INFORMATIKAI BIZTONSÁG

Tóth Péter

ADAT BIZTONSÁG

A digitális adatok védelme a lopás, a korrupció vagy a jogosulatlan hozzáférés ellen a digitális adatok teljes életciklusa során

ADAT BIZTONSÁG

A tárolóeszközök és hardver fizikai biztonságától kezdve, az adminisztratív hozzáférésen keresztül a szoftveres biztonsági tényezőkig mindent magába foglal

Mi ellen védekezünk?

Véletlenek, hozzá nem értés, hiba

Ártó szándékú program (Malware)

- Vírus
- Trójai
- Férgek
- Kiskapuk

Ártó szándékú emberek

Védekezés

Biztonsági mentés

Automatikus mentés

Visszaállítási pontok

Megfelelő jogosultsági szabályzat

Megfelelő eszközhasználati szabályzat

Megfelelő víruskeresési eljárások

Adatfolyam támadása

- Megszakítás (Interruption)
- Elfogás (Interception)
- Módosítás (Modification)
- Gyártás (Fabrication)

Támadók és célcsoportjaik

Ki lehet támadó?

- Kormányok, titkosszolgálatok, kémek
- Terroristák
- Ipari kémek, vállalkozások
- Scammerek, csalók

Támadók és célcsoportjaik

Jellemzőik (scammerek kivételével)

- Szervezettség
- Felsőbb irányítás
- Kitartó támadások
- Széles eszköztár
- „low and slow” megközelítés

Leggyakoribb támadási típusok

- Maleware: kártékony szoftver
- Phising attack (Adathalász támadás): Hivatalosnak tűnő üzenetek, emailek kártékony linkkekkel
- Jelszó támadások: Keylogger, shoulder surfing, Dictionary attacks, brute force https://youtu.be/z4_oqTZJqCo?t=82
- Man in The Middle: Két fél közötti kommunikációs csatornát hallgatja le a támadó
- SQL injection: Weboldalak kéréseibe kártékony SQL lekérdezéseket írnak
- DoS / DDoS (Denial of service / Didtributed Denial of Service): Terheléses támadás
- Zero-Day Exploit: Hálózat, rendszer, alkalmazás üzemeltetője hibát talál, de nem tudja időben kijavítani. Userek tájékoztatása a sebezhetőségről -> Hackerekhez is eljut

Védekezés, megelőzés

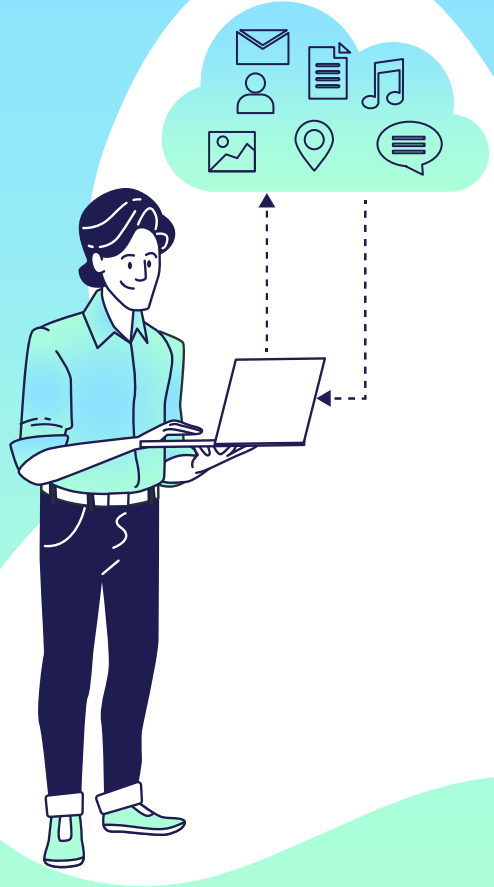
- Maleware: Vírusírtók, tűzfal, rendszeres frissítések, felhasználói magatartás
- Phising attack (Adathalász támadás): Anti-phising eszközök, email szűrők, spam filter
- Jelszó támadások: Nehezen kitalálható jelszó, password policy, gyakori jelszócsere, próbálkozások számának korlátozása, kétfaktor
- Man in The Middle: Nyílvános wifi kerülése, HTTPS, webcímek
- SQL injection: Bemenet validálása, hozzáférés korlátozása
- DoS / DDoS (Denial of service / Didtributed Denial of Service): Forgalomfigyelés, sebességfigyelés
- Zero-Day Exploit: Patch menedzsment, vállalati védelmi stratégiák

