

## 8.3 Ασφάλεια Δικτύων

Με την ανάπτυξη των δικτύων παρουσιάστηκε η ανάγκη προστασίας της πληροφορίας, που μεταδίδεται ή αποθηκεύεται. Στην ενότητα αυτή θα γίνει παρουσίαση προβλημάτων ασφάλειας δικτύων, υπηρεσιών ασφάλειας για την αντιμετώπισή τους, τεχνικών υλοποίησης των υπηρεσιών αυτών καθώς και των προϋποθέσεων ύπαρξης συστήματος ασφάλειας.

### 8.3.1 Ασφάλεια πληροφοριών

Η ασφάλεια των συστημάτων ασχολείται με την προστασία αντικειμένων που αξίζουν να προστατευθούν, τα αγαθά. Τα αγαθά με την σειρά τους έχει νόημα να προστατευθούν μόνο και μόνο επειδή έχουν κάποια αξία. Η αξία των αγαθών μπορεί να μειωθεί εάν υποστούν ζημιά. Από την στιγμή, που μπορεί να προκύψουν κίνδυνοι που θα μειώσουν την αξία των αγαθών πρέπει να ληφθούν μέτρα προστασίας για τα αγαθά, κάτι που συνεπάγεται και κάποιο κόστος (τόσο σε

χρήμα όσο και σε κόπο). Η μερική προστασία των αγαθών, είτε για λόγους υπερβολικού κόστους των μέτρων προστασίας, είτε για λόγους αδυναμίας ύπαρξης των κατάλληλων μηχανισμών, που μπορούν να εξασφαλίσουν την απόλυτη ασφάλεια, έχει ως συνέπεια τη δημιουργία επισφάλειας των αγαθών. Ο ιδιοκτήτης των αγαθών θα πρέπει να κρίνει, ποια είναι η πιο επωφελής ισορροπία ανάμεσα στο κόστος για τη λήψη μέτρων προστασίας και στην επισφάλεια των αγαθών με τις συνέπειες της. Ιδιοκτήτης μπορεί να είναι το πρόσωπο που κατέχει ή είναι υπεύθυνο για ολόκληρο ή για μέρος αγαθού. Σε πληροφοριακό σύστημα, σαν αγαθά μπορούν να θεωρηθούν οι πληροφορίες, που διακινούνται σε αυτό (ή τα δεδομένα) και οι υπολογιστικοί πόροι που χρησιμοποιούμε για να διαχειριστούμε τις πληροφορίες και τα δεδομένα. Ο ιδιοκτήτης διατηρεί το δικαίωμα να καθορίσει πως μπορεί να χρησιμοποιηθεί, να μεταβληθεί ή να διατεθεί το αγαθό. Εκτός, όμως, από τους ιδιοκτήτες, τα αγαθά είναι δυνατό να χρησιμοποιούνται και από τους χρήστες. Οι χρήστες μπορεί να είναι ή να μην είναι τα ίδια πρόσωπα με τους ιδιοκτήτες. Πρέπει να διευκρινίσουμε, ότι με τους όρους ιδιοκτήτες ή χρήστες, δεν αναφερόμαστε αποκλειστικά σε πρόσωπα αλλά και σε διεργασίες, που κάνουν χρήση μέρους ή ολόκληρου του πληροφοριακού συστήματος. Από τη στιγμή, που υπάρχει η έννοια της ιδιοκτησίας, πρέπει να εισάγουμε και την έννοια της εξουσιοδότησης. Ως εξουσιοδότηση μπορούμε να ορίσουμε την άδεια που παρέχει ο ιδιοκτήτης για συγκεκριμένο σκοπό, όπως για παράδειγμα, την άδεια για χρήση κάποιων υπολογιστικών πόρων ή την πρόσβαση σε συγκεκριμένο σύνολο δεδομένων βάσης δεδομένων. Έτσι, για την πρόσβαση σε κάποια μέσα ή πληροφορίες υπάρχει η έννοια του εξουσιοδοτημένου ή του μη εξουσιοδοτημένου.

Μεγάλο μέρος της ασφάλειας πληροφοριών ασχολείται με την εξασφάλιση της συνεχούς παροχής υπηρεσιών στους εξουσιοδοτημένους χρήστες και την προστασία τους από τους μη εξουσιοδοτημένους. Υπάρχουν τέσσερα ζητούμενα στα πλαίσια πολιτικής ασφάλειας, για να εξασφαλισθεί η χρήση των αγαθών από εξουσιοδοτημένους χρήστες:

- **Αυθεντικότητα (authentication):** Η απόδειξη της ταυτότητας του χρήστη για παροχή πρόσβασης στα αγαθά συστήματος.
- **Ακεραιότητα (Integrity):** Η διασφάλιση ότι τα δεδομένα έχουν υποστεί αλλαγές 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 σε συγκεκριμένο χρήστη.

Από τα τέσσερα παραπάνω ζητούμενα μπορούμε να συνθέσουμε και την έννοια της **Εγκυρότητας (Validity)**: ως την απόλυτη ακρίβεια και πληρότητα μιας πληροφορίας. Η εγκυρότητα είναι ο συνδυασμός της Ακεραιότητας και της Αυθεντικότητας.

Επίσης, θα πρέπει να διασφαλίσουμε στους εξουσιοδοτημένους χρήστες, που πιθανόν να κοστολογούνται για τη δυνατότητα πρόσβασης τους σε πληρο-

φορίες, ότι δεν συντρέχει περίπτωση άρνησης παροχής υπηρεσιών, για τις οποίες έχουν εξουσιοδοτήσει. Έτσι, μπορούμε να ορίσουμε και την **Διαθεσιμότητα Πληροφοριών (Information Availability)**: ως την αποφυγή προσωρινής ή μόνιμης άρνησης διάθεσης πληροφορίας σε εξουσιοδοτημένους χρήστες.

Με όσα έχουν αναφερθεί σε αυτήν την ενότητα μπορούμε να προχωρήσουμε στους παρακάτω ορισμούς της ασφάλειας και της ασφάλειας πληροφοριών:

- **Ασφάλεια (Security)**: Η προστασία της Διαθεσιμότητας, της Ακεραιότητας και της Εμπιστευτικότητας Πληροφοριών.
- **Ασφάλεια Πληροφοριών (Information Security)**: Ο συνδυασμός της Εμπιστευτικότητας, της Εγκυρότητας και της Διαθεσιμότητας Πληροφοριών.

Με βάση όσα προαναφέρθηκαν μπορούμε να ορίσουμε ως Παραβίαση (violation) ασφάλειας σε πληροφοριακό σύστημα, την παραβίαση ενός ή περισσότερων ιδιοτήτων, όπως διαθεσιμότητα, εμπιστευτικότητα και εγκυρότητα.

Ένα πληροφοριακό σύστημα είναι εκτεθειμένο σε κινδύνους. Οι κίνδυνοι μπορούν να διαχωριστούν στις απειλές και στις αδυναμίες.

