ΤΕΧΝΟΛΟΓΙΚΟ ΕΚΠΑΙΔΕΥΤΙΚΟ ΙΔΡΥΜΑ ΠΑΤΡΩΝ
ΣΧΟΛΗ : ΔΗΜΟΣΙΑ ΔΙΟΙΚΗΣΗΣ
ΤΜΗΜΑ: ΕΠΙΧΕΙΡΗΜΑΤΙΚΟΥ ΣΧΕΔΙΑΣΜΟΥ ΚΑΙ ΠΛΗΡΟΦΟΡΙΑΚΩΝ ΣΥΣΤΗΜΑΤΩΝ

Π Τ Υ Χ Ι Α Κ Η Ε Ρ Γ Α Σ Ι Α

ΜΕΘΟΔΟΛΟΓΙΑ, ΠΡΟΒΛΗΜΑΤΑ ΚΑΙ ΕΦΑΡΜΟΓΕΣ ΚΑΤΑ ΤΗΝ ΟΡΓΑΝΩΣΗ ΚΑΙ ΕΓΚΑΤΑΣΤΑΣΗ ΕΝΟΣ ΕΠΙΧΕΙΡΗΣΙΑΚΟΥ ΔΙΚΤΥΟΥ

ΟΝΟΜΑΤΕΠΩΝΥΜΟ: ΦΛΟΥΔΑ Γ. ΑΙΚΑΤΕΡΙΝΗ
ΕΠΟΠΤΕΥΩΝ ΚΑΘΗΓΗΤΗΣ: ΔΑΡΣΙΝΟΣ ΒΑΣΙΛΕΙΟΣ

ΠΑΤΡΑ 2011

ΕΙΣΑΓΩΓΗ

Η πρόοδος και η έξαρση της τεχνολογίας αποτελεί ένα αναμφισβήτητο γεγονός στη σύγχρονη εποχή. Το σημαντικότερο τεχνολογικό επίτευγμα αυτής της έξαρσης είναι η εξέλιξη του τομέα της Πληροφόρησης. Η ανάπτυξη του τομέα της τεχνολογίας της Πληροφόρησης έχει επηρεάσει και έχει επιδράσει στην καθημερινότητα χιλιάδων ανθρώπων. Η επίδραση αυτή αφορά πολλούς και διαφορετικούς τομείς της καθημερινότητας. Η σημαντικότερη όμως επίδραση είναι στον τομέα της επικοινωνίας. Η πραγματοποίηση της επικοινωνίας έχει αλλάξει ριζικά τα τελευταία χρόνια. Για παράδειγμα, η πραγμάτωση απλών και καθημερινών δραστηριοτήτων σε σχέση με την επικοινωνία έχει αλλάξει εντελώς τοπίο. Η επικοινωνία είναι πλέον ταχύτερη και πιο άμεση. Επιπλέον, η επικοινωνία αποκτά μεγαλύτερη σιγουριά καθώς υπάρχουν πια πολύ περισσότερα μέσα προς αυτό το σκοπό. Και αυτά τα νέα μέσα είναι σε θέση να προσφέρουν τη σιγουριά πως η επικοινωνία δεν θα διαταραχθεί. Προσφέρεται επίσης η βεβαιότητα πως η ανταλλαγή πληροφοριών μέσω των νέων μέσων δεν αντιμετωπίζει κίνδυνο απώλειας.

Η πιο σημαντική ανάπτυξη προς αυτή την κατεύθυνση είναι η δημιουργία και η εξάπλωση του Διαδικτύου. Η διαφορά ανάμεσα στις δυνατότητες που παρουσιάστηκαν αλλά και που εξακολουθούν να παρουσιάζονται σε σχέση με τις τεχνολογικά παλαιότερες μορφές επικοινωνίας και τον κόσμο του Διαδικτύου, είναι τεράστιες. Το Διαδίκτυο παρουσιάζει την πιο ταχύτατα εξελιγμένη μορφή επικοινωνίας. Η εμφάνιση του, και η απήχηση του στο κοινό, μέσω της εμπορευματοποίησης του, εδραίωσαν τη θέση του μέσου, και το τοποθέτησαν υψηλότερα από οποιοδήποτε άλλο μέσο. Η επιτυχία του μέσου βασίζεται στο γεγονός πως το Διαδίκτυο προσφέρει αποτελεσματική, σίγουρη, γρήγορη ακόμη και σχεδόν άμεση και χαμηλή σε κόστος επικοινωνία. Επιπλέον, η τεχνολογία του Διαδικτύου ανοίγει νέες δυνατότητες για επικοινωνία. Οργανισμοί και εταιρίες έχουν πλέον τη δυνατότητα να επικοινωνούν άμεσα, και με σχεδόν μηδαμινό κόστος, χωρίς να απαιτείται η παρουσία ανθρώπων στο ίδιο μέρος.

ΚΕΦΑΛΑΙΟ 1 : ΕΠΙΧΕΙΡΗΣΙΑΚΑ ΔΙΚΤΥΑ ΥΠΟΛΟΓΙΣΤΩΝ

1.1. ΕΝΝΟΙΑ ΤΟΥ ΔΙΚΤΥΟΥ

Αρχικά η έννοια του δικτύου στις τηλεπικοινωνίες ήταν συνυφασμένη με τα δίκτυα της τηλεφωνίας. Με το πέρασμα των χρόνων, η εμφάνιση των υπολογιστών και η διασύνδεση τους άρχισαν να αναπτύσσονται και σε δίκτυα για τη μετάδοση δεδομένων.

Δίκτυο είναι ένα σύνολο υπολογιστών και συσκευών που διαθέτουν κατάλληλο υλικό εξοπλισμό και λογισμικό, ώστε να επικοινωνούν μεταξύ τους με στόχο το διαμοιρασμό των κοινών πόρων (π.χ. των εκτυπωτών, των δίσκων, των σαρωτών κλπ), την κοινή εκμετάλλευση πληροφοριών μεταξύ των χρηστών. Η δικτύωση των υπολογιστών προσφέρει την δυνατότητα ανάμειξης της πληροφορίας, των επικοινωνιών και της διασκέδασης[1].

Βασικός μας στόχος σε αυτό το κεφάλαιο είναι να αναλύσουμε και να αναφερθούμε στα διάφορα είδη δικτύων και στις κατηγορίες αυτών.

1.2.ΕΤΑΙΡΙΚΑ ΚΑΙ ΕΠΙΧΕΙΡΗΣΙΑΚΑ ΔΙΚΤΥΑ

Η εποχή που οι χρήστες των προσωπικών υπολογιστών δουλεύουν απομονωμένα στα γραφεία τους εκμεταλλευόμενοι μόνο τους υπολογιστικές δυνατότητες, τον αποθηκευτικό χώρο και τα περιφερειακά του υπολογιστή τους, όλο και απομακρύνεται.

Σε ένα σύγχρονο περιβάλλον εργασίας, οι χρήστες των προσωπικών υπολογιστών μπορούν να αντλούν στοιχεία από άλλους υπολογιστές, να εκμεταλλεύονται τις δυνατότητες τους, να επικοινωνούν με άλλους χρήστες ανά πάσα στιγμή, οι οποίοι μπορεί να βρίσκονται και στο ίδιο κτίριο, στον ίδιο όροφο, στην ίδια πόλη, σε οποιοδήποτε σημείο του πλανήτη και όλα αυτά με τη σημαντική βοήθεια των δικτύων.

Κύριες ιδιότητες ενός δικτύου είναι να επιτρέπει σε πολλούς χρήστες να μοιράζονται ή να ανταλλάσουν πληροφορίες και να εκμεταλλεύονται την επεξεργαστική ικανότητα άλλων υπολογιστών, να έχουν πρόσβαση σε βάσεις δεδομένων και άλλα. Όμως, ακριβώς αυτή η προσφερόμενη δυνατότητα όπου ο καθένας με μια φθηνή τερματική συσκευή (π.χ. PC) μπορεί να επικοινωνεί με άλλους υπολογιστές δημιουργεί και τα μεγάλα προβλήματα. Θέλει μεγάλη προσοχή, σαφείς κανόνες, μεγάλη αυστηρότητα και συνεπώς μεγάλη πολυπλοκότητα για να εξασφαλισθεί η με σαφείς όρους συμμετοχή του καθενός σε ένα τέτοιο δίκτυο[2].

Στα πλαίσια του συνεχώς αυξανόμενου ανταγωνισμού στο τομέα των επιχειρήσεων, η χρήση ηλεκτρονικών υπολογιστών έχει γίνει επιτακτική ανάγκη για τη βιώσιμη ανάπτυξη και εξέλιξη τους.

Πολλές εταιρείες διαθέτουν σημαντικό αριθμό υπολογιστών σε λειτουργία τόσο σε μικρή απόσταση όσο και σε μεγάλες αποστάσεις μεταξύ τους.

Έστω ότι σε κάθε υποκατάστημα υπάρχει υπολογιστής για την τήρηση των στοιχείων της αποθήκης, για την παρακολούθηση των λογαριασμών των πελατών, για την εξαγωγή της μισθοδοσίας του προσωπικού και άλλα. Αν οι υπολογιστές της εταιρείας δουλεύουν μεμονωμένα (δεν είναι συνδεδεμένοι σε δίκτυο), τότε τα κεντρικά γραφεία δεν λαμβάνουν έγκαιρα την πραγματική εικόνα της αποθήκης και των οικονομικών των πελατών του υποκαταστήματος, κάτι το οποίο μπορεί να δημιουργήσει σημαντικά και με οικονομικό αντίκτυπο προβλήματα. Για παράδειγμα, δεν είναι δυνατή η άμεση γνώση των ελλείψεων

[1] Γ.Πάγκαλος και Ι.Μαυρίδης “Ασφάλεια Πληροφοριακών Συστημάτων και Δικτύων

[2] Andrew S.Tanenbaum “Δίκτυα Υπολογιστών”

που μπορεί να παρουσιάζονται στις κατά τόπους αποθήκες, ώστε να μπορέσει να γίνει η άμεση και μαζική παραγγελία στους προμηθευτές. Έχοντας γνώση οι ανάλογοι αρμόδιοι κάνοντας την μαζική παραγγελία θα έχει σαν αποτέλεσμα την εξοικονόμηση χρόνου και χρήματος.

Άρα, από την δικτύωση η εταιρεία θα κέρδιζε άμεση ενημέρωση για κεντρική λήψη αποφάσεων, χαμηλότερο κόστος προμηθειών και λειτουργίας και σωστή κατανομή του ανθρώπινου δυναμικού.

Στην περίπτωση όμως που οι υπολογιστές της εταιρίας είναι συνδεδεμένοι σε ένα δίκτυο είναι δυνατό να χρησιμοποιούν όλοι το ίδιο πρόγραμμα (με μικρή σχετικά επιβάρυνση για δικτυακή χρήση) τους ίδιους εκτυπωτές και τον ίδιο δικτυακό εξοπλισμό για τη σύνδεση τους στο Internet και τα άλλα δίκτυα. Άρα, από τη δικτύωση η επιχείρηση θα πετύχαινε καλύτερη αξιοποίηση και εκμετάλλευση των πόρων από την κοινή χρήση εξοπλισμού και προγραμμάτων.

Εκτός όμως από τα οικονομικά οφέλη και την καλύτερη δυνατή εκμετάλλευση προσωπικού και πόρων, η οργάνωση των υπολογιστών σε δίκτυο αυξάνει την αξιοπιστία του όλου συστήματος.

Στα πρώτα μοντέλα υπολογιστικών συστημάτων, που χρησιμοποιήθηκαν από επιχειρήσεις ο καθένας από τους υπολογιστές αυτούς μπορούσε να αξιοποιείται ξεχωριστά από τους υπόλοιπους, όπως αναφέραμε. Με την πάροδο των χρόνων και την αλματώδη ανάπτυξη τόσο της πληροφορικής και των τηλεπικοινωνιών, οι επιχειρήσεις και οι άλλοτε μικρομεσαίες εταιρίες άρχισαν να αποκτούν άμεση πρόσβαση στη πληροφορία, να γιγαντώνονται και έτσι προκύπτει το πρόβλημα του ορθού καταμερισμού των πόρων.

Η διοίκηση τότε των επιχειρήσεων αυτών ήταν αυτή που αποφάσισε την διασύνδεση όλων των υπολογιστών με στόχο αφενός μεν να καταστούν διαθέσιμα όλα τα προγράμματα, ο εξοπλισμός και προπάντων τα δεδομένα σε οποιονδήποτε στο δίκτυο ανεξαρτήτου φυσικής θέσεως του πόρου και του χρήστη, αφετέρου την απόκτηση δυνατότητας εξαγωγής και συσχέτισης πληροφοριών που αφορούν ολόκληρη την επιχείρηση.

Ένα ακόμα πολύ θετικό στοιχείο για τη λειτουργία μιας επιχείρησης που ανακύπτει από την χρήση των δικτύων υπολογιστών, είναι και η υψηλή αξιοπιστία που παρέχει ένα δίκτυο όσων αφορά την ασφάλεια διατήρησης των δεδομένων. Αυτό επιτυγχάνεται μέσω εναλλακτικών πηγών τροφοδοσίας και έχει σαν αποτέλεσμα ακόμη και στην περίπτωση που κάποια μονάδα επεξεργασίας βγει εκτός λειτουργίας, οι άλλες να είναι σε θέση να αναλάβουν την αντικατάστασή της και την άμεση τέλεση της εργασίας της.

Πρέπει να αναφέρουμε όμως ότι πολύ σημαντικός παράγοντας είναι αυτός της εξοικονόμησης χρημάτων τόσο για τις ιδιωτικές επιχειρήσεις που ως γνωστό ο κερδοσκοπικός τους χαρακτήρας το επιβάλλει, όσο και για έναν οργανισμό ή μια δημόσια υπηρεσία με αξιόλογο αριθμό εργαζομένων και κατ' επέκταση μεγάλο αριθμό υπολογιστικών μονάδων.

Είναι αδιαμφισβήτητα γεγονός ότι οι μικροί υπολογιστές, δηλαδή οι υπολογιστές γραφείου, οι οποίοι έχουν χαμηλό κόστος και σχετικά καλή επίδοση. Σε αντίθεση όμως οι μεγάλοι υπολογιστές είναι κατά πολύ ταχύτεροι από τους προσωπικούς υπολογιστές αλλά το κόστος τους είναι πολύ μεγαλύτερο.

Οι ανάγκες που επέβαλαν τη χρησιμοποίηση τοπικών δικτύων ήταν από την ανάγκη να διαμοιραστεί η χρήση εξοπλισμού (π.χ. ειδικοί υπολογιστές). Επίσης από την ανάγκη για προσπέλαση από απόσταση σε υπολογιστικά συστήματα (π.χ. βάσεις δεδομένων, κοινές βιβλιοθήκες προγραμμάτων), από την ανάγκη για αυτοματισμό και συγχρονισμό ορισμένων μηχανημάτων παραγωγής που πρέπει αν ανταλλάξουν πληροφορίες σε στιγμιαίο χρόνο (real-time) και τέλος για την ανάγκη για αυτόματο έλεγχο ενός εργαστηρίου, ενός τμήματος παραγωγής εργοστασίου κ.τ.λ.

Τα τοπικά δίκτυα χρησιμοποιήθηκαν κυρίως μέσα στις επιχειρήσεις σαν ένα κατ' εξοχήν μέσον επικοινωνίας μεταξύ διαφόρων εφαρμογών, υπηρεσιών ή ατόμων. Στην αρχή δεν επεκτεινόταν πέρα από το χώρο ενός γραφείου αλλά σιγά σιγά εξαπλώθηκαν σε όλα τα επίπεδα του βιομηχανικού τομέα και σήμερα υπάρχουν τοπικά δίκτυα που καλύπτουν αποστάσεις μέχρι 200χλμ (περίπτωση δικτύων FDDI) τα οποία τα κατατάσσουμε σε τρεις κατηγορίες:

- Τα τηλεφωνικά τοπικά δίκτυα που εξυπηρετούνται με τους PABX (Private automatic branch exchange)
- Τα τοπικά δίκτυα baseband
- Τα τοπικά δίκτυα ευρείας μετάδοσης (broadband)

Όπως καταλαβαίνουμε υπάρχει μια ανισσοροπία και γι' αυτό το λόγο αναγκάστηκαν οι σχεδιαστές συστημάτων να δημιουργήσουν συστήματα τα οποία θα αποτελούνται από προσωπικούς υπολογιστές, έναν ανά χρήστη, με τα δεδομένα να κρατούνται σε έναν ή περισσότερους εξυπηρετητές. Αυτό που αναφέραμε είναι η αρχιτεκτονική πελάτη/εξυπηρετητή, δηλαδή γίνεται ανταλλαγή μηνυμάτων αίτησης από τον πελάτη στον εξυπηρετητή, οι οποίοι παρέχουν κεντρικές υπηρεσίες προς τους πελάτες (clients). Ο εξυπηρετητής διεκπεραιώνει την εργασία και στέλνει πίσω την απάντηση. Οι εξυπηρετητές που χρησιμοποιούνται στα τοπικά δίκτυα πελάτη/εξυπηρετητή μπορεί να είναι:

- Εξυπηρετητής αρχείων (file server). Κύρια λειτουργία του είναι η κεντρική αποθήκευση και διαχείριση των αρχείων, τα οποία μοιράζονται από κοινού οι σταθμοί πελάτες.
- Εξυπηρετητής εκτυπώσεων (print server). Κύρια λειτουργία του είναι η διαχείριση των εκτυπωτών και των εκτυπώσεων που ζητούνται από τους υπολογιστές του δικτύου.
- Εξυπηρετητής της βάσης δεδομένων (database server). Κύρια λειτουργία του είναι η εκτέλεση εφαρμογών διαχείρισης βάσεων δεδομένων και η διαχείριση των αρχείων των βάσεων δεδομένων.
- Εξυπηρετητής επικοινωνιών (communication server). Κύρια λειτουργία του είναι η διαχείριση των επικοινωνιών. Διακρίνονται σε:

  Ø Εξυπηρετητές ταχυδρομείου (mail servers), που αναλαμβάνουν την υπηρεσία του ηλεκτρονικού ταχυδρομείου μεταξύ των χρηστών.

  Ø Εξυπηρετητές modem (modem servers), που αναλαμβάνουν το διαμοιρασμό των modem μεταξύ των χρηστών.

  Ø Εξυπηρετητές fax (fax servers), που αναλαμβάνουν τη λήψη και την αποστολή fax και τη διανομή τους στους παραλήπτες.

  Ø Πύλες (gateway servers), που αναλαμβάνουν την επικοινωνία των χρηστών με μεγάλους κεντρικούς υπολογιστές (mainframes), μίνι υπολογιστές, αλλά τοπικά δίκτυα και το Internet.

Στα μικρά δίκτυα ένας υπολογιστής μπορεί να παίζει το ρόλο περισσότερων του ενός εξυπηρετητή. Δηλαδή ένας υπολογιστής μπορεί να είναι και εξυπηρετητής αρχείων και εξυπηρετητής εκτυπώσεων. Οι υπολογιστές που παίζουν το ρόλο του πελάτη είναι γνωστοί και ως σταθμοί εργασίας (workstations).

Ομότιμοι σταθμοί (peer- to -peer) : σε ένα δίκτυο ομότιμων σταθμών δεν υπάρχουν κεντρικοί εξυπηρετητές. Κάθε σταθμός εργασίας παρέχει υπηρεσίες τις οποίες μπορούν να χρησιμοποιούν οι άλλοι σταθμοί του δικτύου. Οι διάφορες υπηρεσίες που παρέχουν οι εξυπηρετητές σε ένα δίκτυο πελάτη – εξυπηρετητή, παρέχονται από κάθε υπολογιστή του δικτύου, αρκεί φυσικά να διαθέτει τους αντίστοιχους πόρους. Για παράδειγμα, αν κάποιος χρήστης, θέλει να εκτυπώσει σε ένα δίκτυο ομότιμων σταθμών, μπορεί να δρομολογήσει την εκτύπωση του σε οποιοδήποτε υπολογιστή του δικτύου που έχει εκτυπωτή.

Με μια απλή πρόσθεση περισσοτέρων επεξεργαστών πάνω στη δικτύωση έχουμε αυτόματα βαθμιαία αύξηση της επίδοσης του συστήματος. Ένα μειονέκτημα που υπάρχει όμως στους μεγάλους υπολογιστές είναι ότι σε περίπτωση που το σύστημα έχει εξαντλήσει τις “δυνάμεις” του, αναγκαστικά θα πρέπει να γίνει αντικατάσταση με αποτέλεσμα την ενόχληση των χρηστών και το σημαντικότερο το μεγάλο κόστος που θα επιβαρύνει την επιχείρηση.

Τέλος, ένα ακόμη πλεονέκτημα που έχει μια επιχείρηση είτε αυτή είναι ιδιωτική ή δημόσια ή και οργανισμός, από την εγκατάσταση επιχειρησιακών δικτύων είναι ότι οι εργαζόμενοι βρίσκονται στην πλεονεκτική θέση στο να επικοινωνούν μεταξύ τους άμεσα και ταχύτατα ενώ βρίσκονται σε μεγάλες αποστάσεις να εκτελούν και να φέρνουν εις πέρας εργασίες που απαιτούν ομαδική συμβολή για την επίτευξη των στόχων της επιχείρησης.

1.3. ΟΙΚΙΑΚΑ ΔΙΚΤΥΑ ΥΠΟΛΟΓΙΣΤΩΝ

Με τη πάροδο των χρόνων τα δίκτυα υπολογιστών έγιναν δημοφιλή μόνο όταν τα δίκτυα προσωπικών υπολογιστών άρχισαν να προσφέρουν μεγαλύτερο πλεονέκτημα προς επίδοση, σε σχέση με τους μεγάλους υπολογιστές. Ωστόσο είναι ένα ευέλικτο εργαλείο που μπορεί να χρησιμοποιηθεί για μεγάλο εύρος εφαρμογών[3].

Στις αρχές της δεκαετίας του 1990, τα δίκτυα υπολογιστών άρχισαν να παρέχουν υπηρεσίες σε ιδιώτες, με την μορφή τοπικών οικιακών δικτύων. Οι υπηρεσίες αυτές διακρίνονται: πρόσβαση σε απομακρυσμένες πληροφορίες, η διασκέδαση με αλληλεπίδραση και η επικοινωνία πρόσωπο με πρόσωπο.

Όσον αφορά την πρόσβαση σε απομακρυσμένες πληροφορίες έχει αρκετές μορφές. Οι περισσότεροι άνθρωποι πλέον περατώνουν τραπεζικές συναλλαγές, αγορές μέσω ηλεκτρονικού εμπορίου, οι λίστες των προϊόντων και των υπηρεσιών που προσφέρει το διαδίκτυο ανά τακτά χρονικά διαστήματα, ίσως και σε καθημερινή βάση, ενημερώνονται και προκαλούν το ενδιαφέρον των χρηστών. Σταδιακά, η πρόσβαση στην πληροφόρηση και την ενημέρωση έγινε πολύ πιο εύκολη, δεν χρειάζεται πλέον να ανατρέξει κανείς σε ένα βιβλιοπωλείο ή μια βιβλιοθήκη για να βρει κάποιο βιβλίο η κάποια πληροφορία ή ακόμα και να διαβάσει τα νέα της ημέρας, το μόνο που χρειάζεται να κάνει είναι να δώσει σε μια μηχανή αναζήτησης ένα τίτλο ή μια λέξη και αυτόματα έχει μπροστά του ο χρήστης αμέτρητες πληροφορίες για να διαλέξει.

Στην δεύτερη κατηγορία αναφέραμε τις υπηρεσίες διασκέδασης με αλληλεπίδραση. Δίνεται η δυνατότητα στο χρήστη να εκτελέσει άπειρες εφαρμογές μέσα από τον υπολογιστή του. Το πιο απλό παράδειγμα είναι να ακούσει κάποιο τραγούδι ή και να το εγκαταστήσει, να δει κάποια ταινία που επιθυμεί ή να παίξει κάποιο παιχνίδι, όλα αυτά βέβαια μπορούν να βρεθούν στο προσωπικό υπολογιστή οποιουδήποτε χρήστη δωρεάν ή καταβάλλοντας κάποιο χαμηλό χρηματικό ποσό. Ωστόσο, στην περίπτωση των απλών παιχνιδιών ή παιχνιδιών με διάφορες απαιτήσεις (π.χ. γραφικά, ήχος), τότε η εγκατάσταση δικτύου υπολογιστών απογειώνει την ευχαρίστηση των φανατικών του είδους. Είναι σημαντικό να προσθέσουμε ότι πρόκειται ίσως για την πιο ταχέως αναπτυσσόμενη βιομηχανία.

Τελευταία κατηγορία είναι η επικοινωνία πρόσωπο με πρόσωπο και μάλιστα η πιο ευρέως διαδεδομένη για τη χρήση των δικτύων. Χαρακτηριστικό παράδειγμα αυτής της κατηγορίας αποτελεί το ηλεκτρονικό ταχυδρομείο το οποίο είναι ισοδύναμο της υπηρεσίας του παραδοσιακού ταχυδρομείου. Χρησιμοποιείται από εκατομμύρια ανθρώπους και επιτρέπει εκτός από τη μεταφορά κειμένων αλλά τώρα πια και τη μεταφορά ήχου και εικόνας. Έτσι, μπορούν οι χρήστες να πραγματοποιήσουν τηλεδιασκέψεις και να επικοινωνούν χωρίς καθυστερήσεις, δίνεται η δυνατότητα στο χρήστη να έχει εκπαίδευση από απόσταση. Επίσης, μέσω του ηλεκτρονικού ταχυδρομείου μπορούν να πραγματοποιηθούν εφαρμογές κοινωνικού χαρακτήρα όπως η λήψη ιατρικών διαγνώσεων από ειδικούς σε απομακρυσμένες περιοχές. Το καλό και ταυτόχρονα κακό χαρακτηριστικό του e-mail είναι η

[3] Andrew S.Tanenbaum “Δίκτυα Υπολογιστών”

δυνατότητα του να αποστέλλει μηνύματα προς μεγάλες ομάδες αποδεκτών με την ίδια ευκολία που αποστέλλει προς ένα και μοναδικό δέκτη, με αποτέλεσμα μερικές φορές τον αθέλητο βομβαρδισμό ενός χρήστη με ηλεκτρονική αλληλογραφία.

Τέλος , θα αναφέρουμε τα forum, τα οποία είναι "δωμάτια" συζητήσεων στα οποία μπορεί ο οποιοσδήποτε να συμμετάσχει ανταλλάσσοντας απόψεις πάνω σε θέματα που τον αφορούν. Πρέπει να σημειωθεί ότι η θεματολογία των χωρών αυτών είναι πολύ μεγάλη και συνεχώς περιλαμβάνει καινούρια θέματα.

1.4. ΚΑΤΗΓΟΡΙΕΣ ΔΙΚΤΥΩΝ

Δίκτυα, μια λέξη με τόσο γενικευμένη έννοια, με μεγάλη και ποικίλη χρήση, τέτοια που πολλές φορές δημιουργούνται ακόμα και παρεξηγήσεις για την ερμηνεία της.

Στην περιοχή της τηλεπληροφορικής αναφέρονται τα δημόσια δίκτυα δεδομένων (π.χ. Hellaspac, Hellascom), το παγκόσμιο Διαδίκτυο (Internet), τα ιδιωτικά δίκτυα (όπως τα τραπεζικά), το ISDN και άλλα[4].

Δίκτυο τηλεπληροφορικής είναι ένα σύστημα επικοινωνιών, το οποίο διαθέτει συσκευές τηλεπικοινωνιών, τηλεπικοινωνιακούς κόμβους, καθώς και τα φυσικά μέσα διέλευσης της πληροφορίας. Επίσης στην ευρύτερη έννοια του περιλαμβάνει και τις τερματικές συσκευές, όπως είναι οι υπολογιστές και τα τερματικά κάθε είδους και έχει μια δομή τέτοια ώστε να επιτυγχάνεται η όποια επιθυμητή μεταξύ τους επικοινωνία. Στα δίκτυα τηλεπληροφορικής συναντάμε αυστηρούς κανόνες που διέπουν το τηλεπικοινωνιακό τμήμα του δικτύου καθώς επίσης και κανόνες συνομιλίας μεταξύ των υπολογιστών (πρωτόκολλα επικοινωνίας).

Πολλές φορές στην προσπάθεια των εταιριών υπολογιστών να καλύψουν τα θέματα των τηλεπικοινωνιών, παρατηρείται το φαινόμενο τα σύνορα μεταξύ της πληροφορικής και των τηλεπικοινωνιών να γίνονται δυσδιάκριτα. Άλλωστε ένα μεγάλο μέρος του λογισμικού των επικοινωνιών αλλά και των πρωτοκόλλων φιλοξενείται στους υπολογιστές είτε ενσωματωμένο στο λειτουργικό σύστημα, είτε σαν ανεξάρτητα προγράμματα. Γι' αυτό θα δούμε πολλές φορές να μην είναι εύκολος και σαφής ο προσδιορισμός δικτύων.

Η διάδοση των δικτύων κάνει πιο επιτακτική την ανάγκη για ταξινόμηση τους με βάση τα τεχνικά τους χαρακτηριστικά.

Κάθε δίκτυο δεδομένων σχεδιάζεται έτσι ώστε να εξυπηρετεί τις εκάστοτε λειτουργικές απαιτήσεις των εφαρμογών. Γι' αυτό σε κάθε δίκτυο υπάρχουν διαφορετικές μέθοδοι προσπέλασης της πληροφορίας, διαφορετικά πρωτόκολλα, διασυνδέσεις, φυσικά μέσα, με λίγα λόγια δηλαδή διαφορετικοί όροι παιχνιδιού. Αυτό το φαινόμενο με τη πάροδο του χρόνου τείνει να μειωθεί, καθώς γίνονται συνεχείς προσπάθειες για τυποποίηση όλων των στοιχείων που απαρτίζουν ένα δίκτυο δεδομένων.

Τα δίκτυα διαιρούνται σε κατηγορίες που προσδιορίζονται ανάλογα με την οπτική γωνία από την οποία τα βλέπουμε και όπως φαίνεται υπάρχουν πολλές τέτοιες γωνίες.

Στη συνέχεια θα προσπαθήσουμε να δώσουμε σαφείς ερμηνείες, ούτως ώστε να διαλυθούν οι όποιες παρερμηνείες γύρω από το θέμα.

Γενικά δεν υπάρχει μια αποδεκτή ταξινόμηση στην οποία να ταιριάζουν όλα τα δίκτυα, αλλά δυο χαρακτηριστικά των δικτύων που ξεχωρίζουν είναι η τεχνολογία μετάδοσης (δίκτυα μεταγωγής) και η κλίμακα.

[4] Andrew S.Tanenbaum "Δίκτυα Υπολογιστών"

1.5. ΔΙΚΤΥΑ ΜΕΤΑΓΩΓΗΣ

Κύριο χαρακτηριστικό των δικτύων αυτών είναι η δυνατότητα του κάθε συνδρομητή να καλεί τον ανταποκριτή του με βάση επιλογής του.

Τα δίκτυα μεταγωγής αποτελούνται από κόμβους συνδεδεμένους μεταξύ τους, οι οποίοι αναλαμβάνουν τη δρομολόγηση της εκπεμπόμενης από τον εκάστοτε αποστολέα πληροφορίας.Data που εισέρχονται στο δίκτυο από κάποιο τερματικό σταθμό, δρομολογούνται από κόμβο σε κόμβο μέχρι τον προκαθορισμένο δέκτη. Μερικοί κόμβοι δεν έχουν συνδεδεμένους τερματικούς σταθμούς, απλά παίζουν το ρόλο του διεκπεραιωτή της πληροφορίας. Για λόγους αύξησης της αξιοπιστίας οι συνδέσεις των κόμβων γίνονται με τέτοιο τρόπο ώστε να υπάρχει εναλλακτικός δρόμος μεταξύ των τερματικών σημείων. Τα δίκτυα μεταγωγής συνήθως προσφέρονται από τους οργανισμούς τηλεπικοινωνιών[5].

Υπάρχουν τρεις βασικές μέθοδοι αποκατάστασης σύνδεσης δυο τερματικών σταθμών στα δίκτυα μεταγωγής.

- Μεταγωγή κυκλώματος (Circuit switching)
- Μεταγωγή μηνυμάτων (Message switching)
- Μεταγωγή πακέτων (Packet switching)

Μεταγωγή Κυκλώματος (Circuit Switching)

Η μεταγωγή κυκλώματος είναι τεχνική κατά την οποία αφιερώνεται μια φυσική ζεύξη μεταξύ των συνδρομητών για όλη τη διάρκεια της επικοινωνίας τους. Η σύνδεση είναι τμηματική και αποτελείται από τμήματα γραμμών που συνδέουν τους διάφορους κόμβους του δικτύου. Με τη μεταγωγή κυκλώματος κάθε γραμμή που καταλαμβάνεται για μια σύνδεση απασχολείται πλήρως και αποκλειστικά με την επικοινωνία των δυο συνδρομητών. Κλασσικό παράδειγμα αυτού του είδους τεχνικής είναι το κοινό τηλεφωνικό δίκτυο.

