεδιασμό, έτσι ώστε να ταυτοποιήσει τα πιθανά γεγονότα που μπορεί να επηρεάσουν την επίτευξη των στόχων της».

Κατά καιρούς έχουν προταθεί πολλές μεθοδολογίες Διαχείρισης Κινδύνου. Μερικές από αυτές είναι:

Συγγραφέας - Κείμενο	Βήματα Διαχείρισης Κινδύνου
Project Management Institute (PMI 2004) "A Guide to the project Management Body of Knowledge"	**Έξι Στάδια** ▪ Σχεδιασμός ▪ Αναγνώριση κινδύνων ▪ Ποιοτική ανάλυση κινδύνων ▪ Ποσοτική ανάλυση κινδύνων ▪ Σχεδιασμός ενεργειών μείωσης του κινδύνου ▪ Έλεγχος και παρακολούθηση
Klein και Cork (1998) "An approach to technical risk assessment"	**Τέσσερα Στάδια** ▪ Αναγνώριση ▪ Ανάλυση ▪ Έλεγχος ▪ Τεκμηρίωση - Αναφορά
Chapman και Ward (1999) "Project Risk Management Processes, Techniques and Insights"	**Εννέα Στάδια** ▪ Καθορισμός ▪ Στρατηγική προσέγγιση ▪ Αναγνώριση κινδύνων ▪ Δόμηση πληροφορίας ▪ Αρμοδιότητες – πεδία ευθύνης ▪ Υπολογισμός αβεβαιότητας ▪ Σημαντικότητα κινδύνων ▪ Παρακολούθηση ▪ έλεγχος
Carter et al (2001) "Introducing Riskman Methodology "	**Τρία Στάδια** ▪ Βασικό (ανάλυση με ποιοτικούς όρους) ▪ Ενδιάμεσο (πρόχειρη ποσοτικοποίηση) ▪ Λεπτομέρειες (πλήρης ποσοτικοποίηση)
Fairley (1994) "Risk management Software projects"	**Επτά Στάδια** ▪ Αναγνώριση ▪ Ανάλυση ▪ Περιορισμός κινδύνων ▪ Παρακολούθηση ▪ Σχεδιασμός εναλλακτικών σχεδίων ανάγκης ▪ Διαχείριση κρίσης ▪ Έξοδος από την κρίση
Boehm (1991) "Software Risk Management"	**Δυο Στάδια** ▪ Ανάλυση κινδύνου (αναγνώριση, ανάλυση, ιεράρχηση) ▪ Διαχείριση κινδύνου (σχεδιασμός ενεργειών διαχείρισης κινδύνου, αποφάσεις διαχείρισης, παρακολούθηση και διορθωτικές ενέργειες)
Software Engineering Institute (1992) "The SEI Approach for Technical Risks"	**Πέντε Στάδια** ▪ Αναγνώριση ▪ Ανάλυση ▪ Διαχείριση ▪ Έλεγχος ▪ Παρακολούθηση
IRGC (2005) "White paper on Risk Governance"	**Πέντε Στάδια** ▪ Προ-αξιολόγηση ▪ Αποτίμηση ▪ Εκτίμηση ανεκτικότητας απέναντι στον κίνδυνο ▪ Διαχείριση κινδύνου ▪ Επικοινωνία
Institute of Civil Engineers and the Faculty and Institute of Actuaries (1998) "Risk Analysis and Management for Projects (RAMP)"	**Τέσσερα Στάδια** ▪ Εκκίνηση ▪ Ανασκόπηση ▪ Διαχείριση κινδύνων ▪ Κλείσιμο

Εικόνα 3: Μεθοδολογίες Διαχείρισης Κινδύνου

Όπως θα δούμε αναλυτικότερα και στην επόμενη ενότητα, η διαχείριση κινδύνου είναι μία διαδικασία μέσω της οποίας επιτυγχάνεται ο εντοπισμός, η ανάλυση, η αντιμετώπιση και η παρακολούθηση των απειλών που αφορούν ένα συγκεκριμένο έργο πληροφορικής [6].



Εικόνα 4: Διαχείριση Κινδύνου

Εντοπισμός: Η διαδικασία του εντοπισμού σχετίζεται με τον εντοπισμό όλων των κινδύνων που είναι πιθανό να επηρεάσουν τους στόχους ενός ΠΣ και ταυτόχρονα στην καταγραφή τους. Τα χαρακτηριστικά κάθε κινδύνου μπορούν να καταγραφούν σε ειδικές φόρμες που ονομάζονται φύλλα κινδύνου [7].

Ανάλυση: Η ανάλυση κινδύνων χρησιμοποιείται, αφενός για να καθορισθεί το μέγεθος της συνέπειας του κινδύνου στους στόχους του ΠΣ και αφετέρου να ταξινομηθούν οι κίνδυνοι με βάση τη συνολική τους βαρύτητα. Η βαρύτητα ενός κινδύνου προκύπτει από τον πολλαπλασιασμό της πιθανότητας εμφάνισης επί την αναμενόμενη συνέπεια σε περίπτωση εμφάνισης. Το στάδιο της ανάλυσης των κινδύνων μπορεί να πραγματοποιηθεί είτε ποιοτική, είτε με ποσοτική ανάλυση [8].

Αντιμετώπιση: Στο στάδιο της αντιμετώπισης ορίζονται οι απαραίτητες ενέργειες και οι υπεύθυνοι για την εκτέλεση αυτών. Οι επιλεγμένες ενέργειες πρέπει να είναι ανάλογες με την έκθεση του κινδύνου, και να επιλύουν το πρόβλημα με οικονομικά αποδεκτό τρόπο.

Παρακολούθηση: Αφότου η ομάδα διαχείρισης των κινδύνων έχει εντοπίσει τους κινδύνους, τους έχει κατατάξει με βάση την ανάλυση και έχει προδιαγράψει τις ενέργειες αντιμετώπισης, περνά στο στάδιο της παρακολούθησης. Σε αυτό το στάδιο ελέγχεται η υλοποίηση των ενεργειών, καθώς επίσης και η αποτελεσματικότητά τους. Διορθωτικές κινήσεις καθορίζονται και επανεκτιμούνται τα χαρακτηριστικά των κινδύνων (πιθανότητα εμφάνισης και συνέπεια). Ολόκληρη η διαδικασία επαναλαμβάνεται σε τακτά χρονικά

διαστήματα ώστε να εντοπισθούν νέοι κίνδυνοι και να ενημερωθούν τα φύλλα κινδύνων των υφιστάμενων κινδύνων.

2.4. Πλεονεκτήματα και μειονεκτήματα Διαχείρισης Κινδύνου

Τα πλεονεκτήματα της διαχείρισης κινδύνου ΠΣ περιλαμβάνουν τα παρακάτω:

- Αποτελεί εργαλείο επικοινωνίας μεταξύ των ειδικών του ΠΣ και της διοίκησης του οργανισμού. Επιτρέπει την έκφραση του προβλήματος της ασφάλειας σε γλώσσα κατανοητή από τη διοίκηση, αντιμετωπίζοντας την ασφάλεια ως «επένδυση» που αποτιμάται με όρους κόστους-οφέλους [9].
- Μπορεί να ενταχθεί σε διάφορα επιστημολογικά πλαίσια [9] και εφαρμόζεται είτε αυτούσια, είτε σε συνδυασμό με άλλες μεθοδολογίες.
- Καλύπτει τις απαιτήσεις της ευρωπαϊκής [10] και ελληνικής νομοθεσίας [11], που απαιτούνται από τα ΠΣ. Τα ΠΣ επεξεργάζονται προσωπικά δεδομένα, τη λήψη μέτρων προστασίας, έτσι ώστε «να εξασφαλίζεται επίπεδο ασφάλειας ανάλογο προς τους κινδύνους που συνεπάγεται η επεξεργασία και η φύση των
- Δεδομένων» (Νόμος 2472/1997, άρθρο 10, παρ. 3, [11]).
- Διευκολύνει την καλύτερη κατανόηση της φύσης και της λειτουργίας του ΠΣ. Αποτελεί, δηλαδή, ένα μέσο τεκμηρίωσης και ανάλυσης του ΠΣ.
- Αποτελεί την πλέον διαδεδομένη μεθοδολογία σχεδιασμού και διαχείρισης της ασφάλειας ΠΣ και έχει εφαρμοστεί με επιτυχία σε ένα μεγάλο πλήθος περιπτώσεων.
- Δίνεται η δυνατότητα αιτιολόγησης του κόστους των αντιμέτρων.

Ταυτόχρονα όμως, η μεθοδολογία αυτή παρουσιάζει και σημαντικά μειονεκτήματα, όπως:

- Στηρίζεται σε ένα απλοϊκό μοντέλο ΠΣ και συχνά αγνοεί τα ιδιαίτερα χαρακτηριστικά και τις απαιτήσεις του οργανισμού στον οποίο ανήκει το ΠΣ.
- Εμπεριέχει σημαντική υποκειμενικότητα στις εκτιμήσεις, τόσο της αξίας των αγαθών, όσο και στην αποτίμηση των απειλών και της ευπάθειας. Η υποκειμενικότητα αυτή συχνά συγκαλύπτεται πίσω από την αυστηρότητα των μαθηματικών μοντέλων, στα οποία στηρίζεται, τη συστηματικότητα των περισσότερων μεθόδων ανάλυσης κινδύνου και την «αντικειμενικότητα» των εργαλείων που υποστηρίζουν τις σχετικές μεθόδους.

- Βασίζεται σε απλές στατιστικές μεθόδους για τον υπολογισμό της πιθανότητας εμφάνισης μιας απειλής. Η εγκυρότητα της εφαρμογής των μεθόδων αυτών στον τομέα της ασφάλειας ΠΣ έχει αμφισβητηθεί από πολλούς μελετητές [9].

3. Μεθοδολογία Διαχείρισης Κινδύνου ΠΣ

3.1. Γενικά

Όπως προαναφέρθηκε, η έννοια της διαχείρισης του κινδύνου βασίζεται στον προγραμματισμό και την εφαρμογή συγκεκριμένων διαδικασιών προκειμένου να μειωθεί η σοβαρότητα των παραγόντων του κινδύνου που έχουν προσδιοριστεί κατά τη διάρκεια της διαδικασίας της Ανάλυσης. Οι βασικές δραστηριότητες που ακολουθεί η διαχείριση κινδύνου αναλύονται σύμφωνα με τις παρακάτω ενότητες.

3.2. Εκτίμηση Κινδύνου ΠΣ

Πολύ συχνά, οι οργανισμοί δεν προβαίνουν σε επαρκή εκτίμηση των κινδύνων στο χώρο εργασίας τους. Αυτό που είναι απαραίτητο, είναι μια ολοκληρωμένη προσέγγιση για την εκτίμηση κινδύνου η οποία θα λαμβάνει υπόψη τα διάφορα στάδια της εκτίμησης κινδύνου, τις διαφορετικές ανάγκες κάθε εργοδότη και τον εξελισσόμενο κόσμο της εργασίας.

Η εκτίμηση κινδύνου αποτελεί την αρχή της διαδικασίας διαχείρισης κινδύνου, ένα πρώτο βήμα προς τη συστηματική διαχείριση της ασφάλειας των ΠΣ. Εάν η διαδικασία εκτίμησης κινδύνου δεν πραγματοποιηθεί σωστά ή δεν πραγματοποιηθεί καθόλου, τότε είναι αδύνατο να θεσπιστούν τα κατάλληλα προληπτικά μέτρα. Η εκτίμηση κινδύνου πρέπει να είναι η απαρχή της προσέγγισης για τη διαχείριση των κινδύνων και να αποτελεί τμήμα μιας ορθής και ολοκληρωμένης προσέγγισης για τη διαχείριση της ασφάλειας.

Η διαδικασία εκτίμησης κινδύνων περιλαμβάνει τα επτά βήματα που αναφέρονται παρακάτω [3]:

1. Πληροφορίες σχετικά με το έργο και την αναθέτουσα αρχή: οι συγκεκριμένες πληροφορίες αφορούν το ΠΣ, τον οργανισμό και άλλα παρόμοια έργα πληροφορικής. Η συλλογή αυτών των πληροφοριών βοηθά στην κατανόηση των αναγκών του έργου και του οργανισμού.
2. Πιθανοί κίνδυνοι: στο βήμα αυτό αναζητούνται οι πιθανοί κίνδυνοι κατά τομέα και δημιουργείται μια λίστα καταγραφής τους.

3. Αξιολόγηση ήδη υπαρχόντων ελέγχων: δημιουργείται μια λίστα υπαρχόντων και υποσχεδιασμό ελέγχων.
4. Εκτίμηση πιθανότητας εμφάνισης κινδύνων: παρουσιάζονται τα αίτια εμφάνισης κινδύνου, ο βαθμός έκθεσης στον κίνδυνο και οι υπάρχοντες μηχανισμοί ελέγχου, έτσι ώστε να εκτιμηθεί η πιθανότητα εμφάνισής τους.
5. Αξιολόγηση επιπτώσεων: παρουσιάζονται οι επιπτώσεις κάθε κινδύνου μέσα από την ανάλυση των τομέων που εκτίθενται στον κίνδυνο και της ευαισθησίας του κάθε τομέα.
6. Χαρακτηρισμός επιπέδου έκθεσης σε κάθε κίνδυνο: περιλαμβάνει τον συνυπολογισμό πιθανότητας εμφάνισης και επιπτώσεων του κάθε κινδύνου
7. Σύνταξη αναφοράς με τα αποτελέσματα της παραπάνω ανάλυσης: από τη συλλογή των πληροφοριών των προηγούμενων βημάτων βγαίνει το πόρισμα της εκτίμησης των κινδύνων.

Οι πληροφορίες που πρέπει να συλλεχθούν σχετίζονται με: hardware, software, διεπαφές συστημάτων, βάσεις δεδομένων, στελέχη που θα υποστηρίξουν το νέο σύστημα, καθώς και η αποστολή, η αξία και η ευαισθησία του νέου συστήματος.

