**Α.Τ.Ε.Ι. ΜΕΣΟΛΟΓΓΙΟΥ**
**ΣΧΟΛΗ ΔΙΟΙΚΗΣΗ ΟΙΚΟΝΟΜΙΑΣ**
**ΤΜΗΜΑ ΕΦΑΡΜΟΓΩΝ ΠΛΗΡΟΦΟΡΙΚΗΣ**
**ΣΤΗ ΔΙΟΙΚΗΣΗ ΚΑΙ ΤΗΝ ΟΙΚΟΝΟΜΙΑ**

# Μελέτη σύγχρονων τεχνικών υλικού και λογισμικού σε μια μικρομεσαία επιχείρηση προτεινόμενες βελτιώσεις και επεκτάσεις τους

Επιβλέπων Καθηγητής : Καραγιάννης Γεώργιος

Υπεύθυνη Εργασίας : Σαρίδη Χριστίνα , Α.Μ. 9559

Μεσολόγγι 2006

# Πίνακας Περιεχομένων

# Πρόλογος

Στις μέρες μας για τις περισσότερες επιχειρήσεις , ανεξαρτήτως μεγέθους, η πρόσβαση στο Internet είναι αναγκαίο αν θέλουν να είναι ανταγωνιστικές. Όταν όμως μια επιχείρηση συνδέει το προσωπικό της δίκτυο στο Internet δεν προσφέρει απλά στους υπαλλήλους της πρόσβαση σε πληροφορίες και Διαδικτυακές Υπηρεσίες, αλλά επιπλέον δίνει την δυνατότητα σε εξωτερικούς χρήστες να προσεγγίσουν τις ιδιωτικές πληροφορίες της επιχείρησης.

Σκοπός της πτυχιακής εργασίας είναι η παρουσίαση της δομής του δικτύου μιας μικρομεσαίας επιχείρησης ως προς τον τρόπο λειτουργίας του δικτύου εντός και εκτός της επιχείρησης. Η παρουσίαση άλλων σύγχρονων δικτύων (Intranet, Extranet) έχει ως σκοπό να δείξει την επικοινωνία των επιχειρήσεων μεταξύ τους και αντίστοιχα την επικοινωνία των πελατών με την επιχείρηση και όλα αυτά με γνώμονα την ασφάλεια μέσα από μεθόδους προστασίας και πολιτικές ασφαλείας.

Με μια σύντομη περιγραφή κάθε κεφαλαίου, η παρούσα πτυχιακή μελετά τα παρακάτω.

Το κεφάλαιο 1 αναφέρετε στον σχεδιασμό του δικτύου που αποτελεί την βάση για την δημιουργία ενός πραγματικού δικτύου. Ο σωστός σχεδιασμός είναι απαραίτητος ούτως ώστε το δίκτυο να ικανοποιεί τις απαιτήσεις των χρηστών της διοίκησης αλλά και να συμβαδίζει με τον προϋπολογισμό. Τα τμήματα από τα οποία αποτελείτε ένα δίκτυο και την διαχείριση του δικτύου η οποία περιλαμβάνει τις εργασίες που είναι απαραίτητες για την συνεχή και σωστή λειτουργία του δικτύου.

Το κεφάλαιο 2 αναφέρετε στους σύγχρονους τύπους δικτύου ( Intranet, Extranet). Το Intranet είναι σημαντικό για τις μικρομεσαίες επιχειρήσεις όσο και το Extranet το οποίο αποτελεί κομμάτι του Intranet το οποίο μπορεί να προσεγγιστεί από πελάτες , προμηθευτές , εξωτερικούς συνεργάτες.

Το κεφάλαιο 3 αναφέρετε στα τοπικά δίκτυα και τις τοπολογίες αυτών.

Το κεφάλαιο 4 κάνει αναφορά στο Internet : τι είναι το Internet ; πως λειτουργεί ; και τα πρωτόκολλα αυτού ftp(πρωτόκολλο μεταφοράς αρχείων) e-mail ( πρωτόκολλο) κ.τ.λ.

Το κεφάλαιο 5 αποτελεί την ουσία δημιουργίας αυτής της πτυχιακής και αναφέρεται στην ασφάλεια του δικτύου , ποιες είναι οι απειλές κατά την ασφάλεια τα κακόβουλα προγράμματα καθώς και τα μέσα αποθήκευσης των πληροφοριών που είναι απαραίτητα για την διασφάλιση των πληροφοριών μιας επιχείρησης.

Το κεφάλαιο 7 αναφέρετε στις μεθόδους προστασίας.

Το κεφάλαιο 8 αναφέρεται στις πολιτικές ασφαλείας.

Το κεφάλαιο 9 κάνει αναφορά στα λειτουργικά συστήματα των Servers, ποια λειτουργικά συστήματα επικρατούν και γιατί, τα υπέρ και τα κατά αυτών και ποια από αυτά τα λειτουργικά συστήματα έχουν καθιερωθεί στις μικρομεσαίες επιχειρήσεις

Τέλος η υλοποίηση παρουσιάζει το δίκτυο μιας επιχείρησης και ενός εκπαιδευτικού ιδρύματος στην πράξη. Βλέπουμε τη δομή τους, το τρόπο προστασίας από εσωτερικές και εξωτερικές απειλές και τα προγράμματα ασφάλειας που χρησιμοποιούν.

# Κεφάλαιο 1

# Σχεδιασμός Δικτύου

## 1.1 Σχεδιασμός

Η εγκατάσταση δικτύου αποτελείται από τρία στάδια: Τον σχεδιασμό, την εγκατάσταση, και την συνεχόμενη υποστήριξη.

Το στάδιο του σχεδιασμού είναι το στάδιο της δημιουργίας δικτύου στο οποίο δίνεται η λιγότερη προσοχή. Ωστόσο, ο σωστός σχεδιασμός είναι βασικός για την επιτυχή εγκατάσταση του δικτύου. Ο σωστός σχεδιασμός είναι απαραίτητος ούτως ώστε το δίκτυο να κάνει τα ακόλουθα:

- Να ικανοποιεί τις παρούσες και μελλοντικές ανάγκες και απαιτήσεις χρηστών και διοίκησης.
- Να συμβαδίζει με το ύψος του προϋπολογισμού
- Να εγκαθίσταται με τις λιγότερες δυνατές δυσκολίες.

### Ανάγκες Ανάλυσης

Το πρώτο βήμα στο σχεδιασμό ενός δικτύου με PC είναι να αναγνωρίσετε τις βασικές ανάγκες του οργανισμού που μπορεί να ικανοποιήσει το δίκτυο. Πρέπει να εξετασθούν αρκετές και σημαντικές κατηγορίες αναγκών, όπως:

- Αποδοτικότητα : Να βρείτε τρόπους με τους οποίους το δίκτυο μπορεί να βοηθήσει τους υπαλλήλους να κάνουν τη δουλεία τους καλύτερα και πιο αποδοτικά.
- Ποιότητα :Σκεφτείτε τους τρόπους με τους οποίους οι εφαρμογές του δικτύου μπορούν να δώσουν στους πελάτες καλύτερα προϊόντα και υπηρεσίες κάτι που συνεπώς θα έχει ως αποτέλεσμα αυξημένα κέρδη.
- Λήψη Αποφάσεων: Η πιο δύσκολή δουλεία για τη διοίκηση ενός οργανισμού είναι η λήψη αποφάσεων που θα οδηγήσουν στην επιτυχία – ή την αποτυχία. Οι εφαρμογές του δικτύου μπορούν να παρέχουν στη διοίκηση περισσότερες και πιο ακριβείς πληροφορίες πάνω στις οποίες να βασίσουν τις αποφάσεις τους.
- Αντικατάσταση των Υπαρχόντων Συστημάτων: Πολλοί οργανισμοί αντικαθιστούν τους ήδη υπάρχοντες μινι-υπολογιστές και κεντρικούς υπολογιστές με δίκτυα από PC για να πετύχουν μεγαλύτερη απόδοση και /ή οικονομία.

Μια σωστή ανάλυση αναγκών απαιτεί κάποια προσπάθεια, αλλά όταν αντισταθμίζεται με τα πιθανά πλεονεκτήματα τα οποία μπορεί να εξασφαλίσει ένα σωστά εγκαταστημένο δίκτυο, είναι εμφανές ότι πρόκειται για κάτι στο οποίο αξίζει να αφιερώσετε λίγο παραπάνω χρόνο. Το πρώτο βήμα στην ανάλυση αναγκών είναι να πάρετε μερικές άτυπες πληροφοριακές συνεντεύξεις από ένα αντιπροσωπευτικό δείγμα των ατόμων που μπορεί να επηρεασθούν από το δίκτυο. Σε αυτό το σημείο, προσπαθείτε να καταλάβετε τα ακόλουθα:

- Ποια είναι η δουλειά καθενός
- Ποίες εργασίες συμπεριλαμβάνει κάθε μία από αυτές τις δουλείες
- Τι πληροφορίες χρειάζονται για να κάνουν αυτές τις δουλείες σωστά
- Τα εμπόδια που μπορεί να τους αποτρέψουν από την εκτέλεση της δουλειάς τους

Βοηθάει, επίσης, να πληροφορήσετε αυτούς από τους οποίους παίρνετε συνέντευξη σχετικά με τις δυνατότητες του δικτύου από PC. Εφόσον καταλάβουν αυτές τις δυνατότητες, θα μπορέσουν να ρίξουν μια ματιά στις δουλειές τους και να βρουν τρόπους με τους οποίους μπορούν να αποκομίσουν οφέλη από την επικοινωνία μέσω δικτύου. Για αυτό το σκοπό, θα ήταν χρήσιμο να προγραμματίσετε συμπληρωματικές συνεντεύξεις κάποια στιγμή μετά τις αρχικές για να δώσετε σε αυτούς με τους οποίους συζητάτε την δυνατότητα να σκεφτούν τα πιθανά οφέλη.

Τώρα ήρθε η ώρα να αρχίσετε να οργανώνετε τις πληροφορίες που συγκεντρώσατε από τις άτυπες συνεντεύξεις. Στόχος μας κατά την διάρκεια αυτής της διαδικασίας είναι η κατάρτιση μιας λίστας με τις απαιτήσεις του δικτύου που θα βοηθήσουν περισσότερο τον οργανισμό. Μην ξεχάσετε να ψάξετε για τυχόν προβλήματα, όπως έλλειψη επικοινωνίας ανάμεσα στα τμήματα ή έλλειψη έγκυρης πληροφόρησης. Συγκρίνετε τη λίστα με τις των χρηστών με τις δυνατότητες που μπορεί να προσφέρει το δίκτυο και καταρτίστε μία νέα λίστα με τις δυνατότητες που θα θέλατε να έχει επιπλέον το νέο δίκτυο.

Το επόμενο βήμα στην ανάλυση των αναγκών είναι να καθορίσετε ποιες δυνατότητες του δικτύου θα έχουν περισσότερα οφέλη για την εταιρεία με το λιγότερο δυνατό κόστος. Αναλύστε κάθε σημείο της λίστας με τις δυνατότητες που θα θέλατε, για να καθορίσετε το κόστος της εγκατάστασης αυτής της δυνατότητας σε σύγκριση με τα οφέλη που θα έχει. Προσπαθήστε να καταρτίσετε λίστα με τις δυνατότητες που θα αποφέρουν τα μεγαλύτερα δυνατά οφέλη με το λιγότερο δυνατό κόστος. Θα ήταν χρήσιμο να διανέμεται την λίστα στους μελλοντικούς χρήστες για να ελέγξετε αν τελικά η ανάλυσή σας ήταν ακριβής.

## Σχεδιασμός Συστήματος

Το επόμενο βήμα είναι να φτιάξετε ένα δοκιμαστικό σχέδιο του δικτύου για να εκτιμήσετε το κόστος . Ακολουθούν μερικές προτάσεις:

- Εξισορρόπηση παρόντων και μελλοντικών αναγκών. Όποτε μπορείτε, 'αγοράστε' μελλοντική ευελιξία όταν συνεπάγεται μόνο μικρό πρόσθετο κόστος.

- Ερευνήστε και χρησιμοποιήστε τα υπάρχοντα μέσα. Επικοινωνήστε με την τηλεφωνική σας εταιρία για να εξακριβώσετε αν υπάρχουν καλωδιώσεις που δεν έχουν χρησιμοποιηθεί για το τηλέφωνο και μπορούν να χρησιμοποιηθούν με το δίκτυο.
- Τίποτα δεν αντικαθιστά την πείρα. Βεβαιωθείτε ότι κάποιος από την ομάδα σχεδιαστών σας έχει πραγματικά εγκατάσταση δικτύου. Αν είναι απαραίτητο, προσλάβετε ένα έμπειρο σύμβουλο. Μια μικρή επένδυση στην αρχή μπορεί να σας κάνει οικονομία και να σας σώσει από μελλοντικές απογοητεύσεις.
- Αν είναι δυνατόν, αποκτήστε όλο τον ηλεκτρονικό εξοπλισμό, το λογισμικό και υπηρεσίες από κάποιο πωλητή, κατά προτίμηση κάποιον που ειδικεύεται στην εγκατάσταση δικτύου. Βραχυπρόθεσμα, είναι πιο οικονομικό να αγοράζετε περιστασιακά ηλεκτρονικό εξοπλισμό, λογισμικό και υπηρεσίες ξεχωριστά από την πιο φθηνή πηγή. Ωστόσο, αυτή η οικονομία μπορεί να ωχριά μπροστά στην απογοήτευση σας όταν κάτι θα πάει στραβά, καθώς το μοντέρνο δίκτυο αποτελείται από πολλά τμήματα και αν το καθένα έχει αγοραστεί από διαφορετικό πωλητή, ο ένας θα κατηγορεί τον άλλο ως πηγή του προβλήματος. Αν υπάρχει μόνο ένας πωλητής, τότε υπάρχει μόνο ένα άτομο για να κατηγορήσετε.
- Βεβαιωθείτε ότι οι εκτιμήσεις περιλαμβάνουν το κόστος όλων των εργασιών πέρα από τον ηλεκτρονικό εξοπλισμό και το λογισμικό. Το κόστος μερικών από αυτές, όπως το κόστος για την εγκατάσταση και την εκπαίδευση, υπολογίζονται πιο εύκολα. Το κόστος άλλων, όπως η προσωρινή μείωση της παραγωγικότητας όσο οι χρήστες προσπαθούν να συνηθίζουν τον καινούργιο τρόπο δουλειάς, είναι πιο δύσκολο να υπολογιστεί, αν και οπωσδήποτε θα επηρεάσει τον οργανισμό.
- Καθορίστε το προσωπικό που απαιτείται για να λειτουργεί το δίκτυο μετά την εγκατάσταση. Και πάλι, ένας έμπειρος ειδικός στη δημιουργία δικτύων θα είναι πολύ σημαντικός για αυτή τη δουλειά.

## Δικαιολόγηση του Κόστους

Ο στόχος μια επιχείρησης είναι να βγάλει χρήματα. Το δίκτυο από PC, όπως και όλα τα άλλα, πρέπει να συνεισφέρει σε αυτή την προσπάθεια. Τα οφέλη του δικτύου πρέπει να αυξήσουν τα κέρδη αρκετά ώστε να δικαιολογηθεί η επένδυση στην εγκατάσταση του. Μετά από τον σχεδιασμό, τις εκτιμήσεις και τις συναντήσεις, η δικαιολόγηση του κόστους πάντα θα απαιτείται για την περαιτέρω χρηματοδότηση του δικτύου.

## Υλοποίηση

Η υλοποίηση του δικτύου διευκολύνεται με το σωστό σχεδιασμό. Από την άλλη πλευρά, η έλλειψη του σχεδιασμού εξασφαλίζει το χάος και την απογοήτευση. Είναι καλύτερο να εισάγετε το δίκτυο και τις εφαρμογές του αργά και προσεκτικά. Κατ αυτό τον τρόπο, όταν θα εμφανίζονται προβλήματα, θα μπορείτε εύκολα να εξακριβώνετε από που προέρχονται. Αρχίστε προσθέτοντας μια εφαρμογή, όπως τον επεξεργαστή κειμένου, και δοκιμάστε την. Εφόσον βεβαιωθείτε ότι λειτουργεί, επιτρέψτε σε μικρή ομάδα ατόμων να τη 'δοκιμάσουν'. Μόνο εφόσον περάσει και αυτές τις δοκιμές πρέπει να τη διαθέσετε σε κοινή χρήση. Προσπαθήστε να κάνετε την εγκατάσταση όσο το δυνατόν περισσότερο απρόσβλητη σε ανεπιθύμητες παρεμβάσεις δίνοντας στους χρήστες πρόσβαση μόνο στα

αρχεία που χρειάζονται. Κοινά δεδομένα και προγράμματα αρχείων που δεν πρέπει να μετατρέπονται από τους τελικούς χρήστες μπορούν και πρέπει να προστατεύονται από το λειτουργικό σύστημα του δικτύου.

## Φυσική Εγκατάσταση

Η εγκατάσταση των καλωδίων είναι το πρώτο βήμα της φυσικής εγκατάστασης του δικτύου. Βεβαιωθείτε ότι ο εργολάβος για τις καλωδιώσεις είναι έμπειρος στην εγκατάσταση του συγκεκριμένου καλωδίου που χρησιμοποιείται. Ακόμα και η τηλεφωνική σας εταιρία μπορεί να είναι συχνά καλή βοήθεια για την εγκατάσταση καλωδιώσεων με καλώδιο συνεστραμμένων ζευγών χωρίς προστατευτικό.

Το επόμενο βήμα είναι η εγκατάσταση εξυπηρετητή αρχείων και ενός τερματικού. Δοκιμάστε επισταμένως τις επικοινωνίες χρησιμοποιώντας τις πρωταρχικές εφαρμογές. Προσθέστε δεύτερο τερματικό και δοκιμάστε για να δείτε τι γίνεται όταν δύο χρήστες αποκτούν συγχρόνως πρόσβαση στις εφαρμογές. Αφού βεβαιωθείτε ότι το σύστημα δουλεύει σωστά, ήρθε η ώρα να προσθέσετε τα υπόλοιπα τερματικά.

## Εκπαίδευση των Χρηστών

Η εκπαίδευση των χρηστών είναι ζωτικής σημασίας για την επιτυχία ενός δικτύου από PC. Η εγκαινίαση ενός εντατικού προγράμματος εκπαίδευσης θα συμβάλλει στο να εκμεταλλεύονται σωστά τις δυνατότητες και τις εφαρμογές του δικτύου οι χρήστες του. Η έλλειψη της εκπαίδευσης θα έχει ως αποτέλεσμα τα ακόλουθα:

- Ανεπαρκή χρήση των εφαρμογών και των δυνατοτήτων
- Απογοητευμένοι και εκνευρισμένοι χρήστες
- Ελλιπής χρήση του προσωπικού υποστήριξης δικτύου. (Αντί να συντηρούν , να ανιχνεύουν βλάβες και να προσθέτουν νέες εφαρμογές, θα χάνουν πολύ χρόνο εξηγώντας τις λειτουργίες του δικτύου σε κάθε χρήστη.)

Ακολουθούν μερικές γενικές προτάσεις για να διευκολύνετε το 'πέρασμα' των υπαλλήλων στο δίκτυο:

- Ετοιμάστε ένα εγχειρίδιο όπου θα περιγράφεται η χρήση του συστήματος του δικτύου σας και των εφαρμογών του. Το εγχειρίδιο να βρίσκεται μέσα στο δίκτυο ώστε όλοι οι χρήστες να έχουν πρόσβαση σε αυτό και τις βελτιώσεις του.
- Πραγματοποιήστε επίσημες εκπαιδευτικές συναντήσεις όπου θα περιγράφονται οι λειτουργίες και τα χαρακτηριστικά του δικτύου. Αυτό έχει δύο πλεονεκτήματα: Οι χρήστες θα μάθουν πως να χρησιμοποιούν το σύστημα και ίσως παρουσιάσουν και ιδέες πάνω στο πώς μπορεί να χρησιμοποιηθεί πιο αποδοτικά το δίκτυο.
- Πραγματοποιήστε συχνές ανεπίσημες συναντήσεις όπου οι χρήστες μπορούν να κάνουν ερωτήσεις, προτάσεις, κλπ. Έτσι οι χρήστες θα βρίσκουν απαντήσεις στα ερωτήματα τους και ο διαχειριστής θα καταλαβαίνει καλύτερα πώς χρησιμοποιείται το δίκτυο. Γνωρίζοντας πως χρησιμοποιείται το δίκτυο, από την άλλη, θα μπορέσει

να ρυθμίσει καλύτερα τις διαδικασίες του δικτύου και να προσθέσει νέα χαρακτηριστικά και εφαρμογές.

- Βρείτε ένα σύστημα για την εκπαίδευση των νέων χρηστών. Οι μεγάλοι οργανισμοί ίσως απαιτούν επίσημα μαθήματα, ενώ οι μικτότεροι μπορεί να επιλέξουν κάτι λιγότερο επίσημο.

## Ανίχνευση Βλαβών

Ένα σωστά σχεδιασμένο δίκτυο υπολογιστών δε θα παθαίνει βλάβες πολύ συχνά. Όταν θα παθαίνει βλάβες, η δυνατότητα να επιδιορθωθούν ώστε το δίκτυο να συνεχίσει τη δουλεία του είναι ζωτικής σημασίας για την επιχείρηση. Ο καλύτερος τρόπος για τον εντοπισμό βλαβών είναι σωστός σχεδιασμός του δικτύου. Ο σωστός σχεδιασμός του συστήματος μπορεί να αποτρέψει κάποια βλάβη του δικτύου. Στην σπάνια περίπτωση βλάβης ενός σωστά σχεδιασμένου δικτύου, το πρόβλημα μπορεί να ανιχνευτεί αμέσως και να αντιμετωπιστεί μέσα σε μερικά λεπτά.

Όταν παρουσιαστεί βλάβη, η λύση του προβλήματος εξαρτάται από το διαχωριστή του δικτύου. Επειδή η βλάβη μπορεί να έχει προκληθεί από οποιοδήποτε μέρος του δικτύου, ο διαχειριστής πρέπει να γνωρίζει όλες τις απόψεις του δικτύου και τους τρόπους με τους οποίους χρησιμοποιείται. Συχνά, είναι χρήσιμο για το διαχειριστή του δικτύου να μπορεί να καλέσει μια ομάδα χρηστών, ειδικών σε διάφορες εφαρμογές, για να βοηθήσει στην ανίχνευση βλαβών που προκαλούν προβλήματα στους τελικούς χρήστες.

## 1.2 Τα Τμήματα Ενός Δικτύου

Ένα δίκτυο αποτελείται από πολλά τμήματα ηλεκτρονικού εξοπλισμού και λογισμικού πολύπλοκα συνδεδεμένα. Τα συγκεκριμένα τμήματα που χρησιμοποιούνται για κάθε δίκτυο εξαρτώνται από τι πρέπει να πετύχει αυτό το δίκτυο:Το πρώτο βήμα για τον σχεδιασμό ενός δικτύου είναι να καθορίσετε τον αριθμό των πιθανών χρηστών και τις πιθανές του εφαρμογές.

### Τερματικά

Τα τερματικά (θέσεις εργασίας-workstations)είναι μικρό-υπολογιστές που χρησιμοποιούνται άμεσα από τελικούς χρήστες οι οποίοι εργάζονται με αυτά. Πρόκειται για υπολογιστές που τρέχουν εφαρμογές όπως επεξεργασία κειμένου, λογιστικά φύλλα και λογισμικό για λογιστήριο. Ένα δίκτυο μπορεί να αποτελείται από ένα μέχρι αρκετές χιλιάδες τερματικά.

Κάθε τερματικό διαφέρει από ένα κανονικό μεμονωμένο PC στο γεγονός ότι το τερματικό διαθέτει επιπροσθέτως τον ηλεκτρονικό εξοπλισμό και το λογισμικό του δικτύου. Ο ηλεκτρονικός εξοπλισμός, γνωστός ως κάρτα διασύνδεσης δικτύου(network interface card- NIC) επιτρέπει στο δίκτυο να συνδεθεί φυσικά με τις καλωδιώσεις του δικτύου. Το λογισμικό, γνωστό ως το "κέλυφος " του δικτύου, λέει στον υπολογιστή πώς να χρησιμοποιήσει το δίκτυο για να αποκτήσει πρόσβαση σε μέσα κοινής χρήσης, όπως οδηγούς δίσκων, εκτυπωτές και διαμορφωτές / αποδιαμορφωτές (modem).Τα υπόλοιπα τμήματα του δικτύου ( εξυπηρετητές, καλωδιώσεις και ούτω καθεξής)υπάρχουν μόνο για να υποστηρίζουν τις δραστηριότητες των τερματικών.

### Εξυπηρετητής Αρχείων

Για τον χρήστη ,η έκφραση "εξυπηρετητής αρχείων(file server)είναι απλά ένα περίεργο όνομα για τον οδηγό δίσκου του δικτύου που μοιράζονται οι χρήστες .

Πρακτικά , ο εξυπηρετητής αρχείων είναι ένας υπολογιστής με έναν ή περισσότερους σκληρούς δίσκους μεγάλης χωρητικότητας .Οι περισσότεροι εξυπηρετητές αρχείων είναι απλοί PC που τρέχουν ένα ειδικό λογισμικό που τους επιτρέπει να λειτουργούν ως εξυπηρετητές αρχείων. Οι μίνι-υπολογιστές και οι κεντρικοί υπολογιστές μπορούν, επίσης , να λειτουργούν ως εξυπηρετητές αρχείων.

Ένα δίκτυο μπορεί να διαθέτει ένα ή περισσότερους εξυπηρετητές αρχείων. Σε ορισμένα δίκτυα, ένας προσωπικός υπολογιστής που χρησιμοποιείται ως εξυπηρετητής αρχείων μπορεί να λειτουργεί μόνο ως εξυπηρετητής αρχείων και όχι και ως τερματικό συγχρόνως. Αυτός λέγεται αφιερωμένος εξυπηρετητής αρχείων(dedicated).Άλλα δίκτυα υποστηρίζουν το σύστημα κοινής χρήσης μέσων άκρη με άκρη(peer -to –peer), στο οποίο τα τερματικά μπορούν να λειτουργούν, επίσης, και ως εξυπηρετητές του δικτύου.

## Εξυπηρετητής Βάσης Δεδομένων

Ο εξυπηρετητής βάσης δεδομένων αποτελεί ένα πολύ ενδιαφέρον τμήμα της τεχνολογίας δικτύων προσωπικών υπολογιστών. Μπορούμε να τον παρομοιάσουμε με εξυπηρετητή αρχείων ειδικευμένο στις βάσεις δεδομένων, δηλαδή αποτελεί ειδικό κεντρικό τμήμα αποθήκευσης για μία ή περισσότερες βάσεις δεδομένων.(Μερικά παραδείγματα εφαρμογών για βάσεις δεδομένων περιλαμβάνουν καταχωρήσεις για λογισμικά, αποθεματικά και παραγγελίες.)

Πριν τη δημιουργία του εξυπηρετητή βάσης δεδομένων, ο μόνος τρόπος με τον οποίο μεγάλες ομάδες χρηστών μπορούσαν να έχουν ταυτόχρονη πρόσβαση στην ίδια βάση δεδομένων ήταν κυρίως μέσω μίνι-υπολογιστών και κεντρικών υπολογιστών. Χρησιμοποιώντας εξυπηρετητές βάσης δεδομένων, οι δικτυωμένοι PC μπορούν να λειτουργούν ως βάσεις δεδομένων στην ίδια απόδοση, ή και σε υψηλότερη , με αυτή των κεντρικών υπολογιστών.

Ένα δίκτυο μπορεί να έχει έναν ή περισσότερους εξυπηρετητές βάσης δεδομένων. Είναι συνήθως αφιερωμένοι στην εργασία τους και συνεπώς δε χρησιμοποιούνται και ως τερματικά. Όπως και οι εξυπηρετητές αρχείων, οι εξυπηρετητές βάσης δεδομένων είναι συνήθως PC που τρέχουν ένα ειδικό λογισμικό που τους επιτρέπει να λειτουργούν ως εξυπηρετητές βάσης δεδομένων.

## Εξυπηρετητής Εκτύπωσης

Ο εξυπηρετητής εκτύπωσης είναι ένας μικρό-υπολογιστής που ελέγχει τις δραστηριότητες ενός ή περισσοτέρων εκτυπωτών που χρησιμοποιούνται από πολλούς χρήστες μέσω του δικτύου. Ένα δίκτυο μπορεί να έχει έναν ή περισσότερους εξυπηρετητές εκτύπωσης. Όπως και οι εξυπηρετητές αρχείων, οι εξυπηρετητές εκτύπωσης μπορούν να είναι αφοσιωμένοι στην εργασία τους ή και να χρησιμοποιούνται είτε ως τερματικά είτε ως εξυπηρετητές αρχείων, ανάλογα με τις διάφορες συνθήκες. Μερικοί εκτυπωτές για δίκτυο κατασκευάζονται με ενσωματωμένο εξυπηρετητή εκτύπωσης, κάτι που τους επιτρέπει να συνδεθούν αμέσως με το δίκτυο.

## Κάρτα Διασύνδεσης Δικτύου(NIC)

Οι περισσότεροι προσωπικοί υπολογιστές δεν μπορούν να συνδεθούν στο δίκτυο έτσι όπως είναι. Αυτό σημαίνει ότι πρέπει να γίνει εγκατάσταση κάρτας διασύνδεσης δικτύου. Η κάρτα αυτή είναι τυπωμένο πλαίσιο κυκλωμάτων το οποίο συνδέεται μέσω μιας σχισμής του τερματικού και συνεπώς θεωρείται μέρος του ηλεκτρονικού εξοπλισμού του δικτύου. Κάθε κάρτα διασύνδεσης διαθέτει έναν ή δύο ειδικούς συνδετήρες για να συνδέεται με τις καλωδιώσεις του δικτύου. Κάθε κάρτα διασύνδεσης πρέπει να αντιστοιχεί στο ίδιο πρωτόκολλο ηλεκτρονικού εξοπλισμού στο οποίο αντιστοιχούν και οι άλλες κάρτες (σε άλλους μικρο-υπολογιστές) με τις οποίες συνδέεται μέσω των καλωδιώσεων.

Το πρωτόκολλο ηλεκτρονικού εξοπλισμού αναφέρεται στο φυσικό τρόπο με τον οποίο πραγματοποιείται η επικοινωνία μεταξύ των τμημάτων του δικτύου. Το πρωτόκολλο ηλεκτρονικού εξοπλισμού είναι ξεκάθαρο σε κάθε τελικό χρήστη. Παραδείγματα, πρωτοκόλλου ηλεκτρονικού εξοπλισμού περιλαμβάνουν το Ethernet, το ARCnet και το Token Ring.

## Λειτουργικό Σύστημα Δικτύου

Λειτουργικό σύστημα δικτύου είναι το γενικό όνομα που δίνεται σε όλο το λογισμικό του δικτύου το οποίο είναι άμεσα υπεύθυνο για τις λειτουργίες του δικτύου. Κάθε μικρο-υπολογιστής που χρησιμοποιείται ή χρησιμοποιεί το δίκτυο θα τρέξει κάποιο είδος λογισμικού δικτύου σε συνδυασμό με το σύνηθές του λειτουργικό σύστημα(σχεδόν πάντα το MS-DOS).Το Novell NetWare αποτελεί παράδειγμα λειτουργικού συστήματος δικτύου. Μερικά συνηθισμένα λειτουργικά συστήματα περιλαμβάνουν ενσωματωμένο λειτουργικό σύστημα δικτύου, με αποτέλεσμα να μην είναι αναγκαίο επιπλέον λογισμικό. Το λογισμικό που απλά αξιοποιεί το δίκτυο, όπως το λογισμικό επεξεργασίας κειμένων, δε θεωρείται γενικά λογισμικό του δικτύου. Θεωρείται κυρίως λογισμικό εφαρμογών.

## Γέφυρα

Η γέφυρα (bridge) είναι ένας υπολογιστής με ειδικό λογισμικό και ηλεκτρονικό εξοπλισμό που επιτρέπει σε δύο ή περισσότερα δίκτυα που τρέχουν το ίδιο λειτουργικό σύστημα (αν και συχνά και με διαφορετικό ηλεκτρονικό εξοπλισμό δικτύου) να επικοινωνούν. Για παράδειγμα , μια γέφυρα μπορεί να επιτρέψει σε ένα σύνολο PC με κάρτες διασύνδεσης ARCnet να επικοινωνήσουν με ένα δεύτερο σύνολο PC που χρησιμοποιούν IBM κάρτες διασύνδεσης Token ring.

Οι μικρό-υπολογιστές γέφυρες μπορούν να είναι αφοσιωμένοι στην εργασία τους ή μπορούν, επίσης, να λειτουργούν ως εξυπηρετητές ή ως τερματικά, ανάλογα με το λειτουργικό σύστημα και τις απαιτήσεις σας, όπως ο αριθμός συνδεδεμένων χρηστών στο δίκτυο και τα συγκεκριμένα πρωτόκολλα που πρέπει να "γεφυρωθούν" .

## Πύλη Σύζευξης

Η πύλη (gateway) είναι ένας υπολογιστής με ειδικό λογισμικό και ηλεκτρονικό εξοπλισμό που επιτρέπει σε δύο ή περισσότερα δίκτυα που τρέχουν διαφορετικά λειτουργικά συστήματα(και ίσως διαθέτουν και διαφορετικό ηλεκτρονικό εξοπλισμό) να επικοινωνούν. Θα χρησιμοποιούσαμε πύλη, για παράδειγμα, για να επιτρέψουμε σε PC που τρέχουν με το λογισμικό δικτύου NOS να επικοινωνήσουν με κεντρικούς υπολογιστές DEC που τρέχουν το λειτουργικό σύστημα VMS είναι συγχρόνως και λειτουργικό σύστημα και λειτουργικό σύστημα δικτύου)

Οι μικρό-υπολογιστές πύλες μπορούν να είναι αφοσιωμένοι στην εργασία τους ή μπορούν να λειτουργούν είτε ως τερματικά είτε ως εξυπηρετητές, ανάλογα με το

λειτουργικό σύστημα και τις απαιτήσεις σας, όπως τον αριθμό συνδεδεμένων χρηστών με το δίκτυο ή τα συγκεκριμένα λειτουργικά συστήματα δικτύου με τα οποία θέλετε να συνδεθείτε.

## Καλωδίωση

Η καλωδίωση είναι απλά τα καλώδια που συνδέουν τους υπολογιστές με το δίκτυο. Αν και η εγκατάσταση μερικών καλωδίων μπορεί_να φαίνεται απλή, ο σχεδιασμός της τοπολογίας της καλωδίωσης (διαμόρφωση) μπορεί να αποδειχθεί μία από τις πιο απαιτητικές και σημαντικές εργασίες που περιλαμβάνει ο σχεδιασμός δικτύου. Η εγκατάσταση των καλωδίων μπορεί τελικά να καλύψει μέχρι και το μισό του κόστους που καλύπτει όλο το δίκτυο.

## Κατανεμητής

Ο εξυπηρετητής (HUB) είναι απλά ένας μηχανισμός ο οποίος συνδέει πρακτικά τα καλώδια μεταξύ τους. Η IBM ονομάζει τους μηχανισμούς αυτούς αλλιώς, προτιμώντας να τους λέει Μονάδα Πρόσβασης Πολλαπλών Τερματικών (Multistation Access Units-MAU).

## Εξυπηρετητής Μεμακρυσμένης Πρόσβασης

Ο εξυπηρετητής μεμακρυσμένης πρόσβασης επιτρέπει στους PC, οπουδήποτε στον κόσμο και αν βρίσκονται, να έχουν πρόσβαση σε δίκτυο τοπικής περιοχής μέσω τηλεφώνου. Ένας μόνο εξυπηρετητής μεμακρυσμένης πρόσβασης μπορεί να υποστηρίξει μία ή και περισσότερες μεμακρυσμένες συνδέσεις ταυτόχρονα.

## Εξυπηρετητής Διαμορφωτή / Αποδιαμορφωτής

Ο εξυπηρετητής διαμορφωτή/ αποδιαμορφωτή (_modem) επιτρέπει στους χρήστες του δικτύου να μοιράζονται διαμορφωτές/ αποδιαμορφωτές. Αυτοί οι διαμορφωτές / αποδιαορφωτές μπορούν να χρησιμοποιηθούν για να επιτευχθεί πρόσβαση σε μεμακρυσμένες βάσεις δεδομένων και σε άλλα τοπικά δίκτυα υπολογιστών μέσω τηλεφωνικών γραμμών. Οι εξυπηρετητές διαμορφωτή/ αποδιαμορφωτή μπορούν να υποστηρίζουν ταυτόχρονα ένα ή περισσότερους κοινούς διαμορφωτές / αποδιαμορφωτές.

## Εξυπηρετητή φαξ

Η μηχανή τηλεμοιοτύπου (φαξ) αποτελεί σήμερα βασικό στοιχείο της δουλειάς γραφείου. Τα μηχανήματα φαξ μας επιτρέπουν να στείλουμε ή να λάβουμε αντίγραφα κειμένων ή εικόνων από και προς οποιοδήποτε μέρος του κόσμου στο οποίο υπάρχει τηλέφωνο και συσκευή φαξ.

Ο εξυπηρετητής φαξ επιτρέπει στους χρήστες ενός δικτύου να μοιράζονται μια συσκευή φαξ. Οι συσκευές φαξ που είναι ενσωματωμένες σε υπολογιστές δίνουν τη δυνατότητα στους χρήστες να στέλνουν τα κείμενα που έχουν επεξεργαστεί στο πρόγραμμα επεξεργασίας κειμένου απευθείας από τον υπολογιστή, χωρίς να χρειάζεται να τα εκτυπώσουν πρώτα και μετά να τα περάσουν στη συσκευή του φαξ. Το φαξ που λαμβάνετε μπορούν να τυπώνονται σε συγκεκριμένο εκτυπωτή. Το μειονέκτημα των εξυπηρετητών φαξ είναι ότι αν τα κείμενα που στέλνονται δεν έχουν γραφτεί σε υπολογιστή πρέπει να σκανάρονται κατά κάποιο τρόπο όταν θα περνούν στο υπολογιστή.

## 1.3 Διαχείριση Δικτύου

Το δίκτυο υπολογιστών θεωρείται συχνά συλλογή ηλεκτρονικού εξοπλισμού που συνεργάζεται για να βοηθήσει τους τελικούς χρήστες να εκτελέσουν τις εργασίες τους. Ένα ακόμα στοιχείο είναι ζωτικής σημασίας για τη λειτουργία του δικτύου. Η διαχείριση του δικτύου. Η επιδεξιότητα με την οποία οργανώνεται και εκτελείται η διαχείριση του δικτύου ακριβώς όσο και η επιλογή του ηλεκτρονικού εξοπλισμού και του λογισμικού.

Η διαχείριση του δικτύου περιλαμβάνει τις εργασίες που είναι απαραίτητες για τη συνεχή και σωστή λειτουργία του δικτύου. Σε ένα τέλειο κόσμο, ένα δίκτυο θα έκανε οτιδήποτε του ζητούσαν οι τελικοί χρήστες, άψογα, 24 ώρες το 24ωρο, κάθε μέρα του χρόνου. Στον πραγματικό κόσμο, το καλύτερο που μπορούμε να ζητήσουμε από ένα δίκτυο είναι να εκτελεί τις συγκεκριμένες του λειτουργίες με τις λιγότερες δυνατές διακοπές.

Ανάμεσα στις εργασίες που θα πρέπει να γίνονται για τη διαχείριση του δικτύου είναι οι ακόλουθες:

- Διατήρηση της λειτουργίας του δικτύου για όλους τους χρήστες
- Ενημέρωση των χρηστών του δικτύου σχετικά με το τι μπορούν να κάνουν και πώς μπορούν να το πετύχουν
- Πρόσθεση δυνατοτήτων στο δίκτυο
- Εκπλήρωση των απαιτήσεων της διοίκησης
- Εκπλήρωση των απαιτήσεων των τελικών χρηστών
- Ικανοποίηση των χρηστών που εκνευρίζονται όταν το δίκτυο δεν μπορεί να κάνει αυτό που ήθελαν
- Διαβεβαίωση ότι υπάρχουν αντίγραφα ασφαλείας των δεδομένων που εισάγονται ούτως ώστε να αποκατασταθούν εύκολα σε περίπτωση που το δίκτυο 'κρεμάσει'.

Συχνά δε δίνεται η πρέπουσα σημασία στην πλευρά της διαχείρισης του δικτύου που αφορά στις ανθρώπινες σχέσεις. Ξεχνούμε συχνά ότι οι τελικοί χρήστες έχουν σχέση με τους διαχειριστές, όταν κάτι δεν δουλεύει σωστά, πράγμα που έχει σαν αποτέλεσμα ο τελικός χρήστης να είναι εκνευρισμένος και αναστατωμένος. Είναι, επίσης, σημαντικό ο διαχειριστής του δικτύου να μπορεί να ικανοποιεί τον τελικό χρήστη και πέρα από τη διόρθωση και την εξήγηση της τεχνικής δυσκολίας.

Οι διάφοροι οργανισμοί μπορεί να διαθέτουν διαφορετικές στρατηγικές σχετικά με το πώς οργανώνεται η διαχείριση δικτύου. Οι μικρότεροι οργανισμοί εφαρμόζουν συχνά ένα πιο 'ανεπίσημο' τρόπο προσέγγισης του θέματος της διαχείρισης, διανέμοντας τις διάφορες εργασίες ως μέρος της δουλειάς αρκετών ατόμων. Οι μεγαλύτεροι οργανισμοί διαθέτουν συνήθως ένα ή περισσότερα άτομα των οποίων η δουλεία έχει άμεση σχέση με τη διατήρηση του δικτύου. Η απόφαση του πώς διανέμονται οι εργασίες της διαχείρισης δεν είναι τόσο σημαντική όσο η εξασφάλιση της συνεχούς εκτέλεσης τους.

**Αλλαγή της Διαμόρφωσης του Δικτύου**

Το μόνο σίγουρο πράγμα σε αυτόν τον κόσμο είναι οι αλλαγές. Καθώς περνάει ο καιρός ,τα δίκτυα αλλάζουν. Μια από τις δουλειές του διαχειριστή του δικτύου είναι η 'διαχείριση' αυτών των αλλαγών ούτως ώστε να επιτυγχάνεται η μεγαλύτερη δυνατή λειτουργικότητα του δικτύου και ικανοποίηση του χρήστη. Μερικά από αυτά που πρέπει να εξισορροπηθούν όταν γίνονται αλλαγές στο δίκτυο περιλαμβάνουν τα παρακάτω:

- Οι αλλαγές που πρόκειται να γίνουν
- Οι πιθανές δυσκολίες για τους τελικούς χρήστες όσο καιρό θα υλοποιούν αυτές τις αλλαγές
- Το αποτέλεσμα αυτών των αλλαγών στο πώς οι χρήστες επηρεάζονται στο χειρισμό των τερματικών τους
- Πως οι αλλαγές θα επηρεάσουν τα μελλοντικά σχέδια για το δίκτυο

# Κεφάλαιο 2

# Σύγχρονοι τύποι Δικτύων

## Εισαγωγή

Το Internet δεν αποτελεί πλέον μία κλειστή κοινωνία χωρίς επικοινωνία με τον έξω κόσμο. Είναι τόσο στενά συνδεδεμένο με τον τρόπο που ζούμε και εργαζόμαστε και γίνεται ολοένα και περισσότερο κάθε στιγμή που περνά. Στην εργασία, στην ψυχαγωγία, στα ψώνια, στην εύρεση πληροφοριών, το Internet γίνεται ολοένα και περισσότερο τμήμα της καθημερινής μας ζωής.

Το Internet μπορεί να έχει τις ρίζες του στο στρατό και την ακαδημαϊκή κοινότητα, αλλά η δραματική του ανάπτυξη οφείλεται σε μεγάλο βαθμό στις επιχειρήσεις και τους καταναλωτές. Το Internet μετατρέπεται σε ένα από τα σημαντικότερα μέρη επιχειρηματικών δραστηριοτήτων στο οποίο εκατοντάδες δισεκατομμύρια δολαρίων αγαθών και υπηρεσιών θα πωλούνται και θα αγοράζονται ετησίως.

Χιλιάδες επιχειρήσεις χρησιμοποιούν ήδη το Internet για να διαθέτουν και να πωλούν τα προϊόντα τους και πολλοί άνθρωποι προτιμούν να ψωνίζουν μέσω του Internet παρά να επισκέπτονται τα καταστήματα λιανικής. Μπορούμε να χρησιμοποιήσουμε το Internet για να δούμε καταλόγους προϊόντων και να πραγματοποιήσουμε online αγορές, να αγοράσουμε και να πουλήσουμε μετοχές ή ακόμη και να λάβουμε μέρος σε online δημοπρασίες. Οι εταιρίες προχωρούν όχι μόνο στην online πώληση αγαθών αλλά και στη μεταβίβαση αυτών των συναλλαγών στα εσωτερικά υπολογιστικά συστήματα κοστολόγησης που διαθέτουν.

## 2.1 Τα Intranets

Σε μοία σύγχρονη επιχείρηση υπάρχουν διασκορπισμένες διάφορες πηγές πληροφοριών, όπως αρχεία, βάσεις δεδομένων, συστήματα και φυσικά μη αρχειοθετημένα στοιχεία (έγγραφα, εταιρικά νέα, εγκύκλιοι, εγχειρίδια, εκπαιδευτικό και πληροφοριακό υλικό για προϊόντα και υπηρεσίες, κείμενα περιγραφής εσωτερικών διαδικασιών, ανακοινώσεις, φόρμες αιτήσεων, τηλεφωνικοί κατάλογοι κλπ). Από την άλλη, εργαζόμενοι και διοικητικά στελέχη διάφορων αρμοδιοτήτων καλούνται να λειτουργήσουν παραγωγικά και να συντελέσουν στη λήψη καίριων αποφάσεων για την πορεία της επιχείρησης, αντιμετωπίζοντας συρρέοντες όγκους διάσπαρτης και αδόμητης πληροφορίας που δυσχεραίνουν το έργο τους.

Το ενδοδίκτυο ή Intranet είναι ένα αυτοτελές τοπικό δίκτυο που χρησιμοποιεί τα ίδια πρωτόκολλα επικοινωνιών και τις ίδιες μορφές αρχείων με το Internet. Ένα ενδοδίκτυο μπορεί, χωρίς να είναι απαραίτητο, να συνδέεται με το Internet. Πολλές επιχειρήσεις

χρησιμοποιούν ενδοδίκτυα για τις εσωτερικές επικοινωνίες τους. Για παράδειγμα μια επιχείρηση με 10 υπολογιστές , μπορεί να τους συνδέσει σε ένα ενδοδίκτυο και να ένα site στο οποίο θα έχουν πρόσβαση μόνο οι χρήστες των υπολογιστών.

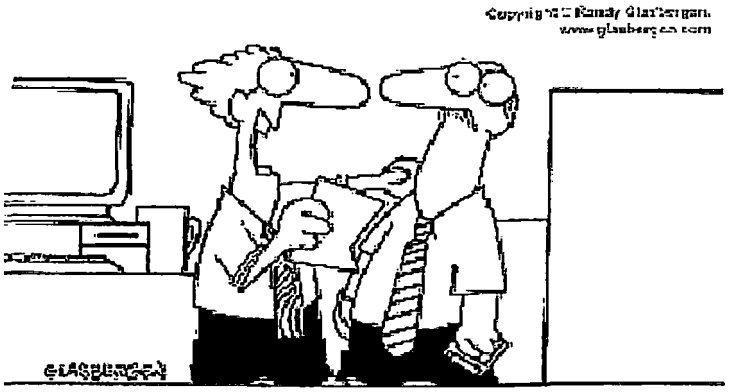
Το Intranet είναι ένα δίκτυο υπολογιστών που βρίσκεται εγκατεστημένο σε μια επιχείρηση, προκειμένου να εξυπηρετήσει τις ανάγκες της για εσωτερική πληροφόρηση και οργάνωση. Αποτελείται από ηλεκτρονικούς υπολογιστές (εκ των οποίων τουλάχιστον ο ένας είναι ο κεντρικός, ο server), οι οποίοι συνδέονται μεταξύ τους ενσύρματα ή, σπανιότερα, ασύρματα. Τη δικτύωση αυτή πλαισιώνουν εξειδικευμένες εφαρμογές λογισμικού, οι περισσότερες από τις οποίες είναι ίδιες με εκείνες που χρησιμοποιούνται στο Internet. Ενδεικτικά, χρησιμοποιούνται τα πρωτόκολλα επικοινωνίας HTTP, TCP/IP, οι γλώσσες προγραμματισμού HTML, XML, ενώ για την πλοήγηση (στο Intranet) χρησιμοποιούνται φυλλομετρητές (browsers), όπως λ.χ. ο Internet Explorer ή ο Netscape Navigator. Λόγω των ομοιοτήτων αυτών, το Intranet αποκαλείται και "Internet της επιχείρησης". Στα ελληνικά, ο όρος Intranet μπορεί να αποδοθεί ως "ενδοδίκτυο" ή "εσωτερικό δίκτυο", ενώ περισσότερο περιγραφικός είναι ο αγγλικός όρος "Enterprise Information Portal", που μεταφράζεται ως "πληροφοριακή πύλη της επιχείρησης".

Δομικό χαρακτηριστικό του Intranet είναι η ιδιωτικότητα, σύμφωνα με την οποία δικαίωμα εισόδου στο δίκτυο έχουν μόνο όσοι διαθέτουν κωδικό πρόσβασης. Τα δικαιώματα πρόσβασης μπορεί να είναι διαβαθμισμένα, δηλαδή η πρόσβαση να μην επιτρέπεται σε όλους και σε όλο το περιεχόμενο του Intranet, αλλά οι εργαζόμενοι να έχουν πρόσβαση ανάλογα με τη θέση και τα καθήκοντά τους. Σημειώνεται ότι παρά την ιδιωτικότητα και τον εσωτερικό τους χαρακτήρα, τα Intranets έχουν διεξόδους πρόσβασης στο Διαδίκτυο.

Η συνηθέστερη μορφή που λαμβάνει το Intranet είναι αυτή του μικρού τοπικού δικτύου, αποτελούμενου από έναν αριθμό υπολογιστών, οι οποίοι στεγάζονται στα γραφεία της επιχείρησης. Μπορεί όμως να αποτελείται και από πολλά μικρά ή μεγαλύτερα τοπικά δίκτυα, τα οποία έχουν ενοποιηθεί μέσω μισθωμένων γραμμών (οι οποίες παρέχονται από τους ISP). Με αυτό τον τρόπο, το Intranet μπορεί να συμπεριλάβει μια ολόκληρη επιχείρηση, από τα κεντρικά της γραφεία μέχρι τα απομακρυσμένα υποκαταστήματα.

Πρακτικά, η πρόσβαση στο Intranet πραγματοποιείται μέσω ενός φυλλομετρητή (browser), που μόλις ενεργοποιηθεί, ανοίγει την αρχική σελίδα του Enterprise Information Portal. Παρενθετικά αναφέρεται ότι ο υπολογιστής μέσω του οποίου θα πραγματοποιηθεί η πρόσβαση στο Intranet δεν είναι απαραίτητο να είναι συνδεδεμένος στο τοπικό δίκτυο. Μπορεί να είναι συνδεδεμένος μόνο στο Internet, και η πρόσβαση στο Intranet να γίνεται μέσω Διαδικτύου.

Η εικόνα της αρχικής σελίδας του Intranet είναι παρόμοια με αυτήν ενός οποιουδήποτε δικτυακού τόπου. Υπάρχουν δηλαδή κείμενα, φωτογραφίες, διάφορες κατηγορίες, σύνδεσμοι (links), εφαρμογές ηλεκτρονικού ταχυδρομείου, εργαλεία αναζήτησης κ.λπ.



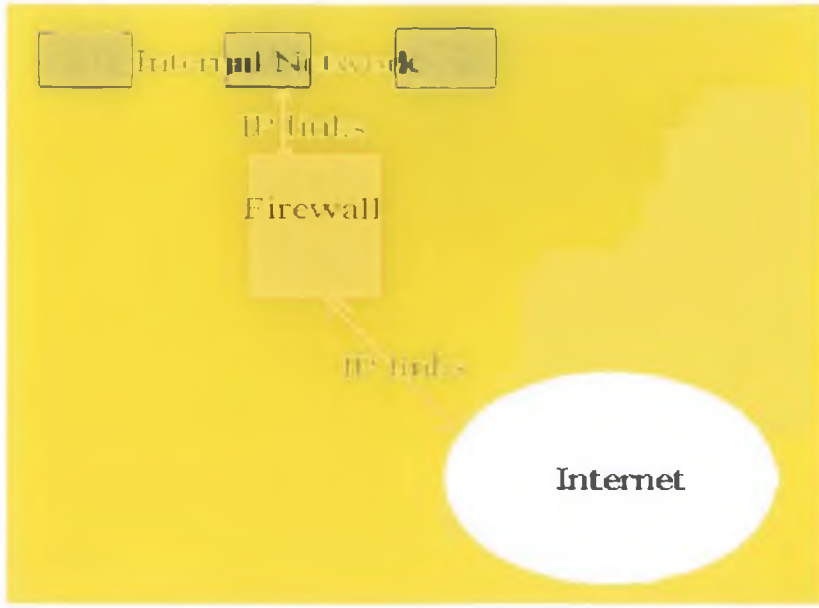
"Why do we need to set up our own corporate Intranet? Because we're guys—and guys love messing around with high-tech, electronic stuff, that's why!"

**Ένα τυπικό Intranet περιλαμβάνει:**

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

Ένα Intranet διαχωρίζεται από το υπόλοιπο Internet με τη χρήση ενός firewall, δηλαδή ενός συνδυασμού hardware και software ο οποίος απαγορεύει την μη εξουσιοδοτημένη πρόσβαση στο Intranet (Σχήμα 20). Οι άνθρωποι που εργάζονται στην επιχείρηση μπορούν να έχουν πρόσβαση στο Internet και να χρησιμοποιούν τους πόρους του, αλλά οι ανεπιθύμητοι επισκέπτες κρατούνται μάκρια από τα firewalls.

Όταν παρέχεται πρόσβαση σε εξωτερικές υπηρεσίες ηλεκτρονικού ταχυδρομείου, γνωστές υπηρεσίες όπως το spam και συγκεκριμένοι τύποι attachments μπλοκάρονται από τον ίδιο τον οργανισμό. Πρέπει επίσης να σημειωθεί ότι τα emails που στέλνονται και λαμβάνονται με αυτόν τον τρόπο, μπάρουν να χρησιμοποιηθούν σε νομικές διαδικασίες της εταιρείας.




**Σχήμα 20. Το Intranet διαχωρίζεται από το Internet μέσω firewall**

Τα Intranets χρησιμοποιούν ένα συνδυασμό έτοιμου λογισμικού όπως οι Web Browsers και ειδικά σχεδιασμένου software όπως εργαλεία αναζήτησης βάσεων δεδομένων.

Επειδή τα Intranets στηρίζονται στα πρωτόκολλα του Internet είναι εφικτή η γρήγορη ενημέρωσή τους με τις νεώτερες τεχνολογίες. Μακροπρόθεσμα η μεγαλύτερη χρήση των Intranets θα οφείλεται σε workgroup εφαρμογές, λογισμικό δηλαδή το οποίο επιτρέπει στους χρήστες να δουλεύουν συνεργατικά με τη βοήθεια των υπολογιστών τους. Υπάρχουν αρκετά είδη workgroup λογισμικού.

Τα εν λόγω προγράμματα επιτρέπουν στους ανθρώπους σε όλο τον κόσμο να παίρνουν μέρος σε συζητήσεις και βιντεοδιασκέψεις, να μμοιράζονται βάσεις δεδομένων, να παρακολουθούν έγγραφα κ.ο.κ.

### 2.1.1 Πλεονεκτήματα των Intranets

Τα οφέλη των Intranets εκτείνονται προς πολλές κατευθύνσεις. Κατ' αρχάς, προς την καθημερινή εργασία του ανθρώπινου δυναμικού, που λόγω και μέσω του Intranet γίνεται πρακτικότερη, λειτουργικότερη και αποτελεσματικότερη. Στη συνέχεια, προς την ηγετική ομάδα, που χάρη στο Intranet μπορεί να συγκεντρώνει πολύτιμες γνώσεις για την εταιρία, τις λειτουργίες της, τα "αδύνατα" και τα "δυνατά" της σημεία. Εν τέλει, προς το σύνολο της επιχείρησης και προς όλα τα συστατικά που την απαρτίζουν, είτε πρόκειται για εργαζομένους είτε για διαδικασίες ή προϊόντα.

Σε γενικές γραμμές, τα οφέλη θα μπορούσαν να κατηγοριοποιηθούν με τον ακόλουθο τρόπο:

**Λειτουργικά οφέλη:** Η ύπαρξη Intranet σε μία επιχείρηση συνεπάγεται εξοικονόμηση χρόνου (εργατοωρών), περιορισμό των λειτουργικών εξόδων και καλύτερη εσωτερική λειτουργία. Ειδικότερα, μειώνει κατακόρυφα τις ανάγκες για απόθεμα φυσικής (έντυπης) πληροφορίας. Οι υπάλληλοι, δηλαδή, δεν χρειάζονται στοίβες εγγράφων (ντοσιέ, φακέλους κ.λπ.) για να κάνουν τη δουλειά τους, αφού οι πληροφορίες βρίσκονται ψηφιοποιημένες μέσα στο Intranet και μπορούν να ανασυρθούν άμεσα.

Επιπλέον, η ψηφιοποίηση της πληροφορίας και η καταχώρησή της σε μία κοινή πλατφόρμα εργασίας, το Intranet, έχουν ως αποτέλεσμα, οι χρήστες να βρίσκουν ευκολότερα και γρηγορότερα αυτό που αναζητούν, χωρίς να απασχολούν συναδέλφους, χωρίς να ανεβοκατεβαίνουν σκάλες, χωρίς να ανοίγουν συρτάρια. Τα πάντα βρίσκονται στο Intranet και είναι άμεσα διαθέσιμα, ενώ μέσω αυτού μπορούν να πραγματοποιηθούν και οι περισσότερες εργασίες ρουτίνας. Για παράδειγμα, οι εργαζόμενοι μπορούν να πραγματοποιήσουν τις παραγγελίες τους για αναλώσιμα, να ενημερώνουν το αρμόδιο τμήμα για ελλείψεις, δυσλειτουργίες, προβλήματα, για παράπονα πελατών και γενικότερα για οτιδήποτε αφορά στην εταιρία.

Πέραν αυτών, η ύπαρξη Intranet διευκολύνει τα μέγιστα τη διανομή της εταιρικής γνώσης σε όλους τους χρήστες. Ως εταιρική γνώση ορίζεται το απόθεμα δεδομένων και πληροφοριών που θεωρείται ιδιαίτερα χρήσιμο για την εξασφάλιση της ομαλής λειτουργίας της επιχείρησης και του ανταγωνιστικού της χαρακτήρα. Η γνώση αυτή, από κεκτημένο λίγων στελεχών, παρέχεται μέσω του δικτύου σε όλους, προκειμένου να αξιοποιηθεί κατάλληλα.

Εξάλλου, το Intranet διευκολύνει την καλλιέργεια κλίματος εμπιστοσύνης, σύμπνοιας και ομοψυχίας μεταξύ των εργαζομένων και αποτρέπει σε υπολογίσιμο βαθμό τις συγκρούσεις, τις ρήξεις και τις αμφιταλαντεύσεις. Η παρουσία του, χρησιμεύει άλλοτε ως πυξίδα, άλλοτε ως καταστατικός χάρτης και άλλοτε ως "φάρος" που υποδεικνύει την πορεία που πρέπει να ακολουθηθεί σε συγκεκριμένα ζητήματα. Έτσι, μπορεί να λειτουργεί ακυρωτικά σε προσπάθειες αυτονόμησης και ατομισμού, καταπολεμώντας παράλληλα το φαινόμενο της διγλωσσίας, το οποίο παρατηρείται όταν διαφορετικοί άνθρωποι (υπάλληλοι) εκφράζουν διαφορετικές απόψεις για το ίδιο ζήτημα, με αποτέλεσμα τη δημιουργία καταστάσεων σύγχυσης και αποπροσανατολισμού. Αυτό συμβαίνει λ.χ. όταν ορισμένοι υπάλληλοι αρέσκονται να ακολουθούν την τακτική του α στελέχους για την επίλυση κάποιου συγκεκριμένου προβλήματος, ενώ μία άλλη μερίδα υπαλλήλων αρέσκεται να ακολουθεί την τακτική του β στελέχους.

**Διοικητικά - στρατηγικά οφέλη:** Ο σχεδιασμός των μελλοντικών κινήσεων της επιχείρησης, τα σχέδια και οι τακτικές που θα ακολουθηθούν στο μέλλον, τροφοδοτούνται και επηρεάζονται από τα δεδομένα που συγκεντρώνονται μέσω του Intranet. Υπενθυμίζεται ότι όλοι οι χρήστες μπορούν και να προσφέρουν πληροφορίες στο Intranet, όχι μόνο να λαμβάνουν. Η συγκέντρωση των πληροφοριών και η ανάλυσή τους, που θα επακολουθήσει, θα προσφέρουν στην ηγετική ομάδα της εταιρίας ποιοτικές πληροφορίες (γνώση), που θα τη βοηθήσουν να χαράξει τη στρατηγική της και να διαχειριστεί τις όποιες κρίσεις με αποτελεσματικότητα. Με τη σειρά της, η ηγετική

ομάδα θα αξιολογήσει τις εισερχόμενες πληροφορίες, και εκείνες που θα κρίνει σημαντικές θα τις διανείμει στους εργαζομένους μέσω του δικτύου. Η αμφίδρομη αυτή διαδικασία (ανατροφοδότηση), φέρνει πιο κοντά ιθύνοντες, στελέχη και υπαλλήλους (χωρίς να καταργεί την ιεραρχία) και διευκολύνει τη διοίκηση της επιχείρησης ως σύνολο.