Με τον όρο απειλές αναφερόμαστε σε ενέργειες ή γεγονότα, που μπορούν να οδηγήσουν στην κατάρρευση κάποιου από τα χαρακτηριστικά ασφάλειας πληροφοριών (όπως αυτά ορίστηκαν πιο πάνω). Οι απειλές μπορεί να προέρχονται είτε από φυσικά γεγονότα (π.χ. πυρκαγιά) είτε από ανθρώπινες ενέργειες, που μπορεί να είναι σκόπιμες ή τυχαίες. Ενώ με τον όρο αδυναμίες αναφερόμαστε στα σημεία του πληροφοριακού συστήματος, που αφήνουν περιθώρια για παραβιάσεις. Οι αδυναμίες μπορεί να οφείλονται σε ανεπαρκή γνώση για υποστήριξη του συστήματος από το ανθρώπινο δυναμικό, ή σε από κατασκευής δυσλειτουργίες του ίδιου του συστήματος (π.χ. ελαττώματα στο λογισμικό).

Στην προσπάθεια μας να δημιουργήσουμε πλαίσιο ασφάλειας για πληροφοριακό σύστημα, θα πρέπει πρώτα να εκτιμήσουμε και να συνυπολογίσουμε διάφορους παράγοντες, πριν προχωρήσουμε στη λήψη μέτρων ασφάλειας. Πρώτα από όλα, θα πρέπει να εντοπίσουμε ποια αγαθά πραγματικά χρήζουν ανάγκης προστασίας και να προσπαθήσουμε να βρούμε τους πιθανούς κινδύνους. Στη συνέχεια, θα πρέπει να προχωρήσουμε σε ένα πρώτο σχεδιασμό της αρχιτεκτονικής ασφάλειας και υπολογισμό του κόστους υλοποίησής της. Στο κόστος θα πρέπει να συμπεριλαμβάνεται το κόστος των υλικών που απαιτούνται για την υλοποίηση της λύσης, το κόστος του ανθρώπινου δυναμικού, που θα κληθεί να πραγματοποιήσει την εγκατάσταση, καθώς και το μόνιμο λειτουργικό κόστος για τη συντήρηση πλαισίου ασφάλειας στο πληροφοριακό σύστημα.

Σε περίπτωση που το κόστος για τα μέτρα προστασίας, που πρέπει να ληφθούν, ξεπερνούν τα προβλεπόμενα όρια, θα πρέπει να προβούμε σε νέες παραδοχές ή και συμβιβασμούς στο τι πραγματικά θα καλύπτει και σε ποιο βαθμό η πολιτική ασφάλειας, θα υλοποιηθεί. Με τον τρόπο αυτό αποδεχόμαστε την απομένουσα επικινδυνότητα και επισφάλεια μετά την εγκατάσταση των σχετικών μέτρων προστασίας.

Τώρα που αναφερθήκαμε γενικά σε θέματα ασφάλειας και έννοιες ασφάλειας

πληροφοριών, μπορούμε να προχωρήσουμε σε πιο τεχνική εξέταση των μεθόδων που συνήθως ακολουθούνται για την επίτευξη παραβιάσεων, αλλά και στα αντίμετρα, που κάποιος μπορεί να υλοποιήσει, για να προστατέψει το πληροφοριακό του σύστημα.

### 8.3.2 Επεξήγηση Ορολογίας

Πριν προχωρήσουμε στην παρουσίαση βασικών τεχνικών για την παραβίαση της ασφάλειας των δικτύων υπολογιστών καθώς και σε τεχνικές προστασίας αυτών, θα αναφερθούμε στην χρησιμοποιούμενη ορολογία. Μερικοί από τους όρους θα γίνουν πλήρως κατανοητοί, όταν θα ενταχθούν μέσα στα πλαίσια τεχνικής ασφάλειας, που θα αναφέρουμε στη συνέχεια. Οι ακόλουθοι όροι είναι από τους πιο βασικούς και ευρέως χρησιμοποιούμενους σε θέματα ασφάλειας πληροφοριακών συστημάτων:

- **Κρυπτογράφηση (Encryption):** Η μέθοδος (συνήθως μαθηματικός αλγόριθμος, το αποτέλεσμα του οποίου μπορεί με αναστροφή να μας δώσει την είσοδο του αλγόριθμου) κωδικοποίησης της αρχικής πληροφορίας, έτσι ώστε να είναι αναγνώσιμη μόνο κατόπιν αποκωδικοποίησής της (αποκρυπτογράφησης της).
- **Αποκρυπτογράφηση (Decryption):** Η μέθοδος (η ανάστροφη λειτουργία του αλγόριθμου κρυπτογράφησης) αποκωδικοποίησης για την ανάκτηση της αρχικής κωδικοποιημένης πληροφορίας.
- **Κλειδί (Key):** Πέρα από την γνωστή εικόνα που όλοι μας έχουμε για το κλειδί, μπορούμε να θεωρήσουμε και ως κλειδί ένα ψηφιακό κωδικό (κάποιος αριθμός από bits), που χρησιμοποιείται από τους αλγόριθμους κρυπτογράφησης ή αποκρυπτογράφησης.
- **Δημόσιο Κλειδί (Public Key):** Ψηφιακός κωδικός που χρησιμοποιείται για την κρυπτογράφηση / αποκρυπτογράφηση πληροφοριών καθώς και για τη πιστοποίηση ψηφιακών υπογραφών. Το δημόσιο κλειδί μοιράζεται σε όλους τους χρήστες ασφαλούς δικτύου και συνδυάζεται πάντα με ιδιωτικό κλειδί.
- **Ιδιωτικό Κλειδί (Private Key):** Ψηφιακός κωδικός, για κρυπτογράφηση / αποκρυπτογράφηση και πιστοποίηση ψηφιακών υπογραφών, που ανήκει μόνο σε ένα χρήστη, είναι καθαρά προσωπικό και συνδυάζεται με δημόσιο κλειδί.
- **Μυστικό Κλειδί (Secret Key):** Ψηφιακός κωδικός, που είναι γνωστός στα δύο μέρη, προκειμένου να επικοινωνήσουν με χρήση κρυπτογράφησης / αποκρυπτογράφησης.
- **Λειτουργία Κατατεμαχισμού (Hash Function):** Μαθηματική συνάρτηση, το αποτέλεσμα της οποίας δεν μπορεί με αναστροφή να μας παράγει την αρχική είσοδο.
- **Σύνοψη Μηνύματος (Message Digest):** Η τιμή, που δίνει η λειτουργία κατατεμαχισμού.
- **Ψηφιακή Υπογραφή (Digital Signature):** Αριθμός από bits, προστιθέμενος στο τέλος μηνύματος για να εξασφαλίσει την αυθεντικότητα και ακεραιότητα του μηνύματος.

### 8.3.3 Μέθοδοι Παραβίασης

Σε δίκτυο υπολογιστών εμπιστευτική πληροφορία μπορεί να υπάρχει αποθηκευμένη σε μέσα αποθήκευσης (σκληροί δίσκοι, μνήμες κ.λ.π.), ή να κυκλοφορεί μέσου του δικτύου με τη μορφή πακέτων. Η ύπαρξη πληροφοριών σε αυτές τις δύο καταστάσεις μπορεί να απειληθεί με διαφόρους τρόπους από ενέργειες χρηστών τόσο του εσωτερικού δικτύου, όσο και από χρήστες του Διαδικτύου στην περίπτωση που έχουμε σύνδεση και με αυτό. Στη συνέχεια θα αναφερθούμε στους πλέον συνηθισμένους τρόπους επιθέσεων, που χρησιμοποιούνται για την παραβίαση της ασφάλειας δικτύου υπολογιστών:

- Επιθέσεις στους κωδικούς πρόσβασης (Password attacks)

Όπως είναι γνωστό, οι μυστικοί προσωπικοί κωδικοί (passwords) είναι η πλέον κοινή μέθοδος ελέγχου της πρόσβασης σε υπολογιστικά συστήματα. Υπάρχουν δύο είδη passwords:

– **Τα επαναχρησιμοποιούμενα passwords**, που μπορούν να χρησιμοποιούνται πολλές φορές για την πρόσβαση στο σύστημα.

