

# Κεφάλαιο 8

## Διαχείριση και Ασφάλεια Δικτύου

### Εισαγωγή

Καθώς σήμερα η ανάγκη δικτύωσης γίνεται όλο και πιο επιτακτική, οι περισσότερες επιχειρήσεις διαθέτουν κάποιο είδος τοπικού δικτύου. Οι μεγαλύτερες εταιρίες έχουν προχωρήσει στη διασύνδεση των απομακρυσμένων υποκαταστημάτων τους με τεχνολογίες WAN ή και απευθείας μέσω του Διαδικτύου και τεχνολογιών VLAN.

Οι δομές των παραπάνω δικτύων μπορούν να γίνουν αρκετά πολύπλοκες. Σε μεγάλες εταιρίες, ακόμα και το τοπικό δίκτυο μπορεί να περιέχει αρκετές δικτυακές συσκευές και να είναι ιδιαίτερα πολύπλοκο. Ειδικά όταν έχουμε δικτυακές συσκευές από διάφορους κατασκευαστές, αυξάνεται ακόμα περισσότερο η δυσκολία διαχείρισης του δικτύου.

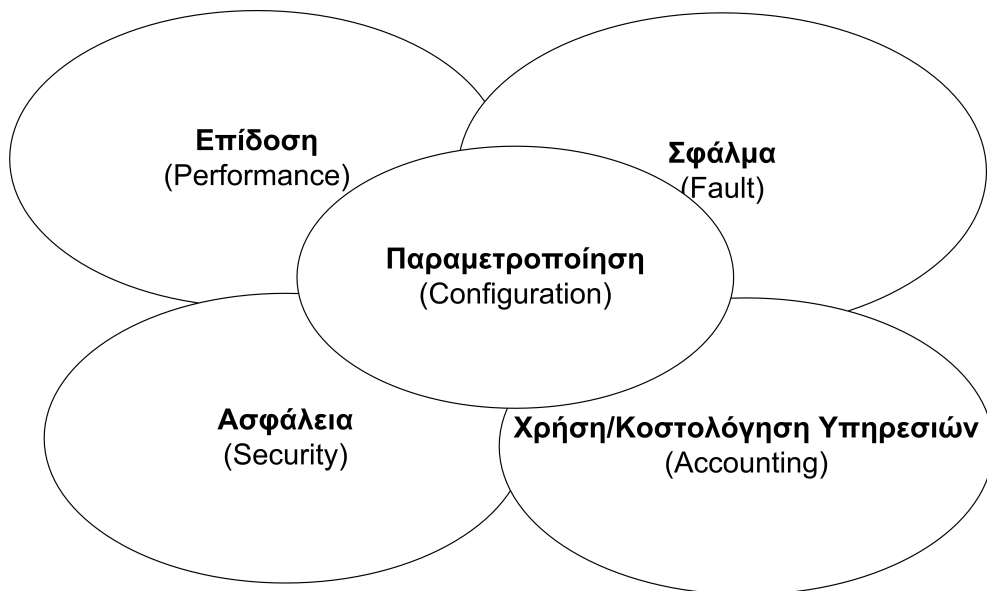
Είναι προφανές ότι υπάρχει ανάγκη για κεντρική διαχείριση σε κάθε πολύπλοκο ή/και καταναμημένο δίκτυο. Η κεντρική διαχείριση μπορεί να παρουσιάζει δυσκολίες, καθώς συσκευές διαφορετικών κατασκευαστών μπορεί να υλοποιούν τους μηχανισμούς διαχείρισης με διαφορετικό τρόπο. Βρίσκεται και σήμερα σε εξέλιξη μια διαδικασία για τη δημιουργία προτύπων στον τομέα της διαχείρισης.

Ένα κομμάτι της διαχείρισης είναι και η ασφάλεια του δικτύου. Πρόκειται για ένα σύνθετο θέμα το οποίο περιλαμβάνει αρκετές παραμέτρους, και είναι πολύ σημαντικό να μπορούμε να τις ελέγχουμε κεντρικά. Και στον τομέα αυτό, γίνεται αυτή τη στιγμή προσπάθεια για τη δημιουργία προτύπων. Στις επόμενες ενότητες θα ασχοληθούμε με θέματα ασφάλειας και διαχείρισης δικτύων.

## 8.1 Διαχείριση Δικτύου

Ο Διεθνής Οργανισμός Πιστοποίησης (ISO, International Standards Organization) έχει ορίσει ένα πλαίσιο λειτουργιών (framework) που αφορά τη διαχείριση δικτύων και ανήκει στο μοντέλο του γνωστού μας OSI. Το μοντέλο αυτό ορίζει πέντε περιοχές διαχείρισης:

- Διαχείριση Παραμέτρων του Δικτύου (Configuration Management)
- Διαχείριση Επίδοσης του Δικτύου (Performance Management)
- Διαχείριση Σφαλμάτων (Fault Management)
- Διαχείριση Κόστους Υπηρεσιών (Accounting Management)
- Διαχείριση Ασφάλειας (Security Management)



Σχήμα 8.1: Η διαχείριση δικτύων κατά το μοντέλο OSI

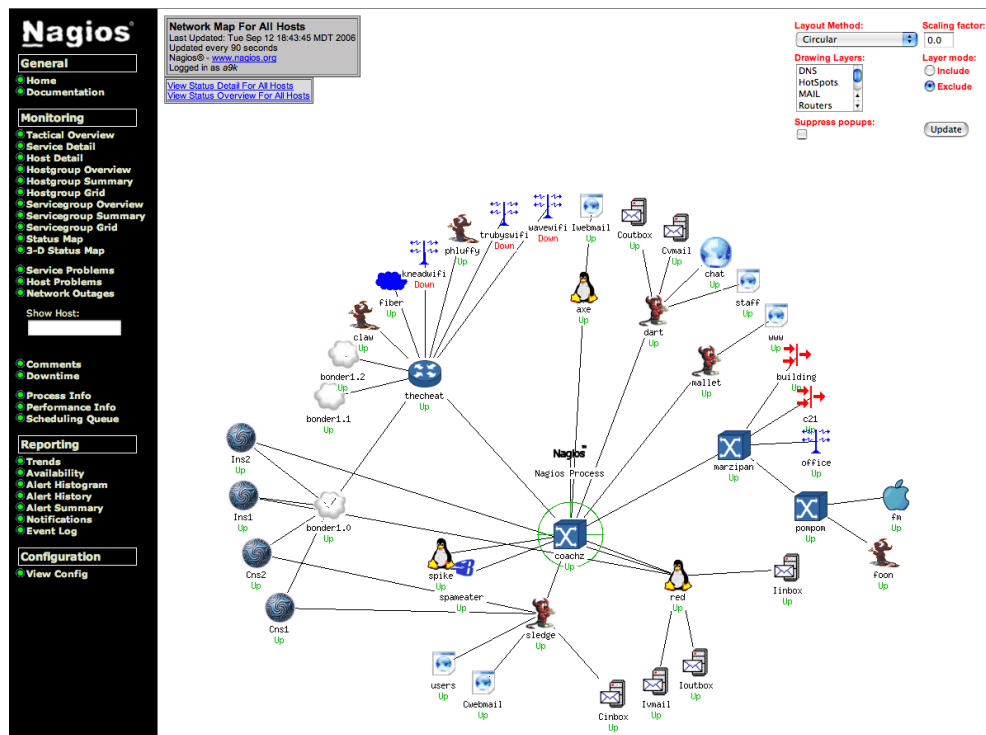
Θα εξετάσουμε αυτές τις πέντε περιοχές διαχείρισης παρακάτω.

### 8.1.1 Διαχείριση Παραμέτρων (Configuration Management)

Ο όρος *διαχείριση παραμέτρων* αναφέρεται στη διαδικασία αλλαγής της τοπολογίας του δικτύου και τη ρύθμιση των παραμέτρων των συσκευών. Οι ρυθμίσεις μπορούν να γίνονται στο επίπεδο του υλικού και του λογισμικού, προκειμένου το δίκτυο να

καλύπτει τις απαιτήσεις που έχουμε κάθε φορά. Η αρχική εγκατάσταση και ρύθμιση του δικτύου, δεν αποτελεί (σύμφωνα με τον επίσημο ορισμό του OSI) μέρος της διαχείρισης του. Ωστόσο τις περισσότερες φορές χρησιμοποιούμε τα ίδια εργαλεία (λογισμικό, εφαρμογές) και τεχνικές κατά την αρχική εγκατάσταση, όσο και μετέπειτα για τη συντήρηση του. Για το λόγο αυτό, η αρχική εγκατάσταση και διαμόρφωση ενός δικτύου θεωρείται από τους περισσότερους ως μέρος της διαχείρισης του.

Προκειμένου να είναι δυνατή η διαχείριση ενός δικτύου, ένα σημαντικό κομμάτι είναι η *τεκμηρίωση (documentation)*. Τεκμηρίωση σε αυτή την περίπτωση είναι η καταγραφή των ρυθμίσεων και του τρόπου λειτουργίας κάθε συσκευής του δικτύου. Για παράδειγμα, μέρος της τεκμηρίωσης μπορεί να είναι τα πρωτόκολλα που χρησιμοποιούνται στο δίκτυο και οι ιδιαίτερες ρυθμίσεις τους σε κάθε συσκευή. Σε ένα switch μπορεί να είναι το πλήθος των θυρών που χρησιμοποιούνται και ποιο τμήμα του δικτύου είναι συνδεδεμένο σε ποια θύρα. Τέλος, για ένα μηχάνημα που έχει το ρόλο του *firewall* (τείχους προστασίας), η τεκμηρίωση θα αναφέρεται για παράδειγμα στις θύρες (TCP ports) που είναι ανοικτές. Η τεκμηρίωση επίσης αναφέρεται και σε γενικότερα θέματα, όπως η τοπολογία του δικτύου και ο τρόπος λειτουργίας του.



Σχήμα 8.2: Παράδειγμα προγράμματος διαχείρισης δικτύου

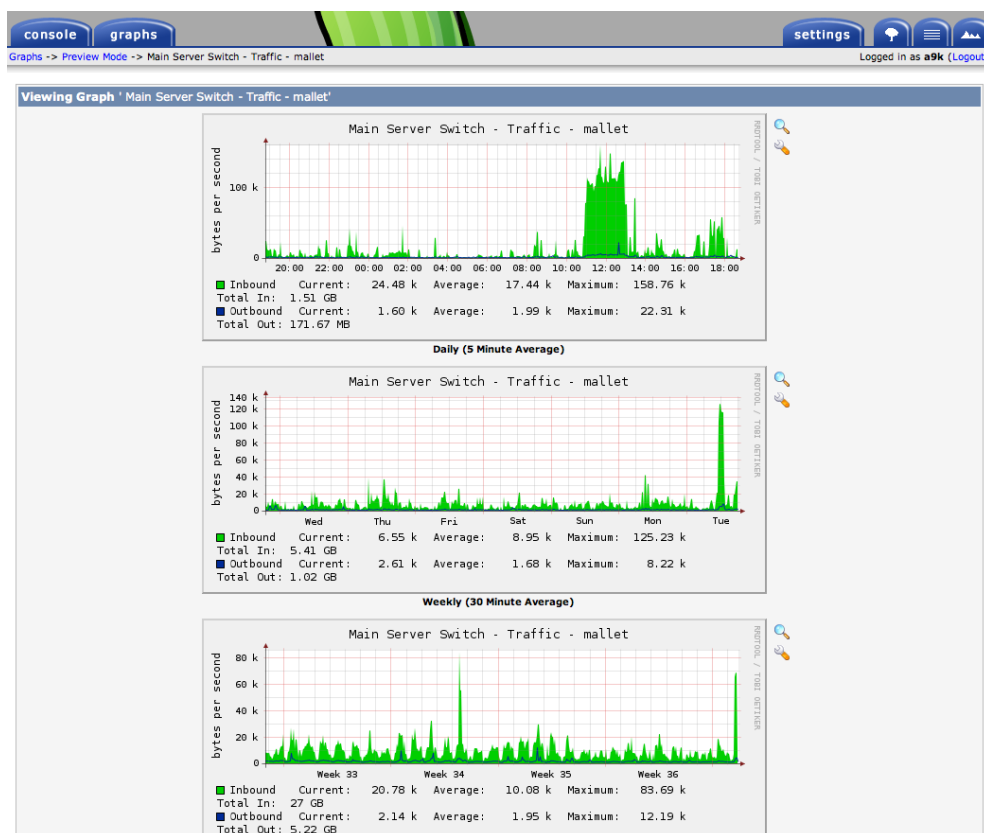
Η τεκμηρίωση μπορεί να βοηθηθεί αρκετά από την ύπαρξη λογισμικού που ανακαλύπτει και καταγράφει σε μια βάση δεδομένων καταλόγου υλικών (*inventory database*) όλες τις συσκευές ενός δικτύου και τον τρόπο διασύνδεσης τους. Προφανώς ένα τέτοιο πρόγραμμα μπορεί να ανακαλύψει μόνο ενεργές συσκευές ενός δικτύου (π.χ. δρομολογητές, υπολογιστές, switches κλπ). Το πρόγραμμα μπορεί επίσης να ανακαλύψει το είδος του τοπικού δικτύου (τμήματα ethernet, token ring κλπ) καθώς και τις όποιες γραμμές WAN ίσως υπάρχουν (μισθωμένες PPP, επιλεγόμενες dial-up / isdn, X.25, Frame Relay κλπ). Αν χρησιμοποιούμε λογισμικό που εκτελεί και λειτουργίες διαχείρισης δικτύου, τότε μπορεί να ανακαλύψει και υπολογιστές, εκτυπωτές και άλλες συσκευές. Οι εφαρμογές αυτές μπορούν συνήθως να αναπαραστήσουν γραφικά (δικτυακός χάρτης) τις συσκευές του δικτύου και την μεταξύ τους συνδεσμολογία.

