



Διαδικτυακές Επιθέσεις

Οι διαδικτυακές επιθέσεις πραγματοποιούνται με σκοπό τη μη εξουσιοδοτημένη πρόσβαση στις πληροφορίες κάποιου ατόμου ή οργανισμού, και στη συνέχεια την καταστροφή ή την κλοπή τους. Στόχοι των διαδικτυακών επιθέσεων μπορούν να είναι πληροφοριακά συστήματα υπολογιστών, δίκτυα υπολογιστών, αλλά και προσωπικοί ηλεκτρονικοί υπολογιστές.

Ενδεικτικοί τύποι επιθέσεων:

- 1. Επιθέσεις τύπου DOS και DDOS (Distributed Denial-of-Service):** Πρόκειται για επιθέσεις που οδηγούν έναν εξυπηρετητή να αρνείται να εξυπηρετήσει. Στόχος είναι να κατακλυστεί η προσφερόμενη υπηρεσία, για παράδειγμα μια ιστοσελίδα, από ταυτόχρονες αιτήσεις, με αποτέλεσμα ο εξυπηρετητής (server) να μην μπορεί να ανταποκριθεί.
- 2. Phishing και Social Engineering Attacks:** Επιθέσεις τύπου ηλεκτρονικού ψαρέματος και κοινωνικής μηχανικής. Οι επιθέσεις αυτού του τύπου εκμεταλλεύονται την παρουσία των ατόμων στα κοινωνικά δίκτυα και την έμφυτη ανάγκη του ατόμου για επικοινωνία σε αυτά. Με τεχνικές όπως ψεύτικες εκστρατείες πληροφόρησης, κατασκευασμένα προφίλ κοινωνικών δικτύων και μηνύματα προσεκτικά κατασκευασμένα ώστε να τραβήξουν την προσοχή του μη υποψιασμένου χρήστη, ένας hacker μπορεί να αντλήσει προσωπικές πληροφορίες και να αποκτήσει μη εξουσιοδοτημένη πρόσβαση στα αρχεία του ή ακόμη και στους τραπεζικούς του λογαριασμούς.
- 3. Λυτρισμικό (Ransomware):** Οι επιθέσεις αυτού του τύπου είναι πολύ επικίνδυνες και βρίσκονται σε έξαρση. Πρόκειται για κακόβουλα προγράμματα που όταν εκτελεστούν στον μολυσμένο υπολογιστή, κρυπτογραφούν το σύνολο των αρχείων, καθιστώντας τη χρήση του πρακτικά αδύνατη. Σε πολλές περιπτώσεις, ο hacker που κατασκεύασε το λυτρισμικό, απαιτεί από τον χρήστη λύτρα προκειμένου να του παρέχει το κλειδί αποκρυπτογράφησης των αρχείων του. Το πρόβλημα μεγενθύνεται όταν η μόλυνση προχωρά πέραν του μεμονωμένου υπολογιστή ενός χρήστη και επεκτείνεται σε ολόκληρα δίκτυα υπολογιστών οργανισμών με καταστροφικά αποτελέσματα.