– **Τα passwords μιας χρήσης**. Τα passwords αυτά αλλάζουν συνεχώς και μπορούν να χρησιμοποιηθούν μόνο μία φορά για πρόσβαση στο σύστημα.

Τα περισσότερα είδη λειτουργικών συστημάτων, όπως το Unix ή τα Windows, προσφέρονται με σύστημα πιστοποίησης χρηστών με τον πρώτο τύπο passwords.

Με την εξέλιξη της τεχνολογίας η προστασία με χρήση μόνο passwords, αποτελεί σύστημα ασθενούς προστασίας της πρόσβασης.

Για την παραβίαση κωδικών πρόσβασης υπάρχουν προγράμματα, που σε μικρό χρονικό διάστημα μπορούν να δοκιμάσουν πολλούς συνδυασμούς χαρακτήρων και αριθμών. Άλλος τρόπος είναι η παρακολούθηση των πλήκτρων (key stroke monitoring), όταν κάποιος εισάγει τον κωδικό του και αυτό μπορεί να γίνει με διάφορους τρόπους, όπως η εκτέλεση προγράμματος, που παρακολουθεί τα πλήκτρα, που έχουν χρησιμοποιηθεί σε ένα πληκτρολόγιο και η αποθήκευση σε ένα αρχείο, ή ο δύσκολος τρόπος της παρακολούθησης της ακτινοβολίας της οθόνης.

Ένας άλλος τρόπος για την παραβίαση κωδικών πρόσβασης αναφέρεται σαν social engineering και επικεντρώνει στην παραπλάνηση χρηστών για την απόκτηση πληροφοριών. Για παράδειγμα, η περίπτωση, που κάποιος προσποιείται τον υπάλληλο γραφείου βοήθειας (help desk) και ζητά το password χρήστη, για να διορθώσει ανύπαρκτο πρόβλημα στο υπολογιστικό σύστημα. Στην κατηγορία αυτή υπάγεται και το λεγόμενο shoulder surfing, δηλαδή το γεγονός της τυχαίας παρακολούθησης της πληκτρολόγησης του password άλλου χρήστη.

Υπάρχει επίσης η δυνατότητα απόκτησης του password με τη χρήση φυσικής βίας. Οι περιπτώσεις φυσικής βίας μπορούν να ενταχθούν σε δύο κατηγορίες: στην εξωτερική και στην εσωτερική βία. Με την εξωτερική βία είναι προφανές, ότι ένας χρήστης, όταν θα κινδυνεύσει η σωματική του ακεραιότητα, μπορεί να αποκαλύψει το password, που χρησιμοποιεί. Με την εσωτερική βία αναφερόμα-

στε στην περίπτωση, όπου κάποιος αντιγράφει νόμιμα ή παράνομα κρυπτογραφημένα passwords και μετά εκτελεί πρόγραμμα crack, για να τα αποκρυπτογραφήσει. Το πρόγραμμα crack παίρνει λέξεις από λεξικό και τις κρυπτογραφεί με τον ίδιο αλγόριθμο, που χρησιμοποιεί το λειτουργικό σύστημα για την κρυπτογράφηση των password των χρηστών. Το πρόγραμμα συγκρίνει το αποτέλεσμα της κρυπτογράφησης με τα υποκλαπέντα passwords και όταν αυτά συμπίσουν, τότε έχουν βρεθεί τα πραγματικά passwords. Τα προγράμματα crack ειδικά για συστήματα Unix είναι αρκετά διαδεδομένα και εξελιγμένα.

- **Παρακολούθηση Δικτύου (Network Monitoring ή Network Packet Sniffing)**

Όπως είναι γνωστό, η επικοινωνία των υπολογιστών μέσω δικτύου βασίζεται σε πρωτόκολλα και τα δεδομένα μεταφέρονται με τη μορφή πακέτων. Πολλές εφαρμογές μεταδίδουν τα πακέτα σε μορφή καθαρού κειμένου (clear text), δηλαδή χωρίς να προβούν από μόνες τους σε κάποιο είδος κωδικοποίησης ή κρυπτογράφησης. Από την στιγμή, που τα πακέτα μεταδίδονται χωρίς κωδικοποίηση, μπορούν να συλλεχθούν με κάποιους τρόπους, να συναρμολογηθούν και να παράγουν στο ακέραιο το σύνολο της πληροφορίας. Τα προγράμματα, που κάνουν ανίχνευση πακέτων (packet sniffing), χρησιμοποιούν την κάρτα δικτύου του υπολογιστή σε κατάσταση promiscuous mode. Στην κατάσταση promiscuous mode, η κάρτα δικτύου διαβάζει και αποθηκεύει όλα τα πακέτα, που κυκλοφορούν στο δίκτυο, που συνδέεται. Τα προγράμματα αυτά μπορούν να χρησιμοποιηθούν στην διάγνωση προβλημάτων από τους διαχειριστές δικτύων, αλλά ταυτόχρονα αποτελεί πολύ ισχυρό εργαλείο για τους επίδοξους εισβολείς. Εκτός του ότι μπορεί να συλλέξουν εμπιστευτική πληροφορία την ώρα, που διέρχεται μέσα από τις γραμμές του δικτύου, είναι πολύ πιθανό να αποκαλύψει και μεταδιδόμενα passwords (η αποκάλυψη των passwords με τον τρόπο αυτό είναι γνωστή και ως Man – In – The – Middle). Επομένως μπορεί η παρακολούθηση των πακέτων στο δίκτυο να χρησιμοποιηθεί και ως μέσο για την παραβίαση των passwords.

- **Μεταμφίεση (Masquerade)**

Επίθεση με μεταμφίεση παρατηρείται όταν ο επιτιθέμενος, που βρίσκεται σε άλλο δίκτυο από το δικό μας, προσποιείται ότι βρίσκεται στο δικό μας. Ειδικά στα πρωτόκολλα TCP/IP, η μέθοδος μεταμφίεσης είναι γνωστή και ως IP Spoofing, όπου ο επιτιθέμενος ανήκει σε άλλο δίκτυο και προσποιείται ότι η διεύθυνση του ανήκει στο δικό μας εύρος IP διευθύνσεων. Η μέθοδος αυτή χρησιμοποιείται κυρίως για να ξεγελάσει ο επιτιθέμενος το firewall που συνδέει το εσωτερικό μας δίκτυο με το διαδίκτυο ή γενικότερα με δίκτυο, που δεν θεωρείται έμπιστο (trusted). Συνήθως το IP Spoofing περιορίζεται στο να εισάγει δεδομένα ή εντολές σε υπάρχον πακέτο δεδομένων, κατά τη διάρκεια επικοινωνίας τύπου client / server ή σε δίκτυα σημείο προς σημείο.