Επιπλέον πληροφορίες, που σχετίζονται με το λειτουργικό περιβάλλον του συστήματος και είναι εξίσου σημαντικές για τη διαδικασία διαχείρισης του κινδύνου, αποτελούν: οι λειτουργικές απαιτήσεις του συστήματος, οι πολιτικές ασφαλείας συστημάτων, η αρχιτεκτονική των συστημάτων ασφαλείας, η τρέχουσα δικτυακή τεχνολογία, η προστασία αποθηκευμένων πληροφοριών, η ροή πληροφοριών σχετικών με το σύστημα, οι τεχνικοί έλεγχοι που χρησιμοποιούνται για το ΠΣ, οι διοικητικοί έλεγχοι για την προστασία του συστήματος, οι λειτουργικοί έλεγχοι, η ασφάλεια των εγκαταστάσεων του οργανισμού και η ασφάλεια σε σχέση με το φυσικό περιβάλλον του ΠΣ.

Η συλλογή όλων αυτών των πληροφοριών προϋποθέτει προσεκτική, επιστημονική και αυστηρά καθορισμένη ενασχόληση από τα άτομα που θα κληθούν να τις συλλέξουν. Τα αποτελέσματα της έρευνας πρέπει να έχουν ουσιαστική αξία, να είναι αξιόπιστα και τεκμηριωμένα και να μπορούν να προσφέρουν στη διαδικασία εκτίμησης κινδύνων ορθά συμπεράσματα. Παρακάτω ακολουθούν τεχνικές για τη συγκέντρωση των πληροφοριών που απαιτούνται [12]:

✓ Ερωτηματολόγια

Το προσωπικό αξιολόγησης των κινδύνων μπορεί να αναπτύξει ένα ή περισσότερα ερωτηματολόγια (εικόνα 4) για να συλλέξει τις σχετικές πληροφορίες και να τα διανείμει στο προσωπικό που σχεδιάζει ή υποστηρίζει το ΠΣ.

- Ποιοι είναι επικυρωμένοι χρήστες;
- Ποιος είναι ο σκοπός του οργανισμού;
- Ποιος είναι ο σκοπός του συστήματος σε σχέση με την αποστολή;
- Πόσο σημαντικό είναι το σύστημα στην αποστολή του οργανισμού;
- Ποια είναι η απαίτηση διαθεσιμότητας του συστήματος;
- Τι είδους πληροφορία παράγεται, καταναλώνεται, επεξεργάζεται, αποθηκεύεται και ανακτάται από το σύστημα;
- Πόσο σημαντική είναι η πληροφορία στην αποστολή του οργανισμού;
- Ποια ροή ακολουθεί η πληροφορία;
- Τι είδους πληροφορία επεξεργάζεται και αποθηκεύεται στο σύστημα (πχ. Οικονομική, προσωπική, έρευνας και ανάπτυξης, ιατρική, εντολών και ελέγχου);
- Ποια είναι το επίπεδο ευαισθησίας (ή ταξινόμησης) της πληροφορίας;
- Ποια από τις πληροφορίες που διαχειρίζεται το σύστημα δεν θα πρέπει να αποκαλυφθεί και σε ποιον;
- Που συγκεκριμένα επεξεργάζεται και αποθηκεύεται η πληροφορία;
- Ποια είναι τα είδη αποθήκευσης της πληροφορίας;
- Ποιες είναι οι απαιτήσεις για της διαθεσιμότητα και την ακεραιότητα της πληροφορίας;
- Ποια θα ήταν η επίδραση στην αποστολή του οργανισμού εάν το σύστημα ή η πληροφορία δεν ήταν αξιόπιστη;
- Πόσος είναι ο χρόνος μη λειτουργίας του συστήματος που μπορεί να αντέξει ο οργανισμός; Τι συσχέτιση θα είχε αυτός ο χρόνος με τον χρόνο επιδιόρθωσης του συστήματος; Σε τι άλλες εναλλακτικές επιλογές επεξεργασίας ή επικοινωνίας θα μπορούσε να έχει πρόσβαση ο χρήστης;
- Θα μπορούσε μία δυσλειτουργία του συστήματος να έχει ως αποτέλεσμα τον τραυματισμό;

Εικόνα 5: Υπόδειγμα ερωτηματολογίου

✓ Συνεντεύξεις

Οι συνεντεύξεις πραγματοποιούνται στο προσωπικό υποστήριξης του ΠΣ και του διοικητικού προσωπικού του οργανισμού και μπορούν να προσφέρουν στα άτομα που πραγματοποιούν την αξιολόγηση των κινδύνων χρήσιμες πληροφορίες για την αξία και την αποστολή του νέου συστήματος, καθώς και τις αντιδράσεις των στελεχών στην εισαγωγή νέων τεχνολογιών. Οι συνεντεύξεις αυτές βοηθούν επίσης στην κατανόηση των λειτουργικών χαρακτηριστικών του οργανισμού και στην αξιολόγηση του φυσικού περιβάλλοντος όπου θα εγκατασταθεί το νέο πληροφοριακό σύστημα.

- ✓ Πόρισμα εμπειρογνωμόνων

Περιλαμβάνει την παρακολούθηση και τη συγκέντρωση πληροφοριών σχετικά με το λειτουργικό και φυσικό περιβάλλον του ΠΣ από το προσωπικό αξιολόγησης κινδύνων, ύστερα από δική τους προσωπική παρατήρηση στο περιβάλλον του οργανισμού. Μέσω αυτού του πορίσματος υλοποιείται η καταγραφή γεγονότων με βάση την αμεροληψία και τη διορατικότητα των εμπειρογνωμόνων.

- ✓ Αναθεώρηση εγγράφων

Περιλαμβάνει πολιτικά έγγραφα (π.χ. νομοθεσία, κρατικές οδηγίες), έγγραφα συστήματος (π.χ. οδηγός χρήσης, διοικητικό εγχειρίδιο συστημάτων, σχέδιο του συστήματος και κατάλογος απαιτήσεων, τίτλοι ιδιοκτησίας) και έγγραφα ασφαλείας (π.χ. προηγούμενη έκθεση λογιστικού ελέγχου και αξιολόγησης κινδύνου, αποτελέσματα δοκιμής συστημάτων, σχεδιασμός ασφαλείας συστημάτων, διαδικασίες ασφαλείας). Τα συγκεκριμένα έγγραφα παρέχουν πληροφορίες για το σχηματισμό μιας άρτιας εικόνας του οργανισμού και της αξίας και λειτουργικότητας του νέου ΠΣ για αυτόν.

- ✓ Πληροφορίες για παρόμοια ΠΣ που έχουν ήδη υλοποιηθεί

Μέσω αυτών των πληροφοριών μπορεί να δοθούν απαντήσεις σε θέματα αντιμετώπισης των επιπτώσεων αφού μπορεί να χρησιμοποιηθεί η προγενέστερη πείρα σε παρόμοια ΠΣ, ώστε να αποφευχθούν λάθη και παραλήψεις του παρελθόντος.

- ✓ Χρήση αυτοματοποιημένου ανιχνευτικού εξοπλισμού

Περιλαμβάνει δυναμικές τεχνικές μεθόδους που μπορούν να χρησιμοποιηθούν για τη συλλογή πληροφοριών.

Αφού συλλεχθούν όλες οι απαραίτητες πληροφορίες, ακολουθεί ο προσδιορισμός των ίδιων των κινδύνων. Η εκτίμηση κινδύνων είναι μια επιστημονική διαδικασία και απαιτεί ένα συνδυασμό γνώσεων, εμπειρίας, πλούσιας φαντασίας και διορατικότητας προκειμένου να εντοπιστούν όλοι οι πιθανοί κίνδυνοι πέραν των τυποποιημένων. Οι πιθανοί κίνδυνοι μπορούν να κατηγοριοποιηθούν ανάλογα με την προέλευσή τους σε:

- Φυσικές καταστροφές: π.χ. σεισμοί, πλημμύρες
- Φυσικό και θεσμικό περιβάλλον του ΠΣ: π.χ. παλαιότητα των εγκαταστάσεων, ηλεκτροδότηση, γειτονικές εγκαταστάσεις και περιβάλλον χώρος του οργανισμού, κρατικές παροχές
- Ανθρώπινος παράγοντας: π.χ. άτομα που σκόπιμα θα προσπαθήσουν να βλάψουν τη λειτουργία του συστήματος ή να την εκμεταλλευτούν για προσωπικό τους όφελος, ανταγωνιστές, hackers
- Κίνδυνοι τεχνολογίας: π.χ. μη λειτουργικές τεχνολογίες, απαρχαιωμένες τεχνολογίες, μη συμβατότητα νέων τεχνολογιών με τον ήδη υπάρχον εξοπλισμό, μη συμβατότητας του εξοπλισμού του ίδιου του ΠΣ
- Επιχειρησιακοί κίνδυνοι: π.χ. μη αφομοίωση νέων τεχνολογιών άμεσα από τη λειτουργία του οργανισμού, καθυστερήσεις από νέες ανάγκες που θα μπορούσαν να καλυφθούν από το νέο λογισμικό, λόγω πρόχειρου αρχικού σχεδιασμού ή της ελλιπής εκπαίδευσης προσωπικού
- Κίνδυνοι οργάνωσης του έργου: π.χ. αδυναμία στη λήψη αποφάσεων και διοίκησης του έργου

Τον προσδιορισμό των κινδύνων ακολουθεί η αξιολόγηση των υπαρχόντων μηχανισμών ελέγχου των ΠΣ του οργανισμού. Οι συγκεκριμένοι μηχανισμοί έχουν να κάνουν με την ασφάλεια του ΠΣ και δεν αφορούν όλες τις κατηγορίες κινδύνων που μπορούν να το προσβάλλουν. Η αξιολόγηση αυτή σκοπό έχει να εντοπιστούν τυχόν ελλείψεις και αδυναμίες στα υπάρχοντα συστήματα ασφαλείας ούτως ώστε να είναι πιο εύκολος αργότερα ο σχεδιασμός των διαδικασιών ασφαλείας του νέου ΠΣ.

3.3. Αξιολόγηση Κινδύνου ΠΣ

Η διαδικασία αξιολόγησης κινδύνου αναλύεται από τεχνικές ανάλυσης κινδύνου, την ποιοτική και την ποσοτική.

Ποιοτική Ανάλυση

Η πρώτη φάση της ανάλυσης είναι η ποιοτική αναγνώριση και υπάρχουν πολλές διαφορετικές τεχνικές με τις οποίες μπορεί να επιτευχθεί. Η ταυτοποίηση μπορεί να επιτευχθεί από:

- ✓ συνεντεύξεις με τα βασικά μέλη της ομάδας του ΠΣ
- ✓ διοργάνωση συναντήσεων ανταλλαγής ιδεών με όλα τα ενδιαφερόμενα μέρη.
- ✓ χρησιμοποίηση της προσωπικής εμπειρίας του αναλυτή κινδύνου.
- ✓ επανεξέταση του παρελθόντος της εταιρικής εμπειρίας, εάν τηρούνται τα βιβλία αποτίμησης.

Εικόνα 6: Ποιοτική Ανάλυση

Τα βήματα που περιγράφονται παρακάτω αναλύουν την λογική των ποιοτικών αναλύσεων κινδύνων:

1. Καθορισμός του σκοπού: Πριν αρχίσει η ανάλυση πρέπει να περιγραφεί το ΠΣ και να καθοριστεί με ακρίβεια ο σκοπός και η εμβέλειά της. Η ανάλυση πρέπει να επικεντρώνεται στα συστήματα εκείνα στα οποία υπάρχει άμεσος τρόπος παρέμβασης και για να αποφευχθεί η ολίσθησή της πρέπει να καθοριστούν με σαφή τρόπο τα όρια της. Στα ΠΣ οι στόχοι της ανάλυσης κινδύνων έχουν να κάνουν με το αντίκτυπο που έχουν οι απειλές στην ακεραιότητα, εμπιστευτικότητα και τη διαθεσιμότητα των πληροφοριών.
2. Δημιουργία ομάδας ανάλυσης κινδύνων: Στο συγκεκριμένο βήμα κρίνεται απαραίτητη η δημιουργία μιας ικανής ομάδας ανάλυσης κινδύνων. Πολλοί ειδικοί ασφαλείας επιλέγουν να κάνουν την ανάλυση μόνοι τους ή σε συνεργασία με την ομάδα

ασφαλείας του ίδιου του οργανισμού. Μια πιο αποτελεσματική διαδικασία ανάλυσης, όμως, πρέπει να περιλαμβάνει στην ομάδα άτομα με εμπειρία από όλες τις κατηγορίες χρηστών και διαχειριστών του ΠΣ, και επιπλέον, εφόσον χρειασθεί, άτομα με εξειδικευμένες γνώσεις (π.χ. για φυσική ασφάλεια ή νομικές γνώσεις).

3. Αναγνώριση απειλών: Η ομάδα ανάλυσης κινδύνων πρέπει να αναγνωρίσει τις διάφορες απειλές που μπορεί να προκαλέσουν απώλειες για κάθε περιουσιακό στοιχείο του οργανισμού.
4. Αξιολόγηση συχνότητας απειλών: Η ομάδα ανάλυσης κινδύνων πρέπει να προσδιορίσει πόσο συχνά αναμένεται να συμβεί η κάθε μια από τις καταγεγραμμένες απειλές. Στο βήμα αυτό δε χρειάζεται να υπολογιστεί η ακριβής συχνότητα της εμφάνισης των απειλών, αρκεί να προσδιοριστεί το πόσο συχνά ή σπάνια εμφανίζεται μια απειλή με βάση μια συγκεκριμένη κλίμακα.
5. Αξιολόγηση απωλειών: Η ομάδα ανάλυσης κινδύνων προσπαθεί να υπολογίσει τις απώλειες που ενδέχεται να προκύψουν σε περίπτωση που μια απειλή πραγματοποιηθεί. Οι απώλειες υπολογίζονται για κάθε περιουσιακό στοιχείο και για κάθε απειλή που αντιστοιχεί σε αυτό. Για την πληρότητα και ορθότητα της ανάλυσης η αξιολόγηση πρέπει να γίνει σαν να μην υπάρχει κανένα αντίμετρο εγκατεστημένο στο ΠΣ.
6. Υπολογισμός δείκτη κινδύνου: Σε αυτή τη φάση η ομάδα προσθέτει τους αριθμούς της συχνότητας και της απώλειας και βρίσκει το δείκτη κινδύνου, ο οποίος κυμαίνεται μεταξύ των τιμών 2 και 10. Ο δείκτης κινδύνου αναγράφεται σε έναν πίνακα και ο πίνακας ταξινομείται με βάση αυτόν, από τη μεγαλύτερη τιμή στη μικρότερη.
7. Αναγνώριση αντιμέτρων: Αφού δοθούν προτεραιότητες στους διάφορους κινδύνους ακολουθεί η αναγνώριση των αντιμέτρων που μπορούν να τους αντιμετωπίσουν. Αρχικά, αναλύονται οι ευπάθειες των περιουσιακών στοιχείων στις διάφορες απειλές και έπειτα γίνεται προσπάθεια εύρεσης των κατάλληλων αντιμέτρων που προσφέρουν αποδεκτό βαθμό ασφάλειας. Τα αντίμετρα χωρίζονται σε τέσσερις κατηγορίες: Πρόληψη, Διασφάλιση, Ανίχνευση, Επαναφορά.
8. Ανάλυση κόστους / οφέλους: Επειδή κάθε αντίμετρο έχει κάποιο κόστος (χρήμα, εργατοώρες, παρεμπόδιση της κανονικής λειτουργίας της επιχείρησης κ.ά.), πρέπει να λαμβάνεται υπόψη και να συγκρίνεται με το όφελος από την χρήση του αντιμέτρου.