Για να γίνει σαφέστερη αυτή η διαδικασία, ας δούμε ένα παράδειγμα: Από τα στατιστικά επισκεψιμότητας του Intranet μιας εταιρίας που αντιμετωπίζει οξύ πρόβλημα με τον ανταγωνισμό, προκύπτει ότι ελάχιστοι χρήστες/εργαζόμενοι έχουν προστρέξει στην κατηγορία "Ανταγωνιστικές εταιρίες και προϊόντα" και έχουν μελετήσει το υλικό που υπάρχει εκεί. Αυτό θορυβεί τους ιθύνοντες, που πιθανολογούν ότι η αδυναμία αντιμετώπισης του ανταγωνισμού μπορεί και να οφείλεται στις ελλιπείς γνώσεις που έχει το προσωπικό για το θέμα. Σε μία πρώτη προσπάθεια επίλυσης του προβλήματος, δίνουν εντολή η συγκεκριμένη κατηγορία να γίνει πιο "ζωηρή", να τοποθετηθεί σε πιο κεντρική θέση στο Intranet, και επιπλέον όλοι να ασχοληθούν με το θέμα επισταμένως (να διαβάσουν το σχετικό υλικό).

**Μαθησιακά οφέλη:** Το Intranet αποτελεί εργαλείο μάθησης και πληροφόρησης για τους υπαλλήλους μιας επιχείρησης, λειτουργώντας "κοινωνικοποιητικά". Οι νεοπροσληφθέντες υπάλληλοι ενσωματώνονται γρηγορότερα και ομαλότερα στην επιχείρηση. Αυτό συμβαίνει γιατί οι περισσότερες απαντήσεις στα εύλογα ερωτήματά τους υπάρχουν στο Intranet, και μερικές ώρες περιήγησης και αναζήτησης από το νέο υπάλληλο αρκούν για να μάθει τα βασικά του καθήκοντα, τους τομείς δραστηριοποίησης της επιχείρησης, τι πρέπει να προσέξει, τι να αποφύγει κ.λπ. Επιπρόσθετα, το Intranet μπορεί να αντικαταστήσει σε αρκετές περιπτώσεις τη φυσική επαφή μεταξύ των εργαζομένων για ενημερωτικούς λόγους (λ.χ. για την κοινοποίηση κάποιας εξέλιξης).

### 2.1.2 Μειονεκτήματα

Για να προετοιμάσετε το intranet για χρήση από τους υπαλλήλους, χρειάζεστε κάποιον που θα δημιουργεί και θα διατηρεί το περιεχόμενο. Η ιδέα είναι να έχετε συνεχώς ενημερωμένες πληροφορίες διαθέσιμες. Ο τρόπος που αναθέτετε αυτές τις εργασίες μπορεί να εξαρτάται από το μέγεθος της εταιρείας σας. Αν έχετε μόνο 10 άτομα, αρκεί ένα άτομο για τη διατήρηση των πληροφοριών.

Αν έχετε μεγαλύτερη εταιρεία, ίσως θελήσετε να διαχωρίσετε τις ενημερώσεις του περιεχομένου για κάθε τμήμα. Όποιο και να είναι το μέγεθος, θα χρειαστεί να συνυπολογίσετε χρόνο για εργασίες ανανέωσης στο πρόγραμμα των υπαλλήλων. Θυμηθείτε, έχουμε να κάνουμε με υπολογιστές, μερικές φορές τα πράγματα δεν πηγαίνουν όπως θα θέλαμε.

Θα χρειαστεί επίσης να αφιερώσετε χρόνο στην εκπαίδευση των εργαζομένων. Ίσως ακόμα χρειαστεί να αφιερώσετε χρόνο ώστε να τους πείσετε να χρησιμοποιήσουν το intranet. Μόλις το σύστημα τεθεί σε εφαρμογή και τα κατανοήσουν όλοι, τα οφέλη θα είναι σημαντικά.

### 2.1.3 Οι λόγοι χρησιμοποιήσεις του Intranet από μικρομεσαίες επιχειρήσεις.

Ένα πράγμα που μου αρέσει με τις μικρές επιχειρήσεις, είναι η ικανότητα για γρήγορη δράση. Οι αποφάσεις δεν επιβραδύνονται από τις διάφορες βαθμίδες της ιεραρχίας. Οι περισσότερες κινήσεις γίνονται γύρω από το τραπέζι σε μια σύσκεψη. Ωστόσο, μπορεί να υπάρξει κάποιο σημείο που η ανάπτυξη της εταιρείας σας ξεπερνά αυτό το διακανονισμό. Χρειάζεστε σταθερές, αξιόπιστες και ασφαλείς επικοινωνίες με τους συναδέλφους στην εταιρεία, για να εξασφαλίσετε την πρόοδο. Θα χρειαστείτε intranet.

Το intranet μοιάζει με τοποθεσία στο Web. Χρησιμοποιεί πρωτόκολλα στο Internet, αλλά πρόκειται για εσωτερικό δίκτυο που είναι αποκλειστικό μόνο για μία εταιρεία. (Το "extranet" είναι και αυτό εσωτερική η ιδιωτική τοποθεσία στο Web, ωστόσο τα δικαιώματα πρόσβασης επεκτείνονται σε συγκεκριμένους πελάτες, συνεργάτες ή /και τρίτους.)

Οι περισσότερες μεγάλες εταιρείες χρησιμοποιούν τη λύση του intranet. Η διανομή των πληροφοριών αποτελεί τεράστια εργασία όταν το προσωπικό σας είναι 10.000 ή παραπάνω υπάλληλοι. Τα intranet τη διευκολύνουν.

**Συνεργασία στο Internet με την δική σας ιδιωτική τοποθεσία στο Web**
Με το Windows SharePoint Services, η λύση για intranet/extranet της Microsoft, μπορείτε να δημιουργήσετε πίνακες ανακοινώσεων στο Internet για την επιχείρησή σας αλλά και να κάνετε κοινή χρήση εγγράφων.

Τρεις κύριοι λόγοι που αξίζουν την επένδυση αυτή:

**1. Η επικοινωνία επιβαρύνεται όταν ασχολείστε με περισσότερα από ένα άτομα**
Ακόμα και μια πολύ μικρή επιχείρηση έχει επικοινωνιακά προβλήματα. Οι περισσότεροι μαθαίνουν τι γίνεται από κουτσομπολιά. Οι ιστορίες παραποιούν καθώς μεταδίδονται και το αποτέλεσμα είναι παραπληροφόρηση και δυσαρεστημένο προσωπικό. Αν απασχολείτε μετακινούμενους εργαζόμενους, εργαζόμενους εκτός γραφείου ή άλλους που ταξιδεύουν πολύ ή μια "εικονική" εταιρεία, τα θέματα επικοινωνίας παρουσιάζουν ακόμα μεγαλύτερες προκλήσεις.

Για να είναι επιτυχημένη μια εταιρεία, όλοι οι εργαζόμενοι πρέπει να κατανοούν τους στόχους της. Οι μακροπρόθεσμοι και οι βραχυπρόθεσμοι στόχοι δεν πρέπει να περιορίζονται στις συσκέψεις των ανώτερων στελεχών. Όλοι πρέπει να εργάζονται για την επίτευξη κοινών στόχων.

Το intranet είναι ιδανικό για τη δημοσίευση εβδομαδιαίων αναφορών, υπενθυμίσεων και στόχων. Έτσι, όλοι έχουν τις ίδιες πληροφορίες.

Ο Toby Ward, πρόεδρος της συμβουλευτικής εταιρείας σε θέματα intranet Prescient Digital Media, σημειώνει ότι ακόμα και οι εταιρείες με λίγους εργαζόμενους μπορούν να

επωφεληθούν από το intranet. Ακόμα και υπάρχουν άτομα που εργάζονται απομακρυσμένα, οι πωλητές ή οι σύμβουλοι δεν είναι πάντα στο γραφείο.

Η δημιουργία ενός intranet μπορεί να ενισχύσει την επικοινωνία μέσω πινάκων ανακοινώσεων, άμεσης ανταλλαγής μηνυμάτων και ελεγχόμενων συζητήσεων. Πώς γίνεται αυτό;

Ας πάρουμε για παράδειγμα ένα τυπικό σενάριο. Το πενταμελές προσωπικό πωλήσεων πρέπει να κάνει μια παρουσίαση στον πρόεδρο σχετικά με αύξηση των πωλήσεων για το επόμενο οικονομικό έτος.

Αυτά τα πέντε άτομα θα μπουν στην αίθουσα συσκέψεων, θα γευματίσουν, θα πιουν καφέ και θα συζητήσουν με τις ώρες. Η πρώτη συνάντηση μετατρέπεται σε 3ωρη ανταλλαγή ιδεών. Η δεύτερη, αρχίζει με μια ανασκόπηση των καλύτερων ιδεών που τέθηκαν στο τραπέζι κατά την πρώτη. Οι συμμετέχοντες συζητούν τους λόγους που θα είναι αποτελεσματικοί ή όχι. Την τρίτη με τέταρτη συνάντηση, οι πέντε τους καταλήγουν με μερικές προτάσεις.

Χρησιμοποιώντας τον πίνακα συζητήσεων τις ημέρες πριν από τις συσκέψεις μπορείτε να απλοποιήσετε την εμπειρία. Συζητήστε τις ιδέες από πριν, Οι συμμετέχοντες θα προσέλθουν στη συνάντηση γνωρίζοντας καλύτερα τι θέλουν να επιτύχουν.

**2. Ο χρόνος είναι χρήμα**

Το intranet σάς επιτρέπει να δημοσιεύετε σημαντικές πληροφορίες ώστε να είναι προσβάσιμες από όλους τους εργαζόμενους. Ακόμα και οι πληροφορίες που είναι σχετικές με το ανθρώπινο δυναμικό είναι χρήσιμες. Ένας από τους υπαλλήλους μου είπε ότι στο προηγούμενο γραφείο που δούλευε ξόδευαν 45 λεπτά για να διαπιστώσουν αν μια επερχόμενη αργία ήταν με αποδοχές ή άνευ. Ο προσωπάρχης έλειπε και κανένας άλλος δεν γνώριζε.

Η δημοσίευση ημερολογίων, πολιτικών της εταιρείας και επιδομάτων είναι καλή αρχή. Θα μειώσουν το χρόνο που σπαταλιέται ανώφελα. Αλλά ένα intranet μπορεί να χρησιμοποιηθεί και για άλλα πράγματα εκτός από τις βασικές πληροφορίες. Το μεγάλο του πλεονέκτημα είναι η αλληλεπιδραστικότητά του.

Μπορείτε να εξοικονομήσετε χρόνο με αλληλεπιδραστικές φόρμες. Οι αιτήσεις για διακοπές, οι παραγγελίες για προμήθειες, οι αλλαγές στα επιδόματα και άλλα διεκπεραιώνονται πιο γρήγορα και αποτελεσματικά.

Βεβαιωθείτε ότι το intranet τηρεί της καλές πρακτικές σχεδίασης. Δεν μπορείτε να δημοσιεύσετε πληροφορίες με την ελπίδα ότι οι ενδιαφερόμενοι θα τις εντοπίσουν. Οργανώστε το intranet ώστε να είναι όσο το δυνατό περισσότερο πιο φιλικό προς το χρήστη. Σκοπός είναι να εξοικονομήσουμε χρόνο, όχι να εκνευρίσουμε τους χρήστες.

**3. Είναι καλύτερο από το ηλεκτρονικό ταχυδρομείο**

Μπορεί να σκέφτεστε, "Γιατί δεν μου στέλνουν με ηλεκτρονικό ταχυδρομείο τη φόρμα;" Ή, "Επικοινωνώ καλά με τους υπαλλήλους μου στις συσκέψεις και με ανακοινώσεις στον πίνακα του γραφείου."

Σύμφωνα με τον Ward, η αποστολή με ηλεκτρονικό ταχυδρομείο πολλών εκδόσεων του ίδιου εγγράφου ή παρουσίασης οδηγεί σε σύγχυση και μερικές φορές σε υπερβολικά πολλές πληροφορίες.

Ας εξετάσουμε τις ίδιες ομάδες πωλήσεων που χρησιμοποιήσαμε προηγουμένως. Έχουν καταλήξει σε τρεις βασικούς τρόπους για το πώς θα αυξήσουν τις πωλήσεις. Τώρα εργάζονται στην παρουσίαση PowerPoint.

Όταν πέντε άτομα συνεργάζονται σε ένα αρχείο PowerPoint, τα αποτελέσματα μπορεί να είναι ολέθρια. Ακούω τις φωνές τους ήδη. "Ποιος έχει την τελευταία έκδοση;" "Ο Παπαδόπουλος μου έδωσε λάθος νούμερα. Νόμιζα ότι το είχαμε διορθώσει." Και άλλα πολλά.

Χρησιμοποιώντας το intranet, οι υπάλληλοι μπορούν να εργαστούν σε ένα κοινόχρηστο αρχείο και να έχουν μια κεντρική θέση όπου θα διατηρούν το πιο πρόσφατο αρχείο.

Αυτό επίσης εξοικονομεί χώρο στο διακομιστή. Ίσως είναι λεπτομέρεια, ωστόσο όταν υπάρχουν εκδόσεις διάφορων αρχείων στους υπολογιστές όλων των υπαλλήλων, δεσμεύεται πολύτιμος αποθηκευτικός χώρος.

**Πώς να ξεκινήσετε**

Πριν δημιουργήστε ένα intranet, πρέπει να κατανοήσετε ποιο σκοπό θέλετε να εξυπηρετεί. Κατανοήστε πώς θα το χρησιμοποιούν οι εργαζόμενοι. Τέλος, χρησιμοποιήστε καλές πρακτικές σχεδίασης. Αν χρειάζονται πέντε ή έξι κλικ για την εύρεση μιας φόρμας για αίτηση άδειας, είναι ήδη περίπλοκο.

Επίσης, θα χρειαστεί να αποφασίσετε αν θέλετε να δημιουργήσετε τη δική σας λύση. Κάποιος σύμβουλος μπορεί να δημιουργήσει το intranet σύμφωνα με τις προδιαγραφές σας. Θα έχει την εμφάνιση και τις σχεδιαστικές αρχές που καθορίζετε. Αυτή η οδός θα σας κοστίσει από 10 μέχρι 500 δολάρια ανά άτομο μηνιαίως.

Υπάρχουν επίσης πακέτα λογισμικού, όπως το Windows SharePoint Services που σας επιτρέπουν να προσαρμόζετε και να σχεδιάζετε τα περισσότερα στοιχεία οι ίδιοι, χρησιμοποιώντας έτοιμα πρότυπα. Το SharePoint αρχίζει από 39,95 δολάρια το μήνα ή 399 δολάρια το χρόνο, όσοι και να είναι οι χρήστες.

Κάποια πακέτα, όπως το Instant Intranet Builder, χρησιμοποιούν τη Microsoft Access ως κεντρική βάση δεδομένων. Περιλαμβάνουν μηχανισμούς σύνδεσης για τη δημιουργία ενός intranet που διευκολύνει την εργασία. Δεν χρειάζεστε αποκλειστικό άτομο IT για να

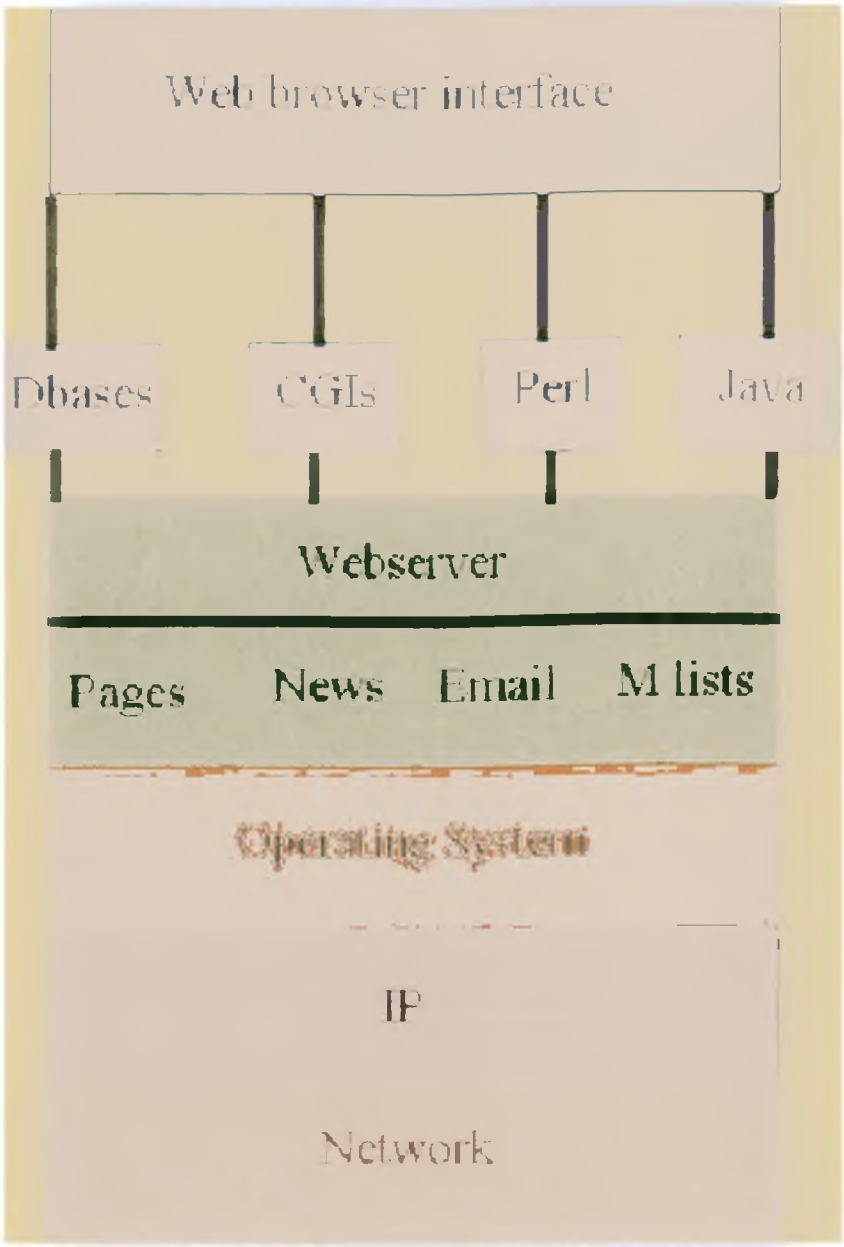
το εγκαταστήσετε και να το διατηρήσετε. Ανάλογα με το μέγεθος της εταιρείας, ολόκληρο το πακέτο είναι διαθέσιμο από μόλις 5 δολάρια ανά άτομο μηνιαίως.

Κάποια άλλα προϊόντα λογισμικού είναι τα InfoStreet, IntraSmart και Intranet Suite. Η τιμολόγηση ποικίλλει, ανάλογα με τον αριθμό των χρηστών.

## 2.2 Το λογισμικό των ομάδων εργασίας

Το λογισμικό των ομάδων εργασίας, που ονομάζεται επίσης groupware, βρίσκεται στην καρδιά των Intranets. Το λογισμικό αυτό επιτρέπει στους ανθρώπους να μοιράζονται αρχεία και πληροφορίες, να συνεργάζονται ευκολότερα κατά τη διάρκεια των projects και γενικά να εργάζονται μαζί με τρόπους που δεν ήταν εφικτοί παλαιότερα. Το σημαντικότερο είναι ότι το groupware λογισμικό δεν επιτρέπει στους ανθρώπους απλώς να επικοινωνούν αλλά και να εργάζονται από κοινού σε διαμοιρασμένα έγγραφα. Μια γραφική αναπαράσταση του λογισμικού των ομάδων εργασίας δίνεται στο Σχήμα 21.

Ένα από τα βασικότερα συστατικά του λογισμικού των ομάδων εργασίας αποτελεί το λογισμικό messaging - προγράμματα που επιτρέπουν στους ανθρώπους να παίρνουν δημόσια μέρος σε ομάδες συζήτησης. Οι εν λόγω ομάδες συζήτησης είναι διεσπαρμένες, που σημαίνει ότι οι χρήστες μπάρουν να διαβάζουν και να απαντούν σε ανεξάρτητες θεματικές περιοχές μιας συζήτησης. Για παράδειγμα, σε μία περιοχή μηνυμάτων που είναι αφιερωμένη στα οικονομικά μιας επιχείρησης μπορεί να υπάρχει μία ενότητα που να αφορά στα οικονομικά του τμήματος έρευνας και ανάπτυξης της εταιρίας και μία άλλη η οποία να αφορά τα οικονομικά του μηχανολογικού τμήματος. Αυτό που κάνει το λογισμικό messaging ιδιαίτερα χρήσιμο είναι ο τρόπος με τον οποίο ολοκληρώνεται με τις υπόλοιπες τεχνολογίες του Internet και των Intranets. Για παράδειγμα, ορισμένα προγράμματα συζητήσεων επιτρέπουν την ενσωμάτωση της γλώσσας HTML στα μηνύματα. Αυτό σημαίνει ότι σε μία συζήτηση κάποιος μπορεί να ενσωματώσει ένα link που να παραπέμπει σε μία Web σελίδα ή σε άλλο πόρο του Intranet.




**Σχήμα 21 : Γραφική αναπαράσταση του λογισμικού**

εφαρμογή είναι οι επιτραπέζιες βιντεοδιασκέψεις. Κάθε χρήστης που μετέχει σε αυτές θα πρέπει να διαθέτει μία βιντεοκάμερα καθώς και hardware και software το οποίο επιτρέπει στους υπολογιστές να λαμβάνουν και να στέλνουν φωνή και ήχο. Τότε οι χρήστες μπορούν να κάθονται στον υπολογιστή τους και να βλέπουν και να μιλούν με τους υπόλοιπους χρήστες.

Μία σχετική με την προηγούμενη τεχνολογία προσφέρει το whiteboard λογισμικό. Το εν λόγω software επιτρέπει στους χρήστες να βλέπουν από τον υπολογιστή τους τι

βρίσκεται στο υπολογιστικό σύστημα κάποιου άλλου χρήστη. Το σημαντικότερο είναι ότι επιτρέπει στους χρήστες να χρησιμοποιήσουν το ποντίκι για να υπερφωτίσουν τμήματα της οθόνης, να γράψουν στην οθόνη κ.ο.κ. Αυτό σημαίνει ότι κάποιος χρήστης που ανήκει σε ένα Intranet μπορεί να σχολιάσει εύκολα τη δουλειά κάποιου άλλου και αντιστρόφως.

Τα προγράμματα διαχείρισης εγγράφων και workflow είναι ιδιαίτερα χρήσιμα για τα επιχειρηματικά Intranets τα οποία έχουν σύνθετες διαδικασίες έργων ή σε εκείνα που πολλοί χρήστες πρέπει να εργάζονται μαζί σε ένα έγγραφο.
Το λογισμικό διαχείρισης εγγράφων σε ένα Intranet επιτρέπει το κλείδωμα ενός εγγράφου έτσι ώστε μόνο ένας χρήστης να μπορεί ανά πάσα στιγμή να το χρησιμοποιεί και να μην μπορεί κανένας χρήστης να διαγράψει τη δουλειά κάποιου άλλου. Μπορεί επίσης να δώσει διαφορετικά επίπεδα πρόσβασης σε κάποιο έγγραφο, ούτως ώστε κάποιοι να μπορούν μόνο να το διαβάσουν, ενώ κάποιοι άλλοι να μπορούν να το επεξεργαστούν και να το τροποποιήσουν. Τα πιο εξελιγμένα προγράμματα διαχείρισης εγγράφων επιτρέπουν σε πολλούς χρήστες να εργάζονται σε διαφορετικά τμήματα του εγγράφου ταυτόχρονα.

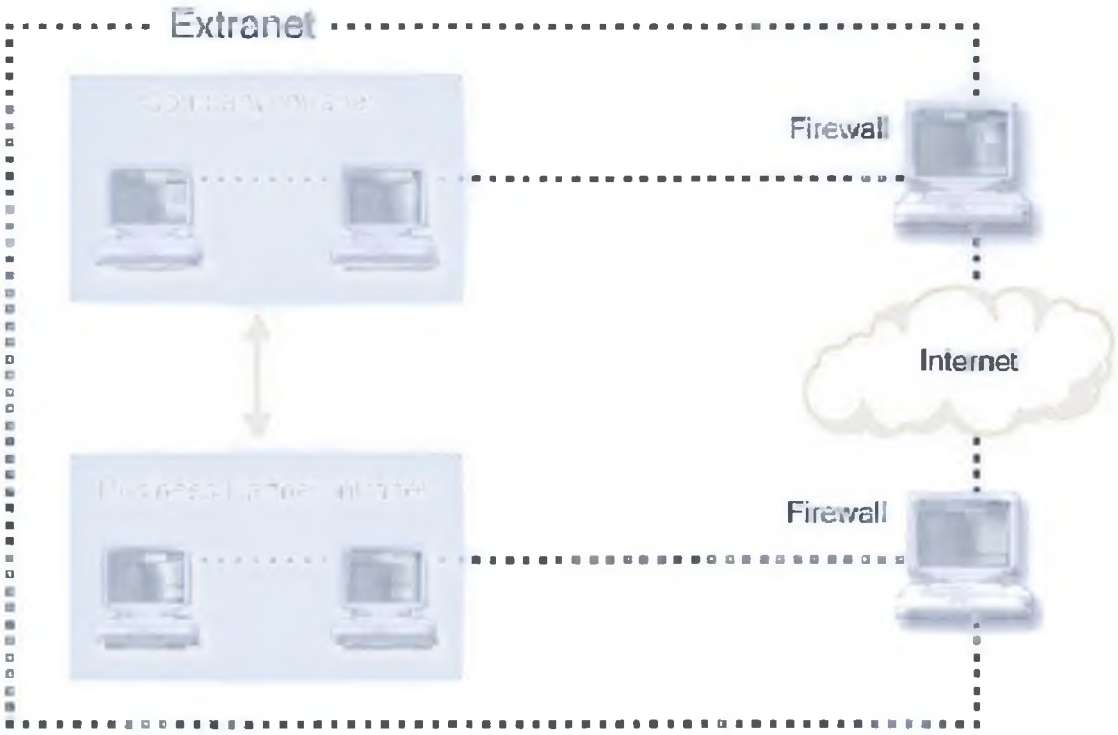
Το λογισμικό workflow μοιάζει με τα προγράμματα διαχείρισης εγγράφων. Αυτό το είδος groupware λογισμικού διαχειρίζεται όλη τη ροή των εργασιών σε έναν οργανισμό, ενώ επιπροσθέτως επιτρέπει και τη διαχείριση ανεξάρτητων εγγράφων.

## 2.3 Extranet

Ένα Extranet μπορεί να περιγραφεί σαν δύο ή περισσότερα Intranets συνδεδεμένα μεταξύ τους σε δίκτυο. Γενικά., και όπως ισχύει και με τα Intranets, ένα Extranet θα βασιστεί πάνω σε πρωτόκολλα του Internet.

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.

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.)




**Σχήμα 22. Extranet μεταξύ δύο εταιρειών**

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.

## 2.4 Intranet και Extranet: Προτάσεις για επιτυχημένη εφαρμογή

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. χρεωπιστωτικές 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.

## 2.5 Intranets και Extranets: Μικρά δίκτυα με μεγάλες επιδόσεις

Μοιάζουν με το Internet, λειτουργούν περίπου το ίδιο, με τη διαφορά ότι απευθύνονται σε πολύ λιγότερους χρήστες και είναι ιδιωτικά.

Ο λόγος για τα Intranets και τα Extranets, τα δίκτυα που χρησιμοποιούνται από επιχειρήσεις για την εσωτερική οργάνωση και τη διανομή της πληροφορίας στους υπαλλήλους. Εξοικονομούν χρόνο και χρήμα, αυξάνουν την απόδοση των εργαζομένων, και βελτιώνουν την εικόνα και την ανταγωνιστικότητα της επιχείρησης.

### 2.6 Σχετικοί Σύνδεσμοι

Ολοκληρωμένη πληροφόρηση για τα Intranets:

- **http://www.intranetroadmap.com/**
- **http://www.intranetinsider.com/**

Εταιρείες ανάπτυξης Intranets στην Ελλάδα:

- **http://www.oracle.gr/**
- **www.sap.com/greece**
- **http://www.noisis.gr/**
- **http://www.analysis.gr/**
- **http://www.enterprise.gr/**
- **http://www.omega.net.gr/**
- **http://www.creative.gr/**

Δημιουργία εικονικού Intranet:
**http://www.intranets.com/**

# Κεφάλαιο 3

# Τοπικά Δίκτυα Υπολογιστών

## Εισαγωγή

Είναι κάπως δύσκολο να δοθεί ο ακριβής ορισμός της έννοιας των τοπικών δικτύων. Μπορεί όμως να γίνει πιο εύκολα κατανοητός εάν τα αντιπαραθέσουμε με τα δίκτυα μεγάλης απόστασης. Εδώ βέβαια η έννοια απόσταση είναι σχετική, διότι πριν από μερικά χρόνια λέγαμε ότι ένα τοπικό δίκτυο είναι ένα σύστημα επικοινωνίας που καλύπτει μια περιοχή από μερικά μέτρα έως 1 χλμ. Σήμερα όμως βλέπουμε , ότι ένα τοπικό δίκτυο μπορεί να επεκταθεί σε μια περιοχή αρκετών χιλιομέτρων.

## 3.1 Τοπικά Δίκτυα (LAN)

Η σύνδεση των υπολογιστών ξεκινά από ένα τοπικό δίκτυο (LAN - Local Area Network), το οποίο επιτρέπει το "μοίρασμα" (καταμερισμό) πληροφοριών ανάμεσα στους υπολογιστές που βρίσκονται στο ίδιο κτίριο ή ακόμη σε μια στενή γεωγραφικά περιοχή (μέχρι 10 km περίπου).

**Τοπικά Δίκτυα**
Γραφική αναπαράσταση ενός τοπικού δικτύου.

Στο δίκτυο, εκτός από υπολογιστές μπορούν να συνδεθούν και διάφορα Περιφεριακά, έτσι ώστε όλοι οι χρήστες του δικτύου να έχουν πρόσβαση σ' αυτά.

Βασική προϋπόθεση για τη διασύνδεση ενός υπολογιστή σε δίκτυο είναι η ύπαρξη μίας "κάρτας δικτύου" .

Γενικά ορίζουμε σαν τοπικό δίκτυο ένα σύστημα επικοινωνίας που συνδέει με υψηλούς ρυθμούς μετάδοσης ένα σύνολο από υπολογιστικά συστήματα και εξοπλισμό όπως εκτυπωτές, τηλεφωνικές συσκευές, τερματικά γραφικών, σταθμούς εργασίας κ.τ.λ. με σκοπό την από κοινού χρήση τους.

Η επόμενη εικόνα δείχνει ένα τοπικό δίκτυο. Στο δίκτυο αυτό διακρίνουμε :

- Servers δικτύου
- Servers τερματικών
- Workstations
- Προσωπικούς υπολογιστές
- Συσκευή πολλαπλής σύνδεσης
- HUB κ.λ.π

Ένα τοπικό δίκτυο θα πρέπει να είναι ικανό να μεταφέρει διάφορες μορφές πληροφορίας π.χ ήχο, εικόνα , δεδομένα, κ.τ.λ .

Αυτό που χαρακτηρίζει επίσης ένα τοπικό δίκτυο είναι ότι αποφεύγεται ο πολλαπλασιασμός των καλωδιώσεων, και γίνεται δυνατή η από κοινού χρήση ακριβού εξοπλισμού ή δεδομένων που βρίσκονται αποκλειστικά σε κάποιο σταθμό του δικτύου. Επίσης επειδή το δίκτυο δεν επεκτείνεται σε πολύ μεγάλες γεωγραφικές αποστάσεις έχουμε ταχύτητες μετάδοσης πολύ ανώτερες από τα μεγάλα δημόσια δίκτυα.

### 3.1.1 Στοιχεία που απαρτίζουν ένα τοπικό δίκτυο

Βασικά στοιχεί που απαρτίζουν ένα τοπικό δίκτυο είναι:

- Ένας αριθμός από σταθμούς εργασίας(PC, workstations)
- Γραμμές και συσκευές επικοικωνίας
- Συσκευές διασυνδέσεως (interfaces) με το μέσο μετάδοσης
- Τα πρωτόκολλα επικοινωνίας και προσπέλασης

Το φυσικό μέσο που χρησιμεύει για τη διασύνδεση ενός σταθμού με το μέσο μετάδοσης είναι συνήθως κάρτες τυπωμένων ηλεκτρονικών κυκλωμάτων που συνήθως τοποθετούνται μέσα σε PC.

Οι servers δικτύου είναι υπολογιστές , που διαθέτουν την απαραίτητη μνήμη για επεξεργασία της πληροφορίας , και εκτελούν σαν ειδική εργασία τη διαχείριση και τον έλεγχο του δικτύου.

Οι couplers παρέχουν τη δυνατότητα σύνθεσης δύο σημάτων. Οι ελεγκτές (controlers) χρησιμοποιούνται για τη λογική και φυσική σύνδεση του κάθε σταθμού στο δίκτυο, περιλαμβάνοντας και τα modem υψηλής συχνότητας. Ορισμένες δε τυποποιήσεις π.χ IEEE 802.χ επιβάλουν προδιαγραφές για το μέγιστό μήκος των καλωδίων.
Για να μεταφερθεί το σήμα από τμήμα σε τμήμα του τοπικού δικτύου, χρησιμοποιούνται οι λεγόμενοι επαναλήπτες (repeaters). Αυτοί είναι όργανα που επιτρέπουν την επαναδυνάμωση του σήματος στα διάφορα τμήματα του δικτύου.

Ο επαναλήπτης δεν επεμβαίνει στο περιεχόμενο του μηνύματος από "λογική" άποψη ούτε και στο πρωτόκολλο που χρησιμοποιείται. Πρόκειται για μια συσκευή αναμετάδοσης που επιτρέπει να χρησιμοποιηθούν μέσα στο ίδιο δίκτυο διαφορετικά είδη μέσου μετάδοσης π.χ οπτικές ίνες ,ομοαξονικά καλώδια κ.τ.λ.

Τέλος θα πρέπει να αναφέρουμε ότι για τα τοπικά δίκτυα υπάρχουν εξειδικευμένα λειτουργικά συστήματα καθώς και πρωτόκολλα επικοινωνίας τα οποία λαμβάνουν υπ'όψιν τη σχετικά μικρή απόσταση και το ότι οι σταθμοί είναι μικροϋπολογιστές.

### 3.1.2 Οι ανάγκες που επέβαλαν τη χρησιμοποίηση τοπικών δικτύων

Η χρήση των τοπικών δικτύων επιβάλλεται:

- Από την ανάγκη να διαμοιραστεί η χρήση ακριβού εξοπλισμού (π.χ ειδικοί υπολογιστές)
- 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 να ανταλλάξουν πληροφορίες σε στιγμιαίο χρόνο (real-time)
- 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 200 χλμ..(περίπτωση δικτύων FDDI).

Πριν περιγράψουμε πιο λεπτομερειακά τα τοπικά δίκτυα, θα λέγαμε ότι μπορούμε να τα κατατάξουμε σε τρεις κατηγορίες.

- Τα τηλεφωνικά τοπικά δίκτυα που εξυπηρετούνται με τους PABX(Private Automatic Branch excange)
- Τα τοπικά δίκτυα baseband
- τα τοπικά δίκτυα ευρείας μετάδοσης (broadband)

**Οι PABX(Private Automatic Branch exchange)**

Αρχικά σχεδιάστηκάν για τη μεταφορά τηλεφωνικών μηνυμάτων. Αυτού του είδους τα δίκτυα, (αρχικά αναλογικού τύπου), δεν μπορούν να μεταδώσουν μεγάλου όγκου πληροφορίες γιατί χρησιμοποιούν τηλεφωνικά καλώδια για τη μετάδοση, τα οποία δεν προσφέρουν αρκετή προστασία από παράσιτα και δεν επιτρέπουν μεγάλες ταχύτητες μετάδοσης με χαμηλό ποσοστό σφάλματος.
Οι PABX επιτρέπουν μεταφορά δεδομένων με μεγάλη ταχύτητα. Το βασικό τους πλεονέκτημα :
Είναι οικονομικοί και εύκολοι στην εγκατάσταση έναντι ορισμένων άλλων τοπικών δικτύων.

## 3.2 Τρόποι μετάδοσης πληροφορίας

Ανεξάρτητα πάντως του είδους της πληροφορίας που πρέπει να μεταδοθεί ,το μέσον μετάδοσης μεταφέρει μόνον ηλεκτρομαγνητικά σήματα. Δηλαδή για να μεταδοθεί η πληροφορία θα πρέπει αυτή να προσαρμοστεί στα χαρακτηριστικά του μέσου μετάδοσης. Για το σκοπό αυτό χρησιμοποιούνται δύο τρόποι:

- Ο τρόπος baseband.
- Ο τρόπος broadband.

**Τα τοπικά δίκτυα baseband**

Με αυτό τον όρο συνήθως προσδιορίζουμε τα τοπικά που χρησιμοποιούν ασύγχρονη ψηφιακή μετάδοση. Η μέθοδος μετάδοσης είναι η baseband δηλαδή το σήμα μεταδίδεται στο μέσο χωρίς καμία διαμόρφωσης ( η δυαδική ακολουθία μεταδίδεται κατευθείαν στο μέσον).Μέσω αυτού του τρόπου μετάδοσης στα δίκτυα μπορούν να συνδεθούν όλοι οι τύποι υπολογιστικού εξοπλισμού:τερματικά, υπολογιστές κ.τ.λ

Αυτού του είδους τα δίκτυα δεν είναι και πολύ κατάλληλα για τη μετάδοση φωνής και κινούμενης εικόνας διότι είναι δύσκολος ο συγχρονισμός τους ένεκα του ότι η τεχνική μεταφοράς δεν εγγυάται καθορισμένο χρόνο μεταβίβασης. Επίσης είναι δύσκολη η μεταφορά video εικόνας ένεκα του απαιτούμενου βασικού εύρους ζώνης (2 μέχρι 200 Mbits/s) πράγμα που δεν προσφέρεται σε τέτοιου είδους δίκτυα.

**Τα τοπικά δίκτυα ευρείας ζώνης**

Ο τρόπος επικοινωνίας σε τέτοιου είδους δίκτυο είναι η πολυπλεξία συχνοτήτων. Δηλαδή, το εύρος συχνότητας μετάδοσης χωρίζεται σε διαφορετικές υποσυχνότητες και η κάθε μια από αυτές αφιερώνεται για τη μεταφορά ενός ορισμένου είδους πληροφορίας. Έτσι μπορούμε να 'χουμε κανάλια αφιερωμένα στη φωνή, στα data στον ήχο κ.τ.λ, όπως π.χ ένας μεγάλος αυτοκινητόδρομος που μπορεί να χωριστεί σε λωρίδες κυκλοφορίας και στην κάθε λωρίδα θα κυκλοφορούν αποκλειστικά ενός είδους οχήματα.

Εδώ μπορούμε να μεταφέρουμε πολλών ειδών πληροφορίες καθώς επίσης να εξασφαλίσουμε πολλές μεταδόσεις ανεξάρτητες μεταξύ τους. Τα δίκτυα broadband είναι πιο πολύπλοκα και λίγο πιο ακριβά στην εγκατάσταση γιατί χρειάζονται ειδικό εξοπλισμό για κάθε εφαρμογή σε σχέση με τα δίκτυα baseband. Αντίθετα παρέχουν μεγαλύτερες δυνατότητες σε ότι αφορά το ρυθμό μετάδοσης και τις αποστάσεις που μπορούν να καλύψουν.

## 3.3 Κατάταξη στα Τοπικά Δίκτυα

Μπορούμε να κατατάξουμε τα τοπικά δίκτυα σε κατηγορίες ανάλογα με το γεωγραφικό χώρο που καλύπτουν όπως:

- Τοπικά δίκτυα εγκαταστημένα μέσα σ' ένα χώρο όσο καταλαμβάνει ένα τμήμα μιας εταιρείας, δηλαδή μερικοί σταθμοί κατανεμημένοι στα γραφεία μερικών ορόφων. Θα λέγαμε ότι είναι αυτά τα οποία 'αγγίζουν' το χρήστη όπως π.χ τοπικό δίκτυο ETHERNET. Βασικός σκοπός τους είναι η επικοινωνία διαφόρων υπολογιστικών συστημάτων όπως π.χ Workstations, printers, κ.τ.λ
- Τοπικά δίκτυα μιας μεγάλης επιχείρησης δηλαδή αυτά επιτρέπουν τη διασύνδεση μικρότερων τοπικών δικτύων όπως αυτά που αναφέραμε στην προηγούμενη

κατηγορία. Τέτοιου είδους δίκτυο είναι το FDDI(Fiber Distributed Data Interface).

- Τοπικά βιομηχανικά δίκτυα που χρησιμοποιούνται στον αυτοματισμό και έλεγχο παραγωγής.

## 3.4 Οι Τεχνικές μεταγωγής

Υπάρχουν τριών ειδών τεχνικές μεταγωγής ή προσωρινής αποκατάστασης μιας σύνδεσης μεταξύ δύο σταθμών:

- Η μεταγωγή κυκλώματος
- Η μεταγωγή μηνυμάτων
- Η μεταγωγή πακέτων.

**Η μεταγωγή κυκλώματος (circuits)**

Είναι η τεχνική κατά την οποία πρώτα αποκαθίσταται ένας φυσικός δρόμος μεταξύ των συνδρομητών και κατόπιν αρχίζει η μετάδοση των δεδομένων από τον σταθμό εκπομπής προς το σταθμό προορισμού.

Καθ' όλη τη διάρκεια της επικοινωνίας οι δυο συνδρομητές χρησιμοποιούν αποκλειστικά αυτόν τον ίδιο δρόμο. Στο τέλος της επικοινωνίας το κύκλωμα διακόπτεται και οι φυσικοί δρόμοι που είχαν αποκατασταθεί μεταξύ των κόμβων απελευθερώνονται. Αυτή η τεχνική χρησιμοποιείται στα τηλεφωνικά δίκτυα είναι όμως ασύμφορη για τη μεταφορά δεδομένων λόγω του κενού χρόνου που παρατηρείται σε μια σύνδεση.

**Η μεταγωγή μηνυμάτων**

Αυτή συνίσταται στην προώθηση του μηνύματος από κόμβο σε κόμβο μέχρι τον παραλήπτη. Το δίκτυο αναλαμβάνει τη διεκπεραίωση του μηνύματος χρησιμοποιώντας ενδιάμεσους σταθμούς (π.χ. υπολογιστές επικοινωνίας) που αποθηκεύουν προσωρινά το μήνυμα μέχρι να βρεθεί ελεύθερος δρόμος. Η διεύθυνση του παραλήπτη είναι επάνω στο κάθε μήνυμα.

**Η μεταγωγή πακέτων**

Χρησιμοποιεί την ίδια λογική με την μεταγωγή μηνυμάτων με τη διαφορά ότι το κάθε μήνυμα τεμαχίζεται προηγουμένως σε πακέτα ορισμένου μήκους. Τα πακέτα προωθούνται από κόμβο σε κόμβο μέχρι τον τελικό σταθμό προορισμού. Αυτή η τεχνική απαιτεί την ύπαρξη ενδιάμεσου χώρου για να αποθηκεύονται τα πακέτα όπως γίνεται και κατά τη μεταγωγή μηνυμάτων.

## 3.5 Τοπολογίες

Η τοπολογία ενός τοπικού δικτύου περιγράφει τον τρόπο με τον οποίο συνδέονται μεταξύ τους οι διάφοροι κόμβοι ή σταθμοί.

Οι τοπολογίες μπορούν να ταξινομηθούν σε κατηγορίες εάν λάβουμε υπ'όψιν τα επόμενα κριτήρια:

- Τον τρόπο με τον οποίο συνδέονται δύο μονάδες του δικτύου δηλαδή αν υπάρχει ένας μοναδικός φυσικός 'δρόμος' που τις συνδέει
- Με πόσες γραμμές (κανάλια) είναι συνδεδεμένη η κάθε μονάδα
- κάθε γραμμή είναι μιας ή δυο κατευθύνσεων δηλαδή απλός δακτύλιος ,διπλός δακτύλιος, αλυσιδωτή πλήρης διασύνδεση

Στα τοπικά δίκτυα οι πιο συνηθισμένες τοπολογίες είναι η αστεριού(ή ακτινωτή,star, η αρτηρίας (bus), η δακτυλίου(ring).Χρησιμοποιούνται επίσης και κάποιοι σύνδεσμοι αυτών όπως η τοπολογία δέντρου(tree) και η τοπολογία αστεριού-δακτυλίου(star-ring).

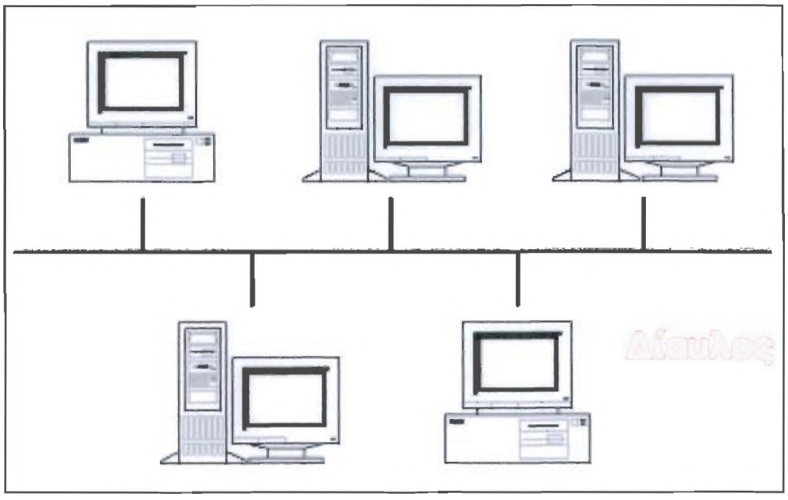
**Η τοπολογία κοινού δρόμου(bus)**

Αυτή η τοπολογία είναι πιο διαδεδομένη από την τοπολογία δακτυλίου και σ'αυτό μεγάλο ρόλο έπαιξε ETHERNET της XEROX.

Εδώ οι σταθμοί συνδέονται πάνω σ' ένα καλώδιο ορισμένου μήκους το οποίο λέγεται bus.Το μήνυμα που εκπέμπεται από οποιοδήποτε σταθμό, μπαίνει στον κοινό δρόμο για να φτάσει στον προορισμό του. Έτσι όλοι οι σταθμοί δέχονται όλα τα μηνύματα που περνάνε πάνω στο κοινό καλώδιο και μπορούν να τα κρατήσουν ή να τα αγνοήσουν, συγκρίνοντας στο πέρασμα τη διεύθυνση του μηνύματος με τη δική τους. Μπορούμε να διακρίνουμε δύο είδη bus:τα μονοκατευθυντήρια δηλαδή αυτά όπου η μετάδοση γίνεται προς μια μόνο κατεύθυνση και αυτά των δύο κατευθύνσεων.

Όπως θα δούμε πιο κάτω, υπάρχουν αρκετές τεχνικές για τον έλεγχο της χρήσης του bus.Η λήψη και η μετάδοση γίνεται πάνω σ' ένα μοναδικό κανάλι. Τα πλεονεκτήματα αυτής της τοπολογίας είναι η ομογένεια του δικτύου, η ευκολία με την οποία μπορεί να υλοποιηθεί, καθώς επίσης και το μικρό κόστος των γραμμών και των συσκευών διασύνδεσης. Παρ'όλες τις δυσκολίες που προέρχονται από τον ανταγωνισμό των σταθμών για την πρόσβαση στο μέσο μετάδοσης αυτές οι τεχνικές αποτελούν μια ενδιαφέρουσα λύση που επικράτησε σε πολλούς κατασκευαστές. Στην τοπολογία bus έχουν επικρατήσει οι τεχνικές μετάδοσης baseband. Επίσης σ'αυτού του είδους την τοπολογία η μη λειτουργία ενός κόμβου δεν έχει καμία σχεδόν συνέπεια στο δίκτυο.

Η απόδοση του εξαρτάται κυρίως από το εύρος ζώνης του bus, από τον αριθμό των κόμβων, από τα χρησιμοποιούμενα πρωτόκολλα προσπέλασης καθώς επίσης και από το είδος των μεταφερόμενων δεδομένων. Παραλλαγή αυτής της τοπολογίας είναι η τοπολογία δέντρου (tree), που χρησιμοποιείται για τις μετάδοσης ευρείας ζώνης και στα δίκτυα starlan.



**Σχήμα 3: Τοπολογία Διαύλου**

**Τοπολογία δακτυλίου (Ring)**

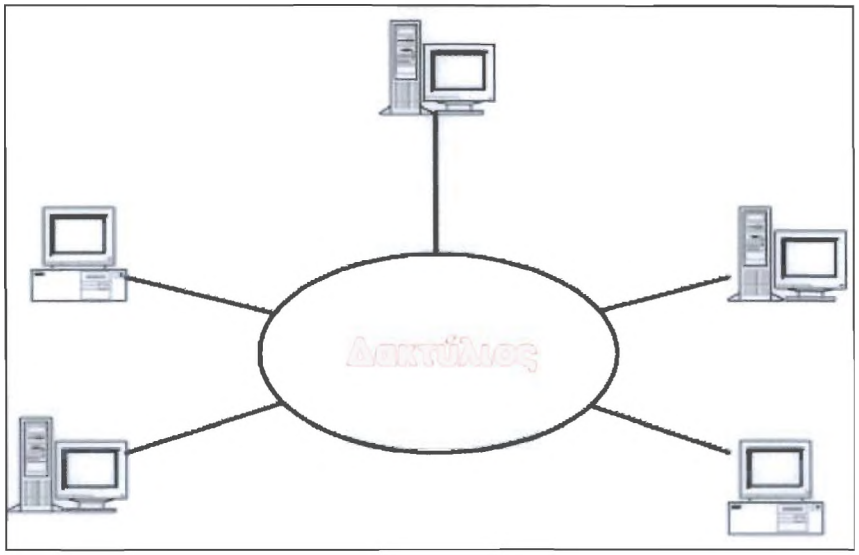
Σ' αυτή τη διάταξη η σύνδεση σταθμών με το φυσικό μέσο είναι τύπου από σημείου σε σημείο ( point to point) , έτσι ώστε να σχηματίζεται ένα κλειστό κύκλωμα όπως δείχνει το σχήμα. Η πληροφορία κυκλοφορεί προς μία μόνο κατεύθυνση κατά μήκος του καλωδιακού δρόμου. Ο κάθε σταθμός που παίρνει το μήνυμα το επαναμεταδίδει προς τον επόμενο μέχρις ότου επανέλθει στον αποστολέα. Επίσης ο κάθε κόμβος στο δίκτυο παίζει το ρόλο του αναμεταδότη (repeater).

Μπορούμε όμως να πραγματοποιήσουμε ένα δίκτυο δύο κατευθύνσεων χρησιμοποιώντας Δύο δακτυλίους με μετάδοση προς τις δύο κατευθύνσεις. Τα πλεονεκτήματα μιας κατεύθυνσης είναι:

- Η απλή δρομολόγηση γιατί υπάρχει ένας μοναδικός δρόμος μεταξύ σταθμού αποστολής και προορισμού.
- Κατά τη μετάδοση ο αποστολέας χρειάζεται να γνωρίζει μόνο τη διεύθυνση του παραλήπτη χωρίς να λαμβάνει υπ' όψιν τη γεωγραφική θέση αυτού.
- Η υλοποίηση είναι εύκολη.
- Η επένδυση μπορεί να ελαττωθεί ανάλογα με τον αριθμό των χρηστών.
- Αυτού του είδους η λύση επιτρέπει επίσης υψηλούς ρυθμούς μετάδοσης.

Οι διάφορες τοπολογίες δακτυλίου διακρίνονται μεταξύ τους ανάλογα με το μηχανισμό μετάδοσης που χρησιμοποιούν και ο οποίος παίζει ρόλο και στην απόδοση. Μπορούμε να φτάσουμε ρυθμούς των 100 Mbits/sec.

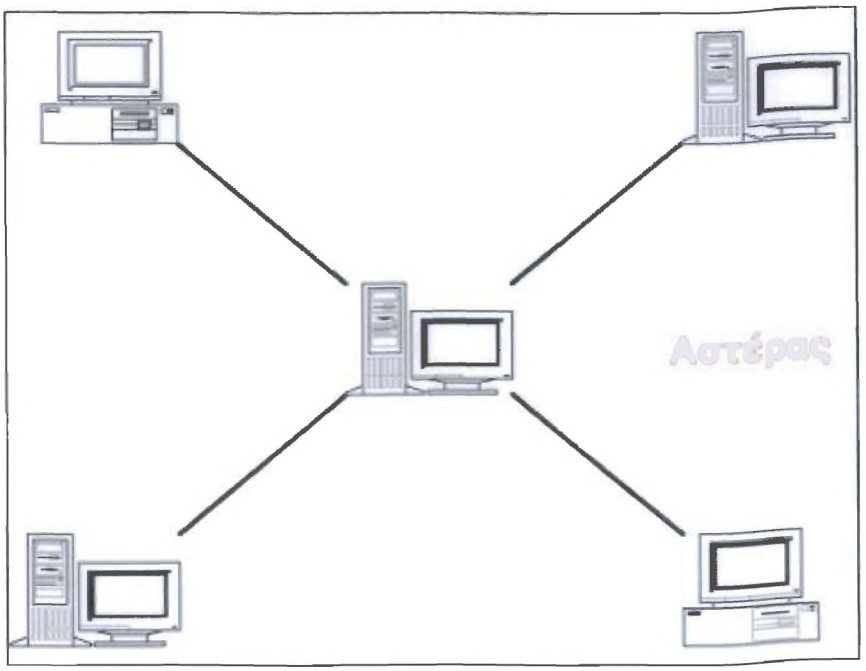
Σ' αυτού του είδους τα δίκτυα το πρόβλημα της αξιοπιστίας είναι κρίσιμο, γιατί όταν ένας σταθμός σταματήσει να λειτουργεί τότε όλο το δίκτυο παραλύει. Υπάρχουν όμως μέθοδοι, που επιτρέπουν τη λύση αυτού του προβλήματος π.χ χρησιμοποίηση διπλών οργάνων στα πιο ευαίσθητα σημεία.




**Σχήμα 2: Τοπολογία Δακτυλίου**

**Η τοπολογία αστέρα (Star)**

Αυτού του είδους η τοπολογία αποτελείται από έναν κεντρικό σταθμό με τον οποίο συνδέονται σημείο προς σημείο οι άλλοι σταθμοί. Ο κεντρικός σταθμός ελέγχει όλη την κυκλοφορία του δικτύου. Πριν τη μετάδοση ένας σταθμός ζητάει απ' τον κεντρικό σταθμό να αποκαταστήσει τη σύνδεση με τον σταθμό προορισμού.
Υπάρχουν δυο τύποι δικτύων τοπολογίας Star. Τα δίκτυα μεταγωγής κυκλώματος και τα δίκτυα μεταγωγής μηνυμάτων. Τέτοιου είδους τοπολογία χρησιμοποιείται στους PABX. Το σταμάτημα λειτουργίας ενός εξωτερικού σταθμού δεν παίζει μεγάλο ρόλο για το δίκτυο και αυτό είναι ένα από τα πλεονεκτήματα της τοπολογίας αυτής. Αντίθετα η μη λειτουργία του κεντρικού σταθμού παραλύει όλο το δίκτυο.
Οι δυνατότητες επέκτασης εξαρτώνται από τη δυνατότητα της κεντρικής μονάδας να μπορέσει να υποστηρίξει επιπλέον φόρτο κυκλοφορίας.




**Σχήμα 1: Τοπολογία Αστέρα**

## 3.6 Δημιουργία Δικτύου Ευρείας Περιοχής

Τα τοπικά δίκτυα υπολογιστών επιτρέπουν στους υπολογιστές να μοιράζονται πληροφορίες από σχετικά μικρές αποστάσεις, το πολύ μερικά μέτρα. Είναι συχνά επιθυμητό να μοιραζόμαστε πληροφορίες από μεγαλύτερες αποστάσεις, ας πούμε πολλών μιλίων ή ακόμα και ανάμεσα σε ηπείρους.

Τα δίκτυα αυτού του μεγέθους ονομάζονται δίκτυα ευρείας περιοχής (Wide area Networks-WAN). Ακολουθούν μερικά παραδείγματα αναγκών που μπορούν να καλυφθούν με την εγκατάσταση δικτύου ευρείας περιοχής.

- Ένας διανομέας ηλεκτρονικού εξοπλισμού έχει πολλές αποθήκες σε ολόκληρη την χώρα. Για να αναφέρει τις ώρες των παραδόσεων , κάθε πωλητής θα πρέπει να μπορεί να μαθαίνει το απόθεμα κάθε αντικείμενου σε κάθε αποθήκη ενώ παίρνει την παραγγελία από τον πελάτη.
- Μια πολυεθνική πετρελαϊκή εταιρία θέλει να μπορεί να στέλνει μηνύματα με το ηλεκτρονικό ταχυδρομείο στα γραφεία όλων των υποκαταστημάτων της σε ολόκληρο τον κόσμο.
- Ένα πείραμα κατά το οποίο παρατηρούνται οι περιβαλλοντογικές συνθήκες χρειάζεται να έχει πολλά απομακρυσμένα μηχανήματα, σκορπισμένα σε μια περιοχή αρκετών εκατοντάδων τετραγωνικών μιλίων, τα οποία δίνουν τα δείγματα τους μέσω υπολογιστών. Κάθε μηχάνημα λαμβάνει σήμα κάθε λεπτό. Κάθε μέρα, ένας κεντρικός υπολογιστής φορτώνει τα συγκεκριμένα στοιχεία για να τα αναλύσει.
- Μια αλυσίδα καταστημάτων ρούχων σε ολόκληρη τη χώρα έχει το ταμείο της σε κάθε τοποθεσία συνδεδεμένο με έναν PC. Κάθε μέρα, κατά το κλείσιμο, οι πληροφορίες σχετικά με τις πωλήσεις της ημέρας αποστέλλονται σε έναν υπολογιστή στο κεντρικό γραφείο του Σικάγο, όπου αναλύονται, ούτως ώστε να υπολογίζεται η κίνηση των χρημάτων, του αποθεματικού και των τάσεων της αγοράς.

Το χαρακτηριστικό των δικτύων ευρείας περιοχής είναι το γεγονός ότι οι πληροφορίες πρέπει να διασχίσουν αποστάσεις οι οποίες είναι πολύ μεγάλες για να συνδέσουν εύκολα με ένα καλώδιο. Συνεπώς πρέπει να βρούμε άλλους τρόπους για να στείλουμε τις πληροφορίες μας.

**Δύο είναι οι βασικοί κανόνες της δημιουργίας δικτύων ευρείας περιοχής :**

1. Όσο πιο μεγάλη είναι η σύνδεση των δεδομένων, τόσο πιο πολύ θα κοστίσει συνήθως η εγκατάσταση και η συντήρηση. Είναι κάτι ανάλογο με το γεγονός ότι πληρώνουμε περισσότερο για υπεραστικά τηλεφωνήματα.
2. Όσα περισσότερα δεδομένα πρέπει να σταλούν ανά χρονική μονάδα, τόσο περισσότερο θα στοιχίσει η εγκατάσταση και η συντήρηση της σύνδεσης δεδομένων.

Συνήθως, δεν μπορούμε να καθορίσουμε το μήκος της σύνδεσης δεδομένων. Απλά μας ανατίθεται η δουλειά να μεταφέρουμε πληροφορίες, για παράδειγμα, από το γραφείο της Νέας Υόρκης στο γραφείο του Μόντρεαλ. Συνεπώς, ο πρωταρχικός στόχος κατά τον σχεδιασμό ενός δικτύου ευρείας περιοχής είναι η μείωση της ποσότητας των δεδομένων που πρέπει να σταλούν σε μεγάλες αποστάσεις.

Υπάρχουν πολλοί τρόποι για να ελαχιστοποιηθούν τα δεδομένα. Ένας από τους πιο κοινούς τρόπους είναι χρησιμοποιώντας κωδικούς. Για παράδειγμα, αντί να περιγράψετε ένα γραφείο ως 'γραφείο από ξύλο βελανιδιάς, ύψους 30 ιντσών, πλάτους 56 ιντσών και βάθους 28 ιντσών, με τέσσερα συρτάρια, δύο εκ των οποίων

είναι 22Χ7 ίντσες και δύο είναι 22χ13 ίντσες', θα μπορούσατε απλά να του δώσετε τον κωδικό DO103 ή κάτι παρόμοιο. Εφόσον όλοι ξέρουμε τι σημαίνει ο κωδικός DO103, μπορούμε να αναφερόμαστε στο γραφείο με τον κωδικό ο οποίος είναι πολύ πιο σύντομος από την πλήρη περιγραφή.