Στη περίπτωση της μεταγωγής κυκλώματος η γραμμή παραμένει κατειλημμένη ακόμα και κατά τα χρονικά διαστήματα όπου δεν μεταφέρονται data. Έχει αποδειχθεί στατιστικά ότι ο κενός χρόνος σε μια σύνδεση δυο τερματικών σημείων είναι σχετικά μεγάλος.

Όμως με την τεχνική circuit switching έχουμε το πλεονέκτημα ότι σε μια αποκατασταθείς σύνδεση οι χρήστες μπορούν να χρησιμοποιήσουν όλη τη μεταφορική ικανότητα (throughput) της γραμμής, με μόνη καθυστέρηση τον μικρό χρόνο μετάβασης (propagation delay) και την αρχική καθυστέρηση για την αποκατάσταση της σύνδεσης.

Μεταγωγή Μηνυμάτων (Message Switching)

Κατ' αυτήν ο αποστολέας οργανώνει την προς μετάδοση πληροφορία σε μήνυμα που το δίνει στο δίκτυο για διεκπεραίωση. Το δίκτυο προωθεί από κόμβο σε κόμβο το μήνυμα μέχρι τον τελικό παραλήπτη.

Το δίκτυο αναλαμβάνει την διεκπεραίωση των μηνυμάτων και όχι την αποκατάσταση του φυσικού δρόμου. Το δίκτυο εκμεταλλεύεται τις φυσικές συνδέσεις μεταξύ των κόμβων για την αποστολή μηνυμάτων όλων των συνδρομητών. Σε κάθε μήνυμα είναι σημειωμένη η διεύθυνση του παραλήπτη, ούτως ώστε ο κάθε κόμβος να το προωθεί στον επόμενο όταν φυσικά βρει ελεύθερο κανάλι[6].

---

[5] Χρήστος Ι. Μπούρας Δίκτυα Δημόσιας Χρήσης και Διασύνδεση Δικτύων Πανεπιστημιακές Σημειώσεις,

[6] Andrew S. Tanenbaum «Δίκτυα Υπολογιστών» 3η έκδοση

Οι κόμβοι ενός δικτύου μεταγωγής μηνυμάτων δεν είναι απλώς ένα ηλεκτρομηχανικό ή ηλεκτρονικό κέντρο που συνδέει κανάλια για να περάσει το μήνυμα, αλλά υπολογιστές επικοινωνιών με αρκετό χώρο μνήμης προκειμένου να αποθηκεύουν τα μηνύματα που λαμβάνουν πριν τα αποστείλουν στον επόμενο κόμβο. Στους κόμβους αυτούς κάθε μήνυμα υπόκειται σε κάποια καθυστέρηση, που οφείλεται στο ότι πρέπει να παραληφθεί πρώτα όλο το μήνυμα και μετά να βρεθεί ο κατάλληλος κενός δρόμος για την περαιτέρω αποστολή του. Λόγω του ότι κάθε κόμβος αποθηκεύει το μήνυμα πριν το μεταδώσει, η τεχνική αυτή ονομάζεται και store-and-forward (αποθήκευση – προώθηση).

Μερικά από τα πλεονεκτήματα της τεχνικής message switching έναντι της circuit switching είναι:

- Δεν ενδιαφέρει αν την ώρα που ο αποστολέας στέλνει το μήνυμα, ο αποδέκτης είναι σε θέση να το δεχτεί. Το δίκτυο μπορεί να φυλάξει το μήνυμα και να το στείλει αργότερα.
- Η εκμετάλλευση των φυσικών συνδέσεων (γραμμών) είναι πολύ καλύτερη, αφού ένα κανάλι μπορεί να διεκπεραιώσει μηνύματα πολλών χρηστών.
- Η τεχνική message switching παρέχει τη δυνατότητα πολλαπλής αποστολής αυτού του μηνύματος σε πολλού χρήστες.
- Ο έλεγχος σφαλμάτων και γενικά οι διαδικασίες προστασίας από τα σφάλματα μπορούν να γίνουν από το δίκτυο.
- Οι δυο τερματικοί σταθμοί έχουν τη δυνατότητα να ανταλλάσσουν μηνύματα γραμμένα σε διαφορετικό κώδικα και με διαφορετική ταχύτητα τη δουλειά της μετατροπής κάνουν οι ακραίοι κόμβοι στους οποίους έχει δηλωθεί από πριν με ποια ταχύτητα και με ποιο κώδικα συνεννοείται ο συγκεκριμένος τερματικός σταθμός.

Ένα βασικό μειονέκτημα της τεχνικής αυτής είναι ότι δεν είναι κατάλληλη για real time εφαρμογές, επειδή οι καθυστερήσεις που υπεισέρχονται από τους κόμβους είναι μεγάλες και αγνώστου διάρκειας. Στην πράξη η τεχνική μεταγωγής μηνυμάτων είναι η λιγότερο εφαρμοσμένη από τις άλλες δυο.

Μεταγωγή πακέτων (Packet Switching)

Με την τεχνική μεταγωγής πακέτων έγινε μια σοβαρή προσπάθεια εκμετάλλευσης των πλεονεκτημάτων του circuit και του message switching και παράλληλης ελαχιστοποίησης των μειονεκτημάτων τους. Το κάθε μήνυμα που πρέπει να μεταφερθεί μέσω ενός τέτοιου δικτύου τεμαχίζεται σε πακέτα. Το μήκος των πακέτων είναι μικρό, συνήθως 128 ή 256 χαρακτήρες, χωρίς να αποκλείονται σε ορισμένες περιπτώσεις μεγαλύτερα ή μικρότερα, ώστε να ελαχιστοποιούνται οι απαιτήσεις μνήμης των κόμβων[7].

Όπως και στην περίπτωση της μεταγωγής των μηνυμάτων, οι κόμβοι οφείλουν να έχουν επεξεργαστική ικανότητα για την προώθηση των πακέτων. Οι μέθοδοι προώθησης των πακέτων είναι δυο:

- Datagram
- Virtual circuit

Με τη μέθοδο datagram τα πακέτα ενός μηνύματος θα φθάσουν στον παραλήπτη χρησιμοποιώντας το καθένα το δικό του συντομότερο δρόμο. Η τεχνική αυτή συναντάται και με τον όρο connectionless με τυπικό παράδειγμα το πρωτόκολλο IP. Τα πακέτα ενώ έχουν

[7] Andrew S.Tanenbaum “Δίκτυα Υπολογιστών

τον ίδιο προορισμό δεν ακολουθούν όλα τον ίδιο δρόμο και λόγω αυτού υπάρχει η πιθανότητα να φτάσουν με διαφορετική σειρά από αυτή που ξεκίνησαν. Ως εκ τούτου η τεχνική αυτή έχει μειωμένη αξιοπιστία οπότε απαιτείται από τους τελικούς σταθμούς του δικτύου η χρήση πρόσθετων πρωτοκόλλων ανώτερων επιπέδων. Τυπικό παράδειγμα είναι το πρωτόκολλο TCP πάνω από δίκτυα IP.

Με τη μέθοδο virtual circuit (νοητού κυκλώματος), πριν αποσταλούν τα πακέτα αποκαθίσταται μια σταθερή νοητή σύνδεση μεταξύ των δυο ανταποκριτών τερματικών σταθμών απ' όπου κατόπιν θα περάσουν όλα τα πακέτα του μηνύματος. Για τον λόγο αυτό η τεχνική αυτή ονομάζεται connection oriented. Η κυρίως διαφορά της virtual circuit με την datagram είναι ότι με την πρώτη τεχνική ο δρόμος για όλα τα πακέτα μιας σύνδεσης, καθορίζεται μια φορά στην αρχή και μετά παραμένει ο ίδιος μέχρι τη διακοπή της, ενώ στη δεύτερη ο κάθε κόμβος επιλέγει κάθε φορά και για κάθε πακέτο τον καταλληλότερο δρόμο. Η πρώτη τεχνική δεν πρέπει να παρομοιαστεί με την circuit switching, καθώς το κάθε πακέτο κρατείται προσωρινά σε κάθε κόμβο πριν ακολουθήσει τη πορεία του. Με αυτή την τεχνική απλώς οι κόμβοι δεν επιλέγουν για κάθε πακέτο και διαφορετικό δρόμο.

Πλεονεκτήματα της virtual circuit έναντι της datagram είναι:

- Γρήγορη και σωστή ταξινόμηση των παρεληφθέντων μηνυμάτων
- Έλεγχος ορθότητας της σειράς λήψης των πακέτων
- Επιβεβαίωση του ότι όλα τα πακέτα παραλήφθηκαν σωστά
- Υπάρχει επιπλέον δυνατότητα για flow control (έλεγχο ροής) ούτως ώστε αν ο παραλήπτης έχει προσωρινή αδυναμία λήψης, ειδοποιεί τον αποστολέα να σταματήσει μέχρι νεωτέρας εντολής.
- Έχει μικρές μεταβολές του χρόνου απόκρισης λόγω της σταθερής διαδρομής
- Έχει μικρότερο overhead καθώς δεν απαιτείται η ύπαρξη της πλήρους διεύθυνσης του παραλήπτη σε κάθε πακέτο.

Πλεονεκτήματα της datagram τεχνικής:

- Είναι πιο διαθέσιμη αφού αν ένας κόμβος χαλάσει, όλα τα νοητά κυκλώματα (virtual circuit) που διέρχονται από τον κόμβο αυτό θα χαθούν, ενώ με τη datagram τα πακέτα θα διοχετευθούν από άλλους εναλλακτικούς δρόμους μέσω άλλων κόμβων.
- Αν έχουμε συμφόρηση της κίνησης σε κάποια μέρη του δικτύου, με την τεχνική virtual circuit είναι αρκετά πιο δύσκολο να αναδρομολογηθούν τα μηνύματα προς άλλη κατεύθυνση απ' ότι με τη datagram.
- Στη datagram δεν απαιτείται η φάση έναρξης της συνομιλίας (call request, call accept).

Σε επικοινωνία με λίγα μηνύματα ευνοείται η datagram, ενώ αν αυτή είναι μακρόχρονη προτιμάται η virtual circuit. Αντιπροσωπευτικά δίκτυα που χρησιμοποιούν τεχνικές νοητών κυκλωμάτων είναι τα X.25, Frame relay, ATM.

1.6. ΚΛΙΜΑΚΑ ΔΙΚΤΥΩΝ ΥΠΟΛΟΓΙΣΤΩΝ

Όπως αναφέραμε και παραπάνω ένα ακόμη κριτήριο ταξινόμησης των δικτύων είναι η κλίμακα τους. Στην κορυφή της ιεραρχίας βάση αυτού του κριτηρίου βρίσκονται οι μηχανές ροής δεδομένων, που είναι υπολογιστές υψηλού βαθμού παραλληλίας με πολλές λειτουργικές μονάδες να δουλεύουν για το ίδιο πρόγραμμα. Ακολουθούν οι πολλαπλοί υπολογιστές, που είναι συστήματα τα οποία επικοινωνούν στέλνοντας μηνύματα μέσω μικρών και πολύ γρήγορων αρτηριών.

Πέρα από τους πολλαπλούς υπολογιστές είναι τα αληθινά δίκτυα στα οποία οι υπολογιστές επικοινωνούν ανταλλάσσοντας μηνύματα μέσω καλωδίων μεγαλύτερου μήκους.

Ως προς τη γεωγραφία τερματικών και υπολογιστικών σημείων διακρίνουμε τα δίκτυα ευρείας περιοχής (Wide area network, WAN), τα τοπικά δίκτυα (Local area network, LAN) και τα αστικά δίκτυα (Metropolitan area network, MAN).

Η σύνδεση δυο ή περισσότερων δικτύων ονομάζεται διαδίκτυο. Η απόσταση στην οποία εκτείνεται το καθένα από τα παραπάνω είναι σημαντική επειδή χρησιμοποιούνται διαφορετικές τεχνικές σε διαφορετικές κλίμακες και για τον λόγο αυτό παραθέτουμε τον παρακάτω πίνακα[8].

Απόσταση μεταξύ επεξεργαστών	Θέση επεξεργαστών	Παραδείγματα
0,1m	Στην ίδια κάρτα	Μηχανή ροής δεδομένων
1m	Στο ίδιο σύστημα	Πολλαπλός υπολογιστής
10m	Στο ίδιο δωμάτιο	Τοπικό δίκτυο
100m	Στο ίδιο κτίριο	Τοπικό δίκτυο
1km	Στην ίδια περιοχή	Τοπικό δίκτυο
10km	Στην ίδια πόλη	Μητροπολιτικό δίκτυο
100km	Στην ίδια χώρα	Δίκτυο ευρείας περιοχής
1000km	Στην ίδια Ήπειρο	Δίκτυο ευρείας περιοχής
10000km	Στον ίδιο πλανήτη	Το διαδίκτυο

1.7.ΔΙΚΤΥΑ ΕΥΡΕΙΑΣ ΠΕΡΙΟΧΗΣ (Wide Area Networks)

Όπως λέει και η ίδια η έκφραση τα δίκτυα ευρείας περιοχής (WAN) είναι ένα σύνολο από υπολογιστές, τερματικά, τηλεπικοινωνιακές συσκευές, τηλεπικοινωνιακές γραμμές και συνδέσεις, τα οποία εκτείνονται σε ευρεία γεωγραφική περιοχή αστική και υπεραστική, φεύγοντας από τα στενά πλαίσια ενός συγκεκριμένου χώρου. Παραδείγματα τέτοιων δικτύων είναι τα διάφορα τραπεζικά δίκτυα που εκτείνονται σε όλη την Ελλάδα και διεθνώς, είναι των αεροπορικών εταιριών, τα δημόσια δίκτυα δεδομένων, το Internet και λοιπά.

1.8.ΤΟΠΟΛΟΓΙΚΗ ΔΙΑΙΡΕΣΗ ΔΙΚΤΥΩΝ WAN

Κρίνοντας τα δίκτυα WAN ως προς την τοπολογική διαίρεση τους τα χαρακτηρίζουμε ακτινωτά και κομβικά[9].

1.8.1.ΑΚΤΙΝΩΤΟ

Ένα δίκτυο χαρακτηρίζεται ως ακτινωτό όταν όλες οι περιφερειακές τερματικές συσκευές του συνδέονται ακτινωτά με ένα κεντρικό σημείο. Τα πλεονεκτήματα ενός ακτινωτού δικτύου είναι

[8] Andrew S.Tanenbaum “Δίκτυα Υπολογιστών

[9] Andrew S.Tanenbaum “Δίκτυα Υπολογιστών

η εύκολη σχεδίαση και υποστήριξη, ο μικρός χρόνος απόκρισης και η πολλή καλή αξιοπιστία του. Ως μειονεκτήματα του ακτινωτού δικτύου αναφέρονται η υποχρεωτική διέλευση από το κέντρο των συνδέσεων μεταξύ των σταθμών εργασίας. Τέτοια δίκτυα συναντάμε σε μικρές και μεσαίες εφαρμογές ή αποτελούν τμήματα μεγαλύτερων δικτύων.

1.8.2.ΔΙΚΤΥΑ ΒΡΟΧΟΥ (Mesh)

Τα δίκτυα βρόχου είναι αυτά που ο κάθε σταθμός είναι συνδεδεμένος με τους άλλους με δυο τουλάχιστον δρόμους και με τέτοιο τρόπο που να κλείνουν βρόχους.

Τα δίκτυα βρόχου χρησιμοποιούνται για σύνδεση τηλεπικοινωνιακών κόμβων μεταξύ τους, σε αντίθεση με τα ακτινωτά που κυρίως συνδέουν τερματικούς σταθμούς με υπολογιστές. Η τοπολογία των δικτύων βρόχου χαρακτηρίζεται από το γεγονός ότι εν γένει υπάρχουν περισσότεροι του ενός δρόμοι για την ανταλλαγή μηνυμάτων μεταξύ δυο σημείων.

Πλεονεκτήματα των δικτύων βρόχου είναι η δυνατότητα επιλογών εναλλακτικής δρομολόγησης των μηνυμάτων σε περίπτωση διακοπής ή υπερφόρτωσης μιας σύνδεσης. Είναι σαφές ότι οι κόμβοι ενός δικτύου βρόχου πρέπει να έχουν την ικανότητα αποθήκευσης δεδομένων, δρομολόγησης και αναδρομολόγησης τους, καθώς και τη γνώση των διαδικασιών χρήσης του δικτύου.

Ένα τέτοιο δίκτυο έχει γενικά μεγαλύτερο κόστος, καθώς απαιτεί πολλαπλές τηλεπικοινωνιακές γραμμές και ιδιαίτερα έξυπνους κόμβους. Η απόδοση ενός δικτύου βρόχου επηρεάζεται από την αξιοπιστία των κόμβων, τους ρυθμούς μετάδοσης, τις μεθόδους δρομολόγησης, τη διαδικασία σύνδεσης κόμβων τερματικών σημείων και κόμβων μεταξύ τους, αλλά και από την αποθηκευτική ικανότητα των κόμβων.

1.8.3.ΚΟΜΒΙΚΑ ΔΙΚΤΥΑ

Το κομβικό δίκτυο που ονομάζεται και αλλιώς ιεραρχικό είναι η σύνθεση πολλών ακτινωτών σε ένα δίκτυο κορμού με κόμβους κατάλληλους για τη δρομολόγηση των μηνυμάτων. Οι κόμβοι αυτοί μπορεί να είναι απλοί κόμβοι μεταγωγής που απλώς συγκεντρώνουν το φόρτο πολλών γραμμών σε μια, μπορεί όμως να είναι και σύνθετοι υπολογιστές τηλεπικοινωνιών με πολλές ικανότητες στη διεκπεραίωση των μηνυμάτων.

Τα κομβικά δίκτυα λόγω της ύπαρξης των έξυπνων κόμβων κάνουν καλύτερη χρήση των γραμμών, παρέχουν λύσεις σε περιπτώσεις διακοπής κεντρικών γραμμών, υποβοηθούν τη χωρίς λάθη (error free) μετάδοση, μειώνουν δε το κόστος των μισθωμένων κυκλωμάτων κατά πολύ όπως φαίνεται και από τη μέχρι σήμερα πρακτική.

1.8.4.ΑΣΤΙΚΑ ΔΙΚΤΥΑ

Μια νέα υποδιαίρεση δικτύων που πρωτοεμφανίστηκε το 1990 είναι τα αστικά δίκτυα ή MAN που αναφέρονται σε δίκτυα που δεν ξεπερνούν τα σύνορα μιας πόλης. Τα δίκτυα αυτά αναπτύσσονται ξεπερνώντας τους περιορισμούς σε ταχύτητα και απόσταση των τοπικών δικτύων. Καλύπτουν τις μεγάλες ανάγκες επικοινωνίας μέσα στην ίδια πόλη, με συχνότερη χρήση τη διασύνδεση τοπικών δικτύων χρησιμοποιώντας κυρίως οπτικές ίνες επιτυγχάνουν ρυθμούς μετάδοσης της τάξης των εκατοντάδων Mbps.

Ένα μητροπολιτικό δίκτυο μπορεί να υποστηρίζει δεδομένα καθώς και φωνή και ίσως ακόμη να σχετίζεται με την καλωδιακή τηλεόραση. Δεν διαθέτει στοιχεία μεταγωγής που να διοχετεύουν τα πακέτα προς τη μια από τις πολλές διαφορετικές γραμμές εξόδου. Η απουσία μεταγωγής απλοποιεί τη σχεδίαση.

Δίκτυο αυτής της μορφής θεωρείται και το FDDI. Η τεχνολογία MAN έχει τυποποιηθεί από την IEEE ως 802.6 που είναι η βάση του SMDS (Switched Multimegabit Data Services).

1.8.5.ΤΟΠΙΚΑ ΔΙΚΤΥΑ

Η σύνδεση των υπολογιστών ξεκινά από ένα τοπικό δίκτυο (LAN-Local Area Network), το οποίο επιτρέπει τον καταμερισμό πληροφοριών που βρίσκονται στο ίδιο κτίριο ή σε εγκαταστάσεις οι οποίες βρίσκονται σε στενή γεωγραφική περιοχή, δηλαδή σε απόσταση μέχρι και 10 km περίπου.

Χρησιμοποιούνται ευρύτατα για να συνδέουν προσωπικούς υπολογιστές και σταθμούς εργασίας σε γραφεία εταιρειών με σκοπό την κοινή χρήση περιφερειακών (χαρακτηρίζονται τα συστήματα ενός Η/Υ που συνδέονται με διαφορετικούς τρόπους με τον κεντρικό επεξεργαστή και τη μνήμη αποτελούν διατάξεις εισόδου και εξόδου δεδομένων) και την ανταλλαγή πληροφοριών, έτσι ώστε όλοι οι χρήστες του δικτύου να έχουν πρόσβαση σε αυτά.

Τα βασικά στοιχεία που απαρτίζουν ένα τοπικό δίκτυο είναι[10]:

- Τα μέσα μετάδοσης και οι συσκευές επικοινωνίας
- Οι σταθμοί εργασίας (υπολογιστές)
- Το Interface κάθε σταθμού, που είναι αρμόδιο για τη σύνδεση με το μέσο μετάδοσης.
- Τα πρωτόκολλα επικοινωνίας ή αλλιώς οι μηχανισμοί ελέγχου μετάδοσης
- Τα εξειδικευμένα λειτουργικά συστήματα για τοπικά δίκτυα.

Τα τοπικά δίκτυα διακρίνονται από τα άλλα είδη δικτύων με βάση το μέγεθος, την τεχνολογία μετάδοσης και την τοπολογία τους. Κλασσικά παραδείγματα είναι το Ethernet και το Token Ring.

Τα τοπικά δίκτυα διαιρούνται σε τρεις κυρίως κατηγορίες[11]:

Στα LAN (Local Area Networks) από πλευράς υπολογιστικών συστημάτων συμμετέχουν κυρίως προσωπικοί υπολογιστές (PC).

Στα εξειδικευμένα τοπικά δίκτυα πολύ υψηλής ταχύτητας (HSLN – High Speed Local Network) που απαρτίζονται κυρίως από μεγάλους υπολογιστές και τα περιφερειακά τους.

Τέλος, στα δίκτυα με προσωπικούς υπολογιστές, που συνδέονται μέσω αυτόματων ηλεκτρονικών μεταγωγικών διατάξεων γνωστών και ως data PABX. Τα δίκτυα της μορφής αυτής τείνουν να εξαλειφθούν.

Ωστόσο, θα αναφέρουμε το συσχετισμό μεταξύ τοπικών δικτύων και συστημάτων single-user και multi-user.

Για τα συστήματα απλού χρήστη (single-user) συνήθως αναφερόμαστε σε προσωπικούς υπολογιστές, όπου είναι τα συστήματα που επιτρέπουν προσπέλαση μόνον σε ένα χρήστη ανά χρονική στιγμή. Όλα τα προγράμματα και οι συσκευές είναι διαθέσιμες ανά πάσα χρονική στιγμή και μονό χρήστη.

[10] Stan Schatt “Τοπικά Δίκτυα Υπολογιστών”

[11] Stan Schatt “Τοπικά Δίκτυα Υπολογιστών”

ΚΕΦΑΛΑΙΟ 2 : ΕΞΟΠΛΙΣΜΟΣ ΕΠΙΧΕΙΡΗΣΙΑΚΩΝ ΔΙΚΤΥΩΝ

2.1.ΔΟΜΗΜΕΝΗ ΚΑΛΩΔΙΩΣΗ

Η δομημένη καλωδίωση συνδυάζει όλες τις καλωδιώσεις για ανταλλαγή δεδομένων, σημάτων, και έλεγχο επικοινωνιών σε ένα ενιαίο παγιωμένο σύστημα καλωδίωσης. Αυτό σημαίνει ότι όλη η καλωδίωση, προγραμματίζεται, σχεδιάζεται, εγκαθίσταται, και ρυθμίζεται ως ένα ενιαίο σύστημα.

Μία εγκατάσταση δομημένης καλωδίωσης αποτελείται από ένα σύνολο καλωδίων και υλικών (πρίζες , κατανεμητές, κλπ) το οποίο πραγματοποιεί την μετάδοση φωνής και δεδομένων σε ένα κτήριο.

Οι εγκαταστάσεις δομημένης καλωδίωσης είναι "ανοιχτής" αρχιτεκτονικής , χρησιμοποιώντας τυποποιημένα υλικά και τοπολογία σύμφωνα με διεθνή πρότυπα για τον σχεδιασμό και την εγκατάσταση.

Για πολλά χρόνια η καλωδίωση που εξυπηρετούσε τις ανάγκες μετάδοσης δεδομένων γινόταν ξεχωριστά από αυτές της καλωδίωσης για την μεταφορά φωνής. Όμως η ενσωμάτωση συστημάτων υψηλής τεχνολογίας σε όλους τους χώρους έκανε την ανάγκη ενός τυποποιημένου τρόπου καλωδίωσης μεγαλύτερη. Έτσι με ένα σύστημα καλωδίωσης μπορούμε να εξυπηρετούμε τις ανάγκες των παρακάτω[12]:

- **ü** Πυρασφάλεια - πυρανίχνευση
- **ü** Σύστημα ασφαλείας και ελέγχου πρόσβασης
- **ü** Σύστημα ελέγχου και εξοικονόμησης ενέργειας
- **ü** Σύστημα ελέγχου θερμοκρασίας και εξαερισμού
- **ü** Μεταφορά δεδομένων (Δίκτυο Η/Υ)
- **ü** Μεταφορά φωνής (Τηλέφωνο - τηλεφωνικό κέντρο)
- **ü** Μεταφορά εικόνας (Ψηφιακή τηλεόραση)

Στις περισσότερες των περιπτώσεων δεν γίνεται σωστός σχεδιασμός και πρόβλεψη για τις καλωδιώσεις σ ένα νέο κτήριο με αποτέλεσμα να γίνεται εγκατάσταση καλωδίων σε διάφορα στάδια της κατασκευής. Αυτό εκτός του ότι αυξάνει το κόστος μας οδηγεί σε λύσεις που δεν μας εξυπηρετούν απόλυτα.

Προβλέποντας κατά την διάρκεια σχεδιασμού μίας οικοδομής το σύστημα καλωδίωσης πετυχαίνουμε οικονομία, απλοποίηση της εγκατάστασης, δυνατότητα μελλοντικών επεκτάσεων, χρήση κοινών προδιαγραφών για όλη την καλωδίωση και τον τερματικό εξοπλισμό. Όλα τα υλικά που προορίζονται για δίκτυα δομημένης καλωδίωσης είναι πιστοποιημένα ανάλογα με τις επιδόσεις τους σε διάφορους ελέγχους και ανήκουν σε μία από τις παρακάτω κατηγορίες:

1. CAT 3 : Επιτρέπει την διέλευση σημάτων με συχνότητες έως 16 MHz (Για χρήση τηλεφωνικών σημάτων)
2. CAT5 : Επιτρέπει την διέλευση σημάτων με συχνότητες έως 100MHz (Για χρήση τηλεφωνικών και σημάτων Η/Υ για δίκτυα 100Mbps)
3. CAT 5e η CAT 6 : Χρησιμοποιείται για δίκτυα Η/Υ τεχνολογίας Gigabit Ethernet

Η καλωδίωση μπορεί να είναι είτε οριζόντια είτε κάθετη. Η οριζόντια καλωδίωση παρουσιάζει τα εξής τεχνικά χαρακτηριστικά:

[12] Cisco Press Publications “Designing Network Security

1. Καλώδιο σιαμαίο UTP 24 AWG, 2X4 ζευγών Κατηγορίας 5, πιστοποιημένο σύμφωνα με ANSI/TIA/EIA 568A και ISO/IEC DIS 11801.
2. Καλώδιο UTP 24 AWG, 4 ζευγών Κατηγορίας 5E (Enhanced), πιστοποιημένο σύμφωνα με ANSI/TIA/EIA 568A και ISO/IEC DIS 11801

Η κάθετη :

1. UTP 25 ζευγών, διαμέτρου 24 AWG

2.2.ΤΟ ΑΠΑΡΑΙΤΗΤΟ HARDWARE

Ένα δίκτυο αποτελείται από τα παρακάτω μέρη :

Διακομιστής αρχείων (File Server). Πρόκειται για τον πυρήνα του δικτύου. Συνήθως είναι ένας πολύ γρήγορος μικροϋπολογιστής που τρέχει το λειτουργικό σύστημα του δικτύου και διαχειρίζεται τη ροή των δεδομένων. Είναι ο μεγαλύτερος υπολογιστής του δικτύου με μεγάλες αποθηκευτικές ικανότητες (συνήθως με σκληρούς δίσκους μερικών GigaBytes) και μεγάλη κεντρική μνήμη. Μερικές από τις υπηρεσίες που παρέχει ο file server είναι[13]:

- **ü** αποθήκευση των προγραμμάτων του λειτουργικού συστήματος του δικτύου καθώς και βοηθητικών προγραμμάτων.
- **ü** αποθήκευση των προγραμμάτων και των δεδομένων των χρηστών του δικτύου.
- **ü** διαχείριση του συστήματος αρχείων, των διαμοιραζόμενων περιφερειακών συσκευών, της δυνατότητας προσπέλασης των χρηστών και της ασφάλειας του δικτύου.
- **ü** παρακολούθηση της λειτουργίας και της αποδοτικότητας του δικτύου.

Οι servers μπορεί να είναι περισσότεροι από ένας προκειμένου να υποστηρίξουν όλες αυτές τις λειτουργίες. Σε περίπτωση που υπάρχει παραπάνω από ένας server τότε αυτοί αναφέρονται ως dedicated servers (αφιερωμένοι servers) και μπορούν να είναι:

- *communication servers (επικοινωνιών).* Διαχειρίζονται τις συνδέσεις μεταξύ των κόμβων του δικτύου καθώς και τις συνδέσεις με άλλα τοπικά δίκτυα ή μεγαλύτερα συστήματα (mainframes) και παρέχουν τη δυνατότητα χρήσης ηλεκτρονικού ταχυδρομείου (e-mail).
- *backup servers.* Εξυπηρετούν τη λήψη αντιγράφων ασφαλείας των αρχείων και των δεδομένων.
- *database servers.* Αποθηκεύουν βάσεις δεδομένων ή object-oriented πληροφορίες που προσπελάσσονται από τους χρήστες.
- *print servers.* Εξυπηρετούν τις εκτυπώσεις στο δίκτυο δίνοντας το δικαίωμα στους χρήστες να προσαρτώνται στους εκτυπωτές του δικτύου μέσω των ουρών εκτύπωσης. Ο print server εγκαθίσταται συνήθως στον file server ή σε κάποιον αφιερωμένο (dedicated) σταθμό του δικτύου.

Σταθμοί εργασίας (workstations). Πρόκειται για προσωπικούς υπολογιστές που έχουν το δικό τους λειτουργικό σύστημα και είναι συνδεδεμένοι με το διακομιστή αρχείων μέσω καλωδίων και καρτών επικοινωνίας. Οι χρήστες δεν χρησιμοποιούν τον file server απ' ευθείας, αλλά μόνον μέσω των σταθμών εργασίας. Μερικές φορές, ένας σταθμός εργασίας αναφέρεται και σαν κόμβος.

Κάρτες διασύνδεσης δικτύου (NIC - Network Interface Card). Προκειμένου να είναι δυνατή η σύνδεση, ο file server και κάθε σταθμός εργασίας περιέχει μια κάρτα διασύνδεσης δικτύου, μέσω της οποίας συνδέεται με όλες τις υπόλοιπες συσκευές. Κάθε κάρτα δικτύου σχεδιάζεται για ένα συγκεκριμένο τύπο δικτύου π.χ. Ethernet, FDDI, token ring κλπ.

[13] http://www.cnc.uom.gr/services/pdf/section1(2).pdf

Λειτουργούν στο φυσικό επίπεδο του μοντέλου OSI καθορίζοντας πρωτόκολλα για τα μηχανικά και ηλεκτρικά χαρακτηριστικά της διασύνδεσης. Χρησιμοποιούν συγκεκριμένες μεθόδους για τη μεταβίβαση των πληροφοριών που λαμβάνουν προς τον υπολογιστή (οι 4 μέθοδοι που αφορούν συστήματα βασισμένα σε επεξεργαστές Intel είναι : direct memory access, shared adapter memory, shared system memory, bus mastering).

Η τοποθέτηση μιας κάρτας δικτύου απαιτεί προσοχή. Πρέπει η διεύθυνση μιας κάρτας δικτύου να μην συμπίπτει με άλλες όπως π.χ. της σειριακής ή της παράλληλης θύρας.

Περιφερειακές συσκευές, (εκτυπωτές, tapes κλπ).

