*Bányász Péter*

# X. BIZTONSÁGTUDATOSSÁG A DIGITÁLIS TÉRBEN

## BEVEZETÉS

*1934, Nagy-Britannia.* Alekszandr Mihajlovics Orlov ezredes Sztálin utasítására londoni rezidensként azt a feladatot kapta, hogy a szocialista eszmékkel barátkozó fiatalokat szervezzen be szovjet ügynöknek, lehetőleg olyanokat, akik Őfelsége titkosszolgálatában fognak elhelyezkedni.[1] A két világháború között Nagy-Britanniában a baloldali, kommunista eszmék fogadtatása a társadalmi elit ifjúsága körében népszerűnek számított, bár a közvélekedés szerint harmincéves korukra „kinőnek" ezekből az eszmékből, és a továbbiakban tisztes életet élnek. Orlov tisztában volt azzal, hogy könnyebb a pályájuk elején álló fiatalokat megkörnyékezni, akiket aztán a kívánt pozíciókba juttathatnak el. A beszervezés különböző stratégiák mentén történhetett: megvesztegetés, zsarolás, de az ideológiai elköteleződés akár ezeknél is hatékonyabb motivációt jelent. Orlov ezért többek között a Cambridge Universityt választotta a „toborzás" helyszínéül, hiszen itt működött a hallgatók körében nagy népszerűségnek örvendő Cambridge University Socialist Society nevű szervezet, amely egy kommunista eszméket valló ifjúsági klub volt, illetve azért is, mert a végzett hallgatók később nagy eséllyel váltak Nagy-Britannia katonai, politikai, nemzetbiztonsági és gazdasági vezetőivé. Orlov stratégiája működött, hiszen az ő nevéhez fűződik a hírszerzés-történelemből jól ismert „cambridge-i ötök" – vagyis Kim Philby, Donald Duart Maclean, Guy Burgess, Anthony Blunt és feltehetően John Cairncross[2] – hírszerző hálózat beszervezése. Mindannyian a brit elit körébe tartoztak. Orlov munkáját segítette az egyetemen tanító kommunista eszméket valló közgazdász, Maurice Dobb, aki nagy hatást gyakorolt a fiatalokra. Az ideológiai elköteleződés mellett a beszervezést segítette, hogy Blunt és Burgess bizonyítottan homoszexuálisok voltak, Maclean valószínűsíthetően biszexuális beállítottságú volt. Az 1930-as évek Nagy-Britanniájában ez súlyos bűncselekménynek számított, ami még

[1] Heffernan 2015: 74–88.

[2] A „cambridge-i ötök" ötödik tagját hivatalosan sosem azonosították.

DOI: https://doi.org/10.36250/01334_10 • ORCID: https://orcid.org/0000-0002-7308-9304

évtizedekig érvényben maradt.[3] Orlov várakozásainak megfelelően az „ötök" később komoly beosztásokat töltöttek be, Kim Philby például egy időben a Szovjetunió elleni brit hírszerzés egyik vezetője lett, ily módon az amerikai–brit partnerszolgálati együttműködés következtében az amerikaiak által megszerzett és a briteknek átadott információ a szovjetekhez is eljutott.[4] Mások a kezdetektől ráláttak az amerikai atomfegyver fejlesztésére.

*

Napjainkban az infokommunikációs technológiák (IKT) egyre kiterjedtebb rendszert alkotnak, számuk a jövőben jelentősen emelkedni fog, ami számos új típusú biztonsági kockázatot jelent. Az *internet of things* (IoT), vagy magyar kifejezést használva a dolgok internete, különböző, egyértelműen azonosítható objektumokra és azok internetszerű hálózatára utal. A kifejezést 2009-ben alkotta meg Kevin Ashton, de a koncepció ötlete 1991-ben vetődött fel először.[5] Objektum alatt értjük ebben az esetben az összes olyan elektronikai eszközt, amely képes valamilyen hasznos információt felismerni, „mérni", és ezt kommunikálni is egy másik eszköz felé. Lehet ez egy okostelefon, egy vérnyomásmérő vagy az autónk fedélzeti számítógépe (ECU). Nincsenek sem méretbeli, sem pedig felhasználási megkötései ezen eszközöknek.

Mindebből látható, hogy nem tudjuk kivonni magunkat ezen eszközöknek a hatása alól, hiszen a társadalmunk minden alrendszerében ezek irányítják a különböző folyamatokat. Ebből következően kiemelten fontos, hogy a felhasználók a lehető legmélyebb ismeretekkel rendelkezzenek az infokommunikációs technológiák használatával kapcsolatban, amelynek nemcsak a digitális írástudásban, hanem az adat- és információbiztonsági tudatosságban is meg kell jelenni. A fejezet célja, hogy ez utóbbival kapcsolatban komplexen mutassa be a biztonságtudatosság szerepét, hiszen ahogy Kim Philby és társai példájában is láthattunk, a közszolgálatban dolgozók az általuk kezelt adatok okán különösen kitettek a támadásokkal szemben.

[3] Ezzel kapcsolatban érdemes felidézni Alan Mathison Turing példáját. Turing a modern számítógép-tudomány egyik atyja, aki a második világháború alatt jelentősen hozzájárult ahhoz, hogy a britek feltörjék a megfejthetetlennek hitt német Enigmát, ami nagyban hozzájárult a szövetségesek győzelméhez. 1952-ben homoszexualitása miatt elítélték, a börtönbüntetés helyett végül a libidócsökkentő hormonkezelést választotta.

[4] Például ennek következtében értesültek 1961-ben a kubaiak a tervezett amerikai inváziójáról a Disznó-öbölben, és az időben megkezdett mozgósítás hatására visszaverték a megszálló erőket.

[5] Lu–Wang 2010.

A „cambridge-i ötök" véleményünk szerint fontos tanulsággal szolgálnak a Nemzeti Közszolgálati Egyetem hallgatói számára.

## AZ INFORMÁCIÓS KÖRNYEZET MEGJELENÉSE

Annak érdekében, hogy a biztonságtudatosság fogalmát komplexen értelmezhessük, szükséges röviden áttekinteni az internet fejlődésének történetét. Az internet olyan globális számítógépes hálózat, amelyen a számítógépek az internetprotokoll (IP) segítségével kommunikálnak. Mint az közismert, az internet egy amerikai katonai fejlesztés eredményeképpen került át a civil életbe. Az 1960-as években a szovjetek űrversenyben betöltött fölényének ellensúlyozására Dwight D. Eisenhower elnök létrehozta a Defense Advanced Research Project Agencyt, ismertebb nevén a DARPA-t. A DARPA egyik projektje volt egy olyan számítógép-hálózat kifejlesztése, amely egy esetlegesen az Amerikai Egyesült Államokat érintő nukleáris támadás esetén a megmaradó infrastruktúrát képes lesz működtetni. Az 1970-es években jelent meg az e-mail, ekkorra az egyetemek, a különböző kutatóintézmények is kapcsolódni tudtak az internethez. Az 1980-as években rohamosan fejlődésnek indult az otthoni személyi számítógépek piaca, ami 1992-re elvezetett a világháló, vagyis a *world wide web* kialakulásához, a ma ismert internet megszületéséhez. Az internetre az 1990-es években a demokrácia zálogaként tekintettek, egy olyan eszköznek tartották, amelyen keresztül mindenki szabadon, az anonimitásnak köszönhetően a felelősségre vonás félelme nélkül kinyilváníthatja politikai, lelkiismereti vagy bármilyen véleményét. Az internet legnagyobb kockázatának ekkor az emberek elmagányosodását látták, hiszen az internetezők eltávolodnak egymástól, kivonulnak a társadalomból, és életüket egy lesötétített szobában a monitor előtt ülve fogják leélni. Mint látni fogjuk, nem csak ez változott meg pár évtized alatt.

A kibertér kifejezésünk a görög *kyber* szóból származik, ami hajózásra alkalmas teret jelent. A kifejezést William Gibson sci-fi-író alkotta meg, először az 1982-ben megjelent *Izzó króm* című regényében használta, de a két évvel később megjelent *Neuromanc* tette közismertté. Gibson regényei óta különböző fogalmi meghatározások születtek a kibertérre, de földrajzi értelemben az infokommunikációs technológiákban megnyilvánuló térfogalmat jelent, nem pedig a technológiára utal.[6] A kibertér térszerkezetének leírására számos kísérlet született geometriai, formai, szerkezeti jellemzőinek meghatározásával. A térgeometriai jellemzők feltárása azonban nem egyszerű, hiszen a kibertér számos különböző, eltérő funkciójú tartományból tevődik

[6] Mészáros 2001: 769–779.

össze, illetve mindegyike mesterségesen konstruált. A különböző térfelfogásokat az alapján alkották meg, hogy a fogalom használói a kibertér mely csoportjával foglalkoztak.[7] Ez alapján beszélünk:

- koncepcionális térfelfogásról, ez alatt az IKT önálló belső terét értjük, az internetet és annak alkotó térrészeit, például e-mailek tere, a fájlátvitel tere. Ebben az értelmezésben az internet az abszolút kibertér;
- infrastrukturális térfelfogásról, e felfogás középpontjában a kibertér leginkább fizikai megközelítése áll, azokat a háttérben meghúzódó infrastrukturális elemeket értik alatta, amelyeken a virtuális interakciók lezajlanak – szerverek, gerincvezetékek, optikai kábelek stb.;
- oldaltérképek terei, nagyban hasonlatos a könyvekben található tartalomjegyzékekhez. Az oldaltérképek egyfajta modellezési eljárások, a honlapokon elhelyezett útmutatók, amelyek a honlap tartalmában segítenek eligazodni a felhasználóknak. Ez esetben már nem beszélhetünk semmiféle fizikai leképezésről, földrajzi lokalizációról, kizárólag a virtuális térben értelmezhető;
- a sajátos pávamodellek terei, az egyik legelvontabb térfelfogás, amelynek a lényege, hogy egy nyomkövető eljárással az információs csomagok útvonalát követik a hálózatban (kiindulási ponttól a célig), majd ezeket vizuális módon faszerkezethez vagy pávatollhoz hasonló ábrán jelenítik meg. Az eljárás célja, hogy az internet belső szerkezetét térképezze fel. Maga a pávatérkép az internethez hasonlóan folyamatosan változik, hol bővül, hol szűkül, így a teljes feltérképezés megoldhatatlan feladatnak bizonyul. A pávamodell térszerkezet már önálló belső teret alkot, híján minden fizikai kapcsolatnak;
- virtuális világok, maga a fogalom egy erőteljes szűkítés az internethez képest, digitális technológiával létrehozott világot jelent, az általa képzett perceptualitást értjük alatta. Megalkotása mögött az az egyszerű igény húzódik meg, hogy az információ könnyebben kezelhetővé váljon. Sajátosságának tekinthető, hogy a digitális környezetben a felhasználó is jelen van. A virtuális valóság eszköze lehet például az okosszemüveg.

A kibertér szakít a klasszikus térfelfogással, hiszen nem képes értelmezni számos fizikai alapvonást, amelyek hatására a tér halmazt alkot, azonban bizonyos térszerkezeti elemek mégis kimutathatók benne, ami által teljesen új interpretációt jelent a virtuális térben. Ilyen kategóriaként értelmezhető a külső és belső tér, a hely, a helyzet, a távolság, az irány, a határ, illetve a különböző szintek.

[7] Jakobi 2002: 1482–1491.

A kibertér fogalmának meghatározására a magyar stratégiai gondolkodásban viszonylag korán születtek kísérletek. A magyar kormányzat az Európai Unió tagállamainak élmezőnyébe tartozott, amikor a 2010-es évek elején megalkotta azokat a stratégiákat, jogszabályokat, amelyek a kibertérrel kapcsolatos kockázatok felmérését, kezelését hivatottak ellátni. A 2012-ben megalkotott Magyarország Nemzeti Kiberbiztonsági Stratégiája új alapokra helyezte Magyarország kibervédelmét.[8] A stratégia a következő megfogalmazást tartalmazza: „A kibertér globálisan összekapcsolt, decentralizált, egyre növekvő elektronikus információs rendszerek, valamint ezen rendszereken keresztül adatok és információk formájában megjelenő társadalmi és gazdasági folyamatok együttesét jelenti."[9] Az 1089/2025. (III. 31.) Korm. határozattal elfogadott Magyarország Kiberbiztonsági Stratégiája 2025-ben váltotta fel a korábbi irányelveket. A dokumentum ugyan nem tartalmaz a „kibertér" fogalmára vonatkozó közvetlen, önálló szakaszban megfogalmazott, explicit definíciót, azonban a stratégiai célkitűzések és leírások alapján egyértelműen kirajzolódik annak értelmezése. Eszerint a kibertér alatt olyan digitális infrastruktúra értendő, amely hálózati összeköttetést biztosít, s amelynek létfontosságú elemei közé tartoznak az információs és kommunikációs technológiák (IKT) termékei és szolgáltatásai. A kibertér heterogén szerkezetű, dinamikusan fejlődő tér, ahol számos piaci szereplő párhuzamosan, gyakran egymással versengve nyújt különféle szolgáltatásokat és technológiai megoldásokat.

Komplexebb megközelítését adja a kibertérnek Haig Zsolt. A szerző megállapítása szerint

> „egyértelműen kijelenthetjük, a kibertér fontos jellemzője, hogy abban az elektromágneses spektrumot felhasználva és/vagy vezetékes kapcsolaton keresztül hálózatba kötött infokommunikációs rendszerek működnek, amelyek különböző elektronikus információkezelési tevékenységeket (elektronikai úton végrehajtott adatszerzés, adatfeldolgozás, adattárolás, kommunikáció stb.) végeznek. A különböző hálózatba kapcsolt infokommunikációs rendszerek az információs környezet azon tartományát használják, amelyben e rendszerek működnek, léteznek (fizikai dimenzióban), a különböző elektronikus információkezelési folyamatok zajlanak (információs dimenzióban), valamint e rendszerek elleni tevékenység és védelem megvalósul (fizikai és információs dimenzióban). Ebből következően tehát a kibertér az információs környezet fizikai és információs dimenziójában értelmezhető."[10]

[8] Rajnai–Fregan 2017: 351–354.
[9] 1139/2013. (III. 21.) Korm. határozat.
[10] Haig 2015.

Véleményem szerint az, hogy mit értünk a kibertér fogalma alatt, milyen térfelfogásként gondolkodunk róla, miket azonosítunk az összetevőiként, nagyban kapcsolódik a kibertér védelméhez. Teljesen más védelmi mechanizmusokat kell alkalmaznunk a koncepcionális, illetve az infrastrukturális térfelfogás esetében, hisz míg előbbi alapvetően az internetet érti a kibertér alatt, addig az infrastrukturális értelmezés esetében a védendő entitások a fizikai térben is jelentkeznek, és ez teljesen eltérő védelmi megoldásokat követel meg. Ennek igazolására az óceánok fenekén található távközlési kábelek kiváló példával szolgálnak: ezek védelme több alkalommal a NATO nyugtalanságát idézte elő, amikor orosz tengeralattjárók rendszeresen megközelítették azokat 2017 decemberében. Az Atlanti-óceán északi részén lefektetett kábelek felelnek Észak-Amerika és Európa között az internetes kommunikáció biztosításáért. Nem nehéz belátni, egy célzott támadással, ami diszfunkciót okoz a távközlési kábelekben, óriási károkat lehet okozni.

