ΤΕΧΝΟΛΟΓΙΚΟ ΕΚΠΑΙΔΕΥΤΙΚΟ ΙΔΡΥΜΑ ΔΥΤΙΚΗΣ ΕΛΛΑΔΟΣ

ΣΧΟΛΗ ΔΙΟΙΚΗΣΗΣ ΚΑΙ ΟΙΚΟΝΟΜΙΑΣ

ΤΜΗΜΑ ΔΙΟΙΚΗΣΗΣ ΕΠΙΧΕΙΡΗΣΕΩΝ (Πάτρα)

Συστήματα διαχείρισης υπηρεσιών πληροφορικής και ασφάλεια των πληροφοριακών συστημάτων

IT services management systems and security of information systems

Πτυχιακή Εργασία *των*

Σαβαρίκα Βασίλειο

Σουσάνη Ελένη

Τζήκα Βικτωρία-Αναστασία

Επιβλέπων :…κ.Ντεμίρης Κωνσταντίνος…….

ΠΑΤΡΑ, Ιούλιος 2015

Περίληψη

Η παρούσα εργασία έχει στόχο να μελετήσει τα συστήματα διαχείρισης υπηρεσιών πληροφορικής, αλλά και την ασφάλεια των πληροφοριακών συστημάτων. Η εργασία ολοκληρώνεται μέσα από πέντε κεφάλαια.

Το πρώτο κεφάλαιο μελετά τις τεχνολογίες διαδικτύου. Το βασικό πλεονέκτημα του διαδικτύου, το οποίο το καθιστά σημαντικό για την εξέλιξη της κοινωνίας μας, είναι ότι δίνει τη δυνατότητα στον οποιονδήποτε πολύ εύκολα να αποκτήσει πρόσβαση χωρίς υψηλό κόστος.

Το δεύτερο ασχολείται με την ασφάλεια των πληροφοριακών συστημάτων. Τα πληροφοριακά συστήματα περιλαμβάνουν την επιχείρηση ή σημαντικά μέρη της, όπως τους εργαζομένους που εισάγουν δεδομένα στο σύστημα και παίρνουν πίσω την εκροή του. Σήμερα με τη χρήση των ηλεκτρονικών υπολογιστών, από όλες σχεδόν τις επιχειρήσεις, η συγκέντρωση εσωτερικών πληροφοριών απλουστεύεται.

Το τρίτο κεφάλαιο αναλύει την ασφάλεια των υπολογιστών από επιθέσεις ιών. Οι ιοί επηρεάζουν αρνητικά τον τομέα εκκίνησης ενός αποθηκευτικού μέσου ή μιας κατάτμησης. Η διαδικασία της μόλυνσης ξεκινά από τη στιγμή που ο ηλεκτρονικός υπολογιστής επιδιώκει να πραγματοποιήσει εκκίνηση από π.χ. μία μολυσμένη δισκέτα και ο ιός μετακινείται από τη δισκέτα στο σύστημα.

Το τέταρτο κεφάλαιο περιγράφει το ISO20000. Το ISO/IEC 20000 είναι διεθνές πρότυπο με στόχο τη Διαχείριση Παροχής Υπηρεσιών Πληροφορικής (ΔΠΥΠ-ITSM) που αφορά ένα πλήρες σύστημα διεργασιών διαχείρισης. Εστιάζει μόνο στις διεργασίες παροχής υπηρεσιών πληροφορικής, και στο διαχειριστικό σύστημα που τις υποστηρίζει.

Τέλος, το πέμπτο και τελευταίο κεφάλαιο περιγράφει το ISO27001, το οποίο είναι το μοναδικό διεθνές πρότυπο που μπορεί να προσδιορίσει τα ζητούμενα για ένα Σύστημα Διαχείρισης Ασφάλειας Πληροφοριών (ΣΔΑΠ-ISMS).

Στο τέλος της εργασίας εκτίθενται τα τελικά συμπεράσματα της μελέτης, βάσει των οποίων η χρήση ενός πληροφοριακού συστήματος από μία

εταιρία ή έναν οργανισμό, όσο μεγάλος ή μικρός και αν είναι, δεν είναι μια απλή υπόθεση. Πρέπει να τηρούνται πολλές προϋποθέσεις, καθώς οι απειλές είναι αρκετές.

Abstract

This paper aims to examine the IT services management systems, but also the security of information systems. The work is completed through five chapters.

The first chapter examines the internet technologies. The main advantage of the Internet, which makes it important for the development of our society, is that it allows anyone to easily access without high cost.

The second chapter is about the security of information systems. The information systems include an enterprise or important parts of an enterprise, such as workers who enter data into the system and get back the outflow. Nowadays with the use of computers, by almost all companies, the concentration of internal information is simplified.

The third chapter analyzes the security of computers from virus attacks. Viruses adversely affect the boot sector of a storage mean or segmentation. The process of infection begins from the moment the computer seeks to boot from an infected disk for example and the virus moves from the floppy disk to the system.

The fourth chapter describes ISO20000. The ISO/IEC 20000 is an international standard aiming Management Services Provider (MSP - ITSM) regarding a complete management system processes. It focuses only in IT service processes and in management system that supports them.

Finally, the fifth and last chapter describes the ISO27001, which is the only international standard that can identify the data required for an Information Security Management System (ISMS).

At the end of paper are exposed the final conclusions of the study, whereby the use of an information system of a company or an organization, no matter how big or small it is, is not a simple affair. Observe many conditions as there are many threats.

Περιεχόμενα

Εισαγωγή

Τα πληροφοριακά συστήματα δεν είναι απλώς οι ηλεκτρονικοί υπολογιστές, αλλά μια ολόκληρη επιχείρηση ή σημαντικά μέρη της, όπως οι εργαζόμενοι που εισάγουν δεδομένα στο σύστημα και παίρνουν πίσω την εκροή του. Τα στελέχη επιχειρήσεων αποτελούν μέρος του πληροφοριακού συστήματος, αφού το πληροφοριακό σύστημα είναι σχεδιασμένο για να υπηρετεί τις ειδικές ανάγκες τους για πληροφορίες. Μερικοί επιχειρηματίες πιστεύουν ότι στον πολύπλοκο σύγχρονο κόσμο, το να διευθύνεις σωστά μια επιχείρηση είναι κατά κύριο λόγο ζήτημα διαχείρισης πληροφοριών.

Τα Ολοκληρωμένα μάλιστα Πληροφοριακά Συστήματα Διαχείρισης (ERP Enterprise Resource Planning Systems) αποτελούν ένα σύνολο εφαρμογών λογισμικού που υποστηρίζουν ένα ευρύ φάσμα επιχειρησιακών δραστηριοτήτων και λειτουργιών.

Ωστόσο πρέπει να δοθεί ιδιαίτερη προσοχή στους ιούς, οι οποίοι επηρεάζουν αρνητικά τον τομέα εκκίνησης ενός αποθηκευτικού μέσου ή μιας κατάτμησης (partition). Ο τομέας εκκίνησης περιέχει ένα πρόγραμμα μικρού μεγέθους το οποίο το λογισμικό εντοπίζει και «φορτώνει» στη κύρια μνήμη.

Ένας Η/Υ μολύνεται αν χρησιμοποιήσει μια «μολυσμένη» δισκέτα εκκίνησης ή αν εκτελέσει ένα μολυσμένο πρόγραμμα. Ο ιός αποτελείται από κώδικα που καλύπτει και τις δύο περιπτώσεις: Ανάλογα με την περίσταση, εκτελείται το αντίστοιχο τμήμα. Το γεγονός αυτό αυξάνει τις πιθανότητες αναπαραγωγής ή/και μόλυνσης.

Για να αφαιρεθεί ο ιός από το σύστημα, θα πρέπει να αφαιρεθούν και τα δύο μέρη του, διαφορετικά το ένα μέρος μπορεί να επανενεργοποιήσει το άλλο. Μελέτη περίπτωσης: ο ιός Melissa (1999) μπορεί να θεωρηθεί ως ιός multipartite (μακρο-ιός & worm).

Το ISO/IEC 20000 είναι διεθνές πρότυπο με στόχο τη Διαχείριση Παροχής Υπηρεσιών Πληροφορικής (ΔΠΥΠ-ITSM) που αφορά ένα πλήρες σύστημα διεργασιών διαχείρισης. Εφόσον ο πρωταρχικός σκοπός λειτουργικότητας ενός οργανισμού είναι η παροχή υπηρεσιών πληροφορικής οπότε και η πιστοποίηση κατά ISO/IEC 20000 είναι απαραίτητη (Dugmore, 2006).

Το ISO/IEC 27001 τέλος, είναι το μοναδικό διεθνές πρότυπο που

μπορεί να προσδιορίσει τα ζητούμενα για ένα Σύστημα Διαχείρισης Ασφάλειας Πληροφοριών (ΣΔΑΠ-ISMS). Το πρότυπο έχει σχεδιαστεί να διασφαλίζει την επιλογή επαρκών και ισορροπημένων ελέγχων ασφάλειας. Αυτή η επιλογή βοηθά ένα οργανισμό να προστατεύσει τα περιουσιακά του στοιχεία πληροφοριών και να τον εμπιστεύονται τα ενδιαφερόμενα μέρη και ιδιαίτερα οι πελάτες του (ISO/IEC FDIS 27001).

Με δεδομένο ότι τα πληροφοριακά συστήματα αποτελούν σήμερα αναπόσπαστο κομμάτι για τις επιχειρήσεις, θα πρέπει οι επιχειρηματίες να διασφαλίζουν την ασφάλειά τους για το καλό της επιχείρησής τους. Ως εκ τούτου η μελέτη του παρόντος θέματος καθίσταται ιδιαίτερα σημαντική και ενδιαφέρουσα.

Σκοπός λοιπόν της παρούσης εργασίας είναι η μελέτη των συστημάτων διαχείρισης υπηρεσιών πληροφορικής, αλλά και της ασφάλειας των πληροφοριακών συστημάτων. Ως επιμέρους στόχοι ορίζονται οι ακόλουθοι:

1. Η μελέτη των πληροφοριακών συστημάτων.
2. Η ανάλυση της ασφάλειας των υπολογιστών από επιθέσεις.
3. Η περιγραφή των ISO/IEC 20000 και ISO/IEC 27001

Η μεθοδολογία της εργασίας στηρίζεται στη συλλογή δευτερογενών δεδομένων, τα οποία συλλέχθηκαν μέσα από βιβλία άρθρα σε περιοδικά αλλά και μέσα από επίσημους διαδικτυακούς τόπους. Αναμένεται το περιεχόμενο της εργασίας και ειδικά η ανάλυση των ISO/IEC 20000 και ISO/IEC 27001 να συμβάλλουν στη νέα γνώση δίνοντας ιδέες στους νέους αλλά και στους παλιούς για τη διασφάλιση των πληροφοριακών τους συστημάτων.

Η εργασία ολοκληρώνεται μέσα από πέντε κεφάλαια.

Το πρώτο κεφάλαιο μελετά τις τεχνολογίες διαδικτύου, το δεύτερο ασχολείται με την ασφάλεια των πληροφοριακών συστημάτων. Αρχικά παρουσιάζει τις βασικές έννοιες της θεωρίας των συστημάτων και εν συνεχεία μελετά τα πληροφοριακά συστήματα. Περιγράφει τους τύπους των πληροφοριακών συστημάτων, κάνει μια ιστορική αναδρομή και εν συνεχεία παρουσιάζει τις διακρίσεις τους. Στο τέλος του κεφαλαίου περιγράφει την ασφάλεια των πληροφοριακών συστημάτων και συγκεκριμένα τις

προϋποθέσεις ασφάλειας, την ανάπτυξη των πολιτικών ασφάλειας, την ανάλυση της επικινδυνότητας και τέλος τα μέτρα ασφαλείας. Το τρίτο κεφάλαιο αναλύει την ασφάλεια των υπολογιστών από επιθέσεις ιών, στοιχειοθετεί τις υπάρχουσες μορφές του ιομορφικού λογισμικού και στο τέλος περιγράφει τις τεχνικές αντιμετώπισης.

Το τέταρτο κεφάλαιο περιγράφει το ISO20000 και συγκεκριμένα το σκοπό τους. τους όρους και τους ορισμούς του, την ασφάλεια των πληροφοριών και τέλος αναλύει τις βασικές παραγράφους ανάπτυξής του. Το πέμπτο και τελευταίο κεφάλαιο περιγράφει το ISO27001 και συγκεκριμένα τα οφέλη του, τον τρόπο λειτουργίας του, τον κύκλο PDCA, τα πεδία ISO 27001: 2005 και το μητρώο των περιουσιακών στοιχείων του. Στο τέλος της εργασίας εκτίθενται τα τελικά συμπεράσματα της μελέτης.

Κεφάλαιο 1ο Τεχνολογίες διαδικτύου

1.1 Ιστορική αναδρομή του ίντερνετ

Το Internet ως όρος προέκυψε από τη σύνθεση των λέξεων Inter και network. Στην ελληνική γλώσσα ο όρος εκφράζεται μέσα από τη λέξη διαδίκτυο. Το internet σήμερα αποτελεί ένα παγκόσμιο δίκτυο που φέρνει σ' επαφή ανθρώπους από διάφορα μέρη του κόσμου, μέσα από τη χρήση του υπολογιστή τους. Το internet λειτουργεί ως πληροφοριακό εργαλείο, ως επικοινωνιακό και ενημερωτικό μέσο και η χρήση του πια είναι αποδεκτή σ' όλες τις αναπτυγμένες και αναπτυσσόμενες χώρες της γης.

Το βασικό πλεονέκτημα του Ίντερνετ το οποίο το καθιστά σημαντικό για την εξέλιξη της κοινωνίας μας, είναι το οτι δίνει τη δυνατότητα στον οποιονδήποτε πολύ εύκολα να αποκτήσει πρόσβαση χωρίς υψηλό κόστος (NUA.2008). Σήμερα το ίντερνετ είναι ένα από τα ποιο φθηνά μέσα επικοινωνίας, προβολής και γενικότερα προώθησης ιδεών και αντιλήψεων.

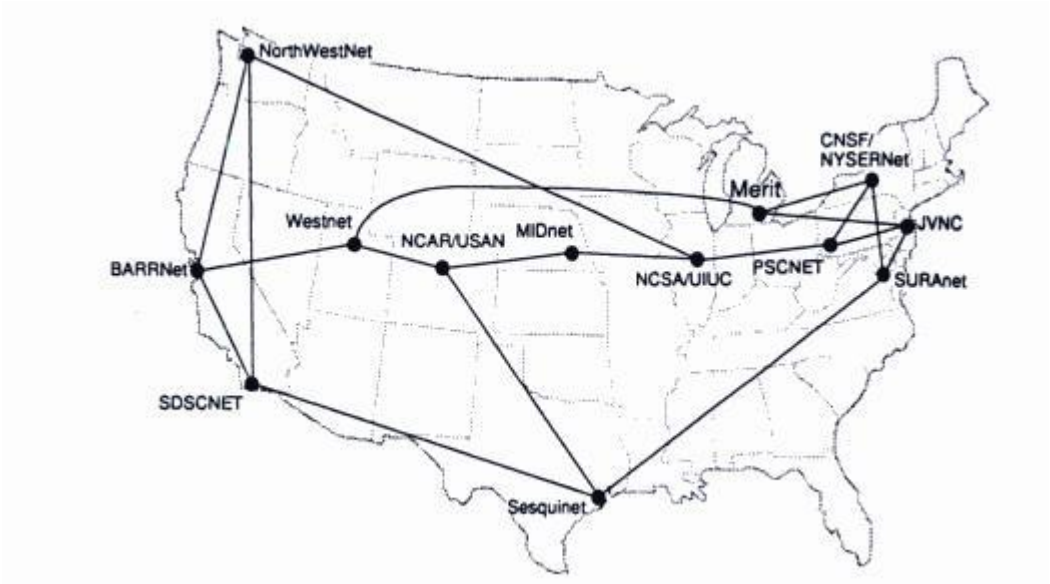
Σύμφωνα με τους Feinler E. και Postel J. το 1978 το internet εμφανίστηκε για πρώτη φορά το 1969 με την ονομασία Apranet, το οποίο για την εποχή του αποτέλεσε ένα ιδιαίτερα πρωτοποριακό εργαλείο. Το πρόγραμμα αυτό αναπτύχθηκε από την Υπηρεσία Προηγμένων Αμυντικών Ερευνών (DAPRA- Defense Advanced Research Projects Agency) του Υπουργείου Άμυνας των ΗΠΑ (Feinler and Postel 1978)

Το αμέσως επόμενο πολύ σημαντικό βήμα για την ανάπτυξη και διεύρυνση του Internet έγινε το 1986 από το Εθνικό Ίδρυμα Επιστημών (National Science Foundation, NSF) των ΗΠΑ, το οποίο έθεσε τις βάσεις για το πρώτο διαδικτυακό πανεπιστημιακό εργαλείο έρευνας, συλλογής και ανταλλαγής δεδομένων, το NSFNet (The Launch of NSFNet, 2010)

Το NSF οραματίστηκε ένα δίκτυο, το οποίο θα καθιστούσε δυνατή τη ταχεία μεταφορά πληροφοριών μεταξύ των ήδη υπαρχόντων εθνικών δικτύων αλλά και των επιμέρους τοπικών ακαδημαϊκών δικτύων (Σχήμα 1-1), ώστε οι χρήστες του να έχουν άμεση πρόσβαση σε απομακρυσμένες πηγές πληροφορίας, χωρίς να χρειάζεται να μετακινηθούν από τον χώρο που εργάζονται. Από την συνένωση πέντε διαφορετικών ακαδημαϊκών δικτύων

προέκυψε το NSFNet, το οποίο στη συνέχεια ενσωματώθηκε στο Apranet, καθιστώντας το με αυτό τον τρόπο ως το πιο πολύτιμο εργαλείο της εποχής του για τους ερευνητές αλλά και την ακαδημαϊκή κοινότητα των ΗΠΑ.

Ωστόσο, η τεράστια ανάπτυξη του Internet επήλθε όταν ο Σύμβουλος του CERN (Conseil Européenne pour la Recherche Nucléaire) Tim Berners Li, δημιούργησε τις υποδομές για την υπηρεσία του Παγκόσμιου Ιστού



Σχήμα 1-1: Το δίκτυο του NSFNet το 1989 του οποίοι οι βασικοί συντελεστές ήταν τα πανεπιστημιακά δίκτυα «υπέρ-υπολογιστών», JVNCNet του Princeton, το NCSAnet του University of Illinois, το PCSnet του Super Computer Center of Pittsburg και το SDSCNet του Πανεπιστημίου του San Diego

Το 1990, το Διαδίκτυο διέθετε πλέον όλες τις προδιαγραφές που θα το οδηγούσαν στην ευρεία αποδοχή των χρηστών παγκοσμίως, καθώς έχοντας ήδη δημιουργήσει ένα φιλικό και εύχρηστο περιβάλλον, πολύ σύντομα απορρόφησε με επιτυχία την πλειοψηφία των παλαιότερων δικτύων υπολογιστών.

Η περιορισμένη χρήση μεταξύ κυβερνητικών προσώπων και

πανεπιστημιακής κοινότητας που το χαρακτήριζε ως τότε και η απαγόρευση της εμπορικής του εκμετάλλευσης (εκτός αν ο σκοπός ήταν προς όφελος της επιστημονικής έρευνας) έληξε επίσημα το 1995, όταν το NSF αποσύρθηκε από την οικονομική υποστήριξη του διαδικτύου, αφήνοντας περιθώριο έτσι για την ανάπτυξη της ιδιωτικής πρωτοβουλίας (AOL, Prodigy, CompuServe).

Οπωσδήποτε πάντως, ένας από τους πλέον σημαντικούς παράγοντες που συντέλεσε στην περεταίρω διάδοσή του, υπήρξε η έλλειψη κεντρικού ελέγχου και το μη ιδιοκτησιακό και διοικητικό καθεστώς από το οποίο διέπεται, γεγονός που αφενός ευνοεί την οργανική του ανάπτυξη και εμπλουτισμό και αφετέρου αποτρέπει την εκμετάλλευσή του -τόσο σε επίπεδο περιεχομένου, όσο και σε εμπορικό επίπεδο- από μία και μόνο εταιρεία (Kotler et all, 2002).

Το επισφράγισμα της νέας εποχής στην οποία επρόκειτο να περιέλθει το Διαδίκτυο, σημειώθηκε τον Ιούνιο του 1998 με την κυκλοφορία των Windows 98 από την Microsoft του Bill Gates, αποδεικνύοντας έμπρακτα ότι στα αμέσως επόμενα χρόνια, το Internet θα αποτελούσε το μείζον πεδίο στο οποίο θα δίνονταν στο εξής οι μάχες για την οικονομική, επιστημονική και τεχνολογική ανάπτυξη.

Με βάση τα παραπάνω κατανοούμε ότι το διαδίκτυο έχει πλέον μια ιστορία τριάντα πέντε χρόνων. Όπως είδαμε στο διάστημα αυτό μετασχηματίστηκε από ένα ερευνητικό πρόγραμμα που αφορούσε σχεδόν αποκλειστικά στην ακαδημαϊκή κοινότητα των ΗΠΑ σ' ένα παγκόσμιο επικοινωνιακό σύστημα που στη πορεία πέτυχε να μεταβάλλει τη καθημερινότητα του μέσου ανθρώπου, τον βοήθησε στην εργασία του, τον βοήθησε να επικοινωνήσει και τέλος λειτούργησε και ως μέσω διασκέδασης και αναψυχής (Λέανδρος, 2005).

Η εξέλιξη μέσα στην ιστορία δεν ήταν κάτι το προσχεδιασμένο αντίθετα οι μεγάλες επιχειρήσεις τηλεπικοινωνιών και πληροφορικής έχοντας άλλες επιχειρηματικές δράσεις και ερευνητικές κατευθύνσεις οδηγήθηκαν σε τεχνολογικές και καινοτόμες δραστηριότητες, οι οποίες μέσα και από τις κινήσεις των χρηστών όπως το ηλεκτρονικό ταχυδρομείο, οι φυλλομετρητές, οι μηχανές αναζήτησης οδήγησαν στην ανάπτυξη του διαδικτυακού

περιβάλλοντος, ως πεδίο υποδοχής όλων των παραπάνω αναγκών και πηγών πληροφόρησης.

Ουσιαστικά οι παραπάνω αναφορές, μας οδηγούν στο συμπέρασμα ότι το διαδίκτυο, ήταν και είναι μια τεχνολογική επανάσταση η οποία ήρθε να καλύψει την ανάγκη της άμεσης και αμφίδρομης επικοινωνίας, δημιουργώντας και την εντύπωση όπως αναφέρει ο Λέανδρος Ν στο βιβλίο του «Το διαδίκτυο» ότι «οι πολίτες λόγω του Διαδικτύου θα μπορούσαν να ποντάρουν σε ένα νέο μοντέλο δημοκρατικής κοινωνικής λειτουργίας και γενικότερης εύρυθμης κοινωνικής ένταξης» (Λέανδρος, 2005).

Σύμφωνα με την αναφορά του Λέανδρου Ν. το 2005 μπορούμε να κατανοήσουμε την ραγδαία και εξελικτική πορεία του Διαδικτύου. Σήμερα οι εμπλεκόμενες σε αυτό εταιρείες προσφέρουν στους χρήστες δωρεάν υπηρεσίες όπως να απολαμβάνουν με αυτό τον τρόπο εμπορικά οφέλη από την διαφήμιση, απαλλάσσοντας ταυτόχρονα τους χρήστες από οποιοδήποτε κόστος.

Την ίδια στιγμή, η ανάπτυξη του ηλεκτρονικού εμπορίου (e-commerce) με πολλά επιτυχημένα παραδείγματα ηλεκτρονικών επιχειρήσεων -όπως το Amazon και το EBay- έδωσαν νέα μορφή στην εμπορική πρακτική, καθιστώντας την καταρχάς ως συναλλαγή που διεξάγεται σε παγκόσμιο επίπεδο, συνεπακόλουθα όμως και σε παγκόσμιο ανταγωνισμό, με αποτέλεσμα και σε αυτή την περίπτωση να ευνοείται ο καταναλωτής-χρήστης.

Ταυτόχρονα με την ανάπτυξη του ηλεκτρονικού «επιχειρείν» παρατηρείται αμεσότητα πρόσβασης στην πληροφορία, σε τέτοιο βαθμό ώστε σήμερα να αποτελούν ένα πολύ σημαντικό μέσο εμπορικής προώθησης (Search Engine Optimization), το οποίο περιλαμβάνει τεχνικές κατασκευής και δικτύωσης ιστοσελίδων που να προσφέρουν καλύτερες θέσεις εμφάνισης στα αποτελέσματα των «λέξεων-κλειδιών» και οι οποίες παραπέμπουν ουσιαστικά σε ηλεκτρονικές σελίδες-επιχειρήσεις.

1.2 Εφαρμογές διαδικτύου

Η αρχική προσπάθεια πλοήγησης των χρηστών στο διαδίκτυο ήταν ανεπιτυχής. Η επίλυση της και η μετέπειτα βελτιωμένη μορφή της σε σχέση με την αναζήτηση, ήταν απόρροια της ανάπτυξης των εργαλείων αναζήτησης. Συγκεκριμένα αυτές ήταν: 1.Η Yahoo, 2.Η AltaVista, 3.Η Infoseek, 4.Η Excite, 5.Ο Lycos, 6.Το Hotbot, 7.Η Google.

Όμως η συνεχής και χωρίς έλεγχο αύξηση των δικτυακών τόπων, οδήγησε στην αύξηση του όγκου του υλικού που ήταν αποθηκευμένο στον ιστό, οπότε και στην αδύνατη εύρεση των κατάλληλων κάθε φορά πληροφοριών. Αυτό ήταν αποτέλεσμα κυρίως της μη οργανωμένης αναζήτησης με τη βοήθεια συγκεκριμένων εφαρμογών. Όπως αναφέρει Prettejohn, M το 1996 στο βιβλίο του *«The First Year: August 1995-August 1996»* το 1995 υπήρχαν περίπου 10.000 δικτυακοί τόποι, ενώ 8 χρόνια αργότερα ο αριθμός τους θα ξεπερνούσε τα 35. εκατομμύρια (Nielsen, et all, 2000).

Η δαιδαλώδης κατάσταση της περιόδου 1995-2005 οδήγησε στη σημερινή δυσχερή κατάσταση, κάτω από την οποία λειτουργεί, αναπτύσσεται και λειτουργεί το διαδίκτυο. Η εστιασμένη προσπάθεια για βελτίωση στην εύρεση δεδομένων, είχε τελικά τα αντίθετα αποτελέσματα, μια και το διαδίκτυο βομβαρδίστηκε πολύ γρήγορα με αμέτρητες πληροφορίες, οι οποίες δίνονταν στο βωμό του ανταγωνισμού και της προσπάθειας για διαφοροποίηση. Σήμερα η κατάσταση αυτή θεωρείται ανεξέλεγκτη.

Μέσα στη δεκαετία του 1990, η οποία θεωρείται η περίοδος των μεγάλων ανακατατάξεων αλλά και των μεγάλων αποκλίσεων από την αρχική σκέψη και προσπάθεια ανάπτυξης του διαδικτύου, εμφανίστηκαν τα πρώτα εργαλεία αναζήτησης που στις περισσότερες περιπτώσεις ήταν το αποτέλεσμα της εργασίας ερευνητών και φοιτητών μεγάλων πανεπιστημιακών ιδρυμάτων των ΗΠΑ, οι οποίοι επιδίωκαν με αυτό τον τρόπο να ενισχύσουν την ερευνητική τους προσπάθεια.

Η αρχική φιλοσοφία του Yahoo, το οποίο δημιουργήθηκε το 1994 από τους David Filo και Jerry Yang υποψήφιους διδάκτορες στο Stanford University, αναφερόταν στη δημιουργία καταλόγων με αγαπημένους

συνδέσμους επικοινωνίας ώστε να διευκολύνεται η πλοήγηση των χρηστών στον ιστό.

Στη συνέχεια οι κατάλογοι αυτοί απέκτησαν κατηγορίες και υποκατηγορίες δημιουργώντας τη βασική δομή του Yahoo, αλλά και ένα ιστοτόπο ο οποίος έδινε τη δυνατότητα στο χρήστη να πλοηγηθεί ευκολότερα και γρηγορότερα σε βασικούς καταλόγους εύρεσης. Ουσιαστικά οι χρήστες ήταν αυτοί που δημιουργούσαν το κατάλογο, με βάση τις προτιμήσεις τους και τις προτεραιότητες τις οποίες είχαν σε σχέση με τις διαδικασίες εύρεσης που ακολουθούσαν. Αρχικά η χρήση γινόταν μόνο από τους ιδρυτές και τους φίλους τους, αλλά στη συνέχεια η φήμη του εξαπλώθηκε στην ευρύτερη κοινότητα των χρηστών του διαδικτύου.

Η βάση της πληροφόρησης της yahoo, ήταν η δυνατότητα αξιολόγησης άλλων ιστοσελίδων αλλά και η διευρυμένη παρουσίαση καταλόγων, οι οποίοι είχαν ενδιαφέρον για τους χρήστες, δίνοντας τους τη δυνατότητα να ερευνήσουν σ' αυτούς και να βρουν πιο εύκολα τα στοιχεία τα οποία έψαχναν. Η yahoo εκμεταλλεύτηκε την έλλειψη πληροφόρησης και τη μετέτρεψε, σε έναν «βομβαρδισμό» ανεξέλεγκτων και πολλές φορές χωρίς έλεγχο πληροφοριών.

Η στήριξη της Yahoo από την εταιρία επενδύσεων χαρτοφυλακίου Sequoia Capital, έδωσε τη δυνατότητα στους ιδρυτές της να τη μετατρέψουν σε μια δυναμική, συνεχώς αναπτυσσόμενη και κερδοφόρα επιχείρηση η οποία δραστηριοποιείται σήμερα σ' όλο τον κόσμο, έχοντας βάσης και δίκτυο σ' όλες τις ηπείρους. Η Yahoo προσπάθησε να αυξήσει τη δυναμική της όχι βελτιώνοντας τη δράση της στο τομέα της πληροφόρησης, αλλά παρέχοντας περισσότερες υπηρεσίες στους χρήστες της προκειμένου να καταφέρει τους εγκλωβίσει στις τάξεις της.

Η κίνηση της αυτή τη χαρακτήρισε ενώ χαρακτήρισε και των ευρύτερο ανταγωνισμό μέχρι και σήμερα. Η στρατηγική που ακολούθησε εστιάσθηκε στην οριζόντια ολοκλήρωση, εξαγοράζοντας μπρος και πίσω εταιρίες με οργάνωση θεματικών ενοτήτων, με υπηρεσίες φιλοξενίας ιστοσελίδων κ.λπ. (Παπαδάκης, 2002)

Οι κινήσεις της τη κατέστησαν ανταγωνιστική, δεν της έδωσαν όμως τη δυνατότητα να εστιάσει και να βελτιώσει τη δυναμική εύρεσης την οποία και παρείχε στους χρήστες της. Η Yahoo από τη στιγμή της ίδρυσης της προχωράει στη συνεχή αύξηση των παρεχόμενων υπηρεσιών της, χωρίς να εστιάζει στη βελτίωση των δυνατοτήτων εύρεσης που δίνει. Οι πρόσφατες κινήσεις της στη παροχή υπηρεσιών αναφέρονται στην παροχή στους χρήστες της προσωπικού ημερολογίου, αλλά και άλλων δυνατοτήτων διαχείρισης του χρόνου τους και της καθημερινότητα τους. Τέλος η Yahoo τα τελευταία χρόνια δρα και στο τομέα, του ηλεκτρονικού εμπορίου δίνοντας τη δυνατότητα στους χρήστες της να προβούν σ' αγορές μέσω του διαδικτύου αλλά και να κάνουν ένα μεγάλο εύρος συναλλαγών.

Αντίθετα με το Yahoo όλες οι ανταγωνίστριες ιστοσελίδες λειτούργησαν ως μηχανές αναζήτησης, δεν αποτέλεσαν ένα απλό πίνακα περιεχομένων αλλά μια αράχνη, η οποία έψαχνε και ψάχνει στον ιστό και διαμορφώνει ευρετήριο με τις λέξεις κλειδιά που βρίσκει. Σαν αποτέλεσμα συνήθως επιστρέφει πολύ περισσότερες θέσεις στις οποίες υπάρχουν λέξεις που ταιριάζουν με τα κριτήρια της αναζήτησης σε σχέση με τον τρόπο που λειτουργεί το Yahoo. Το πρόβλημα αναφέρεται ότι δεν υπάρχει κάποια λογική και στοιχειώδης επιμέλεια, οπότε πολλές φορές ο χρήστης χάνεται ανάμεσα στις χιλιάδες των πληροφοριών ενώ οι περισσότερες από αυτές δε σχετίζονται με το θέμα το οποίο των ενδιαφέρει. Με βάση τα παραπάνω κατανοούμε ότι το φαινόμενο της υπερπληροφόρησης σε σχέση με τις υπάρχουσες δυναμικές ιστοσελίδες εστιάζεται σε δυο πεδία αναφοράς (Λέανδρος, 2005).

1. Στην λειτουργία ως καταλόγου και στην απλή παρουσίαση των ιστοσελίδων που υπάρχουν στο Ίντερνετ και θα μπορούσαν να βοηθήσουν, χωρίς όμως να δίνονται εγγυήσεις.

2. Στη μη καλή γνώση του χρήστη των δυνατοτήτων εύρεσης, οπότε και η μη χρήση σωστά λέξεων κλειδιά. Αυτό έχει ως αποτέλεσμα την άσκοπη εισροή πληροφοριών αλλά και τους συμβιβασμούς που μπορεί και προτίθεται να κάνει ο χρήστης.

1.3 Αξιολόγηση του διαδικτυού και είδη υπηρεσιών

Σε σχέση με τη σημερινή χρήση των δικτυακών τόπων αλλά και την εισροή χιλιάδων πληροφοριών μέσα από τις καθημερινές ευρέσεις που γίνονται, μπορούμε να πούμε ότι ο τεράστιος όγκος πληροφοριών του Internet σε συνδυασμό με την ελάχιστη οργάνωση που υπάρχει στο Δίκτυο καθιστά χρονοβόρα την εύρεση των πληροφοριών. Για την επίλυση αυτού του προβλήματος έχουν αναπτυχθεί διάφορες μέθοδοι, οι οποίοι με βάση και τη παραπάνω ανάλυση καταλήγουμε ότι είναι ανεπαρκείς.

"Οι δύο πιο δημοφιλείς είναι οι **indexes** *(ευρετήρια) και οι* **search engines** *(μηχανές αναζήτησης). Χρησιμοποιώντας τον* **Web browser** *αν γίνει κλικ σε μία κατηγορία θα οδηγηθεί ο χρήστης σε μία σειρά υποκατηγοριών. Στην κατηγορία αθλήματα για παράδειγμα θα οδηγηθείτε σε διάφορες κατηγορίες όπως ποδόσφαιρο, μπάσκετ, βόλεϊ, πόλο, κ.ο.κ. Ανάλογα με το μέγεθος του ευρετηρίου μπορεί να υπάρχουν διάφορα επίπεδα υποκατηγοριών"* (Reid, 2004).

Στο Internet υπάρχουν αρκετές μηχανές αναζήτησης και ευρετήρια, κάθε ένα εκ των οποίων έχει ορισμένα πλεονεκτήματα και μειονεκτήματα. Όταν αναζητά ο χρήστης μία πληροφορία και για να καλύψει το μεγαλύτερο δυνατό τμήμα του Δικτύου θα πρέπει να χρησιμοποιήσει αρκετές μηχανές αναζήτησης. Όμως η διαδικασία είναι αρκετά χρονοβόρα και για το λόγο αυτό έχει αναπτυχθεί ειδικό λογισμικό, ονόματι meta-search, το οποίο αυτοματοποιεί την αναζήτηση.

Για να υπάρχει ένα μέτρο σύγκρισης, αν ήταν εφικτό σύμφωνα με την έρευνα ν' αποθηκεύσει ο χρήστης όλ' αυτά τα στοιχεία σε κοινές δισκέτες κομπιούτερ και τοποθετούσε τις δισκέτες τη μια επάνω στην άλλη, θα κατάληγε σε μια τεράστια στήλη 8 φορές ψηλότερη από την απόσταση Γης-Σελήνης. Η έρευνα αναφέρει ότι ενώ χρειάστηκαν 300.000 χρόνια για να παράγει η ανθρωπότητα 12 τρισεκατομμύρια μεγκαμπάιτ. Με το σημερινό ρυθμό, θα καλύψει το ίδιο νούμερο σε 4 χρόνια. Η έρευνα αναφέρει πως ποσοστό 93% του συνόλου των πληροφοριών είναι σε ψηφιακή μορφή. Η υπερπληροφόρηση, και δη με ιλιγγιώδεις ταχύτητες, αποτελεί χαρακτηριστικό συστατικό της εποχής. Η έρευνα καταλήγει ότι το φαινόμενο της

υπερπληροφόρησης οδηγεί σ' ένα από τα πολλά κεφάλαια του ολοκληρωτισμού – δηλαδή στην παραπληροφόρηση της κοινής γνώμης.

Με βάση το Λέανδρο Ν αν υποθέσουμε ότι κάποιος θέλει να ενημερωθεί για το κίνημα κατά της παγκοσμιοποίηση και κυρίως για την οικολογική συνιστώσα του, θα πρέπει αρχικά να αξιοποιήσει τους δικτυακούς τόπους εγχώριους και διεθνείς που ήδη γνωρίζει και εκτιμά ότι θα του δώσουν χρήσιμες πληροφορίες αναφορικά με το πεδίο έρευνας του. Συγχρόνως μπορεί να καταφύγει σε εκατομμύρια ιστοσελίδες στις οποίες θα τον οδηγήσουν οι ιστοσελίδες εύρεσης (Λέανδρος,2005).

Αφού ο ενδιαφερόμενος συσσωρεύσει ένα μεγάλο όγκο πληροφοριών και διαβάσει έναν αριθμό κειμένων, είναι πιθανό να κρατήσει ορισμένες δικτυακές διευθύνσεις στα «αγαπημένα του». Αυτό θα τον βοηθήσει να παρακολουθεί αυτές τις ιστοσελίδες και στο μέλλον, το πρώτο πρόβλημα εδώ αναφέρεται στην υποκειμενικότητα των ιστοσελίδων σε σχέση με τις απόψεις που εκφέρουν. Το δεύτερο πρόβλημα αναφέρεται στην αύξηση των ιστοσελίδων που ελλοχεύει το κίνδυνο στο εγγύς μέλλον, ο χρήστης να μη μπορεί πια να τις παρακολουθεί χάνοντας έτσι σημαντικές εξελίξεις, αλλά και πληροφορίες που πιθανόν να του ήταν χρήσιμες. Το τρίτο και τελευταίο πρόβλημα αναφέρεται στη γλώσσα, μια και πολλές από τις ιστοσελίδες θα είναι στα αγγλικά, πράγμα που σημαίνει ότι κάποιοι εκ των χρηστών, δε θα μπορούν να τις διαβάσουν (Λέανδρος,2005).

Την σημερινή εποχή η ανταλλαγή σκέψεων, πληροφοριών και ιδεών έχουν κάνει επιτακτική την ανάγκη για βελτίωση των διαδικασιών επικοινωνίας. Η πρόοδος των διαφόρων τεχνολογιών έχει οδηγήσει στην απλούστευση της επικοινωνίας μεταξύ των ανθρώπων μέσα από την χρήση κινητών τηλεφώνων και ηλεκτρονικών υπολογιστών.

Μέσω της τεχνολογίας είναι πλέον δυνατή η επικοινωνία ατόμων από οποιοδήποτε σημείο. Η επικοινωνιακή ικανότητα και η αποτελεσματικότητα επηρεάζουν τις αποφάσεις, τις διαπροσωπικές σχέσεις, τις αντιλήψεις και τις στάσεις όλων των ατόμων. Η έλλειψη της επικοινωνίας οδηγεί σε δυσλειτουργίες, συγκρούσεις, ασυνεννοησία, κακές αποφάσεις, έλλειψη συντονισμού και υποκίνησης. Συνεπώς η επικοινωνία αποτελεί ένα σημαντικό

αντικείμενο μελέτης, την οποία καλούμαστε να προσεγγίσουμε σε συνδυασμό με τις τεχνολογίες που έχουν αναπτυχθεί.

Την σημερινή εποχή η επανάσταση στις τεχνολογίες της επικοινωνίας, οδήγησαν σε μια νέα μορφή επικοινωνίας μεταξύ των ατόμων, η οποία θα μπορούσε να χαρακτηριστεί ως απλοϊκή, ταχύτερη και ευκολότερη.

Τεχνολογίες όπως το διαδίκτυο, η κινητή τηλεφωνία, η τηλεδιάσκεψη και το ηλεκτρονικό ταχυδρομείο, λειτουργούν ως εναλλακτικές μορφές επικοινωνίας διευκολύνοντας τον πομπό και τον δέκτη στην άμεση μεταφορά και κατανόηση του μηνύματος.

Η ψηφιακή επανάσταση οδήγησε τον κόσμο σε ένα τεράστιο δίκτυο διακίνησης και ανταλλαγής πληροφοριών μεταξύ του αποστολέα και του δέκτη. Διάφορες γνώμες, απόψεις και θέσεις, μπορούσαν να διακινηθούν από οποιονδήποτε μέσω ενός ηλεκτρονικού υπολογιστή και του διαδικτύου. Ο συνδυασμός της ανάλυσης της πληροφορίας σε ψηφιακή μορφή και η δυνατότητα μετάδοσής της σε μορφή κατανοητή από τον άνθρωπο, ως κείμενο ή εικόνα, επιτρέπει την συμμετοχή οποιουδήποτε στην διαδικασία παραγωγής και διακίνησης της πληροφορίας.

Αυτό βέβαια δεν καθιστά και την κοινωνία της πληροφορίας περισσότερο δημοκρατική. Αν και η τεχνολογία έχει αποδειχθεί ιδιαίτερα σημαντική στην διαδικασία της επικοινωνίας, παρόλ' αυτά η παραγωγή της είναι εξαιρετικά πολύπλοκη, δαπανηρή, απαιτεί συγκέντρωση πόρων, και είναι συνήθως συγκεντρωμένη σε μεγάλες εταιρείες. Επί πλέον, η παραγωγή, ο έλεγχος και η διάθεση της πληροφορίας αποτελούν δύναμη και εξουσία για αυτούς που αποκτούν τη δυνατότητα να συγκεντρώνουν την πληροφορία. Η οικονομική διάσταση της πληροφορίας, η παραγωγή, ο έλεγχος και η διάθεσή της, ενσωματώθηκε στις διαδικασίες της αγοράς και με την πάροδο του χρόνου εμπορευματοποιήθηκε.