Μπορούμε επίσης να μειώσουμε την ποσότητα των δεδομένων που πρέπει να στείλουμε, κάνοντας κάτι έξυπνο : να καθορίσουμε ακριβώς ποίες πληροφορίες πρέπει να στείλουμε. Ας υποθέσουμε ότι έχουμε μια μεγάλη βάση δεδομένων με αποθεματικό 15.000 κομματιών σε κάθε μία από τις 26 αποθήκες. Κατά τη διάρκεια μίας μέρας πουλάμε και συμπληρώνουμε κατά μέσο όρο το απόθεμα μόνο 400 διαφορετικών αντικειμένων σε κάθε αποθήκη. Στο τέλος κάθε εργάσιμης ημέρας, θέλουμε να ενημερώσουμε το κεντρικό αποθεματικό κατάλογο στο βασικό υπολογιστή στα κεντρικά γραφεία της εταιρείας. Για να το κάνουμε αυτό, έχουμε δύο επιλογές. Μπορούμε:

1. Να στείλουμε τον ολοκληρωμένο τρέχοντα κατάλογο αποθεματικού κάθε αποθήκης στον κεντρικό υπολογιστή, δηλαδή συνολικά 15.000 αντικείμενα Χ 26 αποθήκες = 390.000 πληροφορίες που πρέπει να μεταφερθούν, ή
2. Να στείλουμε απλά τις αλλαγές οι οποίες επήλθαν στο αποθεματικό της κάθε αποθήκης. Αν μια συνηθισμένη μέρα, μόνο 400 αντικείμενα ανά αποθήκη αλλάζουν στον κατάλογο του αποθεματικού, τότε χρειάζεται να στείλουμε μόνο 400 αντικείμενα Χ 26 αποθήκες = 10.400 πληροφορίες. Πρόκειται για 97% μείωση στη ποσότητα των πληροφοριών που πρέπει να σταλούν, και συνεπώς τρομακτική μείωση στο κόστος της αποστολής τους.

Ας ρίξουμε μια ματιά σε μερικούς από τους τρόπους με τους οποίους μπορούμε να στέλνουμε πληροφορίες σε μεγάλες αποστάσεις.

Τηλεφωνικές Γραμμές Διαχωρισμού Φωνής (Voice –Grade) Γνωρίζουμε όλοι καλά το τηλεφωνικό σύστημα. Είναι παγκόσμιο δίκτυο που μας επιτρέπει να επικοινωνούμε προφορικά με άλλους ανθρώπους σε ολόκληρο τον κόσμο. Το τηλεφωνικό σύστημα είναι τόσο συνηθισμένο, τόσο αξιόπιστο και τόσο εύχρηστο που μερικές φορές το θεωρούμε δεδομένο.

Το τηλεφωνικό σύστημα δημιουργήθηκε αρχικά για να επιτυγχάνεται φωνητική επικοινωνία. Γι αυτό τον λόγο, οι συνηθισμένες τηλεφωνικές γραμμές ονομάζονται συχνά και ως γραμμές διαχωρισμού φωνής. Αν και αυτές οι γραμμές σχεδιάστηκαν για φωνητική επικοινωνία, μπορούν να χρησιμοποιούνται επίσης και για τη μεταφορά δεδομένων υπολογιστή. Δυστυχώς οι εκπομπές ψηφιακών υπολογιστών δεν μπορούν συνήθως να χρησιμοποιηθούν απευθείας με τις συνηθισμένες τηλεφωνικές γραμμές. Όπως γνωρίζουμε οι τηλεφωνικές γραμμές είναι αναλογικές και συνεπώς οι τηλεφωνικές γραμμές σχεδιάστηκαν για να εκπέμπουν αναλογικά σήματα. Έτσι μια συσκευή που ονομάζεται διαμορφωτής/ αποδιαμορφωτής(modem) χρησιμοποιείται για να μεταφράζει τα σήματα που εκπέμπονται μέσω τηλεφωνικών γραμμών voice grade. Η εικόνα δείχνει πως χρησιμοποιούνται οι διαμορφωτές/ αποδιαμορφωτές με υπολογιστές και τηλέφωνα για να πραγματοποιηθεί η μεταφορά των δεδομένων. Στην πραγματικότητα, ο

διαμορφωτής/ αποδιαμορφωτής είναι ένας ειδικός μετατροπέας αναλογικού προς ψηφιακό και ψηφιακού προς αναλογικό σήμα.

Κατά τη λειτουργία, ο υπολογιστής στέλνει δεδομένα στον διαμορφωτή / αποδιαμορφωτή τα οποία μεταφράζονται σε σειρά ακουστικών τόνων (διαμορφωμένων) οι οποίοι εκπέμπονται μέσω του τηλεφώνου. Ο διαμορφωτής / αποδιαμορφωτής-παραλήπτης μετατρέπει πάλι τα διαμορφωμένα δεδομένα σε δεδομένα που ο υπολογιστής μπορεί να χρησιμοποιήσει ( αποδιαμόρφωση ). Έχετε υπόψη σας ότι όλοι οι διαμορφωτές / αποδιαμορφωτές μπορούν να στείλουν και να λάβουν δεδομένα.

Όπως ο ηλεκτρονικός εξοπλισμός του δικτύου, οι διαμορφωτές / αποδιαμορφωτές λειτουργούν σύμφωνα με ορισμένα πρωτόκολλα και συνεπώς, και οι δύο διαμορφωτές / αποδιαμορφωτές που συμμετέχουν σε μια επικοινωνιακή συνδιάλεξη πρέπει να λειτουργούν σύμφωνα με το ίδιο πρωτόκολλο. Τα πρωτόκολλα διαφέρουν αρχικά στην ταχύτητα με την οποία μπορούν να μεταφέρουν δεδομένα. Υπάρχουν πρωτόκολλα με ταχύτητα 300, 1200,2400,9600, 19200, 24400 και 28800 bps. Τα πρωτόκολλα με ταχύτητα 300, 1200 και 2400 bps είναι σχετικά στάνταρ. Δυστυχώς, υπάρχουν αρκετά πρωτόκολλα με ταχύτητα 9600 και άνω, καθώς και με άλλους ρυθμούς που τώρα πρωτοεμφανίζονται, γι αυτό πρέπει να προσέξετε ώστε και οι δύο διαμορφωτές/ αποδιαμορφωτές που επικοινωνούν να χρησιμοποιούν το ίδιο πρωτόκολλο.

Για να πάρετε κάποια ιδέα της ταχύτητας της επικοινωνίας ενός διαμορφωτή/ Αποδιαμορφωτή, μπορούμε μα μετατρέψουμε τα bps σε χαρακτήρες ανά δευτερόλεπτο διαιρώντας τα με το 8 ( εφόσον ένας χαρακτήρας είναι των 8 bit ). Ακόμα και ο πιο γρήγορος διαμορφωτής/ αποδιαμορφωτής , με ταχύτητα 19200 bps, μπορεί να στείλει μόνο περίπου 2400 χαρακτήρες (σχεδόν μία κανονική τυπωμένη σελίδα σε κείμενο) ανά δευτερόλεπτο. Μια σύνδεση Ethernet , σε αντίθεση, μπορεί να στείλει αρκετές εκατοντάδες σελίδες ανά δευτερόλεπτο. Μία σελίδα ανά δευτερόλεπτο δεν είναι άσχημη ταχύτητα όταν θέλουμε να στείλουμε ένα σύντομο έγγραφο, αλλά αν θέλουμε να στείλουμε μια βάση δεδομένων 15 Megabyte με αυτή την ταχύτητα θα μας πάρει σχεδόν δύο ώρες.

Παρά τους αργούς ρυθμούς μεταφοράς, υπάρχουν πολλά πλεονεκτήματα που ευνοούν τη χρήση τηλεφωνικών γραμμών διαχωρισμού φωνής , αν η ταχύτητα δεν είναι τόσο σημαντική. Όπως αναφέραμε νωρίτερα, το τηλεφωνικό σύστημα χρησιμοποιείται ευρέως και είναι αξιόπιστο και εύκολο στη χρήση. Τα τηλέφωνα είναι, επίσης, κι ένας σχετικά οικονομικός τρόπος για να στέλνουμε δεδομένα σε μεγάλες αποστάσεις.

Υπάρχουν δυο σημαντικά είδη τηλεφωνικών υπηρεσιών διαχωρισμού φωνής οι οποίες να χρησιμοποιούνται σε δίκτυα ευρείας περιοχής :

1. Η υπηρεσία dial -up είναι η τηλεφωνική υπηρεσία διαχωρισμού φωνής που όλοι γνωρίζουμε. Για να χρησιμοποιήσουμε μια γραμμή dial –up, ο διαμορφωτής/ αποδιαμορφωτής επιλέγει τη σειρά χτύπων και τόνων που αντιπροσωπεύουν το νούμερο τηλεφώνου του κόμβου με τον οποίο θέλουμε να επικοινωνήσουμε. Το τηλέφωνο του παραλήπτη χτυπάει και ο διαμορφωτής/ αποδιαμορφωτής του

απαντάει ολοκληρώνοντας την σύνδεση. Η τηλεφωνική εταιρεία χρεώνει αυτόν που πήρε τηλέφωνο σύμφωνα με το χρόνο του τηλεφωνήματος. Η γραμμή dial – up έχει δύο πλεονεκτήματα:

- Χρεωνόμαστε μόνο για τη διάρκεια της επικοινωνιακής συνδιάλεξης (δηλαδή , του τηλεφωνήματος).
- Μπορούμε να αλλάξουμε την τοποθεσία με την οποία επικοινωνούμε απλά κλείνοντας το τηλέφωνο και πληκτρολογώντας κάποιο άλλο νούμερο.

2. Η μισθωμένη γραμμή (leased line) είναι μια τηλεφωνική γραμμή, που χρησιμοποιείται συνήθως για επικοινωνία μέσω υπολογιστών, η οποία τρέχει ανάμεσα σε δυο συγκεκριμένα σημεία. Η μισθωμένη γραμμή δε μπορεί να αλλάξει προορισμό τόσο εύκολα όσο μια γραμμή dial- up. Η τηλεφωνική εταιρεία χρεώνει ένα καθορισμένο μηνιαίο ποσό για απεριόριστη χρήση της μισθωμένης γραμμής, με κόστος ανάλογο με την απόσταση την οποία καλύπτει.

Οι μισθωμένες γραμμές είναι πιο οικονομικές για εφαρμογές κατά τις οποίες επικοινωνούν τακτικά απομακρυσμένες περιοχές. Για όχι και τόσο συχνή επικοινωνία , πιο οικονομικές είναι συνήθως οι γραμμές dial –up.

# Κεφάλαιο 4

# Διασυνδέσεις Τοπικών Δικτύων

## 4.1 Διασυνδέσεις

Βλέπουμε ότι όλο και πιο πολύ είναι αναγκαίο να επιτρέψουμε σε χρήστες τοπικών δικτύων να κάνουν χρήση κοινών βάσεων δεδομένων ή άλλων πόρων και εξοπλισμού που δε βρίσκονται στον ίδιο γεωγραφικό χώρο που καλύπτει το τοπικό τους δίκτυο π.χ. οι χρήστες ενός τοπικού δικτύου μιας μεγάλης επιχείρησης με μονάδες παραγωγής που βρίσκονται σε διαφορετικές περιοχές χρειάζονται, να επικοινωνήσουν με τον κεντρικό Η/Υ μέσω ενός δικτύου π.χ Χ.25. Επίσης, υπάρχουν ανάγκες ανταλλαγής πληροφοριών μεταξύ χρηστών περισσοτέρων τοπικών δικτύων.
Για τη διασύνδεση τοπικών δικτύων πρέπει να ληφθούν υπ' όψιν ορισμένοι παράγοντες όπως:

- Η ποικιλία των πρωτοκόλλων που χρησιμοποιούνται στα διάφορα δίκτυα.
- Το είδος υπηρεσιών που παρέχει το κάθε δίκτυο.
- Το είδος των προδιαγραφών που πρέπει να ληφθούν υπ' όψιν για τη διασύνδεση τους
- Το είδος των συσκευών που χρησιμοποιείται γι' αυτή.

Μια διασύνδεση λέγεται **ομογενής** όταν συνδέει δίκτυα που χρησιμοποιούν τα ίδια πρωτόκολλα. Αυτή επιτυγχάνεται με τη χρήση συσκευών που λέγονται γέφυρες **(Bridges).**
Λέγεται δε ετερογενής εάν εμπλέκει πρωτόκολλα διαφορετικού τύπου. Αυτή επιτυγχάνεται με τη χρήση συσκευών που λέγονται **πύλες (Gateways).**Μία πύλη χρησιμοποιείται κυρίως για τη διασύνδεση ενός τοπικού με μεγάλο δημόσιο δίκτυο ή για τη διασύνδεση δύο διαφορετικών τοπικών δικτύων και πραγματοποιεί τις αναγκαίες προσαρμογές ταχυτήτων και πρωτοκόλλων.

## 4.2 Οι Γέφυρες

Κατά γενικό τρόπο θεωρούμε σαν γέφυρα μια συσκευή διασύνδεσης τοπικών δικτύων που έχουν διαφορετικές μεθόδους προσπέλασης, αλλά τα πρωτόκολλα των υψηλότερων επιπέδων είναι ίδια. Η λειτουργικότητα αυτών των οργάνων διασύνδεσης είναι απλή γιατί επεμβαίνουν στα χαμηλά επίπεδα, (κάτω από το επίπεδο δικτύου).

Όταν πρόκειται για απομακρυσμένα τοπικά δίκτυα η διασύνδεση γίνεται μέσω ενός άλλου δικτύου μεγάλης απόστασης και χρησιμοποιούνται δυο γέφυρες (μια για κάθε τοπικό δίκτυο). Οι γέφυρες λειτουργούν σαν φίλτρα που επιτρέπουν να μεταδίδονται μόνο τα μηνύματα που πρέπει να μεταδίδονται από δίκτυο σε δίκτυο.

**Ποια είναι τα κύρια χαρακτηριστικά τους**

- Τα πρωτόκολλα του LLC και επάνω δεν τις βλέπουν γιατί οι γέφυρες εργάζονται στο ύψος του υποεπιπέδου MAC. Δε μετατρέπουν ούτε ερμηνεύουν πληροφορίες του πεδίου Data των πλαισίων.
- Δε χρειάζεται να αναφερθεί η διεύθυνση τους στο frame για να εκτελέσουν το ρόλο τους σαν όργανα διασύνδεσης.
- Πραγματοποιούν την ανάλογη προσαρμογή ταχυτήτων των δυο δικτύων που συνδέουν. Αυτή γίνεται χρησιμοποιώντας μια τεχνική αποθήκευσης και αποστολής των μηνυμάτων (store forward).
- Επιτρέπουν τη χρήση διαφορετικών μέσων μετάδοσης για κάθε δίκτυο και μπορούν να διασυνδέσουν τουλάχιστον δυο δίκτυα.
- Εξασφαλίζουν τη μετάδοση μηνυμάτων σε ομάδα σταθμών.

**Πως λειτουργούν**

Μια γέφυρα που συνδέει δυο δίκτυα βλέπει να περνάνε απ' αυτήν όλα τα μηνύματα. Κατά το πέρασμα ελέγχει τη διεύθυνση του αποδέκτη και τη διεύθυνση του αποστολέα. Με τη βοήθεια ενός πίνακα αναγνωρίζει τους ενεργούς σταθμούς στο δίκτυο. Μόνο τα μηνύματα των οποίων ο αποστολέας και ο αποδέκτης δεν ανήκουν στο ίδιο δίκτυο μεταβιβάζονται από το ένα δίκτυο προς το άλλο.

## 4.3 Οι δρομολογητές(routers)

Για να επιτευχθεί η μεταβίβαση μηνυμάτων από δίκτυο σε δίκτυο χρησιμοποιούνται επίσης συσκευές που λέγονται **Routers(δρομολογητές).**
Βασική λειτουργία ενός router είναι να προσδιορίσει τον καταλληλότερο δρόμο για τη διαβίβαση ενός πακέτου από ένα σημείο σ' 'ένα άλλο. Για να το πετύχουν αυτό οι routers χρησιμοποιούν διάφορους αλγόριθμους δρομολόγησης ανάλογα με την τεχνική μεταφοράς που χρησιμοποιείται (δηλαδή datagram ή νοητό κύκλωμα): στην τεχνική datagram η απόφαση για τον επόμενο κόμβο λαμβάνεται κατά την άφιξη του πακέτου στο router ενώ με την τεχνική μεταγωγής κυκλώματος ο δρόμος είναι ο ίδιος για όλη τη διάρκεια της σύνδεσης. Σε αντίθεση με τις γέφυρες οι οποίες συνδέουν δίκτυα ίδιας τοπολογίας π.χ. Ethernet με Ethernet, οι routers μπορούν να συνδέσουν διαφορετικά δίκτυα με την προϋπόθεση ότι έχουν το ίδιο πρωτόκολλο στο επίπεδο (3) δικτύου.

Ο πιο παλιός απ' τους αλγόριθμους δρομολόγησης είναι ο **RIP(routing information protocol)** που χρησιμοποιείται στα δίκτυα TCP/IP και σταθμούς UNIX. Βασίζεται σε αρχεία διευθύνσεων σε κάθε κόμβο για να εκτελέσει τη δρομολόγηση.
Ο αλγόριθμος IGRP (Interior Gateway Routing Protocol) αποτελεί βελτιστοποίηση του προηγούμενου γιατί εισάγει και άλλες παραμέτρους (εκτός από διευθύνσεις) όπως π.χ. ρυθμό μετάδοσης, ενδιάμεση χρονική διάρκεια, καθυστερήσεις, φόρτο γραμμής κ.τ.λ.

Για τη διασύνδεση δικτύων X25 χρησιμοποιείται ένα ειδικό πρωτόκολλο το X75. Πιο συγκεκριμένα το X75 είναι πρωτόκολλο ανταλλαγής πληροφοριών μεταξύ πυλών (Getaways) στα δίκτυα X25.

Για δίκτυα μεγάλων αποστάσεων όπως π.χ το δίκτυο FDDI χρησιμοποιούνται διαφορετικά πρωτόκολλα δρομολόγησης όπως το **IS.IS (Intermediate System to Intermediate System), και ο OSPF( Open shortest path first)** που μπορούν να υποστηρίξουν απεριόριστο αριθμό από routers.

## 4.4 Οι Πύλες

Οι πύλες είναι εξοπλισμός που επιτρέπει τη διασύνδεση δικτύων με διαφερετικά πρωτόκολλα π.χ SNA και ISO, TCP/IP και Decnet κ.τ.λ.. Μια πύλη θα χρησιμοποιηθεί κυρίως για να συνδέσει ένα τοπικό δίκτυο με ένα μεγάλο δημόσιο δίκτυο ή ένα τοπικό δίκτυο με ένα άλλο διαφορετικό δίκτυο.

Η πύλη είναι μια γενική έννοια ενός οργάνου διασύνδεσης δικτύων και συνήθως όταν χρησιμοποιείται στο επίπεδο 3 λέγεται router. Τα συνδεόμενα δίκτυα δεν είναι υποχρεωτικό να είναι δομημένα σύμφωνα με το μοντέλο ISO.

Σε αντίθεση με μια γέφυρα μια πύλη εργάζεται σε υψηλότερα επίπεδα OSI (δηλ 3 και πάνω). Π.χ μια πύλη στο επίπεδο 3 που διασύνδεση δίκτυα πρωτοκόλλων IP εκτελεί πράξεις όπως η δρομολόγηση, τεμαχισμός πακέτων, μέτρηση διάρκειας χρόνου που καταναλώθηκε από το πακέτο για να διασχίσει το δίκτυο κ.τ.λ. Δυο είδη πυλών είναι γνωστά: αυτές που διασυνδέουν δίκτυα υπηρεσιών με σύνδεση και αυτές που διασυνδέουν δίκτυα με σύνδεση χρειάζονται πιο πολύ ενδιάμεση μνήμη για την αποθήκευση ενδιάμεσων πακέτων έτσι ώστε να αποφευχθούν φαινόμενα συμφόρησης.

**Πύλες επιπέδου 4**

Επιτρέπουν την προσαρμογή διαφορετικών κλάσεων πρωτοκόλλων μεταφοράς.

**Πύλες επιπέδων 5,6,7**

Αυτές λέγονται πύλες υψηλότερων επιπέδων και επιτρέπουν την υλοποίηση διαλόγων μεταξύ εφαρμογών (μεταφορά αρχείων, διαχείριση μηνυμάτων, διαχείριση δικτύων κ.τ.λ). που βρίσκονται σε ετερογενή συστήματα (δηλ συστήματα που δεν έχουν την ίδια εσωτερική κωδικοποίηση).

## 4.5 Λειτουργικότητες μιας συσκευής διασύνδεσης

Για τη διασύνδεση δυο δικτύων χρειάζεται προ πάντων καλή γνώση των δυο δικτύων. Ο εξοπλισμός που θα κάνει τη διασύνδεση θα πρέπει ίσως να προσαρμόσει τις ταχύτητες των δικτύων, το μήκος των πακέτων που κυκλοφορούν κ.τ.λ.
Ας πάρουμε το παράδειγμα διασύνδεσης δικτύων που λειτουργούν το ένα με την τυποποίηση IEEE 802.5 και το άλλο με την τυποποίηση IEEE 802.3.
Αυτά, όπως ξέρουμε, χρησιμοποιούν διαφορετικές μεθόδους προσπέλασης και διαφορετικά frames. Άρα η συσκευή θα πρέπει:

- Να προσαρμόσει το μήκος των frames αφού αυτά έχουν διαφορετικό μήκος με πιθανή προσθήκη bits ώστε να επιτευχθεί το αναγκαίο μήκος του frame.
- Να προσαρμόσει τις μορφές των frames διότι μερικά πεδία αυτών δεν έχουν το ίδιο μήκος και μερικά άλλα μάλιστα δεν υπάρχουν και στα δυο δίκτυα.
- Να εκτελέσει μια αναδιάταξη των bits μέσα στο κάθε byte γιατί τα bytes στέλνονται με αντίθετη σειρά στο 802.5 από ότι στο 802.3
- Να υπολογίσει πάλι το FCS αν το frame άλλαξε μορφή.
- Να αναγνωρίσει ορισμένα frames που δε χρειάζεται να μεταδοθούν όπως π.χ το πλαίσιο του Token ή τα πλαίσια που κυκλοφορούν για τον έλεγχο του δικτύου. π.χ το Token δεν έχει καμία έννοια στο IEEE 802.3.

# Κεφάλαιο 5

# Internet

## Εισαγωγή

Σε αντίθεση με τα καλά ορισμένα και αμετάβλητα σύνορα μιας χώρας, τα σύνορα του Internet είναι σε μια συνεχή κατάσταση ροής και ανανέωσης. Το Internet, σαν εικονικό κομμάτι software, computing και networking, είναι απείρως ανανεώσιμο και ευπροσάρμοστο, με αποτέλεσμα να μεγαλώνει και να αλλάζει κάθε μέρα.

Ο ευμετάβλητος χαρακτήρας του Internet και η διείσδυση του σε κάθε γωνιά της υφηλίου, έχουν δημιουργήσει ένα πλούσιο και συχνά απρόβλεπτο περιβάλλον στο οποίο τα κοινά ενδιαφέροντα και η εμπειρία είναι μερικές φορές περισσότερο σημαντικά από τα γεωπολιτικά και κοινωνικά σύνορα που διαχωρίζουν τους χρήστες του. Αυτή η μίξη έχει δημιουργήσει μια συλλογή από παγκόσμια χωριά με την ασυνήθιστη ιδιότητα ότι πολλοί άνθρωποι στο Internet μένουν σε περισσότερα από ένα παγκόσμια χωριά κάθε χρονική στιγμή.

Η εμβέλεια, η πολυπλοκότητα και η μεγαλοπρέπεια του συστήματος που έχουμε σήμερα δεν είχε ποτέ προβλεφθεί. Κοιτάζοντας το Internet του σήμερα, ακόμα με τα μάτια της δεκαετίας του '90, θα μπορούσε κανείς μόνο να αναρωτηθεί για αυτή του την εξέλιξη. Και εξέλιξη είναι ο σωστός όρος. Όπως και η σύνθετη ζωή σχηματίζεται από άλλες απλούστερες, μέσα από γενετικά πειράματα, έτσι και το Internet είναι ένα αναπτυσσόμενο και συστηματοποιημένο εικονικό περιβάλλον. Αλλά, με τη ματιά του σήμερα, αποτελεί επίσης και μία επανάσταση γιατί μεταμορφώνει την κουλτούρα μας.

Η ελευθερία της έκφρασης και πρόσβασης σε πληροφορίες στο Internet είναι επαναστατική. Κατά κάποιο τρόπο, το Internet έχει κάνει κάθε δημιουργό, εκδότη δίνοντας ένα νέο νόημα στη φράση «desktop publishing». Οι κοινωνικές και επιχειρηματικές μας ενέργειες επηρεάζονται ορατά. Το εκπαιδευτικό μας σύστημα μπορεί να υποβληθεί σε αλλαγές καθώς εργαλεία για παραγωγή και διαμοίραση γνώσης

αναμειγνύονται με νέους τρόπους σφυρηλάτησης μαθητών σε μαθησιακές εμπειρίες. Ήδη οι νομοθέτες αναρωτιούνται για το τι μπορεί να προκύψει από ένα online σώμα εκλεκτόρων.

Υπάρχουν βέβαια μειονεκτήματα όσον αφορά τη ροή της πληροφορίας στο Internet. Το πιο προφανές είναι η δυσκολία της εύρεσης απλών αντικειμένων στις απέραντες θάλασσες του διαθέσιμου υλικού. Οι δέκτες της πληροφορίας έπρεπε να γίνουν πραγματικά επιλεκτικοί και σκεπτόμενοι ταξιδιώτες, να ταξινομούν και να αποτιμούν την πληροφορία που τους είναι διαθέσιμη ασταμάτητα, καθώς πλέουν στους ηλεκτρονικούς ωκεανούς και ψάχνουν για πολύτιμο περιεχόμενο. Πράγματι, σαν χρυσός στον ωκεανό, το πολύτιμο περιεχόμενο του Internet είναι τεράστιο σε ποσότητα αλλά δύσκολο να βρεθεί και ακόμη περισσότερο γιατί αυτό αναπαράγεται καθημερινά. Το browsing δίνει νέα ώθηση σε προσπάθειες για εύρεση και τοποθέτηση νέων επιχειρηματικών ευκαιριών στον κατάλογο της ανθισμένης θάλασσας πληροφορίας.

Ήδη ξέρουμε ότι υπάρχουν κάποια ανεπιθύμητα μειονεκτήματα, και πολλοί φαίνονται να προβληματίζονται από την ελευθερία της έκφρασης που το Internet προκαλεί και υποστηρίζει. Έχουν υπάρξει προσπάθειες για κάποιου είδους λογοκρισία ή τουλάχιστον για κάποιο έλεγχο εισόδου για τους ηλικιακά μικρότερους που έχουν πρόσβαση στο Internet. Άλλοι κατηγορούν τη χρήση του δικτύου σαν σημείο συσπείρωσης ομάδων των οποίων οι απόψεις και οι συμπεριφορές, θεωρούνται αντικοινωνικές, καταστροφικές ή ακόμη και προδοτικές. Το τεχνικό και νόμιμο framework της λειτουργίας του Internet θα πρέπει να αντιμετωπίσει την αναταραχή της αστραπιαίας ανάπτυξης μέσα από τη δικιά του διαδικασία εξέλιξης. Αλλά πολλά από αυτά που οι χρήστες μπορούν να βρουν, τα οποία προσφέρονται σαν αποτέλεσμα εργασίας, αγάπης και μοιρασιάς, είναι αμφίβολης ποιότητας και αξίας. Μπορούμε χωρίς αμφιβολία να περιμένουμε για επεκτάσεις του Internet που θα οδηγήσουν σε πλουσιότερα, περισσότερο εκφραστικά μοντέλα επικοινωνίας, συμπεριλαμβανομένου βελτιωμένου ήχου και γραφικών, όπως επίσης ελπίζουμε ότι οι χρήστες θα ωφεληθούν από αυτά τα εργαλεία για ανθρωπιστικούς και έξυπνους σκοπούς.

Ο WWW εκτοξεύθηκε στο Internet μέσα από μια διαδοχική έκρηξη νέων εφαρμογών, μειώνοντας την φαινομενική πολυπλοκότητα της εύρεσης και της χρήσης πληροφοριών αυξάνοντας συγχρόνως την μεγαλοπρέπεια της βασικής του δομής. Το Internet έχει εξελιχθεί με τη βοήθεια του WWW ο οποίος θα συνεχίσει σχεδόν σίγουρα να αναπτύσσεται προς σημαντικότερες δυνατότητες. Η πρόσφατη επίδειξη ανταλλαγής dynamic software από server σε client ή το αντίθετο σηματοδοτεί μια νέα περίοδο με περισσότερη ευελιξία.

Αυτά τα ηλεκτρονικά και computer-based εργαλεία καλούνται «οι τεχνολογίες της ελευθερίας». Φυσικά αυτό έχει το μειονέκτημά του. Σε αυτή τη φράση είναι κρυμμένη η καλή και η μη καλή πλευρά της ανθρώπινης φύσης. Η φιλανθρωπία και η συντροφικότητα διασταυρώνονται με την αγένεια και την απληστία, αλλά αυτό είναι το τίμημα που πληρώνουμε για την ελευθερία της πληροφορίας.

Μακροχρόνιοι κάτοικοι του δικτύου παλεύουν με τα μειονεκτήματα που προέκυψαν από τη μετατροπή της μικρής αυτής πόλης, με τη φιλική ατμόσφαιρα των παλαιότερων χρόνων, σε μια μεγαλούπολη που η φασαρία της φαίνεται να μην έχει όρια. Καθώς οι επιχειρηματικές δραστηριότητες μέσω Internet ωριμάζουν, αρχίζει να δίνεται περισσότερη προσοχή στην ασφάλεια, στην προστασία των προσωπικών δεδομένων και

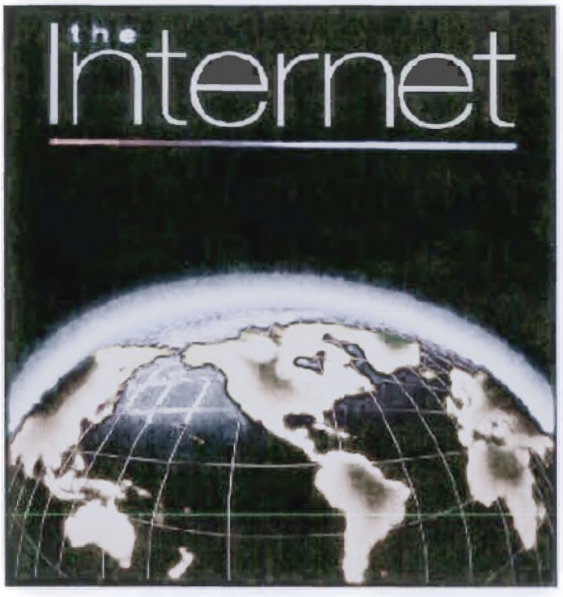
στην εξουσιοδότηση των συναλλαγών που λαμβάνουν χώρα στο περιβάλλον του Internet. Το Internet φαίνεται να πάλλεται από την ενέργεια και τις ιδέες εκατομμυρίων προβλημάτων και καταναλωτών.

Ας σκεφτούμε ένα σημαντικό πλεονέκτημα του Internet : την αυξανόμενη χρήση των αγγλικών. Και όχι μόνο. Πολλές άλλες γλώσσες χρησιμοποιούνται στο Internet και για το λόγο αυτό έγινε η πρόσφατη εργασία για να βελτιωθούν τα τεχνικά standard που χρησιμοποιούνται στα e-mail και σε άλλα επικοινωνιακά πρωτόκολλα για να εξυπηρετηθεί όχι μόνο η χρήση του ASCII (σύνολο χαρακτήρων βασισμένο στην αγγλική γλώσσα). Πράγματι, κυρίως δύο φαινόμενα παρατηρούνται. Τα αγγλικά υποστηρίζονται ευρέως, αλλά παράλληλα και άλλες γλώσσες γίνονται κοινές με ολοένα αυξανόμενο τρόπο. Πολλές εκφράσεις που βρίσκονται στο Internet είναι πολύγλωσσες.(«Πατήστε το κουμπί για αγγλικά, αυτό είναι για γαλλικά, και αυτό για ιαπωνικά»). Με αυτόν τον τρόπο, θα διατηρηθεί και επίσης θα παραταθεί η εκτίμηση και η χρήση των άλλων γλωσσών. Το Internet θα διατηρήσει και θα παρατείνει την μεγαλοπρέπεια της παγκόσμιας, πολιτιστικής κληρονομιάς.

Δεν μπορεί να υπάρξει τυπωμένος κατάλογος που να περιέχει όλο το Internet. Και αυτό γιατί απλώς το Internet αλλάζει τόσο γρήγορα, με τόσες νέες βάσεις δεδομένων, υπηρεσίες, διευθύνσεις και projects τα οποία δεν μπορούν να ενθυλακωθούν καθαρά σε κάποιο σύνολο εντολών ή σταθερών. Όσο χρησιμοποιεί κανείς το Internet, τόσο συνειδητοποιεί ότι κάθε μέρα αποτελεί μια ολοένα αυξανόμενη διαδικασία εκμάθησης.

## 5.1 Τι είναι το internet

Το Internet είναι ένα πλέγμα από εκατομμύρια διασυνδεδεμένους υπολογιστές που εκτείνεται σχεδόν σε κάθε γωνιά του πλανήτη και παρέχει τις υπηρεσίες του σε εκατομμύρια χρήστες. Αποτελεί ένα "**Παγκόσμιο Ηλεκτρονικό Χωριό**", οι "**κάτοικοι**" του οποίου, ανεξάρτητα από υπηκοότητα, ηλικία, θρήσκευμα και χρώμα, μοιράζονται πληροφορίες και ανταλλάσσουν ελεύθερα απόψεις πέρα από γεωγραφικά και κοινωνικά σύνορα. Σύμφωνα με τις σχετικές εκτιμήσεις, αυτός ο παγκόσμιος ιστός υπολογιστών και χρηστών αριθμεί σήμερα πάνω από δέκα εκατομμύρια υπολογιστές και εκατό εκατομμύρια χρήστες, ενώ επεκτείνεται διαρκώς με εκθετικούς ρυθμούς. Αναμένεται ότι το 2000 το Internet θα εξυπηρετεί περισσότερους από ένα δισεκατομμύριο χρήστες.




**Μερικοί ορισμοί**

**1)** Το Internet είναι ένα **διαδίκτυο**, δηλαδή ένα δίκτυο αποτελούμενο από δίκτυα υπολογιστών.
**2)** Τι είναι **δίκτυο** υπολογιστών:

Δύο ή περισσότεροι υπολογιστές που συνδέονται μεταξύ τους σχηματίζουν ένα δίκτυο. Οι κυριότεροι λόγοι ύπαρξης ενός δικτύου είναι:

- να μπορούν οι χρήστες των υπολογιστών να επικοινωνούν μεταξύ τους και
- να χρησιμοποιούν από απόσταση τις υπηρεσίες που προσφέρει κάποιος υπολογιστής του δικτύου.

3) Ένα σύνολο από κανόνες που ονομάζεται **πρωτόκολλο δικτύωσης**, καθορίζει το πώς επικοινωνούν μεταξύ τους οι υπολογιστές του δικτύου.

4) Η φυσική διάταξη των συνδέσεων του δικτύου ονομάζεται **τοπολογία**. Οι τρεις πιο συνηθισμένες τοπολογίες είναι:

- **Αστέρας (star)**

  Υπάρχει ένας κεντρικός υπολογιστής στον οποίον συνδέονται οι υπόλοιποι υπολογιστές του δικτύου.

- **Δακτύλιος (ring)**

  Όλοι οι υπολογιστές είναι συνδεδεμένοι σε έναν πλήρη κλειστό δακτύλιο.

- **Δίαυλος (bus)**

  Όλοι οι υπολογιστές συνδέονται κατά μήκος ενός κεντρικού αγωγού.

5) Τα δίκτυα, ανάλογα με το **εύρος της περιοχής** που καλύπτουν, χωρίζονται σε 3 κατηγορίες:

- **Τοπικά Δίκτυα (Local Area Network - LAN)**

  υπολογιστές που βρίσκονται στο ίδιο ή σε γειτονικά κτίρια.

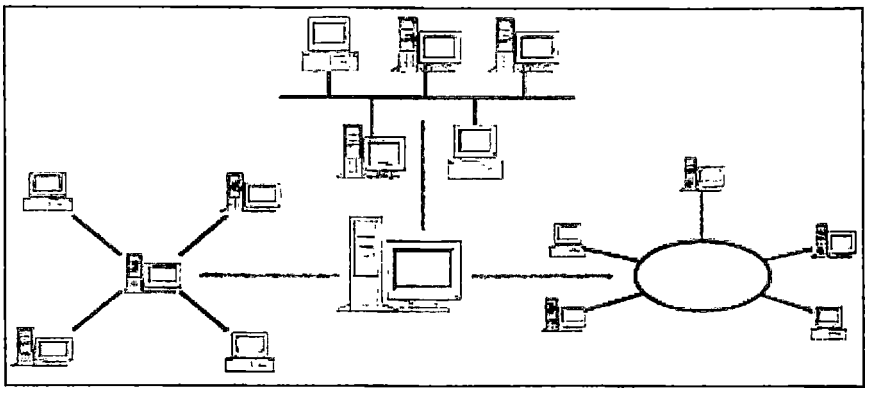
- **Δίκτυα Μητροπολιτικής Περιοχής (Metropolitan Area Network - MAN)**

Συνδέουν υπολογιστές που απέχουν μεταξύ τους μεσαίες αποστάσεις, π.χ. υπολογιστές που βρίσκονται σε διαφορετικά σημεία της ίδιας πόλης.

- **Δίκτυα Ευρείας Περιοχής (Wide Area Network - WAN)**

Συνδέουν υπολογιστές που απέχουν μεταξύ τους μεγάλες αποστάσεις, π.χ. υπολογιστές που βρίσκονται σε διαφορετικές πόλεις.

6) **Διαδίκτυο** είναι ένα δίκτυο από δίκτυα. Π.χ. τρία διαφορετικά τοπικά δίκτυα μπορούν να συνδεθούν μεταξύ τους σχηματίζοντας ένα διαδίκτυο, όπως φαίνεται στην εικόνα που ακολουθεί:



**Σχήμα 4: Ένα δίκτυο δικτύων**

7) Με τον όρο "**Internet**" δεν εννοούμε οποιοδήποτε διαδίκτυο, αλλά το **Παγκόσμιο Διαδίκτυο**, δηλαδή η συνένωση των χιλιάδων δικτύων διαφόρων μεγεθών που καλύπτει σχεδόν ολόκληρη την υδρόγειο.

Πώς συνδέονται όλοι αυτοί οι υπολογιστές μεταξύ τους; Είναι εύκολο να συνδέσουμε δύο υπολογιστές που βρίσκονται στον ίδιο χώρο με την βοήθεια ενός καλωδίου. Όταν η απόσταση μεταξύ των υπολογιστών μεγαλώνει, χρησιμοποιούνται διάφοροι τρόποι σύνδεσης, όπως κοινές τηλεφωνικές γραμμές, μισθωμένες τηλεπικοινωνιακές γραμμές διαφόρων τεχνολογιών, ασύρματες ζεύξεις και ακόμη, συνδέσεις μέσω τηλεπικοινωνιακών δορυφόρων όταν απαιτείται η μετάδοση δεδομένων πάνω από πολύ μεγάλες αποστάσεις.

**Δύο βασικά χαρακτηριστικά του Internet**

1) Ένα βασικό χαρακτηριστικό του Internet είναι ότι μπορεί να **συνδέει υπολογιστές διαφορετικού τύπου**, δηλ. υπολογιστές που μπορεί να διαφέρουν όσον αφορά την αρχιτεκτονική του υλικού (hardware), το λειτουργικό σύστημα που χρησιμοποιούν και το πρωτόκολλο δικτύωσης που εφαρμόζεται στο τοπικό τους δίκτυο. Ακριβώς εξαιτίας αυτής της ευελιξίας του, εξαπλώθηκε σε ολόκληρο τον πλανήτη κατά τη διάρκεια των τελευταίων δεκαετιών.

2) Ένα άλλο ενδιαφέρον χαρακτηριστικό του Internet είναι ότι είναι **αποκεντρωμένο** και **αυτοδιαχειριζόμενο**. Δεν υπάρχει δηλαδή κάποιος κεντρικός οργανισμός που να το διευθύνει και να παίρνει συνολικά αποφάσεις σχετικά με το είδος των πληροφοριών που διακινούνται, τις υπηρεσίες που παρέχονται από τους διάφορους υπολογιστές του ή τη διαχείρισή του. Καθένα από τα μικρότερα δίκτυα που το αποτελούν διατηρεί την αυτονομία του και είναι το ίδιο υπεύθυνο για το είδος των πληροφοριών που διακινεί, τις υπηρεσίες που προσφέρουν οι υπολογιστές του και τη διαχείρισή του.

### 5.1.1 Τι μας προσφέρει το Internet

Οι άνθρωποι χρησιμοποιούν το Internet βασικά για δύο πράγματα: α) για να **αντλήσουν πληροφορίες** και β) για να **επικοινωνήσουν** με άλλους ανθρώπους που είναι κι αυτοί χρήστες του.

Μπορούμε να θεωρήσουμε το Internet σαν μια τεράστια αποθήκη πληροφορίας, μια παγκόσμια βιβλιοθήκη. Στους υπολογιστές του, βρίσκονται αποθηκευμένα χιλιάδες Gigabytes πληροφορίας, αρκετά από τα οποία διατίθενται ελεύθερα στους χρήστες του. Έτσι λοιπόν έχουμε τη δυνατότητα να χρησιμοποιούμε απομακρυσμένες βάσεις δεδομένων, να ανακτάμε αρχεία με προγράμματα, εικόνες, κείμενα, κλπ., να έχουμε πρόσβαση σε βιβλιοθήκες, να διαβάζουμε ηλεκτρονικές εφημερίδες και περιοδικά, ακόμη και να παρακολουθούμε ραδιοφωνικά προγράμματα.

Το Internet είναι επίσης ένα μέσο που μας επιτρέπει να ερχόμαστε σε επαφή με άλλους ανθρώπους γρήγορα και εύκολα. Μπορούμε λοιπόν να ανταλλάξουμε ηλεκτρονικά μηνύματα ή να μιλήσουμε «ζωντανά» με έναν φίλο μας που βρίσκεται π.χ. στις ΗΠΑ, στην Κίνα ή σε κάποιο άλλο μέρος του κόσμου, να γνωρίσουμε καινούργιους ανθρώπους, να εγγραφούμε σε λίστες συζητήσεων εάν μας ενδιαφέρουν οι απόψεις των άλλων γύρω από κάποιο θέμα ή ακόμη να παίξουμε μια σειρά από παιχνίδια με πολλούς αντιπάλους ταυτόχρονα που μπορεί να βρίσκονται διασκορπισμένοι σε διάφορα μέρη της γης.

Με το Internet λοιπόν μπορούμε να κάνουμε το γύρο του κόσμου χωρίς να χρειαστεί να μετακινηθούμε από τον υπολογιστή μας.

## 5.2 Επικοινωνία και ενημέρωση μέσω internet

Από τον πρώτο καιρό της εμφάνισής του, το Internet είναι συνυφασμένο κυρίως μ' ένα στόχο: να διευκολύνει τους ανθρώπους να επικοινωνούν μεταξύ τους χρησιμοποιώντας υπολογιστές.

Το Internet δημιουργήθηκε για να επιτρέψει στους πανεπιστημιακούς ερευνητές να μοιράζονται τις σκέψεις, την εργασία και τις πηγές τους και στους στρατιωτικούς να επικοινωνούν μεταξύ τους στην περίπτωση πολέμου ή πυρηνικής επίθεσης. Σήμερα, δύο και πλέον δεκαετίες μετά την έναρξη των πρώτων δικτύων τα οποία μεγένθυναν το Internet, το Δικτύου παραμένει κυρίως ένα επικοινωνιακό μέσο. Εκατομμύρια ανθρώπων απ' όλο τον κόσμο μοιράζονται σκέψεις, ελπίδες, κουτσομπολιά, σχόλια και εργασίες στα καλώδια και τα υπολογιστικά συστήματα που δημιουργούν το Internet. Πολλά από τα μέσα επικοινωνίας, όπως το ηλεκτρονικό ταχυδρομείο έχουν αλλάξει ελάχιστα τα τελευταία 20 χρόνια. Από την άλλη, επινοήθηκαν εντελώς νέοι τρόποι επικοινωνίας, όπως η χρήση του Internet ως μέσο τηλεφωνίας, εκμηδενίζοντας τα κόστη υπεραστικών κλήσεων σε οποιοδήποτε μέρος του κόσμου. Τεχνολογίες επιτρέπουν στους χρήστες να επικοινωνούν ιδιωτικά ένας προς ένα, άλλες επιτρέπουν την επικοινωνία σε τεράστιες ομάδες συζητήσεων που βρίσκονται διεσπαρμένες σε ολόκληρο τον κόσμο, ενώ άλλες επιτρέπουν και την ιδιωτική επικοινωνία με ένα άτομο και την δημόσια επικοινωνία με μεγαλύτερες ομάδες.

## 5.3 World Wide Web (www) και Web Browsing

Η ιστορία του Internet είναι ουσιαστικά η ιστορία του παγκόσμιου ιστού (World Wide Web). Αρχικός σκοπός εμφάνισης του WWW ήταν το μοίρασμα πληροφοριών για την πυρηνική φυσική. Ο Web είναι το πιο ενδιαφέρον, το πιο πρωτοποριακό και το ταχύτερα αναπτυσσόμενο τμήμα του Internet. Η εκρηκτική ανάπτυξη του Web τα τελευταία χρόνια, έχει προκαλέσει σε μεγάλο βαθμό το έντονο ενδιαφέρον του κόσμου για το Internet. Όταν οι άνθρωποι αναφέρονται στον όρο surfing στο Internet, συνήθως μιλούν για τον World Wide Web.

σύνδεση κλείνει. Μόλις ζητήσουμε μια άλλη σελίδα, π.χ. κάνοντας κλικ πάνω σε έναν σύνδεσμο, η ίδια διαδικασία αρχίζει ξανά. Αυτό επαναλαμβάνεται πολλές φορές, σε αντίθεση π.χ. με το FTP που διατηρεί ανοικτή γραμμή καθ' όλη τη διάρκεια της σύνδεσης. Αυτός ακριβώς ο τρόπος επικοινωνίας εξηγεί και τα πολλαπλά μηνύματα που πιθανόν να βλέπουμε στην τελευταία γραμμή της οθόνης του browser όταν προσπαθεί να εμφανίσει μία Web σελίδα ("Contacting Host...", κλπ.)

Η κατανομή της εργασίας μεταξύ του browser και του Web server επιταχύνει τη διαδικασία με πολλούς τρόπους, αλλά σημαίνει επίσης ότι οι δημιουργοί Web σελίδων δεν μπορούν να ελέγξουν την τελική τους εμφάνιση, η οποία **εξαρτάται από το πώς είναι διαμορφωμένος ο browser**. Για παράδειγμα, ο δικός μας browser μπορεί να χρησιμοποιεί τη γραμματοσειρά Times-Roman για την παρουσίαση του κειμένου, ενώ ο browser ενός άλλου χρήστη μπορεί να χρησιμοποιεί τη γραμματοσειρά Helvetica.

Καθώς "σερφάρουμε" στο Internet χρησιμοποιώντας τον browser μας, προβάλλουμε στην οθόνη του υπολογιστή μας σελίδες που μπορεί να προέρχονται από πολλούς διαφορετικούς Web servers. **Από την ίδια Web σελίδα** μπορεί να ξεκινούν σύνδεσμοι προς άλλες σελίδες που βρίσκονται διασκορπισμένες **σε διάφορους Web servers ανά τον κόσμο**. Έτσι καθώς επιλέγουμε συνδέσμους, ταξιδεύουμε από υπολογιστή σε υπολογιστή μέσα στον Κυβερνοχώρο του Internet.

## 5.4 Το File Transfer Protocol (FTP)

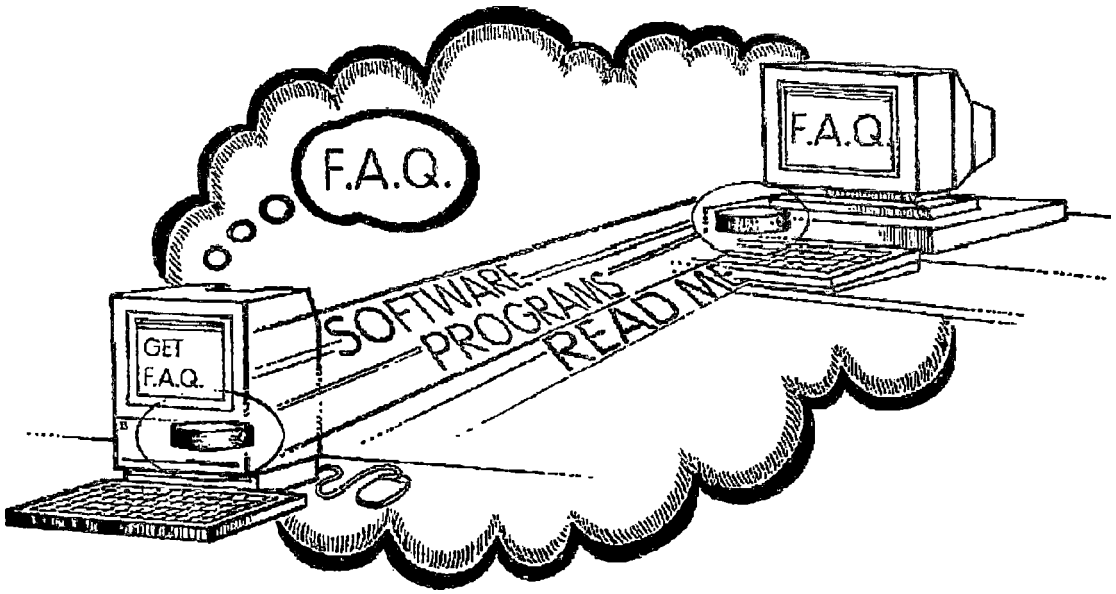
Μία από τις πλέον δημοφιλείς χρήσεις του Internet είναι το File Transfer (Σχήμα 16), δηλαδή η μεταφορά αρχείων από έναν απομακρυσμένο υπολογιστή του Internet σε τοπικό υπολογιστή και αντίστροφα. Οι συγκεκριμένοι υπολογιστές μπορούν να χρησιμοποιούν τελείως διαφορετικά λειτουργικά συστήματα. Ανήκει στο application layer του Internet protocol suite.

Το FTP είναι ένα πρωτόκολλο των 8 bit που στηρίζεται στο client/server. Είναι ικανό να διαχειριστεί οποιοδήποτε είδος αρχείου, χωρίς να χρειάζεται περαιτέρω επεξεργασία, όπως τα MIME και Uuencode. Τα εν λόγω αρχεία μπορεί να είναι διαφόρων τύπων: εκτελέσιμα προγράμματα, γραφικά, ήχοι και μουσική ή κείμενα.

Καθημερινά δεκάδες χιλιάδες αρχεία «κατεβαίνουν» από το Internet. Τα περισσότερα από τα εν λόγω αρχεία «κατεβαίνουν» με τη χρήση του πρωτοκόλλου FTP (File Transfer Protocol). Το FTP μπορεί να χρησιμοποιηθεί επίσης για το «ανέβασμα» αρχείων από τον υπολογιστή μας στο Internet. Ωστόσο, το FTP έχει ιδιαίτερα υψηλό latency. Αυτός ο χρόνος, ανάμεσα στην αρχική στιγμή της αίτησης και στην έναρξη της λήψης των επιθυμητών δεδομένων, μπορεί να είναι αρκετά μεγάλος, και μερικές φορές είναι απαραίτητη η διαδικασία διατήρησης του login για μεγάλο χρονικό διάστημα.

Το FTP συνήθως τρέχει συνήθως σε δύο ports, το 20 και το 21. Το port 20 (datastream) είναι για την μεταφορά δεδομένων μεταξύ client και server. Το port 21 (control stream) είναι το port από το οποίο περνάνε οι εντολές στον ftp server. Ενώ μεταφέρονται τα

δεδομένα μέσα από το data stream, το control stream παραμένει αδρανές. Αυτό μπορεί να προκαλέσει προβλήματα σε μεγάλες μεταφορές δεδομένων διαμέσου firewalls, μιας και τα sessions τους λήγουν μετά από μεγάλα χρονικά διαστήματα αδράνειας. Ενώ το αρχείο μπορεί να μεταφερθεί με επιτυχία, το session του ελέγχου μπορεί να αποσυνδεθεί από το firewall, προκαλώντας την παραγωγή λαθών.




**Σχήμα 16. Το File Transfer μοιάζει με «διάβασμα της σκέψης»**

Το FTP, όπως και πολλές άλλες πηγές του Internet, υιοθετούν το client/server μοντέλο. Στον υπολογιστή μας τρέχουμε το λογισμικό FTP client το οποίο συνδέεται σε έναν FTP server στο Internet. Από τη μεριά του FTP server υπάρχει ένα ειδικό λογισμικό, ονόματι FTP daemon, το οποίο μας επιτρέπει να «κατεβάζουμε» και να «ανεβάζουμε» αρχεία. Για να συνδεθούμε σ' ένα FTP site και να «κατεβάσουμε» αρχεία, χρειάζεται να δώσουμε τον αριθμό του λογαριασμού μας ή το username μας και ένα password. Το FTP daemon αναλαμβάνει τον έλεγχο των προαναφερθέντων στοιχείων πριν επιτρέψει την είσοδο του χρήστη στο FTP site. Ορισμένα sites επιτρέπουν σε όλους να μπαίνουν και να «κατεβάζουν» αρχεία, παρά το γεγονός ότι ζητούν την πληκτρολόγηση του αριθμού του λογαριασμού και του password. Αρκετά συχνά επίσης μπορούμε να μπούμε ανώνυμα, με το username μας και την ηλεκτρονική μας διεύθυνση να παίζουν το ρόλο του password. Τα sites που ακολουθούν αυτήν την πολιτική ονομάζονται anonymous FTP sites. Τέλος, ορισμένα FTP sites είναι ιδιωτικά, επιτρέποντας την είσοδο μόνο σε συγκεκριμένους ανθρώπους, οι οποίοι είναι εφοδιασμένοι με αριθμό λογαριασμού και password.

Το FTP είναι αρκετά εύχρηστο. Όταν συνδεόμαστε σε ένα FTP site μπορούμε να πλοηγηθούμε στα διαθέσιμα αρχεία αλλάζοντας directories, ενώ σε κάθε directory μπορούμε να δούμε έναν κατάλογο των διαθέσιμων αρχείων. Όταν εντοπίσουμε το αρχείο που θέλουμε να «κατεβάσουμε» χρησιμοποιούμε το client λογισμικό μας για να

δώσουμε εντολή στον FTP server να μας στείλει το αρχείο. Η μεγάλη εξάπλωση του World Wide Web απλοποίησε περαιτέρω το «κατέβασμα» του λογισμικού.

Μπορούμε πλέον να χρησιμοποιούμε το Web browser και να κάνουμε κλικ σε links που παραπέμπουν σε αρχεία. Στο παρασκήνιο το FTP αναλαμβάνει συνήθως το «κατέβασμα» των αρχείων. Το FTP παραμένει ο πιο δημοφιλής τρόπος για να «κατεβάσουμε» αρχεία από τον Web και το Internet.

Το πρωτόκολλο HTTP μπορεί να χρησιμοποιηθεί επίσης για το «κατέβασμα» αρχείων από τον Web αλλά δεν είναι τόσο αποτελεσματικό όσο το FTP και ως εκ τούτου δεν χρησιμοποιείται τόσο συχνά.

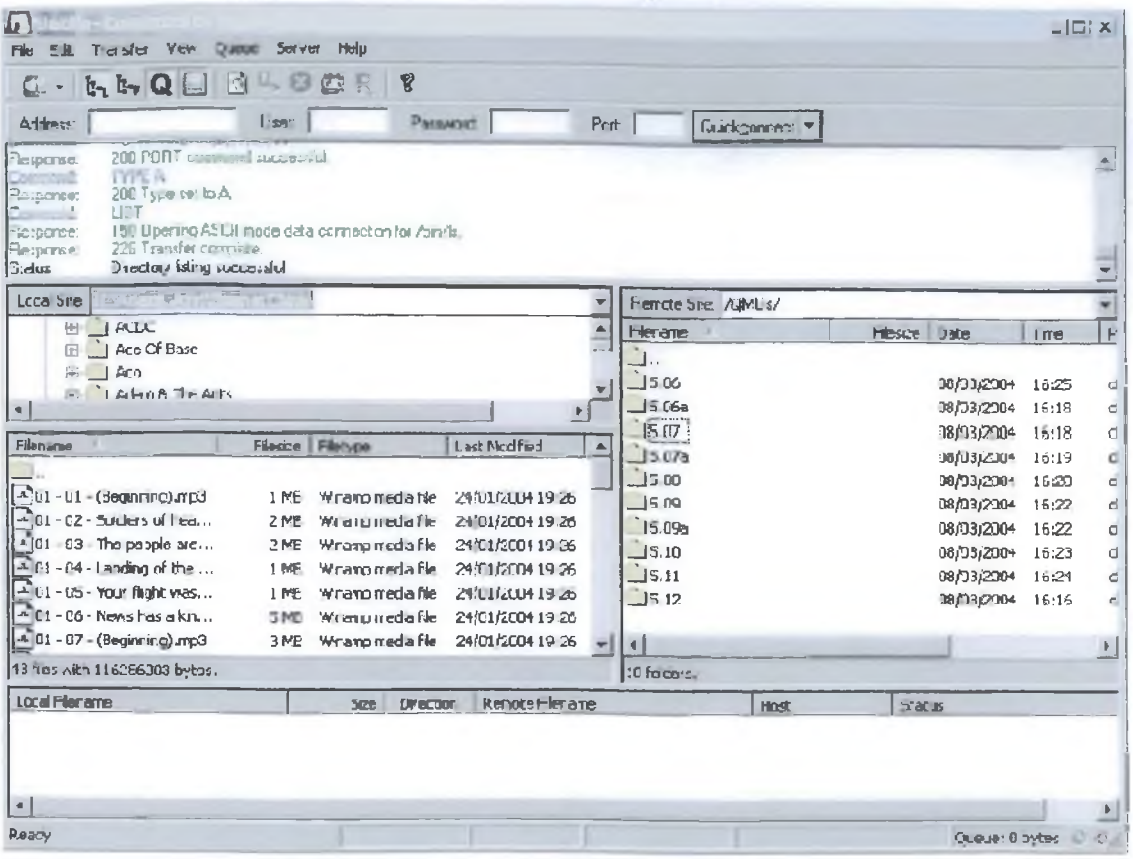
Ένα πρόβλημα με το «κατέβασμα» αρχείων στο Internet είναι το μεγάλο μέγεθος ορισμένων αρχείων. Στην περίπτωση αυτή ο απαιτούμενος χρόνος για το «κατέβασμά» τους είναι εξαιρετικά μεγάλος ιδίως στην περίπτωση της σύνδεσης μέσω modem. Για να επιταχυνθεί η διαδικασία αλλά και για να εξοικονομηθεί χώρος στον FTP server τα αρχεία πολύ συχνά συμπιέζονται - μειώνεται δηλαδή το μέγεθός τους με τη χρήση ειδικών προγραμμάτων συμπίεσης. Αναλόγως του είδους του αρχείου η συμπίεση μπορεί να κυμανθεί από 10 ως 50%. Αφού έχει ολοκληρωθεί το «κατέβασμα» των συμπιεσμένων αρχείων θα πρέπει να χρησιμοποιήσουμε στον υπολογιστή μας το λογισμικό συμπίεσης για να τα αποσυμπιέσουμε πριν τα χρησιμοποιήσουμε.