9. Ταξινόμηση αντιμέτρων με βάση την προτεραιότητα: Η ομάδα ανάλυσης κινδύνων ταξινομεί τα αντίμετρα με βάση την προτεραιότητα για την υλοποίηση. Επειδή οι διατιθέμενοι πόροι για την ασφάλεια είναι περιορισμένοι, η διοίκηση του οργανισμού στηρίζεται στην ομάδα για την παροχή επαρκών πληροφοριών ώστε να προβεί σε σωστές αποφάσεις. Οι παράγοντες που επηρεάζουν τη σειρά προτεραιότητας είναι ο λόγος κόστους / οφέλους, ο αριθμός των απειλών του αντίμετρου, το κατά πόσο μπορεί να υλοποιηθεί εσωτερικά στον οργανισμό ή χρειάζεται βοήθεια από εξωτερικούς φορείς κ.ά.. Στο βήμα αυτό, συχνά, παρουσιάζονται οι λόγοι που οδήγησαν στη συγκεκριμένη επιλογή προτεραιοτήτων για τα αντίμετρα ώστε να γίνει κατανοητή από τη διοίκηση.
10. Παρουσίαση ανάλυσης κινδύνων: Τα αποτελέσματα της ανάλυσης κινδύνου παρουσιάζονται στην διοίκηση του οργανισμού με μορφή έκθεσης. Η έκθεση αυτή υπηρετεί δύο σκοπούς: την αναφορά των αποτελεσμάτων και τη δημιουργία μιας βάσης για μελλοντικές αναλύσεις κινδύνων.

<u>Ποσοτική Ανάλυση</u>

Η ποσοτική ανάλυση έπεται της ποιοτικής ανάλυσης και προσπαθεί να προσδιορίσει με αριθμητικές τιμές κάθε παραμέτρου της ανάλυσης κινδύνων. Η διαδικασία αυτή χρησιμοποιεί τεχνικές όπως η προσομοίωση Monte Carlo και η ανάλυση αποφάσεων, έτσι ώστε να [13]:

- ✓ Υπολογιστεί η πιθανότητα επίτευξης ενός συγκεκριμένου στόχου του ΠΣ.
- ✓ Ποσοτικοποιηθεί η έκθεση σε κίνδυνο του ΠΣ και να υπολογίσει ο επιπλέον χρόνος και το επιπλέον κόστος που ενδεχομένως να απαιτείται.
- ✓ Αναγνωρίσει τους κινδύνους που απαιτούν τη μεγαλύτερη προσοχή ποσοτικοποιώντας τη συμβολή τους στη συνολική έκθεση σε κίνδυνο του ΠΣ.
- ✓ Αναγνωρίσει ρεαλιστικούς και πραγματοποιήσιμους στόχους για το κόστος, το χρόνο, τις δυνατότητες και την ποιότητα του ΠΣ.

Σύμφωνα με τη διεθνή βιβλιογραφία, έχουν αναπτυχθεί διάφορες τεχνικές για την ανάλυση των επιδράσεων του κινδύνου στο τελικό κόστος και το χρονοδιάγραμμα των ΠΣ [14]:

Εικόνα 7: Ποσοτική Ανάλυση

Ανάλυση ευαισθησίας: Η συγκεκριμένη διαδικασία διεξάγεται για παραπάνω από έναν κίνδυνο και περιγράφει την επίδραση στο σύνολο του συστήματος με την αλλαγή μιας μεταβλητής κινδύνου, όπως οι καθυστερήσεις στο σχεδιασμό ή στο κόστος των υλικών. Η σημαντικότητά της είναι ότι συχνά τονίζει πως μια αλλαγή μιας μεταβλητής μπορεί να παράγει σημαντική διαφορά στο αποτέλεσμα του συστήματος.

Πιθανοθεωριτική ανάλυση: Καταγράφει μια σειρά πιθανοτήτων για κάθε κίνδυνο και θεωρεί τις επιδράσεις των κινδύνων σε συνδυασμό. Η μέθοδος αυτ, γνωστή και ως «Προσομοίωση Monte Carlo», βασίζεται στον τυχαίο υπολογισμό των τιμών που εμπίπτουν εντός συγκεκριμένης κατανομής πιθανοτήτων που περιγράφονται συχνά χρησιμοποιώντας τρεις εκτιμήσεις: ελάχιστη, μέση και μέγιστη. Το συνολικό αποτέλεσμα για το ΠΣ προέρχεται από το συνδυασμό των τιμών που επιλέχθηκαν για κάθε έναν από τους κινδύνους. Ο υπολογισμός των τιμών επαναλαμβάνεται πολλές φορές έτσι ώστε να αποκτήσουν την κατανομή πιθανοτήτων των αποτελεσμάτων του ΠΣ.

Δένδρα απόφασης: Απεικονίζουν τα δεδομένα και τις πληροφορίες με δενδροειδή μορφή (δένδρα απόφασης) μέσω της οποίας γίνεται πιο εύκολη η ανάλυση των στοιχείων. Τα δένδρα απόφασης είναι γνωστά και ως δίκτυα ροής απόφασης ή διαγράμματα απόφασης και αποτελούν ισχυρά μέσα κατανόησης και ανάλυσης προβλημάτων στα οποία λαμβάνονται διαδοχικές αποφάσεις και μεταβλητά με το χρόνο αποτελέσματα.

Στην περίπτωση που «ποσοτικοποιηθούν» όλες οι συνιστώσες, όπως η αξία των περιουσιακών στοιχείων, η συχνότητα των απειλών, η αποτελεσματικότητα των αντίμετρων[2], το κόστος των αντίμετρων, η αβεβαιότητα και η πιθανότητα, τότε η ανάλυση ονομάζεται πλήρως ποσοτική. Τα πλεονεκτήματα που προκύπτουν από την μέθοδο της ποσοτική ανάλυσης είναι τα εξής:

- ✓ Τα αποτελέσματα έχουν το κύρος της μαθηματικής απόδειξης.
- ✓ Τα αποτελέσματα μπορούν να εκφραστούν σε γλώσσα κατανοητή από τους διαχειριστές της επιχείρησης.
- ✓ Η ανάλυση κόστους/οφέλους είναι πιο εύκολη και άμεση.
- ✓ Η αξία των περιουσιακών στοιχείων του ΠΣ, όσον αφορά την εμπιστευτικότητα, ακεραιότητα και διαθεσιμότητα, γίνεται καλύτερα κατανοητή όταν εκφράζεται σε χρηματικά ποσά.

3.4. Σχέδιο Δράσης Αντιμετώπισης Κινδύνου ΠΣ

Το Σχέδιο Δράσης Αντιμετώπισης Κινδύνου περιλαμβάνει διαδικασίες για τον καθορισμό προτεραιοτήτων και την αξιολόγηση και εφαρμογή των κατάλληλων μέτρων αντιμετώπισης των κινδύνων που απειλούν το ΠΣ.

Η πρώτη διαδικασία του σχεδίου δράσης αναφέρεται στον μετριασμό των κινδύνων, μια συστηματική διαδικασία που χρησιμοποιείται από την ανώτερη διαχείριση για τη μείωση των κινδύνων στους οποίους εκτίθεται το ΠΣ. Ο στόχος αυτός μπορεί να επιτευχθεί με διάφορες επιλογές όπως την αποδοχή κινδύνου, την αποφυγή κινδύνου, τον περιορισμό επιπτώσεων, τον προγραμματισμό κινδύνου, την έρευνα και αναγνώριση ή την μεταφορά κινδύνου.

Η στρατηγική που εφαρμόζεται για το μετριασμό του κινδύνου ποικίλει ανάλογα με τη φύση του, αλλά και τις ιδιαιτερότητες του κάθε ΠΣ. Τα άτομα ή ομάδες που έχουν την ευθύνη για το σχεδιασμό και την υλοποίηση του ΠΣ και που γνωρίζουν τους πιθανούς κινδύνους και τη σημαντικότητα αυτών, οφείλουν να χρησιμοποιούν τις κατάλληλες

[2] Αντίμετρο (countermeasure): μηχανισμός ή διαδικασία που αποσκοπεί στην μείωση των επιμέρους κινδύνων στους οποίους εκτίθεται το ΠΣ

τεχνολογίες μεταξύ των διαφόρων προϊόντων ασφαλείας, παράλληλα με την κατάλληλη επιλογή μεθόδου μετριασμού κινδύνου.

Η διαδικασία μετριασμού του κινδύνου αποτελείται από τα ακόλουθα βήματα[12]:

1. Καθορισμός προτεραιοτήτων ενεργειών
2. Αξιολόγηση προτεινόμενων ελέγχων
3. Ανάλυση οφέλους-κόστους
4. Επιλογή μεθόδου
5. Ανάθεση αρμοδιοτήτων
6. Ανάπτυξη σχεδίου εφαρμογής προστασίας του έργου
7. Αποτέλεσμα εφαρμογής επιλεγμένης μεθόδου

Τα μέτρα, που καλούνται να πάρουν οι διαχειριστές για το μετριασμό των κινδύνων, μπορούν να κατηγοριοποιηθούν σε τεχνικά (μέτρα υποστήριξης, αποτρεπτικοί έλεγχοι, έλεγχοι ανίχνευσης και ανάκαμψης), διαχειριστικά (αποτρεπτικοί διοικητικοί έλεγχοι, ανιχνευτικοί διοικητικοί έλεγχοι και διοικητικοί έλεγχοι αποκατάστασης) και λειτουργικά (λειτουργικοί αποτρεπτικοί έλεγχοι, λειτουργικοί ανιχνευτικοί έλεγχοι). Πιο συγκεκριμένα, οι διαχειριστές καλούνται να επιλέξουν τον τρόπο με τον οποίο θα αντιμετωπίσουν τους διάφορους κινδύνους, ανάμεσα από αυτές τις κατηγορίες, καθώς υπάρχουν συνήθως περισσότερες από μία προσεγγίσεις για την αντιμετώπιση ενός κινδύνου. Για τη μεγιστοποίηση της προστασίας του ΠΣ μπορεί να χρησιμοποιηθεί και ένας συνδυασμός τέτοιων μέτρων. Στην περίπτωση που τα μέτρα αυτά χρησιμοποιηθούν κατάλληλα, μπορούν να αποτρέψουν την εμφάνιση ενός κινδύνου, να μετριάσουν το επίπεδο έκθεσης σε αυτόν ή και να προσφέρουν τα μέσα αντιμετώπισης των επιπτώσεων από την ενδεχόμενη εκδήλωση μιας απειλής.

Αφού προσδιοριστούν όλοι οι πιθανοί έλεγχοι και αξιολογήσεις των δυνατοτήτων τους και της αποτελεσματικότητάς τους, ακολουθεί η διαδικασία ανάλυσης κόστους-οφέλους. Με βάση αυτή την ανάλυση καθορίζονται ποιοι έλεγχοι είναι κατάλληλοι για την κάθε μία από τις περιπτώσεις και περιλαμβάνει τα εξής:

- Καθορισμός επιπτώσεων από την εφαρμογή νέων ελέγχων ή την αναβάθμιση των υπαρχόντων.

- Καθορισμός επιπτώσεων από τη μη εφαρμογή νέων ελέγχων ή την αναβάθμιση των υπαρχόντων.
- Υπολογισμός του κόστους εφαρμογής (αγορά εξοπλισμού, μείωση αποτελεσματικότητας, κόστος εκπαίδευσης, κόστη συντήρησης κ.ά.)

Κόστος, βέβαια, δεν υπάρχει μόνο για τον απαραίτητο έλεγχο των συστημάτων όπως προαναφέρθηκε, αλλά μπορεί να προκύψει και από τη μη εφαρμογή του ελέγχου. Με το συσχετισμό του αποτελέσματος της μη εφαρμογής ενός ελέγχου με την εφαρμογή αυτού, η διοίκηση δύναται να αποφασίσει εάν είναι εφικτό να αποποιηθεί την εφαρμογή του [12].

Μία ακόμα διαδικασία που μπορεί να διενεργήσει από τη μεριά της η διοίκηση συστημάτων είναι και η ανάλυση του μεγέθους της μείωσης του κινδύνου. Η ενέργεια αυτή μπορεί να προκύψει από την εισαγωγή των νέων μέτρων ή την αναβάθμιση των υπαρχουσών, μέσω της μείωσης της πιθανότητας εμφάνισης ενός κινδύνου ή των επιπτώσεων του (οι παράμετροι αυτοί αναλύθηκαν στη διαδικασία μετρίασης του κινδύνου). Εισάγοντας νέες μεθόδους ή αναβαθμίζοντας τις παλαιότερες, οι επιχειρήσεις μπορούν να μετριάσουν τους κινδύνους τους.

3.5. Παρακολούθηση Κινδύνων ΠΣ

Η διαδικασία διαχείρισης κινδύνου ολοκληρώνεται με την παρακολούθηση των εφαρμοσμένων ελέγχων στο ΠΣ. Η παρακολούθηση αυτών κρίνεται απαραίτητη γιατί υπάρχει πιθανότητα να εμφανιστούν νέοι κίνδυνοι, συνεπώς αποτελεί μία διαρκή διαδικασία που λαμβάνει χώρα καθ’ όλη τη διάρκεια υλοποίησης του ΠΣ.

