
Fotó: Bv. fotó

Böszörményi-Halász Bence

# Az elektronikus információbiztonság alapvetései, valamint a büntetés-végrehajtási szervezet információbiztonsági tudatosságának fejlesztési lehetőségei

## *Fundamentals of cyber security and opportunities for developing the information security awareness of the penitentiary organization*

Napjainkban az állam, valamint annak minden szervezete és polgára kiszolgáltatottá vált a többszörösen összetett elektronikus információs rendszereknek, amelyek nélkül az állam működése elképzelhetetlen volna. A modern gazdasági berendezkedés mellett a társadalom nincs felkészülve arra, hogy a kiesett infrastruktúrák, eszközök vagy szolgáltatások nélkül működjön, így ezeket – egyértelműen – védeni kell. A humán tényező megfelelő affinitás és háttértudás nélkül könnyen támadható és befolyásolható, hiszen a hatékony védekezéshez ismernünk kell az alapvető rendszereket. Tanulmányomban az információbiztonságról, a humán tényező jelentőségeiről, a tudatosság fejlesztéséről, illetve az információvédelem aktuális kérdéseiről értekezem. Bemutatom továbbá az elképzelhető támadások típusait, módszereit, a támadások elleni védekezés lehetőségeit, az oktatás, képzés, tudatosítás jelentőségét és ezek fejlesztési lehetőségeit a büntetés-végrehajtási szervezetben.

**Kulcsszavak:** információbiztonság, tudatosság, információvédelem, humán tényező, képzés

*Nowadays, the state, as well as all its organizations and citizens, have become vulnerable to multi-complex electronic information systems, without which the functioning of the state would be unthinkable. With a modern economic system, society is not prepared to operate when malfunction or breakage occurs in infrastructure, equipment or services, therefore these clearly must be protected. The human factor can be easily attacked and influenced without adequate affinity and background knowledge, as we need to know the basic systems to defend effectively. In my study, I discuss information security, the significance of the human factor, awareness raising, and current issues of information protection. I also present the types and methods of possible attacks, the possibilities of defense against attacks, the importance of education, training, awareness and the possibilities of their development in the penitentiary organization.*

***Keywords:*** *cyber security, awareness, information protection, human factor, training*

## Előszó

A XXI. század elejére az állam, és annak minden szervezete, valamint polgára kiszolgáltatottá vált az összetett elektronikus információs rendszereknek. Ezek nélkül egy állam működése, a különböző szolgáltatások biztosítása és igénybevétele mára már megvalósíthatatlan volna. A modern gazdasági berendezkedés mellett a társadalom nincs felkészülve arra, hogy a kiesett szolgáltatások nélkül működjön, így ezeket – egyértelműen – védeni kell.[1] Különös tekintettel arra, hogy az azok működése során felhasznált és keletkező információk, továbbá az azokban kezelt adatok jelentős vagyont képviselhetnek. A szándékos károkozások egyre gyakrabban fordulnak elő, továbbá ezek egyre vakmerőbbek és egyre bonyolultabbak is. Így napjainkra már folyamatosan növekvő fenyegetést jelent a – sérülékeny elektronikus információs rendszereinkre támadó, és egyre erősödő – kiberterrorizmus. Az elektronikus információs rendszerek, szolgáltatások bármelyikének megsemmisülése vagy sérülése a társadalom széles rétegeit érintheti, továbbá az ezeken kezelt adatvagyon bizalmassága, sértetlensége és rendelkezésre állása alapvető fontossággal bír az állami, különösen a rendvédelmi szervek területén. A büntetés-végrehajtási szervezet esetében kiváltképp a személyi állomány személyes adatai, valamint a fogvatartottak személyi és bűnügyi adatvagyona kiemelt jelentőségű.

## Bevezetés

Napjaink egyik legnagyobb kihívását az információbiztonság megteremtése, annak fejlesztése, illetve jelentőségének hangsúlyozása, tudatosítása jelenti. Az infokommunikációs eszközök és rendszerek robbanásszerű fejlődésével a támadási technikák és módszerek is fejlődnek, éppen ezért szükségszerű, hogy az új támadási alternatívákkal szemben is felkészültek legyünk. Az informatikai rendszerek fejlett védelmének köszönhetően a bizalmas vagy érzékeny információk megszerzésére irányuló támadások immáron legfőképpen a humán tényezőt célozzák. A humán tényező fontossága abban rejlik, hogy az, vagyis mi magunk vagyunk leginkább hatással a legtöbb védendő értekre. Az emberi tényező kapcsolatban áll különféle belső és bizalmas információkkal. Létrehozásuk, megjelenítésük, módosításuk vagy esetleges törlésük, megsemmisítésük érdekében számtalan művelet végrehajtására vagyunk jogosultak. Mindemellett az alkalmazottak kapcsolatban állnak egymással, ezáltal könnyedén oszthatnak meg információkat is. Megfelelő affinitás és háttértudás nélkül az emberi alapterméket – a vele járó hiszékenységgel – könnyen támadhatóságot és befolyásolhatóságot predesztinálhat. A hatékony védekezéshez ismernünk kell az alapvető rendszereket, mi több készség szintjén kell tudnunk kezelni azokat.

1 Nemzeti Egészségbiztosítási Alapkezelő – Elektronikus információbiztonság

## Generációs különbségek

A téma szempontjából fontos tisztázni a generációk fogalmát. A hagyományos, biológiai meghatározás szerint a generáció[2]*"a szülők és utódaik születése közötti átlagos időintervallumot"* jelöli, mely 20-25 évet ölel fel. Mára azonban a csoportok gyors változásai, az új technológiák megjelenése, az átalakuló karrierutak és értékrendek, valamint az eltolódó társadalmi értékek következtében mindez érvényét veszítette. Napjainkban a generáció fogalmát tehát sokkal inkább szociológiai, semmint biológiai szempontból érdemes megközelíteni. A megfelelő készségek vizsgálatának első lépéseként fontos hangsúlyozni, hogy természetesen az alább kifejtett állítások nem mindenkire igazak, a generációs különbségek nem feltétlenül jelentik azt, hogy egy adott korcsoport minden esetben homogén módon használja a technikai rendszereket, valamint az azokon kezelt adatokat. A korcsoportok meghatározásánál az évszámok egyes kutatások tekintetében eltérhetnek, azonban tapasztalatom szerint megközelítőleg minden tanulmányban hasonló időintervallumot fednek le. A generációs különbségeknek kiemelt jelentőséget kell tulajdonítani az egyén információbiztonságban betöltött szerepe tekintetében, hiszen egy adott korcsoporthoz való tartozás jelentősen befolyásolhatja az infokommunikációs eszközök használatát, valamint a különféle információbiztonsági szabályok ismeretét, az ezekhez történő alkalmazkodási képességet, illetve a védendő értékekhez való viszonyulást.