### 8.1.2 Διαχείριση Επίδοσης του Δικτύου (Performance Management)

Για να διαχειριστούμε την απόδοση ενός δικτύου, πρέπει πρώτα να ορίσουμε ποια θα είναι τα μεγέθη που επιθυμούμε να μετρήσουμε. Έπειτα πρέπει να βρούμε τον τρόπο με τον οποίο θα γίνονται οι μετρήσεις μας και τέλος να τις υλοποιήσουμε. Τυπικά, σε ένα δίκτυο μετράμε ανά τακτά διαστήματα χαρακτηριστικά όπως τα παρακάτω:

- Το ποσοστό χρησιμοποίησης των γραμμών WAN ή τμημάτων του τοπικού δικτύου.
- Ανάλυση του ποσοστού κίνησης ανά πρωτόκολλο π.χ. TCP/IP, IPX, Netbios κλπ.
- Το ποσοστό λαθών σε σχέση με όλη την κίνηση.
- Το χρόνο καθυστέρησης σε διάφορα σημεία του δικτύου.
- Το χρόνο απόκρισης κάποιων συσκευών.
- Καθορισμένα κατώφλια (κρίσιμες μέγιστες ή ελάχιστες τιμές). Όταν οι τιμές των μετρούμενων παραμέτρων ξεφεύγουν από αυτά τα όρια, τότε εμφανίζονται κάποιοι συναγερμοί (alarms).

Οι μετρήσεις επίδοσης μπορεί να αποθηκεύονται για μελλοντική επεξεργασία και σύγκριση με επόμενες μετρήσεις. Υπεύθυνος για αυτή την επεξεργασία είναι ο διαχειριστής του δικτύου. Η ανάλυση των μετρήσεων μπορεί να καταδείξει τα σημεία που δημιουργούν προβληματική λειτουργία ή συμφόρηση του δικτύου. Με βάση τα συμπεράσματα των μετρήσεων μπορεί να γίνει ανασχεδίαση σημείων του δικτύου,



Σχήμα 8.3: Παρακολούθηση επιδόσεων δικτύου

αλλαγή υλικού ή ρυθμίσεων κλπ. Μετά τις αλλαγές, η σύγκριση με νέες μετρήσεις θα δείξει κατά πόσο ήταν επιτυχής η επίλυση του προβλήματος.

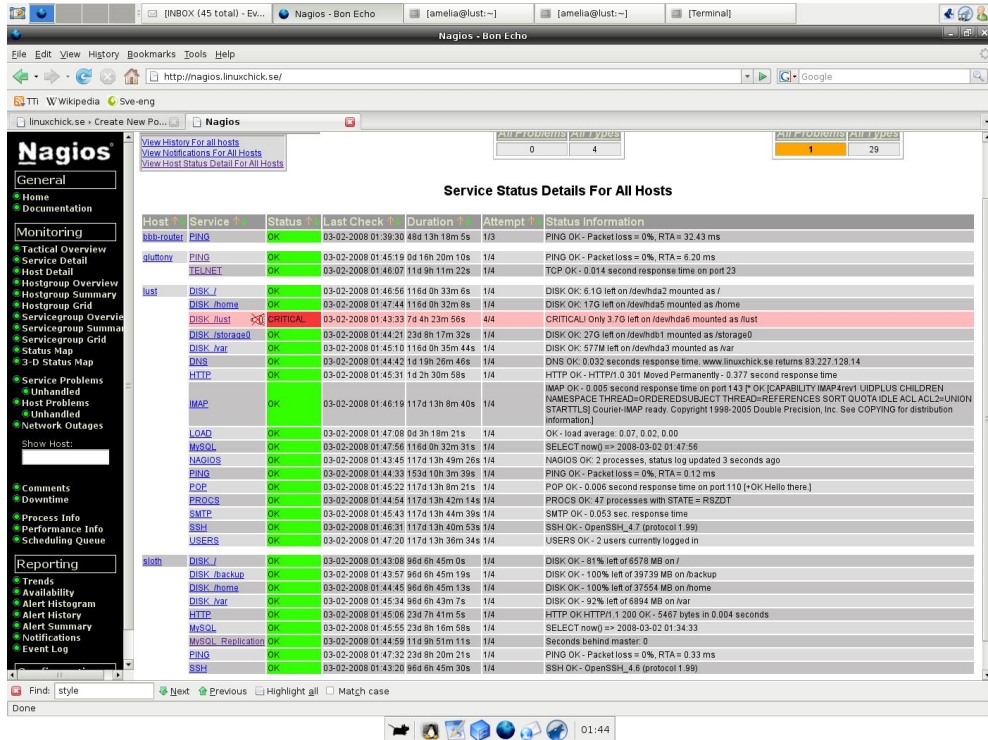
Τυπικά οι μετρούμενες τιμές καταγράφονται σε πίνακες και μπορούν επίσης να αναπαρίστανται με μορφή γραφημάτων (Σχήμα 8.3).

### 8.1.3 Διαχείριση Σφαλμάτων (Fault Management)

Με τη διαχείριση σφαλμάτων μπορούμε να εντοπίσουμε προβλήματα στη λειτουργία του δικτύου. Μπορούμε επίσης να βρούμε το σημείο στο δίκτυο που τα δημιουργεί και ενδεχομένως να το διορθώσουμε, αν πρόκειται απλώς για κάποια ρύθμιση. Σε περίπτωση που το πρόβλημα αφορά υλικό ή βρίσκεται εκτός της δικαιοδοσίας μας, μπορούμε να προωθήσουμε την περιγραφή του προβλήματος (να δημιουργήσουμε δηλ. κατάλληλη τεκμηρίωση) σε μια άλλη ομάδα που θα το αναλάβει.

Σε κάθε περίπτωση, γίνεται καταγραφή του προβλήματος καθώς και των βημάτων

που ακολουθήθηκαν για την επίλυση του, ώστε να υπάρχει έτοιμη λύση σε περίπτωση που το πρόβλημα εμφανιστεί ξανά στο μέλλον. Για κάποιες από τις συσκευές του δικτύου, ίσως να είναι χρήσιμο να τηρούνται στατιστικά σχετικά με το ποσοστό λαθών που εμφανίζουν.



Σχήμα 8.4: Παρακολούθηση σφαλμάτων

Μερικά προβλήματα μπορεί να είναι εύκολο να εντοπιστούν (χαλασμένη ή απενεργοποιημένη συσκευή). Ο σκοπός όμως της διαχείρισης είναι να μπορεί να προβλέψει προβλήματα πριν αυτά παρουσιαστούν και επηρεάσουν τους χρήστες του δικτύου. Η πρόβλεψη πιθανών προβλημάτων σχετίζεται άμεσα με τη διαχείριση επίδοσης του δικτύου.

Τα προβλήματα εμφανίζονται στο πρόγραμμα διαχείρισης με τη μορφή συναγερμών (alarms) και καταγράφονται συνήθως σε αρχεία καταγραφής (log files). Σε περίπτωση γραφικών απεικονίσεων, ενδεχομένως να απεικονίζονται οι προβληματικές συσκευές με διαφορετικό χρώμα. Ανάλογα με το πρόβλημα, μπορεί να χρειάζεται αποσύνδεση ή αντικατάσταση προβληματικών συσκευών από το δίκτυο ή αλλαγή των ρυθμίσεων στο λογισμικό των συσκευών.

#### 8.1.4 Διαχείριση Κόστους (Accounting Management)

Το έργο της διαχείρισης κόστους του δικτύου περιλαμβάνει την παρακολούθηση της χρήσης των πόρων του δικτύου και την ανάλυση των διαθέσιμων ορίων χρήσης του δικτύου για συγκεκριμένες ομάδες χρηστών. Γίνεται ακόμα καταγραφή της χρήσης των πόρων του δικτύου ανά ομάδες χρηστών. Τέλος εξασφαλίζεται ότι οι χρήστες δεν χρησιμοποιούν υπηρεσίες που δεν είναι συμφωνημένες.

#### 8.1.5 Διαχείριση Ασφάλειας (Security Management)

Η διαχείριση ασφάλειας περιλαμβάνει τον έλεγχο πρόσβασης σε συσκευές, δεδομένα και προγράμματα απέναντι σε κάθε μη-εξουσιοδοτημένη χρήση (ηθελημένη ή μη). Μπορούμε με αυτόν τον τρόπο να εντοπίσουμε τυχόν απόπειρες παραβίασης των κανόνων ασφαλείας του δικτύου και να λάβουμε τα απαραίτητα μέτρα. Το ζήτημα της ασφάλειας είναι αρκετά πολύπλοκο και θα το εξετάσουμε αναλυτικότερα σε επόμενες ενότητες.

Σε κάθε πληροφοριακό σύστημα που είναι κατανεμημένο, τα μέτρα ασφάλειας δεν πρέπει να εκτείνονται μόνο σε ένα ή μερικούς τομείς του, αλλά να καλύπτουν το σύνολο του. Ο οργανισμός ή εταιρία που χρησιμοποιεί ένα πληροφοριακό σύστημα, ουσιαστικά δεσμεύεται να οργανώσει και να τηρεί κανόνες ασφαλείας. Τα μέτρα ασφαλείας αφορούν:

- Τη φυσική προστασία των πόρων του συστήματος από μη-εξουσιοδοτημένη πρόσβαση. Αυτό τυπικά σημαίνει ότι τα κρίσιμα μηχανήματα του δικτύου βρίσκονται σε καλά φυλασσόμενο χώρο.
- Την ασφάλεια των συστημάτων που συνδέονται στο δίκτυο. Και αυτό το κομμάτι ανήκει στη διαχείριση ασφαλείας των συστημάτων (για παράδειγμα, μπορεί να υλοποιείται με τη βοήθεια των μηχανισμών ασφαλείας που παρέχει το λειτουργικό σύστημα που χρησιμοποιείται).
- Την ασφάλεια του δικτύου και την προστασία των δεδομένων που μεταφέρονται μέσα από αυτό.

### 8.3 Ασφάλεια Δικτύων

Με την ανάπτυξη των δικτύων αλλά και του Δημόσιου Internet (με το οποίο πλέον πραγματοποιείται μεγάλο μέρος συναλλαγών και διακίνηση κρίσιμων δεδομένων), είναι πλέον σαφής η ανάγκη για προστασία της πληροφορίας που μεταφέρεται και

αποθηκεύεται. Στην ενότητα αυτή θα εξετάσουμε τα διάφορα προβλήματα που εμφανίζονται στην ασφάλεια των δικτύων καθώς και διάφορους τρόπους για την αντιμετώπιση τους. Θα μιλήσουμε για συστήματα και τεχνικές ασφαλείας, για τους τρόπους με τους οποίους υλοποιούνται, καθώς και τις προϋποθέσεις για την ύπαρξη συστημάτων ασφαλείας.

### 8.3.1 Ασφάλεια Πληροφοριών

Η ασφάλεια ενός οποιουδήποτε συστήματος ασχολείται με την προστασία αντικειμένων που έχουν κάποια αξία, γενικά γνωστά ως αγαθά. Η αξία των αγαθών μειώνεται αν υποστούν ζημιά. Αν δεχτούμε ότι υπάρχουν κίνδυνοι που μπορούν να μειώσουν την αξία των αγαθών, θα πρέπει να λάβουμε τα αντίστοιχα μέτρα προστασίας τους. Τα μέτρα αυτά προφανώς θα έχουν κάποιο κόστος (χρηματικό και σε κόπο). Προφανώς θα πρέπει να σταθμίσουμε το κόστος προστασίας των αγαθών με το αντίστοιχο ρίσκο αλλά και με το κόστος των ίδιων των αγαθών. Αν λάβουμε μειωμένα (πλημμελή) μέτρα προστασίας, η ασφάλεια των αγαθών δεν θα είναι εξασφαλισμένη. Ο ιδιοκτήτης των αγαθών είναι υπεύθυνος να σταθμίσει το κόστος προστασίας ανάλογα με το κίνδυνο και την αξία των αγαθών, και να αποφασίσει ποιο είναι το σημείο ισορροπίας.