Fontos megemlíteni a nemzetközi jogban szabadon használható területet, avagy a *res communis omnium usus*-ként használt fogalmat. Ennek lényege, hogy az államok felségjoga csak bizonyos távolságig terjed, ha meghaladják ezt a meghatározott távot, nem érvényesíthetik joghatóságukat. A szabadon használható terek hatályába tartozik a világűr, az Antarktisz, a tengerfenék és a nyílt tenger, amihez újabban ötödikként a kibertér is sorolható. Ezekben a terekben nem értelmezhető az államok szuverenitása, azonban számos olyan biztonsági kockázat forrását jelentik, amelyek jelentősként értékelhetők. Ennek igazolására a Stop Online Piracy Act (SOPA) elleni fellépés kiváló példával szolgál.[11] A szerzői jogvédelemmel foglalkozó lobbicsoportok 2011-ben kiharcolták, hogy az amerikai törvényhozás elé kerüljön a SOPA, ami az online kalózkodással szemben egy korábbiakban nem létező kiterjesztett jogkörrel és szigorral lépett volna fel. Magát a törvénytervezetet a Kongresszus számos tagja mellett Barack Obama elnök is támogatta. Velük szemben határozták meg magukat a nagy technológiai cégek, mint a Google, Facebook és egyebek, amelyek támogatókat szereztek az Anonymous hacktivista csoportok, valamint a világ számos internetezőjének körében.[12] Az egyre növekvő, közösségi oldalakon zajló tiltakozások hatására fokozatosan hátráltak ki a Kongresszusban korábban támogató képviselők, beleértve Obama elnököt is. Mindez végül a törvénytervezet bukásához vezetett, ami, azt gondolom, egy igen fontos fordulópontot jelentett. Egy, az Amerikai Egyesült Államok területén hatályos jogszabályt azért nem fogadott el az amerikai törvényhozás, mert az amerikai állampolgárokon felül világszerte támadták az internetezők. Véleményem szerint ez jogi értelemben

[11] Cartwright 2018: 383–401.

[12] Magyarországon például a népszerű vlogger, Szirmai Gergely buzdította Hollywood Hírügynökség nevű YouTube-csatornájának követőit a petíciók aláírására.

az amerikai szuverenitás csorbulását eredményezte, ami természetesen nem csupán az Egyesült Államokat veszélyezteti, hanem minden szuverén állam esetében kockázatot jelent. Az eset másik tanulsága a technológiai vállalatok ereje, ami a politikai döntéshozatalban betöltött szerepüket is mutatja.

Mindebben komoly változást jelentett a közösségi média megjelenése. A közösségi média definiálására számos kísérlet született, amelyeknek döntő többsége a marketing tudományterületéhez kötődik, így elsősorban a marketinghez kapcsolódó fogalmakkal operál. Az *Oxford Dictionaries* a közösségi médiát weboldalak és alkalmazások összességeként írja le, ahol a felhasználók tartalmat készíthetnek és megoszthatnak a közösségi hálózatokon.[13] Ehhez a definícióhoz köthetők az Andreas Kaplan és Michael Haenlein által megfogalmazottak, miszerint a közösségi média „internetes alkalmazások olyan csoportja, amely a web 2.0 ideológiai és technológiai alapjaira épül, ami elősegíti, hogy kialakuljon és átalakuljon a felhasználó által létrehozott tartalom".[14]

Elfogadva a Kaplan–Haenlein-szerzőpáros által megfogalmazottakat, de mégis kiegészítve a meghatározást, a közösségi média alatt olyan internetes oldalak és alkalmazások összességét értem, amelyeknél a szolgáltató csupán a keretet biztosítja, a tartalmat a felhasználók állítják elő. Ebből következik, hogy a közösségi média elsősorban a felhasználók interakciójából alakul ki, amely a többi felhasználó megosztásából, kiegészítéséből akár részben/teljesen új tartalom előállítását jelentheti. Elméletileg ez a tartalom folyamatosan változhat, kiegészülhet, akár új információk hatására bővülhet. A fogalmi meghatározást alapul véve a közösségi média alkotói tehát olyan oldalak, amelyek megfelelnek a tartalom-előállítás, -megosztás kritériumának. A közösségi oldalak csoportosítására különböző elméletek léteznek, amelyek a felhasználók, alkalmazástípusok függvényében kategorizálják az egyes oldalakat.

Ngai és szerzőtársai például egy olyan konceptuális keretet ajánlanak, amely három egymásra épülő szintet feltételez.[15] Véleményük szerint modelljük adaptálása végül a közösségi médiával kapcsolatos kutatások inter- és multidiszciplináris feldolgozásához vezet.

[13] Oxford Dictionary [é. n.].
[14] Kaplan–Haenlein 2010: 59–68.
[15] Ngai et al. 2015: 769–802.

Az első szint a közösségi médiával kapcsolatos elméleteket, modelleket jelöli. Idesorolják a szerzők:

- a magatartáselméleteket (például személyiségjegyek,[16] TAM-modell[17]);
- a szociális tanuláselméleteket (például társadalmi tőke,[18] társadalmi identitás[19]);
- a tömegkommunikációs elméleteket (például paraszociális kapcsolatok,[20] használati-juttatási modell[21]).

A második szint a platformokat jelöli. Idesorolják a szerzők:

- tartalommegosztó oldalakat (például YouTube, Picasa);
- közösségi könyvjelző oldalakat (például Pinterest);
- blogokat, mikroblogokat (Blogger.com, Twitter);
- virtuális/online közösségeket (például Lonely Planet, Yahoo Answer);
- közösségi hálózatokat (például Facebook, LinkedIn);
- virtuális világokat (például Second Life).

16 Az egyes személyiségjegyek kategóriákba történő sorolásának az oka, hogy ily módon különbséget tudjunk tenni az egyes individuumok között, megértve ezáltal a viselkedésük mögötti motivációt, illetve interperszonális interakcióikat (Pléh–Boros 2010).

17 A TAM-modell *(technology acceptance model),* vagyis a technológiaelfogadás modellje szerint a felhasználó által érzékelt hasznosság, valamint a technológia könnyed használata határozza meg, hogy a felhasználó az adott technológiát milyen könnyen fogadja el (Davis 1989: 319–340). Az eredeti modell megalkotása Davis nevéhez fűződik, ezt azonban továbbfejlesztették. A TAM2-modell a hasznosság mértékét meghatározó tényezőket is figyelembe veszi (Venkatesh–Davis 2000: 186–200), mint például imázs, szubjektív norma, az output minősége, az eredmény bizonyíthatósága és a munkarelevancia.

18 A társadalmi tőke fogalma a közgazdaságtanból ismert tőkefogalomból eredeztethető. A társadalmi tőke az interperszonális interakciókban megbúvó erőforrás, amely a kapcsolatok mennyiségének, minőségének, illetve azok struktúrájának függvénye. A társadalmi tőke elősegítheti az egyén boldogulását, illetve kollektív cselekvések hatására a társadalom prosperálását (Farkas 2013: 106–133).

19 A társadalmi identitás az emberek azon motivációját írja le, amely szerint csoporttagságuk hatására pozitív önértékelésre tegyenek szert. Ez alapján a csoporthoz való tartozás más csoportokkal szembeni pozitívabb percepcióját jelenti (Tajfel 2016: 65–93).

20 Munk Veronika megfogalmazása alapján paraszociális kapcsolatok alatt azokat a kapcsolatokat értjük, „amelyekkel fenntarthatjuk magunkban a közösségiség látszatát, részt vállalhatunk a csoportban, közeliként élhetjük meg néhány ember életét, például a celebrityét. A valódi, közeli emberi kapcsolatainkat – jobb híján – paraszociális viszonyokra váltjuk fel" (Munk 2009).

21 Blumler–Katz 1974.

A harmadik szint pedig az egyes alkalmazási területeket fedi le, amelyek az előző szintek integrációjából valósulnak meg. Ilyen területek:

- a marketing,
- a tudásmegosztás,
- az ügyfélkapcsolat-menedzsment,
- az együttműködésre vonatkozó tevékenységek,
- a szervezeti kommunikáció,
- az oktatás és képzés,
- és az egyebek.

## A KIBERFENYEGETETTSÉGEK OSZTÁLYOZÁSA

A biztonság szó a latin *securus* szóból (se = nélkül, cura = aggodalom, félelem) ered. Meghatározására számos definíciót alkottak, de a legegyszerűbb talán a „fenyegetettség nélküli állapot".[22] A biztonságot általában szűkebb és tágabb értelemben vizsgáljuk. A szűkebb dimenzióhoz az egyéni, kollektív és nemzeti biztonságot soroljuk. Az egyéni biztonság alatt az egyén azon képességét értjük, amely segítségével képes megvédeni magát a káros behatásokkal szemben. A kollektív biztonság az emberek egy szűkebb körének a biztonságát jelenti, míg a nemzeti biztonság a nemzetek képessége az értékek, érdekek védelmével kapcsolatban. Ez esetben jellemzően a más államok agresszív cselekedeteivel szembeni védelmet értjük. Tágabb dimenzióban a nemzetközi biztonságot értjük, amelynek középpontjában az áll, hogy az államok biztonsága összekapcsolható, együttműködés segítségével kölcsönösen erősíthető. Az együttműködéshez megfelelő szervezeti keretek szükségesek, amelyek lehetővé teszik az államok véleménycseréjét és érdekeik harmonizálását a gazdaság, a külpolitika, a biztonságpolitika és a védelem területén. A hidegháború idejében a biztonságot alapvetően a katonai biztonság primátusa jellemezte, azonban a bipoláris világrend felbomlásával paradigmaváltás ment végbe a biztonsági tanulmányokban. Ennek hatására Barry Buzan és társai értelmezésében a biztonság fogalma kiszélesedett, munkásságuk nyomán megkülönböztetünk katonai, politikai, gazdasági, társadalmi és környezeti biztonságot.[23]

A fenyegetettség nélküli állapot azonban nem önmagában való, ahhoz, hogy elérjük, különböző védelmi megoldások sorát szükséges alkalmazni. E megállapítás különösen érvényes a kibertérre, ahol a biztonság megteremtését különböző

[22] Haig 2015.
[23] Buzan – Wæver – De Wilde 1997.

dimenziókban szükséges megvalósítani. A 2013. évi L. törvény[24] (Ibtv.) az információbiztonsággal kapcsolatos normatív szabályozás egyik alapköve volt 2025-ig, amit a 2024. évi LXIX. törvény Magyarország kiberbiztonságáról váltott. A támadók célja – legyen bármi is a motivációjuk – az elektronikus információs rendszerbe történő behatolás. Éppen ezért ennek biztonsága „az elektronikus információs rendszer olyan állapota, amelyben annak védelme az elektronikus információs rendszerben kezelt adatok bizalmassága, sértetlensége és rendelkezésre állása, valamint az elektronikus információs rendszer elemeinek sértetlensége és rendelkezésre állása szempontjából zárt, teljes körű, folytonos és a kockázatokkal arányos".

Vizsgáljuk meg picit alaposabban e fogalmat, ugyanis számos fontos kifejezést tartalmaz. Az első és legfontosabb, hogy az elektronikus információs rendszerben kezelt adatok esetében biztosítani szükséges az úgynevezett CIA-hármast, ami az adatok bizalmasságát *(confidentiality)*, sértetlenségét *(integrity)* és rendelkezésre állását *(availability)* jelöli. A 2024. évi LXIX. tv. meghagyta az Ibtv. fenti fogalmi definícióit. Ez alapján:

- „bizalmasság: 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: 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, azaz hiteles, valamint a származás ellenőrizhetőségét, bizonyosságát, azaz letagadhatatlanságát is, illetve az elektronikus információs rendszer elemeinek azon tulajdonságát, amely arra vonatkozik, hogy az elektronikus információs rendszer eleme rendeltetésének megfelelően használható";
- „rendelkezésre állás: annak biztosítása, hogy az elektronikus információs rendszerek az arra jogosult személy számára elérhetők és az abban kezelt adatok felhasználhatók legyenek."

A zárt védelem lényege, hogy számításba vegyük az összes létező fenyegetést, illetve folytonos, ha az időben változó körülmények és viszonyok között is megszakítás nélkül megvalósul, továbbá teljes körű, ha az elektronikus információs rendszer valamennyi elemére kiterjed, kockázatokkal arányos pedig, amelynek során a védelem költségei arányosak a fenyegetések által okozható károk értékével (lásd érdekességként a 10.1. ábrán ennek matematikai képletét).

[24] 2013. évi L. törvény az állami és önkormányzati szervek elektronikus információbiztonságáról.

$$r = \sum_{t \in T} (p_t \times d_t)$$

*r:* a kockázat (Ft/év),
*T:* a releváns fenyegetések halmaza,
$p_t$: egy adott kockázat bekövetkezésének gyakorisága (1/év),
$d_t$: egy adott kockázat bekövetkezéséből származó kár (Ft).

10.1. ábra. *Kockázattal arányos védelem matematikai képlete*
*Forrás:* MUHA–KRASZNAY 2018

Fontos röviden tisztázni a kockázat fogalmát is, hiszen ennek mértéke befolyásolja a védekezést. A 2024. évi LXIX. tv. meghagyta az Ibtv. kockázatfogalom-meghatározását: „a fenyegetettség mértéke, amely egy fenyegetés bekövetkezése gyakoriságának (bekövetkezési valószínűségének) és az ez által okozott kár nagyságának a függvénye".

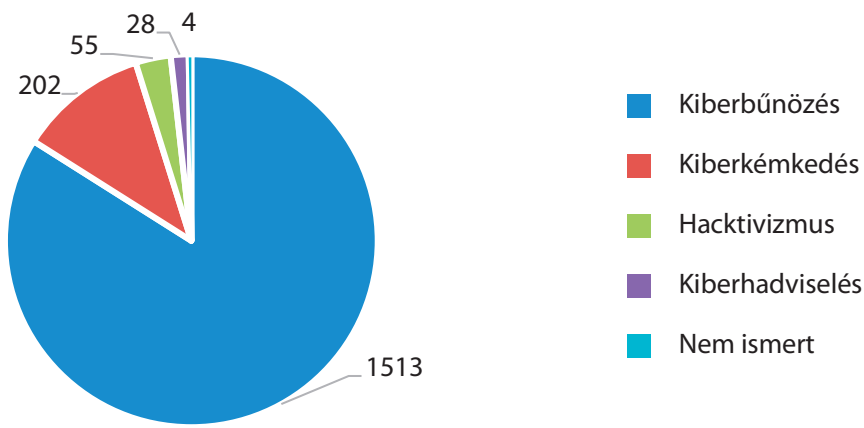
Annak érdekében, hogy csökkentsük a biztonsági események bekövetkezésének valószínűségét, különböző védelmi megoldásokat alkalmazunk, mint:

- adminisztratív védelem: azon szervezési, szabályozási és ellenőrzési intézkedések összessége, amelyek a védelem szervezeti kereteit biztosítják. Idetartozik továbbá a biztonságtudatosság növelését célzó oktatási és képzési tevékenység is;
- fizikai védelem: célja a fizikai környezetben megjelenő fenyegetések elleni hatékony fellépés. E védelem magában foglalja többek között a természeti katasztrófák elleni óvintézkedéseket, a mechanikai védelmi eszközöket, az elektronikai jelző- és megfigyelőrendszereket, az élőerős őrzést, a beléptető rendszereket, a megbízható tápáramellátást, a klimatizálást, a tűzvédelmet, valamint a sugárzott és vezetett zavarok elleni védelmet;
- logikai védelem: az elektronikus információs rendszerek szintjén valósul meg, és információtechnológiai eszközök, protokollok, illetve szoftveres megoldások alkalmazásával biztosítja az adatok integritását, rendelkezésre állását és bizalmasságát.

