Ενότητα 6
Ασφάλεια Δικτύων Υπολογιστών

Υλικό και Δίκτυα Υπολογιστών · Β΄ Τάξη ΕΠΑΛ – Τομέας Πληροφορικής

Πάλλας Αναστάσιος Καθ. Πληροφορικής ΠΕ86

6.1 Ασφάλεια Πληροφοριακού Συστήματος

Εμπιστευτικότητα (Confidentiality)

Ακεραιότητα (Integrity)

Διαθεσιμότητα (Availability)

- Αγαθά (Assets): δεδομένα, λογισμικό, υλικό, άνθρωποι, υπηρεσίες
- Πολιτική Ασφάλειας: γραπτό έγγραφο που ορίζει κανόνες προστασίας
- Στόχοι: αποφυγή απώλειας δεδομένων, μη εξουσιοδοτημένη πρόσβαση
- Κίνδυνοι: φυσικές καταστροφές, κλοπή, βανδαλισμός, κυβερνοεπιθέσεις
- Κόστος ασφάλειας vs Κόστος βλάβης — ισορροπία

6.2.1 Τι είναι Απειλές — Είδη Απειλών

Εσωτερικές Απειλές

- Δυσαρεστημένοι υπάλληλοι
- Αμέλεια — ανθρώπινο λάθος
- Μη εξουσιοδοτημένη πρόσβαση
- Κλοπή εξοπλισμού / δεδομένων
- Κακή χρήση δικαιωμάτων

Εξωτερικές Απειλές

- Hacker / Cracker εισβολή
- Κακόβουλο λογισμικό
- Phishing & Social Engineering
- DDoS επιθέσεις
- Φυσικές καταστροφές

6.2.2–6.2.5 Κακόβουλο Λογισμικό (Malware)

Ιοί (Viruses)

- Προσκολλώνται σε αρχεία
- Εξαπλώνονται μέσω κοινής χρήσης
- Ενεργοποιούνται με εκτέλεση
- Καταστρέφουν δεδομένα

Σκουλήκια (Worms)

- Αυτοαναπαραγωγή στο δίκτυο
- Δεν χρειάζονται αρχείο ξενιστή
- Καταναλώνουν bandwidth
- π.χ. WannaCry

Δούρειοι Ίπποι

- Φαίνονται νόμιμα προγράμματα
- Κρύβουν κακόβουλο κώδικα
- Backdoor — απομακρυσμένη πρόσβαση
- Keyloggers — καταγραφή πληκτρολ.

Άλλα Malware

- Spyware: κατασκοπεία
- Adware: διαφημίσεις
- Ransomware: λύτρα
- Rootkit: βαθιά απόκρυψη

6.2.5 & 6.2.6 Επιθέσεις Εισβολής & Αδυναμίες

- DoS (Denial of Service): πλημμύρα αιτημάτων → αδυναμία εξυπηρέτησης
- DDoS: κατανεμημένο DoS — χιλιάδες υπολογιστές (botnet) ταυτόχρονα
- SQL Injection: εισαγωγή κακόβουλου SQL σε φόρμες
- Man-in-the-Middle (MitM): παρεμβολή στη επικοινωνία
- Brute Force: δοκιμή κωδικών μέχρι επιτυχία
- Αδυναμίες Λογισμικού: buffer overflow, zero-day vulnerabilities
- Αδυναμίες ΛΣ: μη ενημερωμένα patches — εκμεταλλεύονται exploits

6.3.1 Διαχείριση Καταστροφών — Backup & Recovery

Στρατηγικές Backup

- Πλήρες (Full): αντίγραφο όλων
- Σχετικό (Incremental): μόνο αλλαγές
- Διαφορικό (Differential): αλλαγές από τελευταίο full
- 3-2-1 Κανόνας: 3 αντίγραφα, 2 μέσα, 1 εκτός
- Cloud Backup — Ταινία (LTO)

Ανάκαμψη (Disaster Recovery)

- BCP: Business Continuity Plan
- RTO: χρόνος αποκατάστασης
- RPO: μέγιστη αποδεκτή απώλεια δεδομένων
- Cloud DR — Site αντιγράφου
- UPS — Γεννήτρια για αδιάλειπτη λειτουργία