Για να γίνει εφικτή η αμφίδρομη επικοινωνία, ο επιτιθέμενος θα πρέπει να αλλάξει τους πίνακες δρομολόγησης, που έδειχναν προς τη διεύθυνση, που έχει προσποιηθεί ότι βρίσκεται (spoofed IP address). Με τον τρόπο αυτό ο επιτιθέμενος θα μπορεί να λαμβάνει όλα τα πακέτα που προορίζονταν για τη spoofed IP

διεύθυνση. Στην περίπτωση αυτή, ο επιτιθέμενος μπορεί κλέψει passwords. Επίσης μπορεί προσποιούμενος, ότι είναι κάποιος από το δίκτυο μας, να στείλει προς τους συνεργάτες μας ή τους πελάτες μας e-mails.

- **Άρνηση Παροχής Υπηρεσίας (Denial of Service)**

Οι επιθέσεις άρνησης παροχής υπηρεσιών διαφοροποιούνται από τις άλλες, που έχουμε αναφέρει, στο ότι δεν προσπαθούν να πετύχουν πρόσβαση στο δίκτυό μας, ή να συλλέξουν πληροφορίες, που διακινούνται σε αυτό. Οι επιθέσεις αυτές εστιάζονται κυρίως στην εξάντληση των ορίων των πόρων του δικτύου, όπως για παράδειγμα τον αριθμό των πακέτων, που μπορεί να χειριστεί ταυτόχρονα ένας δρομολογητής, ή στις διεργασίες στις οποίες μπορεί να αντεπεξέλθει κεντρικός εξυπηρετητής στο δίκτυο μας (π.χ. web server, mail server). Παραδείγματα τέτοιων επιθέσεων παρατηρούνται πολλά τον τελευταίο καιρό, όπως αυτά που σημειώθηκαν στα site του Yahoo, CNN στις αρχές του 2000. Εάν από ένα εξυπηρετητή ζητηθεί να εξυπηρετήσει πολύ μεγαλύτερο όγκο εργασιών από ότι είναι σχεδιασμένος να εξυπηρετήσει μέσα σε συγκεκριμένο χρονικό διάστημα, τότε είναι λογικό, ότι θα καταρρεύσει. Στο παράδειγμα που προαναφέραμε τα sites δέχθηκαν μέσα σε τρεις ώρες απαίτηση για εξυπηρέτηση διεργασιών, που δέχονται μέσα σε ένα ολόκληρο χρόνο.

Οι επιθέσεις αυτού του είδους δεν χρειάζονται αυξημένες γνώσεις σε σχέση με τις άλλες είδους επιθέσεις, που προαναφέραμε. Βέβαια είναι αποτελεσματικότερες, εάν υπάρχει πληροφόρηση για την αρχιτεκτονική του δικτύου, που πρόκειται να δεχθεί επίθεση.

- **Επιθέσεις στο επίπεδο των Εφαρμογών (Application-Layer Attacks)**

Όπως είναι γνωστό, πολλές φορές εφαρμογές, όπως HTTP, ActiveX, Telnet, Ftp, Telnet κ.λ.π., παρουσιάζουν αδυναμίες στον κώδικά τους (γνωστές και ως τρύπες, holes). Οι γνώστες αυτών των αδυναμιών μπορεί να τις εκμεταλλευθούν, προκειμένου να αποκτήσουν πρόσβαση στο σύστημα, με απώτερο σκοπό την δημιουργία σε αυτό προβλημάτων ή τη συλλογή πληροφοριών.

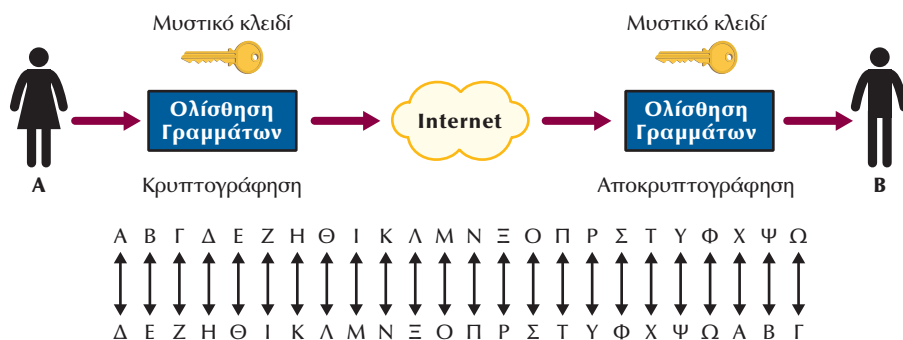
### 8.3.4 Τεχνικές ασφάλειας

Στη συνέχεια, θα παρουσιάσουμε κάποιες βασικές τεχνικές ασφάλειας των, πληροφοριών σε δίκτυο ηλεκτρονικών υπολογιστών. Πρέπει να σημειώσουμε ότι ο τομέας της ασφάλειας δεδομένων σε κατανεμημένο πληροφοριακό σύστημα είναι από τους πλέον εξελισσόμενους και υπάρχει συνεχής παρουσίαση νέων προϊόντων σε θέματα ασφάλειας από τις εταιρείες που δραστηριοποιούνται στον χώρο αυτό.

- **Συμμετρική Κρυπτογράφηση**

Η συμμετρική κρυπτογράφηση πολλές φορές αναφέρεται και ως κρυπτογράφηση συμμετρικού κλειδιού. Η μέθοδος αυτή χρησιμοποιείται κύρια για την εξασφάλιση της εμπιστευτικότητας των μεταδιδόμενων πληροφοριών πάνω από ένα κανάλι επικοινωνίας.





**Σχήμα 8-12** Επικοινωνία με χρήση συμμετρικής κρυπτογράφησης

Στην περίπτωση που (σχήμα 8-12), δύο χρήστες ο Α και ο Β θέλουν να επικοινωνήσουν μεταξύ τους με ασφάλεια, θα πρέπει και οι δύο να συμφωνήσουν στη χρησιμοποίηση του ίδιου αλγόριθμου κρυπτογράφησης, καθώς επίσης και στη χρήση κοινού κλειδιού.

Πολύ απλοϊκός αλγόριθμος κρυπτογράφησης είναι ο Caesar Cipher, που, όπως φαίνεται στο σχήμα 8-12, αντικαθιστά το κάθε γράμμα του αλφαβήτου σε ένα μήνυμα με ένα άλλο γράμμα μερικές θέσεις πιο κάτω στο αλφάβητο. Ο αλγόριθμος ολίσθαινει τα γράμματα προς τα αριστερά, όταν κρυπτογραφεί κάποιο μήνυμα, ενώ προς τα δεξιά, όταν πρόκειται να αποκρυπτογραφήσει ήδη κρυπτογραφημένο μήνυμα. Στο σχήμα 8-12 ο συμφωνημένος αριθμός ολίσθησης στο αλφάβητο από τους χρήστες Α και Β είναι τρία γράμματα. Εύκολα καταλαβαίνουμε ότι, εάν κάποιος δει το κρυπτογραφημένο μήνυμα και γνωρίζει τον αλγόριθμο, θα μπορέσει σχετικά εύκολα να αποκρυπτογραφήσει το μήνυμα και αυτό γιατί ο αλγόριθμος, που προαναφέραμε, δεν είναι ιδιαίτερα σύνθετος.

