Ako posilniť vašu kybernetickú bezpečnosť

Ľuboš Batěk

Pozor, nepřítel naslouchá !

- Ciele útokov
  - Ekonomický zisk (výkupné, vydieranie).
  - Krádež údajov (osobných, finančných, citlivých – zdrojové kódy).
  - Narušenie činnosti organizácie (znefunkčnenie finančnej správy).
  - Poškodenie dobrého mena firmy, politickej strany.
  - Špionáž alebo sabotáž (útoky realizované iným štátom).

Kybernetické hrozby

- Najčastejšie typy útokov
  - Phishing (Podvodné e-maily alebo správy)

    Cieľ: získať prihlasovacie údaje, citlivé dáta vydávaním sa za dôveryhodnú osobu/inštitúciu.

    Príklad: E-mail s falošným linkom na banku, kde má obeť "overiť údaje".
  - Cielený phishing – prispôsobený konkrétnej osobe (napr. zamestnanec úradu).

    Príklad: E-mail od nadriadeného, obchodného partnera o zmene čísla bankového účtu.
  - Malvér (škodlivý softvér)

    Typy: vírusy, trójske kone, ransomware, spyware, keyloggery.

    Cieľ: poškodiť, ukradnúť dáta, vydierať alebo získať prístup, najčastejšie cez prílohu e-mailu, ktorá po otvorení zašifruje disk (ransomware) alebo linku na spustenie nežiadúceho SW
  - Ransomware

    Špecifický typ malvéru – zašifruje dáta a požaduje výkupné.

Kybernetické hrozby

- Najčastejšie typy útokov
  - Zero-day útoky

    Využívanie zraniteľností, ktoré ešte nie sú verejne známe alebo opravené.

    Obzvlášť nebezpečné – obrana je veľmi ťažká.

    Nemusia sa týkať len nového softvéru.

    Vo všeobecnosti sa netýkajú len pracovných staníc.

Kybernetické hrozby - ochrana

- Používanie zdravého rozumu
- Budovanie bezpečnostného povedomia používateľov
  - Učiť sa, učiť sa, učiť sa, aj keď je to otravné
  - Preverovať znalosti používateľov – bonus: môžu ich využiť aj doma
- Antivírusová ochrana
- Zabezpečenie firewallom
  - Dnes štandardná požiadavka, vrátane VPN prístupu
- Zálohovanie dát
  - Pozor, čo sa zálohuje (či to už nie je napadnuté)
  - Jednosmerná, riadená a kontrolovaná komunikácia
  - Offsite zálohy

Kybernetické hrozby - ochrana

- Aktualizácia operačných systémov a programového vybavenia
  - Otravné ! Vyžaduje reštart, stratím rozpracované veci !
  - Interná smernica – Bezpečnosť pracovných staníc

    Kontrola dodržiavania
  - Vynútenie aktualizácií architektúrou

    Neaktualizovaná pracovná stanica nemá prístup do internej siete
  - Aktualizácia aj iného ako Microsoft softvéru
- Kontrola pracovných staníc na výskyt nežiadúceho SW
  - Manuálna náhodná kontrola
  - GDPR

    Služobné auto – GPS, kontrola čistoty
  - Interné smernice, informovanie zamestnanca

Ďakujem za pozornosť

Ing. Ľuboš Batěk, LL.M.

CGEIT, CRISC, CDPSE

lubos.batek@disig.sk

Disig, a.s.

Galvaniho Business Center IV

Galvaniho 17/C, 821 04 Bratislava