**Οι στόχοι του FTP είναι:**

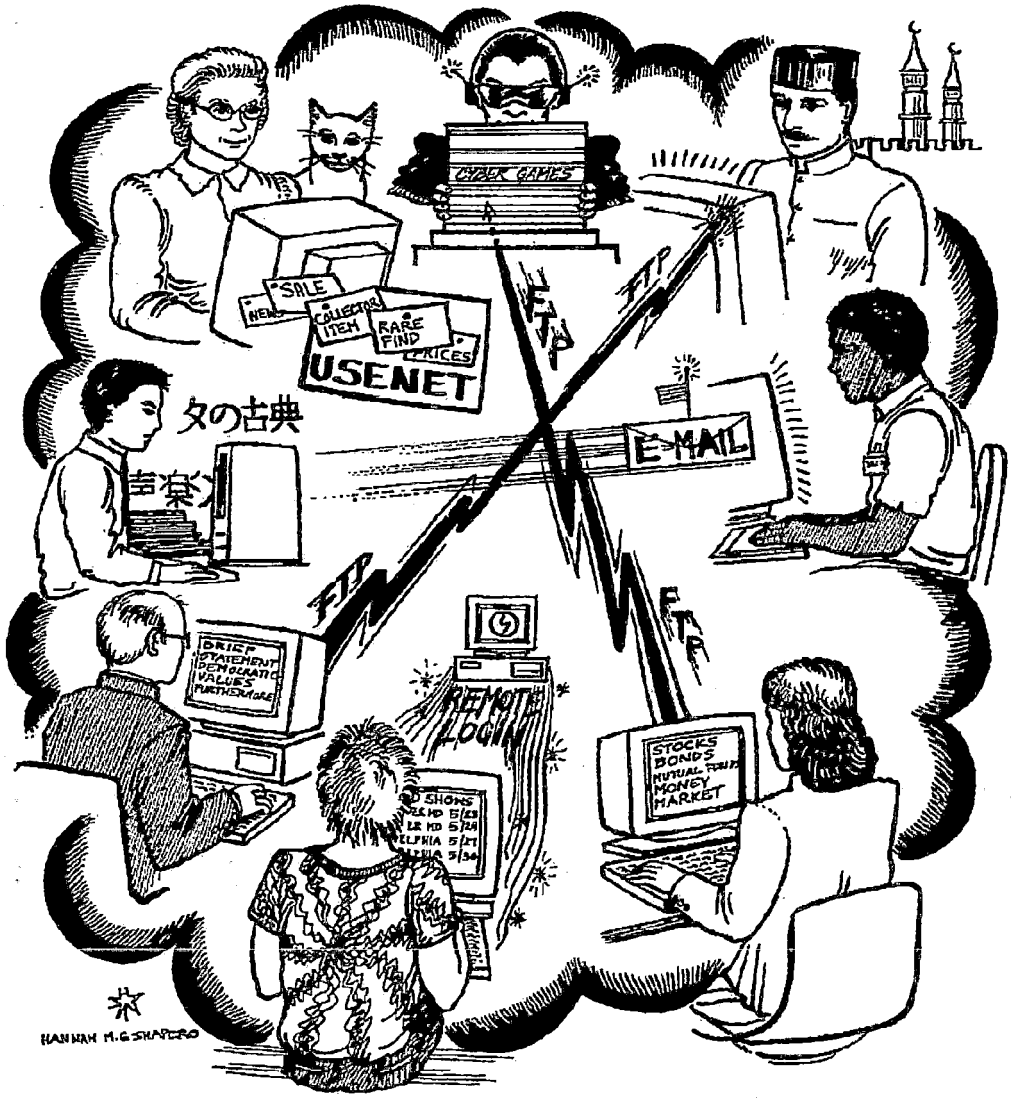
1. Να συμβάλλει θετικά στην διαμοίραση αρχείων (προγραμμάτων υπολογιστών και /ή δεδομένα).
2. Να ενθαρρύνει την έμμεση ή την υπονοούμενη χρήση των απομακρυσμένων υπολογιστών.
3. Να διαφυλάξει έναν χρήστη από παραλλαγές σε συστήματα διαφύλαξης των δεδομένων ανάμεσα σε διαφορετικούς hosts.
4. Να μεταφέρει δεδομένα αξιόπιστα και ικανοποιητικά.

**Τα μειονεκτήματά του είναι:**

1. Τα passwords και περιεχόμενα των αρχείων στέλνονται με την μορφή κειμένων, επιτρέποντας την υποκλοπή, η οποία είναι ανεπιθύμητη.
2. Είναι δύσκολο να φιλτράρουμε την κίνηση του FTP που βρίσκεται σε active mode από τη μεριά του client χρησιμοποιώντας ένα firewall, μιας και ο client πρέπει να έχει ανοιχτό ένα τυχαίο port προκειμένου να κάνει τη σύνδεση. Αυτό το πρόβλημα λύνεται με τη χρήση του FTP σε passive mode.
3. Είναι πιθανό να ζητήσουμε από τον server να συνδεθεί με ένα αυθαίρετο port ενός τρίτου υπολογιστή.
4. Το FTP, παρόλο που χρησιμοποιείται άμεσα από έναν χρήση μέσω κάποιου τερματικού, έχει σχεδιαστεί κυρίως για χρήση από FTP client προγράμματα (Σχήμα 17).




**Σχήμα 17. FileZilla 2.2.1b FTP client για Windows 2000**


CYBER GAMES
SALE
NEW
COLLECTN ITEM
RARE FIND
PRICES
USENET
FTP
FTP
夕の古典
E-MAIL
FTP
FTP
BRIEF STATEMENT DEMOCRATIC VALUES FURTHERMORE
REMOT LOGIN
SHOWS
STOCKS BONDS MUTUAL FUNDS MONEY MARKET
HANNAH M.G SHAPERO

## 5.5 Ηλεκτρονικό Ταχυδρομείο (e-mail)


Το ηλεκτρονικό ταχυδρομείο (electronic mail) ή e-mail αποτελεί το συχνότερα χρησιμοποιούμενο χαρακτηριστικό του Internet. Μπορούμε να το χρησιμοποιήσουμε για να στέλνουμε μηνύματα σε οποιονδήποτε είναι συνδεδεμένος στο Δικτύου ή σε ένα δίκτυο το οποίο διαθέτει μία σύνδεση στο Internet. Εκατομμύρια χρήστες στέλνουν και λαμβάνουν e-mail καθημερινά. Το e-mail αποτελεί έναν εξαιρετικό τρόπο να διατηρούμε επαφή με συγγενείς και φίλους οι οποίοι βρίσκονται μακριά και να επικοινωνούμε με τους συναδέλφους μας που βρίσκονται σε διαφορετικά τμήματα της επιχείρησης. Ο κάθε χρήστης έχει την δική του προσωπική διεύθυνση.

Τα μηνύματα ηλεκτρονικού ταχυδρομείου στέλνονται με τον ίδιο τρόπο όπως και τα περισσότερα δεδομένα του Internet. Το πρωτόκολλο TCP «σπάει» τα μηνύματα σε πακέτα, εν συνεχεία το πρωτόκολλο IP παραδίδει τα πακέτα στον σωστό προορισμό και, τέλος, το TCP συναρμολογεί ξανά το μήνυμα έτσι ώστε να είναι αναγνώσιμο από τον υπολογιστή. Στα μηνύματα ηλεκτρονικού ταχυδρομείου μπορούμε επίσης να επισυνάψουμε δυαδικά αρχεία, όπως εικόνες, βίντεο, ήχους και εκτελέσιμα αρχεία. Επειδή το Internet δεν μπορεί να διαχειριστεί απ' ευθείας δυαδικά αρχεία στο ηλεκτρονικό ταχυδρομείο, το αρχείο πρέπει πρώτα να κωδικοποιηθεί με τη χρήση ενός σχήματος κωδικοποίησης.

Τα πιο δημοφιλή σχήματα είναι το MIME και το uuencode. Ο χρήστης που λαμβάνει το επισυναπτόμενο δυαδικό αρχείο (το οποίο ονομάζεται attachment) πρέπει να αποκωδικοποιήσει το αρχείο με το ίδιο σχήμα που χρησιμοποιήθηκε για την κωδικοποίηση. Τα περισσότερα πακέτα ηλεκτρονικού ταχυδρομείου αναλαμβάνουν πλέον αυτή τη διαδικασία αυτόματα. Όταν στέλνουμε ένα e-mail σε κάποιον στο Internet, το μήνυμα συχνά ταξιδεύει μέσω μιας σειράς δικτύων μέχρι να φτάσει στον παραλήπτη. Σε πολλές δε περιπτώσεις τα δίκτυα μπορεί να χρησιμοποιούν διαφορετικά

format ηλεκτρονικού ταχυδρομείου. Τα gateways αναλαμβάνουν το βάρος της μετατροπής μεταξύ των διαφόρων formats ηλεκτρονικού ταχυδρομείου από το ένα δίκτυο στο άλλο, επιτρέποντας έτσι στα μηνύματα να ταξιδέψουν μεταξύ των διαφόρων δικτύων στο Internet.

# Κεφάλαιο 6

# Ασφάλεια στο Διαδίκτυο

## Εισαγωγή

Ολοένα και περισσότερο υπολογιστές συνδέονται μόνιμα στο internet. Αυτό, πέρα από τα προφανή πλεονεκτήματα, κρύβει σημαντικούς κινδύνους, που στην περίπτωση των εταιρικών χρηστών γίνονται ιδιαίτερα κρίσιμοι. Δείτε ποίες είναι οι συνηθέστερες απειλές και πώς με απλά βήματα θα τις αντιμετωπίσετε.

Καθώς ολοένα και περισσότερες εταιρίες και γραφεία συνδέονται μόνιμα στο internet και όλο και περισσότερα έγγραφα και κρίσιμα, ακόμα και για την ύπαρξη της ίδιας της εταιρείας, δεδομένα διατηρούνται μόνο ηλεκτρονικά, η ασφάλεια των υπολογιστικών συστημάτων αποκτά ιδιαίτερη σημασία.

Η ασφάλεια ενός υπολογιστικού συστήματος που συνδέεται στο internet , δεν μπορεί σε καμία περίπτωση να θεωρείτε ένα επιπλέον συστατικό, το οποίο «καλό θα ήταν να υπάρχει», αλλά θα πρέπει να λαμβάνεται υπ' όψη στον αρχικό σχεδιασμό του.
Καθώς η χώρα μας δεν μπορεί να θεωρηθεί από τις πιο εξελιγμένες στον κόσμο, όσον αφορά στη διείσδυση των υπολογιστών, τόσο στο δημόσιο όσο και στον ιδιωτικό τομέα, παρουσιάζεται μάλιστα η ευκαιρία να δημιουργηθεί τουλάχιστον η κατάλληλη υποδοχή εξαρχής.

Τι σημαίνει όμως 'ασφαλές δίκτυο' και πια είναι τα χαρακτηριστεί ασφαλές; Κατ' αρχήν, όσο και αν φαίνεται οξύμωρο δεν υπάρχει απόλυτα ασφαλές δίκτυο. Η είσοδος ή όχι ενός επιτιθέμενου στο δίκτυο κάποιας επιχείρησης έχει σχέση μόνο με τις γνώσεις που αυτός έχει αλλά και το χρόνο και και τα χρήματα που είναι διατεθειμένος να ξοδέψει στην προσπάθεια του.

Πολλές φορές έχουμε ακούσει για έφηβους που κατάφεραν να διεισδύσουν σε μεγάλα υπολογιστικά δίκτυα ακόμη και στρατιωτικών οργανισμών , ενώ είναι μάλλον βέβαιο ότι τις πιο επιτυχημένες επιθέσεις δεν τις μαθαίνουμε ποτέ, καθώς ούτε ο επιτιθέμενος ούτε το θύμα θα ήθελαν να τις διαφημίσουν.

Ενα δίκτυο, για να μπορεί να χαρακτηριστεί ασφαλές, θα πρέπει να έχει κάποια χαρακτηριστικά. Έτσι, για παράδειγμα, θα πρέπει στο δίκτυο των υπολογιστών να έχουν πρόσβαση μόνο οι χρήστες του. Η πρόσβαση αυτή των χρηστών θα πρέπει να καταγράφεται. Από την άλλη πλευρά, οι χρήστες θα πρέπει να έχουν συνεχή πρόσβαση στο δίκτυο και σε καμία περίπτωση αυτή να μη διακόπτεται, για οποιονδήποτε λόγο. Το λειτουργικό σύστημα των υπολογιστών του δικτύου θα πρέπει να ενημερώνεται με τα τελευταία διορθωτικά πακέτα που εκδίδουν οι εταιρείες software, ώστε να μπορεί να αντιμετωπίσει πιθανές επιθέσεις καλύτερα. Το ίδιο θα πρέπει να συμβαίνει και για όλες τις εφαρμογές που είναι εγκαταστημένες.

Το δίκτυο θα πρέπει να διαθέτει μηχανισμούς ασφαλείας τέτοιους , ώστε, εάν κάτι πάει στραβά, τα δεδομένα των χρηστών να είναι ασφαλή και να μπορούν μέσα σε ελάχιστο χρονικό να επαναφερθούν από κάποιο backup, η τήρηση του οποίου δε θα πρέπει να επαφίεται σε κάποιο χρήστη αλλά να γίνεται αυτόματα.

Τα παραπάνω αποτελούν κάποιο από τα χαρακτηριστικά ενός ασφαλούς δικτύου, τα οποία, βέβαια, έρχονται να συμπληρώσουν την απαίτηση εκπαίδευση των χρηστών έναντι επιθέσεων κοινωνικής μηχανής (social engineering). Ακόμη και το πιο ασφαλές δίκτυο είναι τόσο ευάλωτο όσο αφελείς είναι οι χρήστες του.

Αυτή την αφέλεια ή, αν θέλετε, άγνοια κινδύνου μπορεί να εκμεταλλευτεί ο οποιοσδήποτε και να εισέλθει σε οποιοδήποτε δίκτυο, χωρίς καν να χρειαστεί να παραβιάσει οποιονδήποτε μηχανισμό ασφαλείας, καθώς θα γνωρίζει από πριν τα κλειδιά που του δώσει κάποιος χρήστης εν αγνοία του.

Όπως καταλαβαίνετε, λοιπόν, η ασφάλεια είναι ένας πολύπλοκος παράγοντας, οποίος πολλές φορές έρχεται σε σύγκρουση με την ευχρηστία ενός δικτύου ή την ελευθερία των χρηστών.

Στην πραγματικότητα θα πρέπει να προχωρήσετε σε ένα συμβιβασμό μεταξύ των δύο στοιχείων, από τη μια παρέχοντας στους χρήστες τα δικαιώματα που πραγματικά χρειάζονται για την ολοκλήρωση της εργασίας τους, και από την άλλη φροντίζοντας η ασφάλεια του δικτύου να μην τίθεται σε μεγάλο κίνδυνο.

Για να γίνει πιο κατανοητό το παραπάνω, φανταστείτε έναν εργαζόμενο που μπορεί να εργάζεται και στο σπίτι με ένα φορητό υπολογιστή. Ο ίδιος θα ήθελε να μπορεί να συνδέσει το notebook του οποιαδήποτε στιγμή στο εταιρικό δίκτυο, για να ανταλλάξει

αρχεία και ίσως και να δει το προσωπικό του e-mail χρησιμοποιώντας τη γρήγορη εταιρική σύνδεση στο internet.

Αυτό θα αύξανε την ευχρηστία του δικτύου, αλλά ταυτόχρονα θα αποτελούσε σημαντικότατο κίνδυνο, καθώς στην περίπτωση που κάποιος ιός κατάφερνε να μολύνει το notebook, αυτόματα θα μεταφερόταν στο εσωτερικό του δικτύου της εταιρεία, με απρόβλεπτα αποτελέσματα.

Ανάλογο παράδειγμα, αποτελούν τα ασύρματα δίκτυα. Η χρήση τους επιτρέπει την αύξηση της παραγωγικότητας των χρηστών, καθώς αυτοί μπορούν πλέον να έχουν πρόσβαση στα δεδομένα τους από οποιοδήποτε σημείο μέσα στην επιχείρηση, χωρίς τους περιορισμούς της καλωδίωσης.

## 6.1 Επιθέσεις στο Internet

Αυξάνονται ολοένα και περισσότερο οι ιοί που προσβάλλουν χιλιάδες υπολογιστές και προκαλούν χάος και μεγάλη αναστάτωση στα δίκτυα. Ένας από τους πιο γνωστούς είναι και ο ιός blaster, ο οποίος κατά τη διάρκεια της φετινής χρονιάς, προκάλεσε χάος σε 500.000 υπολογιστές.

Σύμφωνα με αμερικάνους αξιωματούχους του υπουργείου Εσωτερικής Ασφαλείας, ο ιός blaster θεωρείται ασήμαντος μπροστά στους πραγματικούς κινδύνους που θα προκύψουν από συντονισμένη επίθεση στον κυβερνοχώρο. Το Internet είναι ιδιαίτερα ελκυστικός στόχος για τους τρομοκράτες.

Ο Άμιτ Γιόραν, διευθυντής του τμήματος της εθνικής κυβερνητικής ασφαλείας, δήλωσε πως μπορεί οι επιθέσεις μέχρι σήμερα να μην ήταν καταστροφικές, αλλά αυτή η εικόνα μπορεί να ανατραπεί.

## 6.2 Απειλές στον World Wide Web

Ο World Wide Web είναι ίσως το γρηγορότερα αναπτυσσόμενο κομμάτι του Internet. Ολοένα όμως και περισσότερο γίνεται και το κομμάτι του Internet που είναι πιο ευάλωτο σε επιθέσεις. Οι υπολογιστές που φιλοξενούν ιστοσελίδες (Web servers) αποτελούν ελκυστικούς στόχους για πολλούς λόγους:

**Δημοσιότητα**
Οι ιστοσελίδες ενός οργανισμού ή μίας επιχείρησης αποτελούν την εικόνα του τον υπόλοιπο κόσμο του Internet. Μια επιτυχημένη επίθεση σε έναν Web Server μπορεί να αλλάξει πληροφορίες σε ιστοσελίδες που βλέπουν εκατοντάδες χιλιάδες ανθρώπων μέσα σε μερικές ώρες και είτε να προπαγανδίσει διαφορετικές φιλοσοφίες ή ιδεολογίες ή απλώς να χαλάσει τη δημόσια εικόνα του θύματος.
**Εμπόριο**
Πολλές ιστοσελίδες περιέχουν φόρμες για την αγορά αγαθών ή τη πραγματοποίηση άλλων εμπορικών συναλλαγών (π.χ. πληρωμή προστίμων στην τροχαία). Οι συναλλαγές αυτές γίνονται συνήθως μέσω της ανταλλαγής πληροφοριών που περιλαμβάνουν τα στοιχεία κάποιας πιστωτικής κάρτας, τον χρήστη, κάτι που κάνει αυτούς τους υπολογιστές στόχους επιθέσεων με σκοπό την υποκλοπή αυτών των πληροφοριών.
**Εσωτερικές Πληροφορίες**
Πολλές επιχειρήσεις χρησιμοποιούν τον World Wide Web για να μεταδώσουν πληροφορίες στα μέλη τους ή σε άλλους συνεργάτες τους στο εξωτερικό. Οι πληροφορίες αυτές, όπως είναι φυσικό, αποτελούν στόχο των εμπορικών ανταγωνιστών ή εχθρών τους.
**Πρόσβαση σε δίκτυα**
Επειδή οι υπολογιστές που φιλοξενούν ιστοσελίδες κάποιας επιχείρησης χρησιμοποιούνται και από τους εργαζόμενους μέσα στην επιχείρηση αλλά και από τον υπόλοιπο κόσμο του Internet, αποτελούν μία γέφυρα επικοινωνίας ανάμεσα στο Internet και στα διάφορα τοπικά δίκτυα των επιχειρήσεων. Επομένως η θέση τους, τους κάνει ιδανικούς στόχους επίθεσης ώστε στη συνέχεια να αποτελέσουν «ορμητήρια» των εισβολέων στο εσωτερικό δίκτυο της επιχείρησης.

### 6.2.1 Είδη Απειλών στον World Wide Web

Οι απειλές στον World Wide Web χωρίζονται σε τρεις κατηγορίες: Απειλές κατά του Web server για τους λόγους που αναφέρθηκαν παραπάνω. Απειλές κατά τη μεταφορά των δεδομένων και κατά αποθηκευμένων δεδομένων κυρίως όταν πρόκειται για αριθμούς πιστωτικών καρτών ή άλλες ευαίσθητες πληροφορίες εμπορικών επιχειρήσεων ή στρατιωτικών οργανώσεων.
Απειλές κατά του υπολογιστή του χρήστη μέσω προβλημάτων που πολλές φορές υπάρχουν στον κώδικα του προγράμματος που χρησιμοποιεί ο χρήστης για τη ανάγνωση των ιστοσελίδων (π.χ. Microsoft Internet Explorer, Netscape Navigator).

### 6.2.2 Smurf attacks

Μπορεί στα αγγλικά η λέξη smurfs να σημαίνει τα γνωστά σε όλους μας στρουμφάκια αλλά με ο όρος «smurf attacks» αποδίδεται η επίθεση των hackers στις εταιρίες που παρέχουν πρόσβαση στο διαδίκτυο.

Στο στόχαστρο των hackers μπαίνουν αρκετές φορές οι εταιρίες παροχής πρόσβασης στο Internet (ISPs). Ένας hacker μπορεί να επιτεθεί σε έναν ISP για διάφορους λόγους: μπορεί να είναι θυμωμένος με τον ISP ή με κάποιον που τον χρησιμοποιεί ή απλώς για τη γοητεία της περιπέτειας. Μία από τις πιο κοινές επιθέσεις εναντίον ενός ISP ονομάζεται smurf attack ή smurfing. Στην περίπτωση αυτή ένας hacker μπορεί να πλημμυρίσει τον ISP με έναν τόσο μεγάλο αριθμό άχρηστων πακέτων δεδομένων και να καταλάβει όλο το διαθέσιμο bandwidth, έτσι ώστε οι πελάτες της εταιρίας να μην μπορούν να στείλουν ή να λάβουν δεδομένα μέσω του ηλεκτρονικού ταχυδρομείου, του Web ή οποιασδήποτε άλλης Internet υπηρεσίας.

Σε μία smurf attack οι hackers χρησιμοποιούν μία αρκετά γνωστή υπηρεσία του Internet, ονόματι ping (Internet Control Message Protocol). Η ping χρησιμοποιείται συνήθως από εκείνους που θέλουν να δουν αν ένας συγκεκριμένος υπολογιστής ή Server είναι εκείνη τη στιγμή συνδεδεμένος στο Internet και λειτουργεί. Όταν ο υπολογιστής ή ο server λαμβάνει ένα πακέτο ping επιστρέφει ένα πακέτο σε εκείνον που στέλνει το ping λέγοντας ουσιαστικά «Ναι, λειτουργώ και είμαι συνδεδεμένος στο Internet». Σε μία smurf attack οι hackers πλαστογραφούν τη διεύθυνση που πρέπει να επιστρέψουν τα πακέτα κατευθύνοντάς τα προς τον ISP που έχουν στον στόχο τους. Οι hackers μπορούν να χρησιμοποιούν τα δίκτυα που είναι συνδεδεμένα στο Internet για την αναμετάδοση των αιτήσεων ping καθώς και για τον πολλαπλασιασμό κάθε ping. Κατ' αυτόν τον τρόπο οι hackers μπορούν να χρησιμοποιήσουν δίκτυα που είναι συνδεδεμένα στο Internet για να πλημμυρίσουν τον ISP με τόσα πολλά ping πακέτα έτσι ώστε οι πελάτες του ISP να μην μπορούν να χρησιμοποιήσουν τις υπηρεσίες του.

Οι hackers μπορούν επίσης να χρησιμοποιήσουν πολλαπλά δίκτυα συνδεδεμένα στο Internet για την πραγματοποίηση μιας smurf attack. Οι εταιρίες παροχής Internet υπηρεσιών δύσκολα αντιμετωπίζουν τις smurf attacks καθώς τα πακέτα απάντησης στις ping κλήσεις προέρχονται από νόμιμα δίκτυα και όχι από τον hacker. Ο ISP θα πρέπει να καταγράψει από που προέρχονται τα απαντητικά πακέτα ping και να έρθει σε επαφή με τους υπευθύνους των δικτύων ζητώντας τους να διακόψουν την αποστολή των

απαντητικών πακέτων ping. Τα πράγματα είναι αρκετά δυσκολότερα όταν ο ISP διακόψει τη λειτουργία του και πολύ συχνά ορισμένοι πελάτες του στέλνουν πακέτα ping για να δουν αν λειτουργεί και είναι συνδεδεμένος στο Internet.

Στην περίπτωση αυτή ο ISP δυσκολεύεται να ξεχωρίσει ποια είναι τα νόμιμα πακέτα ping και ποια προέρχονται από την smurf attack.
Για την αντιμετώπιση των smurf attacks έχουν αναπτυχθεί διάφορα εργαλεία και προγράμματα. Λίγες όμως εταιρίες τα χρησιμοποιούν καθώς δεν έχουν γνωρίσει μεγάλη αποδοχή και επειδή δεν αναγνωρίζουν όλοι το μέγεθος του προβλήματος των smurf attacks. Πρόβλημα αποτελεί επίσης ότι οι εταιρίες που θα μπορούσαν να χρησιμοποιήσουν το εν λόγω λογισμικό είναι αυτές που προσφέρουν το backbone και οι οποίες δεν βρίσκονται στο στόχαστρο των smurf attacks. Ως εκ τούτου δεν έχουν κανένα οικονομικό όφελος χρήσης του λογισμικού αυτού. Έτσι οι smurf attacks παραμένουν μία οδυνηρή πραγματικότητα του Internet.

## 6.3 Οι εχθροί του Internet

Πολλοί είναι εκείνοι που προσπαθούν να επιτεθούν στο Internet και συγκεκριμένα στους υπολογιστές που είναι ανά πάσα στιγμή συνδεδεμένοι σ' αυτό. Πολλοί είναι επίσης εκείνοι που προσπαθούν να παραβιάσουν το απόρρητο των άλλων και να αποκτήσουν πρόσβαση σε ευαίσθητες πληροφορίες με απώτερο στόχο τους να τις υποκλέψουν.

### 6.3.1 Crackers ή Hackers;

Οι crackers πολλές φορές αναφέρονται, λανθασμένα, σαν hackers. Οι crackers αρέσκονται στο να εισβάλλουν σε Web servers για πλάκα, για βανδαλισμούς ή για επίδειξη. Οι crackers χρησιμοποιούν υπάρχοντα προϊόντα επίθεσης από το δίκτυο ή τα περιοδικά. Συνήθως δεν έχουν δυνατούς υπολογιστικούς πόρους και οι προθέσεις τους συχνά δεν είναι εχθρικές. ωστόσο, προκαλούν ουσιαστικές ζημιές , είτε προκαλώντας βανδαλισμούς, είτε διακόπτοντας λειτουργίες ή τρώγοντας το χρόνο του προσωπικού του

συστήματος στην προσπάθεια τους να καταλάβουν ποια είναι η ζημιά και να την διορθώσουν.

Η σύγχρονη σημασία του όρου είναι πιθανό να ξεκίνησε από το Massachusetts Institute of Technology (MIT) το 1960, πολύ πριν οι υπολογιστές γίνουν συνήθεια. Hacker είναι ο όρος που χρησιμοποιείται για να περιγράψει διαφορετικά είδη Computer experts. Μερικές φορές συνηθίζεται να σημαίνει οποιοδήποτε είδος ειδικών, ιδιαίτερα με την έννοια του ότι έχουν ιδιαίτερα λεπτομερή γνώση ή έξυπνα όρια εξαπάτησης. Η σημασία αυτού του όρου, όταν χρησιμοποιείται στην επιστήμη των υπολογιστών, έχει αλλάξει με το πέρασμα των αιώνων από τότε που χρησιμοποιήθηκε, μιας και δόθηκαν επιπρόσθετα και αντικρουόμενα νοήματα από τους νέους χρήστες της λέξης.
Προς το παρόν, ο όρος «*hacker*» χρησιμοποιείται με δύο τρόπους κυρίως, έναν θετικό και έναν υποτιμητικό. Μπορεί να χρησιμοποιηθεί στην υπολογιστική κοινότητα για να περιγράψει έναν ιδιαίτερα λαμπρό προγραμματιστή ή έναν τεχνικό ειδικό (για παράδειγμα τον Linus Torvald, τον δημιουργό του Linux). Αυτή λέγεται από μερικούς ότι είναι και η σωστή χρήση του όρου. Σε κοινή χρήση και ιδιαίτερα στα μέσα ενημέρωσης, ωστόσο, γενικά περιγράφει τους εισβολείς και τους εγκληματίες.

## 6.4 Απειλές κατά την ασφάλεια

Στα χρόνια πριν από την εξάπλωση της χρήσης των ηλεκτρονικών υπολογιστών ως εργαλεία επεξεργασίας της πληροφορίας, η διασφάλιση της μυστικότητας, ακεραιότητας και διαθεσιμότητας των σημαντικών πληροφοριών ενός οργανισμού γινόταν μέσω της φυσικής προστασίας των, καθώς και μέσω κάποιων διαδικασιών και κανονισμών ασφάλειας. Για παράδειγμα, τα ευαίσθητα έγγραφα κλείνονταν σε ντουλάπες ή χρηματοκιβώτια στιβαρής κατασκευής τα οποία προστατεύονταν από κλειδαριές, ενώ μόνον εξουσιοδοτημένο προσωπικό το οποίο επιλεγόταν αυστηρά, είχε πρόσβαση σε αυτά. Τις τελευταίες δεκαετίες, δύο γεγονότα έχουν αλλάξει δραστικά τις ανάγκες των οργανισμών σε σχέση με την ασφάλεια των πληροφοριών.

Το πρώτο γεγονός είναι η εισαγωγή των υπολογιστών ως εργαλεία αποθήκευσης και επεξεργασίας της πληροφορίας. Η προστασία της πληροφορίας ανάγεται πλέον στην προστασία των αρχείων των υπολογιστών στα οποία είναι αποθηκευμένη η πληροφορία, στον έλεγχο της πρόσβασης στα αρχεία αυτά, καθώς και στην προστασία των προγραμμάτων εκείνων που μπορούν να απειλήσουν την ασφάλεια των αρχείων αυτών. Ο όρος που χρησιμοποιείται για να περιγράψει το σύνολο των εργαλείων και διαδικασιών που έχουν σχεδιασθεί για την προστασία των ηλεκτρονικών δεδομένων είναι "ασφάλεια υπολογιστών" (computer security).

Το δεύτερο γεγονός το οποίο επηρέασε δραστικά τις ανάγκες σε ασφάλεια της πληροφορίας είναι η εισαγωγή των κατανεμημένων συστημάτων και η χρήση δικτύων και τηλεπικοινωνιακών συστημάτων για την μεταφορά δεδομένων μεταξύ υπολογιστών. Ο όρος "ασφάλεια δικτύων" (network security) αναφέρεται στα μέτρα προστασίας των δεδομένων κατά την μεταφορά τους μέσω του δικτύου διασύνδεσης.
Στα πλαίσια της διαχείρισης ενός δικτύου, η διαχείριση ασφάλειας αναφέρεται στην παροχή ασφάλειας σε όλα τα στοιχεία του δικτύου, δηλαδή σε ασφάλεια υπολογιστών και ασφάλεια δικτύου.

**Η ασφάλεια υπολογιστών και δικτύων καλύπτει τις παρακάτω απαιτήσεις:**

**1. μυστικότητα (secrecy):** απαιτείται η πληροφορία να είναι προσπελάσιμη για ανάγνωση μόνον από εξουσιοδοτημένους χρήστες. Αυτού του είδους η πρόσβαση περιλαμβάνει την εκτύπωση, την προβολή και άλλες φορές ακόμη και την αποκάλυψη ύπαρξης κάποιου είδους πληροφορίας
**2. ακεραιότητα (integrity):** απαιτείται οι πόροι του συστήματος (data, processes κλπ) να μπορούν να τροποποιηθούν μόνον από εξουσιοδοτημένους χρήστες. Η τροποποίηση περιλαμβάνει την εγγραφή, τροποποίηση, αλλαγή κατάστασης (status), διαγραφή και δημιουργία.
**3. διαθεσιμότητα (availability):** απαιτείται οι πόροι του συστήματος να είναι διαθέσιμοι στους εξουσιοδοτημένους χρήστες.

## 6.5 Μορφές Απειλών

Οι διαφορετικές μορφές απειλών της ασφάλειας ενός υπολογιστή ή ενός δικτύου μπορούν να χαρακτηριστούν καλύτερα, αν ληφθεί υπ' όψη ότι ο σκοπός ενός υπολογιστή είναι η παροχή πληροφορίας. Γενικά υπάρχει μία ροή πληροφορίας από μία πηγή, όπως π.χ. ένα αρχείο ή μία περιοχή μνήμης, σε κάποιον προορισμό, όπως ένα άλλο αρχείο ή μία εφαρμογή κάποιου χρήστη. Με δεδομένη αυτή την θεώρηση, είναι δυνατές 4 κατηγορίες απειλών:

**1. διακοπή (interruption):** κάποιος πόρος του συστήματος καταστρέφεται ή καθίσταται μη χρησιμοποιήσιμος ή διαθέσιμος. Αυτού του τύπου η απειλή στρέφεται κατά της διαθεσιμότητας του συστήματος. Παραδείγματα τέτοιων απειλών είναι η καταστροφή κάποιας συσκευής του δικτύου, όπως ο σκληρός δίσκος ενός server, το κόψιμο κάποιας γραμμής του δικτύου, ή η διακοπή τροφοδοσίας ενός δρομολογητή.
**2. υποκλοπή (interception):** πρόκειται για απειλή κατά της μυστικότητας της πληροφορίας, όπου κάποιος μη εξουσιοδοτημένος χρήστης, πρόγραμμα ή υπολογιστής αποκτά πρόσβαση στην πληροφορία με δυνατότητα καταγραφής της. Παραδείγματα αποτελούν η παρακολούθηση μίας γραμμής του δικτύου και η απαγορευμένη αντιγραφή αρχείων ή προγραμμάτων.
**3. τροποποίηση (modification):** πρόκειται για απειλή κατά της ακεραιότητας του συστήματος, όπου κάποιος μη εξουσιοδοτημένος χρήστης, πρόγραμμα ή υπολογιστής αποκτά πρόσβαση στο σύστημα με δυνατότητα τροποποίησης. Παραδείγματα αποτελούν η αλλαγή των δεδομένων ενός αρχείου, η τροποποίηση ενός προγράμματος, η έναρξη κάποιας process και η τροποποίηση του περιεχομένου ενός μηνύματος που μεταδίδεται μέσω του δικτύου.
**4. πλαστογράφηση (fabrication):** πρόκειται για απειλή κατά της ακεραιότητας του συστήματος, κατά την οποία εισάγεται κάποιο πλαστό αντικείμενο στο σύστημα. Παραδείγματα τέτοιας απειλής είναι η αποστολή ενός μηνύματος από κάποιον υποτιθέμενο αποστολέα (fake e-mail) και η πρόσθεση εγγραφών σε κάποιο αρχείο.

Οι πόροι του δικτύου, όπως αυτό ορίσθηκε παραπάνω, αποτελούνται από ενεργά στοιχεία, παθητικά στοιχεία, λογισμικό και δεδομένα (static data, traffic data). Συνεπώς στα πλαίσια της ανάπτυξης μίας στρατηγικής για την ασφάλεια όλων των πόρων του δικτύου το ζητούμενο είναι και η ασφάλεια υπολογιστών και η ασφάλεια δικτύου. Στη

συνέχεια θα παρουσιάσουμε τις απειλές κατά της ασφάλειας κάθε κατηγορίας πόρων του δικτύου.

## Απειλές κατά των Ενεργών Στοιχείων

Η κύρια απειλή κατά των ενεργών στοιχείων του δικτύου (routers, hubs, Servers, workstations, hosts, printers κλπ) αφορά στην διαθεσιμότητα των στοιχείων αυτών. Ενέργειες όπως:
1. η σκόπιμη ή ακούσια καταστροφή ή φθορά
2. η κλοπή του στοιχείου ή τμήματος αυτού
3. η σκόπιμη ή ακούσια διακοπή τροφοδοσίας αποτελούν τις πιο συνηθισμένες απειλές κατά του υλικού ενός δικτύου.

## Απειλές κατά των Παθητικών Στοιχείων

Το παθητικό υλικό του δικτύου αποτελείται από τις πρίζες του δικτύου, τα καλώδια χαλκού και οπτικών ινών και τους πίνακες μικτονόμησης (patch panels) και χρησιμοποιείται για την μεταφορά δεδομένων. Όπως και για τα ενεργά στοιχεία, η κύρια απειλή αφορά στην διαθεσιμότητα των στοιχείων και μπορεί να προκύψει από πράξεις όπως:
1. η σκόπιμη ή ακούσια καταστροφή ή φθορά
2. η κλοπή

## Απειλές κατά των Κινούμενων δεδομένων

Οι απειλές κατά της ασφάλειας των κινούμενων δεδομένων (traffic data) αφορούν στην ακεραιότητα, μυστικότητα και διαθεσιμότητα των δεδομένων και μπορούν να χωρισθούν σε δύο κατηγορίες:

**Α. Απειλές Παθητικής Φύσης**
Απειλούν την μυστικότητα των δεδομένων και υλοποιούνται με την παρακολούθηση των δεδομένων (π.χ. μέσω ειδικών προγραμμάτων packet sniffers) με σκοπό την απόκτηση πληροφοριών. Για παράδειγμα ο χρήστης ενός PC μπορεί να χρησιμοποιήσει ένα τέτοιο πρόγραμμα για να παρακολουθεί όλα τα πακέτα που εκπέμπονται στο τοπικό του δίκτυο (Ethernet subnet). Τέτοιου είδους ενέργειες είναι πολύ δύσκολο να αποκαλυφθούν διότι δεν προκαλούν αλλαγή στα δεδομένα και δεν επηρεάζουν την λειτουργία του δικτύου.
Η παρακολούθηση των δεδομένων είναι δυνατή και μέσω παρακολούθησης των καλωδιώσεων χαλκού του δικτύου (wire-tapping) ή των τηλεφωνικών συνδέσεων πρόσβασης στο δίκτυο.

**Β. Απειλές Ενεργητικής Φύσης**
Τέτοιου είδους απειλές έχουν σαν στόχο την τροποποίηση των κινούμενων δεδομένων ή την δημιουργία πλαστών δεδομένων και απειλούν τόσο την μυστικότητα, όσο την διαθεσιμότητα και την ακεραιότητα των δεδομένων. Είναι δυνατή μία περαιτέρω κατηγοριοποίηση τέτοιων απειλών ως εξής:
1. πρόκληση τροποποίησης της ροής των πακέτων δεδομένων (message-stream modification), όπου ένα τμήμα του κανονικού μηνύματος τροποποιείται, ή κάποια

μηνύματα καθυστερούν, επαναλαμβάνονται, ή τροποποιείται η διαδοχή τους για να προκληθεί κάποιο αποτέλεσμα
2. πρόκληση άρνησης παροχής υπηρεσιών (denial of service), κατά την οποία παρεμποδίζεται η κανονική χρήση των πόρων του δικτύου. Μία τέτοια μορφή επίθεσης είναι η υπερφόρτωση του δικτύου με πακέτα με αποτέλεσμα την επιβράδυνση ή και διακοπή της λειτουργίας του. Άλλο παράδειγμα είναι η εξάλειψη μηνυμάτων που απευθύνονται σε κάποιον συγκεκριμένο αποδέκτη, όπως για παράδειγμα σε ένα πρόγραμμα που εκτελεί την υπηρεσία ελέγχου ασφάλειας (security audit service).
3. μεταμφίεση (masquerade) κατά την οποία ο εισβολέας τροποποιεί τα δεδομένα με στόχο να ξεγελάσει τους μηχανισμούς ασφάλειας του δικτύου και να θεωρηθεί ως εξουσιοδοτημένος ή έμπιστος χρήστης. Τέτοια παραδείγματα είναι η αλλαγή της IP διεύθυνσης πακέτων του εξωτερικού εισβολέα, έτσι ώστε το σύστημα firewall να νομίσει ότι τα πακέτα έρχονται από το εσωτερικό δίκτυο, ή η ηχογράφηση κάποιας συνομιλίας ελέγχου αυθεντικότητας (authentication) μεταξύ ενός εξουσιοδοτημένου χρήστη και του συστήματος και κατόπιν η χρήση της από τον εισβολέα.

### Απειλές κατά των Αποθηκευμένων δεδομένων

Όπως και για τα κινούμενα δεδομένα, οι απειλές κατά της ασφάλειας των δεδομένων που είναι αποθηκευμένα σε αρχεία αφορούν στην ακεραιότητα, μυστικότητα και διαθεσιμότητα των δεδομένων. Αυτό που διαφέρει είναι οι μηχανισμοί πρόσβασης στα δεδομένα αυτά, μιας και βρίσκονται αποθηκευμένα στους χώρους μόνιμης αποθήκευσης κάποιων ενεργών στοιχείων.
Η απειλή κατά της μυστικότητας των δεδομένων έγκειται στην πρόσβαση στα αρχεία που τα περιέχουν από μη εξουσιοδοτημένους χρήστες, στους οποίους δίνεται η δυνατότητα να διαβάσουν τα αρχεία αυτά. Η διαθεσιμότητα των αρχείων απειλείται από την εσκεμμένη ή ακούσια διαγραφή των αρχείων. Τέλος, η ακεραιότητα των αρχείων απειλείται από την αλλαγή των χαρακτηριστικών τους (file attributes), την αλλαγή του περιεχομένου τους, καθώς και από την κακόβουλη δημιουργία νέων αρχείων.

## 6.6 Είδη και κίνητρα εισβολέων

Υπάρχουν δύο ειδών εισβολείς. Οι παθητικοί εισβολείς, οι οποίοι απλώς θέλουν να διαβάσουν αρχεία για τα οποία δεν έχουν αυτού του είδους την εξουσιοδότηση. Οι ενεργοί εισβολείς είναι πιο κακόβουλοι, και θέλουν να κάνουν μη εξουσιοδοτημένες αλλαγές σε δεδομένα. Κατά το σχεδιασμό της ασφάλειας ενός συστήματος από τους εισβολείς, πρέπει να γνωρίζουμε το είδος και τα κίνητρα του εισβολέα από τον οποίο θέλουμε να προστατευθούμε. Ορισμένες κοινές κατηγορίες είναι:

1. **Περίεργοι χρήστες χωρίς τεχνικές γνώσεις.** Πολλοί άνθρωποι έχουν στα γραφεία τους τερματικά σε συστήματα διαμερισμού χρόνου (timesharing Systems), και εξαιτίας της ανθρώπινης φύσης, ορισμένοι από αυτούς θα διαβάσουν το ηλεκτρονικό ταχυδρομείο και τα αρχεία άλλων ανθρώπων, αν δεν υπάρχει κανένας φραγμός για αυτό.
2. **Προσπάθεια προσπέλασης από εσωτερικούς εισβολείς.** Οι φοιτητές, οι προγραμματιστές συστημάτων, οι χειριστές και το λοιπό τεχνικό προσωπικό, συχνά θεωρούν ως προσωπική πρόκληση την παράκαμψη της ασφάλειας του τοπικού υπολογιστικού συστήματος. Συχνά έχουν υψηλά προσόντα και είναι αποφασισμένοι να αφιερώσουν ένα σημαντικό μέρος του χρόνου τους στην προσπάθεια αυτή.

**3. Ηθελημένες προσπάθειες για οικονομικά οφέλη.** Ορισμένοι προγραμματιστές που εργάζονται σε τράπεζες έχουν προσπαθήσει να μπουν σε κάποιο σύστημα τράπεζας με σκοπό να κλέψουν από αυτή. Οι τρόποι ποικίλλουν, από την αλλαγή του λογισμικού ώστε να περικόπτει αντί να στρογγυλεύει τους τόκους, την κράτηση ενός κλάσματος της δραχμής για τους εαυτούς τους, την οικειοποίηση λογαριασμών που μένουν αχρησιμοποίητοι για χρόνια, μέχρι και τον εκβιασμό («Πληρώστε με αλλιώς θα καταστρέψω όλες τις εγγραφές της τράπεζας»).
**4. Εμπορική ή στρατιωτική κατασκοπία.** Η κατασκοπία συνίσταται σε μια σοβαρή και με καλή οργάνωση προσπάθεια ενός ανταγωνιστή ή μιας ξένης χώρας με στόχο να κλαπούν προγράμματα, εμπορικά μυστικά, ευρεσιτεχνίες, τεχνολογία, σχέδια κυκλωμάτων, σχέδια για μάρκετινγκ κ,ο.κ. Συχνά αυτή η προσπάθεια περιλαμβάνει παρακολούθηση τηλεπικοινωνιακών γραμμών ή ακόμα τοποθέτηση κεραιών κατευθυνόμενων προς τον υπολογιστή ώστε να λαμβάνουν τις ηλεκτρομαγνητικές του ακτινοβολίες.

## 6.7 Κακόβουλα Προγράμματα

### 6.7.1 Spyware

Τα προγράμματα spyware είναι ένας από τους πιο διαδεδομένους τύπους εχθρικού λογισμικού. Όπως υποδηλώνει το όνομά τους, αυτά τα προγράμματα είναι ειδικά σχεδιασμένα ώστε να «κατασκοπεύουν» τις ενέργειες των χρηστών, κυρίως όταν συνδέονται στο Internet.

Επειδή όλα τα είδη προγραμμάτων spyware ουσιαστικά παραβιάζουν το απόρρητο των δεδομένων που αποθηκεύονται σ' έναν υπολογιστή, θεωρούνται σαν μία εν δυνάμει απειλή η οποία χρήζει αντιμετώπισης.
Αυτά τα προγράμματα συγκεντρώνουν πληροφορίες για τις ιστοσελίδες που επισκέπτονται πιο συχνά οι χρήστες, τον χρόνο σύνδεσης, κ.α., και τις στέλνουν σε κάποιο προορισμό. Επίσης, μπορούν να καταγράφουν δεδομένα σχετικά με τον υπολογιστή στον οποίο είναι εγκατεστημένα: τύπος λειτουργικού συστήματος, τύπος επεξεργαστή, μνήμη, κ.α. Υπάρχουν επίσης «κατασκοπευτικά» προγράμματα τα οποία ανιχνεύουν και αναφέρουν εάν οι εφαρμογές λογισμικού που είναι εγκατεστημένες σ' έναν υπολογιστή είναι νόμιμα αποκτηθέντα αντίγραφα, ή όχι.

Τα spyware έχουν διαφημιστικούς σκοπούς. Ο κυριότερος σκοπός είναι να πλουτίσουν εκείνους που το χρησιμοποιούν, χωρίς καν να χρειαστεί να πουλήσουν κάτι. Αυτό μπορεί να γίνει με δύο τρόπους. Με banners ή και με εξειδικευμένα προγράμματα «κατασκοπείας» της κάθε κίνησης του υπολογιστή.

Η μεγάλη εξάπλωση αυτών των προγραμμάτων οφείλεται κυρίως σ' ένα σύνολο κοινών χαρακτηριστικών, συμπεριλαμβανομένων των σχεδόν τέλειων τεχνικών καμουφλάζ. Το λογισμικό spyware εγκαθίσταται συνήθως κατά την διάρκεια εγκατάστασης άλλων εφαρμογών: client εφαρμογές P2P, βοηθήματα διαχείρισης σκληρών δίσκων, κ.α. Ονόματα αρχείων τα οποία δεν εγείρουν υποψίες, πράγμα το οποίο τους επιτρέπει να περνούν απαρατήρητα μαζί με τα υπόλοιπα αρχεία που ανήκουν σε μία εφαρμογή.

Επειδή δεν είναι ιοί και δεν χρησιμοποιούν κώδικα ο οποίος μπορεί να τα συσχετίσει με ιούς, τα εργαλεία antivirus δεν μπορούν να ανιχνεύουν τα προγράμματα spyware, εκτός κι αν είναι ειδικά σχεδιασμένα γι' αυτό τον σκοπό.

Το μεγαλύτερο ποσοστό τους το δημιουργούν και το διακινούν εταιρείες marketing που σκοπό τους έχουν να συλλέξουν πληροφορίες για τον τρόπο που κινούμαστε στο Internet, για τις προσωπικές μας συνήθειες και τις προτιμήσεις μας και μετά να μας γεμίσουν με spam email, για να διαφημίσουν αμφίβολης ποιότητας υπηρεσίες και προιόντα. Αρκετές φορές εμφανίζουν διαφημιστικά banner ή αλλάζουν την πρώτη ιστοσελίδα στον browser ή προσθέτουν ιστοσελίδες στα αγαπημένα μας.

Αν και από τη φύση τους δεν είναι πάντα «κακόβουλα», τα κατασκοπευτικά προγράμματα προκαλούν σημαντική βλάβη στα νόμιμα προγράμματα, στην απόδοση του δικτύου και στην παραγωγικότητα των εργαζομένων. Μία «παράπλευρη» συνέπεια της εισβολής των spyware στους υπολογιστές είναι η σώρευση παραπόνων των χρηστών στους διαχειριστές των δικτύων για αναδυόμενα παράθυρα (pop-ups), για δυσλειτουργία εφαρμογών και για χαμηλή απόδοση των υπολογιστών.

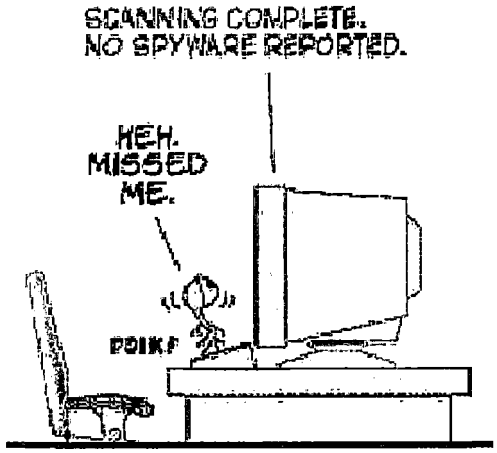
Στη χειρότερη περίπτωση, η δυνατότητα των κατασκοπευτικών προγραμμάτων να καταγράφουν οτιδήποτε πληκτρολογούμε, να «σαρώνουν» τους σκληρούς δίσκους και να αλλάζουν τις ρυθμίσεις του συστήματος και του μητρώου των υπολογιστών, αποτελεί τεράστια απειλή προσωπικής και επιχειρησιακής ασφάλειας που επιτρέπει την κλοπή στοιχείων ταυτότητας, καταστροφή δεδομένων, ακόμα και κλοπή εμπορικών μυστικών μιας εταιρείας.

Υπάρχουν διάφορες στατιστικές αλλά όλες συγκλίνουν στο ότι πάνω από το 80% των υπολογιστών που συνδέονται στο Internet έχουν μολυνθεί με κάποιας μορφής Spyware.

## Προστασία από το Spyware

Η παρουσία τους δεν γίνεται αντιληπτή στον υπολογιστή - ούτε όταν εγκαθίστανται, ούτε όταν τρέχουν. Για τον λόγο αυτό οι χρήστες δεν ανησυχούν ιδιαίτερα γι' αυτά τα είδη προγραμμάτων και, σαν αποτέλεσμα, τα προγράμματα spyware μπορούν να περνούν απαρατήρητα για μεγάλα χρονικά διαστήματα.

Οι δημιουργοί λογισμικού spyware ξέρουν να κρύβουν τέλεια τα προγράμματά τους μέσα σε καθ'όλα νόμιμες εφαρμογές, και για τον λόγο αυτό κανένα πρόγραμμα antivirus δεν μπορεί να τα ανιχνεύσει, εκτός κι αν είναι ειδικά σχεδιασμένο γι' αυτό τον σκοπό. Συνεπώς, για την ανίχνευσή τους πρέπει να χρησιμοποιούνται ειδικές εφαρμογές, ή - ακόμη καλύτερα ένα «πακέτο» εργαλείων ασφάλειας, το οποίο ενσωματώνει μηχανισμούς ικανούς να εξουδετερώσουν οποιαδήποτε προερχόμενη από το Internet απειλή, συμπεριλαμβανομένων των προγραμμάτων.




Η λύση είναι ένα antispyware ή spyware remover πρόγραμμα. Είναι καταπληκτικό το πόσα πολλά προγράμματα κυκλοφορούν στη αγορά και τι μεγάλος ανταγωνισμός υπάρχει, αλλά αυτό δείχνει και το μέγεθος του προβλήματος.

Επίσης, η χρήση των automatic updates (στα συστήματα Windows) καθώς και οι να βαθμίσεις σε προγράμματα antivirus βοηθούν στην προστασία του συστήματος. Καθώς τα προγράμματα spyware εκμεταλλεύονται τις τρωτότητες του Internet Explorer, καλό θα ήταν να χρησιμοποιούμε κάποιον λιγότερο τρωτό browser όπως τον Mozilla Firefox ή τον Opera.

Απενεργοποιώντας το ActiveX στον Internet Explorer μπορεί επίσης να αποτρέψει κάποιες μολύνσεις, ωστόσο κάποια Web sites που χρησιμοποιούν το ActiveX δεν θα λειτουργούν με αυτόν τον τρόπο.

## Antispyware

Αυτά τα προγράμματα λειτουργούν με παρόμοιο τρόπο με τα antivirus. Τα περισσότερα μένουν συνεχώς στη μνήμη του υπολογιστή και ελέγχουν ποια προγράμματα εγκαθίστανται σε αυτόν, τι αλλαγές προκαλούν στην Registry κ.ά. Πέρα από την

παραπάνω λειτουργία, ο χρήστης έχει την δυνατότητα να αναζητήσει στο σκληρό του δίσκο προγράμματα που έχουν ήδη εγκατασταθεί, και να τα απομακρύνει. Είναι ιδιαίτερα σημαντικό ο κατάλογος με τα γνωστά προγράμματα spyware-ad-ware να ανανεώνεται όσο το δυνατόν συχνότερα, καθώς νέες απειλές εμφανίζονται στο internet συνεχώς.

## 6.7.2 Είδη ηλεκτρονικού spam

| | | |
|---|---|---|
| **Διαφήμιση** | **Διάδοση Malware** | **Εξακρίβωση email** |
| **Phishing** | **Φάρσα-Hoax** | **Προσηλυτισμός** |
| Nigeria C. | **Flooding** | DoS |

**Διαφήμιση**

Τα spam email που περιέχουν διαφημίσεις είναι τα πιο συνηθισμένα και ονομάζονται επίσημα "μη ζητηθείσα εμπορική επικοινωνία" (unsolicited email) . Είναι ενοχλητικά γιατί φουσκώνουν το inbox μας με περιττές διαφήμισης ιστοσελίδων ή προϊόντων και επίσης καταλαμβάνουν χώρο, χρόνο και bandwidth καθώς κατεβαίνουν στον υπολογιστή μας. Η μη ζητηθείσα εμπορική αλληλογραφία είναι παράνομη σύμφωνα με το νόμο για την «**Προστασία Δεδομένων Προσωπικού Χαρακτήρα στον Τηλεπικοινωνιακό Τομέα**». Αυτός ο νόμος προβλέπει (άρθρο 9 του Ν.2774/1999):

Η με **οποιοδήποτε τηλεπικοινωνιακό** μέσο απ΄ ευθείας εμπορική προώθηση προϊόντων ή υπηρεσιών επιτρέπεται **μόνον** στην περίπτωση **συνδρομητών**, οι οποίοι έχουν δώσει εκ των προτέρων τη **ρητή συγκατάθεσή τους.**

Αυτό σημαίνει ότι και η τακτική telemarketing ορισμένων εταιριών, όπως κάποιων τραπεζών που προσπαθούν να πουλήσουν πιστωτικές κάρτες από το τηλέφωνο, είναι παράνομη και θα έπρεπε να τιμωρείται. Την επόμενη φορά λοιπόν που κάποιος πωλητής θα σας πάρει τηλέφωνο χωρίς τη ρητή συγκατάθεσή σας, επικαλεστείτε τον νόμο προστασίας προσωπικών δεδομένων και μη τον αφήσετε να σπαταλήσει τον χρόνο σας :Επίσης να προσέχετε που δίνετε τα στοιχεία σας, γιατί πολλές εταιρίες τα πουλάνε σε άλλες για να σας ενοχλούν με διαφημίσεις. Όταν όμως τα δίνετε από μόνοι σας από το τηλέφωνο, είναι σας να δίνετε τη "ρητή συγκατάθεσή σας".

## Πώς θα αποφύγετε το SPAM

Για να αποφεύγουμε το spam πρέπει να προστατεύουμε το email μας και να προσέχουμε να μη το δημοσιεύουμε σε σελίδες του ίντερνετ. Οι spammers χρησιμοποιούν "διαδικτυακά ρομπότ" που σκανάρουν το διαδίκτυο για ηλεκτρονικές διευθύνσεις και τις αποθηκεύουν στα αρχεία τους. Αυτές τις διευθύνσεις μετά τις πουλάνε σε άλλους spammers. Ένας άλλος τρόπος προστασίας του email είναι να μη χρησιμοποιείτε το σύμβολο @ αλλά να περιγράφετε το email όπως ακούγεται (ηχητικά) πχ "my email at yahoo dot com" όπου at=@, dot=. . Άν χρησιμοποιήσετε αρχείο εικόνας, μπορείτε να φτιάξετε ένα στην ιστοσελίδα: **http://www.privacysig.com/**
Ένα άλλο πρόβλημα είναι ότι αν ο ηλεκτρονικός υπολογιστής ενός φίλου σας μολυνθεί από κάποιο κατασκοπευτικό πρόγραμμα, το πιο πιθανό είναι να καταγράψει όλα τα email

που έχει ο φίλος σας αποθηκευμένα στον Η/Υ του και να τα ενσωματώσει στις "διεθνείς" spam λίστες. Έτσι δε φτάνει να προστατεύετε εσείς το email σας. Πρέπει να μάθουμε όλοι να σεβόμαστε το απόρρητο της ηλεκτρονικής διεύθυνσης email και να το διαχειριζόμαστε σαν ένα νούμερο τηλεφώνου που δε θα αποκαλύπταμε πουθενά χωρίς την άδεια του ιδιοκτήτη.

## Έλληνες Spammers

Το Ίντερνετ στην Ελλάδα αναπτύσσεται συνεχώς, ακόμα όμως δεν μπορεί, εκ των πραγμάτων, να συγκριθεί με το αμερικάνικο, το γερμανικό και το αγγλικό ίντερνετ. Όπως έχουν δείξει έρευνες που δημοσιεύονται κατά καιρούς στις αθηναϊκές εφημερίδες, το ποσοστό των ελλήνων που χρησιμοποιούν το διαδίκτυο είναι πολύ μικρό σε σχέση με την Ευρώπη. Πραγματικά δεν θα περίμενε κανείς να υπάρχουν έλληνες spammers, από ότι φαίνεται όμως υπάρχουν αρκετοί webmasters και άλλοι επαγγελματίες που καταφεύγουν σε μεθόδους spam για να διαφημίσουν την ιστοσελίδα και τα προϊόντα τους.

## Spam mail: Ποτέ και πάντα

**Ποτέ** μην απαντάτε σε Spam mail. Για ένα spammer απλά και μόνο ένα click σε κάποιο από τα περιεχόμενα στο μήνυμα links δικαιολογεί αυτήν την ακραία και αντιαισθητική διαφημιστική πράξη.

**Ποτέ** μην ανταποκρίνεστε στο link "remove me from the mailing list". Πρόκειται απλά και μόνο για ένα κόλπο που ενημερώνει τον αποστολέα πως η διεύθυνση ισχύει και κατά συνέπεια ο όγκος των spam mails εφεξής διακρίνεται από ανησυχητικές αυξητικές τάσεις.

**Ποτέ** μη γίνετε συνδρομητές σε sites που υπόσχονται πως θα αφαιρεθεί η e-mail διεύθυνσή σας από spam lists. Σπανίως είναι ειλικρινείς, στις περισσότερες περιπτώσεις είναι άλλο ένα trick των spammers.

**Ποτέ** μην περνάτε στην αντεπίθεση. Αν και ένα mail bombing θα άρμοζε στους spammers, αυτή η τακτική το μόνο αποτέλεσμα που έχει είναι να αυξάνει την σπατάλη του bandwidth στο Internet. Άλλωστε συνήθως οι spammers χρησιμοποιούν ψευδείς e-mail διευθύνσεις (spoof mail address)

**Πάντα** να λαμβάνετε μέτρα αντιμετώπισης του spam. Να ενημερώνετε υπηρεσίες και αρμόδιους οργανισμούς όταν δέχεστε spam από εμπορικές εταιρείες, να κάνετε γνωστά τα παράπονά σας στις τελευταίες και φυσικά να αντιστέκεστε στον κατακλυσμό διαφημίσεων.

**Πάντα** να διατηρείτε μια e-mail διεύθυνση αυστηρά και μόνο για τις πολύ στενές προσωπικές σας επαφές, φροντίζοντας να αποφεύγετε τη δήλωσή της σε Web υπηρεσίες.

## Antispam

Από τα πρώτα δυσάρεστα εμπόδια που κλήθηκαν (και καλούνται) να αντιμετωπίσουν οι χρήστες του Internet ήταν και είναι το **spam** mail

Το spam e-mails είναι συνήθως διαφημιστικά μηνύματα που προτρέπουν το χρήστη να αγοράσει κάποιο προϊόν. Εκμεταλλευόμενα όμως λάθη στην ασφάλεια του λειτουργικού ή του mail client, μπορούν να μεταφέρουν και ιούς, Trojan αλλά και προγράμματα spyware, την αντιμετώπιση των οποίων αναλαμβάνουν οι προηγούμενες κατηγορίες προγραμμάτων. Τα απλά διαφημιστικά mail αντιμετωπίζονται με τη βοήθεια κάποιων μαθηματικών τύπων και φίλτρων που «διαβάζουν» τα μηνύματα και τα βαθμολογούν ανάλογα. Τις περισσότερες φορές, ο χρήστης έχει την δυνατότητα να ορίσει ο ίδιος το ποσοστό των spam e-mails που θα δέχεται, μειώνοντας ή αυξάνοντας το όριο πάνω από το οποίο κάποιο μήνυμα θα θεωρείτε spam. Ακόμη έχει τη δυνατότητα να δημιουργήσει λίστες με γνωστούς παραλήπτες από τους οποίους θέλει να δέχεται ή όχι mails. ), το spam mail παραμένει μια απειλή για την αισθητική μας. Τα τελευταία χρόνια, μάλιστα, έχει αποκτήσει και παρέα: τα διαδοχικά pop-up windows με διαφημιστικά banners που αφαιρούν από το web την βασική του γοητεία: την πλοήγηση.

## 6.7.3 Διάδοση Malware

Ιοί και άλλα προγράμματα που περιέχουν βλαβερό κώδικα στέλνονται συνημμένα σε email. Θα έχετε ακούσει τη συνηθισμένη συμβουλή "μην ανοίγετε συνημμένα από ανθρώπους που δε γνωρίζετε". Πρέπει κανείς να λάβει υπόψη του ότι είναι πολύ εύκολο να παραποιηθεί και να πλαστογραφηθεί η διεύθυνση του πραγματικού αποστολέα. "Θα πλαστογραφούσε ένας spammer τη διεύθυνση ενός φίλου μου;"

Ναι! Έχει συμβεί και δεν είναι σπάνιο φαινόμενο. Πιο πιθανό όμως είναι να έχει κολλήσει κάποιος φίλος σας ένα σκουλήκι (worm) το οποίο στέλνει τον εαυτό του αυτόματα σε όλες τις αποθηκευμένες επαφές του προγράμματος αλληλογραφίας (outlook express, outlook, thunderbird κτλ).

