Cele mai frecvente tipuri de pericole și atacuri cibernetice

Good Digital Hygiene for Startups

https://good-start.eu/

O dată cu digitalizarea, riscul atacurilor cibernetice este în continuă creștere. Cel mai adesea, ținta acestor atacuri sunt informațiile sau datele utilizate de o organizație. Scopul atacurilor este în principal acela de a fura, schimba sau distruge date.
Există o multitudine de tipuri de atacuri, cele mai frecvente fiind cele de mai jos.

1. **Ransomware.** Ransomware este un tip de software rău intenționat conceput pentru a bloca accesul la un sistem informatic sau la fișiere până când o sumă de bani sau răscumpărare este plătită atacatorului. Poate cripta fișierele, făcându-le inaccesibile victimei.
2. **Programe malware.** Malware, prescurtarea pentru software rău intenționat, este un termen folosit pentru a descrie orice software sau cod creat cu intenția de a dăuna unui sistem informatic, de a fura date sau de a perturba operațiunile normale. Acesta include diferite tipuri, cum ar fi viruși, worms și troieni.
3. **Man-in-the-middle (MITM).** MITM este un tip de atac în care atacatorul retransmite în secret și eventual modifică mesajele dintre două părți care cred că comunică direct între ele, deoarece atacatorul s-a introdus între cele două părți utilizatoare.
4. **Inginerie socială.** Ingineria socială este o metodă de manipulare a indivizilor pentru a dezvălui informații sensibile sau pentru a efectua acțiuni care pot compromite securitatea. Tehnicile includ phishing, uzurparea identității și manipularea psihologică pentru a exploata comportamentul uman.
5. **Amenințări la adresa datelor.** Amenințările la adresa datelor includ acțiuni intenționate sau neintenționate care compromit confidențialitatea, integritatea sau disponibilitatea datelor. Aceasta include încălcări ale datelor, scurgeri sau orice acces neautorizat sau divulgare a informațiilor sensibile.
6. **Refuzul serviciului (DoS).** Refuzul serviciului este un atac care are ca scop perturbarea sau dezactivarea funcționării normale a unui sistem informatic, a unei rețele sau a unui serviciu, făcându-l temporar sau pe termen nelimitat indisponibil utilizatorilor. Distributed Denial of Service – refuz de serviciu distribuit (DdoS) implică mai multe sisteme care coordonează atacul.
7. **Amenințări pe internet.** Amenințările pe internet se referă la întreruperi intenționate sau neintenționate ale internetului sau comunicațiilor electronice, provocând întreruperi, opriri sau cenzură. Aceste amenințări pot rezulta din diverși factori, inclusiv atacuri cibernetice, probleme tehnice sau acțiuni direcționate de guvern.
8. **Manipularea informațiilor.** Manipularea informațiilor implică eforturi intenționate și coordonate pentru a avea un impact negativ asupra valorilor, procedurilor și proceselor politice. Aceasta poate include răspândirea dezinformării, a știrilor false sau desfășurarea de activități care manipulează opinia publică sau perturbă fluxurile normale de informații.
9. **Atacuri asupra lanțului de aprovizionare.** Atacurile asupra lanțului de aprovizionare vizează relația dintre organizații și furnizorii lor. Aceste atacuri implică compromiterea securității lanțului de aprovizionare pentru a obține acces neautorizat sau influență asupra unei organizații țintă. Exemplele includ compromiterea actualizărilor software sau a componentelor hardware.
10. **Amenințări la adresa disponibilității – amenințări care împiedică accesul la internet.** Acestea includ capturarea fizică și distrugerea infrastructurii internetului, precum și cenzurarea activă a site-urilor de știri sau a rețelelor sociale.
11. **Dezinformare – distribuirea de informații înșelătoare.** Folosirea crescută a rețelelor sociale și mass-media online a condus la o creștere a campaniilor de răspândire a dezinformarii (informații falsificate intenționat) și intoxicărilor (distribuirea de date greșite). Scopul este de a provoca frică și incertitudine. Tehnologia „deepfake” înseamnă că este deja posibil să fie generate sunet, video sau imagini false care aproape că nu se pot distinge de cele reale. Roboții online care pretind a fi oameni adevărați pot perturba comunitățile online, inundându-le cu comentarii false.