Οι πληροφορίες που απαιτούνται για την παρακολούθηση των κινδύνων κατά τη διάρκεια υλοποίησης του ΠΣ είναι [13]:

- Σχέδιο διαχείρισης κινδύνου
- Σχέδιο αντιμετώπισης κινδύνων
- Αναφορές λειτουργίας του έργου
- Επιπρόσθετη αναγνώριση και ανάλυση
- Αλλαγές στις απαιτήσεις του ΠΣ

Οι μέθοδοι που χρησιμοποιούνται για τη συλλογή και καταγραφή των παραπάνω πληροφοριών είναι[13]:

- Έλεγχοι αντιμετώπισης κινδύνων
- Περιοδική ανασκόπηση των κινδύνων που απειλούν το έργο
- Ανάλυση κεκτημένης αξίας
- Τεχνική αξιολόγηση επιδόσεων
- Επιπρόσθετος σχεδιασμός αντιμετώπισης κινδύνων

Τα αποτελέσματα που προκύπτουν από τη διαδικασία της παρακολούθησης των κινδύνων ΠΣ είναι μια σειρά από ενέργειες που σχετίζονται με [13]:

- Διαδικασίες εκτός αρχικού σχεδιασμού
- Διορθωτικές ενέργειες
- Αλλαγές των απαιτήσεων του ΠΣ
- Ενημέρωση βάση των εξελίξεων του σχεδίου αντιμετώπισης κινδύνων
- Τήρηση αρχείων με στοιχεία κινδύνων

Στην επόμενη ενότητα παρουσιάζονται κάποιες βέλτιστες πρακτικές διαχείρισης κινδύνου ΠΣ που εφαρμόζονται και έχουν δώσει λύσεις σε πολλές επιχειρήσεις μέχρι σήμερα.

4. Τεχνικές Διαχείρισης Κινδύνου ΠΣ

4.1. Εισαγωγή

Σύμφωνα με το προηγούμενο κεφάλαιο, μία μεθοδολογία δίνει το πλαίσιο, εντός του οποίου αναπτύσσονται και εφαρμόζονται μία ή περισσότερες μέθοδοι. Η έννοια της μεθόδου αναφέρεται "στον συστηματικό και προγραμματισμένο τρόπο προσεγγίσεως, εξετάσεως, αναλύσεως και ερμηνείας προβλημάτων ή φαινομένων βάσει συγκεκριμένων κανόνων…" [24].

Στην διαχείριση κινδύνου ΠΣ έχουν αναπτυχθεί μια πληθώρα μεθόδων, πολλές από τις οποίες υποστηρίζονται από εργαλεία λογισμικού (software tools). Στις ενότητες που ακολουθούν περιγράφονται ενδεικτικά πέντε από τις πιο δημοφιλείς μεθόδους.

4.2. ISO/IEC 31010 Risk management – Risk assessment guidelines

Ο Διεθνής Οργανισμός Τυποποίησης (ISO) έχει εκδώσει ένα πρότυπο σχετικά με τις τεχνικές εκτίμησης του κινδύνου το οποία ενώνει μια σειρά τεχνικών αξιολόγησης του κινδύνου, με ειδικές αναφορές σε άλλα διεθνή πρότυπα, όπου η έννοια και η εφαρμογή των τεχνικών που περιγράφονται με μεγαλύτερη λεπτομέρεια.

Το πρότυπο ISI/IEC 31010 είναι μια μεθοδολογία που επικεντρώνεται στην αξιολόγηση του κινδύνου, στις διαδικασίες και την κατάλληλη επιλογή των τεχνικών που πρέπει να ληφθούν για την αξιολόγηση του κινδύνου. Επίσης προσφέρει κατευθυντήριες οδηγίες σχετικά με την κατανόηση των κινδύνων που θα μπορούσαν να επηρεάσουν την υλοποίηση των στόχων που έχει θέσει ένας οργανισμός καθώς και την επάρκεια των ελέγχων που είναι σε διαθεσιμότητα. [15] [16]

Αξίζει να σημειωθεί ότι το συγκεκριμένο πρότυπο:

- δεν μπορεί να χρησιμοποιηθεί για σκοπούς πιστοποίησης αλλά παρέχει καθοδήγηση για τα προγράμματα εσωτερικού ή εξωτερικού ελέγχου.
- δεν προβλέπει συγκεκριμένα κριτήρια για τον εντοπισμό της ανάγκης για την ανάλυση κινδύνου

- δεν προσδιορίζει το είδος της μεθόδου ανάλυσης κινδύνου που απαιτείται για μια συγκεκριμένη εφαρμογή.
- δεν ασχολείται ειδικά με την ασφάλεια ΠΣ. Πρόκειται για ένα γενικό πρότυπο διαχείρισης κινδύνου και οποιαδήποτε αναφορά σχετικά με την ασφάλεια είναι καθαρά ενημερωτικού χαρακτήρα.

Το συγκεκριμένο πρότυπο αποτελεί προέκταση του προτύπου ISO 31000 – Διαχείρισης Κινδύνου, το οποίο αναπτύχθηκε σχετικά με τη διαχείριση των κινδύνων που μπορεί να επηρεάζουν τους οργανισμούς και να έχουν οικονομικό, επαγγελματικό κοινωνικό και περιβαλλοντικό αντίκτυπο.

Η έκδοση ISO 31000:2009 αποτελεί ένα πρότυπο με καθοδηγητικό χαρακτήρα, καθώς περιλαμβάνει μια σειρά από αρχές στα πλαίσια της διαχείρισης των κινδύνων. Σκοπός του είναι να βοηθήσει μία επιχείρηση να ολοκληρώσει με επιτυχία τους στόχους που έχει θέσει, μέσα από τη βέλτιστη προσέγγιση των ευκαιριών και των απειλών που παρουσιάζονται και την αποτελεσματική κατανομή και χρήση των πόρων για την αντιμετώπιση των επιμέρους κινδύνων. Μπορεί να εφαρμοστεί από οποιαδήποτε επιχείρηση ανεξαρτήτως μεγέθους, δραστηριότητας ή τομέα, με τρόπο καθοδηγητικό αναφορικά με τον εσωτερικό και εξωτερικό έλεγχο των προγραμμάτων, ενώ οι επιχειρήσεις με τη σειρά τους μπορούν να συγκρίνουν τις πρακτικές που χρησιμοποιούν για τη διαχείριση των κινδύνων με ένα διεθνώς αναγνωρισμένο σημείο αναφοράς, με την παροχή οδηγιών για την αποτελεσματική διαχείριση και την εταιρική διακυβέρνηση. [16]

Το πρότυπο ISO 73:2009 Είναι ένα πρότυπο που περιέχει όρους και ορισμούς αναφορικά με τη διαχείριση του κινδύνου και θεωρείται συμπληρωματικό του ISO 31000.

4.3. NIST SP800-30 Risk Management Guide for Information Technology Systems

Το NIST- National Institute of Standards and Technology) είναι γνωστό για την παραγωγή ενός ευρέως φάσματος καλογραμμένων και διεξοδικών τεχνικών προτύπων, τα οποία είναι διαθέσιμα σε όλους δωρεάν. Το Εργαστήριο Τεχνολογίας Πληροφοριών του NIST έχει δημοσιεύσει ένα νέο οδηγό για να βοηθήσει τους οργανισμούς να διαχειριστούν τις αξιολογήσεις της ασφάλειας των πληροφοριών τους. Ο συγκεκριμένος οδηγός [17] παρέχει

μια κοινή βάση σε όλο το προσωπικό ενός οργανισμού που εμπλέκεται με τη διαχείριση του κινδύνου ΠΣ με απώτερο σκοπό τη βελτίωση της ασφάλεια. Πιο αναλυτικά, παρουσιάζει τα βασικά στοιχεία του ελέγχου και των αξιολογήσεων της ασφάλειας, εξηγεί συγκεκριμένες τεχνικές που μπορούν να εφαρμοστούν και προτείνει αποτελεσματικές μεθόδους για την υλοποίηση πρακτικών ελέγχου και αξιολόγησης.

Σύμφωνα με το NIST SP800-30, για να αναπτύξουμε ένα μια δημοφιλή τεχνική που να ενισχύει τους σχεδιαστές συστήματος να σκεφτούν για τις απειλές ασφάλειας (μοντελοποίηση απειλής), συστήνεται μια απλή προσέγγιση [18] για την αξιολόγηση κινδύνου. Αυτή η προσέγγιση περιλαμβάνει:

- ✓ Αποσύνθεση της εφαρμογής, για την κατανόηση του πώς λειτουργεί η εφαρμογή, τα αγαθά της, τη λειτουργικότητά της και τη συνδεσιμότητά της.
- ✓ Προσδιορισμός και ταξινόμηση των αγαθών σε υλικές και άυλες και κατάταξή τους ανάλογα με το πόσο σημαντικές είναι. ·
- ✓ Έρευνα πιθανών ευπαθειών – τεχνικές, λειτουργικές ή διαχειριστικές. ·
- ✓ Έρευνα πιθανών απειλών – ανάπτυξη μιας ρεαλιστικής άποψης των πιθανών διανυσμάτων επίθεσης από την προοπτική του επιτιθέμενου, χρησιμοποιώντας σενάρια απειλών ή δένδρα επιθέσεων.
- ✓ Δημιουργία στρατηγικών μετριασμού. Οι στρατηγικές αναπτύσσονται για τις απειλές που θεωρούνται ρεαλιστικές.

Πιο αναλυτικά, η διαχείριση του κινδύνου που περιγράφει το πρότυπο NIST SP800-30 αποτελείται από τρεις διαδικασίες:

- Ανάλυση επικινδυνότητας: περιλαμβάνει τον εντοπισμό των απειλών και κινδύνων που μπορεί να παρουσιάσει ένα ΠΣ, καθώς και τον προσδιορισμό των αντίστοιχων μέτρων αντιμετώπισης. Η ανάλυση της επικινδυνότητας αποτελείται από εννέα βήματα:
    1. Χαρακτηρισμός συστήματος
    2. Προσδιορισμός απειλών
    3. Προσδιορισμός αδυναμιών
    4. Ανάλυση μέτρων ασφάλειας
    5. Προσδιορισμός πιθανότητας

6. Ανάλυση επιπτώσεων
7. Προσδιορισμός κινδύνου
8. Προτάσεις μέτρων ασφάλειας
9. Τεκμηρίωση αποτελεσμάτων

- Μείωση κινδύνων: σχετίζεται με την αξιολόγηση και εφαρμογή των κατάλληλων μέτρων που προσδιορίστηκαν από την ανάλυση της επικινδυνότητας με σκοπό τη μείωση των κινδύνων. Το συγκεκριμένο στάδιο περιλαμβάνει:
  - ✓ Τις υπάρχουσες επιλογές για τη μείωση του κινδύνου
  - ✓ Τη στρατηγική μείωσης του κινδύνου
  - ✓ Προσεγγίσεις για την εφαρμογή μέτρων
  - ✓ Κατηγορίες μέτρων
  - ✓ Ανάλυση κόστους – οφέλους της εφαρμογής των προτεινόμενων μέτρων
  - ✓ Τον εναπομένοντα κίνδυνο
- Αξιολόγηση και Εκτίμηση: αναλύει την ανάγκη για αξιολόγηση και εκτίμηση του κινδύνου, καθώς και των συνιστωσών που θα οδηγήσουν σε ένα επιτυχημένο πλάνο ανάλυσης και διαχείρισης του κινδύνου.

4.4. OCTAVE – Operationally Critical Threat, Asset & Vulnerability Evaluations, CERT

Η μέθοδος OCTAVE [19] [20] [21] αποτελεί μια περιεκτική και επαναληπτική μεθοδολογία που στοχεύει στην εκτίμηση επικινδυνότητας ΠΣ μεγάλων οργανισμών. Αποτελείται από ένα σύνολο εργαλείων, τεχνικών και μεθόδων για εκτίμηση και σχεδιασμό ασφάλειας πληροφοριών σε στρατηγικό επίπεδο βασισμένη στην έννοια της επικινδυνότητας.

Η OCTAVE χρησιμοποιείται για να γεφυρώσει το οργανωσιακό κενό που υπάρχει ανάμεσα στη διοίκηση και το τεχνικό τμήμα ενός οργανισμού και ταυτόχρονα προστατεύει τα συστήματα και τις πληροφορίες από μη εξουσιοδοτημένη χρήση, αλλαγή, καταστροφή ή παρέμβαση. Μέσω της συγκεκριμένης μεθόδου είναι δυνατό να αποκαλυφθούν οι μη εξουσιοδοτημένες ενέργειες χρηστών, να δημιουργηθούν σχέδια ανάκαμψης και επαναφοράς των συστημάτων και να γνωστοποιηθούν οι νομικές ενέργειες για κάθε περίσταση. Τέλος, η OCTAVE θέτει προτεραιότητες για την ανάγκη σε ασφάλεια και

πραγματοποιεί τις απαραίτητες αλλαγές λαμβάνοντας υπόψη τους περιορισμούς σε προϋπολογισμό και μέσα υλοποίησής τους.

Σύμφωνα με τη μεθοδολογία OCTAVE, μια μικρή ομάδα από το εσωτερικό της επιχείρησης ή εξωτερικοί συνεργάτες, μαζί με το τμήμα ΠΣ συνεργάζονται για να αντιμετωπίσουν τις ανάγκες του οργανισμού. Ένας οργανισμός λαμβάνει αποφάσεις για την προστασία της πληροφορίας, με βάση τους κινδύνους για την εμπιστευτικότητα, την ακεραιότητα, και τη διαθεσιμότητα των κρίσιμων περιουσιακών στοιχείων που σχετίζονται με την πληροφορία. Οι ανάγκες του οργανισμού σχετίζονται με θέματα ασφάλειας, εξισορροπώντας τρία βασικά στοιχεία:

- ✓ επιχειρησιακός κίνδυνος
- ✓ πρακτικές ασφαλείας
- ✓ τεχνολογία (εξετάζεται μόνο σε σχέση με τις πρακτικές ασφαλείας, επιτρέποντας στον οργανισμό να βελτιώσει τις πρακτικές ασφάλειας)

Όλοι οι κίνδυνοι που σχετίζονται με στοιχεία ενεργητικού, απειλές, τρωτά σημεία και οργανωτικές επιπτώσεις συνυπολογίζονται στη διαδικασία λήψης αποφάσεων, επιτρέποντας στην επιχείρηση να ταιριάξει μια πρακτική που βασίζεται στη στρατηγική με την προστασία από κινδύνους που συνδέονται με την ασφάλεια της πληροφορίας.