BeEF

https://www.youtube.com/watch?v=3ogyS4KOlXc&ab_channel=NetworkChuck

Social Engineering

Pszichológiai manipuláció



„A social engineering a befolyásolás és 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. kihasználni.” Kevin D. Mitnick: A megtévesztés művészete

„Using cheap dirty psychological tricks to get people to do what you want ” Brian Brushwood

Social engineering

- Emberi tulajdonságok kihasználása:
  - Segítő szándék
  - Konfliktuskerülés
  - Emberi érzelmek
- Módszerei:
  - Elicitation (információ kicsikarása)
  - Pretexting (színlelés)
  - Technikai megoldások

Lépések

- Fontos a fokozatosság, a lépésről lépésre haladás
  - A bizalom kiépítése teljesen ártalmatlan témával/kéréssel
  - Ha már segítettünk valakinek könnyebben segítünk újra és újra
- Cél: általában egy komolyabb támadás előkészítése
  - Ez lehet technikai alapú támadás
  - Újabb Social Engineering alapú támadás
- Lépések
  - Előkészítés, információgyűjtés
  - –„Személyes” kapcsolat kialakítása
  - A már működő kapcsolat felhasználása

Ki lehet Social Engineer?

- Hackerek
- Kémek
- Személyiség tolvajok
- Penetration testers
- Megbántott, elbocsátott alkalmazottak
- Manipulátorok
- Ügynökök
- Kormányok
- Gyerekek

Információ szerzés

- Segítségkérés
    - Indoklás, okok megadása
    - Ügyfelekkel közvetlen kapcsolatú munkatársak
        - Recepció, Help Desk
- Segítségnyújtás
    - Reverse Social Engineering
- Nyilvános források!
- Dumpster Diving kukázás

Információ szerzés (Megszemélyesítés)

- Új alkalmazott
- „Nagyfőnök” félelem keltés
- „A főnök küldött”
- Support team / help desk megszemélyesítése
- Piggybacking - más jogosultságainak használata
- Nyeremények, ajándékok

Információ szerzés (Megszemélyesítés)

- Adatgyűjtő weboldal
- Adathalász weboldalak phishing
- Vishing (Phone phishing)
- SMiShing
- Spear phishing, Whaling
- Trójai programok

Technikai eszközök (hardver)

- Keyloggerek
  - Naplózó szoftverek
  - Hardver eszközök
- Baiting (DVD, Pendrive)
- Engedély nélküli AP

Pinapple WiFi

https://www.youtube.com/watch?v=EbetD2LMbeQ&ab_channel=Felix

Bejutás védett helyekre

- Shoulder Surfing
- Tailgating
- Alapértelmezett kódok
  - Kaputelefon
- Hamis azonosítók
  - Smartcard, proximity kártyák
- Álruha, egyéb kiegészítők


1
2
3
4
5
6
7
8
9
*
0
#

Fontos részletek

- Bizalom, szavahihetőség, hitelesség
- Szaknyelv, szakzsargon
- Megjelenés
  - Stílus
  - Munkaruha, eszközök
- Körültekintő előkészítés
  - Hierarchia, céges struktúra ismerete
  - Fontosabb vezetők, kollégák neve, fényképe
- Helyismeret

Geek Squad

https://www.youtube.com/watch?v=LG_AV0TGoow&ab_channel=SiliconValleyClips

Védekezési lehetőségek

- „Az az igazság, hogy nincs olyan technológia a
- világon, amely megakadályozhatja a Social
- Engineering támadást ” Kevin Mitnick
- Szabályzatok
  - Szabályok betartása, ellenőrzés
  - Tájékoztatás
- Helyzetelemzés, sebezhetőségek keresése
  - IT biztonsági előírások felülvizsgálata
  - Penetration teszt (pentest)
- Tesztek, felülvizsgálatok ismétlése
- Képzés, képzés, képzés

Fontosabb szabályzatok

- Adatok osztályozása, bizalmas adatok kezelése
- Humán erőforrás kezelés
- Beléptetés, vendégek kezelése
- Munkahelyek kialakítására vonatkozó szabályok
- Számítógépekkel kapcsolatos szabályok
  - Hordozható eszközökre vonatkozó szabályok
  - Leselejtezett eszközök kezelése
- Adathordozókra vonatkozó szabályok
- Emailek kezelésének szabályai
- Telefonhívásokra vonatkozó szabályok
- Hulladékkezelés, megsemmisítés