Υπάρχουν προγράμματα, που προσπαθούν να αποκρυπτογραφήσουν μήνυμα, δοκιμάζοντας αρκετούς αλγόριθμους. Εάν ο αλγόριθμος είναι περίπλοκος, το σπάσιμό του ακόμα και με σύγχρονους υπολογιστές με μεγάλη υπολογιστική ισχύ, απαιτεί πολύ χρόνο, ακόμα και χρόνια, οπότε και η αποκάλυψη της πληροφορίας να μην έχει πλέον νόημα. Έχουν αναπτυχθεί πολλοί αλγόριθμοι κρυπτογράφησης, που στηρίζονται σε σύνθετη λογική και περίπλοκους μαθηματικούς συνδυασμούς. Πολλοί αλγόριθμοι μάλιστα, δεν είναι επαρκώς τεκμηριωμένοι, ενώ άλλοι δεν είναι καταχωρημένοι στη βιβλιογραφία, επειδή προστατεύονται ως κρατικά μυστικά. Είναι συνηθισμένο από χώρες, που έχουν αναπτύξει αλγόριθμους, να μην επιτρέπουν στις εταιρείες, που τους έχουν ενσωματώσει στη λειτουργία των προϊόντων τους, να εξάγουν στην πλήρη έκδοσή τους σε άλλες χώρες, χωρίς την έκδοση σχετικής άδειας.

Μερικοί από τους πλέον διαδεδομένους αλγόριθμους κρυπτογράφησης είναι το **Πρότυπο Κρυπτογράφησης Δεδομένων (Data Encryption Standard, DES)**, ο **3DES (triple DES)** και ο **Διεθνής Αλγόριθμος Κρυπτογράφησης Δεδομένων**



(**International Data Encryption Algorithm, IDEA**). Οι αλγόριθμοι αυτοί δέχονται ως είσοδο μηνύματα των 64 bits. Εάν το μήνυμα έχει μεγαλύτερο μήκος, θα πρέπει να σπάσει σε τμήματα των 64 bits.

Όπως αναφέραμε η μέθοδος της συμμετρικής κρυπτογράφησης προσφέρει κυρίως εμπιστευτικότητα στην επικοινωνία. Μπορεί να χρησιμοποιηθεί και για την αυθεντικότητα και ακεραιότητα, αλλά όπως θα δούμε στη συνέχεια, υπάρχουν άλλες καλύτερες τεχνικές για τους σκοπού αυτούς. Πρόκληση αποτελεί η συχνή αλλαγή του χρησιμοποιούμενου κλειδιού καθώς, επίσης και η δημιουργία και η διανομή του κλειδιού με χρήση μη έμπιστου δικτύου, όπου ελλοχεύει ο κίνδυνος υποκλοπής του. Γίνονται πάντως προσπάθειες για την ανάπτυξη τεχνικών για διανομή του κλειδιού με χρήση μη έμπιστου δικτύου, με πιο γνωστό τον αλγόριθμο Diffie – Hellman.

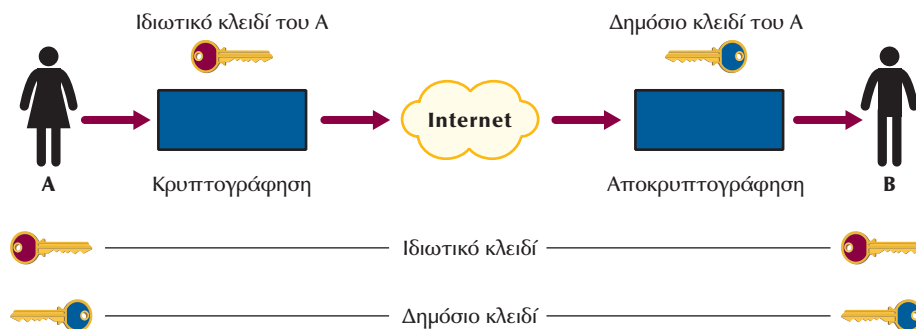
- **Ασυμμετρική Κρυπτογράφηση**

Η ασυμμετρική κρυπτογράφηση αναφέρεται, πολλές φορές, και ως κρυπτογράφηση δημοσίου κλειδιού. Ο μηχανισμός της βασίζεται στην χρήση δύο κλειδιών, ενός δημοσίου κλειδιού και ενός ιδιωτικού. Πρέπει να διευκρινίσουμε, ότι οι αλγόριθμοι ασυμμετρικής κρυπτογράφησης λειτουργούν με τη χρήση δύο διαφορετικών κλειδιών ανά κατεύθυνση και για τον λόγο αυτό ονομάζεται και ασυμμετρική.

Μερικές από τις πιο κοινές χρήσεις της ασυμμετρικής κρυπτογράφησης είναι:

- η εξασφάλιση εμπιστευτικότητας στη μεταδιδόμενη πληροφορία
- η εξασφάλιση αυθεντικότητας

Για να καταλάβουμε, πως διασφαλίζεται η εμπιστευτικότητα και η αυθεντικότητα με τη χρήση της ασυμμετρικής κρυπτογράφησης, θα αναλύσουμε βήμα προς βήμα την επικοινωνία μεταξύ του A και του B.

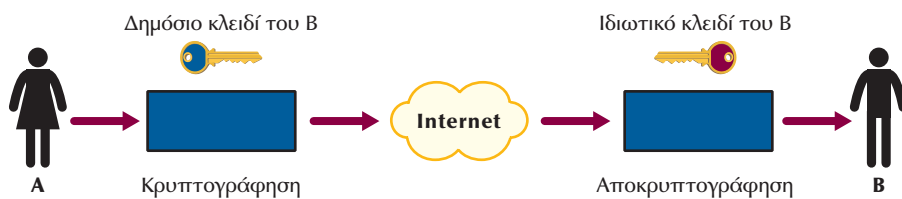


**Σχήμα 8-13** Επικοινωνία με χρήση ασυμμετρικής κρυπτογράφησης

Εάν δύο άτομα ο A και ο B, θέλουν να επικοινωνήσουν, χρειάζεται πρώτα από όλα να έχει ο καθένας από ένα διαφορετικό ζευγάρι δημόσιο / ιδιωτικό κλειδί.

Επίσης, θα πρέπει ο καθένας να είναι γνώστης του δημόσιου κλειδιού του άλλου. Πρέπει να σημειώσουμε ότι η πληροφορία κρυπτογραφείται με το δημόσιο κλειδί και αποκρυπτογραφείται με το ιδιωτικό ή το αντίστροφο. Εδώ πάλι υπάρχει ζήτημα σχετικά με τον τρόπο, που θα μοιραστούν τα δημόσια κλειδιά πάνω από ένα μη ασφαλές δίκτυο.