Η OCTAVE περιλαμβάνει τρεις ακόμα εκδόσεις (μέθοδος OCTAVE, OCTAVE-S για μικρούς οργανισμούς, OCTAVE-Allergo) οι οποίες βασίζονται στα βασικά κριτήρια της αρχικής μεθόδου τα οποία καθορίζουν τις αρχές και τα χαρακτηριστικά της διαχείρισης επικινδυνότητας.

4.5. OSSTMM – ISECOM Open Source Security Testing Methodology Manual (Institute for Security & Open Methodologies)

Ο οδηγός OSSTMM είναι ένα εγχειρίδιο για τον έλεγχο και την ανάλυση της ασφάλειας σε επίπεδο οργανισμού και παρέχεται από την ISECOM, ένα μη κερδοσκοπικό ίδρυμα για την ασφάλεια και τις ανοικτές μεθοδολογίες. Το διάγραμμα μεθοδολογίας που παρέχεται παρουσιάζει τον βέλτιστο τρόπο που μπορεί να διενεργηθεί ένας έλεγχος με δύο ή και παραπάνω ελεγκτές.

Η συγκεκριμένη μεθοδολογία είναι ανοιχτή και δίνει τη δυνατότητα σε κάθε χρήστη ασφάλειας να καταθέσει τις ιδέες του για την εκτέλεση πιο ακριβών και αποτελεσματικών δοκιμών ασφαλείας, ενώ ταυτόχρονα επιτρέπει την ελεύθερη διάδοση των πληροφοριών και της πνευματικής ιδιοκτησίας [22].

Ο βασικός στόχος της OSSTMM οδηγού είναι να δημιουργηθεί μια αποδεκτή μέθοδος για έναν αναλυτικό και επαναλαμβανόμενο έλεγχο ασφάλειας. Κάθε ειδικός δικτύων ή ασφάλειας ΠΣ που καλύπτει τις απαιτήσεις που σκιαγραφούνται σε αυτό το εγχειρίδιο, θα έχει κατορθώσει να δημιουργήσει ένα ολοκληρωμένο προφίλ ασφάλειας του ΠΣ. Πρέπει να σημειωθεί ότι σε καμία περίπτωση δεν συστήνεται να ακολουθηθεί η μεθοδολογία ως ένα διάγραμμα ροής δεδομένων.

Ο έλεγχος του δικτύου ή του συστήματος της OSSTMM περιλαμβάνει τα παρακάτω :

- Έρευνα σχετικά με το υπό δοκιμή δίκτυο ο Πληροφορίες για το δίκτυο
- Ανίχνευση των πορτών
- Προσδιορισμός της κατάστασης των πορτών στις οποίες ακούν διάφορες υπηρεσίες
- Προσδιορισμός των υπηρεσιών
- Εντοπισμός των υπηρεσιών που “τρέχουν” πίσω από τις πόρτες
- Προσδιορισμός του συστήματος
- Εντοπισμός του λειτουργικού συστήματος του Server
- Προσδιορισμός των αδυναμιών του συστήματος
- Έρευνα και επαλήθευση των ευπαθειών
- Προσδιορισμός του δρομολογητή που χρησιμοποιεί το σύστημα
- Έλεγχος του δρομολογητή
- Προσδιορισμός του firewall και της κατάστασης των πορτών
- Έλεγχος του τείχους προστασίας
- Ανακάλυψη των κωδικών όσο αφορά λογαριασμούς χρηστών και αρχείων
- Σπάσιμο κωδικών

Το πιο σημαντικό σε αυτήν την πρακτική είναι ότι οι διάφοροι επιμέρους έλεγχοι αξιολογούνται και εκτελούνται όπου είναι δυνατό και εφαρμόσιμο, έως ότου να προκύψουν τα αναμενόμενα αποτελέσματα μέσα σε ένα δεδομένο χρονικό πλαίσιο. Στην

περίπτωση αυτή, ο ελεγκτής του ΠΣ θα έχει εξετάσει τον έλεγχο σύμφωνα με το πρότυπο OSSTMM και τότε η έκθεση, θα θεωρηθεί επαρκώς λεπτομερής.

4.6. CRAMM

Η CRAMM τεχνική είναι ένα εργαλείο ποιοτικής ανάλυσης κινδύνων που αναπτύχθηκε από το Central Computer and Telecommunications Agency (CCTA) της βρετανικής κυβέρνησης το 1985 ώστε να εφοδιάσει τα διάφορα τμήματα της κυβέρνησης με μια κοινή μέθοδο ανάλυσης κινδύνων ΠΣ.

Η CRAMM έχει μεγάλο κύρος, καθώς χρησιμοποιείται σε παραπάνω από 500 επιχειρήσεις σε διάφορες χώρες παγκοσμίως, συμπεριλαμβανομένου και του NATO. Το πρόγραμμά της ακολουθεί την δική της μέθοδο, η οποία αποτιμά και βοηθάει τις επιχειρήσεις να επιτύχουν συμμόρφωση με το διεθνές στάνταρ ISO17799/BS7799.

Τα βασικά χαρακτηριστικά του προγράμματος είναι:

- Τεράστια βάση αντίμετρων (περίπου 3000 αντίμετρα) που καλύπτει όλες τις πτυχές της ασφάλειας ΠΣ και η οποία ανανεώνεται συνεχώς.
- «What if» ανάλυση.
- Εργαλεία για τη δημιουργία σχεδίων «Business Continuity».
- Οδηγούς για τη δημιουργία πολιτικών ασφαλείας.
- Οδηγούς για τη δημιουργία αναφορών με δυνατότητες χάραξης πινάκων και γραφημάτων και εξαγωγής σε διάφορες μορφές αρχείων.
- Σύγχρονο περιβάλλον σε πλατφόρμα MS Windows.
- Δυνατότητα προσαρμογής του προγράμματος στις ανάγκες του κάθε οργανισμού.

4.7. Επιλογή κατάλληλης τεχνικής

Η επιλογή μιας τεχνικής εξαρτάται από τα ιδιαίτερα χαρακτηριστικά του ΠΣ, στο οποίο πρόκειται να εφαρμοστεί, καθώς και από οικονομικούς και οργανωτικούς παράγοντες. Παρακάτω γίνεται αναφορά σε ορισμένα από τα κριτήρια επιλογής μιας τεχνικής ανάλυσης και διαχείρισης κινδύνου [1]:

- Να ανταποκρίνεται στο μέγεθος και την πολυπλοκότητα του ΠΣ.
- Να έχει χαμηλό κόστος εφαρμογής.
- Να ταιριάζει στα οργανωσιακά χαρακτηριστικά και την κουλτούρα της επιχείρησης.
- Να υποστηρίζεται από εξειδικευμένο λογισμικό.
- Τα πρόσωπα, που θα κληθούν να την εφαρμόσουν, να έχουν εμπειρία από την εφαρμογή της ή τουλάχιστον να έχουν εκπαιδευτή σε αυτήν.
- Να καλύπτει όλους τους παράγοντες (τεχνικούς και κοινωνικούς) που συνδέονται με την ασφάλεια των ΠΣ.

5. Μελέτη Περίπτωσης

5.1. Εισαγωγή

Στο κεφάλαιο αυτό θα γίνει εφαρμογή των διαδικασιών της διαχείρισης κινδύνων, όπως αυτή παρουσιάστηκε αναλυτικά προηγουμένως.

Η O.A.S. International Services είναι μια εταιρεία Outsourcing υπηρεσιών και δραστηριοποιείται στον τομέα των υπηρεσιών Τεχνολογίας Πληροφοριών και Επικοινωνίας (ΤΠΕ). Παρέχει καινοτόμες λύσεις υψηλής ποιότητας και απόδοσης σε ένα ευρύ φάσμα εθνικών και διεθνών οργανισμών του δημόσιου και του ιδιωτικού τομέα. Οι υπηρεσίες της εκτείνονται σε μια ευρεία περιοχή του κλάδου της πληροφορικής που σχετίζονται με τομείς όπως:

- ✓ Service Desk Outsourcing
- ✓ Application Management Services
- ✓ IT Resourcing & Professional services
- ✓ Infrastructure Management & IT Support

Τα πλεονεκτήματα που συντελούν στην ισχύ της συγκεκριμένης εταιρείας είναι:

- Η αποδεδειγμένη ικανότητα και η επιτυχημένη πορεία στην ανάληψη και την παράδοση μεγάλων, πολύπλοκων και υψηλού επιπέδου έργων.
- Η λεπτομερή κατανόηση των πολιτικών της Ευρωπαϊκής Ένωσης, των διαδικασιών λήψης αποφάσεων, της δομής, της πολυπλοκότητας και των αλληλεξαρτήσεων.
- Υψηλή ειδίκευση, αποτελεσματική διαχείριση και ανάπτυξη του ανθρώπινου παράγοντα.
- Ευρωπαϊκή / διεθνή κουλτούρα - παράγοντας επιτυχούς λειτουργίας στις διάφορες τοπικές αγορές σε όλη την Ευρώπη.

5.2. Περιγραφή ΠΣ

Το έργο πληροφορικής που έχει αναλάβει να υλοποιήσει η O.A.S. International Services περιλαμβάνει ανάπτυξη λογισμικού για την Διαχείριση Στοιχείων Διαγωνισμών. Οι ηλεκτρονικές αιτήσεις αποτελούν βασικό στοιχείο της υποδομής της διαχείρισης των ηλεκτρονικών διαγωνισμών και της ασφαλούς ηλεκτρονικής επικοινωνίας με τη χρήση βάσεων δεδομένων Oracle:

- ✓ Oracle Forms
- ✓ Oracle Reports
- ✓ PL/SQL programming

Η συλλογή των πληροφοριών πραγματοποιήθηκε με συνεντεύξεις, στις οποίες έλαβαν μέρος μεσαία και κατώτερα στελέχη από όλους τους τομείς της επιχείρησης, καθώς και στέλεχος της Διεύθυνσης Πληροφορικής της O.A.S. International Services. Αυτή η τακτική ακολουθήθηκε με σκοπό να εξυπηρετήσει βασικούς στόχους όπως:

1) να διευκολύνει τη διεξαγωγή της συνέντευξης,

2) να αντιμετωπίσει την πιθανή καχυποψία με την οποία μπορεί να αντιμετωπίζεται ένας εξωτερικός αναλυτής,

3) να εκπαιδεύσει τα στελέχη της εταιρείας, τα οποία θα αναλάβουν τη διαχείριση της ασφάλειας μετά τη λήξη του έργου.

Μερικές από τις εργασίες που περιλαμβάνονται στο συγκεκριμένο ΠΣ είναι:

- ✓ Διαχείριση εργασίας:
  - Εισαγωγή και Διαχείριση μεγάλου αριθμού αιτήσεων.
  - Εύκολη αξιολόγηση αιτήσεων.
  - Εισαγωγή και διαχείριση δικαιολογητικών.
  - Εισαγωγή των στοιχείων και προσόντων του υποψηφίου.

- Αντιστοίχιση των ειδικοτήτων με τις ειδικές κατηγορίες και τον καθορισμό των θέσεων.
- Αυτόματος έλεγχος αίτησης.
- Διεξαγωγή των τελικών αποτελεσμάτων

✓ Ασφάλεια του συστήματος

Το σύστημα θα διαθέτει πολλαπλά επίπεδα ασφάλειας, δηλαδή η διαφύλαξη της εμπιστευτικότητας, ακεραιότητας (ορθότητας) και διαθεσιμότητας των δεδομένων.

✓ Εξωτερικές επικοινωνίες-ανταλλαγές δεδομένων

Το σύστημα θα πρέπει να ανταλλάσσει στοιχεία με ένα Ολοκληρωμένο Πληροφοριακό Σύστημα (ΟΠΣ). Τα στοιχεία αυτά περιλαμβάνουν κατ' ελάχιστον τη μεταφορά των προσωπικών στοιχείων των χρηστών, την ανάλωση των αντιδραστηρίων και λοιπού υλικού και τις αιτήσεις μέσω του ΟΠΣ και την ενημέρωση του ηλεκτρονικού φακέλου του ΟΠΣ (επιστροφή εγκεκριμένων αποτελεσμάτων).

Σε κάθε εργαστηριακό τμήμα το σύστημα θα συνδέεται με τους αναλυτές με πλήρη εκμετάλλευση όλων των δυνατοτήτων σύνδεσης (μονόδρομη – αμφίδρομη επικοινωνία, χρήση γραμμωτού κώδικα (bar-codes), Ελέγχου Ποιότητας (quality control), έλεγχος του ψηφίου ελέγχου (check digit), κλπ).

5.3. Επιλογή τεχνικής

Ο παράγοντας «ασφάλεια» για την επιτυχία του ΠΣ οδηγεί στην επιλογή της CRAMM τεχνικής για τους ακόλουθους λόγους:

- Είναι αναγνωρισμένη ως έγκυρη και αποτελεσματική μέθοδος, γεγονός που διευκολύνει την αποδοχή της μελέτης από την διοίκηση της O.A.S. International Services.
- Είναι η πιο κατάλληλη για εφαρμογές αυτού του μεγέθους.
- Διαθέτει μια πλούσια βιβλιοθήκη αντιμέτρων.

- Το προσωπικό της O.A.S. International Services έχει αποκτήσει σημαντική εμπειρία από την εφαρμογή της συγκεκριμένης τεχνικής από παρόμοια έργα και έχει προμηθευτεί το σχετικό λογισμικό και υλικό υποστήριξης.

Οι βασικοί στόχοι της συγκεκριμένης μελέτης περίπτωσης είναι:

- ο προσδιορισμός των κινδύνων που εμπλέκονται στο έργο λογισμικού που έχει επιλεχθεί.
- Η ιεράρχηση των κινδύνων κατά σειρά σπουδαιότητας και συχνότητα εμφάνισης.
- Ο προσδιορισμός των δραστηριοτήτων που απαιτούνται από τους διαχειριστές του έργου για τον έλεγχο των κινδύνων που έχουν εντοπιστεί.

