ΛΕΙΤΟΥΡΓΙΚΑ ΣΥΣΤΗΜΑΤΑ Ι

ΑΣΦΑΛΕΙΑ

Περιεχόμενα

- Ιστορικά Στοιχεία
- Εισαγωγικές Έννοιες – Ορισμοί
- Βασικές Αρχές Ασφάλειας
- Έλεγχος πρόσβασης
- Διαχείριση Ασφάλειας
- Ασφάλεια Λογισμικού
- Ασφάλεια Δικτύου
- Φυσική Ασφάλεια

Ιστορικά Στοιχεία

- Από την έναρξη του ανθρώπινου πολιτισμού έγινε σαφές πόσο σημαντική είναι η ασφάλεια των πληροφοριών.
- Ξεκινώντας από τον αρχαίο πολιτισμό (Κρυπτεία σκυτάλη, κώδικας Καίσαρα κλπ), και μεταβαίνοντας στη σύγχρονη εποχή, είτε σε περίοδο ειρήνης, είτε σε περίοδο πολέμου (Αίνιγμα, αμυντικά συστήματα κλπ).

Ιστορικά Στοιχεία

- Σήμερα με την εξάπλωση του διαδικτύου και γενικότερα της επικοινωνίας με πολλαπλούς τρόπους το ζήτημα της ασφάλειας είναι το πρώτο ζήτημα στον τομέα της πληροφορικής αλλά και γενικότερα της ζωής μας (προσωπικά δεδομένα, κυβερνοέγκλημα, οικονομικά και εθνικά συμφέροντα, πνευματικά δικαιώματα κλπ).
- Διάφορες ομάδες ατόμων καραδοκούν και συχνά καταφέρνουν να υποκλέψουν δεδομένα και να τα εκμεταλλευτούν με διάφορους τρόπους.

Εισαγωγικές Έννοιες – Ορισμοί

- **Ηλεκτρονικό Έγκλημα** είναι οι αξιόποινες εγκληματικές πράξεις που τελούνται με την βοήθεια ηλεκτρονικών υπολογιστών και που τιμωρούνται από τη νομοθεσία. Ανάλογα με τον τρόπο που πραγματοποιούνται διαχωρίζονται:
- Εγκλήματα που έγιναν με τη χρήση Ηλεκτρονικών Υπολογιστών (**computer crime**)
- **Κυβερνοεγκλήματα** (**cyber crime**), εάν έγιναν μέσω του Διαδικτύου.

Εισαγωγικές Έννοιες – Ορισμοί

- Υπάρχουν διάφορες περιπτώσεις Ηλεκτρονικών Εγκλημάτων που περιλαμβάνουν:
  - Τροποποίηση δεδομένων – Κλοπή δεδομένων
  - Παρεμπόδιση κυβερνοκυκλοφορίας
  - Εισβολή σε δίκτυο – Σαμποτάζ σε δίκτυο
  - Μη εξουσιοδοτημένη πρόσβαση
  - Διασπορά ιών – Υπόθαλψη αδικημάτων
  - Πλαστογραφία – Απάτη

Εισαγωγικές Έννοιες – Ορισμοί

- Χάκερς (hackers): αυτά τα άτομα ή ομάδες ατόμων, είναι συνήθως εξαιρετικά μεγάλη απειλή για δικτυωμένα συστήματα γιατί εισβάλουν μέσω του διαδικτύου. Έχουν βαθιές γνώσεις Λειτουργικών Συστημάτων (Operating Systems) και γλωσσών προγραμματισμού (Programming languages).

Εισαγωγικές Έννοιες – Ορισμοί

- Ανάλογα με τις ηθικές τους αρχές χωρίζονται τουλάχιστον στις εξής 3 κατηγορίες:
  - Black Hat:συνήθως εισβάλουν σε συστήματα με σκοπό να κλέψουν, να καταστρέψουν δεδομένα, δημιουργούν κακόβουλο λογισμικό, σπάνε προγράμματα, υποκλέπτουν κωδικούς κ.λπ.
  - White Hat: ψάχνουν για «κενά» (vulnerabilities) ασφαλείας σε Λ.Σ., εφαρμογές κλπ. Δεν έχουν σκοπό την καταστροφή δεδομένων και συνήθως ενημερώνουν τους υπεύθυνους για τα κενά ασφαλείας που βρίσκουν, ώστε να επιδιορθωθούν (ηθικό χάκινγκ).