Κακόβουλα προγράμματα μπορούν να περιέχονται και στο κώδικα HTML του email με τη μορφή κάποιου script. Σε αυτή την περίπτωση αρκεί η **απλή προεπισκόπηση του email** για να κολλήσει κανείς ιό. Η λύση είναι να απενεργοποιήσουμε τον κώδικα HTML στο πρόγραμμα αλληλογραφίας.

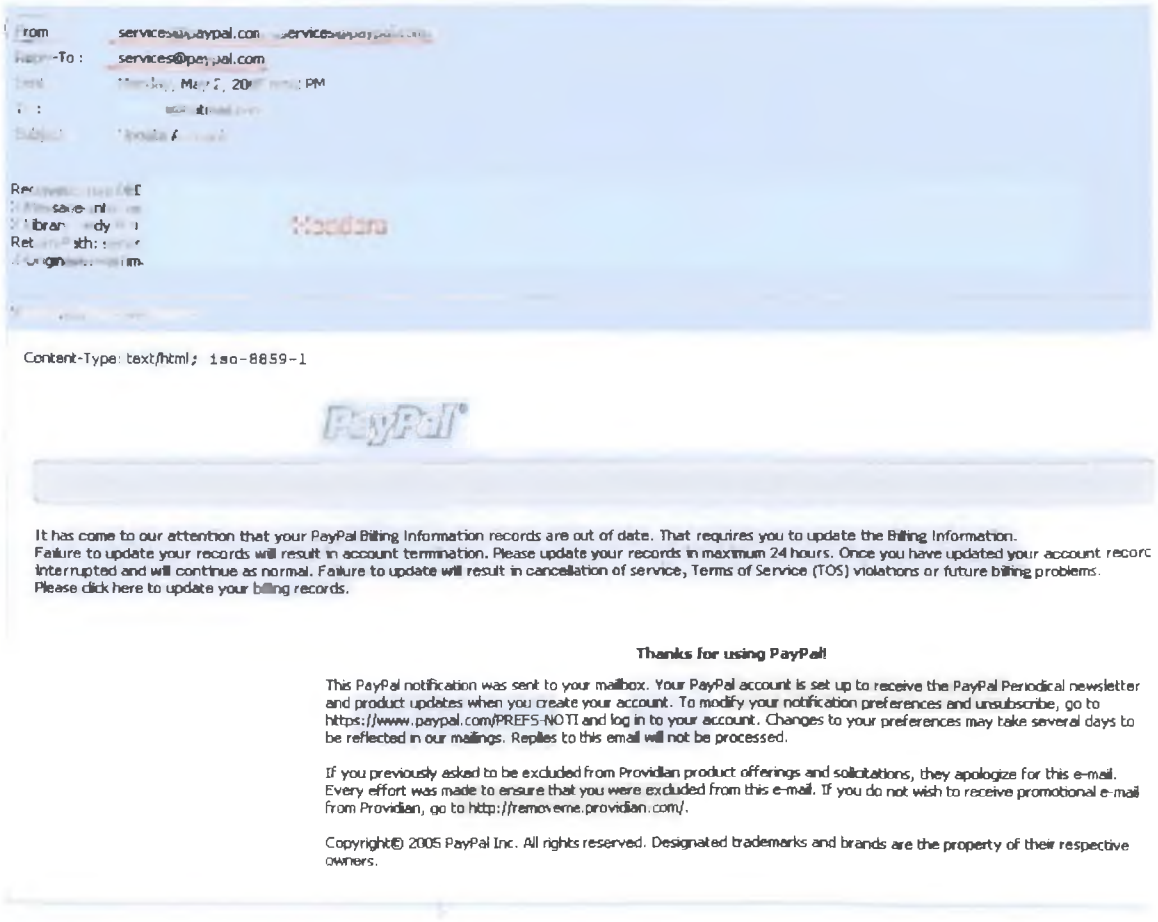
## 6.7.4 Εξακρίβωση Email

Οι spammers στέλνουν συχνά emails τα οποία περιέχουν ένα πρόγραμμα που ενημερώνει τον αποστολέα αν ο λογαριασμός email είναι ενεργός. Όταν σιγουρευτούν συνεχίζουν να στέλνουν SPAM emails και κρατάνε τη διεύθυνση email στα αρχεία τους. Για αυτό τον σκοπό χρησιμοποιούνται και τα αρχεία εικόνας. Ο τρόπος αντιμετώπισης είναι πάλι η απενεργοποίηση του κώδικα HTML και το μπλοκάρισμα της εμφάνισης των εικόνων.

### 6.7.5 Απάτη – Phishing

Phishing = Ψάρεμα! Emails που φαίνονται να προέρχονται από μεγάλες και γνωστές εταιρίες, με όλα τα γραφικά και το κατάλληλο επίσημο κείμενο, προσπαθούν να σας ψαρέψουν και να σας πείσουν ότι πρέπει να εισάγετε τα στοιχεία του λογαριασμού σας για εξακρίβωση ή για να αποφευχθεί κάποιο σοβαρό πρόβλημα. Αυτό το είδος είναι πολύ καλά σχεδιασμένο και στοχεύει σε κωδικούς από πελάτες των amazon, ebay, citybank, paypal και άλλων μεγάλων εταιριών. Δυστυχώς πολλοί αφελείς έχουν πέσει θύμα τέτοιων Phishing email με αποτέλεσμα να αδειάσουν οι λογαριασμοί τους από τους ηλεκτρονικούς εγκληματίες! Η επιτυχία των phishing email βασίζεται σε ψυχολογικούς τρόπους παραπλάνησης ανθρώπων που είναι αφελείς και δεν έχουν τις κατάλληλες γνώσεις. Αυτός ο ψυχολογικός τρόπος παραπλάνησης και καθοδήγησης των θυμάτων λέγεται "κοινωνική μηχανική" (social engineering) και έχει χρησιμοποιηθεί κατά καιρούς από hackers με διάφορες παραλλαγές. Πολλές φορές μάλιστα η κοινωνική μηχανική αποδεικνύεται πιο αποτελεσματική από τεχνολογικά μέσα (κατασκοπευτικά προγράμματα και ιούς) γι' αυτό και χρησιμοποιείται ευρέως.

## Παράδειγμα PHISHING που μιμείται την εταιρία Paypal:



Content-Type: text/html; iso-8859-1

PayPal

It has come to our attention that your PayPal Billing Information records are out of date. That requires you to update the Billing Information.
Failure to update your records will result in account termination. Please update your records in maximum 24 hours. Once you have updated your account record
interrupted and will continue as normal. Failure to update will result in cancellation of service, Terms of Service (TOS) violations or future billing problems.
Please click here to update your billing records.

**Thanks for using PayPal!**

This PayPal notification was sent to your mailbox. Your PayPal account is set up to receive the PayPal Periodical newsletter and product updates when you create your account. To modify your notification preferences and unsubscribe, go to https://www.paypal.com/PREFS-NOTI and log in to your account. Changes to your preferences may take several days to be reflected in our mailings. Replies to this email will not be processed.

If you previously asked to be excluded from Providian product offerings and solicitations, they apologize for this e-mail. Every effort was made to ensure that you were excluded from this e-mail. If you do not wish to receive promotional e-mail from Providian, go to http://removeme.providian.com/.

Copyright© 2005 PayPal Inc. All rights reserved. Designated trademarks and brands are the property of their respective owners.

**Παράδειγμα PHISHING που μιμείται την εταιρία Ebay:**


Your credit/debit card information must be updated

Dear eBay Member,
We recently noticed one or more attempts to log in to your eBay account from a foreign IP address and we have reasons to believe that your account was used by a third party without your authorization. If you recently accessed your account while traveling, the unusual login attempts may have been initiated by you
**The login attempt was made from:**
**IP address:** 172.25.210.65
**ISP Host:** cache-60.proxy.aol.com

By now, we used many techniques to verify the accuracy of the information our users provide us when they register on the Site. However, because user verification on the Internet is difficult, eBay cannot and does not confirm each user's purported identity. Thus, we have established an offline verification system o help you evaluate with who you are dealing with.

### 6.7.6 Φάρσα – Hoax

Ένα ακόμα επικίνδυνο spam το οποίο είναι δυστυχώς αρκετά διαδεδομένο είναι το HOAX. Αυτά είναι email που φαίνεται να περιέχουν πληροφορίες για τον πιο επικίνδυνο ιό και μας καλούν να προωθήσουμε το μήνυμα σε όλα τα άτομα στη λίστα μας. Τέτοια hoax στέλνονται συχνά και μέσω των messengers, δεν περιέχουν ποτέ αξιόπιστες πληροφορίες και σκοπό έχουν να σπείρουν τον τρόμο και τον πανικό ανάμεσα σε άπειρους χρήστες. Να βασίζεστε μόνο σε επίσημες πληροφορίες που μπορείτε να βρείτε σε επίσημες και γνωστές ιστοσελίδες κατασκευαστών antivirus. Εκτός του ότι δεν είναι αστείο να σπέρνουμε τον πανικό με το να προωθούμε τέτοια γελοία email, μαζικές προωθήσεις δημιουργούν μεγάλα προβλήματα και αστάθειες στα δίκτυα.

### 6.7.7 Flooding

Flooding σημαίνει πλημμυρίζω και είναι ένας όρος που χρησιμοποιείται για να περιγράψει το πλημμύρισμα των λογαριασμών email. Στόχος τους είναι να παραλύσουν ένα δίκτυο ή έναν email provider και τα email που στέλνονται είναι συνήθως άδεια, χωρίς κανένα περιεχόμενο.

## 6.8 Το τρίπτυχο του τρόμου

### 6.8.1 Το «Σκουλήκι»

Τα worms, από την άλλη πλευρά, πολλαπλασιάζονται - ωστόσο σε αντίθεση με τους παραδοσιακούς ιούς, δεν απαιτούν την παρεμβολή του ανθρώπινου παράγοντα για να μεταδοθούν από το ένα σύστημα στο άλλο. Η επικινδυνότητα των worms έγκειται στο ότι επιτρέπουν μια ποικιλία επιθέσεων μέσω του Internet.


Για παράδειγμα, ένα καλογραμμένο worm μπορεί να αναζητήσει μόνο του συστήματα

που παρουσιάζουν μια συγκεκριμένη αδυναμία στην ασφάλειά τους, να τα μολύνει και να περιμένει την κατάλληλη στιγμή για να εκκινήσει μια συγχρονισμένη επίθεση DoS (Denial of Service) σε έναν καθορισμένο στόχο.

Η μεγαλύτερη παραβίαση ασφαλείας όλων των εποχών σε υπολογιστές ξεκίνησε το απόγευμα της 2ας Νοεμβρίου 1988, όταν ένας τελειόφοιτος του Πανεπιστημίου Cornell ελευθέρωσε το πρόγραμμα «σκουλήκι» (worm) μέσα στο δίκτυο Internet. Αυτή η πράξη είχε ως αποτέλεσμα να καταρρεύσουν χιλιάδες υπολογιστές σε πανεπιστήμια, εταιρίες και κυβερνητικά εργαστήρια σε ολόκληρο τον κόσμο, προτού αποκαλυφθεί και απομακρυνθεί το «σκουλήκι».

Το «σκουλήκι» εκμεταλλευόταν ένα σφάλμα που είχε τότε το λειτουργικό Berkeley UNIX, χάρη στο οποίο του επιτρεπόταν να έχει μη εξουσιοδοτημένη πρόσβαση σε υπολογιστές οι οποίοι ήταν συνδεδεμένοι στο Internet. Από τη στιγμή που αποκτούσε πρόσβαση σε ένα νέο υπολογιστή αναπαραγόταν σε αυτόν (αντέγραφε τον εαυτό του) και το αντίγραφο του έψαχνε με τη σειρά του να αποκτήσει πρόσβαση σε άλλους υπολογιστές κ,ο.κ. Τίποτα όμως στον κώδικα του «σκουληκιού» δεν υποδήλωνε προσπάθεια για να κλέψει ή να χαλάσει οτιδήποτε στους υπολογιστές που αποκτούσε πρόσβαση. Δεν είναι βέβαια γνωστό αν η μορφή που είχε το πρόγραμμα στις 2 Νοεμβρίου 1988 προοριζόταν απλώς για έλεγχο και ξέφυγε στο Internet κατά λάθος ή ήταν η τελική. Γεγονός πάντως είναι ότι οι «μολυσμένοι» υπολογιστές μετά από κάποιο διάστημα κατακλύζονταν από αντίγραφα του «σκουληκιού» και δεν μπορούσαν να λειτουργήσουν.

### 6.8.2 Ιοί

Ο συνηθέστερος τύπος κακόβουλου λογισμικού (malicious software=malware) είναι ένας ιός(viruses), Ένας ιός είναι ένα κομμάτι προγράμματος το οποίο επισυνάπτεται σε ένα νομότυπο πρόγραμμα με σκοπό να «μολύνει» άλλα προγράμματα.διαφέρει από το «σκουλήκι» μόνο στο ότι ένας ιός προσκολλάται σε ένα ήδη υπάρχον πρόγραμμα ενώ το «σκουλήκι» είναι από μόνο του ένα πλήρες πρόγραμμα. Τόσο οι ιοί, όσο και τα σκουλήκια προσπαθούν να διαδοθούν και μπορούν να προκαλέσουν σοβαρές ζημιές. Αυτός που γράφει έναν ιό συνήθως γράφει ένα χρήσιμο πρόγραμμα, όπως ένα παιχνίδι για MS-DOS και τοποθετεί μέσα του τον κώδικα του ιού. Στη συνέχεια το πρόγραμμα μεταφέρεται σε κάποιο Web site ή προσφέρεται δωρεάν ή σε κάποια χαμηλή τιμή σε δισκέτα. Στη συνέχεια το πρόγραμμα διαφημίζεται, οπότε οι άνθρωποι αρχίζουν να το μεταφέρουν στους υπολογιστές τους και να το χρησιμοποιούν.

Οι παραδοσιακοί ιοί είναι σε θέση να πολλαπλασιάζουν τον εαυτό τους σε ένα σύστημα, ωστόσο χρειάζονται την παρεμβολή του ανθρώπινου παράγοντα για να μεταδοθούν. Όταν το πρόγραμμα του ιού ξεκινάει, αρχίζει αμέσως να εξετάζει όλα τα εκτελέσιμα προγράμματα στο σκληρό δίσκο για να δει αν έχουν ήδη μολυνθεί. Όταν βρει ένα μη μολυσμένο πρόγραμμα, το μολύνει επισυνάπτοντας τον κώδικα του ιού στο τέλος του αρχείου. Με τον τρόπο αυτό, κάθε φορά που ένα μολυσμένο πρόγραμμα εκτελείται προσπαθεί να μολύνει και άλλα προγράμματα. Εκτός όμως από το να αντιγράψει τον εαυτό του ένας ιός μπορεί να κάνει και πολλά άλλα πράγματα, όπως να διαγράψει, να αλλάξει ή να κρυπτογραφήσει αρχεία. Υπήρξε ένας ιός που παρουσίαζε στην οθόνη ένα εκβιαστικό μήνυμα, το οποίο ζητούσε από το χρήστη να στείλει 500 δολάρια μετρητά σε

μία ταχυδρομική θυρίδα στον Παναμά, διαφορετικά θα έχανε για πάντα όλα τα δεδομένα του!

Στις μέρες μας -σε αντίθεση με το πρόσφατο παρελθόν- ο μέσος χρήστης είναι ενήμερος για τους κινδύνους που παρουσιάζουν τα συνημμένα αρχεία e-mail, ωστόσο η εξέλιξη στον χώρο των ιών είναι τέτοια που ακόμα και ένα κλικ σε ένα φαινομενικά αθώο link μιας ιστοσελίδας μέσα από τη χρήση ActiveX περιεχομένου μπορεί να επιτρέψει την εκτέλεση προγραμμάτων στον υπολογιστή σας.

Ακόμα και τα πιο ακραία μέτρα ασφαλείας δεν μπορούν να σας εγγυηθούν την απόλυτη ασφάλεια. Μόνο η συνδυαστική χρήση μιας πληθώρας εργαλείων μπορεί να εξασφαλίσει την διατήρηση της ασφάλειας και της ανωνυμίας κατά τη διάρκεια της σύνδεσης στο Internet.

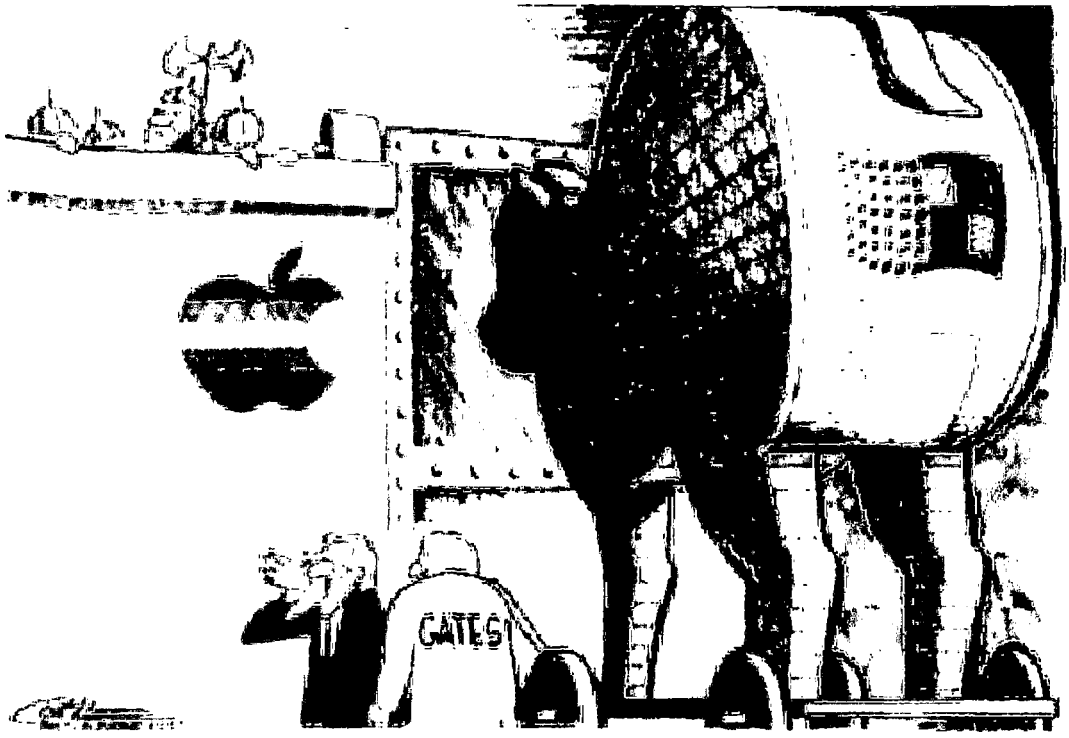
Πέρα από την αυτονόητη χρήση προγραμμάτων antivirus, η χρήση ενός firewall (hardware ή software - θα το αποφασίσετε εσείς ανάλογα με τις ανάγκες σας) είναι επιβεβλημένη.

### 6.8.3 Ο Δούρειος Ίππος (Trojan horse)

Ο όρος προήλθε από τη μυθολογία κυρίως λόγω των ομοιοτήτων που παρουσιάζουν στον τρόπο λειτουργίας τους, αφού συνήθως μεταμφιέζονται σε κάτι χρήσιμο για το χρήστη και περιμένουν την κατάλληλη στιγμή για να ανοίξουν τις πύλες, που εν προκειμένω δεν είναι άλλες από τα ports του υπολογιστή.
Αξίζει να σημειωθεί ότι τα καθαρόαιμα προγράμματα Trojan (δηλαδή τα πρώτα Trojans που δεν ενσωματώνουν λειτουργίες ιού) δεν πολλαπλασιάζουν τον εαυτό τους στο μολυσμένο σύστημα.

Τα προγράμματα Trojan horse μπορεί να φαίνονται χρήσιμα και ενδιαφέροντα σε έναν ανυποψίαστο χρήστη, αλλά στην πραγματικότητα είναι επικίνδυνα όταν εκτελεστούν. Γιατί έχουν έμμεσες ή άμεσες καταστρεπτικές συνέπειες για τον υπολογιστή, επιτρέποντας σε έναν ή περισσότερους crackers να έχουν πρόσβαση σε αυτόν. Δούρειος Ίππος είναι ένα κανονικό γενικά πρόγραμμα που εκτελεί σωστά τη λειτουργία του, αλλά εκτός από αυτήν εκτελεί και άλλες άσχημες για το χρήστη λειτουργίες.

Με το πρόσχημα των δωρεάν γραφικών, αστείων εικόνων, αστείων video κ.λπ., το Trojan Horse ξεγελά το χρήστη, ώστε να το τρέξει, και κατόπιν δημιουργεί ένα backdoor (σημείο πρόσβασης) με ανοιχτά δικαιώματα χρήσης.




"He says he comes bearing gifts."

Για παράδειγμα, αν κάποιος εισβολέας θελήσει να κλέψει τα αρχεία κάποιου άλλου χρήστη μπορεί να δημιουργήσει ένα αντίγραφο του πρωτογενούς κώδικα του κειμενογράφου (editor), να τον μεταβάλλει έτσι ώστε να κλέβει αρχεία (αλλά να συνεχίσει να δουλεύει τέλεια ως κειμενογράφος) και να τον τοποθετήσει σε κάποιο κατάλληλο κατάλογο ώστε να τον εκτελέσει το θύμα αντί για τον πραγματικό κειμενογράφο. Την επόμενη φορά που το θύμα θα καλούσε ανυποψίαστο τον κειμενογράφο θα καλούσε ουσιαστικά την έκδοση του εισβολέα, η οποία θα έκανε τέλεια τη δουλειά της ως κειμενογράφος, αλλά εκτός από αυτό θα έκλεβε και τα αρχεία του θύματος.

Τα Trojans δεν πολλαπλασιάζονται μόνα τους, σε αντίθεση με τους ιούς και τα Worms. Τα Trojans μπορούν να εκτελέσουν πολλές λειτουργίες όπως:

- Να διαγράψουν ή να παραγράψουν δεδομένα του υπολογιστή.
- Να καταστρέψουν αρχεία με επιδέξιο τρόπο.
- Να διαδώσουν άλλα επικίνδυνα προγράμματα όπως ιούς. Σε αυτή την περίπτωση, το Trojan καλείται dropper.
- Να στήσουν δίκτυα από zombie computers προκειμένου να επιτύχουν επιθέσεις DDoS ή να στείλουν spam.
- Να κατασκοπεύσουν τον χρήστη, και να αναφέρουν δεδομένα όπως συνήθειες browsing σε άλλους ανθρώπους.
- Να υποκλέψουν λεπτομέρειες λογαριασμών τραπέζης, κάτι που μπορούν να χρησιμοποιήσουν για εγκληματικές ενέργειες.
- Να αφήσουν μία πόρτα ανοιχτή στο υπολογιστικό μας σύστημα, αφήνοντας ανοιχτή την πιθανότητα μμελλοντικής επίθεσης.

Ένα τυπικό Trojan αποτελείται από δύο συστατικά μέρη-υποπρογράμματα: ένα client και ένα server. Αυτός που θέλει να αποκτήσει πρόσβαση σε κάποιον υπολογιστή εκτελεί το τμήμα client του Trojan και παράλληλα φροντίζει ώστε το τμήμα server να είναι εγκατεστημένο και ενεργό στο σύστημα.

Γνωστά προγράμματα Trojan είναι ο Sub7, το Netbus (με όλα τα παράγωγά του), ενώ το είδος, ο σκοπός χρήσης και η τεχνολογία αυτής της κατηγορία προγραμμάτων παρουσιάζει εντυπωσιακή ποικιλία.

Στη διεύθυνση που ακολουθεί θα βρείτε εκτενείς λίστες με τα ports που χρησιμοποιούν τα πιο δημοφιλή Trojan:

Sys Security
**www.sys-security.com/html/papers/trojan_list.html**

### Προστασία από Δούρειους Ίππους

Βασικός τρόπος προστασίας από τέτοιου είδους απειλές είναι η χρήση μηχανισμού ελεγχόμενης πρόσβασης των αρχείων με ταυτόχρονο έλεγχο των μεγεθών και των ημερομηνιών αλλαγής των αρχείων που περιέχουν τα προγράμματα που εκτελούνται στο σύστημα (audit). Επίσης, ο κάθε χρήστης προστατεύεται αν ο ίδιος κάνει έναν έλεγχο των προγραμμάτων τα οποία κάθε φορά εκτελεί έτσι ώστε να μην εκτελεστεί το πρόγραμμα κάποιου εισβολέα στη θέση του επιθυμητού προγράμματος. Πρέπει επίσης να είναι προσεκτικός κατά την χρήση προγραμμάτων όπως το Kazaa και το Gnutella, καθώς αποτελούν συνηθισμένες πηγές διάδοσης Trojans.

## 6.9 Οι Dialers

Μία από τις μορφές «εχθρικού λογισμικού» (malware, adware, spy ware), που όλους μας έχουν ταλαιπωρήσει κατά καιρούς, είναι και οι «Dialers» που αρχίζουν να αποτελούν ολοένα και μεγαλύτερο πρόβλημα. Οι Dialers είναι προγράμματα που χρησιμοποιούνται από διάφορες ιστοσελίδες ως τρόπος πληρωμής για το περιεχόμενο που προσφέρουν. Για να λειτουργήσουν πρέπει ο χρήστης συνειδητά να συμφωνήσει στο κατέβασμα του Dialer πληκτρολογώντας συνήθως τη λέξη "OK". Ο dialer μετά χρησιμοποιεί την τηλεφωνική γραμμή για να πάρει τηλέφωνο έναν αριθμό που δημιουργεί υψηλότερα κόστη (πχ 090) ώστε να πληρωθεί η εταιρία για τις υπηρεσίες που προσφέρει.

Μέχρι στιγμής αυτό το είδος dialer είναι νόμιμο από τη στιγμή που η εταιρία και το πρόγραμμα της είναι δηλωμένα στην κατάλληλη κρατική υπηρεσία της εκάστοτε χώρας, και εφόσον εξηγούν στον χρήστη το κόστος που προκύπτει και φυσικά του δίνουν τη δυνατότητα να επιλέξει αν θα κατεβάσει το πρόγραμμα ή όχι. Προβλήματα δημιουργούνται όταν οι dialer είναι παράνομοι, κατεβάζονται και εκτελούνται χωρίς την άδεια του χρήστη και χρεώνουν υπέρογκα ποσά. Πολλοί θα αναρωτηθούν: "Είναι δυνατόν να κατεβεί ένα πρόγραμμα χωρίς να κάνω εγώ αυτή την ενέργεια;". Και η απάντηση είναι ναι, εφόσον ο internet explorer δεν έχει ρυθμιστεί κατάλληλα σχετικά με την εκτέλεση active x. Τα active x είναι μια τεχνική που υποστηρίζεται μόνο από τον internet explorer και επιτρέπει την εκτέλεση και το κατέβασμα κώδικα. Άν ο Internet

Explorer έχει ενεργοποιημένα τα active x και δεν έχει ρυθμιστεί έτσι ώστε να προειδοποιεί τον χρήστη για την εκτέλεση και το κατέβασμα αρχείων, τότε μπορεί ένας dialer να κατεβεί χωρίς να το καταλάβουμε. Άλλοι dialers που δίνουν τη δυνατότητα στο χρήστη να τον ακυρώσει, δεν εξηγούν με σαφήνεια τι είναι το πρόγραμμα που προτρέπουν να κατεβεί ή εμφανίζουν δηλώσεις τους τύπου: "πατήστε οκ και θα έχετε άμεση πρόσβαση σε όλες τις υπηρεσίες".

Εφόσον ο Internet explorer είναι ο μοναδικός περιηγητής που χρησιμοποιεί active x, είναι αυτονόητο ότι είναι πολύ πιο ασφαλή η περιήγηση στο διαδίκτυο με την Opera. Μια πολύ καλή συμβουλή είναι να μη κάνετε κλικ σε οτιδήποτε εμφανίζεται. Πάντα να ελέγχετε τι κατεβάζετε και να μην εμπιστεύεστε εύκολα τα διάφορα sites.

Αρχικά αυτό το είδος προγραμμάτων διανεμόταν ελεύθερα από εταιρείες παροχής Internet, για να βοηθούν τους πελάτες να συνδέονται στους servers τους. Τα προγράμματα αυτά, αρχικά αλλά και σήμερα, δημιουργήθηκαν για την εξυπηρέτηση πληρωμών μικρών ποσών, δίνοντας τη δυνατότητα στο χρήστη να εισέρχεται σε συγκεκριμένες ιστοσελίδες (pay per view Websites) και να χρεώνεται στον τηλεφωνικό του λογαριασμό για το περιεχόμενο που λαμβάνει δυστυχώς όμως, λόγω του «εύκολου χρήματος» τα προγράμματα αυτά αποτελούν σήμερα μία από τις μεγαλύτερες απειλές στο χώρο του Διαδικτύου.
Αργότερα αναπτύχθηκαν και άλλες υπηρεσίες οι οποίες ήταν προσπελάσιμες από υπολογιστές. Οι υπηρεσίες αυτές, πολλές εκ των οποίων σχετίζονται με την πορνογραφία, ήταν διαθέσιμες μόνο μέσω ειδικών τηλεφωνικών αριθμών υψηλής χρέωσης, και σαν αποτέλεσμα αναπτύχθηκαν προγράμματα dialer τα οποία επέτρεπαν την πρόσβαση των χρηστών σ' αυτές. Περίπου τότε άρχισαν επίσης να εμφανίζονται ιοί ειδικά σχεδιασμένοι ώστε να κάνουν το ίδιο πράγμα, με το επιπλέον πλεονέκτημα ότι μπορούσαν να εξαπλώνονται πιο γρήγορα.

Οι δύο συνηθέστεροι τρόποι που μπορούν να δράσουν οι dialers είναι οι εξής: Μπορούν να αλλάξουν τις ρυθμίσεις του δικτύου μέσω τηλεφώνου (Dial Up Networking) έτσι ώστε να υποχρεώσουν το χρήστη να καλέσει έναν συγκεκριμένο αριθμό (συνήθως διεθνή κλήση σε αριθμό υψηλού κόστους) άγνωστο στο χρήστη. Διαγράφουν τον αριθμό του παροχέα υπηρεσιών Internet (ISP) που χρησιμοποιεί ο χρήστης και αντικαθιστούν αυτόν τον αριθμό με τον δικό τους. Κατόπιν, αυτός ο αριθμός χρησιμοποιείται κάθε φορά που συνδέεται ο χρήστης στο Internet αντί για τον αριθμό του παροχέα υπηρεσιών Internet (ISP).

Μπορούν να αναγκάσουν τον υπολογιστή να παρακάμψει τις ρυθμίσεις του δικτύου μέσω τηλεφώνου (Dial Up Networking) και να καλέσει ένα συγκεκριμένο αριθμό. Παρόλο που μπορεί να εμφανίζονται οι προεπιλεγμένες ρυθμίσεις του χρήστη όταν συνδέεται στο Internet, θα καλείται ένας άλλος αριθμός που θα έχει οριστεί από τον dialer (συνήθως διεθνή κλήση σε αριθμό υψηλής χρέωσης).

Οι dialers προέρχονται από επισκέψεις σε συγκεκριμένες ιστοσελίδες. Αυτές μπορεί να είναι ιστοσελίδες που παρέχουν πειρατικό λογισμικό, ιστοσελίδες με πορνογραφικό περιεχόμενο, ή ιστοσελίδες με αμφιλεγόμενο περιεχόμενο. Οι ιδιοκτήτες αυτών των ιστοσελίδων έχουν το dialer λογισμικό ενσωματωμένο στον κώδικα του Web site τους ώστε να γίνεται download και να εγκαθίσταται αυτόματα στο σύστημα του χρήστη,

χωρίς να γίνεται αντιληπτό και χωρίς να ζητάει απαραίτητα την συγκατάθεση του. Ένας άλλος τρόπος εμφάνισης αυτών των προγραμμάτων είναι με τη μορφή συνημμένων αρχείων σε ηλεκτρονικά μηνύματα αλληλογραφίας, που παρουσιάζονται ως δημοφιλή προγράμματα όπου εάν ο χρήστης τα αποθηκεύσει και τα εγκαταστήσει, εγκαθιστά εν αγνοία του εφαρμογή dialer.

Η ιδέα πίσω από αυτά τα προγράμματα είναι ότι οι άνθρωποι που τα παράγουν μπορούν να αποκομίσουν έσοδα από τους χρήστες που καλούν τον αριθμό που είναι εγκατεστημένος στην ιστοσελίδα τους. Ο χρήστης αντιμετωπίζει αναπάντεχα αυξημένους λογαριασμούς τηλεφώνου, καθώς οι κλήσεις που κατευθύνουν τα προγράμματα αυτά μπορεί να φτάνουν και τα 2€ το λεπτό, αντί των 0,0058€ το λεπτό για ώρες αιχμής και 0,0029€ το λεπτό για ώρες μη αιχμής που είναι η χρέωση ΕΠΑΚ. Βάση αυτών, διαφαίνεται ότι η χρέωση των κλήσεων σε αριθμούς υψηλής χρέωσης είναι κατά 689 φορές ακριβότερη από τη χρέωση ΕΠΑΚ.

Να σημειώσουμε ότι τα προγράμματα dialer απειλούν κατά κύριο λόγο τους συνδρομητές υπηρεσιών PSTN ή ISDN ή/ και τα συστήματα που έχουν εγκατεστημένο modem (PSTN / ISDN) το οποίο είναι συνδεδεμένο σε τηλεφωνική γραμμή, ενώ οι συνδρομητές υπηρεσιών ADSL δεν διατρέχουν κίνδυνο καθώς εξ' ορισμού δεν έχουν τη δυνατότητα να πραγματοποιήσουν τηλεφωνική κλήση και συνδέονται άμεσα με την υπηρεσία Internet. Ωστόσο στην περίπτωση που ο υπολογιστής εκτός της ADSL σύνδεσης έχει εγκατεστημένο και κάποιο ISDN ή PSTN modem το οποίο είναι συνδεδεμένο σε τηλεφωνική γραμμή, δεν μπορούμε να αποκλείσουμε το γεγονός αυτό.

## Προστασία από dialers

Είναι σημαντικό να θυμόμαστε ότι τα προγράμματα dialer μπορούν να προκαλέσουν προβλήματα μόνο στους υπολογιστές που συνδέονται στο Internet μέσω dial-up δικτύων (δηλ. μέσω modem και τηλεφωνικών γραμμών), δεδομένου ότι οι άλλες μορφές σύνδεσης - π.χ. συνδέσεις ευρείας ζώνης ή καλωδιακές συνδέσεις - λειτουργούν διαφορετικά και δεν απαιτούν την κλήση ενός αριθμού.

Η επίθεση ενός προγράμματος dialer εκκινεί συνήθως όταν ο χρήστης επισκέπτεται συγκεκριμένες ιστοσελίδες. Πρόσφατα οι ιστοσελίδες με «αμφιλεγόμενο» περιεχόμενο (πορνογραφία, εργαλεία για hackers, cracks, παράνομες μεταφορές προγραμμάτων, κ.α.) άρχισαν να τίθενται σε καθεστώς απαγόρευσης. Ταυτόχρονα όμως άρχισαν να αυξάνονται οι αναφορές από χρήστες οι οποίοι έπεσαν θύματα διάφορων μορφών εχθρικού λογισμικού αφού επισκέφτηκαν ιστοσελίδες οι οποίες έδειχναν εντελώς «αθώες». Αυτό σημαίνει ότι τουλάχιστον προς το παρόν, κανένας χρήστης δεν είναι ασφαλής από αυτούς τους τύπους επιθέσεων.

Η καλύτερη προστασία έναντι αυτών των επιθέσεων είναι η εγκατάσταση μιας εφαρμογής η οποία θα μπορεί να εξακριβώνει εάν πρόκειται να υλοποιηθεί μία κλήση μέσω ενός αριθμού διαφορετικού από τον κανονικό, και θα ειδοποιεί τον χρήστη. Επιπλέον, επειδή υπάρχουν ιοί ειδικά σχεδιασμένοι ώστε να εγκαθιστούν προγράμματα dialer στους υπολογιστές που μολύνουν χωρίς να το γνωρίζει ο χρήστης, η ιδανική λύση είναι ο συνδυασμός της προστασίας έναντι των dialer και της προστασίας έναντι των ιών σ' ένα και μόνο προϊόν.

Το Antivirus, δίνει τη δυνατότητα της προστασίας του Η/Υ και από dialers. Κατά την εγκατάσταση ρωτάει τον χρήστη αν επιθυμεί την ανίχνευση και προστασία τυχόν dialers στον Η/Υ.

## 6.10 Windows Rootkits - Αόρατος Εισβολέας

Τα Windows Kernel Rootkits είναι μια πάρα πολύ επικίνδυνη απειλή που δεν εντοπίζεται από τα antivirus, της οποίας το απόλυτο δυναμικό δεν έχει χρησιμοποιηθεί ακόμα από τους Hacker και τους συγγραφείς Ιών. Τα Rootkits για Linux και συστήματα Unix είναι ένα τόσο παλιό όσο και σύγχρονο πρόβλημα, τώρα όμως γίνεται γνωστό ότι έχουν σχεδιαστεί τέτοια προγράμματα και για το λειτουργικό της Microsoft. Η κατασκευάστρια εταιρία των windows προειδοποίησε το ευρύ κοινό γνωστοποιώντας τον κίνδυνο και κατασκευάζοντας ένα πρόγραμμα για τη καταπολέμηση των rootkits (Strider GhostBuster). Ακόμα μια πολύ γνωστή εταιρία antivirus, η F-Secure κατασκεύασε το BlackLight, ένα πρόγραμμα που εντοπίζει γνωστά rootkits και διατίθεται δωρεάν μέχρι τον Ιανουάριο του 2006 (έχει πάρει ήδη πολλές παρατάσεις ώστε να αναπτυχθεί το πρόγραμμα με τη βοήθεια των αναφορών χρηστών).

Τα rootkits είναι προγράμματα που δε λειτουργούν σε επίπεδο χρήστη ή σε επίπεδο απλών εφαρμογών. Είναι έτσι προγραμματισμένα ώστε να λειτουργούν στη "ρίζα" ή στο πυρήνα του λειτουργικού συστήματος. Τα υπόλοιπα προγράμματα, στα οποία συμπεριλαμβάνονται και τα antivirus δεν έχουν δικαιώματα διαχειριστή (root) και δεν ελέγχουν τον πυρήνα του λειτουργικού συστήματος για ιούς και για άλλα βλαβερά προγράμματα. Τα rootkits βέβαια δεν περιέχουν βλαβερό κώδικα. Αυτό που κάνουν είναι να κρύβουν αρχεία και προγράμματα αλλά και να σβήνουν τα ίχνη τους από τα log του Η/Υ. Έτσι όταν ένα rootkit έρχεται με ένα δούρειο ίππο, αυτός εγκαθίσταται χωρίς να μπορεί να τον δει και να τον εντοπίσει κανένα antivirus. Ένας τέτοιος δούρειος ίππος μπορεί να χρησιμοποιηθεί για να εγκατασταθούν και άλλα βλαβερά προγράμματα μέσω δικτύου, παραμένοντας αόρατα. Ένα πρόγραμμα rootkit μπορεί να εντοπιστεί από ένα antivirus όταν ακόμη δεν έχει εγκατασταθεί, όταν ακόμη δεν είναι ενεργό. Ο μόνος πραγματικά αποτελεσματικός τρόπος προστασίας από ένα τέτοιο πρόγραμμα είναι να ελέγχετε όλα τα αρχεία και τα προγράμματα που κατεβάζετε πριν τα ανοίξετε, με το ενημερωμένο antivirus του Η/Υ. Ακόμα και ο έλεγχος των αρχείων πριν εκτελεσθούν όμως μπορεί να μην εντοπίσει ένα νέο rootkit με άγνωστο για το antivirus κώδικα.

Μέχρι στιγμής είναι γνωστά λιγότερο από δέκα rootkits και είναι άγνωστο πόσα από αυτά υπάρχουν ακόμα που δεν έχουν εντοπισθεί. Ορισμένα spyware χρησιμοποιούν rootkits για να γίνονται αόρατα όπως το γνωστό Elite Toolbar, ProAgent, Probot SE και ορισμένα σκουλήκια και δούρειοι ίπποι.

Ορισμένα rootkits μπορούν να αφαιρεθούν σε ασφαλή εκκίνηση της λειτουργίας του συστήματος ή μέσω ενός bootable δίσκου που να περιέχει το Windows PE. Τελικά όμως, ο μόνος σίγουρος τρόπος αφαίρεσης των rootkits και των βλαβερών προγραμμάτων που έχει εγκαταστήσει, είναι το φορμάρισμα (format) του δίσκου.

## 6.11 Εισαγωγή στην ασφάλεια δικτύων συνδεδεμένων με το Internet

Οι πρόσφατες επιθέσεις εναντίον μεγάλων και δημοφιλών sites του δικτύου όπως τα Yahoo!, Amazon, eBay και CNN επανέφεραν στη δημοσιότητα το ζήτημα της ασφάλειας των δεδομένων μέσα στο Internet. Οι χρήστες αναρωτιούνται πώς μπορούν να εμπιστευθούν ένα εταιρικό web site και να του δώσουν τα στοιχεία τους όταν ακόμη και τα μεγαλύτερα ονόματα του χώρου αποδεικνύονται ευάλωτα σε επιθέσεις, ενώ οι επιχειρηματίες προβληματίζονται για τη μακροπρόθεσμη αποδοτικότητα μιας επένδυσης η οποία μπορεί οποιαδήποτε στιγμή να βρεθεί στο έλεος ενός cracker.

θα ασχοληθούμε με τα θέματα ασφαλείας που προκύπτουν από τη σύνδεση ενός δικτύου (π.χ. μιας επιχείρησης) στο Internet, Πριν όμως ασχοληθούμε με το ζήτημα της αρχιτεκτονικής η οποία εξασφαλίζει τη μεγαλύτερη δυνατή ασφάλεια για ένα δίκτυο ας δούμε συνοπτικά ποια είδη επιθέσεων μπορεί να δεχθεί μια εταιρεία η οποία έχει συνδεθεί με το Internet:

**1. Denial of Service**

Η απλούστερη μορφή επιθέσεως ονομάζεται denial of service (παλιά την αποκαλούσαν ping of death) και συνίσταται στην αποστολή πάρα πολλών "νόμιμων" αιτημάτων προς το δίκτυο του θύματος. Για παράδειγμα, αν ο δεχόμενος την επίθεση έχει ένα web site (όπως συνέβη στην περίπτωση των Yahoo!, Amazon, eBay, CNN και άλλων) ο επιτιθέμενος του αποστέλλει διαρκώς από πλαστές διευθύνσεις αιτήματα λήψης web σελίδων. Για να ικανοποιήσει αυτά τα αιτήματα ο web server είτε προσπαθεί να στείλει web σελίδες σε παραλήπτες που δεν τις ζήτησαν, είτε τις στέλνει σε διευθύνσεις που δεν υπάρχουν.

Και στις δύο περιπτώσεις οι σελίδες δεν παραδίδονται ποτέ (ο web server καταλαβαίνει το λάθος του και σταματά την αποστολή). Το σύστημα όμως καταναλώνει μεγάλα ποσά υπολογιστικής ισχύος και bandwidth στην προσπάθειά του να παραδώσει τις σελίδες και να καταλάβει τι συμβαίνει. Αν λοιπόν τα ψεύτικα αιτήματα που λαμβάνει είναι πάρα πολλά, τότε το σύστημα υπερφορτώνεται και παύει πλέον να λειτουργεί ή καθυστερεί πάρα πολύ να εξυπηρετήσει ένα "νόμιμο" αίτημα διότι είναι απασχολημένο με την διαχείριση όλων των πλαστών αιτημάτων τα οποία λαμβάνει συνεχώς.

Όπως φαίνεται από την παραπάνω περιγραφή, οι επιθέσεις αυτής της μορφής δεν κλέβουν δεδομένα ούτε επιτρέπουν στον επιτιθέμενο να αποκτήσει τον έλεγχο του εξοπλισμού μιας επιχείρησης. Απλώς δεν επιτρέπουν στο θύμα να εξυπηρετήσει τους πελάτες και τους συνδρομητές του (γι' αυτό και ονομάζονται denial of service).

Αυτή η ιδιαιτερότητα όμως δεν τις καθιστά λιγότερο επίφοβες. Το πρόβλημα με τις επιθέσεις denial of service είναι πως δεν υπάρχει ακόμη κάποιος απλός και αποτελεσματικός τρόπος προστασίας από αυτές. Συνήθως, ο επιτιθέμενος αποστέλλει τα αιτήματά του από πολλά μηχανήματα μέσα στο δίκτυο (distributed denial-of-service ή DDS), κρύβοντας έτσι τα ίχνη του και κάνοντας πολύ δύσκολη την αναγνώριση μιας επίθεσης denial of service μέχρι να είναι αργά (επειδή είναι πολύ δύσκολο να καταλάβει κανείς ότι τα αιτήματα που λαμβάνει είναι πλαστά, ο συναγερμός δεν δίνεται παρά μόνο

όταν το δίκτυο δέχεται πλέον τόσο μεγάλο όγκο αιτημάτων που σχεδόν παύει να λειτουργεί).

Ωστόσο, αυτή η λύση δεν φαίνεται να αρέσει σε πολλούς, καθώς (παρά την ενσωματωμένη κρυπτογράφηση που διαθέτει) το IPv6 καταργεί πλήρως την ανωνυμία του δικτύου και κάνει εφικτή την παρακολούθηση όλων των δραστηριοτήτων οποιουδήποτε χρήστη. Έτσι μια δικτατορική κυβέρνηση (π.χ. Κίνα, Ιράκ, Βόρεια Κορέα κ.λπ.) δεν θα χρειάζεται να ανησυχεί πλέον για τις επιπτώσεις της ανωνυμίας του δικτύου αφού θα μπορεί να παρακολουθεί με άνεση τις online κινήσεις όλων των κατοίκων της.

## 2. Κλασικές μορφές επίθεσης εναντίον ενός δικτύου

Η συνηθέστερη μορφή επίθεσης συνίσταται στην "κατάληψη" των υπολογιστών ενός τοπικού δικτύου από τρίτους. Πρόκειται για το είδος της εισβολής το οποίο απεικονίζεται σε διάφορες ταινίες και, αν και τα πράγματα δεν είναι τόσο ρομαντικά ή εύκολα όσο παρουσιάζονται εκεί, το κύριο χαρακτηριστικό μιας διείσδυσης αυτής της μορφής είναι πως ο επιτιθέμενος έχει τη δυνατότητα να αντιγράψει, να τροποποιήσει ή να διαγράψει δεδομένα, να αλλάξει τις ρυθμίσεις των εγκατεστημένων προγραμμάτων και, το χειρότερο απ' όλα, να εγκαταστήσει δικά του προγράμματα στο μηχάνημα ή το δίκτυο ενός τρίτου.

Μερικές φορές η επίθεση γίνεται διότι ο εισβολέας ενδιαφέρεται για την ίδια την επιχείρηση (π.χ. θέλει να της κάνει ζημιά ή να κλέψει κάποια στοιχεία). Συχνά όμως ο επιτιθέμενος εισβάλει σε ένα δίκτυο αποκλειστικά και μόνο για να το χρησιμοποιήσει ως εφαλτήριο για την επόμενη επίθεσή του. Για παράδειγμα, μπορεί να θέλει να επιτεθεί στο δίκτυο ενός συνεταίρου ή συνεργάτη της επιχείρησης και εκτιμά πως οι επιθέσεις του θα γίνουν πιο δύσκολα αντιληπτές αν πραγματοποιηθούν από μια αξιόπιστη τοποθεσία όπως το δίκτυο και τα μηχανήματα μιας εταιρείας την οποία εμπιστεύεται ο επιτιθέμενος διότι έχει συχνά (δικτυακές) επαφές μαζί της.

Επίσης, οι επιθέσεις denial of service γίνονται συνήθως από μηχανήματα τρίτων διότι η αποστολή των πλαστών αιτημάτων απαιτεί μεγάλο bandwidth (δυνατότητα μεταφοράς δεδομένων) που είναι δύσκολο να βρεθεί σε ένα μόνο μηχάνημα. Ένας άλλος λόγος για τη χρήση πολλών μηχανημάτων για μια επίθεση denial of service είναι πως η κατανομή της αποστολής των πλαστών αιτημάτων σε πολλά μηχανήματα καθιστά πιο δύσκολη την αναγνώριση και την αντιμετώπισή της (στην αρχή το θύμα νομίζει απλώς πως αυξήθηκε το ενδιαφέρον για τις υπηρεσίες του δικτύου του).

### Στρατηγικά διλήμματα

Το πρόβλημα για κάθε επιχείρηση η οποία θέλει να προστατεύσει το δίκτυό της από τις επιβουλές τρίτων είναι πως οι επιταγές της ασφάλειας απαιτούν την όσο το δυνατόν μικρότερη σύνδεσή της με το Internet, ενώ οι επιταγές της κερδοφορίας (αύξηση της παραγωγικότητάς της και καλύτερη εξυπηρέτηση των πελατών της) απαιτούν το όσο το δυνατόν μεγαλύτερο άνοιγμά της στον εξωτερικό δικτυακό κόσμο.

Ακολουθώντας το μοντέλο e-business η επιχείρηση πρέπει να δίνει στον πελάτη τη δυνατότητα να παρακολουθεί online το υπόλοιπο του λογαριασμού του, να στέλνει παραγγελίες, να μαθαίνει για τη διαθεσιμότητα κάθε προϊόντος και γενικά να προβαίνει σε μια σειρά από εργασίες οι οποίες απαιτούν πρόσβαση στο πληροφοριακό σύστημα της εταιρείας, δηλαδή στο εσωτερικό τοπικό δίκτυο που αυτή διατηρεί και στα μηχανήματα που το απαρτίζουν.

Ακόμη, η εταιρεία πρέπει να παρέχει στο προσωπικό της τη δυνατότητα να συνδέεται με το Internet, ενώ σε πολλές περιπτώσεις πρέπει να επιτρέπει στους εξωτερικούς συνεργάτες της ή στο εκτός γραφείου προσωπικό της να συνδέεται με το εσωτερικό της δίκτυο και να εκτελεί μια σειρά από "ευαίσθητες εργασίες" όπως η αλλαγή του ποσοστού έκπτωσης ή του πιστωτικού ορίου ενός πελάτη, η τροποποίηση του τόπου παράδοσης μιας παραγγελίας κ.λπ.

**Κατανομή δικαιωμάτων πρόσβασης**

Από την παραπάνω περιγραφή γίνεται φανερό πως κάθε επιχείρηση ή οργανισμός χρειάζεται ένα δίκτυο κάποια από τα τμήματα του οποίου θα είναι απόλυτα ανοικτά σε όλους (π.χ. ο τιμοκατάλογος ή οι περιγραφές των προϊόντων), κάποια θα είναι διαθέσιμα μόνο σε ορισμένους (π.χ. πωλητές οι οποίοι συνδέονται από το γραφείο του πελάτη για να οριστικοποιήσουν μια παραγγελία), ενώ κάποια άλλα θα παραμένουν εντελώς κλειστά στον υπόλοιπο κόσμο (π.χ. λογιστήριο).

Το πρώτο βήμα για να επιτευχθεί αυτός ο διαχωρισμός αμνών και εριφίων είναι η λεπτομερής καταγραφή όλων όσων έχουν πρόσβαση στο σύστημα, καθώς και των εργασιών που επιτρέπεται να εκτελέσει ο καθένας. Ο παλαιός τρόπος δικτύωσης (κληρονομιά της εποχής του ανοιχτού σε όλους Internet) ορίζει πως συγκεκριμενοποιούμε τις απαγορεύσεις (ποια πράγματα δεν μπορεί να κάνει κάθε χρήστης) και στη συνέχεια δηλώνουμε στο σύστημα ασφαλείας του δικτύου τι απαγορεύεται. Έτσι, ό,τι δεν απαγορεύεται είναι επιτρεπτό.

Δυστυχώς, η εποχή αυτή ανήκει πια στο παρελθόν και σήμερα ακολουθείται η ακριβώς αντίθετη στρατηγική: Ορίζουμε τι επιτρέπεται και απαγορεύουμε όλα τα υπόλοιπα. Αυτό είναι το πρώτο και πιο ουσιαστικό βήμα για την εγκαθίδρυση μηχανισμών ασφαλείας μέσα σε ένα δίκτυο το οποίο είναι συνδεδεμένο με το Internet.

Ας σημειωθεί πως, παρά τη μεγάλη δημοτικότητα που αποκτούν οι επιθέσεις τρίτων σε επιχειρήσεις, η εμπειρία έχει δείξει πως η πλειοψηφία των παραβιάσεων ασφαλείας δικτύων γίνεται από το ίδιο το προσωπικό της εταιρείας, είτε από κακοήθεια (π.χ. από δυσαρεστημένους εργαζόμενους), είτε από υπολογισμό (π.χ. δωροδοκία από ανταγωνιστές). Για τον λόγο αυτό κάθε μηχανισμός ασφαλείας δεν πρέπει να περιορίζεται στον απλουστευτικό διαχωρισμό του "ξένοι" και "δικοί μας", αλλά να ορίζει με λεπτομέρεια τα δικαιώματα πρόσβασης που δίδονται σε κάθε εργαζόμενο ή κάθε ομάδα του προσωπικού.

## Packet filtering Η πρώτη γραμμή άμυνας

Το επόμενο βήμα, μετά τον καθορισμό των δικαιωμάτων κάθε ομάδας χρηστών, είναι η επιλογή του καταλληλότερου μηχανισμού ασφαλείας, η αξιοπιστία και η αποτελεσματικότητα του οποίου συναρτώνται άμεσα με τις οικονομικές δυνατότητες της επιχείρησης, καθώς και με τις τεχνικές γνώσεις του δικτυακού προσωπικού της.

Η απλούστερη μέθοδος προστασίας ενός δικτύου είναι η χρήση της τεχνικής του Packet Filtering. Όπως είναι γνωστό, όλα τα δεδομένα, τα μηνύματα και οι εντολές διακινούνται μέσα στο Internet με τη μορφή πακέτων δεδομένων τα οποία διαβιβάζονται από τον ένα router (δρομολογητή) στον άλλον, μέχρι να παραδοθούν στον τελικό προορισμό τους (συνήθως στον Η/Υ όπου τρέχει η εφαρμογή η οποία θα τα διαχειριστεί).

Στην πραγματικότητα, ο router είναι και αυτός ένας Η/Υ, με τη διαφορά πως έχει εξειδικευθεί αποκλειστικά στη διακίνηση των στοιχείων που χρησιμοποιούν τα άλλα μηχανήματα του δικτύου. Λόγω αυτής της ιδιαιτερότητας, ο router είναι ο πρώτος ο οποίος θα λάβει και θα διαβιβάσει οποιοδήποτε "παράνομο" αίτημα πρόσβασης ή οποιαδήποτε εντολή δοκιμάζει να δώσει σε κάποιον Η/Υ του τοπικού δικτύου όποιος προσπαθεί να διεισδύσει αδικαιολόγητα σε αυτό.

Για τον λόγο αυτό, πολλοί διαχειριστές συστημάτων χρησιμοποιούν τον router μέσω του οποίου συνδέονται με το Internet ως την πρώτη γραμμή άμυνάς τους, ορίζοντας στους πίνακες δρομολόγησής του (routing tables) πώς πρέπει να αντιδρά σε κάθε αίτημα (π.χ. αν σου ζητήσουν να στείλεις δεδομένα αυτής της μορφής στο μηχάνημα Χ απάντησε πως αυτή η δυνατότητα ή αυτό το μηχάνημα δεν υπάρχουν).

Η τεχνική του Packet Filtering είναι συνήθως απλή στην εφαρμογή της και σχετικά φθηνή (απαιτείται μόνο η ρύθμιση του router ο οποίος υπάρχει ήδη στις εγκαταστάσεις της εταιρείας). Για τον λόγο αυτό υπάρχουν συστήματα Firewall τα οποία βασίζονται αποκλειστικά και μόνο στο Packet Filtering για την προστασία ενός ή περισσότερων δικτύων.

Ένα σοβαρό μειονέκτημα του Packet Filtering είναι πως λειτουργεί αποτελεσματικά μόνο αν ο router πρέπει να διαχειριστεί χαμηλό όγκο κίνησης ή αν ο αριθμός των φίλτρων είναι μικρός. Όσο αυξάνει η κίνηση τόσο περισσότερα πακέτα πρέπει να ελέγξει ο router, ενώ όσο αυξάνουν τα φίλτρα τόσο περισσότεροι έλεγχοι πρέπει να γίνουν πριν επιτραπεί σε ένα πακέτο να μπει στο τοπικό δίκτυο ή να βγει από αυτό. Έτσι όμως επιβαρύνεται υπερβολικά ο επεξεργαστής του router και περιορίζεται η απόδοσή του.

Τέλος, το Packet Filtering είναι εξαιρετικά δύσκολο να εφαρμοστεί σε περίπλοκα τοπικά δίκτυα τα οποία έχουν μεγάλη ποικιλία επαφών με το Internet. Όσο περισσότερες υπηρεσίες (telnet, ftp, smtp, pop, http κ.λπ.) πρέπει να ελεγχθούν από τον router τόσο δυσκολότερη γίνεται η καλή ρύθμισή του για εφαρμογές Packet Filtering. Το πρόβλημα βρίσκεται στο γεγονός ότι όποια παράμετρος δεν έχει προβλεφθεί να φιλτράρεται είναι ελεύθερη να διακινηθεί από και προς το τοπικό δίκτυο. Έτσι, ακόμη και το παραμικρό λάθος ή αβλεψία μπορεί να αποβεί μοιραίο (πολλοί crackers χρησιμοποιούν ειδικά προγράμματα που δοκιμάζουν μια μια όλες τις δυνατές τεχνικές παράκαμψης των

φίλτρων μέχρι να βρουν εκείνη τη δίοδο που από άγνοια, λάθος ή αδιαφορία έχει μείνει ανεξέλεγκτη).

## Firewall Η συνηθέστερη λύση

Το επόμενο, και ανώτερο, επίπεδο προστασίας είναι η εγκατάσταση και καλή αξιοποίηση ενός Firewall. Τα πρώτα Firewalls ήταν απλώς Packet Filtering Routers οι οποίοι τοποθετούνταν σε στρατηγικά σημεία του δικτύου έτσι ώστε ακόμη και αν κάποιος εξωτερικός εχθρός διείσδυε σε ένα μέρος του δικτύου να μην αποκτά αμέσως ελεύθερη πρόσβαση στο σύνολο των μηχανημάτων που το απαρτίζουν. Λειτουργούσαν δηλαδή ως αντιπυρικές πόρτες (Firewalls) οι οποίες εμποδίζουν τη φωτιά η οποία έχει ανάψει σε κάποιο δωμάτιο να εξαπλωθεί στο υπόλοιπο κτίριο.

Ένα Firewall αποτελείται συνήθως από έναν Η/Υ, γνωστό με το όνομα Bastion host (κόμβος προμαχώνας), και μια σειρά από εφαρμογές ανταπόκρισης (proxy services). Ο Bastion host έχει εγκατεστημένη μια ασφαλή έκδοση ενός λειτουργικού συστήματος. Η έκδοση αυτή είναι ουσιαστικά η ίδια με εκείνη που χρησιμοποιείται από την πλειοψηφία των χρηστών (π.χ. UNIX, NT κ.λπ.) με τη διαφορά πως έχουν απενεργοποιηθεί όλα τα χαρακτηριστικά της πλην των απολύτως απαραίτητων (το σκεπτικό εδώ είναι πως όσο λιγότερες εφαρμογές περιλαμβάνει το λειτουργικό, τόσο μειώνονται οι πιθανότητες να ανακαλυφθεί κάποιο τρωτό σημείο σε μια από αυτές).

Μερικές φορές, πάνω στον Bastion host εγκαθιστούμε μια σειρά από Circuit Level Gateways (προγράμματα τα οποία παρακολουθούν ποιος συνδέεται με το εσωτερικό δίκτυο και καθορίζουν ποιες εργασίες μπορεί να κάνει μέσα σε αυτό). Συνήθως όμως ο Bastion host έχει εγκατεστημένα διάφορα Application-Level Gateways τα οποία λειτουργούν ως proxy services, μεταφράζοντας τα αιτήματα από και προς τους Η/Υ του τοπικού δικτύου.

Έτσι, οποιοσδήποτε μέσα στο Internet επικοινωνεί με ένα μηχάνημα του εσωτερικού δικτύου δεν έχει ποτέ απευθείας επαφή με αυτό. Το αίτημά του διατυπώνεται στο αντίστοιχο Application-Level Gateway το οποίο το διαβιβάζει στο μηχάνημα και επιστρέφει την απάντηση.

Χάρη στα Application-Level Gateways απαγορεύεται οποιαδήποτε μορφή επικοινωνίας μεταξύ του εσωτερικού δικτύου και του Internet εκτός από εκείνες για τις οποίες έχει εγκατασταθεί το ανάλογο λογισμικό (το Application-Level Gateway που επιτρέπει τη χρήση της συγκεκριμένης υπηρεσίας). Ο διαχειριστής του συστήματος λοιπόν εγκαθιστά ένα Application-Level Gateway για κάθε εφαρμογή και φροντίζει να το ρυθμίσει κατάλληλα. Με τον τρόπο αυτό, η επικοινωνία μεταξύ τοπικού δικτύου και Internet μπορεί να επιτευχθεί μόνο για όσες υπηρεσίες έχουν εγκατεστημένο το αντίστοιχο Application-Level Gateway στον Bastion host και μόνο αν το Application-Level Gateway έχει ρυθμιστεί με τέτοιο τρόπο ώστε να επιτρέπεται η μορφή επικοινωνίας που ζητεί ο χρήστης. (Η τεχνική αυτή ονομάζεται και protocol filtering διότι απ' όλα τα πρωτόκολλα του Internet, επιτρέπεται η διέλευση μόνο σε όσα ορίζει το Application-Level Gateway.)

