

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 αντιμετώπισή 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 τρόπος είναι για παράδειγμα 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 πληρώνουν 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 ανάγκης 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.