Amikor kiberfenyegetettségekről beszélünk, jellemzően a támadók motivációja alapján kategorizáljuk azokat. A szakirodalom ötféle motivációt különböztet meg, amelyek között gyakran fedezhetünk fel átfedéseket, összemosódásokat. Egy tankönyvben a statisztikai adatok szerepeltetése indokolatlannak tűnhet, hiszen mire vélhetően a kiadvány megjelenik, azok az adatok elavultaknak minősülnek, nem

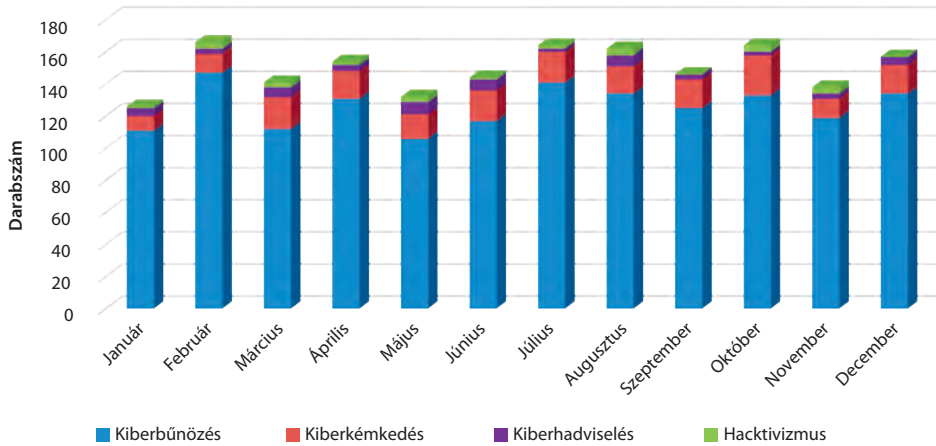
is beszélve az azt követő évekről, amíg a tankönyvet használják.[25] Ennek ellenére az egyes trendek, illetve az indikátorok bemutatására alkalmasak lehetnek. Fontos megjegyezni, hogy a statisztikai adatok – különösen a kiberbiztonság gyorsan változó területén – az idő előrehaladtával óhatatlanul elvesztik aktualitásukat. Ennek ellenére a jelen fejezetben szereplő, a Hackmageddon nevű weboldal által közzétett, a 2019-es évre vonatkozó adatok megtartása indokolt, mivel nem elsődleges céljuk az adott időszak pillanatnyi fenyegetettségi szintjének bemutatása. Az adatok sokkal inkább szemléltető eszközként szolgálnak az egyes kiberfenyegetettségi típusok kategorizálásához és értelmezéséhez. Az így bemutatott tendenciák és példák hozzájárulnak a fogalmi keretek megértéséhez, és elősegítik a tématerület komplex összefüggéseinek feltárását – függetlenül attól, hogy az adatok az adott évre vonatkoznak. Azt is szükséges kiemelni, hogy az adatok kizárólag a bejelentett incidenseket tartalmazzák, ily módon nem teljesek. Ennek egyik oka, hogy számos esetben az áldozatok nem is veszik észre, hogy kibertámadás alanyaivá váltak. Másik ok lehet, hogy nem jelentik az egyes támadásokat. No, de nézzük, mit mutatnak a számok.

A 10.2. ábrán a 2019-ben bekövetkezett kibertámadások számát láthatjuk, ami összesen 1802 esetet számlál, ez 2018-hoz képest 465-tel több esetet jelent, illetve hónapokra történő bontásban a 10.3. ábrán tüntettük fel a trendeket.




10.2. ábra. *Kibertámadások darabszáma 2019-ben motivációk alapján*
*Forrás:* a Hackmageddon.com alapján a szerző szerkesztése

[25] Jelen fejezet 2020 októberében készült.




10.3. ábra. *Kibertámadások megoszlása havonta motiváció alapján 2019-ben*
*Forrás:* a szerző szerkesztése a Hackmageddon.com alapján

Tekintsük át ez alapján, mit is jelentenek az egyes motivációkhoz kapcsolódó támadástípusok. Mint a 10.2. ábrán is látható, a legnagyobb arányban a kiberbűnözéshez köthető eseteket találunk, ami az összes támadás közel 84%-át adja. A kiberbűnözés célja informatikai rendszerek felhasználásával az anyagi haszonszerzés, célpontjaik között az üzleti és politikai világ szereplői egyaránt megtalálhatók.[26] A kiberbűnözők leggyakrabban az alábbi támadástípusokat alkalmazzák:[27]

- *malware*-ekkel[28] (például CryptoLocker, WannaCry, NotPetya stb.) való visszaélés;

[26] Krasznay 2012: 142–151.

[27] Bányász–Krasznay 2019.

[28] Káros szoftver, vagy más néven *malware* az angol *malicious software* összevonásából kialakított mozaikszó. Mint ilyen, a rosszindulatú számítógépes programok összefoglaló neve. Idetartoznak a vírusok, trójai falovak, férgek *(worm)*, kémprogramok *(spyware)*, agresszív reklámprogramok *(adware)*, a rendszerben láthatatlanul megbúvó, egy támadónak emelt jogokat biztosító eszközök *(rootkit)*. A vírus olyan rosszindulatú program, amely képes sokszorosítani és terjeszteni magát, az egyik gépről a másikra. Ugyanez a féregre is igaz, azzal a különbséggel, hogy a vírus általában „befúrja" magát egy futtatható fájlba, hogy teljesítse a célját. A trójai faló egy olyan *malware* program, amely nem próbálja magát lemásolni, hanem inkább úgy tesz, mintha egy legális szoftver lenne, és a felhasználót veszi rá a telepítésre. A nevét a görög mitológiából kapta, mivel ártalmatlan szoftvernek adja ki magát, de valójában rosszindulatú kódot rejt. A vírussal ellentétben nem akar más fájlokat megfertőzni, helyette átadja az irányítást a támadónak. A féreg egy számítógépes vírushoz hasonló önsokszorosító számítógépes program. Míg azonban a vírusok más végrehajtható programokhoz vagy dokumentumokhoz kapcsolódnak hozzá,

- gyerekek szexuális kizsákmányolása;[29]
- fizetőeszközzel elkövetett csalás;
- *social engineer*ing;[30]
- adatok megszerzése, hálózatok támadása;
- létfontosságú rendszerelemek ellen elkövetett támadások;
- különböző pénzügyi tevékenységek *(criminal-to-criminal payments, payment for legitimate services, victim payments);*
- online kommunikáció;
- a kibertér és a terrorizmus összefonódása;
- darknet;[31]

---

illetve válnak részeivé, addig a férgeknek nincs szükségük gazdaprogramra, önállóan fejtik ki működésüket. A kémprogramok segítségével a támadók megfigyelhetik az áldozat internetes tevékenységét, beleértve minden jellegű kommunikációjukat, átvehetik az irányítást a mikrofon, kamera fölött. Több esetben napvilágra került, hogy egyes laptopokba, telefonokba már a gyártósoron előre telepítették ezeket a kémprogramokat. Az *adware* működése során különféle reklámokat jelenít meg, általában trójai programként vagy kereskedelmi alkalmazások ingyenes változataiban települnek a felhasználó eszközére. Az adware-ek egy része *spyware*-ként is funkcionálhat, hogy ily módon minél jobban megismerje a felhasználói szokásokat, preferenciákat, hogy célzott hirdetéseket jeleníthessen meg. A *rootkit* olyan szoftvereszközt jelent, amelynek telepítésével a támadók visszatérhetnek a fertőzött eszközre, ahol magas szintű felhasználói jogosultságot szerez. A *rootkit*et rendkívül nehéz kimutatni, mivel aktívan próbálja elrejteni magát a felhasználó, az operációs rendszer és az antivírus-, *antimalware*-programok elől. Ez a szoftver számos módon települhet a rendszerre, beleértve az operációs rendszer biztonsági réseinek kihasználását vagy adminisztrátori jogok szerzését a számítógépen.

29 Itt nem csupán a pedofil tartalmak terjesztésére kell gondolni, hanem a szexrabszolga-kereskedelemre offline és online (például *stream*) formában egyaránt. Amikor gyermekek szexuális kizsákmányolásáról beszélünk, tisztában kell lenni, hogy csecsemők sérelmére is követnek el ilyen bűncselekményeket. A *darkneten* több olyan hálózatot lepleztek le, amelyek több százezer képet tartalmaztak, amelyek csecsemők megerőszakolását ábrázolták.

30 A fogalmat egy későbbi fejezetben részletesen tárgyaljuk, így most nem foglalkozunk vele ennél a résznél.

31 A *darknet* a *deepweb* azon része, ahol magas szintű titkosítás mellett illegális eszközöket, szolgáltatásokat lehet vásárolni, legyen szó fegyverről, kábítószer-kereskedelemről, bérgyilkosságról, szexuális szolgáltatásokról stb. Annyira speciális szolgáltatásokat is nyújtanak a szervezett bűnözők, hogy ha valaki például egy egykezű, thai, 8 éves fiú szexrabszolgát szeretne vásárolni, akinek zöld haja és zöld szeme van, crackfüggő, akkor ennek megfelelően szállítják le. A magas szintű titkosítás miatt rendkívül nehéz felderíteni az itt elkövetett illegális cselekményeket, amelyek, a példából is látható, igen súlyos bűncselekményeket foglalnak magukba.

- *internet of things, big data, clouds;*
- internetirányítás.[32]

A második legtöbb támadás a kiberkémkedéshez köthető. A kiberkémkedés az államok, piaci szereplők által informatikai eszközökön történő hírszerző tevékenységet jelenti. Maga a hírszerzés egyidős az emberiséggel, és mindig élen járt a technológiai fejlődésben, így nem véletlen, hogy az informatikai eszközök jelentős szerepet töltenek be a hírszerzés világában. A hírszerzésnek a szakirodalom számos információgyűjtő eljárását különbözteti meg, legyen szó a nyílt forrású információgyűjtésről (OSINT), az emberi erővel végzett hírszerzésről (*human intelligence*, HUMINT), az elektronikai felderítésről (*signal intelligence*, SIGINT) vagy a kiberhírszerzésről (*cyber intelligence,* CYBINT). Ezeknek egy hibrid eljárása az elmúlt években külön hírszerzési ágként kezelt közösségi médiás hírszerzés (*social media intelligence,* SOCMINT).[33] Edward Snowden 2013-as színre lépéséből gyakorlatilag köztudottá vált az amerikai nemzetbiztonsági szolgálatok kibertérben végzett, globális megfigyelő képessége, ami többek között a magánszféra létét is megkérdőjelezte.[34] A kiberkémkedéssel kapcsolatban említeni szükséges az úgynevezett APT-támadásokat *(advance persistent threat),* ami fejlett, folyamatos (információbiztonsági) fenyegetést jelent; ez egy olyan támadássorozat, amelynek célja nem a károkozás, hanem a folyamatosan fenntartott rejtett jelenlét és információszerzés. Az ilyen típusú támadások a humán, technológiai, illetve anyagi erőforrások miatt jellemzően állami szereplőket feltételeznek. Fejlettségük okán értelemszerűen sokszor akár évekig rejtve maradnak a megtámadott informatikai rendszerben.

A 10.2. ábrán a harmadik leggyakoribb támadástípus a hacktivizmus: ez számítógépes hálózatokon, általában az interneten, speciális eszközökkel folytatott proaktív politikai aktivizmust jelent, legtöbbször a szólásszabadság, az emberi jogok és az információ szabadsága jegyében. Főbb eszközei lényegében a hagyományos demonstrációk és polgári engedetlenség – egyelőre el nem ismert – digitális megfelelői, illetve a nem

[32] Az internetirányítás fogalma azokat a globális megállapodásokat takarja, amelyek biztosítják az internet megfelelő működését és az internethez való hozzáférést. A legfontosabb kapcsolódó témák az internethez való hozzáférés, valamint az internet biztonsága.

[33] Rolington 2015.

[34] Snowden 2019.

publikus információk megszerzése és kiszivárogtatása. Az egyik legismertebb hacktivista csoport az Anonymous[35] és a WikiLeaks[36].

A 10.2. ábrán negyedikként a kiberhadviselés szerepelt: ez az államok közti konfliktusokban jelenik meg, és segítségével a szemben álló felek számítógépeket és hálózatokat használnak fel katonai célok érdekében, például számítógép-hálózatok működésképtelenné tételére, akár a konvencionális hadviselés támogatására, akár önálló tevékenység folytatására. Kiberhadviselés során a hírszerzés eszközként jelenik meg, amelynek célja, hogy támogassa az adott katonai műveleteket. A kiberhadviselés eszközei a következők:

- nulladik napi sérülékenységek;[37]

[35] A közösség decentralizált, egymáshoz lazán köthető csoportok globális hálózata. Kezdetben az internet cenzúrája ellen, az internet szabadságáért harcoltak, később a fennálló világrend megdöntését, politikai és gazdasági rendszerek átalakítását tűzték ki céljuknak. Célpontjuk volt többek között a Szcientológia Egyház, a Sony, a Los Zetas mexikói drogkartell, a WikiLeakset bojkottáló pénzügyi vállalatok, az iráni, egyiptomi, tunéziai kormányok, újabban az al-Káida és az Iszlám Állam (Berki 2013: 173–185).

[36] A WikiLeakset az oldal önbevallása szerint kínai disszidens újságírók alapították azzal a céllal, hogy a kormányok jogsértéseit, korrupciós ügyeit nyilvánosságra hozzák. A kezdeti ázsiai, afrikai szivárogtatásokat hamar az Egyesült Államokat érintő botrányok váltották fel, amelyek miatt sokan úgy vélik, hogy az USA stratégiai ellenfelei állnak mögötte. A WikiLeaks arca napjainkban Julian Assange.