Μέσω των νέων επικοινωνιακών τεχνολογιών επιτεύχθηκε η ανάπτυξη της οικονομίας της αγοράς στο πλαίσιο των κρατών που τις ανέπτυξαν, αλλά και ενίσχυσε τους μηχανισμούς της αγοράς σε παγκόσμιο επίπεδο.

Η μαζική παραγωγή και η πρόσβαση πολλών στα προϊόντα της ψηφιακής τεχνολογίας και των τηλεπικοινωνιών με σχετικά μικρό κόστος,

επέφερε την εξατομίκευση της πληροφορίας, ενισχύοντας ταυτόχρονα δύο φαινομενικά αντίθετες τάσεις: την ενίσχυση της ατομικότητας αλλά και της συλλογικότητας.

Από τη μια, η δυνατότητα επικοινωνίας του ατόμου μέσω πολλαπλών δικτύων και η αναγωγή του (ατόμου) σε ενεργό πόλο επικοινωνίας, ενίσχυσε την ατομικότητα η οποία όμως για να ολοκληρωθεί απαιτεί μια κοινωνία της πληροφορίας, δηλαδή δέκτες και πόλους επικοινωνίας, στην οποία το άτομο συμμετέχει και ξεπερνά τον έλεγχό και την εμβέλειά του καθώς ολοκληρώνεται επικοινωνιακά σε εθνικό, περιφερειακό και παγκόσμιο επίπεδο. Συνεπώς για να είναι αποτελεσματική η επικοινωνία απαιτεί έναν ενεργό πόλο (ατομικότητα) και την συνεργασία των πόλων μεταξύ τους για την αποδοτικότητα της επικοινωνίας (συλλογικότητα).

Διαπιστώνουμε λοιπόν ότι η τεχνολογία της επικοινωνίας εκτός από το ότι διευκόλυνε τις διαδικασίες επικοινωνίας μεταξύ του πομπού και του δέκτη, παράλληλα βοήθησε και στην ενίσχυση της ατομικότητας και της συλλογικότητας μεταξύ των ατόμων

Το ταχυδρομείο το οποίο αποτελεί το παλαιότερο μέσω επικοινωνίας συνεχίζει να είναι ένα από τα πιο αξιόπιστα μέσα επικοινωνίας της επιχείρησης με τον πελάτη. Συγκεκριμένα προκειμένου μια επιχείρηση να μπορέσει να παραδώσει άμεσα και αποτελεσματικά δέματα στους πελάτες της, τα οποία μάλιστα μπορεί να αποτελούν και προϊόν κάποιας τηλεφωνικής παραγγελίας ή παραγγελίας μέσω email πρέπει να χρησιμοποιήσει το ταχυδρομείο.

Το ηλεκτρονικό ταχυδρομείο email είναι ένα από τα σημαντικότερα μέσα συνεργασίας αλλά και επικοινωνίας μεταξύ επιχειρήσεων και πελατών. Το email έχει τα εξής πλεονεκτήματα (Kotler, 1997):

1. Άμεση επαφή με τον πελάτη.
2. Αποτελεί μια οικονομική λύση για να μπορέσει να επικοινωνήσει ο πελάτης με την εταιρεία αλλά και το αντίστροφο
3. Αποστολή φωτογραφιών γεγονός πολύ σημαντικό για τις επιχειρήσεις.
4. Εξάλειψη του προβλήματος της διαφοράς ώρας από χώρα σε χώρα αλλά

και η πιθανότητα ενόχλησης του πελάτη

5. Μέσω email η επιχείρηση μπορεί να ενημερώσει τον πελάτη της, να διαφημιστεί, να πουλήσει τα είδη της, να θερμάνει τις σχέσεις της μαζί του.

6. Το email δίνει τη δυνατότητα στον πελάτη να εκφράσει το παράπονο, το αίτημα του άμεσα και οικονομικά, αλλά και στην επιχείρηση να τον εξυπηρετήσει άμεσα.

1.4 Η επικοινωνιακή δυναμική internet

Η εξέλιξη μέσα στην ιστορία δεν ήταν κάτι το προσχεδιασμένο αντίθετα οι μεγάλες επιχειρήσεις τηλεπικοινωνιών και πληροφορικής έχοντας άλλες επιχειρηματικές δράσεις και ερευνητικές κατευθύνσεις οδηγήθηκαν σε τεχνολογικές και καινοτόμες δραστηριότητες, οι οποίες μέσα και από τις κινήσεις των χρηστών όπως το ηλεκτρονικό ταχυδρομείο, οι φυλλομετρητές (browsers), οι μηχανές αναζήτησης οδήγησαν στην ανάπτυξη του διαδικτυακού περιβάλλοντος, ως πεδίο υποδοχής όλων των παραπάνω αναγκών και πηγών πληροφόρησης.

Το διαδίκτυο, ήταν και είναι μια τεχνολογική επανάσταση η οποία ήρθε να καλύψει την ανάγκη της άμεσης και αμφίδρομης επικοινωνίας, δημιουργώντας και την εντύπωση όπως αναφέρει ο Ν. Λέανδρος ότι *«οι πολίτες λόγω του Διαδικτύου θα μπορούσαν να ποντάρουν σε ένα νέο μοντέλο δημοκρατικής κοινωνικής λειτουργίας και γενικότερης εύρυθμης κοινωνικής ένταξης»* (Λέανδρος, 2005).

Στο πλαίσιο αυτό μπορεί επίσης να γίνει κατανοητή και η ραγδαία και εξελικτική πορεία του Διαδικτύου. Σήμερα οι εμπλεκόμενες σε αυτό εταιρείες προσφέρουν στους χρήστες δωρεάν υπηρεσίες όπως ηλεκτρονικό ταχυδρομείο (email), ηλεκτρονικές σελίδες (web pages), σελίδες κοινωνικής δικτύωσης (chat rooms), πίνακες μηνυμάτων (message boards), με στόχο οι ίδιες οι εταιρείες να απολαμβάνουν με αυτό τον τρόπο εμπορικά οφέλη από την διαφήμιση, απαλλάσσοντας ταυτόχρονα τους χρήστες από οποιοδήποτε κόστος.

Την ίδια στιγμή, η ανάπτυξη του ηλεκτρονικού εμπορίου (e-commerce)

με πολλά επιτυχημένα παραδείγματα ηλεκτρονικών επιχειρήσεων -όπως το Amazon και το EBay- έδωσαν νέα μορφή στην εμπορική πρακτική, καθιστώντας την καταρχάς ως συναλλαγή που διεξάγεται σε παγκόσμιο επίπεδο, συνεπακόλουθα όμως και σε παγκόσμιο ανταγωνισμό, με αποτέλεσμα και σε αυτή την περίπτωση να ευνοείται ο καταναλωτής-χρήστης.

Ταυτόχρονα με την ανάπτυξη του ηλεκτρονικού «επιχειρείν» παρατηρείται και η εμφάνιση των μηχανών αναζήτησης (search engines), όπως το Yahoo και αρκετά αργότερα το Google, οι οποίες έδωσαν νέα ώθηση στην χρηστικότητα και την αμεσότητα πρόσβασης στην πληροφορία, σε τέτοιο βαθμό ώστε σήμερα να αποτελούν ένα πολύ σημαντικό μέσο εμπορικής προώθησης (Search Engine Optimization), το οποίο περιλαμβάνει τεχνικές κατασκευής και δικτύωσης ιστοσελίδων που να προσφέρουν καλύτερες θέσεις εμφάνισης στα αποτελέσματα των «λέξεων-κλειδιών» και οι οποίες παραπέμπουν ουσιαστικά σε ηλεκτρονικές σελίδες-επιχειρήσεις.

Τα πιο συχνά χρησιμοποιούμενα συστήματα είναι το διαδίκτυο, η κινητή τηλεφωνία και τα ενδοεπιχειρησιακά δίκτυα. Στην παρούσα ενότητα θα αναλύσουμε για το κάθε σύστημα αναλυτικά προκειμένου να δούμε πως η πρόοδος του βοηθά την επικοινωνία μεταξύ των ατόμων.

Διαδίκτυο

Η χρήση του διαδικτύου προκαλεί σημαντικές αλλαγές στον τρόπο επικοινωνίας. Ουσιαστικά το διαδίκτυο με την πάροδο του χρόνου έχει καταφέρει να εξελιχθεί σε μια κινητή βιβλιοθήκη με πολλές πληροφορίες, καθώς επίσης και σε μια βάση μέσω της οποίας μπορούν να επικοινωνούν άτομα από διαφορετικές χώρες με πολύ χαμηλό κόστος. Οι απόψεις σχετικά με τις δυνατότητες που παρέχει η τεχνολογία του διαδικτύου ως πηγή πληροφορίας και ως μέσο επικοινωνίας είναι πάρα πολλές (Ράπτης, & Ράπτη, 1998).

Ως πηγή πληροφορίας, το διαδίκτυο παρέχει πρόσβαση σε μεγάλες βάσεις δεδομένων, σε υλικό σχεδιασμένο για ανοικτή και εξ αποστάσεως εκπαίδευση. Επίσης παρέχει πρόσβαση σε τεράστιες ποσότητες πληροφορίας διαφορετικού τύπου, όπως κείμενα, εικόνες, γραφικά, ήχο. Για παράδειγμα, σε

μια επιχείρηση μέσω του διαδικτύου μπορεί κάποιος να αναζητήσει στοιχεία για ανταγωνιστές, ή ακόμα και εκτός επιχείρησης ένας μαθητής μπορεί να συνδεθεί με μεγάλες ηλεκτρονικές βιβλιοθήκες ώστε να αναζητήσει ερευνητικό υλικό, πολιτιστικές και παιδαγωγικές πληροφορίες.

Ως μέσο επικοινωνίας, το διαδίκτυο, δίνει τη δυνατότητα στους χρήστες να επικοινωνήσουν μεταξύ τους μέσω ποικίλων ασύγχρονων και σύγχρονων υπηρεσιών όπως αυτές του ηλεκτρονικού ταχυδρομείου, της συμμετοχής σε ομάδες συζήτησης με κοινά ενδιαφέροντα, σε διάφορες εξ αποστάσεως συνεδριάσεις και σε ομαδικές δραστηριότητες. Για παράδειγμα, μέσω του διαδικτύου οι μαθητές μπορούν να επικοινωνούν μεταξύ τους για την εκπόνηση ομαδικών εργασιών.

Διαπιστώνουμε λοιπόν ότι μέσω του διαδικτύου, η απόσταση και ο χρόνος δεν αποτελούν πλέον εμπόδια στην ανταλλαγή πληροφοριών και στην επίτευξη της επικοινωνίας. Οι ερευνητές έχουν επιστήσει την προσοχή τους στο γεγονός ότι ο εντοπισμός της κατάλληλης πληροφορίας στο διαδίκτυο γίνεται ολοένα και πιο δύσκολος λόγω της ταχύτατης ανάπτυξης και ποικιλομορφίας της προσφερόμενης πληροφορίας.

Η αλληλεπιδραστική επικοινωνία μέσω διαδικτύου όπως για παράδειγμα ομάδες συζήτησης βασίζεται στην ανταλλαγή κειμένων, χωρίς να γίνεται χρήση των πολυμέσων που παρέχει ο υπολογιστής

Διαπιστώνουμε λοιπόν ότι το διαδίκτυο προσφέρει ευκολία επικοινωνίας μέσω των νέων μορφών επικοινωνίας που παρέχει. Ωστόσο ο ρόλος του διαδικτύου ως επικοινωνιακού εργαλείου ίσως έχει υπερτονιστεί αφού ορισμένες φορές δεν διευκολύνει την αναπαραγωγή απόψεων στο περιβάλλον της οθόνης. Παρόλαυτά, το διαδίκτυο έχει χωρίς αμφιβολία κυρίαρχο ρόλο στην τεχνολογία της επικοινωνίας η οποία εξελίσσεται διαρκώς.

Κινητή τηλεφωνία

Ο τομέας της κινητής τηλεφωνίας αποτελεί ακόμα μια επανάσταση της τεχνολογίας. Η ανακάλυψη της κινητής τηλεφωνίας διευκόλυνε πολλούς και ενίσχυσε την κινητή επικοινωνία. Πριν την ανακάλυψη της κινητής

τηλεφωνίας, πολλές επιχειρήσεις σπαταλούσαν χρόνο προκειμένου να έρθουν σε επαφή με τους συνεργάτες τους. Η εμφάνιση τους διευκόλυνε τις διαπροσωπικές σχέσεις των ατόμων, βελτίωσε τις επιχειρησιακές δραστηριότητες και οδήγησε στην δημιουργία νέων μορφών επικοινωνίας.

Ειδικότερα όπως είδαμε μέσω της κινητής τηλεφωνίας υπάρχει ένας πομπός και ένας δέκτης μηνύματος. Αυτοί οι δύο ανταλλάσσουν απόψεις ή μεταφέρουν πληροφορίες. Εν συνεχεία ο δέκτης του μηνύματος καλείται να κατανοήσει και αναλύσει την πληροφορία που δέχτηκε και να προβεί στην εφαρμογή αυτής.

Η τελευταία εξέλιξη που πραγματοποιήθηκε στην κινητή τηλεφωνία ήταν η πρόσβαση στο διαδίκτυο μέσω κινητού τηλεφώνου.

Η δυνατότητα αυτή μπορεί να πραγματοποιηθεί μέσω του i-mode. Το i-mode είναι ένας τρόπος χρήσης του διαδικτύου ο οποίος παρέχει κινητή πρόσβαση στο διαδίκτυο. Το διαδίκτυο μέσω της κινητής τηλεφωνίας μπορεί να θεωρηθεί ως ένας συνδυασμός τηλεπικοινωνιών και διαδικτυακών τεχνολογιών. Το i-Mode είναι ουσιαστικά ένα μέσο διαφήμισης μέσω του κινητού τηλεφώνου. Αυτή η μορφή είναι εντελώς νέα στον χώρο της κινητής τηλεφωνίας και πολύ ευέλικτη για την διαφήμιση, την ικανοποίηση των πελατών, την ενίσχυση του ονόματος της εταιρίας και τις συναλλαγές.

Για την μεταβίβαση των πληροφοριών, το i-MODE χρησιμοποιεί HTML (HyperText Markup Language) μορφή και δεν απαιτεί την χρήση μετατροπής ιστοσελίδων σε HTML μορφή

Μέσω του i-mode επιτρέπεται στους χρήστες η πρόσβαση στο διαδίκτυο και η επικοινωνία μέσω e-mail.

Συνεπώς με την χρήση του i-mode μπορούν να επιτευχθούν τα κατωτέρω:

1. Μπορεί κάποιος να λάβει ή να στείλει e-mail από το κινητό του και να λάβει μηνύματα κειμένου από τους παροχείς υπηρεσιών
2. Μπορεί κάποιος να διαβάσει και να απαντήσει στα e-mail από τον λογαριασμό του στο διαδίκτυο.

3. Μπορεί να ενημερωθεί για τις υπηρεσίες του i-mode μέσω του μενού αλλά και να έχει πρόσβαση σε πολλές ιστοσελίδες οι οποίες έχουν αναπτυχθεί από ιδιωτικούς παροχείς.

Στην πραγματικότητα το i-mode μπορεί να λαμβάνει και να στέλνει e-mails και να προσφέρει πρόσβαση στον λογαριασμό της τραπέζης μέσω του e-banking.Μεγάλο μέρος της επιτυχίας του κινητού διαδικτύου, οφείλεται στην εξέλιξη των κινητών τηλεφώνων. Τα σημερινά κινητά πλησιάζουν σε δυνατότητες έναν απλό υπολογιστή. Τα έξυπνα κινητά δίνουν προσφέρουν στους χρήστες περιήγηση στο Διαδίκτυο και μεταφορά σε μια ιστοσελίδα μέσω της διεύθυνσης

Ενδοεπιχειρησιακή επικοινωνία

Η επικοινωνία στο εσωτερικό μιας επιχείρησης, αποτελεί την βάση πάνω στην οποία θα αναπτυχθούν οι δραστηριότητες της και θα είναι αποτελεσματική η πολιτική της. Η αποτελεσματική επικοινωνία σε μια επιχείρηση εξασφαλίζει την αρμονική συνύπαρξη των κέντρων αποφάσεων που διαθέτει η οργάνωση, και εμποδίζει την ανεξέλεγκτη δημιουργία νέων ανεξάρτητων κέντρων τα οποία θα μπορούσαν να προκαλέσουν διάσπαση της ενότητας στο οργανωτικό σχήμα.

Η επικοινωνία παίζει το σημαντικότερο ρόλο μέσα στην επιχείρηση, προκειμένου να υπάρχει καλή επαφή μεταξύ προϊσταμένων και υφισταμένων και των διαφόρων τμημάτων μέσα στον οργανισμό. Η καλή επικοινωνία βοηθάει να μην δημιουργηθούν ανεξάρτητα και αυτόνομα κέντρα που θα μπορούσαν να διασπάσουν την οργανωτική δομή του οργανισμού (Τζωρτζάκης και Τζωρτζάκη, 2002) .Η καθοδήγηση, η ηγεσία, η υποκίνηση και το κατάλληλο κοινωνικό κλίμα στο εσωτερικό της επιχείρησης δεν είναι δυνατόν να επιτευχθεί χωρίς αποτελεσματική επικοινωνία. Η επικοινωνία είναι απαραίτητη για την καλή λειτουργία και για το σωστό προφίλ της επιχείρησης.

Μια επιχείρηση δίνει ιδιαίτερη βαρύτητα στην διαπροσωπική επικοινωνία και στα επικοινωνιακά δίκτυα που δεν περιορίζονται μόνο στην ομαλή ενδοργανωσιακή επικοινωνία αλλά περιλαμβάνουν και εξωγενείς

παράγοντες σχετικούς με τις δραστηριότητες και τις πρακτικές της οργάνωσης.

Κεφάλαιο 2ο Πληροφοριακά συστήματα και ασφάλεια

2.1 Εισαγωγή

Ένα πληροφοριακό σύστημα μπορεί να οριστεί ως ένα σύνολο ανθρώπων, δεδομένων, τεχνολογίας και οργανωτικών μεθόδων που δουλεύουν μαζί για να συλλέξουν, να επεξεργαστούν, να αποθηκευτούν και να μεταβιβάσουν πληροφορίες για να στηρίξουν τη λήψη αποφάσεων και τον έλεγχο: Ειδικά, θα εστιάσουμε την ανάλυση στα πληροφοριακά συστήματα διοίκησης, τα οποία είναι συστήματα που στηρίζουν τη λήψη αποφάσεων και τον έλεγχο από τη διεύθυνση των επιχειρήσεων.

Τα πληροφοριακά συστήματα δεν είναι απλώς οι ηλεκτρονικοί υπολογιστές. Συνήθως, το πληροφοριακό σύστημα περιλαμβάνει και την επιχείρηση ή σημαντικά μέρη της, όπως τους εργαζομένους που εισάγουν δεδομένα στο σύστημα και παίρνουν πίσω την εκροή του. Τα στελέχη επιχειρήσεων είναι (ή θα έπρεπε να είναι) μέρος του πληροφοριακού συστήματος, αφού το πληροφοριακό σύστημα είναι σχεδιασμένο για να υπηρετεί τις ειδικές ανάγκες τους για πληροφορίες.

Μερικοί επιχειρηματίες πιστεύουν ότι στον πολύπλοκο σύγχρονο κόσμο που ζούμε, το να διευθύνεις σωστά μια επιχείρηση είναι κατά κύριο λόγο ζήτημα διαχείρισης πληροφοριών. Αυτό ισχυρίζονται ότι πετυχημένος διευθυντής είναι εκείνος που μπορεί να συγκεντρώσει, να ελέγξει και να χρησιμοποιήσει τις πληροφορίες με επιτυχία (Clarke, 2012).

Η λήψη αποφάσεων είναι, στην ουσία, ένα ρεύμα από αλληλένδετους, συνεχείς και ταυτόχρονους τρόπους εκλογής. Για να είναι σε θέση ένα διοικητικό στέλεχος να παίρνει σωστές αποφάσεις, πρέπει να έχει πληροφορίες και ορισμένα διοικητικά μέσα. Αν και σπάνια ένα διοικητικό στέλεχος έχει στη διάθεσή του όλες τις απαιτούμενες πληροφορίες, εφόσον οι υπόλοιπες συνθήκες παραμένουν οι ίδιες, όσο περισσότερες πληροφορίες έχει αυτός στη διάθεσή του τόσο ορθότερες θα είναι οι αποφάσεις του (Avison & Fitzgerald, 1998).

Οι πληροφορίες μπορούν να συγκεντρωθούν από πηγές, οι οποίες

βρίσκονται μέσα και έξω από την επιχείρηση, οπότε καλούνται αντίστοιχα εσωτερικές ή εξωτερικές πληροφορίες. Οι εξωτερικές πληροφορίες συγκεντρώνονται από πηγές, οι οποίες βρίσκονται εκτός της επιχείρησης . Στις πηγές αυτές, περιλαμβάνονται οι δημοσιεύσεις της Εθνικής Στατιστικής Υπηρεσίας, των αρμοδίων κρατικών υπηρεσιών, των τραπεζών, των ειδικών ινστιτούτων του συνδέσμου του κλάδου της επιχείρησης των επιμελητηρίων και διάφορες άλλες Ελληνικές και ξένες δημοσιεύσεις (Βασιλακόπουλος & Χρυσικόπουλος, 1990).

Οι εσωτερικές πληροφορίες είναι στοιχεία, τα οποία μπορεί να συγκεντρώνονται από τις εκθέσεις και τα αρχεία της επιχείρησης. Η διαφορά εξωτερικών και εσωτερικών πληροφοριών, βρίσκεται στο γεγονός ότι ενώ οι εξωτερικές πληροφορίες συγκεντρώνονται και διατίθενται σε όλους, οι εσωτερικές πληροφορίες πρέπει να δημιουργηθούν από την ίδια επιχείρηση. Όσο οι πελάτες θα γίνονται περισσότερο απαιτητικοί αναφορικά με τις προτιμήσεις τους και όσο ο ανταγωνισμός θα γίνεται εντονότερος τόσο θα αυξάνει η σπουδαιότητα για οργάνωση, ανάπτυξη και χρησιμοποίηση από την επιχείρηση ενός συστήματος πληροφόρησης (Οικονόμου & Γεωργόπουλος, 1995).

Σήμερα με τη χρήση των ηλεκτρονικών υπολογιστών, από όλες σχεδόν τις επιχειρήσεις, η συγκέντρωση εσωτερικών πληροφοριών απλουστεύεται. Η επιχείρηση μπορεί να έχει καταχωρημένες πολλές και διάφορες πληροφορίες, τόσο για τους πελάτες της όσο και για τους ανταγωνιστές της. Εκτός από τις παραπάνω πηγές,, η έρευνα αποτελεί ένα από τα σπουδαιότερα μέσα πληροφόρησης για την επιχείρηση (Whitman & Mattord, 2011). Σήμερα οι αποφάσεις της διοίκησης πρέπει να βασίζονται σε θεμελιωμένες και κατάλληλες πληροφορίες και όχι σε απλές προαισθήσεις και υποθέσεις της διοίκησης, όπως συνέβαινε στο παρελθόν. Για το λόγο αυτό, οι επιχειρήσεις σήμερα χρηματοδοτούν τις έρευνες σε διάφορους τομείς προκειμένου να μπορούν τα διοικητικά στελέχη να έχουν ακριβείς και κατάλληλες πληροφορίες για τη λήψη ορθών αποφάσεων . Στο μέλλον, η επιτυχημένη διοίκηση θα στηρίζεται ακόμη περισσότερο στην ορθή διαχείριση των πληροφοριών (Dhillon, 2007).

2.2 Βασικές έννοιες θεωρίας συστημάτων

Τα Ολοκληρωμένα Πληροφοριακά Συστήματα Διαχείρισης (ERP Enterprise Resource Planning Systems) αποτελούν ένα σύνολο εφαρμογών λογισμικού που υποστηρίζουν ένα ευρύ φάσμα επιχειρησιακών δραστηριοτήτων και λειτουργιών (Ιωάννου 2006). Ειδικότερα το ERP είναι ένα επιχειρησιακό εργαλείο που εξυπηρετεί και διευκολύνει τον έλεγχο, την παρακολούθηση και τον συντονισμό των εργασιών μιας επιχείρησης (τόσο στις κεντρικές όσο και στις απομακρυσμένες εγκαταστάσεις της). Τα Ολοκληρωμένα Πληροφοριακά Συστήματα Διαχείρισης επιχειρησιακών πόρων αποσκοπούν στην αυτοματοποίηση των επιχειρησιακών διαδικασιών σε τομείς, όπως:

- Τα οικονομικά
- Την διαχείριση της εφοδιαστικής αλυσίδας
- Την παραγωγή
- Το ηλεκτρονικό εμπόριο
- Την διαχείριση των ανθρώπινων πόρων
- Την διαχείριση των έργων
- Την διαχείριση των πελατειακών σχέσεων

Με την χρήση των ERP μπορούν να επιτευχθούν τα ακόλουθα:

- Η συγκέντρωση δεδομένων
- Η ενοποίηση και ολοκλήρωση όλων των εφαρμογών μιας επιχείρησης
- Ο επανασχεδιασμός των επιχειρησιακών διαδικασιών
- Η βελτιστοποίηση των διαδικασιών λειτουργίας
- Η εξοικονόμηση των επιχειρησιακών πόρων
- Η αύξηση της παραγωγικότητας
- Η απόκτηση συγκριτικού πλεονεκτήματος μέσα από την χρήση νέων τεχνολογιών πληροφορικής

Δεδομένου ότι η σύγχρονη επιχειρηματική δραστηριότητα στηρίζεται στην κοινωνία της πληροφορίας και οι επιχειρήσεις πρέπει να είναι σε θέση να

ανταποκριθούν σε υψηλές απαιτήσεις και προκλήσεις, οφείλουν να διαθέτουν βασικές διαδικασίες διαχείρισης που να παρέχουν ολοκληρωμένη εικόνα της οργάνωσης της επιχείρησης ώστε να είναι εφικτή η αποτελεσματική ανταλλαγή δεδομένων μεταξύ των τμημάτων και των λειτουργιών μιας επιχείρησης. Τα συστήματα ERP που καταγράφουν και συλλέγουν στις συναλλαγές μιας επιχείρησης καθιστούν εφικτή την παροχή πληροφοριών προς όλα τα επίπεδα οργάνωσής της σε πραγματικό χρόνο. Τα συστήματα ERP μέσω μιας συνεκτικής βάσης δεδομένων, είναι μια σύνθεση από ολοκληρωμένες εφαρμογές λογισμικού που συνδέει ποικίλες επιχειρηματικές διαδικασίες, ώστε να ικανοποιήσει στόχους που αφορούν την αποτελεσματικότερη οργάνωση της παραγωγής και των σταδίων που προηγούνται ή έπονται αυτών καθώς και την αρτιότερη και ποιοτικότερη εξυπηρέτηση των πελατών.

Το σύγχρονο επιχειρηματικό και οικονομικό περιβάλλον στο οποίο δραστηριοποιούνται οι επιχειρήσεις είναι ιδιαίτερα ανταγωνιστικό με το άνοιγμα νέων αγορών, αλλά και τις συνεχώς αυξανόμενες απαιτήσεις των πελατών. Κατά συνέπεια οι επιχειρήσεις πιέζονται όλο και περισσότερο για μείωση του κόστους σε όλο το εύρος της εφοδιαστικής αλυσίδας, δραστική μείωση των αποθεμάτων, ελαχιστοποίηση των καθυστερήσεων στις παραδόσεις των παραγόμενων προϊόντων, βελτίωση της ποιότητας των παρεχόμενων υπηρεσιών. Έτσι οι πρακτικές και οι διαδικασίες διαχείρισης των επιχειρήσεων οφείλουν να αναπροσαρμοστούν και η ζήτηση, η παραγωγή και ο εφοδιασμός να λειτουργούν κατά το δυνατό περισσότερο αποτελεσματικά.

Σε μια επιχείρηση μπορούν να υπάρχουν αρκετά διαφορετικά Πληροφοριακά Συστήματα ή ένα Πληροφοριακό Σύστημα να αποτελείται από αρκετά ξεχωριστά Πληροφοριακά Συστήματα. Τα Πληροφοριακά Συστήματα είναι συνδεδεμένα μέσω ηλεκτρονικών δικτύων, ενώ υπάρχουν διεταιρικά Πληροφοριακά Συστήματα που συνδέουν την ροή πληροφοριών σε δύο ή και περισσότερες επιχειρήσεις (Σιασιάκος 2006). Τα Πληροφοριακά Συστήματα μπορούν να ταξινομηθούν και να διακριθούν ανάλογα:

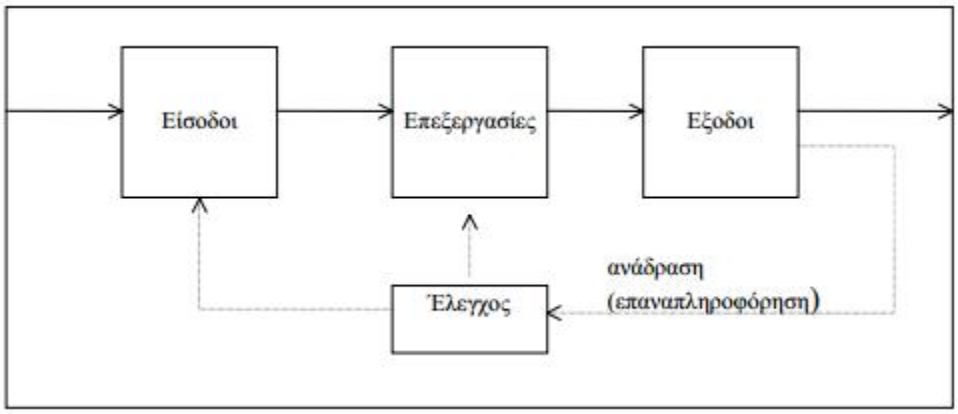
1. Την Οργανωτική Δομή

- Τα ΠΣ τμημάτων / διευθύνσεων (Departmental I.S)
- Τα Εταιρικά ΠΣ (Enterprise I.S)
- Τα Διεπιχειρησιακά ΠΣ (Inter- organizational I.S – IOS)

2. Την Περιοχή Λειτουργίας
   - Τα λογιστικά ΠΣ (Accounting I.S)
   - Τα οικονομικά ΠΣ (Finance I.S)
   - Τα κατασκευαστικά (λειτουργίες / παραγωγή) ΠΣ (Manufacturing I.S)
   - Τα ΠΣ Μάρκετινγκ (Marketing I.S)
   - Τα ΠΣ Διοίκησης Ανθρωπίνων Πόρων (H.R.M.I.S)
3. Την Παρεχόμενη Υποστήριξη
   - Τα Συστήματα Διεκπεραίωσης Συναλλαγών
   - Τα Πληροφοριακά Συστήματα Διοίκησης
   - Τα Συστήματα Αυτοματοποίησης Γραφείου
   - Τα Συστήματα Υποστήριξης Αποφάσεων
   - Τα Συστήματα Υποστήριξης Ανώτατης Διοίκησης
   - Τα Συστήματα Υποστήριξης Ομάδων
   - Τα Συστήματα Γνώσης
4. Την Αρχιτεκτονική Συστήματος
   - Σύστημα βασισμένο σε υπολογιστή μεγάλης ισχύος
   - Σύστημα βασισμένο σε ένα προσωπικό υπολογιστή
   - Κατανεμημένο ή δικτυωμένο υπολογιστικό σύστημα
5. Τις Ενέργειες ή τις Λειτουργίες που Υποστηρίζουν
   - Λειτουργικές
   - Διοικητικές
   - Στρατηγικές

Οι βασικές έννοιες θεωρίας συστημάτων είναι οι ακόλουθες (Ρηγόπουλος, 2011):

1. Σύστημα (system) είναι ένα σύνολο από (βλέπε σχήμα 2.1).



Σχήμα 2.1 Τα στοιχεία που απαρτίζουν ένα σύστημα

Πηγή: Ρηγόπουλος Γ., (2011), *Πληροφοριακά συστήματα και ομαδικές αποφάσεις*, Εκδόσεις Νέων Τεχνολογιών

2. Είσοδος, ή εισροές είναι τα στοιχεία εκείνα τα οποία εισέρχονται στο σύστημα.

3. Η ανάδραση ή επαναπληροφόρηση (feedback) είναι πληροφορία που αφορά την απόδοση του συστήματος.

Τα πληροφοριακά συστήματα αποτελούν βασική προϋπόθεση επιβίωσης μιας επιχείρησης. Συγκεκριμένα στόχος τους είναι (Δημητριάδης, 1998):

1. Η υποστήριξη των διοικητικών στελεχών, όλων των επιπέδων, στη λήψη έγκαιρων και κατά το δυνατόν κοντά στη πραγματικότητα αποφάσεων, κατά την άσκηση των διοικητικών τους καθηκόντων.
2. Η υποστήριξη της διαχείρισης της καθημερινής λειτουργίας της επιχείρησης.
3. Ο έλεγχος λειτουργίας της επιχείρησης.

Πολλές εταιρίες ανεξάρτητα από το μέγεθος ή τα χρήματα τα οποία

επενδύθηκαν από τους ιδρυτές τους, στο ξεκίνημα τους κατάφεραν να έχουν μια επιτυχημένη πορεία λόγω της κατανόησης από τη πρώτη στιγμή που ξεκίνησαν σε σχέση με τη σημασία και τη σπουδαιότητα των πληροφοριακών συστημάτων (Slack, 2004).

Ως παράδειγμα μπορεί ν' αναφερθεί η αμερικανική εταιρία διανομής αεροπορικών και επίγειων δεμάτων, United Parcel Service, την οποία μπορεί οι ιδρυτές της να έκαναν την έναρξη της σ' ένα υπόγειο γραφείο μεγέθους ντουλάπας και αρχικά να έκαναν τη διανομή των δεμάτων με ποδήλατα, όμως κατάφεραν να τη φτάσουν σήμερα να είναι η μεγαλύτερη εταιρία διανομής στην Αμερική μια και από τη πρώτη στιγμή έδωσαν μεγάλη βαρύτητα στη λειτουργία και σημασία των πληροφορικών συστημάτων επενδύοντας μέσα στα χρόνια οι ίδιοι και οι διάδοχοι τους μεγάλα ποσά στις νέες τεχνολογίες, πετυχαίνοντας έτσι να διαφοροποιούνται συνεχώς αλλά και ν' εξυπηρετούν καλύτερα τους τελικούς πελάτες τους (Λαοπόδης, 1992).

Το παραπάνω παράδειγμα υποδεικνύει τη σημασία των πληροφορικών συστημάτων, των οποίων η χρήση έχουν την ικανότητα ένα μικρό οργανισμό να τον μετατρέψουν σε μεγάλο, αλλά και το αντίθετο είναι δυνατόν να συμβεί όταν η χρήση τους είναι ελλιπής ή αόριστη.

2.3 Πληροφοριακά συστήματα

Η τεχνολογία των πληροφοριών αναφέρεται στις διαδικασίες, τις πρακτικές ή τα συστήματα που διευκολύνουν την επεξεργασία και τη μεταφορά πληροφοριών. Αναμφίβολα, σήμερα οι περισσότεροι είναι πολύ εξοικειωμένοι με τα σύγχρονα συστατικά της τεχνολογίας των πληροφοριών. Για παράδειγμα, μπορεί να χρησιμοποιούν προσωπικό ηλεκτρονικό υπολογιστή και από τη δουλειά την οποία κάνουν. να είναι εξοικειωμένοι με τα πληροφοριακά συστήματα διοίκησης. Πιθανόν χρησιμοποιούν κυψελοειδή τηλέφωνα, τηλεομοιοτυπία (fax) και τα όλο και πιο διαδεδομένα συστήματα ηλεκτρονικού ταχυδρομείου και ταχυδρομείου φωνής. Αυτού του είδους οι τεχνολογίες των πληροφοριών άλλαξαν δραματικά τον τρόπο με τον οποίο οι άνθρωποι κάνουν τις δουλειές τους και τον τρόπο με τον οποίο διοικούνται οι επιχειρήσεις (Kennedy, 1997).

Τα πληροφοριακά συστήματα δεν είναι απλώς οι ηλεκτρονικοί υπολογιστές. Συνήθως, το πληροφοριακό σύστημα περιλαμβάνει και την επιχείρηση ή σημαντικά μέρη της, όπως τους εργαζομένους που εισάγουν δεδομένα στο σύστημα και παίρνουν πίσω την εκροή του. Τα στελέχη επιχειρήσεων είναι (ή θα έπρεπε να είναι) μέρος του πληροφοριακού συστήματος, αφού το πληροφοριακό σύστημα είναι σχεδιασμένο για να υπηρετεί τις ειδικές ανάγκες τους για πληροφορίες.

2.4 Τύποι πληροφοριακών συστημάτων

Τα πληροφοριακά συστήματα αποτελούν σημαντικό θέμα για μια εταιρία αφού συμβάλλουν στο να καθορίσει τη θέση της στην αγορά και να αναζητήσει αποτελεσματικά συστήματα διαχείρισης πληροφορίας και γνώσης σχετικά με τις διαδικασίες μάρκετινγκ και μάνατζμεντ (Βεργίνης, κ.α 2000).

Ένα μέρος των πληροφοριακών συστημάτων αναφέρεται στην ανάπτυξη του ηλεκτρονικού εμπορίου εξελίχθηκε σημαντικά τα τελευταία χρόνια, με την ισχυρή παρουσία του Internet.

Οι υπολογιστές και τα δίκτυα επικοινωνίας αποτελούν σπουδαίο εργαλείο για τις επιχειρήσεις (Avison, Fitzgerald, 1995). Σήμερα, η πληροφορία και οι τεχνολογίες επικοινωνίας (information and communication technologies – ICT) δεν είναι απλά μηχανισμός υποστήριξης, αλλά θεωρούνται κύριος μοχλός δράσης για τις σύγχρονες επιχειρήσεις. Η δημιουργία ιστοσελίδων (web page) και το ηλεκτρονικό ταχυδρομείο (e-mail) εξελίχθηκαν σημαντικά τα τελευταία χρόνια. Η εξέλιξη του Internet ως επιχειρηματικός μηχανισμός άλλαξε τις συνιστώσες του ηλεκτρονικού εμπορίου (Κιουντούζης 2000).

Το πιο σημαντικό μέσο για την διεξαγωγή Ηλεκτρονικού Εμπορίου είναι η χρήση του Internet τόσο ως μέσο άντλησης πληροφοριών όσο και ως εργαλείο διεξαγωγής των εμπορικών δραστηριοτήτων με τους πελάτες, τους εταίρους αλλά και με το κράτος (Αναστασιάδης, 1998).

Είναι γνωστό ότι οι εξελίξεις στον τομέα της πληροφορικής είναι ραγδαίες (Αναστασιάδης, 1998).

Το Internet, αποτελείται από ένα σύνολο δικτύων δηλαδή από έναν

αριθμό κόμβων που βρίσκονται σε όλα τα πλάτη και τα μήκη του κόσμου και είναι συνδεδεμένοι μεταξύ τους.

Ο κάθε κόμβος είναι δυνατόν να παρέχει πληροφορίες, το Internet ενεργεί κυρίως ως ανεξάντλητη πηγή πληροφοριών παγκοσμίως (Βασιλείου, 1999).

Σε κάθε τύπο συστήματος οι κύριες λειτουργίες είναι οι παρακάτω (Μάλλας 2007):

1. Εισαγωγή δεδομένων στο σύστημα
2. Επεξεργασία των δεδομένων
3. Διατήρηση Αρχείων
4. Ανάπτυξη Διαδικασιών
5. Εξαγωγή Πληροφοριών από το σύστημα

Η διαφορά τους φαίνεται στο ότι στα χειρογραφικά συστήματα βασικό ρόλο παίζει ο άνθρωπος μιας και από αυτόν υλοποιούνται όλες οι λειτουργίες.

Συγκεκριμένα, λαμβάνει τα διάφορα δεδομένα μέσω της όρασης και της ακοής του τα αποθηκεύει στο μυαλό του ή σε άλλα βοηθητικά μέσα.

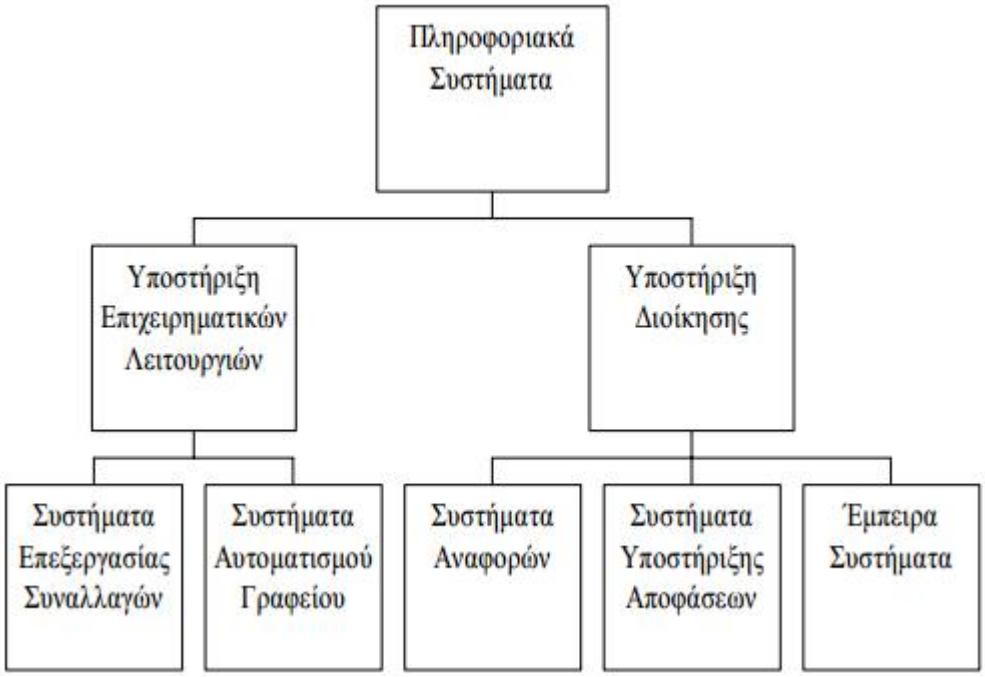
Αναπτύχθηκαν ποικίλα είδη συστημάτων:

- Τα συστήματα λειτουργικού επιπέδου
- Τα συστήματα επιπέδου γνώσης
- Τα συστήματα διοικητικού επιπέδου
- Τα συστήματα στρατηγικού επιπέδου

Στον εκάστοτε οργανισμό εμφανίζονται τύποι πληροφοριών που αναλογούν σε κάθε οργανωτικό επίπεδο. Ο κάθε οργανισμός έχει συστήματα υποστήριξης διοίκησης (ESS) στο στρατηγικό επίπεδο, συστήματα πληροφοριών διοίκησης (MIS) και συστήματα υποστήριξης αποφάσεων (DSS) στο διοικητικό επίπεδο, συστήματα γνώσης (KWS) και συστήματα γραφείου στο επίπεδο γνώσης και συστήματα επεξεργασίας συναλλαγών (TPS) στο λειτουργικό επίπεδο.