Εισαγωγικές Έννοιες – Ορισμοί

- Ανάλογα με τις ηθικές τους αρχές χωρίζονται τουλάχιστον στις εξής 3 κατηγορίες:
  - Gray Hat: είναι άτομα που χρησιμοποιούν τους υπολογιστές για να τιμωρήσουν υποτιθέμενους εγκληματίες του Κυβερνοχώρου (Cyberspace). Ονομάζονται και χακτιβιστές (hacktivists) όταν μεταφέρουν πολιτικά μηνύματα μέσω διαδικτύου.

Εισαγωγικές Έννοιες – Ορισμοί

- **Κοινωνική Μηχανική** (social engineering): έχει την έννοια της εξαπάτησης διαφόρων ατόμων, με σκοπό την απόσπαση εμπιστευτικών πληροφοριών. Τέτοια στοιχεία μπορούν να χρησιμοποιηθούν σε διαδικτυακές αγορές ή να πουληθούν σε τρίτους ή για εκφοβισμό και για εκβιασμό των ιδιοκτητών τους.
- Η γνωστότερη τεχνική που χρησιμοποιούν για την απόσπαση πληροφοριών είναι το **ηλεκτρονικό ψάρεμα** (phishing), όπου συνήθως χρησιμοποιούνται πλαστά ηλεκτρονικά μηνύματα (πχ. από τράπεζες) και σύνδεσμοι προς πλαστές ιστοσελίδες και ζητούν την καταχώρηση των πληροφοριών.

Εισαγωγικές Έννοιες – Ορισμοί

- **Απειλές κατά των Δεδομένων**: ονομάζεται ότι μπορεί να συμβεί από εσωτερικό ή εξωτερικό παράγοντα, φυσική καταστροφή, ανθρώπινο λάθος, λογισμικό (πχ. κακόβουλο ή κενό ασφαλείας), εισχώρηση στο δίκτυο, και να προκαλέσει πρόβλημα σ' έναν οργανισμό.
- Μερικά προβλήματα που μπορούν να προκληθούν είναι τα εξής: διαρροή πληροφοριών, τροποποίηση δεδομένων ή η αναστολή λειτουργίας κάποιου υπολογιστικού συστήματος, όπως ένας διακομιστής ιστοσελίδων.

Βασικές Αρχές Ασφαλείας

- Η Ασφάλεια στηρίζεται σε τρεις βασικές αρχές απαραίτητες για την σωστή λειτουργία των Πληροφοριακών Συστημάτων. Αυτές είναι, **Εμπιστευτικότητα**, **Ακεραιότητα**, **Διαθεσιμότητα** ΕΑΔ – (Confidentiality–Integrity–Availability – CIA triad).

Βασικές Αρχές Ασφαλείας

- **Εμπιστευτικότητα (confidentiality)**: Η εξασφάλιση πως τα δεδομένα δε θα γίνουν διαθέσιμα, δε θα μπορούν να τα διαβάσουν δηλαδή, μη εξουσιοδοτημένα άτομα.
- Τα δεδομένα θα πρέπει να κατηγοριοποιούνται ανάλογα με την σημαντικότητά τους και να μπουν διαφορετικοί περιορισμοί σε κάθε κατηγορία που θα δημιουργηθεί.

Βασικές Αρχές Ασφαλείας

- Όσο σημαντικότερα είναι αυτά που πρέπει να προστατευτούν τόσο ισχυρότερα μέτρα θα πρέπει να λαμβάνονται (πχ απομόνωση από το δίκτυο συστημάτων με κρίσιμα δεδομένα, τοποθέτηση επιπλέον μέτρων προστασίας, απενεργοποίηση USB θυρών, κρυπτογράφηση και σε ακραία περίπτωση θα μπορούν να υπάρχουν μόνο τυπωμένα όσα θέλουμε να προστατευτούν πχ: σχέδια, οδηγίες κ.λπ.).