Σε ένα πληροφοριακό σύστημα, ως αγαθά θα πρέπει να θεωρήσουμε τα δεδομένα που διακινούνται και αποθηκεύονται σε αυτό, καθώς και τους υπολογιστικούς πόρους (εξοπλισμό) που το απαρτίζουν. Ο ιδιοκτήτης έχει τη δυνατότητα να καθορίσει ποιος μπορεί να έχει χρησιμοποιήσει, να μεταβάλλει, ή να διαθέσει το αγαθό. Εκτός από τους ιδιοκτήτες τα αγαθά μπορεί να χρησιμοποιούνται και από τους χρήστες, οι οποίοι μπορεί να έχουν διαφορετικούς βαθμούς πρόσβασης σε αυτά. Για παράδειγμα, ο χρήστης μιας ιστοσελίδας έχει δυνατότητα να διαβάσει το περιεχόμενο ή να “κατεβάσει” αρχεία, αλλά δεν μπορεί να αλλάξει το περιεχόμενο τους. Από το παράδειγμα μας είναι ήδη προφανές ότι ιδιοκτήτης και χρήστης ενός πληροφοριακού αγαθού, δεν είναι απαραίτητα το ίδιο άτομο. Η έννοια του χρήστη δεν αναφέρεται αναγκαστικά σε κάποιο φυσικό πρόσωπο: διεργασίες που εκτελούνται μέσα στο ίδιο το σύστημα και έχουν πρόσβαση στα δεδομένα θεωρούνται επίσης “χρήστες” των δεδομένων.

---

**Σημείωση κατανόησης:** Σε ένα σύστημα UNIX οι διεργασίες που εκτελούν λειτουργίες χωρίς την παρέμβαση χρηστών είναι γενικά γνωστές ως “δαίμονες” (daemons). Αντίστοιχα, σε συστήματα Windows είναι γνωστές ως “υπηρεσίες” (services). Γενικά στα σύγχρονα λειτουργικά συστήματα, η δυνατότητα κάποιου χρήστη να χρησιμοποιήσει ή να μεταβάλλει δεδομένα ή ρυθμίσεις ρυθμίζεται από το διαχειριστή ο οποίος παραχωρεί τα αντίστοιχα απαιτούμενα δικαιώματα. Θυμίζουμε ότι

ένας χρήστης αναγνωρίζεται τυπικά από κάποιο όνομα χρήστη και κωδικό.

Με τον ίδιο τρόπο που κάποιος πραγματικός χρήστης (άνθρωπος) διαθέτει δικαιώματα, το ίδιο και οι υπηρεσίες που εκτελούνται αυτόματα σε ένα σύστημα χρησιμοποιούν κάποιο λογαριασμό χρήστη στον οποίο έχουν παραχωρηθεί τα ελάχιστα απαραίτητα δικαιώματα που απαιτούνται για να διεκπεραιώσουν την εργασία που τους έχει ανατεθεί. Έτσι για παράδειγμα, μια διεργασία που αναλαμβάνει να εξυπηρετήσει ιστοσελίδες σε χρήστες (web server) έχει μόνο τη δυνατότητα να διαβάσει τα συγκεκριμένα αρχεία που χρειάζεται για αυτή τη λειτουργία (δηλ. τις html σελίδες που έχει αποθηκεύσει ο διαχειριστής σε κάποιους καταλόγους). Για το σκοπό αυτό δημιουργείται ένας λογαριασμός χρήστη με τα αντίστοιχα δικαιώματα και η διεργασία εξυπηρέτησης φαίνεται σαν να εκτελείται από το χρήστη αυτό.

Από τη στιγμή που υπάρχει η έννοια της ιδιοκτησίας, θα πρέπει να εισάγουμε και την έννοια της *εξουσιοδότησης*. Εξουσιοδότηση είναι η άδεια που παρέχει ο ιδιοκτήτης σε κάποιον τρίτο (χρήστη) για τη χρήση των δεδομένων ή/και των υπολογιστικών πόρων του δικτύου. Ένα από τα σημαντικότερα προβλήματα ασφάλειας είναι η εξασφάλιση ότι μόνο εξουσιοδοτημένοι χρήστες θα έχουν πρόσβαση στα δεδομένα. Ένα ακόμα πρόβλημα είναι ότι οι εξουσιοδοτημένοι χρήστες μπορεί να θελήσουν να χρησιμοποιήσουν την πρόσβαση τους για να αποκτήσουν περισσότερα δικαιώματα σε σημεία του συστήματος που δεν έχουν πρόσβαση. Για την εξασφάλιση της χρήσης των αγαθών από εξουσιοδοτημένους χρήστες, υπάρχουν τέσσερα ζητούμενα στα πλαίσια της πολιτικής ασφαλείας:

- **Αυθεντικότητα (authentication):** Η απόδειξη της ταυτότητας του χρήστη προκειμένου να του επιτραπεί η πρόσβαση στα αγαθά που παρέχει το σύστημα. Ένας γνωστός τρόπος είναι η χρήση του συνδυασμού ονόματος χρήστη/κωδικού πρόσβασης (username/password).
- **Ακεραιότητα (integrity):** Η διασφάλιση ότι τα δεδομένα δεν έχουν αλλοιωθεί ή ότι η όποια μεταβολή τους έχει επέλθει μόνο από εξουσιοδοτημένα άτομα.
- **Εμπιστευτικότητα (confidentiality):** Ο περιορισμός της πρόσβασης στα δεδομένα μόνο σε άτομα που επιτρέπεται να έχουν πρόσβαση σε αυτά.
- **Μη άρνηση ταυτότητας (non-repudiation):** Η δυνατότητα απόδοσης πράξεων (ευθυνών) σε κάποιο συγκεκριμένο χρήστη. Πολύ απλά, η δυνατότητα να δούμε ποιος έκανε οποιαδήποτε αλλαγή στο σύστημα.

Από τα τέσσερα παραπάνω μπορούμε ακόμα να ορίσουμε:

- **Εγκυρότητα (validity):** Την απόλυτη ακρίβεια και πληρότητα μιας πληροφορίας. Η εγκυρότητα είναι συνδυασμός της *Ακεραιότητας* και της *Αυθεντικότητας*.

- **Διαθεσιμότητα Πληροφοριών (Information Availability):** Την αποφυγή προσωρινής ή μόνιμης απώλειας πρόσβασης στις πληροφορίες από εξουσιοδοτημένους χρήστες. Σε κάποιες περιπτώσεις, οι χρήστες μπορεί να πληρώσουν κάποιο αντίτιμο για να έχουν πρόσβαση στις πληροφορίες που παρέχει το σύστημα μας. Είναι απαραίτητο να εξασφαλίσουμε ότι η πρόσβαση σε αυτές τις πληροφορίες θα είναι αδιάλειπτη.

Μπορούμε τώρα να δώσουμε και τους παρακάτω ορισμούς:

- **Ασφάλεια (security):** Η προστασία της *Διαθεσιμότητας, Ακεραιότητας και Εμπιστευτικότητας* των πληροφοριών.
- **Ασφάλεια Πληροφοριών (information security):** Ο συνδυασμός της *Εμπιστευτικότητας, Εγκυρότητας και Διαθεσιμότητας Πληροφοριών*.
- **Παραβίαση Ασφαλείας (security violation):** Η παραβίαση ενός ή περισσότερων από τις παραπάνω ιδιότητες, όπως διαθεσιμότητα, εμπιστευτικότητα και εγκυρότητα.

Γενικά ένα πληροφοριακό σύστημα είναι εκτεθειμένο σε κινδύνους. Οι κίνδυνοι μπορούν να διαχωριστούν σε *απειλές* και *αδυναμίες*.

Με τον όρο “απειλές” (threats) αναφερόμαστε σε ενέργειες ή γεγονότα που μπορούν οδηγήσουν στην κατάρρευση κάποιου από τα χαρακτηριστικά ασφαλείας που ορίσαμε προηγουμένως. Οι απειλές μπορεί να οφείλονται σε τυχαία ή φυσικά γεγονότα (πυρκαγιά, πλημμύρα κλπ) ή σε ανθρώπινες ενέργειες (σκόπιμες ή μη).

Με τον όρο “αδυναμίες” (vulnerabilities) αναφερόμαστε σε σημεία του πληροφοριακού συστήματος τα οποία (ενδεχομένως λόγω κακού σχεδιασμού ή υλοποίησης) αφήνουν περιθώρια για παραβιάσεις. Σε πολλές περιπτώσεις οι αδυναμίες οφείλονται σε λάθη του λογισμικού ή σε ανεπαρκή παραμετροποίηση του από το προσωπικό που το εγκατέστησε και το συντηρεί.

Πριν προχωρήσουμε στη λήψη μέτρων ασφαλείας, θα πρέπει να εκτιμήσουμε και να υπολογίσουμε διάφορους παράγοντες. Θα πρέπει αρχικά να αξιολογήσουμε ποια είναι τα αγαθά που χρήζουν προστασίας και να εντοπίσουμε τους πιθανούς κινδύνους από τους οποίους θα πρέπει να προστατευθούν. Έπειτα θα πρέπει να προχωρήσουμε σε ένα αρχικό σχεδιασμό της αρχιτεκτονικής ασφαλείας που θα ακολουθήσουμε και να εκτιμήσουμε το κόστος του. Το συνολικό κόστος πρέπει να περιλαμβάνει το κόστος αγοράς εξοπλισμού και λογισμικού που θα χρησιμοποιήσουμε, το κόστος εγκατάστασης του από κατάλληλο προσωπικό, αλλά και το μόνιμο λειτουργικό κόστος που θα έχει η συντήρηση και αναβάθμιση του.

Αν το κόστος που υπολογίσουμε υπερβαίνει τα προβλεπόμενα όρια, θα πρέπει να κάνουμε κάποιες νέες παραδοχές ή συμβιβασμούς σχετικά με το τι προβλήματα ασφαλείας και σε τι βαθμό θα καλύπτει η πολιτική ασφαλείας. Με τον τρόπο αυτό

αποδεχόμαστε τους εναπομείναντες κινδύνους που δεν καλύπτονται από την τελική πολιτική ασφαλείας.

Στις επόμενες ενότητες θα εξετάσουμε τις τεχνικές μεθόδους που χρησιμοποιούνται για την επίτευξη των παραβιάσεων, αλλά και τα αντίμετρα που μπορούμε να υλοποιήσουμε για να προστατέψουμε ένα πληροφοριακό σύστημα.

### 8.3.2 Επεξήγηση Ορολογίας

Πριν προχωρήσουμε στις διάφορες τεχνικές ασφαλείας και μεθόδους παραβίασης, θα κάνουμε μια σύντομη αναφορά στην ορολογία που χρησιμοποιείται. Κάποιοι από τους όρους που θα παρουσιάσουμε εδώ, εξηγούνται καλύτερα παρακάτω σε συνδυασμό με τον αντίστοιχο τρόπο χρήση τους.

Οι πιο βασικοί όροι σε θέματα ασφαλείας πληροφοριακών συστημάτων είναι οι παρακάτω:

- **Κρυπτογράφηση (Encryption):** Η κρυπτογράφηση είναι η διαδικασία με την οποία μετατρέπονται τα αρχικά δεδομένα (γνωστά και ως *plaintext*) σε μορφή (κρυπτόγραμμα) η οποία δεν μπορεί πλέον να γίνει κατανοητή χωρίς να αποκρυπτογραφηθεί. Η κρυπτογράφηση γίνεται με τη βοήθεια αλγορίθμου, το αποτέλεσμα του οποίου μπορεί να αντιστραφεί ώστε να παράγει ξανά τα αρχικά δεδομένα εισόδου. Για την κρυπτογράφηση και την αποκρυπτογράφηση χρησιμοποιείται το κλειδί.
- **Αποκρυπτογράφηση (Decryption):** Προφανώς η αντίστροφη διαδικασία της κρυπτογράφησης. Ο αλγόριθμος δέχεται ως είσοδο τα κρυπτογραφημένα δεδομένα (κρυπτόγραμμα) και με τη βοήθεια του κλειδιού (το οποίο προφανώς είναι διαθέσιμο μόνο σε εξουσιοδοτημένα άτομα) τα μετατρέπει ξανά στα κανονικά δεδομένα. Τα δεδομένα πλέον δεν είναι κωδικοποιημένα και μπορούν να χρησιμοποιηθούν κανονικά.
- **Κλειδί (Key):** Στο πεδίο της κρυπτογράφησης, το κλειδί είναι ένας ψηφιακός κωδικός (ένας αριθμός από bits) ο οποίος χρησιμοποιείται για την κρυπτογράφηση και αποκρυπτογράφηση της πληροφορίας. Προφανώς το κλειδί φυλάσσεται σε ασφαλές μέρος και είναι διαθέσιμο μόνο στα μέρη που επιτρέπεται να έχουν πρόσβαση στα δεδομένα.
- **Δημόσιο Κλειδί (Public Key):** Στην *ασυμμετρική* κρυπτογράφηση, χρησιμοποιούνται για κάθε χρήστη δύο κλειδιά, το δημόσιο και το ιδιωτικό. Η βασική ιδέα είναι ότι το δημόσιο το γνωρίζει καθένας, ενώ το ιδιωτικό μόνο ο χρήστης. Το δημόσιο κλειδί χρησιμοποιείται για να “κλειδώσει” (κρυπτογραφεί) ενώ το ιδιωτικό ξεκλειδώνει. Όποιος θέλει να μας στείλει κρυπτογραφημένα δεδομένα, χρησιμοποιεί το δημόσιο μας κλειδί για να τα κλειδώσει.