Η επιλογή του ιδανικού πληροφοριακού συστήματος είναι πάρα πολύ σημαντική με κριτήρια επιλογής τα παρακάτω (Μάλλας 2007).

1. Προσήλωση στις απαιτήσεις των χρηστών
2. Ευκολία χρήση/ Ευχρηστία
3. Όγκος δεδομένων και φόρτος Εργασιών
4. Απόδοση
5. Ασφάλεια και Έλεγχος
6. Ανάκτηση δεδομένων
7. Διαδικασίες και τεκμηρίωση
8. Πολλαπλές τοποθετήσεις
9. Συμβίωση με άλλα συστήματα



Σχήμα 2-2. Τύποι Π.Σ. ανάλογα με το είδος της υποστήριξης που παρέχουν

Πηγή: Δρανίδης, Δ. και Κεχρής Ε. (2012). Πληροφοριακά Συστήματα. ΤΕΙ Θεσσαλονίκης, σελ 39.

Οι κύριες κατηγορίες είναι Π.Σ. που βασίζονται σε (Δρανίδης & Κεχρής,

2012):

1. Κύριους υπολογιστές
2. Προσωπικούς υπολογιστές
3. Κατανεμημένα συστήματα

2.5 Ιστορική εξέλιξη των πληροφοριακών συστημάτων

Τα πρώτα συστήματα που τοποθετήθηκαν την δεκαετία του 70, χαρακτηρίζονταν από αρχιτεκτονική κεντρική, που αποτελούνταν από ένα κεντρικό υπολογιστή και περιφερειακά συνδεδεμένα σε αστέρα. Σε αρχιτεκτονικές τέτοιου τύπου ένας κεντρικός υπολογιστής διαχειρίζεται όλη την πληροφορία και τα τερματικά και οι εκτυπωτές που χρησιμοποιούνται για την ανταλλαγή πληροφορίας (Anderson & Jacobsen, 1999).

Τα κατανεμημένα δίκτυα παρέχουν απευθείας υποστήριξη σε αποκεντρωμένες μονάδες. Τα τοπικά δίκτυα κάνουν χρήση της δικιάς τους δυνατότητας επεξεργασίας ενώ παράλληλα τους δίνεται η δυνατότητα πρόσβασης σε πληροφορίες που προέρχονται και αφορούν το σύνολο του οργανισμού. Με αυτή την αρχιτεκτονική μεγιστοποιείται η χρήση δικτυακών πόρων, υπηρεσιών και βάσεων δεδομένων. Ένα από τα βασικά τους πλεονεκτήματα είναι ότι υπάρχει η δυνατότητα ενσωμάτωσης νέων εφαρμογών που μπορεί να προέρχονται από διαφορετικές πηγές (Anderson & Jacobsen, 1999).

Έτσι εξασφαλίζεται η συνεχής εξέλιξη και ανάπτυξη του συνολικού πληροφοριακού δικτύου (Anderson & Jacobsen, 1999).

Σαν απάντηση στην τεχνολογική διασύνδεση των κατανεμημένων συστημάτων προτείνονται στοιχεία ενδιάμεσου επιπέδου (middleware) (Βεργίνης κ.α, 2000).

Το CEN ENV 12967–1 (HISA) είναι ένα πρότυπο που προωθείται από την Ευρωπαϊκή Επιτροπή Προτυποποίησης (CEN), που αγκαλιάζει την ιδέα αυτή του ενδιάμεσου επιπέδου. Το πληροφοριακό μοντέλο που προτείνεται αποτελείται από τρία επίπεδα που συνεργάζονται μεταξύ τους: τις εφαρμογές, το ενδιάμεσο επίπεδο και τα bitways.

Στόχος είναι να εξασφαλίζεται η επικοινωνία μεταξύ όλων αυτών των διαφορετικών τμημάτων ανεξάρτητα από τον κατασκευαστή ή την τεχνολογία κατασκευής του κάθε υποσυστήματος. Από το 2003 ιδρύθηκε και λειτουργεί στην Ελλάδα, το ελληνικό τμήμα του οργανισμού HL7. Πέρα από την προώθηση της χρήσης και αποδοχής των προτύπων HL7 στην Ελλάδα, το τμήμα αυτό είναι επιφορτισμένο με την τεχνική προσαρμογή των προτύπων του HL7 στις απαιτήσεις του ελληνικού χώρου. Απώτερος στόχος είναι η δημιουργία Εθνικών οδηγών υλοποίησης προκειμένου να τεθούν οι βάσεις για την μείωση των λαθών και την αποτελεσματικότερη παροχή υπηρεσιών υγείας, ενώ ταυτόχρονα να βελτιωθεί η ανταγωνιστικότητα των εταιριών που δραστηριοποιούνται στο χώρο της ιατρικής πληροφορικής στην Ελλάδα (Βεργίνης κ.α, 2000).

2.6 Διακρίσεις των πληροφοριακών συστημάτων

Τα πληροφοριακά συστήματα διακρίνονται στα εξής βασικά είδη :

Α) Συστήματα Επεξεργασίας Δοσοληψιών (Transaction Processing Systems – T.P.S)

Μια δοσοληψία είναι ένα συμβάν που επηρεάζει την επιχείρηση. Η πρόσληψη ενός εργαζομένου, η πώληση εμπορεύματος, η πληρωμή ενός εργαζομένου και η παραγγελία προμηθειών είναι δοσοληψίες. Στην ουσία, τα συστήματα επεξεργασίας δοσοληψιών συλλέγουν και διατηρούν λεπτομερειακά αρχεία για τις δοσοληψίες της επιχείρησης. Στις επιχειρήσεις η συλλογή και η διατήρηση αρχείων για τις καθημερινές δοσοληψίες ήταν δύο από τις πρώτες διαδικασίες που άρχισαν να γίνονται μέσω ηλεκτρονικών υπολογιστών. Έτσι, με τα συστήματα επεξεργασίας δοσοληψιών αυτοματοποιήθηκαν οι διαδικασίες εκείνες που επαναλαμβάνονται. Ως παραδείγματα μπορεί να αναφερθούν η χρήση των Η/Υ για τους παρακρατούμενους φόρους (Φ.Π.Α., Ο.Γ.Α., κ.ά.), για την επεξεργασία επιταγών πληρωτέων λογαριασμών, κ.ά. Τα συστήματα επεξεργασίας δοσοληψιών μπορεί να έχουν πέντε χρήσεις. Έτσι αυτά χρησιμοποιούνται (Reichheld & Schefter, 2000):

1. Για την ταξινόμηση δεδομένων που βασίζονται στα κοινά χαρακτηριστικά

μιας ομάδας (όπως, π.χ., να βρουν τους εργαζομένους στο τμήμα πωλήσεων, με πενταετή υπηρεσία).

2. Για υπολογισμούς ρουτίνας (όπως το να περνούν στον Η/Υ τις καθαρές αμοιβές μετά από τους φόρους και τις κρατήσεις για κάθε εργαζόμενο).

3. Για την ταξινόμηση σε ομάδες (για παράδειγμα, συγκέντρωση τιμολογίων κατά ομάδες ανάλογα με τον ταχυδρομικό τομέα, προκειμένου να γίνεται πιο αποδοτικά η διανομή τους).

4. Για συνοπτικούς λογαριασμούς (για παράδειγμα, συνοπτικό λογαριασμό για κάθε προϊστάμενο τμήματος, που δείχνει τις μέσες μισθολογικές δαπάνες του τμήματός του σε σύγκριση με τα άλλα τμήματα).

5. Τέλος, τα συστήματα επεξεργασίας δοσοληψιών μπορεί να χρησιμοποιηθούν για αποθήκευση (για παράδειγμα, αποθήκευση πληροφοριών για τις μισθολογικές καταστάσεις τα τελευταία πέντε χρόνια).

Β. Πληροφοριακά Συστήματα Διοίκησης (Management Information Systems - M.I.S.):

Ένα πληροφοριακό σύστημα διοίκησης στηρίζει τη λήψη αποφάσεων των στελεχών των επιχειρήσεων, παράγοντας πρότυπες, συνοπτικές εκθέσεις σε τακτική βάση. Τα συστήματα αυτά παράγουν εκθέσεις για μακροπρόθεσμους στόχους, σε σύγκριση με τα συστήματα επεξεργασίας δοσοληψιών που ασχολούνται με διαδικασίες ρουτίνας (Kroenke & Hooper, 2011).

Γ. Συστήματα Υποστήριξης Αποφάσεων (Decision Support Systems - D.S.S.):

Τα συστήματα υποστήριξης αποφάσεων βοηθούν τα στελέχη των επιχειρήσεων στη λήψη των αποφάσεων. Τα συστήματα αυτά συνδυάζουν δεδομένα, επεξεργασμένα αναλυτικά πρότυπα και ένα φιλικό για το χρήστη λογισμικό σε ένα ενιαίο ισχυρό σύστημα, που μπορεί να υποστηρίξει ημιδομημένα ή μη δομημένα προβλήματα. Με άλλα λόγια, αυτά τα συστήματα μπορεί να βοηθήσουν τα στελέχη επιχειρήσεων να πάρουν

αποφάσεις για μη δομημένα προβλήματα.

Ένα σύστημα υποστήριξης αποφάσεων (D.S.S.) διαφέρει από ένα πληροφοριακό σύστημα διοίκησης (M.I.S.) σε πολλά σημεία. Ένα σύστημα υποστήριξης αποφάσεων είναι πιο ικανό να αναλύει ποικίλες εναλλακτικές λύσεις, επειδή τα συστήματα υποστήριξης αποφάσεων επιτρέπουν στο χρήστη να περιλαμβάνει διάφορα υποπρογράμματα, τα οποία δείχνουν πώς σχετίζονται μεταξύ τους τα διάφορα συστατικά μέρη των υποπρογραμμάτων αυτών.

Έτσι, τα συστήματα υποστήριξης αποφάσεων ασχολούνται με προβλήματα που δεν είναι προγραμματισμένα, τα οποία όμως χρειάζονται την κριτική παρέμβαση του στελέχους, ενώ τα πληροφοριακά συστήματα διοίκησης ασχολούνται βασικά με προβλήματα που είναι προγραμματισμένα και με αποφάσεις ρουτίνας. Επιπλέον, ένα σύστημα υποστήριξης αποφάσεων δεν στηρίζεται μόνο στις εσωτερικές πληροφορίες από το σύστημα επεξεργασίας δοσοληψιών, όπως στηρίζεται τυπικά το πληροφοριακό σύστημα διοίκησης. Αντίθετα, ένα σύστημα υποστήριξης αποφάσεων είναι έτσι δομημένο προκειμένου να απορροφά στην ανάλυση νέες εξωτερικές πληροφορίες (Baden-Fuller & Pitt, 2006).

Δ. Συστήματα Υποστήριξης της Εκτελεστικής Εξουσίας (Executive Support systems - E.S.S.):

Τα συστήματα υποστήριξης της εκτελεστικής εξουσίας είναι πληροφοριακά συστήματα σχεδιασμένα για να βοηθούν την εκτελεστική εξουσία ανώτερου επιπέδου να αποκτά, να χειρίζεται και να χρησιμοποιεί τις πληροφορίες που χρειάζεται, προκειμένου να διατηρεί τη συνολική αποτελεσματικότητα της επιχείρησης. Αυτά τα συστήματα εστιάζονται συχνά στο να παρέχουν στην ανώτερη διεύθυνση πληροφορίες για τη λήψη στρατηγικών αποφάσεων. Βοηθούν την ανώτερη διεύθυνση να αντιμετωπίζει τις αλλαγές του περιβάλλοντος, λαμβάνοντας υπόψη της τα δυνατά και τα αδύνατα σημεία της επιχείρησης (Davenport, 1998).

Οι εκτελεστικοί μάνατζερ χρησιμοποιούν, επίσης, τα συστήματα υποστήριξης της εκτελεστικής εξουσίας για να ανιχνεύσουν το περιβάλλον

της επιχείρησης. Για παράδειγμα, πολλές πληροφορίες είναι διαθέσιμες σε ηλεκτρονικές τράπεζες δεδομένων, στις οποίες περιλαμβάνονται πληροφορίες για πολλές επιχειρήσεις της χώρας μας. Οι εκτελεστικοί μάνατζερ μπορούν να χρησιμοποιούν ένα τέτοιο σύστημα υποστήριξης της εκτελεστικής εξουσίας για να μπαίνουν σε αυτές τις τράπεζες δεδομένων, προκειμένου να σταχυολογούν δεδομένα σχετικά με την ανταγωνιστικότητα των άλλων επιχειρήσεων του κλάδου τους.

Τέλος, ένα σύστημα υποστήριξης της εκτελεστικής εξουσίας επιτρέπει στους εκτελεστικούς μάνατζερ να έχουν άμεση πρόσβαση στα δεδομένα. Χρησιμοποιώντας τα τερματικά τους και τις τηλεφωνικές γραμμές τους, οι εκτελεστικοί μάνατζερ μπορούν να χρησιμοποιήσουν ένα σύστημα υποστήριξης της εκτελεστικής εξουσίας για να μπαίνουν άμεσα στα αρχεία δεδομένων της εταιρείας, προκειμένου να παίρνουν ειδικές πληροφορίες για τις οποίες μπορεί να ενδιαφέρονται, χωρίς να περιμένουν να τους τις συγκεντρώσουν άλλοι (Gilaninia et al., 2012).

Ε. Έμπειρα Συστήματα (Expert Systems - E.S):

Ένα έμπειρο σύστημα είναι ένα πληροφοριακό σύστημα, στο οποίο τα προγράμματα ηλεκτρονικού υπολογιστή αποθηκεύουν γεγονότα και κανόνες (αποκαλούνται συχνά βάση γνώσεων), προκειμένου να αντιγράφουν τις ικανότητες και τις αποφάσεις ανθρώπων που είναι έμπειροι. Για παράδειγμα, μια πρώιμη εφαρμογή εντόπιζε τα κριτήρια ενός συμβούλου επενδύσεων με βάση τα οποία σύστηνε επενδύσεις σε πελάτες που ήταν σε διάφορες δημογραφικές κατηγορίες και σε ποικίλες κατηγορίες ως προς την τάση ανάληψης κινδύνων. Κατόπιν αυτές οι παρατηρήσεις χρησιμοποιούνταν για να αναπτυχθεί ένα πρόγραμμα ηλεκτρονικού υπολογιστή, το οποίο αναπαρήγαγε τις περισσότερες από τις αποφάσεις επενδύσεων τις οποίες θα είχε κάνει ο (έμπειρος) σύμβουλος επενδύσεων. Τα έμπειρα συστήματα χρησιμοποιούνται σε όλους τους τομείς επιχειρήσεων, από την παραγωγή μέχρι το μάρκετινγκ και το χρηματοοικονομικό τομέα . Ωστόσο όλο και περισσότερο, μια από τις πιο προσβεβλημένες χρήσεις, είναι στο χρηματοοικονομικό τομέα και στις επενδύσεις (Nilson, 1994).

2.7 Ασφάλεια πληροφοριακών συστημάτων και προβλήματα

Η ροή πληροφοριών, που παρέχει το Internet καθώς και το ηλεκτρονικό εμπόριο έχουν ωθήσει μέχρι και τις μικρότερες επιχειρήσεις να επενδύσουν στην χρήση Π.Σ και διαδικτυακών εφαρμογών. Η λειτουργικότητα των οργανισμών αυτών στηρίζεται στην λειτουργία των Π.Σ και η ορθή και ασφαλή λειτουργία τους κρίνεται απολύτως απαραίτητη για την επίτευξη των στόχων τους. Η παραμικρή δυσλειτουργία, διακοπή ή παράνομη διείσδυση στα συστήματα αυτά μεταφράζεται σε κόστος. Σε συστήματα που περιέχουν ευαίσθητα δεδομένα οι επιπτώσεις δεν είναι μόνο οικονομικές αλλά ζωτικής σημασίας (Tipton & Krause, 2012).

Ενώ η χρήση Π.Σ είναι δεδομένη για κάθε οργανισμό η ασφάλεια τους ταυτόχρονα απειλείται. Έρευνες Παραβίασης Δεδομένων (Data Breach Investigations Report, DBIR) που ξεκίνησαν από το 2004, έδειξαν ότι στην πραγματικότητα, το 2011 μπορεί να είναι περήφανη για τα υψηλά ποσοστά απώλειας δεδομένων.

Αποτέλεσμα των παραβιάσεων και των επιθέσεων αυτών κατά των Π.Σ ενός οργανισμού οδηγούν στην ρήξη χαρακτηριστικών, όπως η εμπιστευτικότητα (Spears & Barki, 2010).

Η ασφάλεια των Π.Σ αποτελεί κομβικό σημείο για την σύγχρονη κοινωνία, Ανάμεσα στους τομείς της ασφάλειας Π.Σ συμπεριλαμβάνονται η ψηφιακή εγκληματολογία και η εφαρμοσμένη κρυπτογραφία (Peltier, 2013).

2.7.1 Προϋποθέσεις ασφάλειας ενός Π.Σ.

Η ασφάλεια των Π.Σ είναι πολύ σημαντική καθώς στηρίζεται σε τρεις βασικές ιδέες οι οποίες είναι σημαντικές για την ορθή λειτουργία ενός Π.Σ., και είναι οι εξής (Hamlen et al., 2010):

1. Ακεραιότητα (Integrity): Η ακεραιότητα αναφέρεται στη διατήρηση των δεδομένων ενός ΠΣ σε μια γνωστή κατάσταση δίχως τροποποιήσεις.

2. Διαθεσιμότητα (Availability): Τα δεδομένα και οι υπολογιστικοί πόροι είναι η εξασφάλιση ότι οι υπολογιστές, τα δίκτυα και τα δεδομένα θα είναι στη διάθεση των χρηστών όποτε απαιτείται η χρήση τους.
3. Εμπιστευτικότητα (Confidentiality): σημαίνει ότι ευαίσθητες πληροφορίες δεν θα έπρεπε να ανακοινώνονται σε μη εξουσιοδοτημένα άτομα.

Σχήμα 2-3. Βασικές αρχές ασφάλειας

Πηγή: Hamlen, K., Kantarcioglu, M., Khan, L., & Thuraisingham, B. (2010). Security issues for cloud computing. *International Journal of Information Security and Privacy (IJISP)*, *4*(2), 36-48.

2.7.2 Εμπλεκόμενοι στην ανάπτυξη πολιτικών ασφαλείας

Οι απαιτήσεις ασφάλειας μπορεί να προέρχονται από διαφορετικές πηγές, όπως (Whitman & Mattord, 2011):

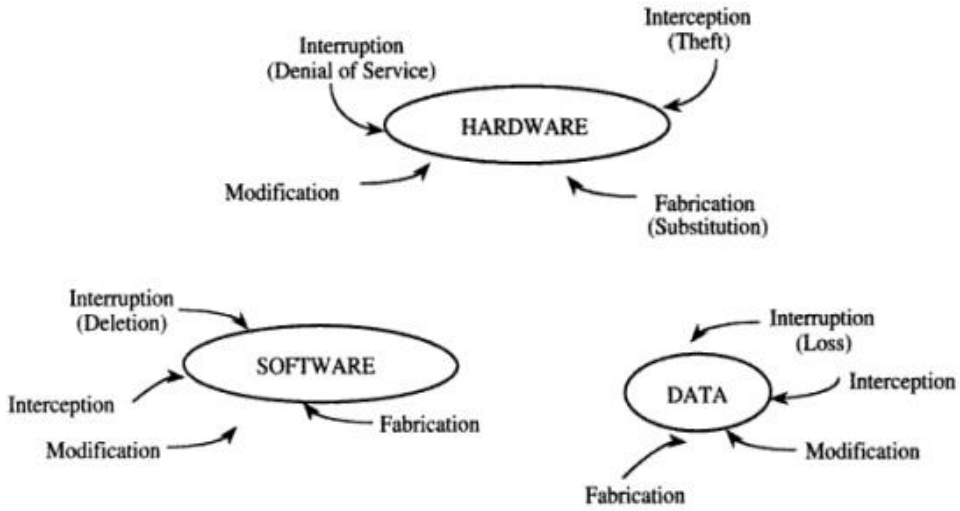
1. Οι χρήστες των ΠΣ.
2. Η διοίκηση του οργανισμού που επιθυμεί την απρόσκοπτη χρήση των ΠΣ στις λειτουργίες του οργανισμού.

3. Οι πελάτες του οργανισμού, είναι και συνιστώσα του πληροφοριακού συστήματος.
4. Το νομικό και ρυθμιστικό πλαίσιο όπου λειτουργεί ο οργανισμός.

2.7.3 Ανάλυση επικινδυνότητας

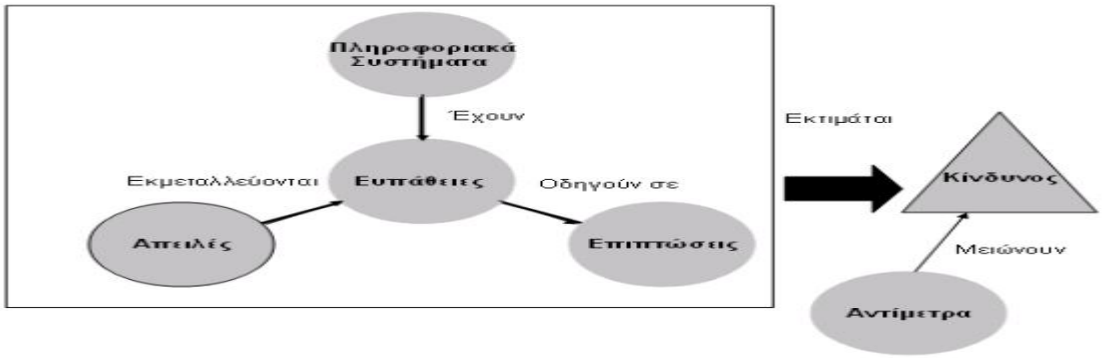
Η πολιτική ασφάλειας για τα ΠΣ μιας επιχείρησης έπεται της αξιολόγησης του επιπέδου ασφάλειας των συστημάτων αυτών. Η αξιολόγηση της ασφάλειας μπορεί να πραγματοποιηθεί με ποικίλους τρόπους, όπως χρήση προτύπων διαχείρισης σχετικά με την ασφάλεια. Στη συνέχεια δίνονται οι ορισμοί που για στην ανάλυση κινδύνων (Spears & Barki, 2010):

1. **Απειλή**: Ένα μη επιθυμητό γεγονός που μπορεί να προξενήσει μη διαθεσιμότητα του συστήματος
2. **Ευπάθεια**: Μια σχεδιαστική ατέλεια σε ένα σύστημα, με δυνατότητα παραβίασης της ασφάλειας του συστήματος.
3. **Κίνδυνος**: Ενδεχόμενο κινδύνου στο να εκμεταλλευτεί μια απειλή μια ευπάθεια.
4. **Αντίμετρο**: Μέτρο που εφαρμόζεται για την προστασία του ΠΣ και την αντιμετώπιση των απειλών.



Σχήμα 2.4. Ευπάθειες ενός πληροφοριακού συστήματος

Πηγή:Spears, J. L., & Barki, H. (2010). User participation in information systems security risk management. *MIS quarterly*, *34*(3), 503-522.



Σχήμα 2.5. Συσχέτισης των παραγόντων της ανάλυσης επικινδυνότητας

Πηγή:Spears, J. L., & Barki, H. (2010). User participation in information systems security risk management. *MIS quarterly*, *34*(3), 503-522.

2.7.4 Μέτρα ασφαλείας

Η πολιτική ασφαλείας αφορά κάθε τεχνική και ενέργεια που περιορίζει τις ευπάθειες του πληροφοριακού συστήματος.(Whitman & Mattord, 2013):

Πρόληψη, Διασφάλιση, ανίχνευση σε τεχνικές, επαναφορά. Για την επιτυχή εφαρμογή της πολιτικής ασφαλείας, το σχέδιο ασφαλείας πρέπει να περιλαμβάνει και συγκεκριμένες διαδικασίες συνεχούς ενημέρωσης με επισκοπήσεις - επιθεωρήσεις της εφαρμογής του, ώστε με τις κατάλληλες αναθεωρήσεις να είναι πάντα up-to-date σε σχέση με τις τεχνολογικές εξελίξεις και τις αλλαγές στην εταιρεία.

Με την πλήρωση του σχεδίου ασφαλείας της επιχείρησης, θα καταρτισθεί αναλυτικό σχέδιο έκτακτης ανάγκης. Η εισαγωγή μηχανισμών ασφαλείας σε ένα ΠΣ αποτελεί περίπλοκο έργο. Για την Ελλάδα η πιο σημαντική δυσκολία οφείλεται στο μαγάλο κόστος της ασφάλειας (Peltier, 2013).

Κεφάλαιο 3ο Ασφάλεια υπολογιστών από επιθέσεις

3.1 Κλασσικοί Ιοί – Ιοι boot sector

Οι συγκεκριμένοι ιοί επηρεάζουν αρνητικά τον τομέα εκκίνησης ενός αποθηκευτικού μέσου ή μιας κατάτμησης (partition). Ο τομέας εκκίνησης περιέχει ένα πρόγραμμα μικρού μεγέθους το οποίο το λογισμικό εντοπίζει και «φορτώνει» στη κύρια μνήμη. Ένας ιός boot sector μπορεί επίσης να μολύνει την περιοχή MBR (Master Boot Record) που περιέχει τον πίνακα κατατμήσεων του δίσκου.

Η διαδικασία της μόλυνσης ξεκινά από τη στιγμή που ο ηλεκτρονικός υπολογιστής επιδιώκει να πραγματοποιήσει εκκίνηση από π.χ. μία μολυσμένη δισκέτα και ο ιός μετακινείται από τη δισκέτα στο σύστημα. Αφού ενεργοποιηθεί, ο ιός μολύνει όλους τους δίσκους καθώς και τις δισκέτες που θα τοποθετηθούν στον οδηγό δισκετών.

Ένας ιός boot sector με καταστροφικές παρενέργειες μπορεί να έχει ως αποτέλεσμα την αδυναμία εκκίνησης ενός συστήματος. Ένα χαρακτηριστικό παράδειγμα αποτελεί ο ιός Michelangelo. Ο συγκεκριμένος ήταν προγραμματισμένος να απενεργοποιήσει τους μολυσμένους Η/Υ στις 6 Μαρτίου 1992 («λογική βόμβα»).

Σε ένα άλλο παράδειγμα, ο Ιός Brain (1986) ήταν ο πρώτος που εμφάνιζε χαρακτηριστικά stealth: Σε περίπτωση που ένα πρόγραμμα antivirus εξέταζε τον τομέα εκκίνησης, ο Brain (ο οποίος ήταν «φορτωμένος» στη μνήμη – memory resident) προωθούσε το αίτημα στον αυθεντικό τομέα εκκίνησης προκειμένου να «ξεγελάσει» το λογισμικό antivirus (Wenbo, 2003).

Οι Κλασσικοί ιοί – Υβριδικοί ή πολυμερείς Ιοί (Multi-partite, ή Hybrid), είναι ιοί που συνδυάζουν χαρακτηριστικά δύο ή περισσότερων κατηγοριών. Κατά το παρελθόν, οι ιοί αυτού του τύπου συνδύαζαν χαρακτηριστικά ιών boot sector και παρασιτικών ιών.

Ένας Η/Υ μολύνεται αν χρησιμοποιήσει μια «μολυσμένη» δισκέτα εκκίνησης ή αν εκτελέσει ένα μολυσμένο πρόγραμμα. Ο ιός αποτελείται από κώδικα που καλύπτει και τις δύο περιπτώσεις: Ανάλογα με την περίσταση,

εκτελείται το αντίστοιχο τμήμα. Το γεγονός αυτό αυξάνει τις πιθανότητες αναπαραγωγής ή/και μόλυνσης.

Για να αφαιρεθεί ο ιός από το σύστημα, θα πρέπει να αφαιρεθούν και τα δύο μέρη του, διαφορετικά το ένα μέρος μπορεί να επανενεργοποιήσει το άλλο. Μελέτη περίπτωσης: ο ιός Melissa (1999) μπορεί να θεωρηθεί ως ιός multipartite (μακρο-ιός & worm).

Όταν το «θύμα» άνοιγε το αρχείο word που λάμβανε μέσω email, ο ιός (ρόλος: μακρο-ιός) ενεργοποιούνταν και μόλυνε το πρότυπο normal.dot της εφαρμογής Word. Αυτό είχε ως συνέπεια να μολύνονται όλα τα έγγραφα .doc που θα δημιουργούσε στο μέλλον ο χρήστης.

Στη συνέχεια ο ιός έστελνε τον εαυτό του (ρόλος: worm) μέσω e-mail στις πρώτες 50 διευθύνσεις από το βιβλίο διευθύνσεων (address book) του χρήστη. Ο ιός είχε ως στόχο μια επίθεση Άρνησης Εξυπηρέτησης (DOS) στους διακομιστές αλληλογραφίας (mail servers). Ο ιός δεν μόλυνε προγράμματα (όπως οι παρασιτικοί ιοί) αλλά μόνον έγγραφα και πρότυπα (templates) (Wenbo, 2003).

Οι κλασσικοί Ιοί – Ιοί Συστήματος Αρχείων (File System), είναι τύπου Link, γνωστοί και ως Cluster, FAT, ή ιοί «file system», δεν συμπεριφέρνονται όπως οι παραδοσιακοί ιοί, δηλαδή δε μολύνουν τον κώδικα εκτελέσιμων ή άλλων αρχείων.

Έχουν τη δυνατότητα να παρεμβάλλονται κατά την κλήση ενός προγράμματος και να εκτελούν τον καταστρεπτικό τους κώδικα. Για να το επιτύχουν αυτό, τροποποιούν τον πίνακα FAT του Η/Υ. Ο πίνακας FAT είναι ένας πίνακας, στο σκληρό δίσκο του Η/Υ, όπου είναι καταχωρημένη η ακριβής θέση (διεύθυνση) του κάθε αρχείου στο δίσκο. Το Λ.Σ. χρησιμοποιεί τον πίνακα FAT για να οργανώσει τα αρχεία στο δίσκο, καθώς και κάθε φορά που γίνεται κλήση ενός αρχείου. Ο ιός αλλάζει τον πίνακα διευθύνσεων ώστε όταν ζητείται η εκτέλεση του «μολυσμένου» προγράμματος **X**, το Λ.Σ. παραπέμπετε στη θέση **Y** όπου βρίσκεται ο κώδικας του ιού, που στη συνέχεια φορτώνεται στη μνήμη και εκτελείται.

Πέρα από τις όποιες άλλες παρενέργειες, από τη θέση αυτή ο ιός έχει τη δυνατότητα να μολύνει όλα τα προγράμματα που θα εκτελεστούν στη

συνέχεια από τον χρήστη. Συνήθως οι ιοί αυτής της κατηγορίας εμφανίζουν χαρακτηριστικά ιών stealth: αφού παρεμβληθούν κατά την εκτέλεση ενός προγράμματος και απελευθερώσουν το φορτίο τους, στη συνέχεια φορτώνουν και εκτελούν το νόμιμο πρόγραμμα που είχε ζητηθεί αρχικά (Μελέτη περίπτωσης: Ο ιός DIR-II) (Wenbo, 2003) .

Οι Ιοί Flash Bios, αναπτύσσονται μέσα από τη διαδικασία που ακολουθούν οι κατασκευαστές μητρικών. Οι κατασκευαστές αποθηκεύουν το πρόγραμμα BIOS σε ένα ολοκληρωμένο μνήμης flash ROM. Η μνήμη αυτή είναι επανεγγράψιμη.

Οι ιοί flash BIOS επανεγγράφουν το λογισμικό BIOS στην μητρική πλακέτα. Το αποτέλεσμα της «μόλυνσης» είναι καταστρεπτικό (π.χ. διαγραφή των περιεχομένων του σκληρού δίσκου).

Ο ιός CIH ή Chernobyl αποτελεί ένα χαρακτηριστικό παράδειγμα ιού που τροποποιούσε τον κώδικα του προγράμματος BIOS. Σε μια από (τις αρκετές) εκδόσεις του ο ιός περιείχε μια «λογική βόμβα»: στις 26 Απριλίου ενεργοποιούνταν το φορτίο και δεν μπορούσε να γίνει εκκίνηση του συστήματος. Σε ορισμένες περιπτώσεις κρίθηκε απαραίτητη η αντικατάσταση του chip ή της μητρικής πλακέτας (motherboard) του συστήματος.

Οι Κλασσικοί Ιοί - Μακρο-Ιοί προσβάλλουν αρχεία δεδομένων που περιέχουν μακροεντολές. Οι μακρο-εντολές είναι κώδικας εντολών, γραμμένος με γλώσσες συγγραφής σεναρίων π.χ. VBA (Visual Basic for Applications) και χρησιμοποιούνται κυρίως σε προγράμματα εφαρμογών γραφείου για την αυτοματοποίηση ορισμένων από τις λειτουργίες που εκτελεί ο χρήστης.

Για παράδειγμα, κάποιος μπορεί να δημιουργήσει μια μακροεντολή στο Word ώστε με το πάτημα ενός πλήκτρου, να εκτελεί ταυτόχρονα τις ακόλουθες λειτουργίες: α) Επιλογή κειμένου, β) μορφοποίηση με γραμματοσειρά Arial, γ) αλλαγή μεγέθους γραμματοσειράς σε 14. Οι μακροεντολές αποθηκεύονται μαζί με το αρχείο δεδομένων στο δίσκο.

Οι μακρο-ιοί λοιπόν είναι μακροεντολές που αυτοματοποιούν ένα σύνολο από καταστροφικές ενέργειες: όταν π.χ. σε έναν επεξεργαστή κειμένου εκτελεστεί η μακροεντολή ενός μολυσμένου εγγράφου, ο ιός

ενεργοποιείται και απελευθερώνει το καταστροφικό του φορτίο.

Η δημοτικότητα των εφαρμογών γραφείου, έχει συνεισφέρει στην εξάπλωση αυτού του είδους των ιών. Επίσης, ο κώδικας που δημιουργείται από μια γλώσσα συγγραφής σεναρίων, μπορεί να εκτελεστεί σε όλες τις πλατφόρμες: ένας μακρο-ιός μπορεί να εκτελεστεί σε ένα PC και σε ένα MAC.

Η διαδικασία της μόλυνσης γίνεται μέσα από τη λήψη και άνοιγμα εγγράφου που περιέχει μακρο-εντολές. Οι περισσότερες μακρο-εντολές ενεργοποιούνται με το άνοιγμα ενός εγγράφου (π.χ. λειτουργία Auto-open). Στις τελευταίες εκδόσεις των εφαρμογών γραφείου, ο χρήστης προειδοποιείται για την ύπαρξη τέτοιων εντολών.

Ο μακρο-ιός συνήθως είναι προγραμματισμένος να μετατρέπει τα μολυσμένα έγγραφα σε πρότυπα προκειμένου να μολυνθούν όλα τα έγγραφα που θα δημιουργήσει μελλοντικά ο χρήστης. Η μετάδοση του γίνεται με αφαιρούμενα αποθηκευτικά μέσα ή μέσω δικτύου (Matyas et al., 2000).

3.2 Στοιχειοθέτηση στις υπάρχουσες μορφές ιομορφικού λογισμικού

Τα όπλα που σχετίζονται με δραστηριότητες των κυβερνοτρομοκρατών δεν σχεδιάστηκαν με στόχο να σκοτώνουν ανθρώπους αλλά να προξενούν ζημιές σε υπολογιστικά συστήματα. Τα συστήματα αυτά υφίστανται προκειμένου να καταστρέφουν ηλεκτρονικά αρχεία. Τα συγκεκριμένα όπλα όπως αποκαλούνται αναπτύσσονται στον κυβερνοχώρο. Ανεξάρτητα αν ο άνθρωπος είναι αυτός που τα δημιούργησε αποτελεί και ο βασικός στόχος των επιθέσεων τους σε σχέση με τα λειτουργικά συστήματα τα οποία χρησιμοποιεί. Ορισμένα από τα όργανα που επιδρούν στα δίκτυα και μέσα από αυτά θα γίνει η στοιχειοθέτηση στις υπάρχουσες μορφές ιομορφικού λογισμικού είναι τα ακόλουθα (Κάτσικα κ.α, 2004):

1. Ιοί: Ένα από τα πιο αποδοτικά μέσα των κυβερνοτρομοκρατών είναι η ανάπτυξη ιών. Οι ιοί είναι προγράμματα που αναπτύσσονται για να υλοποιήσουν τις προθέσεις του δράστη Οι δράσεις αυτές αναφέρονται

στην απώλεια ή μεταβολή των δεδομένων με κάποιο κακόβουλο ή μη μέσο. Ο ιός με τη παρούσα ονομασία παρασιτεί σε ένα άλλο οργανισμό και διαδίδεται χωρίς κάποια δεδομένη δράση. Ένας από τους πιο δυναμικούς ιούς ήταν το 1992, ο ιός Michelangelo, ο οποίος πήρε το όνομα του από το γνωστό ζωγράφο, μια και εμφανίστηκε στις 6 Μαρτίου ημέρας που γεννήθηκε ο καλλιτέχνης.

2. Άλογα Trojan: Ο δεύτερος τύπος είναι τα Άλογα Trojan. Το συγκεκριμένο πρόγραμμα δεν έχει κάποια ουσιαστική καταστροφική δράση, έχει όμως τη δυνατότητα απελευθέρωσης ενός προγράμματος το οποίο έχει τη δυνατότητα να βλάψει εντολές λειτουργικά συστήματα. Το συγκεκριμένο πρόγραμμα χρησιμοποιείται για την εγκατάσταση ενός προγράμματος το οποίο συγκεντρώνει κώδικες εισόδου από νόμιμους χρήστες και τους αρχειοθετεί προκειμένου να τους χρησιμοποιήσει στο εγγύς μέλλον. Το συγκεκριμένο μέσο χρησιμοποιείται για να αποσπάσει πληροφορίες, εισβάλλοντας σε ένα σύστημα έχοντας αναπτύξει ένα ψεύτικο προφίλ.

3. Σκουλήκια: Στη παρούσα κατηγορία εντάσσεται το εξεταζόμενο Stuxnet, το οποίο αποτελεί ένα ιό σκουλήκι. Το συγκεκριμένο αποτελεί πρόγραμμα που αναπτύσσεται για να ταξιδεύει μέσω συστημάτων και να εκτελούν εργασίες όπως διαγραφή εργασιών και συλλογή διαφόρων δεδομένων. Το Stuxnet, μπορεί να έχει καταστροφικά αποτελέσματα μια και εκτείνετε σε όλο το σύστημα που προσβάλει. Ο ιός με την ονομασία Stuxnet, αναπτύχθηκε όντας ως αποστολή του να βλάψει όπως αναφέρθηκε και παραπάνω τους υπολογιστές των ιρακινών εγκαταστάσεων και να αναπροσαρμόσει τα λογισμικά του προκειμένου να επιφέρει την αχρήστευση συγκεκριμένων μηχανικών τμημάτων και συστημάτων (Επίσημη εφημερίδα της Ευρωπαϊκής Ένωσης, 2010). Η διείσδυσή του στα λογισμικά συστήματα που ελέγχουν την πυρηνική εγκατάσταση πραγματοποιήθηκε όχι μέσω διαδικτύου, αλλά μέσω της χρήσης φορητών μνημών τύπου USB. Ο Stuxnet είναι προγραμματισμένος με τέτοιον τρόπο προκειμένου να μην είναι ορατός από τα συστήματα ελέγχου, παρά μόνο, όταν οι μηχανικές βλάβες που θα προκύψουν γίνουν εκ των υστέρων αντιληπτές. Καθ' όλη την

χρονική διάρκεια που πραγματοποιεί τις τροποποιήσεις του λογισμικού των Windows των PC που είναι συνδεδεμένα σε δίκτυα τύπου SCADA WinCC και PCS 7. Η πολυπλοκότητα του ιού πάνω στην σχεδίαση του και την υλοποίηση επίθεσης σε πεδίο εφαρμογής καθώς και για την εξουδετέρωσή του, απαιτεί ένα σύνολο εξειδικευμένων προγραμματιστών με διαφορετικές και ποικίλες επιστημονικές γνώσεις που θα τους επιτρέψουν όχι μόνο να τον θέσουν σε πλήρη λειτουργία, αλλά και από την άλλη πλευρά η κατοχή απαραίτητης τεχνογνωσίας για την αναγκαία εξουδετέρωσή του.

4. Όπλα ηλεκτρομαγνητικών παλμών: Τα συγκεκριμένα είναι υψηλής ποιότητας και μπορούν να καταστρέψουν δίκτυα και συστήματα υπολογιστών μέσω ηλεκτρομαγνητικών παλμών. Τα συγκεκριμένα δύσκολα εντοπίζονται ενώ και δύσκολα μπορούν να αντιμετωπιστούν.

Spy ware – Ad ware: Το συγκεκριμένο Κακόβουλο λογισμικό πλησιάζει τις λειτουργίες ενός Δούρειου Ίππου αναφορικά με τον τρόπο μόλυνσης με σκοπό την παρακολούθηση - υποκλοπή ευαίσθητων δεδομένων, ή την αποστολή ανεπιθύμητων διαφημιστικών μηνυμάτων αναφερόμενα ως μέλη της ίδιας κατηγορίας, καθώς συνήθως συνεργάζονται για να πετύχουν τον σκοπό τους (Ross, 2001).

Rootkits: Το συγκεκριμένο αποτελεί ένα κακόβουλο λογισμικό το οποίο λειτουργεί σε πολύ χαμηλό επίπεδο, και συνήθως ενσωματώνει λειτουργίες απόκρυψης - stealth προκειμένου να παρακάμπτει τους μηχανισμούς πρόληψης και ανίχνευσης, όπως firewalls και antivirus. Μπορεί να ανήκει σε οποιαδήποτε από τις ως άνω κατηγορίες, ωστόσο συνήθως ανοίγει κερκόπορτες που θα επιτρέψουν τη μετέπειτα απομακρυσμένη διαχείριση του ξενιστή από κάποιον τρίτο (Schneier, 2003).

Bots – zombies: Ο συγκεκριμένο ιός προσβάλλει ηλεκτρονικούς υπολογιστές καθιστώντας τους μέλη ενός δικτύου Η/Υ που ελέγχεται από μακριά από τρίτους, με σκοπό επιθέσεων κατά τις οποίες ένας αριθμός μολυσμένων υπολογιστών προσπαθεί να συνδεθεί στον Η/Υ-στόχο μέσω δικτύου. Ο όρος «bot», χρησιμοποιείται για να περιγράψει κάθε είδους αυτοματοποιημένη διαδικασία. Ένας Η/Υ που έχει μολυνθεί από ένα bot

συχνά αναφέρεται ως «zombie». Οι Η/Υ – zombies μπορεί να χρησιμοποιηθούν για επιθέσεις DOS σε εξυπηρετητές Web, για την αποστολή μηνυμάτων spam, για την πραγματοποίηση επιθέσεων παραπλάνησης (Cohen, 2005).