Αξίζει να σημειωθεί πως τα Firewalls δεν ελέγχουν μόνο ό,τι εισέρχεται στο εσωτερικό δίκτυο, αλλά και ό,τι εξέρχεται από αυτό. Έτσι, μερικές φορές, οι χρήστες του εσωτερικού δικτύου μπορούν να δουν sites στο Internet, αλλά δεν μπορούν να επικοινωνήσουν με αυτά, πράγμα που φυσικά προκαλεί δυσφορία και έντονες διαμάχες μεταξύ των διαχειριστών του εσωτερικού δικτύου (οι οποίοι θέλουν να το κρατήσουν όσο πιο "κλειστό" γίνεται) και των χρηστών του (οι οποίοι θέλουν να έχουν πρόσβαση σε όσο το δυνατόν περισσότερες υπηρεσίες).

Η παραπάνω δομή επιτυγχάνει υψηλά επίπεδα ασφαλείας, καθώς το Firewall λειτουργεί πάντοτε ως ενδιάμεσος, ελέγχοντας και μεταφράζοντας όλες τις επαφές του τοπικού δικτύου με το Internet. Δυστυχώς, αυτή η μετάφραση αποτελεί και το μεγαλύτερο μειονέκτημα των Firewalls, καθώς πολλές φορές απαιτείται η χρήση ειδικών εφαρμογών από τον χρήστη του Internet ο οποίος θέλει να επικοινωνήσει με κάποιο μηχάνημα του εσωτερικού δικτύου.

άλλα μειονεκτήματα των Firewalls είναι το μεγάλο κόστος προμήθειας εξοπλισμού και εκπαίδευσης προσωπικού και η μειωμένη ταχύτητα επικοινωνίας του εσωτερικού δικτύου με το Internet. Γενικά, η λειτουργία των Firewalls απαιτεί ισχυρά μηχανήματα με μεγάλη υπολογιστική ισχύ, καθώς το Firewall είναι υποχρεωμένο όχι μόνο να μεταφράζει κάθε μεταφορά δεδομένων από και προς το εσωτερικό δίκτυο, αλλά και να επιβεβαιώνει πως κάθε αίτημα σύνδεσης έρχεται από "έμπιστη" IP διεύθυνση. (Πολύ συχνά οι crackers ακολουθούν μια τεχνική με το όνομα IP spoofing χάρη στην οποία ένα μηχάνημα μπορεί να ιδιοποιηθεί την IP διεύθυνση ενός άλλου. Έτσι, ένας "απλός" router μπορεί να εξαπατηθεί και να επιτρέψει τη χρήση του εσωτερικού δικτύου σε έναν Η/Υ ο οποίος κανονικά δεν δικαιούται πρόσβαση σε αυτό.)

Παρόλα αυτά, η λύση των Firewalls αποτελεί σήμερα τον πιο δημοφιλή τρόπο προστασίας ενός δικτύου. Πολλές επιχειρήσεις μάλιστα συνδυάζουν τη χρήση των Firewalls με Packet Filtering για να αυξήσουν ακόμη περισσότερο τη δυσκολία διείσδυσης ανεπιθύμητων μέσα στο εσωτερικό δίκτυό τους. (Η τεχνική του συνδυασμού Packet Filtering με Circuit Level και Application-Level Gateways ονομάζεται Stateful Multilayer Inspection Firewall.)

**Demilitarized Zone Η προχωρημένη λύση**

Το υψηλότερο επίπεδο ασφαλείας δικτύων επιτυγχάνεται με μια άλλη μέθοδο γνωστή με το όνομα Demilitarized Zone (DMZ) ή Screened-Subnet Firewall. Η τεχνική αυτή χρησιμοποιεί ένα Firewall και ένα Packet Filtering router μέσω των οποίων εξασφαλίζεται η επικοινωνία ενός τμήματος του εσωτερικού δικτύου, γνωστού με το όνομα Demilitarized Zone (αποστρατιωτικοποιημένη περιοχή), με το Internet. Αυτή η περιοχή περιέχει μόνο τις πολύ βασικές υπηρεσίες (π.χ. web) και τα μηχανήματά της της είναι προσβάσιμα από το Internet μέσω του Firewall και του Packet Filtering router.

Στην αρχιτεκτονική αυτή όμως υπάρχει και ένας δεύτερος Packet Filtering router ο οποίος συνδέει την Demilitarized Zone με το υπόλοιπο εσωτερικό δίκτυο της εταιρείας και καθιστά το τμήμα αυτό του δικτύου αόρατο από τον έξω κόσμο (από το υπόλοιπο Internet). Με τον τρόπο αυτό επιτυγχάνεται το υψηλότερο δυνατό επίπεδο προστασίας αφού ουσιαστικά κρύβουμε από τους πιθανούς εισβολείς ακόμη και την ύπαρξη των πιο

ευαίσθητων από τα μηχανήματά μας, ενώ απαγορεύουμε σε οποιαδήποτε δεδομένα από το Internet να φθάσουν μέχρι το αόρατο δίκτυο (όλα τα αιτήματα διεκπεραιώνονται από τα μηχανήματα της Demilitarized Zone).

**Intrusion Detection Systems: Το σύστημα συναγερμού**

Οι παραπάνω τεχνικές αναφέρονται στους τρόπους παθητικής προστασίας ενός δικτύου. Ουσιαστικά αποτελούν εμπόδια με τα οποία φράζουμε τον δρόμο των εισβολέων, δυσκολεύοντας την πρόσβασή τους στο εσωτερικό δίκτυο μιας επιχείρησης ή ενός οργανισμού. Ωστόσο, η ιστορία μας διδάσκει πως ποτέ ένα φυσικό εμπόδιο δε στάθηκε ικανό από μόνο του να εμποδίσει κάποιον εισβολέα. Πάντοτε θα χρειάζονται φρουροί για να σημαίνουν συναγερμό κάθε φορά που ο εχθρός βρίσκεται ante portas και πάντοτε θα πρέπει να υπάρχουν πολεμιστές έτοιμοι να του κλείσουν το δρόμο, αν τύχει και ανακαλύψει κάποια ξεχασμένη Κερκόπορτα.

Στην περίπτωση της ασφάλειας δικτύων, οι φρουροί αυτοί ονομάζονται Intrusion Detection Systems (IDSs). Πρόκειται για ειδικά προϊόντα λογισμικού τα οποία έχουν ως έργο την παρακολούθηση της λειτουργίας όλου του δικτύου και της αναφοράς οποιασδήποτε "ύποπτης" κίνησης ανιχνευθεί.

Για ένα IDS ύποπτοι θεωρούνται τόσο οι εξωτερικοί χρήστες που συνδέονται στο εσωτερικό δίκτυο μέσω του Internet, όσο και οι εσωτερικοί χρήστες του δικτύου (όσοι έχουν πρόσβαση από τοπικά συνδεδεμένα μηχανήματα). Τα IDSs παρακολουθούν το δίκτυο όλο το 24ωρο, δίνοντας συνεχώς αναφορές τόσο για επικίνδυνα περιστατικά (π.χ. ένας χρήστης προσπάθησε να διαγράψει ή να αντιγράψει αρχεία στα οποία δεν έχει δικαίωμα πρόσβασης) όσο και για ύποπτες ανωμαλίες οι οποίες μπορεί να υποδηλώνουν την αρχή μιας επίθεσης. (Π.χ. η εφαρμογή X έχει πολύ περισσότερη κίνηση απ' ό,τι συνήθως και οι περισσότερες εντολές που λαμβάνει είναι λανθασμένες. Αυτό μπορεί να σημαίνει πως κάποιος δοκιμάζει να της στείλει διάφορες "τρελές" εντολές, ελπίζοντας πως θα την μπερδέψει ώστε να του δώσει πρόσβαση στο σύστημα.)

Ένα καλό IDS θα πρέπει να είναι αρκετά ευαίσθητο για να αναγνωρίζει όλες τις ύποπτες καταστάσεις, αλλά αρκετά έξυπνο ώστε να μην κρούει συχνά τον κώδωνα του κινδύνου χωρίς λόγο. Είναι αναπόφευκτο πως μερικές φορές το IDS θα κάνει λάθη σημαίνοντας συναγερμό για ασυνήθιστες, αλλά όχι επικίνδυνες, καταστάσεις. Αν όμως αυτό γίνεται συχνά, τότε οι χειριστές του θα συνηθίσουν να θεωρούν ως λανθασμένες όλες τις προειδοποιήσεις του και πιθανόν να μην το πιστέψουν ακόμη κι αν γίνεται πραγματικά επίθεση.

Το IDS θα πρέπει να ελέγχει συχνά τον εαυτό του για να εξασφαλίσει ότι λειτουργεί σε άριστη κατάσταση και ότι δεν έχει αποκτήσει πρόσβαση σε αυτό κάποιος τρίτος δίνοντάς του παραπλανητικά στοιχεία (συνήθως ένας άνθρωπος αναλαμβάνει να ελέγχει σε τακτά χρονικά διαστήματα το σύστημα, εξασφαλίζοντας έτσι ακόμη περισσότερο την αξιοπιστία του). Το IDS θα πρέπει επίσης να ελέγχει σε τακτά χρονικά διαστήματα τα δεδομένα που είναι αποθηκευμένα στο εσωτερικό δίκτυο (π.χ. συγκρίνοντάς τα με κάποια δικά του εφεδρικά αρχεία) για να εξασφαλίσει πως δεν έχουν τροποποιηθεί.

Τέλος, το IDS θα πρέπει να έχει καλή μνήμη και να μην ξεγελιέται από μεμονωμένες, φαινομενικά αθώες, ενέργειες (συχνά μια επίθεση κατανέμεται σε πολλές μικρές ήσσονος σημασίας και φαινομενικά άσχετες μεταξύ τους εργασίες οι οποίες περνούν απαρατήρητες, αλλά τελικά καταφέρνουν να παρακάμψουν τα συστήματα ασφαλείας και να επιτρέψουν την είσοδο του εισβολέα στο σύστημα).

**Ο παράγων άνθρωπος**

Τα Intrusion Detection Systems αποτελούν την προτελευταία γραμμή αμύνης ενός δικτύου απέναντι στους εσωτερικούς και εξωτερικούς εισβολείς. Υπάρχει ένα ακόμη επίπεδο ασφαλείας το οποίο, αν και δύσκολο στην εφαρμογή του, είναι απαραίτητο για την εξασφάλιση της μακροπρόθεσμης ασφάλειας κάθε δικτύου. Αναφερόμαστε φυσικά στο προσωπικό που χρησιμοποιεί το δίκτυο.

Πρέπει να γίνει κατανοητό σε όλους πως η ασφάλεια δικτύων αποτελεί μια συνεχώς μεταβαλλόμενη διαδικασία και όχι ένα οχυρό η κατασκευή του οποίοι αρκεί για να κρατήσει μακριά τους ανεπιθύμητους. Οι διαχειριστές των δικτύων κάθε επιχείρησης πρέπει να έχουν άριστη γνώση της δομής του δικτύου που επιβλέπουν και να παρακολουθούν στενά τις εξελίξεις στο χώρο της ασφάλειας δεδομένων για να εξασφαλίζουν πως οι άμυνές τους παραμένουν πάντοτε ισχυρές.

Κάθε μέρα που περνά γινόμαστε μάρτυρες της αποκάλυψης νέων τρωτών σημείων στα ήδη υπάρχοντα συστήματα ασφαλείας, καθώς και της εμφάνισης νέων ισχυρότερων προγραμμάτων αυτόματης "σάρωσης" ενός δικτύου για την ανακάλυψη και εκμετάλλευση ευάλωτων σημείων (τα αυτόματα προγράμματα αξιοποίησης αυτών των αδυναμιών ονομάζονται exploits).

Κάθε διαχειριστής δικτύου λοιπόν πρέπει να σκέφτεται και να ενεργεί ως cracker του δικού του δικτύου, δοκιμάζοντας κάθε νέο εργαλείο εύρεσης αδυναμιών όπως το SATAN (Security Administrator Tool for Analyzing Networks) και κλείνοντας ο ίδιος τις τρύπες που ανακαλύπτει, ή που ανακαλύπτουν άλλοι σε άλλα παρόμοια δίκτυα, πριν αυτές γίνουν αντιληπτές από τρίτους και χρησιμοποιηθούν εναντίον του.

Οι διαδικασίες ασφαλείας όμως δεν περιορίζονται μόνο στους διαχειριστές του εσωτερικού δικτύου. Πρέπει να γίνουν συνείδηση για όλους τους εργαζομένους, καθώς ακόμη και το υψηλότερο επίπεδο ασφαλείας είναι άχρηστο αν η γραμματέας κολλήσει το password της επάνω στην οθόνη για να το έχει πρόχειρο, αν ο πωλητής χάσει το notebook μέσα στο οποίο είναι γραμμένα τα στοιχεία πρόσβασης στο δίκτυο ή αν το υψηλόβαθμο στέλεχος επιλέξει ως συνθηματικό το 123456 "για να το θυμάται εύκολα" (πράγμα συχνά κατανοητό αφού πολλές φορές για λόγους ασφαλείας η μηχανογράφηση έχει την παράλογη απαίτηση από το προσωπικό να θυμάται 27 διαφορετικά passwords τα οποία φυσικά δεν επιτρέπεται να γράψει πουθενά).

Τέλος, πολλά αξιόλογα συστήματα ασφαλείας παραβιάζονται καθημερινά επειδή κάποιοι από τους χρήστες του εσωτερικού δικτύου συνδέονται μέσω dialup με το Internet, παρακάμπτοντας το εταιρικό Firewall για "να κάνουν πιο εύκολα τη δουλειά τους" (π.χ. να χρησιμοποιήσουν εκείνο το πρόγραμμα χρηματιστηρίου που δεν μπορεί να λειτουργήσει για όσους χρήστες συνδέονται μέσω Firewall).

Δυστυχώς, δεν υπάρχουν εύκολες απαντήσεις στον τομέα της ασφάλειας δικτύων. Με προσοχή και μεθοδικότητα μπορούμε να αυξήσουμε τη δυσκολία προσβολής, αλλά ο κίνδυνος παραβίασης κάθε εταιρικού δικτύου θα παραμείνει πάντοτε μια λιγότερο ή περισσότερο πιθανή εξέλιξη.

Η προοπτική αυτή όμως δεν πρέπει να μας αποθαρρύνει από τη χρήση του Internet και την επένδυση του εταιρικού μας μέλλοντος σε αυτό. Όπως μια αεροπορική τραγωδία δεν τρέπει τους περισσότερους από μας σε φυγή από το αεροδρόμιο, έτσι και τα προβλήματα ασφαλείας πρέπει να λειτουργούν προειδοποιητικά και όχι αποτρεπτικά για τη χρήση του Internet. Αφού λοιπόν πρέπει να συνεχίσουμε να πετάμε, ας διαβάσουμε τουλάχιστον το φυλλάδιο οδηγιών για την περίπτωση ατυχήματος και ας επιλέξουμε να ταξιδέψουμε με μια καλή εταιρεία και όχι με την Air Banania.

## 6.12 Ασφάλεια στο Διαδίκτυο: Τι πρέπει να προσέξουν οι μικρομεσαίες επιχειρήσεις.

Δεν υπάρχει τίποτα σημαντικότερο σήμερα από την ασφάλεια στο Internet, καθώς χάκερ, «ιοί» και πληθώρα άλλων απειλών, καραδοκούν. Διαβάστε εδώ πως μπορεί μια μικρομεσαία επιχείρηση να ενισχύσει την άμυνά της αποτελεσματικά με μερικά απλά βήματα.
Τίποτα δεν μπορεί να εξασφαλίσει απόλυτη προστασία από τις απειλές που υπάρχουν στο Internet. Ιοί, τα λεγόμενα «σκουλήκια» (worms), και άλλες παρόμοιες απειλές, κάνουν κάθε μέρα την αναζήτηση ασφάλειας μια όλο και πιο περίπλοκη υπόθεση. Στα παρακάτω σημεία αναλύεται τι πρέπει να κάνει μια μικρομεσαία επιχείρηση για να προστατευθεί καλύτερα από τις απειλές του Διαδικτύου:

**1. Μείνετε Ενημερωμένοι:** Παρακολουθήστε δικτυακούς τόπους με προγράμματα προστασίας και εγγραφείτε σε mailing list που ενημερώνουν μέσω ηλεκτρονικού ταχυδρομείου για τις νέες απειλές. Είναι βασικό να γνωρίζετε τις απειλές πριν διαδοθούν ευρέως. Έτσι μπορείτε να τις αντιμετωπίσετε καλύτερα.

**2. Διαλέξτε «δύσκολα» συνθήματα:** Τα προγράμματα των χάκερ στο Διαδίκτυο περιλαμβάνουν δεκάδες χιλιάδες πιθανών συνθημάτων. Με αυτά τα προγράμματα, όταν το σύνθημα είναι συνηθισμένο και απλό να βρεθεί οι χάκερ μπορούν να εισβάλουν στα συστήματα των υπολογιστών. Ένα ιδανικό σύνθημα μπορεί να είναι ο συνδυασμός συμβόλων και αριθμών όπως π.χ. το 45#B&90!

**3. Αλλάξτε συχνά το σύνθημά σας:** Ακόμα και να το βρουν οι χάκερ, εσείς ήδη θα χρησιμοποιείτε ένα καινούργιο.

**4. Βεβαιωθείτε ότι έχετε ενημερώσει το πρόγραμμα προστασίας που έχετε:** Πολλές εταιρείες λογισμικού προσφέρουν ανανεώσεις και συμπληρώματα στα προγράμματα ασφαλείας που παρέχουν, για να μπορούν αυτά να ανταποκρίνονται στις νέες απειλές. Οι μικρές επιχειρήσεις θα πρέπει να ελέγχουν τακτικά το πρόγραμμα ασφαλείας που διαθέτουν και να το ανανεώνουν για να μπορεί να αντιμετωπίζει τις απειλές που εμφανίζονται.

**5. Προστατέψτε τα συστήματα ηλεκτρονικού ταχυδρομείου που χρησιμοποιεί η επιχείρηση:** Διαλέξτε συστήματα e-mail που μπορούν να «μπλοκάρουν» ιούς που μπορεί να περιέχονται σε mail που λαμβάνει μια επιχείρηση. Οι υπάλληλοι της επιχείρησης θα πρέπει να εκπαιδευθούν για να μην ανοίγουν συνημμένα αρχεία (file attachments) από πηγές που δεν γνωρίζουν, και που είναι ο συνηθέστερος τρόπος για να εισέλθει ένας ιός στον υπολογιστή.

**6. Τεστάρετε το σύστημα για αδυναμίες:** Πραγματοποιήστε τακτικά τεστ για να βρείτε τυχόν αδυναμίες του συστήματος. Αυτά τα τεστ μπορούν να γίνουν τόσο μέσα από το δίκτυο της εταιρείας όσο και με εργαλεία που μπορούν να βρεθούν στο διαδίκτυο. Για παράδειγμα, μπορείτε με ένα πρόγραμμα που «σπάει» συνθήματα να δείτε αν πρέπει να αλλαχθούν τα συνθήματα πρόσβασης των χρηστών της εταιρείας.

**7. Εκπαιδεύστε τους υπαλλήλους σας:** Οι υπάλληλοι της εταιρείας πρέπει να κατανοήσουν πόσο σημαντικό είναι εταιρικά στοιχεία και πληροφορίες να παραμένουν εμπιστευτικά και κυρίως να μην κυκλοφορούν ευρέως στο Διαδίκτυο.

**8. Διατηρείστε τα προγράμματα σας και το λειτουργικό σύστημα ενημερωμένα:** Διατηρείστε το λειτουργικό σας σύστημα και τα προγράμματα σας ενημερωμένα και εγκαταστήστε τις τελευταίες ενημερώσεις. Έτσι και το σύστημα θα είναι πιο σταθερό και οι νέες συμπληρώσεις στα προγράμματα ασφαλείας θα λειτουργούν καλύτερα.

**9. Αντι-ιϊκά παντού:** Όλα τα συστήματα, από φορητούς υπολογιστές μέχρι τους εξυπηρετητές (servers) της επιχείρησης θα πρέπει προστατεύονται από ιούς. Αν έχετε εγκαταστήσει τέτοια προγράμματα βεβαιωθείτε ότι έχουν ρυθμιστεί κατάλληλα. Επίσης βεβαιωθείτε ότι οι υπάλληλοι της εταιρείας δεν έχουν το δικαίωμα να απενεργοποιήσουν αυτά τα συστήματα.

**10. Δημιουργείστε Εταιρική Πολιτική Ασφαλείας:** Καταγράψτε την πολιτική ασφαλείας της επιχείρησης σας και ανανεώστε την ανά τακτά χρονικά διαστήματα για να περιγράφει και να ανταποκρίνεται καλύτερα σε νέες απειλές που προκύπτουν. Φροντίστε όλοι οι υπάλληλοι να εφαρμόζουν τις αρχές αυτής της πολιτικής.

## 6.13 Αντίγραφα Ασφαλείας και Αρχειοθέτηση

Το πιο ακριβό και ζωτικό τμήμα ενός συστήματος υπολογιστών είναι οι πληροφορίες που διαθέτει. Χρησιμοποιούμε τους υπολογιστές γιατί μας δίνουν την δυνατότητα να αποθηκεύουμε και να επεξεργαζόμαστε πληροφορίες. Οι υπολογιστές είναι σημαντικοί μα όχι όσο οι πληροφορίες που διαθέτουν. Άσχετα με το πόσο καλά σχεδιάζουμε και συντηρούμε το δίκτυο μας, μπορεί να 'κρεμάσει' και να χάσουμε πληροφορίες. Στην πραγματικότητα, αυτό που συμβαίνει συνήθως είναι να σβήνονται, να τοποθετούνται σε λάθος σημείο ή να χάνονται με κάποιο τρόπο πληροφορίες λόγω σφάλματος και απροσεξίας του χρήστη.

Όποια κι αν είναι η αιτία της απώλειας των δεδομένων, είναι ζωτικής σημασίας η δυνατότητα να ανακτούμε όσο το δυνατόν ταχύτερα τα δεδομένα. Για να εξασφαλιστεί η

δυνατότητα να ανακτούμε δεδομένα, πρέπει να κάνουμε αντίγραφα των δεδομένων μας, τα οποία λέγονται αντίγραφα ασφαλείας(backup), σε δισκέτες ή άλλα μέσα κατά τακτά χρονικά διαστήματα. Συνεπώς, όταν θα χαθούν τα δεδομένα, θα μπορούμε να τα αντιγράψουμε από την συσκευή αντιγράφων ασφαλείας στο δίκτυο.

Καθώς χρησιμοποιούμε ένα σύστημα υπολογιστών, με το χρόνο όλο και περισσότερες πληροφορίες αποθηκεύονται σε αυτό. Μετά από λίγο, η ποσότητα πληροφοριών που βρίσκονται αποθηκευμένες στον υπολογιστή για εύκολη πρόσβαση μπορεί να γίνει μεγαλύτερη από ότι θα θέλαμε. Μπορεί να ο χώρος αποθήκευσης του υπολογιστή ή μπορεί ποσότητα των πληροφοριών να αυξηθεί τόσο που να μην επιτρέπει εύκολα την αναζήτηση και την επεξεργασία.

Σε αυτό το σημείο, μπορεί να θελήσουμε να μετακινήσουμε από τον υπολογιστή πληροφορίες παλιές ή που σπάνια χρησιμοποιούνται, αλλά να τις κρατήσουμε σε μορφή που μας επιτρέπει να τις φορτώσουμε εύκολα στον υπολογιστή σε περίπτωση που αυτό χρειαστεί. Αυτή η διαδικασία είναι γνωστή ως αρχειοθετημένη αποθήκευση ή αρχειοθέτηση (archiving).

Η δημιουργία αντιγράφων ασφαλείας και η αρχειοθέτηση είναι παρόμοιες διαδικασίες από την άποψη ότι ο στόχος και των δύο είναι να δημιουργήσουν ένα ιδιαίτερα αξιόπιστο αντίγραφο των πληροφοριών που υπάρχουν στο σύστημα υπολογιστών μας. Στη πράξη, η αρχειοθέτηση και η δημιουργία αντιγράφων ασφαλείας εκτελούνται συχνά χρησιμοποιώντας τον ίδιο εξοπλισμό, αν και αυτή δεν είναι πάντα η καλύτερη τακτική. Κανένα μέσω αποθήκευσης δεν είναι ιδανικό για δύο εργασίες.

**Μέσα Αποθήκευσης**

Το μέσο αποθήκευσης είναι αυτό καθ' εαυτό το υλικό ή μηχανισμός που διατηρεί τα αντίγραφα ασφαλείας ή τα αρχεία. Υπάρχουν πολλοί παράγοντες οι οποίοι πρέπει να σταθμιστούν κατά τον σχεδιασμό ενός δικτύου, αλλά υπάρχει μόνο ένας πρωταρχικός παράγοντας κατά την επιλογή του συστήματος δημιουργίας αντιγράφων ασφαλείας ή αρχειοθέτησης: η αξιοπιστία. Το μόνο πράγμα για το οποίο θέλουμε να είμαστε σίγουροι είναι ότι θα μπορούμε να ανακτήσουμε τα δεδομένα μας.

**Μαγνητική ταινία**

Η μαγνητική ταινία είναι ένας πολύ αξιόπιστος (τουλάχιστον , βραχυπρόθεσμα) και οικονομικός τρόπος για την αποθήκευση των δεδομένων. Για παράδειγμα, ένα σύστημα ταινίας 4mm DAT μπορεί να αποθηκεύσει, με κόστος περίπου 10 δολαρίων, 4 gigabytes(gigabyte=1000 megabytes) δεδομένων, ή λιγότερο από το 1% του αντιστοίχου μεγέθους του χώρου του σκληρού δίσκου. Ωστόσο, τα συστήματα ταινίας έχουν και μειονεκτήματα:

- Είναι αργά. Χρειάζονται ώρες για να αντιγραφούν 4gigabytes σε ταινία, ενώ θα χρειάζονταν μόνο μερικά λεπτά για να εγγραφούν τα ίδια δεδομένα στο σκληρό δίσκο.
- Οι ταινίες έχουν την τάση να καταστρέφονται μετά από μεγάλες χρονικές περιόδους (ας πούμε, πάνω από πέντε χρόνια).

- Εφόσον οι ταινίες αποθηκεύουν τα δεδομένα μαγνητικά, μπορεί να καταστραφούν από τυχαία έκθεση σε ισχυρά μαγνητικά πεδία.

  Οι μαγνητικές ταινίες διατίθενται σε αρκετές μορφές, συμπεριλαμβανομένων και των nine-track reel-to-reel (συνηθισμένες στους κεντρικούς υπολογιστές), DAT 4mm, DC1000,DC2000 και DC2120. Προσέξτε ότι αν και δύο μοντέλα οδηγών ταινιών χρησιμοποιούν το ίδιο είδος ταινίας, μια ταινία που γράφτηκε στο από αυτά μπορεί να μην διαβάζεται από το άλλο. Λόγω του συνδυασμού πλεονεκτημάτων και προβλημάτων των μαγνητικών ταινιών, είναι ιδανικές για τη δημιουργία αντιγράφων ασφαλείας.

**Μαγνητικό-Οπτικοί Δίσκοι(MO)**

Οι δίσκοι MO είναι δίσκοι που μπορούν να εισαχθούν και να μετακινηθούν σε έναν οδηγό όπως οι δισκέτες. Όπως και οι μαγνητικές ταινίες , τα συστήματα μαγνητικό-οπτικών (MO) δίσκων αποθηκεύουν τα δεδομένα ως μαγνητικές πληροφορίες. Αντίθετα με τις ταινίες, οι μαγνητικές πληροφορίες σε ένα συγκεκριμένο σημείο ενός δίσκου MO μπορούν να αλλάξουν μόνο αν θερμανθούν με έντονες ακτίνες λέιζερ. Αυτό καθιστά τους δίσκους MO ιδανικούς για μακροπρόθεσμη αποθήκευση. Αν ο δίσκος εκτεθεί τυχαία σε ιδιαίτερα ισχυρό μαγνητικό πεδίο, δε θα πάθει τίποτα, εκτός εάν επακολουθήσει και μεγάλη υπερθέρμανση, συνδυασμός που δεν είναι πιθανό να πραγματοποιηθεί.

Οι δίσκοι MO είναι, επίσης, ικανοποιητικά γρήγοροι, έχοντας σχεδόν την ίδια ταχύτητα με τους πιο αργούς σκληρούς δίσκους. Ωστόσο, οι δίσκοι MO έχουν δύο μειονεκτήματα:

- Αν και οι δίσκοι MO είναι λιγότερο ακριβοί από τους οδηγούς σκληρών δίσκων, παραμένουν αρκετές φορές πολύ πιο ακριβοί από την αποθήκευση σε μαγνητικές ταινίες.
- Υπάρχουν πολλά διαφορετικά είδη δίσκων MO και σχεδόν κανένα καθορισμένο πρότυπο. Πρέπει να βεβαιωθείτε ότι οποιοδήποτε είδος και να αγοράσετε θα υποστηρίζεται και στο μέλλον, εκτός αν ο οδηγός σας καταστραφεί και έτσι δεν έχετε τρόπο να διαβάσετε τους δίσκους σας!

Δεδομένου του συνδυασμού των πλεονεκτημάτων και των προβλημάτων των δίσκων MO, είναι ιδανικοί για αρχειοθέτηση.

**Ευκολίες Αποθήκευσης**

Προχωρώντας λίγο στο θέμα της αξιοπιστίας, πρέπει να προσέχουμε που αποθηκεύονται τα αντίγραφα ασφαλείας. Η αποθήκευση των αντιγράφων ασφαλείας κοντά στο σύστημα υπολογιστών (γνωστή ως αποθήκευση on site) είναι βολική, γιατί είναι εύκολο να αποθηκεύσετε τα αντίγραφα ασφαλείας και να τα ανακτήσετε όταν είναι απαραίτητο. Η αποθήκευση on-site εγκυμονεί, επίσης, ένα μικρό κίνδυνο καθώς αν μια μεγάλη καταστροφή, όπως φωτιά ή πλημμύρα, προκαλέσει ζημιά στον υπολογιστή μας, μπορεί να γίνουν άχρηστα και τα αντίγραφα ασφαλείας μας.

Για να αποφευχθεί η καταστροφή των αντιγράφων ασφαλείας από τις καταστροφές, μπορούμε να αποθηκεύσουμε τα αντίγραφα ασφαλείας μας μακριά από το σύστημα μας (off-site), σε ειδικά σχεδιασμένες και κατασκευασμένες συσκευές αποθήκευσης δεδομένων. Αυτές οι συσκευές είναι συνήθως απρόσβλητες από τις ζημίες που προκαλούνται από καταστροφές, πέρα από τις πιο σοβαρές (όπως, πόλεμος).

Στην πράξη, πολλοί οργανισμοί θα επιλέξουν τον συνδυασμό on-site και off-site αποθήκευσης για να πετύχουν τον συνδυασμό μεταξύ ευκολίας και ασφάλειας.

**Πλήρη και Προσθετικά Αντίγραφα Ασφαλείας**

Ας πούμε ότι μόλις εγκαταστήσαμε το σύστημα υπολογιστών μας εισάγουμε πληροφορίες στο πρόγραμμα λογιστικών. Στο τέλος της πρώτης μέρας, κάναμε αντίγραφο ασφαλείας όλων των πληροφοριών του υπολογιστή. Επειδή αντιγράφουμε όλες τις πληροφορίες του υπολογιστή, αυτή η διαδικασία είναι γνωστή ως δημιουργία πυλών (full) αντιγράφων ασφαλείας.

Στο τέλος της δεύτερης μέρας, θα θέλαμε να κάνουμε νέα αντίγραφα ασφαλείας. Μπορούμε να κάνουμε πλήρες αντίγραφο, όπως κάναμε και την προηγούμενη. Διαφορετικά, μπορούμε να κάνουμε αντίγραφό ασφαλείας μόνο των πληροφοριών που άλλαξαν από τότε που έγιναν τα τελευταία αντίγραφα ασφαλείας. Αυτά είναι γνωστά ως προσθετικά(incremental) αντίγραφα ασφαλείας. Το σύστημα υπολογιστών καταγράφει πότε τα αρχεία υπέστησαν μετατροπές και μπορεί να δοθεί εντολή στο λογισμικό αντιγράφων ασφαλείας να κάνει αντίγραφα μόνο των αρχείων που άλλαξαν μετά από συγκεκριμένη ώρα, και ημερομηνία, για παράδειγμα, από τη δημιουργία των τελευταίων αντιγράφων ασφαλείας.

Το πλεονέκτημα των προσθετικών αντιγράφων ασφαλείας είναι η ταχύτητα. Αν μόνο το 20% των πληροφοριών του δικτύου άλλαξε από τότε που έγινε το τελευταίο αντίγραφο ασφαλείας, το προσθετικό αντίγραφο ασφαλείας μπορεί να ολοκληρωθεί σε ποσοστό 20% του χρόνου που απαιτείται για να γίνει πλήρες αντίγραφα ασφαλείας. Όσα αρχεία δεν άλλαξαν από το τελευταίο αντίγραφο ασφαλείας. Το μειονέκτημα των προσθετικών αντιγράφων ασφαλείας είναι ότι δεν περιλαμβάνουν πλήρη καταγραφή του τι υπάρχει στον σκληρό δίσκο. Για να βρούμε κάποιο αρχείο που μας λείπει, μπορεί να χρειαστεί να ψάξουμε σε αντίγραφα ασφαλείας πολλών γενεών.

Στην πράξη, οι περισσότερες εφαρμογές χρησιμοποιούν ένα συνδυασμό πλήρων και προσθετικών αντιγράφων ασφαλείας. Τα ταχέα προσθετικά αντίγραφα ασφαλείας πραγματοποιούνται συχνά, ίσως και καθημερινά, ενώ τα πλήρη αντίγραφα ασφαλείας γίνονται λιγότερο τακτικά, ίσως μια φορά την εβδομάδα. Κάνοντας περιοδικά πλήρη αντίγραφα ασφαλείας, αν και θεωρητικά δεν είναι απαραίτητο, εξασφαλίζετε τη δυνατότητα να μη χρειάζεται να ψάχνετε ανάμεσα σε πολλά αντίγραφα ασφαλείας σε περίπτωση που κάποιο αρχείο πάθει ζημιά ή χαθεί.

# Κεφάλαιο 7

# Μέθοδοι Προστασίας

## Εισαγωγή

Η στρατηγική για να προστατευτεί ο Web server από ενδεχόμενες εισβολές είναι ο περιορισμός των υπηρεσιών που παρέχει ο υπολογιστής αυτός πέραν του Web σε όσο γίνεται λιγότερες.


Επίσης, καλή στρατηγική είναι και ο περιορισμός των χρηστών που έχουν λογαριασμό (account) σε αυτόν τον υπολογιστή, ενώ αυτοί που έχουν λογαριασμό και επικοινωνούν με τον υπολογιστή αυτό από μακριά πρέπει να χρησιμοποιούν κάποιο ασφαλές πρόγραμμα επικοινωνίας (π.χ. Kerberised Telnet, ssh). Για να προστατευτούν οι πληροφορίες κατά τη μεταφορά τους μέσω του World Wide Web ακολουθείται η στρατηγική της κρυπτογράφησης. Ένα τέτοιο σύστημα κρυπτογράφησης δεδομένων που στέλνονται μέσω του World Wide Web είναι το Secure Socket Layer (SSL) και θα πρέπει οι χρήστες να το χρησιμοποιούν κάθε φορά που στέλνουν ευαίσθητες πληροφορίες.

Απειλές στον World Wide Web προέρχονται και από προγράμματα που εκτελούνται άμεσα από τα προγράμματα ανάγνωσης των ιστοσελίδων (browsers), όπως προγράμματα Java, JavaScript, ActiveX κτλ ή από τη χρήση των λεγόμενων cookies. Αν και τέτοια προγράμματα δίνουν ζωή στις ιστοσελίδες του World Wide Web εντούτοις μπορούν να αποτελέσουν πολύ επικίνδυνα όπλα. στα χέρια πιθανών εισβολέων οι οποίοι θα εκμεταλλευτούν λάθη στην κατασκευή των browsers ώστε να μπορέσουν να προκαλέσουν ζημιά ή να αποκτήσουν μη εξουσιοδοτημένη πρόσβαση σε διάφορους υπολογιστές.

Προστασία από τέτοιες απειλές παρέχουν τα ίδια τα προγράμματα ανάγνωσης ιστοσελίδων (browsers) μέσα από επιλογές για απενεργοποίηση της δυνατότητας εκτέλεης τέτοιων δυναμικών προγραμμάτων ανάλογα με την προέλευσή τους.

## 7.1 Antivirus

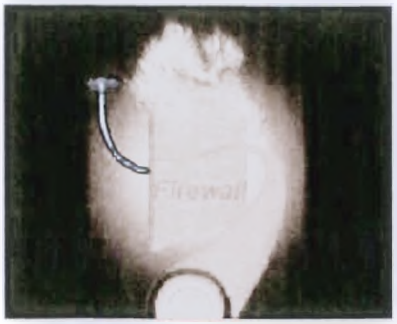
Τα προγράμματα antivirus ουσιαστικά αναλαμβάνουν να προστατεύσουν τους υπολογιστές του δικτύου, όπως υποδηλώνει και του ονόματος, από ιούς. Τον τελευταίο καιρό, ο ρυθμός διάδοσης των ιών έχει πλέον αυξηθεί δραματικά, ενώ δεν είναι πια απαραίτητο να προβεί ο χρήστης σε κάποια ενέργεια για να μολυνθεί ο υπολογιστής του.
Τα τελευταία χρόνια έχουν ύπαρξη περιπτώσεις στις οποίες ιοί κατάφεραν μέσα σε μερικά μόλις λεπτά να μολύνουν χιλιάδες συστήματα, γεγονός που στοιχίζει τόσο σε χρόνο όσο και σε χρήμα, καθώς η λειτουργικότητα του δικτύου μειώνεται ενώ υπάρχει πάντα η περίπτωση απώλειας σημαντικών δεδομένων. Η πολυπλοκότητα των επιθέσεων από ιούς αλλά και τα υπόλοιπα προγράμματα που ανήκουν σε αυτήν την γενικότερη κατηγορία, όπως worms, Trojan horses κ.λπ., είναι τέτοια, ώστε να μπορεί κάλλιστα να προσομοιωθεί με τις επιθέσεις hacker. Πως λειτουργεί όμως ένα antivirus;
Η λειτουργία ενός τέτοιου προγράμματος βασίζεται σε δύο τομείς. Στον πρώτο, το πρόγραμμα ελέγχει όλη την εισερχόμενη (και κάποια προγράμματα και την εξερχόμενη κίνηση) του δικτύου για γνωστούς ιούς, συγκρίνοντας τα δεδομένα που συλλέγει, με μια βάση η οποία περιλαμβάνει περιγραφές ιών (virus definitions) και θα πρέπει να ανανεώνεται συχνά. Δεύτερος εξίσου σημαντικός τομέας είναι η δυνατότητα του προγράμματος να ελέγξει και να αναγνωρίσει νέους ιούς. Τα προγράμματα ελέγχουν τα κομμάτια του κώδικα που φορτώνονται στη μνήμη, για πιθανές επικίνδυνες ενέργειες.
Ένα καλά ενημερωμένο πρόγραμμα antivirus διασφαλίζει τη μεγαλύτερη δυνατή διάρκεια λειτουργίας του δικτύου.

**Προγράμματα Antivirus**

- Norton Antivirus 2003
- McAfee virusScan 7.0
- Panda Antivirus Plati

## 7.2 Firewalls: Αδιαπέραστα τείχη

Ο όρος firewall έχει επικρατήσει τα τελευταία χρόνια σαν ένας από τους πιο καλούς τρόπους για να διατηρήσει κάποιος ασφαλή τα δεδομένα του στον υπολογιστή του, όταν αυτός είναι συνδεδεμένος στο Διαδίκτυο. Το firewall, ή αλλιώς ο τοίχος της φωτιάς, είναι ένα λογισμικό το οποίο αναλαμβάνει να ελέγχει όλες τις πληροφορίες που φθάνουν στον υπολογιστή μας από τον «έξω» κόσμο.



Το Firewall μπορεί να είναι εκτός από software και hardware, μία συσκευή δηλαδή που τοποθετείται στην σύνδεση του ηλεκτρονικού υπολογιστή με το διαδίκτυο. Στην περίπτωση που έχουμε εγκαταστήσει ένα λογισμικό firewall στον προσωπικό μας υπολογιστή τότε με αυτό μπορούμε να καθορίσουμε από ποιους υπολογιστές και με ποιους τρόπους θα δεχόμαστε πληροφορίες. Αυτό επιτυγχάνεται με την χρήση διάφορων φίλτρων τα οποία αναλύουν τα εισερχόμενα πακέτα και ανάλογα με τις οδηγίες που υπάρχουν τα αφήνουν να περάσουν ή όχι (Σχήμα 23).

Η μεγάλη σημασία του firewall έγκειται στο ότι δεν μπορούμε να γνωρίζουμε απόλυτα τι λογισμικά υπάρχουν εγκατεστημένα στον υπολογιστή μας και ποιες «πόρτες» είναι ανοιχτές. Για παράδειγμα, ο υπολογιστής μας μπορεί να είναι μολυσμένος από ένα worm το οποίο δίνει τη δυνατότητα σε κάποιον άλλο υπολογιστή να χρησιμοποιεί το CPU μας! Το firewall δηλαδή είναι αυτό που συγκεντρώνει τον πλήρη έλεγχο των πακέτων που εισέρχονται στον υπολογιστή αποτελώντας ουσιαστικά έναν πύργο ελέγχου της πληροφορίας. Βέβαια, η σημασία του firewall είναι πολύ πιο μεγάλη όταν πίσω από αυτό δεν υπάρχει μόνο ένας υπολογιστής αλλά μία μεγάλη ομάδα υπολογιστών π.χ. μία εταιρία, η οποία εμπιστεύεται το firewall για όλα τα πακέτα που καταφθάνουν σε αυτήν.

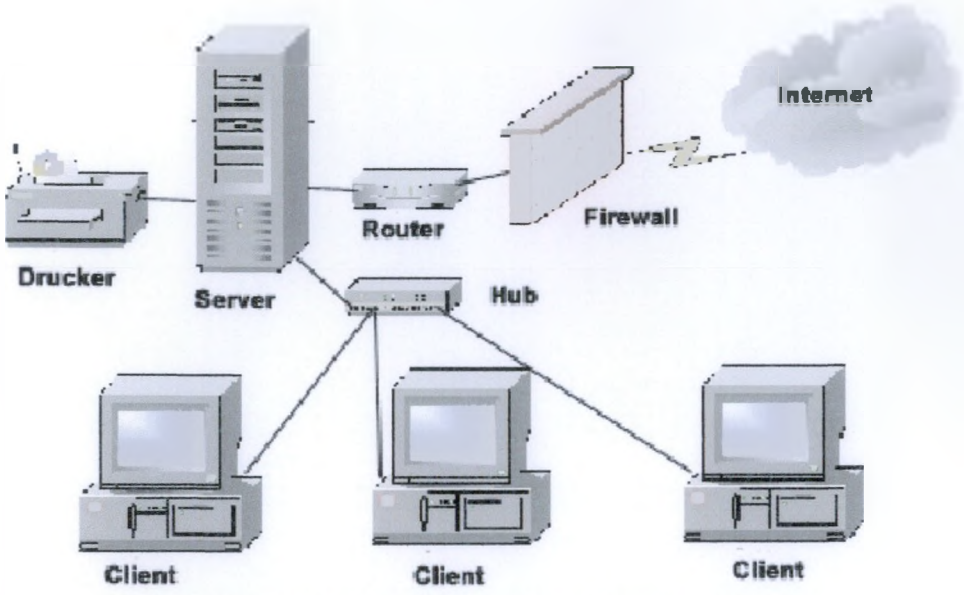

Όταν μία εταιρία συνδέει το εσωτερικό επιχειρηματικό της δίκτυο στο Internet αντιμετωπίζει ορισμένους σημαντικούς κινδύνους. Εξαιτίας της ανοικτής δομής του Internet, κάθε επιχειρησιακό δίκτυο που είναι συνδεδεμένο σ' αυτό είναι εκτεθειμένο σε

επιθέσεις. Οι hackers του Internet μπορούν θεωρητικά να εισέλθουν στο επιχειρησιακό δίκτυο και να προκαλέσουν ζημιά με διάφορους τρόπους: μπορούν να κλέψουν ή να καταστρέψουν σημαντικά δεδομένα, να προκαλέσουν ζημιά σε ανεξάρτητους υπολογιστές ή σε ολόκληρο το δίκτυο, να χρησιμοποιήσουν τους πόρους των επιχειρησιακών υπολογιστών ή να χρησιμοποιήσουν το επιχειρηματικό δίκτυο και τους πόρους του και να φαίνεται ότι το κάνει κάποιος υπάλληλος της επιχείρησης.

Η λύση δεν είναι η αποκοπή του δικτύου από το Internet. Αντιθέτως, η εταιρία μπορεί να δημιουργήσει firewalls για να προστατεύσει το δίκτυό της. Τα εν λόγω Firewalls αφ' ενός επιτρέπουν στους υπαλλήλους της επιχείρησης να έχουν πρόσβαση στο Internet και αφ' ετέρου εμποδίζουν τους επίδοξους hackers και crackers να αποκτήσουν πρόσβαση στο επιχειρηματικό δίκτυο και να προκαλέσουν ζημιές.

Τα firewalls αποτελούν συνδυασμούς hardware και software και δημιουργούνται χρησιμοποιώντας routers, servers και μία ποικιλία λογισμικού. Τα firewalls τοποθετούνται στο πιο ευπαθές σημείο μεταξύ του επιχειρησιακού δικτύου και του Internet και μπορεί να είναι από απλά ως εξαιρετικά πολύπλοκα συστήματα (Σχήμα 24).

Υπάρχουν πολλά είδη firewalls αλλά τα περισσότερα από αυτά διαθέτουν ορισμένα κοινά χαρακτηριστικά. Ένα από τα απλούστερα είδη των firewalls χρησιμοποιεί την τεχνική του φιλτραρίσματος των πακέτων. Στην περίπτωση αυτή ένας router εξετάζει την επικεφαλίδα κάθε πακέτου δεδομένων που ταξιδεύει μεταξύ του Internet και του επιχειρησιακού δικτύου. Οι επικεφαλίδες αυτές διαθέτουν διάφορες πληροφορίες όπως την IP διεύθυνση του αποστολέα και του παραλήπτη, το πρωτόκολλο που χρησιμοποιείται για την αποστολή και άλλες παρόμοιες πληροφορίες. Βασιζόμενός σε αυτές τις πληροφορίες ο router γνωρίζει το είδος της Internet υπηρεσίας που χρησιμοποιείται για την αποστολή των δεδομένων καθώς και την ταυτότητα του αποστολέα και του παραλήπτη των δεδομένων. Αφού διευκρινιστούν αυτές οι πληροφορίες, ο router μπορεί να εμποδίσει την αποστολή ορισμένων πακέτων μεταξύ του Internet και του επιχειρησιακού δικτύου. Για παράδειγμα ο router θα μπορούσε να μπλοκάρει όλη την κίνηση εκτός του ηλεκτρονικού ταχυδρομείου. Επιπροσθέτως θα μπορούσε να μπλοκάρει την κίνηση από και προς κάποιες ύποπτες τοποθεσίες ή από ορισμένους χρήστες.




**Σχήμα 24. Η χρήση του firewall σε ένα δίκτυο**

Οι proxy servers χρησιμοποιούνται αρκετά συχνά στα firewalls. Ένας proxy server είναι λογισμικό σε επίπεδο server το οποίο τρέχει σ' έναν host σ' ένα firewall και παίζει το ρόλο του οχυρού. Στην περίπτωση αυτή μόνο ο proxy server αλληλεπιδρά με το Internet (και όχι μεμονωμένα οι ανεξάρτητοι υπολογιστές του δικτύου) και ως εκ τούτου μπορούν να παρακολουθηθούν καλύτερα τα θέματα ασφάλειας. Είναι σαφώς ευκολότερο να κρατήσεις ασφαλή τον εν λόγω server παρά τους εκατοντάδες, σε ορισμένες περιπτώσεις, ανεξάρτητους υπολογιστές του δικτύου. Όταν κάποιος χρήστης του επιχειρησιακού δικτύου θέλει να έχει πρόσβαση σε κάποιον server στο Internet, στέλνει μία αίτηση από τον υπολογιστή του στον proxy server, εν συνεχεία ο Proxy server έρχεται σε επαφή με τον server του Internet και, τέλος, ο proxy server στέλνει τις πληροφορίες από τον Internet server στον υπολογιστή του επιχειρησιακού δικτύου ως εκ τούτου ο proxy server δρα σαν ενδιάμεσος προσφέροντας μεγαλύτερη ασφάλεια και καταγράφοντας όλη την κίνηση μεταξύ του Internet και του επιχειρηματικού δικτύου.

Η κλασική διάταξη που σήμερα θεωρείται από πολλούς ξεπερασμένη αποτελείται από δύο router και ανάμεσά τους έναν proxy server, ο οποίος αποκαλείται και «οχυρό» (bastion host). Οι router μπορούν και ελέγχουν τα πακέτα IP του δικτύου, φιλτράροντάς τα ανάλογα με τη διεύθυνσή τους ή το πρωτόκολλο στο οποίο ανήκουν.
Ο proxy server εκτελεί ελέγχους ανώτερου επιπέδου, όπως η πιστοποίηση των χρηστών, το φιλτράρισμα συγκεκριμένων εφαρμογών και η διατήρηση στατιστικών στοιχείων για το τι έγινε όλη την ημέρα. Σήμερα, συναντάμε firewall ενσωματωμένα σε μία μόνο συσκευή, είτε αυτή είναι εξειδικευμένη (Cisco PIX) είτε είναι ένας υπολογιστής που τρέχει ένα τέτοιο πρόγραμμα (CheckPoint Firewall-1).

Τα σύγχρονα firewall εκτελούν πολύπλοκους ελέγχους και είναι σε θέση να ανιχνεύσουν και να αποκρούσουν τις πιο σύνθετες και πολύπλοκες δικτυακές επιθέσεις, με ένα τίμημα όμως: το κόστος τους.

## 7.3 Κρυπτογράφηση δεδομένων

Κάθε πακέτο δεδομένων που στέλνεται μέσω του Internet διασχίζει πολλά δημόσια δίκτυα, γεγονός που σημαίνει ότι η πρόσβαση σε αυτά τα πακέτα δεν είναι ιδιωτική. Πρόκειται για ένα σημαντικό πρόβλημα όταν στο Internet χρειάζεται να ταξιδέψουν εμπιστευτικές πληροφορίες όπως επιχειρησιακά δεδομένα ή αριθμοί πιστωτικών καρτών. Αν δεν βρεθεί κάποιος τρόπος προστασίας αυτού του είδους των πληροφοριών, το Internet δεν θα αποτελέσει ποτέ ένα ασφαλές μέρος για την πραγματοποίηση εμπορικών πράξεων ή την αποστολή ιδιωτικής, προσωπικής αλληλογραφίας.

Ευτυχώς οι μηχανικοί λογισμικού έχουν αναπτύξει διάφορους τρόπους για την ασφαλή αποστολή εμπιστευτικών πληροφοριών. Συγκεκριμένα, χρειάζεται να γίνει απόκρυψη των πληροφοριών ώστε σε όλους τους άλλους πλην του παραλήπτη να φαίνονται σαν ένα ακατάληπτο μήνυμα. Εν συνεχεία πρέπει να γίνει από τον παραλήπτη - και μόνο από τον παραλήπτη - η αποκωδικοποίηση των πληροφοριών.

Πολλά σύνθετα κρυπτογραφικά συστήματα χρησιμοποιούν αυτό το είδος της απόκρυψης και της αποκωδικοποίησης. Για να καταλάβουμε πώς λειτουργούν τα κρυπτογραφικά συστήματα αρκεί να κατανοήσουμε το θέμα των κλειδιών. Τα κλειδιά είναι μυστικοί αριθμοί που χρησιμοποιούν οι υπολογιστές σε συνδυασμό με σύνθετους μαθηματικούς τύπους που ονομάζονται αλγόριθμοι για την κωδικοποίηση και αποκωδικοποίηση των μηνυμάτων. Η ιδέα που κρύβεται πίσω από τα κλειδιά είναι ότι αν κάποιος αποκρύπτει ένα μήνυμα με ένα κλειδί, μόνο κάποιος άλλος με το ίδιο κλειδί μπορεί να το διαβάσει.

Δύο είναι τα συνηθέστερα συστήματα απόκρυψης: η κρυπτογραφία με μυστικό κλειδί η οποία καλείται επίσης συμμετρική κρυπτογραφία και η κρυπτογραφία με δημόσιο κλειδί που καλείται και μη συμμετρική κρυπτογραφία. Το πιο συνηθισμένο σύστημα στην πρώτη κατηγορία είναι το Data Encryption Standard (DES), ενώ στη δεύτερη κατηγορία το RSA.

Στην κρυπτογραφία με μυστικό κλειδί, μόνο ένα κλειδί χρησιμοποιείται για την απόκρυψη και αποκωδικοποίηση των μηνυμάτων. Στην περίπτωση αυτή, ο αποστολέας και ο παραλήπτης χρειάζονται αντίγραφα του ίδιου μυστικού κλειδιού.

Αντιθέτως, στην περίπτωση της κρυπτογραφίας με δημόσιο κλειδί υπάρχουν δύο κλειδιά: ένα δημόσιο κλειδί και ένα ιδιωτικό. Κάθε άτομο έχει και τα δύο κλειδιά. Το δημόσιο κλειδί διατίθεται ελεύθερα, ενώ το ιδιωτικό κλειδί κρατείται μυστικό στον υπολογιστή του χρήστη. Το δημόσιο κλειδί μπορεί να κρυπτογραφήσει μηνύματα αλλά μόνο το ιδιωτικό κλειδί μπορεί να αποκρυπτογραφήσει μηνύματα που έχουν κρυπτογραφηθεί με το δημόσιο κλειδί. Αν κάποιος θέλει να μας στείλει ένα μήνυμα μπορεί να το κρυπτογραφήσει με τη βοήθεια του δημόσιου κλειδιού. Αλλά μόνο εμείς που έχουμε το ιδιωτικό κλειδί μπορούμε να αποκρυπτογραφήσουμε το μήνυμα και να το διαβάσουμε. Με το δημόσιο κλειδί δεν μπορεί να γίνει αποκρυπτογράφηση.

Σε εφαρμογές όπως το ηλεκτρονικό εμπόριο δεν είναι εφικτή η ευρεία χρήση στο Internet κρυπτογραφικών συστημάτων με ιδιωτικό κλειδί. Αν μία εταιρία αποφάσιζε να χρησιμοποιήσει ένα τέτοιο σύστημα για την πραγματοποίηση συναλλαγών μέσω του Internet θα έπρεπε να δημιουργήσει εκατομμύρια διαφορετικά ιδιωτικά κλειδιά - ένα για κάθε χρήστη που θα μετέχει στην συναλλαγή - και να βρει κάποιον ασφαλή τρόπο να τα στείλει στους αποδέκτες τους μέσω του Internet. Στο σύστημα με δημόσιο κλειδί η

εταιρία θα πρέπει να δημιουργήσει έναν μόνο συνδυασμό δημόσιου και ιδιωτικού κλειδιού. Η εταιρία στέλνει το δημόσιο κλειδί σε οποιονδήποτε θέλει να κωδικοποιήσει τις πληροφορίες αλλά μόνο όσοι κατέχουν το ιδιωτικό κλειδί μπορούν να αποκρυπτογραφήσουν τα δεδομένα.

## 7.4 Τα ψηφιακά πιστοποιητικά

Το Internet σ' ένα μεγάλο βαθμό στηρίζεται στην εμπιστοσύνη. Πρόκειται για έναν παγκόσμιο εικονικό κόσμο στον οποίο δεν βλέπουμε τους ανθρώπους ή τους φορείς με τους οποίους επικοινωνούμε παίρνοντας και δίνοντας πληροφορίες. Δεν βλέπουμε για παράδειγμα τον χρήστη στον οποίο στέλνουμε το e-mail μας αλλά εμπιστευόμαστε ότι είναι αυτός που ισχυρίζεται ότι είναι.

Στην περίπτωση όμως των οικονομικών συναλλαγών ή σημαντικών επικοινωνιών η εμπιστοσύνη δεν είναι αρκετή. Στο δίκτυο υπάρχουν hackers, crackers καθώς και άλλοι που εποφθαλμιούν τον αριθμό της πιστωτικής μας κάρτας ή που θα ήθελαν να μάθουν τα προσωπικά, επαγγελματικά ή οικονομικά μυστικά μας. Κατά τον ίδιο τρόπο οι επιχειρήσεις πρέπει να γνωρίζουν ότι το πρόσωπο που στέλνει έναν αριθμό πιστωτικής κάρτας είναι πράγματι αυτός που δηλώνει ότι είναι και όχι ένας απατεώνας που κατόρθωσε να κλέψει τον αριθμό της πιστωτικής κάρτας κάποιου άλλου.

Ο σημαντικότερος τρόπος αποφυγής του προαναφερθέντος προβλήματος είναι η χρήση των ψηφιακών πιστοποιητικών (digital certificates). Τα ψηφιακά πιστοποιητικά χρησιμοποιούνται για να πιστοποιήσουν ότι το άτομο που στέλνει πληροφορίες ή έναν αριθμό πιστωτικής κάρτας ή ένα μήνυμα ή οτιδήποτε άλλο στο Internet είναι πραγματικά αυτό που δηλώνει ότι είναι.


Τα πιστοποιητικά τοποθετούν τις πληροφορίες στον σκληρό δίσκο του χρήστη και χρησιμοποιούν τεχνολογία απόκρυψης για να δημιουργήσουν ένα μοναδικό ψηφιακό πιστοποιητικό για κάθε χρήστη. Όταν κάποιος που διαθέτει ένα ψηφιακό πιστοποιητικό επισκεφθεί κάποιο site ή στείλει e-mail το πιστοποιητικό αυτό παρουσιάζεται στο site ή επισυνάπτεται στο e-mail και πιστοποιεί ότι ο χρήστης είναι αυτός που ισχυρίζεται ότι είναι.

Τα ψηφιακά πιστοποιητικά είναι αρκετά ασφαλή επειδή χρησιμοποιούν πανίσχυρη τεχνολογία απόκρυψης. Στην πραγματικότητα είναι πιο ασφαλή ακόμη και από τις υπογραφές. Στην πραγματική ζωή μία υπογραφή μπορεί να πλαστογραφηθεί. Αντιθέτως, στο Internet δεν μπορεί να πλαστογραφηθεί το ψηφιακό πιστοποιητικό.

Τα ψηφιακά πιστοποιητικά εκδίδονται έναντι χρεώσεως από ιδιωτικές εταιρίες που ονομάζονται Digital Authorities. Μία τέτοια εταιρία είναι η πολύ γνωστή VeriSign. Τα

ψηφιακά πιστοποιητικά περιλαμβάνουν διάφορες πληροφορίες όπως το όνομα του χρήστη, το όνομα της εταιρίας που το εκδίδει, έναν σειριακό αριθμό και άλλες παρόμοιες πληροφορίες. Οι πληροφορίες έχουν κωδικοποιηθεί μ' έναν τρόπο που τις κάνει μοναδικές για τον κάθε χρήστη. Όπως στα περισσότερα πράγματα στο Internet έτσι και στην περίπτωση των ψηφιακών πιστοποιητικών υπάρχει ένα πρότυπο που επικρατεί και είναι γνωστό με την ονομασία X.509.

## 7.5 Τα δημοφιλέστερα πρωτόκολλα ασφαλείας

Έχουν αναπτυχθεί ή βρίσκονται υπό ανάπτυξη διάφορα πρωτόκολλα ασφαλείας που κάνουν χρήση των παραπάνω τεχνικών, όπως το SSL (Secure Sockets Layer), που αναπτύχθηκε από τη Netscape, και το SET (Secure Electronic Transactions), που αναπτύχθηκε από τη Visa και τη Mastercard και βρίσκεται στο στάδιο της πιλοτικής εφαρμογής. Να σημειώσουμε ότι πρωτόκολλο είναι ένα σύνολο από κανόνες και πρότυπα που δίνουν τη δυνατότητα στον υπολογιστή να ανταλλάσσει πληροφορίες.

### Secure Sockets Layer (SSL)

Από τα προαναφερθέντα πρωτόκολλα σήμερα χρησιμοποιείται το SSL. Το πρωτόκολλο αυτό αναπτύχθηκε από την Netscape Communications Corporation με σκοπό την ασφάλεια και την προστασία των ιδιωτικών δεδομένων. Η έκδοση SSL 3.0 αναπτύχθηκε το 1996, η οποία αργότερα χρησιμοποιήθηκε σαν βάση για την ανάπτυξη του Transport Layer Security (TLS), ένα IETF standard πρωτόκολλο. Όπως και το SSL, το TLS πρωτόκολλο λειτουργεί με παρόμοιο τρόπο: οι σχεδιαστές του το σχεδίασαν για επεκτασιμότητα, με υποστήριξη μπρος και πίσω συμβατότητας και διαπραγμάτευσης μεταξύ των peers.