Καλώδιο σύνδεσης. Τα συνηθέστερα καλώδια είναι τα χάλκινα καν των οπτικών ινών. Τα χάλκινα είναι φθηνά και αποτελούν την πλειοψηφία των εγκαταστάσεων, ενώ οι οπτικές ίνες κερδίζουν συνεχώς έδαφος, λόγω της μείωσης του κόστους, της απλοποίησης των τεχνικών εγκατάστασης και της ανάγκης για ολοένα και μεγαλύτερη ταχύτητα. Υπάρχουν τρεις τύποι χάλκινων καλωδίων : ομοαξονικό, συνεστραμμένου ζεύγους με θωράκιση και χωρίς θωράκιση.

2.3.ΤΡΟΠΟΙ ΣΥΝΔΕΣΗΣ

Οι τρόποι, με τους οποίους συνδέεται ένα επιχειρησιακό δίκτυο είναι δύο. Συγκεκριμένα είτε μέσω ενός εσωτερικού δικτύου της επιχείρησης, όπου οι ηλεκτρονικοί υπολογιστές είναι συνδεδεμένοι σε κάποιο τοπικό δίκτυο (LAN) μέσω κάρτας δικτύου. Κάθε ηλεκτρονικός υπολογιστής έχει μία διεύθυνση μέσω της οποίας συνδέεται στο Internet.

Δεύτερον, μέσω του επιλεγόμενου τηλεφωνικού δικτύου (DIAL-UP). Η τηλεφωνική γραμμή που φθάνει σε κάθε σπίτι είναι μια γραμμή dial-up και η σύνδεση που γίνεται όταν καλούμε κάποιον αριθμό διαρκεί μέχρι να κλείσουμε το τηλέφωνο. Μια σύνδεση dial-up μεταξύ δύο δικτύων θα μπορούσε να δημιουργείται για μεταφορά δεδομένων και στη συνέχεια να διακόπτεται. Η υλοποίηση μιας σύνδεσης dial-up απαιτεί την ύπαρξη ενός ηλεκτρονικού υπολογιστή και ενός modem.

Το Modem (Modulator / Demodulator) είναι συσκευή που χρησιμοποιείται για επικοινωνία δεδομένων, συνδέοντας τους ηλεκτρονικούς υπολογιστές στο δημόσιο επιλεγόμενο τηλεφωνικό δίκτυο. Το Modem Μετατρέπει (modulate) τα ψηφιακά σήματα των υπολογιστών σε αναλογικά σήματα που μπορούν να «ταξιδέψουν» διαμέσου των τηλεφωνικών γραμμών. Ένα modem στην άλλη άκρη της σύνδεσης αποδιαμορφώνει (demodulates) τα ψηφιακά σήματα πάλι σε αναλογικά[14].

Και τα δύο modems πρέπει να χρησιμοποιούν συμβατές τεχνικές επικοινωνίας που υπακούουν σε γνωστά standards (CCITT V , MNP). Η σύνδεση από τον ηλεκτρονικό υπολογιστή προς το modem είναι η τυπική σειριακή σύνδεση RS-232, ενώ η σύνδεση από το modem προς την τηλεφωνική πρίζα γίνεται με RJ-11C.

Τα modems μπορούν να είναι εσωτερικά (internals) στον ηλεκτρονικό υπολογιστή ή εξωτερικά (Externals). Ένα εσωτερικό modem είναι μια «κάρτα» (adapter) που τοποθετείται σε μια ελεύθερη θέση του ηλεκτρονικό υπολογιστή. Ένα εξωτερικό modem είναι ένα μικρό κουτί που βρίσκεται εκτός του ηλεκτρονικό υπολογιστή και συνδέεται με αυτόν μέσω της σειριακής θύρας επικοινωνίας.

Όταν ένα modem «καλεί» κάποιο άλλο, το modem «δέκτης» απαντά και γίνεται μια ανταλλαγή σημάτων που εγκαθιστά τις παραμέτρους της επικοινωνίας. Αποφασίζεται η μέγιστη ταχύτητα ανταλλαγής δεδομένων μεταξύ των δύο modems καθώς και η σχέση συμπίεσης. Η ταχύτητα μεταφοράς δεδομένων μετρείται σε bps (bits per second), Kbps και Mbps. Συνήθεις ταχύτητες επικοινωνίας είναι 14400 Kbps, 28800 Kbps και33600 Kbps. Τα modems «υπακούουν» σε διεθνή standards τεχνικών και λειτουργικών προδιαγραφών που

[14] http://www.cnc.uom.gr/services/pdf/section1(2).pdf

είναι γνωστά σαν «V.» π.χ. V.22, V.34, V.42 . Τα περισσότερα περιλαμβάνουν τεχνικές κωδικοποίησης και συμπίεσης των δεδομένων ώστε το πραγματικά μεταφερόμενο «ποσό» δεδομένων να είναι μεγαλύτερο.

Η χρήση των τηλεφωνικών γραμμών θέτει μερικούς περιορισμούς στο ρυθμό μεταφοράς δεδομένων :

1. Τα τηλεφωνικά κυκλώματα επικοινωνίας έχουν «εύρος ζώνης» (bandwidth) 300 – 3300 Hz . Η περιοχή αυτή είναι κατάλληλη για μεταφορά φωνής αλλά θέτει περιορισμούς στην μεταφορά δεδομένων.
2. Εξ αιτίας της κακής ποιότητας των τηλεφωνικών συνδέσεων δεν μπορεί να χρησιμοποιηθεί όλο το διαθέσιμο bandwidth για μεταφορά δεδομένων.
3. Το εύρος ζώνης διαιρείται σε δύο κανάλια για να μπορεί να υποστηρίξει τη δυνατότητα των modems να εκπέμπουν και να λαμβάνουν σε διαφορετικά κανάλια (duplexing).

ΚΕΦΑΛΑΙΟ 3 : ΔΙΚΤΥΑΚΕΣ ΤΕΧΝΟΛΟΓΙΕΣ

3.1. ETHERNET

Το Ethernet είναι το συνηθέστερα χρησιμοποιούμενο πρωτόκολλο ενσύρματης τοπικής δικτύωσης υπολογιστών. Αναπτύχθηκε από την εταιρεία Xerox κατά τη δεκαετία του '70 και έγινε δημοφιλές αφότου η Digital Equipment Corporation και η Intel, από κοινού με τη Xerox, προχώρησαν στην προτυποποίησή του το 1980. Το 1985 το Ethernet έγινε αποδεκτό επίσημα από τον οργανισμό IEEE ως το πρότυπο 802.3 για ενσύρματα LAN.

Το αρχικό Ethernet επέτρεπε ονομαστικούς ρυθμούς μετάδοσης δεδομένων της τάξης των 3 Mbps, μέσω ενός ομοαξονικού καλωδίου στο οποίο συνδέονταν οι επιμέρους υπολογιστές του δικτύου. Τη διασύνδεση αναλάμβανε μία κάρτα δικτύου Ethernet προσαρτημένη σε κάθε κόμβο, με κάθε κάρτα να χαρακτηρίζεται από μία μοναδική, εργοστασιακή 48-bit διεύθυνση MAC. Σήμερα έχουν εμφανιστεί νεότερες εκδόσεις του Ethernet με επιτρεπτούς ρυθμούς μετάδοσης δεδομένων μέχρι 10Gbps[15].

Οι προδιαγραφές που ορίζει το Ethernet αφορούν το φυσικό επίπεδο και το υποεπίπεδο MAC του μοντέλου αναφοράς OSI. Στη μεγάλη πλειονότητα των περιπτώσεων μαζί με το Ethernet χρησιμοποιείται, στο υποεπίπεδο LLC, το πρωτόκολλο IEEE 802.2. Για τον έλεγχο πρόσβασης στο κοινό μέσο το Ethernet αξιοποιεί τον αλγόριθμο CSMA/CD (Carrier Sense Multiple Access with Collision Detection).

Το Ethernet IEEE 802.3 είναι και πολύ διαδεδομένο σήμερα, ειδικά σε γραφεία και επιχειρήσεις. Η τοπολογία του είναι bus. Η συμπεριφορά του είναι πολύ ικανοποιητική για την μετάδοση δεδομένων. Παρουσιάζει όμως προβλήματα στην μετάδοση σε πραγματικό χρόνο πληροφορίας πολυμέσων. Το Etrhernet είναι δίκτυο πολλαπλής προσπέλασης μέσου (CSMA/CD : Carrier Sense Multiple Access/Collision Detection οι χρήστες διαμοιράζονται το φυσικό δρόμο). Στο δίκτυο αυτό κάθε σταθμός προσπαθεί να μεταδώσει τα δεδομένα του στο δίκτυο (οργανωμένα σε πακέτα / πλαίσια) και εφ' όσον διαπιστώσει ότι κανένας άλλος δεν μεταδίδει, τότε προχωρά σε μετάδοση, αλλιώς αναβάλει την μετάδοση για αργότερα (deferring). Λειτουργεί σε ταχύτητα 10 Mbits/sec. Υπάρχουν τρεις μορφές του Ethernet:

1. ***Το thick Ethernet ή 10-Base-S.*** Χρησιμοποιεί ομοαξονικό καλώδιο και το μέγιστο μήκος του bus μπορεί να φθάσει τα 500 m. Μπορούμε όμως να συνδέσουμε μεταξύ τους έως πέντε τέτοια τμήματα, με την χρήση 4 repeaters, φθάνοντας συνολικά τα 2.5 Km. Οι σταθμοί συνδέονται στο δίκτυο με την βοήθεια των tranceivers (πομποδεκτών). Το μέγιστο μήκος καλωδίου από τον πομποδέκτη ως τον υπολογιστή είναι 50 m.
2. ***Το thin Ethernet ή 10-Base-2.*** Χρησιμοποιεί ομοαξονικό καλώδιο με το μέγιστο μήκος του bus να μπορεί να φθάσει τα 185 m. Μπορούμε όμως και εδώ να συνδέσουμε μεταξύ τους έως και πέντε τέτοια τμήματα, με την χρήση 4 repeaters, φθάνοντας συνολικά τα 925 m. Το ομοαξονικό καλώδιο που χρησιμοποιείται είναι λεπτότερο από αυτό του thick Ethernet. Οι σταθμοί συνδέονται στο ομοαξονικό καλώδιο με την χρήση καρτών. Μπορούμε να έχουμε έως 30 σταθμούς ανά τμήμα.
3. ***Το 10-Base-T,*** το οποίο χρησιμοποιεί UTP καλώδια. Οι σταθμοί συνδέονται ακτινωτά σε ένα hub με μέγιστη απόσταση τα 100 μέτρα. Η φυσική τοπολογία είναι αστέρας, αλλά η λογική τοπολογία παραμένει bus. Αυτός είναι και ο πλέον διαδεδομένος τύπος Ethernet δικτύου σήμερα. Στο δίκτυο Ethernet δεν είναι δυνατή η επίτευξη περιορισμένης καθυστέρησης από άκρο σε άκρο, λόγω των συγκρούσεων, ενώ η απόδοση του δικτύου πέφτει κατακόρυφα σε συνθήκες υψηλής φόρτισης.
4. ***Fast Ethernet 100-Base-T.*** Το δίκτυο αυτό άρχισε να αναπτύσσεται το 1993, με σκοπό να αντικαταστήσει το Ethernet, αφού παρέχει πολύ μεγαλύτερη ταχύτητα (100

[15] Εγκυκλοπαίδεια Βικιπαίδεια: http://el.wikipedia.org/wiki/Ethernet

Mbits/sec) και το κόστος κάθε κάρτας δικτύου δεν είναι ιδιαίτερα αυξημένο σε σχέση με αυτό μιας αντίστοιχης κάρτα για το απλό Ethernet. Κατά τα άλλα, είναι ακριβώς της ίδιας τοπολογίας με το Ethernet 10-BASE-T (bus), διατηρώντας την υπάρχουσα καλωδίωση (UTP5 και 100 Mbps). Το Fast Ethernet αποτελεί μια ανταγωνιστική και οικονομικότερη λύση απέναντι στο FDDI, αν και το τελευταίο είναι περισσότερο αξιόπιστο. Επίσης, λόγω των μηχανισμών που χρησιμοποιεί, όπως ίδιο MAC πρωτόκολλο, ίδια πλαίσια, κτλ., δεν μπορεί να εγγυηθεί υψηλή ποιότητα υπηρεσίας σε καταστάσεις υψηλής φόρτισης.

5. ***Gigabit Ethernet.*** Το δίκτυο αυτό τυποποιήθηκε τα τελευταία 6 χρόνια, με στόχο την αύξηση της ταχύτητας του Fast Ethernet από 100 Mbps σε 1000 Mbps. Χρησιμοποιεί σε γενικές γραμμές το ίδιο MAC πρωτόκολλο (CSMA/CD), το ίδιο frame format και το ίδιο μέγεθος πακέτων. Η ταχύτητα των 1000 Mbps, μπορεί να επιτευχθεί με χρήση UTP 5 στα 100 m, με Multimode Fiber στα 550 m και με SingeMode Fiber στα 5 Km. Υπάρχουν διάφορες παραλλαγές του Gigabit Ethernet, με σημαντικότερη την 1000-Base-T, όπου υποστηρίζει την χρήση του UTP5 καλωδίου. Ετσι, η εισαγωγή του σε περιβάλλον εργασίας όπου υπήρχε το 100-Base-T, θα προκαλέσει αύξηση της ταχύτητας στις παρεχόμενες υπηρεσίες. Επιπλέον, μπορεί να χρησιμοποιηθεί και σε αρκετές περιπτώσεις για να διασυνδέσει 100-Base-T Hubs.

3.1.1.ΚΑΛΩΔΙΩΣΕΙΣ ETHERNET ΔΙΚΤΥΟΥ

Δύο είναι τα χρησιμοποιούμενα standard για την κατασκευή (pin-out) των απολήξεων και την τοποθέτηση των ακροδεκτών τύπου RJ-45 σε καλώδια για δίκτυο Ethernet:

1. Το T-568A (1995) και
2. το 568B (2002) – Αυτό είναι και το πλέον χρησιμοποιούμενο standard σήμερα.

Τα καλώδια Ethernet είναι μη θωρακισμένα καλώδια συνεστραμμένων ζευγών (UTP : Unshielded Twisted Pair) και απαντώνται σε τρεις κατηγορίες :

1. UTP cat 5
2. UTP cat 5e (πιο συνηθισμένη)
3. UTP cat 6 (ανώτερη ποιοτικά από τις προηγούμενες κατηγορίες)

Επίσης υπάρχουν δύο ειδών καλώδια :

1. Straight Through καλώδιο : για την σύνδεση του Η/Υ με τον Switch (διακόπτη δικτύου Ethernet) ή σύνδεση του Η/Υ με την πρίζα δικτύου
2. Crossover καλώδιο : για σύνδεση απευθείας 2 Η/Υ μεταξύ τους (back-to-back) χωρίς την χρήση ενδιάμεσου διακόπτη

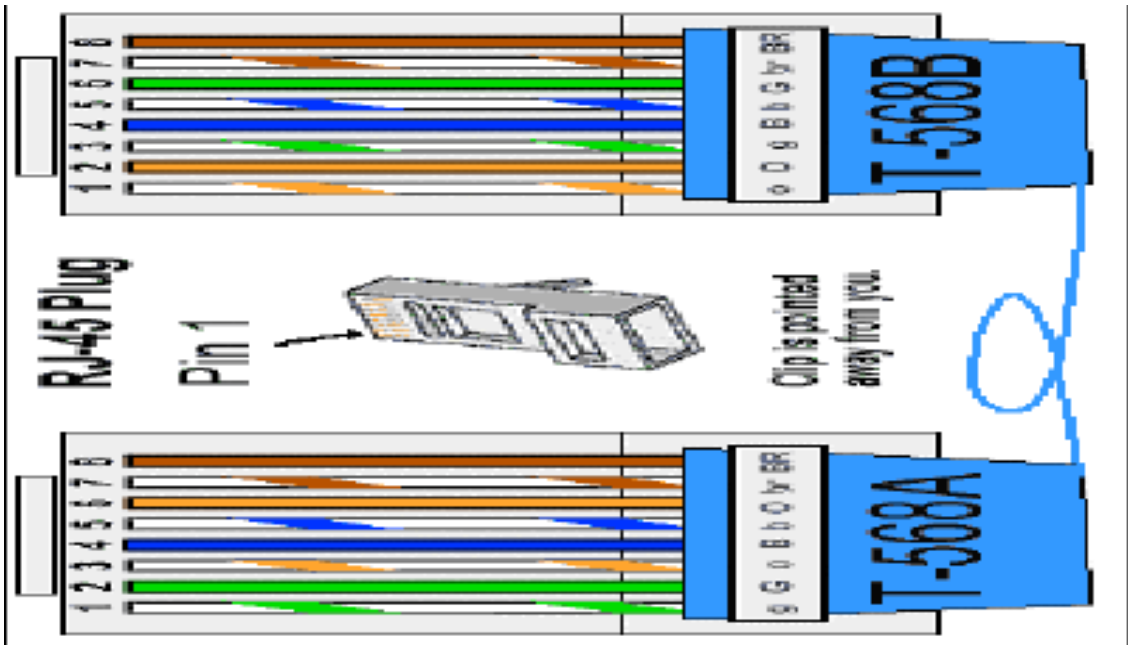
Οι κωδικοί δικτύου είναι:

- **ü** Ethernet, ταχύτητας 10 Mbps : IEEE 802.3 (10Base-T)
- **ü** Fast Ethernet, ταχύτητας 100 Mbps : IEEE 802.3u (100Base-T)

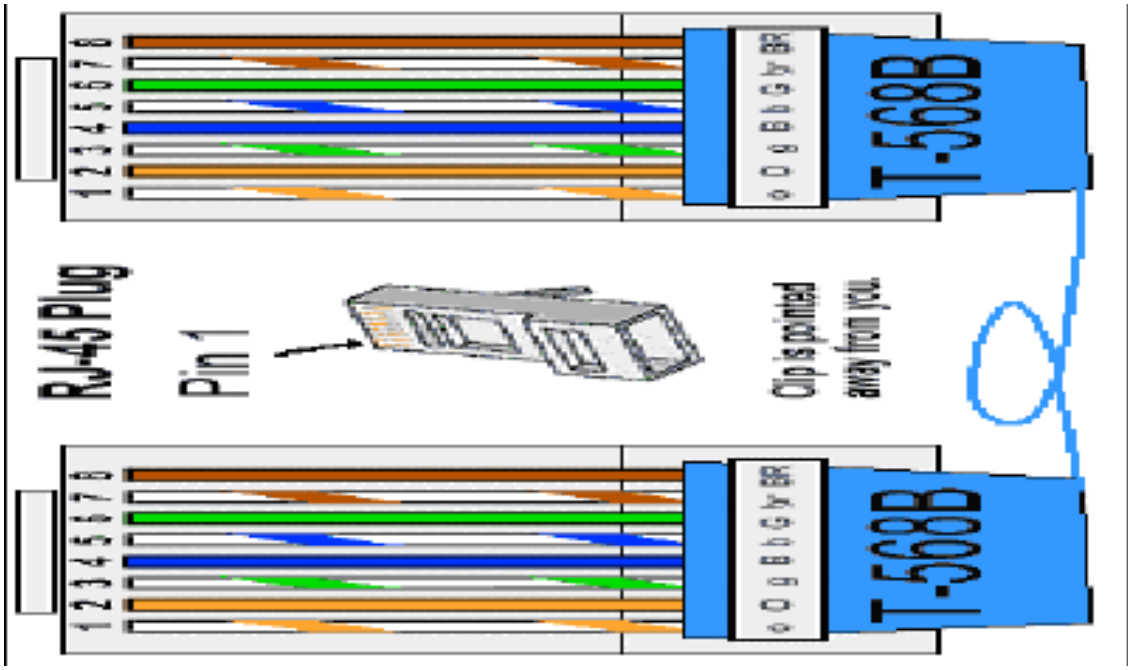
Μέγιστο επιτρεπτό μήκος καλωδίου στο Fast Ethernet μεταξύ 2 Η/Υ ή μεταξύ Η/Υ και διακόπτη είναι τα 100 μέτρα Το UTP είναι οκτάκλωνο καλώδιο με 4 ζεύγη συνεστραμμένων καλωδίων.

Παρακάτω παρουσιάζονται οι καλωδιώσεις του δικτύου Ethernet:

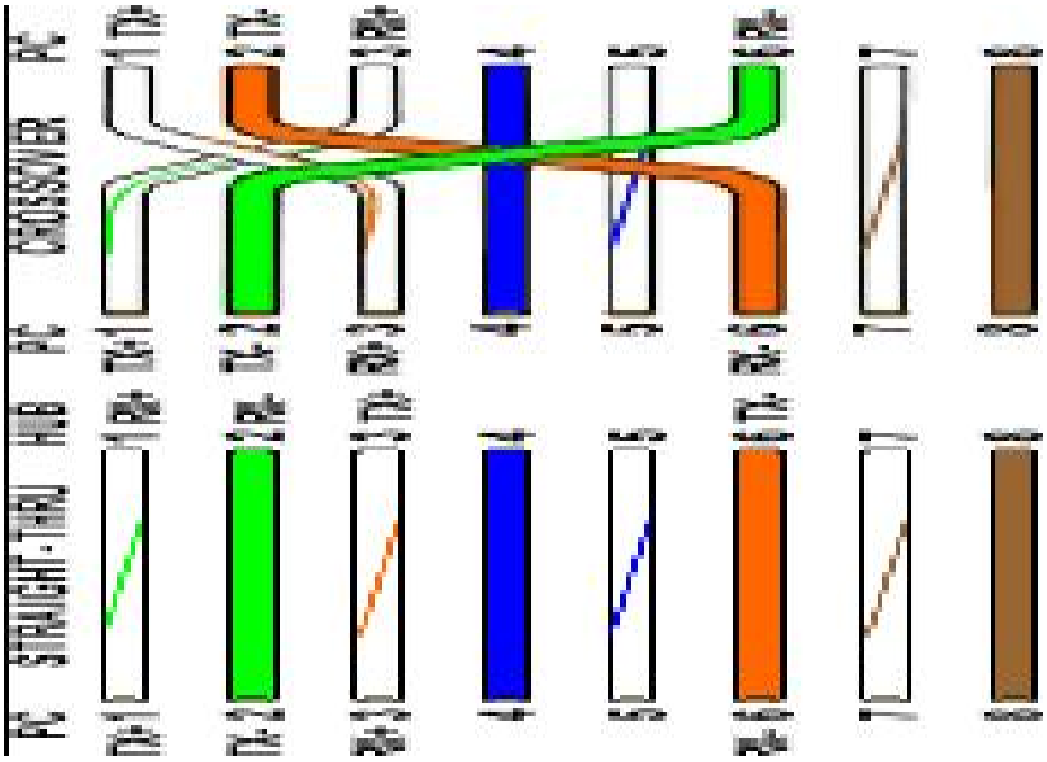
T-568A Straight-Through Ethernet Cable (1995)RJ-45 Crossover Ethernet Cable



T-568B Straight-Through Ethernet Cable (2002)



Σήματα καλωδίων



*3.2.*INTRANET

Με τον όρο intranet (ελληνικά αποδίδεται και με τον όρο "ενδοδίκτυο") νοείται ένα ιδιωτικό δίκτυο ηλεκτρονικών υπολογιστών που χρησιμοποιεί τις τεχνολογίες του Διαδικτύου, όπως τα πρωτόκολλα επικοινωνίας της σουίτας TCP/IP, το σύστημα μεταφοράς αρχείων FTP και τις τεχνολογίες του Παγκόσμιου Ιστού. Ο ίδιος όρος μπορεί να χρησιμοποιηθεί επίσης μόνο για το πιο εμφανές μέρος ενός intranet, δηλαδή για όσες ιστοσελίδες και διαδικτυακές εφαρμογές ενός οργανισμού είναι προσβάσιμες μόνο από τα μέλη του.

Ένα intranet λοιπόν μπορεί να περιγραφεί ως μια μικρή, ιδιωτική έκδοση του Διαδικτύου που χρησιμοποιείται αποκλειστικά από ένα και μόνο οργανισμό.

Οι βασικές χρήσεις των intranets είναι οι ίδιες με αυτές οποιουδήποτε δικτύου ηλεκτρονικών υπολογιστών, όπως η μεταφορά αρχείων, το ηλεκτρονικό ταχυδρομείο, η κοινοχρησία καταλόγων (address books), ημερολογίων, κτλ. Τα τελευταία χρόνια, τα intranets χρησιμοποιούνται όλο και περισσότερο και ως πλατφόρμες διαδικτυακών εφαρμογών[16].

Σήμερα, οι τεχνολογίες του Διαδικτύου είναι οι πιο διαδεδομένες και υποστηρίζονται από όλα σχεδόν τα λειτουργικά συστήματα και πλατφόρμες ανάπτυξης προγραμμάτων. Αυτό επιτρέπει στους οργανισμούς που χρησιμοποιούν intranets να παρέχουν πρόσβαση στις πληροφορίες και λειτουργίες του δικτύου τους σε οποιοδήποτε υπολογιστή, κινητό τηλέφωνο ή τερματικό, χωρίς την ανάγκη αγοράς επιπλέον εξοπλισμού ή εγκατάστασης προγραμμάτων. Το μόνο που χρειάζεται είναι η ύπαρξη ενός μοντέρνου λειτουργικού συστήματος (όπως Windows, Mac OS X ή Unix) και ενός φυλλομετρητή όπως ο Mozilla Firefox ή ο Internet Explorer.

Επιπλέον, οι τεχνολογίες διαδικτύου είναι βασισμένες ως επί το πλείστον σε ανοικτά πρότυπα, κάτι που επιτρέπει την απροβλημάτιστη ανταλλαγή πληροφοριών ανάμεσα στον οργανισμό και σε τρίτα μέρη, όπου αυτό είναι επιθυμητό. Παραδείγματα τέτοιων προτύπων

[16] Εγκυκλοπαίδεια Βικιπαίδεια, http://el.wikipedia.org/wiki/Intranet

είναι τα πρωτόκολλα POP3 και SMTP για τη μεταφορά μηνυμάτων ηλεκτρονικού ταχυδρομείου, CIFS και FTP για τη μεταφορά αρχείων, XML για την αποθήκευση και μεταφορά δεδομένων και XHTML για την παρουσίαση πληροφοριών στην οθόνη του χρήστη.

Τέλος, τα intranets επιτρέπουν την εύκολη πρόσβαση στο τοπικό δίκτυο του οργανισμού από απομακρυσμένους χρήστες, μέσω των διάφορων τεχνολογιών VPN.

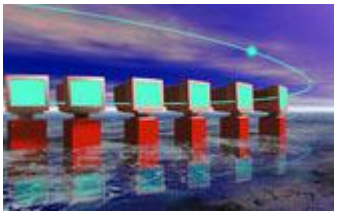
Ένα τυπικό Intranet μιας επιχείρησης περιλαμβάνει:

1. Γενικές πληροφορίες για την εταιρία (σύσταση, τομείς δραστηριοποίησης, μετοχική σύνθεση, ετήσιες οικονομικές εκθέσεις, οργανόγραμμα κ.ά.).
2. Ειδικές πληροφορίες για την εταιρία ("ταυτότητα" εργαζομένων, αρμοδιότητες τμημάτων, καθήκοντα και υποχρεώσεις υπαλλήλων κ.ά.).
3. Κατευθυντήριες γραμμές για τους επιμέρους τομείς δράσης της εταιρίας (πωλήσεις, marketing κ.λπ.).
4. Πληροφορίες για τους πελάτες και τους προμηθευτές (λ.χ. λίστες, κατάλογοι πιστωτών και χρεωστών).
5. Πληροφορίες για τα προϊόντα και τις υπηρεσίες της επιχείρησης (λ.χ. τιμοκατάλογοι).
6. Πληροφορίες για τις ανταγωνιστικές εταιρίες και τα προϊόντα τους.
7. Στοιχεία για την πολιτική που ακολουθεί η επιχείρηση σε συγκεκριμένα θέματα.
8. Εργαλεία αναζήτησης από βάσεις δεδομένων, συνδυαστικά εργαλεία ανάλυσης και εργαλεία προσθήκης πληροφοριών στο Intranet.
9. Εφαρμογές ηλεκτρονικού ταχυδρομείου.
10. Γενικές πληροφορίες (ημερολόγιο, εορτολόγιο, τρέχουσα ειδησεογραφία, τηλεφωνικός κατάλογος κ.λπ.).

3.3. EXTRANET

Το Extranet (στα ελληνικά θα μπορούσε να αποδοθεί ως "εξωδίκτυο") είναι εκείνο το κομμάτι του Intranet το οποίο μπορεί να προσεγγιστεί από πελάτες, προμηθευτές και εξωτερικούς συνεργάτες της εταιρίας μέσω Διαδικτύου, με τη χρήση κωδικού πρόσβασης. Ουσιαστικά πρόκειται για ένα μικρό ιδιωτικό τοπικό δίκτυο που επικοινωνεί τόσο με το Intranet όσο και με το Internet, ευρισκόμενο στο μέσο και λειτουργώντας συνδετικά. Ως κατασκευή έχει παρόμοια χαρακτηριστικά με το Intranet, με τη διαφορά ότι για τη δημιουργία του απαιτείται πρόσθετο υλικό (hardware) και λογισμικό (software), όπως firewalls και routers[17].

Η ανάπτυξη Extranet αφορά σε επιχειρήσεις που διαθέτουν εκτεταμένο εμπορικό δίκτυο σε διαφορετικά γεωγραφικά σημεία και επιθυμούν να προσφέρουν στους συνεργάτες τους υπηρεσίες προστιθέμενης αξίας. Οι συνηθέστερες εργασίες που μπορούν να πραγματοποιηθούν μέσω του Extranet είναι η υποστήριξη των συνεργατών (έλεγχος αποθεμάτων, καταστάσεις χρεωστών και πιστωτών, συμβουλευτικές υπηρεσίες κ.ά.) και η εξυπηρέτηση των εταιρικών πελατών και προμηθευτών (εισαγωγή παραγγελιών, έλεγχος διαδικασιών κ.ά.).



[17] http://andronianoi.ucoz.com/arxeia_pdf/ti_enai_to_intranet.pdf

Τα περιεχόμενα του Extranet είναι πολύ λιγότερα από αυτά του Intranet, η δε πρόσβαση σε αυτό είναι διαβαθμισμένη. Ένας συνεργάτης λ.χ. μπορεί να έχει πρόσβαση μόνο σε ορισμένες κατηγορίες του περιεχομένου και όχι γενικώς και αδιακρίτως. Έχει δικαίωμα, για παράδειγμα, να ενημερώνεται για το απόθεμα κάποιου συγκεκριμένου προϊόντος στην αποθήκη (και έτσι να κάνει την παραγγελία του), δεν έχει όμως δικαίωμα να λαμβάνει γνώση για συγκεντρωτικά στοιχεία παραγγελιών ή πελατών.

Η δημιουργία Intranet και Extranet δεν θεωρείται γενικά ούτε τεράστια επένδυση ούτε εξαιρετικά δύσκολη υπόθεση, χωρίς αυτό να σημαίνει ότι πρόκειται για έργο ήσσονος σημασίας. Αντιθέτως, η υλοποίηση εταιρικού δικτύου απαιτεί καλό σχεδιασμό και προσεκτική μελέτη όλων των παραμέτρων, η δε επιτυχία του εξαρτάται σε μεγάλο βαθμό από την ανταπόκριση που θα βρει μεταξύ των εργαζομένων.

Όσον αφορά στο πρώτο σκέλος, αυτό της κατασκευής του δικτύου, δύο είναι τα βασικά σημεία: το κόστος και ο φορέας υλοποίησης. Το κόστος εξαρτάται από το μέγεθος του δικτύου, το απαιτούμενο υλικό και λογισμικό, τα ποιοτικά/ποσοτικά χαρακτηριστικά του (πλήθος εφαρμογών), καθώς και από το ποιος θα το κατασκευάσει. Αν η άμεσα ενδιαφερόμενη επιχείρηση διαθέτει ικανό τμήμα πληροφορικής, τότε η ανάπτυξή του μπορεί να γίνει εκ των έσω. Αν δεν υπάρχει τέτοιο τμήμα, τότε η ανάπτυξή του θα πρέπει να ανατεθεί σε κάποια εξειδικευμένη εταιρία. Με δεδομένο ότι ελάχιστες μικρομεσαίες επιχειρήσεις έχουν την άνεση να διαθέτουν οργανωμένο (και ειδικευμένο σε θέματα Intranet) τμήμα πληροφορικής, ως προσφορότερη λύση προβάλλει η δεύτερη.
Υπάρχει όμως και μία τρίτη λύση, πολύ οικονομικότερη: η δημιουργία εικονικού Intranet σε έναν server στο Διαδίκτυο, μέσω εγγραφής σε κάποια υπηρεσία τους είδους. Η συγκεκριμένη υπηρεσία λειτουργεί ως εξής: με λίγες εκατοντάδες ευρώ το χρόνο, ο ενδιαφερόμενος δημιουργεί το δικό του ενδοδίκτυο σε μια προκατασκευασμένη πλατφόρμα εφαρμογών Intranet, που φιλοξενείται σε κάποιον server. Ο συγκεκριμένος τύπος Intranet είναι προσβάσιμος από οπουδήποτε στον κόσμο, μέσω του web, και για τη δημιουργία του δεν απαιτείται απολύτως τίποτα επιπρόσθετο σε εξοπλισμό ή λογισμικό. Πρόκειται, δηλαδή, για ένα εικονικό Intranet, που αποτελείται από υπολογιστές που δεν βρίσκονται συνδεδεμένοι μεταξύ τους αλλά με το διακομιστή.
Η λύση του εικονικού Intranet ενδείκνυται για μικρές επιχειρήσεις που χρειάζεται να οργανώσουν την εσωτερική τους λειτουργία με το μικρότερο δυνατό κόστος. Ωστόσο, υπάρχουν και ορισμένες επιφυλάξεις, κυρίως για την ασφάλεια των δεδομένων. Είναι μάλλον επισφαλές να εμπιστευθεί κάποια επιχείρηση τα κρίσιμα δεδομένα της (λ.χ. χρεοπιστωτικές καταστάσεις) σε κάποιον server του κυβερνοχώρου. Πάντως, αν στο περιεχόμενο του Intranet δεν σκοπεύετε να τοποθετήσετε κρίσιμα δεδομένα, αλλά επιθυμείτε να περιοριστείτε στην παράθεση γενικών στοιχείων, τότε η λύση του εικονικού δικτύου είναι η πλέον ενδεδειγμένη.