Σε σχέση με το Stuxnet η διαδικασία μόλυνσης είναι η ακόλουθη (Schneier, 2003):

1. Μέσω Ηλεκτρονικής Αλληλογραφίας. Το κακόβουλο λογισμικό βρίσκεται συνημμένο σε ένα μήνυμα ηλεκτρονικής αλληλογραφίας. Η αποστολή του μηνύματος μπορεί να είναι είτε ηθελημένη από κάποιον τρίτο, είτε ως αποτέλεσμα αυτόματης μετάδοσης.
2. Μέσω αφαιρούμενων αποθηκευτικών μέσων. Ο τρόπος αυτός μόλυνσης ήταν και είναι ο πλέον δημοφιλής στην κατηγορία των κλασσικών ιών.
3. Μέσω Web μέσω δηλαδή ενός εκτελέσιμου κώδικας ενσωματωμένος σε σελίδες html).
4. Μέσω άλλων υπηρεσιών διαδικτυακής επικοινωνίας. Υπηρεσίες συνομιλίας σε πραγματικό χρόνο υπηρεσίες Ομάδων Συζήτησης (newsgroups), προγράμματα ανταλλαγής αρχείων (Peer to Peer) κ.λ.π
5. Μέσω Δικτύων (LAN, WAN). Το κακόβουλο λογισμικό (π.χ. τύπου Worm) εκμεταλλεύεται ευπάθειες δικτυακών πρωτοκόλλων, υπηρεσιών, εφαρμογών και δικτυακών λειτουργικών συστημάτων προκειμένου να μεταδίδεται αυτόματα μέσω τοπικών δικτύων ή Δικτύων Ευρείας Περιοχής που εκτελούν την οικογένεια πρωτοκόλλων TCP/IP.

Επίσης, η κοινή χρήση αρχείων, εγγράφων και φακέλων σε τοπικά δίκτυα, διευκολύνει την εξάπλωση του κακόβουλου λογισμικού. Σε ένα παρεμφερές σενάριο, το κακόβουλο λογισμικό αντιγράφει τον εαυτό του στους φακέλους με τα διαμοιραζόμενα αρχεία που χρησιμοποιούν οι εφαρμογές ανταλλαγής αρχείων.

Οι παρενέργειες του φορτίου ενός κακόβουλου λογισμικού ποικίλλουν και αναφέρονται στα ακόλουθα (Matyas et al., 2000; Cohen, 1987):

1. Ενοχλητικά μηνύματα, διαφημίσεις κ.λ.π .
2. Επιθέσεις υποκλοπής δεδομένων και πληροφοριών, ή κλήσης (dialers) με υπεραστική χρέωση (σχετική κατηγορία: Trojans, spy ware)
3. Επιθέσεις Διακοπής, Αλλοίωσης, Εισαγωγής - Διαγραφή ή αλλοίωση δεδομένων, εφαρμογών και αρχείων συστήματος - Αντιγραφή αρχείων στο τοπικό δίκτυο ή στο Internet.
4. Αναστολή λειτουργίας ή δυσλειτουργία του Ηλεκτρονικού Υπολογιστή.
5. Καταστροφή των τομέων εκκίνησης (boot sectors), πινάκων καταχώρησης αρχείων (FAT), και πινάκων κατατμήσεων (partition tables).
6. Δημιουργία «κερκόπορτας» (back door) με σκοπό την (μετέπειτα) παραβίαση της ασφάλειας του συστήματος.
7. Επιθέσεις εναντίον της διαθεσιμότητας συστημάτων (σχετικές κατηγορίες: worms, bots- zombies)
8. Κατανάλωση υπολογιστικών πόρων (κύρια μνήμη, αποθηκευτικός χώρος)
9. Κατανάλωση της χωρητικότητας (bandwidth) του δικτύου
10. Χρήση των ξενιστών για συγχρονισμένη επίθεση σε κάποιον τρίτο, στα πλαίσια μιας επίθεσης DDOS (Distributed DOS).

3.2.1 Παράδειγμα Ιομορφικού Λογισμικού-Stuxnet

Το stuxnet αποτελεί ένας ιός ο οποίος ανακαλύφθηκε και χρησιμοποιήθηκε για πρώτη φορά τον Ιούνιο του 2010 και πιστεύεται ότι πρώτοι το χρησιμοποίησαν οι Ηνωμένες Πολιτείες της Αμερικής σε συνεργασία με το Ισραήλ προκειμένου να επιτεθούν στα πυρηνικά όπλα τα οποία διέθετε το Ιράν (Legal Experts 2013). Το stuxnet, αρχικά υποστηρίχτηκε από τα Microsoft Windows και στόχευσε το βιομηχανικό λογισμό της Siemens. Δεν ήταν η πρώτη φορά στην ιστορία που οι hackers εστίασαν στην καταστροφή βιομηχανικών συστημάτων, ήταν όμως η πρώτη φορά που

ανακαλύφθηκε ένας ιός ο οποίος κατασκόπευε και κατάστρεφε διάφορα βιομηχανικά συστήματα και το πρώτο το οποίο συμπεριλάμβανε programmable logic controller (McMillan 2010).

Το συγκεκριμένο πρόγραμμα όντας αρκετά εξειδικευμένο, εμπεριέχει μια υψηλής τεχνολογίας δυναμική η οποία αρχικά σχεδιάστηκε για να χτυπήσει τη Siemens, στην πορεία όμως ανέκυψαν πολλές χρήσεις προκειμένου να ελεγχθούν και να καταγραφούν συγκεκριμένες βιομηχανικές διαδικασίες. Το Stuxnet επηρεάζει τους υπολογιστές δημιουργώντας πρόβλημα στο 7 βήμα της φόρτωσης μιας εφαρμογής και πρέπει να επανα-προγραμματιστεί (http://www.symantec.com). Για παράδειγμα πέντε διαφορετικά είδη ιών του Stuxnet στόχευσαν 5 Ιρακινούς οργανισμούς (Fredrik and Westall, 2010) . Μέσα στον Αύγουστο του 2010, το Stuxnet ήταν υπεύθυνο για το 60% των κατεστραμμένων υπολογιστών σε παγκόσμια κλίμακα και ειδικά στο Ιράν και τη Siemens, η επίδραση ήταν καταλυτική.

3.3 Τεχνικές αντιμετώπισης

Για να προστατευτεί το λογισμικό ενός υπολογιστή έχουν αναπτυχθεί τα προγράμματα Antivirus τα οποία από τη μία εντοπίζουν τον ιό και από την άλλη τον καταστρέφουν.

Κάνουν έλεγχο συνεχώς στον υπολογιστή σε αρχεία δεδομένων, αρχεία συστήματος, ή αρχεία εφαρμογών ενώ, μπορεί να είναι αποθηκευμένα σε κάποια μονάδα βοηθητικής μνήμης ή να εισέρχονται στο σύστημα μέσω δικτύου (LAN, Internet).

Ο κώδικας κάθε ιού έχει ορισμένα χαρακτηριστικά που τον διαφοροποιούν από τους υπόλοιπους ιούς. Το τμήμα εκείνο του κώδικα ενός ιού που χαρακτηρίζει μοναδικά τον ιό ονομάζεται υπογραφή ή αποτύπωμα του ιού.

Ένα πρόγραμμα για ιούς έχει μια Βάση Δεδομένων με τις υπογραφές όλων των γνωστών ιών, και ελέγχει όλα τα εκτελέσιμα αρχεία ενός Η/Υ (κατά την αποθήκευση ή εκτέλεση τους) για τον εντοπισμό μιας υπογραφής που έχει ήδη αποθηκευτεί στη Β.Δ. Εφόσον βρει κάποιο «ταίριασμα», το πρόγραμμα

antivirus μπλοκάρει την εκτέλεση του κακόβουλου προγράμματος και ενημερώνει το χρήστη. Συνήθως προτρέπει το χρήστη να αποφασίσει αν επιθυμεί:

1. διαγραφή.
2. απομόνωση.
3. επιδιόρθωση του μολυσμένου αρχείου.

Το πρόγραμμα antivirus μπορεί να εντοπίσει και να αποκρίνει ιούς που είναι ήδη γνωστοί. Αυτό σημαίνει πως δεν προσφέρει προστασία έναντι ιών που δεν έχουν ανιχνευθεί ακόμα (τουλάχιστον, μέχρι να γίνει η ενημέρωση - λήψη της υπογραφής τους από τον διακομιστή Web).

Επιπλέον, τα προγράμματα antivirus παραδοσιακά δυσκολεύονται στην καταπολέμηση πολυμορφικών ιών καθώς και ιών τύπου stealth/rootkits. Για το λόγο αυτό τα προγράμματα antivirus συχνά επιστρατεύουν προηγμένες τεχνικές όπως heuristic scanning, behavior blocking και integrity checking.

Οι μέθοδοι αυτές εντοπίζουν κώδικα που μπορεί να μη βρίσκεται στη ΒΔ αλλά συγκεντρώνει αρκετές πιθανότητες να είναι κακόβουλος. Αυτό έχει ως αποτέλεσμα η διάγνωση να μην είναι πάντα επιτυχημένη (π.χ. λάθος συναγερμός). Οι Βασικές (Ελάχιστες) Δυνατότητες που έχει μια εφαρμογή Antivirus είναι οι ακόλουθες (Κοτζανικολάου, 2005):

1. Εύχρηστο Interface -Χαμηλή κατανάλωση πόρων: Το περιβάλλον της εφαρμογής πρέπει να είναι λιτό, και φιλικό προς τον χρήστη. Πολλά παράθυρα, πολύπλοκες ρυθμίσεις και παράμετροι μπορούν να έχουν εντελώς αντίθετα αποτελέσματα και να θέσουν σε ρίσκο την ασφάλεια του συστήματος. Επίσης, ένα πρόγραμμα antivirus θα πρέπει να προσφέρει τις υπηρεσίες του δεσμεύοντας μικρό μόνο ποσοστό από τους πόρους του υπολογιστή (μνήμη και υπολογιστική δύναμη).
2. Προστασία σε πραγματικό χρόνο: Τα προγράμματα antivirus συνήθως διαθέτουν ένα υποσύστημα διάγνωσης και προστασίας σε πραγματικό χρόνο. Το antivirus φορτώνεται στην κεντρική μνήμη κατά την εκκίνηση του Η/Υ και λειτουργεί στο παρασκήνιο, ελέγχοντας τη μνήμη του συστήματος, καθώς και τα αρχεία και τις εφαρμογές που

εκτελούνται ή εισέρχονται στο σύστημα για την ύπαρξη κακόβουλου λογισμικού.

3. Αυτόματη ενημέρωση: Σε αντίθεση με το παρελθόν, όπου τη διαδικασία ενημέρωσης την εκκινούσε ο χρήστης χειρωνακτικά, σήμερα τα προγράμματα antivirus ενημερώνουν αυτόματα τη βάση δεδομένων τους με τις πρόσφατες υπογραφές των ιών. Η ενημέρωση θα πρέπει να είναι τακτική (ο αποδεκτός σήμερα ρυθμός ενημέρωσης είναι της τάξης των λίγων ημερών), με δεδομένο ότι καθημερινά εμφανίζονται καινούριοι ιοί.

4. Προστασία Ηλεκτρονικής Αλληλογραφίας: Το πρόγραμμα για ιούς ελέγχει τα εισερχόμενα και εξερχόμενα μηνύματα ηλεκτρονικής αλληλογραφίας για την ύπαρξη ιών (στα συνημμένα έγγραφα). Για να συμβεί αυτό το πρόγραμμα θα πρέπει να συνεργάζεται με τα πλέον δημοφιλή προγράμματα ηλεκτρονικής αλληλογραφίας.

5. Προγραμματισμένος Έλεγχος: Το antivirus επιτρέπει τον καθορισμό (scheduling) προγραμματισμένων ελέγχων στους δίσκους του συστήματος, σε συγκεκριμένη ημερομηνία ή ανά τακτά χρονικά διαστήματα.

6. Δισκέτα Εκκίνησης: Για την αντιμετώπιση των ιών τύπου boot sector, ή για την αντιμετώπιση περιπτώσεων όπου η εκκίνηση του Λ.Σ. είναι αδύνατη, συνήθως τα προγράμματα antivirus προσφέρουν τη δυνατότητα δημιουργίας μιας δισκέτας εκκίνησης. Η δισκέτα αυτή ενσωματώνει εφαρμογές διάγνωσης και καθαρισμού του boot sector ή/και (κρίσιμων) αρχείων συστήματος, σε περίπτωση που αυτά έχουν επικαλυφθεί (overwrite) από κακόβουλο λογισμικό.

7. Ευρετικές (heuristic) μέθοδοι: Έλεγχος κώδικα για εύρεση πιθανό Ιού. Σε αντίθεση με τους αλγόριθμους ελέγχου της υπογραφής ενός ιού, η ευρετική μέθοδος εξετάζει τον εκτελέσιμο κώδικα ενός αρχείου με σκοπό την εύρεση εντολών (ή συνόλου από εντολές) που θα μπορούσαν να αποτελούν τμήμα κακόβουλου κώδικα, με μεγάλη πιθανότητα. Παραδείγματα αποτελούν η ύπαρξη μακροεντολών σε ένα έγγραφο Office, εντολές κλήσης-τροποποίησης προγραμμάτων,

ρουτίνες αποκρυπτογράφησης, εντολές διαγραφής αρχείων ή τροποποίησης του μητρώου του συστήματος, κ.λ.π. Η τεχνική αυτή είναι προενεργή, δηλαδή προσπαθεί να εντοπίσει «ύποπτο» τμήμα κώδικα πριν αυτός εκτελεστεί.

8. Έλεγχος Ακεραιότητας: Κατά την αποθήκευση ενός αρχείου, υπολογίζονται και αποθηκεύονται το μέγεθος του αρχείου, καθώς και ένα άθροισμα ελέγχου Το άθροισμα ελέγχου είναι ένας αριθμός μοναδικός για το αρχείο αυτό: Η αλλαγή έστω και ενός bit στο αρχείο θα έχει ως αποτέλεσμα την αλλαγή του αθροίσματος ελέγχου με μεγάλη πιθανότητα. Για μεγαλύτερη ασφάλεια, μπορεί να χρησιμοποιηθεί η κρυπτογραφική τιμή hash του κώδικα του προγράμματος. Κάθε φορά που εκτελείται ένα αρχείο, το antivirus υπολογίζει το άθροισμα ελέγχου και το συγκρίνει την αποθηκευμένη τιμή.
9. Έλεγχος Συμπεριφοράς: Η τεχνική αυτή μοιάζει με την τεχνική εκτέλεσης σε «προστατευμένο περιβάλλον» που χρησιμοποιείται κατά την εκτέλεση των προγραμμάτων Java. Δεν ελέγχεται ο κώδικας του εκτελέσιμου αρχείου καθ' αυτός, ωστόσο ελέγχεται η συμπεριφορά του προγράμματος καθώς εκτελείται. Έχοντας δηλαδή υπόψη ένα σύνολο από συμπεριφορές που θεωρούνται «ύποπτες - επικίνδυνες» το πρόγραμμα antivirus προσπαθεί να ανιχνεύσει και να αποτρέψει σε πραγματικό χρόνο τις παρενέργειες ενός (άγνωστου) ιού. Αν ανιχνευτεί «ύποπτη» συμπεριφορά, το πρόγραμμα εφαρμόζει την πολιτική ασφαλείας (την οποία διαμορφώνει ο χρήστης μέσα από τις επιλογές-ρυθμίσεις του προγράμματος) (Schneier, 2006). Η τεχνική αυτή είναι «αντιδραστική» δηλαδή το πρόγραμμα antivirus προσπαθεί να εντοπίσει «ύποπτο» κώδικα αφού αυτός εκτελεστεί.

Τα προγράμματα ενσωματώνουν ορισμένες επιπλέον λειτουργίες προστασίας, προσφέρουν τη δυνατότητα ελέγχου αλληλογραφίας (εισερχόμενης/εξερχόμενης) για κακόβουλο λογισμικό, έλεγχο και παρεμπόδιση «υπόπτων» αρχείων που ανταλλάσσονται μέσω προγραμμάτων ανταλλαγής αρχείων P2P, φιλτράρισμα αρχείων που ανταλλάσσονται μέσω προγραμμάτων συνομιλίας (chat, ανταλλαγή μηνυμάτων – instant messaging),

προστασία από κινητό κώδικα στο Web, κ.λπ. Επιπλέον, αρκετά προγράμματα antivirus συχνά αποτελούν ολοκληρωμένα πακέτα εφαρμογών και ενσωματώνουν λειτουργίες firewall, ανίχνευσης εισβολών, καθώς και προστασίας από (μη μολυσματικό) λογισμικό τύπου spyware-adware (Schneier, 2006).

3.3.1.Ασφάλεια των δικτυών των τραπεζών

Οι εισβολείς έχουν αρκετούς τρόπους να επιτύχουν τους σκοπούς τους. Τα κλεμμένα στοιχεία είναι η πρώτη φάση που τους απασχολεί να επιτύχουν και αυτό γίνεται παριστάνοντας μέσω διαδικτύου μια ξένη ταυτότητα.

Άλλος τρόπος είναι να απευθυνθούν σε μια από τις εταιρείες που συνεργάζονται με τη τράπεζα και όχι ευθέως με αυτήν ώστε να διαχειριστούν τις πληρωμές των λογαριασμών και τις συναλλαγές με τους πελάτες της.

Ένας άλλος τρόπος είναι να χτυπήσουν τις μικρές, τοπικές τράπεζες οι οποίες μπήκαν πρόσφατα στο τομέα του e-banking και παρουσιάζουν πολλά κενά στην ασφάλεια τους.

Το πλαστικό χρήμα – δηλαδή οι συναλλαγές με τις πιστωτικές κάρτες – αναπτύχθηκε στις Η.Π.Α. επειδή οι Αμερικανοί αντιμετώπιζαν πρόβλημα στην εξαργύρωση των επιταγών τους από την μία τράπεζα στην άλλη, και από την μία πολιτεία στην άλλη γεγονός που τους ανάγκαζε να μεταφέρουν μετρητά μαζί τους και αυτό εγκυμονούσε πολλούς κίνδυνους. Έτσι σε μία προσπάθεια να λυθεί το πρόβλημα τους, δημιούργησαν τις πιστωτικές κάρτες. Με αυτόν τον τρόπο, ο κάτοχος της κάρτας δεν χρειαζόταν να μεταφέρει μετρητά μαζί του, αλλά παρουσίαζε την κάρτα του και απολάμβανε την τραπεζική εξυπηρέτηση

Το ίδιο πρόβλημα, όμως, παρουσιαζόταν και στα ταξίδια προς την Ευρώπη μια και δεν υπήρχε τρόπος, η τράπεζα στην Ευρώπη να παίρνει τα χρήματα της από την Αμερική. Έτσι, δημιουργήθηκε ένας διεθνής οργανισμός που αγοράζοντας τα δικαιώματα από την Bank of America έγινε πλέον αυτός υπεύθυνος για την έκδοση των καρτών. Από τότε όλες οι τράπεζες που εκδίδουν κάρτες πρέπει να είναι μέλη αυτού

του οργανισμού. Το όνομα του, VISA προέρχεται από την VISA που χρησιμοποιείται από ορισμένες χώρες στα διαβατήρια. Το κύκλωμα των πιστωτικών καρτών αποτελείται από τρία μέρη (Cisco Systems, 2000):

1) Ο κάτοχος, δηλαδή αυτός που χρησιμοποιεί την κάρτα για τις διάφορες συναλλαγές του.

2) Η τράπεζα, που πιστώνει τον κάτοχο με τα ποσά των συναλλαγών που πρέπει να αναπληρωθούν.

Ο έμπορος, που είναι αυτός που προμηθεύει τα αγαθά στον κάτοχο της κάρτας και πληρώνει κάποια προμήθεια στην τράπεζα ανάλογα με το είδος των αγαθών που διακινούνται με την πιστωτική κάρτα.

Πιστωτικές κάρτες είναι οι κάρτες που παρέχουν στον κάτοχο τους την πιστωτική δύναμη μέχρι ενός ορίου. Το ποσό των συναλλαγών που γίνονται από τον κάτοχο μίας τέτοιας κάρτας θα πρέπει να αναπληρωθεί στην τράπεζα που την εκδίδει είτε ολόκληρο μέσα σε διάστημα 30 ως 45 ημερών, είτε σε έντοκες μηνιαίες δόσεις και εδώ βρίσκεται το κύριο πλεονέκτημα των πιστωτικών καρτών.

Η έκδοση τέτοιων καρτών δεν προϋποθέτει ύπαρξη λογαριασμού του κατόχου στην τράπεζα έκδοσης της κάρτας. Η πιστωτικές κάρτες εκδίδονται είτε για χρήση στο εξωτερικό, είτε για χρήση στο εσωτερικό ή και για τα δύο. Οι πιστωτικές κάρτες εξωτερικού δίνουν το δικαίωμα στον κάτοχο τους να πραγματοποιήσει έξοδα στο . Βέβαια, οι κάρτες αυτές απαιτούν υψηλή ετήσια συνδρομή.

Στην Ελλάδα, σήμερα, όλες σχεδόν οι τράπεζες εκδίδουν πιστωτικές κάρτες. Κυριότερες αυτόνομες κάρτες Ελληνικών τραπεζών είναι η Εθνοκάρτα της Εθνικής τράπεζας, η Εμποροκάρτα της εμπορικής, η Ιονοκάρτα της Ιονικής και η Αγροκάρτα της Αγροτικής τράπεζας. Παράλληλα, όλες οι τράπεζες σε συνεργασία με ξένες τράπεζες ή πιστωτικούς οργανισμούς, υποστηρίζουν τις κυριότερες διεθνής πιστωτικές κάρτες κυρίως την visa (Εμπορική, Ιονική τελευταία η Εθνική και άλλες τράπεζες) και την MasterCard (Εθνική κ.τ.λ.). Συγχρόνως κυκλοφορούν και οι κλασσικές κάρτες dinner’s, American

express κτλ.. Όλες οι τράπεζες εκδίδουν κάρτες πού, στην πλειοψηφία τους, καλύπτουν όλο το εύρος της αγοράς (απλές πιστωτικές κάρτες, κάρτες διευκόλυνσης και επαγγελματικές κάρτες για υψηλόβαθμα στελέχη).

Η χρήση των πιστωτικών καρτών παρουσιάζει σημαντικά πλεονεκτήματα. Όπου αναφέρονται όρια ή επιτόκια , είναι φυσικό αυτά να αναπροσαρμόζονται και να αλλάζουν συνέχεια. Συγκεκριμένα η χρήση καρτών προσφέρει:

1. Ασφάλεια, γιατί ο κάτοχος της κάρτας δεν χρειάζεται να κυκλοφορεί με πολλά μετρητά.

2. Ευκολία και ταχύτητα συναλλαγών με απεριόριστο όριο δαπανών.

3. Καλύτερο προγραμματισμό των μηνιαίων εσόδων και εξόδων.

4. Διευκόλυνση για αγορά διαρκών καταναλωτικών προϊόντων (π.χ. ηλεκτρικά) με δόσεις (πολλές φορές άτοκες) που προσφέρει η κάρτα.

5. Προσφορά τηλεφωνικών και ταχυδρομικών πωλήσεων.

6. Έκδοση ειδικών περιοδικών, πληροφόρηση και συμμετοχή σε εκπτώσεις, διοργανώσεις διαγωνισμών, κληρώσεων κτλ.

7. Ασφάλιση αγορών για ζημιά ή κλοπή.

8. Αυτόματη εξόφληση δαπανών διαμέσου του τραπεζικού λογαριασμού.

9. Χρήση της κάρτας στα ΑΤΜ και δυνατότητα χορήγησης καρνέ εγγυημένων επιταγών.

10. Προνομιακές τιμές και προσφορές από επιχειρήσεις που συνεργάζονται με την πιστωτική κάρτα.

11. Ενίσχυση χωρίς επιβάρυνση κοινωφελών οργανισμών

12. Ευχάριστη ψυχολογική διάθεση (αίσθηση αγοραστικής δύναμης και ελευθερίας).

13. Παροχή ικανοποιητικού πιστωτικού ορίου .

14. Μεγάλη περίοδος αποπληρωμής του ποσού των συναλλαγών που

γίνονται με αυτές .

15. Δυνατότητα αποπληρωμής του λογαριασμού – εφόσον αυτός δεν ξεπερνά το πιστωτικό όριο – σε έντοκες μηνιαίες δόσεις.

16. Καλύτερο έλεγχο των μηνιαίων εξόδων του κατόχου με τον αναλυτικό λογαριασμό που λαμβάνει.

17. Παροχή επιπλέον συναλλάγματος και διευκολύνσεις στα ταξίδια εξωτερικού. Επιπλέον ασφάλεια ταξιδιού με διάφορα ποσά και καλύψεις όπως ασφάλεια ζωής, ιατρική και νομική βοήθεια, ασφάλιση καθυστέρησης ή ακύρωσης πτήσης, ασφάλιση καθυστέρησης ή απώλειες αποσκευών και τέλος εξασφαλισμένη κράτηση ξενοδοχείου.

Η έκδοση πιστωτικών καρτών σήμερα αποτελεί πρωταρχική ανάγκη για όλες τις τράπεζες, τόσο για λόγους εκσυγχρονισμού, όσο και για λόγους ανταγωνισμού στην Ελληνική αγορά. Για τον λόγο αυτό οι διάφορες εμπορικές τράπεζες διαφοροποιούν τα προϊόντα, τους προσφέροντας στους κατόχους των πιστωτικών καρτών τους, παροχές και διευκολύνσεις που δεν δεσμεύονται από το σημερινό νομικό καθεστώς πίστωσης. Η παρουσίαση των παροχών διαφόρων πιστωτικών καρτών είναι πολύ χρήσιμη γιατί διαφαίνεται το πλαίσιο ανταγωνισμού τους. Ειδικότερα:

Στην Ελλάδα, το 2005, κυκλοφορούσαν γύρω στις 950.000 κάρτες που αντιστοιχεί σε ένα ποσοστό 9% του πληθυσμού. Αυτό το γεγονός, δείχνει την ύπαρξη ενός μεγάλου πεδίου ανάπτυξης της αγοράς των πιστωτικών καρτών, ιδιαίτερα, αν συγκρίνει κανείς το ποσοστό αυτό με αντίστοιχα άλλων δυτικών χωρών. Ενδεικτικά, στην Αγγλία κυκλοφορούσαν 13,4 εκατομμύρια κάρτες. Την ίδια χρονιά εκτιμάται ότι ποσοστό άνω του 55% των Άγγλων, άνω των 18 ετών διαθέτουν μία ή περισσότερες πιστωτικές κάρτες. Το αντίστοιχο ποσοστό στην Γαλλία ανέρχεται στο 20%, ενώ στην Ισπανία κυκλοφορούν γύρω στα τρία εκατομμύρια κάρτες Visa μόνο, χωριστά από τις άλλες πιστωτικές κάρτες, που αντιστοιχούν σε ποσοστό 15% των ατόμων άνω των 17 ετών.

Είναι λοιπόν, φανερό ότι σε πολλές χώρες, ο θεσμός της πιστωτικής κάρτας είναι καλά εδραιωμένος, όπως, επίσης, ότι υπάρχουν περιθώρια για την Ελληνική αγορά, η οποία τα τελευταία χρόνια αρχίζει και αναπτύσσεται με γρήγορους ρυθμούς. Οι κάτοχοι και χρήστες των πιστωτικών καρτών έχουν συγκεκριμένα δημογραφικά στοιχεία, εισόδημα, ηλικία, φύλλο κ.τ.λ. (Meidan, 2006)

Οι τράπεζες εστιάζουν σήμερα πολύ στη διασφάλιση της συναλλαγής με τον τελικό χρήστη. Μία από τις δικλείδες ασφαλείας των συναλλαγών του πελάτη είναι το πρώτο στάδιο όπου πραγματοποιείται η ταυτοποίηση του χρήστη.

Όταν ο πελάτης εγγραφεί στις υπηρεσίες της ηλεκτρονικής τραπεζικής, θα παραλάβει προσωπικά ή ταχυδρομικά μετά την πάροδο λίγων ημερών έναν ειδικό φάκελο ασφαλείας που περιέχει τους ατομικούς κωδικούς πρόσβασης. Το επόμενο βήμα είναι η σύνδεση και ταυτοποίηση του χρήστη στην αντίστοιχη ιστοσελίδα της τράπεζας, για να ξεκινήσει τις συναλλαγές του.

Ο τρόπος πρόσβασης στις υπηρεσίες της ηλεκτρονικής τραπεζικής και κατά συνέπεια ο αντίστοιχος βαθμός ασφάλειας που έχουν οι χρήστες, διαφέρει από τράπεζα σε τράπεζα.

Έτσι, ανάλογα με την πολιτική ασφαλείας που ακολουθεί η κάθε τράπεζα, υπάρχουν διάφορα είδη ταυτοποίησης του χρήστη και πρόσβασής του στις υπηρεσίες ηλεκτρονικής τραπεζικής μέσω του διαδικτύου. Οι συνήθεις μέθοδοι ταυτοποίησης` είναι οι ακόλουθοι:

Η κρυπτογράφηση των προσωπικών κωδικών των χρηστών, από τη στιγμή που πληκτρολογούνται από τους ίδιους στην ιστοσελίδα της τράπεζας είναι ζήτημα που άπτεται των τραπεζών. Επίσης, οι τράπεζες είναι υπεύθυνες για θέματα καθορισμού του κατάλληλου μήκους κωδικού, απενεργοποίησης των κωδικών και τερματισμού της σύνδεσης χρηστών μετά από ένα χρονικό διάστημα μη χρήσης των υπηρεσιών. Σε κάθε περίπτωση οι τράπεζες πρέπει να ενημερώνουν τους χρήστες της ηλεκτρονικής τραπεζικής για το ευαίσθητο θέμα της ασφάλειας τους. Τα τελευταία χρόνια μερικές τράπεζες έχουν υιοθετήσει για λόγους επιπρόσθετης ασφάλειας, τα λεγόμενα εικονικά

πληκτρολόγια.

Η χρήση αιθμών TAN προϋποθέτει μια συγκεκριμένη διαδικασία εγκατάστασης και ταυτοποίησης. Αρχικά θα πρέπει να γίνει η εγκατάσταση Λογισμικού Token. Η εγκατάσταση, μετά την εισαγωγή του οπτικού δίσκου στο PC από όπου θα εκτελούνται οι συναλλαγές στο e-banking, γίνεται ακολουθώντας τα παρακάτω βήματα (Εργαστήριο Εκπαιδευτικής και Γλωσσικής Τεχνολογίας.,2010):

1ο βήμα: επιλογή γλώσσας εμφάνισης μηνυμάτων του προγράμματος

2ο βήμα: εγκατάσταση οδηγών συσκευής (drivers)

3ο βήμα: εγκατάσταση λογισμικού

Η πρόσβαση στο e-Banking της Τράπεζας θα γίνεται ως εξής:

1. Εισάγει ο χρήστης τη συσκευή token στην USB θύρα του υπολογιστή του.
2. Πληκτρολογεί τη διεύθυνση του δικτυακού τόπου της τράπεζας στον Internet Explorer.
3. Επιλέγει το ψηφιακό πιστοποιητικό ασφαλείας πατά OK και μετά πληκτρολογεί τον αριθμό token pin και Enter.
4. Μόλις φορτωθεί η αρχική σελίδα του site θα εισάγει στο πεδίο «Όνομα Χρήστη» το user name.
5. Τέλος εισάγουμε στο πεδίο «Κωδικός χρήστη» το password.

Αναλυτικά τώρα τα σημεία ελέγχου είναι τα εξής:

1. Registration: Η εγγραφή στην υπηρεσία e-banking όπως σχεδιάζεται είναι εξαιρετικά εύκολη και απλή. Με μια μόνο επίσκεψη στη τράπεζα ο χρήστης θα αποκτά πρόσβαση και θα πραγματοποιεί τις συναλλαγές του γρήγορα, απλά και με απόλυτη ασφάλεια. Τα βασικά δεδομένα τα οποία χρειάζεται είναι τα ακόλουθα:

1. Να έχει έναν καταθετικό λογαριασμό.
2. Να έχετε στην κατοχή του ενεργή χρεωστική κάρτα από το κατάστημα με το άνοιγμα του λογαριασμού.

3. Να συμπληρώσει μία αίτηση εγγραφής στα Εναλλακτικά δίκτυα σε οποιοδήποτε κατάστημα της
4. Να γνωρίζει τους 2 κωδικούς

Όλα τα παραπάνω αλλά και το συγκεκριμένο βήμα το συμπεριλαμβάνουμε γιατί αποτελεί τη διαδικασία πιστοποίησης του χρήστη. Στο σημείο αυτό δίνεται η μοναδικότητα ανά χρήση, όπου ο καθένας έχοντας ένα μοναδικό κωδικό εντάσσεται στο σύστημα. Η διαδικασία εγγραφής (registration) εξασφαλίζει τη μυστικότητα και το αναλλοίωτο των δεδομένωνμέσω ενός πρωτοκόλλου επικοινωνίας, το οποίο βασίζεται είτε στην κρυπτογράφηση (encryption) 40bit ή 128 bit (ισχυρή κρυπτογράφηση).

Για την ασφαλή λειτουργία του Internet Banking, χρησιμοποιείται στο σύστημα η κρυπτογράφηση 128 **bit των διακινουμένων στοιχείων, η οποία θεωρείται απαραβίαστη για τις εφαρμογές στο Διαδίκτυο** (Γιαννόπουλος 2001).

Σε οποιαδήποτε διαταραχή ή παρεμβολή στην επικοινωνία, η συναλλαγή θα διακόπτεται. Για την ταυτοποίηση των χρηστών e-Banking, χρησιμοποιείται ένας κωδικός χρήστη (username) και ένα προσωπικό κωδικό εισόδου (password), μοναδικούς για κάθε χρήστη της υπηρεσίας (Ιγγλεζάκης 2001).

Για τη διενέργεια όμως χρηματικών συναλλαγών, οι τράπεζες δεν αρκούν σε αυτό το επίπεδο ταυτοποίησης του χρήστη αλλά απαιτούν μια επιπλέον δικλείδα ασφαλείας, την ψηφιακή πιστοποίηση (EFG.,2009; Bayne, 2000).

Πιστοποίηση Χρήστη: Η πιστοποίηση χρήστη στο **Internet Banking βοηθά στην αναγνώριση των χρηστών και επιτρέπει την** πρόσβασή τους στο Σύστημα

Η τράπεζα επιδιώκει για την πρόσβασή σε συναλλαγές μέσω του e-banking ν’ απαιτείται Κωδικός Χρήστη και Προσωπικός Κωδικός (PIN) τους οποίους θα επιλέγει ο χρήστης μόνος του ενώ θα μπορεί να τους αλλάζει όποτε επιθυμεί. Επίσης, για την είσοδό του στο e-banking θα του ζητούνται κάθε φορά 2 τυχαία ψηφία της χρεωστικής του κάρτας τα οποία δεν θα

πληκτρολογεί, αλλά θα τα επιλέγει από μια αναδιπλούμενη λίστα. Με αυτό τον τρόπο θα του παρέχεται μια ακόμα δικλείδα ασφαλείας από τα προγράμματα που καταγράφουν τους κωδικούς ασφαλείας που πληκτρολογεί (Millennium.2010; OnlineTools.2009)

Η υποκλοπή μέσω key logging είναι μια μέθοδος συγκέντρωσης προσωπικών πληροφοριών χρηστών του διαδικτύου μέσω προγραμμάτων που εγκαθίστανται στον ηλεκτρονικό υπολογιστή του χρήστη χωρίς να γίνεται αντιληπτό από αυτόν.

Αυτό μπορεί να συμβεί όταν ο χρήστης κάνει κλικ σε συνδέσμους (links) ή αρχεία που παραλαμβάνει με e-mails, καθώς και όταν κατεβάζει άλλα προγράμματα από το διαδίκτυο. Τα προγράμματα αυτά (spyware programs) έχουν τη δυνατότητα να καταγράφουν οτιδήποτε πληκτρολογεί ο χρήστης (κωδικούς, λογαριασμούς, αριθμούς καρτών κλπ) (Bank of Cyprus.,2009).

Ο κίνδυνος είναι μεγαλύτερος σε PCs που χρησιμοποιούνται από πολλούς χρήστες, όπως στα Internet Cafe. Για να αποφευχθεί η χρήση τυχαίων κωδικών το σύστημα ηλεκτρονικής τραπεζικής διαθέτει συνήθως τη δυνατότητα μετά από τρεις λανθασμένες προσπάθειες εισαγωγής στην υπηρεσία e-banking να μην επιτρέπεται η πρόσβαση σε αυτήν (μπλοκάρισμα κωδικού).

Εάν δεν υπάρξει δραστηριότητα για 10 λεπτά γίνεται αυτόματη αποσύνδεση από την υπηρεσία e-banking. Αυτό θα προστατεύει τους χρήστες από ανεπιθύμητη πραγματοποίηση ηλεκτρονικών συναλλαγών από τρίτους, σε περίπτωση που απομακρυνθεί ο χρήστης από το χώρο εργασίας ή τον υπολογιστή του για κάποιο χρονικό διάστημα (Αρσάνογλου 2007).

Ο χρήστης, εκτός από την αναγνώρισή του μέσω του ονόματος και του προσωπικού κωδικού, θα αναγνωρίζεται επιπλέον και μέσω του συγκεκριμένου υπολογιστή ο οποίος είναι και ο μόνος από τον οποίο ο χρήστης θα μπορεί να πραγματοποιεί εγχρήματες συναλλαγές (EFG.,2010).

Σύστημα ελέγχου της αυθεντικότητας της ιστοσελίδας: Το σύστημα το οποίο βασίζεται στην αυθεντικότητα της ιστοσελίδας. Συγκεκριμένα οι χρήστες θα πρέπει να πληκτρολογούν τη διεύθυνση της ιστοσελίδας μόνοι

τους και όχι μέσω σύνδεσης που πιθανόν έχει σταλθεί μέσω e-mail ή δημοσιεύεται σε ιστοσελίδες άλλων εταιριών.

Συγχρόνως θα επιβεβαιώνεται στο χρήστη η διεύθυνση της ιστοσελίδας ενώ τέλος θα υπάρχει η ένδειξη  η οποία θα εμφανίζεται στις ασφαλείς ιστοσελίδες του συστήματος. Εκτός αυτών, κατά την είσοδο στην ιστοσελίδα με τους κωδικούς, θα εμφανίζεται και άλλο πιστοποιητικό υπογραφής προγραμμάτων, που θα έχει προμηθευτεί η Τράπεζα και το οποίο θα πιστοποιεί ότι τα προγράμματα που μεταφέρονται στο σταθμό του χρήστη είναι τα γνήσια που έχουν εκπονηθεί από το σύστημα (NBG.,2009).

Ασφάλεια επικοινωνίας μέσω **e-mail : Τα e-mail από το σύστημα θα υπογράφονται ψηφιακά.**

Οι ψηφιακές υπογραφές, χρησιμοποιώντας το διαδικτυακό πρότυπο Secure Multipurpose Internet Mail Extensions (S/MIME), παρέχουν βεβαιότητα στους πελάτες της ως προς το ότι το μήνυμα e-mail προέρχεται πράγματι από την Τράπεζα Εάν κάνει κλικ στο εικονίδιο με την κορδέλα, θα εμφανιστεί το παρακάτω μήνυμα. Το μήνυμα αυτό ενημερώνει για την εγκυρότητα ή όχι της ψηφιακής υπογραφής. Κάνοντας κλικ στο κουμπί “Λεπτομέρειες” μπορεί ο χρήστης να διαβάσει όλες τις πληροφορίες του ψηφιακού πιστοποιητικού όπως (NBG.,2009):

1. Ποιος υπογράφει. Υπογεγραμμένο με χρήση RSA/SHA1 σε 9:34:07 πμ 22/2/2006
2. Ποιος είναι ο κάτοχος.
3. Ποιος ο σκοπός έκδοσής του. Βεβαίωση ότι το ηλεκτρονικό μήνυμα ήρθε από τον αποστολέα
4. Περίοδος εγκυρότητας.

Άλλα δεδομένα στην ασφάλιση των χρηστών: Πέρα των προαναφερθέντων μέτρων ασφαλείας που θα έχει το σύστημα για τις συναλλαγές είναι απαραίτητο, να υπάρχουν οι ακόλουθες αρχές. Οι κωδικοί πρόσβασης (NBG.,2009):

1. Δεν θα πρέπει να αποκαλύπτονται ποτέ σε τρίτα πρόσωπα,

συμπεριλαμβανομένων και των υπαλλήλων της Τράπεζας.

2. Η φύλαξη τους αποτελεί προσωπική ευθύνη του χρήστη και συνιστούμε να απομνημονεύονται και στη συνέχεια να καταστρέφονται τα σχετικά έγγραφα που τους περιέχουν.
3. προτείνεται να τροποποιούνται συχνά, να μην αποθηκεύονται στον υπολογιστή σας αλλά να πληκτρολογούνται εκ νέου κάθε φορά.
4. Κατά την επιλογή κωδικού ασφαλείας προτείνεται να αποφεύγεται η εισαγωγή προβλεπόμενων στοιχείων (π.χ. ημερομηνίες γενεθλίων, ονόματα).
5. Σε περίπτωση απώλειας ή διαρροής των κωδικών ασφαλείας σε τρίτους, οι χρήστες οφείλουν να τους αλλάξουν άμεσα και να ενημερώσουν το συντομότερο δυνατό.

Σε σχέση με την ασφάλεια υποδομών αναπτύσσονται οι ακόλουθες δράσεις (Σταματίου.,2009):

1. Το σύστημα αρχικά ταυτοποιείται, συγκεκριμένα η τράπεζα επιλέγει ένα φορέα ταυτοποίησης της ταυτότητας και του συστήματος της στο διαδίκτυο. Μια από τις πιο γνωστές ταυτοποιήσεις είναι αυτό της εταιρίας Verisign.
2. Μια επιπρόσθετη δικλίδα στην υποδομή του συστήματος που σχεδιάζεται είναι η κρυπτογράφηση, για την οποία έχουμε αναφερθεί και παραπάνω. Το πρωτόκολλο επικοινωνίας SSL μαζί με τη κρυπτογράφηση στα 128bit εξασφαλίζει την ασφάλεια των συναλλαγών μέσω του διαδικτύου Η κρυπτογράφηση είναι αδύνατο να παραβιαστεί, η διεύθυνση της μετατρέπεται από http σε https ενώ εμφανίζεται και το λουκέτο στο κάτω μέρος της σελίδας.
3. Η πρόσβαση στα συστήματα των περισσότερων τραπεζών από τελευταία τεχνολογία Firewall και IDS, η οποία επιτρέπει τη χρήση συγκεκριμένων υπηρεσιών, απαγορεύοντας παράλληλα την πρόσβαση σε συστήματα βάσεις δεδομένων με απόρρητα στοιχεία και πληροφορίες.
4. Ως επιπρόσθετες δικλείδες ασφαλείας ορίζονται οι ακόλουθες:

- Εισαγωγή στοιχείων εισόδου: Η τράπεζα καθιερώνει τη χρήση εικονικού πληκτρολογίου για την καταχώρηση των στοιχείων χρήστη ή επιλεκτικά την καταχώρηση ορισμένων από τα στοιχεία αυτά.
- Αυτόματη αποσύνδεση χρήστη: Στις περισσότερες εφαρμογές δίνεται η δυνατότητα διακοπής μιας συναλλαγής σε πέντε ως δεκαπέντε λεπτά.
- Υποχρεωτική αλλαγή κωδικών: Η τράπεζα υποχρεώνει τους χρήστες σε συχνή αλλαγή των κωδικών τους.

