Bevezetés a kiberbiztonságba - Biztonságtudatosság

Social Engineering

Bonifert Tamás

2023. 05. 25.

Tartalom

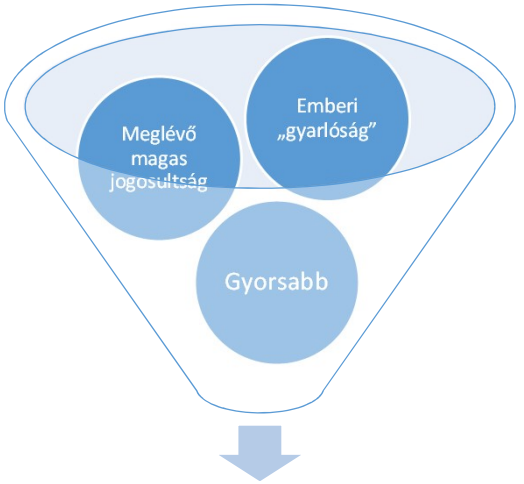
Social engineering típusú támadások

- Fogalom
- Social Engineering támadások típusainak ismertetése
- Védekezés, biztonsági kontrollok

Social Engineering támadás

„A leggyengébb láncszem a felhasználó”

- A támadó nem, vagy nem csak technikai módszerekkel ér el eredményt
- Nem a rendszereket, hanem az embert, a felhasználót támadja
- Pszichológiai módszerek: bizalom megszerzése, manipuláció, megtévesztés
- Az emberek önként tesznek meg lépéseket



Social Engineering támadás

ADATHALÁSZAT (PHISHING)

- Személyes, vagy bizalmas adat megszerzésének kísérlete megtévesztés által
- A támadó megbízható félnek, vagy jól ismert szervnek adja ki magát
- Leggyakoribb módja az e-mail phishing, de létezik telefonos, web portálos, vagy social media változata is
- Legtöbbször weboldal meglátogatására, vagy csatolmány megnyitására kér fel

Tömeges phishing e-mail

- Legitim szervezetre hasonlító küldő domain és dizájn
- A címzett nem nevesített, bárkinek szólhat
- Sokszor kötődik sok embert érintő eseményekhez (pl. Covid teszt)

Spear phishing (Célzott phishing)

- Célcsoportot, vagy egyetlen célszemélyt céloz meg
- Precízen megszerkesztett, személy specifikus információkat tartalmazó e-mail-ek
- OSINT kutatásnak kell megelőznie

