6.1 Πληροφοριακό Σύστημα – ΠΣ (*Information System*) : το οργανωμένο σύνολο που περιλαμβάνει επιπρόσθετα με α) το Υλικό και β) το Λογισμικό Μέρος ενός υπολογιστή και γ) τα Δεδομένα δ) τις υπολογιστικές Διαδικασίες καθώς και ε) το ανθρώπινο Δυναμικό που εμπλέκεται στις διαδικασίες. τα οποία συνεργάζονται αρμονικά.

Ασφάλεια ΠΣ (*Security*) **:** το οργανωμένο πλαίσιο για την προστασία των δεδομένων ενός ΠΣ από σκόπιμες ή τυχαίες απειλές από άτομα χωρίς εξουσιοδότηση**.**

Αγαθά ή Πόροι (*Assets*) : Αναφέρεται στις πληροφορίες και στις συσκευές (υπολογιστικοί πόροι).

Τα Μέσα Προστασίας λαμβάνονται με σκοπό :

α) να μειώσουν το κίνδυνο προσβολής από απειλές και

β) να μειώσουν τις επιπτώσεις σε περίπτωση προσβολής.

Αρχές της Ασφάλειας ΠΣ :

1. **Ακεραιότητα** (*Integrity*) : Τα δεδομένα δεν θα πρέπει να τροποποιηθούν ή να αλλοιωθούν. Η λύση που ενδείκνυται είναι η αποτροπή πρόσβασης από μη εξουσιοδοτημένα άτομα.
2. **Διαθεσιμότητα** (*Availability*) : Τα δεδομένα και οι υπηρεσίες θα πρέπει να είναι πάντα στη διάθεση των εξουσιοδοτημένων χρηστών.
3. **Εμπιστευτικότητα** (*Confidentiality*) : Οι ευαίσθητες ή απόρρητες πληροφορίες δεν θα πρέπει να έρθουν στα χέρια μη εξουσιοδοτημένων ατόμων.

6.2 Απειλές

1. **α. Ιοί** (*virus*) : Πρόκειται για ένα πρόγραμμα υπολογιστή το οποίο ενσωματώνεται σε κάποιο αρχείο του υπολογιστή μας και αναπαράγεται δημιουργώντας αντίγραφα του εαυτού του σε κάποιο αρχείο ενός άλλου υπολογιστή (μετά από ανθρώπινη παρέμβαση). Κάποια στιγμή το πρόγραμμα αυτό ενεργοποιείται αυτόματα προκαλώντας ζημιά στον υπολογιστή μας.
   β. Βακτήρια ή προγράμματα κουνέλια (*bacterium*) : Πρόκειται για ένα πρόγραμμα υπολογιστή το οποίο σε αντίθεση με τους ιούς δεν ενσωματώνεται σε κάποιο αρχείο του υπολογιστή μας. Αναπαράγεται δημιουργώντας αντίγραφα του εαυτού του σε άλλες θέσεις του υπολογιστή μας και κάποια στιγμή, όλα τα αντίγραφα αυτά, εκτελούνται ταυτόχρονα με σκοπό να εξαντλήσουν τους πόρους του υπολογιστή.
   γ. Σκουλήκια (worms) : Πρόκειται για ένα πρόγραμμα υπολογιστή το οποίο αναπαράγεται αυτόματα δημιουργώντας αντίγραφα του εαυτού του σε άλλους υπολογιστές. Διασπείρεται αυτόματα (χωρίς ανθρώπινη παρέμβαση) από τον ένα υπολογιστή σε άλλους μέσω του δικτύου στο οποίο ανήκουν.
2. **Κακόβουλο Λογισμικό** (*malware*) : πρόγραμμα με σκοπό να αποκτήσει πρόσβαση σε πόρους του υπολογιστή μας με σκοπό να υποκλέψει προσωπικές μας πληροφορίες.
   α. Λογισμικό Κατασκοπίας (*spyware*) : κυριότερος εκπρόσωπος τα προγράμματα καταγραφής πληκτρολογίου (*key loggers*).
   β. Διαφημιστικό Λογισμικό (*adware*) : τα οποία συνήθως εκτελούν και κατασκοπία καταγράφοντας τις συνήθειες μας ή πρόκειται για λογισμικό κατασκοπίας καμουφλαρισμένο σε αθώο πρόγραμμα διαφημίσεων.
3. **Δούρειος Ίππος** (*Trojan horse*) : πρόγραμμα το οποίο εγκαθίσταται μετά από παραπλάνηση του χρήστη, το οποίο δίνει πρόσβαση σε μη εξουσιοδοτημένα άτομα στον υπολογιστή μας.
4. **Rootkit :** είναι λογισμικό το οποίο μπορεί να ανήκει πολύ εύκολα σε οποιαδήποτε από τις παραπάνω κατηγορίες. Αυτό το λογισμικό έχει την ιδιαιτερότητα να χώνεται ύπουλα σε βασικά αρχεία του Λειτουργικού Συστήματος χωρίς να γίνεται αντιληπτό και να κρύβει με τη σειρά του κάποια κακόβουλα προγράμματα ώστε να μη γίνονται ορατά από το λογισμικό ασφαλείας.
5. **Επιθέσεις Εισβολής** : πρόκειται για ενέργειες ατόμων ώστε να διεισδύσουν σε ένα ΥΣ ή απλώς να το θέσουν σε αδυναμία εξυπηρέτησης των εξουσιοδοτημένων χρηστών του. Η πιο συνηθισμένη επίθεση είναι η DOS (Deny Of Service) που οδηγεί σε αδυναμία εξυπηρέτησης του ΥΣ λόγω υπερβολικού φόρτου εργασίας.