Βασικές Αρχές Ασφαλείας

- **Ακεραιότητα (integrity)**: Εξασφαλίζει πως τα δεδομένα δε θα υποστούν καμία αλλοίωση από μη εξουσιοδοτημένα άτομα ή με μη ανιχνεύσιμο τρόπο. Σε περιπτώσεις τροποποίησης θα πρέπει να παράγονται σχετικά μηνύματα ειδοποίησης (π.χ. με χρήση ελέγχου αθροίσματος MD5, Αντιγράφων ασφαλείας κ.λπ.)

Βασικές Αρχές Ασφαλείας

- **Διαθεσιμότητα (Availability)** Αυτή εξασφαλίζει πως το σύστημα θα μπορεί να παρέχει τις πληροφορίες του, όταν του ζητηθούν και μέσα σε αποδεκτά χρονικά όρια.
- Υπολογιστές, δίκτυα και συσκευές δικτύου θα πρέπει να επιδιορθώνονται όσο γίνεται γρηγορότερα. (π.χ. με Σχέδιο Αποκατάστασης από Καταστροφή – Disaster Recovery Plan και Σχέδιο Επιχειρησιακής Συνέχειας – Business Continuity)

Έλεγχος Πρόσβασης

- Έλεγχος Πρόσβασης (Access Control). Για να μπορέσει ένας οργανισμός να προστατεύσει τις πληροφορίες του από τυχαίες ή εσκεμμένες αλλοιώσεις εξουσιοδοτημένων και από εσκεμμένες αλλοιώσεις από μη εξουσιοδοτημένα άτομα θα πρέπει να εφαρμόσει ελέγχους πρόσβασης στα συστήματα και τους δικτυακούς του πόρους.
- Ο έλεγχος πρόσβασης εφαρμόζεται σε τρεις περιπτώσεις:
  - Δικτυακή πρόσβαση
  - Πρόσβαση σε συστήματα
  - Πρόσβαση στα δεδομένα

Έλεγχος Πρόσβασης

- **Δικτυακή πρόσβαση**: οι χρήστες έχουν την δυνατότητα πρόσβασης σ' όλους τους πόρους του δικτύου. Για το λόγο αυτό θα πρέπει στους πόρους του δικτύου να μπουν περιορισμοί (πχ ποιος-τι), να προστατευτούν και να παρακολουθούνται. Οι χρήστες του Τμήματος Προσωπικού για παράδειγμα, δε θα πρέπει να έχουν πρόσβαση στο δίκτυο του Οικονομικού Τμήματος ενός οργανισμού.

Έλεγχος Πρόσβασης

- **Πρόσβαση σε συστήματα**: οι χρήστες χρησιμοποιούν διάφορα συστήματα του δικτύου όπως διακομιστές (servers), εκτυπωτές (printers) αλλά και κάθε άλλο είδος διαμοιραζόμενης συσκευής (shared device) στο δίκτυο. Η πρόσβαση σ' αυτές τις συσκευές θα πρέπει να περιορίζεται, να προστατεύεται και να παρακολουθείται.

Έλεγχος Πρόσβασης

- Πρόσβαση στα δεδομένα: οι χρήστες έχουν πρόσβαση στα δεδομένα του δικτύου. Διαβάζουν και τροποποιούν αρχεία (files) και Βάσεις Δεδομένων (Databases). Τα δεδομένα θα πρέπει να υπόκεινται σε περιορισμούς, προστασία και παρακολούθηση

Έλεγχος Πρόσβασης

- Ο Έλεγχος Πρόσβασης είναι σημαντικότατος για επιχειρήσεις και οργανισμούς.
  - Η Ακεραιότητα Δεδομένων θα πρέπει να προστατεύεται, δίνοντας δικαιώματα πρόσβασης σε πόρους με βάση τις αρχές: need-to-know και needto-do.
  - Τα δικαιώματα χρηστών θα πρέπει να χορηγούνται ανάλογα με τον ρόλο, τις ευθύνες και τις εργασίες τους.
  - Οι πόροι θα πρέπει να κατηγοριοποιούνται σε επίπεδα (Απόρρητο, Εμπιστευτικό, Δημόσιο).
  - Θα πρέπει να υπάρχουν Αρχεία Καταγραφής συμβάντων (Log files) για εντοπισμό.