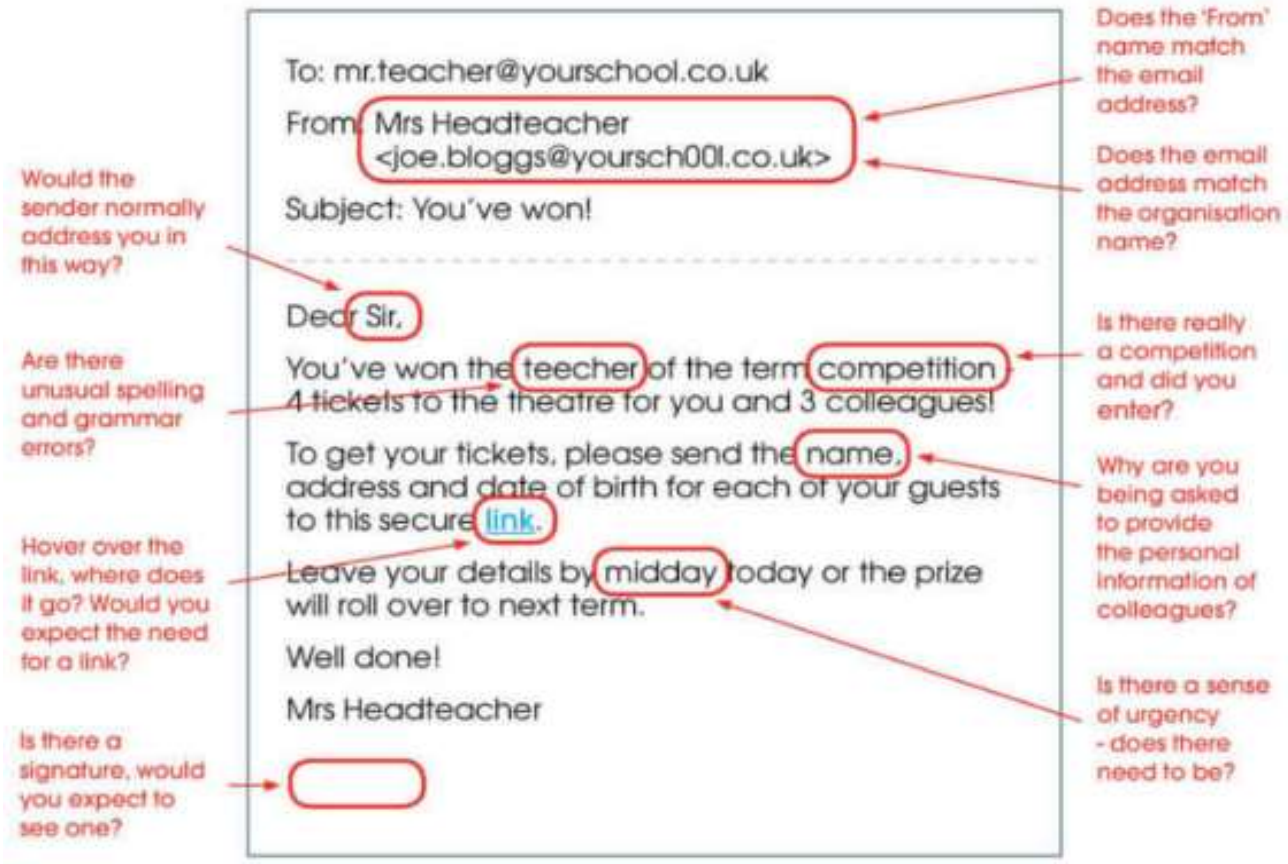
Social Engineering támadás

PHISING E-MAIL FELISMERÉSE

- Bár egyre szofisztikáltabbak az adathalász levelek, sok gyanús pontjuk lehet:
  - E-mail cím nem azonos a küldő szervezet nevével
  - Szokatlan, túl általános, vagy nem létező megszólítás
  - Személyes információ megadására, vagy egy oldal meglátogatására buzdít
  - Nyelvtani hibák (fordító program hiba)
  - Gyanús link, mely az egeret fölé helyezve más helyre mutat
  - Sürgetést tartalmaz
  - Semmi köze a címzettnek a levél tárgyához, tartalmához
- Technikai szinten
  - E-mail eredetiség teszteken nem megy át: SPF,DKIM,DMARC

Social Engineering támadás

PHISING E-MAIL FELISMERÉSE



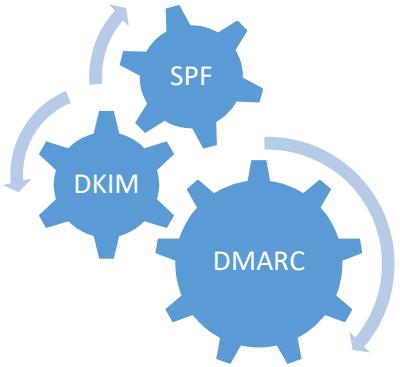
Social Engineering támadás

PHISING E-MAIL ELLENI VÉDEKEZÉS

- Spam filter használata
- E-mail címek interneten történő megadásának mellőzése
- E-mail hitelesítési protokollok bevezetése: SPF,DKIM,DMARC
- Ne küldjünk soha személyes információt e-mailben kérésre
- Legyünk elővigyázatosak, figyeljünk a spam e-mail jelekre
- Ne nyissunk meg ismeretlen csatolmányt
- Dolgozók oktatása a biztonsági tudatosságra

Social Engineering támadás

PHISING E-MAIL ELLENI VÉDEKEZÉS



SENDER POLICY FRAMEWORK (SPF)

- DNS bejegyzés, ami azokat az IP címeket tartalmazza, melyek az adott domain nevében levelet küldhetnek
- Ha a küldő IP nincs a megadott domain névhez regisztrálva, a spam folderbe kerül a mail

DOMAINKEYS IDENTIFIED MAIL (DKIM)

- Digitális aláírás alapú e-mail szerver hitelesítés

DOMAIN-BASED MESSAGE AUTHENTICATION, REPORTING & CONFORMANCE (DMARC)

- Ez a szabály mondja meg, hogy ha egy e-mail üzenet nem hiteles, mi történjen vele
- Lehetséges átengedés, spam/karentén folderbe tétel, vagy visszautasítás

Social Engineering támadás

CSALIZÁS (BAITING)

- Ajándék, vagy nyeremény reményén alapuló támadás
- Online és Offline típusa van
- Az ajándék malware-t tartalmaz, mely adatlopást hajt végre
- Az emberi kíváncsiságon, és az ajándék felett érzett örömön alapul

Online baiting

- **Visszautasíthatatlan ajánlatok**
- **Ingyenes zene, film, szoftver stb.**
- **Pénznyereménnyel történő kecsegtetés**
- **A nyeremény helyett malware töltődik le a linkről**

Offline baiting

- **Ajándék, vagy elhagyott pendrive**
- **A pendrive malware-t tartalmaz**
- **A Social Engineering pendrive-ok kártékony kódjainak elkészítésére konkrét megoldások léteznek ingyenesen**

Social Engineering támadás

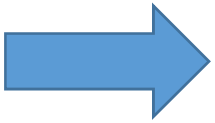
BAITING USB PENDRIVE KÉSZÍTÉSE

- Az ajándék, vagy elszórt pendrive-ra ártó kódot telepít a támadó
- A kódnak automatikusan kell indulnia
- Mivel a kód a belső hálózatban fog futni, könnyen okoz kárt
- Metasploit framework ingyenes és egyszerű megoldás