Το SSL προστατεύει το κανάλι επικοινωνίας λειτουργώντας χαμηλότερα στο μοντέλο διαστρωμάτωσης δικτύου (μεταξύ του επιπέδου εφαρμογών και επιπέδου TCP/IP μετάδοσης). Είναι συνεπώς ανεξάρτητο εφαρμογής και επιτρέπει σε πρωτόκολλα όπως τα HTTP, Telnet, FTP να «κάθονται» διαφανώς πάνω του.

Είναι υπεύθυνο για την αυθεντικοποίηση και διατήρηση της ασφάλειας της επικοινωνίας, χρησιμοποιώντας τη μέθοδο της RSA κρυπτογράφησης. Σε γενική χρήση, μόνο ο server επικυρώνεται ενώ για τον client κάτι τέτοιο δεν είναι απαραίτητο. Η αμοιβαία αυθεντικοποίηση απαιτεί τη χρήση δημοσίου κλειδιού. Έτσι υπάρχει επικοινωνία μεταξύ servers και clients χωρίς υποκλοπές, ξένες παρεμβάσεις, και πλαστογραφία μηνυμάτων. Ένας server S επικυρώνεται σε έναν client C, στέλνοντας στο C το πιστοποιητικό του, το περιεχόμενο του οποίου επικυρώνεται μέσω της ψηφιακής υπογραφής της αρχής πιστοποίησης, της οποίας το δημόσιο κλειδί είναι γνωστό. Ένας client επικυρώνεται με τη βοήθεια ενός πιστοποιητικού X.509 που επιτρέπει στον server να ελέγξει την ψηφιακή υπογραφή του client.

Πολλές τοποθεσίες στο Internet είναι εξοπλισμένες με προγράμματα που χρησιμοποιούν το πρωτόκολλο αυτό, αποτρέποντας με αυτό τον τρόπο τα μη εξουσιοδοτημένα πρόσωπα από το να βλέπουν δεδομένα που στέλνονται από και προς αυτές τις τοποθεσίες. Οι τοποθεσίες αυτές αποκαλούνται «ασφαλείς». Τα κυριότερα προγράμματα ανάγνωσης σελίδων στο Web υποστηρίζουν το πρωτόκολλο SSL και την κρυπτογράφηση που

προσφέρει, ενώ ενημερώνουν το χρήστη ότι βρίσκεται σε ασφαλή τοποθεσία και μπορεί να στέλνει πληροφορίες χωρίς να διακινδυνεύει. Με το πρωτόκολλο αυτό οι επικοινωνίες πραγματοποιούνται σε κωδικοποιημένη μορφή και επιπλέον γίνεται και έλεγχος της αυθεντικότητας της τοποθεσίας.

Το μειονέκτημά του είναι η επιβράδυνση της επικοινωνίας λόγω του ότι είναι απαραίτητη η κρυπτογράφηση και αποκρυπτογράφηση του δημοσίου κλειδιού.

**Το πρωτόκολλο περιλαμβάνει ένα σύνολο βασικών φάσεων :**

- Διαπραγμάτευση μεταξύ των peers για την υποστήριξη του αλγορίθμου.
- Κρυπτογράφηση δημοσίου κλειδιού, βασισμένη στην ανταλλαγή και πιστοποίηση κλειδιών και πιστοποιητικού.
- Κρυπτογράφηση βασισμένη στον συμμετρικό αλγόριθμο.

**Το πρωτόκολλο SSL εξασφαλίζει:**

- Την κρυπτογράφηση των δεδομένων πριν την αποστολή.
- Την πιστοποίηση του Web Server όπου βρίσκεται το ηλεκτρονικό κατάστημα από τον browser του υπολογιστή του καταναλωτή.
- Τη συμμετρική κρυπτογράφηση, με γνωστό το κλειδί αποκρυπτογράφησης μόνο στις δύο εμπλεκόμενες πλευρές (πελάτης - έμπορος), γεγονός που εξασφαλίζει και την αναλλοίωτη μετάδοση των δεδομένων.

## Secure Electronic Transactions (SET)

Αναπτύχθηκε από τις Visa και MasterCard για να προσφέρει συναλλαγές με πιστωτική κάρτα πάνω στο Διαδίκτυο. Αυτό το πρωτόκολλο προσδιορίζει τη ροή επικοινωνίας ανάμεσα στους διάφορους συμμετέχοντες σε μία συναλλαγή. Η κρυπτογράφηση δημοσίου κλειδιού χρησιμοποιείται για να προστατεύει τον αριθμό πιστωτικής κάρτας.

Ο έμπορος ανοίγει λογαριασμό σε τράπεζα αποδέκτη (Acquiring Bank). Η τράπεζα αποδέκτης καθορίζει ποιες πιστωτικές κάρτες γίνονται δεκτές στις συναλλαγές. Ο πελάτης δίνει τα στοιχεία της πιστωτικής του κάρτας στον έμπορο πάνω από το Διαδίκτυο μέσω ασφαλούς σύνδεσης. Ο έμπορος μεταβιβάζει ασφαλώς τα στοιχεία που δέχτηκε στο διατραπεζικό σύστημα επεξεργασίας χρεώσεων και διαπιστώνει την πιστοληπτική ικανότητα του πελάτη χάρη στην αυτόματη επικοινωνία με την τράπεζα έκδοσης της πιστωτικής κάρτας του πελάτη (Issuing Bank). Η μεταφορά των χρημάτων στο λογαριασμό του εμπόρου γίνεται σε μεταγενέστερο στάδιο λόγω νομικών περιορισμών που διέπουν το χώρο του ηλεκτρονικού εμπορίου. Το SET είναι πρωτόκολλο βασισμένο σε ψηφιακές υπογραφές, οπότε λύνονται οι παρεξηγήσεις «αποποίησης παραγγελιάς».

Οι προδιαγραφές του πρωτοκόλλου απαιτούν την ύπαρξη λογισμικού στον υπολογιστή τόσο του πελάτη όσο και του εμπόρου. Επιπλέον, υπάρχει λογισμικό στην πλευρά του πωλητή για να αποκρυπτογραφεί πληροφορία οικονομικής φύσεως και στην πλευρά της Αρχής Πιστοποίησης για να εκδίδει τα ψηφιακά πιστοποιητικά. Δημόσιο και ιδιωτική

κρυπτογράφηση, αυθεντικοποίηση μηνύματος και πιστοποίηση κλειδιού είναι τα βασικά χαρακτηριστικά του SET πρότυπου. Συγκεκριμένα, τα προαπαιτούμενα για την υλοποίηση του πρωτοκόλλου SET είναι τα παρακάτω:

- Λογισμικό, ηλεκτρονικό πορτοφόλι (SET wallet) το οποίο είναι ενσωματωμένο στους σύγχρονους browsers.
- Πιστοποιητικό πωλητή, υπογεγραμμένο με το δημόσιο κλειδί της «τράπεζας αποδέκτη» και το δημόσιο κλειδί του εκδοτικού οργανισμού της κάρτας (π.χ. Visa ή MasterCard) διαδοχικά.
- Προαιρετικά πιστοποιητικό πελάτη από την «τράπεζα έκδοσης» της πιστωτικής κάρτας.

Υπάρχει πληθώρα απαιτήσεων τις οποίες οφείλει να ικανοποιήσει το SET: εμπιστευτικότητα, πληρωμών, διαλειτουργικότητα παροχέων λογισμικού και δικτυακής υποδομής, ακεραιότητα δεδομένων, αυθεντικοποίηση του κατόχου της κάρτας, διαπίστωση της ικανότητας του εμπόρου να δεχτεί ένα συγκεκριμένο είδος πληρωμής, διασφάλιση των βέλτιστων πρακτικών ασφαλείας για όλα τα εμπλεκόμενα μέρη και ανεξαρτησία από τους μηχανισμούς ασφαλείας σε επίπεδο μετάδοσης.

## Secure Hypertext Transfer Protocol (S-HTTP)

Το συγκεκριμένο πρωτόκολλο υποστηρίζει το ίδιο σύνολο υπηρεσιών ασφαλείας με το SSL. Όμως το S-HTTP διαφέρει από το SSL επειδή το SSL είναι ένα session-layer πρωτόκολλο, ενώ το S-HTTP είναι application-layer πρωτόκολλο που ενσωματώνεται στο HTTP.

Στοχεύει στην παροχή αυθεντικοποίησης και εμπιστευτικότητας σε Web συναλλαγές. Εφαρμόζεται σε browsers, Web servers και άλλες internet εφαρμογές.

Το σχήμα κρυπτογράφησης διαπραγματεύεται μεταξύ του client και του server, καθώς και μεταξύ των κλειδιών κρυπτογράφησης που χρησιμοποιούνται. Η εξουσιοδότηση του server εξασφαλίζεται πάντα ενώ η εξουσιοδότηση του client είναι προαιρετική στο S-HTTP. Τα κυριότερα χαρακτηριστικά του πρωτοκόλλου είναι:

- Το S-HTTP υποστηρίζει μία ποικιλία μηχανισμών ασφαλείας στους HTTP clients και servers. Το πρωτόκολλο παρέχει συμμετρικές δυνατότητες στον client και server που σημαίνει ότι τα μηνύματα και οι προτιμήσεις και των δύο πλευρών μεταχειρίζονται με τον ίδιο τρόπο, ενώ παράλληλα διατηρούνται το μοντέλο συναλλαγής και τα χαρακτηριστικά επικοινωνίας του HTTP.
- Αρκετά κρυπτογραφικά standards ενσωματώνονται στους S-HTTP clients και servers συμπεριλαμβανομένων των PEM, PGP, Kerberos και PKCS-7 (ο πρόγονος του CMS). Είναι συμβατό με το HTTP.
- Το S-HTTP δεν απαιτεί πιστοποιητικά δημοσίων κλείδων από την μεριά του client, καθ' ότι υποστηρίζει και τα συμμετρικά κλειδιά. Αυτό είναι σημαντικό γιατί αυθόρμητες ιδιωτικές συναλλαγές μπορούν να λάβουν χώρα, χωρίς την απαίτηση από τους χρήστες να έχουν ένα έγκυρο ζεύγος δημόσιας – ιδιωτικής κλείδας. Βέβαια,

είναι σε θέση να εκμεταλλευτεί την υπάρχουσα υποδομή πιστοποιητικών και ασύμμετρων κλειδιών.

- Το S-HTTP υποστηρίζει απ' άκρη σ' άκρη ασφαλής συναλλαγές, σε αντίθεση με το HTTP που προϋποθέτει μία αποτυχημένη προσπάθεια πρόσβασης του χρήστη πριν την εφαρμογή οποιωνδήποτε μηχανισμών ασφαλείας. Με το S-HTTP, σε καμία περίπτωση ευαίσθητα δεδομένα δε θα μεταδοθούν στο δίκτυο απροστάτευτα.
- Επιτρέπει πλήρη ευελιξία όσον αναφορά τους κρυπτογραφικούς αλγόριθμούς και τις παραμέτρους αυτών. Το είδος της παρεχόμενης προστασίας (κρυπτογράφηση, ψηφιακή υπογραφή, και τα δύο), οι αλγόριθμοι και τα πιστοποιητικά μπορούν να διαπραγματευτούν.
- Οι χρήστες αναμένονται να έχουν (αν και δεν συνιστάται) πολλαπλά πιστοποιητικά.

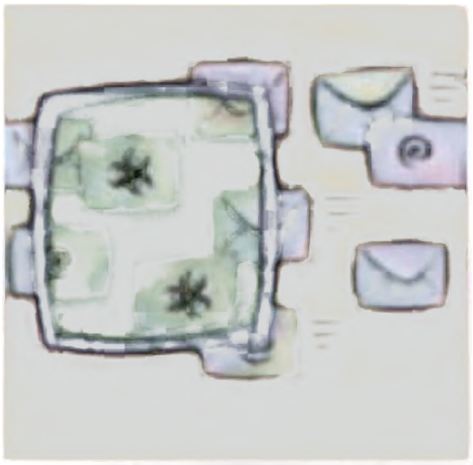
## Πρωτόκολλα ηλεκτρονικού ταχυδρομείου

Μια ποικιλία πρωτοκόλλων ασφαλείας έχουν προταθεί για το ηλεκτρονικό ταχυδρομείο στο Διαδίκτυο, αλλά μόνο ένα ή δύο έχουν γνωρίσει ευρεία αποδοχή.

Simple Mail Transfer Protocol (SMTP)

Το SMTP, το πρωτόκολλο επικοινωνίας για τα e-mails που μας εξυπηρετεί εδώ και δύο δεκαετίες, παραείναι «εύπιστο» και γεμάτο «τρύπες», δείχνοντας πλέον τα «χρόνια» του...

Το SMTP κατασκευάστηκε και χρησιμοποιήθηκε για χρήση σχεδόν από ακαδημαϊκούς χρήστες, πράγμα που σήμαινε ότι σχεδόν ήξεραν ποιος το χρησιμοποιούσε, καθώς αυτός ο κύκλος χρηστών ήταν γνωστός.



Η λειτουργία του ηλεκτρονικού ταχυδρομείου είναι απλή και στηρίζεται στο πρωτόκολλο SMTP. Μόλις τελειώσουμε το γράμμα που θέλουμε, το πρόγραμμα στέλνει το μήνυμα στο διακομιστή SMTP που του έχουμε δηλώσει (Outgoing SMTP Server). Το πρόγραμμα πακετάρει το μήνυμα ή το έγγραφό μας σε ένα «φάκελο». Στη συνέχεια δρομολογείται προς τον παραλήπτη, ακολουθώντας όλη τη διαδικασία μέσα από τη ραχοκοκαλιά, τις πύλες και τα πρωτόκολλα του Internet. Η λήψη ενός μηνύματος γίνεται

το ίδιο απλά. Το πρόγραμμα ελέγχει το διακομιστή SMTP που του έχουμε δηλώσει για να δει αν υπάρχουν νέα γράμματα και τα μεταφέρει στον τοπικό σκληρό δίσκο.

Αργότερα όμως, όταν το Internet έγινε το πλατύ μέσο επικοινωνίας που τώρα όλοι γνωρίζουμε, το SMTP δεν εκσυγχρονίστηκε ώστε να καλύψει τις σύγχρονες ανάγκες. Πριν 20 χρόνια που πρωτοεμφανίστηκε, δεν υπήρχε ο κίνδυνος να σου έρθει με mail κάποιος ιός, ένα μήνυμα από κάποιον Αφρικανό «αξιωματούχο» που ζητούσε βοήθεια ή απίθανες «προσφορές» για viagra και ναρκωτικά! Το πρωτόκολλο, «εύπιστο» από τη φύση του, δεν μπορεί να ξεχωρίσει τι είναι κακό και τι καλό απ' αυτά που μεταφέρει.

«Θα πρότεινα να γραφτεί ένα νέο πρωτόκολλο από την αρχή», προτείνει η Suzanne Sluize, συμπαραγωγός του SMTP και λέκτορας στο πανεπίστημιο του Νέου Μεξικού. «Από την πείρα μου στους υπολογιστές», συνεχίζει η Suzanne, «γνωρίζω ότι είναι πλέον δύσκολο κι ανώφελο να προσπαθείς να εκσυγχρονίσεις μια τέτοια απαρχαιωμένη τεχνολογία και πιο εύκολο να γράψεις κάτι καινούριο».

Η Suzanne Sluize ήταν συμπαραγωγός του SMTP το 1981, όταν εργαζόταν ως τεχνικό προσωπικό στο University of Southern California's Information Sciences Institute στη Marina del Rey της Καλιφόρνια, τόπο «γέννησης» κι άλλων γνωστών πρωτοκόλλων, όπως το TCP/IP.

**Privacy Enhanced Mail (PEM)**

Είναι ένα standard για την ασφάλεια ηλεκτρονικού ταχυδρομείου που χρησιμοποιεί συμμετρική ή ασύμμετρη κρυπτογραφία. Το PEM έχει φθίνουσα πορεία διότι αδυνατεί να διαχειριστεί το νεώτερο πολυμελές ηλεκτρονικό ταχυδρομείο (multipart e-mail) το οποίο υποστηρίζεται από το MIME (Multipurpose Internet Mail Extensions) ενώ απαιτεί αυστηρή ιεραρχία αρχών πιστοποίησης για να εκδώσει κλειδιά. Secure/ Multipurpose Internet Mail Extensions (S/MIME)

Το S/MIME είναι ένα πρωτόκολλο που προσθέτει ψηφιακές υπογραφές και κρυπτογράφηση στα Διαδικτυακά MIME μηνύματα. Το MIME είναι το επίσημο standard για εκτεταμένο Διαδικτυακό ηλεκτρονικό ταχυδρομείο. Καθορίζει τη δομή του κυρίου μέρους ενός ηλεκτρονικού μηνύματος. Το S/MIME βασίζεται στη χρήση ενός ψηφιακού φακέλου (digital envelope). Το μήνυμα κρυπτογραφείται με ένα συμμετρικό αλγόριθμο, όπως DES ή RC2. Το συμμετρικό κλειδί κρυπτογραφείται με το δημόσιο κλειδί του παραλήπτη οπότε μαζί με το κρυπτογραφημένο μήνυμα τοποθετούνται στο ψηφιακό φάκελο και στέλνονται στον παραλήπτη.

Το S/MIME έχει υιοθετηθεί από πλήθος ηγετικών παραγωγών στο δικτυακό και διαμηνυματικό χώρο, όπως οι ConnectSoft, Frontier, FTP Software, Microsoft, Lotus, SecureWare, Verisign, Netscape και Novell. Αποτελεί λοιπόν δοκιμασμένο υπόβαθρο για την ανάπτυξη συστήματος ηλεκτρονικού ταχυδρομείου στα πλαίσια εφαρμογών ηλεκτρονικού ταχυδρομείου

Pretty Good Privacy (PGP)

Μια δημοφιλής εφαρμογή που αναπτύχθηκε με σκοπό την ασφάλεια μηνυμάτων και αρχείων είναι το PGP. Είναι ίσως η ευρύτερα διαδεδομένη εφαρμογή ασφαλείας για ηλεκτρονικό ταχυδρομείο στο Διαδίκτυο. Το PGP είναι πακέτο λογισμικού που παρέχει ρουτίνες κρυπτογράφησης για e-mail και εφαρμογές αποθήκευσης αρχείων. Το PGP

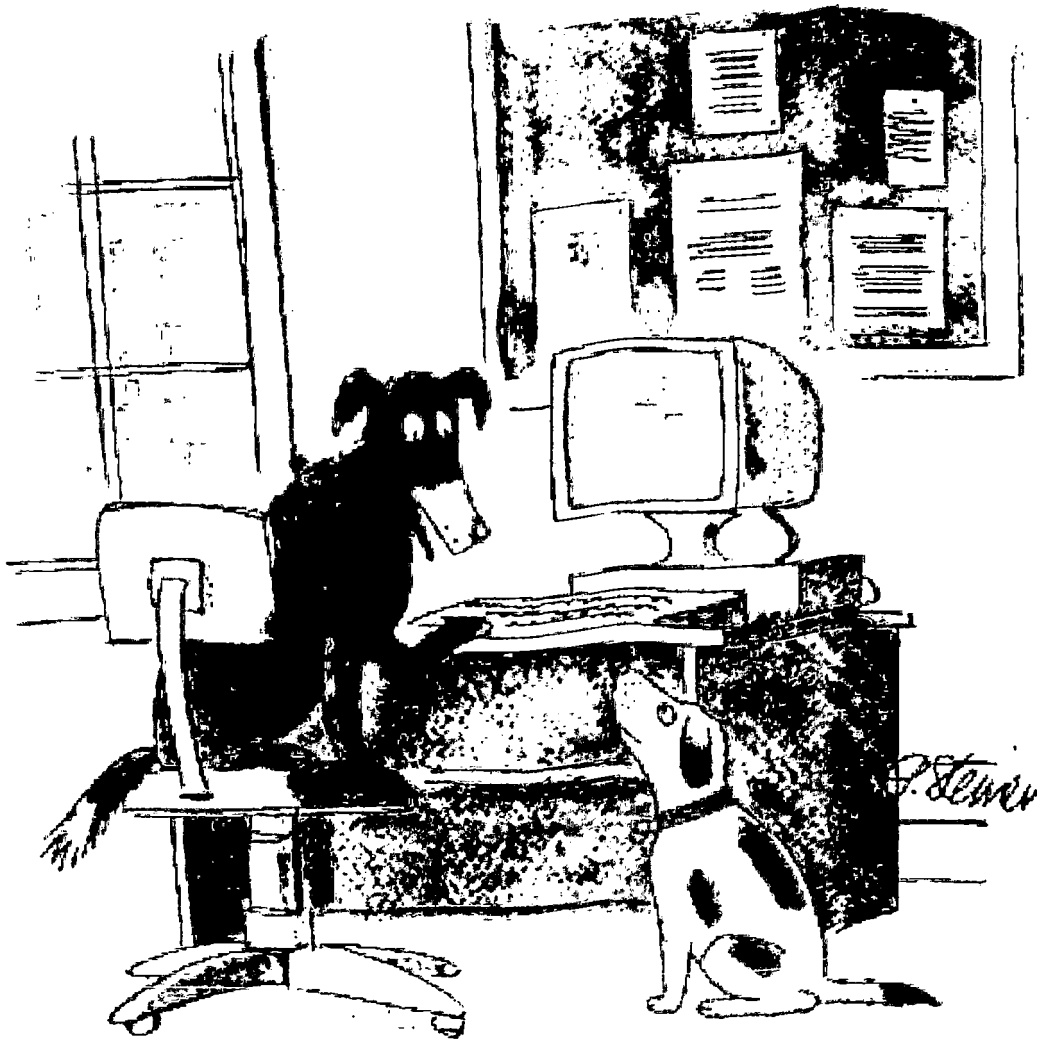
απαρτίζεται από υπάρχοντα κρυπτοσυστήματα και πρωτόκολλα κρυπτογράφησης. Τρέχει σε διάφορες πλατφόρμες. Προσφέρει κρυπτογράφηση μηνύματος, ψηφιακές υπογραφές, συμπίεση δεδομένων και e-mail συμβατότητα.

Η τελευταία έκδοσή του για χρήστες εκτός των ΗΠΑ παρέχει έναν εύκολο τρόπο κρυπτογράφησης, διαχείρισης κλειδιών μέσα από γραφικό περιβάλλον. Το PGP συνδυάζει και τους δύο τρόπους κρυπτογράφησης, μεταφέροντας με ασφαλή τρόπο το ιδιωτικό κλειδί μέσα από τεχνικές δημοσίου κλειδιού. Μετά την εγκατάσταση του προγράμματος και κατά τη διαδικασία δημιουργίας του δημοσίου κλειδιού ο χρήστης καλείται να δώσει το επιθυμητό μέγεθος του κλειδιού. Εδώ πρέπει να τονιστεί ότι χρησιμοποιείται συμμετρικός αλγόριθμος για να μεταδώσει με ασφαλή τρόπο το ιδιωτικό κλειδί, το οποίο χρησιμοποιείται τελικά για την κρυπτογράφηση του κυρίως μηνύματος. Το PGP προσφέρει τρεις συμμετρικούς αλγόριθμους, οι οποίοι είναι οι: CAST και IDEA με 128 bits μέγεθος κλειδιού, καθώς και ο Triple-DES με 168 bits μέγεθος κλειδιού. Εκτός από την κρυπτογράφηση, το PGP επιτρέπει στον χρήστη να υπογράψει ψηφιακά οποιοδήποτε κείμενο αποστέλλει, καθώς επίσης και να ελέγξει την πατρότητα του ψηφιακά υπογεγραμμένου κειμένου που έχει λάβει. Το PGP σχεδιάστηκε γύρω από την ιδέα ενός αξιόπιστου Web το οποίο θα επιτρέπει στους χρήστες να μοιράζονται τα κλειδιά τους χωρίς να απαιτείται η ιεραρχία των αρχών πιστοποίησης.

## 7.6 Το προσωπικό απόρρητο

Η διαφύλαξη του προσωπικού απορρήτου αποτελεί ένα ακανθώδες θέμα στο Internet. Ένας μεγάλος όγκος πληροφοριών μπορεί να συλλεχθεί σχετικά με τους χρήστες του Δικτύου και πολλές φορές δεν είναι ξεκάθαρο ποιος ή με ποιο τρόπο θα χρησιμοποιήσει αυτές τις πληροφορίες.

Συγκεκριμένα δύο είναι οι σημαντικότερες τεχνολογίες που σχετίζονται με το θέμα: τα cookies και το Web tracking. Και οι δύο εξυπηρετούν χρήσιμους σκοπούς αλλά πολλοί άνθρωποι ανησυχούν ότι ενέχουν τον κίνδυνο του «Μεγάλου Αδελφού». Μία ακόμη τεχνολογία, τα Internet passports, διασφαλίζει το προσωπικό απόρρητο του χρήστη, ενώ ταυτόχρονα επιτρέπει στα Web sites να συλλέγουν πληροφορίες που χρειάζονται για να προσφέρουν εξειδικευμένες υπηρεσίες στους επισκέπτες τους.



"On the Internet, nobody knows you're a dog."

- **Τα Cookies**

Τα cookies αποτελούν δεδομένα τα οποία τοποθετούνται στον σκληρό δίσκο κάποιου που επισκέπτεται ορισμένα Web sites. Η πιο κοινή χρήση των δεδομένων αυτών είναι να διευκολύνει την είσοδο των χρηστών σε Web sites που ζητούν όνομα χρήστη και password. Το cookie που βρίσκεται στον σκληρό δίσκο περιλαμβάνει το όνομα του χρήστη και το password, έτσι ώστε οι χρήστες δεν χρειάζεται να τα δηλώνουν σε κάθε σελίδα που χρειάζεται αυτή την πληροφορία. Αντιθέτως, το cookie στέλνει τις πληροφορίες στον server και ο χρήστης εισέρχεται στο site ελεύθερα.

Τα cookies μπορεί να περιλαμβάνουν σχεδόν κάθε είδος πληροφοριών, όπως την τελευταία φορά που ένας χρήστης επισκέφτηκε κάποιο site, τα αγαπημένα του sites και άλλες παρόμοιες πληροφορίες. Μπορούν επίσης να χρησιμοποιηθούν για την παρακολούθηση των χρηστών όσο βρίσκονται σε κάποιο site και τη συλλογή πληροφορίες σχετικών με τις σελίδες που προτιμούν να επισκέπτονται. Παρά το γεγονός ότι τα cookies θεωρούνται από ορισμένους ότι παραβιάζουν το προσωπικό απόρρητο, βοηθούν στην βελτίωση του Web διευκολύνοντας σημαντικά ορισμένες διαδικασίες. Τα cookies που έχει τοποθετήσει στον σκληρό δίσκο κάποιο site δεν μπορούν να διαβαστούν από άλλα sites. Οι χρήστες πάντως έχουν ανά πάσα στιγμή τη δυνατότητα να απαγορεύσουν την τοποθέτηση cookies στο σύστημά τους, απενεργοποιώντας την κατάλληλη επιλογή στον browser που διαθέτουν.

- **Το Web Tracking**

Εκτός από τα cookies υπάρχουν και άλλες μέθοδοι παρακολούθησης του τρόπου με τον οποίο οι χρήστες χρησιμοποιούν ένα Web site. Μία από αυτές προτείνει τη λεπτομερή εξέταση του ημερολογίου λειτουργίας του Web server. Η εξέταση αυτή επιτρέπει τον προσδιορισμό των δημοφιλέστερων σελίδων του site, των sites που μόλις επισκέφτηκαν οι χρήστες, του αριθμού των σελίδων που διαβάζουν σε μία τυπική επίσκεψη και άλλων σχετικών πληροφοριών.

Άλλες μέθοδοι στηρίζονται στην χρήση ορισμένων προγραμμάτων λογισμικού, ονόματι sniffers, τα οποία εξετάζουν κάθε πακέτο που εισέρχεται ή εξέρχεται από ένα Web site. Οι υπεύθυνοι των Web sites μπορούν να χρησιμοποιούν τις πληροφορίες που συλλέγονται για να βελτιώσουν τα sites τους ή για να συλλέξουν δημογραφικές πληροφορίες τις οποίες και να πουλήσουν σε διαφημιστές. Στην πραγματικότητα, οι υπεύθυνοι των sites θέλουν να γνωρίζουν αρκετά στοιχεία για τον τρόπο χρήσης των sites τους όπως τον συνολικό ημερήσιο αριθμό επισκεπτών, τον συνολικό αριθμό των σελίδων που έχουν ειδωθεί, τον τρόπο με τον οποίο οι χρήστες μετακινούνται στο site, από που προέρχονται οι χρήστες που επισκέπτονται το site και που πηγαίνουν όταν φεύγουν από αυτό.

- **Τα Internet Passports**

Για τη διαφύλαξη του ιδιωτικού απορρήτου έχουν αναπτυχθεί αρκετές τεχνολογίες και πρότυπα. Σ' αυτά περιλαμβάνονται τα Platform for Privacy Preferences (P3P), Internet Content and Exchange standard (ICE) και Open Profiling Standard (OPS). Οι τεχνολογίες αυτές ονομάζονται γενικά Internet passports.

Τα Internet passports επιτρέπουν στους χρήστες να ελέγχουν ποιες προσωπικές πληροφορίες θα γίνουν διαθέσιμες στα Web sites καθώς και τον τρόπο με τον οποίο αυτά θα τις χρησιμοποιήσουν. Επιτρέπουν επίσης στους χρήστες να ελέγχουν το είδος των πληροφοριών που θα συλλέξει το site κατά τη διάρκεια της πλοήγησής τους καθώς επίσης και το πως θα τις χρησιμοποιήσει.

# Κεφάλαιο 8

# Πολιτική ασφάλειας

## Εισαγωγή

Πολιτική ασφάλειας είναι ένα σύνολο κανόνων μέσα από τους οποίους πρέπει να διακρίνεται τι επιτρέπεται και τι δεν επιτρέπεται να γίνεται σε ένα σύστημα κατά την διάρκεια κανονικής λειτουργίας του. Πρέπει να είναι διατυπωμένη με γενικούς όρους και να περιγράφει τις απαιτήσεις ασφάλειας για το πληροφοριακό σύστημα.

Μέσα από αυτή ορίζεται το κανονιστικό πλαίσιο σύμφωνα με το οποίο προδιαγράφεται ο τρόπος πρόσβασης των οντοτήτων ενός συστήματος στα αντικείμενα του. Επίσης μέσα από αυτή πρέπει να περιγράφεται η μέθοδος προστασίας του συστήματος εκτιμώντας οικονομικά ισορροπημένες και υλοποιήσιμες λύσεις και να περιλαμβάνονται στο σχεδιασμό όλες οι οντότητες και τα αντικείμενα του συστήματος.

Η Ανάλυση Απειλών (Threat Analysis) παρέχει σημαντικές πληροφορίες για τον καθορισμό πολιτικής ασφάλειας και αποτελεί τη διαδικασία μέσω της οποίας αναγνωρίζονται όλες οι πιθανές απειλές στις οποίες είναι εκτεθειμένο ένα σύστημα.

Αποτέλεσμα της ανάλυσης αυτής είναι η δημιουργία μιας λίστας απειλών που υφίστανται και του βαθμού επικινδυνότητας που τις χαρακτηρίζει. Η λίστα αυτή μπορεί να αποτελέσει τη βάση για τον περαιτέρω καθορισμό πολιτικής.

## 8.1 Πολιτική ασφάλειας απομακρυσμένης πρόσβασης

Σε πολλές περιπτώσεις είναι απαραίτητη η απομακρυσμένη πρόσβαση κάποιου χρήστη στο εταιρικό δίκτυο. Μερικές φορές είναι αναγκαίο η δυνατότητα αυτή να δίνεται ακόμη και σε εξωτερικούς συνεργάτες, προμηθευτές ή και πελάτες. Οι απομακρυσμένες συνδέσεις επιτυγχάνονται με διάφορους τρόπους, όπως με dial-in modems, frame relay, DSL, VPN, κ.λπ

Οι κανόνες που ορίζουν το γενικό πλαίσιο χρήσης της απομακρυσμένης πρόσβασης συνοψίζονται στα παρακάτω:

- Οι χρήστες είναι υποχρεωμένοι να μην παρακάμπτουν τα δικαιώματα πρόσβασης που έχουν με τη σύνδεση αυτή.
- Δεν θα πρέπει να κάνουν χρήση της σύνδεσης αυτής για προσωπικούς λόγους, π.χ. Internet, παρά μόνο για σκοπούς που έχουν άμεση σχέση με την εργασία τους.
- Όταν μεταφέρουν αρχεία μέσω αυτής της σύνδεσης, οφείλουν να τηρούν την πολιτική ασφάλειας που ισχύει για τις διαβαθμισμένες πληροφορίες (κρυπτογράφηση, ταυτοποίηση). Επίσης θα πρέπει να τηρούν τις αντίστοιχες πολιτικές χρήσης Διαδικτύου και ηλεκτρονικού ταχυδρομείου.

- Είναι απαραίτητο να υπάρχουν οι κατάλληλοι μηχανισμοί που να ελέγχουν την απομακρυσμένη σύνδεση και να διαχειρίζονται από το Τμήμα Ασφάλειας της εταιρίας.
- Ό έλεγχος πρόσβασης θα πρέπει να γίνεται με προηγμένους μηχανισμούς ταυτοποίησης, π.χ. κωδικοί μιας χρήσης, PKI/δημόσια και ιδιωτικά κλειδιά.
- Οι υπολογιστές που είναι συνδεδεμένοι με το εταιρικό δίκτυο δεν θα είναι συνδεδεμένοι και με άλλο δίκτυο ταυτόχρονα.
- Ο εξοπλισμός που χρησιμοποιείται για τις απομακρυσμένες συνδέσεις θα πρέπει να εγκρίνεται από το Τμήμα Ασφάλειας και να προβλέπει μηχανισμούς ταυτοποίησης/αναγνώρισης.
- Όλοι οι υπολογιστές που χρησιμοποιούνται θα πρέπει να διαθέτουν ενημερωμένο λογισμικό καταπολέμησης ιών (anti-virus).

Οι πολιτικές ασφάλειας δικτύων που περιγράφονται παραπάνω αποτελούν πραγματική ανάγκη για τις σύγχρονες επιχειρήσεις που βασίζονται στην προστασία και ασφαλή ανταλλαγή ευαίσθητων πληροφοριών, τόσο των ίδιων των εταιριών όσο και των πελατών τους. Ωστόσο, όλο το ανθρώπινο δυναμικό των επιχειρήσεων οφείλει να είναι σωστά εκπαιδευμένο και πάντοτε ενημερωμένο για τους υφιστάμενους κινδύνους σε ένα δικτυωμένο περιβάλλον, προκειμένου να τηρούνται όλες οι πολιτικές ασφάλειας και να ελαχιστοποιείται το ρίσκο απώλειας ή διαρροής διαβαθμισμένου υλικού.

## 8.2 Πολιτική ασφάλειας Firewall

Το Firewall αποκαλείται το λογισμικό που ελέγχει ή και απαγορεύει την απομακρυσμένη πρόσβαση σε ένα υπολογιστή, ασκώντας παράλληλο έλεγχο στα εισερχόμενα / εξερχόμενα δεδομένα από και προς αυτόν. Το Firewall μπορεί να εγκατασταθεί ως μέρος μιας ολοκληρωμένης "σουίτας" προγραμμάτων ασφαλείας (Norton & McAfee Internet Security κλπ) ή ακόμη και ως ενσωματωμένο χαρακτηριστικό ενός λειτουργικού συστήματος (Linux).

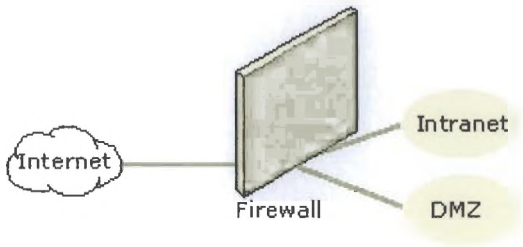
Οι λειτουργίες ελέγχου της εξερχόμενης κυκλοφορίας (traffic) θα πρέπει να είναι ένα από τα πιο σημαντικά κριτήρια επιλογής Internet firewall αφού είναι αυτές που ρυθμίζουν τις επιλογές αποδοχής ή απόρριψης (πρόσκαιρης ή μόνιμης) της αποστολής των packets που επιχειρεί να στείλει μια εφαρμογή.

Η πολιτική ασφάλειας δικτύου με τη χρήση firewall θα πρέπει γενικά να ακολουθεί τα εξής:

- Όλες οι συνδέσεις από το δίκτυο της εταιρίας προς το Internet θα πρέπει να γίνονται μέσω του Firewall (software ή hardware που αποτρέπει τις "επιθέσεις" σε κάποιο προσωπικό υπολογιστή ή σε ένα δίκτυο).
- Θα πρέπει να είναι ξεκάθαρο ποιοι είναι οι υπεύθυνοι για τα firewalls, οι οποίοι και τα διαχειρίζονται.
- Τα firewalls θα πρέπει να παρακολουθούνται και να ελέγχονται σε τακτά χρονικά διαστήματα (audits).
- Εισερχόμενες συνδέσεις από το Internet θα πρέπει να χρησιμοποιούν προηγμένους μηχανισμούς ταυτοποίησης/αναγνώρισης, π.χ. με κωδικούς μιας χρήσης. Το ίδιο ισχύει και για τους λογαριασμούς των διαχειριστών.
- Όλες οι υπηρεσίες/εφαρμογές που δεν χρειάζονται θα πρέπει να είναι απενεργοποιημένες.
- Όλα τα λειτουργικά θα πρέπει να είναι ενημερωμένα με τα τελευταία patches/hot fixes των κατασκευαστών τους, ακόμη και για τις υπηρεσίες που δεν είναι ενεργοποιημένες.
- Οι υπεύθυνοι των συστημάτων θα πρέπει να είναι εκπαιδευμένοι και ενημερωμένοι για αυτά.
- Το firewall θα πρέπει να είναι διαθέσιμο όλο το εικοσιτετράωρο.
- Όλες οι αλλαγές και οι αναβαθμίσεις θα πρέπει να καταγράφονται και να ακολουθούν την αντίστοιχη πολιτική.

Θα πρέπει να υπάρχει γρήγορη και αποτελεσματική ενημέρωση σε περίπτωση που κάποιο service δεν λειτουργεί.

## 8.3 Πολιτική ασφάλειας DMZ




Στην **DMZ** (Demilitarized Zone - "αποστρατιωτικοποιημένη ζώνη") αναλύονται οι επιχειρηματικές ανάγκες και η στρατηγική της επιχείρησης όσον αφορά στο Internet και τοποθετούνται συστήματα που παρέχουν υπηρεσίες προσβάσιμες από οποιονδήποτε μέσω του Διαδικτύου. Όλες λοιπόν οι μηχανές, συμπεριλαμβανομένων και των δρομολογητών, switches και υπολογιστών, καθώς και το ανάλογο λογισμικό θα πρέπει να ακολουθούν την πολιτική αυτή.

Συγκεκριμένα, θα πρέπει να λαμβάνονται υπόψη τα παρακάτω:

- Θα πρέπει κατ' αρχάς να είναι ξεκάθαρο ποιοι είναι οι υπεύθυνοι για τη διαχείριση των συστημάτων στην DMZ. Στη συνέχεια, όλος ο εξοπλισμός, οι εφαρμογές και οι κωδικοί πρόσβασης που τοποθετούνται σε αυτή τη ζώνη θα πρέπει να εγκρίνονται από το Τμήμα Ασφάλειας και να είναι καταγεγραμμένοι με λεπτομέρεια. Αλλαγές στον υπάρχοντα εξοπλισμό ή προσθήκη νέου θα πρέπει να γίνονται στο πλαίσιο της αντίστοιχης πολιτικής.
- Θα πρέπει να γίνεται λεπτομερής καταγραφή της κίνησης αλλά και αποτελεσματικός έλεγχος της καταγραφής με αυτοματοποιημένο τρόπο από τους υπεύθυνους του συστήματος. Ειδικότερα, πρέπει να καταγράφονται οι αποτυχημένες προσπάθειες πρόσβασης, παράκαμψης δικαιωμάτων καθώς και η μη τήρηση της πολιτικής πρόσβασης σε αυτά.
- Ποτέ δεν θα πρέπει να χρησιμοποιείται λογαριασμός συστήματος (admin-root) για κάτι το οποίο μπορεί να γίνει με απλό λογαριασμό που έχει λιγότερα δικαιώματα.
- Όλα τα συστήματα θα πρέπει να είναι ενημερωμένα με τα τελευταία patches/hot fixes (προγράμματα διόρθωσης κάποιου προβλήματος ασφαλείας) των κατασκευαστών τους, ακόμη και για τις υπηρεσίες που δεν είναι ενεργοποιημένες.
- Οι υπεύθυνοι των συστημάτων οφείλουν να είναι εκπαιδευμένοι και ενημερωμένοι για αυτά.
- Εφαρμογές και υπηρεσίες που δεν χρησιμοποιούνται θα πρέπει να απενεργοποιούνται, ενώ όσες δεν είναι διαθέσιμες σε όλους να προστατεύονται με έλεγχο πρόσβασης και ταυτοποίηση υψηλής ασφάλειας.
- Σε τακτά χρονικά διαστήματα θα πρέπει να γίνεται καταγραφή των συστημάτων από το Τμήμα Ασφάλειας της εταιρίας αλλά και από τρίτους για περισσότερη αντικειμενικότητα.

## 8.4 Πολιτικές Ασφάλειας Δικτύων

Το Internet έχει επιφέρει πραγματική επανάσταση στον τρόπο με τον οποίο λειτουργούν οι επιχειρήσεις, "πιέζοντάς" τες είτε να εδραιώσουν την παρουσία τους στον πολλά υποσχόμενο κόσμο του ηλεκτρονικού επιχειρείν, είτε να ρισκάρουν το μέλλον τους μένοντας ενδεχομένως και εκτός αγοράς. Δυστυχώς, η πίεση αυτή οδηγεί συχνά τις εταιρίες να μπαίνουν βιαστικά στο "παιχνίδι", προκειμένου να μη χάσουν το ανταγωνιστικό τους πλεονέκτημα, παραβλέποντας έτσι ή αναβάλλοντας την υλοποίηση πολιτικών και μηχανισμών για τη δημιουργία ενός ασφαλούς ηλεκτρονικού περιβάλλοντος. Αναμφισβήτητα οι απειλές είναι πλέον πάρα πολλές (ιοί, κακόβουλες επιθέσεις σε εταιρικές βάσεις δεδομένων, λογαριασμοί και στοιχεία πελατών που εκτίθενται σε κοινή χρήση, κ.λπ.) και αυξάνονται ραγδαία. Θα πρέπει λοιπόν η κάθε επιχείρηση που δραστηριοποιείται στο δικτυωμένο περιβάλλον να δίνει ιδιαίτερη βαρύτητα στην αξιοπιστία και την ασφάλεια των ηλεκτρονικών συναλλαγών.

# Κεφάλαιο 9

# Λειτουργικά Συστήματα

## Εισαγωγή

Είδαμε πως τα βασικά στοιχεία που ενώνονται για να δημιουργήσουν έναν Η/Υ είναι το υλικό (hardware) και το λογισμικό (software), και πως το κάθε ένα από αυτά τα στοιχεία είναι άχρηστο από μόνο του. Σε αυτό το Κεφάλαιο θα δούμε το λογισμικό, δηλαδή τα προγράμματα που δίνουν εντολές στα διάφορα μέρη του υλικού ώστε να λειτουργήσει ο υπολογιστής μας.

Ένα πρόγραμμα αποτελείται από εντολές και πληροφορίες (δεδομένα) που ελέγχουν τις λειτουργίες του υπολογιστή. Το λογισμικό διακρίνεται σε δυο μεγάλες κατηγορίες: στα λειτουργικά συστήματα και στις εφαρμογές.
Το λειτουργικό σύστημα (Operating System), είναι ένα σύνολο από προγράμματα τα οποία ελέγχουν και συντονίζουν τις λειτουργίες του υπολογιστή. Τα προγράμματα αυτά λειτουργούν ως σύνδεση μεταξύ του υλικού του υπολογιστή (π.χ. Επεξεργαστή, Μνήμη κτλ.) και των εφαρμογών.

Τα πρώτα λειτουργικά συστήματα εμφανίστηκαν κατά τη δεκαετία του '50 και είχαν ελάχιστες δυνατότητες. Από τότε η εξέλιξη στον τομέα της πληροφορικής είχε ως αποτέλεσμα την ανάπτυξη λειτουργικών συστημάτων που ήταν πολύ φιλικά ως προς τον χρήστη και με μεγάλες δυνατότητες. Το πιο διαδεδομένο λειτουργικό σύστημα σήμερα για προσωπικούς υπολογιστές είναι το **Microsoft Windows** το οποίο χρησιμοποιεί ένα περιβάλλον επικοινωνίας που βασίζεται σε γραφικά στοιχεία. Τα γραφικά αυτά είναι βασικά παράθυρα και εικονίδια που αντιπροσωπεύουν πληροφορίες και προγράμματα που βρίσκονται μέσα στον υπολογιστή.

Εκτός όμως από το λειτουργικό σύστημα των προσωπικών υπολογιστών υπάρχει και το λειτουργικό σύστημα των servers που μπορεί να είναι το ίδιο με αυτό των προσωπικών υπολογιστών μπορεί όμως και να διαφέρει. Εμείς μπορούμε να διακρίνουμε το λειτουργικό σύστημα σε δύο κατηγορίες σύμφωνα με τις εκδόσεις του

- Εκδόσεις windows
- Εκδόσεις Linux και Unix.

Το λειτουργικό σύστημα Linux είναι γνωστό και ως λειτουργικό σύστημα ανοικτού κώδικα.

## 9.1 Τι είναι το Linux;

Το Linux είναι ένας πυρήνας λειτουργικού συστήματος που μοιάζει με τον πυρήνα του AT&T UNIX. Είναι μία από το μηδέν υλοποίηση πυρήνα λειτουργικού συστήματος και δεν χρησιμοποιεί κώδικα του UNIX. Μπορεί να θεωρηθεί σαν UNIX κλώνος αφού διαθέτει τις περισσότερες εντολές του, ενώ η φιλοσοφία της σχεδίασης του πλησιάζει περισσότερο το UNIX από οποιοδήποτε άλλο λειτουργικό σύστημα. Το Linux αναπτύσσεται με βάση το POSIX πρότυπο, το οποίο είναι μία προσπάθεια τυποποίησης όλων των UNIX κλώνων.

Παρ' όλο που Linux είναι ο πυρήνας του λειτουργικού συστήματος, πολλές φορές αναφερόμαστε σε αυτό εννοώντας όλο το λειτουργικό σύστημα, που περιλαμβάνει και το περιβάλλον εργασίας, και το συνοδευτικό λογισμικό (κάτι το οποίο συνήθως οδηγεί σε παρανοήσεις).

Η ανάπτυξη του πυρήνα Linux ξεκίνησε κάπου στο 1990 από ένα φοιτητή (τότε) τον Linus Torvalds, ο οποίος με βοήθεια πολλών εθελοντών προγραμματιστών (από χόμπι ή επαγγελματίες) μέσω του Internet, κατάφερε να δημιουργήσει ένα πυρήνα που ανταγωνίζεται πυρήνες μεγάλων εταιριών.. Αρχικά είχε σαν πρότυπο το MINIX (ένα άλλο UNIX-like λειτουργικό), μα γρήγορα το ξεπέρασε. Η δημιουργία του Torvald ολοκληρώθηκε το 1994 με τον πυρήνα Linux 1.0 (Linux Kernel). Στη συνέχεια, αναπτύχθηκαν διάφορες εφαρμογές που πλαισίωσαν και πλαισιώνουν το δημιούργημα του Torvald. Σήμερα το Linux παρέχει όλα όσα θεωρούνται αναγκαία για ένα σύγχρονο πυρήνα λειτουργικού, όπως:

- υποστήριξη πολυεπεξεργαστικών συστημάτων (SMP)
- πραγματική πολυδιεργασία
- εικονική μνήμη
- διαμοιραζόμενες βιβλιοθήκες
- σωστή διαχείριση μνήμης
- δικτύωση μέσω TCP/IP κ.α.

Ο πυρήνας Linux αρχικά σχεδιάστηκε για επεξεργαστές της οικογένειας x86 (386/486/Pentium), αλλά σήμερα τρέχει σε πολύ μεγάλη ποικιλία επεξεργαστών, όπως οι Alpha (64 bit), οι Motorola 68000 (Amiga), PowerPC, MIPS κ.α.

Αν και η προσπάθεια δημιουργίας του Linux πυρήνα άρχισε το 1990, η δημιουργία ενός ελεύθερου λειτουργικού συστήματος χωρίς περιορισμούς στον τελικό χρήστη, είχε ξεκινήσει παλαιότερα από τον Richard Stallman ιδρυτή του Free Software Foundation και του GNU project. Έτσι το Linux είχε στο ξεκίνημά του ένα ολόκληρο σύστημα να βασιστεί. Το GNU σχέδιο είχε ήδη δημιουργήσει ένα C μεταγλωττιστή (τον gcc) και μια πλειάδα υψηλής ποιότητας προγραμματιστικών εργαλείων, ενώ είχε έτοιμα προγράμματα που αντικαθιστούσαν όλα τα βασικά προγράμματα σε ένα *NIX σύστημα. Το μόνο που έλειπε ήταν ένας σταθερός πυρήνας. Έτσι το GNU βρήκε ένα πυρήνα για να λειτουργήσει, και το Linux βρήκε έτοιμη μια μεγάλη ποικιλία προγραμμάτων. (Το GNU

σχέδιο συνεχίζει σήμερα και με το υπό κατασκευή λειτουργικό σύστημα, Hurd, το οποίο βασίζεται στον μικροπυρήνα Mach)

Το Linux είναι το πιο επιτυχημένο από τα ελεύθερα λειτουργικά συστήματα, ενώ ανταγωνίζεται και τα υπόλοιπα. Στην καθιέρωση του βοήθησαν πολύ εταιρίες και εθελοντές που κατασκεύασαν και οργάνωσαν διανομές, δηλαδή συγκέντρωσαν συλλογές προγραμμάτων που συνόδευαν τον πυρήνα. Σήμερα υπάρχουν πολλές διαφορετικές διανομές που καλύπτουν διαφορετικές ανάγκες. Μερικές χαρακτηριστικές είναι:

- Slackware Linux (http://www.slackware.com): το αγαπημένο αυτών που ξεκίνησαν με το Linux στις αρχές της δεκαετίας του '90. Είναι η διανομή που έκανε το Linux αγαπητό στους διαχειριστές συστημάτων.
- το Redhat Linux (http://www.redhat.com): μία από τις πρώτες εταιρίες που αντιμετώπισαν σοβαρά το Linux. Σήμερα κατέχει ένα μεγάλο ποσοστό της αγοράς.
- το Debian GNU/Linux (http://www.debian.org): Οργανωμένο από μια ομάδα εθελοντών, και είναι η διανομή με τα περισσότερα πακέτα σήμερα. Είναι η μοναδική διανομή που αποτελείται μόνο από ελεύθερα πακέτα.
- SuSe Linux (http://www.suse.com): Έγινε ιδιαίτερα δημοφιλής λόγω της φιλικότητας της και των πολλών πακέτων που διαθέτει.
- Caldera Linux (http://www.caldera.com): Διανομή που έγινε γνωστή λόγω του γραφικού της περιβάλλοντος.
- Corel Linux (http://linux.corel.com): Βασισμένο στο Debian αλλά με ωραίο, εντυπωσιακό γραφικό περιβάλλον.
- Mandrake Linux (http://www.linux-mandrake.com): Βασισμένο στο RedHat, αλλά με ιδιαίτερα προσεγμένο γραφικό περιβάλλον.

Στην πλειονότητα αυτών των διανομών περιλαμβάνονται και προγράμματα που δεν ανήκουν στην κατηγορία του **ελεύθερου λογισμικού**.

Κάποιος μπορεί εύλογα να αναρωτηθεί, πώς μπορεί ένα λειτουργικό σύστημα που διατίθεται δωρεάν να είναι καλό και αξιόπιστο; Σε αυτό το ερώτημα λίγοι μπορούν να απαντήσουν, όπως επίσης και στο ερώτημα για το πώς απόκτησε τόσο μεγάλη βάση χρηστών τόσο γρήγορα. Είναι απίστευτο για πολλούς το πώς μπορεί μια ομάδα από "hackers" να κυριαρχήσει σε ένα τομέα που μέχρι σήμερα κυριαρχούσαν κολοσσοί της πληροφορικής. Το Linux μπορεί να χαρακτηριστεί σαν ένα φαινόμενο του Internet, είναι ένα πείραμα που πέτυχε.

## Έχει γραφικό περιβάλλον το Linux;

Το Linux όπως προαναφέραμε είναι πυρήνας, και πάνω σε αυτόν μπορεί να εκτελεστεί οποιοδήποτε περιβάλλον εργασίας. Το διαδεδομένο παραθυρικό σύστημα όμως είναι το X Window System και πιο συγκεκριμένα η υλοποίηση από την Xfree86 ομάδα. Το X Window System (ή πιο απλά τα X), είναι ένα γραφικό σύστημα που συντηρείται και αναπτύσσεται σήμερα από το OpenGroup και πέρα από της συνήθεις λειτουργίες ενός παραθυρικού συστήματος, είναι κατασκευασμένο για δικτυακή λειτουργία. Δηλαδή

μπορεί πολύ απλά μια παραθυρικέ εφαρμογή να εκτελείται στον Α υπολογιστή, και η έξοδος (τα παράθυρα) να εμφανίζονται στον δικό μας υπολογιστή.

Πέρα όμως από αυτές τις χαμηλού επιπέδου λειτουργίες του X διακομιστή, δεν διαθέτει τίποτα παραπάνω. Αυτό το κενό καλύπτουν τα λεγόμενα Desktop Environments (περιβάλλοντα εργασίας), τα οποία μπορεί να περιέχουν Taskbars, εικονίδια στο Desktop, backgrounds, screensavers, Panels, καθώς και ένα αριθμό προγραμμάτων που διευκολύνουν την διαχείριση του Desktop ή και του συστήματος. Τα πιο υψηλού επιπέδου περιβάλλοντα εργασίας για Linux είναι τα KDE και GNOME, τα οποία έχουν ήδη φτάσει (αν όχι ξεπεράσει) τα αντίστοιχα περιβάλλοντα εργασίας σε άλλα *NIX workstations.

## Σε ποιους απευθύνεται το Linux;

Θεωρητικά απευθύνεται σε όλους, ακόμα και προς τον άπειρο χρήστη, που δεν διαθέτει ιδιαίτερες γνώσεις για τους υπολογιστές. Στην πράξη, όμως, απευθύνεται κυρίως σε διαχειριστές συστημάτων, προγραμματιστές και επιχειρήσεις με ανάγκες δικτύωσης. Το Linux μπορεί να αξιοποιηθεί από μια μικρομεσαία επιχείρηση για την επιτέλεση πληθώρας λειτουργιών και μπορεί να αντικαταστήσει με το παραπάνω οποιοδήποτε άλλο λειτουργικό σύστημα. Μπορεί να εξυπηρετήσει την **τοπική δικτύωση**, να λειτουργήσει ως **mail server**, ως application server, ως **ftp server**, ως **web server**, ως **DNS** server, ως σταθμός εργασίας κ.ά. Είναι αξιοσημείωτο ότι υπολογίσιμο ποσοστό επιχειρήσεων σε ολόκληρο τον κόσμο χρησιμοποιεί Linux για να εξυπηρετήσει τις εργασίες του. Ανάμεσά τους και η Oracle, ο μεγαλύτερος προμηθευτής επιχειρηματικού λογισμικού, η SAP, η HP, η Dell κ.ά. Παράλληλα, το ίδιο έχουν πράξει δημόσιοι και κυβερνητικοί οργανισμοί, καθώς και φορείς τοπικής αυτοδιοίκησης, σε Γερμανία, Κίνα, Βραζιλία και αλλού. Όλα αυτά δείχνουν ότι το μέλλον (κάποιο κομμάτι του τουλάχιστον) ανήκει στο Linux.

Το Linux εξαπλώθηκε χωρίς διαφήμιση, εμπορικά τεχνάσματα, και μονοπώλια. Αυτό που το κάνει να διαφέρει από τα υπόλοιπα ΛΣ, είναι ευκολία με την οποία μπορεί να επεκταθεί για να καλύψει και τις πιο απαιτητικές ανάγκες. Ακόμα και αν δεν έχει κάποιος γνώσεις προγραμματισμού, μπορεί να προτείνει βελτιώσεις στους αρχικούς προγραμματιστές ή ακόμα να χρηματοδοτήσει κάποιον για να υλοποιήσει αυτές τις βελτιώσεις (πολλά ελεύθερα προγράμματα χρηματοδοτούνται, και αναπτύσσονται με αυτόν τον τρόπο).

## Πλεονεκτήματα

Κάνοντας μία κωδικοποίηση των πλεονεκτημάτων, τα σημαντικότερα από αυτά είναι:

- Η λογική της ανάπτυξής του είναι τέτοια ώστε επιτρέπει τον ποιοτικό του έλεγχο από πολλούς ανθρώπους. Μάλιστα, αρκετοί από αυτούς ενδέχεται να είναι ικανότατοι προγραμματιστές και πολύ εξειδικευμένοι.

- Υπάρχει τεράστια δυνατότητα προσαρμογής του λογισμικού στις ανάγκες (ιδιωτών ή εταιριών).

- Μπορεί να αποτελέσει σημαντικό εκπαιδευτικό εργαλείο ή εργαλείο για απόκτηση προγραμματιστικής εμπειρίας από αυτούς που αναπτύσσουν κώδικα.

- Το κόστος (χρήση + απόκτηση) του ελεύθερου λογισμικού ή του λογισμικού ανοικτού κώδικα είναι συνήθως σημαντικά μικρότερο από το κόστος αντίστοιχων εμπορικών λύσεων.

- Όταν πρόκειται για δημοφιλή προγράμματα, τα οποία χρησιμοποιούνται σε πληθώρα εγκαταστάσεων ανά τον κόσμο, η υποστήριξη σε περίπτωση εμφάνισης προβλημάτων μπορεί να προέλθει άμεσα, με τη χρήση των καναλιών επικοινωνίας του Internet (λ.χ. newsgroups).

- Η χρήση ελεύθερου λογισμικού ή λογισμικού ανοικτού κώδικα δε δημιουργεί εξαρτήσεις από κάποια συγκεκριμένη εταιρία.

Επειδή ο κώδικας είναι διαθέσιμος, μπορεί να ελεγχθεί η αξιοπιστία του, κάτι που δεν μπορεί να γίνει σε εμπορικά προγράμματα, όπου ο κώδικας δεν είναι διαθέσιμος.

## Μειονεκτήματα

Το βασικό μειονέκτημα του Linux είναι ότι δεν υπάρχουν πολλοί προγραμματιστές, τεχνικοί και γενικά στελέχη πληροφορικής που να γνωρίζουν το αντικείμενο σε όλες του τις διαστάσεις. Αυτό συσχετίζεται ασφαλώς με το χαμηλό μερίδιο αγοράς που κατέχει το Linux στην Ελλάδα, καθώς και με τον πολύ μικρό αριθμό εταιριών που ασχολούνται με θέματα εγκατάστασης και υποστήριξης Linux και άλλων εφαρμογών **ελεύθερου λογισμικού**. Ο συνδυασμός των παραπάνω δημιουργεί αμηχανία στα εταιρικά στελέχη που είναι αρμόδια για τη λήψη τέτοιου είδους αποφάσεων, και συχνά η υιοθέτηση του Linux απορρίπτεται "λόγω αμφιβολιών" ή επιφυλάξεων. Περαιτέρω, οι πολλές και διαφορετικές διαθέσιμες διανομές, τα πολλά και διαφορετικά περιβάλλοντα εργασίας και εφαρμογές, μπορεί να προκαλέσουν σύγχυση τόσο στον άπειρο όσο και στο μέσο χρήση. Σε κάθε περίπτωση, η εισαγωγή του Linux στη λειτουργία μιας επιχείρησης απαιτεί σωστό προγραμματισμό και ειδικευμένο προσωπικό με κατάλληλες γνώσεις, προκειμένου να μπορέσει να προσφέρει λύσεις σε οποιαδήποτε προβλήματα παρουσιαστούν κατά τη διάρκεια της υλοποίησης.

## Γιατί να προτιμώ linux

Εκτός του ότι είναι πολύ οικονομικότερο από όλα τα άλλα λειτουργικά συστήματα (στην ουσία δωρεάν), παρουσιάζει πληθώρα πλεονεκτημάτων. Είναι ιδιαίτερα αξιόπιστο στη λειτουργία του, δεν "κολλάει" σχεδόν ποτέ, είναι απόλυτα σταθερό, μπορεί να χρησιμοποιηθεί με μεγάλη επιτυχία σε υπολογιστές κάθε είδους (από έναν υπολογιστή παλάμης μέχρι έναν υπερυπολογιστή), και είναι γρηγορότερο από κάθε άλλο λειτουργικό σύστημα. Ακόμη, είναι συμβατό με εφαρμογές των Windows και του Unix, θεωρείται δυσπρόσβλητο στους ιούς και συντηρείται εύκολα. Επιπρόσθετα, οι διανομές του Linux είναι πληρέστατες και οι εφαρμογές που περιέχονται μπορούν να καλύψουν το σύνολο των αναγκών μιας επιχείρησης, όσο μεγάλη κι αν είναι. Ο ενδιαφερόμενος δηλ. δεν

χρειάζεται να αγοράσει άλλα πακέτα λογισμικού, καθώς είναι καλυμμένος από τις εφαρμογές της διανομής. Τέλος, το Linux αξιοποιεί την εργασία χιλιάδων προγραμματιστών σε ολόκληρο τον κόσμο, που δουλεύουν εθελοντικά για τη βελτίωση του συστήματος και τη διόρθωση των πιθανών σφαλμάτων (bugs).