Μετά από αυτό η αποκρυπτογράφηση γίνεται μόνο με το δικό μας ιδιωτικό κλειδί. Γενικά η ασυμμετρική κρυπτογράφηση θεωρείται πιο ασφαλής από τη συμμετρική, καθώς δεν γνωρίζει κανείς άλλο το ιδιωτικό μας κλειδί. (Στη συμμετρική κρυπτογράφηση χρησιμοποιείται το ίδιο κλειδί και για τις δύο λειτουργίες, άρα πρέπει να το έχουν και τα δύο μέρη της επικοινωνίας)

- **Ιδιωτικό Κλειδί (Private Key):** Το ιδιωτικό κλειδί χρησιμοποιείται στην ασυμμετρική κρυπτογράφηση για να αποκρυπτογραφεί και να υπογράψει δεδομένα. ΠΡΟΣΟΧΗ: το σχολικό βιβλίο γράφει λανθασμένα ότι το ιδιωτικό κλειδί κρυπτογραφεί και ελέγχει υπογραφές - αυτά τα κάνει το δημόσιο κλειδί. Το ιδιωτικό κλειδί συνδυάζεται πάντα (σαν ζεύγος) με ένα αντίστοιχο δημόσιο. Η πλήρης διαδικασία εξηγείται σε επόμενη ενότητα.
- **Μυστικό Κλειδί (Secret Key):** Ψηφιακός κωδικός που είναι γνωστός και στα δύο μέρη προκειμένου να τον χρησιμοποιήσουν σε ανταλλαγή δεδομένων με χρήση κρυπτογράφησης / αποκρυπτογράφησης.
- **Λειτουργία (Συνάρτηση) Κατατεμαχισμού (Hash Function):** Μαθηματική συνάρτηση της οποίας η έξοδος δεν μπορεί με αντιστροφή (με κανένα τρόπο) να μας παράγει την αρχική είσοδο. Προφανώς δεν μπορεί να χρησιμοποιηθεί για κρυπτογράφηση, καθώς δεν μπορούμε μετά να αποκρυπτογραφήσουμε το κείμενο, αλλά χρησιμοποιείται για την παραγωγή συνόψεων (digests).
- **Σύνοψη Μηνύματος (Message Digest):** Η σύνοψη ενός μηνύματος είναι το αποτέλεσμα (έξοδος) της συνάρτησης κατατεμαχισμού. Η σύνοψη δεν έχει το ίδιο μέγεθος (είναι συνήθως μικρότερη) με το αρχικό μήνυμα – κάτι το οποίο έχει νόημα, γιατί όπως εξηγήσαμε δεν μπορούμε έτσι και αλλιώς να ξαναγυρίσουμε στο αρχικό μήνυμα. Οι αλγόριθμοι κατατεμαχισμού είναι φτιαγμένοι με τέτοιο τρόπο ώστε μια μικρή μεταβολή στα δεδομένα εισόδου (π.χ. ένα μόνο γράμμα ή ακόμα και ένα μόνο bit) να προκαλεί ολοκληρωτική αλλαγή στην έξοδο (πλήρης αλλαγή της σύνοψης). Για το λόγο αυτό η σύνοψη χρησιμοποιείται πολύ συχνά για να ελέγξουμε την ακεραιότητα κάποιου αρχείου που κατεβάσαμε π.χ. από το Internet. Σε μεγάλα downloads, μπορούμε συνήθως να κατεβάσουμε και ένα αρχείο CHECKSUM (αθροίσματος ελέγχου) που περιέχει μέσα την σύνοψη του μεγάλου αρχείου. Εκτελώντας τη συνάρτηση κατατεμαχισμού στο δικό μας μηχάνημα, μπορούμε να συγκρίνουμε τις συνόψεις: αν είναι ίδιες το αρχείο έχει κατέβει σωστά.
- **Ψηφιακή Υπογραφή (Digital Signature):** Η ψηφιακή υπογραφή είναι τυπικά ένας αριθμός από bit που προστίθεται στο τέλος κάποιου αρχείου και εξασφαλίζει την αυθεντικότητα (“το έστειλε πράγματι ο χρήστης Α”) και την ακεραιότητα (“το έχουμε λάβει σωστά”) ενός μηνύματος.

### 8.3.3 Μέθοδοι Παραβίασης

Σε κάθε δίκτυο υπολογιστών μπορεί να υπάρχουν εμπιστευτικές πληροφορίες. Τυπικά, αυτές θα είναι αποθηκευμένες σε διάφορα αποθηκευτικά μέσα (σκληροί δίσκοι κλπ) ενώ κατά τη διάρκεια της επεξεργασίας τους θα βρίσκονται και στην κύρια μνήμη (RAM) των υπολογιστών. Οι πληροφορίες μεταδίδονται επίσης στο δίκτυο με τη μορφή πακέτων. Η ύπαρξη πληροφοριών σε αυτές τις καταστάσεις μπορεί να απειληθεί με διάφορους τρόπους από ενέργειες χρηστών, τόσο του εσωτερικού δικτύου, όσο και του Internet (εφόσον υπάρχει σύνδεση σε αυτό). Στην ενότητα αυτή θα αναφερθούμε στους συνηθισμένους τρόπους επιθέσεων που χρησιμοποιούνται για την παραβίαση της ασφάλειας ενός δικτύου υπολογιστών.

#### Επιθέσεις στους Κωδικούς Πρόσβασης (Password Attacks)

Οι κωδικοί πρόσβασης είναι ένας από τους πλέον συνηθισμένους μεθόδους ελέγχου πρόσβασης σε υπολογιστικά συστήματα. Γενικά υπάρχουν δύο είδη κωδικών:

- **Τα επαναχρησιμοποιούμενα passwords:** Πρόκειται για τον πλέον συνηθισμένο τύπο κωδικού πρόσβασης. Μπορεί να χρησιμοποιηθεί πολλές φορές για την εξακρίβωση των στοιχείων του χρήστη.
- **Τα passwords μια χρήσης, OTP (One Time Password):** Τα passwords αυτά αλλάζουν συνεχώς, καθένα είναι έγκυρο για μια και μοναδική χρήση.

Στα περισσότερα είδη λειτουργικών συστημάτων, όπως το UNIX και τα Windows, υποστηρίζεται η χρήση επαναχρησιμοποιούμενων κωδικών πρόσβασης. (Στο UNIX υποστηρίζονται και τα OTP, αλλά το βιβλίο σας ντρέπεται να το πει).

Με την εξέλιξη της τεχνολογίας (αλλά και με την άνοδο των τεχνικών “ψαρέματος” των χρηστών) η προστασία ενός υπολογιστικού συστήματος μόνο με τη χρήση κωδικών (και ειδικά επαναχρησιμοποιούμενων) θεωρείται πολύ ασθενής.

Για την παραβίαση κωδικών πρόσβασης υπάρχουν προγράμματα που σε μικρό χρονικό διάστημα μπορούν να δοκιμάσουν πολύ μεγάλο συνδυασμό χαρακτήρων και γραμμάτων (brute force attack). Ένας άλλος τρόπος παραβίασης είναι η παρακολούθηση των πλήκτρων (key stroke monitoring) με τη βοήθεια κάποιου προγράμματος (keylogger) που καταγράφει τα πλήκτρα που πιέζονται, ενδεχομένως σε κάποιο αρχείο. Προφανώς το πρόγραμμα αυτό πρέπει να εγκατασταθεί εν αγνοία του αρχικού χρήστη του συστήματος. Με την ανάλυση των στοιχείων που έχουν καταγραφεί στο αρχείο, μπορεί να αποκαλυφθεί ο κωδικός πρόσβασης (και ενδεχομένως και άλλες εμπιστευτικές πληροφορίες, π.χ. αριθμοί πιστωτικών καρτών κλπ).

Ένας άλλος ιδιαίτερα συνηθισμένος στις μέρες μας τρόπος ανάκτησης κωδικών πρόσβασης αναφέρεται ως *social engineering* και επικεντρώνει στην παραπλάνηση των

χρηστών για την απόκτηση πληροφοριών. Για παράδειγμα, φανταστείτε ότι σας καλεί στο τηλέφωνο κάποιος που υποτίθεται ότι ανήκει στο τεχνικό τμήμα του παροχέα σας υπηρεσιών Internet (ISP) και σας ζητάει να του δώσετε τον κωδικό σας γιατί θέλουν να κάνουν κάποιες αλλαγές ρυθμίσεων στα συστήματά τους. Πάρα πολλοί χρήστες το πιστεύουν αυτό και πραγματικά δίνουν τους κωδικούς τους. Γιατί άραγε ένας τεχνικός του ISP σας να θέλει τον κωδικό σας; Ο διαχειριστής ενός συστήματος έχει πλήρη πρόσβαση σε όλα τα στοιχεία και τους λογαριασμούς και δεν χρειάζεται ποτέ κανένα κωδικό χρήστη! Στην ίδια κατηγορία εντάσσεται και η δυνατότητα να δούμε τυχαία (*shoulder surfing*) τον κωδικό πρόσβασης ενός χρήστη την ώρα που τον πληκτρολογεί (αρκεί να περνάμε δίπλα του εκείνη τη στιγμή).

Υπάρχει προφανώς η πιθανότητα απόκτησης ενός κωδικού πρόσβασης και με τη χρήση φυσικής βίας. Οι περιπτώσεις φυσικής βίας μπορούν να ενταχθούν σε δύο κατηγορίες: στην εξωτερική και στην εσωτερική βία. Είναι προφανές ότι με την εξωτερική βία, ο χρήστης του οποίου απειλείται η σωματική ακεραιότητα θα αποκαλύψει ενδεχομένως τον κωδικό του. Με την εσωτερική βία, αναφερόμαστε στην περίπτωση όπου κάποιος αντιγράφει (νόμιμα ή παράνομα) κρυπτογραφημένα passwords και στη συνέχεια χρησιμοποιεί κάποιο πρόγραμμα *crack* για να προσπαθήσει να τα αποκρυπτογραφήσει.

---

Οι κωδικοί πρόσβασης δεν αποθηκεύονται απευθείας σε ένα σύστημα. Αντίθετα, περνούν από λειτουργία κατατεμαχισμού και αποθηκεύεται η σύνοψη τους (*digest*). Για τον έλεγχο έπειτα του κωδικού που εισάγει ο χρήστης, γίνεται ξανά η ίδια διαδικασία: παράγεται το *digest* και συγκρίνεται με το αποθηκευμένο. Αν είναι ίδιο, ο κωδικός που δίνει ο χρήστης είναι ο σωστός. Από τα παραπάνω, μπορούμε να αντιληφθούμε ότι δεν είναι δυνατόν να πάρουμε με κάποιο τρόπο τον αρχικό κωδικό με αποκρυπτογράφηση του αποθηκευμένου, καθώς έχει προέλθει από λειτουργία κατατεμαχισμού (που δεν αντιστρέφεται).

Ένα πρόγραμμα τύπου *crack* χρησιμοποιεί μια απλή μέθοδο: αν έχουμε αποκτήσει τα *digests* των κωδικών πρόσβασης (γνωστά και ως *hashes*) και γνωρίζουμε τον αλγόριθμο κατατεμαχισμού που έχει χρησιμοποιηθεί για την παραγωγή τους, μπορούμε να αρχίζουμε να δοκιμάζουμε τυχαίους συνδυασμούς γραμμάτων, μέχρι να παράγουμε το ίδιο *digest*. Τότε θα έχουμε βρει τον κωδικό πρόσβασης. Η μέθοδος αυτή είναι γνωστή ως *brute force attack*.

Τα πράγματα γίνονται πιο εύκολα αν αναλογιστούμε ότι οι περισσότεροι χρήστες (για ευκολία τους) χρησιμοποιούν μάλλον απλές λέξεις ως κωδικούς πρόσβασης. Έτσι, αντί να ψάχνουμε τυχαία γράμματα μπορούμε να ψάχνουμε για λέξεις. Τα περισσότερα προγράμματα *crack* διαθέτουν ένα λεξικό αγγλικών (συνήθως) λέξεων τις οποίες δοκιμάζουν. Ένα γνωστό τέτοιο πρόγραμμα για UNIX είναι το *Jack the Ripper*, το οποίο χρησιμοποιούν και οι διαχειριστές για να ελέγξουν αν ο κωδικός

κάποιου χρήστη είναι “ασθενής”.