ΣΤΑΔΙΑ CRAMM	ΕΠΙΜΕΡΟΥΣ ΒΗΜΑΤΑ ΜΕΘΟΔΟΥ
Στάδιο 1 Προσδιορισμός και αξιολόγηση των αγαθών *(identification and valuation of assets)*	*Βήμα 1.1*: Δημιουργία μοντέλου ΠΣ. *Βήμα 1.2*: Αποτίμηση στοιχείων - αγαθών του ΠΣ. *Βήμα 1.3*: Επιβεβαίωση και επικύρωση της αποτίμησης.
Στάδιο 2 Ανάλυση κινδύνου *(Risk analysis)*	*Βήμα 2.1*: Προσδιορισμός των Απειλών που αφορούν το κάθε Αγαθό. *Βήμα2.2*: Εκτίμηση Απειλών *(threat assessment)* και Αδυναμιών - Σημείων Ευπάθειας *(vulnerability assessment)*. *Βήμα 2.3*: Υπολογισμός Κινδύνου για κάθε συνδυασμό Αγαθού - Απειλής. *Βήμα 2.4*: Επιβεβαίωση και Επικύρωση του βαθμού Κινδύνου
Στάδιο 3 Διαχείριση κινδύνου *(Risk management)*	*Βήμα 3.1*: Προσδιορισμός της λίστας των προτεινόμενων αντίμετρων *(safeguards - countermeasures)*. *Βήμα 3.2*: Κατάρτιση Σχεδίου - Πλάνου ασφάλειας *(security plan)*.

Όπως φαίνεται από την παραπάνω εικόνα, κάθε στάδιο εκτελείται σε συγκεκριμένα βήματα:

Στάδιο 1: Προσδιορισμός και αξιολόγηση των αγαθών

Αναφέρεται στον προσδιορισμό και την αξιολόγηση των στοιχείων των Π.Σ. που χρειάζονται προστασία. Αποτελείται από τα εξής βήματα:

Βήμα 1: Δημιουργία μοντέλου ΠΣ

Αναφέρεται στον προσδιορισμό των στοιχείων των ΠΣ που απαιτούν προστασία, δηλαδή τα δεδομένα που χειρίζονται, όπως επίσης το λογισμικό και το υλικό των ΠΣ. Τα στοιχεία αυτά βρίσκονται σε αλληλεπίδραση και η συλλογή αυτών βασίζεται στην τεκμηρίωση του συστήματος και στον πρώτο κύκλο συνεντεύξεων που αφορά το τεχνικό προσωπικό και τους κύριους χρήστες του συστήματος.

Βήμα 2: Αποτίμηση αγαθών

Κατά το στάδιο αυτό, δίνεται έμφαση στην αποτίμηση των αγαθών που διαχειρίζεται προκειμένου να προσδιοριστεί η σπουδαιότητα που έχουν αυτά για τις υπηρεσίες του οργανισμού. Η αξία κάθε κατηγορίας αγαθών αποτιμάται με βάση την «επίπτωση» που θα είχε η απώλειά της. Συγκεκριμένα εξετάζονται οι εξής περιπτώσεις:

- Μη-διαθεσιμότητα: Λιγότερο από 15 λεπτά, 1 ώρα, 3 ώρες, 12 ώρες, 1 μέρα, 2 μέρες, 1 εβδομάδα, 2 εβδομάδες, 1 μήνα, 2 μήνες και περισσότερο.
- Καταστροφή: Απώλεια των δεδομένων μετά τη λήψη του τελευταίου αντιγράφου ασφαλείας, απώλεια όλων των δεδομένων μαζί με το τηρούμενο αντίγραφο.
- Αποκάλυψη: Αποκάλυψη των δεδομένων σε μη εξουσιοδοτημένα άτομα εντός του οργανισμού, αποκάλυψη των δεδομένων σε άτομα εκτός του οργανισμού, αποκάλυψη των δεδομένων σε παρόχους υπηρεσιών.
- Μη-εξουσιοδοτημένη μεταβολή: Μικρής έκτασης σφάλματα - Μεγάλης έκτασης σφάλματα.
- Εκούσια μεταβολή των δεδομένων.
- Σφάλματα μετάδοσης δεδομένων: Παρεμβολή λανθασμένων μηνυμάτων, άρνηση αποστολής μηνύματος, άρνηση παραλαβής μηνύματος, αποτυχία αποστολής μηνύματος, επανάληψη μηνύματος, λανθασμένη δρομολόγηση, παρακολούθηση κίνησης, απώλεια ακολουθίας μηνυμάτων.

Για κάθε υποπερίπτωση εκτιμάται το δυσμενέστερο πιθανό σενάριο και υπολογίζονται οι επιπτώσεις από την πραγματοποίησή του. Το μέγεθος της επίπτωσης εκτιμάται αριθμητικά με βάση κλίμακα 1-10.

Βήμα 3: Επιβεβαίωση και επικύρωση της αποτίμησης

Προτού υλοποιηθούν τα επόμενα στάδια, θα πρέπει πρώτα να επικυρωθεί η αποτίμηση. Το κύριο χαρακτηριστικό αυτού του σταδίου είναι η αποτίμηση των αγαθών ΠΣ. Τα αποτελέσματα του πρώτου σταδίου παρουσιάζονται σε σχετική έκθεση η οποία περιλαμβάνει:

- Τον ορισμό του προς ανάλυση συστήματος και των ορίων του.
- Τη μέθοδο εργασίας που ακολουθήθηκε.
- Την αποτίμηση των περιουσιακών στοιχείων των Π.Σ.
- Γενικά συμπεράσματα.

Στάδιο 2: Ανάλυση επικινδυνότητας

Στο αρχικό στάδιο έγινε η αποτίμηση της αξίας των στοιχείων των ΠΣ. Στο δεύτερο στάδιο υπολογίζονται οι άλλοι δύο παράγοντες, το επίπεδο των απειλών και το επίπεδο των αδυναμιών του συστήματος. Ο συνδυασμός των τριών παραγόντων δίδει το βαθμό επικινδυνότητας του συστήματος, έτσι ώστε να επιλεγούν τα κατάλληλα αντίμετρα.

Βήμα 1: Προσδιορισμός των απειλών που αφορούν κάθε αγαθό

Η μέθοδος CRAMM επικεντρώνεται στον προσδιορισμό συγκεκριμένων απειλών για κάθε αγαθό και παρέχει μία ενδεικτική λίστα, καθώς και συστάσεις για το ποιες κατηγορίες στοιχείων ενός ΠΣ αντιμετωπίζουν συνήθως τη συγκεκριμένη απειλή.

Όταν ένα από τα στοιχεία των ΠΣ αντιμετωπίζει απειλή τότε και τα δεδομένα ή οι υπηρεσίες που αυτό υποστηρίζει αντιμετωπίζουν την ίδια απειλή. Με την CRAMM ο αναλυτής δε χρειάζεται να υπολογίζει ο ίδιος τις συσχετίσεις και αλληλεπιδράσεις. Η CRAMM τεχνική ζητά από τους αναλυτές να συσχετίσουν τα αγαθά με κατηγορίες απειλών από την παραπάνω κατάσταση. Έτσι, το εργαλείο CRAMM προβαίνει σε συμπεράσματα με βάση το μοντέλο του συστήματος.

Βήμα 2: Εκτίμηση απειλών αδυναμιών

Για κάθε συνδυασμό αγαθού - απειλής εκτιμάται το μέγεθος της απειλής και η σοβαρότητα των αδυναμιών που μπορεί να οδηγήσουν στην πραγματοποίηση της απειλής. Η CRAMM υπολογίζει το επίπεδο της απειλής χρησιμοποιώντας απαντήσεις σε ερωτηματολόγια των απειλών. Η εκτίμηση της απειλής γίνεται σε κλίμακα από 1-5 (very low, low, medium, high, very high). Για τις αδυναμίες συμπληρώνονται ερωτηματολόγια αδυναμιών και υπολογίζεται η σοβαρότητα της αδυναμίας σε κλίμακα 1-3 (low, medium, high). Οι απαντήσεις που θα δοθούν στα ερωτηματολόγια προκύπτουν από τα στοιχεία που συλλέγουν οι αναλυτές από τους χρήστες του συστήματος.

Βήμα 3: Υπολογισμός επικινδυνότητας για κάθε συνδυασμό αγαθό - απειλή - αδυναμία

Η CRAMM υπολογίζει για κάθε συνδυασμό αγαθό - απειλή - αδυναμία το βαθμό επικινδυνότητας. Για το σκοπό αυτό, χρησιμοποιούνται τόσο τα αποτελέσματα της εκτίμησης απειλών και αδυναμιών, όσο και το μοντέλο των ΠΣ. Έτσι, ο βαθμός επικινδυνότητας λαμβάνει υπόψη και τη συσχέτιση και τις εξαρτήσεις μεταξύ των στοιχείων των ΠΣ και ακολουθεί μία κλίμακα 1-7 και γίνεται αυτόματα για κάθε συνδυασμό.

Βήμα 4: Επικύρωση του βαθμού επικινδυνότητας

Στο συγκεκριμένο βήμα η ομάδα μελέτης χρησιμοποιεί τις αναφορές που παράγει το λογισμικό της CRAMM για να εξετάσει συνολικά το βαθμό επικινδυνότητας. Σε περίπτωση που κριθεί ότι χρειάζεται να γίνουν κάποιες αλλαγές, τότε οι αναλυτές έχουν τη δυνατότητα είτε να αλλάξουν τις τιμές της επικινδυνότητας είτε να αλλάξουν τις τιμές που έχουν προκύψει από την εκτίμηση των απειλών και αδυναμιών και να υπολογίσουν εκ νέου την επικινδυνότητα.

Στάδιο 3: Διαχείριση επικινδυνότητας

Η μέθοδος CRAMM, στηριζόμενη στα αποτελέσματα του δεύτερου σταδίου, παράγει ένα σχέδιο ασφάλειας για το ΠΣ. Αυτό περιλαμβάνει:

- Μία σειρά αντιμέτρων τα οποία κρίνονται απαραίτητα για την αντιμετώπιση και διαχείριση της επικινδυνότητας και τα οποία θα πρέπει να εφαρμοστούν

- Μία σειρά επιλογών και εναλλακτικών λύσεων, ώστε να παρέχεται ευελιξία στην εφαρμογή του.

Για συστήματα τα οποία έχουν αναπτυχθεί και λειτουργούν ήδη, το προτεινόμενο σχέδιο ασφάλειας μπορεί να συγκριθεί με τα υπάρχοντα αντίμετρα. Η τελική επιλογή των αντιμέτρων που θα εφαρμοστούν λαμβάνει υπόψη και το κόστος που έχουν τα αντίμετρα για τον οργανισμό.

Βήμα 1: Προσδιορισμός των προτεινόμενων αντιμέτρων

Η CRAMM περιλαμβάνει μία ευρεία βάση αντιμέτρων (τεχνικά, διοικητικά, οργανωτικά), γνωστή ως βιβλιοθήκη αντιμέτρων. Το λογισμικό της CRAMM μπορεί να επιλέξει αυτόματα μία κατάσταση προτεινόμενων αντιμέτρων με βάση τα αποτελέσματα της ανάλυσης επικινδυνότητας.

Τα αντίμετρα χωρίζονται σε ομάδες, ανάλογα με το είδος των απειλών που καλούνται να αντιμετωπίσουν και ανάλογα με το είδος των αγαθών που καλούνται να προστατέψουν. Η βάση των αντιμέτρων περιλαμβάνει τόσο τις εναλλακτικές λύσεις, δηλαδή ποιο αντίμετρο μπορεί να χρησιμοποιηθεί εναλλακτικά άλλου, καθώς και επιλογές υλοποίησής τους.

Μεταξύ των προτεινόμενων αντίμετρων πρέπει να γίνουν συγκεκριμένες επιλογές οι οποίες βασίζονται σε σημαντικό βαθμό στην εμπειρία των αναλυτών. Η CRAMM βοηθά, ώστε οι επιλογές να ακολουθούν μία δομημένη προσέγγιση και να αιτιολογούνται επαρκώς. Τα κριτήρια που λαμβάνονται υπόψη στην τελική επιλογή περιλαμβάνουν τα εξής:

- Την επίδραση που θα έχουν τα αντίμετρα στη λειτουργία του οργανισμού.
- Τον υπάρχοντα προϋπολογισμό για την ασφάλεια των ΠΣ.
- Το κόστος εγκατάστασης και λειτουργίας των αντιμέτρων.
- Την άποψη της διοίκησης και τους στόχους της.
- Ενδεχόμενες ενδείξεις ότι οι απειλές θα αυξηθούν στο μέλλον.

Ακολούθως τα προτεινόμενα αντίμετρα συγκρίνονται με τα υπάρχοντα. Το λογισμικό της CRAMM περιέχει μία βάση με περισσότερα από 2.500 αντίμετρα, ενταγμένα σε ομάδες και ιεραρχημένα ανάλογα με το επίπεδο ασφάλειας που προσφέρουν. Το CRAMM εργαλείο

επιλέγει αυτόματα τα αντίμετρα σύμφωνα με τα αποτελέσματα της ανάλυσης επικινδυνότητας, τα οποία μπορεί να είναι:

- Εγκατεστημένο
- Προς υλοποίηση
- Υπό υλοποίηση
- Προτεινόμενο για υλοποίηση
- Έχει καλυφθεί ήδη
- Αναλαμβάνεται η επικινδυνότητα
- Υπό συζήτηση
- Μη εφαρμόσιμο

Βήμα 2: Σχεδιασμός του Σχεδίου Ασφάλειας

Στο βήμα αυτό σχεδιάζεται το σχέδιο ασφάλειας που περιλαμβάνει το σχέδιο πολιτικής ασφάλειας, τους ρόλους και τις υποχρεώσεις του κάθε ρόλου, τα συμπληρωματικά έργα που απαιτούνται για την υλοποίηση της ασφάλειας. Το προϊόν του τρίτου σταδίου είναι το Σχέδιο Ασφάλειας.

5.4. Προσδιορισμός και αξιολόγηση των αγαθών

Στο συγκεκριμένο στάδιο παρουσιάζονται τα αποτελέσματα της αποτίμησης των αγαθών που διαχειρίζεται το ΠΣ του οργανισμού. Γενικά, το αγαθό μιας υποδομής είναι εκείνο το στοιχείο που παρουσιάζει κρισιμότητα για την ομαλή λειτουργία της και μπορεί να υποστεί ζημία, βλάβη ή να απειληθεί από κάποιον κίνδυνο. Από πλευράς ασφάλειας, τα αγαθά ορίζονται και κατηγοριοποιούνται με την ευρεία έννοια του όρου, δηλαδή ως ανθρώπινο δυναμικό, πληροφορίες ακόμα και η ίδια η υποδομή.

Η τεχνική CRAMM δίνει ιδιαίτερη σημασία στα δεδομένα και λιγότερο στο υλικό και λογισμικό.