[37] A nulladik napi támadás alatt olyan biztonsági fenyegetést értünk, amelyben a támadók egy szoftvernek még a fejlesztők által sem ismert sebezhetőségét használják ki. Mivel a hiba senki által nem ismert, így értelemszerűen nem készült biztonsági javítás. *Zero-day exploit*nak nevezik azt a tényleges kódot, amelyet a támadók használnak a sérülékenység kiaknázására, mielőtt a szoftver fejlesztője tudna arról. A kifejezés az *exploit* keletkezésének időpontjából adódik. Amikor a szoftverfejlesztő tudomást szerez egy biztonsági résről, megkezdődik a verseny a támadók és a fejlesztők között; a felelősségteljes fejlesztő igyekszik befoltozni a hibát, mielőtt nyilvánosságra kerül. A nulladik napi támadás az első vagy nulladik napon történik, amikor a fejlesztő már tud a hibáról, így még nem volt lehetősége arra, hogy a biztonsági javítást eljuttassa a szoftver felhasználóihoz. Számos esetben azonban hiába derül ki egy szoftverről, hogy biztonsági rést tartalmaz, ami súlyos következménnyel járhat a felhasználóra, a kiadott frissítőcsomagokat nagyon kevesen telepítik, így hiába van megoldás a probléma befoltozására, a nem frissített alkalmazások ugyanolyan kockázatot jelentenek. Sok alkalmazás esetében van lehetőség bekapcsolni az automatikus frissítést, de több esetben előfordult már, hogy egy letöltött alkalmazás nem tartalmazott kártékony kódot, azonban a később letöltött frissítésbe rejtették el a támadók a fertőzött állományokat, és így fértek hozzá a rendszerhez. A nulladik napi sebezhetőségek rendkívül értékesek a támadók számára. Ezzel a típusú sebezhetőséggel a támadók változatos tevékenységeket végezhetnek, legyen szó például zsarolóvírusok terjesztéséről, számítógépek irányításának megszerzéséről vagy nukleáris erőművek tönkretételéről. Ez utóbbit kiválóan illusztrálja az iráni natanzi urándúsító esete, amelyben az azóta hírhedté vált kiberfegyver, a Stuxnet, egyes szakértők becslése alapján, hat évre vetette vissza az iráni

- botnetek;[38]
- (célzott) *malware*-ek;
- DoS, DDoS;[39]
- APT-k;
- *social engineer*ing;
- irányított energiájú fegyverek.[40]

nukleáris programot. A Stuxnet négy nulladik napi sebezhetőséget használt ki, köztük a Windows operációs rendszerek korábbi sebezhetőségét, amely a számítógéphez csatlakoztatott külső adathordozókat automatikusan elindította. Ezt a fajta sebezhetőséget azóta a Microsoft befoltozta, és a Windows 7 óta a rendszer rákérdez, hogy mit szeretnénk tenni a csatlakoztatott adathordozóval, nem futtatja automatikusan. A 2017-ben a WikiLeaks által nyilvánosságra hozott Vault 7 iratok tanulsága szerint, ami az oldal állítása szerint a CIA kibertámadási képességéről rántja le a leplet, a szervezet közel 250 nulladik napi sérülékenységet ismert. Ezeket hol a CIA, hol a partnerszervezetei, például az NSA fedezte fel, nem kevés anyagi ráfordítással, hol pedig hackerektől vásárolták meg.

38 Robot- vagy más néven zombihálózat alatt olyan fertőzött informatikai eszközök hálózatát értjük, amelyek fölött a támadók átvették az irányítást, és az eszköz erőforrásait saját céljaikra használják fel. Ezeket legtöbbször kéretlen levelek küldésére, bitcoinbányászatra használják, azonban ilyen bothálózatokat használnak rendszerek támadására is. A fertőzött eszközök tulajdonosai sok esetben nincsenek tisztában azzal, hogy a gépük egy bothálózat tagja, csupán annyit tapasztalnak, hogy az eszköz rendkívül lelassult. A dolgok internetének terjedése növelte a zombihálózatok számát, ugyanis rengeteg IoT-eszköz nem rendelkezik megfelelő informatikai védelemmel, így ezek fölött a támadók könnyűszerrel átvehetik az irányítást. 2016 októberében a fél internetet bénította meg egy olyan túlterheléses támadás, amelyet több tízmillió eszközből álló botnethálózat irányított. A hálózat jelentős részét IoT-eszközök, így okoshűtők, webkamerák stb. alkották.

39 A túlterheléses támadásnak két fajtáját különböztetjük meg, ezek a szolgáltatásmegtagadásos (*denial of service* vagy DoS) és az elosztott szolgáltatásmegtagadásos (*distributed denial of service* vagy DDoS) támadások. A támadás célja az informatikai szolgáltatás teljes vagy részleges megbénítása, helyes működési módjától való eltérítése. Egy meghatározott alkalmazás, operációs rendszer ismert gyengeségeit vagy valamilyen speciális protokolltulajdonságait (gyengéit) támadja meg. Célja, hogy az alkalmazás vagy rendszer elérésére feljogosított felhasználókat megakadályozza a számukra fontos információk, a számítógéprendszer vagy akár a számítógéphálózat elérésében. A támadás eredményeképpen a rendszer nagyon lelassul, elérhetetlenné válik, esetleg össze is omolhat. A lényege, hogy lehetőség szerint megakadályozza a célgép elérését. A támadást botnethálózatok segítségével végzik.

40 Irányított energiájú fegyver *(directed-energy weapon):* olyan fegyver vagy rendszer, amely irányított energiát használ, hogy használhatatlanná tegye, megrongálja vagy megsemmisítse az ellenség felszerelését, létesítményeit és/vagy élőerejét. Ez alapján beszélhetünk kinetikus eszközökről, akusztikus eszközökről, rádiófrekvenciás eszközökről, lézereszközökről, részecskesugár-eszközökről. Az elektromágneses tartományt célszerűségi okokból és az alkalmazott eszközök alapvető különbözőségei miatt már itt célszerű önálló csoportba sorolni.

A 10.2. ábrán nem szerepelnek ezzel kapcsolatos adatok, de ettől függetlenül a támadások közé sorolhatjuk ötödikként a kiberterrorizmust, ami Keith Lourdeau megfogalmazásában:

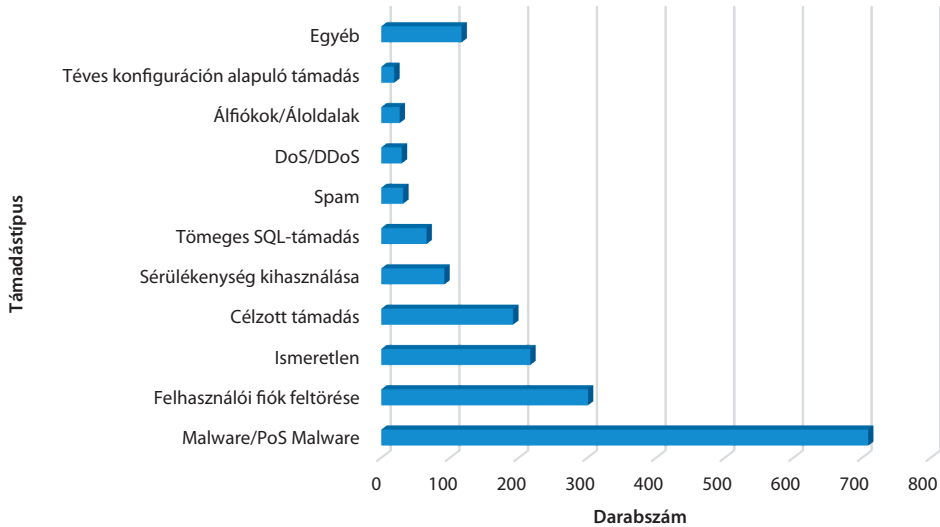
> „A kiberterrorizmus olyan bűncselekmény, amelyeket számítógépekkel és telekommunikációs eszközökkel úgy hajtanak végre, hogy azok rombolják és/vagy megzavarják a szolgáltatások működését, zavart és bizonytalanságot keltve ezzel a lakosságban. Ezen akciók célja a kormányzat vagy a lakosság erőszakos befolyásolása a szervezet egyéni politikai, társadalmi vagy ideológiai céljai érdekében."[41]

Szerencsére elmondható, hogy a terroristák napjainkban nem rendelkeznek azokkal a képességekkel, amelyekkel komplex kibertámadást tudnának végrehajtani, de egyrészt ettől függetlenül számos területen használják a kiberteret, másrészt adott esetben a darkneten megvásárolhatják azt a képességet, ami ahhoz szükséges. Meg kell említeni a magát Iszlám Államnak nevező terrorszervezetet, amely tevékenységeivel, közösségimédia-használatával igazi paradigmaváltást hozott. Nyolc különböző területet azonosíthatunk, amelyben a terroristák sikeresen alkalmazhatják a kiberteret. Ezek az alábbiak:

- információgyűjtés;
- *social engineer*ing;
- kapcsolattartás;
- propaganda;
- új tagok toborzása;
- támogatók szerzése;
- lélektani műveletek;
- kibertámadás.

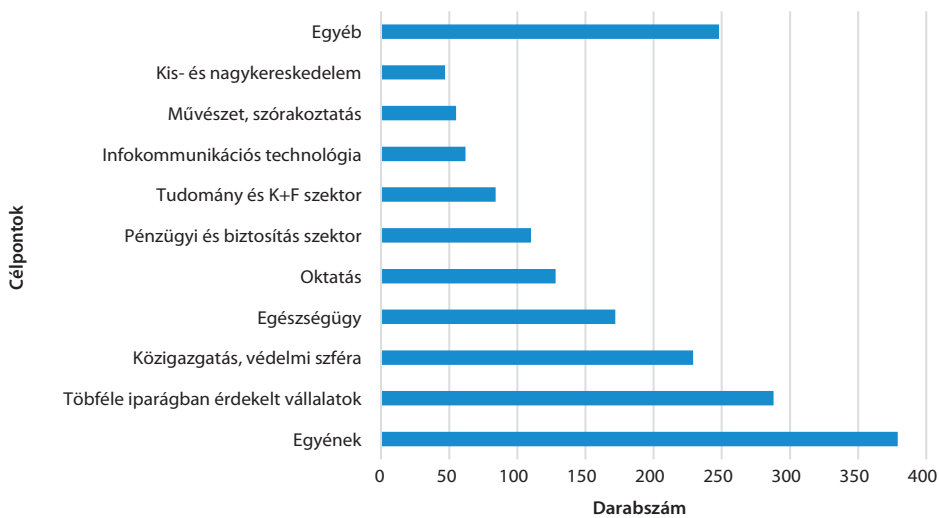
Támadástípusok alapján vizsgálva a 2019-es incidenseket (lásd 10.4. ábra), megállapíthatjuk, hogy a *malware*-ek közel 40%-át teszik ki a támadásoknak.

[41] Bányász 2019.



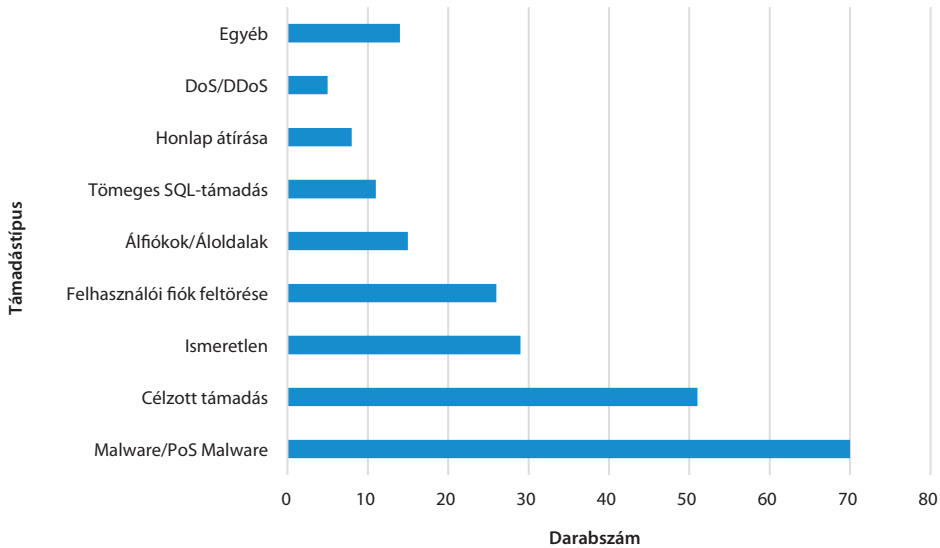

10.4. ábra. *Kibertámadások megoszlása támadástípusok alapján 2019-ben*
*Forrás:* a szerző szerkesztése a Hackmageddon.com alapján

Célpontok szerint (lásd 10.5. ábra) legnagyobb arányban az egyéneket (21%), a többféle iparágban érdekelt vállalatokat (16%), illetve a közigazgatás, védelmi szféra szereplőit (12,7%) érik kibertámadások.



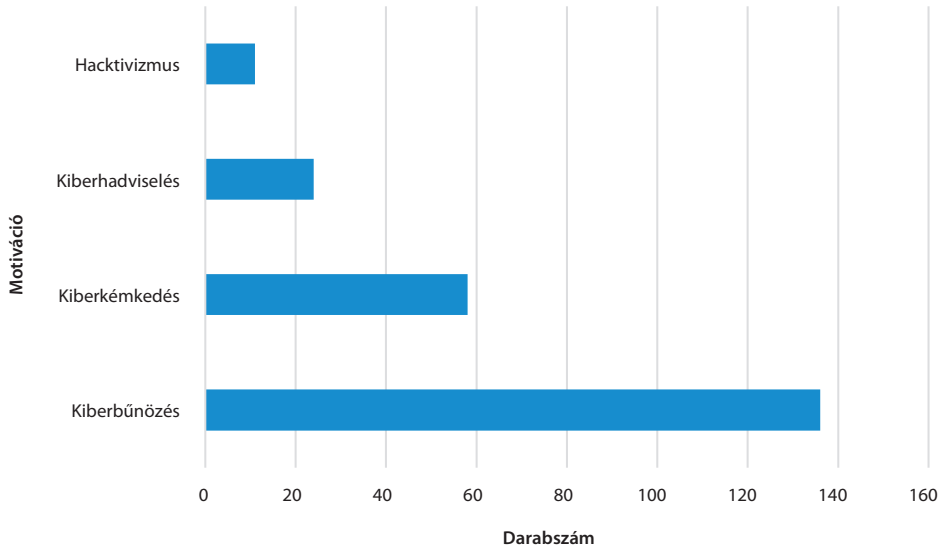

10.5. ábra. *Kibertámadások megoszlása célpontok alapján 2019-ben*
*Forrás:* a szerző szerkesztése a Hackmageddon.com alapján

Ahogy e tankönyvfejezet bevezetőjében fogalmaztam, az állami szféra munkatársai különösen kitettek a kibertámadásokkal szemben. Ha a fenti adatokat lebontjuk a közigazgatás, védelmi szféra területére, azt tapasztaljuk, hogy bár itt is a legnagyobb számban a *malware*-t (30,5%) azonosíthatjuk mint fő támadástípust, de jelentősen megnő a célzott támadások (22,2%) száma (lásd 10.6. ábra), ami az állami szférában kezelt adatok értéke miatt érthető.




10.6. ábra. *Kibertámadások megoszlása a közigazgatásban, védelmi szférában támadástípusok alapján 2019-ben*
*Forrás:* a szerző szerkesztése a Hackmageddon.com alapján

A motivációkat illetően (lásd 10.7. ábra): a trendeknek megfelelően a kiberbűnözéssel kapcsolatos esetek dominálnak, az összes támadás 59,3%-a idesorolható, míg a kiberkémkedés az összes támadás 23,3%-áért, a kiberhadviselés 10,4%-áért, a hacktivizmus pedig 4,8%-áért felel.