Να σημειώσουμε βέβαια ότι πρόσβαση στο αρχείο των κρυπτογραφημένων κωδικών σε ένα UNIX σύστημα έχει μόνο ο διαχειριστής (root) και τα προγράμματα που εξασφαλίζουν την είσοδο των χρηστών και την αλλαγή των κωδικών (login και passwd αντίστοιχα). Αν το αρχείο αυτό έχει πέσει στα χέρια κάποιου άλλου, τα προβλήματα μας είναι συνήθως πολύ πιο σοβαρά από την απλή παραβίαση κωδικών...

### Παρακολούθηση Δικτύου (Network Monitoring ή Network Packet Sniffing)

Όπως είναι γνωστό, τα δεδομένα μέσα σε ένα δίκτυο μεταφέρονται μεταξύ υπολογιστών με τη μορφή πακέτων. Σε αρκετές εφαρμογές (για παράδειγμα το telnet και το ftp για τα οποία έχουμε ήδη μιλήσει), τα δεδομένα αλλά και οι ίδιοι οι κωδικοί πρόσβασης μεταφέρονται με μορφή απλού κειμένου, χωρίς κανένα είδος κρυπτογράφησης (clear text). Είναι φανερό, ότι κάποιος με τα κατάλληλα τεχνικά μέσα και γνώσεις μπορεί να λάβει τα πακέτα, να τα συναρμολογήσει και να παράγει έτσι το σύνολο των πληροφοριών που παρέχονται σε αυτά, συμπεριλαμβανομένων και τυχόν κωδικών.

Τα προγράμματα που κάνουν ανίχνευση πακέτων (packet sniffing) χρησιμοποιούν την κάρτα δικτύου του υπολογιστή σε κατάσταση λειτουργίας promiscuous. Στο promiscuous mode η κάρτα δικτύου λαμβάνει όλα τα πακέτα που κυκλοφορούν στο δίκτυο, και όχι μόνο αυτά που απευθύνονται σε αυτήν. Τα προγράμματα για packet sniffing μπορούν να χρησιμοποιηθούν για επίλυση προβλημάτων δικτύου από τους διαχειριστές συστημάτων, αλλά αποτελούν και ένα πολύ ισχυρό εργαλείο για επίδοξους εισβολείς. Τα προγράμματα αυτά μπορούν να συλλέξουν εμπιστευτικές πληροφορίες την ώρα που διέρχονται μέσα από τις γραμμές του δικτύου και πιθανόν και κωδικούς που μεταδίδονται σε μορφή κειμένου. Η αποκάλυψη passwords με αυτό τον τρόπο είναι γνωστή και ως επίθεση *Man-in-the-Middle*. Είναι φανερό ότι η παρακολούθηση δικτύου μπορεί να χρησιμοποιηθεί και για την παραβίαση κωδικών πρόσβασης.

### Μεταμφίηση (Masquerade)

Η επίθεση με μεταμφίηση παρατηρείται όταν ο επιτιθέμενος που βρίσκεται σε δίκτυο έξω από το δικό μας, προσποιείται ότι βρίσκεται στο δικό μας. Ειδικά για τα πρωτόκολλα TCP/IP, το παραπάνω είναι γνωστό και ως *IP Spoofing* καθώς ο επιτιθέμενος αλλάζει την διεύθυνση IP των πακέτων του ώστε να φαίνεται ότι προέρχονται από το εσωτερικό μας δίκτυο (ότι ανήκουν δηλ. στο εύρος των δικών μας IP διευθύνσεων). Η μέθοδος αυτή χρησιμοποιείται κυρίως για να ξεγελάσει ο επιτιθέμενος το

firewall που συνδέει το εσωτερικό μας δίκτυο με τον έξω κόσμο (το Internet ή γενικά με δίκτυο που δεν θεωρείται έμπιστο (trusted)). Τυπικά, το IP spoofing περιορίζεται στο να εισάγει δεδομένα ή εντολές σε υπάρχον πακέτο δεδομένων σε επικοινωνίες τύπου client – server ή σημείου προς σημείο (point to point).

Για να είναι δυνατή η αμφίδρομη επικοινωνία (τη στιγμή που η διεύθυνση αφετηρίας δεν είναι η πραγματική του εισβολέα), θα πρέπει ο εισβολέας να έχει αλλάξει κατάλληλα τους πίνακες δρομολόγησης που δείχνουν προς τη διεύθυνση που έχει προσποιηθεί ότι βρίσκεται, ώστε να κατευθύνουν τα δεδομένα προς την πραγματική του διεύθυνση. Έτσι θα λαμβάνει όλα τα πακέτα που κατευθύνονται προς την “ψεύτικη” διεύθυνση. Στην περίπτωση αυτή, ενδέχεται να λάβει και πακέτα που περιέχουν κωδικούς πρόσβασης. Μπορεί επίσης να στέλνει emails προς το εσωτερικό μας δίκτυο, στους πελάτες ή τους συνεργάτες μας και να χρησιμοποιήσει τεχνικές social engineering που αναφέραμε προηγουμένως για να ανακτήσει κωδικούς.

### **Αρνηση Παροχής Υπηρεσίας (Denial of Service)**

Αυτή η κατηγορία επιθέσεων διαφοροποιείται από αυτές που έχουμε περιγράψει ως τώρα, καθώς δεν προσπαθεί να αποσπάσει τους κωδικούς από το δίκτυο μας, αλλά έχει ως στόχο την *διαθεσιμότητα* των δεδομένων μας. Σκοπός μιας τέτοιας επίθεσης είναι να φτάσει το δικτυακό εξοπλισμό (ή την υπολογιστική ισχύ) στα όρια, ώστε να μην μπορούν να εξυπηρετηθούν πλέον οι νόμιμοι χρήστες του δικτύου. Η επίθεση γίνεται συνήθως με εξάντληση των ορίων των πόρων του δικτύου (π.χ. μέγιστος αριθμός πακέτων ανά δευτερόλεπτο που μπορεί να αντέξει το δίκτυο μας, μέγιστος αριθμός πακέτων ανά δευτερόλεπτο σε κάποιο δρομολογητή ή και μέγιστος αριθμός διεργασιών κάποιου εξυπηρετητή κλπ).

Οι επιθέσεις του παραπάνω τύπου είναι διαδεδομένες ειδικά σε γνωστά και μεγάλα sites στο Internet (Yahoo, CNN, twitter κλπ). Επειδή δεν είναι γενικά δυνατόν να παράγονται και να αποστέλλονται όλα αυτά τα πακέτα της επίθεσης από ένα μόνο υπολογιστή, τυπικά χρησιμοποιούνται μηχανήματα γνωστά ως *zombies* που ανήκουν σε κάποιο *botnet*.

---

**Σημείωση:** Ένας υπολογιστής που έχει μολυνθεί με κατάλληλο κακόβουλο πρόγραμμα (malware) μπορεί να δίνει τη δυνατότητα σε κάποιον να τον κατευθύνει από μακριά. Ένας τέτοιος υπολογιστής ονομάζεται *zombie*. Πολλοί υπολογιστές που έχουν μολυνθεί από το ίδιο πρόγραμμα και τους χειρίζεται το ίδιο άτομο ταυτόχρονα, αποτελούν ένα *botnet*. Ο “χειριστής” του botnet μπορεί να στείλει εντολή σε όλα τα *zombies* που το αποτελούν να αρχίσουν να στέλνουν πακέτα προς μια συγκεκριμένη διεύθυνση δικτύου, δημιουργώντας έτσι μια επίθεση τύπου Denial Of Service. Μάλιστα, επειδή η επίθεση αυτή δεν προέρχεται από ένα μόνο μηχάνημα και διεύ-

θυση IP (ένα botnet μπορεί να περιέχει υπολογιστές σε κάθε σημείο του κόσμου), ονομάζεται καταναμημένη (Distributed Denial of Service Attack, ή DDOS) και είναι αρκετά πιο δύσκολο να αντιμετωπιστεί από το απλό Denial of Service.

Σε σχέση με τις άλλες επιθέσεις που αναφέραμε, οι τεχνικές τύπου Denial of Service δεν απαιτούν ειδικές γνώσεις. Είναι πάντως πιο αποτελεσματικές αν υπάρχει γνώση της εσωτερικής δομής του δικτύου στο οποίο πρόκειται να γίνει η επίθεση.

### Επιθέσεις στο Επίπεδο Εφαρμογών (Application-Layer Attacks)

Ορισμένες εφαρμογές όπως το HTTP, ActiveX, Telnet, FTP κλπ. παρουσιάζουν αδυναμίες σε συγκεκριμένα σημεία της ασφάλειας τους, που οφείλονται πολλές φορές σε αδυναμίες στον κώδικα τους (γνωστές και ως τρύπες, holes). Οι γνώστες αυτών των αδυναμιών μπορούν να τις εκμεταλλευθούν για να αποκτήσουν πρόσβαση στο σύστημα με απώτερο σκοπό τη δημιουργία προβλημάτων ή τη συλλογή πληροφοριών.

### 8.3.4 Τεχνικές Ασφάλειας

Ο τομέας της ασφάλειας δεδομένων σε καταναμημένα πληροφοριακά συστήματα είναι από τους πιο ραγδαία αναπτυσσόμενους σήμερα, με συνεχή παρουσίαση νέων τεχνολογιών και προϊόντων σε θέματα ασφάλειας από διάφορες εταιρίες. Στην ενότητα αυτή θα παρουσιάσουμε κάποιες βασικές τεχνικές ασφάλειας πληροφοριών που χρησιμοποιούνται σε σύγχρονα δίκτυα.

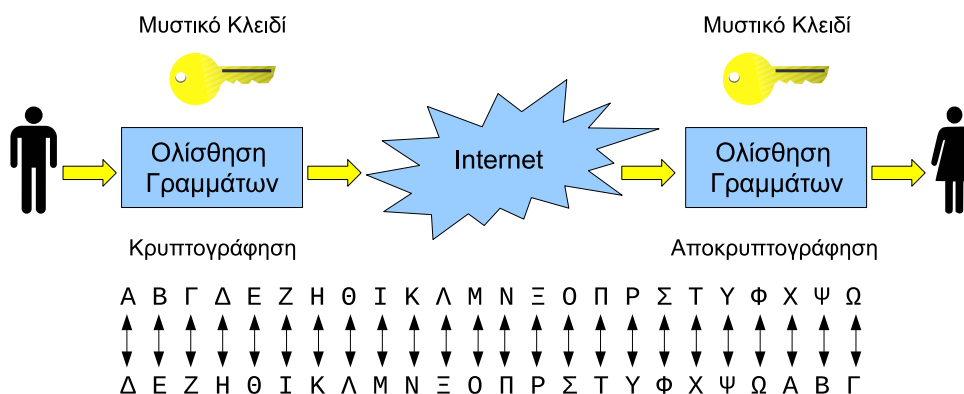
#### Συμμετρική Κρυπτογράφηση

Η συμμετρική κρυπτογράφηση (ή κρυπτογράφηση συμμετρικού κλειδιού όπως αναφέρεται συχνά) αποτελεί μια μέθοδο για την εξασφάλιση της εμπιστευτικότητας κατά τη μετάδοση πληροφοριών πάνω από ένα κανάλι επικοινωνίας.

Ας υποθέσουμε ότι έχουμε δύο χρήστες A και B που θέλουν να επικοινωνήσουν μεταξύ τους με ασφάλεια. Η κρυπτογράφηση που περιγράφουμε ονομάζεται συμμετρική επειδή χρησιμοποιείται το ίδιο ακριβώς κλειδί τόσο για την κρυπτογράφηση (παραγωγή του κρυπτογραφημένου μηνύματος από το απλό κείμενο εισόδου) όσο και για την αποκρυπτογράφηση (εξαγωγή του αρχικού μηνύματος από το κρυπτογραφημένο). Προφανώς, για να είναι εφικτή η επικοινωνία του A με τον B, θα πρέπει:

- Να χρησιμοποιούν και οι δύο το ίδιο κλειδί, το οποίο πρέπει να έχουν από πριν συμφωνήσει (και για το οποίο είναι βέβαιοι ότι δεν το έχει υποκλέψει και κάποιος τρίτος).
- Να έχουν συμφωνήσει σε ένα κοινό αλγόριθμο κρυπτογράφησης.

