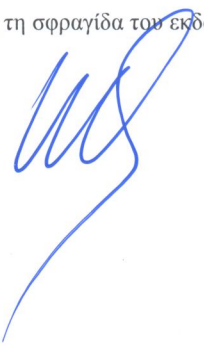
Γ. ΠΑΓΚΑΛΟΣ – Ι. ΜΑΥΡΙΔΗΣ

ΑΣΦΑΛΕΙΑ ΠΛΗΡΟΦΟΡΙΑΚΩΝ ΣΥΣΤΗΜΑΤΩΝ ΚΑΙ ΔΙΚΤΥΩΝ

ΑΝΙΚΟΥΛΑ

Κάθε γνήσιο αντίτυπο φέρει την υπογραφή του συγγραφέα και τη σφραγίδα του εκδότη



ISBN 960-516- 018- 8

ΕΚΔΟΣΕΙΣ ΑΝΙΚΟΥΛΑ
Δημ. Γούναρη 44 τηλ. 0310-235.297, Fax 0310-265.126
Εγνατία 148 τηλ. 0310-239.537 - 546 21 Θεσσαλονίκη
Εγνατία 156 τηλ. 0310-861.917, Fax 0310-265.126, εντός Πανεπιστημίου Μακεδονίας

ΕΠΕΞΕΡΓΑΣΙΑ ΚΕΙΜΕΝΟΥ: Κώστας Κορδαλής - Τηλ. 0310-234.694

ΕΞΩΦΥΛΛΟ: Alter Vision - Τηλ. 0310-322.031

Ενότητα

1

ΒΑΣΙΚΑ ΘΕΜΑΤΑ ΑΣΦΑΛΕΙΑΣ ΠΛΗΡΟΦΟΡΙΑΚΩΝ ΣΥΣΤΗΜΑΤΩΝ

1. Βασικές Έννοιες

Η σημερινή εποχή χαρακτηρίζεται από την ιδιαίτερα μεγάλη ανάπτυξη και την γενικευμένη χρήση της τεχνολογίας της πληροφορικής και των επικοινωνιών. Οι υπολογιστές χρησιμοποιούνται σήμερα σε όλες σχεδόν τις ανθρώπινες δραστηριότητες και σε κάθε είδους εργασίες, εμπορικές, επιστημονικές, κλπ. Παράλληλα όμως αυξάνονται οι κίνδυνοι και τα κρούσματα από ηθελημένες ή τυχαίες καταστροφές, αλλοιώσεις ή μη εξουσιοδοτημένη χρήση των δεδομένων και γενικότερα των υπολογιστικών πόρων. Οι συνέπειες από πιθανές καταστροφές, αλλοιώσεις ή κακή χρήση των δεδομένων μπορούν να σημαίνουν όχι μόνο σημαντικές ζημίες και κόστη, αλλά και κινδύνους για την προστασία των ατομικών δικαιωμάτων των πολιτών.

1.1. Εισαγωγή

Το πρόβλημα της ασφάλειας των πληροφοριών είναι ιδιαίτερα σημαντικό στα σύγχρονα πληροφοριακά συστήματα. Η χρησιμοποίηση όλο και πιο προχωρημένων τεχνικών και τεχνολογιών, όπως για παράδειγμα οι σύγχρονες βάσεις δεδομένων και τα δίκτυα, προσφέρει αναμφισβήτητα σημαντικά πλεονεκτήματα και δυνατότητες, αυξάνει όμως ταυτόχρονα σημαντικά τα προβλήματα τα σχετικά με την προστασία και τη διαθεσιμότητα των πληροφοριών. Στην περίπτωση ενός ιατρικού πληροφοριακού συστήματος, για παράδειγμα, ο ασθενής θα πρέπει να είναι βέβαιος ότι οι προσωπικές του πληροφορίες, ή τα ευαίσθητα προσωπικά του δεδομένα που δόθηκαν κατά την είσοδο του στο νοσοκομείο, ή αυτά που δημιουργήθηκαν κατά την διάρκεια της θεραπείας του σε αυτό, συλλέγονται, αποθηκεύονται και επεξεργάζονται με ένα τρόπο που αποκλείει τυχόν λάθη, διατίθενται μόνο σε ε-

ξουσιοδοτημένους χρήστες και χρησιμοποιούνται με νόμιμο τρόπο.

Η ικανοποίηση των απαιτήσεων για την ασφάλεια των πληροφοριών (information security) είναι συνεπώς μια από τις βασικές προϋποθέσεις για την εισαγωγή και αξιοποίηση της τεχνολογίας της πληροφορικής.

Η ασφάλεια αποτελεί αναγκαία συνθήκη και είναι απαραίτητη, σε συνδυασμό με τις άλλες βασικές προϋποθέσεις λειτουργίας (ποιότητα, απόδοση, κ.ά.), για την εξασφάλιση της εύρυθμης λειτουργίας ενός οργανισμού. Αυτό είναι ιδιαίτερα σημαντικό σήμερα όπου πολύ συχνά το σύνολο των παρεχόμενων υπηρεσιών ενός οργανισμού στηρίζεται στην πληροφορική (π.χ. πάνω από το 80% των υπηρεσιών μιας τράπεζας).

1.2. Τι είναι η Ασφάλεια των Πληροφοριακών Συστημάτων;

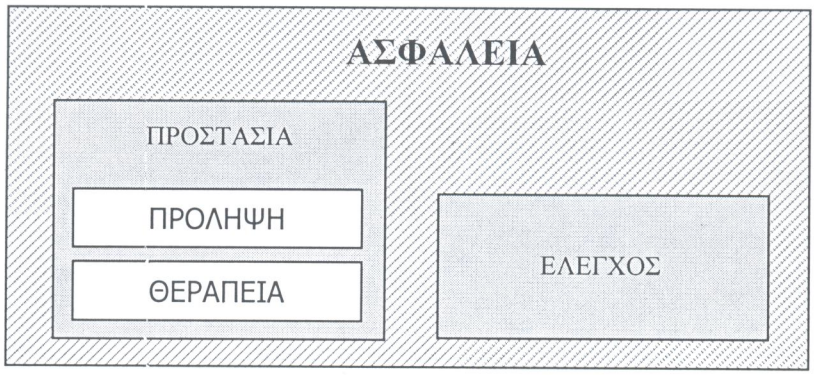
Η έννοια της *ασφάλειας* ενός πληροφοριακού συστήματος σχετίζεται με την ικανότητα ενός οργανισμού να προστατεύει τις πληροφορίες του από τυχόν αλλοιώσεις και καταστροφές, καθώς και από μη εξουσιοδοτημένη χρήση των πόρων του. Σχετίζεται επίσης με την ικανότητά του να παρέχει ορθές και αξιόπιστες πληροφορίες, οι οποίες είναι διαθέσιμες στους εξουσιοδοτημένους χρήστες κάθε φορά που τις αναζητούν. Η ικανότητα αυτή στηρίζεται στη λήψη μέτρων τα οποία διασφαλίζουν την ακεραιότητα και την εμπιστευτικότητα των δεδομένων, καθώς και την αδιάλειπτη λειτουργία του υπολογιστικού συστήματος.