### *„Veterán" generáció (1925 és 1945 között születettek)*

Tagjaira az óvatos, visszafogott, biztonságra törekvő magatartás a jellemző. Magánéletükben a családi értékek kiemelt fontossággal bírnak. Életük nagy részét a szocializmusban élték le. Biztonságot és társaságot elsősorban a szűk családban keresnek, és amennyiben nem muszáj, nem alkalmazkodnak a legújabb technológiákhoz. Nehezen tudnak megbirkózni a digitális társadalom kihívásaival, a „felgyorsult világgal".

### *„Baby boom" korszak (1946 és 1965 között születettek)*

Ők az utolsó generáció, akik még magázták a szüleiket, de egyben az első, akiket már tegeztek a gyerekeik. Náluk jelent meg az igény az individualizációra. Zömében szigorú nevelést kaptak és egész életükben feladatorientáltak voltak, ennek köszönhetően idős korukban is tevékenyek. A „baby boom" korszakba tartozók kevésbé tudnak alkalmazkodni az információtechnológia fejlődéséhez. Csak felnőttkorukban ismerkedhettek meg a különféle infokommunikációs eszközökkel, ezért jellemzően technikai és tudásbeli hiányosságaik is lehetnek. Ez a csoport a legfőbb célközönsége

2 Komár Zita: Generációk akkor és most

a kibertámadásoknak, hiszen korukból adódóan még aktív dolgozók, állományi tagok lehetnek, azonban a jelenlegi munkaerőpiacon a legidősebb korosztálynak számítanak.

## *X generáció (1965 és 1980 között születettek)*

Az X generáció tagjai tinédzserként vagy fiatal felnőttként kerültek kapcsolatba a digitális világgal, így munkájukat jelentősen befolyásolja az új technológia, és azt magánemberként is egyre gyakrabban, egyre szélesebb felhasználási körben alkalmazzák. Az X generáció tagjai tehát csak életük során találkoztak ezzel a világgal, jobb esetben elfogadták és elkezdték használni a digitális világ új eszközeit. Összességében elmondható, hogy sokkal nyitottabbak ezekre, mint az őket megelőző korosztály. Információbiztonsági szempontból azonban egyes tanulmányok szerint az X generáció tagjai követik el a legtöbb hibát, jellemzően a jelszóhasználatban és azok tárolásában adódhatnak nehézségeik.

## *Y generáció (1980 és 2000 között születettek)*

*„A digitális bennszülöttek első generációja”.*[3]

Ők a posztmodern világ szülöttei, akik a 2001. szeptember 11-e utáni krízisperiódusban élik fiatalkorukat. Tagjai magabiztos, energikus, kifejezetten tehetséges, kreatív személyek, akik a korábbi generációktól jelentősen eltérő viselkedést mutatnak a tanulás és a munkavégzés területén. Együtt nőttek fel a modern technika fejlődésével, információéhségük kifejezett, a multikulturális környezetet könnyedén, laza attitűddel kezelik, és jellemző rájuk a „multitasking”[4]. Az Y generációt jellemzi, hogy mivel tagjai a számítógépekkel együtt nőttek fel, életüket már el sem tudják képzelni a technológia nélkül, az a mindennapjaik nélkülözhetetlen részévé vált. A kiberterroristák jellemzően ebből a csoportból származnak, hiszen pontosan ismerik a saját korlátjaikat, sebezhetőségüket, valamint a korszak szülöttjei mesterei a „social engineering” technikáknak (kifejtés a támadások módszerei fejezetben).

## *Z generáció (2000 és 2010 között születettek)*

Ezen csoport tagjai a terrorizmus krízisperiódusában, a globális válság és a klímaváltozás idején születtek a digitális technológiák világába, amelyben már elképzelhetetlen

3 Komár Zita: Generációk akkor és most

4 A „multitasking” magyarul több feladat egyidejű elvégzését jelenti. Eredetileg a számítástechnikából származik a kifejezés, ahol a korai számítógépeket egymagos processzorok hajtották, amelyek egyszerre csak egyetlen feladatot tudtak elvégezni, és csak annak befejezését követően tértek át az újra. A többmagos processzorok elterjedésével azonban a számítógépek már több feladatot is el tudtak végezni egyszerre.

a különféle infokommunikációs eszközök nélkül élni. Számukra a közösségi média, az okostelefonok használata már egyfajta szükségletté vált. Életüket „bedrótozva" élik, azaz szimultán több médium felhasználói. Bátrak, kezdeményezőek, kevésbé kételkednek saját képességeikben és korlátaikban, ezáltal könnyen támadhatóak. Motivációs struktúrájuk szerint „beleszülettek" az internet világába, mely emberi kapcsolataikat és kommunikációjukat is átalakítja, az online világ kitágítja énjük határait és formálja identitásukat. Az offline, azaz a „való" világban konfliktuskezelési készségük hiányos (pl. indulatkezelési nehézségek, agresszió, a tekintélyhez való megváltozott viszony). A kibertérben jól elboldogulnak ugyan, ám azon kívül meglehetősen instabil személyiségük lehet, így nemzedékük tagjai olykor hiszékenyebbnek bizonyulhatnak az élő szóval tett támadások kapcsán.

Az őket követő „ALFA" generációval (2010 után születettek) szervezeti szinten természetesen még nem érdemes hosszan foglalkozni, mivel jelenleg nem tartoznak a munkaerőpiachoz.



## Az információbiztonság lélektana

### *A jelszó fontossága*

A számítógépes rendszerek világában leggyakrabban felhasználónév és jelszó párossal azonosítjuk magunkat. A támadóknak sokszor elegendő, ha csupán egyetlen felhasználó jelszava feltörhető, ezt kihasználva a teljes rendszert kompromittálhatják.