Όσον αφορά στο δεύτερο σκέλος, το ρόλο δηλαδή των εργαζομένων (χρηστών), είναι σαφές ότι οι χρήστες είναι αυτοί που θα καθορίσουν την τελική επιτυχία ή την αποτυχία του εγχειρήματος. Αν οι χρήστες περιβάλλουν το νέο δίκτυο με θέρμη και ενδιαφέρον, αν συμμετέχουν ενεργά στην ποσοτική και ποιοτική αναβάθμισή του, τότε το μέλλον μπορεί να θεωρείται ευοίωνο. Αν, από την άλλη, οι χρήστες επιδείξουν ράθυμη και αδιάφορη συμπεριφορά, αν το χρησιμοποιούν φειδωλά και σε περιορισμένο βαθμό, τότε οι ιθύνοντες της επιχείρησης οφείλουν να αντιστρέψουν το κλίμα με συστηματική προσπάθεια πειθούς, που θα επικεντρώνεται στις ωφέλειες των εργαζομένων από τη χρήση του εταιρικού δικτύου.

3.4.ΔΙΚΤΥΟ TOKEN RING IEEE 802.5

Είναι τοπολογίας δακτυλίου και προσφέρει μέγιστη ταχύτητα 16 Mbits/sec (ξεκίνησε με αρχική ταχύτητα 4 Mbps). Αναπτύχθηκε από την IBM και σε αντίθεση με την χρήση πρωτοκόλλων πολλαπλής προσπέλασης (CSMA/CD) ανήκει στην κατηγορία TDM πρωτοκόλλων. Οι σταθμοί είναι συνδεδεμένοι λογικά, ο ένας μετά τον άλλο, σε ένα δακτύλιο και ο καθένας παίρνει με την σειρά του το δικαίωμα να μεταδώσει δεδομένα. Το δίκτυο αυτό

έχει καλύτερη συμπεριφορά από το Ethernet σε καταστάσεις υψηλής φόρτισης. Στο δίκτυο αυτό μπορεί να οριστεί ο μέγιστος χρόνος, κατά τον οποίον ένας σταθμός θα κατέχει το token (Token Holding Timer-THT). Ένα άλλο πλεονέκτημα αυτού του τύπου δικτύου, είναι ότι μπορούν να καθοριστούν προτεραιότητες στα πακέτα κάθε σταθμού (μέχρι οκτώ προτεραιότητες). Υπάρχουν δύο βασικοί τύποι πλαισίων στο token ring : ένας για τα πλαίσια πληροφορίας (με μεταβλητό μήκος) και ένας για τα πλαίσια ελέγχου. Η χρησιμοποιούμενη κωδικοποίηση είναι η διαφορική Manchester. Σχετικά με την χρησιμοποίηση του δικτύου αυτού σε δεδομένα ευαίσθητα στον χρόνο, σημαντικό στοιχείο είναι η περιορισμένη καθυστέρηση λόγω του χρόνο THT, όμως τίθενται περιορισμοί σχετικοί με το μέγεθος του THT και το διαθέσιμο εύρος ζώνης του

καναλιού.

3.5.FDDI

Το δίκτυο FDDI (Fibre Distributed Data Interface) είναι ένα τοπικό δίκτυο υπολογιστών (LAN), ταχύτητας 100 Mbits/s, με ρυθμό μετάδοσης στα 125 Mbaud (χρησιμοποιούμενη κωδικοποίηση 4B5B, όπου για κάθε 4 bits δεδομένων μεταδίδονται 5). Το δίκτυο αυτό χρησιμοποιεί διπλή οπτική ίνα σαν το φυσικό μέσο μετάδοσης και ένα πρωτόκολλο προσπέλασης του μέσου, (MAC protocol) βασισμένο στη μέθοδο προσπέλασης IEEE 802.5 του δημοφιλούς token ring LAN.

Με την χρήση της διπλής οπτικής ίνας επιτυγχάνεται μεγάλη αξιοπιστία στην μεταφορά δεδομένων έναντι πιθανών βλαβών στην γραμμή μετάδοσης. Το δίκτυο FDDI μπορεί να υποστηρίξει μέχρι 1000 φυσικές μονάδες σ' ένα μέγιστο μήκος ίνας 200 χιλιομέτρων. Τα στοιχεία από τα οποία αποτελείται το δίκτυο FDDI είναι[18]:

• Διαχείριση Σταθμού - SMT (Station Management), η οποία καθορίζει επακριβώς την διαχείριση του τοπικού δικτύου, συμπεριλαμβάνοντας εσωτερική διαμόρφωση και λειτουργία του σταθμού.

• Έλεγχος Προσπέλασης του Μέσου - MAC (Media Access Control), ο οποίος παρέχει προσπέλαση στο μέσο, ικανότητα ελέγχου των δεδομένων και δημιουργίας πλαισίων (frames).

1. Πρωτόκολλο Φυσικού Επιπέδου, που πραγματοποιεί διαδικασίες κωδικοποίησης, αποκωδικοποίησης, κ.ά.
2. Φυσικό επίπεδο εξαρτημένο από το μέσο, που καθορίζει τις στάθμες ισχύος, τον οπτικό πομπό / δέκτη, τις απαιτήσεις σηματοδότησης, τα σημεία σύνδεσης, τα χαρακτηριστικά της ίνας και το ρυθμό λαθών στα bit πληροφορίας.

Αν και το δίκτυο FDDI παρέχει μία σύγχρονη υπηρεσία για την μετάδοση κίνησης συνεχών δεδομένων, θα μπορούσε να χρησιμοποιηθεί για ήχο και video με χαμηλές απαιτήσεις στην τάξη της επικοινωνίας. Το FDDI, χρησιμοποιεί στο MAC επίπεδο το πρωτόκολλο TTR (Time Token Rotation), σύμφωνα με το οποίο ο χρόνος κατά τον οποίο ένας σταθμός μπορεί να μεταδίδει δεδομένα συγκεκριμένης κλάσης και συνεπώς να διατηρεί το token, εξαρτάται εν μέρει από τον χρόνο περιστροφής του token. Με την βοήθεια κάποιων χρονιστών (π.χ. TTRT) εξασφαλίζεται ότι όταν ένας σταθμός έχει περιορισμένη καθυστέρηση στην μετάδοση των δεδομένων του, τότε θα λάβει το token στον κατάλληλο χρόνο, ώστε να τηρηθούν οι περιορισμοί αυτοί.

Δύο κλάσεις υπηρεσιών είναι διαθέσιμες: η σύγχρονη με υψηλή προτεραιότητα, η οποία έχει και εγγυημένο εύρος ζώνης καθώς και καθυστέρηση μετάδοσης και η ασύγχρονη. Το εύρος ζώνης που απομένει αποδίδεται στην ασύγχρονη κλάση και υποδιαιρείται σε οκτώ προτεραιότητες.

[18] http://www.it.uom.gr/project/MultimediaTechnologyNotes/chap2d_3.htm

3.6. FRAME RELAY.

Η υπηρεσία Frame Relay (FR) αποτελεί εξέλιξη του δικτύου μεταγωγής πακέτων X.25. Τα δίκτυα FR είναι γρηγορότερα από τα X.25, γιατί ενώ στα X.25 ο έλεγχος για λάθη γίνεται σε κάθε ενδιάμεσο κόμβο και το αποτέλεσμα αυτού του ελέγχου γνωστοποιείται στον αμέσως προηγούμενο κόμβο, ο οποίος αναμεταδίδει όλα τα πακέτα τα οποία ήταν λανθασμένα, στα δίκτυα FR ο έλεγχος γίνεται στις άκρες της διαδρομής, με αποτέλεσμα να μειώνεται η πολυπλοκότητα ελέγχων και συνεπώς να αυξάνεται η ταχύτητα του συστήματος. Αυτό προϋποθέτει βέβαια, ότι κατά την μετάδοση δεν εμφανίζονται πολλά σφάλματα, δηλαδή ότι η γραμμή μετάδοσης είναι σχετικά καλή και με μικρό ποσοστό εμφάνισης σφαλμάτων. Έτσι, εάν ένα πλαίσιο είναι λανθασμένο, προωθείται και αναμεταδίδεται στο τέλος από άκρη σε άκρη. Αποτέλεσμα της όλης διαδικασίας είναι να μειώνεται η καθυστέρηση μετάδοσης.

Το FR είναι πρωτόκολλο με φάση εγκατάστασης σύνδεσης, γεγονός που σημαίνει ότι τα πλαίσια μεταβλητού μήκους που υποστηρίζει, μεταφέρονται μέσω μοναδικών και συγκεκριμένων νοητών συνδέσεων, με την βοήθεια του πεδίου διεύθυνσης που περιλαμβάνεται στην επικεφαλίδα του πλαισίου. Στην Ευρώπη η ταχύτητα που υποστηρίζει το δίκτυο αυτό είναι 2,048 Mbps και βρίσκει μεγάλη χρήση στην διασύνδεση τοπικών ή ευρύτερης περιοχής δικτύων ή ακόμα και για την διασύνδεση δημοσίων δικτύων.

3.7. SWITCHED MULTIMEGABIT DATA SERVICE (SMDS)

Η υπηρεσία SMDS παρέχει δυνατότητα μεταφοράς δεδομένων χωρίς εγκατάσταση σύνδεσης (connectionless) και χρησιμοποιείται κυρίως στην διασύνδεση τοπικών δικτύων. Στην Ευρώπη είναι γνωστή ως Connectionless Broadband Data Service (CBDS). Οι ταχύτητες λειτουργίας κυμαίνονται συνήθως από 1,5 Mbps έως 35 Mbps ή και ακόμα υψηλότερες με την χρήση της ATM (AAL 3/4) μετάδοσης. Οι υπηρεσίες SMDS/CBDS μπορούν και δεσμεύουν το εύρος ζώνης που χρειάζονται δυναμικά (bandwidth-on-demand) και ως εκ' τούτου θα μπορούσαν να υποστηρίξουν εφαρμογές πολυμέσων. Παρόλα αυτά η κύρια χρήση τους είναι η σύνδεση τοπικών δικτύων, όπως αναφέρθηκε και νωρίτερα.

3.8. xDSL ΤΕΧΝΟΛΟΓΙΕΣ

Το xDSL αποτελεί μια οικογένεια DSL (Digital Subscriber Line) επικοινωνιακών τεχνολογιών οι οποίες χρησιμοποιούν την υπάρχουσα τηλεφωνική υποδομή για την μετάδοση δεδομένων. Οι τεχνολογίες DSL υποστηρίζουν δικατευθυντήρια μετάδοση και χρησιμοποιούν ένα εύρος από 30 KHz έως 1 MHz. Το βασικό πλεονέκτημα των DSL τεχνολογιών είναι ότι επιτρέπουν την ταυτόχρονη λειτουργία των τηλεφωνικών υπηρεσιών, ενώ μπορούν πάνω από τηλεφωνικές γραμμές να δώσουν υπηρεσίες όπως, γρήγορη σύνδεση στο Internet, τηλεϋπηρεσίες, μετάδοση video, κ.ά. Οι xDSL τεχνολογίες χωρίζονται με βάση τον ρυθμό και την απόσταση μετάδοσης καθώς και τον αριθμό των καλωδίων που απαιτούν. Ακολουθεί μια συνοπτική περιγραφή των βασικών xDSL τεχνολογιών. Η κύρια ιδέα του ADSL (Asymmetric DSL) είναι η λειτουργία των δικτύων σε ταχύτερους ρυθμούς μέσα όμως από την τεχνολογία των σημερινών καλωδίων χαλκού. Η εφαρμογή της τεχνολογίας αυτής επιτρέπει στους χρήστες να λαμβάνουν δεδομένα 100 φορές πιο γρήγορα σε σύγκριση με τα σημερινά V90 modem. Το ADSL εκμεταλλεύεται κατά τον βέλτιστο τρόπο το υποστηριζόμενο φάσμα συχνοτήτων των καλωδίων χαλκού (χρησιμοποιεί ένα φάσμα από 30 KHz έως 1 MHz). Ο διαχωρισμός της τηλεφωνικής κίνησης και της κίνησης δεδομένων γίνεται με μια αναλογική συσκευή η οποία ονομάζεται “splitter” και τοποθετείται τόσο στη πλευρά του κέντρου όσο και στην πλευρά του χρήστη.

Το ADSL υποστηρίζει ασύμμετρη ροή δεδομένων, που αποτελεί και το κύριο χαρακτηριστικό της τεχνολογίας, παρέχοντας ένα σημαντικό μέρος του εύρους στο καθοδικό κανάλι (προς

τον χρήστη). Οι θεωρητικοί ρυθμοί που μπορεί να επιτύχει είναι 8 Mbps και 1,5 Mbps για το καθοδικό και ανοδικό κανάλι αντίστοιχα[19].

3.9. SDH/SONET

Η ανάγκη των χρηστών να μεταφέρουν μεγαλύτερο όγκο πληροφορίας από τα 43,736 Mbps (DS-3) οδήγησε προς την τεχνική SDH (Synchronous Digital

Hierarchy) στην Ευρώπη και στο αντίστοιχο της SONET (Synchromous Optical NETwork) στην Αμερική. Ο βασικός στόχος ήταν η δυνατότητα χρήσης οπτικών ινών για την επίτευξη υψηλών ταχυτήτων. Το SDH είναι μια τεχνική πολύπλεξης ψηφιακών συστημάτων. Ετσι, τα ψηφιακά σήματα (ροές εισόδου ή tributaries) μπορούν να συνδεθούν και επομένως να συγχρονιστούν μεταξύ τους. Η έννοια "συγχρονισμένα" επιτρέπει παρ' όλα αυτά κάποια παραλλαγή στην ταχύτητα των ρολογιών. Επειδή το κάθε tributary (π.χ. DS-1, E1, E2, κ.ά) έχει διαφορετικό ρολόι, το πρόβλημα αυτό αντιμετωπίζεται με τα bit γεμίσματος (bit stuffing), ώστε να "γεμίζονται" τα σήματα με την υψηλότερη ταχύτητα ρολογιού. Η βασική σταθερά χρόνου των 8000 πλαισίων ανά δευτερόλεπτο διατηρείται στο SDH. Αυτό που μεταδίδεται σε αυτά τα 125 μsec, αναπαρίσταται σε ένα "ορθογώνιο", το οποίο περιγράφει την διαμόρφωση του πρώτου (χαμηλότερου) επιπέδου της σύγχρονης ιεραρχίας. Όλη η πληροφορία συλλέγεται σε bytes (οκτάδες) και όχι σε bits. Τα bytes μεταδίδονται κατά μια σειρά την φορά από "πάνω προς τα κάτω". Το μεγαλύτερο μέρος του ορθογωνίου είναι για πληροφορία που μεταδίδεται (261 x 9 bytes) ενώ το μέρος της αριστερής πλευράς (overhead bytes) είναι για άλλες πληροφορίες, όπως δείκτες (pointers) των tributaries (για κάθε διαφορετική ροή εισόδου υπάρχει και ένας δείκτης : π.χ. για 3 E-3 tributaries υπάρχουν 3 δείκτες σε κάθε πλαίσιο STM) και OAM πληροφορίες (πληροφορίες επίβλεψης).

Όταν το n είναι 1, τότε έχουμε το χαμηλότερο επίπεδο της σύγχρονης ιεραρχίας (STM-1) με ρυθμό 270 x 9 x 8000 x 8 bits/sec = 155.52 Mbps. Το STM-4 (n=4) δίνει ταχύτητα 622 Mbps, ενώ το STM-16 συνδυάζει 4 STM-4 με ταχύτητα 2.4 Gbps. Αυτά τα πλαίσια χρησιμοποιούνται και για την μετάδοση ATM δεδομένων μέσα από οπτικές ίνες (π.χ. STM-1 μια μετάδοση ATM στα 155.52 Mbps σε MultiMode ή SingleMode οπτική ίνα).

3.10. ISDN

Από τα τέλη της δεκαετίας του '90 έχει εμφανιστεί η τάση για την ύπαρξη ενός Ολοκληρωμένου Δικτύου, μέσω του οποίου θα παρέχονται στον χρήστη όλες οι υπηρεσίες που ως τώρα παρέχονται από ξεχωριστά δίκτυα, καθώς και νέες και περισσότερο εξελιγμένες υπηρεσίες. Έτσι δημιουργήθηκε το N-ISDN (Ψηφιακό Δίκτυο Ολοκληρωμένων Υπηρεσιών Στενής Ζώνης), το οποίο ολοκληρώνει τις υπηρεσίες και τις τεχνολογίες που αυτές χρησιμοποιούν. Το N-ISDN προσφέρει τηλεφωνία (εύρους ζώνης 3.1 KHZ και 7 KHZ), fax (G4), μεταφορά δεδομένων (με ταχύτητα μεγαλύτερη από 64Kbps), e-mail, teletex, telewriting, μεταφορά ακίνητων εικόνων, συνδυασμένη μετάδοση text και fascimile (ISDN mixed mode), βιντεοτηλέφωνο, telealarm, teleaction, videotex και μεταφορά μηνυμάτων. Οι παραπάνω υπηρεσίες μπορούν να συνδυάζονται μεταξύ τους. Για παράδειγμα κάποιος μπορεί να μιλάει στο τηλέφωνο και ταυτόχρονα να λαμβάνει δεδομένα.

Το N-ISDN παρέχει δύο είδη προσπέλασης: την προσπέλαση βασικού ρυθμού (BRI) στον απλό χρήστη με ταχύτητα 192 Kbps (καθαρή πληροφορία 144 Kbps σε 2B+D κανάλια) και την προσπέλαση πρωτεύοντος ρυθμού (PRI) με ταχύτητα 2048 Kbps (CEPT, 30B+D κανάλια) ή 1544 Kbps (T1, 23B+D κανάλια). Τα B κανάλια μεταφέρουν τις πληροφορίες του χρήστη, ενώ τα D κανάλια περιέχουν πληροφορίες σηματοδοσίας. Τα δύο αυτά είδη καναλιών πολυπλέκονται μεταξύ τους στον χρόνο και μεταδίδονται στο ίδιο φυσικό μέσο. Η

[19] Β.Σκουλάτος ,Σύγχρονα Τηλεπικοινωνιακά Δίκτυα Α' τόμος Φεβ. 2000

ανάπτυξη του N-ISDN θα βασιστεί σε μεγάλο βαθμό στο υπάρχον ψηφιακό τηλεφωνικό δίκτυο[20].

Στην Ευρώπη το N-ISDN έχει τυποποιηθεί από τον οργανισμό ETSI (European Telecommunication Standardisation Institute) με την έκδοση σειράς προτύπων (κυρίως η σειρά ETSI ETS 300 xxx). Έτσι, στην Ευρώπη έχουμε το Ευρωπαϊκό πρότυπο του ISDN στενής ζώνης, το Euro-ISDN. Αυτή τη στιγμή βρίσκεται σε εμπορική εφαρμογή από αρκετούς τηλεπικοινωνιακούς οργανισμούς σε όλο τον κόσμο και στην Ευρώπη, ενώ η τιμολογιακή πολιτική που ακολουθείται ευνοεί την χρήση του.

[20] Χ.Μπούρας ,Δικτυα Δημόσιας Χρήσης και σύνδεση δικτύων Π.Σ 2006

ΚΕΦΑΛΑΙΟ 4 : ΜΕΘΟΔΟΛΟΓΙΑ, ΑΣΦΑΛΕΙΑ ΚΑΙ ΚΟΣΤΟΣ ΕΓΚΑΤΑΣΤΑΣΗΣ ΔΙΚΤΥΑΚΩΝ ΤΕΧΝΟΛΟΓΙΩΝ

Όπως είναι γνωστό, το ενδιαφέρον των επιχειρήσεων που δραστηριοποιούνται στη χώρα μας για τα επιχειρησιακά δίκτυα έχει τα τελευταία χρόνια απογειωθεί. Ο ανταγωνισμός και η τεχνολογική ανάπτυξη ωθούν τις επιχειρήσεις στη συνεχή αναβάθμιση του επιπέδου των υπηρεσιών και των προϊόντων τους, με την υιοθέτηση μεθόδων και εργαλείων νέας τεχνολογίας, έτσι ώστε να διατηρήσουν και να επεκτείνουν το μερίδιο της αγοράς στο οποίο στοχεύουν.
Ένα γνωστό επιχειρησιακό δίκτυο είναι το ERP, το οποίο αφορά στις διαδικασίες ολόκληρης της επιχείρησης φέρνοντας όλες αυτές τις διαδικασίες να συναντήσουν τους επιχειρηματικούς στόχους και ενοποιώντας – ολοκληρώνοντας διαλειτουργικά όλα τα τμήματα της επιχείρησης. Μέσω της διαλειτουργικής ολοκλήρωσης επιτυγχάνεται η ταχύτατη, ακριβής και έγκαιρη μετάδοση της πληροφορίας στο εσωτερικό της επιχείρησης. Αυτή η πληροφορία μπορεί να αφορά σε κόστος, έσοδα, κέρδη, υλικά και άλλα.
Τα επιχειρησιακά δίκτυα αποτελούν το μέσο για την αρμονική συνεργασία ανθρώπινου δυναμικού, δεδομένων, διαδικασιών και τεχνολογιών πληροφορίας και επικοινωνιών. Προέκυψαν ως γέφυρα μεταξύ των πρακτικών εφαρμογών της επιστήμης υπολογιστών και του επιχειρηματικού κόσμου.

4.1. ΠΑΡΑΓΟΝΤΕΣ ΑΝΑΓΚΑΙΟΤΗΤΑΣ ΕΠΙΧΕΙΡΗΣΙΑΚΟΥ ΔΙΚΤΥΟΥ

Τα επιχειρησιακά δίκτυα είναι μια αρκετά μεγάλη δαπάνη για την επιχείρηση καθώς απαιτούν αρκετό χρόνο και μεγάλα χρηματικά ποσά για να εγκατασταθούν. Επομένως μια επιχείρηση θα πρέπει να σιγουρευτεί πως η εγκατάσταση ενός τέτοιου δικτύου, της είναι αναγκαία. Κάποιοι από τους παράγοντες που εξετάζουν την αναγκαιότητα ενός τέτοιου δικτύου είναι οι εξής:

- ΄Υπαρξη περίπλοκων και αναποτελεσματικών επιχειρησιακών διαδικασιών
- Διαπίστωση υψηλών λειτουργικών δαπανών.
- Ανεπαρκής ανταπόκριση στις απαιτήσεις των πελατών.
- Αδυναμία υλοποίησης νέων επιχειρηματικών στρατηγικών και πολιτικών.
- Ανάγκη προσαρμογής στις απαιτήσεις τις διεθνούς ή τοπικής αγοράς
- Μικρή ή μη διαθεσιμότητα της πληροφορίας κατά μήκος του οργανισμού.
- Απαρχαιωμένα επιχειρησιακά δίκτυα
- Πολλά και ασύμβατα συστήματα.

Τα πλεονεκτήματα που μπορεί να προσφέρει η εγκατάσταση ενός επιχειρησιακού δικτύου, στην επιχείρηση, είναι πολλά. Ορισμένα από αυτά τα πλεονεκτήματα είναι τα εξής:

- Απόκτηση μιας ολοκληρωμένης πληροφόρησης για όλα τα τμήματά της επιχείρησης.
- Αυτοματοποίηση των διαδικασιών σε όλα τα τμήματα.
- Δυνατότητα προσομοίωσης της πραγματικής λειτουργίας όλων των τμημάτων της επιχείρησης.
- Επεκτασιμότητα που χαρακτηρίζει τα επιχειρησιακά δίκτυα, τα οποία μπορούν να συνδεθούν με πολλούς άλλους οργανισμούς και πολλές άλλες τεχνολογίες, ώστε να διευρύνουν το φάσμα λειτουργιών της επιχείρησης.

4.2. ΜΕΘΟΔΟΛΟΓΙΑ ΕΓΚΑΤΑΣΤΑΣΗΣ ΕΠΙΧΕΙΡΗΣΙΑΚΟΥ ΔΙΚΤΥΟΥ

Κάθε προμηθευτής ενός δικτύου έχει τη δική του μεθοδολογία εγκατάστασης που διαφέρει από τους υπολοίπους. Η κάθε μεθοδολογία διαφέρει επίσης στο χρόνο και στο κόστος υλοποίησής της. Για τα επιχειρησιακά δίκτυα υπάρχουν τρεις βασικές επιλογές, που η κάθε μία έχει διαφορετικές επιπτώσεις στον οργανισμό. Αποδοχή, αποδοχή με αλλαγές και απόρριψη.

Στην περίπτωση που το σύστημα γίνει αποδεκτό από την επιχείρηση, τότε θα πρέπει η επιχείρηση να ευθυγραμμίσει τις επιχειρηματικές του διαδικασίες με αυτές που εμπεριέχονται στο επιχειρησιακό δίκτυο. Στην περίπτωση που το σύστημα γίνει αποδεκτό με αλλαγές, τότε εκτός από το σύστημα και η επιχείρηση θα πρέπει να επιφέρει αλλαγές στις επιχειρηματικές της διαδικασίες. Τέλος στην περίπτωση της απόρριψης του δικτύου, θα πρέπει να επανεκτιμηθεί ή η επιχείρηση να προμηθευτεί κάποιο άλλο.

Η σωστή μεθοδολογία εγκατάστασης ενός επιχειρησιακού δικτύου περιλαμβάνει δύο κατηγορίες θεμάτων. Η πρώτη κατηγορία είναι τα επιχειρηματικά θέματα, όπου τα βήματα που πρέπει να ακολουθηθούν είναι τα εξής:

- Επιλογή των επιχειρηματικών διαδικασιών που θα αναδιοργανωθούν για να ενταχθούν στο νέο σύστημα.
- Εξέταση όλων των βασικών λειτουργιών που θα εκτελούνται από το σύστημα.
- Ιεράρχηση της σειράς με την οποία θα ενταχθούν στο δίκτυο οι επιλεγμένες επιχειρηματικές διαδικασίες.
- Καθορισμός του εμπλεκομένου στην εκπαίδευση προσωπικού και προσδιορισμός έκτασης της εκπαίδευσης.
- Παρακολούθηση και προσδιορισμός της αναμενόμενης ανάπτυξης.

Η δεύτερη κατηγορία που πρέπει να εξεταστεί είναι τα τεχνολογικά θέματα. Τα προτεινόμενα βήματα είναι τα εξής:

- Απόφαση της έκτασης της αρχικής παραμετροποίησης του δικτύου.
- Απόφαση για τις επιλογές που πρέπει να γίνουν σχετικά με το κάθε λειτουργικό τμήμα του δικτύου ξεχωριστά.
- Υπολογισμός των απαιτήσεων του δικτύου σε επεξεργασία δεδομένων, καθώς και των απαιτήσεων των αλληλεπιδράσεων με τους χρήστες.
- Εκτίμηση του τελικού αριθμού των χρηστών και του προφίλ της χρήσης του δικτύου από αυτούς.
- Εκτίμηση του όγκου των δεδομένων και του ρυθμού αύξησής τους με την πάροδο του χρόνου.
- Ενοποίηση σε μια ολοκληρωμένη πλατφόρμα όλων των εφαρμογών του δικτύου με τις υπάρχουσες εφαρμογές λογισμικού και δεδομένα που αυτές χρησιμοποιούν.

Οι απαιτούμενες ενέργειες για την επιτυχημένη εγκατάσταση ενός επιχειρησιακού δικτύου μπορούν να συνοψιστούν στα παρακάτω:

- Κωδικοποίηση πρώτων και δευτέρων υλών καθώς και των έτοιμων προϊόντων
- Δημιουργία κάθετων ιεραρχιών.
- Αναγνώριση των ροών από το ένα υποσύστημα στο άλλο και ορισμός των οριζόντιων διασυνδέσεων μεταξύ των διαφόρων φάσεων των κύριων επιχειρηματικών διαδικασιών.
- Αποσαφήνιση του τρόπου με τον οποίο το νέο δίκτυο θα μπορέσει να βοηθήσει στην εξάλειψη των βημάτων ή δραστηριοτήτων μη προστιθέμενης αξίας
- Αποσαφήνιση των οργανωτικών αλλαγών που απαιτούνται για την ομαλή μετάβαση στο δίκτυο.
- Καθορισμός των ρόλων που θα έχουν οι χρήστες, καθώς και οι υποχρεώσεις και αρμοδιότητες του καθενός.
- Αποσαφήνιση του θέματος των πληροφοριακών στοιχείων που θα πρέπει να συγκεντρώνονται ή ανταλλάσσονται μεταξύ των διαφόρων υποσυστημάτων του νέου δικτύου.
- Ανάπτυξη δικτύου χρηματοοικονομικής παρακολούθησης, καθώς και συστήματος

κοστολόγησης.

4.3. ΒΗΜΑΤΑ ΕΓΚΑΤΑΣΤΑΣΗΣ ΕΠΙΧΕΙΡΗΣΙΑΚΟΥ ΔΙΚΤΥΟΥ

Η εγκατάσταση ενός επιχειρησιακού δικτύου αποτελείται από τις διαδικασίες πριν την εγκατάσταση, τις διαδικασίες κατά τη διάρκεια της εγκατάστασης και διαδικασίες μετά την εγκατάσταση.
Η φάση των διαδικασιών πριν την εγκατάσταση αποτελείται από τα παρακάτω στάδια:

- Με αφορμή την εγκατάσταση του επιχειρησιακού δικτύου, η επιχείρηση θα πρέπει να αναδιοργανώσει κάποιες από τις διαδικασίες της. Οι προσπάθειες επικεντρώνονται στην καταγραφή, ανάλυση και μέτρηση της απόδοσης των υφιστάμενων επιχειρηματικών διαδικασιών, αλλά και στην εύρεση και επιλογή της κατάλληλης παραλλαγής από πολλές εναλλακτικές διαδικασίες.
- Οργάνωση ομάδας έργου εγκατάστασης. Η δομή της ομάδας αυτής διαφέρει ανάλογα τις απαιτήσεις του δικτύου. Μια τυπική ομάδα περιλαμβάνει τον χορηγό του έργου που εξασφαλίζει τους πόρους που απαιτούνται, τον υπεύθυνο έργου που αναλαμβάνει τη διοίκηση του έργου εγκατάστασης, την επιτροπή καθοδήγησης που ασκεί την εποπτεία του έργου και λαμβάνει σημαντικές αποφάσεις για τον τρόπο εγκατάστασής του και τέλος την ομάδα έργου που εκτελούν τα βασικά τμήματα του έργου.
- Σχεδιασμός και ανάπτυξη προγράμματος εγκατάστασης. Σε αυτό το στάδιο σχεδιάζεται και αναπτύσσεται το πρόγραμμα εγκατάστασης του δικτύου. Αρχικά γίνεται ο χρονοπρογραμματισμός του έργου και η τμηματοποίηση του σε ορθολογικά οριοθετημένες και διακριτές εργασίες, για τις οποίες καθορίζονται ο χρόνος υλοποίησης, οι απαιτούμενοι πόροι, τα χρονικά ορόσημα, οι υπεύθυνοι, ο μέγιστος δυνατός χρόνος εγκατάστασης και οι προϋποθέσεις επιτυχίας. Ακολουθεί η ανάθεση των απαιτούμενων πόρων στις προσδιορισμένες εργασίες.
- Στο επόμενο στάδιο γίνεται έλεγχος επιχειρηματικών δεδομένων και πληροφοριών. Σημαντικό ρόλο επίσης παίζουν η έγκαιρη αξιολόγηση της ορθότητας των υφιστάμενων δεδομένων και πληροφοριών της επιχείρησης, ο κατάλληλος μετασχηματισμός τους ώστε να ανταποκρίνονται στις δομές δεδομένων του δικτύου και η ορθή μεταφορά τους από το παλαιό δίκτυο στο νέο.
- Επιλογή τρόπου μετάβασης στο νέο επιχειρησιακό δίκτυο. Για την μετάβαση από το παλαιό στο νέο δίκτυο υπάρχουν οι παρακάτω επιλογές:
    - Άμεση διακοπή λειτουργίας του παλαιού δικτύου.
    - Σταδιακή διακοπή λειτουργίας του παλαιού δικτύου.
    - Παράλληλη εκτέλεση των δύο δικτύων.
    - Πιλοτική εκτέλεση του νέου δικτύου.

