Hogyan védd jelszavaidat?

NEMZETI TEHETSÉG PROGRAM

Az előadás a NEMZETI TEHETSÉG PROGRAM - „A hazai és a határon túli felsőoktatási intézmények tehetséggondozó programjainak támogatása" címmel kiírt nyílt pályázat keretében a **„Digitális technológiák használata a közösség szolgálatában" című „NTP-FKT-20-0002"** azonosító számú pályázat keretében valósult .

A KIBERTÉREN TÖRTÉNŐ VISSZAÉLÉSEK CÉLJAI ÉS MÓDJAI

- **Kibertér:** *információtechnológiai infrastruktúrák összefüggő hálózata*
- Alapvetően érdemes megkülönböztetnünk azt, hogy a visszaélés személy ellen történik, vagy valamilyen szervezet rendszere ellen
- 1. az információs rendszer működésének zavarása,
- 2. adat megszerzésére irányuló támadás,
- 3. adat módosítására irányuló támadás.
- Ezek tehát az adat, információ úgynevezett rendelkezésére állását (1.), bizalmasságát (2.) és sértetlenségét (3.) fenyegetik. Ezek a fogalmak azért is fontosak, mert a hatályos magyar jogszabályozás is nevesíti őket
- Az információs visszaélések számos formáját ismerjük. Ezeket két csoportba tudjuk sorolni attól függően, hogy emberi tényezők által következnek be, vagy valamilyen informatikai rést használnak ki:
- 1. valamilyen rosszindulatú szoftverrel (malware) előidézett információs visszaélés,
- 2. social engineering módszerrel előidézett információs visszaélés (humán és nem humán eredetű visszaélések), korrupció.

Biztonsági követelmények

- **bizalmasság** (confidentiality): röviden annyit jelent, hogy valamit csak az arra jogosultak ismerhetnek meg, korlátozott a megismerése jogosultak köre; vagy ahogyan az Infotörvény fogalmazza meg – az elektronikus információs rendszer azon tulajdonsága, hogy a benne tárolt adatot, információt csak az arra jogosultak és csak a jogosultságuk szintje szerint ismerhetik meg, használhatják fel, illetve rendelkezhetnek a felhasználásáról.

- **sértetlenség, vagy integritás** (integrity): röviden úgy mondanánk, hogy valami az eredeti állapotának megfelel és teljes. Az Infotörvény értelmezésében az adat tulajdonsága, amely arra vonatkozik, hogy az adat tartalma és tulajdonságai az elvárttal megegyeznek, ideértve a bizonyosságot abban, hogy az az elvárt forrásból származik (hitelesség) és a származás ellenőrizhetőségét, bizonyosságát (letagadhatatlanságát) is, illetve az elektronikus információs rendszer elemeinek azon tulajdonságát, amely arra vonatkozik, hogy az elektronikus információs rendszer eleme rendeltetésének megfelelően használható;

- **rendelkezésre állás** (availability): lényegében annyit jelent, hogy a szükséges infrastruktúrák valamint adatok ott és akkor állnak a felhasználó rendelkezésére, amikor arra szükség van, vagy ahogyan az Infotörvény fogalmazza meg, annak biztosítása, hogy az elektronikus információs rendszerek az arra jogosult személy számára elérhetőek és az abban kezelt adatok felhasználhatóak legyenek.

VÉDELEM… de mi ellen?

- egyre többekben merül fel az igény, hogy amennyire lehet, megpróbálják megvédeni magukat a kiberbűnözők, a kormányzati hekkerek, a megfigyelő állam, a mindent tudó techcégek, az adatainkkal kereskedő netszolgáltatók vagy éppen a kellemetlenkedő ex ellen

- biztonság – fenyegetettség

- a rossz hír: nincs rövid válasz, mindenre jó, egyszerű és univerzális megoldás mert a biztonság nem mindenkinél ugyanazt jelenti

- saját döntés legyen

Jelszavak, jelszókezelők

- top 10

1. 123456
2. 123456789
3. qwerty
4. 12345678
5. 111111
6. 1234567890
7. 1234567
8. password
9. 123123
10. 987654321

Jelszavak, jelszókezelők

- a felhasználók edukálásának vannak korlátai, és egy számottevő méretű kisebbség soha nem fog a saját biztonságára figyelni, bármennyiszer is figyelmeztetik ennek a szükségességére

- ezért a biztonság megteremtése részben az informatikusok dolga is, egyszerűbben használható biztonsági megoldások bevezetésével, illetve a meglévő módszerek használatának a kikényszerítésével

- például, hogy ne lehessen ilyen egyszerű jelszóval regisztrálni, vagy kötelező legyen a kétlépcsős azonosítás

Jelszavak, jelszókezelők

- megoszlanak a szakértői vélemények, hogy pontosan milyen egy igazán jó jelszó
- ökölszabályként elég annyit megjegyezni, hogy ne könnyen kitalálható dolgokat adjon meg
- mivel olyan sok helyre kell manapság regisztrálni, csábítóan egyszerű lenne mindenhol ugyanazt a jelszót használni, hogy elég legyen csak azt az egyet megjegyezni **Ne tegye!**
- használjon jelszókezelőt: Abban biztonságosan tárolhatja az összes jelszavát, és erős jelszavakat is generálhat vele. Megjegyeznie innentől már csak egyetlen jelszót kell: a jelszókezelője mesterjelszavát, amellyel az összes többihez hozzáfér. Természetesen a jelszókezelőket is meghekkelhetik, de egyrészt ők megfelelően titkosítva tárolják a jelszavakat, szóval a hekkerek nem sok mindenre mennének velük, másrészt ennek sokkal-sokkal kisebb az esélye

ellenőrzés

- a **Have I Been Pwned** oldalán ellenőrizheti, hogy érintett-e valamilyen adatszivárgásban.