Ένας απλοϊκός αλγόριθμος κρυπτογράφησης, είναι ο Caesar Cipher που φαίνεται στο σχήμα 8.5. Στον αλγόριθμο αυτό, γίνεται αντικατάσταση κάθε γράμματος του



Σχήμα 8.5: Επικοινωνία με χρήση συμμετρικής κρυπτογράφησης

μηνύματος με ένα άλλο που βρίσκεται μερικές θέσεις πιο κάτω στο αλφάβητο. Για παράδειγμα, μπορούμε να συμφωνήσουμε ότι θα μετακινούμε κάθε γράμμα κατά τρεις θέσεις, έτσι για παράδειγμα το A γίνεται Δ, το B γίνεται E κ.ο.κ. Προφανώς εδώ το κλειδί είναι στην πραγματικότητα το πόσες θέσεις έχουμε κάνει τη μετακίνηση. Ο αλγόριθμος ολισθαίνει τα γράμματα δεξιά όταν γίνεται κρυπτογράφηση και αριστερά (πάντα τον ίδιο αριθμό από θέσεις) όταν γίνεται αποκρυπτογράφηση. Καθώς ο αλγόριθμος δεν είναι σύνθετος, είναι πολύ εύκολο να γίνει αποκρυπτογράφηση ακόμα και αν δεν διαθέτουμε το κλειδί: με ένα υπολογιστή είναι πολύ εύκολο να δοκιμάσουμε όλες τις πιθανές τιμές θέσεων, μέχρι να βρούμε κάποια που το αποκρυπτογραφημένο κείμενο να βγάζει νόημα. Οι πιθανές θέσεις είναι πολύ λίγες (θεωρώντας κεφαλαία ελληνικά, μόνο 24) και έτσι δεν έχει νόημα να χρησιμοποιήσουμε πρακτικά πουθενά αυτό τον αλγόριθμο.

Υπάρχουν προγράμματα που προσπαθούν – με διάφορες μεθόδους – να αποκρυπτογραφήσουν μηνύματα δοκιμάζοντας διάφορους αλγόριθμους ώστε να ανακτήσουν το μήνυμα χωρίς να διαθέτουν το κλειδί. Εάν ο αλγόριθμος είναι πολύπλοκος, το σπάσιμο του (ακόμα και σε μηχανήματα με τεράστια υπολογιστική ισχύ) μπορεί να διαρκέσει πάρα πολύ χρόνο (χρόνια ως και αιώνες ακόμα!) σε σημείο που ακόμα και αν τελικά επιτευχθεί να μην προστατεύει πλέον κάποια πληροφορία με αξία.

Έχουν αναπτυχθεί πολλοί αλγόριθμοι κρυπτογράφησης που βασίζονται σε πολύπλοκα μαθηματικά μοντέλα και σύνθετη λογική. Ορισμένοι από αυτούς δεν είναι καν τεκμηριωμένοι, ενώ άλλοι φυλάσσονται ως κρατικά μυστικά και η εξαγωγή τους σε τρίτες χώρες απαγορεύεται. Μάλιστα, αν χρησιμοποιούνται σε προϊόντα εταιριών, η εξαγωγή της πλήρους έκδοσης τους σε άλλες χώρες μπορεί να γίνεται μόνο μετά από χορήγηση σχετικής άδειας.

---

**Σημείωση:** Άσχετα με αυτά που γράφει το βιβλίο σας παραπάνω, έχει αποδειχθεί και είναι πλέον κοινά αποδεκτό ότι οι μόνοι αλγόριθμοι κρυπτογράφησης που παρέχουν αρκετή ασφάλεια είναι οι ανοικτού κώδικα. Σε αυτούς καθένας μπορεί να δει πως λειτουργούν και να τους βελτιώσει ή να βρει τυχόν προβλήματα που μπορούν να οδηγήσουν σε ασθενή κρυπτογράφηση. Για το λόγο αυτό η βελτίωση τους είναι συνεχής. Αντίθετα οι περισσότεροι κλειδωμένοι και κρυφοί αλγόριθμοι έχουν σπάσει: CSS (κρυπτογράφηση ταινιών DVD), A5/1 (κρυπτογράφηση δεδομένων φωνής σε κινητά τηλέφωνα GSM), κρυπτογράφηση Blue-Ray κλπ.

---

Μερικοί από τους πιο διαδεδομένους αλγόριθμους κρυπτογράφησης είναι:

- DES, Data Encryption Standard, Πρότυπο Κρυπτογράφησης Δεδομένων
- 3DES, Triple DES
- IDEA, International Data Encryption Algorithm, Διεθνής Αλγόριθμος Κρυπτογράφησης Δεδομένων.

Οι παραπάνω αλγόριθμοι δέχονται ως είσοδο μηνύματα μεγέθους 64 bits. Αν το μήνυμα είναι μεγαλύτερο από 64 bits, θα πρέπει να σπάσει σε κομμάτια των 64 bits.

Όπως αναφέραμε, η συμμετρική κρυπτογράφηση προσφέρει κυρίως εμπιστευτικότητα στην επικοινωνία. Αν και μπορεί να χρησιμοποιηθεί και για την εξασφάλιση της αυθεντικότητας και της ακεραιότητας, υπάρχουν αρκετά καλύτερες τεχνικές για αυτούς τους σκοπούς. Συγκεκριμένα, η συμμετρική κρυπτογράφηση έχει το σημαντικό μειονέκτημα ότι πρέπει με κάποιο ασφαλές τρόπο να γνωστοποιήσουμε το κλειδί στην άλλη μεριά προκειμένου να αποκρυπτογραφήσει το μήνυμα. Προφανώς, δεν μπορούμε να χρησιμοποιήσουμε για αυτό το σκοπό κάποιο μη-έμπιστο μέσο (π.χ. το Διαδίκτυο) γιατί υπάρχει κίνδυνος υποκλοπής του. Ωστόσο γίνονται κάποιες προσπάθειες και σε αυτό τον τομέα: για παράδειγμα, ο αλγόριθμος Diffie Hellman επιτρέπει τη διανομή ενός συμμετρικού κλειδιού με ασφάλεια σε κάποιο απομακρυσμένο παραλήπτη, ακόμα και μέσω του Διαδικτύου.

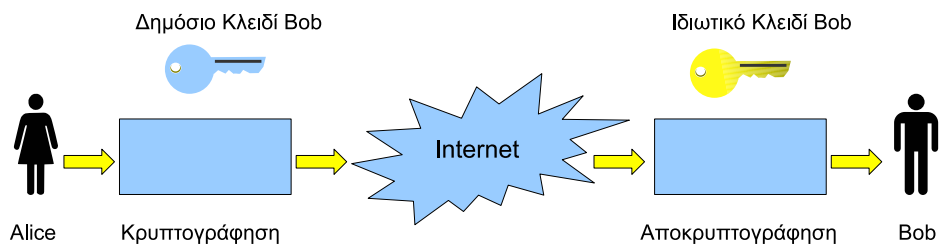
## Ασυμμετρική Κρυπτογράφηση

Η ασυμμετρική κρυπτογράφηση ονομάζεται συχνά και κρυπτογράφηση δημόσιου κλειδιού. Σε αντίθεση με την συμμετρική κρυπτογράφηση που περιγράψαμε προηγουμένως, η ασυμμετρική χρησιμοποιεί διαφορετικά κλειδιά για την κρυπτογράφηση και την αποκρυπτογράφηση – για το λόγο αυτό άλλωστε ονομάζεται και ασυμμετρική.

Συνηθισμένες χρήσεις της ασυμμετρικής κρυπτογράφησης είναι:

- Εξασφάλιση εμπιστευτικότητας στη μεταδιδόμενη πληροφορία
- Εξασφάλιση αυθεντικότητας

Για να δούμε με ποιο τρόπο διασφαλίζονται η εμπιστευτικότητα και η αυθεντικότητα, θα αναλύσουμε βήμα προς βήμα μια επικοινωνία ανάμεσα στα δύο μέρη A και B (στην διεθνή βιβλιογραφία χρησιμοποιούνται πάντα ως παραδείγματα για την κρυπτογράφηση ο Bob και η Alice!)



Σχήμα 8.6: Εμπιστευτικότητα δεδομένων με χρήση δημόσιου κλειδιού

Για να ξεκινήσει η επικοινωνία μεταξύ του Bob και της Alice, πρέπει πρώτα να διαθέτει ο καθένας από ένα ζεύγος κλειδιών, ιδιωτικό και δημόσιο. Το ιδιωτικό κλειδί ονομάζεται έτσι ακριβώς επειδή δεν πρέπει ποτέ να γνωστοποιηθεί πουθενά, προορίζεται μόνο για τον κάτοχο του. Αντίθετα, το δημόσιο κλειδί γίνεται διαθέσιμο σε οποιονδήποτε (πρακτικά, τα δημόσια κλειδιά μεταφορτώνονται σε ειδικούς εξυπηρετητές, τους λεγόμενους *keyservers* όπου μπορεί όποιος θέλει να τα αναζητήσει και να τα ανακτήσει). Η δημιουργία του ζεύγους κλειδιών είναι μια απλή διαδικασία και μπορεί να γίνει από κάθε χρήστη που το επιθυμεί.

Στην ασυμμετρική κρυπτογράφηση, η διαδικασία της κρυπτογράφησης γίνεται με τη βοήθεια του δημόσιου κλειδιού, ενώ της αποκρυπτογράφησης με τη βοήθεια του ιδιωτικού. Αυτό σημαίνει ότι για να στείλει η Alice ένα κρυπτογραφημένο μήνυμα στον Bob θα πρέπει:

- Να ανακτήσει το δημόσιο κλειδί του Bob.

- Να χρησιμοποιήσει το δημόσιο κλειδί του Bob για να κρυπτογραφήσει το μήνυμα που θέλει να στείλει.

Από τη μεριά του, ο Bob θα πρέπει:

- Να λάβει το κρυπτογραφημένο μήνυμα από την Alice.
- Να χρησιμοποιήσει το ιδιωτικό του κλειδί για να το αποκρυπτογραφήσει.

Γενικά, στην ασυμμετρική κρυπτογράφηση, ο ένας χρήστης χρειάζεται πάντα το δημόσιο κλειδί του άλλου προκειμένου είτε να του στείλει κάποιο κρυπτογραφημένο μήνυμα ή να ελέγξει την ψηφιακή υπογραφή (θα δούμε αργότερα) ενός μηνύματος που έλαβε από αυτόν. Καθώς το δημόσιο κλειδί διανέμεται μέσω μη έμπιστου δικτύου, τίθεται επίσης θέμα πως θα γίνει ο διαμοιρασμός του.

---

**Σημείωση:** Φυσικά το βιβλίο εδώ έχει λάθος: δεν υπάρχει θέμα διαμοιρασμού του δημοσίου κλειδιού. Τη στιγμή που είναι δημόσιο, είναι διαθέσιμο σε όλους και μπορούμε να το στείλουμε από μη έμπιστο δίκτυο. Το πραγματικό πρόβλημα είναι πως γνωρίζουμε ότι ένα δημόσιο κλειδί που κατεβάσαμε, ανήκει πραγματικά στο άτομο στο οποίο θέλουμε να στείλουμε το μήνυμα, και όχι σε κάποιο τρίτο που επιθυμεί να το υποκλέψει. Για το λόγο αυτό, κάθε κλειδί είναι επίσης εφοδιασμένο με μια τιμή γνωστή ως *δακτυλικό αποτύπωμα (fingerprint)*, που είναι μοναδική και μπορούμε να τη δούμε. Μετά, αν θέλουμε, μπορούμε να επικοινωνήσουμε (με συμβατικό τρόπο, π.χ. τηλέφωνο) με τον κάτοχο του κλειδιού για να επιβεβαιώσουμε ότι πράγματι πρόκειται για το δικό του κλειδί.

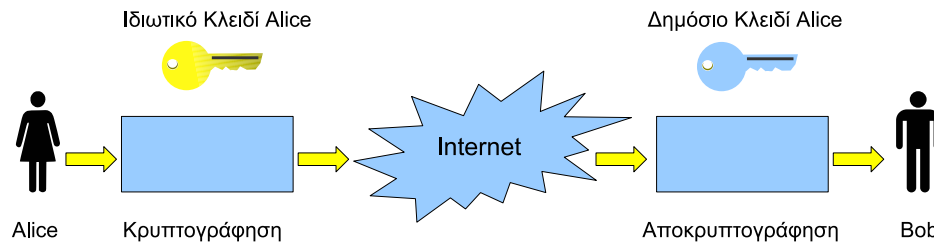
---

Γενικά λοιπόν, η κρυπτογράφηση ενός μηνύματος απαιτεί τη χρήση από τον αποστολέα του δημοσίου κλειδιού **του παραλήπτη**, ώστε η αποκρυπτογράφηση να μπορεί να γίνει μόνο από τον παραλήπτη με τη χρήση του δικού του, καλά προστατευμένου, ιδιωτικού κλειδιού.