10.7. ábra. *Kibertámadások megoszlása a közigazgatásban, védelmi szférában motivációk alapján 2019-ben*
*Forrás:* a szerző szerkesztése, a Hackmageddon.com alapján

## ÖN A LEGGYENGÉBB LÁNCSZEM

Mivel ez a tankönyv a közigazgatás-szervező alapképzéses hallgatók kurzusához készült, így e fejezetben részletesen nem foglalkozunk a védelem logikai és fizikai megoldásaival, a fókuszt a humán aspektusra helyezzük. Ebből fakadóan az egyes támadástípusokkal kapcsolatos jó tanácsokat, megoldásokat vizsgáljuk meg a *social engineer*ing támadásokon keresztül. Maga a fogalom egy olyan támadástípust takar, amelynek során a támadók egy szervezet munkatársán keresztül igyekeznek hozzáférést szerezni egy védett rendszerhez vagy információhoz. Fontos látni, hogy nemcsak az informatikai rendszereknek, hanem az embereknek is vannak sebezhetőségeik, amelyek jellemzően a személyiségükből fakadnak. Idesorolhatjuk például a naivitást, a hiszékenységet, a biztonságtudatosság hiányát, a monotonitást, a különböző függőségeket stb. Kevin D. Mitnick[42] megfogalmazásában: „A *social engineer*ing a befolyásolás és rábeszélés eszközével megtéveszti az embereket, manipulálja

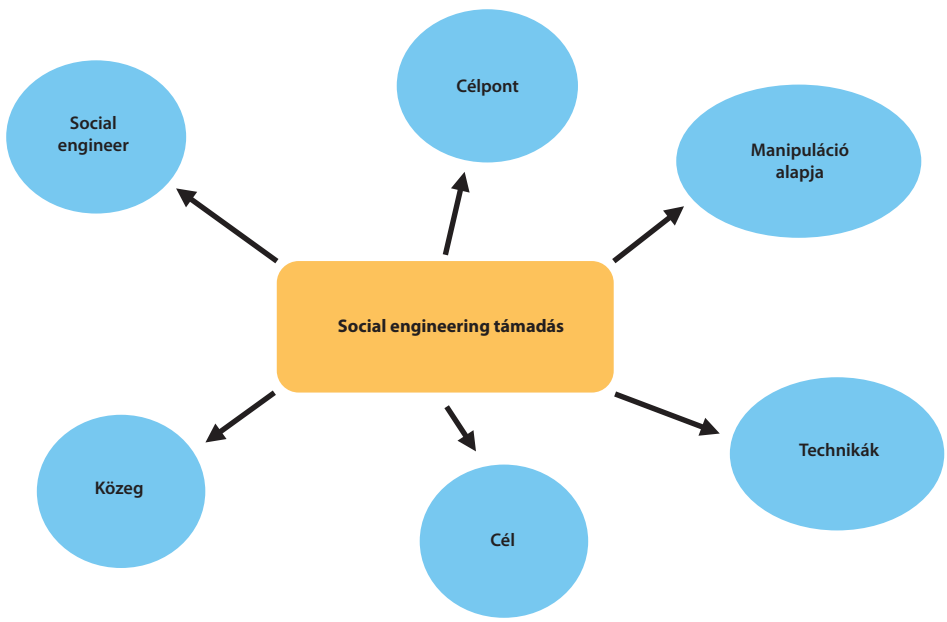
[42] Kevin Mitnick magát sosem tartotta igazán kiemelkedő hackernek, elmondása szerint sikereit inkább *social engineer*ként érte el. Letartóztatását követően szakított a rendszerekbe történő illegális behatolásokkal, biztonsági céget alapított, azóta etikus hackerként tevékenykedik.

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."[43]

A *social engineer*ing támadások taxonómiájára rengeteg felosztás létezik. Mitnick alapvetően négy kategóriára osztotta egy támadás felépítését:[44]

1) információgyűjtés;
2) kapcsolat kiépítése;
3) kapcsolat kihasználása;
4) támadás végrehajtása.

Mitnick modelljét Mouton és szerzőtársai egy komplexebb ontológiai modellé fejlesztették,[45] amelyben az alábbi tényezők szerint kategorizálja a *social engineer*ing támadásokat (lásd 10.8. ábra):




10.8. ábra. *A social engineering támadások ontológiai modellje*
*Forrás:* Dub Máté szerkesztése Mouton–Leenen–Venter 2016 alapján

[43] Mitnick–Simon 2003a.
[44] Mitnick–Simon 2003b.
[45] Mouton–Leenen–Venter 2016: 186–209.

1) *social engineer*:
   a) egyén,
   b) csoport;
2) célpont:
   a) egyén,
   b) szervezet;
3) manipuláció alapja:
   a) barátság vagy jó viszony: az egyén hajlamosabb megtenni valamit, ha az illető a barátja vagy kedveli,
   b) elkötelezettség vagy következetesség: ha az egyén elkötelezte magát valami mellett, hajlandóbb több dolgot megtenni érte,
   c) hiány: az egyének hajlamosabbak teljesíteni a kéréseket, ha hiányt szenvednek bizonyos dolgokból,
   d) reciprocitás: ha az egyén úgy érzi, valakinek a lekötelezettje, hajlamos viszonozni a szívességet,
   e) társadalmi validitás: ha az egyén úgy érzi, a társadalom helyesli a cselekedetét, nagyobb valószínűséggel tesz meg valamit,
   f) autokrácia: ha az egyén úgy érzi, hogy a hatalmi hierarchiában magasabban áll az illető, aki a szívességet kéri, hajlamosabb teljesíteni azt;
4) közeg:
   a) e-mail,
   b) személyes találkozó,
   c) telefon,
   d) SMS,
   e) hagyományos levél,
   f) adathordozó,
   g) weboldal,
   h) röpirat;
5) cél:
   a) anyagi haszonszerzés,
   b) nem engedélyezett hozzáférés,
   c) szolgáltatás megzavarása;
6) eljárás:
   a) adathalászat,
   b) indok kreálása, ez esetben a támadó egy forgatókönyv alapján megteremti azt a környezetet, amelyben ráveszi az áldozatot valamilyen tevékenység elvégzésére,

c) beetetés, ez esetben jellemzően fertőzött adathordozókat szórnak szét, amelyeket az óvatlan áldozat csatlakoztat informatikai eszközéhez,
d) *quid pro quo,* vagyis valamit valamiért;

7) kommunikáció módja:
a) közvetlen,
i) egyirányú, ez esetben csak a támadó kommunikál, a kérést teljesítő félnek nincs lehetősége reagálni a támadó által kommunikált tevékenységre,
ii) kétirányú, ez esetben mindkét fél aktívan részt vesz a kommunikációs csatornában, például e-mail-váltás, telefon,
b) közvetett, ez esetben a kommunikáció indirekt formában zajlik egy harmadik „fél" közreműködésével. E harmadik fél lehet egy eszköz is, mint például egy elszórt fertőzött adathordozó.

A szakirodalom gyakran az alapján tesz különbséget a *social engineer*ing támadások között, hogy használ-e valamilyen informatikai eszközt a támadó. Ily módon beszélhetünk humán és IT-alapú támadásokról.[46] A humán alapú támadásokra az alábbiak szolgálnak példával.[47]

- Segítségkérés – sok esetben sikerrel járnak a támadók, ha valamilyen információt kérnek. Ez természetesen csak egy lépése a végcélnak, de sokszor nagyon jó alapot ad a további információgyűjtésnek, például egy munkatársról olyan, elsőre érdektelennek tűnő információk, amelyek a támadónak hasznosak lehetnek a későbbiekben. Elsődleges célpontjai a help deskek, titkárságok, ügyfélszolgálatok, recepciók munkatársai.
- Segítség nyújtása (fordított *social engineer*ing) – a támadó első lépésként valamilyen problémát okoz, aminek segédkezik a megoldásában, ezzel kiépítve a bizalmat a célpont és közte, majd ezt használja ki a továbbiakban, például előzetesen egy olyan kártevőt küld az áldozat számítógépére, amely akkor fejti ki hatását, amikor a támadó is jelen van.
- Identitáslopás – a támadó a számára legelőnyösebb álcát ölti magára. Az alkalmazottak, különösen nagyobb munkahelyeken, nem ismernek mindenkit, így könnyebben vezethetik meg a gyanútlan munkatársakat. Ilyenkor szervezeten belüli (például karbantartó, rendszergazda, más szervezeti egység vezetője, új munkatárs) vagy szervezeten kívüli (például futár, valamilyen fontos ember, hivatalos személy, auditor) személyek álcáját veheti fel.

[46] Bányász– Bóta–Csaba 2019: 12–37.
[47] Bányász 2018: 59–77.

- Sírkőlopás *(tombstone theft)* – ritka, de létező támadási forma, amelyben a támadó azt használja ki, hogy a vállalatok informatikai rendszerét nem frissítették, és olyan személyek jogosultságait is tartalmazza még a rendszer,[48] akik már nem dolgoznak a munkahelyen.
- Felhatalmazás – a támadó egy harmadik félre hivatkozva kér valamilyen információt, például egy szabadságon levő munkatárs kérte meg, hogy határidőre készítsen el egy jelentést, amelyhez nincs meg minden információja, így ahhoz kér adatokat.
- Jelszavak kitalálása – sok esetben nem szükséges a jelszavakat valamilyen algoritmus használatával feltörni, gyakran kitalálható a felhasználó jelszava, mert nem megfelelő jelszószabályt alkalmaznak. Még mindig rendkívül gyakori az „12345678", „abcd1234" „jelszó" és hasonlók. Ennél valamivel bonyolultabb, de ugyanúgy könnyen kitalálhatók a felhasználóra utaló szavak (születési ideje, kutyája neve stb.). A segítségkérés esetében megszerzett információk adott esetben is hasznosak lehetnek, például a célszemély e-mail-címe, amely egy gyakori vezetéknév esetén sokszor a születési idejét is tartalmazza.
- Baráti üdvözlet – ha bizalmatlanok is vagyunk az ismeretlenekkel szemben, a barátaink esetében már nem vagyunk ennyire óvatosak. A támadók ilyenkor barátaink nevében küldenek például valamilyen fertőzött fájlt, amelyet, bízva a küldő személyben, megnyitunk.
- Bejutás az épületbe – számos módja van ennek, például a takarítókhoz vagy épp a cigiszünetet tartó munkatársakhoz csatlakoznak stb. Használhatnak hamis belépőkártyát; ez lehet egy sima fehér lap, amelyre rányomtatták a támadó fényképét, a szervezet logóját, és belépéskor fontos embernek adja ki magát a támadó, miközben valami fontos emberrel telefonál, bízva abban, hogy elég csak felmutatnia a kártyát, az őrök nem ellenőrzik rendesen, és beengedik anélkül, hogy a kártyát le kellene húznia az érintőpanelen.
- Más jogosultságának felhasználása *(piggybacking)* – a támadó egy szervezeten belüli munkatársnak adja ki magát, aki otthon felejtette a belépőkártyáját, kulcsait stb.

[48] Általában ennek oka az integritás hiányában található meg, például az informatikusok vagy a HR-esek nem kommunikálnak egymással, a HR-esek nem jelzik az informatikusoknak, hogy kik nem dolgoznak már a szervezetnél, így ennek az információnak a hiányában az informatikusok nem törlik a rendszerből az érintett személyeket. Előfordulhat az is, hogy más munkakörbe kerül egy alkalmazott, ami nem követel meg olyan szintű hozzáférést, mint ami az előző munkakörében volt, de ez az információ sem jut el az informatikusokhoz, így továbbra is azzal a hozzáférési szinttel rendelkezik a munkatárs.

- Kukabúvárkodás *(dumpster diving)* – mindig célszerű átvizsgálni a célszemély szemetesét, hiszen rengeteg értékes információhoz férhetünk így hozzá. Ez mind szervezetek, mind magánszemélyek esetében hasznos lehet.
- Vállszörfölés *(shoulder surfing)* – a támadó úgy helyezkedik el a célszemély körül, hogy kileshesse jelszavát, PIN-kódját.

Az IT-alapú támadások a következők:[49]

- Adathalászat *(phishing)* – a támadásnak több válfaját különböztetjük meg:
  - hamis e-mailek és weboldalak. Ezek a támadások szofisztikáltságuktól függően nagyon eltérők. A támadók olyan weboldalakat hoznak létre, amelyek külsőségeikben hasonlítanak egy létező oldalra (gyakran banki oldalakra), ezek vagy e-mailben, vagy nem túl megbízható weboldalaknál jelennek meg felugró ablakként. Jellemzően internetes szoftverekkel fordítják a szövegeket, és bár az eredmény gyakran magyartalan, mégis sok embert megtévesztenek vele. Pénzügyi tranzakciókat másoló oldalak esetében az adathalász oldalak többnyire nem titkosított kommunikációt biztosító kapcsolaton üzemelnek,[50] amit egy tudatos internetező egyből kiszúr;
  - *vishing* – hangalapú adathalászat, alapvetően valamilyen VoIP-technológiát[51] használó támadás;
  - *smishing* – sms-ben történő támadás;
  - *pharming* – eltérítéses adathalászat, amikor a támadók nem szimplán létrehozzák a másolatát egy weboldalnak, hanem a szolgáltatás domainnevének eltérítésével irányítják a hamisított weboldalra. Ez esetben hiába írja be a felhasználó az URL-t, amit fel szeretne keresni, a támadók ezt az elérési útvonalat támadják meg, a DNS-szerver egy másik IP-címre irányítja a felhasználót. Ha a támadók valósághűen másolják le az eredeti oldalt, ráadásul ügyelnek arra is, hogy az oldal titkosított kapcsolaton keresztül üzemeljen, nagyon nehéz dolga van a felhasználónak, hogy kiszűrje;

[49] Bányász 2018.

[50] A kapcsolat csak http és nem https, ahol az „s" jelzi a titkosított kapcsolatot. Titkosított kapcsolat esetén általában a böngészők címsorában egy zöld lakat is szerepel, de a böngészők gyakran „biztonságos" felirattal is jelzik.

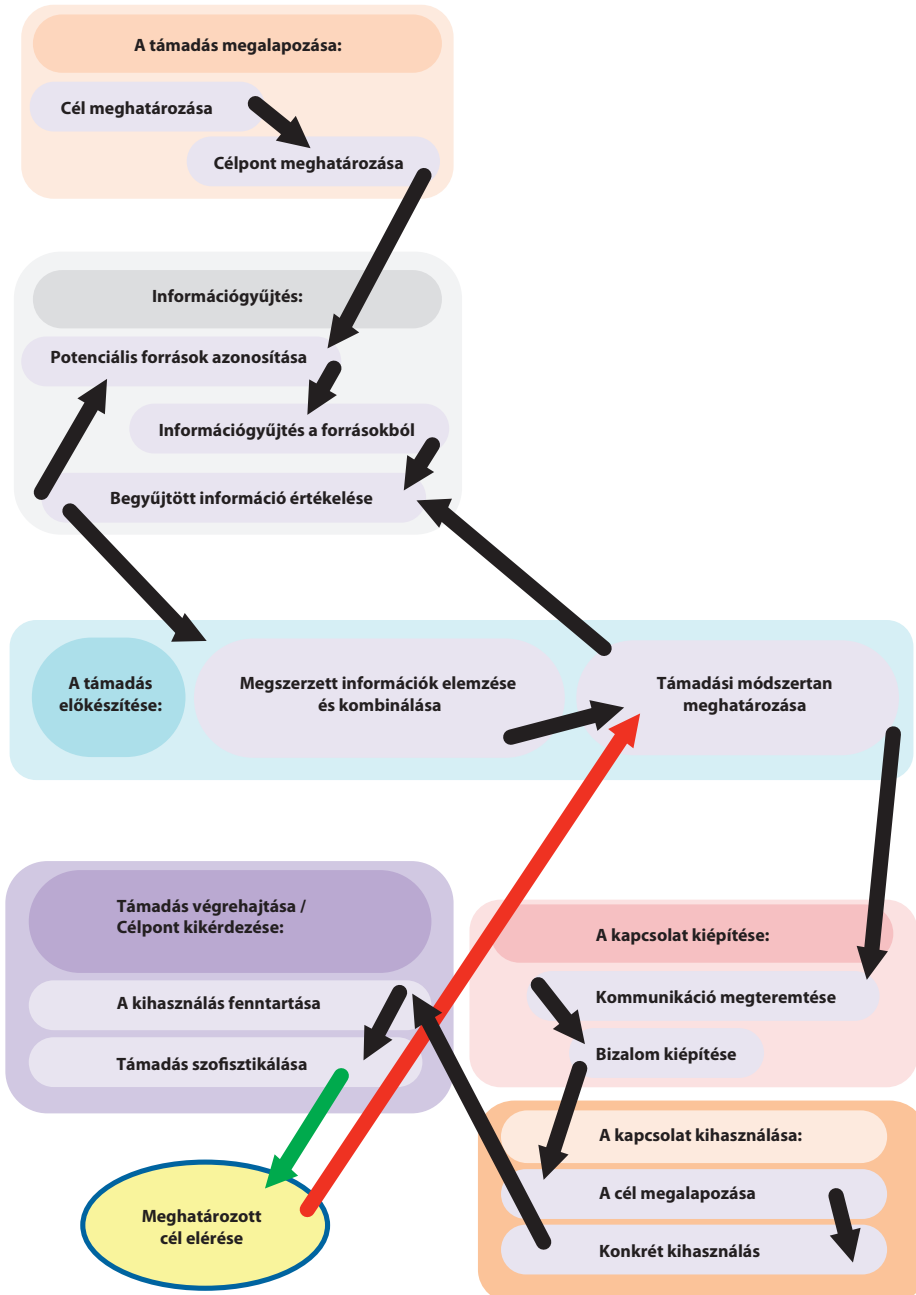
[51] Internetprotokoll feletti hangátvitel, olyan telekommunikációs forma, ahol a kommunikáció nem hagyományos telefonhálózaton keresztül valósul meg, hanem IP-alapú adathálózaton.