Η εφαρμογή των όσων αναφέρθηκαν μέχρι τώρα προϋποθέτει και την υλοποίηση υποδομών, οι οποίες έχουν σαφή πελατοκεντρικά χαρακτηριστικά.

Η τεχνολογία είναι το μέσο αλλά και η δύναμη που επιτρέπει σήμερα την υλοποίηση διαφόρων υπηρεσιών. Το σύστημα της τράπεζας θα πρέπει να βασιστεί σε τεχνολογίες διαχείρισης των σχέσεων με τους πελάτες (Relationship technologies). Η χρήση ενός συστήματος CRM, είναι απαραίτητη, η εφαρμογή του είναι δύσκολη και πολύπλοκη σε σχέση με τη καθημερινή του συντήρηση και ενημέρωση.

Σε σχέση με τα e-mail των χρηστών του συστήματος, εκτός από τον αποστολέα και τον παραλήπτη, μπορεί να διαβαστεί εύκολα και από τους εργαζόμενους στην Εταιρία Παροχής Υπηρεσιών Διαδικτύου (ISP - Internet Service Provider) του αποστολέα, τους εργαζόμενους στον ISP του παραλήπτη, από οποιονδήποτε ελέγχει τους δρομολογητές (routers) από τους οποίους θα περάσουν τα «πακέτα» του μηνύματος και από οποιονδήποτε έχει πρόσβαση στον εξοπλισμό τηλεφωνίας στην τηλεφωνική εταιρία.

Αν το μήνυμα αποστέλλεται ή παραλαμβάνεται από κινητό τηλέφωνο με σύνδεση στο Διαδίκτυο, τότε μπορεί να υποκλαπεί από άτομα με ειδικές συσκευές υποκλοπής, επιπλέον, είναι πολύ απλό να πλαστογραφηθεί η διεύθυνση αποστολής, ακόμα και με ένα πρόγραμμα e-mail.

Η τράπεζα για να επιλύσει το παραπάνω πρόβλημα θα εστιάσει στις τεχνολογίες που αναφέραμε παραπάνω αυτές της κρυπτογράφησης. Οι τεχνολογίες αυτές θα εξασφαλίζουν ότι το μήνυμα θα μπορεί να το διαβάσει μόνο ο παραλήπτης του, καθώς στα ενδιάμεσα στάδια το μήνυμα εμφανίζεται

με ακατάληπτους χαρακτήρες, είναι δηλαδή μη αναγνώσιμο.

Εκτός από την κρυπτογράφηση, μια άλλη τεχνολογία που μπορεί να χρησιμοποιήσει η τράπεζα και παρέχει τέτοιου είδους ασφάλεια είναι η ηλεκτρονική υπογραφή.

3.3.2 Το Παράδειγμα του Stuxnet-Τεχνικές αντιμετώπισης

Το Stuxnet, όπως αναφέρθηκε παραπάνω είναι αρκετά περίπλοκο, σε σχέση με τη πολυπλοκότητα και τη προηγούμενη δομή του μια και αξιοποιεί τέσσερα διαφορετικά σημεία των Windows, ενώ έχει στη κατοχή του και δυο κλεμμένα πιστοποιητικά και με τη βοήθεια αυτών επίθετε στα περίπλοκα συστήματα SCADA της Siemens. Το Stuxnet αποτελεί το πρώτη χτύπημα σε μια σειρά επιθέσεων που θα επιλέξουν να κάνουν στη πορεία οι δημιουργοί του.

Οι αρνητικές επιδράσεις σε υποδομές στρατηγικής δράσης σε κάποια χώρα οι οποίες αναπτύσσονται μεταξύ μετά από τη δράση τέτοιων cyber arms επιφέρουν συγκεκριμένους τρόπους και μεθόδους αντιμετώπισης όχι μόνο από μεμονωμένα κράτη αλλά από διεθνή όργανα.

Τα firewall συστήματα προφυλάσσουν τους πληροφοριακούς πόρους ενός Η/Υ ή ενός δικτύου Η/Υ από επιθέσεις μη εξουσιοδοτημένης πρόσβασης (Ferguson, 2003).

"Τα συστήματα IDS κατηγοριοποιούνται ως εξής:

1. Ανίχνευση επιθέσεων: Το IDS όταν πρόκειται για ανάλυση επιθέσεων αναλύει την πληροφορία που έχει συγκεντρώσει και συγκρίνει τα αποτελέσματα της ανάλυσης με γνωστές επιθέσεις, οι «υπογραφές» των οποίων είναι αποθηκευμένες σε μια βάση δεδομένων.

2. Ανίχνευση Ανωμαλιών: "Η λειτουργία των IDS αυτού του τύπου μπορεί να παρομοιαστεί με την ευρετική (heuristic) λειτουργία ενός προγράμματος antivirus (Kurose, 2005)

3. Παθητικά και Ενεργητικά IDS: "Ένα παθητικό IDS, έχει κυρίως ενημερωτικό χαρακτήρα, δηλαδή «ανιχνεύει» και καταγράφει μια επίθεση ή μια «ύποπτη» ενέργεια χωρίς να την αποτρέπει ή να την αντιμετωπίζει"

(Ferguson, 2003)

3.3.3 128 bit encryption

Τη μυστικότητα και το αναλλοίωτο των δεδομένων: Και τα δύο εξασφαλίζονται μέσω του πρωτοκόλλου επικοινωνίας, το οποίο μπορεί να είναι δύο ειδών: 40bit encryption ή 128 bit encryption (ισχυρή κρυπτογράφηση).

Η τράπεζα για την ασφαλή λειτουργία του Internet Banking, χρησιμοποιεί κρυπτογράφηση 128 bit των διακινουμένων στοιχείων, μέσω του πρωτοκόλλου SET, το οποίο θεωρείται απαραβίαστο για τις εφαρμογές στο Διαδίκτυο.

Το σύστημα αυτό, εκτός της κρυπτογράφησης που πραγματοποιεί, ελέγχει συνεχώς την αυθεντικότητα της επικοινωνίας μεταξύ του PC και του κεντρικού συστήματος. Σε οποιαδήποτε διαταραχή ή παρεμβολή στην επικοινωνία, η συναλλαγή διακόπτεται άμεσα και η επικοινωνία με το κεντρικό σύστημα της Τράπεζας πρέπει να αποκατασταθεί από την αρχή (αναγνώριση χρήστη, κλπ.).

Αναβάθμιση των browsers ώστε να υποστηρίζουν την 128-bit SSL κρυπτογράφηση. Για να επιτευχθεί το πιο υψηλό διαθέσιμο επίπεδο ασφάλειας, πρέπει να αναβαθμιστούν τα προγράμματα, browsers και εφαρμογών για να υποστηρίζουν την 128-bit SSL κρυπτογράφηση ή τα υψηλότερα πρότυπα κρυπτογράφησης.

3.3.4 Πρωτόκολλο Ασφάλειας SSL

Το SSL (Secure Socket Layer) είναι ένα ευέλικτο, γενικού σκοπού σύστημα κρυπτογράφησης για την προστασία της επικοινωνίας μέσω του Παγκόσμιου Ιστού, το οποίο είναι ενσωματωμένο και στα προγράμματα πλοήγησης της Netscape και της Microsoft.

Το πρωτόκολλο SSL έχει σχεδιαστεί για να παρέχει απόρρητη επικοινωνία μεταξύ δύο συστημάτων, από τα οποία το ένα λειτουργεί σαν πελάτης (client) και το άλλο σαν εξυπηρετητής (server). Δηλαδή το πρωτόκολλο αυτό μπορεί να παρέχει απόρρητη επικοινωνία μεταξύ εμπόρου και πελάτη σε μια συναλλαγή

πληρωμής και για το λόγο αυτό το SSL αποτελεί το κύριο πρωτόκολλο ασφάλειας για το ηλεκτρονικό εμπόριο (Freier, Karlton& Kocher, 2011).

Συγκεκριμένα, το πρωτόκολλο SSL παρέχει κρυπτογράφηση της μεταδιδόμενης πληροφορίας (data encryption), υποχρεωτική πιστοποίηση της ταυτότητας του εξυπηρετητή (server authentication) και προαιρετική πιστοποίηση της ταυτότητας του πελάτη (client authentication) μέσω έγκυρων πιστοποιητικών που έχουν εκδοθεί από έμπιστες Αρχές Πιστοποίησης.

Υποστηρίζει πληθώρα μηχανισμών κρυπτογράφησης και ψηφιακών υπογραφών για την αντιμετώπιση όλων των διαφορετικών αναγκών. Επιπλέον εξασφαλίζει την ακεραιότητα των δεδομένων (data integrity), εφαρμόζοντας την τεχνική των Message Authentication Codes (MACs), ώστε κανείς να μην μπορεί να αλλοιώσει την πληροφορία χωρίς να γίνει αντιληπτός. Για κάθε κρυπτογραφημένη συναλλαγή δημιουργείται ένα κλειδί συνόδου (session key) το μήκος τουοποίου μπορεί να είναι 40 bits ή 128 bits. Είναι γνωστό ότι όσο μεγαλύτερο είναι το μήκος του κλειδιού, τόσο πιο ασφαλής είναι η κρυπτογραφημένη επικοινωνία.

Το πρωτόκολλο SSL αναπτύχθηκε από την Netscape Communications Corporation για την ασφαλή επικοινωνία ευαίσθητων πληροφοριών όπως προσωπικά στοιχεία και αριθμούς πιστωτικών καρτών. Έχουν υπάρξει τρεις εκδόσεις του SSL. Η ιστορία της εξέλιξης του SSL έχει ως εξής: (Freier, Karlton& Kocher, 2011).

Ιούλιος 1994: Κυκλοφόρησε η πρώτη έκδοση v.1.0 του πρωτοκόλλου SSL από τη Netscape, η οποία χρησιμοποιήθηκε μόνο για εσωτερικές ανάγκες της εταιρείας.

Δεκέμβριος 1994: Κυκλοφόρησε η δεύτερη έκδοση v.2.0 του πρωτοκόλλου, η οποία ενσωματώθηκε στο web browser της Netscape, τον Netscape Navigator.

Ιούλιος 1995: Εκδόθηκε ο αντίστοιχος web browser της Microsoft, ο Internet Explorer, ο οποίος υποστηρίζει και αυτός την έκδοση v.2.0 του SSL, με κάποιες όμως επεκτάσεις της Microsoft.

Το SSL πρωτόκολλο, στην έκδοση v.2.0, καθιερώθηκε ως de facto πρότυπο για κρυπτογραφική προστασία της HTTP κυκλοφορίας δεδομένων. Το HTTP (Hyper Text Transfer Protocol) είναι ένα πρωτόκολλο που φροντίζει τη μεταφορά και τον τρόπο μετάδοσης δεδομένων στο διαδίκτυο. Ωστόσο το SSL v.2.0 είχε αρκετούς περιορισμούς τόσο ως προς την κρυπτογραφική ασφάλεια όσο και ως προς τη λειτουργικότητα του. Για το λόγο αυτό υπήρχε η ανάγκη για βελτίωση της έκδοσης v.2.0. Έτσι το πρωτόκολλο αναβαθμίστηκε σε SSL v.3.0 με δημόσια αναθεώρηση και σημαντική συνεισφορά από τη βιομηχανία.

Νοέμβριος 1995: Κυκλοφόρησε επισήμως η έκδοση v.3.0 του SSL, ενώ λίγους μήνες πιο πριν εφαρμοζόταν σε προϊόντα της εταιρείας, όπως τον Netscape Navigator.

Μάιος 1996: Το SSL περνά στη δικαιοδοσία του Internet Engineering Task Force -IETF, ο οποίος δημιουργεί την ειδική ομάδα εργασίας TLS group και μετονομάζει την νέα έκδοση του SSL, σε TLS (Transport Layer Security).

Η ομάδα εργασίας TLS group καθιερώθηκε το 1996 για να τυποποιήσει το πρωτόκολλο Transport Layer Security. Η TLS group εργάστηκε πάνω SSL v.3.0 πρωτόκολλο. Η ομάδα αυτή έχει ολοκληρώσει μια σειρά από προδιαγραφές που περιγράφουν τις εκδόσεις 1.0 και 1.1 του TLS πρωτοκόλλου, και ετοιμάζει την έκδοση 1.2.

Ιανουάριος 1999: Εκδίδεται η πρώτη έκδοση του πρωτοκόλλου TLS, η οποία μπορεί να θεωρείται και ως η έκδοση v.3.1 του SSL.

Δεκέμβριος 2005: Δημοσιεύεται η έκδοση 1.1 του TLS πρωτοκόλλου από την TLS group.

Η τρίτη έκδοση του πρωτοκόλλου SSL κάλυψε πολλές αδυναμίες της δεύτερης έκδοσης. Οι σημαντικότερες αλλαγές αφορούν: α) στη μείωση των απαραίτητων μηνυμάτων κατά το στάδιο εγκαθίδρυσης της σύνδεσης («χειραψία», «handshake»), β) στην επιλογή των αλγορίθμων συμπίεσης και κρυπτογράφησης από τον εξυπηρετητή και γ) στην εκ νέου διαπραγμάτευση του κυρίως κλειδιού (master-key) και του «αναγνωριστικού» συνόδου (session-id). Ακόμη αυξάνονται οι διαθέσιμοι αλγόριθμοι κρυπτογράφησης και προστίθενται νέες τεχνικές για τη διαχείριση των κλειδιών. Γενικά, η τρίτη έκδοση του SSL (v.3.0) είναι πιο

ολοκληρωμένη σχεδιαστικά από τη δεύτερη, με μεγαλύτερο εύρος υποστήριξης και λιγότερες ατέλειες.

Επειδή η Netscape επιθυμούσε την παγκόσμια υιοθέτηση του πρωτοκόλλου SSL, γεγονός που ερχόταν σε σύγκρουση με την τότε νομοθεσία των Η.Π.Α περί εξαγωγής κρυπτογραφικών αλγορίθμων, αναγκάστηκε να επιτρέψει τη χρήση αλγορίθμων κρυπτογράφησης με κλειδί των 40 bits στις προς εξαγωγή εφαρμογές SSL, τη στιγμή που η κανονική έκδοση χρησιμοποιεί κλειδί των 128 bits (Freier, Karlton& Kocher, 2011).

3.4 Ορισμός FIREWALL

Ο πρωταρχικός σκοπός ενός firewall είναι η αποτροπή μη εξουσιοδοτημένης πρόσβασης μεταξύ δικτύων. Σε γενικές γραμμές αυτό σημαίνει να προστατεύει το εσωτερικό δίκτυο μίας εγκατάστασης (site) από το υπόλοιπο Internet (DoD , 1983).

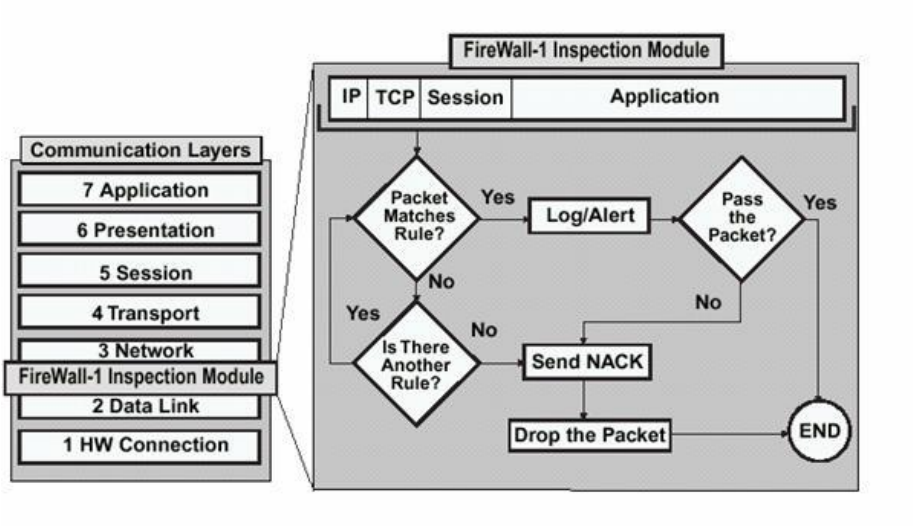
Αν η εγκατάσταση διαθέτει firewall, θα πρέπει να ληφθούν αποφάσεις για το τι πρέπει να επιτραπεί ή όχι να περάσει το firewall. Αυτές οι αποφάσεις θα πρέπει να απορρέουν ευθέως από την πολιτική ασφαλείας και πιθανόν θα περιορίσουν τις διαθέσιμες επιλογές εγκατάστασης των διαδικτυακών υπηρεσιών όπως UDP, HTTP, DNS, SMTP, FTP κ.α.

Η βασική αρχή λειτουργίας του firewall είναι η εξέταση των IP πακέτων που ταξιδεύουν μεταξύ του Internet και του εσωτερικού δικτύου. Αυτή είναι μία μέθοδος για τον έλεγχο της ροής της πληροφορίας για κάθε υπηρεσία (service) κατά IP address, θύρα (port) και προς κάθε κατεύθυνση.

Το εκάστοτε firewall υλοποιεί μια πολιτική ασφάλειας η οποία καθορίζει τις ισορροπίες μεταξύ διατήρησης της ασφάλειας και ευκολίας χρήσης - διαχείρισης.

Μια αυστηρή πολιτική της μορφής “ότι δεν επιτρέπεται απαγορεύεται” απαιτεί την ανεξάρτητη ενεργοποίηση κάθε υπηρεσίας. Αντιθέτως η πολιτική “ότι δεν απαγορεύεται επιτρέπεται” θυσιάζει ένα μέρος της ασφάλειας χάριν ευκολίας. Αν κάποια ενέργεια δεν επιτρέπεται βάση της πολιτικής αυτής το firewall θα πρέπει να διασφαλίσει την αποτυχία κάθε προσπάθειας εκτέλεσης της ενέργειας

αυτής. Συγκεκριμένα κάθε ενέργεια όπως ηλ. ταχυδρομείο, απομακρυσμένη σύνδεση, μεταφορά αρχείων εξετάζεται αν επιτρέπεται σύμφωνα με μια προκαθορισμένη πολιτική ασφάλειας (Buffenoir , 1988).



Εικόνα 3.1- Επικοινωνία

Λογικά ένα firewall είναι ένας απομωνωτής και ένας αναλυτής δεδομένων - πακέτων. Είναι ένα σύνολο εξοπλισμού και λογισμικού και μπορεί να υλοποιηθεί εναλλακτικά με τις επόμενες διατάξεις (Champine G., Geer , 1990):

- ένας δρομολογητής,
- ένας εξυπηρετητής,
- συνδυασμός δρομολογητών και εξυπηρετητών,
- συνδυασμός δρομολογητών και εξυπηρετητών και δικτύων.

Τα ύποπτα γεγονότα που εξακριβώνονται θα πρέπει να καταχωρούνται σε ένα ειδικό αρχείο. Επίσης θα πρέπει να υπάρχει ειδοποίηση των διαχειριστών της εγκατάστασης για κάθε προσπάθεια εισβολής στο δίκτυο. Κάποια firewall μπορούν να παρέχουν ακόμη και στατιστικά διακίνησης πληροφοριών, καθώς και υπηρεσίες κρυπτογράφησης και αποκρυπτογράφησης πληροφοριών κατά την είσοδο και έξοδο από το Internet αντίστοιχα.

Ερευνάται επίσης η δυνατότητα ελέγχου των μεταφερόμενων δεδομένων-αρχείων-ηλεκτρικού ταχυδρομείου για τυχόν μόλυνση από «ιούς». Τα αρχεία αυτά αποθηκεύονται προσωρινά, ελέγχονται για τυχόν «μόλυνση» και επαναναποστέλλονται στον τελικό προορισμό τους.

3.5. Αρχιτεκτονικές FIREWALL

Οι τρόποι υλοποίησης ενός firewall αν και είναι εξαρτώμενοι από τις εκάστοτε ανάγκες, διαδικτυακές εφαρμογές και την τοπολογία του εσωτερικού δικτύου μπορούν να περιγραφούν μέσω των παρακάτω τεσσάρων μεθόδων. Οι άλλες είναι συνδυασμοί των βασικών αυτών αρχιτεκτονικών (Stallings , 1999).

3.5.1. Συστήματα φίλτρου πακέτων

Τα συστήματα φίλτρου πακέτων δρομολογούν επιλεκτικά πακέτα μεταξύ των εσωτερικών και εξωτερικών εξυπηρετητών. Επιτρέπουν ή περιορίζουν τη κυκλοφορία κατηγοριών πακέτων ανάλογα με την πολιτική ασφάλειας που έχει προκαθορισθεί. Αυτό το είδος των δρομολογητών (router) ονομάζεται screening router. Όπως είναι γνωστό κάθε πακέτο περιλαμβάνει επικεφαλίδες που περιέχουν τις ακόλουθες πληροφορίες :

- IP διεύθυνση αποστολέα.
- IP διεύθυνση παραλήπτη.
- Πρωτόκολλο (TCP, UDP, ICMP).
- TCP ή UDP υποδοχέα (port) αποστολέα.
- TCP ή UDP υποδοχέα (port) προορισμού.
- Τύπος μηνύματος ICMP.

Επιπλέον ένας δρομολογητής γνωρίζει την σύνδεση (interface) στην οποία φθάνει το πακέτο και την σύνδεση από την οποία θα εξέλθει από αυτόν. Οι κύρια λειτουργία ενός απλού δρομολογητή είναι η επιλογή του καλύτερου (συμφερότερου) τρόπου αποστολής των πακέτων στις διευθύνσεις προορισμού.

Επιπλέον, οι screening routers εξετάζουν και το αν θα πρέπει να δρομολογηθεί το πακέτο προς τον κόμβο προορισμού με βάση τις πληροφορίες που περιέχονται στις επικεφαλίδες των πακέτων. Μερικά παραδείγματα φίλτρου της κυκλοφορίας είναι τα ακόλουθα (Hawa& Petr, 2002) :

1. Απαγόρευση όλων των συνδέσεων από συστήματα του εξωτερικού δικτύου (INTERNET) εκτός αυτών που υλοποιούν SMTP συνδέσεις (ηλεκτρικό Ταχυδρομείο).

2. Περιορισμός όλων των συνδέσεων από και προς τα «ευαίσθητα συστήματα» που χρειάζονται ιδιαίτερη προστασία.
3. Ελευθερία συνδέσεων που υλοποιούν ηλ. ταχυδρομείο (e-mail) και υπηρεσίες FTP, απαγόρευση των συνδέσεων που αφορούν υπηρεσίες όπως TFTP, X-Window system, RPC, και «r» υπηρεσίες (rlogin, rsh, rcp, κ.λπ.). Τα κυριότερα μειονεκτήματα της αρχιτεκτονικής αυτής είναι τα ακόλουθα :

   · Υλοποιείται με μία συσκευή, ή οποία επιπλέον εκτελεί και λειτουργίες δρομολόγησης. Σε περίπτωση βλάβης, δυσλειτουργίας ή «κατάληψης» από εισβολέα το εσωτερικό δίκτυο μένει απροστάτευτο.

   · Περιορίζει ή επιτρέπει υπηρεσίες στο σύνολό τους και δεν προστατεύει από ενέργειες που εκτελούνται διαμέσου μίας υπηρεσίας.

   · Σημαντική δυσκολία στον προγραμματισμό των ειδικών δρομολογητών και αδυναμία εκτέλεσης λειτουργιών κρυπτογράφησης.

3.5.2. DUAL - HOMED GATEWAY

Το Dual - Homed Gateway είναι ένα firewall που αποτελείται από ένα και μόνο σύστημα με δύο τουλάχιστον interfaces δικτύου (κάρτες). Το σύστημα αυτό είναι κατάλληλα παραμετροποιημένο ώστε τα πακέτα να μη δρομολογούνται άμεσα μεταξύ του εσωτερικού δικτύου και του Internet. Δηλαδή τα συστήματα του εσωτερικού δικτύου όπως και του Internet έχουν τη δυνατότητα να επικοινωνούν με το σύστημα αυτό αλλά όχι και μεταξύ τους. Στην τοπολογία αυτή συνηθίζεται το Dual - Homed Gateway να καλείται και Bastion (προμαχώνας) (Wongthavarawat & Ganz, 2003).

Το κυριότερο μειονέκτημα αυτής της τοπολογίας αυτής είναι ότι εμποδίζει την αμφίδρομη απευθείας επικοινωνία (Direct IP traffic). Αυτό επαληθεύεται και από τους χρήστες του δικτύου αλλά περισσότερο από αυτούς που επιχειρούν να παρέχουν υπηρεσίες σε χρήστες εκτός του εσωτερικού δικτύου. Έτσι οποιαδήποτε εφαρμογή που εκτελείται στο εσωτερικό δίκτυο και απαιτεί μονοπάτι

δρομολόγησης προς τα εξωτερικά συστήματα μέσω του Internet δεν μπορεί να λειτουργήσει σε αυτό το περιβάλλον.

Τα προβλήματα αυτά περιορίζονται με την εκτέλεση πληρεξούσιου λογισμικού (proxy) στα Dual - Homed Gateway συστήματα τα οποία προωθούν τα πακέτα των εφαρμογών μεταξύ των δικτύων- διαδικτύων.

Το λογισμικό αυτό ελέγχει τη συνδιαλλαγή μεταξύ των διεργασιών του πελάτη (client) και του εξυπηρετητή (server) της υπηρεσίας σε ένα παρόμοιο περιβάλλον. Έτσι, αντί να επικοινωνούν απευθείας ο πελάτης με τον εξυπηρετητή μεσολαβεί η πληρεξούσια (proxy) εφαρμογή, η οποία συνήθως εκτελείται στο ίδιο το bastion host. Επιδιώκεται το πληρεξούσιο (proxy) λογισμικό να είναι διαφανές στους χρήστες (Paschos et al, 2006).

Ωστόσο το πληρεξούσιο (proxy) λογισμικό που εκτελείται στο bastion host δεν επιτρέπει την ελεύθερη ροή πακέτων για συγκεκριμένες υπηρεσίες. Τα περισσότερα απ' αυτά μπορούν να παραμετροποιηθούν με τέτοιο τρόπο ώστε να εμποδίζουν ή να προωθούν τα πακέτα με κριτήριο την προέλευση ή τον προορισμό τους. Ακόμη μπορούν να εκτελέσουν διαδικασίες βασισμένες ακόμη και σε κρυπτογράφηση ή passwords.

Η χρήση πληρεξούσιων (proxy) εφαρμογών στο bastion host, μπορεί να σημαίνει ότι ο διαχειριστής του firewall θα πρέπει να εγκαθιστά «πελάτες» clients που θα αντικαταστήσουν τους συμβατικούς «πελάτες» δικτύωσης. Πρέπει να τονιστεί ότι αυτό είναι πραγματικό φορτίο τόσο για το διαχειριστή όσο και για το χρήστη, ειδικά σε ετερογενή περιβάλλοντα, εκείνα δηλαδή που περιλαμβάνουν πλατφόρμες διαφορετικών λειτουργικών συστημάτων. Γενικά, αυτό που χαρακτηρίζει λοιπόν τα Dual - Homed Gateway firewall είναι η υποχρεωτική χρήση πληρεξούσιων (proxy) προγραμμάτων.

3.5.3. ΤΟ SCREENED - HOST GATEWAY

Το Screened - Host Gateway είναι μια αρχιτεκτονική firewall που αποτελείται από τουλάχιστον ένα δρομολογητή και ένα bastion host με ένα interface δικτύου (Μπούρας , 2009).

Ο δρομολογητής είναι τυπικά παραμετροποιημένος να περιορίζει όλη την

κίνηση προς το εσωτερικό δίκτυο έτσι ώστε το bastion host να είναι το μοναδικό σύστημα που μπορεί να πλησιάσει κάποιος που βρίσκεται εκτός. Σε αντίθεση με το Dual - Homed Gateway, η εν λόγω τοπολογία δεν υποχρεώνει τη διέλευση όλης της κίνησης από το bastion host.

Παραμετροποιώντας το δρομολογητή παρέχεται η δυνατότητα στον διαχειριστή να καθορίσει διόδους στο firewall προς τα άλλα συστήματα του εσωτερικού δικτύου. Το bastion host σ' αυτή την τοπολογία προστατεύεται από το εξωτερικό δίκτυο από το δρομολογητή.

Το κυριότερο μειονέκτημα αυτής της τοπολογίας αυτής είναι ότι εμποδίζει την αμφίδρομη απευθείας επικοινωνία (Direct IP traffic). Αυτό επαληθεύεται και από τους χρήστες του δικτύου αλλά περισσότερο από αυτούς που επιχειρούν να παρέχουν υπηρεσίες σε χρήστες εκτός του εσωτερικού δικτύου.

Έτσι οποιαδήποτε εφαρμογή που εκτελείται στο εσωτερικό δίκτυο και απαιτεί μονοπάτι δρομολόγησης προς τα εξωτερικά συστήματα μέσω του Internet δεν μπορεί να λειτουργήσει σε αυτό το περιβάλλον.

Το Dual - Homed Gateway σύστημα που αναφέρθηκε στη προηγούμενη ενότητα περιορίζει τα συγκεκριμένα αυτά προβλήματα με την εκτέλεση πληρεξούσιου λογισμικού (proxy) το οποίο προωθεί τα πακέτα των εφαρμογών μεταξύ των δικτύων- διαδικτύων.

3.5.4 Εμπόδια για τους παροχής υπηρεσιών

Όταν κάποιος προσπαθήσει να χρησιμοποιήσει και ακόμη περισσότερο να εγκαταστήσει μια υπηρεσία σε σύστημα ενός συστήματος firewall, θα συναντήσει πλήθος προβλημάτων. Καταρχήν θα πρέπει να ακολουθήσει την πολιτική ασφαλείας της δεδομένης εγκατάστασης. Αυτό σημαίνει την αποφυγή προσθηκών ή μεταβολών με σκοπό την υποστήριξη της υπηρεσίας.

Η υψηλή τεχνογνωσία σχετικά με τον τρόπο με τον οποίο η υπηρεσία επικοινωνεί με τους πελάτες (clients) είναι επίσης πολύ σημαντική. Έτσι είναι απαραίτητη η γνώση της διεύθυνσης προς την οποία γίνεται κάθε σύνδεση, το χρησιμοποιούμενο πρωτόκολλο και η λειτουργία των ενδεχομένως πρόσθετων συνδέσεων που διεξάγονται κατά την επικοινωνία (Wood, 2006).

Ακόμη πρέπει να καθορίσει τη σωστή τοποθέτησή της, καθώς και τα επίπεδα πρόσβασης της υπηρεσίας. Βασικό κριτήριο στα παραπάνω αποτελεί η χρησιμοποιούμενη τοπολογία και οι δυνατότητες παραμετροποίησης του firewall. Έτσι στην περίπτωση της Dual - Homed τοπολογίας το πληρεξούσιο λογισμικό (proxy) μπορεί να ρυθμιστεί ώστε να απαγορεύει την πρόσβαση ανάλογα με το χρήστη, τη σύστημα ή το δίκτυο, ενώ στην Screened - Subnet τοπολογία ο δρομολογητής μπορεί να λειτουργήσει παρόμοια εκτός από τη διάκριση κατά χρήστη (διότι οι δρομολογητές ως συσκευές, λειτουργούν σε επίπεδο δικτύου σύμφωνα με το μοντέλο OSI/ISO).

Έχοντας εξασφαλίσει τις προηγούμενες συνθήκες λειτουργίας θα πρέπει να γίνεται επιπλέον καταγραφή της κίνησης της υπηρεσίας σε ένα ασφαλές από τους κινδύνους του Internet σύστημα. Μια πιθανή τακτική είναι η εκτύπωση των ύποπτων κινήσεων κατά την πραγματοποίησή τους, από κάποια αυτοματοποιημένη διαδικασία. Αυτό μας εξασφαλίζει από την περίπτωση που ο εισβολέας θα καταστρέψει αργότερα τα αρχεία καταγραφής. Ακόμα πιο δραστικό θα ήταν ο αυτόματος περιορισμός λειτουργίας του συστήματος, ή και του δικτύου αμέσως μετά την καταγραφή ύποπτης.

3.6. CHECKPOINT FIREWALL

Οι σημερινές επιχειρήσεις ολοένα και περισσότερο αντιμετωπίζουν την ανάγκη της άμεσης σύνδεσης των προμηθευτών, συνεργατών, πελατών καθώς και απομακρυσμένων χρηστών τους με τα κεντρικά γραφεία της εκάστοτε επιχείρησης. Μέσω του διαδικτύου, αυτή η ανάγκη γίνεται πραγματικότητα καθώς το Internet είναι «ανοιχτό», προσβάσιμο από παντού και προσφέρει σημαντικά πλεονεκτήματα από άποψης κόστους. Καθίσταται, άρα, προφανές ότι τα χαρακτηριστικά ενός τέτοιου συστήματος θα πρέπει να εξισορροπηθούν με την ανάγκη προστασίας και ακεραιότητας των ευαίσθητων επιχειρησιακών επικοινωνιών.

Ως συνέπεια όλων των παραπάνω, οι οργανισμοί ανά τον κόσμο θα πρέπει να εξασφαλίσουν και να μπορούν να εγγυηθούν για την ασφάλεια και διαθεσιμότητα των δικτυακών τους πηγών και δεδομένων.

Κάτι τέτοιο, παρόλο αυτά, προϋποθέτει μια ολοκληρωμένη λύση

ασφαλείας που θα είναι σε θέση να προστατέψει όλα τα επιμέρους στοιχεία ενός οργανισμού (δίκτυα, συστήματα, εφαρμογές και χρήστες). Η αρχιτεκτονική Ασφαλούς Εικονικού Δικτύου του Checkpoint μπορεί να εξασφαλίσει τη δικτυακή ασφάλεια από άκρο σε άκρο, δίνοντας παράλληλα τη δυνατότητα στις επιχειρήσεις να εγγυηθούν για την προστασία της επιχειρησιακά κρίσιμης κυκλοφορίας και επικοινωνίας του οργανισμού τόσο εσωτερικά όσο και με τον έξω κόσμο.

Πιο συγκεκριμένα, το Checkpoint αποτελεί βασικό στοιχείο της αρχιτεκτονικής SVN και επιτρέπει να διαχειρίζεται η δικτυακή ασφάλεια μέσω μιας κοινής πολιτικής ασφαλείας για ολόκληρο τον οργανισμό. Μπορεί να εγγυηθεί για την ασφάλεια του δικτύου οποιασδήποτε επιχείρησης και μας προσφέρει πολλά παραπάνω από κανόνες που ελέγχουν απλά την πρόσβαση και την κυκλοφορία σε ένα προστατευμένο δίκτυο. Πιο συγκεκριμένα, το Firewall-1 είναι μια ολοκληρωμένη πλατφόρμα ασφαλείας που ενσωματώνει και διαχειρίζεται όλα τα στοιχεία της επιχείρησης, όπως (Schneier, 2007).:

1. Έλεγχο πρόσβασης (Access Control).
2. Πιστοποίηση χρηστών (User Authentication).
3. Απόκρυψη εσωτερικών διευθύνσεων (Network Address Translation).
4. Εικονικά Προσωπικά Δίκτυα (Virtual Private Networks).
5. Υψηλή Διαθεσιμότητα (High Availability).
6. Ασφάλεια περιεχομένου (Content Security - anti-virus, URL and Java/ActiveX screening).
7. Παρακολούθηση και Αναφορές (Auditing and Reporting).
8. Διαχείριση χρηστών μέσω LDAP (LDAP-based User Management).
9. Έλεγχο Εισβολής (Intrusion Detection - Malicious Activity Detection).
10. Διαχείριση Συσκευών άλλων κατασκευαστών (Third-Party Device Management)

Επιπλέον, η επιχειρησιακή ασφάλεια εκτείνεται ακόμα περισσότερο μέσω του Open Platform for Security (OPSEC) που ενσωματώνει το Firewall-1, προσφέροντας κεντρική διαχείριση συμπληρωματικών εφαρμογών και υπηρεσιών ασφαλείας.

Το Firewall-1 της Checkpoint υποστηρίζει περισσότερες από 200 προκαθορισμένες εφαρμογές, υπηρεσίες και πρωτόκολλα. Συγκεκριμένα, υπάρχει υποστήριξη για όλες τις γνωστές υπηρεσίες του διαδικτύου, συμπεριλαμβάνοντας εφαρμογές HTTP, SMTP, Telnet, FTP κλπ. Επίσης, υποστηρίζεται όλη την «οικογένεια» εφαρμογών TCP καθώς και connectionless πρωτόκολλα όπως UDP. Τέλος, σημαντικές επιχειρησιακές εφαρμογές (εφαρμογές πολυμέσων όπως Real-Audio και υπηρεσίες H.323, Voice over IP (VoIP), κλπ.) καθώς και βάσεις δεδομένων όπως Oracle SQL μπορούν να διαχειριστούν μέσα από το Firewall-1.

Ένα χαρακτηριστικό του Firewall-1 είναι η scripting γλώσσα που ενσωματώνει με τη βοήθεια της οποίας υποστηρίζεται οποιαδήποτε custom εφαρμογή. Η δυνατότητα αυτή κάνει το Firewall-I εύκολα προσαρμόσιμο σε οποιαδήποτε ειδική ανάγκη του οργανισμού καθώς και σε συνεχώς εξελίξιμες ανάγκες ασφαλείας ώστε να ικανοποιεί τελικά ακόμα και τις πιο απαιτητικές ανάγκες ασφαλείας.

Περαιτέρω, θα πρέπει να σημειωθεί ότι το Firewall-1 βασίζεται σε Stateful Inspection, τεχνολογία που έχει εφευρεθεί από την Check Point Software Technologies (U.S. Patent No. 5,606,668 and 5,835,716). Η τεχνολογία του Stateful Inspection παρέχει το υψηλότερο πιθανό επίπεδο ασφαλείας ενσωματώνοντας έλεγχο τόσο σε επίπεδο communication όσο και σε επίπεδο application. Πιο συγκεκριμένα, εξομοιώνει την τεχνολογία ενός application firewall έχοντας τη δυνατότητα να διαχειριστεί πακέτα στο application layer χωρίς όμως να χρειάζεται ένα ξεχωριστό proxy για κάθε υπηρεσία (service).

Αυτό έχει σαν αποτέλεσμα τη βελτίωση της απόδοσης και της κλιμάκωσης καθώς και τη δυνατότητα υποστήριξης νέων και custom εφαρμογών γρήγορα και εύκολα. Αυτοί είναι κατ' ουσία μερικοί από τους λόγους για τους οποίους η τεχνολογία Stateful Inspection έχει υιοθετηθεί και προτιμάται από τους περισσότερους οργανισμούς που αποφασίζουν να προχωρήσουν σε μια αυστηρή αλλά παράλληλα ευέλικτη πολιτική ασφαλείας.

Εκτός όμως από τα παραπάνω, το προϊόν ενσωματώνει και αρκετές ακόμα λειτουργίες. Το NAT (Network Address Translation) για παράδειγμα, είναι ένα χαρακτηριστικό του προγράμματος που βοηθά στη απόκρυψη των εσωτερικών διευθύνσεων του δικτύου από το Internet, αποφεύγοντας με αυτόν τον τρόπο την

αποκάλυψη σημαντικών πληροφοριών στο έξω κόσμο. Εκτός όμως από τη βελτίωση της επιχειρησιακής ασφάλειας, η λειτουργία NAT εξασφαλίζει τη δυνατότητα να διατηρηθούν εσωτερικά οι κατοχυρωμένες σε κάποιον ISP εσωτερικές IP διευθύνσεις δίνοντας παράλληλα πρόσβαση στο διαδίκτυο σε όλους τους χρήστες του δικτύου κάνοντας χρήση μίας μόνο κατοχυρωμένης IP διεύθυνσης. Επιπλέον, οι κανόνες που αφορούν στο NAT δημιουργούνται αυτόματα από πληροφορίες που παρέχονται κατά τη διαδικασία του ορισμού των αντικειμένων του δικτύου μας. Κάτι τέτοιο, όπως είναι προφανές, καθιστά την υλοποίηση του NAT μια απλή και γρήγορη διαδικασία.

Βασικό στοιχείο για τα VPN’s είναι η διαδικασία με την οποία γίνεται η πιστοποίηση των χρηστών που περνούν μέσα από το firewall (User Authentication). Τα δίκτυα των επιχειρήσεων δεν περιλαμβάνουν μόνο εσωτερικούς χρήστες οι οποίοι θα πρέπει να πιστοποιηθούν ώστε να έχουν πρόσβαση στο διαδίκτυο αλλά και απομακρυσμένους χρήστες οι οποίοι είτε χρησιμοποιώντας φορητά τερματικά είτε από διαφορετικές κάθε φορά τοποθεσίες προσπαθούν να συνδεθούν στο τοπικό δίκτυο της εταιρείας. Προτού, τους χορηγηθεί άδεια πρόσβασης στους ευαίσθητους πόρους του δικτύου, ο εκάστοτε οργανισμός θα πρέπει να έχει ένα μηχανισμό πιστοποίησης τους.

Το Firewall-1 ανταποκρίνεται στην παραπάνω ανάγκη μια και υποστηρίζει την πιστοποίηση των χρηστών με τρεις διαφορετικές μεθόδους (User Authentication, Client Authentication, Session Authentication), καθώς και πολλαπλά σχήματα πιστοποίησης, περισσότερα από οποιονδήποτε άλλο κατασκευαστή. Οι χρήστες μπορούν να πιστοποιηθούν χωρίς να γίνει καμία αλλαγή τόσο στο server όσο και στον client. Θα πρέπει να σημειωθεί στο σημείο αυτό, ότι το Firewall-1 μπορεί να πιστοποιήσει τους χρήστες οποιασδήποτε IP-based εφαρμογής. Η πιστοποίηση των χρηστών γίνεται με κωδικούς πρόσβασης (password), smart cards, token-based προϊόντα όπως το SecurelD, LDAP-stored κωδικούς πρόσβασης, authentication servers όπως RADIUS ή TACACS+, ψηφιακά πιστοποιητικά X. 5 09, ακόμα και με τις νέες βιομετρικές μεθόδους. Επιπλέον, το προϊόν ενσωματώνει μεθόδους (API) που καθιστούν εφικτή τη συμβατότητα του με προϊόντα πιστοποίησης άλλων κατασκευαστών.