Έλεγχος Πρόσβασης

- Πιστοποίηση Ταυτότητας (Authentication) και Εξουσιοδότηση (Authorization) είναι η διαδικασία ταυτοποίησης και επιβεβαίωσης πως κάποιος έχει εξουσιοδότηση πρόσβασης στους δικτυακούς πόρους του οργανισμού, κάτι ανάλογο με το να δείξουμε την αστυνομική μας ταυτότητα για να μπούμε σε κάποιο φυλασσόμενο κτίριο.

Έλεγχος Πρόσβασης

- Στην πληροφορική η πιστοποίηση ταυτότητας γίνεται συνήθως με το Όνομα Χρήστη (username) και με τον κωδικό του (password). Δεν είναι ο ασφαλέστερος τρόπος και υπάρχουν πολλοί άλλοι, για παράδειγμα με βιομετρικά στοιχεία (δακτυλικό αποτύπωμα, ίριδα ματιού κ.λπ.).

Έλεγχος Πρόσβασης

- Εφαρμογή Έλεγχου Πρόσβασης. Δύο διαδομένες μορφές υλοποίησης Ελέγχου Πρόσβασης είναι:
  - οι Λίστες Ελέγχου Πρόσβασης (ACL – Access Control Lists)
  - Το Active Directory (AD) ή LDAP

Έλεγχος Πρόσβασης

- Με τις Λίστες Ελέγχου Πρόσβασης (ACL) σε κάθε πόρο του δικτύου ή του συστήματος μπορούν να εφαρμοστούν δύο βασικοί κανόνες: επιτρέπεται (allow) και δεν επιτρέπεται (deny).
- Οι ACL μπορούν να εφαρμοστούν σε συστήματα αρχείων (file systems) και σε δίκτυα (networks).

Έλεγχος Πρόσβασης

- ACL συστήματος αρχείων. Τα αρχεία έχουν τριών ειδών δικαιώματα: **Ανάγνωσης** (**Read**), **Εγγραφής** (**Write**) και **Εκτέλεσης** (**eXecute**) που επιτρέπουν τις ανάλογες ενέργειες πάνω στα αρχεία. Τα δικαιώματα μπορούν να δοθούν σε χρήστες και σε ομάδες (σε ΛΣ Linux με την εντολή chmod).

Έλεγχος Πρόσβασης

- ACL δικτύου: με τις ACL μπορούν να δοθούν δικαιώματα πρόσβασης στους πόρους του δικτύου. Λειτουργούν σαν φίλτρα και μπορούν να ελέγχουν την κίνηση ΑΠΟ και ΠΡΟΣ το δίκτυο του οργανισμού (κυρίως επίπεδο δικτύου και μεταφοράς του TCP/IP).

Έλεγχος Πρόσβασης

- Το **LDAP (Lightweight Directory Access Protocol)** είναι ανοιχτού κώδικα (open source) και ορίζει τον τρόπο που οι πληροφορίες του οργανισμού μπορούν να προσπελαθούν από τον καθένα. Χρησιμοποιείται για την αποθήκευση πληροφοριών **Πιστοποίησης Ταυτότητας, Εξουσιοδότησης** των χρηστών αλλά και **Ρόλων.**

Έλεγχος Πρόσβασης

- Λειτουργεί με το μοντέλο **πελάτη/εξυπηρετητή (Client/Server)**. Οι πελάτες για να αποκτήσουν πρόσβαση στους πόρους του δικτύου και σε εφαρμογές, θα πρέπει πρώτα να Πιστοποιήσουν την Ταυτότητά τους στον LDAP Server, για να τους δώσει εξουσιοδότηση χρήσης τους.

Έλεγχος Πρόσβασης

- Το **Active Directory** (AD) είναι αναπτυγμένο από την Microsoft και παρέχει υπηρεσίες Πιστοποίησης Ταυτότητας και Εξουσιοδότησης. Έχει κεντρική διαχείριση και αποθηκεύει πληροφορίες Χρηστών, Ομάδων, Συστημάτων και πόρων ως αντικείμενα (Objects). Τα αντικείμενα αυτά οργανώνονται σε Οργανικές Μονάδες (Organizational Units – OU) και μπορούν να εφαρμοστούν πάνω τους πολιτικές δικαιωμάτων.