## Συμφέρουσες λύσεις

Σε ένα λογισμικό, το κόστος είναι συνάρτηση πολλών παραγόντων, οι οποίοι διαμορφώνουν το συνολικό κόστος χρήσης. Οι παράγοντες αυτοί είναι το κόστος αγοράς, το κόστος συντήρησης, υποστήριξης και διαχείρισης, το κόστος αναβάθμισης κ.ο.κ. Στη διαμόρφωση του συνολικού κόστος χρήσης, σε βάθος χρόνου, το κόστος αγοράς και αναβάθμισης είναι συνήθως ένα μικρό κομμάτι, τουλάχιστον στην πλειοψηφία των περιπτώσεων.

Έτσι, ανεξάρτητα από το εάν χρησιμοποιείται εμπορικό λογισμικό ή όχι, το συνολικό κόστος χρήσης του λογισμικού είναι περίπου το ίδιο. Κατά συνέπεια, τα κριτήρια για να επιλέξουμε και να αποφασίσουμε εάν το ελεύθερο λογισμικό και το λογισμικό ανοικτού κώδικα είναι συμφέρον για τον επιχείρηση, δεν είναι τόσο οικονομικά.

Για παράδειγμα, εάν μία εταιρία θέλει την ανεξαρτησία της από συγκεκριμένους κατασκευαστές, το ελεύθερο λογισμικό και το λογισμικό ανοικτού κώδικα είναι μία καλή λύση. Εάν θέλει να έχει έλεγχο στον πηγαίο κώδικα των προγραμμάτων που χρησιμοποιεί, τέτοιου τύπου λογισμικό είναι επίσης καλές λύσεις.

Εάν χρειάζεται αρκετές τροποποιήσεις στον κώδικα, το ελεύθερο λογισμικό την εξυπηρετεί. Βλέπουμε, λοιπόν, ότι τα κριτήρια για να αποφασίσουμε τι είναι πιο συμφέρον για την επιχείρησή μας, δεν είναι απαραίτητα οικονομικά, ή τουλάχιστον δεν ξεκινούν έτσι.

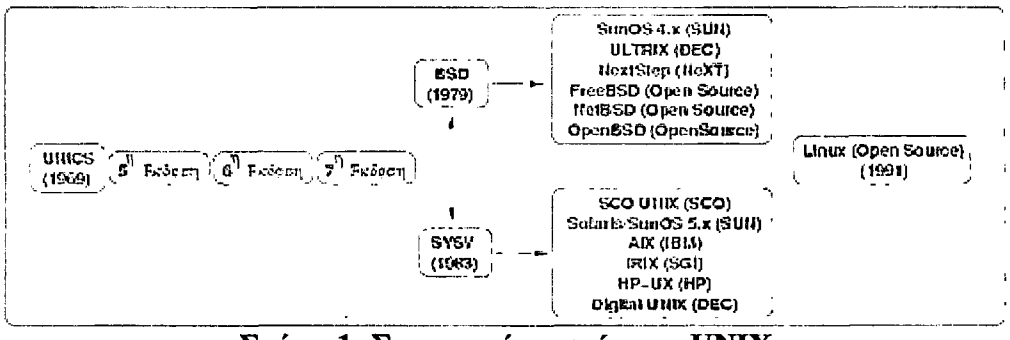
Όπως είναι λογικό, όταν αυξάνεται η χρήση σε κάτι και δημιουργείται η κρίσιμη μάζα, εμφανίζονται και αυτοί που αναλαμβάνουν την υποστήριξη των συστημάτων. Έτσι, υπάρχουν αρκετές εταιρίες αλλά και μεμονωμένα άτομα που αναλαμβάνουν την υποστήριξη συστημάτων που βασίζονται σε ελεύθερο λογισμικό και λογισμικού ανοικτού κώδικα.

Οι διαχειριστές των συστημάτων, οι προγραμματιστές και γενικότερα οι τεχνικοί αυξάνουν τις γνώσεις τους γύρω από αυτά τα συστήματα, όπως ακριβώς συμβαίνει και με τα συστήματα που βασίζονται σε εμπορικό λογισμικό.

Κατά συνέπεια, σε πρακτικό επίπεδο, μία επιχείρηση που θα επιλέξει να χρησιμοποιήσει ελεύθερο λογισμικό ή λογισμικό ανοικτού κώδικα, μπορεί να βρει ανθρώπους με την κατάλληλη τεχνογνωσία που θα την υποστηρίξουν.

## 9.2 Unix

Ένα από τα πιο παλιά Λ.Σ που δημιουργήθηκαν είναι το Λ.Σ UNIX. Οι αρχές τις ιστορίας του φτάνουν στο έτος 1969. Αναπτύχθηκε κυρίως μέσα σε ακαδημαϊκούς και ερευνητικούς χώρους πανεπιστημίων και εταιριών. Η ανάγκη που οδήγησε στην δημιουργία ενός Λ.Σ από μέρους τους, ήταν ότι χρειάζονταν ένα τρόπο να μπορούν να μπορούν πολλοί διαφορετικοί άνθρωποι να χρησιμοποιούν ένα υπολογιστή (μην ξεχνάτε ότι στην αρχή της ιστορίας των υπολογιστών, ένας και μόνο υπολογιστής κόστιζε αρκετά εκατομμύρια δολάρια και ήταν πραγματικά ογκώδης), να μπορεί κάποιος να κάνει πολλά διαφορετικά πράγματα την ίδια στιγμή, να μην σταματάει η λειτουργία του για κάποιο λόγο και να δίνει την δυνατότητα σε πολλούς διαφορετικούς ανθρώπους να ανταλλάσσουν μεταξύ τους δεδομένα. Όλα αυτά που με την συνήθη ορολογία των υπολογιστών ονομάζονται multi-user, multi-tasking environment, stability, network και connectivity τα έδωσε το Λ.Σ. UNIX.




**Σχήμα 1: Συνοπτική ιστορία του UNIX**

### Τι είναι το Unix

Το λειτουργικό σύστημα UNIX αναπτύχθηκε από την AT&T (Bell Laboratories) στα τέλη της δεκαετίας του 60. Εξαπλώθηκε σε ολόκληρο τον κόσμο και εγκαταστάθηκε σε μια ποικιλία συστημάτων από μεγάλα υπολογιστικά συστήματα έως μικρούς προσωπικούς υπολογιστές. Η ευρεία διάδοση του οφείλεται στο ότι επειδή είναι γραμμένο σε μια γλώσσα ανωτέρου επιπέδου (γλώσσα C) είναι εύκολα προσαρμόσιμο σε διαφορετικά συστήματα, και στο ότι είναι ένα πολύ αξιόπιστο λειτουργικό σύστημα.
Κυκλοφορούν διάφορες εκδόσεις του UNIX. Οι δύο βασικότερες είναι η έκδοση System V που προέκυψε από την αρχική έκδοση της AT&T και η έκδοση BSD που αναπτύχθηκε από το Πανεπιστήμιο του Berkeley στην Καλιφόρνια. Υπάρχουν μια σειρά από παραλλαγές που βασίζονται στις δύο παραπάνω εκδόσεις, π.χ. οι εκδόσεις SunOS και Solaris της Sun, το SCO UNIX και το LINUX που είναι εκδόσεις του UNIX για PC και πολλές άλλες.
Τα δύο βασικά χαρακτηριστικά του UNIX είναι ότι είναι: α) **πολύ-επεξεργαστικό** (multi-tasking), δηλ. επιτρέπει την ταυτόχρονη εκτέλεση πολλών διεργασιών χωρίς η εκτέλεση μιας διεργασίας να εμποδίζει την εκτέλεση των άλλων και β) επιτρέπει την ταυτόχρονη σύνδεση στο σύστημα σε **περισσότερους από έναν χρήστες** (multi-user), οι οποίοι μπορούν να χρησιμοποιούν ακόμη και τα ίδια ακριβώς προγράμματα, χωρίς οι ενέργειες του ενός χρήστη να επηρεάζουν τις ενέργειες των άλλων.

Για να ξεχωρίζει ο ένας χρήστης του συστήματος από τον άλλον, σε κάθε χρήστη αντιστοιχίζεται ένας **λογαριασμός (account)** που αποτελείται από ένα **όνομα χρήστη (user name ή login name)** που είναι διαφορετικό για κάθε χρήστη και γνωστό σε όλους και ένα μυστικό **συνθηματικό (password)** γνωστό μόνον στον ίδιο το χρήστη το οποίο εξασφαλίζει ότι ο λογαριασμός του συγκεκριμένου χρήστη δεν χρησιμοποιείται από άλλα πρόσωπα. Για να αποκτήσει πρόσβαση στο σύστημα, ο χρήστης πρέπει να δώσει το σωστό συνδυασμό ονόματος χρήστη και συνθηματικού. Τέλος, κάθε χρήστης ανήκει σε ένα ή και περισσότερα **group**. Ένα group είναι μια **ομάδα χρηστών** στην οποία εκχωρούνται κάποια συγκεκριμένα δικαιώματα σχετικά με τη χρήση του συστήματος από το διαχειριστή συστήματος.

## Το σύστημα αρχείων του UNIX

Τα μέσα αποθήκευσης μιας μηχανής UNIX (σκληρός δίσκος, cd-rom, κλπ.) είναι οργανωμένα με τη λογική μορφή ενός ανεστραμμένου "δέντρου". Κάθε κλαδί του δέντρου είναι ένας **κατάλογος** (directory) που περιέχει **αρχεία** (files) και άλλους καταλόγους (subdirectories). Ο κατάλογος που βρίσκεται στην κορυφή του δέντρου ονομάζεται **κατάλογος ρίζα (root directory)**.

Η δομή αυτή μοιάζει αρκετά με την αντίστοιχη του MS-DOS. Μια διαφορά που υπάρχει είναι ότι ο χαρακτήρας που διαχωρίζει τα ονόματα καταλόγων και αρχείων σε μια διαδρομή (path) είναι ο "/" και όχι ο "\", π.χ.: /usr/bin, κοκ. Το / συμβολίζει τον κατάλογο ρίζα: sxima1

Όταν ένας χρήστης αποκτά λογαριασμό σε ένα σύστημα UNIX, ο διαχειριστής συστήματος δημιουργεί έναν κατάλογο για τον χρήστη ο οποίος λέγεται **προσωπικός κατάλογος (home directory)** και πρόσβαση σε αυτόν έχει μόνον ο συγκεκριμένος χρήστης και κανένας άλλος. Στην περιοχή αυτή του δίσκου, ο χρήστης μπορεί να αποθηκεύει τα αρχεία του, να δημιουργεί υποκαταλόγους για να τα οργανώνει καλύτερα, κλπ. Όταν ο χρήστης συνδέεται με το σύστημα δίνοντας όνομα χρήστη και συνθηματικό, "μπαίνει" στον προσωπικό του κατάλογο.

Τα **ονόματα αρχείων και καταλόγων** στο UNIX ακολουθούν τους εξής **κανόνες**:

**1)** Ένα όνομα έχει μήκος μέχρι 14 χαρακτήρες, οι οποίοι μπορεί να είναι: i) τα γράμματα του λατινικού αλφάβητου a-z, A-Z, ii) οι αριθμοί 0-9, iii) οι ειδικοί χαρακτήρες: ".", "_", ",", "-", "+". Ένα όνομα δεν μπορεί να ξεκινά με "-" ή "+"

**2)** Το UNIX **διαχωρίζει μικρά από κεφαλαία γράμματα** στα ονόματα: αν τα ίδια γράμματα αλλάξουν από πεζά σε κεφαλαία ή αντίστροφα, τότε έχουμε και διαφορετικό όνομα. Π.χ. τα REPORT.TEXT, Report.text και report.text είναι τρία διαφορετικά ονόματα αρχείων.

## Δομή και Αρχιτεκτονική του Λ.Σ UNIX

**Ένα τυπικό Λ.Σ απαρτίζεται από τέσσερα κύρια μέρη:**

- **kernel:** πρόκειται για το πιο βασικό τμήμα του Λ.Σ και είναι το software εκείνο που αναλαμβάνει τη βασική διαχείριση του υπολογιστή (κάρτες οθόνης, περιφερειακά, σκληρούς δίσκους κλπ). Όλα τα προγράμματα που χρησιμοποιούν κάποια τμήματα του υπολογιστή, συνεργάζονται με τον kernel προκειμένου να χρησιμοποιήσουν κάποιο κομμάτι του hardware.
- **Shells και GUIs:** είναι ένα σετ από προγράμματα που έχουν σαν σκοπό να δώσουν στον χρήστη του Η/Υ την δυνατότητα να "επικοινωνήσει" με το Λ.Σ και κατά συνέπεια με το hardware του υπολογιστή. Δεν είναι τίποτε άλλο από προγράμματα που περιμένουν από τον χρήστη εντολές/οδηγίες για το τι θέλει να κάνει ο υπολογιστής. Στο UNIX γενικά, ο όρος shell έχει να κάνει με προγράμματα που περιμένουν ο χρήστης να πληκτρολογήσει κάποιες εντολές για να εκτελεστούν, ενώ με τον όρο GUI εννοούμε προγράμματα που εκτελούν εντολές με την χρήση γραφικής απεικόνισης. Για παράδειγμα, αν θέλουμε να ξεκινήσουμε ένα πρόγραμμα αναπαραγωγής μουσικών CDs, ένα GUI θα εμφανίζει πάνω στην οθόνη ένα κουμπί που όταν πατηθεί θα ξεκινήσει το πρόγραμμα που "παίζει" CD. Σε ένα UNIX shell αντίθετα, θα πρέπει να θυμάται ο χρήστης το όνομα του προγράμματος και να το πληκτρολογήσει προκειμένου να εκτελεστεί το πρόγραμμα που τον ενδιαφέρει.
- **System Utilities / Daemons:** είναι προγράμματα που επιτελούν μερικές βασικές διεργασίες σε ένα UNIX σύστημα. Για παράδειγμα, ένα πρόγραμμα που υπολογίζει ολοκληρώματα δεν μπορεί να πει κανείς ότι είναι system utility, αλλά ένα άλλο που ελέγχει αν το hardware του υπολογιστή λειτουργεί σωστά, είναι.
- **Application Programs:** είναι προγράμματα που επιτελούν μερικές από τις πιο συνηθισμένες λειτουργίες ενός υπολογιστή. Για παράδειγμα στην κατηγορία αυτή θα ανήκει ένα πρόγραμμα που χρησιμοποιείται για τη συγγραφή κειμένων ή την επεξεργασία εικόνων.

**Χρήστες, Περιοχές Χρηστών & Κωδικοί Πρόσβασης**

Χρήστες (users)

Ένα από τα βασικά χαρακτηριστικά του Λ.Σ UNIX, είναι η δυνατότητα που δίνει σε πολλούς διαφορετικού ανθρώπους να χρησιμοποιήσουν τον ίδιο υπολογιστή ανεξάρτητα ο ένας από τον άλλο. Για να είναι διακριτοί οι χρήστες, κάθε ένας από αυτούς έχει ένα μοναδικό όνομα, το username. Η πρώτη πληροφορία που πρέπει να δώσει κανείς ώστε να αποκτήσει πρόσβαση στον υπολογιστή είναι αυτό το χαρακτηριστικό όνομα (username).

Κωδικοί πρόσβασης (passwords)

Το username του κάθε χρήστη είναι γενικά κάτι που χρειάζεται να το ξέρουν πολλά διαφορετικά άτομα προκειμένου να μπορούν να επικοινωνήσουν μαζί του ή να ανταλλάξουν πληροφορίες. Έτσι είναι απαραίτητο να υπάρχει κάποιο στοιχειώδες επίπεδο ασφάλειας στην χρήση του username ώστε να μην είναι δυνατή η χρήση του για μη ενδεδειγμένους σκοπούς. Έτσι λοιπόν όταν κάποιος ζητάει πρόσβαση στον

υπολογιστή δίνοντας το username του, ο υπολογιστής ζητά αμέσως μετά τον κωδικό πρόσβασης (password). Το password έχει προσωπικό χαρακτήρα και πρέπει να παραμένει κρυφό σε κάθε περίπτωση. Η σημασία του μπορεί να αντιστοιχηθεί με το PIN (Personal Identification Number) που αποκτάει κανείς όταν προμηθεύεται μια κάρτα ανάληψης μετρητών από μια τράπεζα.

Ομάδες χρηστών (user groups)
Εκτός από το username που έχει ο κάθε χρήστης ένα άλλο χαρακτηριστικό του είναι και η ομάδα (group) στο οποίο ανήκει. Ο λόγος που υπάρχει η έννοια του group είναι ότι υπάρχουν περιπτώσεις που χρειάζεται για μια συγκεκριμένη δουλειά, να χειριστεί το λειτουργικό σύστημα ένα σύνολο από χρήστες με κάποια κοινά χαρακτηριστικά. Είναι απλούστερη η διαδικασία όταν αυτοί οι χρήστες είναι ομαδοποιημένοι σε κάποιο group.

Περιοχές χρηστών (home directories)
Κάθε υπολογιστής έχει κάποιες μονάδες αποθήκευσης στις οποίες κρατάει δεδομένα που αφορούν το Λ.Σ, αλλά και τα δεδομένα των χρηστών. Κάθε χρήστης ενός UNIX συστήματος έχει μια προσωπική περιοχή στις μονάδες αποθήκευσης του υπολογιστή μέσα στην οποία μπορεί να κρατά τις πληροφορίες που τον αφορούν. Στις περισσότερες περιπτώσεις ο χώρος που είναι διαθέσιμος στον κάθε χρήστη είναι περιορισμένος και το μέγεθος της περιοχής που διαθέτει εξαρτάται από την συνολική χωρητικότητα των αποθηκευτικών μονάδων.

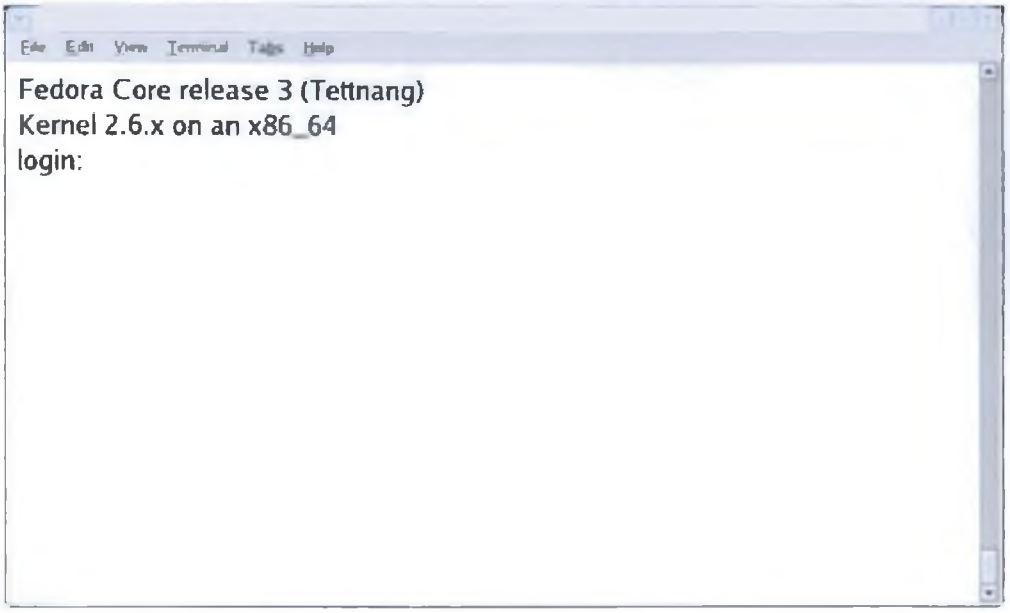
**Είσοδος / Έξοδος σε ένα UNIX Σύστημα**

Σε ένα UNIX σύστημα το πρώτο πράγμα που χρειάζεται να κάνει κάποιος για να αποκτήσει πρόσβαση είναι να δώσει στον υπολογιστή το username του. Κατόπιν, ο υπολογιστής θα ζητήσει το password που αντιστοιχεί στο username που δόθηκε. Με την επιτυχή είσοδο αυτών των δύο δεδομένων, ο υπολογιστής δίνει πρόσβαση στον χρήστη κατόπιν εκτελεί το shell του χρήστη. Αν πρόκειται για γραφικό περιβάλλον (GUI) τότε θα εμφανιστεί στην οθόνη κάτι αντίστοιχο με αυτό που φαίνεται στο ακόλουθο σχήμα:

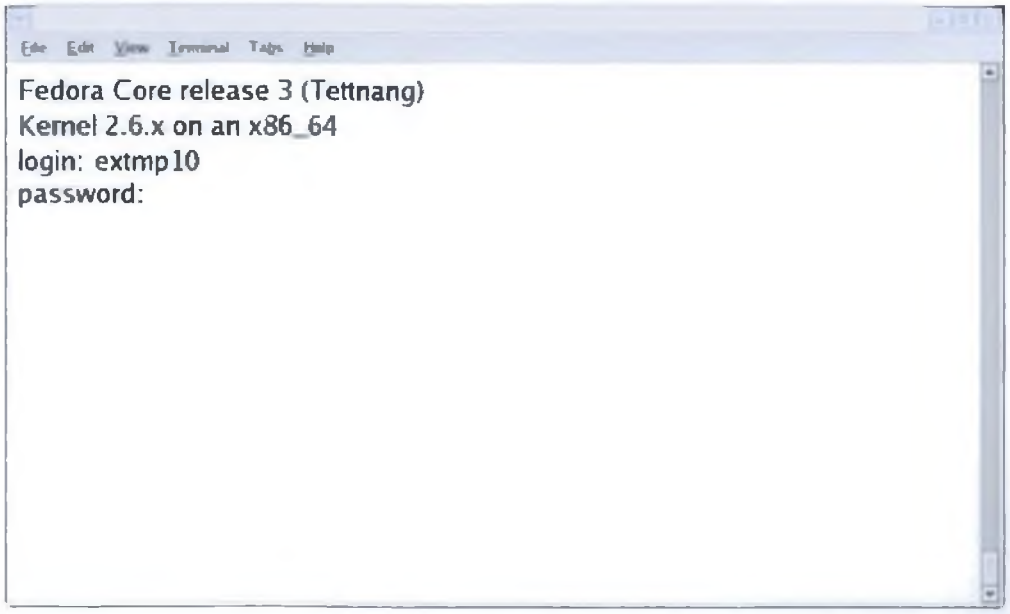

**Σχήμα 2: Παράδειγμα οθόνης login σε γραφικό περιβάλλον**

Ανάμεσα στα άλλα το βασικό σημείο σε αυτή την οθόνη είναι το κεντρικό σημείο όπου το σύστημα ζητάει από τον χρήστη το username του προκειμένου να του επιτρέψει την πρόσβαση. Το πως θα μοιάζει αυτή η οθόνη είναι κάτι τελείως υποκειμενικό, αλλά το σίγουρο είναι ότι κάπου θα υπάρχει το σημείο στο οποίο ζητάει το username. Με την πληκτρολόγηση του username από τον χρήστη, το σύστημα θα ζητήσει το password του και στη συνέχεια, αν ο συνδυασμός username και password είναι σωστός θα επιτρέψει την είσοδο του χρήστη στο σύστημα.

Σε πλήρη αντιστοιχία με το παραπάνω σχήμα, αν δεν είναι διαθέσιμη μια γραφική οθόνη για την είσοδο του username και του password του χρήστη, τότε αυτό που θα εμφανιστεί θα έχει μια μορφή όπως την ακόλουθη:




Οι δύο πρώτες γραμμές που εμφανίζονται έχουν γενικές πληροφορίες σχετικά με το σύστημα, και στην τρίτη όπου υπάρχει η λέξη login, ο υπολογιστής περιμένει από τον χρήστη να εισάγει το username του. Σαν παράδειγμα, ας θεωρήσουμε ότι το username του χρήστη είναι το extmp10. Αμέσως μετά από αυτό, ζητάει το password:



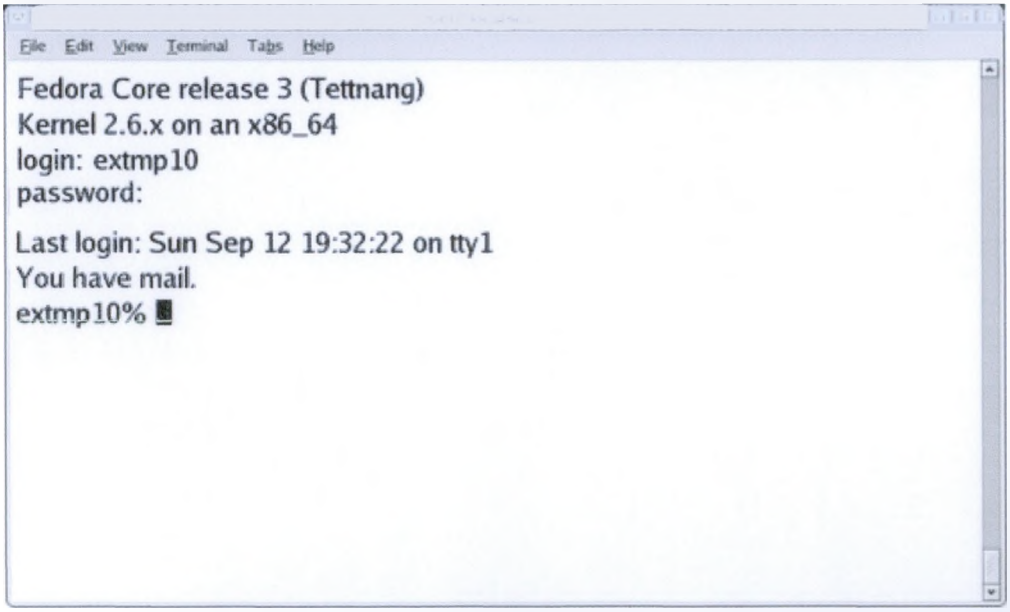

Κατά την εισαγωγή του, το password δεν εμφανίζεται στην οθόνη. Επίσης δεν εμφανίζεται κάτι άλλο που να δηλώνει την εισαγωγή στοιχείων στον υπολογιστή.

## Το κέλυφος του UNIX

Μόλις συνδεθούμε με μια UNIX μηχανή, εμφανίζεται στην οθόνη μας η **προτροπή** (**prompt**) του UNIX, σημάδι ότι το λειτουργικό σύστημα περιμένει τις εντολές μας. Το prompt είναι συνήθως ένα σύμβολο όπως το "**$**" ή το "**%**".

Στο UNIX, ένα τμήμα του λειτουργικού συστήματος που ονομάζεται **κέλυφος** (**shell**) δέχεται τις εντολές που πληκτρολογούμε, τις ερμηνεύει και εκτελεί κάποια ενέργεια βασιζόμενος σε αυτές. Το πρόγραμμα αυτό είναι επομένως ο "**διερμηνέας**" των εντολών μας. Επειδή το shell εκτελείται σαν οποιοδήποτε άλλο πρόγραμμα, μπορούμε να χρησιμοποιούμε διαφορετικά shell - αρκεί βέβαια να είναι διαθέσιμα στο σύστημα στο οποίο δουλεύουμε.

Υπάρχει μια ποικιλία από shell. Το βασικό shell που περιλαμβάνεται σε όλα τα UNIX συστήματα είναι το Bourne shell (**sh**) που χρησιμοποιεί σαν prompt το "**$**". Υπάρχουν επίσης το Korn shell (**ksh**) που επίσης χρησιμοποιεί σαν prompt το "**$**", το C shell (**csh**) που χρησιμοποιεί σαν prompt το "**%**", κ.α.
Αμέσως μετά και αν όλα είναι σωστά, το σύστημα δίνει πρόσβαση στον χρήστη ξεκινώντας ένα shell για αυτόν.




Κατά την είσοδο του χρήστη στο σύστημα, εμφανίζονται διάφορες πληροφορίες (όπως για παράδειγμά αν έχει e-mail,ή κάποιο μήνυμα από τον διαχειριστή του συστήματος) και στο τέλος εμφανίζεται το prompt. Το prompt είναι απλά μια ακολουθία χαρακτήρων ή κάποια λέξη ή κάποιο σύμβολο ή και συνδυασμός όλων αυτών που εμφανίζει το shell προκειμένου να δείξει ότι είναι έτοιμο να δεχτεί εντολές. Το τι θα είναι το prompt είναι κάτι που αποφασίζει ο ίδιος ο χρήστης, αν και γενικά υπάρχει ένα προκαθορισμένο από το σύστημα για κάθε περίπτωση. Στο παράδειγμα που χρησιμοποιήσαμε το prompt είναι το "extmp10 %" .Μετά από αυτό εμφανίζεται ο cursor (δρομέας) με το χαρακτηριστικό

σχήμα (■) που αναβοσβήνει, δείχνοντας την αναμονή του συστήματος για την είσοδο νέων εντολών.
Για την αποσύνδεσή του από το σύστημα, ο χρήστης πρέπει να δώσει την εντολή **logout** ή **exit** που τερματίζει το shell και κατά συνέχεια και την σύνδεσή του.

## 9.3 Λειτουργικό σύστημα Windows

Τα Microsoft Windows βοηθούν άτομα σε ολόκληρο τον κόσμο να αξιοποιούν τις δυνατότητές τους στην εργασία, το σπίτι και σχεδόν παντού στο ενδιάμεσο. Τα Windows προσφέρουν βελτιωμένη ενοποίηση με προγράμματα του Microsoft Office System, συμπεριλαμβανομένων των Microsoft Office Word, PowerPoint, Outlook και OneNote, καθώς και με άλλα λογισμικά της Microsoft.

**Επιχειρησιακά οφέλη**

Τα Windows XP Professional σχεδιάστηκαν για επιχειρήσεις όλων των μεγεθών και ιδιώτες που απαιτούν τα μέγιστα από την εμπειρία τους με τους υπολογιστές. Ο διάδοχός τους, τα Windows Vista, που είναι τώρα σε μορφή beta και έχει προγραμματιστεί να κυκλοφορήσουν το 2006, θα προσφέρουν ακόμα περισσότερες εξελίξεις στην αξιοπιστία, την ασφάλεια, την ευκολία ανάπτυξης, την απόδοση και τη διαχείριση.

**Λειτουργικά συστήματα Windows**

**Windows XP Professional**

Τα Windows XP Professional βοήθησαν στη δημιουργία ενός νέου προτύπου για απόδοση και αξιοπιστία. Εάν απαιτείται τα μέγιστα από το λειτουργικό σύστημα, αυτή η έκδοση των Windows έχει σχεδιαστεί για εσάς. Δείτε όλα τα κορυφαία χαρακτηριστικά της.

Τα Windows XP Tablet PC Edition —ένα νεότερο λειτουργικό σύστημα της Microsoft— προετοιμάζει το έδαφος για μία από τις πιο ευέλικτες εμπειρίες με τους υπολογιστές που είχατε ποτέ. Η φορητότητα του Tablet PC συνδυάζει εργαλεία μελάνης και ομιλίας για να μπορείτε να παίρνετε τον υπολογιστή σας σε πολλά περισσότερα μέρη και να τον χρησιμοποιείτε με πολλούς νέους τρόπους.

**Windows XP Professional x64 Edition**

Τα Windows XP Professional x64 Edition έχουν σχεδιαστεί για να ανταποκρίνονται στις ανάγκες των χρηστών τεχνικού σταθμού εργασίας και στους λάτρεις των προσωπικών υπολογιστών οι οποίοι απαιτούν την υψηλότερη απόδοση και δυνατότητα κλιμάκωσης.

## Το δίκτυο μιας επιχείρησης στην πράξη

Μέσα από μια έρευνα που έγινε σε επιχειρήσεις διαπιστώθηκε ότι η δομή του δικτύου τους ως προς την ασφάλεια στις γύρω απειλές διαφέρει τόσο από το μέγεθός της και την οικονομική της δυναμική όσο και από το αν αποτελείται από υποκαταστήματα ή όχι.

Η έρευνα μας λοιπόν κάλυψε τους δύο κυρίως τομείς που είναι ο ιδιωτικός και ο δημόσιος τομέας. Έτσι μπορούμε να αναφέρουμε δύο χαρακτηριστικά παραδείγματα: μιας μικρομεσαίας επιχείρησης και ενός εκπαιδευτικού ιδρύματος.

Μια εταιρεία για να προστατέψει το σύστημα της από απειλές χρησιμοποιεί Firewall. Ένα Firewall αποτελείτε συνήθως από έναν Η/Υ ή συσκευή γνωστό με το όνομα Bastion host (κόμβος προμαχώνας) και μια σειρά από εφαρμογές ανταπόκρισης (Proxy Services). Τα Firewalls δεν ελέγχουν μόνο ότι εισέρχεται στο εσωτερικό δίκτυο αλλά και ότι εξέρχεται από αυτό. Έναν Router έναν υπολογιστή που λειτουργεί ως μεσολαβητής ή δρομολογητής σε ένα δίκτυο. Δημιουργεί συνδέσεις με άλλους υπολογιστές , μεταβιβάζει εισερχόμενα δεδομένα στους παραλήπτες ή σε άλλους Routers. Αυτά αποτελούν τείχος προστασίας της εταιρείας και διαχωρίζουν το έξω δίκτυο (Internet) με το εσωτερικό δίκτυο της εταιρείας. Ένας Reverse Proxy είναι ένας υπολογιστής με software που διαχειρίζεται τις αιτήσεις έτσι ώστε κάποιος που θα μπει στο Internet να μην βλέπει απευθείας το εσωτερικό της εταιρείας.

Εσωτερικά της εταιρείας υπάρχει ένας Web Server ο οποίος παρέχει την δυνατότητα στον χρήστη να δει αποθηκευμένες πληροφορίες. Γενικότερα σε κάθε Web Server πραγματοποιείτε μια αντιστοίχιση των domain names στο Internet. Αποτελείτε ακόμη από έναν Proxy Server ο οποίος εκτελεί ελέγχους ανώτερου επιπέδου, όπως πιστοποίηση των χρηστών, το φιλτράρισμα συγκεκριμένων εφαρμογών και διατηρούν στατιστικά στοιχεία για το τι έγινε όλη μέρα για παράδειγμα. Υπάρχει ακόμα ένας FTP Server ο οποίος διαχειρίζεται αρχεία. Βοηθά στην μεταφορά δεδομένων δηλαδή στο ανέβασμα και το κατέβασμα, υπάρχει ακόμη χώρος για το χρήστη. Τέλος ένας Email Server ο οποίος περιλαμβάνει μηχανισμούς ελέγχου Ιών και Spam mail.

Το εσωτερικό δίκτυο της επιχείρησης αποτελείτε από δύο υποδίκτυα και ένα δίκτυο Web εφαρμογών και βάσεων. Αναφερόμενη στο υποδίκτυο αυτό (Web εφαρμογών και βάσεων) αποτελείτε από ένα Firewall το οποίο είναι είτε Software Firewall είτε Hardware Firewall συνήθως όμως έχουμε Hardware Firewall. Υπάρχει ακόμα ένα Portal Web Server για τα έργα που υλοποιούνται για Web εφαρμογές. Η προστασία κρίνεται κυρίως από έναν συνδυασμό του Firewall και το πώς θα στήσουμε την βάση. Η πρόσβαση μας στην βάση καθορίζετε από το authentication δηλαδή για να μπορέσει να έχει πρόσβαση κάποιος χρειάζεται όνομα χρήστη και Password ώστε να μπορέσουν να αποκτήσουν τα δικαιώματα που πρέπει.

Τα δύο κεντρικά υποδίκτυα ( Πάτρας και Θεσ/νίκης ) δεν διαθέτουν Firewall γιατί τους καλύπτει η προστασία του κεντρικού Firewall και Router. Συνδέονται με τα κεντρικά με μισθωμένη ψηφιακή γραμμή. Το λειτουργικό σύστημα των Servers είναι :

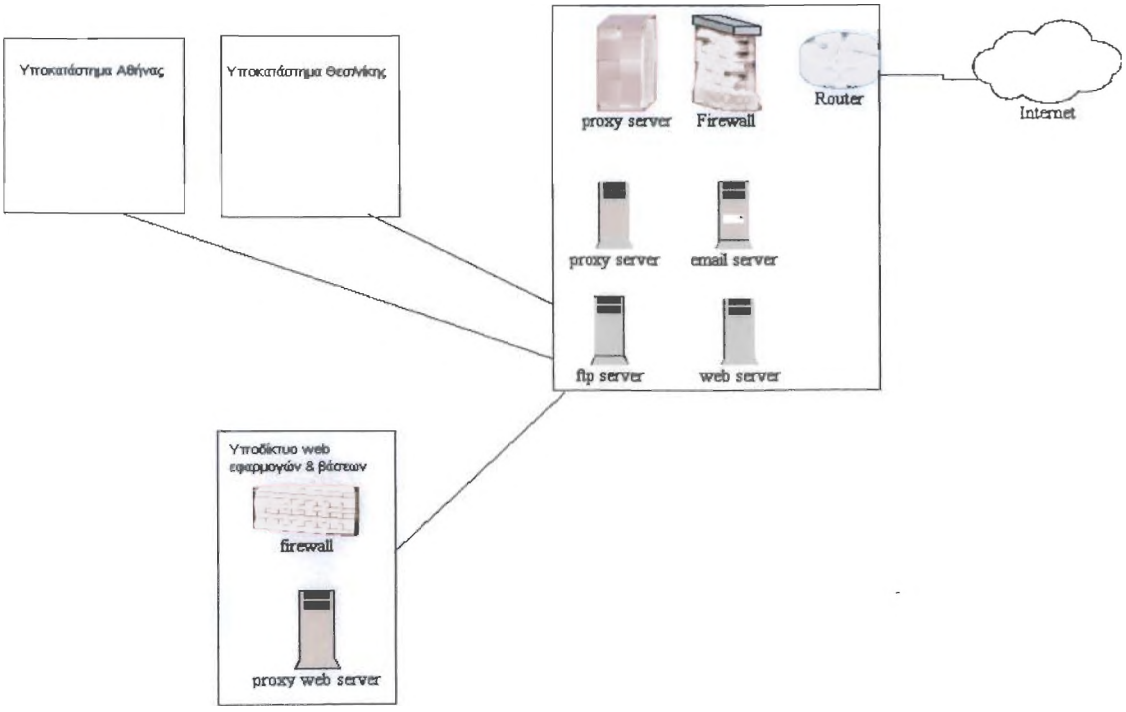
Windows 2000, 2003 και mail exchange 2003. Το site του ομίλου είναι σε oracle tomcat application και υπάρχουν ακόμα Servers με Unix και κυρίως Linux.

Για την προστασία της επιχείρησης από Ιούς , δούρειους ίππους σκουλήκια , dialers κ.λ.π υπάρχει το Firewall όπως προαναφέραμε και κάποια antivirus και Antispam. Συγκεκριμένα χρησιμοποιούν το Norton Antivirus corporate edition, αυτά αποτελούν την βάση προστασίας μιας επιχείρησης από απειλές.

Οι απειλές όμως ποικίλουν έτσι λοιπόν μια μικρομεσαία επιχείρηση πρέπει να προστατευτεί από εσωτερικούς και εξωτερικούς χρήστες. Αυτό ορίζεται από τα δικαιώματα που έχει ο κάθε χρήστης. Έτσι λοιπόν μια επιχείρηση προστατεύεται δημιουργώντας μέσα από την διαχείριση των Windows τέτοια πρόσβαση η οποία εξαρτάται από τα group χρηστών που θα ορισθούν. Γενικότερα οι χρήστες είναι ελεγχόμενοι δηλαδή έχουν πρόσβαση σε συγκεκριμένους πόρους σύμφωνα με την ιδιότητα του κάθε χρήστη στην εταιρεία.

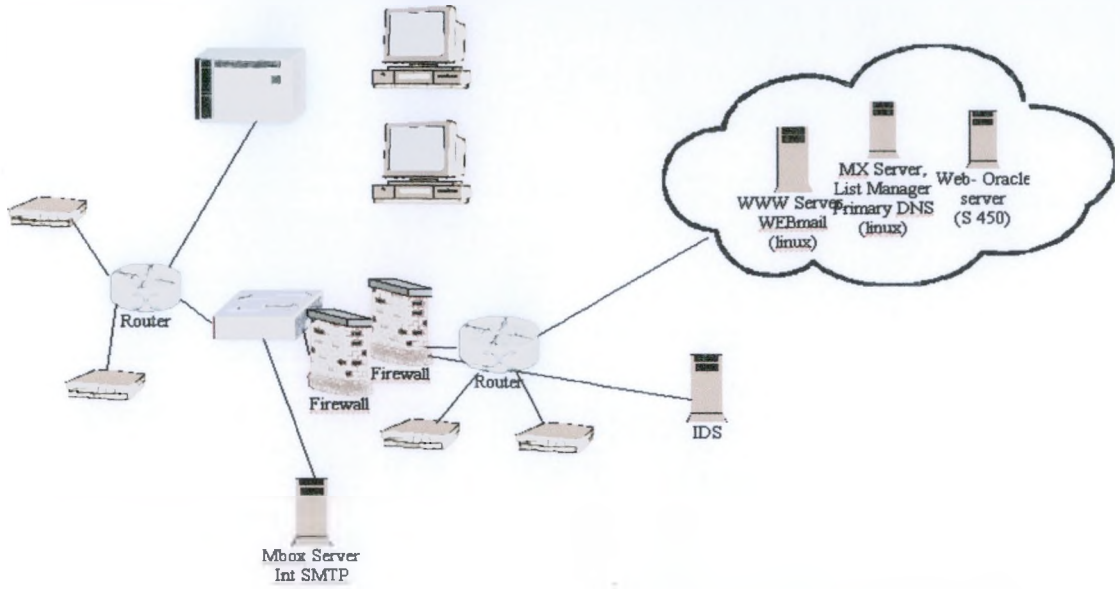
Ένας ακόμη σημαντικός παράγοντας είναι η τήρηση back-up. Κάθε επιχείρηση είναι υποχρεωμένη να διατηρεί back up. Υπάρχουν για παράδειγμα ένας mail server ένας file server που κρατάει την δουλειά και ένας data base server μέσα από τον οποίο γίνεται export όλο το υλικό και το αποθηκεύει σε συσκευές back up. Για παράδειγμα DLT σειριακές κασέτες.

## Δομή εταιρείας Logic DIS



# Δομή Ελληνικού Ανοικτού Πανεπιστημίου

Η δομή του Ελληνικού Ανοικτού Πανεπιστημίου που φαίνεται παρακάτω είναι πανομοιότυπη με τις εταιρίας Logic DIS και βασισμένη στις βασικές αρχές ασφαλείας και επικοινωνίας. Οι διαφορές τις είναι πως χρησιμοποιεί δύο firewall αντί για ένα, τρεις routers αντί για έναν και μια ακόμη εφεδρική γραμμή επικοινωνίας με τον "έξω" κόσμο.



# Όροι Δημιουργίας Δικτύων

**Analog:** Αναλογικό. Σήμα ανάμεσα σε δύο αξίες που μπορεί να ποικίλει συνεχώς. Για παράδειγμα, ένα αναλογικό ηλεκτρικό σήμα σε καλώδιο μπορεί να έχει οποιαδήποτε αξία ανάμεσα στα 0 και 12 βολτ ανά πάσα στιγμή. Συγκρίνεται με το ψηφιακό σήμα(digital).

**Application software:** Το πρόγραμμα υπολογιστή στο οποίο έχει πρόσβαση ο χρήστης. Παράδειγμα λογισμικού εφαρμογών αποτελούν η επεξεργασία κειμένου, το λογιστικό φύλλο και το λογισμικό βάσης δεδομένων.

**Backups (αντίγραφα ασφάλειας):** Αντίγραφα δεδομένων που βρίσκονται αποθηκευμένα σε υπολογιστή. Στην περίπτωση που χαθούν δεδομένα από τον υπολογιστή, το αντίγραφο ασφαλείας θα διαθέτει πρόσφατα επεξεργασμένα δεδομένα

**Baseband:** Σύστημα επικοινωνίας στο οποίο μόνο μια πληροφορία μπορεί να μεταφερθεί με μια σύνδεση τη φορά. Συγκρίνετε με broadband.

**Bit**: Συντομογραφία του Binary Digit (Δυαδικό ψηφίο). Η πιο βασική μονάδα των ψηφιακών υπολογιστών. Το bit μπορεί να βρίσκεται μόνο σε δύο θέσεις, το 0 ή το 1.

**Active X:** Τεχνολογία της Microsoft που επιτρέπει την ύπαρξη interactive περιεχομένου (π.χ. εφέ ή κίνηση) σε ιστοσελίδες.

**Client:** Πελάτης. Στο Internet σημαίνει το πρόγραμμα το οποίο στέλνει ένα request προς έναν server (για παράδειγμα ένας Browser).

**Cookies:** Αρχεία που Εναποθέτουν τα sites στον υπολογιστή σας ώστε να σας αναγνωρίσουν την επόμενη φορά που θα τα επισκεφτείτε. Συνήθως περιέχουν πληροφορίες όπως το username και το password σας, και αναζητούν το cookie για να εξακριβώσουν αν έχετε το δικαίωμα πρόσβασης στα αρχεία που ζητήσατε. Επίσης χρησιμοποιείται από τα sites για την αποθήκευση των προτιμήσεων σας για το πως θέλετε να εμφανίζεται η σελίδα ή ποιες πληροφορίες θέλετε να βλέπετε σε κάποιο portal. Τέλος, μπορεί να καταγράφει τις κινήσεις σας στο Internet έτσι ώστε να χρησιμοποιηθούν για την αποστολή διαφημίσεων που κρίνονται ενδιαφέρουσες για εσάς βάσει των σελίδων που επισκεφτήκατε.

**Database:** Βάση δεδομένων. Οργανωμένη συλλογή πληροφοριών οργανωμένα σε εγγραφές που αποτελούνται από έναν αριθμό πεδίων. Σε κάθε βάση δεδομένων μπορούμε να προβάλλουμε, να μεταβάλλουμε, να διαγράψουμε ή να προσθέσουμε δεδομένο, αρκεί να έχουμε την απαραίτητη εξουσιοδότηση.

**Dial up:** Σύνδεση με το Internet για την οποία απαιτείται και χρησιμοποιείται μια σταθερή γραμμή και ένα modem. Η σύνδεση με το Internet επιτυγχάνεται μέσω τηλεφωνικής κλήσης σε κάποιον ISP

**DNS:** (Domain Name System) Σύστημα εξυπηρέτησης domain names στο Internet. Σε κάθε Web Server, πραγματοποιείται μια αντιστοίχηση των domain names σε αριθμητικές διευθύνσεις. Έτσι, π.χ. στο domain name www.manesis.gr αντιστοιχεί κάποια αριθμητική διεύθυνση τύπου 000.00.00.0. Ο DNS αναλαμβάνει αυτή την αντιστοίχηση και μετατροπή / αναγνώριση.

**Domain:** Περιοχή. Το τελευταίο τμήμα μιας διεύθυνσης Web Server / Site, μετά την τελευταία τελεία. Οι περιοχές συμβολίζουν τόσο το όνομα της χώρας, π.χ. .gr για την Ελλάδα, όσο και συγκεκριμένους τομείς, όπως .com για commercial Web Sites .edu για εκπαιδευτικά και .org για οργανισμούς.

**Domain Name:** Τμήμα ενός URL που ακολουθεί μετά τη φράση http://www. ή http:// και ολοκληρώνεται με μια τελεία. Παράδειγμα : στο URL http://www.manesis.gr το domain name είναι manesis και todomain είναι .gr

**E-mail:** (Electronic Mail): Ηλεκτρονικό ταχυδρομείο. Μέσω e-mail επιτυγχάνεται η γρήγορη μεταβίβαση αλληλογραφίας καθώς επίσης και αρχείων εικόνας και κειμένου. Το e-mail είναι μια από τις δημοφιλέστερες υπηρεσίες του Internet.

**Extranet:** Όρος που περιγράφει την παροχή πρόσβασης σε ένα κλειστό δίκτυο Intranet, σε χρήστες που βρίσκονται σε άλλη φυσική τοποθεσία. Η επικοινωνία επιτυγχάνεται μέσω του Internet. Παράδειγμα : Πρόσβαση υποκαταστημάτων κάποιας επιχείρησης στο κεντρικό Intranet που βρίσκεται στην έδρα της επιχείρησης.

**Freeware:** Πρόγραμμα το οποίο διατίθεται από τους κατασκευαστές προς τους ενδιαφερομένους ελεύθερα χωρίς χρέωση.

**FTP:** (File Transfer Protocol) Το FTP είναι το πρωτόκολλο μεταφοράς αρχείων και αποτελεί ένα πρότυπο με το οποίο χρησιμοποιώντας ειδικά προγράμματα (FTP Clients) μπορείτε να «κατεβάσετε» μέσω του Internet αρχεία στον υπολογιστή σας.

**Firewall:** Ένα πρόγραμμα ή υπολογιστής, ο οποίος αναλαμβάνει καθήκοντα «φύλακα», ελέγχοντας κάθε εισερχόμενο ή εξερχόμενο δεδομένο, για λόγους ασφάλειας. Το Firewall λειτουργεί σαν «τοίχος» αποτρέποντας επίσης τους όποιους εισβολείς προς κάποιο εσωτερικό δίκτυο, Intranet.

**Hacker:** Χρήστης ο οποίος εισβάλει σε σύστημα στο οποίο δεν έχει νόμιμη πρόσβαση. Ένας hacker μπορεί να παραποιήσει ή ακόμη και να καταστρέψει δεδομένα και πληροφορίες.
**Host:** Υπολογιστής /Server που φιλοξενεί Web Sites ή παρέχει έτοιμα δεδομένα και υπηρεσίες με έτοιμες εφαρμογές σε τρίτους.

**HTML:** (Hyper Text Markup language): Γλώσσα προγραμματισμού για το περιβάλλον του Web, η οποία επιτρέπει την μορφοποίηση και «στήσιμο» των δεδομένων σε αρχεία html τα οποία διαβάζονται και εμφανίζονται από τους Web Browsers.

**HTTP:** (Hyper Text Transfer Protocol): Το πρωτόκολλο που διέπει την μεταφορά και τον τρόπο μετάδοσης δεδομένων στο Web.

**Hyperlink:** Ένα αντικείμενο το οποίο κατόπιν επιλογής και ενεργοποίησης είτε οδηγεί σε άλλη πληροφορία είτε εκτελεί κάποια εφαρμογή. Στην Ελλάδα λέγεται και σύνδεσμος ή παραπομπή. Βλέπε Link.

**Internet:** Ένα τεράστιο δίκτυο πολλών διαφορετικών διασυνδεμένων υπολογιστών (Servers) οι οποίοι επικοινωνούν μεταξύ τους με ένα κοινό πρωτόκολο επικοινωνίας. Το Internet: (ή Διαδίκτυο στα Ελληνικά) απαρτίζεται αυτή την στιγμή από εκατομύρια Servers και χρήστες που καθημερινά ανταλλάσσουν δισεκατομύρια πληροφοριών. Το Internet δεν έχει βάση ή ιδιοκτησία καθώς ουσιαστικά συντελείται από την παραπάνω υποδομή. Αυτό σημαίνει ότι αν κάποια μέρα αποφασίζαμε όλοι να αποσυνδέσουμε τους υπολογιστές , Servers από τις γραμμές τους τότε το Internet με την ευρεία έννοια θα έπαυε να υπάρχει. Σημαντικές λειτουργίες/ υπηρεσίες του Internet είναι το Web, E-mail, FTP, Chat, Newsgroups κ.α.

**Internet Server:** Υπολογιστής συνδεμένος με το Internet ο οποίος με τη χρήση κατάλληλου λογισμικού επιτρέπει σε άλλες ηλεκτρονικές συσκευές (H/Y, Palmtops, Mobile Phones) να έχουν πρόσβαση στις πληροφορίες ή υπηρεσίες που αυτός παρέχει και με αυτή την έννοια να εξυπηρετεί αυτές τις συσκευές.

**Internet User:** Φυσικό πρόσωπο που έχει χρησιμοποιήσει έστω και μία εφαρμογή Internet στο Internet (World Wide Web, File Transfer Protocol, chat, forum, ηλεκτρονικό ταχυδρομείο, audio, video) από οποιοδήποτε ISP (Internet Service Provider) η IAP (Internet Access Provider) σε ορισμένο χρονικό διάστημα. Οι μετρήσεις του 2001 θεωρούν ότι υπάρχουν πάνω από 350 εκατ. Χρήστες παγκοσμίως. Στην Ελλάδα υπολογίζονται στο 1,2 εκατ. χρήστες. Βλέπε επίσης User.

**Intranet:** Ένα μικρό δίκτυο που βασίζεται στην τεχνολογία του Web και το οποίο χρησιμοποιείται ενδοεπιχειρισιακά για την εξυπηρέτηση στελεχών μίας επιχείρησης.

**IP:** (Internet Protocol): Πρότυπο του Internet. Μέρος του TCP / IP

**IP Address** Διεύθυνση με τη μορφή ακολουθίας αριθμών που προσδίδεται σε κάθε υπολογιστή ή δίκτυο που είναι συνδεδεμένο στο Internet.Μία διεύθυνση IP έχει 4 μέρη με δεκαδικούς αριθμούς από το 0- 255 για το κάθε μέρος. Ένας υπολογιστής μπορεί να αποκτά διαφορετική IP διεύθυνση κάθε φορά που συνδέεται ενώ, αντίστροφα, μία IP διεύθυνση μπορεί να αντιστοιχεί σε αρκετούς διαφορετικούς υπολογιστές, για παράδειγμα όταν χρησιμοποιείται τοπικός Web Server (proxy server).

**Mail Server:** Υπολογιστής ενός ISP, ο οποίος διεκπεραιώνει την κυκλοφορία των e-mails διατηρεί γραμματοκιβώτια κ.τ.λ.

**Mailbox:** Όπως και στο παραδοσιακό γραμματοκιβώτιο ή την ταχυδρομική θυρίδα, σε ένα mailbox καταχωρείται η αλληλογραφία που έχει σταλεί μέσω e-mail.

**Modem:** Συσκευή για τη μετάδοση δεδομένων μέσω της γραμμής του τηλεφώνου που χρησιμοποιείται για να συνδεθούμε στο Internet ή για αποστολή και λήψη Fax κ.α.. Συνδυασμός των λέξεων Modulator/ Demodulator (διαμορφωτής/ αποδιαμορφωτής).

**Proxy Server:** Ένας Server στο οποίο πραγματοποιείται ενδιάμεση αποθήκευση πληροφοριών του Web με σκοπό την εύκολη ανάκλησή τους. Για παράδειγμα, εκεί αποθηκεύονται εικόνες ή σελίδες που ζητάει ένας χρήστης από κάποιο Web Site έτσι ώστε να υπάρχουν πρόχειρες για τον επόμενο χρήστη που θα τις ξαναζητήσει. Το πλεονέκτημα του Proxy Server είναι η βελτιστοποίηση στην αναμετάδοση δεδομένων ενώ παράλληλα μειώνεται ο φόρτος διακίνησης στα δικτύα. Το μειονέκτημα μπορεί να είναι ότι αν κάποιος χρήστης βρίσκεται πίσω από κάποιον Proxy Server (π.χ. σε εταιρίες) τότε πιθανόν δεν θα δει την τελευταία έκδοση του Site (ή κάποιας διαφήμισης) που επισκέπτεται αλλά αυτή που είχε αποθηκευτεί στον Proxy Server την τελευταία φορά που κάποιος άλλος επισκέφτηκε το ίδιο Site.

**Router:** Υπολογιστής που λειτουργεί ως μεσολαβητής ή δρομολογητής σε ένα δίκτυο. Δημιουργεί συνδέσεις με άλλους υπολογιστές, μεταβιβάζοντας τα εισερχόμενα δεδομένα στους παραλήπτες ή σε άλλους routers.

**Server:** Κεντρικός υπολογιστής ο οποίος εξυπηρετεί άλλους υπολογιστές (Clients) και προμηθεύει στους χρήστες αυτών των υπολογιστών με το υλικό που του ζητήθηκε το οποίο είναι αποθηκευμένο στον σκληρό του δίσκο. Ένας Web Server π.χ. παρέχει σε έναν χρήστη τη δυνατότητα, να δει τις αποθεκευμένες πληροφορίες που υπάρχουν μέσα στον δίσκο του, υπό την μορφή HTML.

**SMTP:** (Simple Mail Transfer Protocol) Πρωτόκολλο μεταφοράς email

**Spam:** Spamming: Εχθρική μαζική επίθεση ή ανεπιθύμητα διαφημιστικά μηνύματα μέσω e-mail.

**SSL:** Το Secure Socket Layer είναι ένα πρωτόκολλο που χρησιμοποιείται από την Netscape για προσφορά ασφαλών συναλλαγών στους χρήστες στο δίκτυο.

**TCP/IP:** (Transmission Control Protocol/Internet Protocol): Βασικό πρότυπο του Internet που διέπει τη μετάδοση δεδομένων, τη ροή δεδομένων και την απόδοση. Το TCP/IP εφαρμόζεται όλο και περισσότερο σε Extranets (υπερενδοδίκτυα) και Intranets (ενδοδίκτυα).

**UNIX:** (UNIpleXed Information and computing system): Λειτουργικό σύστημα υπολογιστών και Web Servers. Είναι ευρέως διαδεδομένο στο Internet.

**USEnet:** Δίκτυο ειδήσεων και ηλεκτρονικού ταχυδρομείου στο Internet

**User:** Χρήστης μιας online υπηρεσίας ή του Internet γενικότερα.

**URL:** (Uniform Resource Locator): Η διεύθυνση που συνολικά καθορίζει ένα Web Site. Όπως σε μια ατζέντα διευθύνσεων προσδιορίζεται ακριβώς η θέση του κωδικού πόλης και του αριθμού, έτσι και στο URL ορίζεται η ακριβής δομή των στοιχείων μιας διεύθυνσης. Αρχικά αναφέρεται η μέθοδος (πρωτόκολο) μετάδοσης των δεδομένων, όπως http ή ftp, η οποία ακολουθείται από διπλή κάθετο. Στη συνέχεια ακολουθεί η διεύθυνση του Web Server (Domain Name), π.χ.
http://www.cnn.com και ενδεχομένως ο προσδιορισμός της τοποθεσίας μίας συγκεκριμένης σελίδας στο Web Site πχ http://www.cnn.com/sports/football/news.html
Το URL μπορεί να πληκτρολογηθεί στον Web Browser με ή χωρίς το http://

**Virus:** Επιβλαβής ιός (πρόγραμμα) το οποίο κατόπιν δικής μας ενέργειας ή εν αγνοία μας, εισβάλλει σε εφαρμογές. Μπορεί να «κολλήσει» στον υπολογιστή μας μέσω του Internet από κάποιο e-mail που ήρθε ή κάποιο αρχείο που ενεργοποιήσαμε και να οδηγήσει σε απώλεια δεδομένων, να προκαλέσει βλάβη ή να καταστρέψει ολοκληρωτικά το σύστημά μας. Για την προστασία των υπολογιστών απαιτούνται ειδικά προγράμματα κατά των ιών (Antivirus Programs).

**WAIS :**(Wide Area Information Server-Διακομιστής πληροφοριών ευρείας ζώνης) Ένα πανίσχυρο σύστημα για την αναζήτηση μεγάλων ποσοτήτων πληροφοριών στο Internet πολύ γρήγορα

**Web Address:** Μοναδικός χαρακτηρισμός για έναν υπολογιστή ή ένα Web Site στο Internet . Η πιό συνηθισμένη της μορφή είναι το γνωστό www.site.gr κτλ. Βλέπε Domain Name.

**Web Broswer:** Πρόγραμμα με το οποίο μπορεί κάποιος να επισκεφτεί Web Sites και να δει Web Pages Γνωστοί Web Browsers είναι: Microsoft Internet Explorer, Netscape Communicator, Mosaic, Opera.

**Web Page:** Μεμονωμένη «σελίδα» προγραμματισμένη στην γλώσσα HTML η οποία είναι μέρος ενός συνολικού Web Site. Μία Web Page πρέπει να περιέχει κείμενα με links και μπορεί να περιέχει επίσης εικόνες, animation αλλά και ήχο, video κτλ. Στα Ελληνικά λέγεται και Ιστοσελίδα.

**Web Site:** Χαρακτηρισμός της παρουσίας στο World Wide Web. Μία δικτυακή τοποθεσία ή Ιστότοπος όπως πολλοί το αναφέρουν στα Ελληνικά. Ένα Web Site περιλαμβάνει εκτός από την αρχική σελίδα, πρόσθετες σελίδες Web, καθώς και άλλα στοιχεία όπως εικόνες, video, ήχο και πρέπει να χαρακτηρίζεται μία διεύθυνση (URL ή Domain Name) π.χ. **www.manesis.gr**

**WWW:** Χαρακτηρισμός του γραφικού περιβάλλοντος που πλέον διέπει το Internet. Χάρη στις δυνατότητες multimedia που προσφέρει, το Web συνέβαλλε σημαντικά στην ραγδαία εξάπλωση του Internet. Αποτελεί ωστόσο μόνο μία από τις πολλές δυνατότητες επικοινωνίας που διαθέτει το Internet. Στην Ελλάδα λέγεται και παγκόσμιος Ιστός.

# Βιβλιογραφία


- **Alam M. Cohen - [Δίκτυα Υπολογιστών]**
- **William Stallings - [Επικοινωνία Υπολογιστών και Δεδομένων]**
- **Πανεπιστήμιο Μακεδονίας - [ Κέντρο Υπολογιστών και Δικτύων ]**
- **Ιστοσελίδα** – [ www.go-online.gr ]
- **Ιστοσελίδα** – [ www.tmth.edu.gr ]
- **Ιστοσελίδα** – [ www.noc.uom.gr ]