6. **Αδυναμίες Λογισμικών και Λειτουργικών Συστημάτων** (*bugs*) **:** Η λύση που ενδείκνυται είναι η τακτική ενημέρωση όλων των προγραμμάτων και ειδικά του ΛΣ με τις νεώτερες ενημερώσεις (*updates*) καθώς και η εγκατάσταση ενός προγράμματος Τείχους Προστασίας (*fireware*).
7. **Κοινωνική Μηχανική** (*social engineering*) : Μέθοδοι εξαπάτησης διαφόρων ατόμων στηριζόμενοι στις ανθρώπινες συμπεριφορές και αδυναμίες, με σκοπό την απόσπαση εμπιστευτικών πληροφοριών.

6.2 Μέθοδοι προστασίας

1. Διαχείριση καταστροφών

Οι καταστροφές μπορεί :

α) να οφείλονται σε φυσικές αιτίες (π.χ. φωτιά, πλημμύρα, σεισμός).

β) να προέλθουν από ανθρώπινη παρέμβαση λόγω λανθασμένης συμπεριφοράς ή από κακόβουλη πρόθεση.

Αντιμετώπιση :

i. **Αντίγραφα Ασφαλείας** (*back up*)
Πλήρες, Διαφορικό και Αυξητικό

ii. **Πλεονάζων Εξοπλισμός** (*redundant infrastructure*) : Ύπαρξη εφεδρικού εξοπλισμού όμοιο με τον πρώτο το οποίο λειτουργεί ταυτόχρονα. (*mirroring*). Όταν παρουσιαστεί βλάβη στον αρχικό εξοπλισμό μπαίνει σε λειτουργία ο εφεδρικός.
Δεύτερος Δίσκος RAID, Δεύτερος εξυπηρετητής.

iii. **Υπολογιστική Νέφους** (*cloud computing)* : ύπαρξη εξυπηρετητή (ή στην απλούστερη περίπτωση μόνο των δεδομένων) σε μία περιοχή του κυβερνοχώρου. Χρησιμοποιείται ως επέκταση του Πλεονάζοντος Εξοπλισμού.

2. Έλεγχος Πρόσβασης

α) Πρόσβαση με εξουσιοδότηση (*Authorization*) – με χρήση στην απλούστερη περίπτωση ενός ονόματος χρήστη και ενός κωδικού πρόσβασης για κάθε εξουσιοδοτημένο χρήστη - μετά από αυθεντικοποίηση (*Authentication*) – έλεγχο για το δικαίωμα πρόσβασης από το ΥΣ.

β) Χρήση αρχείων καταγραφής για όλες τις ενέργειες οποιουδήποτε χρήστη.

Στα ασύρματα δίκτυα τα πράγματα είναι πιο πολύπλοκα αφού δεν υπάρχει ο περιορισμός της φυσικής παρουσίας του χρήστη μπροστά από τους ελεγχόμενους υπολογιστές του δικτύου. Σήμερα χρησιμοποιούνται τα πρωτόκολλα κρυπτογράφησης WPE, WPA και WPA2.

3. Συστήματα Προστασίας

α) Συστήματα Ανίχνευσης Εισβολής (*IDS*) : Σύστημα παρακολούθησης και ανάλυσης συμβάντων. Δεν έχει σκοπό να αποτρέψει μία απειλή αλλά να εντοπίσει αργότερα τον υπεύθυνο της δολιοφθοράς.

β) Λογισμικό Προστασίας

i. **Προγράμματα προστασίας από ιούς** (*antivirus*)

ii. **Προγράμματα προστασίας από κακόβουλο λογισμικό** (*anti-malware*) : προσφέρει προστασία από μεγαλύτερη γκάμα κακόβουλου λογισμικού. Χρησιμοποιείται συμπληρωματικά με τα προγράμματα προστασία από ιούς.

iii. **Προγράμματα προστασίας από διαφημίσεις** (*anti-adware)* :
Χρησιμοποιείται συμπληρωματικά με τα προγράμματα προστασία από ιούς.

iv. **Προγράμματα Internet Security** : επέκταση της προστασίας από ιούς με ύπαρξη ενός λογισμικού τείχους προστασίας για προστασία από ανεπιθύμητη πρόσβαση.

γ) Τείχος Προστασίας (*fireware)* : Ελέγχει την εισερχόμενη και εξερχόμενη κίνηση των δεδομένων σε ένα δίκτυο και εμποδίζει την πρόσβαση σε δεδομένα τα οποία δεν έχουν ζητηθεί από κάποιον εξουσιοδοτημένο χρήστη του δικτύου και σε περίεργες εφαρμογές λογισμικού. Υλοποιείται και με υλικό το οποίο ενσωματώνεται σε άλλες συσκευές δικτύου.