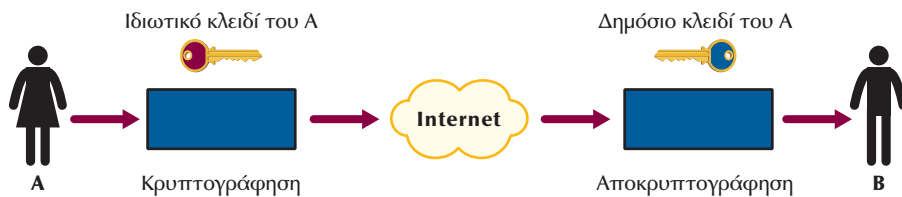
Εάν ο Α θέλει να εξασφαλίσει την εμπιστευτικότητα των δεδομένων, που θα στείλει προς τον Β, δηλαδή να εξασφαλίσει ότι μόνο ο Β θα μπορεί να καταλάβει το περιεχόμενο του μηνύματος, τότε θα κρυπτογραφήσει το μήνυμα, που πρόκειται να μεταδώσει με το δημόσιο κλειδί του Β.



**Σχήμα 8-14** Εμπιστευτικότητα Δεδομένων με χρήση δημόσιου κλειδιού

Με τον τρόπο αυτό, έχουμε εξασφαλίσει ότι μόνο ο Β θα μπορέσει να αποκρυπτογραφήσει το μήνυμα κάνοντας χρήση του ιδιωτικού του κλειδιού, που γνώστης του είναι βέβαια μόνο ο Β.

Στη συνέχεια, θα δούμε με ποιόν τρόπο μπορεί να εξασφαλισθεί η αυθεντικότητα στην επικοινωνία μεταξύ του Α και Β. Για παράδειγμα, πως ο Β θα είναι σίγουρος ότι το μήνυμα έχει σταλεί από τον Α και όχι από κάποιον, που προσποιείται ότι είναι ο Α.



**Σχήμα 8-15** Αυθεντικοποίηση αποστολέα με χρήση δημόσιου κλειδιού

Εάν ο Α κρυπτογραφήσει το μήνυμα με το ιδιωτικό του κλειδί, τότε ο Β θα μπορέσει να το αποκρυπτογραφήσει κάνοντας χρήση του δημοσίου κλειδιού του Α. Εάν η αποκρυπτογράφηση είναι επιτυχής τότε ο Β ξέρει ότι ο Α είναι αυτός που του έστειλε το μήνυμα, αφού μόνο αυτός έχει το ιδιωτικό κλειδί.

Από όσα έχουμε αναφέρει, γίνεται αντιληπτό, ότι η ασυμμετρική κρυπτογράφηση στηρίζεται στο ότι τα ιδιωτικά κλειδιά είναι γνωστά από τους πραγματικούς τους κατόχους και ότι δεν έχουν διαρρεύσει σε άλλα άτομα. Για να αποφευχθούν προβλήματα κλοπής των κλειδιών, που είναι αποθηκευμένα στα λειτουργικά συστήματα των υπολογιστών, έχουν αναπτυχθεί τεχνικές, που κάνουν χρήση έξυπνων καρτών (smartcard).

Οι μηχανισμοί παραγωγής των ζευγαριών δημοσίου / ιδιωτικού κλειδιού είναι σύνθετοι και οδηγούν στη δημιουργία δύο πολύ μεγάλων τυχαίων αριθμών. Η δημιουργία αυτή απαιτεί μεγάλη υπολογιστική ισχύ και πρέπει να τηρείται η εκπλήρωση αυστηρών μαθηματικών κριτηρίων.

Μερικοί από τους πιο κοινούς αλγόριθμους ασυμμετρικής κρυπτογράφησης είναι οι RSA (Rivest, Shamir, Adelman) και ElGamal.

#### • Ψηφιακές υπογραφές

Η ψηφιακή υπογραφή είναι σύνοψη μηνύματος η οποία προσκολλάται στο τέλος ηλεκτρονικού εγγράφου. Η ψηφιακή υπογραφή χρησιμοποιείται κύρια για την απόδειξη της ταυτότητας του αποστολέα καθώς και για την ακεραιότητα των δεδομένων.

Οι ψηφιακές υπογραφές προκύπτουν από το συνδυασμό αλγόριθμου κατατεμαχισμού και ασυμμετρικής κρυπτογράφησης. Οι αλγόριθμοι κατατεμαχισμού δέχονται συνήθως ως είσοδο μηνύματα τυχαίου μήκους και παράγουν συνόψεις μηνύματος συγκεκριμένου μήκους. Οι πλέον διαδεδομένοι αλγόριθμοι κατατεμαχισμού είναι: **Message Digest 4(MD4)**, **Message Digest 5(MD5)** και **Secure Hash Algorithm (SHA)**.

Στη συνέχεια, θα δούμε πως δημιουργείται η ψηφιακή υπογραφή και πως αυτή με τη σειρά της εξασφαλίζει την αυθεντικότητα και την ακεραιότητα, στην επικοινωνία μέσου του δικτύου δύο χρηστών, του Α και Β. Πρώτα από όλα, θα πρέπει οι Α και Β να έχουν συμφωνήσει σε αλγόριθμο δημοσίου κλειδιού (π.χ. τον Digital Signature Standard) και σε αλγόριθμο κατατεμαχισμού (π.χ. MD5). Θα πρέπει, επίσης, να έχουν δημιουργήσει οι Α και Β το ζευγάρι δημόσιου / ιδιωτικού κλειδιού και να ανταλλάξουν τα δημόσια κλειδιά τους. Ας υποθέσουμε, στη συνέχεια, ότι ο Α θέλει να στείλει έγγραφο στον Β κάνοντας χρήση ψηφιακής υπογραφής. Θα πρέπει ο Α να βάλει ως είσοδο στον αλγόριθμο κατατεμαχισμού το έγγραφο και να παράγει το message digest. Στη συνέχεια θα πρέπει να κρυπτογραφήσει το message digest με το ιδιωτικό του κλειδί. Το αποτέλεσμα της κρυπτογράφησης του message digest είναι η ψηφιακή υπογραφή του Α για το συγκεκριμένο έγγραφο και τίθεται στο τέλος του αρχικού εγγράφου. Στη συνέχεια, ο Α θα αποστείλει το αρχικό μήνυ-

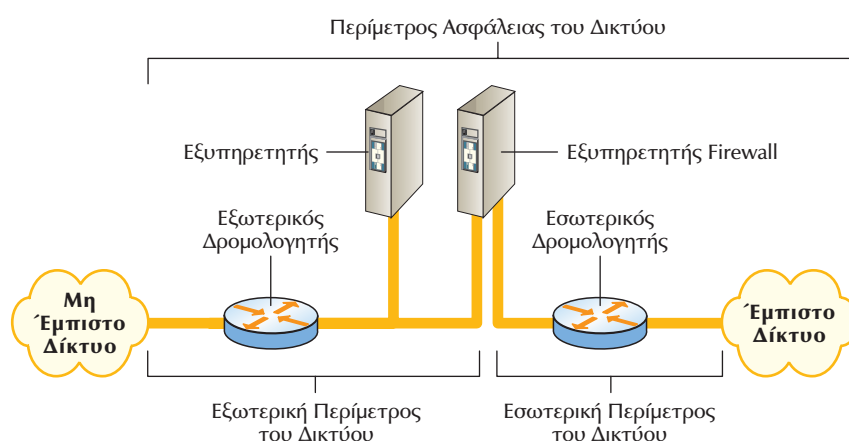
μα μαζί με τη ψηφιακή υπογραφή στον B. Με την σειρά του, ο B θα πάρει το κρυπτογραφημένο μέρος και θα το αποκρυπτογραφήσει με το δημόσιο κλειδί του A. Το αποτέλεσμα της αποκρυπτογράφησης είναι το message digest του εγγράφου. Στη συνέχεια, ο B θα πάρει το αρχικό έγγραφο και θα το περάσει από τον αλγόριθμο κατατεμαχισμού και θα παράγει message digest, το οποίο θα συγκρίνει, εάν είναι το ίδιο με το message digest που προέκυψε από την αποκρυπτογράφηση. Εάν τα δύο message digest είναι ίδια, ο B μπορεί να είναι σίγουρος, ότι το μήνυμα έχει σταλεί από τον A αφού μπόρεσε να κάνει αποκρυπτογράφηση με το δημόσιο κλειδί του A και ότι το έγγραφο δεν έχει υποστεί αλλαγές από τρίτους κατά την αποστολή, αφού τα δύο message digest είναι τα ίδια.