Η πιστοποίηση των χρηστών (User Authentication) στο Firewall-1 γίνεται τελείως διάφανα για χρήστες των υπηρεσιών Telnet, FTP, HTTP και RLOGIN.

Αυτό σημαίνει ότι όταν χρήστης ζητά να συνδεθεί κατευθείαν με το δικτυακό πόρο που επιθυμεί και όχι με το firewall. Κατά τη διαδικασία της σύνδεσης, το Firewall-1 αυτόματα διακόπτει τη σύνδεση και ζητά από τους χρήστες να πιστοποιήσουν την ταυτότητα τους, αν βέβαια κάτι τέτοιο απαιτείται από το πρόγραμμα το οποίο χρησιμοποιούν.

Κεφάλαιο 4ο ISO 20000

4.1 Γενικά

Το ISO/IEC 20000 είναι διεθνές πρότυπο με στόχο τη Διαχείριση Παροχής Υπηρεσιών Πληροφορικής (ΔΠΥΠ-ITSM) που αφορά ένα πλήρες σύστημα διεργασιών διαχείρισης. Εφόσον ο πρωταρχικός σκοπός λειτουργικότητας ενός οργανισμού είναι η παροχή υπηρεσιών πληροφορικής οπότε και η πιστοποίηση κατά ISO/IEC 20000 είναι απαραίτητη (Dugmore, 2006).

Το ISO/IEC 20000 εστιάζει μόνο στις διεργασίες παροχής υπηρεσιών πληροφορικής, και στο διαχειριστικό σύστημα που τις υποστηρίζει. Παρέχει ένα εμπεριστατωμένο, σύστημα διαχείρισης, δίνοντας τη δυνατότητα να βελτιώσει τις υπηρεσίες του.

Το πρότυπο εστιάζει στους εταιρικούς ελέγχους που καλύπτουν τα όποια ρίσκα, πόρους κτλ.

Το ISO/IEC 20000 είναι ιδανικό για κάθε οργανισμό, από κάθε εργασιακό χώρο με πρότυπο είναι ιδιαίτερα κατάλληλο για εσωτερικούς (μέσα στον οργανισμό) παρόχους υπηρεσιών πληροφορικής, όπως τμήματα πληροφορικής, και εξωτερικούς παρόχους υπηρεσιών πληροφορικής, όπως εταιρείες παροχής υπηρεσιών

Τα πλεονεκτήματα του ISO 20000 αναφορικά με την ασφάλεια των πληροφοριακών συστημάτων είναι τα εξής (ISO/IEC 20000):

1. Καλύτερη ποιότητα των εταιρικών λειτουργιών
2. Οι πελάτες ξέρουν τι να περιμένουν από τον εκάστοτε οργανισμό
3. Αποδεκτά κόστη για την υποδομή πληροφορικής
4. Η επίγνωση στον οργανισμό για τις υπηρεσίες πληροφορικής επιτρέπουν τη καλύτερη χρήση μέσω.
5. Η αυξημένη επίγνωση των εταιρικών αναγκών διευκολύνει καινοτόμες προσεγγίσεις.
6. Βελτιωμένη ικανότητα στην αναγνώριση αλλαγών τάσεων

7. Βελτιωμένη ικανότητα μετρήσεων

Οι εθνικοί οργανισμοί που είναι μέλη του ISO ή IEC συμμετέχουν στην ανάπτυξη διεθνών προτύπων μέσω τεχνικών επιτροπών που έχουν συσταθεί από την αντίστοιχη οργάνωση για να ασχοληθεί με τα εν λόγω πεδία της τεχνικής δραστηριότητας. Οι ISO και IEC Τεχνικές Επιτροπές συνεργάζονται σε τομείς αμοιβαίου ενδιαφέροντος.

Οι απαιτήσεις του ISO/IEC 20000-1:2011 (Part 1) αφορούν το σχεδιασμό, τη μετάβαση, που πληρούν τις απαιτήσεις και παρέχουν αξία στον πελάτη και τον πάροχο υπηρεσιών.

Η λειτουργία των φάσεων που ορίζονται στο παρόν τμήμα του ISO / IEC 20000 απαιτεί από το προσωπικό να είναι καλά οργανωμένο και συντονισμένο. Κατάλληλα εργαλεία μπορούν να χρησιμοποιηθούν για να μπορέσουν οι διεργασίες να είναι αποτελεσματικές και αποδοτικές.

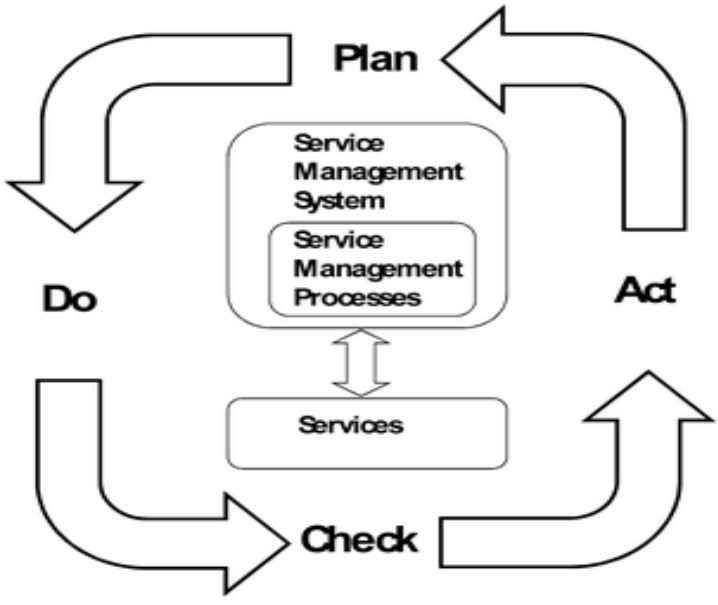
Οι πιο αποτελεσματικοί πάροχοι υπηρεσιών εξετάζουν τον αντίκτυπο των SMS σε όλα τα στάδια του κύκλου ζωής της υπηρεσίας, από τη στρατηγική του σχεδιασμού, τη μετάβαση και τη λειτουργία, συμπεριλαμβανομένης της συνεχούς βελτίωσης.

Αυτό το τμήμα του ISO / IEC 20000 απαιτεί την εφαρμογή της μεθοδολογίας που είναι γνωστή ως "Plan-Do-Check-Act» (PDCA) σε όλα τα μέρη του SMS και των υπηρεσιών. Η μεθοδολογία PDCA, όπως εφαρμόζεται σε αυτό το τμήμα του ISO / IEC 20000, μπορεί να περιγραφεί εν συντομία ως εξής (Dugmore, 2006a):

1. Σχέδιο: την ίδρυση, την τεκμηρίωση και τη συμφωνία των SMS. Το SMS περιλαμβάνει τις πολιτικές, τους στόχους, τα σχέδια και τις διαδικασίες για να πληρούν τις απαιτήσεις των υπηρεσιών.
2. Εφαρμογή: την εφαρμογή και τη λειτουργία των SMS για το σχεδιασμό, τη μετάβαση, την παράδοση και τη βελτίωση των υπηρεσιών.
3. Έλεγχος: την παρακολούθηση, μέτρηση και τον έλεγχο των SMS και των υπηρεσιών κατά τις πολιτικές, τους στόχους, τα σχέδια και τις απαιτήσεις των υπηρεσιών και την αναφορά των αποτελεσμάτων.

4. Πράξη: λήψη μέτρων για την συνεχή βελτίωση των επιδόσεων των SMS και των υπηρεσιών. Όταν χρησιμοποιείται μέσα σε ένα SMS, οι παρακάτω είναι οι πιο σημαντικές πτυχές μιας ολοκληρωμένης προσέγγισης της διαδικασίας και της μεθοδολογίας PDCA: α) η κατανόηση και η εκπλήρωση των απαιτήσεων των υπηρεσιών για την επίτευξη της ικανοποίησης των πελατών, β) ο καθορισμός της πολιτικής και των στόχων για τη διαχείριση των υπηρεσιών, γ) ο σχεδιασμός και η παροχή υπηρεσιών με βάση τα SMS που προσθέτουν αξία για τον πελάτη, δ) η παρακολούθηση, μέτρηση και η επανεξέταση των επιδόσεων των SMS και των υπηρεσιών, ε) η συνεχής βελτίωση τα SMS και οι υπηρεσίες που βασίζονται σε αντικειμενικές μετρήσεις.

Το Σχήμα 4.1 απεικονίζει το πώς η μεθοδολογία PDCA μπορεί να εφαρμοστεί στα SMS, συμπεριλαμβανομένων των διαδικασιών διαχείρισης υπηρεσιών που προσδιορίζονται στα σημεία 5 έως 9, και τις υπηρεσίες. Κάθε στοιχείο της μεθοδολογίας PDCA είναι ένα ζωτικό μέρος μιας επιτυχούς εφαρμογής ενός SMS. Η διαδικασία βελτίωσης που χρησιμοποιείται σε αυτό το τμήμα του ISO / IEC 20000 βασίζεται στη μεθοδολογία PDCA.



Σχήμα 4.1 -PDCA μεθοδολογία που εφαρμόζεται για τη διαχείριση των υπηρεσιών

Πηγή: Dugmore, J. (2006a). "BS 15000 to ISO/IEC 20000 What difference does it make?". *ITNOW* 48 (3): 30.

Αυτό το τμήμα του ISO / IEC 20000 επιτρέπει σε ένα φορέα παροχής υπηρεσιών να ενσωματώσει το SMS του με άλλα συστήματα διαχείρισης στην οργάνωση του φορέα παροχής υπηρεσιών. Η υιοθέτηση μιας ολοκληρωμένης προσέγγισης της διαδικασίας και της μεθοδολογίας PDCA επιτρέπει στον πάροχο υπηρεσιών να ευθυγραμμίσει ή να ενσωματώσει πλήρως πολλαπλά πρότυπα συστημάτων διαχείρισης. Για παράδειγμα, ένα SMS μπορεί να ενσωματωθεί με ένα σύστημα διαχείρισης ποιότητας με βάση το πρότυπο ISO 9001 ή της ασφάλειας των πληροφοριών του συστήματος διαχείρισης με βάση το πρότυπο ISO / IEC 27001.

Το ISO / IEC 20000 είναι σκόπιμα ανεξάρτητο από συγκεκριμένες κατευθύνσεις. Ο φορέας παροχής υπηρεσιών μπορεί να χρησιμοποιήσει ένα συνδυασμό με γενικά αποδεκτές οδηγίες και τη δική του εμπειρία.

Οι χρήστες ενός διεθνούς προτύπου είναι υπεύθυνοι για την ορθή εφαρμογή του. Ένα διεθνές πρότυπο δεν φιλοδοξεί να περιλαμβάνει όλες τις απαραίτητες νομικές και κανονιστικές απαιτήσεις και τις συμβατικές υποχρεώσεις του παρόχου υπηρεσιών. Συμμόρφωση προς ένα διεθνές πρότυπο δεν παρέχει ασυλία από νομικές και κανονιστικές απαιτήσεις.

Για τους σκοπούς της έρευνας για τα πρότυπα διαχείρισης των υπηρεσιών, οι χρήστες ενθαρρύνονται να μοιραστούν τις απόψεις τους σχετικά με το πρότυπο ISO / IEC 20000-1 και τις προτεραιότητές τους για τις αλλαγές στο υπόλοιπο του ISO / IEC 20000 σειρά (ISO/IEC 20000).

4.2 Σκοπός

4.2.1 Γενικά

Αυτό το τμήμα του ISO / IEC 20000 είναι ένα πρότυπο σύστημα διαχείρισης της υπηρεσίας (SMS). Διευκρινίζει τις απαιτήσεις για τον πάροχο υπηρεσιών για το σχεδιασμό, τη δημιουργία, την υλοποίηση, τη λειτουργία, την παρακολούθηση, αναθεώρηση, τη συντήρηση και τη βελτίωση ενός SMS. Οι απαιτήσεις περιλαμβάνουν το σχεδιασμό, τη μετάβαση, την παράδοση και τη βελτίωση των υπηρεσιών για να καλύψει τις ανάγκες των υπηρεσιών. Αυτό το τμήμα του ISO / IEC 20000 μπορούν να χρησιμοποιηθεί από (Dugmore,

J2006a):

α) μια οργάνωση που αναζητά υπηρεσίες από τους παρόχους υπηρεσιών και απαιτεί διασφάλιση ότι οι ανάγκες των υπηρεσιών της θα πρέπει να πληρούνται

β) μια οργάνωση που απαιτεί μια συνεκτική προσέγγιση από όλους τους παρόχους υπηρεσιών της, συμπεριλαμβανομένων εκείνων σε μια αλυσίδα εφοδιασμού

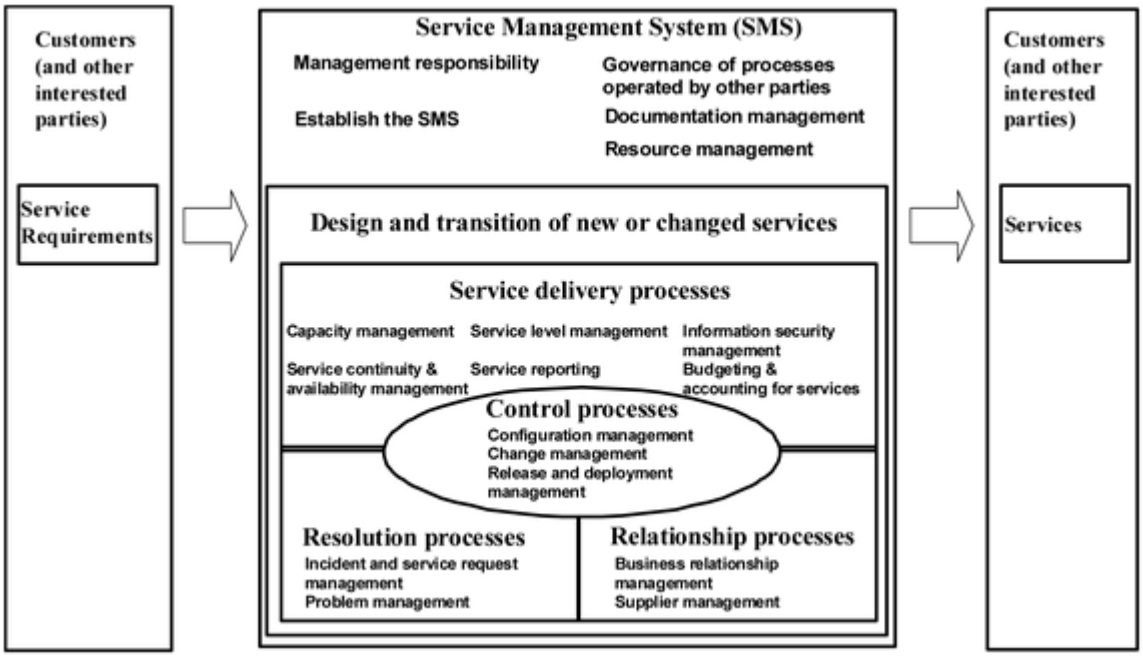
γ) έναν πάροχο υπηρεσιών που σκοπεύει να αποδείξει την ικανότητά του για το σχεδιασμό, τη μετάβαση, την παράδοση και τη βελτίωση υπηρεσιών που πληρούν τις απαιτήσεις των υπηρεσιών

δ) έναν πάροχο υπηρεσιών για την παρακολούθηση, μέτρηση και αναθεώρηση των διαδικασιών διαχείρισης των υπηρεσιών

ε) έναν πάροχο υπηρεσιών για τη βελτίωση του σχεδιασμού, της μετάβασης και την παροχή υπηρεσιών μέσω της αποτελεσματικής εφαρμογής και λειτουργίας του

στ) έναν αξιολογητή ή ελεγκτή, όπως τα κριτήρια για την αξιολόγηση της συμμόρφωσης ενός παρόχου υπηρεσιών προς τις απαιτήσεις σε αυτό το μέρος του ISO / IEC 20000.

Το σχήμα 4.2 απεικονίζει ένα SMS, συμπεριλαμβανομένων των διαδικασιών διαχείρισης υπηρεσιών. Οι διαδικασίες διαχείρισης των υπηρεσιών και οι σχέσεις μεταξύ των διαδικασιών μπορούν να υλοποιηθούν με διαφορετικούς τρόπους από διάφορους φορείς παροχής υπηρεσιών. Η φύση της σχέσης μεταξύ ενός παρόχου υπηρεσιών και του πελάτη θα επηρεάσει το πώς εφαρμόζονται οι διαδικασίες διαχείρισης υπηρεσιών.



Σχήμα 4.2-Σύστημα διαχείρισης υπηρεσιών (SMS)

Πηγή: Dugmore, J. (2006a). "BS 15000 to ISO/IEC 20000 What difference does it make?". *ITNOW* 48 (3): 30.

4.2.2 Εφαρμογή

Όλες οι απαιτήσεις σε αυτό το τμήμα του ISO / IEC 20000 είναι γενικές και προορίζονται για εφαρμογή σε όλους τους παρόχους υπηρεσιών, ανεξάρτητα από τον τύπο, το μέγεθος και τη φύση των παρεχόμενων υπηρεσιών. Αποκλεισμός οποιασδήποτε από τις απαιτήσεις στις ρήτρες 4 έως 9 δεν είναι αποδεκτή όταν ένας πάροχος υπηρεσιών ισχυρίζεται συμμόρφωση προς αυτό το τμήμα του ISO / IEC 20000, ανεξάρτητα από τη φύση της οργάνωσης του φορέα παροχής υπηρεσιών.

Συμμόρφωση προς τις απαιτήσεις του άρθρου 4 μπορεί να αποδειχθεί μόνο από πάροχο υπηρεσιών μαρτυρούν την εκπλήρωση όλων των απαιτήσεων του άρθρου 4. Ένας πάροχος υπηρεσιών δεν μπορεί να επικαλεστεί στοιχεία της διακυβέρνησης των διαδικασιών που λειτουργούν από τρίτους για τις απαιτήσεις του άρθρου 4.

Συμμόρφωση προς τις απαιτήσεις των άρθρων 5 έως 9 μπορεί να αποδειχθεί από τον πάροχο υπηρεσιών με την εκπλήρωση όλων των

απαιτήσεων. Εναλλακτικά, ο πάροχος υπηρεσιών μπορεί να αποδείξει την εκπλήρωση της πλειοψηφίας των απαιτήσεων τους και τα αποδεικτικά στοιχεία της διακυβέρνησης των διαδικασιών που λειτουργούν από τρίτους για αυτές τις διαδικασίες, ή τμήματα διαδικασιών, ότι ο πάροχος υπηρεσιών δεν λειτουργεί άμεσα.

Το πεδίο εφαρμογής του παρόντος μέρους του ISO / IEC 20000 αποκλείει τις προδιαγραφές για ένα προϊόν ή εργαλείο. Ωστόσο, οι οργανισμοί μπορούν να χρησιμοποιούν αυτό το τμήμα του ISO / IEC 20000 για να τους βοηθήσει να αναπτύξουν τα προϊόντα ή τα εργαλεία που υποστηρίζουν τη λειτουργία ενός (ISO/IEC 20000).

4.3 Όροι και ορισμοί

Η ικανότητα μιας υπηρεσίας ή ενός συστατικού μιας υπηρεσίας να εκτελέσει την απαιτούμενη λειτουργία του σε συμφωνημένη στιγμή ή κατά τη διάρκεια μιας συμφωνημένης χρονικής περιόδου. Η Διαθεσιμότητα συνήθως εκφράζεται ως αναλογία ή το ποσοστό του χρόνου που η συνιστώσα των υπηρεσιών ή η υπηρεσία είναι πράγματι διαθέσιμη για χρήση από τον πελάτη στον συμφωνηθέντα χρόνο ότι η υπηρεσία πρέπει να είναι διαθέσιμη. Η Βασική ρύθμιση παραμέτρων αναφέρετε σε πληροφορίες διαμόρφωσης που έχουν ορισθεί επισήμως σε μια συγκεκριμένη χρονική στιγμή κατά τη διάρκεια μιας υπηρεσίας ή τη ζωή μιας συνιστώσας των υπηρεσιών του

Το CI αποτελεί στοιχείο που πρέπει να ελέγχεται, προκειμένου να παραδώσει μια υπηρεσία ή υπηρεσίες. Το CMDB εστιάζει στην αποθήκευση δεδομένων που χρησιμοποιούνται για την καταγραφή των χαρακτηριστικών στοιχείων διαμόρφωσης και τις σχέσεις μεταξύ των στοιχείων διαμόρφωσης, καθόλη τη διάρκεια ζωής τους. Παρακάτω παραθέτονται επιπρόσθετοι ορισμοί, οι οποίοι είναι οι ακόλουθοι (ISO/IEC 20000):

1. Συνεχή βελτίωση: Επαναλαμβανόμενη δραστηριότητα για την αύξηση της ικανότητας να εκπληρώσει τις απαιτήσεις της υπηρεσίας
2. Διορθωτικά μέτρα: Δράση για την εξάλειψη της αιτίας ή τη μείωση της πιθανότητας επανάληψης μιας εντοπισμένης μη συμμόρφωσης ή άλλης

ανεπιθύμητης κατάστασης

3. Πελάτης: Μια οργάνωση ή μέρος μιας οργάνωσης που λαμβάνει μια υπηρεσία ή υπηρεσίες. Ένας πελάτης μπορεί να είναι εσωτερική ή εξωτερική οργάνωσης του φορέα παροχής υπηρεσιών .

4. Έγγραφο: Πληροφορίες και τα αποδεικτικό μέσο της. Οι πολιτικές, τα σχέδια, οι περιγραφές της διαδικασίας, τις διαδικασίες, συμφωνίες επιπέδου υπηρεσιών, συμβάσεις ή αρχεία. Η τεκμηρίωση μπορεί να είναι σε οποιαδήποτε μορφή ή το είδος του μέσου. Στο ISO / IEC 20000, έγγραφα, εκτός από τα αρχεία, δείχνουν την πρόθεση που πρόκειται να επιτευχθεί.

5. Αποτελεσματικότητα: Ο βαθμός στον οποίο πραγματοποιούνται οι προγραμματισμένες δραστηριότητες και επιτυγχάνονται τα αποτελέσματα

6. Περιστατικό: Η μη-προγραμματισμένη διακοπή μιας υπηρεσίας, η μείωση της ποιότητας μιας υπηρεσίας ή ενός γεγονότος που δεν έχει ακόμη επηρεάσει την εξυπηρέτηση του πελάτη

4.4 Ασφάλεια των πληροφοριών

Η Διατήρηση της εμπιστευτικότητας, της ακεραιότητας και της προσβασιμότητας των πληροφοριών. Επιπλέον, άλλες ιδιότητες όπως η αυθεντικότητα, η λογοδοσία, μη άρνηση και η αξιοπιστία μπορεί να συμπεριληφθούν.

Ο όρος "διαθεσιμότητα" δεν έχει χρησιμοποιηθεί σε αυτόν τον ορισμό, γιατί είναι ένας όρος που ορίζεται σε αυτό το τμήμα του ISO / IEC 20000 το οποίο δεν θα ήταν κατάλληλο για τον ορισμό αυτό .

Το Περιστατικό ασφάλειας πληροφορίας, αποτελεί ένα μεμονωμένο ή μια σειρά από ανεπιθύμητα ή απρόβλεπτα συμβάντα ασφάλειας των πληροφοριών που έχουν σημαντική πιθανότητα να θέτουν σε κίνδυνο τις επιχειρηματικές δραστηριότητες και απειλεί την ασφάλεια των πληροφοριών. Το Ενδιαφερόμενο μέρος είναι ένα άτομο ή ομάδα που έχει ένα ιδιαίτερο ενδιαφέρον για την απόδοση ή την επιτυχία της δραστηριότητας ή των

δραστηριοτήτων του φορέα παροχής υπηρεσιών. Οι πελάτες, οι ιδιοκτήτες, η διαχείριση, οι άνθρωποι στην οργάνωση, οι προμηθευτές του φορέα παροχής υπηρεσιών, οι τραπεζίτες, οι συνδικαλιστικές οργανώσεις ή οι εταίροι.

Η Εσωτερική ομάδα αποτελεί μέρος της οργάνωσης του φορέα παροχής υπηρεσιών που συνάπτει τεκμηριωμένη συμφωνία με τον πάροχο υπηρεσιών να συμβάλλει στο σχεδιασμό, τη μετάβαση, την παράδοση και τη βελτίωση της υπηρεσίας ή υπηρεσιών. Η εσωτερική ομάδα είναι εκτός του πεδίου εφαρμογής των SMS του φορέα παροχής υπηρεσιών. Ένα άλλο σημαίνον στοιχείο αποτελεί ένα γνωστό σφάλμα, το αποτελεί ένα πρόβλημα που έχει εντοπισμένη αιτία ή μια μέθοδος μείωσης ή εξάλειψης των επιπτώσεων του σε μια υπηρεσία μέσω της εργασίας γύρω από αυτό (ISO / IEC 20000).

Σημαίνον στοιχείο στην ασφάλεια των πληροφοριακών συστημάτων καθίσταται η οργάνωση η οποία είναι μια ομάδα ανθρώπων και εγκαταστάσεων, με διάταξη των ευθυνών, των αρχών και των σχέσεων. Ένα άλλο σημαίνον στοιχείο είναι η λεγόμενη Προληπτική δράση, η οποία αποτελεί μια δράση για την αποφυγή ή την εξάλειψη των αιτίων ή τη μείωση της πιθανότητας εμφάνισης μιας πιθανής μη συμμόρφωσης ή άλλων δυνητικών ανεπιθύμητων καταστάσεων. Παρακάτω παραθέτονται επίσης σημαίνοντες ορισμοί:

1. Πρόβλημα: Αιτία από ένα ή περισσότερα επεισόδια. Η αιτία δεν είναι συνήθως γνωστή κατά το χρόνο καταγραφής του προβλήματος και η διαδικασία διαχείρισης των προβλημάτων είναι υπεύθυνη για την περαιτέρω έρευνα .
2. Διαδικασία: Καθορισμένος τρόπος για την πραγματοποίηση μια δραστηριότητας ή διαδικασίας
3. Διεργασία: Το σύνολο των αλληλένδετων ή αλληλεπιδρώντων δραστηριοτήτων που μετατρέπει τις εισροές σε εκροές
4. Καταγραφή: Έγγραφο που αναφέρει αποτελέσματα που επιτεύχθηκαν ή παρέχει αποδείξεις δραστηριοτήτων που πραγματοποιήθηκαν
5. Απελευθέρωση: Συλλογή ενός ή περισσοτέρων νέων ή τροποποιημένων στοιχείων διαμόρφωσης που έχουν αναπτυχθεί στο

ζωντανό περιβάλλον ως αποτέλεσμα μίας ή περισσοτέρων αλλαγών

6. Αίτημα για αλλαγή: Πρόταση για μια αλλαγή που πρέπει να γίνει σε μια υπηρεσία, στοιχείο υπηρεσίας ή του συστήματος διαχείρισης των υπηρεσιών. Μια αλλαγή σε μια υπηρεσία περιλαμβάνει την παροχή μιας νέας υπηρεσίας ή την αφαίρεση μιας υπηρεσίας η οποία δεν είναι πλέον απαραίτητη .

7. Κίνδυνος: Επίδραση της αβεβαιότητας για τους στόχους. Ένα αποτέλεσμα είναι μια απόκλιση από την αναμενόμενη - θετική ή / και αρνητική. Οι στόχοι μπορούν να έχουν διαφορετικές πτυχές (όπως οικονομικούς στόχους, την υγεία και την ασφάλεια, και περιβαλλοντικούς στόχους) και μπορεί να εφαρμοστεί σε διαφορετικά επίπεδα (όπως στρατηγικά, σε ολόκληρο τον οργανισμό, το έργο, το προϊόν και τη διαδικασία) .

8. Υπηρεσία: Μέσο για την παροχή αξίας στον πελάτη, διευκολύνοντας τα αποτελέσματα που θέλει να επιτύχει ο πελάτης. Μια υπηρεσία μπορεί επίσης να παραδοθεί με τον παροχέα υπηρεσιών από έναν προμηθευτή, μιας εσωτερικής ομάδας ή ενός πελάτη που ενεργεί ως προμηθευτής.

9. Συνιστώσα των υπηρεσιών: Ενιαία μονάδα μιας υπηρεσίας που όταν συνδυάζεται με άλλες μονάδες θα παραδώσει μια πλήρη υπηρεσία.

10. Συνέχεια των υπηρεσιών: Δυνατότητα διαχείρισης των κινδύνων και των γεγονότων που θα μπορούσαν να έχουν σοβαρές επιπτώσεις σε μια υπηρεσία ή υπηρεσίες, προκειμένου να παραδώσει συνεχώς τις υπηρεσίες σε αποδεκτά επίπεδα

11. Σύμβαση Παροχής Υπηρεσιών: Τεκμηριωμένη σύμβαση μεταξύ του παρόχου υπηρεσιών και του πελάτη που προσδιορίζει τις υπηρεσίες και τους στόχους των υπηρεσιών. Μια συμφωνία σε επίπεδο υπηρεσιών μπορεί επίσης να καθοριστεί μεταξύ του παρόχου υπηρεσιών και του προμηθευτή, μιας εσωτερικής ομάδας ή ενός πελάτη που ενεργεί ως προμηθευτής .Μια συμφωνία σε επίπεδο υπηρεσιών μπορεί να συμπεριληφθεί σε μια σύμβαση ή άλλου τύπου τεκμηριωμένη σύμβαση .

12. Διαχείριση υπηρεσιών: Το σύνολο των δυνατοτήτων και των διαδικασιών που κατευθύνουν και να ελέγχουν τις δραστηριότητες και τους πόρους του φορέα παροχής υπηρεσιών για το σχεδιασμό, τη μετάβαση, την παράδοση και τη βελτίωση των υπηρεσιών για την κάλυψη των απαιτήσεων των υπηρεσιών

13. Σύστημα διαχείρισης υπηρεσιών: Σύστημα διαχείρισης για να κατευθύνει και να ελέγχει τις δραστηριότητες παροχής υπηρεσιών διαχείρισης του παρόχου υπηρεσιών Ένα σύστημα διαχείρισης είναι ένα σύνολο αλληλένδετων ή αλληλεπιδρώντων στοιχείων για τη δημιουργία της πολιτικής και των στόχων και την επίτευξη των στόχων αυτών .Το SMS περιλαμβάνει όλες τις πολιτικές διαχείρισης των υπηρεσιών, τους στόχους, τα σχέδια, τις διαδικασίες, την τεκμηρίωση και τους πόρους που απαιτούνται για το σχεδιασμό, τη μετάβαση, την παράδοση και τη βελτίωση των υπηρεσιών και την εκπλήρωση των απαιτήσεων σε αυτό το τμήμα του ISO / IEC 20000 .

14. Πάροχος υπηρεσιών: Οργάνωση ή μέρος μιας οργάνωσης που διαχειρίζεται και παρέχει μια υπηρεσία ή υπηρεσίες για τον πελάτη. Ένας πελάτης μπορεί να είναι εσωτερική ή εξωτερική οργάνωσης του φορέα παροχής υπηρεσιών .

15. Αίτηση υπηρεσίας: Αίτηση παροχής πληροφοριών, συμβουλών, την πρόσβαση σε μια υπηρεσία ή ένα προ-εγκεκριμένο αλλαγή

16. Απαίτηση υπηρεσίας: Ανάγκες του πελάτη και των χρηστών της υπηρεσίας, συμπεριλαμβανομένων των απαιτήσεων σε επίπεδο εξυπηρέτησης, και τις ανάγκες του παρόχου υπηρεσιών

17. Προμηθευτής: Οργάνωση ή μέρος μιας οργάνωσης που είναι εξωτερική οργάνωση του φορέα παροχής υπηρεσιών και να συνάπτει σύμβαση με τον πάροχο υπηρεσιών να συμβάλλουν στο σχεδιασμό, τη μετάβαση, την παράδοση και τη βελτίωση της υπηρεσίας ή υπηρεσιών ή διαδικασιών.

18. Ανώτατα διοικητικά στελέχη: Πρόσωπο ή ομάδα ανθρώπων που διευθύνουν και ελέγχουν τον πάροχο υπηρεσιών στο υψηλότερο επίπεδο

19. Μετάβαση: Δραστηριότητες που εμπλέκονται στη μετακίνηση νέων ή τροποποιημένων δρομολογίων από και προς το ζωντανό περιβάλλον

4.5 Βασικοί παράγραφοι ανάπτυξης του ISO 20000

Παρακάτω αναλύονται μία προς μία η κάθε παράγραφος που παρατίθεται μέσα στο πρότυπο ISO/IEC 20000, με αναφορές στην αρίθμηση των παραγράφων βάσει του προτύπου.

Η χρήση της παραγράφου 4 να καθορίσει «τις απαιτήσεις του συστήματος διαχείρισης» ενισχύει την ευθυγράμμιση με άλλα πρότυπα διαχείρισης του συστήματος, ιδίως το πρότυπο ISO / IEC 9001:2008 και ISO / IEC 27001:2005.

Η παράγραφος 4 της παρούσας προδιαγραφής είναι μια εκτεταμένη ανάπλαση των άρθρων 3 και 4 του ISO 20000-1:2005, μεταφέροντας τις ώριμες αρχές του συστήματος διαχείρισης που θεσπίζονται από το ISO 9001 σε αυτό το πρότυπο. Εντούτοις, δεν είναι μια υιοθέτηση αντικατάστασης. Ενώ οι απαιτήσεις και η ορολογία μπορεί να είναι οικείοι, το άρθρο 4 του εν λόγω προτύπου συγχωνεύει ισοδύναμα στοιχεία από έναν αριθμό παραγράφων του ISO 9001 (και, ομοίως, ISO 27001), όπως περιγράφεται στο Παράρτημα Α.

Στην παράγραφο 4.1 η ευθύνη διοίκησης είναι μια αναθεώρηση εκ βάθρων του έργο του ISO 20000-1:2005 ενότητα 3.1, εισάγοντας έναν αριθμό πρόσθετων απαιτήσεων. Η δέσμευση της ανώτατης διοίκησης, η πολιτική της διαχείριση, η εποπτεία και η ευθύνη είναι καθορισμένα και οι απαιτήσεις της εκπροσώπησης της διοίκησης ορίζονται με περισσότερες λεπτομέρειες.

Το ISO 20000-1:2005 απαιτούσε αμοιβαία συμφωνία της ερμηνείας του όρου «προμηθευτής» κατά την αξιολόγηση συμμόρφωσης των εξαρτήσεων παροχής υπηρεσιών μέσω της παραγράφου προμηθευτή. Το ISO / IEC 20000-1:2011 εισάγει την παράγραφο 4.2 ‘Διακυβέρνηση των διαδικασιών που χρησιμοποιούνται από άλλους’ για να αναγνωρίσει και να διευκρινίσει το φάσμα των εμπλεκομένων μερών που συμβάλουν στην επιτυχημένη υπηρεσία παράδοσης (εσωτερικές ομάδες παροχής υπηρεσιών, εξωτερικούς προμηθευτές ή ο πελάτης εισφορών). Περαιτέρω, στην

παράγραφο 1.2 αναφέρεται ότι «ο πάροχος υπηρεσιών δεν μπορεί να επικαλεστεί στοιχεία της διακυβέρνησης διεργασιών που εκτελούνται από τρίτους για τις απαιτήσεις στην παράγραφο 4': Η συμμόρφωση απαιτεί τώρα ο πάροχος υπηρεσιών να αποδείξει τόσο την ευαισθητοποίηση του φάσματος των εξαρτήσεων των υπηρεσιών παράδοσης και της διακυβέρνησης αυτών.

Το ISO / IEC TR 20000-3 παρέχει περαιτέρω οδηγίες σχετικά με τη διακυβέρνηση των διαδικασιών που λειτουργούν με άλλα μέρη.

Η παράγραφος 4.3 της Διαχείρισης Τεκμηρίωσης ορίζει το SMS με περισσότερη λεπτομέρεια και εισάγει επίσημο έγγραφο και τους ελέγχους καταγραφών. Μια αξιοσημείωτη επιπλέον προσθήκη είναι η ρητή υποχρέωση να τεκμηριωθεί ένας «κατάλογος των υπηρεσιών' ως ένα ξεχωριστό και διακριτό έγγραφο από τη Συμφωνία επιπέδου υπηρεσιών (SLA).

Στην παράγραφο 4.4 η διαχείριση των πόρων ξεκαθαρίζει τον ορισμό των SMS πόρων ως 'ανθρώπινες, τεχνικέ πληροφορίες και οικονομικές πηγές, μαζί με τις απαιτήσεις συμμόρφωσης για τον καθορισμό και την πρόβλεψη αυτών.

Στην παράγραφο 4.5 ο σχεδιασμός και η υλοποίηση ενός συστήματος διαχείρισης πληροφοριών, έτσι όπως προκύπτει από την παράγραφο 4 του ISO 20000-1:2005 έχει επανεξεταστεί σε αυτό το πρότυπο. Ενώ οι αρχές και η βασική δομή έχουν διατηρηθεί, υπάρχουν αρκετές αλλαγές στις απαιτήσεις μέσω των οποίων απομακρύνονται πολλά σημεία αμφιβολίας και απόδοσης και επιτρέπουν μια βελτιωμένη εφαρμογή. Για παράδειγμα, το πλάνο της διαχείρισης των υπηρεσιών περιλαμβάνει τώρα 'νόμιμες και κανονικές απαιτήσεις και 'κριτήρια για αποδοχή κινδύνων'.

Οι πρακτικές και οι απαιτήσεις έτσι όπως αναφέρονται στο ISO 20000-1:2005, παράγραφος 5 έχουν επεκταθεί και αναθεωρηθεί για να δημιουργήσουν την παράγραφο 5 του παρόντος προτύπου.

Η παράγραφος 5.1 υπογραμμίζει εκ νέου την αλλαγή στη διαχείριση ως προνομιακή διαδικασία ελέγχου. Αν και αναγνωρίζει ότι ο σχεδιασμός των νέων ή τροποποιημένων υπηρεσιών μπορεί να οδηγήσει σε ορισμένες προτεινόμενες αλλαγές που έχουν απορριφθεί, η παράγραφος καθιστά σαφές ότι ο πάροχος υπηρεσιών πρέπει να λαμβάνει τα αναγκαία μέτρα προκειμένου

να εξασφαλίζει ότι οι υπόλοιπες αποδεκτές αλλαγές είναι επαρκείς για να εκτελέσουν τις νέες ή τροποποιημένες υπηρεσίες αποτελεσματικά (μια έμμεση απαίτηση συμμόρφωσης για την αποτελεσματικότητα μετά την αλλαγή παρακολούθησης και επανεξέτασης που γίνεται πιο ρητά στη ρήτρα 9.2).

Οι παράγραφοι 5.2 και 5.3 παραθέτουν αρκετά περιεκτικά τις απαιτήσεις για τον προγραμματισμό, το σχεδιασμό και την ανάπτυξη των νέων ή τροποποιημένων υπηρεσιών, περιλαμβάνοντας ειδικές απαιτήσεις για τις υπηρεσίες που πρόκειται να «αφαιρεθούν» και λόγω της επιμέλεια των εξαρτήσεων με τα άλλα κόμματα που συμβάλλουν στην η παροχή των συστατικών υπηρεσιών.

Στην παράγραφος 5.4 η μετάβαση των νέων ή τροποποιημένων υπηρεσιών ορίζει ξανά τις απαιτήσεις για προ-εγκατάσταση δοκιμών υπηρεσίας ενάντια στα προκαθορισμένα κριτήρια αποδοχής μεταξύ του παρόχου υπηρεσιών και των ενδιαφερομένων μερών, τη χρήση της αναθεωρημένης διεργασίας έκδοση και ελέγχου για τη μετεγκατάσταση των υπηρεσιών στο ζωντανό περιβάλλον και την μετά-την-εγκατάσταση κριτική από τα αναμενόμενα αποτελέσματα.

Η γενική δομή και ο σκοπός αυτής της παραγράφου παραμένουν αμετάβλητα. Ωστόσο, μια λεπτομερής ανασκόπηση αποκαλύπτει πολλές πρόσθετες απαιτήσεις συμμόρφωσης. Οι σημαντικότερες αλλαγές περιγράφονται παρακάτω.

Υπάρχουν δύο αξιοσημείωτες αλλαγές στην παράγραφο 6.1 Διαχείριση επιπέδου παροχής υπηρεσιών. Η πρώτη αλλαγή ανανεώνει την απαίτηση του ISO 20000-1:2005 ότι κάθε υπηρεσία πρέπει να ορίζεται, συμφωνείτε και αποδεικνύεται σε ένα ή περισσότερα επίπεδα. Το ISO/IEC 20000-1:2011 αναγνωρίζει ότι ένας πελάτης μπορεί να αναθέσει το χαρτοφυλάκιο των υπηρεσιών από έναν πάροχο και ότι αυτές θα πρέπει τώρα να καθοριστούν σε ένα κατάλογος υπηρεσιών για τον πελάτη, που περιλαμβάνει «τις εξαρτήσεις μεταξύ των υπηρεσιών και των στοιχείων της υπηρεσίας ». Αυτό Στη συνέχεια συμπληρώνεται με ένα ή περισσότερα SLAs για καθεμία από τις υπηρεσίες που παρέχονται.

Η άλλη αλλαγή αφορά στη διακυβέρνηση των διαδικασιών που

λειτουργούν από άλλα μέρη (άρθρο 4.2): Ξεχωριστά από τον προμηθευτή διαχείρισης (εξετάζονται παρακάτω στην ενότητα 7.2), το τελικό εδάφιο της παραγράφου 6.1 δίνει τις απαιτήσεις διακυβέρνησης για τις «συνιστώσες υπηρεσιών που παρέχονται από μια εσωτερική ομάδα ή από τον πελάτη.

Η παράγραφος 6.2 Αναφορά Υπηρεσιών είναι σε γενικές γραμμές μια αμετάβλητη αρχή, ωστόσο, το πλαίσιο και το περιεχόμενο της έκθεσης για τις απαιτήσεις των υπηρεσιών είναι πιο καθορισμένο/

Στην παράγραφο 6.3 η συνέχεια και των υπηρεσιών και η διαχείριση της διαθεσιμότητας επεκτάθηκε και αναδιαρθρώθηκε σε τρεις υποπαραγράφους με αποσαφηνισμένες απαιτήσεις συμμόρφωσης ως εξής.