A túl rövid jelszavak számítástechnikai eszközökkel könnyedén feltörhetőek. Ezt a technikát (brute force) nyers erőn alapuló jelszótörésnek nevezik, ami szisztematikus próbálgatást jelent, vagyis a jelszavunk minden egyes karakterét egyesével próbálja meg kitalálni az erre speciálisan elkészített szoftver. A legtöbben ráadásul olyan jelszót választanak maguknak, ami a hétköznapi életből vett, gyakori kifejezéseket tartalmaz (pl. asztal, monitor, jelszó). Mivel emberek vagyunk, ez természetes, azonban a probléma az, hogy a hekkerek ezzel értelemszerűen tisztában vannak, mi több a gyakori kifejezésekből szótárlistákat készítenek, ami még inkább megkönnyíti számukra a jelszótörést. A harmadik jellemző hiba, hogy sokan olyan információt használnak fel a jelszavukban, ami a személyükhöz köthető (pl. a háziállatuk neve, a születési évszámuk, illetve rendvédelem esetén sokszor a jelvényszám jellemző).


**1. ábra: Példák a „brute force" technikán alapuló jelszavak feltörésére**[5]



A fenti ábrán jól látszik, hogy erős jelszó az, amit nehéz feltörni, mert megfelelően hosszú (lehetőleg 12 karakter vagy akár még hosszabb is), továbbá nem tartalmaz nagyon tipikus kifejezéseket és sorozatokat (pl. 54321), nem jellemző a személyünkre, valamint a jelszótörténetnek is megfelel a visszafejthetőség szempontjából (tehát bizonyos számú, korábban használt jelszót nem engedélyez újra alkalmazni a rendszer, ami akár visszamenőleg 24 alkalom is lehet.) Ezek a szabályok minden esetben rögzítve vannak az egyes szervezeteknél, így a büntetés-végrehajtási szervezetnél is az Informatikai Biztonsági Szabályzatban (a továbbiakban: IBSZ). Érdemes megemlíteni, hogy a támadások esetén az adatszivárgások 80%-a a jelszavakhoz kötődik.

Kiemelten fontos a megfelelő jelszótárolás is. A jelszókezelő szoftverek megkönnyítik a sokféle online, esetleg munkahelyi szolgáltatáshoz tartozó jelszó kezelését a szórakoztató, a munkával kapcsolatos és a kritikus fontosságú – például a pénzügyi és az egészségügyi – szolgáltatások használatakor is. Azonban több olyan jelszókezelő szoftver létezik, amelyik valójában csak problémát okoz. Egyes esetekben nehéz használni a túlbonyolított kezelőfelületet, sőt a program akár veszélybe sodorhatja az adatainkat, az anonimitásunkat és a pénzünket is. Nagyon fontos tehát, hogy a megfelelő szoftvert használjuk. Tapasztalataim szerint minimum 256 bites AES kulccsal titkosított, lehetőség szerint biometrikus zárral ellátott programokat alkalmazzunk. Így egy esetleges mobiltelefon-elhagyás esetén sem kompromittálódik a jelszavaink biztonsága. Ezzel együtt ilyen esetben javaslom azonnal megváltoztatni a különösen fontos alkalmazások jelszavait, hiszen nem lehetünk elég óvatosak, ha a saját adatvagyonunk a tét.

## *Önellenőrzés*

Jelszavaink, valamint az információbiztonság védelmének érdekében az alábbi szempontokat javaslom megvizsgálni; ezek segítséget nyújthatnak a kibertérben töltött mindennapokban.

5 A tanulmányban található ábrák forrása a szerző.

**1. Jelszavaim erőssége**
A fenti táblázat alapján könnyedén el lehet dönteni, hogy elég erősek-e az általunk használt jelszavak. Hány karakteresek, van-e bennük kis, illetve nagybetű, szám, valamint speciális karakter(ek). Számok esetén lehetőleg ne tartalmazzon a személyünkhöz köthető számkombinációkat (pl. dátumok), valamint túl egyértelmű számsorokat, sorozatokat.

**2. Jelszavaim gyakorisága**
Érdemes sűrűn cserélgetni a titkos kódjainkat, valamint nem ajánlott több online felületen ugyanazt többször használni, illetve plurális pin kódot megadni.

**3. Munkaállomás zárolása**
Munkahelyi környezetben, amikor elhagyjuk a munkaállomásunkat, minden esetben szükséges zárolni azt. *(Bv. IBSZ 51. pontja: „A munkaállomás illetéktelen hozzáférés elleni védelme érdekében a felhasználó köteles a munkaállomást zárolni, illetve ha ez nem lehetséges, köteles a munkaállomásból kijelentkezni, vagy azt kikapcsolni, amennyiben azt felügyelet nélkül hagyja”.)* Ez a sietség vagy a túlzott bizalom, esetleg jóhiszeműség okán gyakorta elmaradhat, pedig felhasználói jogosultságainkat alkalmazva könnyedén illetéktelenek férhetnek kényes munkahelyi adatokhoz.

**4. Ismerjük-e munkahelyünk információbiztonsági követelményeit, szabályozóit?**
Az előző ponthoz csatlakozva kiemelten fontos, hogy a személyi állomány tagja megfelelően megismerje szervezete információbiztonsági szabályozóit és betartsa azokat.

**5. Szemetesünk ellenőrzése (fizikailag vagy szoftveresen)**
Egy meglehetősen elterjedt social engineering technika a „Dumpster diving”, azaz a „Kukabúvárkodás”, mely a kuka átvizsgálását jelenti. Az emberek bele se gondolnak, hogy milyen értékes információkat tudhat meg róluk a támadó az irodai vagy otthoni szemetesük átvizsgálásával. Elég csak kidobni egy havi bankszámla részletezőt, a támadó már meg is tudhatja a bankszámlaszámunkat, de az is elég, ha egy nem megfelelő jelszótárolásból eredő „jelszavas cetli” belekerül a kukába, és máris hozzáférhetnek a belépési kódunkhoz. Szoftveres szempontból hasonló a helyzet, előfordulhat, hogy olyan érzékeny információt tartalmazó fájlt törlünk, amit véglegesen nem távolítunk el, így az a rendszer lomtárából könnyedén visszaállítható.