Σύμφωνα με τον προηγούμενο ορισμό της ασφάλειας, η *ασφάλεια πληροφοριακών συστημάτων* έχει να κάνει με την πρόληψη και ανίχνευση μη εξουσιοδοτημένων ενεργειών των χρηστών ενός υπολογιστικού συστήματος καθώς και την λήψη μέτρων. Ποιο συγκεκριμένα η ασφάλεια των πληροφοριακών συστημάτων σχετίζεται με:

- *Πρόληψη (prevention)*: Την λήψη δηλαδή μέτρων για να προληφθούν 'φθορές' των συστατικών ενός πληροφοριακού συστήματος.
- *Ανίχνευση (detection)*: Την λήψη μέτρων για την ανίχνευση του πότε, πως και από ποιον προκλήθηκε φθορά σε ένα συστατικό ενός πληροφοριακού συστήματος.
- *Αντίδραση (reaction)*: Την λήψη δηλαδή μέτρων για την αποκατάσταση ή ανάκτηση των συστατικών ενός πληροφοριακού συστήματος.

Παραδείγματα για κάθε ένα από τα παραπάνω σημεία είναι:

Α. Από την καθημερινή μας ζωή:



Εικόνα 1: **Η έννοια της ασφάλειας.**

- η τοποθέτηση κλειδαριών στις πόρτες ή κάγκελων στα παράθυρα (πρόληψη),
- το σύστημα συναγερμού ή το κλειστό κύκλωμα τηλεόρασης (ανίχνευση),
- η κλήση της ς στυνομίας και η αντικατάσταση κλεμμένων αντικειμένων ή η ασφαλιστική κάλυψη (αντίδραση).

Β. Από το χώρο του ηλεκτρονικού εμπορίου:

- η κρυπτογρ.φημένη διακίνηση δεδομένων παραγγελιών και πληρωμών (πρόληψη),
- η καταγραφή μιας ξένης συναλλαγής στη λίστα της πιστωτικής κάρτας (ανίχνευση),
- και τα πιθανά παράπονα, η ακύρωση συναλλαγής, η αλλαγή κάρτας, κλπ (αντίδραση).

Η ασφάλεια μπερεί ακόμη να θεωρηθεί ότι αποτελείται από δύο κύριες συνιστώσες, την προστασία και τον έλεγχο, από τις οποίες η προστασία αναλύεται στην πρόληψη και την θεραπεία. Αυτό αναπαρίσταται στο σχήμα της παραπάνω εικόνας 1.

Αξίζει να σημειώσουμε σε αυτό το σημείο, ότι δεν είναι εύκολο να δοθεί ένας μονοσήμαντος γενικός ορισμός της ασφάλειας πληροφοριακών συστημάτων. Κατά την μελέτη της ασφάλειας κάθε επιμέρους συστήματος τεχνολογιών πληροφορικής και επικοινωνιών (όπως για παράδειγμα, οι κινητές επικοινωνίες) πρέπει συχνά να δίνεται εξ αρχής ο κατάλληλος ορισμός. Επομένως, πρέπει να δίνεται ιδιαίτερη προσοχή, όταν για παράδειγμα, διαβάζουμε κάποιο σχετικό βιβλίο ή άρθρο, διαφορετικά υπάρχει κίνδυνος να δημιουργηθεί σύγχυση ανάμεσα σε αυτό που εμείς θεωρούμε ως ορισμό της ασφάλειας και τον ορισμό που εννοεί ο συγγραφέας.

1.3. Θεμελιώδεις έννοιες

Είναι γενικά αποδεκτό σήμερα ότι η έννοια της ασφάλειας των πληροφοριακών συστημάτων (information system security) συνδέεται στενά με τρεις βασικές έννοιες:

- *Εμπιστευτικότητα (Confidentiality)*
- *Ακεραιότητα (Integrity),* και
- *Διαθεσιμότητα (Availability)*

1.3.1. Εμπιστευτικότητα

Σε πολλές περιπτώσεις της καθημερινής ζωής οι έννοιες της ασφάλειας και της εμπιστευτικότητας σχεδόν ταυτίζονται, όπως για παράδειγμα στα στρατιωτικά περιβάλλοντα όπου η ασφάλεια έχει τη σημασία του να κρατούνται μυστικές οι πληροφορίες.

Η εμπιστευτικότητα σημαίνει πρόληψη μη εξουσιοδοτημένης (unauthorized) αποκάλυψης πληροφοριών, δηλαδή, πρόληψη από μη εξουσιοδοτημένη ανάγνωση. Επομένως, σημαίνει ότι τα δεδομένα ενός υπολογιστικού συστήματος, καθώς και τα διακινούμενα μεταξύ των υπολογιστών δεδομένα, αποκαλύπτονται μόνο σε εξουσιοδοτημένα άτομα. Αυτό αφορά όχι μόνο την προστασία από μη εξουσιοδοτημένη αποκάλυψη των δεδομένων αυτών καθαυτών αλλά ακόμη και από το γεγονός ότι τα δεδομένα απλώς υπάρχουν. Έτσι για παράδειγμα, το γεγονός ότι κανείς έχει φάκελο εγκληματία είναι συχνά το ίδιο σημαντικό όπως και οι λεπτομέρειες για το έγκλημα που διαπράχθηκε.

Άλλες εκφάνσεις της εμπιστευτικότητας (confidentiality) είναι:

- Η ιδιωτικότητα (privacy): προστασία των δεδομένων προσωπικού χαρακτήρα, δηλαδή αυτών που αφορούν συγκεκριμένα πρόσωπα και
- Η μυστικότητα (secrecy): προστασία των δεδομένων που ανήκουν σε έναν οργανισμό.

1.3.2. Ακεραιότητα

Η ακεραιότητα μπορεί να οριστεί γενικότερα ως η απαίτηση να είναι τα πράγματα όπως πρέπει να είναι. Στην πληροφορική, ακεραιότητα σημαίνει πρόληψη μη εξουσιοδοτημένης μεταβολής πληροφοριών, δηλαδή, πρόληψη από μη εξουσιοδοτημένη εγγραφή ή διαγραφή, συμπεριλαμβανομένης και της μη εξουσιοδοτημένης δημιουργίας δεδομένων.

Επομένως, σημαίνει ότι η μετατροπή, διαγραφή και δημιουργία των δεδομένων ενός υπολογιστικού συστήματος, γίνεται μόνο από εξουσιοδοτημένα μέρη.

1.3.3. Διαθεσιμότητα

Διαθεσιμότητα ονομάζεται η ιδιότητα του να είναι προσπελάσιμες και χωρίς αδικαιολόγητη καθυστέρηση οι υπηρεσίες ενός πληροφοριακού συστήματος (ΠΣ) όταν τις χρειάζεται μια εξουσιοδοτημένη οντότητα. Αυτό σημαίνει ότι οι εξουσιοδοτημένοι χρήστες των υπολογιστικών συστημάτων και των επικοινωνιακών μέσων δεν αντιμετωπίζουν προβλήματα άρνησης εξυπηρέτησης (denial of service) όταν επιθυμούν να προσπελάσουν τους πόρους του συστήματος.