Η δεύτερη φάση είναι οι διαδικασίες κατά την εγκατάσταση του επιχειρησιακού δικτύου. Σε αυτή τη φάση αφού εγκατασταθεί ο απαραίτητος εξοπλισμός ξεκινάει η πιλοτική εφαρμογή του δικτύου. Η πιλοτική εφαρμογή επικεντρώνεται σε ένα αντιπροσωπευτικό δείγμα περιπτώσεων - λειτουργικών τμημάτων, αλλά εισχωρεί σε βάθος στις ιδιαιτερότητες κάθε διαδικασίας. Κατά τη διάρκεια της πιλοτικής εφαρμογής αναγνωρίζονται τυχόν προβλήματα στο σχεδιασμό και στην υλοποίηση των διαδικασιών, καθώς και στην παραμετροποίηση του συστήματος. Αυτά τα προβλήματα οδηγούν στον περαιτέρω σχεδιασμό των επιχειρηματικών διαδικασιών και στον ανασχεδιασμό των αναφορών, των μενού, των εντολών και των επιπέδων πρόσβασης των χρηστών. Σε αυτή τη φάση γίνεται και η διαδικασία μετάβασης δεδομένων από το παλαιό δίκτυο, στο νέο.
Μετά από αυτή τη φάση ακολουθεί η Τρίτη φάση που περιλαμβάνει τις διαδικασίες μετά την εγκατάσταση του δικτύου. Η κυριότερη διαδικασία αυτής της φάσης είναι η εκπαίδευση των διαχειριστών και των τελικών χρηστών. Η διαδικασία αυτή περιλαμβάνει διαφορετικά στάδια, όπως τη γενική εισαγωγή στη χρήση του δικτύου, την εκπαίδευση στις διαδικασίες και στις

μεθόδους που υποστηρίζει το δίκτυο, τη λεπτομερή εκπαίδευση στις οθόνες που χρησιμοποιεί και τα βήματα που εκτελεί ο κάθε χρήστης, την εκπαίδευση στα εργαλεία του δικτύου, και άλλα.

4.4. ΛΟΓΟΙ ΑΠΟΤΥΧΙΑΣ ΕΠΙΧΕΙΡΗΣΙΑΚΟΥ ΔΙΚΤΥΟΥ

Η εγκατάσταση ενός επιχειρησιακού δικτύου είναι μια περίπλοκη διαδικασία με πολλά στάδια εξέλιξης. Η έναρξή της σηματοδοτείται από τη στιγμή που η επιχείρηση θα πρέπει να επιλέξει το καταλληλότερο για τις ανάγκες της δίκτυο. Τα κυριότερα προβλήματα που σχετίζονται με την εγκατάσταση ενός επιχειρησιακού δικτύου είναι το μέγεθος του έργου, η υπέρβαση του χρονοδιαγράμματος, οι πολιτικές οργάνωσης, ενδεχόμενα λειτουργικά προβλήματα, η επικοινωνία με άλλα δίκτυα, και άλλα.
Οι κίνδυνοι υλοποίησης του επιχειρησιακού δικτύου είναι οι εξής:

- Έλλειψη κατάλληλης τεχνολογικής υποδομής
- Έλλειψη τεχνικής εξειδίκευσης
- Τεχνική πολυπλοκότητα
- Έλλειψη γνώσης του δικτύου.
- Έλλειψη ομοφωνίας ως προς τους στόχους του έργου.
- Έλλειψη αφοσίωσης από τους χρήστες και αναποτελεσματική επικοινωνία με αυτούς
- Ελλιπής εμπλοκή της διοίκησης
- Ανεπαρκείς πόροι
- Συγκρούσεις μεταξύ λειτουργικών τμημάτων
- Έλλειψη συστήματος μέτρησης ελέγχου κινδύνου και ανεπαρκής διαχείριση έργου

Επομένως για μια επιτυχημένη εγκατάσταση θα πρέπει να ληφθούν υπόψη όλοι οι παραπάνω κίνδυνοι και να αντιμετωπιστούν οποιαδήποτε ενδεχόμενα προβλήματα προκύψουν.

4.5. ΑΠΟΤΙΜΗΣΗ ΕΓΚΑΤΑΣΤΑΣΗΣ ΕΠΙΧΕΙΡΗΣΙΑΚΟΥ ΔΙΚΤΥΟΥ

Η αποτίμηση του επιχειρησιακού δικτύου αναφέρεται στην αξιολόγηση πριν και μετά την υλοποίηση του δικτύου. Η αξιολόγηση πριν την υλοποίηση προσπαθεί να εκτιμήσει και να αξιολογήσει τη θετική ή αρνητική επίδραση του δικτύου όταν αυτό εγκατασταθεί, με τελικό σκοπό να υποστηρίξει τη δικαιολόγηση της επένδυσης.
Το επιχειρησιακό δίκτυο καλείται να βελτιώσει διαδικασίες μέσα στην επιχείρηση, ώστε να επιτύχει την άψογη λειτουργία της, αυτοματοποιώντας σε μεγάλο βαθμό διαδικασίες που παραδοσιακά εκτελούνταν χειρόγραφα και μη τυποποιημένα. Βέβαια με την εγκατάσταση του δικτύου στην επιχείρηση δε σημαίνει ότι λύνονται αυτόματα όλα τα λειτουργικά προβλήματά της. Ακόμα και αυτά που λύνονται στην αρχή, πρέπει να αξιολογούνται λειτουργικά στην πορεία του χρόνου, καθώς από διάφορες αιτίες η λειτουργία του δικτύου μπορεί να μην είναι πάντα η αναμενόμενη. Τα αίτια για τις δυσλειτουργίες του συστήματος μπορεί να οφείλονται σε διάφορες παραμέτρους, όπως:

- Ανεπαρκές hardware
- Προσωπικό που έχει έρθει πρόσφατα στην επιχείρηση και δεν έχει την απαιτούμενη εκπαίδευση στο σύστημα
- Σταδιακή αποστασιοποίηση του προσωπικού από το δίκτυο
- Η επιχείρηση δεν προέβλεψε να επιλύσει έγκαιρα τα προβλήματα των χρηστών με το σύστημα και εκείνοι το παρακάμπτουν
- Το δίκτυο έχει φορτωθεί υπερβολικά, με αποτέλεσμα να καθυστερεί τους χρήστες.

Έτσι, λοιπόν, το επιχειρησιακό δίκτυο δε θα πρέπει να αντιμετωπίζεται ως ένα project με ορισμένη αρχή και τέλος. Το τέλος του έργου αυτού δεν έρχεται με την εγκατάσταση του δικτύου στην επιχείρηση αλλά εξακολουθεί να αποτελεί ένα έργο διαρκείας, εφόσον η

επιχείρηση επιθυμεί πραγματικά να έχει οφέλη από αυτό. Η εγκατάσταση ενός επιχειρησιακού δικτύου σε μία επιχείρηση πρακτικά τελειώνει με την αντικατάστασή του από ένα άλλο δίκτυο, όταν και εάν αυτή συμβεί.

4.6. ΑΣΦΑΛΕΙΑ ΕΠΙΧΕΙΡΗΣΙΑΚΟΥ ΔΙΚΤΥΟΥ

Οι τεχνολογίες ασφαλείας δικτύου προστατεύουν το δίκτυό από κλοπή και κατάχρηση απόρρητων επιχειρηματικών πληροφοριών, καθώς και από κακόβουλες επιθέσεις από ιούς του Internet και ιούς τύπου worm. Χωρίς εγκατεστημένη ασφάλεια δικτύου, η επιχείρηση διατρέχει κίνδυνο παρείσφρησης από μη εξουσιοδοτημένους χρήστες, διακοπής λειτουργίας του δικτύου, διακοπής υπηρεσιών, μη συμμόρφωσης με κανονισμούς, ακόμα και νομικής δίωξης.

Λειτουργία Ασφαλείας

Η ασφάλεια δικτύου δεν βασίζεται σε μία μέθοδο, αλλά χρησιμοποιεί ένα σύνολο φραγμών που υπερασπίζονται την επιχείρησή με διάφορους τρόπους. Ακόμα και αν μια λύση αποτύχει, οι υπόλοιπες εξακολουθούν να είναι ενεργές, προφυλάσσοντας την εταιρεία και τα δεδομένα της από διάφορες επιθέσεις μέσω δικτύου.

Τα διάφορα επίπεδα ασφαλείας στο δίκτυό υποδεικνύουν ότι οι πολύτιμες πληροφορίες, στις οποίες βασίζονται για τις επιχειρηματικές συναλλαγές, είναι διαθέσιμες στην επιχείρηση και παραμένουν προστατευμένες από απειλές.

Συγκεκριμένα, η ασφάλεια δικτύου:

Προστατεύει από εσωτερικές και εξωτερικές επιθέσεις μέσω δικτύου. Οι απειλές μπορεί να προέρχονται τόσο μέσα όσο και έξω από τους χώρους της επιχείρησής. Ένα αποτελεσματικό σύστημα ασφαλείας παρακολουθεί όλη τη δραστηριότητα δικτύου, επισημαίνει την ασυνήθιστη συμπεριφορά και ενεργεί κατάλληλα.

Διασφαλίζει το ιδιωτικό απόρρητο όλων των επικοινωνιών. Οι εργαζόμενοι μπορούν να συνδέονται στο δίκτυο από το σπίτι τους ή ενώ βρίσκονται καθ' οδόν με τη βεβαιότητα ότι οι επικοινωνίες τους παραμένουν απόρρητες και προστατεύονται.

Ελέγχει την πρόσβαση στις πληροφορίες, προσδιορίζοντας με ακρίβεια την ταυτότητα των χρηστών και των συστημάτων τους. Οι επιχειρήσεις μπορούν να ορίζουν τους δικούς τους κανόνες σχετικά με την πρόσβαση στα δεδομένα. Η απόρριψη ή έγκριση μιας άδειας πρόσβασης μπορεί να γίνει βάσει της ταυτότητας των χρηστών, των επαγγελματικών αρμοδιοτήτων ή άλλων συγκεκριμένων κριτηρίων που καθορίζονται από την επιχείρηση.

Καθιστά την επιχείρησή πιο αξιόπιστη. Εφόσον οι τεχνολογίες ασφαλείας επιτρέπουν στο σύστημά να εμποδίζει γνωστές επιθέσεις και να προσαρμόζεται σε νέες απειλές, οι εργαζόμενοι, οι πελάτες και οι επιχειρησιακοί συνεργάτες μπορούν να είναι βέβαιοι ότι οι πληροφορίες τους παραμένουν απόλυτα ασφαλείς.

Τρόποι Χρήσης Τεχνολογιών Ασφαλείας

Η ασφάλεια δικτύου αποτελεί πλέον κύρια απαίτηση για τις επιχειρήσεις, ειδικά για εκείνες που βασίζονται στο Internet. Οι πελάτες, οι προμηθευτές και οι επιχειρηματικοί συνεργάτες πιθανώς θεωρούν δεδομένο ότι θα προστατευτούν οι πληροφορίες τους που χρησιμοποιούνται από κοινού.

Ενώ η ασφάλεια δικτύου αποτελεί σχεδόν προϋπόθεση για τη λειτουργία μιας επιχείρησης, παράλληλα αποδίδει με πολλούς τρόπους. Εδώ παρουσιάζονται ορισμένα οφέλη που μπορεί να προσφέρει ένα ασφαλές δίκτυο:

Εμπιστοσύνη πελατών

- Διασφάλιση ιδιωτικού απόρρητου
- Ενθάρρυνση συνεργασίας

Ένα ισχυρό σύστημα ασφαλείας διαβεβαιώνει τους πελάτες ότι δεν είναι δυνατή η πρόσβαση σε ευαίσθητες πληροφορίες, όπως σε αριθμούς πιστωτικών καρτών ή εμπιστευτικές επιχειρηματικές λεπτομέρειες, και η κακόβουλη εκμετάλλευσή τους. Οι επιχειρησιακοί

συνεργάτες θα αισθάνονται μεγαλύτερη σιγουριά κατά την κοινή χρήση δεδομένων, όπως π.χ. προβλέψεις πωλήσεων ή αρχικά σχέδια προϊόντων. Επιπλέον, οι ίδιες τεχνολογίες που αποτρέπουν τους εισβολείς μπορούν να επιτρέψουν στους συνεργάτες πρόσβαση υψηλής ασφαλείας σε πληροφορίες του δικτύου, εξυπηρετώντας την αποτελεσματικότερη συνεργασία.

Φορητότητα

- Πρόσβαση υψηλής ασφαλείας καθ' οδό
- Ευνοεί την παραγωγικότητα εκτός των εγκαταστάσεων του γραφείου.

Η ισχυρή ασφάλεια δικτύου επιτρέπει στους εργαζόμενους της εταιρείας να συνδέονται με ασφάλεια στο δίκτυο, ενώ βρίσκονται καθ' οδό ή από το σπίτι τους χωρίς το φόβο προσβολής από ιούς ή τον κίνδυνο άλλων απειλών. Η άνετη πρόσβαση υψηλής ασφαλείας στο δίκτυο σημαίνει ότι οι εργαζόμενοι μπορούν να χρησιμοποιούν πληροφορίες κρίσιμης σημασίας όποτε τις χρειάζονται, με αποτέλεσμα να είναι παραγωγικότεροι ακόμα και όταν δεν βρίσκονται στο γραφείο τους.

Βελτιωμένη παραγωγικότητα

- Λιγότερο χρονοβόρα διαχείριση ανεπιθύμητης αλληλογραφίας
- Επαγγελματική δεοντολογία υψηλού επιπέδου και βελτιωμένη συνεργασία

Ένα αποτελεσματικό πρόγραμμα ασφάλειας δικτύου μπορεί να δώσει ώθηση στην παραγωγικότητα της επιχείρησής. Οι εργαζόμενοι δαπανούν λιγότερο χρόνο σε μη παραγωγικές εργασίες, όπως η σχολαστική διαλογή μηνυμάτων ανεπιθύμητης αλληλογραφίας ή η αντιμετώπιση ιών. Το δίκτυο και η σύνδεσή στο Internet παραμένουν ασφαλή, εξασφαλίζοντας στους εργαζόμενούς τακτική πρόσβαση στο Internet και στο ηλεκτρονικό ταχυδρομείο.

Μειωμένο κόστος

- Δυνατότητα αποφυγής των διακοπών υπηρεσίας
- Ασφαλής ανάπτυξη σύνθετων υπηρεσιών

Η διακοπή λειτουργίας δικτύου είναι επιζήμια για κάθε τύπο επιχείρησης. Διασφαλίζοντας ότι το δίκτυο και η σύνδεσή στο Internet λειτουργούν κανονικά και με ασφάλεια, μπορείτε να είναι βέβαιη η επιχείρηση ότι οι πελάτες της μπορούν να τους βρίσκουν όποτε τους χρειάζονται. Η αποτελεσματική ασφάλεια επιτρέπει την προσθήκη νέων υπηρεσιών και εφαρμογών στην επιχείρησή χωρίς να χρειάζεται να διακοπεί η απόδοση του δικτύου. Η προληπτική προσέγγιση όσον αφορά την προστασία των δεδομένων, εξασφαλίζει τη λειτουργία της επιχείρησής όπως απαιτείται.

Καθώς η εταιρεία αναπτύσσεται, οι ανάγκες δικτύωσης μεταβάλλονται. Με την εγκατάσταση ενός ισχυρού δικτύου υψηλής ασφαλείας, θα μπορεί να προσθέτει σύνθετες δυνατότητες, όπως ασφαλή ασύρματη δικτύωση, λειτουργίες φωνής και τηλεδιάσκεψης.

4.7. ΓΕΝΙΚΕΣ ΑΡΧΕΣ ΤΗΣ ΑΝΑΛΥΣΗΣ ΚΟΣΤΟΥΣ – ΟΦΕΛΟΥΣ

Η Ανάλυση Κόστους-Οφέλους είναι ένα εργαλείο, μία τεχνική οικονομικής εκτίμησης που χρησιμοποιείται για τη σύγκριση των αναμενόμενων οφελών από προτεινόμενες επενδύσεις, έργα με τα σχετικά μεγέθη κόστους, ώστε να βοηθούνται οι χρήστες στον προσδιορισμό της εναλλακτικής λύσης με το μέγιστο καθαρό όφελος (οφέλη μείον κόστος). Όσο περισσότερο τα οφέλη υπερβαίνουν το κόστος, τόσο περισσότερο θα ωφεληθούν οι τελικοί χρήστες (η κοινωνία) από τη δραστηριότητα του έργου ή από τη σχετική απόφαση πολιτικής.

Με άλλα λόγια, η οικονομική Ανάλυση Κόστους-Οφέλους επιδιώκει να καταγράψει όλα τα οφέλη και τα μεγέθη κόστους, ανεξάρτητα από το ποιος επηρεάζεται από αυτά. Βέβαια, στην περίπτωση επενδύσεων ή έργων όπου το κόστος και τα οφέλη περιορίζονται ως προς τις επιπτώσεις τους σε μία μόνον υπηρεσία ή σε ένα μόνον τμήμα (π.χ. αγορά νέων φορητών

Η/Υ τύπου notebook για ένα τμήμα, απόφαση μίσθωσης ή αγοράς κτιρίου για μία υπηρεσία), θα πρέπει να χρησιμοποιείται «χρηματοοικονομική Ανάλυση Κόστους-Οφέλους» (Financial CBA), δηλαδή να εξετάζονται τα οφέλη και το κόστος για την επιμέρους υπηρεσία ή το επιμέρους τμήμα.
Η εκπόνηση Ανάλυσης Κόστους/ Οφέλους είναι συνήθως σύνθετη και πολύπλοκη εργασία που θα πρέπει να διεκπεραιώνεται από εξειδικευμένο προσωπικό ή να ανατίθεται σε εξωτερικούς συμβούλους, καθώς περιλαμβάνει σύνθετους υπολογισμούς και προηγμένες μεθόδους χρηματοοικονομικής ανάλυσης που απαιτούν σχετικό υπόβαθρο γνώσεων και εξοικείωση με τεχνικές εκτίμησης επενδύσεων. Η Ανάλυση Κόστους-Οφέλους θα πρέπει να εκπονείται πολύ προσεκτικά και από εξειδικευμένους συμβούλους, ώστε να αιτιολογεί την αίτηση για συγχρηματοδότηση και να λαμβάνει τη σχετική έγκριση.
Τα σημαντικότερα μέρη της Ανάλυσης Κόστους-Οφέλους είναι τα εξής:

- Καθορισμός της διάρκειας ζωής της επένδυσης/ του Έργου (περίοδος ανάλυσης).
- Προσδιορισμός όλων των σχετικών μεγεθών κόστους και των οφελών μίας δεδομένης επένδυσης /πρότασης /επιλογής.
- Εκτίμηση όλων των σχετικών μεγεθών κόστους και των οφελών μίας δεδομένης επένδυσης/ πρότασης/ επιλογής (απόδοση χρηματικών αξιών).
- Κατάρτιση των ταμειακών ροών για την περίοδο ανάλυσης.
- Αναγωγή των ταμειακών ροών σε παρούσες αξίες.
- Υπολογισμός της Καθαρής Παρούσας Αξίας (Net Present Value – NPV).
- Αξιολόγηση των εναλλακτικών επιλογών και εκλογή της προτιμώμενης επιλογής.

4.8. ΑΠΟΔΟΣΗ ΕΠΕΝΔΥΣΗΣ (RETURN ON INVESTMENT ROI)

Ο δείκτης "απόδοση επένδυσης" (ROI) χρησιμοποιείται για την αξιολόγηση της απόδοσης μιας επένδυσης ή για να συγκρίνει την αποδοτικότητα διαφορετικών επενδύσεων. Για τον υπολογισμό του ROI, το όφελος (απόδοση) μιας επένδυσης διαιρείται με το κόστος της και το αποτέλεσμα εκφράζεται ως ποσοστό.

$$\text{Απόδοση της επένδυσης} = \frac{(\text{Κέρδος επένδυσης} - \text{Κόστος επένδυσης})}{\text{Κόστος επένδυσης}}$$

Ο ROI μετρά πόσο αποτελεσματικά η επιχείρηση χρησιμοποιεί τα κεφάλαια της για να παράγει κέρδος κι είναι ένας πολύ δημοφιλής δείκτης μέτρησης λόγω της ευελιξίας και της απλότητα του. Εάν η επένδυση δεν έχει θετικό πρόσημο ή αν υπάρχουν άλλες επενδύσεις με υψηλότερη απόδοση, τότε η επένδυση δεν θα πρέπει να αναληφθεί.
Παράδειγμα:
Αν η απόδοση της επένδυσής μακροπρόθεσμα, είναι χαμηλότερη από το κόστος κεφαλαίου, τότε είναι προτιμότερο για την επιχείρηση να ρευστοποιήσει τα περιουσιακά στοιχεία της και να καταθέσει τα έσοδα σε μια τράπεζα.
Η μέτρηση της απόδοσης μιας επένδυσης μπορεί να μεταβάλλεται ανάλογα με την κατάσταση, βάζοντας ως κόστη και κέρδη κάθε φορά τα απαιτούμενα.
Παράδειγμα:
Ένας έμπορος μπορεί να συγκρίνει δύο διαφορετικά προϊόντα, με τη διαίρεση του μικτού κέρδους κάθε προϊόντος δια των αντίστοιχων διαφημιστικών δαπανών.
Ένας οικονομικός αναλυτής, ωστόσο, μπορεί να συγκρίνει τα δύο ίδια προϊόντα χρησιμοποιώντας ένα εντελώς διαφορετικό υπολογισμό ROI, διαιρώντας π.χ. τα συνολικά έσοδα από την πώληση των προϊόντων με τα συνολικά κόστη παραγωγής.
Αυτή η ευελιξία έχει κι ένα μειονέκτημα όμως, καθώς ο υπολογισμός του ROI μπορεί εύκολα να χειραγωγηθεί και να εκφράσει διαφορετικό αποτέλεσμα κάθε φορά ώστε να εξυπηρετεί

τους σκοπούς του χρήστη.
Ο ROI χρησιμοποιείται επίσης από τους τραπεζίτες, τους επενδυτές και τους αναλυτές των επιχειρήσεων για να αξιολογήσουν την οικονομική ισχύ και την αποτελεσματική διαχείριση των πόρων μιας επιχείρησης.
Οι ειδικοί λένε ότι οι εταιρείες συνήθως χρειάζονται τουλάχιστον 10-14% απόδοση της επένδυσης προκειμένου να χρηματοδοτήσουν τη μελλοντική τους ανάπτυξη. Αν η αναλογία αυτή είναι πολύ χαμηλή, είτε η διοίκηση δεν είναι πολύ αποτελεσματική, είτε η πολιτική της επιχείρησης είναι ιδιαίτερα συντηρητική.
Από την άλλη, ένα υψηλό ROI μπορεί να σημαίνει είτε ότι η διαχείριση κάνει καλή δουλειά, ή ότι η επιχείρηση δεν έχει τα απαιτούμενα για τον κύκλο εργασιών της κεφάλαια.
Ο ROI μπορεί επίσης να χρησιμοποιηθεί για την αξιολόγηση μιας προτεινόμενης επένδυσης σε νέο εξοπλισμό, διαιρώντας την αύξηση των κερδών που οφείλεται στον νέο εξοπλισμό με την αύξηση των δαπανών που απαιτούνται για την απόκτηση του.
Παράδειγμα:
Μια μικρή επιχείρηση μπορεί να είναι σε θέση να αυξήσει τα λειτουργικά της κέρδη κατά 1.000€, επενδύοντας 5.000€ σε αναβάθμιση εξοπλισμού.
Αυτό παράγει ένα ROI των 1.000 / 5.000 ή 20%. Εάν το ποσοστό αυτό είναι υψηλότερο από το κόστος ευκαιρίας του κεφαλαίου (του επιτοκίου που καταβάλλεται στο χρέος και τα μερίσματα που καταβάλλονται σε επενδυτές) πριν από την επένδυση, και δεν υπάρχουν καλύτερες επενδυτικές ευκαιρίες, αξίζει η αναβάθμιση.

ΚΕΦΑΛΑΙΟ 5: ΑΣΦΑΛΕΙΑ

Στην καθομιλουμένη γλώσσα ασφάλεια είναι η κατάσταση εκείνη, στην οποία δεν υπάρχει κίνδυνος, όπου αισθάνεται κάποιος ότι, δεν απειλείται. Είναι επίσης η αποτροπή κινδύνου ή απειλής, ή εξασφάλιση σιγουριάς και βεβαιότητας . Στην καθημερινή πρακτική, ο καθένας δίνει στον όρο ασφάλεια, το περιεχόμενο εκείνο, που καθορίζουν οι συνθήκες ασκήσεως του επαγγέλματός του και η γενικότερη κοσμοθεωρία του.
Σε κάθε περίπτωση όλοι, όσοι ασχολούνται με θέματα ασφαλείας "συναντώνται" στην κατάσταση εκείνη, όπου δεν υπάρχει κίνδυνος, όπου αισθάνονται ασφαλείς, όπου δεν απειλούνται, όπου πρέπει να αποτρέψουν τον κίνδυνο ή την απειλή και όπου πρέπει να εξασφαλίσουν την σιγουριά και την βεβαιότητα κατά την ενάσκηση του έργου των. Είναι ευνόητο βέβαια ότι, η ασφάλεια στο διαδίκτυο είναι ένα θέμα που αφορά όλους, δηλαδή τόσο τα μεμονωμένα άτομα, τις επιχειρήσεις, αλλά ακόμα και αυτές τις οργανωμένες πολιτείες .

5.1 Η ΝΟΜΙΚΗ ΕΝΝΟΙΑ ΤΗΣ ΑΣΦΑΛΕΙΑΣ

Για τον νομικό, κάθε έννοια έχει το περιεχόμενο εκείνο, που με ακρίβεια καθορίζει ο νόμος για το συγκεκριμένο θέμα. Το ίδιο συμβαίνει βέβαια και με την έννοια της ασφάλειας. Άρα για το νομικό ασφάλεια στο διαδίκτυο σημαίνει αυτό που ο νόμος ορίζει ως ασφάλεια στο διαδίκτυο. Ο νόμος επίσης καθορίζει και το περιεχόμενο όλων εκείνων των επιμέρους εννοιών που αναφέρονται στον βασικό ορισμό της ασφάλειας. Έτσι αν π.χ. ο νομοθέτης ορίσει ως ασφάλεια στο διαδίκτυο "τον κίνδυνο να επέλθει κάποια βλάβη", θα πρέπει να ορίσει ταυτόχρονα και τους όρους "κίνδυνο" και "βλάβη".
Για το συγκεκριμένο θέμα, της ασφάλειας του διαδικτύου, ή της ασφάλειας στο διαδίκτυο η Ελληνική νομοθεσία δεν έχει δώσει ακόμα ορισμό. Θα έλεγα, χωρίς επιφύλαξη ότι, ουδόλως έχει ασχοληθεί με το θέμα. Αυτό σημαίνει πρακτικώς ότι, ο ποινικός νομοθέτης δεν έχει (ακόμα) θεωρήσει την ασφάλεια στον κυβερνοχώρο ως έννομο αγαθό .
Βέβαια, η έννοια της ασφάλειας δεν είναι άγνωστη στο ποινικό δίκαιο. Έτσι, στο 14ο κεφάλαιο του ποινικού Κώδικα και στα άρθρα 290 επόμενα, ο ποινικός νομοθέτης με συγκεκριμένες διατάξεις προσδιορίζει τα εγκλήματα κατά της ασφάλειας των συγκοινωνιών και κατά των κοινωφελών εγκαταστάσεων. Επίσης στο άρθρο 388 Π.Κ. που ρυθμίζει την απάτη την σχετική με τις ασφάλειες, η έννοια της ασφάλειας λαμβάνεται από το ασφαλιστικό δίκαιο, ενώ στα άρθρα 69 επόμ. Π.Κ. που αναφέρονται στα μέτρα ασφαλείας, ως μέρος της επιβολής ή εκτέλεσης των ποινών, η έννοια της ασφάλειας λαμβάνεται από το δημόσιο δίκαιο (δημόσια ασφάλεια).
Συμπερασματικός μπορεί να λεχθεί ότι, η έννοια της ασφάλειας στο διαδίκτυο δεν έχει καθοριστεί ακόμα από το νομοθέτη. Κατά τον καθορισμό της όμως, πρέπει να ληφθούν υπόψη οι βασικές Αρχές του Δικαίου, όπως αυτές προσδιορίζονται στο Ελληνικό Σύνταγμα και στους ισχύοντες Διεθνείς Κανόνες.

5.2 ΒΑΣΙΚΕΣ ΑΡΧΕΣ ΤΟΥ ΟΡΟΥ "ΑΣΦΑΛΕΙΑ" ΣΤΙΣ ΣΥΝΑΛΛΑΓΕΣ

Στο διαδίκτυο ``διακινούνται`` πληροφορίες - δεδομένα (data) που έχουν σχέση με την προσωπική και ιδιωτική σφαίρα του ατόμου (χρήστη ή μη χρήστη του διαδικτύου). Κάθε άτομο έχει το δικαίωμα να απαιτήσει την μη διαρροή των στοιχείων αυτών σε τρίτα ``αδιάκριτα βλέμματα``. Κατά συνέπεια απαιτεί τα στοιχεία αυτά να κινούνται με ασφάλεια και μυστικότητα. Η ελεύθερη διακίνηση των ιδεών, ο σεβασμός της αξίας και η προστασία του ατόμου, η ελεύθερη ανάπτυξη της προσωπικότητας, το απόρρητο και το απαραβίαστο της επικοινωνίας, αποτελούν μερικές από τις βασικότερες Αρχές του δικαίου. Είναι ευνόητων ότι, οι θεμελιώδεις αυτές Αρχές πρέπει να εφαρμόζονται και στον κυβερνοχώρο. Ο υπερβολικός αστυνομικός έλεγχος (αστυνόμευση) του κυβερνοχώρου, δηλαδή η ευρεία διατύπωση του όρου ασφάλεια έρχεται ή ενδεχομένως να έρχεται σε αντίθεση με τις παραπάνω Αρχές. Δεν μπορούμε να ομιλούμε για κρατικό έλεγχο, καθότι η έννοια του κράτους και της κρατικής κυριαρχίας είναι έννοιες άγνωστες στο διαδίκτυο.

Η εφαρμογή όμως των Αρχών αυτών στο διαδίκτυο είναι ένα από τα πλέον δύσκολα και περίπλοκα θέματα, τόσο από τεχνικής, όσο και από νομικής απόψεως. Από τεχνική άποψη διότι, κάθε τεχνικός τρόπος που αποβλέπει στην ασφάλεια του διαδικτύου, μπορεί να εξουδετερωθεί και συνήθως εξουδετερώνεται) από ένα άλλο τρόπο "αντιασφάλειας". Από νομική άποψη διότι, ο νομοθέτης δεν "προφταίνει" να παρακολουθεί τις τεχνολογικές εξελίξεις και τις κοινωνικές επιπτώσεις και συνέπειες των, ώστε να μπορέσει να τις ρυθμίσει. Με άλλα λόγια οι αλλαγές στην τεχνική δομή του κυβερνοχώρου και κατά συνέπεια στη νομική αντιμετώπισή του, είναι τόσο ραγδαίες, που, εάν το θέμα δεν "σταθεροποιηθεί" κάπου από τεχνολογικής απόψεως, ο νομοθέτης δεν θα καταφέρει να λάβει οποιοδήποτε μέτρο , σε ουσιαστικό ή δικονομικό επίπεδο.

5.3 Η ΤΕΧΝΙΚΗ ΔΙΑΣΤΑΣΗ ΤΟΥ ΟΡΟΥ ΑΣΦΑΛΕΙΑ

Από τεχνική άποψη, ασφάλεια είναι η προστασία ενός συστήματος υπολογιστών και των δεδομένων του από απώλεια ή ζημιά. Αυτή επιτυγχάνεται με την πρόληψη της πρόσβασης μη εξουσιοδοτημένων ατόμων στο σύστημα . Κλασσικό παράδειγμα ασφαλείας αποτελεί η συναλλαγή (αγοραπωλησία) που γίνεται στο διαδίκτυο με την χρήση πιστωτικής κάρτας. Σ' αυτήν την περίπτωση πρέπει να εξασφαλιστεί ότι, δεν είναι δυνατόν να «συλλάβει» (υποκλέψει) κάποιος τον αριθμό της πιστωτικής κάρτας ή να τον αντιγράψει από τον διακομιστή, που είναι αποθηκευμένος. Επίσης πρέπει να επαληθευτεί ότι, ο αριθμός της πιστωτικής κάρτας αποστέλλεται πράγματι, από το πρόσωπο, που ισχυρίζεται ότι τον στέλνει. Η ασφάλεια δηλαδή των δεδομένων που διακινούνται στο διαδίκτυο πρέπει να ικανοποιεί την εμπιστευτικότητα, την ακεραιότητα και την διαθεσιμότητα των δεδομένων. Εμπιστευτικότητα (confidentiality) των δεδομένων είναι η ιδιότητά τους να καθίστανται προσπελάσιμα μόνο από εξουσιοδοτημένους χρήστες του συστήματος. Ακεραιότητα των δεδομένων είναι η ιδιότητά των στοιχείων να είναι ακριβή και να αντιπροσωπεύουν την πραγματικότητα, κάθε δε αλλαγή των να είναι αποτέλεσμα εξουσιοδοτημένης ενέργειας. Διαθεσιμότητα των πόρων ενός πληροφοριακού συστήματος είναι η ιδιότητά τους να καθίστανται άμεσα προσπελάσιμοι σε κάθε εξουσιοδοτημένο χρήστη του συστήματος .

