Információs rendszerek biztonságtechnikája

Social engineering

Vakulya Gergely

A social engineering

- Az emberi tényező kihasználható tulajdonságaira építő támadási forma
- Az emberek befolyásolására, manipulálására alapoz
- Lehetséges célok:
  - Bizalmas információk megszerzése
  - Szándékos károkozás
- *A social engineering a befolyásolás és a rábeszélés eszközével megtéveszti az embereket, manipulálja, vagy meggyőzi őket, hogy a social engineer tényleg az, akinek mondja magát. Ennek eredményeként a social engineer – technológia használatával vagy anélkül – képes az embereket információszerzés érdekében kihasználni.* – Kevin Mitnick

Miért hatékony a social engineering?

- A munkavállaló a legtöbb védendő értékhez közvetlenül hozzáférheti
  - Hardver
  - Szoftver
  - Adatok (például fejlesztési, üzleti, kontakt stb.)
- Ez a fajta támadás nem a (fizikai, vagy logikai) biztonsági rendszert, hanem a humán erőforrást támadja.
- A munkavállalók nem tulajdonítanak kellő jelentőséget a rájuk bizott adatoknak. Önmagukban, kontextus nélkül nem értelmezhetők.
  - Felhasználónév jelszó nélkül
  - Jelszó felhasználónév nélkül
  - Akár felhasználónév és jelszó együtt, amivel *úgysem tud mit kezdeni*
  - Születési idők, becenevek, hobbik, gyerekek, házikedvencek nevei.
  - Infrastruktúrára vonatkozó adatok (gépek nevei, számozási sémák stb.)

Social engineering módszerek

Az áldozat megtévesztéséhez, a ráhatáshoz nincsen szükség számítógép használatára.

- Telefonhívás: A partner nehezen tudja a támadót azonosítani
  - Segítség kérése, főleg ha sürgős
  - Felettesnek adja ki magát
  - Látszólag lényegtelen dolgokat kérdez statisztikai céllal
  - Adategyeztetés
- Személyes behatolás: Bizonyos feltételek esetén (nem túl kicsi vállalat, de nincs belépőkártya, vagy kód)
  - Új alkalmazott
  - Látogató
  - Ügyfél
  - Eltévedt
  - Karbantartó
  - Valakihez jött

Két klasszikus példa

Piggybacking

- Valakihez csatlakozva hatol be a támadó.
- Pl. otthon hagyott belépőkártya, vagy épp nem becsukódó ajtó

Tailgating

- A támadó egy csoporthoz csatlakozik, majd leválik

Esettanulmány: CVE-2024-3094 (XZ-Utils SSH backdoor