Természetesen megannyi lehetőség áll még rendelkezésre a megfelelő önellenőrzés végrehajtására. Több fontos szempont adódhat a fentieken kívül, melyeket érdemes alaposan átgondolni (pl.: harmadik félnek megadott adatok, munkát érintő kérdések munkahelyen kívül, közösségi oldalakon miket osztok meg stb.).

## A támadók és a támadások típusai

A támadók kategorizálásának alapjául a támadások megvalósításának eszközei, céljai és motivációi szolgálnak. A különféle támadó típusok megkülönböztetésének szempontjai a következőek:

1. Az adott támadónak mi a célja a támadás végrehajtásával,
2. Milyen előnyre, haszonra kíván szert tenni,
3. Milyen eszközök segítségével valósítja meg a támadást.

A támadók kategorizálásakor – kutatásaim alapján – három főbb csoport különböztethető meg, azonban a felhasznált eszközök tárháza és főként a motiváció okán természetesen temérdek potenciális támadó típus akadhat még.

A főbb csoportok szerint:

**1. Fehérkalapos („white hat") hackerek**
Fehérkalapos hackernek nevezzük azokat a kiemelt tudással rendelkező informatikai szakembereket, akik tudásukat arra használják fel, hogy – eseti vagy állandó jelleggel – biztonsági hibákra világítanak rá, ezáltal elkerülve és megelőzve a feketekalapos hackerek betörési kísérleteit. A fehérkalapos hackerek csoportjába tartozik az úgynevezett etikus hacker, illetve a „Penetration Tester" is.

- Etikus hacker: Egy adott számítógéprendszer vagy számítógép-hálózat biztonsági tesztelését végzi hibakeresési céllal.
- Penetration Tester: Megpróbálja a „veszélyes hibákat" felderíteni és kiaknázni, ezáltal bizonyítva az adott hibában rejlő veszélyeket a rendszer üzemeltetőjének.

**2. Szürkekalapos („grey hat") hacker**
A támadó az adott biztonsági rés feltárása közben kihasználja azt, majd a sebezhetőségről értesíti a rendszer üzemeltetőjét, valamint előfordulhat, hogy segítségét is felajánlja a hiba elhárítása érdekében. A legfőbb különbséget az jelenti, hogy a fehérkalapos hackerrel ellentétben a megtámadott rendszer üzemeltetőjével nincs előre egyeztetett megbízás, így alapvetően illegális tevékenységnek minősül. Vannak példák olyan esetekre, amikor a hibát felderítő, majd jelentő hacker pénzjutalmat kért és kapott is, de mindenképpen rizikós és illegális vállalkozás. A szürkekalapos hackerek közé tartoznak a manapság divatos „internetes trollok" is, akiknek egy része a szakértelmét felhasználva, pusztán szórakozásból okoz felfordulást akár közösségi oldalak üzenőfalain – annak biztonsági hibáit kihasználva –, akár komolyabb rendszerekben is.

**3. Feketekalapos („black hat") hackerek**
Valamilyen haszonszerzés (pl. gazdasági, politikai stb.), valamint károkozás céljából vagy szimplán rosszindulatból, illetve kíváncsiságból hatolnak be jogosulatlanul

számítógépekbe vagy számítógép-hálózatokba. Az általuk végzett tevékenység minden esetben illegális. A motivációjuk sokrétű lehet, azonban elsődlegesen a pénzszerzés – az adott információ birtoklása által –, vagy a puszta kíváncsiságuk hajtja őket: *„Meg tudom-e csinálni, jobb vagyok-e az üzemeltetők rendszergazdáinál?"*. Sajnálatosan azonban ebben az esetben a kíváncsiságot nem kíséri önmérséklet, így a feketekalapos hacker nem kér engedélyt a tesztelésre, a sikeres behatolás végén nem értesíti az üzemeltetőket, hanem igyekszik kihasználni az illegálisan megszerzett információkat. Gyakran hallani nagyobb multinacionális cégek vagy akár kormányszervek ellen elkövetett „hackertámadásokról", és az sem ritka, hogy azokat egy másik ország titkosszolgálatához vagy egy ahhoz kapcsolódó csoporthoz kötik. Ilyen esetekben előállhat az a helyzet is, hogy az etikus és etikátlan közti határvonal meglehetősen elmosódik. Ha az adott tevékenységgel egy potenciálisan háborús helyzet elkerülése a cél, akkor az rögtön más megvilágításba helyezi a történéseket.

Érdekesség a hackerek típusai kapcsán, hogy azok elnevezéseit az amerikai western filmekben megjelenő motívumból kölcsönözték, ahol gyakran a kalapok színéből lehet következtetni, hogy általában az a „jó fiú", aki fehér vagy világos kalapot visel, ellentétben a „rossz fiúkkal", akik többnyire sötét vagy fekete kalapot hordanak.

A főbb csoportokon kívül, valamint azokon belül is számtalan típust különböztethetünk meg, ezek lehetnek többek között:

**4. Hacktivisták**
Akik a számítógépes hálózatokon – speciális eszközökkel – proaktív politikai aktivizmust hajtanak végre, a legtöbb esetben a szólásszabadság, az emberi jogok és az információszabadság jegyében.

**5. Ipari kémek**
Céljuk az iparban elkövetett illegális információszerzés úgy, hogy az ellenérdekelt fél ne szerezzen tudomást arról, hogy információs rendszerét támadás érte, és bizalmas adatok kerültek illetéktelen kezekbe. A feketekalapos hackerek csoportjába tartoznak azok az ipari kémek, akik technológiai fejlesztések után kutatva törnek be hálózatokba.

**6. Ex-munkatársak**
Az elbocsátásuk következtében sértődött korábbi munkatársak a rendszerről meglévő ismereteiket kihasználva hatalmas károkat okozhatnak mind a szervezet informatikai, információs rendszerében, mind a bizalmas információk illetéktelen kezekbe jutásának tekintetében. A rendvédelemben nem gyakori az előfordulásuk, ez főként nagyobb IT cégek elbocsátott munkatársaira jellemző magatartásmód.