Η διαθεσιμότητα καλύπτει περιοχές πέρα από το φυσικό σκοπό της ασφάλειας. Για παράδειγμα, ένα μεγάλο μέρος της τεχνολογίας που απαιτείται για τη διασφάλιση της διαθεσιμότητας προέρχεται από άλλες περιοχές, όπως fault-tolerant computing.

Για τους σκοπούς της ασφάλειας, μας απασχολεί βασικά η παρεμπόδιση κακόβουλων επιθέσεων που αποσκοπούν στο να παρακωλύσουν την πρόσβαση των νόμιμων χρηστών σε ένα πληροφοριακό σύστημα. Αυτές οι επιθέσεις ονομάζονται *επιθέσεις άρνησης παροχής υπηρεσιών* (denial of service attacks). Η άρνηση παροχής υπηρεσιών σημαίνει παρεμπόδιση της εξουσιοδοτημένης προσπέλασης πληροφοριών και πόρων ή πρόκληση καθυστέρησης των λειτουργιών που είναι κρίσιμες στο χρόνο (time-critical). Η αντιμετώπισή τους αποσκοπεί στο να υπερνικήσει την σκόπιμη (που προκαλείται από κακόβουλα μέρη) παρά τυχαία απώλεια της διαθεσιμότητας. Ένα παράδειγμα επίθεσης άρνησης παροχής υπηρεσιών είναι οι επιθέσεις «πλημμύρας» στο διαδίκτυο, όπου ο επιτιθέμενος κατακλύζει έναν εξυπηρετητή στέλνοντάς του έναν τεράστιο αριθμό αιτήσεων σύνδεσης.

Παρόλο που η διαθεσιμότητα συχνά αναδεικνύεται στο πλέον σημαντικό χαρακτηριστικό της ασφάλειας, εντούτοις λίγοι μηχανισμοί υπάρχουν για να βοηθήσουν στην υποστήριξή της.

1.4. Δευτερεύουσες Έννοιες

Εκτός από τις παραπάνω τρεις θεμελιώδεις έννοιες, υπάρχουν μερικές ακόμη δευτερεύουσες έννοιες της ασφάλειας ΠΣ, όπως:

- *εξουσιοδοτημένη χρήση* (authorized use): μόνο εξουσιοδοτημένα άτομα μπορούν να χρησιμοποιούν το υπολογιστικό σύστημα ή τις περιφερειακές συσκευές του και μόνο σύμφωνα με ένα προκαθορισμένο τρόπο.

- *αυθεντικοποίηση μηνυμάτων* (message authentication)*:* η επιθυμία να γνωρίζουμε με βεβαιότητα κατά τη λήψη ενός μηνύματος (μέσω δικτύου) ότι το άτομο που το σύστημα αξιώνει ότι έστειλε το μήνυμα ότι πράγματι το έστειλε.

- *μη-απάρνηση (non repudiation):* η επιθυμία να γνωρίζουμε με βεβαιότητα κατά πόσον ένα άτομο παρέλαβε ένα μήνυμα που στάλθηκε, έτσι ώστε να μην μπορεί να απαρνηθεί την παραλαβή του.

- *απόδοση ευθυνών* (accountability)*:* στην πράξη δεν είναι εφικτό να προλαμβάνονται και να εμποδίζονται όλες οι ακατάλληλες ενέργειες, αφού ακόμη και εξουσιοδοτημένες ενέργειες μπορεί να προκαλέσουν προβλήματα ασφάλειας, ενώ ολοένα ανακαλύπτονται νέα ρήγματα στην ασφάλεια των συστημάτων. Για την αντιμετώπιση πιθανών παραβάσεων της ασφάλειας, πρέπει οι χρήστες να είναι υπεύθυνοι (υπόλογοι) για τις πράξεις τους. Αυτό γίνεται με την ασφαλή αναγνώριση των χρηστών και τη διατήρηση εγγραφών ελέγχου (audit trails) για τα συμβάντα που αφορούν την ασφάλεια. Στην περίπτωση παράβασης της ασφάλειας του ΠΣ οι εγγραφές αυτές θα χρησιμοποιηθούν για την εξιχνίαση του προβλήματος και την ανακάλυψη του θύτη.

- *αξιοπιστία* (reliability) και *σιγουριά* (safety)*:* η ασφάλεια (security) σχετίζεται με την αξιοπιστία (reliability) και την σιγουριά (safety) καθώς έχει να κάνει με συστήματα που πρέπει να λειτουργούν κανονικά σε αντίξοες συνθήκες, π.χ. συστήματα πυρηνικών σταθμών και ελέγχου εναέριας κυκλοφορίας.

1.4. Παραβάσεις Ασφάλειας

Στο χώρο της ασφάλειας, *έκθεση σε κίνδυνο (exposure)* ονομάζουμε μια μορφή πιθανής απώλειας (loss) ή ζημιάς (harm) σε ένα υπολογιστικό σύστημα. Παραδείγματα εκθέσεων σε κίνδυνο είναι:

- η μη εξουσιοδοτημένη αποκάλυψη δεδομένων
- η μη εξουσιοδοτημένη τροποποίηση δεδομένων
- η άρνηση θεμιτής προσπέλασης υπολογιστικών πόρων

Ευπάθεια (vulnerability) ονομάζεται μια αδυναμία ή ένα ευάλωτο σημείο στο σύστημα ασφάλειας που μπορεί, αν αξιοποιηθεί κατάλληλα, να προκαλέσει απώλειες ή ζημιές.

Όταν ένα άτομο εκμεταλλεύεται μια ευπάθεια τότε διαπράττει μια *επίθεση (attack)* στο σύστημα.

Απειλή (threat) για ένα υπολογιστικό σύστημα αποτελούν καταστάσεις όπου υπάρχει το ενδεχόμενο πρόκλησης απωλειών ή ζημιών. Παραδείγματα απειλών είναι:

- ανθρώπινες επιθέσεις,
- φυσικές καταστροφές,
- ακούσια ανθρώπινα λάθη,
- εσωτερικές ατέλειες του εξοπλισμού ή του λογισμικού.

Έλεγχος (control) είναι ένα προστατευτικό μέτρο, όπως μια πράξη, συσκευή, διαδικασία ή τεχνική, που μειώνει μια ευπάθεια του συστήματος.

1.5. Ευπάθειες

Κάθε ΠΣ είναι ευπαθές σε πιθανές επιθέσεις. Οι πολιτικές και τα προϊόντα ασφάλειας μπορούν να μειώσουν την πιθανότητα του να καταστεί δυνατόν μια επίθεση να διαπεράσει τις άμυνες του συστήματος (ή τουλάχιστο απαιτούν από έναν φιλόδοξο εισβολέα να επενδύσει τόσο χρόνο και πόρους ώστε να μην αξίζει πλέον να συνεχίσει). Θα πρέπει να έχουμε σχετικά υπόψη μας ότι, στην πράξη για καμία σχεδόν δραστηριότητα δεν υπάρχει αυτό που αποκαλούμε πλήρης ασφάλεια ή τελείως ασφαλές σύστημα.