Διαχείριση Ασφάλειας

- Η Διαχείριση Ασφαλείας έχει ως σκοπό την προστασία των Πληροφοριακών Συστημάτων περιορίζοντας την επικινδυνότητα παραβίασης κάποιας από τις τρεις Βασικές Αρχές ΕΑΔ σε αποδεκτό όριο.

Διαχείριση Ασφάλειας

- Οι διαδικασίες που περιλαμβάνει συνοπτικά είναι:
  - Η **Διαχείριση Κινδύνου**, για να προσδιοριστεί το αποδεκτό επίπεδο ασφαλείας
  - Η **ανάπτυξη και εφαρμογή Σχεδίου Ασφαλείας** με την οποία θα μπορεί να επιτευχθεί το επιθυμητό επίπεδο ασφάλειας
  - Η **Επαναφορά από Καταστροφή** και η **Επιχειρησιακή Συνέχεια.**

Διαχείριση Ασφάλειας

- Διαχείριση Κίνδυνου ή Επικινδυνότητας (Risk Management). Είναι μια διαδικασία εύρεσης:
  - Ευπαθειών (vulnerabilities) και Απειλών (threats) στις οποίες μπορούν εκτεθούν οι πληροφορίες
  - των Αντιμέτρων (Countermeasures) ή Μέτρων Ασφαλείας (Security Measures) ή Μέτρων Προστασίας (Controls) που θα παρθούν για να μειωθεί ο κίνδυνος αλλοίωσης των πληροφοριών αυτών

Διαχείριση Ασφάλειας

- Οι Απειλές και οι Ευπάθειες μεταβάλλονται με την πάροδο του χρόνου, επομένως η διαδικασία αναγνώρισής τους είναι μια διαδικασία που δε γίνεται μόνο μια φορά, αλλά επαναλαμβάνεται συχνά. Για την καλύτερη δίνουμε τους εξής ορισμούς:
  - **Κίνδυνος**: είναι η πιθανότητα μια απειλή να γίνει πραγματικότητα.
  - **Αντίμετρα** (Countermeasures) ή **Μέτρα Ασφαλείας** (Security Measures) ή **Μέτρα Προστασίας** (Controls): είναι το μέτρα που λαμβάνονται για την αντιμετώπιση μιας απειλής σε ένα Πληροφοριακό Σύστημα.

Διαχείριση Ασφάλειας

- **Απειλή (Threat)**: είναι καθετί που μπορεί να συμβεί από ανθρώπινο παράγοντα (πχ. λάθος χειρισμός), φυσικό συμβάν (πχ. πλημμύρα) ή λογισμικό (πχ. κακόβουλο λογισμικό) και να παρακάμψει κάποια από τις τρεις Βασικές Αρχές: Εμπιστευτικότητα, Ακεραιότητα, Διαθεσιμότητα του Πληροφοριακού Συστήματος.

Διαχείριση Ασφάλειας

- **Ευπάθεια (Vulnerability)**: είναι οι αδυναμίες που μπορεί να υπάρξουν σ' ένα Πληροφοριακό Σύστημα και επιτρέπουν να γίνει κάποια Απειλή πραγματικότητα. Τέτοιες αδυναμίες μπορεί να υπάρξουν για παράδειγμα: στις ρυθμίσεις παραμέτρων του δικτύου, σε εγκατεστημένα προγράμματα, στον τρόπο που λειτουργεί ο οργανισμός κ.λπ.

Ασφάλεια Λογισμικού

- Λογισμικό Κακόβουλης Χρήσης (Malware) είναι το λογισμικό που μπορεί να προκαλέσει κάποιου είδους ζημιά στα συστήματα. Υπάρχουν άτομα αλλά και ομάδες ατόμων που χρησιμοποιούν προγράμματα ή εκμεταλλεύονται (exploit) κενά ασφαλείας εγκατεστημένων προγραμμάτων για διάφορους λόγους. Διασκέδαση, επίδειξη ικανοτήτων, οικονομικό όφελος, εκδίκηση αλλά και εκφοβισμό.