Θα δούμε τώρα πως μπορεί να εξασφαλιστεί η αυθεντικότητα ενός μηνύματος κατά την επικοινωνία του Bob και της Alice. Να θυμίσουμε εδώ ότι αυθεντικότητα είναι η δυνατότητα επαλήθευσης της ταυτότητας του χρήστη. Άρα όταν λέμε για εξασφάλιση αυθεντικότητας ενός μηνύματος που προέρχεται από τον Bob, σημαίνει ότι μπορούμε να επαληθεύσουμε ότι έρχεται πραγματικά από τον Bob και όχι από οποιοδήποτε άλλο πρόσωπο. Να σημειώσουμε εδώ ότι για παράδειγμα το απλό email δεν παρέχει καμιά εξασφάλιση αυθεντικότητας, αφού μπορούμε να προσποιηθούμε ότι έχει γίνει αποστολή του από οποιονδήποτε θέλουμε.

Ας υποθέσουμε ότι η Alice στέλνει ένα μήνυμα στον Bob και επιθυμεί να έχει ο Bob την δυνατότητα να ελέγξει ότι η Alice είναι πράγματι ο αποστολέας. Στην περίπτωση αυτή, ακολουθείται η παρακάτω διαδικασία:

- Η Alice δημιουργεί το μήνυμα και το κρυπτογραφεί με το ιδιωτικό της κλειδί.



Σχήμα 8.7: Αυθεντικοποίηση αποστολέα με χρήση ασυμμετρικής κρυπτογράφησης

- Ο Bob λαμβάνει το μήνυμα και το αποκρυπτογραφεί με το δημόσιο κλειδί της Alice (το οποίο φυσικά πρέπει να έχει ανακτήσει από πριν).
- Αν η αποκρυπτογράφηση είναι σωστή το μήνυμα έχει πράγματι προέλθει από την Alice και δεν έχει αλλοιωθεί (τυχαία ή εσκεμμένα) στη διαδρομή. Σε κάθε άλλη περίπτωση η διαδικασία θα αποτύχει.

**Σημείωση:** Όταν κρυπτογραφούμε κάτι με ένα δημόσιο κλειδί, αυτό αποκρυπτογραφείται μόνο με το αντίστοιχο ιδιωτικό. Αυτό σημαίνει ότι η αποκρυπτογράφηση του μπορεί να γίνει μόνο από ένα άτομο. Αντίθετα, όταν κρυπτογραφούμε κάτι με το ιδιωτικό κλειδί, η αποκρυπτογράφηση μπορεί να γίνει από τον καθένα. Προφανώς ο λόγος για να κάνουμε μια τέτοια κρυπτογράφηση δεν είναι για να προστατεύσουμε τα δεδομένα: καθένας μπορεί να τα αποκρυπτογραφήσει. Όμως εξασφαλίζουμε την αυθεντικότητα των δεδομένων, δηλ. την ταυτότητα του αποστολέα. Σε αυτό βασίζεται και η λειτουργία της ψηφιακής υπογραφής που περιγράφεται στην επόμενη ενότητα.

#### 8.3.4.1 Ψηφιακές Υπογραφές

Η ψηφιακή υπογραφή είναι σύνοψη ενός μηνύματος, η οποία προσκολλάται στο τέλος του ηλεκτρονικού εγγράφου. Η ψηφιακή υπογραφή χρησιμοποιείται για την απόδειξη της ταυτότητας του αποστολέα (αυθεντικοποίηση) καθώς και για την απόδειξη της ακεραιότητας των δεδομένων.

Οι ψηφιακές υπογραφές προκύπτουν από το συνδυασμό ενός αλγόριθμου ασυμμετρικής κρυπτογράφησης και ενός αλγόριθμου κατατεμαχισμού (hash). Οι αλγόριθμοι κατατεμαχισμού συνήθως δέχονται ως είσοδο μηνύματα τυχαίου μήκους και δίνουν στην έξοδο τους μια σύνοψη (digest) συγκεκριμένου μήκους. Γνωστοί αλγόριθμοι κατατεμαχισμού είναι οι MD4, Message Digest 4, MD5, Message Digest 5 και SHA, Secure Hash Algorithm και οι παραλλαγές τους (π.χ. SHA1, SHA256).

Η διαδικασία δημιουργίας και επαλήθευσης μιας ψηφιακής υπογραφής, περιγράφεται παρακάτω:

- Αρχικά πρέπει τα δύο μέρη της επικοινωνίας (π.χ. ο Bob και η Alice) να έχουν συμφωνήσει σε κάποιο αλγόριθμο δημοσίου κλειδιού (ασυμμετρικής κρυπτογράφησης, π.χ. PGP, Digital Signature Standard κλπ) και κάποιο αλγόριθμο κατατεμαχισμού (π.χ. MD5).
- Και τα δύο μέρη πρέπει να έχουν ζευγάρια δημοσίων και ιδιωτικών κλειδιών σύμφωνα με τον αλγόριθμο που επέλεξαν προηγουμένως. Θα πρέπει να ανταλλάξουν μεταξύ τους τα δημόσια κλειδιά τους.
- Ας υποθέσουμε ότι η Alice θέλει να στείλει στον Bob ένα υπογεγραμμένο μήνυμα. Αρχικά θα περάσει το μήνυμα από τον αλγόριθμο κατατεμαχισμού ο οποίος θα παράγει μια σύνοψη (digest).
- Θα κρυπτογραφήσει τη σύνοψη με το ιδιωτικό της κλειδί, και θα προσθέσει την κρυπτογραφημένη εκδοχή της στο τέλος του εγγράφου. Θα αποστείλει στον Bob το τελικό αυτό έγγραφο.
- Ο Bob θα εξάγει τη κρυπτογραφημένη σύνοψη από το τέλος του εγγράφου και θα την αποκρυπτογραφήσει χρησιμοποιώντας το δημόσιο κλειδί της Alice. Εφόσον η αποκρυπτογράφιση γίνει σωστά, γνωρίζουμε ότι η σύνοψη δεν έχει αλλοιωθεί. Έπειτα, θα πάρει το μήνυμα, θα το περάσει από τον αλγόριθμο κατατεμαχισμού και θα συγκρίνει τη σύνοψη που υπολόγισε ο ίδιος με τη σύνοψη που έλαβε από την Alice. Αν οι συνόψεις είναι ίδιες τότε γνωρίζει ότι το αρχικό μήνυμα δεν έχει αλλοιωθεί.

Με τον παραπάνω τρόπο, έχουμε εξασφαλίσει τόσο την αυθεντικότητα (ελέγχοντας ότι γίνεται σωστά η αποκρυπτογράφιση της σύνοψης) όσο και την ακεραιότητα (συγκρίνοντας τη σύνοψη που λάβαμε με αυτήν που υπολογίζουμε) του μηνύματος. Έτσι είμαστε σίγουροι και για την ταυτότητα του παραλήπτη και για τη μη-αλλοίωση του περιεχομένου του μηνύματος.

---

**Εργαστηριακή Επίδειξη:** Μπορείτε να χρησιμοποιήσετε το πρόγραμμα GPG σε περιβάλλον Linux/FreeBSD (και Windows) για να δείτε στην πράξη τις βασικές έννοιες της κρυπτογράφησης και υπογραφής με τη χρήση τεχνολογιών δημοσίου κλειδιού. Θα γίνει μια σύντομη επίδειξη στο εργαστήριο σχετικά με τη χρήση αυτού του προγράμματος.

---

### 8.3.5 Τεχνολογίες Ασφάλειας

Όπως αναφέραμε σε προηγούμενη ενότητα, υπάρχει πλήθος τεχνικών που εξασφαλίζουν λύσεις για τα βασικά στοιχεία μιας πολιτικής ασφαλείας. Στην αγορά υπάρχει μεγάλο πλήθος προϊόντων ασφαλείας. Μερικές από τις πιο δημοφιλείς λύσεις για την εμπιστευτικότητα των δεδομένων και την πιστοποίηση των χρηστών αναφέρονται επιγραμματικά παρακάτω:

- **Σταθερά passwords και passwords μιας χρήσης (One Time Passwords, OTP):** για πιστοποίηση χρηστών.
- **SSL / SSH / SOCKS:** Κρυπτογράφηση δεδομένων για εξασφάλιση ακεραιότητας και εμπιστευτικότητας.
- **Radius / Tacacs:** Συστήματα για πιστοποίηση dial-up χρηστών και εκχώρηση συγκεκριμένων δικαιωμάτων.
- **PAP / CHAP:** Συστήματα για πιστοποίηση δικτυακών συσκευών σε συνδέσεις point to point (το βιβλίο γράφει ότι δεν χρησιμοποιούνται για πιστοποίηση χρηστών, αλλά είναι λάθος).
- **Single Sign On:** Βασίζεται σε πιστοποιήσεις ενός παράγοντα και είναι συνήθως λιγότερο ασφαλές από τη χρήση πολλαπλών passwords. Single Sign On ουσιαστικά σημαίνει ότι ένας χρήστης μπορεί να εισέλθει με το όνομα και τον κωδικό του σε ένα σύστημα και να χρησιμοποιήσει έπειτα όλες τις υπηρεσίες που του παρέχει το δίκτυο, χωρίς να χρειαστεί επιπλέον αυθεντικοποίηση.
- **Κέρβερος:** Κρυπτογράφηση για τη διασφάλιση της εμπιστευτικότητας των δεδομένων και πιστοποίηση των χρηστών.
- **IPSec (IP Security):** Το Internet Protocol Security είναι ένα αναπτυσσόμενο πρότυπο για ασφάλεια στο επίπεδο δικτύου. Πριν την ανάπτυξη του, η ασφάλεια συνήθως εστιάζονταν στο επίπεδο εφαρμογής με βάση το μοντέλο OSI. Το IPSec παρέχει δύο επιλογές ασφαλείας:
  - **Αυθεντικότητα της επικεφαλίδας των IP πακέτων:** παρέχεται η δυνατότητα αυθεντικοποίησης του αποστολέα των πακέτων.
  - **ESP, Encapsulation Security Payload:** υποστηρίζεται η αυθεντικότητα τόσο της επικεφαλίδας των πακέτων όσο και των δεδομένων που μεταφέρουν.

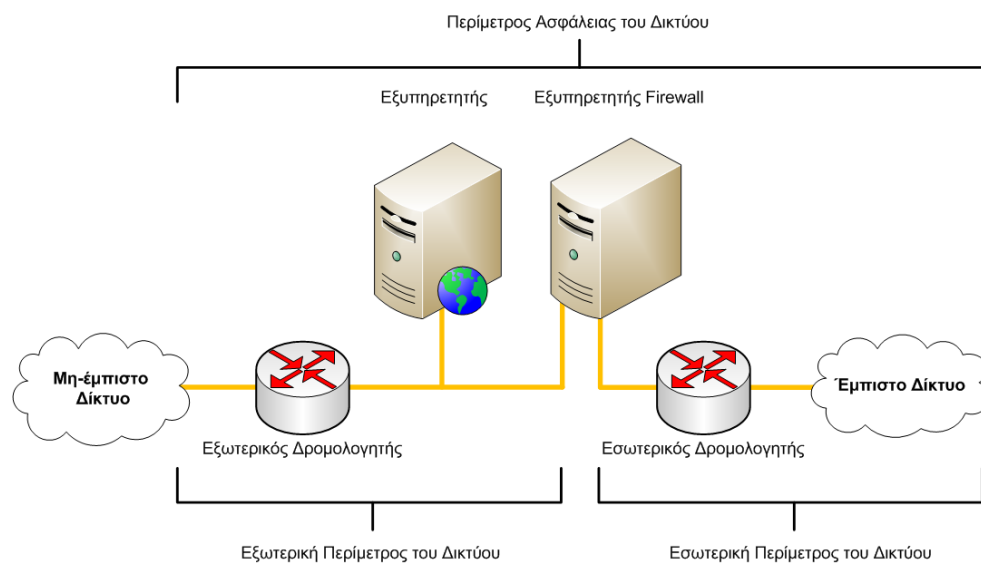
Το IPSec είναι ιδιαίτερα χρήσιμο για δίκτυα VPN (εικονικά ιδιωτικά δίκτυα, Virtual Private Networks) όσο και για χρήστες που συνδέονται στο δίκτυο μέσω επιλεγόμενων τηλεφωνικών γραμμών (dial up).

- **Firewall ή τείχος προστασίας:** Το εξηγούμε παρακάτω.

## Firewall

Η έννοια αναφέρεται στο σύνολο των προγραμμάτων και φίλτρων που έχουμε εγκαταστήσει στις πύλες (gateways, τα σημεία στο δίκτυο που μας συνδέουν με κάποιο εξωτερικό μη-έμπιστο δίκτυο, π.χ. το Internet και γενικά δίκτυα που δεν ελέγχονται από εμάς). Τα προγράμματα και τα φίλτρα που συνιστούν το firewall, εγκαθίστανται σε δρομολογητές και σε υπολογιστές που τυπικά αναλαμβάνουν αποκλειστικά αυτό το ρόλο.