6.3.2 Έλεγχος Πρόσβασης

- **Αυθεντικοποίηση** (Authentication): επαλήθευση ταυτότητας χρήστη
- **Εξουσιοδότηση** (Authorization): δικαιώματα πρόσβασης σε πόρους
- **Κωδικός πρόσβασης**: minimum 12 χαρακτήρες, περίπλοκος, μοναδικός
- **MFA** (Πολυπαραγοντική Αυθεντικοποίηση): password + OTP + biometrics
- **ACL** (Access Control List): λίστα δικαιωμάτων ανά χρήστη/ομάδα
- **Wireless**: WPA3 + RADIUS server + MAC filtering + ξεχωριστό Guest SSID
- **VLAN**: εικονική τμηματοποίηση δικτύου για απομόνωση

6.3.3 Συστήματα Προστασίας

IDS/IPS

- Ανίχνευση (IDS) / Πρόληψη (IPS)
- Εισβολής
- Signature-based & Anomaly-based
- Network (NIDS) / Host (HIDS)
- Ειδοποίηση ή αποκλεισμός

Antivirus / Anti-malware

- Ανίχνευση γνωστών απειλών
- Real-time scan
- Ενημέρωση ορισμών (virus defs)
- Quarantine — απομόνωση
- Προστασία web & email

Τείχος Προστασίας (Firewall)

- Φιλτράρει κίνηση δικτύου
- Κανόνες (rules) allow/deny
- Packet Filtering — Stateful
- Application Firewall (WAF)
- Hardware vs Software

Ασφάλεια Wi-Fi

- WEP: παλαιό & μη ασφαλές
- WPA: βελτιωμένο — TKIP
- WPA2: AES — ισχυρό
- WPA3: 2018 — ισχυρότατο
- RADIUS: επιχειρηματική λύση

Βέλτιστες Πρακτικές Ασφάλειας Δικτύου

- Τακτικές ενημερώσεις (patches) σε λειτουργικά & εφαρμογές
- Ισχυροί κωδικοί + MFA για όλους τους λογαριασμούς
- Αρχή ελάχιστων δικαιωμάτων: ο χρήστης έχει μόνο όσα δικαιώματα χρειάζεται
- Κρυπτογράφηση δεδομένων: HTTPS, VPN, TLS/SSL, AES
- Τακτικά backups + επαλήθευση αποκατάστασης
- Εκπαίδευση χρηστών: phishing awareness, κοινωνική μηχανική
- Καταγραφή (Logging) & παρακολούθηση (Monitoring) δικτύου

Κρυπτογράφηση & VPN

Συμμετρική Κρυπτογράφηση

- Ένα κλειδί για κρυπτ. & αποκρ.
- Γρήγορη — AES 128/256-bit
- Κίνδυνος κοινής χρήσης κλειδιού
- π.χ. AES, DES, 3DES

Ασύμμετρη Κρυπτογράφηση

- Ζεύγος δημόσιο/ιδιωτικό κλειδί
- Αργή — ασφαλής ανταλλαγή
- Ψηφιακές υπογραφές
- RSA, ECC — TLS/SSL

VPN (Virtual Private Network)

- **Εικονικό** Ιδιωτικό Δίκτυο
- Κρυπτογραφημένο tunnel
- Ασφαλής απομακρυσμένη πρόσβαση
- IPsec, OpenVPN, WireGuard

Ανακεφαλαίωση Ενότητας 6

- CIA: Εμπιστευτικότητα, Ακεραιότητα, Διαθεσιμότητα — ο πυρήνας της ασφάλειας
- Απειλές: εσωτερικές & εξωτερικές — DoS, DDoS, MitM, SQL Injection
- Malware: Ιοί, Worms, Trojans, Ransomware, Spyware
- Διαχείριση Καταστροφών: 3-2-1 Backup, BCP, RTO, RPO
- Έλεγχος Πρόσβασης: MFA, ACL, VLAN, WPA3, RADIUS
- Προστασία: Firewall (stateful), IDS/IPS, Antivirus, WAF
- Κρυπτογράφηση: AES (συμμ.), RSA (ασύμμ.) — VPN για ασφαλή σύνδεση