SOCIAL ENGINEERING TOOLKIT

```
Select from the menu:

  1) Spear-Phishing Attack Vectors
  2) Website Attack Vectors
  3) Infectious Media Generator
  4) Create a Payload and Listener
  5) Mass Mailer Attack
  6) Arduino-Based Attack Vector
  7) Wireless Access Point Attack Vector
  8) QRCode Generator Attack Vector
  9) Powershell Attack Vectors
 10) SMS Spoofing Attack Vector
 11) Third Party Modules
```



- AUTORUN.INF
- REVERSE SHELL
- SAJÁT PROGRAM

Social Engineering támadás

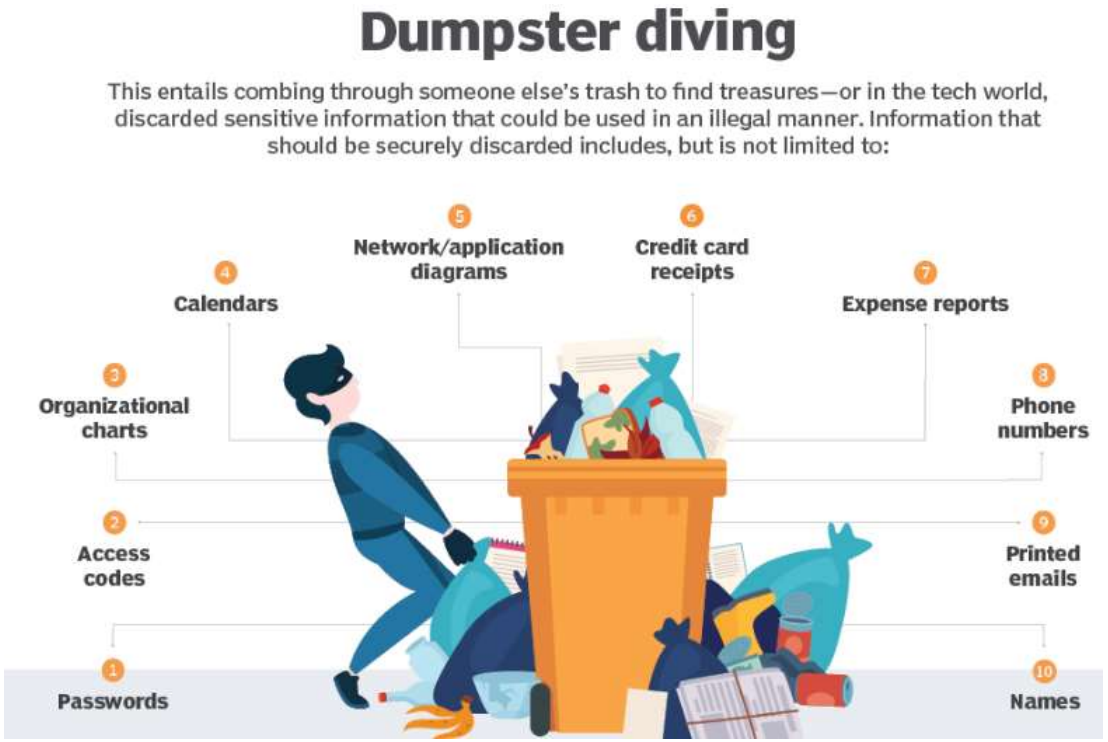
FIZIKAI HOZZÁFÉRÉS SZERZÉSE MEGTÉVESZTÉSSEL

- **Számos információt szerezhet a támadó az épületbe bejutással**
- **Veszélyesebb, mint a távoli Social Engineering: fizikailag el lehet kapni a támadót**
- **Lehetőséget ad Dumpster diving, Shoulder surfing tevékenységre például**
- **Lényege, hogy a támadó valakit megszemélyesít: pl. karbantartó, ügyfél, új alkalmazott, így bejuthat az épületbe**

Social Engineering támadás

KUKABÚVÁRKODÁS (DUMPSTER DIVING)

- **Információgyűjtési módszer további social engineering támadáshoz**
- **Fizikai hozzáférés szükséges az épülethez, pl. vendég státusz**
- **Számos információt rejthet egy kuka, pl. telefonszámok, nevek, hosztnevek, akár jelszavak**



Social Engineering támadás

FIZIKAI HOZZÁFÉRÉS SZERZÉSE MEGTÉVESZTÉSSEL

- **Információgyűjtési módszer további social engineering támadáshoz**
- **Egy dolgozó képernyőjéről információ lelesése**
- **Fizikai hozzáférés szükséges az épülethez, pl. vendég státusz**
- **Bizalmasabb légkör megteremtését feltételezi**

Social Engineering támadás

Esettanulmányok

KÖSZÖNÖM A FIGYELMET!

Kérdések?