5.4 ΣΧΕΣΗ ΑΣΦΑΛΕΙΑΣ ΚΑΙ ΜΥΣΤΙΚΟΤΗΤΑΣ.

Μυστικότητα είναι το δικαίωμα που έχει κάποιος να μην μοιράζεται τις πληροφορίες (π.χ. ηλικία, θρήσκευμα, αριθμούς πιστωτικής κάρτας κ.λ.π) που αφορούν το άτομό του με άλλους. Οι πληροφορίες αυτές είναι καταγεγραμμένες στο διαδίκτυο. Η ασφάλεια και η μυστικότητα στο χώρο του διαδικτύου είναι (ουσιαστικός) θεωρητικές έννοιες. Στην πράξη, ότι κινείται στον χώρο του διαδικτύου μπορεί να γίνει γνωστό, ουσιαστικός δηλαδή να υποκλαπεί. Έχει χαρακτηριστικά λεχθεί ότι, ``κανένα κινούμενο ηλεκτρόνιο του πλανήτη δεν μπορεί να τρέφει σοβαρές ελπίδες ότι θα ξεφύγει από τον ιστό της παρακολούθησης.
Κατά συνέπεια η ασφάλεια και η μυστικότητα του διαδικτύου δεν είναι μόνο νομικές, αλλά και τεχνικές έννοιες . Μπορεί όμως να λεχθεί ότι, η ασφάλεια είναι πρωτίστως τεχνική και δευτερευόντως νομική έννοια, ενώ αντίθετα η μυστικότητα είναι πρωτίστως νομική και δευτερευόντως τεχνική έννοια. Σε κάθε περίπτωση όμως, με την χρήση της τεχνολογίας και ιδιαίτερα του διαδικτύου, η προσωπική ζωή του ατόμου έχει γίνει "διαφανής". Συμπερασματικός, μυστικότητα και η ασφάλεια είναι εντελώς διαφορετικά πράγματα, δεν είναι όμως υπερβολικό να λεχθεί ότι, ασφάλεια και μυστικότητα στο διαδίκτυο αποτελούν τις δυο διαφορετικές όψεις, ενός και του ίδιου νομίσματος.
Κρυπτογραφία είναι η χρήση κωδίκων για την μετατροπή δεδομένων, κατά τέτοιο τρόπο, ώστε να μπορούν να διαβαστούν μόνο από συγκεκριμένο παραλήπτη με τη χρήση ενός κλειδιού . Σκοπός της κρυπτογραφίας είναι να αποτραπεί η πρόσβαση στα δεδομένα, σε μη εξουσιοδοτημένα άτομα ιδιαίτερα κατά την διάρκεια μετάδοσής των. Σχετικοί είναι οι όροι " διαχείριση κινδύνων και ανάλυση κινδύνων. Είναι χαρακτηριστικό ότι οι μεγάλες εταιρείες προσλαμβάνουν ειδικώς εκπαιδευμένο προσωπικό, που καταστρώνει ειδικά σχέδια προστασίας του δικτύου της εταιρείας.

Μέχρι προσφάτως ο όρος κρυπτογραφία περιοριζόταν μόνο στον στρατιωτικό και τον διπλωματικό χώρο. Σήμερα όμως που η επικοινωνία με το ηλεκτρονικό ταχυδρομείο (e-mail) έχει αυξηθεί αλματωδώς, η κρυπτογραφία αποτελεί σημαντικό παράγοντα του κυβερνοχώρου. Με την χρήση της κρυπτογραφίας δεν διακινούνται βέβαια μόνον νόμιμα, αλλά και παράνομα δεδομένα στον κυβερνοχώρο, όπως π.χ. ανταλλαγή υλικού, ανταλλαγή παρανόμων μηνυμάτων από οργανωμένους ή μη εγκληματίες κλπ.
Η διαδικασία της κωδικοποίησης των δεδομένων λέγεται κρυπτογράφηση. Η κρυπτογράφηση στηρίζεται σε κλειδί που πρέπει να κατέχει τόσο αυτός που στέλνει τα δεδομένα, όσο και αυτός που τα παραλαμβάνει. Αν ο παραλήπτης δεν κατέχει το κλειδί, υπάρχει κίνδυνος να γίνει υποκλοπή του κατά την μεταβίβαση (διαδρομή). Γενικώς η κρυπτογράφηση - αποκρυπτογράφηση γίνεται με την βοήθεια μιας μαθηματικής διαδικασίας. Η διαδικασία της αποκατάστασης των κρυπτογραφημένων δεδομένων στην αρχική τους μορφή λέγεται αποκρυπτογράφηση. Είναι ευνόητο ότι, με την χρήση της κρυπτογραφίας αποκρύπτετε, όχι μόνον το περιεχόμενο του παράνομου υλικού που διακινείται, αλλά αποφεύγεται επιπλέον και ο εντοπισμός του δράστη. Βέβαια ο εντοπισμός του δράστη μπορεί να αποφευχθεί και με την λεγομένη «ανωνυμία στον κυβερνοχώρο».
Από νομικής απόψεως ενδιαφέρον παρουσιάζει το ερώτημα, εάν είναι σύμφωνα με τις βασικές Αρχές του Δικαίου, η απαγόρευση χρήσεως της κρυπτογραφίας ή ο περιορισμός αυτής σε άτομα ή φορείς (π.χ. κρατικούς), που έχουν ειδική προς τούτο άδεια.

5.5 ΣΧΕΣΗ ΑΣΦΑΛΕΙΑΣ ΚΑΙ ΔΙΚΑΙΩΜΑΤΟΣ ΔΡΑΣΗΣ

Είναι γνωστό ότι κάθε χρήστης του διαδικτύου (Internet) αφήνει στον χώρο την (ηλεκτρονική) ταυτότητά του. Με κατάλληλες όμως τεχνικές παρεμβάσεις μπορεί να έχει κάποιος πρόσβαση στο διαδίκτυο ως ανώνυμος ή ακόμα και με ψευδή στοιχεία που αναφέρονται σε άλλο άτομο. Η παρουσίαση βέβαια με ψευδή στοιχεία μπορεί να γίνει και στο "κοινό" εγκληματικό περιβάλλον. Εκεί όμως ο εντοπισμός του δράστη είναι ευκολότερος. Μπορεί ακόμα ο χρήστης του διαδικτύου να έχει ως στοιχείο ταυτότητος το όνομα "ανώνυμος", οπότε τυπικά φαίνεται ότι έχει όνομα. Η δυνατότητα αυτής της ανωνυμίας στο διαδίκτυο (Internet) διευκολύνει την διάπραξη παρανομιών και κάνει δύσκολο, αν όχι και αδύνατο τον εντοπισμό του δράστη. Επιπλέον η ανωνυμία, σε συνδυασμό με την ανυπαρξία ή την δυσκολία εφαρμογής των νομικών κανόνων, κάνει τους ``ηλεκτρονικούς δράστες`` να αισθάνονται ασφαλείς κατά την διάπραξη των εγκλημάτων των.
Το ερώτημα που προκύπτει στο σημείο αυτό είναι, μήπως σε περίπτωση ψήφισης σχετικού νόμου για το διαδίκτυο, πρέπει να ποινικοποιηθεί η ανώνυμη χρήση του, ή ακόμα και η παρουσία με ψευδή στοιχεία. Κάτι τέτοιο βέβαια επαφίεται στην βούληση του νομοθέτη. Αξίζει όμως να σημειωθεί, σχετικός νόμος που ψηφίστηκε στις Η.Π.Α και τιμωρούσε ποινικά την ανώνυμη χρήση ή την χρήση με ψεύτικο όνομα στο διαδίκτυο , κηρύχθηκε αντισυνταγματικός από τα Δικαστήρια των ΗΠΑ . Και αυτό γιατί, η ανωνυμία δεν χρησιμοποιείται στο διαδίκτυο μόνον από τους παράνομους, αλλά και από όσους θέλουν να αποκρύψουν αυστηρός προσωπικά των (νόμιμα) στοιχεία .

ΚΕΦΑΛΑΙΟ 6: ΕΠΙΒΛΕΨΗ ΚΑΙ ΔΙΑΡΚΗΣ ΔΙΑΧΕΙΡΙΣΗ ΤΟΥ ΕΠΙΧΕΙΡΗΣΙΑΚΟΥ ΔΙΚΤΥΟΥ

Η Επίβλεψη και διαρκής διαχείριση του επιχειρησιακού δικτύου βασίζεται στην οργάνωση μιας επιχείρησής αλλά και στους Σχεδιασμούς που θα μπορούσε πιθανώς να αντιμετωπίσει. Συγκεκριμένα η ανάλυση Επιχειρηματικού Μοντέλου αναφέρεται στα ακόλουθα:

- Στο να διαθέτει η επιχείρησή συγκεκριμένα λογιστική οργάνωση βασισμένη σε ηλεκτρονικές διαδικασίες. Στη στρατηγική που ακολουθεί η επιχείρηση σε σχέση με την τεχνολογική ολοκλήρωση των ενδοεπιχειρησιακών διαδικασιών, οι οποίες Ελέγχονται από την εταιρεία ή τις αναθέτει σε εξωτερικούς συνεργάτες.
- Στη παροχή υπηρεσιών προς τρίτους με ηλεκτρονικά μέσα;

Σε σχέση με τη διαχείριση επιχειρησιακού δικτύου υπάρχει για τις επιχειρήσεις η ανάγκη για την ανάλυση Πνευματικού Κεφαλαίου, σε σχέση με την αξία του πνευματικού κεφαλαίου της επιχείρησης, όπως βάσεις δεδομένων, πνευματικά δικαιώματα, διπλώματα ευρεσιτεχνίας, εμπορικά σήματα, κ.λπ. Επιπροσθέτως η διαχείριση επιχειρησιακού δικτύου αναφέρετε σε συνεργασίες σε σχέση με τις βασικές επιχειρηματικές δραστηριότητες οι οποίες αναφέρονται σε προμηθευτές, πελάτες, συνεργάτες), οι οποίοι θα μπορούσαν να επηρεαστούν από μια σωστή ή λαθεμένη διαχείριση ενός επιχειρησιακού δικτύου.

Η τεχνολογική ανάλυση ενός επιχειρησιακού δικτύου αναφέρεται

- Στην τεχνολογική υποδομή της στρατηγικής μιας επιχείρησης εστιάζοντας και στο e-επιχειρήν.
- Σε λειτουργικούς περιορισμούς.
- Στην προστασία των προσωπικών δεδομένων των πελατών, υπαλλήλων, επιχειρηματικών συνεργατών, καθώς και τις οικονομικές και νομικές πληροφορίες της επιχείρησής σας.
- Στην ακολουθία της στρατηγικής και στην εναρμόνιση της με τη σχετική νομοθεσία, όπως οι κανονισμοί EU Data Directive, Digital Millennium Copyright Act, κ.λπ.;
- Στην ασφάλεια των ηλεκτρονικών συναλλαγών.

Οι συμβατικές υποχρεώσεις ενός επιχειρησιακού δικτύου αναφέρονται

- Σε δηλώσεις προστασίας προσωπικών δεδομένων, παραίτησης από ευθύνη, κ.λπ.;
- Στην αναγνώριση των κυρώσεων σε περίπτωση που αποδειχθεί ότι παραβήκατε κάποια από τις παραπάνω δηλώσεις;

6.1 Η ΔΙΑΦΟΡΑ ΜΕΤΑΞΥ ΤΩΝ ΕΝΝΟΙΩΝ ΤΗΣ ΑΣΦΑΛΕΙΑΣ ΠΛΗΡΟΦΟΡΙΩΝ ΚΑΙ ΤΗΣ ΔΙΑΧΕΙΡΙΣΗΣ ΕΠΙΧΕΙΡΗΣΙΑΚΟΥ ΣΧΕΔΙΑΣΜΟΥ

Η έννοια της Διαχείρισης Επιχειρηματικού Σχεδιασμού στο πλαίσιο του η-επιχειρείν είναι ευρύτερη και συμπεριλαμβάνει την έννοια της Ασφάλειας Πληροφοριών. Ενώ η τελευταία εστιάζει στην προστασία και την ακεραιότητα των πληροφοριακών κεφαλαίων, η Διαχείριση Επιχειρηματικού Σχεδιασμού αφορά σε γενικότερα ζητήματα, τα οποία επηρεάζουν άμεσα τη βιωσιμότητα του η-επιχειρείν. Η Ασφάλεια Πληροφοριών είναι λοιπόν μια υποκατηγορία της Διαχείρισης Κρίσεων, για την ακρίβεια μία από τις σημαντικότερες.

Η κύρια διαφοροποίηση εντοπίζεται στον καθορισμό της έννοιας "κεφάλαιο" αντίστοιχα στις δύο περιπτώσεις. Η Ασφάλεια Πληροφοριών αποκρούει τις απειλές εναντίον του πληροφοριακού και υπολογιστικού κεφαλαίου, ενώ η Διαχείριση Επιχειρηματικού Σχεδιασμού αφορά στην πρόληψη οικονομικών και γενικότερα εσωτερικών κρίσεων, οι οποίες μάλιστα αντικατοπτρίζονται στους συνεργάτες και το προσωπικό της επιχείρησης, γι' αυτό και επηρεάζουν παράγοντες όπως η οικονομική ασφάλεια, η νομική και εμπορική αξιοπιστία (η καλή φήμη της επιχείρησης, τόσο προς τους καταναλωτές όσο και προς άλλες επιχειρήσεις), κ.λπ.

6.2 Ο ΡΟΛΟΣ ΤΩΝ ΕΤΑΙΡΙΩΝ

Οι "παραδοσιακές" εταιρίες δεν επεκτείνουν τις δράσεις τους σε "καταστροφές" που απειλούν τον επιχειρησιακό σχεδιασμό, κατά συνέπεια αρκετοί τομείς επιχειρηματικής ευθύνης μένουν εκτός ασφαλιστικής κάλυψης, ενώ και οι ίδιες οι μικρομεσαίες επιχειρήσεις δεν διαθέτουν την ετοιμότητα να δράσουν κατάλληλα στην πιθανότητα απρόβλεπτων κρίσεων στον επιχειρησιακό σχεδιασμό. Μολονότι οι ειδικοί εκτιμούν ότι οι πρακτικές αξιολόγησης και κάλυψης επιχειρηματικού Σχεδιασμού θα παραμείνουν σχετικά "αδύναμες" στο προσεχές διάστημα, η εξέλιξη και ωρίμανση των τεχνολογιών αλλά και οι οικονομικές πιέσεις όσο και η παγκοσμιοποίηση του επιχειρησιακού σχεδιασμού πιθανότατα θα εξαναγκάσουν τους κυβερνητικούς φορείς να αναπτύξουν μια πιο στιβαρή πολιτική. Επιχειρήσεις οι οποίες κάνουν σημαντικά βήματα στον επιχειρησιακό σχεδιασμό, προκειμένου να παραμείνουν ανταγωνιστικές, θα έχουν στη διάθεσή τους όλο και περισσότερους τρόπους εκτίμησης και διαχείρισης κρίσεων, οι οποίοι ωστόσο θα απαιτούν σημαντική οικονομική επένδυση. Οι ασφαλιστικοί οργανισμοί θα υποχρεωθούν να αυξήσουν τόσο τη συχνότητα όσο και την αναλυτικότατα των δοκιμών "ανάνηψης" επιχειρήσεων έπειτα από κρίση, των ελέγχων ευπάθειας δικτύων και συστημάτων, της αξιολόγησης των επιχειρηματικών διαδικασιών και εφαρμογών, και του σχεδιασμού απόκρουσης ηλεκτρονικών απειλών. Θα αναγκαστούν ακόμη να εκτιμήσουν τις συνέπειες του η-επιχειρηματικού Σχεδιασμού σε όλα τα επίπεδα, και θα προσαρμόσουν ανάλογα τα ασφαλιστικά τους προγράμματα.

6.3 ΔΙΑΧΕΙΡΙΣΗ ΚΡΙΣΕΩΝ ΣΤΟΝ ΕΠΙΧΕΙΡΗΣΙΑΚΟ ΣΧΕΔΙΑΣΜΟ

Η διαχείριση κρίσεων σε σχέση με τον επιχειρησιακό σχεδιασμό αναφέρεται στην υποδομή:

1. Ανάπτυξη, συντήρηση και προστασία βάσεων δεδομένων.
2. Επεκτασιμότητα δικτύων και διακομιστών.
3. Προστασία υποδομής από φυσικές καταστροφές.
4. Δοκιμές καλής λειτουργίας μεμονωμένων στοιχείων.
5. 24ωρη παρακολούθηση δικτύων και συστημάτων.
6. Δοκιμές υπερφόρτωσης δικτύων.
7. Ανάπτυξη συστήματος έγκαιρης ειδοποίησης σε περιπτώσεις εκτάκτων αναγκών.
8. Επαναφορά/ανάνηψη έπειτα από καταστροφή και καθορισμός διαδικασιών και ευθυνών για την αδιάκοπη λειτουργία της επιχείρησης.
9. Έλεγχος πληροφορικών συστημάτων και ασφάλεια διαδικασιών αναβάθμισης εφαρμογών ή εξοπλισμού.
10. Έλεγχος εναρμόνισης με τις τεχνολογικές εξελίξεις, για την αποφυγή "απαρχαίωσης" των συστημάτων.
11. Έλεγχος ποιότητας των υπηρεσιών που παρέχονται από τρίτα μέρη και αφορούν σε κρίσιμες λειτουργίες της επιχείρησης.

Σε σχέση με την ασφάλεια στον επιχειρησιακό σχεδιασμό έχουμε τα ακόλουθα δεδομένα. Συγκεκριμένα συμμόρφωση με τα διεθνή πρότυπα ασφαλείας, εκτίμηση ετοιμότητας σε έξωθεν εισβολές (χάκερ, ιούς, κ.λπ.), εγκατάσταση, διαχείριση και επανεκτίμηση των υποδομών πιστοποίησης και εξουσιοδότησης για την πρόσβαση στα δίκτυα της επιχείρησης, εκτίμηση και διαχείριση της φυσικής ασφάλειας, διαχείριση δικαιωμάτων πρόσβασης του προσωπικού, βάσει ρόλων στην επιχείρηση. Ακόμα έχουμε τα ακόλουθα:

1. Συντήρηση του υπάρχοντος λειτουργικού συστήματος και συνεχής αναβάθμισή του
2. Εντοπισμός κρουσμάτων απάτης

3. Έλεγχος ασφαλείας των προμηθευτών ή άλλων τρίτων μερών που διαχειρίζονται τα στοιχεία των πελατών ή έχουν πρόσβαση σε αυτά.
4. Ασφάλεια επικοινωνιών και πρόσβασης δικτύων από απόσταση.
5. Συνεχής αξιολόγηση της επίδρασης νέων πρωτοβουλιών η-επιχειρείν στην ετοιμότητα της εταιρίας ως προς τη διαχείριση κρίσεων.
6. Στόχος των μέτρων ασφαλείας πρέπει να είναι τόσο η πρόληψη (π.χ. η εκτίμηση, η διόρθωση και η ενίσχυση των λειτουργικών συστημάτων και του γενικότερου πλαισίου υποδομής της επιχείρησης) όσο και η αποτελεσματική αντίδραση.

6.4 ΠΡΟΣΩΠΙΚΑ ΔΕΔΟΜΕΝΑ

Σε σχέση με τα προσωπικά δεδομένα στον επιχειρησιακό σχεδιασμό έχουμε τη παρεμπόδιση μη εξουσιοδοτημένης πρόσβασης στα προσωπικά και συναλλακτικά στοιχεία των πελατών, τα οποία τηρούνται σε ειδικές εταιρικές εφαρμογές και βάσεις δεδομένων, τη διαχείριση των επιλογών "opt in" ή "opt out" των πελατών, που αφορούν στην κοινοποίηση ή μη των προσωπικών τους στοιχείων σε συνεργαζόμενες εταιρίες για λόγους προώθησης/marketing, τη διαχείριση στοιχείων πελατών τρίτων επιχειρήσεων, που συγκεντρώθηκαν κατόπιν συμφωνίας των ίδιων, τη προστασία όλων των εσωτερικών και εξωτερικών επικοινωνιών που διεξάγονται μέσω Διαδικτύου, την εκούσια ή ακούσια κοινοποίηση εμπιστευτικών πληροφοριών εμπορικών συνεργατών, τη συμμόρφωση προς τη διεθνή νομοθεσία σχετικά με τις online συναλλαγές από χώρες του εξωτερικού

6.5 ΕΠΙΧΕΙΡΗΜΑΤΙΚΕΣ ΔΙΑΔΙΚΑΣΙΕΣ

Η επιχειρησιακή διαδικασία αναφέρεται στα ακόλουθα:

1. Στη διατήρηση της ακεραιότητας των online συναλλαγών και πληρωμών.
2. Στην ικανότητα ολοκλήρωσης των συναλλαγών σε περιπτώσεις πτώσης του δικτύου ή άλλης βλάβης
3. Στη χρήση και διασύνδεση τρίτων μερών για την ασφαλή διαχείριση και ολοκλήρωση επιχειρηματικών διαδικασιών.
4. Στη παρακολούθηση και διαχείριση του ηλεκτρονικού ταχυδρομείου και των επισυναπτόμενων αρχείων.
5. Στον εντοπισμό και διαχείριση καίριων ηλεκτρονικών αρχείων.

Προστασία κατά των σφαλμάτων, διακοπών ή καθυστερήσεων στην παροχή υπηρεσιών με βάση το Internet, όπως π.χ.:

1. Διαθεσιμότητα λογισμικού ή άλλων αρχείων τα οποία οι χρήστες κατεβάζουν στον υπολογιστή τους από το δικτυακό τόπο της επιχείρησης
2. Διαθεσιμότητα του ίδιου του δικτυακού τόπου, τόσο των περιοχών που απευθύνονται στους καταναλωτές όσο και εκείνων στις οποίες έχουν πρόσβαση οι συνεργάτες της επιχείρησης
3. Διαθεσιμότητα του Διαδικτύου για την αποστολή και λήψη e-mail
4. Παροχή τεχνικής υποστήριξης τόσο για την ίδια την επιχείρηση όσο και για τους συνεργάτες της
5. Διαχείριση εσωτερικών και εξωτερικών.
6. Ευθυγράμμιση των δραστηριοτήτων επιχειρησιακού σχεδιασμού.
7. Διαδικασίες προτυποποίησης και ελέγχου της εμπορικής δραστηριότητας μέσω

Διαδικτύου

8. Ετοιμότητα επικοινωνίας με τα Μέσα Ενημέρωσης
9. Αναγνώριση του συμβάντος/της κρίσης και άμεση απόκριση
10. Αποκατάσταση και ανασυγκρότηση
11. Αυστηρά δομημένο σχέδιο αντίδρασης
12. Παρακολούθηση της επαγγελματικής συμπεριφοράς του προσωπικού.
13. Εκπαίδευση μέρους του προσωπικού για την υποστήριξη αναγκών που σχετίζονται με τις νέες τεχνολογίες και τον επιχειρησιακό σχεδιασμό.
14. Έλεγχος των σχέσεων συνεργασίας με τρίτα μέρη.
15. Αποτελεσματική διαχείριση έργων.
16. Συνεχής ενημέρωση και εκπαίδευση.
17. Δημιουργία και διαχείριση πολυμεσικού περιεχομένου.
18. Διαχείριση ηλεκτρονικών αρχείων περιεχομένου.

Η Προστασία εταιρικής πνευματικής ιδιοκτησίας (με χρήση τεχνολογιών όπως η ψηφιακή υδατογράφηση, η κρυπτογράφηση κ.λπ. αλλά και με την προστασία των εταιρικών δικτύων). Οι διαδικασίες για την αποτροπή της παράνομης χρήσης της πνευματικής ιδιοκτησίας τρίτων. Οι διαδικασίες εντοπισμού και διαχείρισης σφαλμάτων στο περιεχόμενο του δικτυακού τόπου της επιχείρησης και λανθασμένων συνδέσμων/"σπασμένων" links. Η Διαχείριση Πληροφοριών σε σχέση με τον επιχειρησιακό σχεδιασμό αναφέρεται στα ακόλουθα:

1. Συγκέντρωση και αναφορά λειτουργικών στατιστικών στοιχείων σχετικά με την παρακολούθηση της απόδοσης και τις τάσεις της αγοράς.
2. Παρακολούθηση συναλλαγών για τον εντοπισμό κρουσμάτων απάτης (π.χ. μη εξουσιοδοτημένη χρήση πιστωτικής κάρτας)

6.6 ΕΦΑΡΜΟΓΗ ΚΟΙΝΗΣ ΠΟΛΙΤΙΚΗΣ ΣΤΗΝ ΑΠΟΣΤΟΛΗ ΜΗΝΥΜΑΤΩΝ ΗΛΕΚΤΡΟΝΙΚΟΥ ΤΑΧΥΔΡΟΜΕΙΟΥ

Αρχικά το e-mail επινοήθηκε ως μέσο με σκοπό την άμεση και ανεπίσημη ηλεκτρονική επικοινωνία. Ενώ κάποτε οι επιχειρήσεις χρησιμοποιούσαν κυρίως το τηλέφωνο για την ανταλλαγή εμπορικών πληροφοριών, σήμερα έχουν στραφεί στο ηλεκτρονικό ταχυδρομείο. Δυστυχώς, η αντικατάσταση των "ανεπίσημων" τηλεφωνικών κλήσεων με το e-mail δημιούργησε μια καθημερινότητα κατά την οποία οι συζητήσεις μας "καταγράφονται" και οι επιχειρηματικές αποφάσεις είναι ως επί το πλείστον καταχωρημένες σε ηλεκτρονική μορφή. Έτσι, "τα γραπτά μένουν" και μπορούν μεν να σώσουν, μπορούν όμως και να λειτουργήσουν εις βάρος μιας επιχείρησης σε περιπτώσεις δικαστικής δίωξης κατά της εταιρίας σας, ακόμα κι αν αποτελούν προσωπική επικοινωνία των υπαλλήλων σας, εφόσον αποκαλύπτουν εταιρικές πληροφορίες. Χάρη στο ηλεκτρονικό ταχυδρομείο, υπάρχει σήμερα διαθέσιμη μια πληθώρα σελίδων επιχειρηματικής επικοινωνίας. Οφείλει λοιπόν μια επιχείρηση να καταρτίσει κανόνες για το τι οι υπάλληλοί μπορούν ή δεν μπορούν να γράφουν όταν εκπροσωπούν την επιχείρηση στην ηλεκτρονική της επικοινωνία με πελάτες ή συνεργάτες.

Μια εταιρεία σε σχέση με τον επιχειρησιακό σχεδιασμό ορίζει ένα ενιαίο σύστημα ονομασίας, αρχειοθέτησης και διαγραφής ηλεκτρονικών αρχείων, βάσει της σπουδαιότητας και του βαθμού εμπιστευτικότητας που φέρουν. Αναλόγως δώστε δικαιώματα πρόσβασης στους υπαλλήλους σας βάσει του ρόλου και της παλαιότητάς τους στην εταιρία.

Η αποτελεσματική διαχείριση κρίσεων συνδυάζει τεχνολογικές εφαρμογές με άρτια εκπαιδευμένο προσωπικό. Συχνά η χρήση της κοινής λογικής είναι αρκετή για την αποτροπή δυσάρεστων εκπλήξεων για την επιχείρηση, κυρίως σε ότι αφορά τους κωδικούς

πρόσβασης:

- Εφαρμογή μιας πολιτικής συχνής αλλαγής των κωδικών πρόσβασης. Τήρηση αρχείου με τους κωδικούς πρόσβασης όλων των υπαλλήλων.
- Αποσαφήνιση στους υπαλλήλους.
- Η επιχείρηση θα πρέπει να αποφύγει τη χρήση κωδικών που αποκαλύπτουν την ταυτότητα του χρήση, όπως ονοματεπώνυμα, ημερομηνίες γέννησης, κ.λπ.
- Η επιχείρηση θα πρέπει να εμποδίσει την πρόσβαση μη εξουσιοδοτημένων χρηστών, επισκεπτών κ.λπ. στους υπολογιστές της εταιρίας. Η επιχείρηση θα πρέπει να εντοπίσει "ασυνήθιστες συμπεριφορές" υπαλλήλων.

Προκειμένου μια επιχείρηση να αναπτύξει ένα εσωτερικό εργαλείο αποτίμησης και αποτελεσματικής διαχείρισης επιχειρησιακού σχεδιασμού και κρίσεων, θα πρέπει να κατέχει πλήρως τα ζητήματα που σχετίζονται με την τεχνολογία, τις διαδικασίες και τη διοίκηση. Η εκπαίδευση του προσωπικού, η χρήση ικανών εξωτερικών συνεργατών και συμβούλων ή η ανάθεση σε εξειδικευμένο ασφαλιστικό φορέα είναι παράγοντες που σίγουρα οδηγούν στην καλύτερη προστασία της επιχείρησης από εσωτερικούς και εξωτερικούς Σχεδιασμούς. Τέλος, σημαντική είναι και η ανάγκη συγκρότησης κυβερνητικών φορέων αλλά και κατάρτισης ειδικών πολιτικών διαχείρισης κρίσεων για τη στήριξη και τη βιωσιμότητα των ΜΜΕ στον ηλεκτρονικό επιχειρηματικό στίβο.

ΚΕΦΑΛΑΙΟ 7 : ΠΡΟΒΛΗΜΑΤΑ ΤΩΝ ΕΠΙΧΕΙΡΗΣΙΑΚΩΝ ΔΙΚΤΥΩΝ

7.1.ΗΛΕΚΤΡΟΝΙΚΟ ΄ΕΓΚΛΗΜΑ

Η ραγδαία εξέλιξη της τεχνολογίας, η ανάπτυξη της πληροφορικής καθώς και το Διαδίκτυο έχουν επιφέρει πρωτόγνωρες αλλαγές στην παραγωγική διαδικασία, στις εργασιακές σχέσεις, στις συναλλαγές και σε κάθε έκφανση της καθημερινότητας και της ανθρώπινης επαφής. Μαζί όμως με τις αλλαγές αυτές που διευκολύνουν, προάγουν και βοηθούν στην καλυτέρευση της ποιότητας ζωής και στην τάχιστη εξυπηρέτηση των αναγκών που δημιουργεί η σύγχρονη κοινωνίας, οι νέες τεχνολογίες και το Ίντερνετ διευκόλυναν και δημιούργησαν ιδανικές συνθήκες για την καλλιέργεια και ανάπτυξη νέων μορφών εγκληματικότητας που συνοψίζονται στον όρο Ηλεκτρονικό έγκλημα

Ο όρος Ηλεκτρονικό έγκλημα ή Ηλεκτρονική εγκληματικότητα αποτελεί μια ευρεία έννοια στην οποία εμπίπτουν όλες εκείνες οι αξιόποινες πράξεις που τελούνται με τη χρήση ενός συστήματος ηλεκτρονικής επεξεργασίας δεδομένων. Ο όρος αυτός διακρίνεται σε στενή και σε ευρεία έννοια. Η εν στενή έννοια ηλεκτρονική εγκληματικότητα αναφέρεται στις αξιόποινες πράξεις όπως είναι η ηλεκτρονική απάτη , η χωρίς άδεια απόκτηση δεδομένων, η παραποίηση δεδομένων και η δολιοφθορά δηλαδή εγκλήματα όπου ο ηλεκτρονικός υπολογιστής αποτελεί κύριο μέσο τέλεσης των εγκλημάτων. Αντίθετα η εν ευρεία έννοια εγκληματικότητα μέσω Η/Υ περιλαμβάνει όλα εκείνα τα αδικήματα για την τέλεση των οποίων ο ηλεκτρονικός υπολογιστής χρησιμοποιείται ως βοηθητικό μέσο.