Μια κατηγοριοποίηση των τυπικών σημείων *ευπάθειας (vulnerability)* σε ένα υπολογιστικό σύστημα θα μπορούσε να περιλαμβάνει τα εξής:

- Φυσικές Ευπάθειες (Physical)
- Εκ Φύσεως Ευπάθειες (Natural)
- Ευπάθειες Υλικού και Λογισμικού (Hardware and Software)
- Ευπάθειες Μέσων (Media)
- Ευπάθειες Εκπομπών (Emanation)
- Ευπάθειες Επικοινωνιών (Communications)
- Ανθρώπινες ευπάθειες (Human), κ.ά.

1.5.1. Φυσικές Ευπάθειες

Αφορούν το 'φυσικό περιβάλλον' (για παράδειγμα τα κτίρια και τους χώρους των μηχανογραφικών κέντρων (computer rooms)). Μια πρώτη άμυνα ενάντια σε πιθανές εισβολές παρέχουν τα κλασσικά μέσα προστασίας, όπως ο έλεγχος της

φυσικής προσπέλασης, οι φύλακες, οι βιομετρικές συσκευές, οι αντικλεπτικοί συναγερμοί, κ.ά.).

1.5.2. Εκ Φύσεως Ευπάθειες

Οι υπολογιστές είναι ιδιαίτερα ευπαθείς σε φυσικές καταστροφές και περιβαλλοντικές απειλές, όπως οι πυρκαγιές, οι πλημμύρες, οι σεισμοί, οι κεραυνοί και οι διακοπές ρεύματος. Ακόμη επηρεάζονται αρνητικά από τη σκόνη, την υγρασία και τις ακραίες θερμοκρασιακές συνθήκες.

1.5.3. Ευπάθειες Υλικού και Λογισμικού

Πιθανές δυσλειτουργίες του υλικού και του λογισμικού μπορεί να προκαλέσουν την διακοπή παροχής των υπηρεσιών ενός ΠΣ είτε λόγω ενδογενών σφαλμάτων είτε λόγω εσφαλμένης εγκατάστασης των συστατικών μερών του.

1.5..4. Ευπάθειες Μέσων

Η κλοπή ή καταστροφή μαγνητικών μέσων και εκτυπωτικών καταστάσεων μπορεί να προκαλέσει την απώλεια ή διαρροή ευαίσθητων δεδομένων.

1.5.5. Ευπάθειες Εκπομπών

Όλες οι ηλεκτρονικές συσκευές εκπέμπουν ηλεκτρομαγνητική ακτινοβολία. Με κατάλληλο εξοπλισμό είναι πιθανή η υποκλοπή των εκπεμπόμενων σημάτων από συστήματα και δίκτυα υπολογιστών και η αποκωδικοποίησή τους με σκοπό την υφαρπαγή κρίσιμων πληροφοριών, ή την παρεμπόδιση της ομαλής λειτουργίας ενός πληροφοριακού συστήματος.

1.5.6. Ευπάθειες Επικοινωνιών

Η σύνδεση ενός υπολογιστή σε ένα ανοικτό δίκτυο (όπως το διαδίκτυο (Internet)) αυξάνει τον κίνδυνο διείσδυσης από τρίτα μη εξουσιοδοτημένα μέρη. Με αυτό τον τρόπο, μηνύματα μπορούν να υποκλαπούν, να αλλάξουν διαδρομή και να χαλκευτούν. Οι γραμμές σύνδεσης των υπολογιστών είναι τα συνηθέστερα σημεία που μπορούν να χρησιμοποιηθούν για υποκλοπή ή ακόμη και για καταστροφή.

1.5.7. Ανθρώπινες Ευπάθειες

Οι άνθρωποι που διαχειρίζονται και χρησιμοποιούν ένα υπολογιστικό σύστημα αποτελούν συνήθως την μεγαλύτερη πηγή ευπαθειών για αυτό. Συνήθως, η ασφάλεια ενός ΠΣ εξαρτάται κατά πρώτο λόγο από τους ανθρώπους που το χρησιμοποιούν νόμιμα. Η έλλειψη εκπαίδευσης, ο δόλος, η απροσεξία και η επιπολαιότητα στο χειρισμό ευαίσθητων στοιχείων, όπως για παράδειγμα τα συνθηματικά, καθώς και οι κακοπροαίρετοι ή παραπονεμένοι υπάλληλοι αποτελούν τις μεγαλύτερες απειλές (insiders) για την ασφάλεια ενός ΠΣ.

1.6. Απειλές

Όπως αναφέρθηκε και προηγούμενα, *απειλές* (threats) για ένα υπολογιστικό σύστημα αποτελούν καταστάσεις όπου υπάρχει το ενδεχόμενο πρόκλησης απωλειών ή ζημιών.

Εικόνα 2. **Κανονική ροή**.

1.6.1. Είδη απειλών

Σε σχέση με τους κύριους πόρους ενός πληροφοριακού συστήματος, δηλαδή το υλικό (hardware), το λογισμικό (software) και τα δεδομένα (data), διακρίνουμε τα ακόλουθα είδη απειλών (threats) του:

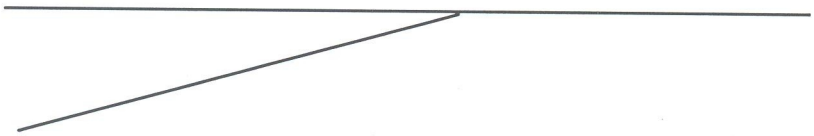
- *Υποκλοπή (interception)*: κάποιο μη-εξουσιοδοτημένο μέρος έχει καταφέρει να αποκτήσει προσπέλαση σε ένα τμήμα του συστήματος. Ενδεικτικά παραδείγματα είναι η κλοπή εξαρτημάτων, η αθέμιτη αντιγραφή προγραμμάτων ή αρχείων δεδομένων, η καλωδιομένη παρακολούθηση ή υποκλοπή γραμμής (wiretapping) με σκοπό την απόκτηση δεδομένων καθώς κυκλοφορούν σε ένα δίκτυο κλπ. Πρόκειται για απειλή κυρίως κατά της εμπιστευτικότητας του συστήματος.

Εικόνα 3. **Υποκλοπή (interception)**.

- *Μεταβολή (modification)*: κάποιο μη-εξουσιοδοτημένο μέρος δεν έχει απλά καταφέρει να αποκτήσει πρόσβαση, αλλά επιπλέον παραποιεί λογισμικό ή δεδομένα. Ενδεικτικά παραδείγματα είναι η τροποποίηση ενός προγράμματος από έναν ιό (virus), η αλλαγή των τιμών σε μια βάση δεδομένων κλπ. Πρόκειται για απειλή κυρίως κατά της ακεραιότητας του συστήματος.