  - *whaling* – az adathalászat egy specifikusabb verziója, ebben az esetben vezetők a célpontok, gyakran többlépcsős támadást építenek fel, hogy sikerrel járjanak.
- Kártékony programok – a támadás során olyan rosszindulatú kódok vannak elrejtve az eszközön vagy a fájlon, amelynek segítségével megszerezhetik a célszemély adatait. Ennek módja lehet:
  - frissítés, javítás felajánlása – a támadók sokszor azzal környékezik meg a célszemélyt, hogy egy biztonsági frissítés vagy akár egy vírusirtó telepítése megmenti a káresemény bekövetkezésétől. Az informatikában kevésbé járatos felhasználók egy ilyen üzenettől általában megriadnak, és telepítik a felajánlott programot. Különösen gyakori ez a támadástípus az okoseszközök esetében;
  - billentyűzetnaplózó *(keylogger)* – a támadás lényege, hogy a megfertőzött eszközön a kártevő minden leütött billentyűt megjegyez, és az erről készített naplófájlokat elküldi a támadók részére;
  - trójai programok – a trójai programok a kártevőknek azon változatai, amelyek segítségével a támadók egy hátsó kaput nyitnak az áldozat eszközén, és így szereznek hozzáférést az azon tárolt adatokhoz. Gyakran olyan programokba ágyazzák, amelyek valóban valami hasznos tevékenységre valók;
  - veszélyes csatolmányok – a támadók olyan e-mailt küldenek, amelyben a csatolmány valamilyen kártékony kódot tartalmaz. Ennek fejlettebb módszere, amikor mindezt egy barátunk nevében teszik.
- *Baiting* – a támadás során különböző adathordozókat (DVD, *pendrive,* egyéb eszközök stb.) szórnak szét a támadók, amelyek kártékony kódokat tartalmaznak, majd a számítógéphez való csatlakoztatást követően fertőzik meg az eszközt. Ilyenkor szándékosan figyelemfelkeltő tartalmakat „ígérnek" (például a DVD-k *blockbuster* filmeket, erotikus tartalmakat), így véve rá a célszemélyt, hogy lejátssza azt. Célzott támadás esetén humán alapú technikákkal is vegyíthetik.[52]
- Wi-Fi – a hálózat üzemeltetője képes monitorozni a hálózaton zajló adatforgalmat. Napjainkra talán kezd tudatosulni, hogy egy nyílt Wi-Fi-hálózat milyen kockázatokkal jár, azonban sajnos gyakran nincsenek tisztában azzal,

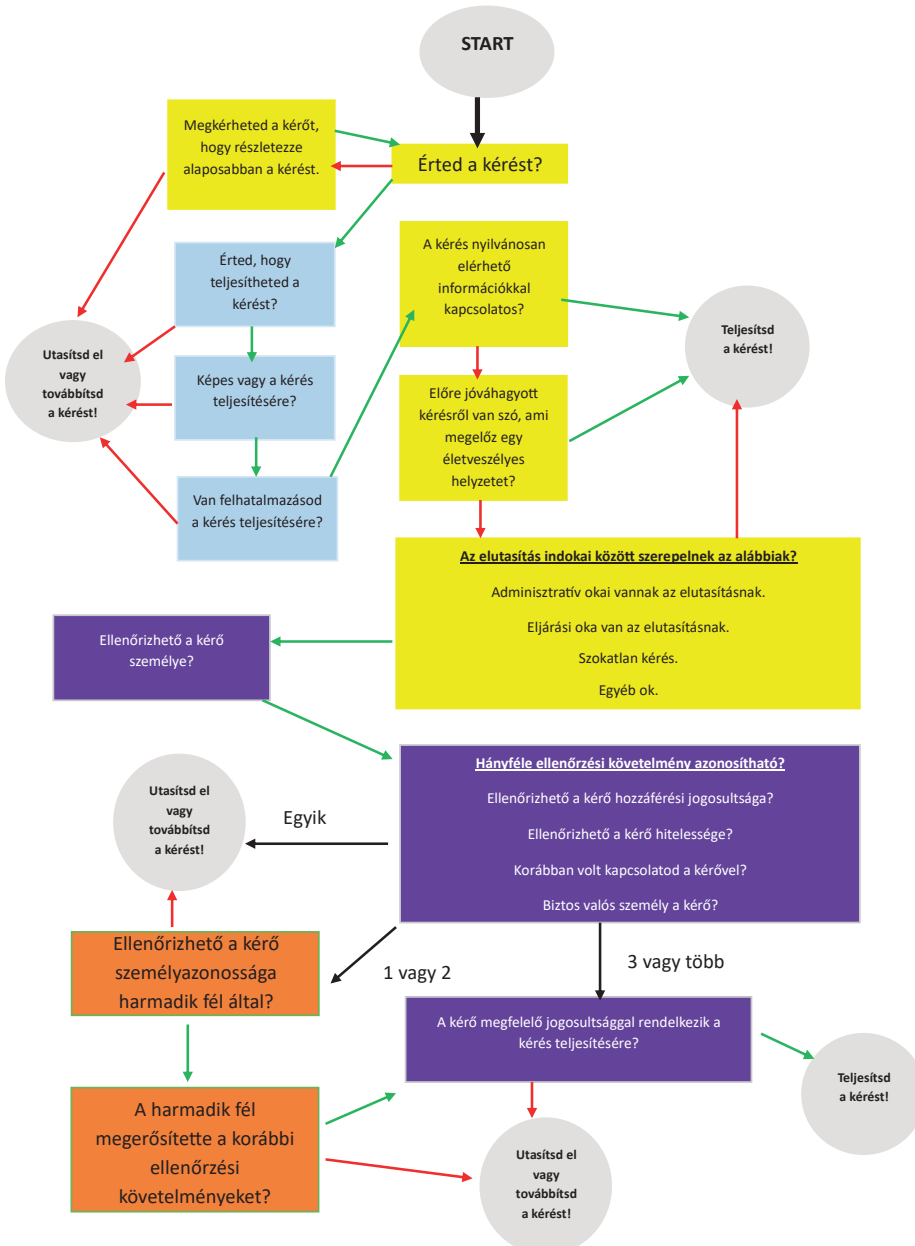
[52] Például kormányablakban a támadó ott felejti a *pendrive*-ot, miközben úgy viselkedik, hogy a következő kapcsolatfelvételnél a célszemély mindenképpen emlékezzen rá. Később kétségbeesetten felhívja, hogy nem találja sehol a *pendrive*-ját, de rajta van a gyerekének a határidős feladata, amit ki akart nyomtatni. Sajnos nem tud bemenni, mert dolgozik, de ha átküldené e-mailben a rajta található fájlt, megmentené a gyereket a bukástól.

hogy a jelszóval védett hálózatok ugyanúgy lehetnek veszélyesek, ugyanúgy megfigyelhetnek azon keresztül a támadók. Igaz ez a biztonságosnak hitt otthoni hálózatunkra is. A felhasználók döntő többsége a *router* jelszavát alapértelmezetten hagyja, ami egy egyszerű Google-kereséssel (ha ismerjük a *router* típusát) kikereshető.

- Alkalmazásengedélyek – a felhasználók nagy része egyáltalán nem olvassa el egy alkalmazás telepítése során, hogy mihez ad engedélyt, éppen ezért rengeteg alkalmazást adathalász célból készítenek el. Ha letöltünk és telepítünk egy alkalmazást, a használatáért cserébe különböző engedélyeket követel meg. Egy alkalmazás letöltése lehet ingyenes, de a használatért cserébe az adatainkat kéri. Alkalmazástól függ, hogy mihez akar hozzáférést szerezni. Ne legyenek illúzióink, ha valami ingyenes, ott minden esetben mi vagyunk a termék. Minden esetben, mielőtt egy alkalmazás telepítése mellett döntenénk, olvassuk el figyelmesen, milyen engedélyeket kér a használatért cserébe, és ha túlzónak ítéljük meg, szakítsuk meg a telepítési folyamatot. Célszerű telepítés előtt ellenőrizni az egyes alkalmazásokat különböző adatbiztonsággal foglalkozó honlapokon. Ilyen weboldal például a Privacy Grade (http://privacygrade. org/home), amely biztonsági kategóriába sorolja az alkalmazásokat annak függvényében, hogy milyen engedélyeket kér a használatáért cserébe, és ez mennyire reális az alkalmazás alapvető funkciójához képest. Egy alkalmazás adatkezelési gyakorlatánál mindig komoly kockázatot jelent, hogy nem tudjuk, a rólunk gyűjtött adatokat ki kezeli, és milyen módon. Nem egy esetben volt már rá precedens, hogy az alkalmazásfejlesztők harmadik félnek adták el az adatokat. Rendkívül jól jövedelmező üzletág az adatok forgalmazása. Egy alkalmazás a legkülönfélébb adatainkhoz kérhet hozzáférést. A legnépszerűbb alkalmazások, mint a Facebook vagy a Google alkalmazásai többek között az alábbi adatokhoz férnek hozzá: személyes adatok (névjegyadatok), tartózkodási hely (hálózat- és GPS-alapú helymeghatározás), hálózati kommunikáció (teljes internethozzáférés), fiókok adatai (üzenetek olvasása), tárhely (lehetőség az USB-tároló tartalmának módosítására vagy törlésére), telefonhívások, hardvervezérlők (fénykép- és videókészítés, hangrögzítés), rendszereszközök (szinkronizálás).




10.9. ábra. *Social engineering keretrendszer*
*Forrás:* Dub Máté szerkesztése Mouton–Leenen–Venter 2016 alapján




10.10. ábra. *A social engineering támadásának észlelési modellje*
*Forrás:* a szerző szerkesztése Mouton–Leenen–Venter 2016 alapján

Mouton és szerzőtársai az idézett tanulmányukban az ontológiai modell mellett egy keretrendszert is megalkottak a *social engineer*ing támadásokkal kapcsolatban (lásd 10.9. ábra), amellyel a fentebb idézett Mitnick-féle modellt komplexebbé bővítették. Ez alapján hat fő eseménysorozatot azonosíthatunk:

- A támadás megalapozása: a támadás céljának és a célpontjának kiválasztása.
- Az információgyűjtés: a célpont különböző forrásból történő felderítése, a sebezhető pontok feltárása, az információk elemzése, értékelése.
- A támadás előkészítése: az értékelt információk alapján a megfelelő támadási közeg, technika meghatározása. Szükség esetén további információgyűjtés.
- A kapcsolat kiépítése: kommunikációs csatorna megnyitása a célponttal, bizalom kiépítése.
- A kapcsolat kihasználása: a meghatározott célok alapján az áldozat kihasználása ennek érdekében.
- Támadás végrehajtása/Célpont kikérdezése: a kapcsolat kihasználásának folytonos fenntartása a támadónak szükséges ideig és mértékig. Amennyiben az elérni kívánt cél ezen a ponton nem megvalósítható, úgy a 3. pontra, a támadás előkészítése tartományon belülre kell visszatérnie a támadónak a helyes támadási módszertan meghatározásához, és aszerint folytatni le a támadást, a keretrendszernek megfelelően. Amennyiben megvalósítható a cél minden kívánt aspektusa, a támadás szofisztikálása, úgy a támadó a célját elérte.

Tegyük fel, hogy a támadó célja egy állami szervezet védett informatikai rendszerébe történő behatolás, hogy az ott tárolt adatokat gazdasági célból értékesítse. Ez esetben az alábbi modell a gyakorlatban a következőképpen nézhet ki:

- A támadás megalapozása: cél a védett informatikai rendszerbe történő behatolás, abból információk megszerzése.
- Az információgyűjtés: a teljesség igénye nélkül a szervezet hivatalos internetes felületeinek (weboldal, hivatalos közösségi oldalak) feltérképezése, telephelyek, munkatársak, szervezeti egységek elérhetőségének azonosítása. A szervezet helyszínének felmérése, milyen szintű a fizikai védelem, mennyire könnyű behatolni az épületbe. A begyűjtött információk alapján a sebezhető pontok azonosítása.
- A támadás előkészítése: amennyiben a támadó úgy ítéli meg, maga is be tud hatolni az épületbe és hozzáférést tud szerezni a hálózathoz, akkor előkészíti az ehhez szükséges eszközöket, például egy megfelelő álcát (pizzafutár stb.). Amennyiben úgy ítéli meg, hogy harmadik felet is igénybe kell vennie a támadás sikeres előkészítéséhez, további információgyűjtés szükséges, amelynek során meghatározza azt a célszemélyt, akin keresztül eléri a célját.

- A kapcsolat kiépítése: amennyiben harmadik felet kell igénybe vennie, a róla gyűjtött információk segítségével „véletlen" események sorozataképpen kiépíti a kapcsolatot a célszeméllyel. Például ugyanazon a szórakozóhelyen többször találkoznak, és a támadó az előzetesen gyűjtött információkat felhasználva kiépíti a bizalmat a célszeméllyel.
- A kapcsolat kihasználása: a bizalom megszerzését követően a támadó ráveszi a célszemélyt valamilyen tevékenység elvégzésére. Fertőzött e-mailt küld például, amelynek megnyitását követően hozzáférést szerez a védett informatikai rendszerhez. A kapcsolat kihasználása megvalósulhat zsarolással, de akár anyagi ellentételezés segítségével is.
- Támadás végrehajtása/Célpont kikérdezése: a megszerezni kívánt információ lementése.

Fontos látni, hogy az egyes támadástípusok kiegészíthetik egymást, illetve egymásra épülhetnek. Hogyan szúrhatunk ki egy *social engineer*ing támadást? A 10.10. ábra ezzel kapcsolatban nyújt hasznos tanácsokat. Az ábrán az egyes megfogalmazott kérdésekre a zöld színnel jelölt nyilak az „igen", míg a pirossal ábrázolt nyilak a „nem" választ jelzik. A modell négy különböző kategóriát jelöl: a kérést, a kérőt, a teljesítőt, illetve harmadik felet. A sárga színnel jelölt részek a kéréssel kapcsolatos szituációkat jelentik. A kékkel jelölt részek közvetlenül a teljesítő személy kéréssel kapcsolatos opcióival foglalkoznak. A lilával ábrázolt kérdések a kérő személyének ellenőrzésére, míg a narancssárga mezők harmadik fél által történő ellenőrzésre vonatkoznak.