## A támadók lélektani módszerei

A támadások módszerei nagyon változatosak lehetnek. A korábban már említett „social engineering" technika, azaz az emberi tényező és az infokommunikációs eszközök gyengeségeit, illetve sérülékenységeit együttesen kihasználó támadási módszer a legelterjedtebb és a leginkább működőképes pszichológiai manipulációs technika a már taglalt emberi tényezők okán. *„A csalás vagy rábeszélés gyakorlati alkalmazása bizonyos információk, ingóságok megszerzése érdekében."*[6] *„A social engineering a befolyásolás és rábeszélés eszközével megtéveszti az embereket, manipulálja vagy meggyőzi őket, hogy a social engineer tényleg az, akinek mondja magát"*.[7] Legelterjedtebb módszerei a következők:

**1. Adathalászat**
A pszichológiai manipuláció azon esete, amikor látszólag megbízható partnerként elektronikus levélben vagy honlapon próbálnak bizalmas információhoz jutni. A támadó által megszerezni kívánt információk a legkülönbözőbbek lehetnek pl.: felhasználónév, jelszó, hitelkártyaszám, bankszámla adatok stb. Az üzenet arra hívja fel a felhasználót, hogy az jelentkezzen be valamilyen ismert honlapra (PayPal, eBay, valamilyen ismert bank stb.) nagyon hasonlító oldalra, ami a manipulátor által üzemeltetett weblap, ahol a feltett kérdések lehetőséget adnak bizalmas információk megszerzésére. (Fontos: Valójában komoly szervezetek, bankok soha nem kérnek bizalmas adatokat elektronikus levélben.)

**2. Álruha**
A támadó egy másik személy (például rendszergazda, karbantartó, takarító, futár) bőrébe bújik, ezzel tévesztve meg az alkalmazottat.

**3. Segítségkérés**
A segítségkérést eljátszó támadások – funkciójukból fakadóan – leginkább a helpdesk-en, titkárságon, ügyfélszolgálaton, recepción dolgozókat veszik célba, hiszen ők azok, akik folyamatosan ugyanazt a típusú munkát végzik, emberekkel foglalkoznak, és általában hasonló megkeresésekkel találkoznak nap, mint nap. Éppen ezért nem biztos, hogy azonnal ki tudják szűrni a valótlan megkeresést. Ez a rendészetben is megtalálható jelenség, így telefonon semmilyen bizalmas információt nem szabad kiadni!

**4. Új munkatárs**
Ezen módszer jellegzetessége, hogy a támadó új kollégának adja ki magát, amely a rendvédelem esetében párosulhat az álruha technika alkalmazásával is, hiszen egyenruhában könnyen megtéveszthető még egy tapasztaltabb kolléga is.

6 Douglas P. Twitchell egyetemi professzor értekezése
7 Kevin, D. Mitnick (2003)

**5. Jóhiszeműség**
A technika sajátossága a munkatársak segítőkészségének, naivságának, jóhiszeműségének kihasználása. A social engineerek sok esetben választják ezt a módszert, hiszen a legtöbb ember segítőkész. Szinte minden kolléga szívesen segít a nehéz helyzetben lévőknek, és együtt is érez velük. Továbbá itt kell megemlíteni azt is, hogy az emberek nagy része megbízik a másikban, és nem is sejtené, hogy az, aki például felhívja telefonon, és megemlít pár belső információt, használja a szervezeten belüli szakzsargont, esetleg egy támadó lehet, és éppen bizalmas információt próbál meg kicsalni belőle.

**6. Dumpster diving („Kukabúvárkodás")**[8]

**7. Baráti üdvözlet**
Lehet, hogy odafigyelünk számos veszélyesnek tűnő jelre, és az ismeretlen címről érkező e-mailekkel nem törődünk, azokat rögtön töröljük (jobb esetben jelezzük őket a bv. szervezet információbiztonsági felelősének), hiszen ennek jelentőségét – úgy vélem – mindenki ismeri már a szervezetünknél, ám ha egy kedves barát küld nekünk üzenetet, azt feltehetően automatikusan megnyitjuk, hiszen nem hisszük, hogy bármi veszélyt is rejthet. Azért nagyon veszélyes ez a technika, mert eszünkbe sem jut, hogy az adott e-mail veszélyforrás lehet, hiszen megbízható személytől kaptuk. Ahhoz pedig, hogy a támadó hiteles legyen, elég csak megnéznie az érintett közösségi oldalát, és rögtön talál számtalan barátot, akiket alapul véve elküldheti a vírust.

Összességében a social engineer ugyanazokat a meggyőző technikákat alkalmazza, mint amelyeket mindannyian használunk a mindennapok során. Szerepeket veszünk fel, szívességeket teszünk másoknak. A támadó azonban manipulálja és megtéveszti az embereket, illetve etikátlan módon alkalmazza ezen technikákat, amelyekkel gyakran jelentős sikereket ér el.

## A támadások elleni védekezés

### *A tudatosság fontossága*

Abban az esetben, ha a felhasználók nem ismerik a különféle információk megszerzésére irányuló támadások technikáit, módszereit, felismerni sem fogják majd azokat, valamint a védekezési alternatívákat sem tudják majd hatékonyan és eredményesen alkalmazni. Továbbá, ha a felhasználó nem ismeri a különféle információbiztonsági szabályokat, akkor az ezekből adódó mulasztásokat könnyedén kihasználhatja a támadó. Nem győzöm elégszer kihangsúlyozni a szabályzatok ismeretének fontosságát. Napjainkban már minden szervezet rendelkezik valamilyen biztonsági szabályzattal,

8 Lásd bővebben az „Önellenőrzés" című fejezetben.

előírással, melynek megismerésével és elsajátításával a támadások bekövetkezésének valószínűsége csökkenthető. A biztonsági szabályok elkészítését követően a legfontosabb ezek megismertetése a személyi állománnyal, melynek során tudatosítani kell a munkatársakban, hogy a biztonsági előírások betartásával járó korlátozások az általuk végzett munka hatékonyságát és eredményességét is szolgálják.

A büntetés-végrehajtásnál a már többször említett IBSZ, valamint szervezetünk kiberstratégiája nyújthatja jelenleg a legtöbb segítséget.



## *A támadások elleni védekezés fázisai*

### *Első fázis – Tudás*

A kibertámadások elleni harc első védvonala a tudás. Ismerni kell a biztonságtudatosság alapelveit, a szervezetünk belső szabályozóit, a felelősségi rendszert, illetve a ránk vonatkozó kötelezettségeket. Magyarországon az állami és önkormányzati szervek elektronikus információbiztonságáról szóló 2013. évi L. törvény határozza meg ezek kereteit, nevesíti a szervezetekre vonatkozó követelményeket, és azokat az alapvető szabályokat, amelyek garantálják a biztonságos működést. A támadások elleni sikeres védekezéshez nem csak az informatikai üzemeltetési terület, illetve a rendszergazdák és a vezetők felkészültségére, hanem valamennyi kolléga tudatosságára is szükség van.