Εικόνα 4. **Μεταβολή (modification).**

- *Πλαστογραφία (fabrication)*: είναι απειλή αποκλειστικά ενάντια στα δεδομένα ενός συστήματος και συμβαίνει όταν κάποιο μη εξουσιοδοτημένο μέρος εισάγει επιπρόσθετα - παραποιημένα δεδομένα σε ένα ΠΣ. Ενδεικτικά παραδείγματα είναι η εισαγωγή πλαστών συναλλαγών σε ένα τραπεζικό περιβάλλον, η προσπάθεια αναπαραγωγής παλιών μηνυμάτων (replay), κλπ. Πρόκειται για απειλή κατά της ακεραιότητας και της διαθεσιμότητας του συστήματος.



Εικόνα 5. **Πλαστοπροσωπία (fabrication).**

- *Διακοπή (interruption)*: ένα μέρος του συστήματος γίνεται μη-διαθέσιμο, ή άχρηστο ή χάνεται εντελώς. Ενδεικτικά παραδείγματα είναι το σβήσιμο προγραμμάτων ή αρχείων, η κακοήθης καταστροφή μιας συσκευής, κλπ. Πρόκειται κυρίως για απειλή κατά της διαθεσιμότητας του συστήματος. Ο όρος άρνηση εξυπηρέτησης (denial of service) - αντίθετος του όρου διαθεσιμότητα - περιγράφει συνήθως μια επιτυχημένη επίθεση διακοπής.

Εικόνα 6. **Διακοπή (interruption).**

1.6.2. Κατηγορίες απειλών

Σε σχέση με την προέλευση τους, οι απειλές εντάσσονται στις τρεις ακόλουθες κατηγορίες:

- *Φυσικές απειλές*: Τέτοιου είδους καταστροφές (φωτιά, πλημμύρα κλπ.) δεν είναι πάντα δυνατόν να αποτραπούν. Όμως είναι σημαντικό η εκδήλωση παρόμοιων γεγονότων να διαπιστώνεται έγκαιρα, ώστε να ελαχιστοποιούνται οι πιθανότητες δραματικών ζημιών. Όπως επίσης σημαντικό είναι να αποφεύγονται ενέργειες που αυξάνουν την πιθανότητα εκδήλωσής τους (όπως για παράδειγμα, το κάπνισμα). Τέλος, η ετοιμότητα χρήσης εφεδρικού συστήματος, σε συνδυασμό με τη λήψη τακτικών εφεδρικών αρχείων (back-ups) για τα κρίσιμα δεδομένα, περιορίζει τις πιθανές δυσάρεστες συνέπειες.
- *Ακούσιες απειλές*: Προκαλούνται είτε από αστοχίες υλικού ή λογισμικού (HW/SW failures), είτε από άγνοια ή αδιαφορία του ανθρώπινου παράγοντα. Σημαντικός παράγοντας πρόκλησης τέτοιων απειλών είναι η έλλειψη σωστής εκπαίδευσης, είτε πρόκειται για απλούς χρήστες είτε για διαχειριστές των συστημάτων. Να σημειωθεί ότι το ποσοστό των προβλημάτων που δημιουργούνται από άγνοια στα πληροφορικά συστήματα είναι πολύ μεγαλύτερο από εκείνο που οφείλεται σε κακή πρόθεση.
- *Εκούσιες απειλές*: Είναι αυτές που απασχολούν περισσότερο τη δημοσιότητα. Στη κατηγορία αυτή, οι κακόβουλοι χρήστες μπορεί να ανήκουν στο εσωτερικό του συστήματος (insiders), για παράδειγμα κάποιοι δυσαρεστημένοι υπάλληλοι. Είναι όμως πιθανό οι απειλές να προέρχονται από κάποιους επίδοξους εισβολείς που είναι εξωτερικοί χρήστες (outsiders). Στη περίπτωση αυτή η επιτυχία των επιθέσεων εξαρτάται κυρίως από τα μέσα που διαθέτουν δηλαδή το χρόνο, την υπολογιστική ισχύ, τις γνώσεις, τα άτομα, τα χρήματα, τις συσκευές και τα εξαρτήματα. Οι κακοήθεις χρήστες μπορεί να επιδιώκουν εκδίκηση, οικονομικό κέρδος, αναγνώριση ή λόγω ιδιοσυγκρασίας απλά τη δημιουργία προβληματικών καταστάσεων και τη διάπραξη βανδαλισμών.

1.7. Μέτρα Προστασίας

Τα *μέτρα προστασίας* (controls) ή *αντίμετρα* (countermeasures) είναι όλες εκείνες οι διαδικασίες, τεχνικές, ενέργειες και συσκευές που περιορίζουν τις ευπάθειες ενός ΠΣ.

Οι διαφορετικοί τύποι αντίμετρων έχουν ως αποτέλεσμα την ανάλυση του προβλήματος της ασφάλειας πληροφοριακών στις ακόλουθες συνιστώσες:

- *Φυσική ασφάλεια συστήματος (physical security).* Αναφέρεται στη προστασία ολόκληρου του σχετικού εξοπλισμού του υπολογιστή από φυσικές καταστροφές, όπως κλοπή, βανδαλισμοί, πλημμύρες, φωτιά κλπ.
- *Ασφάλεια υπολογιστικού συστήματος (computer security).* Αναφέρεται στη προστασία εκείνων των πληροφοριών του υπολογιστή που διαχειρίζεται άμεσα το λειτουργικό σύστημα (προγράμματα εφαρμογών, αρχεία δεδομένων, κ.ά.). Επικεντρώνεται κυρίως στις συγκεκριμένες υπηρεσίες των λειτουργικών συστημάτων που καθορίζουν το ποιος και πως θα δικαιούται να προσπελάσει τα δεδομένα και τις εφαρμογές που φιλοξενεί το υπολογιστικό σύστημα.
- *Ασφάλεια βάσεων δεδομένων (database security).* Αναφέρεται στην ικανότητα του συστήματος να εφαρμόσει μια προκαθορισμένη πολιτική προστασίας των περιεχομένων μιας βάσης δεδομένων, στην οποία διευκρινίζεται ποιοι εξουσιοδοτούνται να δουν ή/και να τροποποιήσουν τα προστατευμένα δεδομένα.
- *Ασφάλεια δικτύων επικοινωνιών (network security).* Αναφέρεται στη προστασία των πληροφοριών κατά τη μετάδοσή τους μέσω των τηλεφωνικών, δορυφορικών ή άλλων δικτύων, όπως είναι τα τοπικά δίκτυα και το Internet.