ΔΕΔΟΜΕΝΑ

Τα δεδομένα συστήματος αναφέρονται στη πληροφορία που επεξεργάζεται και αποθηκεύει το Π.Σ. Για λόγους πρακτικότητας, τα δεδομένα μπορούν να ομαδοποιηθούν με βάση

κάποιο κοινό χαρακτηριστικό. Επίσης, η αξία των δεδομένων εκτιμάται βάσει των συνεπειών που θα μπορούσαν να προκύψουν από την απώλεια της διαθεσιμότητα, της εμπιστευτικότητας και της ακεραιότητας των δεδομένων.

Τα δεδομένα που διαχειρίζεται το συγκεκριμένο ΠΣ είναι:

1. Υπηρεσία Καταλόγου πληροφοριών εκδοθέντων αιτήσεων
2. Ιδιωτικό Κλειδί (Private Key)
3. Δημόσια Δεδομένα
4. Εμπιστευτικά / Απόρρητα Δεδομένα

Παρακάτω παρουσιάζονται οι επιπτώσεις που θα έχει καθεμία από τις ακόλουθες περιπτώσεις:

- απώλεια της διαθεσιμότητας των δεδομένων,
- παραβίαση της ακεραιότητας των δεδομένων,
- αποκάλυψη των δεδομένων.

1. Υπηρεσίες καταλόγου

Οι υπηρεσίες καταλόγου (directory services) δίνουν τη δυνατότητα να αφαιρεθεί ένα μεγάλο μέρος από την πολυπλοκότητα των ηλεκτρονικών συναλλαγών - αιτήσεων. Αυτό έχει σαν αποτέλεσμα οι ηλεκτρονικές συναλλαγές να υλοποιούνται ευκολότερα καθώς ορίζουν απλές και διαφανείς διαδικασίες για την αναζήτηση πληροφοριών σχετικών με χρήστες ή/και υπηρεσίες του δικτύου. Έχουν αποθηκευμένο ένα μεγάλο, κατά κανόνα, όγκο στοιχείων που αφορούν τους χρήστες του δικτύου, τις συσκευές του ή ακόμα και την οργάνωση της εταιρείας. Σε ένα σύστημα καταλόγων είναι σύνηθες φαινόμενο το 90% των προσπελάσεων στη βάση δεδομένων να αποτελείται από αναζητήσεις και ανακτήσεις στοιχείων, και μόνο το 10% να αποτελεί αιτήσεις διαγραφής ή αλλαγής εγγραφών.

Επιπτώσεις: Η μη διαθεσιμότητα των πληροφοριών του καταλόγου μπορεί να προκαλέσει τις διαμαρτυρίες των εναλλασσόμενων – χρηστών και σχετίζεται με το χρονικό διάστημα με το οποίο μπορεί να διαρκέσει. Ζήτημα εμπιστευτικότητας δεν τίθεται, αλλά η απώλεια

τέτοιου είδους πληροφοριών μπορεί να είναι αρκετά σοβαρή και εξαρτάται από την ύπαρξη σχετικών εφεδρικών αντιγράφων.

Αποτίμηση: Η συνέπεια της απώλειας διαθεσιμότητας των πληροφοριών καταλόγου για μικρό διάστημα (ωρών ή λίγων ημερών) μπορεί να έχει περιορισμένες συνέπειες. Στην περίπτωση, όμως, που το διάστημα είναι μεγαλύτερο, συνεπάγεται η αναστολή λειτουργίας του συστήματος. Επιπλέον, αν καταστραφούν τα εφεδρικά αντίγραφα, θα διακοπεί η λειτουργία πιστοποίησης των αιτήσεων, διότι δίχως λίστες ανάκλησης, όλα τα απαραίτητα έγγραφα των αιτήσεων και τα συνοδευτικά δικαιολογητικά θα πρέπει να θεωρηθούν άκυρα και να εκδοθούν νέα.

2. Ιδιωτικό Κλειδί

Το ιδιωτικό (private key) χρησιμοποιείται για σφράγισμα μιας ηλεκτρονικής υπογραφής και είναι απόρρητο. Το ιδιωτικό κλειδί το γνωρίζει ο αποστολέας του μηνύματος και μόνο με αυτό μπορεί κανείς να επέμβει στο κείμενο.

Επιπτώσεις: Η απώλεια της διαθεσιμότητας του ιδιωτικού κλειδιού οδηγεί στην αναστολή λειτουργίας πιστοποίησης μιας αίτησης. Επίσης, η διαρροή ή κλοπή του ιδιωτικού κλειδιού είναι εξαιρετικά σοβαρή και ιδιαίτερα αν η διαπίστωσή της γίνει με σημαντική καθυστέρηση. Τέλος, ένα επιπλέον πρόβλημα είναι και η απώλεια της ακεραιότητας του ιδιωτικού κλειδιού που μπορεί να προκληθεί από τυχαία αλλοίωση ή καταστροφή π.χ. λόγω φυσικής καταστροφής ή αστοχίας των μέσων αποθήκευσης.

Αποτίμηση: Εκτιμάται ότι η αναστολή λειτουργίας πιστοποίησης για χρονικό διάστημα λίγων ωρών δημιουργεί σημαντικό πρόβλημα για τον φορέα, ενώ η κατάσταση θεωρείται ιδιαίτερα κρίσιμη όταν το διάστημα αυτό υπερβαίνει την μία ώρα και φτάσει ακόμα και τη μία εβδομάδα. Όλες οι συναλλαγές του αιτήσεων που έχουν γίνει μπορεί να αμφισβητηθούν και ο φορέας μπορεί να αποκτήσει αρνητική δημοσιότητα και να χάσει την αξιοπιστία του. Τέλος, η έκταση των συνεπειών θα εξαρτηθεί από την ύπαρξη εφεδρικών αντιγράφων και από το χρόνο αποκατάστασης των κλειδιών.

3. Δημόσια Δεδομένα

Στα δεδομένα αυτού του τύπου ανήκουν τα επεξεργασμένα δεδομένα που αναρτώνται στη Δικτυακή Πύλη και παρέχονται ελεύθερα προς δημόσια χρήση. Πρόκειται για πληροφοριακού χαρακτήρα δεδομένα, που δεν περιέχουν προσωπικές ή ευαίσθητες προσωπικές πληροφορίες προσώπων.

Επιπτώσεις: Η απώλεια της διαθεσιμότητας των δημόσιων δεδομένων μπορεί να προκαλέσει την όχληση των χρηστών της Δικτυακής Πύλης και να επηρεάσει τη φήμη του φορέα. Επίσης, επειδή πρόκειται για δεδομένα πρωτογενούς επεξεργασίας, η απώλεια ή καταστροφή τους μπορεί να επιφέρει οικονομικό κόστος ανάκτησης ή αναδημιουργίας τους. Τέλος, η πληροφορία αυτή είναι δημόσιας χρήσης και δεν υπάρχουν επιπτώσεις από τυχόν διαρροή της.

Αποτίμηση: Η απώλεια της διαθεσιμότητας εκτιμάται να έχει συνέπειες που σχετίζονται με τη φύση του φορέα και είναι ανάλογες με την καθυστέρηση της επαναφοράς τους στη Δικτυακή Πύλη. Η επίπτωση από την ολοκληρωτική απώλεια ή καταστροφή αποτιμάται με χαμηλό βαθμό και γενικότερα, όπως προαναφέρθηκε, δεν τίθεται θέμα εμπιστευτικότητας.

4. Εμπιστευτικά / Απόρρητα Δεδομένα

Οι όροι «εμπιστευτικά δεδομένα» και «απόρρητα δεδομένα» υποδηλώνουν στοιχεία τα οποία καθιστούν δυνατή την άμεση και την έμμεση, αντίστοιχα, αναγνώριση των μονάδων στατιστικών στοιχείων, δια της αποκαλύψεως εξατομικευμένων πληροφοριών. Πρόκειται για δεδομένα που θεωρούνται χρήσιμα και η μη εξουσιοδοτημένη πρόσβαση σε αυτά θα μπορούσε να επιφέρει σημαντικές επιπτώσεις.

Επιπτώσεις: Η μη διαθεσιμότητα των εμπιστευτικών / απόρρητων δεδομένων για σημαντικό χρονικό διάστημα καθώς και η καταστροφή τους, μπορεί να επηρεάσει τη φήμη του φορέα, να παρεμποδίζει τη λειτουργία του, να υποβαθμίσει την αποτελεσματικότητα των δράσεων του και να προκαλέσει κόστος. Η σκόπιμη αλλοίωση των πληροφοριών αυτής της ομάδας θα μπορούσε να έχει ως αποτέλεσμα τη διευκόλυνση τέλεσης αξιόποινων πράξεων, την υπονόμευση της λειτουργίας και των δράσεων του φορέα και, η τυχόν παραβίασή τους αποτελεί παραβίαση της νομοθεσίας και συνεπάγεται νομικές κυρώσεις.

Αποτίμηση: Η συνέπεια της απώλειας διαθεσιμότητας των δεδομένων αυτών για διάστημα μερικών λεπτών αποτιμάται με υψηλό βαθμό επικινδυνότητας και ο βαθμός αυτός ολοένα και αυξάνει με το πέρασμα μερικών ωρών. Η επίπτωση από την ολοκληρωτική απώλεια – καταστροφή αποτιμάται επίσης με υψηλό βαθμό και από την μερική απώλεια – καταστροφή των δεδομένων με λίγο χαμηλότερο. Σημαντικό είναι και το κόστος της σκόπιμης αλλοίωσής τους, ενώ η συνέπεια από την αποκάλυψή τους σε τρίτους είναι εξίσου σημαντική.

Οι παρακάτω εικόνες παρουσιάζουν συγκεντρωτικά τις προαναφερθείσες εκτιμήσεις:

Αγαθό	1 ώρα	3 ώρες	12 ώρες	1 Ημέρα	2 Ημέρες
Πληροφορίες Καταλόγου	2	2	2	3	3
Ιδιωτικό Κλειδί	2	2	2	3	3
Δημόσια Δεδομένα	2	5	7	7	7
Εμπιστευτικά/απόρρητα δεδομένα	5	7	8	8	8

Εικόνα 8: Εκτίμηση 1

Αγαθό	Ολική καταστροφή	Μερική καταστροφή	Σκόπιμη αλλοίωση	Μικρής έκτασης λάθη	Μεγάλης έκτασης λάθη	Αποκάλυψη
Πληροφορίες Καταλόγου	7	3	5	3	5	
Ιδιωτικό Κλειδί	5		6	5	5	7
Δημόσια Δεδομένα	3	2	5	2	3	
Εμπιστευτικά/απόρρητα δεδομένα	5	3	7	3	5	5

Εικόνα 9: Εκτίμηση 2

ΥΛΙΚΟ

Το υλικό που χρησιμοποιείται για το σύστημα Διαχείρισης Αιτήσεων Διαγωνισμών αποτελείται από:

- ✓ 5 εξυπηρετητές (servers)
  - 1 backup server
  - 2 DNS servers
  - 2 Authentication servers
- ✓ 1 σταθμό εργασίας (PC)
- ✓ Δικτυακός εξοπλισμός
- ✓ Κασέτες που περιέχουν τα backup που παίρνει ο server

Η αξία του εκτιμάται στα 10.000 ευρώ περίπου.

ΛΟΓΙΣΜΙΚΟ

- ✓ Λειτουργικό Σύστημα
- ✓ Εξυπηρετητής Ιστού
- ✓ Λογισμικό Υποστήριξης SSL/TLS
- ✓ Διαχειριστής Βάσης Δεδομένων

Η αξία του εκτιμάται στα 12.500 ευρώ περίπου.

5.5. Ανάλυση Επικινδυνότητας

Στην προηγούμενη ενότητα, με την χρήση της CRAMM, παρουσιάστηκαν τα αποτελέσματα της αξιολόγησης των αγαθών του ΠΣ που απαιτούν προστασία. Η αποτίμηση των αγαθών που προέκυψε, αποτελεί έναν από τους δύο παράγοντες που συνθέτουν την επικινδυνότητα των ΠΣ. Ο δεύτερος παράγοντας είναι η πιθανότητα (ενδεχόμενο) που προκύπτει από την απειλή και την ευπάθεια, ως εξής:

Πιθανότητα (Ενδεχόμενο) = Απειλή x Ευπάθεια

Ως επικινδυνότητα ορίζεται η πιθανότητα μια συγκεκριμένη απειλή να εκμεταλλευτεί μια συγκεκριμένη ευπάθεια. Στον τομέα της ασφάλειας, ο βασικός τύπος που αποτελεί την

ανάλυση της Επικινδυνότητα ορίζεται ως το γινόμενο της Πιθανότητας πραγματοποίησης ενός επεισοδίου ασφάλειας επί την επίπτωση που θα επιφέρει, δηλαδή:

Επικινδυνότητα = Πιθανότητα (Ενδεχόμενο) x Επίπτωση

Το επόμενο στάδιο, λοιπόν, είναι η εκτίμηση των απειλών που αντιμετωπίζει το σύστημα καθώς και οι αδυναμίες που ενδέχεται να προκύψουν με την πραγματοποίηση των απειλών.

Όπως αναφέρθηκε στο κεφάλαιο 2, μια απειλή μπορεί να είναι ένα οποιοδήποτε συμβάν ή περιστατικό που ενδέχεται να προκαλέσει πρόβλημα ή ακόμα και ολοσχερή καταστροφή σε ένα αγαθό ή σύνολο αγαθών. Οι κυριότερες απειλές και αδυναμίες που αντιμετωπίζει το συγκεκριμένο ΠΣ είναι οι ακόλουθες:

<u>Εξωτερικές απειλές:</u>

• Εξωτερικοί εισβολείς (outsiders): Hackers, crackers, vandals, hacktivists

- ✓ Εύρεση στοιχείων για την επιχείρηση π.χ. IP διευθύνσεις, e-mail, τοπολογία δικτύου, ονόματα υπολογιστών, διάρθρωση της επιχείρησης κ.λπ.
- ✓ Επιθέσεις πλαστοπροσωπίας
- ✓ Παράκαμψη του μηχανισμού ασφάλειας με σκοπό τη μη εξουσιοδοτημένη πρόσβαση σε κάποιο αγαθό του συστήματος.