### *Második fázis – A biztonságtudatosság elősegítése megfelelő belső szervezeti szabályrendszerrel + ISO 22301*

Belső szabályrendszerünket többször említettem már. Egyfelől érdemes tudnunk a 2013. évi L. törvény alapvetéseit, másrészről részletesen szükséges ismernünk és alkalmaznunk szervezetünk IBSZ-ét, harmadrészt iránymutatást kaphatunk a bv. szervezet kiberstratégiájából is. Ezen ismeretek nélkül csak a szerencsén és az affinitásunkon, valamint az önszorgalmunkon múlik egy esetleges támadás kimenetele.

**ISO 22301 szabvány:** Az ISO 22301 szabvány szerint a szervezetnek képesnek kell lennie arra, hogy egy kárt okozó esemény (pl.: egy dolgozó figyelmetlenségéből vagy tájékozatlanságából adódó kártékony program rendszerbe kerülése) esetén is olyan szinten tudjon tovább működni, ami jelentős mértékben nem befolyásolja az általa végzett tevékenységet. A büntetés-végrehajtási szervezet esetében ez főképp a biztonságos fogvatartást jelenti.

### *Harmadik fázis – Információbiztonsági felelős kijelölése*

Szervezetünknél van olyan felelős személy, aki kimondottan információbiztonsági feladatokkal, azok összehangolásával foglalkozik, ő az információbiztonsági felelős. Tőle kérhetünk segítséget a ránk vonatkozó szabályokkal kapcsolatos kérdéseink esetén, vele egyeztethetjük az információbiztonság kapcsán felmerülő problémáinkat, neki kell jeleznünk, ha valamilyen rendellenességet tapasztalunk. Az ő felelőssége az is, hogy a tudatosítás folyamatos legyen és a számunkra szükséges képzéseken részt vehessünk.

### *Negyedik fázis – Adatbiztonsági kérdések fontossága*

Az adatbiztonság nem teljesen azonos az információbiztonsággal, azonban nem egzakt tudomány, pár magától értetődő szabályt kell csak betartani:

1. Lehetőség szerint csak a szervezetünk által biztosított eszközön dolgozzunk.
2. Ezt az eszközt magáncélra ne használjuk, másoknak ne adjuk kölcsön.
3. Csak titkosított (VPN) kapcsolaton keresztül érjük el a szervezeti infrastruktúrát.
4. Fokozottan ügyeljünk arra, milyen weboldalakat nyitunk meg.
5. Ha műszaki problémánk adódik, lépjünk kapcsolatba a saját szervezetünk informatikai főosztályával, ne kezdjük el magunk megoldani a problémát és semmiképpen ne forduljunk szervezeten kívüli személyhez.
6. Ha szenzitív adatokat kérnek tőlünk, akkor győződjünk meg arról, hogy az illető valóban az, akinek vallja magát (emlékezzünk a social engineering technikákra).
7. Ne használjuk nyílt, publikus hálózatokat munkavégzésre.

### *Ötödik fázis – Oktatás, képzés, érzékenyítés*

Az oktatás és a képzés fontossága arra a tényezőre reflektál, miszerint – ahogy azt már korábban kifejtettem – a kibertámadások sikeressége nagymértékben a humán tényező függvénye. A személyi állomány tagjai jelentik hagyományosan a „leggyengébb láncszemet" a kibervédelemben, értve ez alatt a nem kellően biztonságtudatos viselkedést, a túlzott technológiai bizalmat vagy éppen a hiányzó kételkedést. Az oktatás és a képzés célja nem önmagában egy komplex oktatási vagy vizsgarendszer kialakítása, hanem annak olyan hatékony módon való működtetése, amely a szervezeti kultúrába építi be a biztonságtudatos viselkedést. A képzési rendszerek kialakítása során meg kell szervezni és működtetni azt a hatékony oktatási rendszert, amely a teljes állomány biztonságtudatos viselkedésének növelését eredményezi. Ez véleményem szerint részben megvalósul a Belügyminisztérium Rendészeti Továbbképzési Rendszerén, valamint annak e-learning tananyagain keresztül. Általánosságában elmondható azonban,

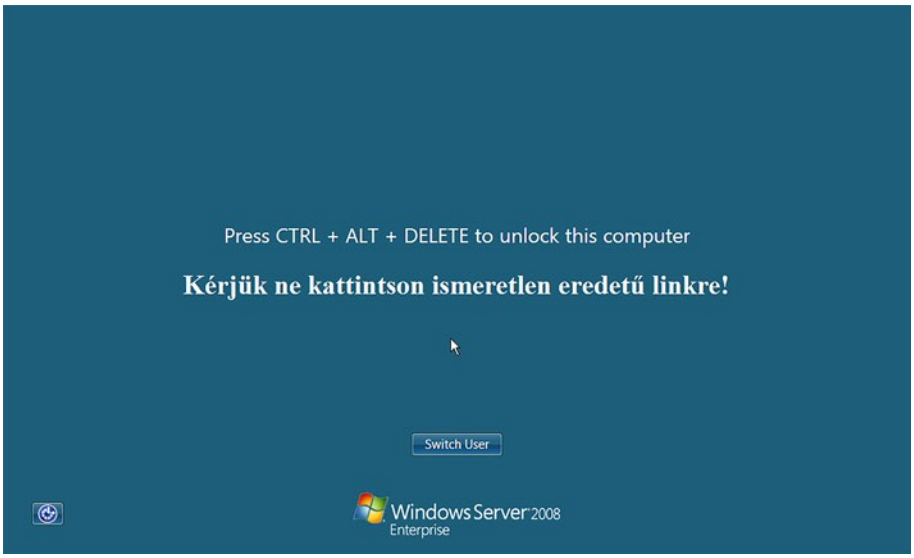
hogy a tananyagokat sajnálatosan nem mindenki tekinti át kellő alapossággal, csupán „lekattintja" a feladatokat, ezért az nyilvánvalóan nem tud rögzülni. Következésképpen úgy vélem, hogy nem elég pusztán az e-learning tananyagok elvégzése ahhoz, hogy mindig és minden helyzetben tudatosan tudjuk kezelni a minket körülvevő kiberteret. Ezen a vonalon haladva kerestem meg Keleti Arthur urat, az Önkéntes Kibervédelmi Összefogás (KIBEV) alapítóját és elnökét, valamint az ITBN CONF-EXPO szakmai összefogás ötletgazdáját, amely képviseli és felvonultatja az informatikai és információvédelemért tenni akaró szervezeteket, gyártókat, disztribútorokat, valamint az őket képviselő tanácsadó és integrátor szolgáltatókat. Keleti Arthur úrral történt hosszas beszélgetésünkben megvitattuk a lehetséges veszélyforrásokat, illetve azon lehetőségeket, melyek segíthetnek az érzékenyítésben. Közös véleményünk szerint több módja is lehet a megfelelő információbiztonsági tudatosítás fejlesztésének. Fontos azonban leszögezni, hogy az érzékenyítés szerepe azon kollégák esetében a legfontosabb, akik saját elhatározásból kevésbé vagy minimálisan sem nyitottak az információbiztonsági intézkedések felé. Ezek a kollégák képviselik azt a réteget, akiket a legnehezebb megszólítani és rábírni a megfelelő lépések megtételére. Keleti Arthur szavait idézve: *„A gond sohasem a fogékony emberekkel van, mindig az elutasító (renitens) kollégák a problémásak."*.