1.7.1. Κατηγορίες Μέτρων Προστασίας

Γενικά, υπάρχουν τέσσερις βασικοί τρόποι άμυνας οι οποίοι μπορεί να βοηθήσουν ώστε να υπάρξει επαρκής ασφάλεια σε ένα πληροφοριακό σύστημα:

- *Μέτρα προσπέλασης συστήματος.* Εξασφαλίζουν ότι οι μη εξουσιοδοτημένοι χρήστες δεν εισάγονται (log in) στο σύστημα.
- *Μέτρα προσπέλασης δεδομένων.* Ελέγχουν ποιος μπορεί να έχει πρόσβαση σε ποια δεδομένα και με ποιο σκοπό. Οι εφαρμογές βάσεων δεδομένων τυπικά απαιτούν έναν υψηλό βαθμό λεπτομέρειας (granularity) του ελέγχου προσπέλασης.
- *Διαχείριση συστήματος και ασφάλειας.* Εκτέλεση των off-line διαδικασιών που διαμορφώνουν ή επιβάλλουν ένα ασφαλές σύστημα, ορίζοντας ξεκάθαρα τις υπευθυνότητες του διαχειριστή συστήματος, εκπαιδεύοντας τους χρήστες κατάλληλα και ελέγχοντας ότι οι διαδικασίες ασφάλειας τηρούνται από τους χρήστες.
- *Σχεδιασμός συστήματος.* Αξιοποίηση βασικών χαρακτηριστικών και δυνατοτήτων ασφάλειας του υλικού και του λογισμικού.

1.7.2. Τύποι Μέτρων Προστασίας

Οι κύριοι τύποι *μέτρων* (controls) για την πρόληψη της εκμετάλλευσης των ευπαθειών ενός πληροφοριακού συστήματος είναι:

- *Κρυπτογράφηση (encryption).*
  Μετασχηματίζοντας τα δεδομένα ώστε να είναι ακατάληπτα από τον εξωτερικό παρατηρητή, η αξία των υποκλοπών και η πιθανότητα για τροποποιήσεις σχεδόν εκμηδενίζεται.

- *Μέτρα Λογισμικού (software controls).*
  Τα προγράμματα πρέπει να είναι αρκετά ασφαλή και αξιόπιστα ώστε να αποτρέπουν εξωτερικές επιθέσεις. Τα μέτρα προγραμμάτων περιλαμβάνουν:
  - *Μέτρα ανάπτυξης (development controls)*: Πρόκειται για τα πρότυπα (standards) σύμφωνα με τα οποία σχεδιάζονται, κωδικοποιούνται, ελέγχονται και συντηρούνται τα προγράμματα.
  - *Μέτρα λειτουργικού συστήματος (operating system controls)*: Πρόκειται για περιορισμούς που επιβάλλονται από το λειτουργικό σύστημα με σκοπό τη προστασία κάθε χρήστη από τους υπόλοιπους χρήστες.
  - *Μέτρα μέσα στα προγράμματα (internal program controls)*: Πρόκειται για μέτρα που επιβάλλουν περιορισμούς ασφάλειας, όπως για παράδειγμα οι περιορισμοί προσπέλασης σε ένα σύστημα διαχείρισης βάσης δεδομένων (ΣΔΒΔ).

- *Μέτρα Υλικού (hardware controls).*
  Έχουν εφευρεθεί αρκετές συσκευές για να βοηθούν στην ασφάλεια υπολογιστών. Αυτές ποικίλλουν από την υλοποίηση της κρυπτογράφησης με υλικό μέχρι τις συσκευές για επιβεβαίωση της ταυτότητας των χρηστών.

- *Φυσικά Μέτρα Υλικού (physical controls).*
  Τα φυσικά μέτρα είναι από τα πιο εύκολα, πιο αποτελεσματικά και λιγότερο δαπανηρά μέτρα για την ασφάλεια των πληροφοριακών συστημάτων και των συστημάτων βάσεων δεδομένων (για παράδειγμα, κλειδαριές στις πόρτες, φύλακες, αντίγραφα ασφάλειας, κ.ά.).

- *Πολιτικές Ασφάλειας (security policies).*
  Μερικά άλλα μέτρα αποτελούν αντικείμενο πολιτικής, όπως για παράδειγμα ο έλεγχος προσπέλασης. Παρά τα προβλήματα διαχείρισης σε μεγάλους και εξελισσόμενους οργανισμούς, οι πολιτικές ελέγχου προσπέλασης πρέπει να προσαρμόζονται στις επιμέρους συνθήκες και απαιτήσεις ασφάλειας του κάθε πληροφοριακού συστήματος.

1.7.3. Αποτελεσματικότητα των μέτρων προστασίας

Η αποτελεσματικότητα των μέτρων προστασίας ή αντίμετρων εξαρτάται από το πόσο σωστά χρησιμοποιούνται. Ορισμένοι βασικοί παράγοντες που επηρεάζουν την αποτελεσματικότητα των αντίμετρων είναι:

- Η επίγνωση του μεγέθους του προβλήματος.
  Τα άτομα που εφαρμόζουν τα μέτρα, ή ακόμη περισσότερο αυτά που είναι υπεύθυνα για τη διαμόρφωσή τους, πρέπει να έχουν πειστεί για την ανάγκη για ασφάλεια και για το επίπεδο της ασφάλειας που προβλέπεται σε κάθε περίπτωση.

- Οι περιοδικές αναθεωρήσεις.
  Η αμφισβήτηση της αποτελεσματικότητας ενός μέτρου πρέπει να είναι συνεχής. Το περιβάλλον λειτουργίας ενός ΠΣ είναι δυναμικό αφού συνεχώς οι συνθήκες, οι απειλές και οι ανάγκες εξελίσσονται. Είναι πολύ λογικό λοιπόν τα περισσότερα μέτρα προστασίας να παύουν να είναι αποδοτικά αν δεν γίνουν οι κατάλληλες προσαρμογές και αντικαταστάσεις.

- Η αλληλοεπικάλυψη μέτρων.
  Στις περισσότερες περιπτώσεις η ορθή αντιμετώπιση μιας ευπάθειας απαιτεί την εφαρμογή διαφορετικών μεταξύ τους αντίμετρων. Ένας συνδυασμός φυσικών, δικτυακών-επικοινωνιακών και υπολογιστικών μέτρων προστασίας ελαχιστοποιεί τις υπαρκτές απειλές, ενώ συχνά η συνολική αξιοπιστία του συστήματος προστασίας στηρίζεται στις δυνατότητες αλληλοσυμπλήρωσης και αλληλοεπικάλυψης των μέτρων αυτών. Αυτό φυσικά δεν σημαίνει ότι το κάθε μέτρο μεμονωμένα δεν είναι ανθεκτικό και ισχυρό.
  Άλλωστε, σύμφωνα με την *«αρχή του ασθενέστερου σημείου» (weakest point philosophy)*, οι ειδικοί στην ασφάλεια πληροφοριακών συστημάτων πρέπει να συνυπολογίζουν όλα τα υπάρχοντα ρήγματα ασφάλειας, διότι οχυρώνοντας μόνον κάποια από αυτά απλώς κάνουν τις υπόλοιπες ευπάθειες πιο ελκυστικές για όσους κακοήθεις σκοπεύουν να εκδηλώσουν επιθέσεις. Συχνά λέγεται σχετικά ότι η ασφάλεια έχει παρόμοια συμπεριφορά με μια αλυσίδα: η ισχύς της είναι τόση όση και η ισχύς του ασθενέστερου κρίκου της.