Ha igen, mindenhol cserélje le az ellopott jelszót

Két tényezős hitelesítés

• a jelszavak ellopása és gondatlan kiadása ellen a legjobb védelem a két tényezős hitelesítés (2-factor authentication, 2FA)

• lényege, hogy a bejelentkezéskor beírt jelszó mellett egy második azonosítási módot is kér a szolgáltatás, mielőtt beenged, ez leggyakrabban egy eldobható számkód, amelyet vagy sms-ben kap meg a felhasználó, vagy egy erre szolgáló mobilapp generálja

• elég sok megbízható kódgeneráló app közül lehet ízlés szerint válogatni, és nagyjából ugyanazt tudják: akármennyi fiókot fel lehet venni bennük, és mindhez folyamatosan, netkapcsolat nélkül gyártják a fél perc alatt lejáró kódokat

• a legelterjedtebbek a **Google Hitelesítő** (Android, iOS), az **Authy** (Android, iOS) és a **Microsoft Authenticator** (Android, iOS), de a **Lastpass Authenticator** (Android, iOS) jól működik a **Lastpass** jelszókezelővel párban

Még tovább

- az igazán paranoiásak hardveres megoldást is használhatnak: egy pendrive-hoz hasonló USB-kulcsot, amelyet a belépéshez be kell dugni a gépbe, majd megérinteni, vagy az erre alkalmas változatokat egyszerűen hozzáérinteni a mobilhoz

- a hardveres kulcs előnye, hogy gyakorlatilag lehetetlen adathalászattal megkerülni, és számsorokat se kell bepötyögni

- messze a legnépszerűbb hardveres kulcs a YubiKey, ennek a legújabb generációjával már úgy is be lehet lépni, hogy jelszót nem is használunk, csak magát a kulcsot,

és ha már, akkor

- a titkosítás a digitális biztonság alapköve
- PortableApps

HOVÁ KERÜLNEK A KISZIVÁRGOTT ADATOK?

- clearweb – deepweb – darknet
- ~70 milliárd - *1000 – 70 k / 5 k exit

egyet az ultizóknak, egyet a betlizőknek

- e-mail
- plain – vpn – tor

VPN

- virtuális magánhálózat
- lehetővé teszi a felhasználók számára, hogy egy megosztott vagy nyilvános hálózaton keresztül úgy küldjenek és fogadjanak adatokat, mintha számítógépeik közvetlenül kapcsolódnának a helyi hálózathoz
- a VPN-en keresztül menő adatok a titkosítás miatt nem láthatók az eredeti hálózaton
- gyakori alkalmazása, amikor a munkatársak a cég belső hálózatához távolról biztonságosan férhetnek hozzá: az interneten keresztül titkosított csatorna hozható létre a dolgozó számítógépe és a vállalat szervere között

VPN

- számos cég kínálja nyilvános szolgáltatásként, hogy VPN-szerveren keresztül böngészhetünk a világhálón, ilyen szolgáltatás igénybevétele esetén a saját gépünk és a VPN-szolgáltató szervere között egy titkosított kapcsolatot építünk ki, és a publikus internetre a szolgáltató szerverének nevében lépünk ki

- Előnyei a közvetlen internethasználathoz képest:
  - a webhelyek számára az adatforgalom a VPN-szerver országából érkezőnek látszik;
  - a saját internetszolgáltató nem látja az adatforgalom részleteit;
  - nyilvános hálózat használata esetén nehezíti az adathalászok dolgát.
- Hátrányai:
  - lassabb internetelérés;
  - az adatforgalom részleteit a VPN-szolgáltató látja.

Tor

• lehetővé teszi az anonim jelenlétet (például böngészést) az interneten, valamint nem utolsósorban a cenzúrázott internetes tartalmak megjelenítését (mint pl. a tartalomszűrés megkerülését)

• a hálózatban részt vevő tagok opcionálisan konfigurálhatják a Tor kliensüket úgynevezett node-nak, vagy Tor-exit-nek, a node engedélyezi, hogy rajta keresztül csomagok fussanak, de nem engedélyezi a hálózatból való kilépést a hagyományos internetre, míg a Tor-exit ezt is engedélyezi

• a Tor hálózat minden tagja titkosítva kommunikál egymással 128 bites szimmetrikus kulcsolású kódokat használva

Tor

- a node-ok - mivel csak titkosított adatokat láthatnak - egyrészt nem tudják, honnan indult el a csomag, másrészt nem tudják, hogy mit tartalmaz, csakúgy, mint az esetleges külső támadó, lehallgató
- a Tor nem titkosításra, hanem anonimizálásra szolgál, tehát nem az átküldött adatot védi, hanem a névtelenséget
- a Tor csak egy dolgot garantál: a szerver nem fogja ismerni a kliens valódi IP címét

Titkosítás

- szimmetrikus: a küldőnek és a fogadónak is ismernie kell a művelethez használt kulcsot
- aszimmetrikus (nyílvános kulcsú): a felhasználó egy kulcspárral – egy nyilvános és egy titkos kulccsal rendelkezik,
- a kulcsok matematikailag összefüggnek, ám a titkos kulcsot gyakorlatilag nem lehet meghatározni a nyilvános kulcs ismeretében
- egy, a nyilvános kulccsal kódolt üzenetet csak a kulcspár másik darabjával, a titkos kulccsal lehet visszafejteni