## *Oktatási, képzési és érzékenyítési módszerek*

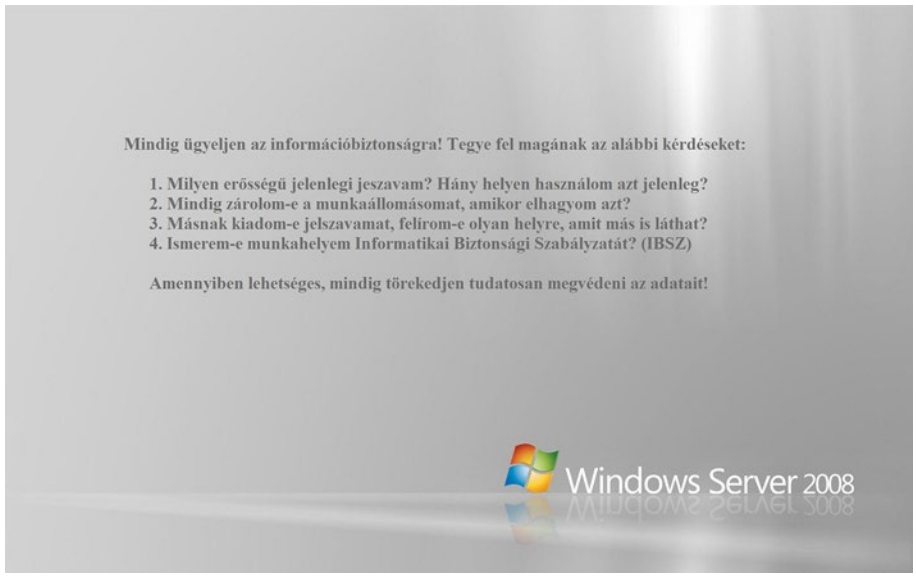
### *Az internalizáció kikényszerítése (sulykolás)*

Az első – és egyben talán leghatásosabb – módszer a viselkedési szabályok elsajátításának kikényszerítése, azaz egyfajta „sulykolás". Minél többször találkozunk egy témával, annál jobban képes rögzülni az adott tudásanyag. A figyelem felkeltésére nincsenek meghatározott módszerek, kreativitás és találékonyság útján lehet elérni a kívánt hatást. Fontos az erős felhívó jelleg, melynek kapcsán találkozhatunk a „blickfang" (a reklám figyelmet megragadó része, amely feltűnő, szembeötlő, harsány, néha akár kirívó is lehet) kifejezéssel, ami a pillantás elkapását jelenti. Ennek a koncepciónak fontos eleme, hogy nem csupán a szokásos eszközökön keresztül érdemes működtetni (faliújság, körüzenet, feladatszabó levél stb.), hanem olyan helyeken is, amiket nem lehet figyelmen kívül hagyni és nehéz elkerülni. Ezen a vonalon haladva készítettem el az alábbi látványterveket, melyek alkalmazása részben megoldást kínálhat a most tárgyalt módszerre. A koncepcióban az alábbi üzenetek ciklikusan változnának, így nagy mennyiségű fontos tartalmat lehet eljuttatni a teljes állomány számára.

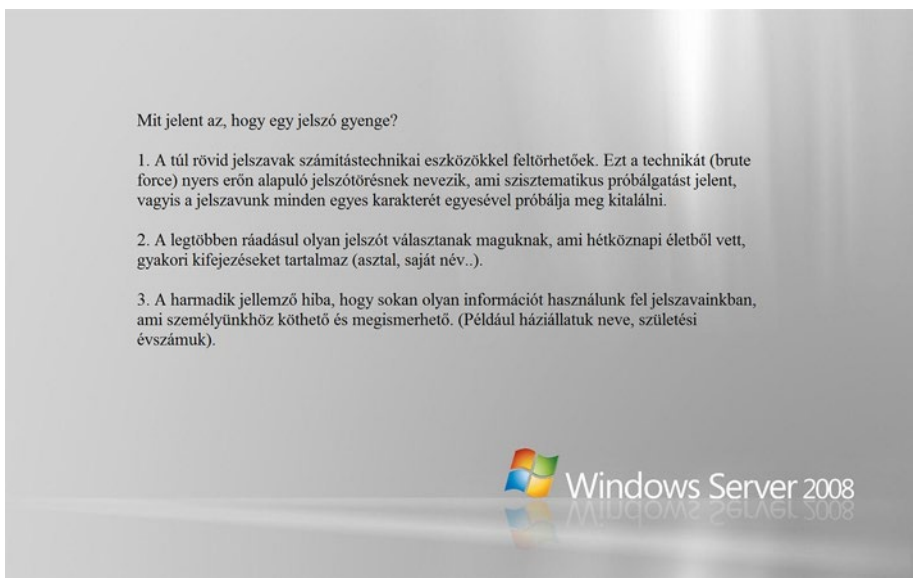



**2. ábra: Lezárt/zárolt képernyő a saját rendszerünkben, mely az ismeretlen eredetű linkre kattintás tilalmára hívná fel a figyelmet, ami gyakori módja az adathalász támadásoknak**