### 8.3.5 Τεχνολογίες ασφάλειας

Όπως αναφέραμε και στην αρχή της παραγράφου 8.3.4, υπάρχει πληθώρα τεχνικών, που προσπαθούν να εξασφαλίσουν λύσεις για τα βασικά στοιχεία που συνθέτουν πολιτική ασφάλειας. Ταυτόχρονα, στην αγορά κυκλοφορούν πολλά προϊόντα ασφάλειας. Επιγραμματικά θα αναφερθούμε ορισμένες από τις πιο δημοφιλείς λύσεις για την εμπιστευτικότητα των δεδομένων και την πιστοποίηση των χρηστών:

- **Σταθερά passwords και passwords μιας χρήσης για πιστοποίηση χρηστών**
  - **SSL / SSH / SOCKS** – συστήματα κρυπτογράφησης δεδομένων για την εξασφάλιση της ακεραιότητας και εμπιστευτικότητας των δεδομένων
  - **Radius / Tacacs** – συστήματα για πιστοποίηση dial up χρηστών και εκχώρηση συγκεκριμένων δικαιωμάτων
  - **PAP / CHAP** – συστήματα για πιστοποίηση δικτυακών συσκευών αλλά όχι χρηστών σε συνδέσεις point to point
  - **Single Sign On** – βασίζεται σε πιστοποιήσεις ενός παράγοντα. Είναι συνήθως, λιγότερο ασφαλές από τη χρήση πολλαπλών passwords
  - **Κέρβερος** – κρυπτογράφηση για τη διασφάλιση της εμπιστευτικότητας των δεδομένων και πιστοποίηση χρηστών
  - **IPSec (IP Security)** – Το Internet Protocol Security είναι αναπτυσσόμενο πρότυπο για ασφάλεια στο επίπεδο του δικτύου. Προηγούμενες προσεγγίσεις ασφάλειας εστιάζονταν στο επίπεδο της εφαρμογής με βάση το OSI μοντέλο. Το IPSec παρέχει δύο επιλογές ασφάλειας:
    - Αυθεντικότητα της Επικεφαλίδας των Ip πακέτων (Authentication Header – AH), όπου παρέχεται η δυνατότητα αυθεντικοποίησης του αποστολέα των πακέτων
    - ESP (Encapsulation Security Payload), όπου υποστηρίζει την αυθεντικότητα τόσο της επικεφαλίδας των πακέτων όσο και των δεδομένων.
- Το IPSec είναι ιδιαίτερα χρήσιμο για δίκτυα VPN καθώς επίσης και για χρήστες που συνδέονται στο δίκτυό με χρήση επιλεγόμενων τηλεφωνικών γραμμών.

- **Firewall** – Με την έννοια Firewall αναφερόμαστε στο σύνολο των προγραμμάτων / φίλτρων, που έχουμε εγκαταστήσει σε πύλες (σημεία σύνδεσης) του εσωτερικού μας δικτύου με άλλα δίκτυα, π.χ το Internet ή άλλο ιδιωτικό / δημόσιο δίκτυο, που δεν ελέγχονται από εμάς. Οι συσκευές που εγκαθίστανται τα προγράμματα / φίλτρα και συνθέτουν ένα Firewall, είναι δρομολογητές και εξυπηρετητές ειδικοί για τον σκοπό αυτόν.



**Σχήμα 8-16** Παράδειγμα δικτύου με χρήση firewall

Στο παραπάνω Σχήμα 8-16 βλέπουμε διαχωρισμό του εσωτερικού δικτύου επιχείρησης με τα υπόλοιπα δίκτυα με την βοήθεια αρχιτεκτονικής βασισμένης σε δρομολογητές και εξυπηρετητές. Οι χρήστες, που βρίσκονται στο τμήμα του δικτύου ευρείας περιοχής πίσω από τον εσωτερικό δρομολογητή, θεωρούμε, ότι ανήκουν στο λεγόμενο έμπιστο δίκτυο αφού συνδέονται άμεσα σε δομή που ελέγχεται, διαχειρίζεται και γενικότερα διέπεται από κανόνες ασφάλειας, που καθορίζονται πλήρως από την επιχείρηση, που κατέχει το δίκτυο. Αντίθετα, το τμήμα του δικτύου ευρείας περιοχής, που συνδέεται στον εξωτερικό δρομολογητή ονομάζεται μη έμπιστο δίκτυο. Η επιχείρηση δεν διαχειρίζεται χρήστες, που ανήκουν στο μη έμπιστο δίκτυο, δηλαδή δεν διέπονται από τις ίδιες διαδικασίες ελέγχου αυθεντικότητας με τους χρήστες του εσωτερικού δικτύου.

Στην παραπάνω τοπολογία, το firewall δημιουργείται από φίλτρα στους δύο δρομολογητές καθώς και από προγράμματα στον firewall server.

Με τους κανόνες, που έχουμε επιβάλει στο firewall, μπορούμε να επιτρέψουμε την πρόσβαση από τα μη έμπιστα δίκτυα προς συγκεκριμένους εξυπηρετη-

τές του εσωτερικού μας δικτύου, καθώς επίσης και το είδος των εφαρμογών, που επιτρέπεται να χρησιμοποιήσουν οι μη έμπιστοι χρήστες, για να συνδεθούν σε αυτούς. Για παράδειγμα μπορούμε να επιτρέψουμε πρόσβαση σε συγκεκριμένες IP διευθύνσεις του εσωτερικού δικτύου και με συγκεκριμένα πρωτόκολλα, όπως HTTP, ενώ προσπάθειες σύνδεσης με άλλα πρωτόκολλα όπως telnet, ftp, tftp rlogin κ.λ.π να απορρίπτονται από το firewall. Το φιλτράρισμα των πρωτοκόλλων γίνεται με βάση τον αριθμό πόρτας που χρησιμοποιούν στην TCP/IP δομή. Στη συνέχεια, το firewall εξετάζει τις επικεφαλίδες των πακέτων από τα μη έμπιστα δίκτυα προς τα έμπιστο δίκτυο, ανιχνεύοντας και απορρίπτοντας άμεσα τα πακέτα με προορισμούς προς απαγορευμένες TCP πόρτες και IP διευθύνσεις. Υπάρχουν αρκετές αρχιτεκτονικές στην τοπολογία διασύνδεσης δρομολογητών και εξυπηρετητών, που συνθέτουν ένα firewall. Ανάλογα με την πολυπλοκότητα της τοπολογίας τόσο πιο δύσκολη είναι η παραβίαση της ασφάλειας του εσωτερικού δικτύου επιχείρησης.