## VÉDJÜK MAGUNKAT AZ ONLINE TÉRBEN!

A kibertérben rengeteg olyan információ található meg rólunk, amelyeket felhasználhatnak ellenünk, még akkor is, ha olyan apróságokról van szó, amelyekről nem gondolnánk, hogy valaha kompromittálhatnak. Elég csak arra gondolni, hogy a támadók az internetes felületeken használt becenevünket felhasználva a felépített legendájuk során úgy hivatkozhatnak ránk, mintha régi barátok lennénk, ezzel is igyekezve erősíteni a bizalmi viszonyt, amit kiépíteni szándékoznak.

A bizalmi viszony könnyen kiépíthető, ahogy erre két biztonsági kutató, Aamir Lakhani és Joseph Muniz kísérlete is rávilágított.[53] Ennek során létrehozták egy fiatal, csinos, intelligens, a Massachusetts Institute of Technologyn végzett lány, Emily Williams Facebook- és LinkedIn-profiját. A legenda felépítéséhez használt

[53] Lakhani–Muniz 2021.

képeket egy ismerősük engedélyével posztolták Emily profiljaiban. A legenda szerint Emily éppen munkát keresett, ezért kapcsolatépítésbe kezdett egy meg nem nevezett, amerikai kormányügynökség tagjaival, akik valamilyen kiberbiztonságért felelős szervezetnél dolgoztak. A nem létező Emilyt, aki több dolgozónak lett ismerőse a közösségi oldalakon, ezzel is erősítve az új kapcsolatoknál a bizalmi viszonyt, elég hamar hívták randevúra a beszélgetések során, volt, aki laptopot ajándékozott neki, illetve több állásajánlatot is kapott a szövetségi hatóságnál. Egy közelgő ünnep alkalmából Emily elektronikus képeslapot küldött a partnereinek, amibe egy kártékony kódot rejtettek el a kutatók. Az ügynökség több munkatársa, köztük az informatikai biztonságért felelős vezető is a munkahelyi számítógépén nyitotta meg az elektronikus képeslapot, így a támadók hozzáférhettek a rendszerhez, és bizalmas információkat tölthettek le.

Annak érdekében, hogy csökkenthessük digitális lábnyomunkat és minimalizáljuk a rólunk gyűjthető információkat, ebben az alfejezetben bizonyos gyakorlati tanácsokat fogalmazunk meg.

Fontos, hogy a közösségi oldalakon alkalmazható adatvédelmi beállítások során a legszigorúbbakat alkalmazzuk. Ez nemcsak azért fontos, mert ennek hiányában az egyén profilozását könnyíthetjük meg, de ugyanúgy segíthet kapcsolati háló feltérképezésében, ami értelemszerűen a kollegiális viszonyok kapcsán külön kockázatot jelent,[54] ahogy azt Emily példája is mutatta. A közösségi oldalak rendszeresen változtatják a felhasználási feltételeiket, adatvédelmi tájékoztatójukat. Ennek egyik következménye lehet, hogy korábban alapértelmezett biztonsági beállításokat megváltoztatnak. Ily módon hiába korlátoztuk már például profilunk nyilvános láthatóságát, ezt felülírhatják, és a korábban privát kör számára engedélyezett láthatóságot teljesen nyilvánosra változtatják. Ebből következően szükséges rendszeresen ellenőrizni beállításainkat.

Nyílt forrású információgyűjtéssel nemcsak a felhasználó által megosztott tartalmakat szerezhetjük meg, de Facebookon többek között például az általa használt alkalmazásokat, csoportokhoz való tartozását, oldalak kedvelését, meglátogatott helyeket, más személyek által megosztott fényképekhez, tartalmakhoz való hozzászólásait. Komoly adatvédelmi kockázatot jelent ez utóbbi, hiszen a saját megosztásaink kapcsán dönthetünk a korlátozott nyilvánosságról, de ismerőseink esetében erre nem nyílik módunk. Amennyiben olyan személy megosztásához szólunk hozzá, aki nem korlátozza a nyilvánosságot, úgy a mi hozzászólásaink is nyilvánosak lesznek, ezáltal kereshetők. E tankönyv előző, a közösségi média szervezeti használatával

[54] Heaven 2018: 42–43.

kapcsolatáról szóló IX. fejezetében már volt szó[55] és a speciális szabályairól[56] az egyes oldalakon tanúsítható magatartásaival kapcsolatban. Mivel olyan tartalmat egyébként sem lehet megosztani nyilvánosság előtt, amelyet a jogalkotó a Hjt.-ben és a Hszt.-ben is külön nevesített, információbiztonsági szempontból érdemes a szabályzóban felhívni a figyelmet arra, hogy a magánélettel összefüggésben megosztott tartalmat, amely egyébként csak egy szűkebb nyilvánosságra tartozik, csupán erre a körre szűkített adatvédelmi beállítás mellett érdemes megosztani. Más személyek profilja esetében a láthatóság ellenőrzésére lehetőségünk van; amennyiben a fenti kitétel nem valósul meg, úgy nem javasolt a tervezett tartalom megosztása.

Az adatgyűjtésekkel szembeni védekezés egyik legegyszerűbb módjának a pszeudonimizálást tekinthetjük. A folyamat lényege, hogy megfosztjuk az adatokat az egyértelmű személyes adatoktól (például felhasználónév, név), és azokat pszeudonim azonosítókra cseréljük, például véletlenszerűen generált számokra. Ezáltal az egyes rekordok érintettel való kapcsolatának visszaállítása bonyolultabb tevékenységet jelent. Ezzel kapcsolatban a később részletezendő Általános Adatvédelmi Rendelet konkrét rendelkezést fogalmaz meg. A pszeudonomizáláshoz hasonló folyamat az anonimizálás, azonban ez tágabb tevékenységi kört jelent. Bár célja azonos a pszeudonomizálással, anonimizálás során további követelményként fogalmazódik meg, hogy az anonimizálás során létrejövő rekordokat ne lehessen az adatot szolgáltató eredeti személyhez kötni.

Az okosmobileszközök, internetes oldalak, közösségi oldalak használata számtalan olyan lehetőséget biztosít, amelyekkel valós időben, akár tömegesen figyelhetők meg a személyek. Fontos rögzíteni, attól, hogy egy beszélgetés privát módon zajlik, nincs garancia arra, hogy az érintetteken kívül harmadik fél nem fér hozzá annak tartalmához. Ez egyben azt jelenti, hogy ezeken a felületeken célszerű kerülni az intim témákat, hiszen azok harmadik fél kezében akár befolyásolásra, akár zsarolásra is használhatók. Szükséges az okosmobileszköz használatára vonatkozó szabályok kidolgozása is, amelyek vonatkoznak az alkalmazások használatára (figyelembe véve az alkalmazásengedélyeket), a wifihálózatok biztonságára, a megfelelő védelmi eljárások használatára (az operációs rendszer és az alkalmazások rendszeres frissítése, lehetőség szerint VPN, titkosítást alkalmazó kommunikációs alkalmazások használata stb.).

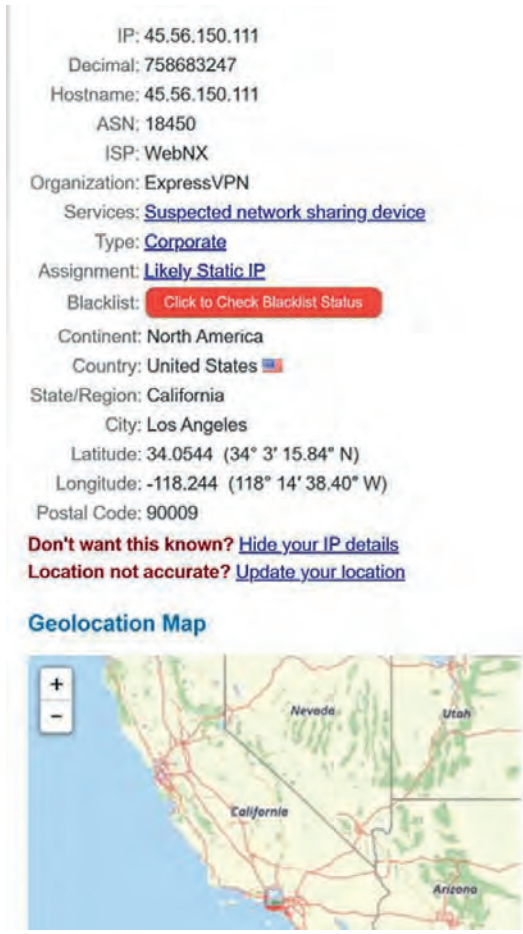
Mi is a VPN? A kifejezés a *virtual private network* kifejezésből származik, és virtuális magánhálózatot értünk alatta. Maga a VPN eredetileg arra szolgált, hogy egy szervezet különböző telephelyei között biztonságos hálózatot építsenek ki, amelynek

[55] 2012. évi CCV. törvény a honvédek jogállásáról.

[56] 2015. évi XLII. törvény a rendvédelmi feladatokat ellátó szervek hivatásos állományának szolgálati jogviszonyáról.

keretében a más telephelyen dolgozók is hozzáférhetnek a szervezet informatikai rendszereihez. A Nemzeti Közszolgálati Egyetem VPN-je például a hallgatók számára is lehetővé teszi, hogy otthonról, saját eszközről hozzáférjenek az NKE által előfizetett tudományos adatbázisokhoz, és azokból díjmentesen tölthessenek le tudományos szakirodalmat. Az évek során azonban a VPN-ek piaca jelentős fejlődésen ment keresztül. A különböző hirdetések napjainkra „mindenre is" csodaszerként ajánlják a VPN-előfizetéseket, amelyek megvédenek a hackerektől, a vírusoktól, a hatóságok zaklatásától, a nemzetbiztonsági szolgálatok megfigyelésétől, az ígéretek szerint teljesen nyomtalanok lehetünk az interneten, illetve használatával számos régiós megkötést cselezhetünk ki, ami például a multimédiás tartalmakhoz való hozzáférésben fontos szempont lehet.[57] Mindebből könnyen kitalálhatjuk, hogy az ilyen csodaeszközök csak a mesékben léteznek. A VPN lehetővé teszi a felhasználók számára, hogy egy megosztott vagy nyilvános hálózaton keresztül úgy küldjenek és fogadjanak adatokat, mintha eszközeik közvetlenül kapcsolódnának a helyi hálózathoz, ily módon a saját eszközünk és a VPN-szolgáltató szervere között egy titkosított kapcsolatot építünk ki, és a publikus internetre a szolgáltató szerverének nevében lépünk ki. Ez a gyakorlatban azt jelenti, hogy a saját internetszolgáltatónk elvileg nem tudja összekötni az internetes tevékenységünket velünk, mert nem a saját IP-címünket használjuk, hanem egy, a szolgáltató által biztosított szerver oszt ki nekünk IP-címet. Az egyes szolgáltatók számos országból kínálnak szervereket, így ha egy amerikai szerverhez csatlakozunk, akkor a szolgáltató, illetve az általunk felkeresett weboldalak oly módon fognak azonosítani, mintha ott lennénk.

[57] Számos streamingszolgáltató az általa sugárzott multimédiás tartalom esetében régiós korlátozásokat alkalmaz, ennek következében a magyarországi előfizető jelentősen kevesebb tartalomhoz fér hozzá, mint egy amerikai.




10.11. ábra. *Példa egy VPN-szolgáltatást használó felhasználó geolokációjára*
*Forrás:* a szerző szerkesztése

A 10.11. ábrán látható, hogy az általam használt VPN-szolgáltatásban amerikai szerverre csatlakoztam, így elrejtve a valódi tartózkodási helyem, a magyar IP-címem. Fontos látni azonban, hogy a VPN nem feltétlenül anonimizál bennünket, hiszen a szolgáltatónk továbbra is látni fogja a valódi IP-címünket, és rendelkezhet olyan pénzügyi információkkal, amelyeket közvetlenül vissza lehet kapcsolni hozzánk.[58] Az is fontos szempont lehet a szolgáltató kiválasztásakor, hogy melyik országban

[58] Például ha csak bankkártyával fizethetünk elő a szolgáltatásra, akkor az ebből származó adatokat hozzánk lehet kötni. Egyes VPN-szolgáltatók az anonimizálás érdekében lehetővé teszik, hogy a szolgáltatásukért kripotovalutával fizessünk, ezáltal rejtve a pénzügyi információinkat.

üzemel, ugyanis ennek függvényében jogszabályi kötelezettségi alapon az internetes tevékenységünket naplózhatják, annak ellenére, hogy ezt tagadják, és az érintett állam nemzetbiztonsági szolgálatainak ezeket az adatokat kiadhatják. Ily módon a VPN használata erősen a bizalmi kategória, meg kell bíznunk egy szolgáltatóban,[59] hinnünk kell abban, hogy valóban úgy teljesíti a szerződésben vállalt tevékenységeket, ahogy az abban szerepel. Amennyiben ez történik, akkor az internetes tevékenységünk olyan lesz, mint egy tű abban a bizonyos nagy szénakazalban. Még így is megtalálhatják, de jelentősen csökken az esélye. Mindenesetre azt leszögezhetjük, a VPN sem véd meg bennünket a kártékony kódoktól, a hackerektől. Az anonimizálás bizonyos szintjét teszi lehetővé, amellett, hogy hozzáférhetünk a streamingszolgáltatónál bizonyos régiós tartalmakhoz.

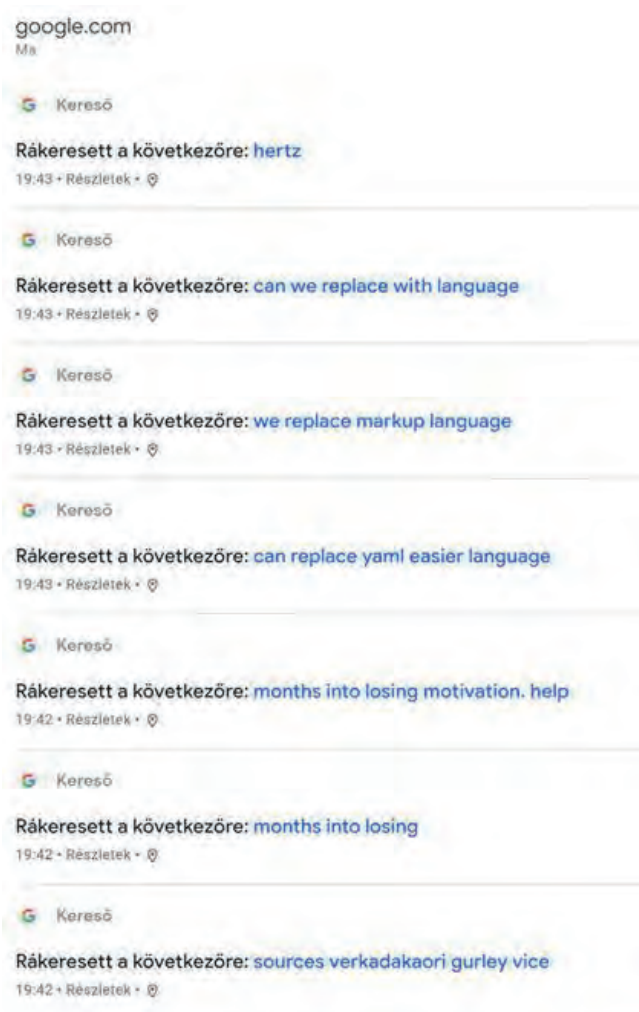
Nyilvánvalóan a fenti védelmi megoldásokat nem csupán okosmobileszközök esetében kell alkalmazni, hanem minden olyan informatikai eszközön, amelyet az állomány tagjai használnak szabadidejükben. Ebben a *privacy by design* elvének gyakorlati megvalósulását elősegítő, a privát szférát erősítő technológiák[60] (PET-ek) jó kiindulási alapot jelentenek. Nézzünk pár ilyen PET-et!