Ασφάλεια Λογισμικού

- Υπάρχουν πολλά είδη κακόβουλου λογισμικού με γνωστότερες κατηγορίες τις εξής:
  - **Spyware**: σκοπό έχουν την συλλογή πληροφοριών και την αποστολή τους στον δημιουργό τους. Καταγράφουν τις δραστηριότητες σε σελίδες αλλά και ό,τι πληκτρολογεί (keylogger) ο χρήστης.
  - **Adware**: προβάλλουν ανεπιθύμητες διαφημίσεις και καταγράφουν τις συνήθειες του χρήστη και τις αποστέλλουν. Συνήθως είναι μέρος δωρεάν προγραμμάτων και πρόσθετων σε φυλλομετρητές.

Ασφάλεια Λογισμικού

- Trojan (horse): αυτό που επιδιώκουν είναι να δώσουν άμεση πρόσβαση στον διαχειριστή τους στο σύστημα και τα αρχεία του. Η εγκατάστασή του γίνεται υπό την κάλυψη κάποιου χρήσιμου προγράμματος ή παιχνιδιού. Με την εκτέλεση του μολυσμένου αρχείου (του Δούρειου ίππου – trojan) το οποίο έχει μέσα του δυο προγράμματα, το χρήσιμο και το Trojan, εγκαθίστανται και τα δυο και το χρήσιμο εκτελείται κανονικά.

Ασφάλεια Λογισμικού

- Viruses: ο προορισμός τους καθορίζεται από τον δημιουργό τους. Μπορεί να είναι ακίνδυνοι αλλά και επιβλαβής για συστήματα και χρήστες. Μεταδίδονται μέσω της εκτέλεσης των αρχείων στα οποία έχουν προσκολληθεί σε άλλα υγιή αρχεία.
- Worms: μπορούν να στέλνουν προσωπικά δεδομένα στους δημιουργούς τους. Μεταδίδονται μέσω δικτύων και ηλεκτρονικών μηνυμάτων (emails) και επιβαρύνουν την κίνηση του δικτύου.

Ασφάλεια Λογισμικού

- **Backdoor**: με τις Κερκόπορτες ο δημιουργός τους αποκτά κανάλι επικοινωνίας με τον Η/Υ όπου εγκαταστάθηκε και μπορεί να εκτελέσει εντολές σε αυτόν όποτε θελήσει. Συνήθως εισχωρούν με την βοήθεια Trojan.

Ασφάλεια Λογισμικού

- **Botnet**: είναι το δίκτυο από Bots, δηλαδή τους Η/Υ θύματα με το κακόβουλο λογισμικό. Η εγκατάσταση του λογισμικού γίνεται συνήθως από φυλλομετρητές, από Trojan και από συνημμένα ηλεκτρονικών μηνυμάτων (email attachments). Το δίκτυο των Η/Υ θυμάτων μπορεί και ελέγχεται κεντρικά μέσω πρωτοκόλλων όπως το IRC, HTTP και συχνά χρησιμοποιείται για επιθέσεις Άρνησης Υπηρεσιών (Denial of Services).

Ασφάλεια Λογισμικού

- **Rootkit**: είναι ένα πολύ δύσκολα εντοπιζόμενο κακόβουλο λογισμικό που συνήθως καλύπτει άλλα κακόβουλα λογισμικά όπως τα Backdoors.

Ασφάλεια Λογισμικού

- Η χρήση προγραμμάτων **προστασίας (antivirus) από κακόβουλα λογισμικά** είναι απαραίτητη. Η προσβολή συστημάτων εντός ενός οργανισμού μπορεί να προκαλέσει προβλήματα στις Βασικές Αρχές ασφαλείας, τριάδα ΕΑΔ, Εμπιστευτικότητα, Ακεραιότητα και Διαθεσιμότητα.

Ασφάλεια Λογισμικού

- Η επιλογή των προγραμμάτων αυτών δεν θα πρέπει να γίνεται με κριτήρια, όπως τις δυνατότητες προστασίας που προσφέρει αλλά και τις δυνατότητες του συστήματος που θα εγκατασταθεί. Ενδεικτικά θα πρέπει να έχει τις εξής δυνατότητες:
  - Ανίχνευση όλων των ειδών κακόβουλων λογισμικών
  - Ανίχνευση συμπιεσμένων αρχείων
  - Αυτόματη ανίχνευση USB συσκευών
  - Προστασία των ηλεκτρονικών μηνυμάτων και άμεσων μηνυμάτων