### 8.3.6 Αποφυγή καταστροφών

Κάθε επιχείρηση που έχει αναπτύξει πληροφοριακό σύστημα και βασίζει την λειτουργία της στην εύρυθμη και απρόσκοπτη λειτουργία του πληροφοριακού συστήματός της, θα πρέπει να είναι σε ετοιμότητα να αντιμετωπίσει προβλήματα μικρά ή μεγάλα, που πιθανόν θα προκύψουν.

Τα προβλήματα ενός μοντέρνου και κατανεμημένου πληροφοριακού συστήματος δεν περιορίζονται μόνο στις βλάβες του ενεργού ή παθητικού εξοπλισμού, αλλά συμπεριλαμβάνουν και δυσλειτουργίες των λειτουργικών συστημάτων, των πρωτοκόλλων επικοινωνίας καθώς και των ίδιων των δεδομένων. Τα προβλήματα μπορεί να προέρχονται από συνηθισμένες αστοχίες του εξοπλισμού ενεργού ή παθητικού (π.χ αστοχία σκληρού δίσκου, κάψιμο τροφοδοτικού), από κακές ρυθμίσεις – προγραμματισμούς, από εγγενείς δυσλειτουργίες του εξοπλισμού ή λογισμικού (π.χ bugs), από φυσικές καταστροφές (π.χ πλημμύρες, σεισμούς) αλλά και από κακόβουλες ενέργειες (π.χ επιθέσεις από χάκερ, ή τρομοκρατικές επιθέσεις). Μια επιχείρηση, που σέβεται τους πελάτες της αλλά και το όνομα της, θα πρέπει να είναι σε θέση να αντεπεξέλθει στα προβλήματα, ανεξάρτητα από το μέγεθος και την προέλευση τους, στον ελάχιστο δυνατό χρόνο και με τις λιγότερες συνέπειες, τόσο για την ίδια την εταιρεία όσο και για τους πελάτες της. Για παράδειγμα φανταστείτε τι πλήγμα είναι για την αξιοπιστία μίας τράπεζας ή μιας χρηματιστηριακής εταιρείας η μη εξυπηρέτηση των πελατών της, λόγω τεχνικών προβλημάτων για μεγάλο χρονικό διάστημα. Από όλα όσα έχουμε αναφέρει, οδηγούμαστε στο συμπέρασμα, ότι είναι απαραίτητη η ύπαρξη σχεδίων αποφυγής καταστροφών.

Στο σημείο αυτό, θα αναφερθούμε σε κάποιες έννοιες που σχετίζονται άμεσα με το σχεδιασμό της αποφυγής καταστροφών πληροφοριακού συστήματος:

- **Ανάκαμψη (Recovery)** – Η αποκατάσταση της λειτουργίας πληροφοριακού συστήματος σε επιθυμητό επίπεδο μετά από κάποιο δυσλειτουργία.
- **Σχέδιο Συνέχειας (Continuity Plan)** – Η σαφής και πλήρης περιγραφή των ενεργειών που θα πραγματοποιηθούν, ώστε να επιτευχθεί ανάκαμψη μετά από σοβαρή παραβίαση.
- **Εφεδρικό Αντίγραφο Πληροφοριών (Information back up)** – Η τήρηση αντιγράφων των πληροφοριών, που θα μπορεί να χρησιμοποιηθεί, για να επιτευχθεί ανάκαμψη. Θα μπορούσαμε να συμπεράνουμε ότι απαίτηση για ανάκαμψη πληροφοριακού συστήματος σε μηδέν χρόνο, δηλαδή στην ουσία να μην σταματά ποτέ η λειτουργία του, συνεπάγεται κλωνοποίηση δομής του δικτύου δύο ή ίσως και παραπάνω φορές. Αυτό, όσο και να φαίνεται υπερβολικό, συμβαίνει σε επιχειρήσεις, που βασίζουν την παροχή υπηρεσιών σε πελάτες εξολοκλήρου στο πληροφοριακό τους σύστημα. Αυτό, βέβαια, συνεπάγεται για την επιχείρηση πολύ υψηλό κόστος εγκατάστασης, λειτουργίας και συντήρησης.

Μια επιχείρηση πρέπει να προβεί στη διαβάθμιση της κρισιμότητας των επιμέρους στοιχείων, που συνθέτουν το πληροφοριακό της σύστημα. Με βάση την ανάλυση των κινδύνων που θα προκύψουν, σε περίπτωση καταστροφής κάποιων βαθμίδων του πληροφοριακού συστήματος, θα πρέπει να ληφθούν και τα αντίστοιχα μέτρα προστασίας. Τα περισσότερα πληροφοριακά συστήματα, σήμερα, είναι κατακευκτωμένα και οι εφαρμογές τους κάνουν χρήση της αρχιτεκτονικής client – server. Στις περιπτώσεις αυτές, το κτίριο με τον κεντρικό υπολογιστή (main site) αποτελεί το πιο κρίσιμο σημείο του συστήματος. Για το λόγο αυτό υπάρχουν πολλοί οργανισμοί που έχουν υλοποιήσει δύο κεντρικά sites, έτσι ώστε σε περίπτωση καταστροφής του ενός αυτόματα να αναλάβει το δεύτερο. Η ύπαρξη δύο site προϋποθέτει δύο κεντρικά σχεδόν ισοδύναμα υπολογιστικά συστήματα, καθώς και την κατάλληλη τηλεπικοινωνιακή υποδομή για την πρόσβαση των διαφόρων κατακευκτωμένων σημείων με τα δύο κεντρικά site. Επίσης, τα κεντρικά site θα πρέπει να περιλαμβάνουν πρόβλεψη για επαλληλία των κεντρικών switches, routers καθώς και εναλλακτικότητα στη διασύνδεση των διαφόρων εσωτερικών LAN. Βέβαια πέρα από τις προβλέψεις για την εναλλακτικότητα της δικτυακής υποδομής, θα πρέπει να έχουν καταστρωθεί και σχέδια για αντίστοιχες εφεδρικές λύσεις τόσο για τη τα συστήματα εξοπλισμού του πληροφοριακού συστήματος όσο και για τις εφαρμογές και τα δεδομένα (π.χ. την πολιτική των back up).

Γενικά, δεν υπάρχει καθιερωμένη συνταγή, για τη μορφή σχεδίου αποφυγής καταστροφών για μια επιχείρηση, αφού αυτό ποικίλει με βάση τη δομή του πληροφοριακού συστήματος, τη σπουδαιότητά του καθώς και το χρηματικό ποσό, που είναι διατεθειμένη να ξοδέψει η επιχείρηση. Το σίγουρο είναι ότι πρόκειται για πολύ σοβαρό έργο, η αναβολή ή ο κακός σχεδιασμός του οποίου μπορεί να αποδειχθεί μοιραίο κάποια στιγμή για την ίδια την επιχείρηση.