Οι μορφές του Ηλεκτρονικού εγκλήματος είναι ποικίλες και με τη συνεχή ανάπτυξη της τεχνολογίας και του διαδικτύου πολλαπλασιάζονται. Για την αντιμετώπιση του κινδύνου αυτού ήταν απαραίτητη η συνεννόηση μεταξύ των κρατών και η εκπόνηση μιας αναλυτικής και αποτελεσματική στρατηγικής. Ο σκοπός αυτός επετέθη με το Συνέδριο για το Ηλεκτρονικό έγκλημα (Convention on Cybercrime), του οποίου όλα τα συμπεράσματα αποκρυσταλλώνονται στην συνθήκη που υπογράφει στην Βουδαπέστη στις 23.11.2001[21].

7.2.ΚΥΒΕΡΝΟΣΦΕΤΕΡΙΣΜΟΣ

Κυβερνοσφετερισμός (cybersquatting) είναι το ηλεκτρονικό αδίκημα κατά το οποίο κάποιος χρήστης του Διαδικτύου για εμπορικούς σκοπούς κατοχυρώνει και χρησιμοποιεί ηλεκτρονική διεύθυνση (domain name) που περιέχει είτε την επωνυμία γνωστών επιχειρήσεων είτε σήματα φήμης με αποτέλεσμα να προκαλείται βλάβη στη φήμη των νόμιμων δικαιούχων αλλά και αποκλεισμός τους από τη χρήση του Διαδικτύου με την επωνυμία τους[22].

7.3.ΠΑΡΑΝΟΜΗ ΔΙΕΙΣΔΥΣΗ ΣΕ ΔΕΔΟΜΕΝΑ

Hacking αποτελεί η μη εξουσιοδοτημένη πρόσβαση σε ξένο υπολογιστή ή συστήματα υπολογιστών η οποία καταρχήν δε γίνεται με το σκοπό της υποκλοπής, της καταστροφής ή της κατασκοπείας αλλά για την ικανοποίηση από την επιτυχία παράκαμψης των συστημάτων ασφαλείας των ηλεκτρονικών υπολογιστών.

Cracking είναι η αλλαγή των κωδίκων πρόσβασης και η άρση της προστασίας των προγραμμάτων, η οποία καθιστά δυνατή την παράνομη αντιγραφή τους.

---

[21] http://www.lawnet.gr/case_study.asp

[22] E-business Forum - Γενική Γραμματεία Βιομηχανίας

"Ο Τελικός Δεκάλογος για θέματα Ασφάλειας Πληροφοριακών Συστημάτων και Προστασίας Προσωπικών Δεδομένων στο Ηλεκτρονικό Επιχειρείν

7.4.ΑΠΑΤΗ ΜΕΣΩ ΤΟΥ ΔΙΑΔΙΚΤΥΟΥ

Από τη σκοπιά του ποινικού δικαίου κατά τη χρήση του Διαδικτύου είναι δυνατό να τελεστούν απάτες μέσω υπολογιστή όπου ο υπολογιστής είναι απλώς το μέσω τέλεσης της κοινής απάτης (ΠΚ 386) αλλά και απάτες με υπολογιστή όπου το οικονομικό όφελος ή η ζημιά προκύπτει με απευθείας παρέμβαση στον υπολογιστή στο πρόγραμμα και στα δεδομένα του (ΠΚ 386Α).

7.5.SPAMMING

Το μεγαλύτερο πρόβλημα που αφορά στις διαδικτυακές διαφημίσεις είναι το λεγόμενο spamming, δηλαδή η αποστολή πολυάριθμων e-mails με διαφημιστικό περιεχόμενο σε χιλιάδες καταναλωτές-χρήστες του διαδικτύου . Η τακτική αυτή απαγορεύεται από την Οδηγία 2002.58 όπου στο άρθρο 13 αναφέρεται ότι « η χρησιμοποίηση αυτόματων συστημάτων κλήσης χωρίς ανθρώπινη παρέμβαση (συσκευές αυτόματων κλήσεων), τυλεομοιοτυπικών συσκευών (φαξ) ή ηλεκτρονικού ταχυδρομείου για σκοπούς απευθείας εμπορικής προώθησης επιτρέπεται μόνον στην περίπτωση συνδρομητών οι οποίοι έχουν δώσει εκ των προτέρων τη συγκατάθεσή τους» καθώς και από άλλα νομοθετήματα.

7.6.ΠΝΕΥΜΑΤΙΚΗΣ ΙΔΙΟΚΤΗΣΙΑΣ

Η μετάβαση από τη βιομηχανική κοινωνία στη λεγόμενη κοινωνία των πληροφοριών, της ψηφιακής τεχνολογίας και επικοινωνίας προκαλεί βαθιές επικοινωνιακές , πολιτισμικές και οικονομικές αλλαγές. Η αξία και η οικονομική σημασία των άυλων αγαθών και των πληροφοριών έχει πολλαπλασιασθεί σε μια κοινωνία της οποίας η οικονομία και η επικοινωνία έχει διεθνοποιηθεί. Η πνευματική ιδιοκτησία παρέχει την κινητήρια δύναμη στην κοινωνία της διασκέδασης και της παγκόσμιας επικοινωνίας.

Πνευματική ιδιοκτησία ονομάζεται το δικαίωμα που η έννομη τάξη απονέμει στον δημιουργό ενός πνευματικού έργου πάνω στον έργο αυτό. Πνευματικός δημιουργός είναι εκείνος που δημιουργεί νέες μορφές και ιδέες έστω και αν ενσωματώνει τα δημιουργήματά του σε ύλη που προϋπήρχε.

Η πνευματική ιδιοκτησία παρουσιάζει τρεις ιδιομορφίες. Η πρώτη είναι ότι το αντικείμενό της είναι άυλο δηλαδή είναι το πνευματικό δημιούργημα και όχι το υλικό αντικείμενο πάνω στο οποίο το δημιούργημα έχει ενσωματωθεί. Ο άυλος χαρακτήρας του αντικειμένου της πνευματικής ιδιοκτησίας επιτρέπει τη σύγχρονη παρουσία του έργου σε άπειρους τόπους.

Η δεύτερη ιδιομορφία είναι ότι η πνευματική ιδιοκτησία δεν προστατεύει μόνο περιουσιακά το δημιουργού σε σχέση με το έργο του αλλά και συμφέροντα που ανάγονται στη σφαίρα της προσωπικότητας του δημιουργού, δηλαδή στην ιδιαίτερη ηθική σχέση του κάθε δημιουργού με το δημιούργημά του. Έτσι η πνευματική ιδιοκτησία έχει ένα μικτό χαρακτήρα προσωπικό και περιουσιακό που προκαλεί περίεργες διχοτομήσεις του δικαιώματος, ιδίως σε ότι αφορά τη δυνατότητα μεταβίβασής του.

Η τρίτη ιδιομορφία της πνευματικής ιδιοκτησίας προκαλείται από το γεγονός ότι κάθε πνευματικό δημιούργημα είναι μοναδικό και ανεπανάληπτο. Ο πνευματικός δημιουργός έχει μια θέση μονοπωλιακή αναφορικά με το κάθε δημιούργημά του[23].

[23] Ed Tittel, Mike Chapple and James Michael Stewart Study Guide Certified Information Systems Security Professional"

ΚΕΦΑΛΑΙΟ 8: ΝΟΜΟΘΕΣΙΑ

8.1.ΝΟΜΟΘΕΣΙΑ ΗΛΕΚΤΡΟΝΙΚΟΥ ΕΓΚΛΗΜΑΤΟΣ

Στη συνθήκη της Βουδαπέστη, που υπέγραψε μεταξύ πολλών άλλων χωρών και η Ελλάδα υπάρχουν επεξηγήσεις και ρυθμίσεις για όλα τα ηλεκτρονικά εγκλήματα:
1. Για τα αδικήματα κατά της εμπιστευτικότητας, της ακεραιότητας και της διαθεσιμότητας των δεδομένων και των συστημάτων ηλεκτρονικών υπολογιστών. Τέτοια αδικήματα είναι η παράνομη πρόσβαση, η παράνομη υποκλοπή, η επέμβαση σε δεδομένα, η επέμβαση σε συστήματα και η κακή χρήση συσκευών.
2. Για τα αδικήματα που σχετίζονται με τους υπολογιστές όπως η απάτη με ηλεκτρονικό υπολογιστή και η πλαστογραφία.
3. Για τα αδικήματα σχετικά με το περιεχόμενο όπως είναι το αδίκημα της παιδικής πορνογραφίας.
4. Για τα αδικήματα που σχετίζονται με καταπάτηση πνευματικής ιδιοκτησίας.
Επίσης η συνθήκη περιέχει ρυθμίσεις για την συνεργεία, την απόπειρα και την υποκίνηση ηλεκτρονικών εγκλημάτων καθώς και την ευθύνη των επιχειρήσεων. Ακόμα τονίζει την αναγκαιότητα της διεθνούς συνεργασίας μεταξύ των κρατών για την καταπολέμηση του ηλεκτρονικού εγκλήματος και θίγει το πολύ σημαντικό θέμα της αρμοδιότητας και της δικαιοδοσίας των δικαστηρίων σχετικά με τα εγκλήματα αυτά. Η συνθήκη αυτή αποτελεί το πιο άρτιο κείμενο σχετικά με το ηλεκτρονικό κείμενο στην Ευρωπαϊκή ένωση. Υπάρχουν φυσικά και άλλα γενικά νομοθετήματα που βοηθούν στην καταπολέμηση του Ηλεκτρονικού εγκλήματος.
Στην Ευρωπαϊκή Ένωση ισχύουν:
1. Η Σύσταση του Συμβουλίου με αριθμό 9193/01, με την οποία καλούνται τα κράτη μέλη να συμμετάσχουν στο δίκτυο πληροφόρησης της Ομάδας των Οκτώ, το οποίο λειτουργεί 24 ώρες το εικοσιτετράωρο, για την καταπολέμηση του εγκλήματος υψηλής τεχνολογίας.
2. Το Ψήφισμα του Συμβουλίου με αριθμό 2003/ C 48/01, για την ασφάλεια των δικτύων και των πληροφοριών.
3. Η Σύσταση του Συμβουλίου με αριθμό 95/144/ΕΚ, όπου αναφέρονται οι προτροπές του Συμβουλίου σχετικά με την ασφάλεια των συστημάτων πληροφορικής.
4. Η Κοινή θέση της 27ης Μαΐου 1999 (1999/364/ΔΕΥ), όπου τα κράτη μέλη υποστηρίζουν την κατάρτιση του σχεδίου σύμβασης του Συμβουλίου της Ευρώπης σχετικά με την καταπολέμηση του εγκλήματος στον κυβερνοχώρο και ότι φροντίζουν ώστε να περιληφθούν στη σύμβαση διατάξεις που θα διευκολύνουν την αποτελεσματική διερεύνηση και δίωξη εγκλημάτων που άπτονται των ηλεκτρονικών συστημάτων και δεδομένων.
5. Το Ψήφισμα του Συμβουλίου με αριθμό 2002/C 43/02 για κοινή προσέγγιση και ειδικές δράσεις στον τομέα της ασφάλειας των πληροφοριών και των δικτύων.
6. Το έγγραφο με αριθμό 2000/C 124/01 σχετικά με τη στρατηγική της Ευρωπαϊκής Ένωσης για την πρόληψη και τον έλεγχο του οργανωμένου εγκλήματος. Στο έγγραφο αυτό αναλύονται διεξοδικά τα μέτρα που πρέπει να ληφθούν για την πρόληψη και την καταπολέμηση του οργανωμένου εγκλήματος όπου εντάσσονται και πολλές μορφές του ηλεκτρονικού εγκλήματος.
7. Το Σχέδιο Δράσης με αριθμό 97/C 251/01 για την καταπολέμηση του οργανωμένου εγκλήματος.
Στην Ελλάδα ισχύει ο νόμος 2928 του 2001 για την προστασία του πολίτη από αξιόποινες πράξεις εγκληματικών οργανώσεων.

8.2.ΝΟΜΟΘΕΣΙΑ ΚΥΒΕΡΝΟΣΦΕΤΕΡΙΣΜΟΥ

Η προστασία των domain name παρέχεται ανάλογα με το περιεχόμενο του δεύτερου μέρους τους. Αν τη διαδικτυακή διεύθυνση αποτελεί ένα όνομα, τότε παρέχεται η προστασία των άρθρων 57 και 58 ΑΚ. Αν πρόκειται για εμπορική επωνυμία, δηλαδή ένα όνομα με το οποίο ο έμπορος διεξάγει τις συναλλαγές του ή για διακριτικό τίτλο τότε μαζί με την

προστασία του άρθρου 58 ΑΚ παρέχεται και η προστασία του άρθρου 13 του νόμου 146/1914. Το άρθρο 13 του νόμου 1146/1914 εφαρμόζεται και όταν ένα domain name αποτελεί εικονικό κατάστημα που είναι γνωστό και επικρατεί στις ηλεκτρονικές συναλλαγές. Αν η ηλεκτρονική διεύθυνση ταυτίζεται με το σήμα και υπάρχει κίνδυνος σύγχυσης στις συναλλαγές παρέχεται η προστασία των άρθρων 4, 18 και 26 του νόμου 2239/1994 περί σημάτων.

8.3.ΝΟΜΟΘΕΣΙΑ ΠΑΡΑΝΟΜΗΣ ΔΙΕΙΣΔΥΣΗΣ ΣΕ ΔΕΔΟΜΕΝΑ

Η χωρίς δικαίωμα διείσδυση – πρόσβαση σε συστήματα επεξεργασίας δεδομένων έστω και όταν γίνεται χωρίς πρόθεση βλάβης τιμωρείται με το άρθρο 370Γ του Ποινικού κώδικα.

Στην Ευρωπαϊκή Ένωση δεν έχουν ακόμα ψηφιστεί ειδικά νομοθετήματα για την αντιμετώπιση του hacking αλλά έχουν ήδη αρχίσει οι προπαρασκευαστικές εργασίες για την δημιουργία τους. Τέτοια είναι:

1.Η Ανακοίνωση της Επιτροπής με αριθμό COM/2001/0298 για την ασφάλεια δικτύων και πληροφοριών όπου γίνεται αναλυτική αναφορά για τη μη εξουσιοδοτημένη πρόσβαση σε υπολογιστές και δίκτυα υπολογιστών, μνεία στις ζημιές που μπορούν να προκληθούν και παράθεση πιθανών λύσεων.

2. Πρόταση Κανονισμού με αριθμό 2003.0063 για τη δημιουργία του Ευρωπαϊκού Οργανισμού για την Ασφάλεια Δικτύων και Πληροφοριών στόχος του οποίου θα είναι να διευκολύνει την εφαρμογή των κοινοτικών μέτρων σχετικά με την ασφάλεια δικτύων και πληροφοριών και να συμβάλλει στη διασφάλιση της διαλειτουργικότητας των λειτουργιών ασφαλείας στα δίκτυα και τα συστήματα πληροφοριών.

3. Πρόταση Απόφασης Πλαισίου του Συμβουλίου με αριθμό COM/2002/0173-CNS 2002/0086 για τις επιθέσεις κατά των συστημάτων πληροφοριών όπου στοιχειοθετείται το αδίκημα της επίθεσης μέσω παράνομης πρόσβασης σε συστήματα πληροφοριών και γίνεται αναλυτική αναφορά στο τι αποτελεί παράνομη παρεμβολή σε συστήματα πληροφοριών.

8.4.ΠΡΟΣΤΑΣΙΑ ΤΩΝ ΔΕΔΟΜΕΝΩΝ ΑΠΟ ΙΟΥΣ

Μια ιδιαίτερα συχνή και επικίνδυνη μορφή εγκληματικότητας που εμφανίζεται στο διαδίκτυο είναι η αλλοίωση ή διαγραφή των δεδομένων με ιούς. Οι ιοί των υπολογιστών, όπως είδαμε και σε προηγούμενο κεφάλαιο, είναι ειδικά προγράμματα που έχουν την ικανότητα να ανατυπώνονται από μόνα τους. Διακρίνονται σε δύο μορφές: στους ιούς των προγραμμάτων και στους ιούς των συστημάτων. Η παρεμβολή ιών στο πρόγραμμα ενός υπολογιστή γεννά την αστική ευθύνη του προμηθευτή και κάθε υπαιτίου και τη συμβατική ευθύνη του προμηθευτή του προγράμματος εφόσον υπάρχει πώληση προγράμματος. Σε αυτές τις περιπτώσεις εφαρμόζονται τα άρθρα 577 και 578 του ΑΚ. Επίσης γεννά και αδικοπρακτική ευθύνη του δράστη κατά τα άρθρα 914, 919 ΑΚ. Ο υπαίτιος όμως υπέχει και ποινική ευθύνη σύμφωνα με το άρθρο 381 ΠΚ.

Στην Ευρωπαϊκή Ένωση υπάρχει η Ανακοίνωση της Επιτροπής με αριθμό COM/2001/0298 για την ασφάλεια δικτύων και πληροφοριών όπου γίνεται αναλυτική αναφορά και λεπτομερής επεξήγηση της έννοιας του ιού, του τρόπου που λειτουργεί και των τρόπων αντιμετώπισης του. Το νομοθέτημα αυτό δεν έχει ακόμα ψηφιστεί ώστε να ισχύει.

8.5.ΠΡΟΣΤΑΣΙΑ ΔΕΔΟΜΕΝΩΝ ΠΡΟΣΩΠΙΚΟΥ ΧΑΡΑΚΤΗΡΑ

Η ανάπτυξη των νέων τεχνολογιών και οι νέες μορφές διαφήμισης και ηλεκτρονικών συναλλαγών οδήγησαν στην αυξημένη ζήτηση προσωπικών πληροφοριών από τον ιδιωτικό και δημόσιο τομέα. Οι προσωπικές αυτές πληροφορίες που αναφέρονται σε κάθε είδους δραστηριότητα προσωπική είτε επαγγελματική του ατόμου ονομάζονται προσωπικά δεδομένα

Προσωπικά δεδομένα είναι , σύμφωνα με τον *Νόμο 2472/1997* και την *Οδηγία 95/46/ΕΚ* κάθε πληροφορία που αναφέρεται στο πρόσωπό του κάθε ατόμου, π.χ. το όνομα και το επάγγελμά του ατόμου, η οικογενειακή του κατάσταση, η ηλικία του, ο τόπος κατοικίας, η φυλετική του προέλευση, τα πολιτικά του φρονήματα, η θρησκεία που πιστεύει, οι φιλοσοφικές του απόψεις, η συνδικαλιστική του δράση, η υγεία του, η ερωτική του ζωή και οι τυχόν ποινικές του διώξεις και καταδίκες.

Για την επεξεργασία και συλλογή προσωπικών δεδομένων είναι απαραίτητη άδεια από την Αρχή Προστασίας Προσωπικών Δεδομένων. Οι οδηγίες για την χορήγηση άδειας επεξεργασίας αναλύονται στην *Κανονιστική Πράξη 1/1999 ΑΠΠΔ* σχετικά με την ενημέρωση υποκειμένου των δεδομένων *κατ' άρθρο 11 Ν. 2472/1997* και στην *Απόφαση 408.1998 ΑΠΠΔ* σχετικά με την ενημέρωση υποκειμένων επεξεργασίας δεδομένων προσωπικού χαρακτήρα δια του τύπου.

Η συγκέντρωση και επεξεργασία δεδομένων προσωπικού χαρακτήρα αποτελεί έναν από τους μεγαλύτερους κινδύνους επέμβασης στην προσωπική σφαίρα και στην ιδιωτική ζωή του ατόμου. Κάθε δραστηριότητα του σύγχρονου ανθρώπου γίνεται καθημερινά αντικείμενο επεξεργασίας και ανάλυσης γεγονός που χρήζει αντιμετώπισης και νομική κατοχύρωσης.

Στην Ελλάδα και την Ευρώπη ισχύουν πολλά νομοθετήματα που προστατεύουν τους πολίτες από την επεξεργασία προσωπικών δεδομένων σε διάφορους τομείς. Έτσι έχουμε:

Τον *Νόμο 2774.1999*, την *Οδηγία 97/66/ΕΚ,* και την *Σύσταση 558.2003* που αναφέρονται στην ιδιωτική ζωή στον τηλεπικοινωνιακό τομέα. Την *Υπουργική απόφαση 80329.2003*, *την Οδηγία 2002.58.ΕΚ*, *την Σύσταση R(99)5, το Ψήφισμα 2003.C48* και *τη Σύσταση 2003.203* που αναφέρονται στην προστασία της ιδιωτικής ζωής στις ηλεκτρονικές επικοινωνίες και συναλλαγές.

Όμως ισχύουν και γενικότερου περιεχομένου νομοθετήματα που είτε συστήνουν Αρχές που εποπτεύουν την επεξεργασία προσωπικών δεδομένων όπως είναι στην Ελλάδα "Η Αρχή Προστασίας Προσωπικών Δεδομένων" (*Νόμος 2472.1997*) και η "Αρχή Διασφάλισης Απορρήτου" *(Νόμος 3115.2003*) και στην Ευρώπη "Ο Ευρωπαίος Επόπτης Προσωπικών Δεδομένων" *(Απόφαση 1247.2002.ΕΚ*) είτε ρυθμίζουν την διαβίβαση προσωπικών δεδομένων από την Κοινότητα σε άλλες χώρες *(Απόφαση 2003.490, Απόφαση του Συμβουλίου 2004/644/ΕΚ*).

Η συγκέντρωση και επεξεργασία ηλεκτρονικών δεδομένων αντιμετωπίστηκε από πολύ νωρίς ως ένας από τους μεγαλύτερους κινδύνους επέμβασης στην ιδιωτική και προσωπική σφαίρα. Τόσο στην Ελλάδα όσο και στην Ευρωπαϊκή Ένωση υπάρχει νομοθεσία που ρυθμίζει τα σχετικά με την επεξεργασίας δεδομένων όπως η Οδηγία 2002/58 σχετικά με την επεξεργασία των δεδομένων προσωπικού χαρακτήρα και την προστασία της ιδιωτικής ζωής στον τομέα των ηλεκτρονικών επικοινωνιών και η Οδηγία 95/46 για την προστασία των φυσικών προσώπων έναντι της επεξεργασίας δεδομένων προσωπικού.

8.6.ΑΠΑΤΗ ΜΕΣΩ ΤΟΥ ΔΙΑΔΙΚΤΥΟΥ

Στην Ευρωπαϊκή ένωση ισχύει η Απόφαση-πλαίσιο του Συμβουλίου με αριθμό 2001/413/ΔΕΥ για την καταπολέμηση της απάτης και της πλαστογραφίας που αφορούν τα μέσα πληρωμής πλην των μετρητών.

8.7.SPAMMING

Στην Ελλάδα υπάρχουν πολλά νομοθετήματα για την προστασία των καταναλωτών αλλά αναφέρονται στα μηνύματα μέσω τηλεφώνου και φαξ κυρίως και μόνο αναλογικά στο ηλεκτρονικό ταχυδρομείο

8.8.ΤΟ ΔΙΚΑΙΟ ΤΗΣ ΠΝΕΥΜΑΤΙΚΗΣ ΙΔΙΟΚΤΗΣΙΑΣ ΣΕ ΣΧΕΣΗ ΜΕ ΤΗΝ ΚΟΙΝΩΝΙΑ ΤΩΝ ΠΛΗΡΟΦΟΡΙΩΝ ΚΑΙ ΤΟ INTERNET

Την κύρια πηγή του δικαίου της πνευματικής ιδιοκτησίας στην Ελλάδα αποτελεί ο Νόμος 2121/1993 με τίτλο "Πνευματική ιδιοκτησία, συγγενικά δικαιώματα και πολιτιστικά θέματα" όπως τροποποιήθηκε από τον Νόμο 3057/2002. Με την έναρξη της ισχύος αυτού του νόμου όλοι σχεδόν οι προγενέστεροι νόμοι που αφορούσαν την πνευματική ιδιοκτησία καταργήθηκαν.

Στον νόμο αυτόν περιέχονται μεταξύ άλλων και διατάξεις σχετικές με τα προγράμματα ηλεκτρονικών υπολογιστών και τις βάσεις δεδομένων και φωτογραφιών. Ανάλογες διατάξεις περιλαμβάνονται και στη συνθήκη του Παγκόσμιου Οργανισμού Διανοητικής Ιδιοκτησίας για την πνευματική ιδιοκτησία που κυρώθηκε με τον Νόμο 3184/2003. Επίσης ισχύει και η Συνθήκη του Παγκόσμιου Οργανισμού Διανοητικής Ιδιοκτησίας για τις εκτελέσεις και τα φωνογραφήματα, που κυρώθηκε με τον Νόμο 3183/2003. Σημαντική αρωγή στην προστασία των πνευματικών δικαιωμάτων προσφέρουν η Επιτροπή Ανταγωνισμού, που με σχετικές αποφάσεις της (π.χ. 245/ΙΙΙ.2003 σχετικά με την καταγγελία μουσικοσυνθετών κατά της "ΑΕΠΙ") βοηθά στην διασφάλιση των δικαιωμάτων πνευματικής ιδιοκτησίας, αλλά και οργανισμοί που ως σκοπό λειτουργίας τους έχουν τη διαχείριση πνευματικών δικαιωμάτων (ΥΑ 2170/2003)[24].

Η Ελληνική Νομολογία ενισχύει και αυτή με τη σειρά της την μάχη κατά της παραβίασης δικαιωμάτων πνευματικής ιδιοκτησίας, αν και κυρίως εστιάζεται σε θέματα συλλογικής διαχείρισης πνευματικών δικαιωμάτων (π.χ. 687/2003 Απόφαση Μονομελούς Πρωτοδικείου Τρικάλων) και ραδιοτηλεοπτικής φύσεως διενέξεων (π.χ. 1404/2002 Απόφαση του Συμβουλίου της Επικρατείας).

Στην Ευρώπη ισχύει η Οδηγία 93/98 περί εναρμονίσεως της διάρκειας προστασίας του δικαιώματος πνευματικής ιδιοκτησίας και ορισμένων συγγενών δικαιωμάτων καθώς και η Οδηγία 2001/29 για την εναρμόνιση ορισμένων πτυχών του δικαιώματος του δημιουργού και συγγενικών δικαιωμάτων στην κοινωνία της πληροφορίας.

Σχετικά με την πνευματική ιδιοκτησία στην κοινωνία των πληροφοριών υπάρχουν πληθώρα αποφάσεων νομολογίας που αναφέρονται τόσο σε προϊόντα λογισμικού δηλαδή προγράμματα ηλεκτρονικών υπολογιστών όσο και σε παράνομη αναπαραγωγή και ανταλλαγή δεδομένων και αρχείων μέσω του Internet που καταπατούν δικαιώματα πνευματικής ιδιοκτησίας των δημιουργών τους.

Η εμφάνιση των βάσεων δεδομένων σε συνδυασμό με τη διάδοση του Διαδικτύου έχει κάνει την αντιγραφή και την ηλεκτρονική διάδοση των πνευματικών δημιουργημάτων αποτελεσματική και εξαιρετικά απλή. Με τον τρόπο αυτό όμως καταστρατηγούνται τα δικαιώματα της πνευματικής ιδιοκτησίας των δημιουργών πάνω στα δημιουργήματά τους.

Τα δικαιώματα πνευματικής ιδιοκτησίας λοιπόν καθώς και η κατοχύρωση και προστασία τους αποτελούν απαραίτητη προϋπόθεση ανάπτυξης του πολιτισμού γενικότερα αλλά και κάθε επιχείρησης μεμονωμένα.

8.9. ΔΙΚΑΙΟΔΟΣΙΑ ΣΤΟ ΔΙΑΔΙΚΤΥΟ

Το πρόβλημα της δικαιοδοσίας στα εγκλήματα που τελούνται στο Διαδίκτυο δεν είναι απλό καθώς το Διαδίκτυο λόγω της παγκοσμιότητάς του επιτρέπει στον οποιοδήποτε να εισάγει και να καταστήσει προσβάσιμη από όλα τα σημεία του πλανήτη οποιαδήποτε πληροφορία θελήσει.

[24] http://www.lawnet.gr/case_study.asp

Για την ανεύρεση της αρμοδιότητας του δικαστηρίου πρέπει να καθοριστεί ο τόπος τέλεσης του αδικήματος. Για τον καθορισμό του τόπου τελέσεως του αδικήματος υποστηρίζονται τέσσερις θεωρίες[25].
Α) Η θεωρία του τόπου ενέργειας, σύμφωνα με την οποία ως τόπος τέλεσης του αδικήματος θα πρέπει να θεωρηθεί ο τόπος όπου ετελέσθη η ενέργεια που έτεινε στο άδικο αποτέλεσμα και αν η ενέργεια έλαβε χώρα σε περισσότερα από ένα κράτη, ο τόπος όπου ολοκληρώθηκε.
Β) Η θεωρία του τόπου του αποτελέσματος, όπου ως τόπος τελέσεως του αδικήματος θεωρείται ο τόπος όπου εκδηλώθηκε το ζημιογόνο αποτέλεσμα.
Γ) Η μικτή θεωρία, όπου ως τόπος τελέσεως του αδικήματος θεωρείται τόσο ο τόπος ενέργειας όσο και ο τόπος του αποτελέσματος με δικαίωμα επιλογής του αδικηθέντος.
Δ) Η θεωρία του βαρύνοντος τόπου, σύμφωνα με την οποία ο τόπος του αδικήματος εντοπίζεται στο κράτος όπου το έγκλημα εκδηλώθηκε κατά την κύρια σημασία του. Βέβαια υπάρχουν δυσκολίες κατά την εφαρμογή της θεωρίας δεδομένου ότι είναι δύσκολο να καθοριστεί ο βαρύνων τόπος για την τέλεση της διαδικτυακής αδικοπραξίας. Η κρατούσα θεωρία στην Ελλάδα και στην Ευρώπη είναι η θεωρία του βαρύνοντος τόπου.
Μέσω της δυναμικής εισβολής του ηλεκτρονικού υπολογιστή και της λειτουργίας του Διαδικτύου αναπτύσσονται αναρίθμητες δυνατότητες χρήσης και κατάχρησης που αφορούν την ηλεκτρονική επεξεργασία δεδομένων. Η ηλεκτρονική εγκληματικότητα συνεχώς εμπλουτίζεται με νέες εκφάνσεις και καθίσταται σαφές ότι μεμονωμένες προσπάθειες εκ μέρους του νομοθέτη ή των ιδιωτών δεν αρκούν για να δώσουν λύσεις. Για την καταπολέμηση της ηλεκτρονικής εγκληματικότητας απαιτείται συνεργασία μεταξύ όλων των κρατών όπως αναφέρεται σε πολλά νομοθετικά κείμενα.

8.10. ΔΙΚΤΥΑ ΥΠΟΛΟΓΙΣΤΩΝ ΚΑΙ ΝΟΜΟΘΕΣΙΑ

Η ασφάλεια των πληροφοριακών συστημάτων και ειδικότερα των δικτύων υπολογιστών μιας επιχείρησης είναι μία υποχρέωση που δεν αφορά μόνο την προστασία της επιχείρησης, αλλά και την προστασία των προσώπων, στοιχεία των οποίων έχουν καταχωριστεί στα συστήματα αυτά.

Ήδη ο νόμος 2472/97 (άρθρο 10) έχει επιβάλει υποχρεώσεις προστασίας της εμπιστευτικότητας – μυστικότητας των πληροφοριών και λήψης μέτρων ασφαλείας. Ο υπεύθυνος επεξεργασίας οφείλει να λαμβάνει όλα τα κατάλληλα οργανωτικά και τεχνικά μέτρα για την ασφάλεια των δεδομένων και την προστασία τους από τυχαία ή αθέμιτη καταστροφή, τυχαία απώλεια, αλλοίωση, απαγορευμένη διάδοση ή πρόσβαση και κάθε άλλη μορφή αθέμιτης επεξεργασίας. Τα μέτρα ασφαλείας που λαμβάνονται θα πρέπει να είναι ανάλογα προς τους κινδύνους που συνεπάγεται η επεξεργασία και η φύση των δεδομένων που είναι αντικείμενο της επεξεργασίας. Στις υποχρεώσεις μιας επιχείρησης περιλαμβάνεται η επιλογή συνεργατών που διαθέτουν όχι μόνο τεχνικές γνώσεις αλλά και προσωπική ακεραιότητα που διασφαλίζει την τήρηση του απορρήτου της επεξεργασίας[26].

Η Αρχή Προστασίας Προσωπικών Δεδομένων, όπως θα δούμε και στην συνέχεια, αποδίδει ιδιαίτερη σημασία στην εκπόνηση σχεδίου Ασφαλείας (security plan) και έκτακτης ανάγκης από τον υπεύθυνο επεξεργασίας, αλλά και στη συνεχή αναθεώρηση των σχεδίων αυτών ώστε να ανταποκρίνεται στις τεχνολογικές εξελίξεις. Συχνά μάλιστα οι άδειες επεξεργασίας ευαίσθητων δεδομένων συνοδεύονται από την επιβολή όρων ασφαλείας των δεδομένων και την υποχρέωση επεξεργασίας τέτοιων σχεδίων. Χωρίς να υπεισέρχεται σε λεπτομέρειες, η Αρχή Προστασίας Προσωπικών Δεδομένων έχει συντάξει ένα κείμενο οδηγιών, όπου αναφέρεται το βασικό περιεχόμενο των σχεδίων ασφαλείας και εκτάκτου

[25] Ed Tittel, Mike Chapple and James Michael Stewart Study Guide “Certified Information Systems Security Professional”

[26] http://www.lawnet.gr/case_study.asp

ανάγκης, ώστε αυτά να κρίνονται επαρκή από την άποψη της προστασίας της εμπιστευτικότητας.