Στο σχήμα 8.8 βλέπουμε το διαχωρισμό του δικτύου της επιχείρησης με τα υπόλοιπα δίκτυα με τη βοήθεια αρχιτεκτονικής που βασίζεται σε δρομολογητές και εξυπηρετητές. Ο εξωτερικός δρομολογητής συνδέει το εξωτερικό μη-έμπιστο δίκτυο (συνήθως το Internet) με το εσωτερικό μας δίκτυο. Η σύνδεση δεν γίνεται απευθείας, αφού παρεμβάλλεται το μηχάνημα που στο σχήμα φαίνεται ως “εξυπηρετητής firewall”. Ο εξωτερικός δρομολογητής μπορεί να περιέχει ένα πρόγραμμα φίλτρου που κόβει από την αρχή πακέτα που γνωρίζουμε ότι δεν μπορεί να είναι έγκυρα για το δίκτυο μας (π.χ. που απευθύνονται σε ports ή μηχανήματα που δεν παρέχουν τις αντίστοιχες υπηρεσίες).



Σχήμα 8.8: Παράδειγμα δικτύου με χρήση firewall

Ο υπολογιστής που βρίσκεται στην εξωτερική περίμετρο του δικτύου, αμέσως μετά τον εξωτερικό δρομολογητή, αναλαμβάνει τυπικά να παρέχει κάποιες υπηρεσίες σε όσους συνδέονται στο δίκτυο της εταιρίας από το μη έμπιστο δίκτυο. Π.χ. μπορεί να είναι ένας web server που να περιέχει τον δικτυακό τόπο (ιστοσελίδες) της εταιρίας.

Τα πακέτα που κατευθύνονται προς το εσωτερικό δίκτυο της εταιρίας, εφόσον περάσουν από το πρώτο φίλτρο στον εξωτερικό δρομολογητή, εισέρχονται στο μηχάνημα firewall. Εκεί διευκρινίζεται σε ποιο εσωτερικό μηχάνημα και port κατευθύνονται και ανάλογα τους επιτρέπεται ή τους απαγορεύεται η είσοδος. Τυπικά, τα πακέτα στα οποία δεν επιτρέπεται να περάσουν απλώς απορρίπτονται. Το firewall μπορεί να επιτρέψει πακέτα τα οποία έρχονται ως απάντηση σε μια επικοινωνία που ξεκίνησε ένας χρήστης από το εσωτερικό δίκτυο (π.χ. ένας υπάλληλος που διαβάζει μια ιστοσελίδα στο Διαδίκτυο), αλλά απαγορεύει την είσοδο πακέτων που δεν κατευθύνονται σε κάποια ενεργή υπηρεσία. Μπορεί να επιτρέπεται επίσης πρόσβαση σε συγκεκριμένες IP (μηχανήματα) του εσωτερικού δικτύου ή σε συγκεκριμένες ports που εκτελούνται υπηρεσίες (π.χ. HTTP), αλλά να απαγορεύεται σε άλλες που προορίζονται μόνο για εσωτερική χρήση (π.χ. telnet, rlogin κλπ).

Το φιλτράρισμα γίνεται με βάση τον αριθμό της πόρτας (TCP ή UDP port) στην οποία κατευθύνεται το πακέτο. Για το σκοπό αυτό εξετάζεται η επικεφαλίδα των πακέτων και απορρίπτονται όσα κατευθύνονται σε απαγορευμένες διευθύνσεις ή ports. Μετά τον εξυπηρετητή firewall, επιπλέον πακέτα μπορούν να απορριφθούν και στο δεύτερο (εσωτερικό) δρομολογητή εφόσον εκτελεί και αυτός κάποιο πρόγραμμα φίλτρου.

Γενικά υπάρχουν πολλές διαφορετικές αρχιτεκτονικές στην τοπολογία διασύνδεσης δρομολογητών και εξυπηρετητών που απαρτίζουν ένα firewall. Όσο πιο πολύπλοκη είναι η αρχιτεκτονική (κάτι που συνήθως επιτυγχάνεται με πολλαπλά στρώματα προστασίας το ένα μετά το άλλο), τόσο πιο δύσκολο είναι να παραβιαστεί η ασφάλεια του εσωτερικού δικτύου της επιχείρησης.

### 8.3.6 Αποφυγή Καταστροφών

Το πληροφοριακό σύστημα μιας εταιρίας είναι πολύ σημαντικό στην εύρυθμη λειτουργία της. Ουσιαστικά σήμερα οι εταιρίες βασίζονται στα πληροφοριακά τους συστήματα για την καθημερινή τους εργασία – σε περίπτωση βλάβης ή απώλειας δεδομένων, η εταιρία συνήθως δεν μπορεί να λειτουργήσει καθόλου. Είναι πολύ σημαντικό η εταιρία να είναι προετοιμασμένη να επιλύσει προβλήματα που ίσως παρουσιαστούν στο συντομότερο δυνατό χρονικό διάστημα.

Τα προβλήματα ενός μοντέρνου, κατανεμημένου πληροφοριακού συστήματος εντοπίζονται συνήθως σε κάποιον από τους παρακάτω τομείς:

- Βλάβες ενεργού εξοπλισμού (σκληροί δίσκοι, τροφοδοτικά, μητρικές κάρτες, δρομολογητές κλπ), παθητικού εξοπλισμού (καλωδιώσεις, racks κλπ).
- Δυσλειτουργίες λειτουργικών συστημάτων και εφαρμογών που μπορεί να οφείλονται σε προβληματικές ρυθμίσεις ή εγγενή προβλήματα τους (bugs).

- Δυσλειτουργίες πρωτοκόλλων επικοινωνίας.
- Δυσλειτουργίες που οφείλονται στα δεδομένα (π.χ. προβληματικά (corrupted) δεδομένα προκαλούν την κατάρρευση κάποιας εφαρμογής).
- Φυσικές καταστροφές (φωτιές, πλημμύρες κλπ).
- Επιθέσεις από κακόβουλα άτομα (crackers, και παρακαλώ να μην το μπερδεύουμε με τους hackers όπως κάνει το σχολικό βιβλίο).

Κάθε επιχείρηση που σέβεται το όνομα της και τους πελάτες της, θα πρέπει να είναι σε θέση να αντεπεξέλθει σε οποιαδήποτε από τις παραπάνω καταστάσεις, στο συντομότερο χρονικό διάστημα και με τις λιγότερες πιθανές επιπτώσεις, τόσο για την ίδια όσο και για τους πελάτες της. Φανταστείτε για παράδειγμα τι πλήγμα είναι για μια χρηματιστηριακή εταιρία ή τράπεζα να μην μπορεί να εξυπηρετήσει για μεγάλο διάστημα τους πελάτες της για λόγους τεχνικών προβλημάτων. Η ύπαρξη σχεδίου αποφυγής καταστροφών (και ανάκαμψης από αυτές) είναι απαραίτητη.

Κάποιες έννοιες που σχετίζονται με το σχεδιασμό αποφυγής καταστροφών είναι οι παρακάτω:

- **Ανάκαμψη (recovery):** Η αποκατάσταση της λειτουργίας του συστήματος μετά από κάποια δυσλειτουργία.
- **Σχέδιο Συνέχειας (Continuity Plan):** Η πλήρης λεπτομερή περιγραφή των βημάτων που πρέπει να πραγματοποιηθούν για να ανακάμψει το σύστημα μετά από μια σοβαρή παραβίαση.
- **Εφεδρικό Αντίγραφο Πληροφοριών (Information Backup):** Η τήρηση πλήρους αντίγραφου των πληροφοριών που μπορεί να χρησιμοποιηθεί για ανάκαμψη ακόμα και από πλήρη απώλεια. Υπάρχουν περιπτώσεις που χρειάζεται να έχουμε ανάκαμψη σε μηδενικό χρόνο, δηλ. να μην υπάρχει καμιά καθυστέρηση όταν έχουμε μια σοβαρή βλάβη. Ουσιαστικά αυτό σημαίνει ότι η λειτουργία του πληροφοριακού συστήματος δεν σταματά ποτέ. Για να γίνει αυτό, πρέπει να έχουμε περισσότερα από ένα πληροφοριακά συστήματα που να λειτουργούν παράλληλα χρησιμοποιώντας τα ίδια δεδομένα (τα δεδομένα πρέπει να είναι συνέχεια σε συγχρονισμό μεταξύ των δύο συστημάτων). Πρόκειται πρακτικά για κλωνοποίηση του αρχικού συστήματος και της δομής του δικτύου. Μπορεί το παραπάνω να φαίνεται υπερβολικό και είναι γεγονός ότι έχει μεγάλο κόστος, ωστόσο σε ορισμένες περιπτώσεις εταιριών (που βασίζουν όλο το μοντέλο λειτουργίας τους στο πληροφοριακό τους σύστημα) δεν υπάρχει άλλη λύση.

Προφανώς κάθε επιχείρηση θα πρέπει να αναλύσει τους κινδύνους που διατρέχει κάθε τμήμα του πληροφοριακού της συστήματος και να αποφασίσει πόσο κρίσιμοι είναι και μέχρι ποιο σημείο είναι διατεθειμένη να το προστατεύσει. Η λύση θα πρέπει

να λαμβάνει υπόψη το κόστος υλοποίησης σε συνάρτηση με την κρισιμότητα των δεδομένων που προστατεύει ή το πόσο εύκολο είναι να αναδημιουργηθούν αυτά τα δεδομένα. Γενικά, τα περισσότερα πληροφοριακά συστήματα σήμερα βασίζονται σε αρχιτεκτονικές πελάτη – εξυπηρετητή (client – server). Σε τέτοια συστήματα, το πιο κρίσιμο σημείο είναι το κτήριο που στεγάζει τους βασικούς υπολογιστές (servers), γνωστό ως main site. Αρκετές εταιρίες και οργανισμοί μεγάλου μεγέθους και με κρίσιμα δεδομένα, επιλέγουν να υλοποιήσουν δύο main sites, ώστε σε περίπτωση καταστροφής του ενός να αναλάβει αυτόματα το δεύτερο. Τα δύο αυτά κεντρικά sites πρέπει προφανώς να είναι αρκετά απομονωμένα μεταξύ τους ώστε να μην επηρεαστούν και τα δύο από την ίδια φυσική καταστροφή (π.χ. φωτιά, πλημμύρα).

Η ύπαρξη δυο κεντρικών site προϋποθέτει και την ύπαρξη δύο ουσιαστικά ισοδύναμων υπολογιστικών συστημάτων καθώς και της απαραίτητης τηλεπικοινωνιακής υποδομής μεταξύ τους ώστε να γίνεται συνέχεια συγχρονισμός των δεδομένων. Τα κεντρικά site θα πρέπει να περιλαμβάνουν πρόβλεψη για επαλληλία των κεντρικών δικτυακών συσκευών (δρομολογητών, switches κλπ). Πρακτικά, αυτό σημαίνει ότι για κάθε τέτοια συσκευή θα πρέπει να υπάρχει μια εναλλακτική έτοιμη να αναλάβει (ενδεχομένως αυτόματα) σε περίπτωση βλάβης της πρώτης. Πρέπει επίσης να υπάρχει εναλλακτικότητα στη διασύνδεση των διάφορων εσωτερικών τοπικών δικτύων (LANs). Αυτό σημαίνει ότι αν για παράδειγμα χαλάσει ένας δρομολογητής που ενώνει δύο εσωτερικά δίκτυα και δεν μπορεί να αντικατασταθεί άμεσα, να υπάρχει κάποια εναλλακτική διαδρομή μέσω άλλων δρομολογητών ώστε τα δίκτυα αυτά να συνεχίσουν να είναι συνδεδεμένα (έστω και με πιο αργή ταχύτητα).

Πέρα φυσικά από τις παραπάνω προβλέψεις εναλλακτικότητας και επαλληλίας, θα πρέπει να υπάρχει και αντίστοιχο σχέδιο για εφεδρικές λύσεις τόσο για τον εξοπλισμό του πληροφοριακού συστήματος όσο και για τις εφαρμογές και τα δεδομένα (π.χ. πολιτική τήρησης αντιγράφων ασφαλείας – backup. Συνηθίζεται να τηρούνται περισσότερα από ένα αντίγραφα ασφαλείας, με ένα πάντα να φυλάσσεται σε προστατευμένο χώρο εκτός του main site ώστε να μην επηρεαστεί από τυχόν καταστροφή του).

Γενικά δεν υπάρχει καθιερωμένη λύση για τη μορφή του σχεδίου αποφυγής και αντιμετώπισης καταστροφών μιας επιχείρησης. Η λύση διαφέρει ανάλογα με τη δομή του συστήματος, την σπουδαιότητα και κρισιμότητα των δεδομένων, το χρόνο που μπορούμε να ανεχθούμε μέχρι την ανάκαμψη της λειτουργίας και φυσικά τα χρήματα που είναι η επιχείρηση διατεθειμένη να ξοδέψει. Σίγουρα πρόκειται για ένα πολύ σοβαρό έργο, το οποίο δεν μπορεί να αναβληθεί ή να μην σχεδιαστεί σωστά από την αρχή, καθώς αυτό θα αποδειχθεί κάποια στιγμή μοιραίο για την επιχείρηση.