- Οι πιθανότητες χρησιμοποίησης.
  Σύμφωνα με την «*αρχή της αποτελεσματικότητας*» (*principle of effectiveness*), για να είναι αποτελεσματικά τα μέτρα πρέπει να χρησιμοποιούνται και να είναι επαρκή, κατάλληλα και εύκολα στη χρήση τους. Δηλαδή, υπονοείται εδώ ότι πρωταρχική προϋπόθεση για την απόδοση ενός μέτρου είναι το να βρίσκεται σε εφαρμογή τη κρίσιμη στιγμή. Αυτό σημαίνει ότι η χρήση των αντίμετρων δεν πρέπει να επηρεάζει αρνητικά τις εργασίες που αυτά προστα-

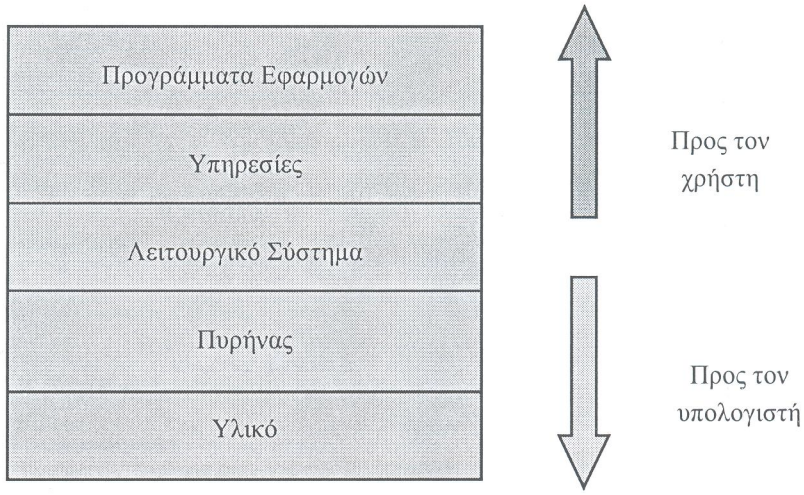
τεύουν και να είναι «οικονομική» ως προς τη κατανάλωση των πόρων του συστήματος (χρόνο, χώρο μνήμης, ανθρώπινη δραστηριότητα κλπ).

1.7.4. Τοποθέτηση των Μέτρων Προστασίας

Ένα τυπικό ΠΣ μπορεί να μοντελοποιηθεί χρησιμοποιώντας πέντε διαφορετικά στρώματα (layers) συστατικών:

- Τα Προγράμματα Εφαρμογών, που είναι προσαρμοσμένα να ικανοποιούν τις απαιτήσεις των χρηστών
- Τις Υπηρεσίες, που χρησιμοποιούνται από τα προγράμματα εφαρμογών, όπως για παράδειγμα αυτές που παρέχονται από ένα ΣΔΒΔ ή ένα κατανεμημένο σύστημα αρχείων.
- Το Λειτουργικό Σύστημα, με βάση το οποίο παρέχονται οι υπηρεσίες και το οποίο παρέχει διαχείριση αρχείων, εκτυπωτών, κ.λ.π.
- Τον Πυρήνα (το κεντρικό τμήμα του λειτουργικού συστήματος), που κανονίζει την προσπέλαση της μνήμης και του επεξεργαστή.
- Το Υλικό, για παράδειγμα επεξεργαστές και μνήμη.

Με βάση τον παραπάνω διαχωρισμό, τα μέτρα προστασίας μπορούν να τοποθετηθούν σε ένα ή περισσότερα στρώματα, όπως δείχνεται στην εικόνα που ακολουθεί:



Εικόνα 7. **Τοποθέτηση των μέτρων προστασίας.**

Οι μηχανισμοί των στρωμάτων που βρίσκονται πιο κοντά στο υλικό θεωρούνται περισσότερο γενικοί και προσανατολισμένοι στον υπολογιστή (computer-oriented), ενώ αυτοί που είναι κοντά στις εφαρμογές είναι περισσότερο προσανατολισμένοι στον χρήστη (user-oriented).

1.8. Απαιτήσεις Ασφάλειας ΠΣ

Ο βασικός σκοπός της ασφάλειας πληροφοριακών συστημάτων πρέπει να είναι η προστασία του υπολογιστικού συστήματος και οποιουδήποτε άλλου στοιχείου που σχετίζεται με αυτό (όπως για παράδειγμα ο Η/Υ αυτός καθαυτός, οι κτιριακές εγκαταστάσεις, οι θέσεις εργασίας, η καλωδίωση, τα μαγνητικά και οπτικά μέσα αποθήκευσης, κ.ά.), με πρώτη προτεραιότητα για τις πληροφορίες που είναι αποθηκευμένες στο ΠΣ.

Αξίζει να σημειωθεί ότι η μη-εξουσιοδοτημένη ενέργεια δεν περιορίζεται μόνο σε μη-εξουσιοδοτημένα πρόσωπα, όπως οι επισκέπτες ενός νοσοκομείου. Ακόμη και εξουσιοδοτημένοι χρήστες, ή ακόμη χειρότερα, διαχειριστές συστήματος, πιθανόν να προσπαθήσουν να εκτελέσουν μη-εξουσιοδοτημένες ενέργειες. Αυτό αυξάνει την ανάγκη για μια τεχνολογία πληροφορικής που να είναι ικανή να παρέχει σε ένα άτομο αναμφισβήτητες αποδείξεις για το αν έκανε μια κάποια ενέργεια ή όχι (*απόδοση ευθυνών*).

1.9. Ασφάλεια των Πληροφοριών που Διακινούνται στο Διαδίκτυο

Η διακίνηση των δεδομένων μέσω του διαδικτύου προσφέρει σημαντικά πλεονεκτήματα σε σχέση με τις κλασικές μεθόδους διακίνησής τους. Τα δεδομένα γίνονται διαθέσιμα σε ελάχιστο χρόνο για χρήση και αξιοποίηση, ανεξάρτητα από τον όγκο τους, ενώ το κόστος αποστολής σε οποιαδήποτε απόσταση είναι εξαιρετικά μικρό. Η χρήση του διαδικτύου προσθέτει όμως επιπλέον απειλές κατά της ασφάλειας των πληροφοριών. Ακόμη, οι συνδεδεμένοι στο διαδίκτυο υπολογιστές είναι δυνατόν να αποτελέσουν στόχο διάφορων επιθέσεων.

Κατά την πραγματοποίηση οποιασδήποτε επικοινωνίας ή συναλλαγής μέσω του διαδικτύου θα πρέπει λοιπόν να εξασφαλίζεται για τα δεδομένα που διακινούνται ότι:

- Δεν είναι αναγνώσιμα και αναγνωρίσιμα παρά μόνο από τον νόμιμο αποστολέα και τον αποδέκτη τους.
- Δεν έχουν αλλοιωθεί κατά τη μεταφορά τους μέσω του διαδικτύου. Δηλαδή, το μήνυμα που παραλήφθηκε είναι το ίδιο με αυτό που αποστάλθηκε .