8.11. ΑΡΧΕΣ ΠΡΟΣΤΑΣΙΑΣ ΔΕΔΟΜΕΝΩΝ ΣΤΑ ΔΙΚΤΥΑ ΥΠΟΛΟΓΙΣΤΩΝ

Η συγκέντρωση και επεξεργασία ηλεκτρονικών και μη δεδομένων αντιμετωπίστηκε από νωρίς και συνεχίζει να αντιμετωπίζεται ως ένας από τους μεγαλύτερους κινδύνους επέμβασης στην ιδιωτική ζωή. Η υπάρχουσα νομοθεσία παρέχει επαρκή προστασία στους πολίτες αλλά με την πάροδο του χρόνου και την περαιτέρω ανάπτυξη της τεχνολογίας χρειάζονται ειδικότερες διατάξεις που θα αντικαταστήσουν τις γενικές και από τις οποίες θα προκύπτει με σαφήνεια ποιος, πότε ακριβώς, σε ποια δεδομένα και με ποιο σκοπό θα έχει δικαίωμα πρόσβασης και επεξεργασίας. Στην προσπάθεια του Ελληνικού κράτους για εξασφάλιση υψηλού βαθμού εμπιστευτικότητας των πολιτών στις νέες τεχνολογίες επικοινωνιών είτε μέσω υπολογιστών είτε μέσω άλλων τηλεπικοινωνιακών μέσων, έχουν ιδρυθεί δύο αρχές προστασίας που σχετίζονται με τα προσωπικά δεδομένα, η Αρχή Προστασίας Προσωπικών Δεδομένων και η Αρχή Διασφάλισης του Απορρήτου των Επικοινωνιών[27].

8.11.1: ΑΡΧΗ ΠΡΟΣΤΑΣΙΑΣ ΠΡΟΣΩΠΙΚΩΝ ΔΕΔΟΜΕΝΩΝ

Για την αμεσότερη και ταχύτερη προστασία των πολιτών από την επεξεργασία προσωπικών δεδομένων θεωρήθηκε αναγκαία η ίδρυση μιας Αρχής που θα εποπτεύει και θα ασχολείται αποκλειστικά με αυτό το αντικείμενο. Η αρχή αυτή, που ιδρύθηκε το 1997 και ονομάστηκε Αρχή Προστασίας Προσωπικών Δεδομένων (ΑΠΠΔ) έχει ποικίλες αρμοδιότητες μεταξύ των οποίων είναι να εκδίδει οδηγίες και αποφάσεις και να γνωμοδοτεί για κάθε ρύθμιση που αφορά την επεξεργασία και προστασία δεδομένων προσωπικού χαρακτήρα. Οι σημαντικότερες Οδηγίες της ΑΠΠΔ είναι :

- Η *Οδηγία 1122.2000* για τα κλειστά κυκλώματα τηλεόρασης και
- Η *Οδηγία 115/2001* για την επεξεργασία δεδομένων των εργαζομένων όπου επειδή αποτελεί και την ουσία της συγκεκριμένης εργασίας παρατίθεται στο Παράρτημα Α.

Οι σπουδαιότερες αποφάσεις της ΑΠΠΔ, που έχουν φυσικά συνάφεια με το αντικείμενο της συγκεκριμένης εργασίας, είναι οι εξής:

- Η *Απόφαση 50/2000* σχετικά με τους όρους για την νόμιμη επεξεργασία δεδομένων προσωπικού χαρακτήρα για τους σκοπούς της άμεσης εμπορίας ή διαφήμισης και της διαπίστωσης πιστοληπτικής ικανότητας.
- Η *Απόφαση 120/2001* για την επεξεργασία Προσωπικών Δεδομένων σχετικά την παροχή υπηρεσιών καρτοκινητής τηλεφωνίας
- Η *Απόφαση 1469.2000* για τη συλλογή προσωπικών δεδομένων από εταιρείες τηλεπικοινωνιακών δραστηριοτήτων.
- Η *Απόφαση 147/2001* για την χρήση ευαίσθητων δεδομένων ενώπιον δικαστηρίου
- Η *Απόφαση 8/2003* σχετικά με την πρόσβαση τρίτου σε δεδομένα εταιρείας κινητής τηλεφωνίας για άσκηση δικαιώματος υπεράσπισης ενώπιον δικαστηρίου.

Οι πιο άξιες προσοχής, τέλος, γνωμοδοτήσεις της ΑΠΠΔ είναι[28]:

[27] http://www.lawnet.gr/case_study.asp

[28] www.dpa.gr

- Η *Γνωμοδότηση 71/2002* σχετικά με την επεξεργασία προσωπικών δεδομένων στην αυτόματη αναγνώριση της ταυτότητας του συνδρομητή καλούσας γραμμής σε ψηφιακά δίκτυα ενοποιημένων υπηρεσιών (ISDN),
- Η *Γνωμοδότηση 78/2002* για τις προϋποθέσεις διασταύρωσης προσωπικών δεδομένων στο χώρο της σταθερής τηλεφωνίας,
- Η *Γνωμοδότηση 86/2001* σχετικά με την είσοδο και παραμονή αλλοδαπών στην ελληνική επικράτεια,
- Η *Γνωμοδότηση 15/2001* σχετικά με την ανάλυση γενετικού υλικού για σκοπούς εξιχνίασης εγκλημάτων και ποινικής δίωξης.

8.11.2 Αρχή Διασφάλισης Του Απορρήτου Των Επικοινωνιών

Η Αρχή Διασφάλισης του Απορρήτου των Επικοινωνιών (Α.Δ.Α.Ε.) προβλέπεται από το Ν.3115/2003. Είναι ανεξάρτητη αρχή με διοικητική αυτοτέλεια και έχει ως σκοπό την προστασία του απορρήτου των επιστολών και της ελεύθερης ανταπόκρισης και επικοινωνίας με οποιονδήποτε άλλο τρόπο. Στο πλαίσιο αυτό, η Α.Δ.Α.Ε. είναι η αρμόδια αρχή για τον έλεγχο της τήρησης των όρων και της διαδικασίας άρσης του απορρήτου. Η δράση της διέπεται πάντοτε από τις αρχές της διαφάνειας, της αντικειμενικότητας και της αμεροληψίας.

Η Α.Δ.Α.Ε. αποτελείται από 7 μέλη και ισάριθμα αναπληρωματικά, τα οποία απολαμβάνουν κατά την άσκηση των καθηκόντων τους πλήρη προσωπική και λειτουργική ανεξαρτησία. Ωστόσο, έχουν καθήκον εχεμύθειας, το οποίο υφίσταται και μετά την αποχώρησή τους. Τα πρόσωπα που θα γίνουν μέλη της Α.Δ.Α.Ε. επιλέγονται από τη Βουλή και πρέπει να τυγχάνουν ευρείας κοινωνικής αποδοχής και να διακρίνονται για την επιστημονική τους κατάρτιση και την επαγγελματική τους ικανότητα στο νομικό τομέα ή στον τεχνικό τομέα των επικοινωνιών

Η Α.Δ.Α.Ε. στο πλαίσιο εκπλήρωσης του σκοπού της, μπορεί[29]:

- Να διενεργεί αυτεπαγγέλτως ή έπειτα από καταγγελία τακτικούς ή έκτακτους ελέγχους σε εγκαταστάσεις, τεχνικό εξοπλισμό, αρχεία, τράπεζες δεδομένων και έγγραφα της Εθνικής Υπηρεσίας Πληροφοριών, άλλων δημόσιων υπηρεσιών, οργανισμών, επιχειρήσεων του ευρύτερου δημόσιου τομέα και ιδιωτικών επιχειρήσεων που ασχολούνται με ταχυδρομικές, τηλεπικοινωνιακές ή άλλες υπηρεσίες σχετικές με την ανταπόκριση και την επικοινωνία.
- Να καλεί σε ακρόαση τις διοικήσεις, τους νόμιμους εκπροσώπους και τους υπαλλήλους των ως άνω δημοσίων υπηρεσιών ή ιδιωτικών εταιριών.
- Να συνεργάζεται με άλλες αρχές της χώρας, με αντίστοιχες αρχές άλλων κρατών και με ευρωπαϊκούς ή διεθνείς οργανισμούς.
- Να γνωμοδοτεί και να απευθύνει συστάσεις και υποδείξεις για τη λήψη μέτρων διασφάλισης του απορρήτου των επικοινωνιών, καθώς και για τη διαδικασία άρσης αυτού.

Τα μέλη και το προσωπικό της Α.Δ.Α.Ε., για να διαπιστώσουν παράβαση της νομοθεσίας για την προστασία του απορρήτου, μπορούν να ελέγχουν τα βιβλία και στοιχεία των ελεγχόμενων υπηρεσιών, οργανισμών και επιχειρήσεων, καθώς και πάσης φύσεως αρχεία, βιβλία, στοιχεία και λοιπά έγγραφα των προσώπων που ελέγχουν. Επιπλέον, έχουν δικαίωμα να ενεργούν έρευνες στα γραφεία και τις λοιπές εγκαταστάσεις των ελεγχόμενων και να διενεργούν ένορκες και μη καταθέσεις, με την επιφύλαξη του επαγγελματικού απορρήτου των εξεταζόμενων προσώπων.

Σε περίπτωση που κατά τον έλεγχο διαπιστωθεί παραβίαση του απορρήτου, τα μέλη της Α.Δ.Α.Ε. μπορούν να κατασχέσουν τα μέσα με τα οποία πραγματοποιείται η παραβίαση

[29] www.dpa.gr

αυτή, ενώ παράλληλα καταστρέφουν τις πληροφορίες, τα δεδομένα ή τα στοιχεία που αποκτήθηκαν με παράνομη παραβίαση του απορρήτου των επικοινωνιών. Για τα μέσα που κατάσχονται, ορίζεται μεσεγγυούχος ωσότου αποφανθούν τα αρμόδια δικαστήρια.

Η Α.Δ.Α.Ε. αποφασίζει με απόλυτη πλειοψηφία των παρόντων μελών της με φανερή ψηφοφορία. Για να είναι όμως νόμιμη η συνεδρίαση, θα πρέπει να μετέχουν τουλάχιστον 3 μέλη. Οι αποφάσεις της πρέπει να είναι αιτιολογημένες, καταχωρούνται σε ειδικό βιβλίο και μπορούν να δημοσιεύονται, εφόσον δεν αφορούν στην εθνική άμυνα ή τη δημόσια ασφάλεια.

Σε κάθε περίπτωση, η Α.Δ.Α.Ε. οφείλει να μην αποκαλύπτει πληροφορίες και δεδομένα για φυσικά ή νομικά πρόσωπα, τα οποία ενδέχεται να προσβάλλουν την προσωπικότητά τους ή να επηρεάσουν δυσμενώς την επαγγελματική ή την κοινωνική τους θέση, εκτός εάν προκύπτει τέτοια υποχρέωση από το νόμο.

Ο πολίτης δικαιούται να υποβάλει καταγγελία προς την Α.Δ.Α.Ε., οπότε, εφόσον κριθεί αναγκαίο, η Αρχή μπορεί να τον καλέσει για να παράσχει έγγραφες ή προφορικές διευκρινίσεις. Εφόσον ο πολίτης είναι ο άμεσα ενδιαφερόμενος, έχει δικαίωμα πρόσβασης από το νόμο στους φακέλους των υποθέσεων που τον αφορούν και στα πρακτικά των αντίστοιχων συνεδριάσεων, εκτός αν οι υποθέσεις αυτές αφορούν στην εθνική άμυνα ή τη δημόσια ασφάλεια.

Οι αποφάσεις της Α.Δ.Α.Ε. μπορούν να προσβληθούν δικαστικά και συγκεκριμένα κατά των εκτελεστών αποφάσεων της Α.Δ.Α.Ε. μπορεί να ασκηθεί αίτηση ακύρωσης ενώπιον του Συμβουλίου της Επικρατείας καθώς και οι προβλεπόμενες από το Σύνταγμα και τη νομοθεσία διοικητικές προσφυγές. Κατά των αποφάσεων αυτών μπορεί να ασκεί ένδικα βοηθήματα και ο υπουργός Δικαιοσύνης.

8.11.3.Δεσμεύσεις για μία Επιχείρηση που Συναλλάσσεται Ηλεκτρονικά

Η συλλογή και επεξεργασία προσωπικών δεδομένων εξελίσσεται σε συστατικό στοιχείο των ενδοδικτυακών συναλλαγών. Προσωπικά δεδομένα συλλέγονται συνήθως ήδη κατά την αρχική φάση σύνδεσης του ενδιαφερόμενου καταναλωτή με το δικτυακό χώρο της επιχείρησης, συχνά μέσω εντύπων που συμπληρώνει ψηφιακά ο πλοηγός-αγοραστής. Η συλλογή δεδομένων, συνήθως με απώτερο σκοπό τη δημιουργία του προφίλ του «πελάτη», γίνεται συχνά και με άλλους τρόπους, όπως εγκατάσταση cookies, τεχνικές εξόρυξης δεδομένων κλπ.. Η χρήση τέτοιων τεχνικών παρουσιάζεται συνήθως ως αναγκαιότητα για τη διαμόρφωση των πολιτικών και της στρατηγικής των επιχειρήσεων.

Ωστόσο, όσοι δραστηριοποιούνται στο πεδίο των ηλεκτρονικών συναλλαγών οφείλουν να γνωρίζουν πως ό,τι είναι τεχνικά δυνατό δεν είναι αυτονόητα και νόμιμο ή θεμιτό. Η συλλογή και επεξεργασία προσωπικών δεδομένων στο πλαίσιο του ηλεκτρονικού επιχειρείν υπόκειται στις ρυθμίσεις, τις προϋποθέσεις και απαγορεύσεις των νόμων 2472/97 για την προστασία του ατόμου από την επεξεργασία προσωπικών δεδομένων και 2774/99 για την προστασία προσωπικών δεδομένων στον τηλεπικοινωνιακό τομέα και τις επιμέρους ερμηνευτικές Οδηγίες που έχει εκδώσει η Αρχή Προστασίας Προσωπικών Δεδομένων (http://www.dpa.gr).

Ένα κρίσιμο στοιχείο είναι ότι η συλλογή και επεξεργασία προσωπικών δεδομένων επιτρέπεται καταρχήν μόνο με συγκατάθεση του χρήστη-πελάτη ή στο πλαίσιο της εκπλήρωσης μιας σύμβασης που ήδη συνδέει την επιχείρηση με αυτόν. Σε άλλη περίπτωση η συλλογή τέτοιων δεδομένων είναι νόμιμη εφόσον αυτά προέρχονται από καταλόγους και πηγές δημόσια προσβάσιμες που απευθύνονται στο ευρύ κοινό καθώς και προηγούμενες συναλλακτικές επαφές στο πλαίσιο συναφών σκοπών.

Τα προσωπικά δεδομένα των αντισυμβαλλόμενων ή των ενδιαφερομένων επισκεπτών των ιστοσελίδων μιας επιχείρησης πρέπει να συλλέγονται με τρόπο νόμιμο, θεμιτό και διαφανή. Όπως τονίζεται στην νέα Οδηγία 2002/58/ΕΚ «σχετικά με την επεξεργασία δεδομένων προσωπικού χαρακτήρα και την προστασία της ιδιωτικής ζωής στον τομέα των ηλεκτρονικών επικοινωνιών» λογισμικό παρακολούθησης, δικτυακοί «κοριοί», κρυφά

αναγνωριστικά στοιχεία και άλλες παρόμοιες διατάξεις που μπορούν να εισέλθουν στο τερματικό του χρήστη εν αγνοία του με σκοπό την πρόσβαση σε πληροφορίες, την αποθήκευση αθέατων πληροφοριών ή την ανίχνευση των δραστηριοτήτων του χρήστη, συνιστούν ενδεχόμενη σοβαρή παραβίαση της ιδιωτικής ζωής του χρήστη. Η χρησιμοποίηση τέτοιων διατάξεων θα πρέπει να επιτρέπεται μόνο για θεμιτούς σκοπούς και εφόσον το γνωρίζουν οι χρήστες αυτοί.

Η ενημέρωση των χρηστών κατά το στάδιο της συλλογής των προσωπικών δεδομένων που τους αφορούν, έχει κεφαλαιώδη σημασία για την προστασία των προσωπικών δεδομένων αλλά και για τη νομιμότητα της επεξεργασίας τους και δε συνιστά μόνο αυτοτελή υποχρέωση που έχει εισαγάγει η νομοθεσία για την προστασία προσωπικών δεδομένων, αλλά αποτελεί ταυτοχρόνως και προϋπόθεση για την έγκυρη συγκατάθεση του χρήστη. Η συγκατάθεση στην ελληνική νομοθεσία για την προστασία προσωπικών δεδομένων νοείται ως «ενημερωμένη συγκατάθεση» (informed consent).

Η ενημέρωση πρέπει να αναφέρεται καταρχήν στο γεγονός καθαυτό της συλλογής και επεξεργασίας προσωπικών δεδομένων και τη βάση στην οποία αυτή θεμελιώνεται (συγκατάθεση, σύμβαση). Οπωσδήποτε πρέπει να περιλαμβάνει την (online και offline) ταυτότητα αυτού που συλλέγει τα δεδομένα, το σκοπό για τον οποίο συλλέγονται τα δεδομένα, καθώς και πληροφορίες για τους τυχόν περαιτέρω αποδέκτες των δεδομένων. Είναι επίσης αναγκαίο και σκόπιμο να ενημερώνονται οι επισκέπτες/συναλλασσόμενοι για τα δικαιώματα που τους παρέχει η νομοθεσία για την προστασία προσωπικών δεδομένων (δικαίωμα πρόσβασης, διόρθωσης, αντίταξης κλπ.).

Εφόσον οι επιχειρήσεις έχουν εκπονήσει πολιτικές Ασφαλείας της ιδιωτικότητας είναι χρήσιμο και εξυπηρετεί ταυτόχρονα τους σκοπούς της ενημέρωσης, να ανακοινώνονται σε εμφανή σημεία των αντίστοιχων ηλεκτρονικών σελίδων. Είναι αυτονόητο ότι αυτές οι πολιτικές πρέπει να είναι σύμφωνες και να εναρμονίζονται με το γράμμα και το πνεύμα της νομοθεσίας για την προστασία προσωπικών δεδομένων. Η ενημέρωση είναι απαραίτητη και στην περίπτωση της εγκατάστασης «cookies» ή άλλων συναφών διατάξεων. Όταν οι διατάξεις αυτές προορίζονται για σκοπούς που η έννομη τάξη κρίνει ως θεμιτούς, η χρησιμοποίησή τους επιτρέπεται μόνο υπό τον όρον ότι παρέχονται στους χρήστες σαφείς και ακριβείς πληροφορίες για τον προορισμό των «cookies» ή τυχόν ανάλογων διατάξεων, ώστε να εξασφαλίζεται ότι είναι εν γνώσει του χρήστη οι πληροφορίες που αποθηκεύονται στον τερματικό υπολογιστή που χρησιμοποιεί και να παρέχεται στους χρήστες η δυνατότητα να αρνηθούν την αποθήκευση «cookies» ή παρόμοιων διατάξεων στον τερματικό τους εξοπλισμό. Οι τρόποι της παροχής πληροφοριών, της παροχής του δικαιώματος άρνησης ή αίτησης συγκατάθεσης θα πρέπει να είναι όσο το δυνατόν πιο προσιτοί για το χρήστη.

8.11.4.Παραβάσεις της Νομοθεσίας περί Ασφάλειας Δικτύων και Ποινές

Η τήρηση των επιταγών και απαγορεύσεων που σχετίζονται με την επεξεργασία αλλά και την ασφάλεια των προσωπικών δεδομένων επιβάλλεται από την οικεία νομοθεσία. Τυχόν παράβαση των υποχρεώσεων αυτών για προστασία και ασφάλεια των δεδομένων ενδέχεται να έχει ως αποτέλεσμα την επιβολή διοικητικών κυρώσεων από την Αρχή Προστασίας Προσωπικών Δεδομένων (όπως 11 πρόστιμα, αναστολή επεξεργασίας, καταστροφή αρχείων κλπ.) ή/και τη γέννηση αξιώσεων και υποχρεώσεων αποζημίωσης ή χρηματικής ικανοποίησης των προσώπων που θίγονται από τις παραβάσεις των νομοθετικών διατάξεων και των υποχρεώσεων ασφαλείας.

Όποιος παραβιάζει με οποιονδήποτε τρόπο το απόρρητο των επικοινωνιών ή τους όρους και τη διαδικασία άρσης αυτού, τιμωρείται με ποινή φυλάκισης τουλάχιστον ενός έτους και χρηματική ποινή από 15.000 έως 60.000 ευρώ. Σε περίπτωση που ο παραβάτης ανήκει στο προσωπικό υπηρεσίας, οργανισμού, νομικού προσώπου ή επιχείρησης που ασχολείται με ταχυδρομικές, τηλεπικοινωνιακές ή άλλες υπηρεσίες σχετικές με την ανταπόκριση ή την επικοινωνία, η επιβαλλόμενη ποινή φυλάκισης είναι τουλάχιστον 2 ετών και η χρηματική ποινή τουλάχιστον 30.000 ευρώ.

Συγκεκριμένες παραβάσεις συνιστούν μάλιστα ποινικά αδικήματα και επισύρουν και ποινικές κυρώσεις. Ωστόσο, η μεγαλύτερη κύρωση είναι η δυσπιστία των συναλλασσόμενων. Πολλές πρόσφατες μελέτες έχουν αποδείξει ότι πολλοί άνθρωποι απέχουν από ηλεκτρονικές συναλλαγές από φόβο για τη μεταχείριση και την τύχη των προσωπικών τους δεδομένων. Η επένδυση σε τεχνολογίες ενίσχυσης της ιδιωτικότητας (Privacy Enhancing Technologies), η ύπαρξη, τήρηση και διαφήμιση πολιτικών για την προστασία της ιδιωτικότητας δεν είναι απλά συμμόρφωση προς το νόμο. Είναι ανταγωνιστικό πλεονέκτημα. Είναι προϋπόθεση για να αποκτηθεί η εμπιστοσύνη των καταναλωτών.

Εκτός από την Ελληνική δικαιοσύνη και την Αρχή Προστασίας Προσωπικών Δεδομένων που επιβάλει κυρώσεις σε περιπτώσεις άρσης του απορρήτου στην επικοινωνία μέσω τηλεπικοινωνιακών δικτύων ή δικτύων υπολογιστών, και η Αρχή Διατήρησης της Ακεραιότητας των Επικοινωνιών μπορεί να επιβάλει στον παραβάτη διοικητικές κυρώσεις. Η απόφασή της πρέπει να είναι πλήρως αιτιολογημένη και πάντοτε ύστερα από προηγούμενη κλήτευση και ακρόαση του φερόμενου ως υπαιτίου, ο οποίος μπορεί να παραστεί μετά ή διά πληρεξουσίου δικηγόρου, εκτός αν ο Πρόεδρος της Α.Δ.Α.Ε. διατάξει την αυτοπρόσωπη παρουσία του. Οι διοικητικές κυρώσεις που μπορεί να επιβάλει η Αρχή είναι:

- Σύσταση για συμμόρφωση σε συγκεκριμένη διάταξη της νομοθεσίας με προειδοποίηση επιβολής κυρώσεων σε περίπτωση υποτροπής του παραβάτη, και
- Πρόστιμο από 15.000 έως 1.500.000 ευρώ.

Παράλληλα με τα παραπάνω νομοθετικά κείμενα και την δραστηριότητα της Α.Π.Π.Δ. και της Α.Δ.Α.Ε. οι πολίτες που γίνονται υποκείμενα επεξεργασίας προσωπικών δεδομένων προστατεύονται όπως αναφέραμε και από τα δικαστήρια. Πληθώρα δικαστικών αποφάσεων, ελληνικών και ξένων, αναφέρονται και ρυθμίζουν κάθε είδους διαφορά που ανακύπτει σχετικά με την επεξεργασία προσωπικών δεδομένων.

Μερικές από τις ελληνικές αποφάσεις είναι οι εξής[30]:

- Η *1129.2001* του Μον.Πρωτ.Τρ. σχετικά με την προστασία προσωπικών δεδομένων στον τηλεπικοινωνιακό τομέα.
- Η *1988.2002* του Μον.Πρωτ.Αθ. σχετικά με την πώληση προϊόντων εξ αποστάσεως και την παράνομη αποστολή διαφημιστικών εντύπων
- Η *2950.2002* του Μον.Πρωτ.Θεσ. σχετικά με την δωσιδικία νομικού προσώπου σε υπόθεση επεξεργασία δεδομένων προσωπικού χαρακτήρα
- Η *2279.2001* του ΣτΕ σχετικά με την σύσταση της Αρχής Προστασίας Δεδομένων Προσωπικού Χαρακτήρα
- Η *2286.2001* του ΣτΕ σχετικά με την άσκηση αίτησης ακυρώσεως κατά πράξεως της Αρχής Προστασίας Προσωπικών Δεδομένων από Πολιτικό κόμμα.
- Η *984.2001* του Συμβουλίου Εφετών για την παράνομη γνώση, αλλοίωση και ανακοίνωση ευαίσθητων προσωπικών δεδομένων
- Η *3545/2002* του ΣτΕ σχετικά με την συμμετοχή σε συνεδρίαση της Αρχής Προστασίας Προσωπικών Δεδομένων αναπληρωματικού μέλους της, στο οποίο έχουν ανατεθεί καθήκοντα εισηγητή.

Κάποιες από τις ξένες δικαστικές αποφάσεις σχετικά με τα προσωπικά δεδομένα είναι οι ακόλουθες:

- Απόφαση Αμερικανικού Δικαστηρίου για παραβίαση Ιδιωτικής Ζωής μέσω του Διαδικτύου όπου αναφέρεται ότι η παροχή συμβουλευτικών υπηρεσιών και οι κάθε είδους γραπτές αναφορές μέσω ηλεκτρονικού ταχυδρομείου (e-mail) στο κοινό δεν παρέχει το

[30] http://www.lawnet.gr/case_study.asp

δικαίωμα ελέγχου των προσωπικών δεδομένων του παρόχου και αποκάλυψης της ηλεκτρονικής του αλληλογραφίας.

- Απόφαση Αμερικανικού Δικαστηρίου για παραβίαση Ιδιωτικής Ζωής που ρυθμίζει υπόθεση όπου ηλεκτρονικές βιβλιοθήκες χρησιμοποιήθηκαν για την παροχή πληροφοριών μέσω Internet
- Απόφαση Αμερικανικού Δικαστηρίου για παραβίαση ιδιωτικής ζωής εργαζομένου που ρυθμίζει υπόθεση όπου εργαζόμενος, ο οποίος απολύθηκε από την εταιρία που εργαζόταν διατυπώνει την επιφύλαξη του κατά πόσο η δημιουργία εσωτερικού δικτύου επικοινωνίας με τους υπόλοιπους εργαζομένους από αυτόν συνιστά παραβίαση της ιδιωτικής του σφαίρας μετά την απόλυσή του.

ΕΠΙΛΟΓΟΣ

Η σημασία της εξέλιξης και ανάπτυξης της τεχνολογίας είναι αναμφισβήτητης αξίας. Η δημιουργία νέων επιτευγμάτων τα οποία άλλαξαν ριζικά την ζωή και την καθημερινότητά μας είναι επίσης πολύ σημαντική. Τα σημαντικότερα όμως επιτεύγματα έχουν σχέση με την τεχνολογία της πληροφόρησης και της επικοινωνίας. Οι σύγχρονες τεχνολογικές μέθοδοι συνέβαλλαν προς την κατεύθυνση της έξαρσης της επικοινωνίας. Έννοιες όπως η πληροφορία και η σημασία της απέκτησαν νέο νόημα και απέκτησαν σημαντική πια αξία στην ψηφιακή εποχή. Ο συνδυασμός της τεχνολογίας την πληροφορίας αλλά και η εξάπλωση και εξέλιξη των σύγχρονων τεχνολογιών δημιούργησαν ή ενίσχυσαν πολλά νέα μέσα επικοινωνίας. Ένα χαρακτηριστικό παράδειγμα αποτελεί η εμφάνιση των επιχειρησιακών δικτύων. Παρότι όχι νέο επίτευγμα από τεχνολογική πλευρά, παρουσίασε σημαντική άνοδο και πρόοδο τα τελευταία χρόνια. Τεράστιος αριθμός επιχειρήσεων έχει πια ένα δίκτυο. Στόχος του δικτύου αυτού είναι η καλύτερη και πιο αποτελεσματική επικοινωνία και ανταλλαγή πληροφοριών ανάμεσα στα μέλη του δικτύου. Πολλά χαρακτηριστικά διέπουν τη λειτουργία και τους σκοπούς αυτών των δικτύων. Αυτό όμως που παρουσιάζει εξαιρετικό και σημαντικό ενδιαφέρον είναι το κοινωνικό στοιχείο αυτών των δικτύων. Αφορούν ανθρώπινο δημιούργημα και εξυπηρετούν ανθρώπινους και φυσικά επιχειρησιακούς σκοπούς.

ΒΙΒΛΙΟΓΡΑΦΙΑ

1. Andrew S. Tanenbaum «Δίκτυα Υπολογιστών» 3ηέκδοση
2. Cisco Press Publications “Designing Network Security
3. E-business Forum - Γενική Γραμματεία Βιομηχανίας
4. Ed Tittel, Mike Chapple and James Michael Stewart Study Guide “Certified Information Systems Security Professional”
5. http://andronianoi.ucoz.com/arxeia_pdf/ti_enai_to_intranet.pdf
6. http://www.cnc.uom.gr/services/pdf/section1(2).pdf
7. http://www.it.uom.gr/project/MultimediaTechnologyNotes/chap2d_3.htm
8. http://www.lawnet.gr/case_study.asp
9. Stan Schatt “Τοπικά Δίκτυα Υπολογιστών”
10. Venieris G. and J. Zorgios: " Capturing the Cost of Quality of ISO 9000 Quality Management Systems" , Ανακοίνωση στο 22ο Ετήσιο Συνέδριο της European Accounting Association στο Bordeaux Γαλλίας, 1999
11. Venieris G., J. Zorgios and S. Cohen: " Learning Curve Costs: Can They Be Captured Through ABC?", Ανακοίνωση στο 23ο Ετήσιο Συνέδριο της European Accounting Association στο Munich Γερμανίας, 2000.
12. www.dpa.gr
13. Β.Σκουλάτος ,Σύγχρονα Τηλεπικοινωνιακά Δίκτυα Α’ τόμος Φεβ. 2000
14. Γ.Πάγκαλος και Ι.Μαυρίδης “Ασφάλεια Πληροφοριακών Συστημάτων και Δικτύων
15. Εγκυκλοπαίδεια Βικιπαίδεια, http://el.wikipedia.org/wiki/Intranet
16. Εγκυκλοπαίδεια Βικιπαίδεια: http://el.wikipedia.org/wiki/Ethernet
17. Εγκυκλοπαίδεια Βικιπαίδεια, http://el.wikipedia.org/wiki/ Πληροφοριακά συστήματα
18. Ο Τελικός Δεκάλογος για θέματα Ασφάλειας Πληροφοριακών Συστημάτων και Προστασίας Προσωπικών Δεδομένων στο Ηλεκτρονικό Επιχειρείν
19. Χ.Μπούρας ,Δίκτυα Δημόσιας Χρήσης κ διασύνδεση δικτύων Π.Σ 2006
20. Χρήστος Ι. Μπούρας Δίκτυα Δημόσιας Χρήσης και Διασύνδεση Δικτύων Πανεπιστημιακές Σημειώσεις,
21. Ιδομενέας Μανωλιτσάκης: http://www.plant-management.gr
22. Καλλιρρόη Γεωργιλά , «Αξιολόγηση επενδύσεων σε νέες τεχνολογίες βάσει παραγόντων Διοικητικής Λογιστικής: Μια πρώτη διερεύνηση των τάσεων στο Ηλεκτρονικό Εμπόριο στην Ελλάδα», Αθήνα 2003
23. CISCO, http://www.cisco.com/, Ασφάλεια δικτύου
24. Παπασωτηρίου Θεόδωρος, «Ολοκληρωμένα Πληροφοριακά Συστήματα Διαχείρισης Επιχειρησιακών Πόρων (E.R.P.)» , Πτυχιακή εργασία, Ιούνιος 2007
25. http://en.wikipedia.org/wiki/Rate_of_return
26. Γεώργιος Καραθανάσης: «Χρηματοοικονομική Διοίκηση και Χρηματιστηριακές Αγορές», Εκδόσεις Μπένου, Αθήνα 1999
27. Δρ. Φοίβη Κουντούρη, «Αξιολόγηση Επενδύσεων και Προγραμμάτων», Σεπτέμβριοςς 2008