- Κακόβουλο λογισμικό: π.χ. Ιομορφικό Λογισμικό

<u>Εσωτερικές Απειλές:</u>

- Χρήστες της επιχείρησης που παρακάμπτουν τις διαδικασίες ελέγχου για την πρόσβαση σε διαβαθμισμένα δεδομένα/πληροφορίες.
- Χρήστες που αποκτούν πρόσβαση σε λογαριασμούς χρηστών με περισσότερα δικαιώματα σε σχέση με τα δικαιώματα που ήδη έχουν.

<u>Αδυναμίες:</u>

- «Εγγενείς» π.χ. υπερχείλιση καταχωρητή, «κακή» διαχείριση μνήμης από το ίδιο το λειτουργικό σύστημα.

- Κακή χρήση - διαχείριση του συστήματος π.χ. λάθος ορισμός των δικαιωμάτων (permissions) σε ένα αρχείο.

Στη συνέχεια παρουσιάζονται τα αποτελέσματα της αποτίμησης των βασικότερων προαναφερθέντων απειλών και αδυναμιών του συγκεκριμένου συστήματος από την προηγούμενη ενότητα:

Απειλή 1: Επίθεση πλαστοπροσωπίας

	Απειλή	Ευπάθεια	Επίπτωση	Επικινδυνότητα
ΜΔ 1 ώρα	Υ	Μ	3	3
ΜΔ 3 ώρες	Υ	Μ	3	3
ΜΔ 12 ώρες	Υ	Μ	3	3
ΜΔ 1 ημέρα	Υ	Μ	4	4
ΜΔ 2 ημέρες	Υ	Μ	5	4

Εικόνα 10: Πλαστοπροσωπία

Απειλή 2: Μη εξουσιοδοτημένη χρήση εφαρμογής

	Απειλή	Ευπάθεια	Επίπτωση	Επικινδυνότητα
ΜΔ 1 ώρα	Μ	Μ	3	3
ΜΔ 3 ώρες	Μ	Μ	3	3
ΜΔ 12 ώρες	Μ	Μ	3	3
ΜΔ 1 ημέρα	Μ	Μ	4	3
ΜΔ 2 ημέρες	Μ	Μ	5	4

Εικόνα 11: Μη εξουσιοδοτημένη χρήση εφαρμογής

Απειλή 3: Εισαγωγή ιομορφικού λογισμικού

	Απειλή	Ευπάθεια	Επίπτωση	Επικινδυνότητα
ΜΔ 1 ώρα	Υ	Μ	3	3
ΜΔ 3 ώρες	Υ	Μ	3	3
ΜΔ 12 ώρες	Υ	Μ	3	3
ΜΔ 1 ημέρα	Υ	Μ	4	4
ΜΔ 2 ημέρες	Υ	Μ	5	4

Εικόνα 12: ιομορφικό λογισμικό

	Απειλή	Ευπάθεια	Επίπτωση	Επικινδυνότητα
ΦΚ	X	M	7	4
ΜΔ 1 ώρα	X	M	3	2
ΜΔ 3 ώρες	X	M	3	2
ΜΔ 12 ώρες	X	M	3	2
ΜΔ 1 ημέρα	X	M	4	3
ΜΔ 2 ημέρες	X	M	5	3

Εικόνα 13: Φυσική καταστροφή υλικού

Σημείωση: Συντομογραφία ΜΔ: Μη Διαθεσιμότητα

5.6. Διαχείριση Επικινδυνότητας

Στη φάση της διαχείρισης της επικινδυνότητας η ομάδα που ασχολείται με τη διαδικασία διαχείρισης των κινδύνων πρέπει να βρει την κατάλληλη μέθοδο αντιμετώπισης του κάθε κινδύνου. Όπως αναφέρθηκε σε προηγούμενη ενότητα, οι μέθοδοι αντιμετώπισης των απειλών είναι η αποφυγή, η μεταφορά, η μείωση/μετριασμός και η αποδοχή. Η επιλογή της κατάλληλης στρατηγικής σχετίζεται με τη σοβαρότητα της συνέπειας και της φύσης του κινδύνου, καθώς και την επάρκεια των πόρων.

Τα μέτρα προστασίας που θα παρουσιαστούν στην συγκεκριμένη ενότητα συνθέτουν το προτεινόμενο σχέδιο ασφάλειας, για τις υπηρεσίες του επιλεχθέντος ΠΣ και τα οποία αναφέρονται σε:

1. Πολιτική ασφάλειας
2. Νομικό Πλαίσιο
3. Οργάνωση Υπηρεσίας Πληροφορικής
4. Εκπαίδευση προσωπικού
5. Έλεγχος προσπέλασης
6. Ακεραιότητα Λογισμικού
7. Ασφάλεια κτηρίου
8. Ασφάλεια εξοπλισμού

Συμπεράσματα και μελλοντικές επεκτάσεις μελέτης

Συμπεράσματα

Μέσα από τα μέτρα προστασίας που παρουσιάστηκαν διαφαίνεται καθαρά ο σημαντικός ρόλος του υπεύθυνου ασφαλείας. Ο υπεύθυνος ασφαλείας είναι ένα άτομο ή μια ομάδα με κατάλληλες γνώσεις πάνω σε ζητήματα ασφάλειας και επιλέγεται από την ανώτερη διοίκηση του οργανισμού για το συγκεκριμένο σκοπό.

Ένα σημαντικό κομμάτι της διαχείρισης του κινδύνου αφορά την συλλογή πληροφοριών και την ανάλυση τους για να εντοπιστούν πιθανοί κίνδυνοι της επιχείρησης. Είναι μια δημιουργική διαδικασία που περιλαμβάνει τον προσδιορισμό, την αξιολόγηση και τον μετριασμό των επιπτώσεων της εκδήλωσης κινδύνου. Η διαχείριση του κινδύνου μπορεί να είναι πολύ τυπική, με καθορισμένες διαδικασίες εργασίας, ή άτυπη, χωρίς ορίζονται διαδικασίες ή μέθοδοι.

Μελλοντικές επεκτάσεις

Η Διαχείριση Κινδύνου αποτελεί ένα καινούριο, σημαντικό και κατ' επέκταση συνεχώς εξελισσόμενο εργαλείο του κλάδου του Management, το οποίο χρησιμοποιεί ένα μεγάλο εύρος δραστηριοτήτων. Η μεθοδολογία στην οποία στηρίζεται, για αρκετά μεγάλα επιχειρησιακά προγράμματα, με μεγάλο πλήθος έργων, απαιτεί τεράστιο αριθμό πράξεων, που δυσχεραίνουν πολύ το έργο των διαχειριστών, οι οποίοι με τη σειρά τους χρειάζονται ένα πολύπλοκο ολοκληρωμένο ΠΣ για την υποστήριξή τους.

Για τους παραπάνω λόγους, λοιπόν, η Διαχείριση Κινδύνου, στη μορφή που είναι σήμερα, θεωρείται ότι βρίσκεται σε πρώιμο στάδιο, συνεπώς υπάρχουν προοπτικές για περαιτέρω ανάπτυξη των επιμέρους σταδίων της. Με τα χρόνια, θα αναπτυχθούν όλο και περισσότερα εργαλεία λογισμικού, προγράμματα και ολοκληρωμένα ΠΣ για την ακριβή, εύκολη και έγκυρη εφαρμογή των μεθόδων και μεθοδολογιών διαχείρισης του κινδύνου. Τέλος, άλλο ένα πεδίο με προοπτικές ανάπτυξης είναι η λήψη συλλογικών αποφάσεων και κυρίως η σύνθεση των επιμέρους αποφάσεων.

Παράρτημα:

Υπόδειγμα Φύλλο Κινδύνου

ΟΝΟΜΑ ΕΡΓΟΥ:	Πληροφοριακό Σύστημα Διαχείρισης Στοιχείων Διαγωνισμών
ΟΝΟΜΑ ΚΙΝΔΥΝΟΥ:	Επίθεση πλαστοπροσωπίας

ΕΝΤΥΠΟ ΑΝΑΦΟΡΑΣ ΚΙΝΔΥΝΟΥ #1

ΑΝΑΦΕΡΕΤΑΙ ΑΠΟ:	*Βαρβάρα Αλεξανδρή*
ΗΜΕΡΟΜΗΝΙΑ ΑΝΑΦΟΡΑΣ:	*25/4/2016*

ΑΝΑΛΥΤΙΚΑ ΣΤΟΙΧΕΙΑ ΚΙΝΔΥΝΟΥ
Περιγραφή Κινδύνου:
Προσπάθεια αντιγραφής προσωπικών στοιχείων κατά την αίτηση του διαγωνισμού
Πιθανότητα Κινδύνου:
*Περιγράψετε και εκτιμήστε την πιθανότητα επέλευσης του κινδύνου (**ΠΧ**=«Πολύ Χαμηλή», **Χ**=«Χαμηλή», **Χ**=«Μέτρια», **Υ**=«Υψηλή», **ΠΥ**=«Πολύ Υψηλή»).* *[να συμπληρώνεται από τον αναφέροντα τον κίνδυνο (risk originator) και να επισκοπείται από τον Υπεύθυνο Συντονιστή]*
Επίπτωση Κινδύνου:
*Περιγράψετε και εκτιμήστε το επίπεδο της επίπτωσης του κινδύνου στο Έργο (**ΠΧ**=«Πολύ Χαμηλό», **Χ**=«Χαμηλό», **Χ**=«Μέτριο», **Υ**=«Υψηλό», **ΠΥ**=«Πολύ Υψηλό»).* *[να συμπληρώνεται από τον αναφέροντα τον κίνδυνο (risk originator) και να επισκοπείται από τον Υπεύθυνο Συντονιστή]*

ΠΡΟΤΑΣΗ ΠΡΟΛΗΠΤΙΚΩΝ ΕΝΕΡΓΕΙΩΝ/ ΕΝΕΡΓΕΙΩΝ ΑΝΤΙΜΕΤΩΠΙΣΗΣ ΑΠΡΟΒΛΕΠΤΩΝ

Προτεινόμενες Προληπτικές Ενέργειες:
Περιγράψετε συνοπτικά τις ενέργειες που προτείνετε να αναληφθούν για την πρόληψη της επέλευσης του κινδύνου. *[συμπληρώνεται από τον Υπεύθυνο Συντονιστή]*
Προτεινόμενες Ενέργειες Αντιμετώπισης:
Περιγράψετε συνοπτικά τις ενέργειες που προτείνετε να αναληφθούν για την ελαχιστοποίηση της επίπτωσης ενός κινδύνου όταν αυτός επέλθει. *[συμπληρώνεται από τον Υπεύθυνο Συντονιστή]*

ΕΓΚΡΙΣΗ:
Υπογραφή Ημερομηνία: *Θα πρέπει να υπογράφεται είτε από τον Υπεύθυνο Συντονιστή είτε από την Καθοδηγητική Επιτροπή Έργου, ανάλογα με το ποιος είναι υπεύθυνος για την παροχή έγκρισης.*

Πηγές

[1] Κοκολάκης Σπ., Ανάπτυξη και Διαχείριση Ασφάλειας Πληροφοριακών Συστημάτων: Εννοιολογικό Πλαίσιο, Μεθοδολογίες και Εργαλεία, Διδακτορική Διατριβή, Τμήμα Πληροφορικής, Οικονομικό Πανεπιστήμιο Αθηνών, 2000

[2] Gerber, M., & von Solms, (2005). Management of Risk in the information age, Computers and Security 24, pp. 11-16

[3] Lhabitant F. & Tinguely T., Financial Risk Management: An Introduction, Thunderbird International Business Review, Vol. 43 (3), 343-363, 2001

[4] Miguel Marquez Garcia A. & Jesus Hernandez Ortiz M., Firms Facing Uncertainty: The Cooperation Option, included in Zopounidis C. & Pardalos M., 154 Managing in Uncertainty: Theory and Practice, Kluwer Academic Publishers, Dordrecht, 1998

[5] Meredith Jack R, Mantel Samuel “Project Management – A managerial approach”, 2002

[6] PMI, A guide to the project management body of knowledge: PMBOK guide. – 3rd ed., Project Management Institute, 2004

[7] Tatsiopoulos, I., Leopoulos, V. and Kirytopoulos, K., 2001, Risk as a strategic decision factor for the competitive bidding process in contract manufacturing. Proceedings of the IFIP Conference, Denmark, pp. 223-231

[8] Leopoulos, V., Kirytopoulos, K. and Malandrakis, C. 2003, ‘An applicable methodology for strategic risk management during the bidding process’, International Journal of Risk Assessment and Management, vol. 4, no. 1, pp. 67-80

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

[10] European Commission, "Directive of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free

movement of such data (Directive 95/46/EC)", Official Journal of the European Communities, L281, Vol.38, pp.31-50, 23rd November 1995

[11] ΝΟΜΟΣ 2472/97, "Προστασία του ατόμου από την επεξεργασία δεδομένων προσωπικού χαρακτήρα", 10-4-1997/ΦΕΚ 50/Τεύχος Α', 1997

[12] Gary Stoneburner, Alice Goguen, Alexis Feringa, "Risk Management Guide for Information Technology Systems", NIST, 2001

[13] Project Management Institute, "A Guide to the Project Management Body of Knowledge (PMBOK® Guide)", Four Campus Boulevard, 2000

[14] Duane Bong, "Introduction to Monte Carlo Simulation", Article www.visionengineer.com/mech/monte_carlo_simulition.shtml

[15] http://www.previ.be/pdf/31010_FDIS.pdf

[16] https://managementjournal.wordpress.com/2010/02/11/isoiec-310102009

[17] National Institute for Standards and Technology, Risk management guide for information technology systems, NIST Special Publication 800-30, USA, July 2002.

[18] Gary Stoneburner, Alice Goguen, and Alexis Feringa, (2002) NIST Special Publication 800-30, Risk management guide for information technology systems - http://csrc.nist.gov/publications/nistpubs/800-30/sp800-30.pdf

[19] http://www.cert.org

[20] Carnegie Mellon University, "OCTAVE method implementation guide". Version 2.0, June 2001

[21]https://eclass.icsd.aegean.gr/modules/document/file.php/ICSD206/Διαφάνειες%20Διαλέξεων/Octave-Allegro-Overview.pdf

[22] [Osstm, 2010] Herzog, P. (2010) OSSTMM 3 – The Open Source Security Testing Methodology Manual

[23] OSSTMM, http://www.osstmm.org

[24] Μπαμπινιώτης Γ., "Λεξικό της Νέας Ελληνικής Γλώσσας", Κέντρο Λεξικολογίας, Αθήνα 1998