Ασφάλεια Λογισμικού

- Πέρα της επιλογής του κατάλληλου προγράμματος προστασίας θα πρέπει στη συνέχεια να γίνουν και οι σωστές ρυθμίσεις του:
  - Αυτόματη ενημέρωση της βάσης του και του προγράμματος
  - Ενεργοποίηση των δυνατοτήτων του προγράμματος προστασίας
  - Τακτικό πλήρη έλεγχο του συστήματος
  - Προστασία των ρυθμίσεων με κωδικό

Ασφάλεια Λογισμικού

- Σημαντικότατος είναι ο ρόλος των χρηστών στην έκθεση συστημάτων σε απειλές. Επιβάλλεται οι χρήστες να συνδέονται στα συστήματα με λογαριασμούς περιορισμένων δικαιωμάτων (τυπικού χρήστη – typical user).
- Σε περιπτώσεις συνδέσεως με πλήρη δικαιώματα (διαχειριστή – Administrator) είναι ιδιαίτερα επικίνδυνη η προσβολή από κακόβουλο λογισμικό γιατί αυτό θα μπορεί να επηρεάσει πολύ σοβαρότερα ένα σύστημα από ότι εάν είχε γίνει σε σύνδεση απλού χρήστη.

Ασφάλεια Δικτύου

- Σημαντικά τμήματά της για την ασφάλεια και την σωστή λειτουργία του δικτύου είναι:
  - Τείχος Προστασίας (Firewall), μπορεί να είναι λογισμικό ή υλικό και σκοπός του είναι να ελέγχει την κίνηση μεταξύ των δικτύων που συνδέει και ανάλογα με τις λίστες ελέγχου πρόσβασης (ACL) που έχει να την επιτρέπει ή να την απορρίπτει.

Ασφάλεια Δικτύου

- **Εικονικό Ιδιωτικό Δίκτυο (Virtual Private Network – VPN)** είναι μια υπηρεσία πελάτη/εξυπηρετητή (client/server) που επιτρέπει την επικοινωνία συστημάτων με ασφάλεια μέσω ενός εικονικού τούνελ. Έτσι θα μπορούσε κάποιος που βρίσκεται μακριά , με την χρήση ενός προγράμματος πελάτη VPN που θα τρέξει στον Η/Υ του να συνδεθεί στον εξυπηρετητή VPN του οργανισμού και αυτός να του δώσει πρόσβαση στο εσωτερικό δίκτυο σαν να βρισκότανε εντός του δικτύου.

Ασφάλεια Δικτύου

- **Σύστημα Ανίχνευσης Εισβολής** (Intrusion Detection System – IDS), με αυτό παρακολουθείται και αναλύεται ό,τι συμβαίνει στο δίκτυο του οργανισμού. Σκοπός του είναι, να εντοπίζει προσπάθειες εισβολής μη εξουσιοδοτημένων ατόμων σε συστήματα, καθώς κάτι τέτοιο θα έβαζε σε κίνδυνο παραβίαση κάποιας αρχής από την τριάδα των Βασικών Αρχών (ΕΑΔ). Το IDS παρακολουθεί όλη την κίνηση του δικτύου που πρέπει κάπως να του διοχετεύεται.

Φυσική Ασφάλεια

- **Φυσική ασφάλεια** είναι η προστασία του χώρου ενός οργανισμού και του εξοπλισμού του από απειλές όπως φωτιά, κλοπή κ.λπ. Είναι εξίσου σημαντική με τα άλλα μέτρα ασφαλείας γιατί μέσα στον χώρο υπάρχει η υποδομή του Πληροφοριακού Συστήματος.
- Θα πρέπει να εξασφαλίζονται οι απαιτούμενες περιβαλλοντολογικές συνθήκες. Να υπάρχει συναγερμός για παραβιάσεις αλλά και για έκτακτες περιπτώσεις, όπως φωτιά και να γίνεται έλεγχος φυσικής πρόσβασης.

Αναφορές

- Wikipedia (https://en.wikipedia.org/)
- Λειτουργικά Συστήματα και Ασφάλεια Πληροφοριακών Συστημάτων, Β' Τάξη ΕΠΑΛ, Τομέα Πληροφορικής