- Ο αποστολέας και ο παραλήπτης είναι πράγματι αυτοί που ισχυρίζονται ότι είναι.
- Ο αποστολέας δεν είναι δυνατόν να αρνηθεί το γεγονός ότι έστειλε το μήνυμα.
- Οι εμπιστευτικές πληροφορίες προστατεύονται από μη εξουσιοδοτημένη αποκάλυψη.
- Οι υπολογιστές διαθέτουν ικανοποιητική προστασία από ιούς που μεταδίδονται μέσω του διαδικτύου.
- Οι ευαίσθητες πληροφορίες (όπως για παράδειγμα, αριθμοί πιστωτικών καρτών, θέματα εξετάσεων, κλπ.) προστατεύονται επαρκώς όταν διακινούνται μέσω του διαδικτύου (για παράδειγμα, με επαρκή κρυπτογράφηση).

1.10. Προβλήματα κατά την Εισαγωγή Ασφάλειας

Η εισαγωγή (προσθήκη μηχανισμών) ασφάλειας σε ένα ΠΣ είναι ένα δύσκολο και περίπλοκο έργο. Η δυσκολία οφείλεται κυρίως στο ότι:

- τα σύγχρονα πληροφοριακά συστήματα περιέχουν συχνά ένα τεράστιο σε όγκο και πολυπλοκότητα όγκο λογισμικού, και τα μεγάλα έργα λογισμικού έχει ιστορικά αποδειχθεί ότι είναι σχεδόν αδύνατο να υλοποιηθούν χωρίς λάθη.
- η ασφάλεια συνήθως δεν περιλαμβάνεται στο αρχικά σχεδιασμένο ή υλοποιημένο σύστημα αλλά προστίθεται κατόπιν.
- η ασφάλεια κοστίζει, συνήθως αρκετά.
- πολύ συχνά το πρόβλημα έγκειται στους ανθρώπους που χρησιμοποιούν το σύστημα και όχι στην τεχνολογία που χρησιμοποιείται.

1.11. Αναγκαιότητα και Σκοπιμότητα της Ασφάλειας

Είναι γεγονός ότι, παρά την προφανή της χρησιμότητα, η λήψη των απαραίτητων μέτρων ασφάλειας δημιουργεί πολλές φορές κάποια πρόσθετη επιβάρυνση στην απόδοση και το κόστος λειτουργίας του πληροφοριακού συστήματος του οργανισμού. Θα πρέπει ακόμη να αποδεχτούμε το κόστος της ασφάλειας και ως κόστος χρόνου και ως κόστος χρήματος. Συνεπώς, μπορεί να θεωρηθεί ότι η ασφάλεια βρίσκεται σε σχέση αντιστρόφως ανάλογη με την αποδοτικότητα του πληροφοριακού συστήματος του οργανισμού. Αυτό όμως δεν είναι σωστό γιατί η ασφάλεια είναι κόστος αναγκαίο για την ομαλή και εύρυθμη λειτουργία του.

Το συγκεκριμένο κόστος για την ασφάλεια των πληροφοριακών συστημάτων ενός οργανισμού εξαρτάται και προκύπτει από την εκάστοτε ακολουθούμενη πολι-

τική ασφάλειας. Απαιτείται συνεπώς μια πολιτική ασφαλείας η οποία θα πρέπει να εξισορροπεί το κόστος εισαγωγής ασφάλειας από την μία πλευρά και το κόστος ζημιών από πιθανολογούμενο κίνδυνο από την άλλη. Επίσης, θα πρέπει να δημιουργούνται τέτοιες συνθήκες ασφάλειας ώστε να μη παρεμποδίζεται η ευελιξία και η ανάπτυξη του οργανισμού.

Η αναγκαία πολιτική ασφάλειας καθορίζεται από μία δυναμική εκτίμηση του κόστους των μέτρων ασφάλειας σε σχέση με τις συνέπειες που θα έχει για τον οργανισμό οποιαδήποτε πρόκληση δυσλειτουργίας. Ο βασικός αυτός κανόνας ισχύει για όλους τους τομείς και όλα τα επίπεδα ασφάλειας. Έτσι, σε κάθε περίπτωση όπου απαιτείται η λήψη κάποιου μέτρου ασφάλειας, πρέπει να εξετάζεται η πιθανότητα να συμβεί κάποιο γεγονός / πρόβλημα ασφάλειας (possibility of event), σε σχέση με τις συνέπειες που αυτό θα δημιουργήσει (impact). Εάν η τιμή των δύο αυτών παραμέτρων είναι υψηλή, τότε πρέπει απαραίτητα να ληφθούν μέτρα, ανεξάρτητα από το κόστος πρόληψης.

Τέλος, πρέπει να σημειωθεί ότι η ασφάλεια χαρακτηρίζεται από την φύση της ως δυναμική παράμετρος και όχι στατική, καθώς η τεχνολογία, ο ανταγωνισμός, η πολυπλοκότητα των πληροφοριακών συστημάτων και η ολοένα βελτιούμενη επιτηδειότητα των 'επιτιθέμενων', απαιτούν τη λήψη νέων και συνεχώς αυστηρότερων μέτρων ασφάλειας. Συνεπώς, η ακολουθούμενη πολιτική ασφαλείας θα πρέπει να επανεξετάζεται τακτικά και να διορθώνεται όπου αυτό κρίνεται απαραίτητο.

1.12. Προστασία των Προσωπικών Δεδομένων - Νόμος 2472/97

Ένας από τους βασικούς λόγους ανάδειξης της σημαντικότητας της ασφάλειας ΠΣ είναι η διαφύλαξη του προσωπικού απορρήτου (privacy) των ατόμων των οποίων οι εγγραφές διατηρούνται σε υπολογιστικά συστήματα διαφόρων οργανισμών. Αυτή είναι μια δικαιολογημένη και γενικότερα αποδεκτή αρχή, με ελάχιστες αντίθετες απόψεις, καθώς αν ζούσαμε σε μια κοινωνία όπου καθένας ενεργούσε πάντοτε σύμφωνα με την ηθική δεν θα υπήρχε πρόβλημα. Δυστυχώς όμως, ζούμε σε μια κοινωνία όπου οι ενέργειες των λίγων απαιτούν κάποιες προφυλάξεις από τους υπόλοιπους.

Έτσι, «... για την προστασία του ατόμου στην κοινωνία της πληροφορίας δεν αρκούν οι παραδοσιακές θεσμικές εγγυήσεις και ρυθμίσεις, αλλά χρειάζεται ειδική αντιμετώπιση.

Στην Ελλάδα, για τον σκοπό αυτό ιδρύθηκε με τον Νόμο 2472/97 ως ανεξάρτητος διοικητικός φορέας η "ΑΡΧΗ ΠΡΟΣΤΑΣΙΑΣ ΔΕΔΟΜΕΝΩΝ ΠΡΟΣΩΠΙΚΟΥ ΧΑΡΑΚΤΗΡΑ" που λειτουργεί από τον Νοέμβριο του 1997...».

Η σχετική διεύθυνση στο διαδίκτυο είναι : http://www.dpa.gr