Η παράγραφος 6.3.1 Συνέχεια της υπηρεσίας και απαιτήσεις διαθεσιμότητας δίνει έμφαση στην αξιολόγηση κινδύνων της υπηρεσίας συνέχειας και διαθεσιμότητας ως το πρώτο βήμα για τον προσδιορισμό των απαιτήσεων «του πελάτη» και άλλων ενδιαφερόμενων μερών. Ωστόσο, κατά την εκτίμηση της συμμόρφωσης ενός φορέα παροχής υπηρεσιών που προσφέρει μια τυποποιημένη υπηρεσία σε μια σειρά από πελάτες, η συνέχεια και η διαθεσιμότητα αυτής της υπηρεσίας θα αξιολογούταν ως κίνδυνος. Η εμπορική σύμβαση θα αποτελέσει στη συνέχεια τη συμφωνία του πελάτη στις δεσμεύσεις συνέχειας και διαθεσιμότητας.

Στην παράγραφο 6.3.2 η συνέχεια της υπηρεσίας και τα σχέδια διαθεσιμότητας δεν συνεχίζουν την πρώην απαίτηση να «διασφαλίσει ότι οι απαιτήσεις πληρούνται όπως είχε συμφωνηθεί σε όλες τις περιστάσεις », όπως ότι διαψεύδεται η φύση της συνέχειας των υπηρεσιών και η διαχείριση διαθεσιμότητα, που ήταν βασισμένες στον κίνδυνο. Η παράγραφος αυτή εμπεδώνει το σχέδιο της συνέχεια των υπηρεσιών και το περιεχόμενο του σχεδίου διαχείρισης της διαθεσιμότητας, με τη σημείωση ότι τα σχέδια αυτά μπορούν να συνδυαστούν σε ένα έγγραφο.

Στην παράγραφο 6.3.3 η συνέχεια της υπηρεσίας και η παρακολούθηση και δοκιμή της διαθεσιμότητας μειώνει την απαίτηση να επανεξετάζονται τα σχέδια «τουλάχιστον ετησίως ». Αυτό το πρότυπο παίρνει μια προσέγγιση καθοδηγούμενη από κάποιο περιστατικό για να την αναθεωρήσει ύστερα από τον έλεγχο των σχεδίων ή μετά την επίκληση του σχεδίου υπηρεσίας της

συνέχειας. Όπως και προηγουμένως, «τα σχέδια συνέχειας και διαθεσιμότητας της υπηρεσίας θα πρέπει να δοκιμάζεται εκ νέου μετά από σημαντικές αλλαγές στην υπηρεσία περιβάλλοντος ». Επιπλέον, οι δοκιμές πρέπει να διεξάγονται ως προς τις απαιτήσεις της συνέχειας και διαθεσιμότητας, τα αποτελέσματα να καταγραφούν και να αξιολογηθούν, να γίνουν οι απαραίτητες ενέργειες και να αναφερθούν τα αποτέλεσμα των ενεργειών αυτών.

Στην παράγραφο 6.4 ο προϋπολογισμός και η λογιστική για τις υπηρεσίες παραμένουν σε γενικές γραμμές αμετάβλητα, αν η αναθεωρημένη διάταξη βοηθά τη διευκρίνιση. Μια αξιοσημείωτη προσθήκη είναι η απαίτηση για «τον ορισμό μιας διεπαφή μεταξύ του προϋπολογισμού και της λογιστική της διαδικασίας των υπηρεσιών και άλλων διεργασιών οικονομική διαχείρισης».

Παρομοίως, η παράγραφος 6.5 για τη διαχείριση της χωρητικότητας γενικά αναπαράγει την προηγούμενη έκδοση του προτύπου, αν και πάλι υπάρχουν μικρές αλλαγές. Ο σκοπός των πόρων που πρόκειται να διαχειριστούν αναφέρεται ρητά ως «ανθρώπινος, τεχνικός, οικονομικός και πληροφοριακός πόρος». Επιπλέον, υπάρχει μια λεπτή αλλαγή στη διατύπωση για το επιθυμητό αποτέλεσμα.

Στην παράγραφο 6.6 η διαχείριση της ασφάλειας πληροφοριών έχει αναδιατυπωθεί για τη βελτίωση της εναρμόνισης με τις απαιτήσεις του ISO 27001.Έχει χωριστεί σε παραγράφους που να καλύπτουν την πολιτική ασφάλειας των πληροφοριών, ελέγχους κινδύνων και την αλλαγή και τη διαχείριση περιστατικών. Η νέα πολιτική και τις απαιτήσεις ελέγχου, αν και πιο ελαφριές σε σύγκριση με το πρότυπο ISO 27001, είναι αυστηρότερες από την προηγούμενη έκδοση αυτού του προτύπου και μπορούν να αμφισβητήσουν ορισμένες οργανώσεις που δεν έχουν εφαρμόσει μια πληροφορία του συστήματος διαχείρισης της ασφάλειας σύμφωνα με το ISO 27001.

Σε σύγκριση, το 6.6.3 Αλλαγές στην ασφάλεια των πληροφοριών και περιστατικά θα πρέπει να είναι λιγότερο προκλητική, καθώς αυτό γενικά αναπαράγει τις απαιτήσεις της προηγούμενης έκδοσης της παρούσας πρότυπο

για την ενσωμάτωση πληροφοριών για τη διαχείριση της ασφάλειας σε υφιστάμενη διαχείριση της αλλαγής, της διαχείρισης συμβάντων και διαδικασίες βελτίωσης.

Η γενική δομή και το περιεχόμενο της εν λόγω παραγράφου παραμένει αμετάβλητο, αν και υπάρχουν ορισμένες λεπτομερείς αλλαγές. Στην παράγραφο 7.1 η διαχείριση επιχειρηματικών σχέσεων έχει μεγαλύτερη εστίαση στον πελάτη και είναι λιγότερο περιοριστική για τις σχέσεις με άλλα ενδιαφερόμενα μέρη.

Η «ετήσια υπηρεσία επανεξέτασης όπως ορίζεται στο πρότυπο ISO 20000-1:2005 έχει αντικατασταθεί σε αυτό το πρότυπο από την απαίτηση για έναν «μηχανισμό επικοινωνίας», επιτρέποντας μια ποικιλία των ρυθμίσεων από την ετήσια επανεξέταση σε μια συνεχή, προκαθορισμένη επανεξέταση προσαρμοσμένη στις απαιτήσεις των επιχειρήσεων. Ο σκοπός της παρούσας ανακοίνωσης ορίζεται, αν και η διατύπωση είναι λίγο διφορούμενη. Μια λογική ερμηνεία συνιστάται ως «η προώθηση της αμοιβαίας κατανόησης του επιχειρηματικό περιβάλλον στο οποίο οι υπηρεσίες αυτές λειτουργούν και λαμβάνουν χώρα οι απαιτήσεις για νέες ή τροποποιημένες υπηρεσίες». Αυτό θα επιτρέψει, για παράδειγμα (ISO / IEC 9001:2008;ISO / IEC 27001:2005):

1. πάροχος υπηρεσιών να εξακολουθήσει να έχει επίγνωση της επιχείρησης του πελάτη και του επιχειρησιακού περιβάλλοντος και τις απαιτήσεις για αλλαγή που προκύπτουν από τον πελάτη, και
2. πάροχος υπηρεσιών να ανταποκριθεί στις αλλαγές στο δικό τους στρατηγικό και εμπορικό περιβάλλον και να βελτιωθεί, να προσαρμόσει ή να αντικαταστήσει στοιχεία μιας γενικής υπηρεσίας που παρέχεται σε ένα αριθμό πελατών.

Ενώ οι απαιτήσεις για τη διαχείριση των καταγγελιών του πελάτη παραμένουν αμετάβλητες, η ικανοποίηση του πελάτη τώρα παίρνει μια ρεαλιστική άποψη και επιτρέπει μετρήσεις και αναλύσεις που να βασίζονται σε ένα αντιπροσωπευτικό δείγμα των πελατών και των χρηστών των υπηρεσιών».Στην παράγραφο 7.2 η διαχείριση των προμηθευτών καταγράφει μια περιοριστική λίστα των στοιχείων που πρέπει να περιλαμβάνονται ή να γίνεται αναφορά σε έναν προμηθευτή σύμβασης .

Η «ετήσια αναθεώρηση σύμβασης με τον προμηθευτή» που καθορίζεται στο πρότυπο ISO 20000-1:2005 έχει αντικαθίσταται με την πιο παθητική απαίτηση να «παρακολουθεί την απόδοση του προμηθευτή σε προγραμματισμένα χρονικά διαστήματα ». Ιδιαίτερης σημασίας είναι η αντικατάσταση των δύο «διαδικασιών» απαίτησης με:

1. την απαίτηση για τη σύμβαση με τον προμηθευτή να οριστούν ή να αναφερθούν ευθύνες αναφοράς για τον τερματισμό της σύμβασης και τη μεταφορά των υπηρεσιών σε ένα διαφορετικό μέρος», εξασφαλίζοντας ότι αυτή προληπτικά θα αντιμετωπιστεί και θα τεκμηριωθεί πριν προκύψει ανάγκη για μεταφορά ή η καταγγελία, και
2. την απαίτηση για μια τεκμηριωμένη « διαδικασία για τη διαχείριση συμβατικών διαφορών » .

Στην παράγραφο 8.1 η διαχείριση περιστατικών και των υπηρεσιών αιτήσεων αναγνωρίζει τη σύγχρονη πρακτική σε πολλούς οργανισμούς για την επεξεργασία των εκθέσεων συμβάντων και των αιτημάτων αλλαγής υπηρεσίας μέσω ενός πελάτη και μίας κοινής διαδικασίας.

Το πρότυπο απαιτεί η διαδικασία διαχείρισης της αίτησης συμβάντος και των υπηρεσιών να ορίζεται από δύο χωριστές τεκμηριωμένες διαδικασίες για το περιστατικό και τον κύκλο ζωής των υπηρεσιών διαχείρισης από τη στιγμή της καταγραφής ως το κλείσιμο. Οι πληροφορίες που θα διατίθενται στο προσωπικό που εκτελεί τη διαδικασία συνταγογραφούνται και περιλαμβάνουν πληροφορίες από τη διαδικασία απελευθέρωσης και την διαχείριση ανάπτυξης .

Η τελευταία παράγραφος ορίζει πώς σημαντικά γεγονότα πρέπει να αντιμετωπιστούν με μία τεκμηριωμένη διαδικασία . Στην παράγραφο 8.2 η διαχείριση των προβλημάτων παραμένει σε γενικές γραμμές αμετάβλητη, παρόλο που η αναθεωρημένη διάταξη και διατύπωση δίνει σαφήνεια. Μια αξιοσημείωτη βελτίωση είναι η ρητή αναγνώριση του γεγονότος ότι δεν είναι όλα τα προβλήματα είναι μόνιμα επιλύσιμα. Εμπορικοί, τεχνικοί ή εξωτερικούς περιορισμοί μπορούν να αποτρέψουν αυτό να συμβεί . Η παράγραφος αναφέρει πλέον ότι «όταν η πρωταρχική αιτία έχει προσδιοριστεί, αλλά το πρόβλημα δεν έχει οριστικά επιλυθεί, ο πάροχος

υπηρεσιών πρέπει να προσδιορίσει δράσεις για τη μείωση ή την εξάλειψη των επιπτώσεων του προβλήματος σχετικά με τις υπηρεσίες .

Στην παράγραφο 9.1 οι αλλαγές στη διαχείριση της απαίτηση διαμόρφωσης περιλαμβάνουν:

- ελάχιστα υποχρεωτικά πεδία πληροφοριών περιουσιακών στοιχείων για κάθε CI στο CMDB,
- μια τεκμηριωμένη διαδικασία για την καταγραφή, τον έλεγχο και παρακολούθηση εκδόσεων των πιστωτικών ιδρυμάτων που ενσωματώνει στοιχεία του ενεργητικού με βάση τον κίνδυνο ελέγχου, πρωτότυπα αντίγραφα των πιστωτικών ιδρυμάτων που καταγράφονται στο CMDB πρέπει να αποθηκεύονται σε ασφαλές φυσικό ή ηλεκτρονικές βιβλιοθήκες γίνεται αναφορά από το αρχεία διαμόρφωσης,
- έλεγχο των εγγραφών που είναι αποθηκευμένες στο CMDB σε προγραμματισμένα χρονικά διαστήματα.

Στην παράγραφο 9.2 οι αλλαγές στη διαχείριση της απαίτησης αλλαγής περιλαμβάνουν :

- ελάχιστη διαχείριση της αλλαγής του περιεχομένου της πολιτικής,
- Αφαίρεση ή μεταφορά μιας υπηρεσίας θα πρέπει να ταξινομείται ως αλλαγή σε μια υπηρεσία με τη δυνατότητα να έχει μια σημαντική επίπτωση,
- μια τεκμηριωμένη διεργασία καταγραφής, ταξινόμησης, αξιολόγησης και έγκρισης των αιτήσεων για αλλαγή,
- μια τεκμηριωμένη αναλυτική διαδικασία για την διαχείριση των αλλαγών έκτακτης ανάγκης .

Οι απαιτήσεις για τη διαχείριση των αιτήσεων για την αλλαγή είναι παρόμοια πιο ισχυρές ως εξής :

- Αιτήσεις για την αλλαγή που ταξινομούνται ως έχοντας τη δυνατότητα να έχουν σημαντικές επιπτώσεις για τις υπηρεσίες ή ο πελάτης πρέπει να διαχειρίζεται χρησιμοποιώντας τη διαδικασία για το σχεδιασμό και

τη μετάβαση των νέων ή τροποποιημένων υπηρεσιών . Όλες οι άλλες αιτήσεις για την αλλαγή σε πιστωτικά ιδρύματα που ορίζονται στην πολιτική διαχείρισης της αλλαγής πρέπει να διαχειρίζονται σύμφωνα με τη διαδικασία διαχείρισης της αλλαγής».

- «Ο φορέας παροχής υπηρεσιών και τα ενδιαφερόμενα μέρη πρέπει να λαμβάνουν αποφάσεις σχετικά με την αποδοχή των αιτημάτων για αλλαγή»
- «Οι δραστηριότητες που απαιτούνται για την ανατροπή ή τη διόρθωση μιας ανεπιτυχούς αλλαγής πρέπει να σχεδιάζονται και, όπου είναι δυνατόν, να ελέγχονται.
- «Ο πάροχος υπηρεσιών πρέπει να αναθεωρήσει τις αλλαγές για την αποτελεσματικότητα » ISO 20000-1:2005 απαιτείται μόνο ότι « οι αλλαγές πρέπει να είναι αξιολόγηση για την επιτυχία

Στην παράγραφο 9.3 η διαχείριση έκδοσης και ανάπτυξης, που τώρα αναγνωρίζεται ως μια διαδικασία ελέγχου, έχει γενικό σκοπό και το περιεχόμενο που παραμένει αμετάβλητο, αν και υπάρχουν κάποιες λεπτομέρειες αλλαγές. Αξιοσημείωτες πρόσθετες απαιτήσεις έχουν ως εξής. Δεν υπάρχει πλέον ρητή απαίτηση να συντονιστεί το σχέδιο ανάπτυξης με τη διαδικασία διαχείρισης της αλλαγής και περιλαμβάνει αναφορές στα σχετικά αιτήματα για αλλαγή. Ο σχεδιασμός θα πρέπει να περιλαμβάνει επίσης τις ημερομηνίες για την ανάπτυξη κάθε έκδοσης, τα σχετικά παραδοτέα και τις μεθόδους που προορίζονται για ανάπτυξης .

Ο ορισμός της απελευθέρωσης έκτακτης ανάγκης πρέπει να τεκμηριώνονται και η απελευθέρωση να γίνεται σύμφωνα με μια τεκμηριωμένη διεργασία που να συνδέεται με τη διαδικασία αλλαγής έκτακτης ανάγκης. Για κάθε έκδοση, τα κριτήρια αποδοχής για την απελευθέρωση πρέπει να συμφωνηθούν με τον πελάτη και τα ενδιαφερόμενα μέρη. Πριν από την ανάπτυξη, η απελευθέρωση πρέπει να επαληθεύεται με βάση τα συμφωνηθέντα κριτήρια αποδοχής και να εγκριθεί. Εάν δεν πληρούνται τα κριτήρια, ο πελάτης και τα ενδιαφερόμενα μέρη πρέπει να συμμετέχουν στην απόφαση σχετικά με τις ενέργειες που απαιτούνται για να προχωρήσει .

Κεφάλαιο 5ο ISO 27001

5.1 Εισαγωγή

Το ISO/IEC 27001 είναι το μοναδικό διεθνές πρότυπο που μπορεί να προσδιορίσει τα ζητούμενα για ένα Σύστημα Διαχείρισης Ασφάλειας Πληροφοριών (ΣΔΑΠ-ISMS).

Η πληροφορία είναι μεγάλης σημασίας για τη λειτουργία του εκάστοτε οργανισμού. Η πιστοποίηση του υπό εξέταση iso εξυπηρετεί κάθε οργανισμό να διαχειριστεί τα περιουσιακά του στοιχεία που περιέχουν δεδομένα με σημαντικές πληροφορίες.

Το πρότυπο έχει σχεδιαστεί να διασφαλίζει την επιλογή επαρκών και ισορροπημένων ελέγχων ασφάλειας. Αυτή η επιλογή βοηθά ένα οργανισμό να προστατεύσει τα περιουσιακά του στοιχεία πληροφοριών και να τον εμπιστεύονται τα ενδιαφερόμενα μέρη και ιδιαίτερα οι πελάτες του (ISO/IEC FDIS 27001).

Το πρότυπο στηρίζεται στη διεργασιακή σκοπιά για την εδραίωση, συντήρηση και καλυτέρευση ενός ΣΔΑΠ. Το ISO/IEC 27001 είναι ιδανικό για κάθε οργανισμό. Είναι ιδανικό για χρηματοπιστωτικούς οργανισμούς που η προστασία της πληροφορίας είναι κρίσιμη (ISO. Standards Catalogue: ISO/IEC JTC 1/SC 27).

5.2 Οφέλη του ISO/IEC 27001

Τα οφέλη εστιάζουν στο ότι:

1. Αποδεικνύει ότι οι εσωτερικοί έλεγχοι του οργανισμού ικανοποιούν τους εταιρικούς στόχους
2. Αποδεικνύει ότι οι απαιτήσεις για σωστή διακυβέρνηση πραγματοποιούνται
3. Αποδεικνύει ότι η σχετική νομοθεσία πραγματικά εφαρμόζεται
4. Προσδίδει ανταγωνιστικό πλεονέκτημα στην ικανοποίηση συμβατικών υποχρεώσεων

5. Αποδεικνύει ότι τα οργανωτικά ρίσκα έχουν αναγνωριστεί, όπως πρέπει
6. Αναδεικνύει την ύπαρξη λειτουργικού συστήματος ασφάλειας δεδομένων
7. Αποδεικνύει ότι μέσω τακτικών αξιολογήσεων εξυπηρετεί την επιχείρηση να παρακολουθεί την απόδοσή και να γίνεται καλύτερη
8. χρησιμοποιεί κάθε ρίσκο προκειμένου να υλοποιηθεί ένα ιδανικό διαχειριστικό σύστημα

5.3 Γενικά

Το ISO / IEC 27001:2005, μέρος της οικογένειας ISO / IEC 27000 των προτύπων, είναι ένα πρότυπο Σύστημα Διαχείρισης Ασφάλειας Πληροφοριών (ISMS) που δημοσιεύθηκε τον Οκτώβριο του 2005 από τον Διεθνή Οργανισμό Τυποποίησης (ISO) και της Διεθνούς Ηλεκτροτεχνικής Επιτροπής (IEC). Το πλήρες όνομα του είναι ISO / IEC 27001:2005 - τεχνολογία της πληροφορίας - τεχνικές ασφάλειας - συστήματα διαχείρισης ασφάλειας πληροφοριών - Απαιτήσεις. Από τον Ιούλιο του 2013, η νέα έκδοση είναι στα σχέδια: ISO / IEC 27001:2013.

Το ISO / IEC 27001:2005 καθορίζει επίσημα ένα σύστημα διαχείρισης που έχει ως στόχο να φέρει την ασφάλεια των πληροφοριών με το ρητό έλεγχο της διαχείρισης. Όντας μια επίσημη προδιαγραφή σημαίνει ότι έχει ειδικές απαιτήσεις. Οργανισμοί που ισχυρίζονται ότι έχουν υιοθετήσει το πρότυπο ISO / IEC 27001 μπορεί επομένως να έχουν επισήμως ελεγχθεί και πιστοποιηθεί ότι συμμορφώνονται με το πρότυπο. ο πρότυπο περιλαμβάνει 11 τομείς (εκτός από τις εισαγωγικές ενότητες) (Security updates: The upcoming revision of ISO/IEC 27001):

1. Πολιτική Ασφάλειας - κατεύθυνση της διαχείρισης
2. Οργάνωση της ασφάλειας των πληροφοριών - διαχείριση της ασφάλειας των πληροφοριών
3. Διαχείριση περιουσιακών στοιχείων - καταγραφή και ταξινόμηση των περιουσιακών στοιχείων πληροφοριών

4. Ασφάλεια των ανθρώπινων πόρων - πτυχές της ασφάλειας για τους εργαζομένους που εισέρχονται, κινούνται και αφήνουν έναν οργανισμό
5. Φυσική και περιβαλλοντική ασφάλεια - προστασία των εγκαταστάσεων υπολογιστών
6. Επικοινωνίες και διαχείριση λειτουργιών - διαχείριση των τεχνικών ελέγχων ασφάλειας στα συστήματα και δίκτυα
7. Έλεγχος πρόσβασης - περιορισμό των δικαιωμάτων πρόσβασης σε δίκτυα, συστήματα, εφαρμογές, λειτουργίες και δεδομένα
8. Καταγραφή, ανάπτυξη και συντήρηση συστημάτων πληροφοριών - ασφάλεια κτιρίου σε εφαρμογές
9. Πληροφορίες διαχείρισης περιστατικών ασφάλειας - πρόβλεψη και ανταπόκριση δεόντως στις παραβιάσεις της ασφάλειας των πληροφοριών
10. Η διαχείριση της επιχειρησιακής συνέχειας - στην προστασία, τη διατήρηση και την ανάκτηση των επιχειρήσεων-κρίσιμες διαδικασίες και συστήματα
11. Συμμόρφωση - διασφάλιση της συμμόρφωσης με τις πολιτικές ασφάλειας των πληροφοριών, τα πρότυπα, τους νόμους και τους κανονισμούς

5.4 Πως λειτουργεί το πρότυπο

Οι περισσότεροι οργανισμοί έχουν ένα αριθμό ελέγχων της ασφάλειας των πληροφοριών. Ωστόσο, χωρίς την ασφάλεια του συστήματος διαχείρισης πληροφοριών (ISMS), οι έλεγχοι έχουν την τάση να είναι κάπως ανοργάνωτοι και αποσπασματικοί, αφού έχουν εφαρμοστεί συχνά ως σημείο λύσεις σε συγκεκριμένες καταστάσεις ή απλώς ως θέμα της σύμβασης. Έλεγχοι ασφαλείας σε λειτουργία αφορούν κατά κανόνα ορισμένες πτυχές της πληροφορικής και της ασφάλειας των δεδομένων, αφήνοντας μη -IT στοιχεία (όπως η γραφειοκρατία και ιδιόκτητη γνώση) με μικρότερη προστασία για το σύνολο. Επιπλέον σχεδιασμός της συνέχισης των επιχειρήσεων και της φυσικής ασφάλειας μπορεί να γίνεται εντελώς ανεξάρτητα από το IT ή την

ασφάλεια των πληροφοριών, ενώ πρακτικές Ανθρώπινου Δυναμικού μπορούν να κάνουν λίγη αναφορά στην ανάγκη να καθοριστούν και να ανατεθούν ρόλοι για την ασφάλεια των πληροφοριών και των ευθυνών σε όλη την οργάνωση. Το ISO / IEC 27001 απαιτεί από τη Διοίκηση να (Kosutic, 2013):

- Εξετάζει συστηματικά τις πληροφορίες του οργανισμού κινδύνων για την ασφάλεια, λαμβάνοντας υπόψη τις απειλές, τα τρωτά σημεία και οι επιπτώσεις
- Σχεδιάζει και να εφαρμόζει μια συνεκτική και ολοκληρωμένη σουίτα ελέγχων της ασφάλειας των πληροφοριών και / ή άλλες μορφές θεραπείας κινδύνου (όπως είναι η αποφυγή του κινδύνου ή τη μεταφορά του κινδύνου) για την αντιμετώπιση των κινδύνων αυτών που θεωρούνται απαράδεκτοι και,
- Υιοθετήσει μια γενική διαδικασία διαχείρισης για τη διασφάλιση ότι οι έλεγχοι ασφάλειας των πληροφοριών εξακολουθούν να πληρούν τις πληροφορίες ανάγκες του οργανισμού ασφαλείας σε συνεχή βάση.

Τα βασικά πλεονεκτήματα του 27001 είναι :

- Μπορεί να λειτουργήσει ως επέκταση του υφιστάμενου συστήματος ποιότητας σχετικά με την ασφάλεια
- Παρέχει μια ευκαιρία για τον εντοπισμό και τη διαχείριση των κινδύνων σε βασικά συστήματα πληροφοριών και στοιχείων
- Παρέχει εμπιστοσύνη και ασφάλεια στους εμπορικούς εταίρους και τους πελάτες και λειτουργεί ως εργαλείο μάρκετινγκ
- Επιτρέπει μια ανεξάρτητη επανεξέταση και διασφάλιση σχετικά με τις πρακτικές ασφάλειας των πληροφοριών
- Μια εταιρεία μπορεί να θέλει να υιοθετήσει το πρότυπο ISO 27001 για τους ακόλουθους λόγους:
- Είναι κατάλληλο για την προστασία των κρίσιμων και ευαίσθητων πληροφοριών
- Παρέχει μια ολιστική, προσέγγιση βασιζόμενη στον κίνδυνο για την εξασφάλιση πληροφοριών και την τήρηση

- Επιδεικνύει την αξιοπιστία, την εμπιστοσύνη, την ικανοποίηση και την εμπιστοσύνη με τους εταίρους ενδιαφερομένους, τους πολίτες και τους πελάτες
- Επιδεικνύει την κατάσταση της ασφάλειας, σύμφωνα με διεθνώς αποδεκτά κριτήρια
- Δημιουργεί μια διαφοροποίηση της αγοράς που οφείλεται στην υπεραξία, το κύρος, την εικόνα και την εξωτερική φήμη
- Εάν μια εταιρεία είναι πιστοποιημένη μια φορά, είναι αποδεκτή σε παγκόσμιο επίπεδο .

Ενώ άλλα σύνολα των ελέγχων της ασφάλειας των πληροφοριών μπορεί δυνητικά να χρησιμοποιηθούν μέσα σε ένα πρότυπο ISO / IEC 27001 ISMS καθώς και, ή ακόμα και αντί του ISO / IEC 27002 (ο Κώδικας Πρακτικής για την Διαχείριση της Πληροφοριακής Ασφάλειας), αυτά τα δύο πρότυπα χρησιμοποιούνται συνήθως μαζί στην πράξη. Στο παράρτημα Α του προτύπου ISO / IEC 27001 παρατίθενται συνοπτικά τα στοιχεία ελέγχου της ασφάλειας των πληροφοριών από το ISO / IEC 27002, ενώ το ISO / IEC 27002 παρέχει συμπληρωματικές πληροφορίες και συμβουλές για την εφαρμογή των ελέγχων. Οι τομείς που καλύπτονται από το πρότυπο ISO 27002 περιλαμβάνουν (ISO 27002):

- Πολιτική ασφάλειας
- Οργάνωση της ασφάλειας των πληροφοριών
- Διαχείριση περιουσιακών στοιχείων
- Ανθρώπινοι πόροι ασφάλειας
- Φυσική και περιβαλλοντική ασφάλεια
- Διαχείριση των επικοινωνιών και των λειτουργιών
- Έλεγχος πρόσβασης
- Συστήματα απόκτησης, ανάπτυξης και συντήρησης πληροφοριών
- Πληροφορίες διαχείρισης περιστατικών ασφάλειας
- Διαχείριση της επιχειρησιακής συνέχειας

§ Κανονιστική συμμόρφωση

Οργανισμοί που εφαρμόζουν μια σουίτα των ελέγχων της ασφάλειας των πληροφοριών, σύμφωνα με το πρότυπο ISO / IEC 27002 είναι ταυτόχρονα πιθανό να ανταποκριθούν σε πολλές από τις απαιτήσεις του ISO / IEC 27001, αλλά μπορεί να στερούνται ορισμένων από τους γενικούς όρους του συστήματος διαχείρισης .

Το αντίστροφο είναι επίσης αλήθεια, με άλλα λόγια, ένα πρότυπο ISO / IEC 27001 πιστοποιητικό συμμόρφωσης παρέχει εγγυήσεις ότι το σύστημα διαχείρισης της ασφάλειας των πληροφοριών είναι στη θέση του, αλλά λέει λίγα πράγματα για την απόλυτη κατάσταση της ασφάλειας των πληροφοριών εντός του οργανισμού. Τεχνικοί έλεγχοι ασφάλειας, όπως antivirus και firewalls συνήθως δεν ελέγχονται από τους ISO / IEC 27001 ελέγχους πιστοποίησης: η οργάνωση ουσιαστικά θεωρείται ότι έχει υιοθετήσει όλες τις απαραίτητες πληροφορίες για την ασφάλεια ελέγχου, δεδομένου ότι η γενική ISMS είναι σε θέση και θεωρείται επαρκής εφόσον πληροί τις απαιτήσεις του ISO / IEC 27001 . Επιπλέον, η διοίκηση προσδιορίζει το πεδίο εφαρμογής της ISMS για σκοπούς πιστοποίησης και μπορεί να την περιορίσουν σε μια ενιαία επιχειρηματική μονάδα ή τοποθεσία. Το ISO / IEC 27001 πιστοποιητικό δεν σημαίνει κατ' ανάγκη ότι το υπόλοιπο του οργανισμού, εκτός της ελεγχόμενης περιοχής, έχει επαρκή προσέγγιση της διαχείρισης πληροφοριών ασφάλειας .

Άλλα πρότυπα της οικογένειας ISO / IEC 27000 των προτύπων παρέχουν επιπρόσθετες διευκρινίσεις σχετικά με ορισμένες πτυχές του σχεδιασμού, της υλοποίησης και της λειτουργίας ενός ISMS, για παράδειγμα, σχετικά με τη διαχείριση των κινδύνων ασφάλειας των πληροφοριών (ISO / IEC 27005).

5.5 Ο Κύκλος PDCA

Το 27001:2005 υιοθετεί τη διαδικασία του μοντέλου "Plan-Do-Check-Act» (PDCA), το οποίο εφαρμόζεται στη δομή όλων των διαδικασιών στο ISMS. Συγκεκριμένα αναφέρεται στα ακόλουθα:

1. Σχέδιο (για την ίδρυση της ISMS): Καθιέρωση της πολιτικής, των

στόχων του ISMS, των διεργασιών και διαδικασιών που σχετίζονται με τη διαχείριση των κινδύνων και τη βελτίωση της ασφάλειας των πληροφοριών να παρέχουν αποτελέσματα σύμφωνα με τις παγκόσμιες πολιτικές και στόχους της οργάνωσης.

2. Do (για την εφαρμογή και τη λειτουργία της ISMS): Εφαρμογή και εκμετάλλευση της πολιτικής ISMS, των ελέγχων, των διαδικασιών.
3. Έλεγχος (παρακολούθηση και επανεξέταση της ISMS): Αξιολόγηση και, κατά περίπτωση, μέτρηση των επιδόσεων των διεργασιών κατά της πολιτικής, των στόχων και της πρακτικής εμπειρίας και τα αποτελέσματα αναφορά προς τη διοίκηση για την αναθεώρηση.
4. Πράξη (επικαιροποίηση και βελτίωση του ISMS): Ανάληψη διορθωτικών και προληπτικών ενεργειών, με βάση τα αποτελέσματα του ελέγχου ISMS εσωτερική και επανεξέτασης της διαχείρισης, ή άλλες σχετικές πληροφορίες για την συνεχή βελτίωση του εν λόγω συστήματος.

5.6 Προέλευση ΤΟΥ ISO/IEC 27001

Το BS 7799 ήταν ένα πρότυπο που αρχικά δημοσιεύθηκε από τον Όμιλο BSI το 1995. Γράφτηκε από το Τμήμα της κυβέρνησης του Ηνωμένου Βασιλείου Εμπορίου και Βιομηχανίας (DTI), και αποτελούνταν από διάφορα μέρη.

Το πρώτο μέρος, που περιέχει τις βέλτιστες πρακτικές για τη διαχείριση της ασφάλειας των πληροφοριών, αναθεωρήθηκε το 1998. Μετά από μια μακρά συζήτηση στους παγκόσμιους οργανισμούς τυποποίησης, πράγμα που τελικά υιοθετήθηκε από την ISO ως ISO / IEC 17799, «Πληροφορική - Κώδικας πρακτικής για την ασφάλεια των πληροφοριών διαχείρισης" το 2000. Το ISO / IEC 17799 στη συνέχεια αναθεωρήθηκε τον Ιούνιο του 2005 και τελικά ενσωματώθηκε στη σειρά προτύπων ISO 27000 ως ISO / IEC 27002 τον Ιούλιο του 2007 (Kosutic, 2013).

Το δεύτερο μέρος του BS7799 εκδόθηκε για πρώτη φορά από την BSI το 1999, γνωστό και ως BS 7799 Part 2, με τίτλο «Συστήματα Διαχείρισης

Ασφάλειας Πληροφοριών -. Απαιτήσεις και καθοδήγηση για τη χρήση". Το BS 7799-2 επικεντρώθηκε στο πώς να εφαρμοστεί ένα Σύστημα Διαχείρισης Ασφάλειας Πληροφοριών (ISMS), αναφερόμενο στην διαχείριση της ασφάλειας των πληροφοριών δομής και των ελέγχων που προσδιορίζονται στο BS 7799-2. Αυτό έγινε αργότερα το πρότυπο ISO / IEC 27001:2005. Το 2002 έκδοση του BS 7799-2 εισήγαγε τον Plan-Do-Check-Act (PDCA) κύκλο (Deming κύκλου), την ευθυγράμμισή του με τα πρότυπα ποιότητας όπως το ISO 9000. Το BS 7799 Part 2 εγκρίθηκε από το ISO, ως το πρότυπο ISO / IEC 27001, το Νοέμβριο του 2005. Το BS 7799 Part 3 δημοσιεύθηκε το 2005, καλύπτοντας την ανάλυση και διαχείριση των κινδύνων. Είναι ευθυγραμμισμένο με το πρότυπο ISO / IEC 27001:2005.

5.7 Πιστοποίηση

Μια ISMS μπορεί να πιστοποιηθεί ότι συμμορφώνεται με το πρότυπο ISO / IEC 27001 από έναν αριθμό διαπιστευμένων καταχωρητών σε όλο τον κόσμο . Πιστοποίηση κατά οποιαδήποτε από τις αναγνωρισμένες εθνικές εκδοχές του ISO / IEC 27001 (π.χ. JIS Q 27001, η ιαπωνική έκδοση) από διαπιστευμένο φορέα πιστοποίησης είναι λειτουργικά ισοδύναμη με την πιστοποίηση κατά ISO / IEC 27001.

Σε ορισμένες χώρες, οι φορείς που πιστοποιούν τη συμμόρφωση των συστημάτων διαχείρισης σε καθορισμένα πρότυπα ονομάζονται «φορείς πιστοποίησης», ενώ σε άλλα αναφέρονται κοινώς ως «φορείς καταχώρισης», «αξιολόγηση και φορείς καταχώρισης», «πιστοποίηση / καταγραφή φορέων», και μερικές φορές « καταχωρητές » (ISO/IEC FDIS 27001).

Το ISO / IEC 27001, όπως και οι άλλες πιστοποιήσεις ISO σύστημα διαχείρισης, συνήθως περιλαμβάνει μια διαδικασία εξωτερικού ελέγχου τριών σταδίων που ορίζονται από το πρότυπο ISO / IEC 17021 και το πρότυπο ISO / IEC 27006:

- Το Στάδιο 1 είναι μια προκαταρκτική, άτυπη αναθεώρηση του ISMS, για παράδειγμα, για τον έλεγχο της ύπαρξης και της πληρότητας των βασικών εγγράφων, όπως η πολιτική ασφαλείας των πληροφοριών του οργανισμού, δήλωση εφαρμογής (SOA), και σχέδιο θεραπείας

κινδύνου (RTP) . Το στάδιο αυτό χρησιμεύει για την εξοικείωση των ελεγκτών με την οργάνωση και το αντίστροφο .

- Το Στάδιο 2 είναι ένας πιο λεπτομερής και επίσημος έλεγχο της συμμόρφωσης, που ελέγχει ανεξάρτητα την ISMS με βάση τις απαιτήσεις που ορίζονται στο πρότυπο ISO / IEC 27001 . Οι ελεγκτές θα αναζητήσουν στοιχεία που να επιβεβαιώνουν ότι το σύστημα διαχείρισης έχει σχεδιαστεί σωστά και εφαρμοστεί, και είναι στην πραγματικότητα σε λειτουργία (για παράδειγμα, με την επιβεβαίωση ότι η επιτροπή ασφαλείας ή παρόμοιος φορέας διαχείρισης συνέρχεται τακτικά για να επιβλέπει την ISMS). Οι έλεγχοι πιστοποίησης διεξάγονται συνήθως κατά ISO / IEC 27001 Lead Συνέδριο. Περνώντας αυτό έχει ως αποτέλεσμα το στάδιο στο ISMS να είναι πιστοποιημένο σύμφωνα με το πρότυπο ISO / IEC 27001 .
- Το Στάδιο 3 περιλαμβάνει την σχόλια ή ελέγχους για να επιβεβαιώσει ότι ο οργανισμός παραμένει σε συμμόρφωση με το πρότυπο. Πιστοποίηση συντήρησης απαιτεί την περιοδική επαναξιολόγηση ελέγχων για να επιβεβαιωθεί ότι η ISMS συνεχίζει να λειτουργεί όπως προβλέπεται και προορίζεται . Αυτά πρέπει να συμβεί τουλάχιστον μία φορά ετησίως, αλλά (μετά από συμφωνία με τη διοίκηση) είναι συχνά διεξάγονται πιο συχνά, ιδιαίτερα κατά το ISMS είναι εξακολουθούν να ωριμάζουν .

5.8 Τα Πεδία του ISO 27001:2005

Το μητρώο περιουσιακών στοιχείων καταγράφει τα περιουσιακά στοιχεία της εταιρείας ή την έκταση αυτών. Ο τομέας διαχείρισης περιουσιακών στοιχείων ασχολείται με την ανάλυση και την επίτευξη του αναγκαίου επιπέδου προστασίας των οργανωτικών στοιχείων . οι τυπικοί στόχοι του τομέα διαχείρισης περιουσιακών στοιχείων είναι να εντοπίσει και να δημιουργήσει μια απογραφή όλων των περιουσιακών στοιχείων, να δημιουργήσει μια ιδιοκτησία για τον εντοπισμό όλων των περιουσιακών στοιχείων, τη θέσπιση ενός συνόλου κανόνων για την αποδεκτή χρήση των περιουσιακών στοιχείων, τη δημιουργία ενός πλαισίου για την ταξινόμηση

των στοιχείων του ενεργητικού, τη δημιουργία ενός περιουσιακού στοιχείου ετικετοποίησης και κατευθυντήριων γραμμών . Διαχείριση περιουσιακών στοιχείων, σε γενικές γραμμές ορίζεται ως η αναφορά σε οποιοδήποτε σύστημα που θα παρακολουθεί και θα υποστηρίζει τα πράγματα της αξίας σε μια οικονομική οντότητα ή ομάδα . Μπορεί να ισχύει τόσο σε ενσώματα περιουσιακά στοιχεία, όπως κτίρια και σε άυλες έννοιες όπως η πνευματική ιδιοκτησία και η καλή θέληση (ISO 27001:2005).

Ένα περιουσιακό στοιχείο είναι κάτι που έχει αξία για τον οργανισμό . Περιουσιακά στοιχεία μπορεί να περιλαμβάνουν υποδομές (π.χ. κτίρια, αποθήκες, πύργους κ.λπ.), φυσικά περιουσιακά στοιχεία (εξοπλισμός πληροφορικής, επικοινωνιών, εξοπλισμού χρησιμότητας, τα βαρέα μηχανήματα), περιουσιακά στοιχεία του λογισμικού (εφαρμογές, κώδικα λογισμικού, εργαλεία ανάπτυξης, τα επιχειρησιακά προγράμματα software κ.λ.π), πληροφορίες (πληροφορίες της βάσης δεδομένων, νομικά έγγραφα, εγχειρίδια, πολιτικές και διαδικασίες, οργανωτικά έγγραφα, κλπ.), υπηρεσίες (μεταφορές, κλιματισμό, επικοινωνίες, επιχειρήσεις κοινής ωφέλειας, κλπ.), οι άνθρωποι (διαχείριση, τις δεξιότητες, την εμπειρία κ.λπ.) και ανεπαίσθητη (φήμη, εικόνα κλπ.) .

Η διαχείριση προσόντων είναι μια συστηματική διαδικασία λειτουργίας, συντήρησης, αναβάθμισης, και διάθεσης των περιουσιακών στοιχείων με οικονομικά αποδοτικό τρόπο. Οργανισμοί πρέπει να εντοπίζουν όλα τα περιουσιακά στοιχεία και να δημιουργούν και να διατηρούν τους ελέγχους ασφαλείας γύρω τους.

