Elenco delle minacce

1. Malware:

Descrizione: Software dannoso che può infettare computer e sistemi informatici.

Esempi: Virus, worm, Trojan horse, ransomware, spyware.

Danni: Furto di dati, danni ai sistemi, perdita di produttività.

Prevenzione: Antivirus, firewall, software di anti-malware, aggiornamenti software regolari.

2. Phishing:

Descrizione: Tentativo di ingannare gli utenti per indurli a rivelare informazioni sensibili.

Esempi: Email di phishing, siti web contraffatti, social engineering.

Danni: Furto di dati, accesso non autorizzato agli account, frode finanziaria.

Prevenzione: Formazione sulla sicurezza informatica, attenzione ai link sospetti, verifica delle email e dei siti web.

3. Attacchi DDoS:

Descrizione: Tentativo di sovraccaricare un server o un sito web con traffico falso.

Esempi: Attacchi SYN flood, UDP flood, HTTP flood.

Danni: Interruzione del servizio, perdita di fatturato, danni alla reputazione.

Prevenzione: Soluzioni di protezione DDoS, firewall, bilanciamento del carico.

4. Furto di dati:

Descrizione: Accesso non autorizzato e acquisizione di dati sensibili.

Esempi: Hacking, violazioni di dati, insider threat.

Danni: Perdita finanziaria, danni alla reputazione, violazione della privacy.

Prevenzione: Crittografia dei dati, controllo degli accessi, formazione sulla sicurezza informatica.

5. Social engineering:

Descrizione: Manipolazione psicologica degli utenti per indurli a compiere azioni dannose.

Esempi: Phishing, vishing, baiting.

Danni: Furto di dati, accesso non autorizzato agli account, frode finanziaria.

Prevenzione: Formazione sulla sicurezza informatica, consapevolezza dei rischi, attenzione alle richieste sospette.

6. Ransomware:

Descrizione: Tipo di malware che blocca l'accesso ai dati e richiede un riscatto per sbloccarli.

Esempi: CryptoLocker, WannaCry, Locky.

Danni: Perdita di dati, interruzione del servizio, perdita finanziaria.

Prevenzione: Backup regolari, antivirus, software di anti-ransomware.

7. Zero-day attacks:

Descrizione: Attacchi che sfruttano vulnerabilità software sconosciute ai vendor.

Esempi: Stuxnet, Spectre, Meltdown.

Danni: Furto di dati, accesso non autorizzato agli account, danni ai sistemi.

Prevenzione: Aggiornamenti software regolari, patch di sicurezza, soluzioni di protezione avanzate.

8. Insider threat:

Descrizione: Minacce provenienti da persone interne all'azienda con accesso ai dati o ai sistemi.

Esempi: Dipendenti infedeli, ex dipendenti, hacker con accesso privilegiato.

Danni: Furto di dati, sabotaggio, danni alla reputazione.

Prevenzione: Controlli di accesso rigorosi, formazione sulla sicurezza informatica, monitoraggio delle attività degli utenti.