**3. ábra: Lezárt/zárolt képernyő a saját rendszerünkben, mely arra figyelmeztet, ügyeljünk rá, hogy az általunk küldött e-mailek címzettje ne lehessen más személy, mint a tényleges címzett**




**4. ábra: Munkaállomásunk háttere (munkahelyi környezetben), mely az információbiztonsági tudatosságra hívja fel a figyelmünket**




**5. ábra: Munkaállomásunk háttere (munkahelyi környezetben), mely a nem megfelelő jelszóhasználatra figyelmeztet**

Természetesen tekintettel szervezetünk fegyveres jellegére, a túlzottan kirívó, akár játékos, a szó jó értelmében vett infantilis figyelemfelhívó üzeneteket nem célszerű kivitelezni. Vállalati szinten azonban, a civil szféra kiberszakemberei gyakran alkalmaznak ilyen „blickfang" módszereket is, mint például egy óriási széf a közösségi térben

elhelyezve, amihez a megfelelő kódok el vannak rejtve az épület különböző pontjain, ezzel felhívva a figyelmet arra, hogy a nem megfelelően tárolt jelszóval egy jól elzárt adatot is meg lehet szerezni. Álláspontom szerint megfelelően figyelemfelkeltő lehet egy képernyőkép is, amit hatékonyan el lehet juttatni a teljes személyi állományhoz, hiszen napi munkánk során elkerülhetetlenül látjuk a munkaállomásunk képernyőjét.

### *Előadás – személyes megjelenéssel*

Keleti Arthur úrral történt interjúm során számos módszer merült fel, azonban véleményem szerint azok főként vállalati szinten működnének, ellenben egy megfelelően prezentált, érdekes és figyelemfelhívó előadással szintén nagy célközönséget lehet elérni, ebben mindketten egyetértettünk. Egy előadáson történő kötelező megjelenés elrendelésével pedig elősegíthető, hogy az említett „renitens" (információbiztonsági szempontból kevésbé progresszív szemléletű) kollégák is részt vegyenek egy ilyen oktatáson. Ezen esetben pedig egyetlen tényezőn áll vagy bukik a koncepció sikere: az előadó kommunikációs képességein. Kézenfekvő megoldásnak tűnhet egy információbiztonsági felelős által prezentált előadás, azonban ez nagyban függ annak retorikai képességeitől is, éppen ezért „külső", a témában szakértő előadókat érdemes felkérni a prezentációk megtartására, akik az adott témakört közérthetően, esetenként játékos jelleggel, mégis rendkívül informatív módon tárják a személyi állomány elé.

### *Informatikai oktatás*

Mint korábban említettem, ez részben megvalósul a Belügyminisztérium Rendészeti Továbbképzési Rendszerén, valamint annak e-learning tananyagain keresztül. Úgy hiszem, hogy ezt a rendszert nem kell részletesen bemutatni, hisz minden, a bv. szervezetnél foglalkoztatott kolléga ismeri, használja és tanulhat belőle.

## Konklúzió

Tanulmányomban olvashatóak a téma kapcsán a legfőbb hibák és problémák, valamint a lehetséges megoldások, a támadások típusai, módszerei, lélektani hatásai, illetve az ezekre javasolt főbb védekezési stratégiák. Összességében azonban elmondható, hogy a cél nem más, mint egy olyan biztonságtudatos szemlélet kialakítása, melynek köszönhetően a legtöbb incidens elkerülhető, illetve azok súlyossága vagy következményei elhanyagolhatóak. Természetesen nem foglalkoztam az összes fenyegetéstípussal és nem foglaltam össze minden támadási lehetőséget, hiszen napról napra újabb technikák jelennek meg. Igyekeztem az elmúlt pár év tapasztalataira fókuszálni, a minket leginkább körülvevő veszélyekre figyelmeztetni. Meglátásom szerint a kibervédelem hasonlatos az objektumvédelemhez. Ha fejlett, korszerű, jószerével áthatolhatatlan védelemmel látjuk el magunkat, valamint a területet védő személyek is csalhatatlanul, tökéletesen

végzik a feladataikat, vélhetőleg akkor is lesz olyan támadó, aki képes ezt a védelmet kijátszani, megtéveszteni, manipulálni az emberi komponenst. A kiberterrorizmus a társadalom széles rétegeit érintő probléma, azonban sokan még mindig úgy reagálnak a fenyegetésekre, hogy: *„Engem úgysem vernek át", „engem úgysem célozna meg senki", „úgyis észreveszem, ha valaki át akar verni"*. Ezzel szemben bárki válhat a legkifinomultabb megtévesztési módszerekkel, pszichológiai trükkökkel vagy pusztán megfelelő technikai háttérrel rendelkező támadó áldozatává.

A tökéletes védekezés alighanem utópia. Ellenben helyes jelszógyakorlattal, szabálykövető hozzáállással, megfontolt informatikai magatartással, felelősséggel, a szabályzatok ismeretével, megfelelő oktatással, befogadó hozzáállással és némi fogékonysággal már megtettünk mindent az információbiztonsági tudatosságunk megszerzése, valamint annak fejlesztése érdekében.

*„A kiberbiztonság nemcsak közös érdek, hanem közös felelősség is"*[9]

9 Dr. Szabó Hedvig nb. altábornagy

# Felhasznált irodalom

Az információbiztonság lélektana (Psychology of Information Security) - *„KÖFOP keretében megvalósuló fejlesztések IT biztonságának növelése, ezáltal rendszerekkel összefüggő korrupciós lehetőségek és kockázatok csökkentése”* tanulmány

Belügyminisztérium Rendészeti Továbbképzési Rendszer – Információbiztonság lélektana e-learning tananyagai

Kevin D. Mitnick (2003): A legendás hacker – A megtévesztés művészete

Komár Zita: Generációk akkor és most. https://folyoiratok.oh.gov.hu/uj-kozneveles/generacioelmeletek

Nemzeti Egészségbiztosítási Alapkezelő – Elektronikus információbiztonság http://www.neak.gov.hu/felso_menu/lakossagnak/adatvedelem/elektronikus_informaciobiztonsag