Για κάθε περιουσιακό στοιχείο ένα καθορισμένος ιδιοκτήτης που πρέπει να είναι υπεύθυνος για την εφαρμογή των κατάλληλων ελέγχων ασφαλείας. Κατά τη δημιουργία μιας πολιτικής διαχείρισης περιουσιακών στοιχείων ο οργανισμός πρέπει να καθορίσει το πεδίο της πολιτικής (ποια μέρη του οργανισμού που καλύπτονται στο πλαίσιο της πολιτικής), την ευθύνη (που έχει την τελική ευθύνη για την πολιτική), τη συμμόρφωση (είναι η συμμόρφωση υποχρεωτική ή όχι, ποιες είναι οι οδηγίες που ακολουθούν), τα κριτήρια απαλλαγής (σε ποια βάση μπορεί κάποιος να ζητήσει την παραίτηση) και ημερομηνία έναρξης ισχύος (από τη στιγμή που για το πότε είναι η πολιτική που εφαρμόζεται). Τυπικές δηλώσεις πολιτικής για τη

διαχείριση ενεργητικού περιλαμβάνουν (ISO 27001:2005):

- Όλα τα περιουσιακά στοιχεία θα πρέπει να προσδιορίζονται σαφώς, να τεκμηριώνονται και να ενημερώνονται τακτικά σε μητρώο περιουσιακών στοιχείων
- Όλα τα περιουσιακά στοιχεία θα πρέπει να έχουν ορίσει τους ιδιοκτήτες και τους θεματοφύλακες που αναφέρονται στο περιουσιακό στοιχείο μητρώο
- Όλα τα περιουσιακά στοιχεία θα πρέπει να έχουν την αντίστοιχη CIA Βαθμολογία (εμπιστευτικότητας, ακεραιότητας και διαθεσιμότητας) εγκατεστημένη στο μητρώο περιουσιακών στοιχείων
- Όλοι οι εργαζόμενοι πρέπει να χρησιμοποιούν τα πάγια στοιχεία της εταιρείας, σύμφωνα με την αποδεκτή χρήση των στοιχείων του ενεργητικού των διαδικασιών
- Όλα τα περιουσιακά στοιχεία πρέπει να ταξινομούνται σύμφωνα με την κατευθυντήρια γραμμή ταξινόμησης περιουσιακών στοιχείων της εταιρείας

Η διαχείριση περιουσιακών στοιχείων αποτελείται από το σύνολο των δραστηριοτήτων που συνδέονται με τη συνεχή διαχείριση και την παρακολούθηση των περιουσιακών στοιχείων μερικές από τις οποίες είναι οι εξής: ανακάλυψη (φυσική και λογική), δημιουργία και διατήρηση βιβλιοθήκης λογισμικού, τη δημιουργία και τη διατήρηση αποθέματος υλικού, τη διαχείριση της διάρθρωσης, φυσική εντοπισμού περιουσιακών στοιχείων, άδειας χρήσης λογισμικού της διαδικασίας διαχείρισης, αίτηση και έγκριση, τη διαχείριση των συμβάσεων, την αξιολόγηση για το πρότυπο ISO 27001 και PCI ελέγχου, η διαχείριση του προμηθευτή/πωλητή, την ανακατανομή και κίνηση, τη συνταξιοδότηση και διάθεση, τη συμμόρφωση με τους νόμους κατά περίπτωση κ.λπ.

5.9 Μητρώο περιουσιακών στοιχείων

Συνήθως όλες οι λειτουργίες των επιχειρήσεων υποχρεούνται να τηρούν μητρώο περιουσιακών στοιχείων των επιχειρηματικών μονάδων τους .

Το μητρώο περιουσιακών στοιχείων πρέπει να περιλαμβάνει, τουλάχιστον, τις ακόλουθες πληροφορίες σχετικά με τα περιουσιακά στοιχεία: το περιουσιακό στοιχείο ταυτοποίησης, το όνομα του περιουσιακού στοιχείου, το είδος και την τοποθεσία των περιουσιακών στοιχείων, το όνομα της συνάρτησης και της διαδικασίας που χρησιμοποιεί αυτό το περιουσιακό στοιχείο, ο ιδιοκτήτης του περιουσιακού στοιχείου, το θεματοφύλακα και το χρήστη και τη CIA (εμπιστευτικότητα, ακεραιότητα, διαθεσιμότητα) αξιολόγηση του περιουσιακού στοιχείου (ISO 27001:2005).

Οι οργανισμοί μπορούν να επιλέξουν να περιληφθούν πρόσθετες πληροφορίες στο περιουσιακό στοιχείο κατά την εγγραφή, αν κρίνεται απαραίτητο. Για παράδειγμα, IT περιουσιακά στοιχεία μπορούν να έχουν διευθύνσεις IP ως μέρος του μητρώου περιουσιακών στοιχείων. Για όλα τα μητρώα περιουσιακών στοιχείων, ένα πρωταρχικό πρόσωπο που είναι υπεύθυνο για το μητρώο περιουσιακών στοιχείων θα πρέπει να προσδιοριστεί . Συνήθως ο επικεφαλής της επιχειρηματικής μονάδας ή ο διευθυντής είναι ο ιδιοκτήτης του μητρώου περιουσιακού στοιχείου.

Ο ιδιοκτήτης του περιουσιακού στοιχείου είναι υπεύθυνος για την ολοκληρωμένη προστασία των περιουσιακών στοιχείων που ανήκουν σε αυτόν / αυτήν . Ο ιδιοκτήτης του περιουσιακού στοιχείου μπορεί να αναθέτει την ευθύνη της εφαρμογής των σχετικών ελέγχων για τη διατήρηση των περιουσιακών στοιχείων σε ένα άτομο / λειτουργία που αναφέρεται ως «θεματοφύλακα περιουσιακού στοιχείου». Είναι η ευθύνη του θεματοφύλακα του περιουσιακού στοιχείου για την εφαρμογή κατάλληλης διαδικασίας ασφαλείας που απαιτείται για την προστασία των περιουσιακών στοιχείων πληροφοριών . Είναι η ευθύνη όλων των εργαζομένων και το τρίτο προσωπικό του κόμματος να διατηρήσει την εμπιστευτικότητα, την ακεραιότητα και τη διαθεσιμότητα των περιουσιακών στοιχείων που χρησιμοποιούν.

Τα περιουσιακά στοιχεία πρέπει να ταξινομηθούν για να παρέχεται ένα κατάλληλο επίπεδο προστασίας για μια συγκεκριμένη κατηγορία στοιχείων του ενεργητικού. ενεργές πληροφορίες πρέπει να ταξινομούνται σε συνάρτηση με την αξία, τις απαιτήσεις και την κρισιμότητα των επιχειρηματικών δραστηριοτήτων της εταιρείας. Τυπικές οδηγίες ταξινόμησης της εταιρείας

ακολουθούν περιοριστικές αρχές. Μερικά από τα κοινά κριτήρια ταξινόμησης που χρησιμοποιούνται από εταιρείες δίνονται παρακάτω:

Εμπιστευτικό: Η κατηγορία αυτή αναφέρεται σε πληροφορίες του ενεργητικού που σχετίζεται με άτομα ή με άλλο τρόπο περιορίζεται μόνο σε εξουσιοδοτημένους χρήστες, και εφόσον αποκαλυφθούν, εκτός της εταιρείας θα βλάψουν την οργάνωση, τους πελάτες, ή τους συνεργάτες της. Η κατάταξη αυτή ισχύει για κάθε ευαίσθητες επιχειρηματικές πληροφορίες που προορίζεται για χρήση εντός της εταιρείας. Παραδείγματα των εμπιστευτικών πληροφοριών περιλαμβάνουν πληροφορίες για τους πελάτες, διαπραγματευτικές θέσεις, στρατηγική μάρκετινγκ, τα στοιχεία του προσωπικού, εσωτερικά σημειώματα της εταιρείας και παρουσιάσεις

Περιορισμένο: Η περιορισμένη περιεκτικότητα των περιουσιακών στοιχείων αφορά τις πληροφορίες για εξαιρετικά ευαίσθητες πληροφορίες για την εταιρεία, το οποίο όταν αποκαλυφθεί θα μπορούσε να προκαλέσει σημαντική ζημιά στη φήμη και την ανταγωνιστική θέση της εταιρείας στην αγορά . Μη εξουσιοδοτημένη αποκάλυψή του θα μπορούσε να επηρεάσει αρνητικά τις επιχειρήσεις της, τους μετόχους της, τους συνεργάτες της και / ή τους πελάτες της, που οδηγούν σε νομικές και οικονομικές επιπτώσεις και τις δυσμενείς κοινής γνώμης. Παραδείγματα των περιορισμένων πληροφοριών είναι λεπτομέρειες σημαντικών εκποιήσεων, εξαγορές και συγχωνεύσεις, επιχειρήσεις και στρατηγική του ανταγωνισμού, ευαίσθητος πελάτης, ανταγωνιστής, εκτιμήσεις εταίρου ή εργολάβου, πληροφορίες πνευματικής ιδιοκτησίας, επιβολή του νόμου και της κυβέρνησης των σχετικών πληροφοριών.

Εσωτερική συνεργάτες: Η κατάταξη αναφέρεται σε πληροφορίες περιουσιακών στοιχείων που είναι δυνητικά διαθέσιμες σε όλο το προσωπικό εντός της εταιρείας, αλλά δεν είναι δημόσια. Αυτό μπορεί να περιλαμβάνει επίσης πληροφορίες που περιορίζεται σε μια ομάδα ή ένα έργο εντός της εταιρείας, αλλά δεν έχει οριστεί ως "Ιδιωτικό" ή "Περιορισμένο". Παραδείγματα εσωτερικών πληροφοριών περιλαμβάνουν πληροφορίες για το σχεδιασμό του προϊόντος, την τεκμηρίωση του συστήματος, τα στοιχεία των εργαζομένων της εταιρείας, τα οργανογράμματα της εταιρείας, τα πρακτικά των συνεδριάσεων των τμημάτων .

Δημόσιο: Η ταξινόμηση αναφέρεται στα στοιχεία των πληροφοριών που έχουν δημοσιευθεί ή μπορούν να ληφθούν από μια δημοσιευμένη πηγή, π.χ. το Διαδίκτυο. Παράδειγμα των πληροφοριών του δημόσιου περιλαμβάνουν δημοσιευμένο υλικό μάρκετινγκ, δημόσιες δηλώσεις ή ανακοινώσεις της εταιρίας, δημοσιευμένες πληροφορίες για τις επιδόσεις της εταιρείας, δημοσιευμένες κενές θέσεις εργασίας (ISO 27001:2013 – Understanding the New Standard).

5.9.1 Σήμανση περιουσιακών στοιχείων

Όλα τα σημαντικά και κρίσιμα περιουσιακά στοιχεία στην εταιρεία πρέπει να φέρουν φυσική/ηλεκτρονική σήμανση σύμφωνα με τις πληροφορίες ετιεκτοποίησης και διαδικασίες της εταιρείας. Οι ιδιοκτήτες των περιουσιακών στοιχείων απαιτείται να εξασφαλίσουν ότι τα περιουσιακά τους στοιχεία επισημαίνονται κατάλληλα για την ευκολία της αναγνώρισης . Αυτό μπορεί να αποκλείσει πληροφορίες που ταξινομούνται ως «δημόσιες» . Για κάθε επίπεδο ταξινόμησης, οι διαδικασίες χειρισμού θα πρέπει να περιλαμβάνουν την εισαγωγή στοιχείων, ασφαλή επεξεργασία, την αποθήκευση, τη μετάδοση και την καταστροφή . Διαβάθμιση πρέπει να αναγράφεται στο μέτρο του δυνατού για όλες τις μορφές των φυσικών ή / και ηλεκτρονικών πληροφοριών που είναι ευαίσθητες στη φύση. Για παράδειγμα : θέμα του μηνύματος σφραγίζονται με "Εμπιστευτικό", κλπ.

Έλεγχος περιουσιακών στοιχείων

Ο τομέας ελέγχου πρόσβασης σχετίζεται με την εφαρμογή του ελέγχου πρόσβασης σε όλες τις ηλεκτρονικές φόρμες των συστημάτων επεξεργασίας πληροφοριών, όπως τα λειτουργικά συστήματα, τις εφαρμογές, τα δίκτυα και κινητές πλατφόρμες . Ο έλεγχος πρόσβασης είναι ο επιλεκτικός περιορισμός της πρόσβασης σε έναν τόπο ή άλλων πόρων. Συνήθως μια οργάνωση πολιτικής ελέγχου πρόσβασης θεσπίζει την υποχρέωση των ελέγχων που πρέπει να εφαρμόζονται για τον έλεγχο της πρόσβασης σε πληροφορίες, τις εγκαταστάσεις επεξεργασίας των πληροφοριών και των επιχειρηματικών διαδικασιών με βάση τις επιχειρήσεις και τις απαιτήσεις ασφαλείας (ISO

27001:2013 – Understanding the New Standard).

Η πολιτική θα πρέπει να στοχεύει να ελέγξει την αφομοίωση, την έγκριση και τη διάδοση των πληροφοριών σε ένα ελεγχόμενο τρόπο . Οι τυπικά οργανωτικοί στόχοι της πολιτικής ελέγχου πρόσβασης είναι η θέσπιση μιας διαδικασίας για την εγγραφή και διαγραφή του χρήστη από το μητρώο, τη θέσπιση μιας διαδικασίας για τη χορήγηση του σωστού επιπέδου των προνομίων πρόσβασης, την καθιέρωση μίας διαδικασίας για τον έλεγχο της χρήσης κωδικού πρόσβασης, την αλλαγή του κωδικού πρόσβασης και την αφαίρεση κωδικού πρόσβασης, τη δημιουργία διαδικασίας αναθεώρησης των δικαιωμάτων πρόσβασης, τη θέσπιση διαδικασίας για αφύλακτο εξοπλισμό, τη διατήρηση μιας σαφούς πολιτικής γραφείου, την καθιέρωση διαδικασίας για τον έλεγχο της πρόσβασης στο δίκτυο παροχής υπηρεσιών, τη δημιουργία μιας μέθοδος ελέγχου για την εξακρίβωση της γνησιότητας των απομακρυσμένων χρηστών, τη θέσπιση διαδικασίας για τις ρυθμίσεις των θυρών, θέσπιση διαδικασίας να διαχωρίσουν τα δίκτυα, την καθιέρωση διαδικασίας προκειμένου να χρησιμοποιούν ακριβείς ελέγχους δρομολόγησης, την καθιέρωση μίας διαδικασίας για τον έλεγχο βοηθητικών προγραμμάτων του συστήματος και τη θέσπιση μιας διαδικασίας για ασφαλείς επικοινωνίες μέσω κινητών υπολογιστικών συσκευών.

Ο εγγεγραμμένος χρήστης είναι αυτός που χρησιμοποιεί μια μονάδα επεξεργασίας των πληροφοριών και παρέχει τα διαπιστευτήριά του/της, αποδεικνύοντας την αποτελεσματική ταυτότητά του . Σε γενικές γραμμές, κάθε άτομο μπορεί να γίνει εγγεγραμμένος χρήστης, παρέχοντας κάποιες πιστοποιήσεις, συνήθως με τη μορφή ενός ονόματος χρήστη (ή e-mail) και τον κωδικό πρόσβασης.

Μετά από αυτό, μπορεί κανείς να έχει πρόσβαση σε πληροφορίες και προνόμια που δεν είναι διαθέσιμα σε μη εγγεγραμμένους χρήστες, που συνήθως αναφέρονται απλώς ως επισκέπτες. Η εισαγωγή των κατάλληλων πιστοποιήσεων για ένα σύστημα ονομάζεται σύνδεση (logging in). Χωρίς την κατάλληλη πολιτική που να διέπει την εγγραφή του χρήστη, μη εξουσιοδοτημένα άτομα μπορούν να αποκτήσουν πρόσβαση σε εμπιστευτικές πληροφορίες της εταιρείας που μπορεί να διαρρεύσουν προς τα έξω, προκαλώντας βλάβη στον οργανισμό, στην οικονομική του κατάσταση και

την φήμη . Οι οργανισμοί θα πρέπει να δημιουργήσουν μια διαδικασία εγγραφής χρήστη, η οποία περιλαμβάνει ελέγχους για λειτουργικά συστήματα και εφαρμογές πρόσβασης. Τυπικές δηλώσεις πολιτικής μπορεί να περιλαμβάνουν (ISO/IEC FDIS 27001):

- Όλοι οι χρήστες πρέπει να έχουν ένα μοναδικό αναγνωριστικό χρήστη που βασίζεται σε μια τυποποιημένη σύμβαση ονομασίας
- Μια επίσημη διαδικασία αδειοδότησης ορίζεται για τροφοδότηση των ταυτοτήτων των χρηστών .
- Μια διαδρομή ελέγχου πρέπει να τηρείται για όλες τις αιτήσεις για να προστεθεί, να τροποποιηθεί ή να διαγραφεί ένας λογαριασμός ενός χρήστη
- Οι λογαριασμοί χρηστών πρέπει να επανεξετάζονται σε τακτά χρονικά διαστήματα
- Οι εργαζόμενοι πρέπει να υπογράψουν ένα έντυπο προνόμιο αναγνωρίζοντας τα δικαιώματα πρόσβασής τους
- Τα δικαιώματα πρόσβασης θα πρέπει να ανακληθεί για αλλαγές υπαλλήλων ή αν εγκαταλείψουν τη δουλειά τους
- Προνόμια χορηγείται σε άτομα με βάση την ανάγκη.
- Μια καταγραφή όλων των προνομιούχων λογαριασμών πρέπει να διατηρηθεί και να ενημερώνεται σε τακτική βάση

Η διαχείριση του κωδικού πρόσβασης σχετίζεται με την κατανομή, τη ρύθμιση και την αλλαγή των κανόνων κωδικού πρόσβασης του οργανισμού . Οργανισμοί αντιμετωπίζουν σημαντική έκθεση ασφαλείας κατά τη διάρκεια των συνήθων λειτουργιών πληροφορικής. Για παράδειγμα, δεκάδες διαχειριστές του συστήματος μπορούν να μοιράζονται τους κωδικούς πρόσβασης για προνομιούχους λογαριασμούς για χιλιάδες συσκευές. Όταν οι διαχειριστές του συστήματος συνεχίσουν, οι κωδικοί πρόσβασης που χρησιμοποιούσαν κατά τη διάρκεια της εργασίας τους, συχνά παραμένουν αμετάβλητοι, αφήνοντας τις εταιρίες ευάλωτες σε επιθέσεις από πρώην υπαλλήλους και εργολάβους .

Ασθενής διαχείριση κωδικού πρόσβασης σημαίνει ότι οι πιο

ευαίσθητοι κωδικοί πρόσβασης είναι συχνά οι λιγότερο καλά προστατευμένοι . Η ανάγκη για το συντονισμό ενημέρωσης των κωδικών σε πολλούς ανθρώπους και προγράμματα καθιστά την αλλαγή των πιο ευαίσθητων κωδικών τεχνικά δύσκολο. Αδυναμία για την εξασφάλιση ευαίσθητων κωδικών πρόσβασης εκθέτει οργανισμούς σε μια ποικιλία εκμεταλλεύσεων την ασφάλειας . Ισχυροί, χειροκίνητοι έλεγχοι πρόσβασης σε προνομιακούς λογαριασμούς μπορεί να δημιουργήσει μερικές φορές απροσδόκητους κινδύνους, όπως η διαταραχή της υπηρεσίας στον τομέα της πληροφορικής επιχειρήσεων και κλιμάκωση των φυσικών καταστροφών από μια περιοχή σε μια ολόκληρη οργάνωση.

Αδυναμία σύνδεσης διοικητικών ενεργειών με τους ανθρώπους που τα ξεκίνησαν ενδέχεται να παραβιάζει τις ανάγκες εσωτερικού ελέγχου. Τυπικά οργανωτικές πολιτικές διαχείρισης κωδικού πρόσβασης περιλαμβάνουν (ISO. Standards Catalogue: ISO/IEC JTC 1/SC 27):

- Οι χρήστες θα πρέπει να αναγκαστούν να αλλάξουν τους κωδικούς πρόσβασής τους κατά τη στιγμή της πρώτης χρήσης
- Οι κωδικοί πρόσβασης πρέπει να έχουν μήκος τουλάχιστον οκτώ χαρακτήρες
- Κωδικοί πρόσβασης για όλους τους χρήστες λήγει σε 30 / 60 ημέρες
- Ένα ρεκόρ των πέντε προηγούμενων κωδικών πρόσβασης πρέπει να διατηρηθεί για να αποτραπεί η εκ νέου χρήση αυτών των κωδικών πρόσβασης
- Ένα μέγιστο τρεις διαδοχικές αποτυχημένες προσπάθειες σύνδεσης θα έχει ως αποτέλεσμα στο λογαριασμό του χρήστη να κλειδωθεί έξω
- Οι κωδικοί πρόσβασης δεν πρέπει να εμφανίζονται σε μορφή απλού κειμένου όταν πληκτρολογούνται
- Οι κωδικοί πρόσβασης πρέπει να περιλαμβάνουν τουλάχιστον ένα μικρό χαρακτήρα (a-z), ένας χαρακτήρας κεφαλαίων (A-Ω) και έναν αριθμητικό χαρακτήρα (0 - 9) / μία ειδικό χαρακτήρα (@ # $ & / +)
- Όλες ο προσπάθειες εισαγωγής κωδικού προσπαθεί πρέπει να συνδεθούν μαζί με την ημερομηνία, ώρα, διεύθυνση IP, το όνομα του

μηχανήματος, την εφαρμογή και την ταυτότητα χρήστη για την επιτυχή, ανεπιτυχείς προσπάθειες σύνδεσης

Το σαφές περιβάλλον εργασίας μπορεί να βοηθήσει σε μεγάλο βαθμό στην εξασφάλιση της κατάστασης της ασφάλειας στους οργανισμούς . Το πιο σημαντικά οργανωτικά έγγραφα γενικά βρίσκονται γύρω στα γραφεία του εργαζομένου σε επιτραπέζιους υπολογιστές ανοικτή σε όλα τα άτομα εντός της εταιρείας .

Οι κύριοι λόγοι για μια καθαρή πολιτική γραφείου είναι οι εξής: μια καθαρή επιφάνεια μπορεί να παράγει μια θετική εικόνα όταν οι πελάτες επισκεφθούν την εταιρεία, μειώνει την απειλή ενός περιστατικού ασφάλειας, όπως εμπιστευτικές πληροφορίες να κλειδωθούν μακριά όταν είναι αφύλακτο, ευαίσθητα έγγραφα χωρίς επίβλεψη μπορεί να κλαπούν από κάποιον κακόβουλο. Παραδείγματα σαφών πολιτικών περιβάλλοντος εργασίας περιλαμβάνουν (Kosutic, 2013):

- Κρίσιμες πληροφορίες πρέπει να προστατεύονται όταν δεν απαιτείται για τη χρήση
- Μόνο εξουσιοδοτημένοι χρήστες χρησιμοποιούν το φωτοτυπικό μηχάνημα
- Όλα τα λυτά έγγραφα από τα γραφεία του εργαζομένου θα πρέπει να κατασχεθούν στο τέλος της εργάσιμης ημέρας
- Η επιφάνεια εργασίας των χρηστών δεν πρέπει να περιέχει αναφορά σε οποιοδήποτε έγγραφο, άμεσα ή έμμεσα,

Η διαχείριση της ρύθμισης ελέγχους ασφαλείας που είναι ενσωματωμένη στο λειτουργικό σύστημα ή την εφαρμογή . Στο πεδίο εφαρμογής του ISMS πλαισίου, στόχος είναι να διασφαλιστούν οι ρυθμίσεις ασφαλείας του συστήματος / εφαρμογής που είναι αρκετά περιοριστική για την προστασία του συστήματος (πληροφορίες) χωρίς να επηρεάζει δυσμενώς τη διαθεσιμότητα στην επιχείρηση .

Εάν ένας εισβολέας μπορεί να δει εύκολα το όνομα χρήστη και τον κωδικό πρόσβασης κάποιου, μπορεί να οικειοποιηθούν το εν λόγω χρήστη, και να κάνει τεράστια ζημιά τροποποιώντας κρίσιμες πληροφορίες, να

διαβάσει εταιρικά e-mail, να προκαλέσει ζημιές σε εταιρικές ιστοσελίδες, κλπ. Η διαδικασία σύνδεσης σε ένα λειτουργικό σύστημα ή έλεγχο της εφαρμογής θα πρέπει να ελαχιστοποιεί τον κίνδυνο από μη εξουσιοδοτημένη πρόσβαση. Η διαδικασία ακολουθεί, συνεπώς, ένα αυστηρό σύνολο κανόνων που θα διέπουν τις πληροφορίες που εμφανίζονται στον δυνητικό χρήστη κατά τη διαδικασία log -in .

Δείγμα του λειτουργικού συστήματος και των πολιτικών ελέγχου της εφαρμογής περιλαμβάνουν (Security updates: The upcoming revision of ISO/IEC 27001):

- Όλοι οι χρήστες στην οργάνωση πρέπει να έχει ένα μοναδικό αναγνωριστικό
- Δεν πρέπει να εμφανίζονται λεπτομέρειες του συστήματος ή της εφαρμογής πριν από την log -in
- Στην κατάσταση της log -in αποτυχίας, το μήνυμα λάθους δεν αναφέρει ποιο μέρος των διαπιστευτηρίων είναι εσφαλμένο
- Ο αριθμός των ανεπιτυχών log -in προσπαθειών θα πρέπει να περιορίζεται σε 3/5/6 προσπάθειες
- Κατά τη διάρκεια της log -in διαδικασίας, όλες οι καταχωρήσεις κωδικού πρόσβασης πρέπει να είναι κρυμμένες με ένα σύμβολο
- Η χρήση βοηθητικού προγράμματος πρέπει να περιορίζεται π.χ. βοηθητικό πρόγραμμα κωδικού πρόσβασης
- Όλα τα λειτουργικά συστήματα και εφαρμογές θα πρέπει να λήγουν λόγω αδράνειας σε 5/10/15/30 λεπτά
- Όλες οι αιτήσεις θα πρέπει να έχουν αποκλειστικά διοικητικά μενού για να ελέγχονται τα δικαιώματα πρόσβασης των χρηστών

Η ασφάλεια των δικτύων αποκτά σημασία στην οργάνωση, όταν έγινε αντιληπτό ότι τα δίκτυα αλλάζουν συχνά, καθώς νέοι χρήστες και συσκευές προστίθενται και εισάγονται νεότερες τεχνολογίες επικοινωνίας δεδομένων, γίνεται χρήση διαφόρων δικτύων, επικοινωνιών και τεχνολογιών πληροφορικής με σκοπό να αντιμετωπιστεί αποτελεσματικά η ανάγκη επέκτασης, τα ευαίσθητα δεδομένα μεταδίδονται συνεχώς μέσω δικτύων, η

διάδοση της πρόσβασης στο Διαδίκτυο έχει αυξήσει την ευπάθεια καθώς οι εργαζόμενοι χρησιμοποιούν στο διαδίκτυο για περισσότερες πληροφορίες και γνώσεις.

Οι κύριοι στόχοι της πολιτικής ασφάλειας του δικτύου θα πρέπει να είναι να διασφαλιστεί ότι η πρόσβαση στο δίκτυο της εταιρείας παρέχεται μόνο σε εξουσιοδοτημένους χρήστες, την ύπαρξη επαρκών ελέγχων για τη διαχείριση απομακρυσμένων χρηστών, ότι όλος ο εξοπλισμός μπορεί να αναγνωριστεί μοναδικά, ότι τα δίκτυα θα πρέπει να διαχωρίζονται με βάση τις ανάγκες και τα κατάλληλα πρωτόκολλα δρομολόγησης του δικτύου. Τυπικά πολιτικές δηλώσεις για την Ασφάλεια Δικτύων περιλαμβάνουν (Security updates: The upcoming revision of ISO/IEC 27001):

- Κατάλληλοι μηχανισμοί ελέγχου ταυτότητας πρέπει να χρησιμοποιηθούν για τον έλεγχο της πρόσβασης των απομακρυσμένων χρηστών .
- Κατανομή των δικαιωμάτων πρόσβασης στο δίκτυο πρέπει να παρέχεται σύμφωνα με τις απαιτήσεις των επιχειρήσεων και της ασφάλειας
- Έλεγχος ταυτότητας δύο παραγόντων πρέπει να χρησιμοποιείται για τον έλεγχο ταυτότητας των χρηστών που χρησιμοποιούν κινητά / απομακρυσμένα συστήματα

Συμπεράσματα

Κατά την εκπόνηση της πτυχιακής μας εργασίας μελετήσαμε σε βάθος τα πληροφοριακά συστήματα και ασχοληθήκαμε με την ασφάλειά τους. Κατανοήσαμε τι είναι ένα πληροφοριακό σύστημα, πού και πώς χρησιμοποιείται και πού αποσκοπεί η χρήση του από μια εταιρία ή έναν οργανισμό.

Σχετικά με την ασφάλεια των πληροφοριακών συστημάτων, μελετήθηκε βιβλιογραφικά με ποιους τρόπους μπορεί να απειληθεί ένα πληροφοριακό σύστημα και ποιοι είναι οι πιο άμεσοι τρόποι αντιμετώπισης μιας τέτοιας απειλής.

Στη συνέχεια της εργασίας ασχοληθήκαμε εκτενώς με δύο πρότυπα: το ISO 20000 και το ISO 27001, που αφορούν στην τεχνολογία της πληροφορίας, στις τεχνικές ασφαλείας, σε συστήματα διαχείρισης ασφάλειας της πληροφορίας και απαιτήσεις αυτών. Στο κεφάλαιο 2 έγινε μια εκτενής αναφορά στα περιεχόμενα του προτύπου ISO 20000, αναφέροντας τις βασικές γραμμές που επισημαίνονται σε κάθε παράγραφο του αυθεντικού κειμένου. Τέλος, στο κεφάλαιο 3 έγινε ανάλυση του προτύπου ISO 27001, αναφέροντας τα βασικά σημεία τα οποία καταγράφονται μέσα σε αυτό.

Όπως έγινε κατανοητό από την εκπόνηση της συγκεκριμένης πτυχιακής εργασίας, η χρήση ενός πληροφοριακού συστήματος από μία εταιρία ή έναν οργανισμό, όσο μεγάλος ή μικρός και αν είναι, δεν είναι μια απλή υπόθεση. Πρέπει να τηρούνται πολλές προϋποθέσεις, καθώς οι απειλές είναι αρκετές.

Βιβλιογραφία

- Anderson, R., & Jacobsen, B. (1999). The soul at work – unleashing the power of complexity science for business success. *Orion Business*, 1st ed., Orion Publishing Group Ltd, London
- Avison, D. Fitzgerald, G.(1995), *Information Systems Development*, 2nd ed, McGraw-Hill.
- Baden-Fuller, C., & Pitt, M. (2006), *Strategic Innovation: An International Casebook on Strategic Management*. London: Routledge
- Bank of Cyprus.,(2009), Χρήση Υπηρεσίας Internet, Ανάκτηση στις 15-3-2015 από http://www.bankofcyprus.gr/main.asp?id=8819
- Bayne (2000), Trust in E-Banking, CRC Press LLC, CIMdata
- Buffenoir T. 'Security in the OSI Model', Computer Networks and ISDN Systems 15, 1988, 145-150.
- Champine G., Geer D., 'Project ATHENA as a Distributed Computer System', Computer, Sep. 1990, 40-51.
- Chapman, D. B., & Elizabeth, D. BUILDING internet.
- Cisco Systems, Inc "Reference Guide A Primer for Implementing a Cisco Virtual Private Network", Aug 2000
- Clarke, S. (2012). *Information systems strategic management: an integrated approach*. Routledge.
- Cohen, F. (1987). Computer viruses: Theory and experiments. *Computers & Security*, 6(1), 22-35
- Cohen, F.(2005),*Computer Viruses*, ASP Press
- Davenport, T. (1998). Putting the enterprise into the enterprise system. *Harvard Business Review*, 76(4)
- Dhillon, G. (2007). *Principles of Information Systems Security: text and cases*(pp. 97-129). New York: Wiley.
- DoD, 'Trusted Computer Evaluation Criteria', CSC-STD-001-83,

Department of Defence, Computer Security Center, 1983.

- Dugmore, J. (2006a). "BS 15000 to ISO/IEC 20000 What difference does it make?". *ITNOW* 48 (3): 30.
- EFG.,(2009), Ασφάλεια Συναλλαγών, Ανάκτηση στις 15-3-2015 από http://www.eurobank.gr/online/home/viewServices.aspx?id=89&mid=394&lang=gr
- Feinler E and Postel J., (1978), APRANET Protocol handbook, Defence Communications Agency, Data Composition, San Francisco.
- Ferguson, N.(2003), *Practical Cryptography*. John Wiley & Sons
- Fredrik D., and Westall S.(2010) "Technical Woes Halt Some Iran Nuclear Machines – Dips," *Reuters*, November
- Freier, A., Karlton, P., & Kocher, P. (2011). The secure sockets layer (SSL) protocol version 3.0.
- Gilaninia, S., Mousavian, S. J., Taheri, O., Nikzad, H., Mousavi, H., & Zadbagher Seighalani, F. (2012). Information Security Management on performance of Information Systems Management. *J. Basic. Appl. Sci. Res*,*2*(3), 2582-2588.
- Hamlen, K., Kantarcioglu, M., Khan, L., & Thuraisingham, B. (2010). Security issues for cloud computing. *International Journal of Information Security and Privacy (IJISP)*, 4(2), 36-48.
- Hamlin, C. L. (2006). U.S. Patent No. 7,155,616. Washington, DC: U.S. Patent and Trademark Office.
- Hawa, M., & Petr, D. W. (2002). Quality of service scheduling in cable and broadband wireless access systems. In Quality of Service, 2002. Tenth IEEE International Workshop on (pp. 247-255). IEEE.
- http://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/w32_stuxnet_dossier.pdf.
- http://www.symantec.com/content/en/us/enterprise/media/security_response/white0papers/w32_stuxnet_dossier.pdf.

· ISO 20000-1:2011 Part 1

· ISO 27001:2013 – Understanding the New Standard". The Pragmatic Auditor.

· ISO. Standards Catalogue: ISO/IEC JTC 1/SC 27

· ISO/IEC 27001

· ISO/IEC FDIS 27001

· John Wiley & Sons, Second edition,1996 , ISBN: 0-471-11709-9

· Kennedy D. (1997). Who' s on line ; *Inc Technology*, 1, 34-39

· Kosutic, D. (2013). A first look at the new ISO 27001.

· Kotler, P.(2002) *Marketing Principles*, McGraw Hill

· Kotler, P., (1997), "Marketing Management" 9thEd.N.J.: Prentice - Hall

· Kroenke, D. M., & Hooper, T. (2011). *Using Mis*. Pearson.

· Kurose, J.(2005), *Computer Networking – A Top-Down approach featuring the Internet*. Addison-Wesley

· Matyas, V., & Zdenek, J.R. (2000). *Biometric authentication systems*. Technical report, ECOM-Monitor

· Meidan (2006), Consumer Behavior: Concepts and Applications, 4th ed., McGraw-Hill, New York, NY.,

· Millennium.,(2010), Ασφάλεια στο Banking, Ανάκτηση στις 15-3-2015 απόhttps://ebanking.millenniumbank.gr/eBankingWeb/assets/userManualPDFs/el_GR/Retail_manual.pdf

· NBG.,(2009), E-Banking, Ανάκτηση στις 15-3-2015 από https://homebank.nbg.gr/nbgib/helpFiles/el_GR/info/security_info.jsp

· Nicolas Falliere, Liam O Murchu, and Eric Chien, W32.Stuxnet Dossier, Version 1.1, Symantec, accessed at

· Nilson, A. (1994). *Standard a system of business*. Stockholm:IMIT

· NUA.,(2008), Η χρήση του Ίντερνετ-Κατανομή Χρηστών Παγκοσμίως, Ανάκτηση στις 16-7-2014 από http://www.nua.com

· OnlineTools.,(2009), Ασφάλεια Συναλλαγών, Ανάκτηση στις 15-3-2015 απόhttp://www.onlinetools.gr/index.php?target=pages&page_id=asfaleiasinallagon

· Paschos, G. S., Papapanagiotou, I., Argyropoulos, C. G., & Kotsopoulos, S. A. (2006, August). A heuristic strategy for ieee 802.16 wimax scheduler for quality of service. In 45th Congress FITCE.

· Peltier, T. R. (2013). *Information security fundamentals*. CRC Press.

· Reichheld, T.Y., & Schefter, K.J. (2000). Supply networks and complex adaptive systems: control versus emergence. *Journal of Operations Management*, 19(3), 351-66

· Reid, R. and Trueman,M.(2004) 'The internet: new international marketing issues' Management research news, Vol. 25, No.12, p.59

· Robert McMillan (2010). "Siemens: Stuxnet worm hit industrial systems". Computerworld. Retrieved 16 September 2010.

· Ross, A.(2001), *Security Engineering: A Guide To Building Dependable Distributed Systems.* John Wiley and Sons Ltd,

· Schneier, B. (2007). Applied cryptography: protocols, algorithms, and source code in C. john wiley & sons.

· Schneier, B.(2006), *Applied Cryptography*. John Wiley & Sons, Inc., 2nd edition

· Security updates: The upcoming revision of ISO/IEC 27001. DNV Business Assurance.

· Simkin D, Pride and Ferrell.,(2006),Marketing, concepts and strategies, Houghton Mifflin

· Slack, N-Chambers, S. and Johnston, R.(2004), *Operations Management*, 4th Edition, Harlow: FT/Prentice Hall

· Spears, J. L., & Barki, H. (2010). User participation in information systems security risk management. *MIS quarterly*, *34*(3), 503-522.

· Tipton, H. F., & Krause, M. (2012). *Information security management handbook*. CRC Press.

· Wenbo, M.(2003), *Modern Cryptography: Theory and Practice*. Prentice Hall

· Whitman, M., & Mattord, H. (2013). *Management of information security*. Cengage Learning.

· William Stallings, "Cryptography and Network Security: Principles and Practice, second edition", Prentice Hall, 1999, ISBN: 0-13-869017-0

· Wongthavarawat, K., & Ganz, A. (2003). Packet scheduling for QoS support in IEEE 802.16 broadband wireless access systems. International Journal of Communication Systems, 16(1), 81-96.

· Wood, M. C. (2006). An Analysis of the Design and Implementation of QoS over IEEE 802.16. Washington University, St. Louis http://www. cse. wustl. edu/~ jain/cse574-06/ftp/wimax_qos.

· Αναστασιάδης, Τ. (1998), "Ηλεκτρονικό Εμπόριο: Αγοράζοντας Μέσω Internet", Δημοσιογραφικός Οργανισμός Λαμπράκη, Οικονομικός Ταχυδρόμος, (23),19, σ.σ.51-60

· Αρσάνογλου Γ.(2007), Ανάπτυξη Λογισμικού Προσομοίωσης Ασυρμάτων Δικτύων τύπου Μανετ, Αριστοτέλειο Πανεπιστήμιο Θεσσαλονίκης

· Βασιλακόπουλος, Γ., & Χρυσικόπουλος, Β. (1990). *Πληροφοριακά Συστήματα Διοίκησης: Ανάλυση και Σχεδιασμός*. Αθήνα: Σταμούλη.

· Βασιλείου, Μ.(1999), "Η Ελληνική Επιχείρηση στο Internet", Δημοσιογραφικός Οργανισμός Λαμπράκη, (23) 71, σ.σ.38-48

· Βεργίνης, Δ., Κοντούλη, Ε., Λάλας, Χ., Λαοπόδης, Β., Μανουσαρίδης, Ζ., Μπακογιάννης, Σ. (2000). *Πληροφοριακά Συστήματα*, Αθήνα: Οργανισμός Λιβάνης ΑΒΕ.

· Γ. (2006), Ολοκληρωμένα Συστήματα Διαχείρισης Επιχειρησιακών Πόρων, Αθήνα, Εκδόσεις Σταμούλης, σελ. 16
· Γιαννόπουλος Γ.Ν.,(2001), Προστασία Προσωπικών Δεδομένων και διανοσυριακή ροή πληροφοριών, Τόμος 11, Εκδόσεις Σάκουλας, σελ. 733
· Δημητριάδης, Α.(1998), *Διοίκηση-Διαχείριση πληροφοριακών Συστημάτων*, Νέες Τεχνολογίες, σελ 26
· Δρανίδης, Δ., & Κεχρής, Ε. (2012). *Πληροφοριακά Συστήματα*. ΤΕΙ Θεσσαλονίκης
· Επίσημη εφημερίδα της Ευρωπαϊκής Ένωσης[http://eur-lex.europa.eu/JOIndex.do?ihmlang=it], αρ. φυλ. C115, 4/5/2010, σελ. 24-25: http://eur-lex.europa.eu/ LexUriServ/LexUriServ.do?uri= OJ:C:2010:115:FULL:IT:PDF
· Εργαστήριο Εκπαιδευτικής και Γλωσσικής Τεχνολογίας.,(2010), Token Ring, http://hermes.di.uoa.gr/RETUDIS/Token%20ring/Main.htm
· Ιγγλεζάκης Ι.,(2001), Τραπεζικές συναλλαγές μέσω Ίντερνετ, περιγραφή και Νομική προβληματική, Συνήγορος, σελ. 205
· Ιωάννου Γ. (2006), Ολοκληρωμένα Συστήματα Διαχείρισης Επιχειρησιακών Πόρων, Αθήνα, Εκδόσεις Σταμούλης, σελ. 16
· Κάτσικα, Σ., Γκρίτζαλη, Δ., & Γκρίτζαλη, Σ. (2004). *Ασφάλεια Πληροφοριακών Συστημάτων*. Εκδόσεις Νέων Τεχνολογιών
· Κιουντούζης Ε.(2000), *Μεθοδολογίες Ανάλυσης και Σχεδιασμού Πληροφοριακών Συστημάτων*, Μπένος
· Κοτζανικολάου, Π. (2005). *Τεχνολογίες και Πολιτικές Ασφάλειας*. Τμήμα Πληροφορικής, Πανεπιστήμιο Πειραιώς
· Λαοπόδης Β, 1992, Πληροφοριακά Συστήματα: Υλοποίηση και Μάνατζμεντ Συστημάτων, Εκδ. Νέων Τεχνολογιών.
· Λέανδρος, Ν.(2005), Το διαδίκτυο Ανάπτυξη και Αλλαγή, Αθήνα: Εκδόσεις Καστανιώτη, σελ 13-14

· Μάλλας Δημάτρης, (2007). Νέες τεχνολογίες πληροφορικής .Βήμα Net Economy

· Μπούρας Χ.Ι.,(2009), Δίκτυα Δημόσιας Χρήσης και Διασύνδεση Δικτύων', Πανεπιστημιακές σημειώσεις

· Οικονόμου, Γ., & Γεωργόπουλος, Ν. (1995). *Πληροφοριακά Συστήματα για την Διοίκηση Επιχειρήσεων*. Αθήνα: Ευγ. Μπένου

· Παπαδάκης Β(2002), Στρατηγική των Επιχειρήσεων, Μπένος, σελ 53-62

· Ράπτης, Α. & Ράπτη, Α., 1998, «Πληροφορική και Εκπαίδευση: συνολική προσέγγιση», Αθήνα

· Σιασιάκος Κ. (2006), Συστήματα Πληροφοριών Διοίκησης, ΑΤΕΙ Χαλκίδας, ανακτήθηκε από http://www.teihal.gr/bus/labs/downloads/kef2mis.pdf

· Σιασιάκος Κ. (2006), Συστήματα Πληροφοριών Διοίκησης, ΑΤΕΙ Χαλκίδας, ανακτήθηκε από http://www.teihal.gr/bus/labs/downloads/kef2mis.pdf

· Σταματίου.,(2009), Κρυπτογραφικά ασφαλής επικοινωνία, Ανάκτηση στις 15-3-2015 από http://docs.google.com/viewer?a=v&q=cache:gzAnxlc0KJYJ:nefeli.dsmc.eap.gr/ojs-2.1.1/index.php/HOUJOI/article/view

· Τζωρτζάκης και Τζωρτζάκη, 2002, «Οργάνωση και διοίκηση επιχειρήσεων», Rossili

· Χαραμής, Γ. (1994). *Ανάλυση και Σχεδιασμός Πληροφοριακών Συστημάτων*. Αθήνα: Ανικούλα.