A Firefox böngészőhöz készült TrackMeNot[61] nevet viselő böngészőkiegészítő egy olyan anonimizáló alkalmazás, amely meghatározott időnként véletlenszerűen indít kereséseket a megadott keresőmotorokon. Ennek a lényege, hogy az általunk indított keresésekből pontosan meg lehet határozni a profilunkat. Azonban, ha ezt felhígítjuk nagyszámú, véletlenszerűen indított kereséssel, ebben elrejthetjük a valódi kereséseinket, ami nehezíti a profilozásunkat. Személyes példán bemutatva: korábban átlagosan naponta 20–30 keresést indítottam a Google keresőjében, ez a bővítmény telepítését követően napi 750–800 keresésre növekedett (lásd 10.12. ábra).

[59] A bizalom egyik nagyon fontos sarokköve, hogy az ingyenes VPN-szolgáltatók vélhetően nem nyújtanak valódi szolgáltatást, mi több, előfordulhat, hogy az ingyenesség valójában egy trükk, amivel kártékony kódot telepítenek eszközünkre, vagy a valóságban adathalászatra használják az alkalmazást.

[60] Kiss 2017.

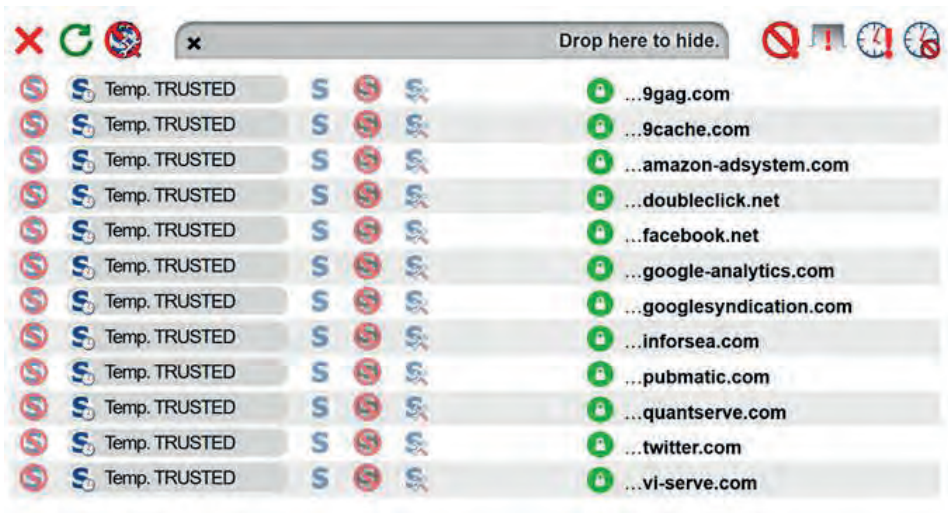
[61] Magyarul: Ne kövess!




10.12. ábra. *Példa a keresés anonimizálására*
*Forrás:* a szerző szerkesztése

Az anonimizálás hasznos eszközei a reklámblokkoló alkalmazások (például Adblock Plus, uBlock Origin), ugyanis a weboldalakon megjelenített hirdetések gyakran olyan nyomkövetőket is alkalmaznak, amelyek egyrészt lehetővé teszik a felhasználók beazonosítását, másrészt bizonyos *script*ek futtatását is tiltják. Script alatt olyan rövid programokat értünk, amelyek jellemzően valamilyen részfeladat automatizálására szolgálnak. Például amikor a Facebook létrehozta a weboldalakra integrálható kis

ikont, amelynek segítségével a felhasználók azonnal megoszthatták a hírfolyamukban az általuk érdekesnek talált tartalmat, azt is egy ilyen kis *script* segítségével oldották meg. Csakhogy ezzel a *script*tel egyúttal nyomon követték, a felhasználó melyik oldalról érkezett ide, mennyi időt tölt el ott, hová megy tovább stb. Ennek a *script*nek a segítségével gyűjtöttek adatokat azokról az emberekről is, akik soha nem regisztráltak a Facebookra, de mégis egy úgynevezett árnyékprofilt kötöttek hozzájuk.[62] A nyomkövetésen túl komolyabb kockázatot is rejthetnek az egyes oldalak által használt *script*ek. Több torrentoldal és nem hivatalos online streamingoldal esetében derült ki, hogy olyan *script*eket futtatnak az oldalon, amelyek átvették az irányítást a látogató eszközén, és annak erőforrását kriptovaluta-bányászásra fordították. Az említett reklámblokkolók ezt a folyamatot megakadályozták. Léteznek természetesen egyéb kiegészítők, amelyek segítségével tilthatjuk a *script*ek automatikus futtatását, és egyenként engedélyezhetjük, mi fusson az oldalon, lásd például a NoScript nevű PET-et (10.13. ábra). Nyilvánvalóan az egyes oldalakon a kezelt *script*ek nagyban ronthatják a felhasználói élményt, hiszen a különböző beágyazott tartalmakat engedély hiányában nem tölti be az oldal (például beágyazott YouTube-videó, Instagram-kép, X-bejegyzés stb.).




10.13. ábra. *Példa scriptkezelő alkalmazásra*
*Forrás:* a szerző szerkesztése

62 Mark Zuckerberg a szenátusi meghallgatáson ezt azzal védte, hogy csupán meg akarták könnyíteni az emberek dolgát, ha mégis regisztrálnak Facebookra, akkor azonnal élvezhessék az oldal kényelmi funkcióit, amelyek a személyre szabott élményből következnek.

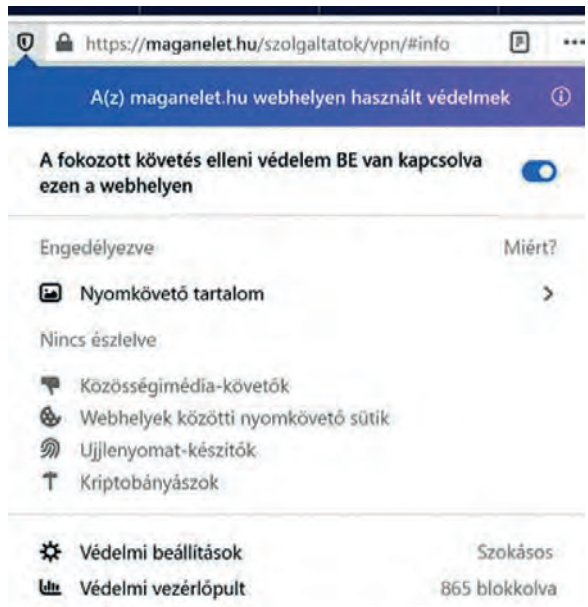
A weboldalak nyomkövetését segítik az úgynevezett sütik, eredeti terminológia szerint *cookie*-k. A nyomon követés azonban oldalakon keresztül is megvalósulhat, például a Google azt követően is követi a felhasználót sütik segítségével, hogy elnavigált az Google oldaláról.[63] Mivel a sütik lehetővé teszik a természetes személyek azonosítását, így a GDPR rendelkezései alapján a sütik által gyűjtött adatok kezeléséről egyértelmű és pontos leírást kell adni az adatvédelmi tájékoztatóban, továbbá az érintettnek minden kétséget kizáróan jóvá kell hagyni a sütik használatát. Azonban annak megállapítása is nyomkövetés, hogy az érintett járt-e korábban az oldalon. Erre két lehetőség van, első esetben az oldalra történt regisztráció során a felhasználó engedélyezi a sütiket, ez esetben a weboldal következő meglátogatásakor nem jelenik meg újból az engedélyezésre vonatkozó tájékoztató. Regisztráció híján, ha jóváhagyja a sütik kezelését, következő alkalommal már nem jelenik meg a tájékoztató. Kivételt képez ez alól, ha a felhasználó törli a korábban engedélyezett sütiket. Ezzel kapcsolatban a GDPR világosan fogalmaz, az érintett bármikor visszavonhatja a korábban engedélyezett sütiket. Erre egyébként a böngészők egyszerű lehetőséget biztosítanak, de ezenkívül számos olyan PET található böngészőkiegészítőként, amelyek automatikusan eltávolítják az oldal vagy a böngésző bezárását követően a nyomkövetőket (például ClearURL, Cookie AutoDelete).

Rendkívül fontos, hogy bizonyos internetes tevékenységeket megfelelő titkosítással működő oldalon végezzünk, ugyanis ennek hiányában mások is láthatják, mit csinálunk. Amikor például online fizetünk, és ezt nem titkosított csatornán keresztül tesszük, a bankkártyánk adatait, amelyeket a fizetéshez meg kell adnunk, harmadik fél is láthatja, akik aztán ezeket felhasználva megkárosíthatnak. Annak eldöntése, hogy titkosított adatforgalom van-e az általunk használt oldalon, nagyon könnyű, hiszen az URL-ből kiolvasható: a http:// formátumba beágyazódik a titkosított adatforgalmat kezelő oldalaknál egy „s" betű, így https:// formátumot kell látnunk. A legtöbb böngésző egyébként a címsorban az URL előtt, ha biztosítja a https://-t, egy (zöld) lakatot jelenít meg (lásd 10.14. ábra). Ha az egerünket a lakatra visszük, akkor megjeleníti a titkosítást auditáló szervezetet is. A legtöbb esetben a forgalom nagy része már titkosítva van, a 3000 legnépszerűbb webhely több mint 98%-a biztosít https-t, azaz a nem DNS-forgalom biztonságos, függetlenül a VPN-től. Hihetetlenül ritka, hogy a személyes adatokat kezelő weboldalak napjainkban ne támogassák a https-t, különösen olyan szolgáltatásokkal, mint a Let's Encrypt, amely ingyenes https-tanúsítványokat kínál minden weboldal-üzemeltető számára. A https:// titkosítás használatához is telepíthetünk különböző PET-eket, mint például a HTTPS Everywhere-t.

[63] Ezt nevezik *cross site tracking*nek.


10.14. ábra. *Példa a biztonságos kapcsolatra*
*Forrás:* a szerző szerkesztése

A különböző böngészők is folyamatosan fejlesztik a magánszféra védelmével kapcsolatos technológiai eszköztárukat. A Firefox például támogatja a fokozott követés elleni védelmet (lásd 10.15. ábra), és tájékoztat a meglátogatott oldalak nyomkövetéssel kapcsolatos aspektusairól. Fontos látni, hogy a Chrome böngésző használatát nem igazán szokták javasolni a Google adatgyűjtési gyakorlata miatt. A Firefox mellett a TOR böngészőt javasolják általában. A TOR a *the onion router* rövidítése, amely az adatvédelem megóvására használatos többrétegű titkosításra utal. A TOR alapvető funkciója, hogy elrejti az internetes lábnyomainkat, lehetővé téve, hogy anonimán böngésszünk és tölthessünk le tartalmakat. A böngészőt eredetileg az amerikai haditengerészet fejlesztette ki, hogy megvédelmezze az USA kormányzati kommunikációját az ügynöki tevékenységek közben. Jelenleg nonprofit szervezetként promotálja az online adatvédelmet. A TOR ugyanúgy működik, mint a Firefox vagy egyéb böngésző, a különbség, hogy titkosított csomagokba teszi az adatainkat, mielőtt azok a hálózatra jutnának. A TOR ezután eltávolítja a csomag azon részét, amely olyan információkat tartalmaz, mint a forrás, méret, célhely és időzítés – amelyek mindegyikével új információk derülhetnek ki a küldőről (akár rólunk is). A következőkben titkosítja a csomagolt információk maradékát, mielőtt végül elküldené a titkosított adatokat számos szerveren, relén keresztül, így nem lehet nyomon követni a folyamatot. Minden egyes relé felold, majd újratitkosít éppen elegendő mennyiségű adatot ahhoz, hogy tudjuk, honnan jött és legközelebb hová megy, de ezenfelül követhetetlen az információ útja. A TOR által alkalmazott erős titkosításnak a következménye, hogy jelentősen lassítja a le- és feltöltési sebességet. A TOR az általa használt titkosítás miatt fontos eszköz egyébként a politikai aktivisták, újságírók kezében, de egyúttal „belépőkapu" is a korábban említett *darknet*be.




10.15. ábra. *Fokozott követés elleni védelem a Firefox böngészőben*
*Forrás:* a szerző szerkesztése

A felsoroltokon felül számos, a privát szférát erősítő technológia létezik, amelyek között a 10.15. ábrán látható www.maganelet.hu segít eligazodni. Az oldalon emellett rengeteg hasznos tanácsot találunk digitális ujjlenyomatunk csökkentésére. Idézve az oldalról pár beállítási javaslatot:

„Ezek az adatvédelmet fokozó beállítások a Firefox böngésző about:config beállítás menedzsment részében találhatók meg. Megmutatjuk, hogy hogyan tudod javítani a böngésződ adatvédelmét.

Előkészület:

Írja be a »about:config« parancsot a Firefox címsorába, és nyomd meg az Enter billentyűt.
Nyomd meg az »Elfogadja a kockázatot és folytassa« vagy az »Elfogadom a kockázatot« gombot.
Kövesd az alábbi utasításokat…

Beállítások:

privacy.firstparty.isolate = true
A TOR Uplift projekt erőfeszítésének eredményeként ez a beállítás az összes böngésző-azonosító forrást (például sütiket) elkülöníti az első fél domainjéről, azzal a céllal, hogy ezáltal megakadályozzuk a követést a különböző domainek között. (Ne alkalmazd ezt a beállítást, ha telepítetted a Firefox »Cookie Auto-Delete« kiegészítőt.)

privacy.resistFingerprinting = true
A TOR Uplift projekt erőfeszítésének eredményeként ez a beállítás lehetővé teszi, hogy a Firefox ellenállóbb legyen a böngésző ujjlenyomata ellen.

privacy.trackingprotection.fingerprinting.enabled = true
Ujjlenyomat küldés blokkolása

privacy.trackingprotection.cryptomining.enabled = true
Kriptobányász *script*ek blokkolása

privacy.trackingprotection.enabled = true
Ez a Mozilla új beépített nyomkövető elleni védelme.

browser.send_pings = false
Ezzel a beállítással megtiltható a webhelyek számára, hogy a látogatók kattintásait nyomon követhessék.

browser.urlbar.speculativeConnect.enabled = false
Az automatikus URL kiegészítés előtöltésének letiltása. A Firefox automatikusan kitölti az URL-t, amikor a felhasználó beírja a címsorba a címet, ami aggodalomra ad okot.

dom.event.clipboardevents.enabled = false
Ezzel a beállítással letilthatod, hogy a webhelyek értesítést kapjanak arról, ha valamit másolsz, beillesztesz vagy kivágsz onnan.

media.eme.enabled = false

Ez a beállítás letiltja a DRM-vezérelt HTML5 tartalom lejátszását, amely engedélyezése esetén automatikusan letölti a Google Inc. által biztosított Widevine tartalom visszafejtési modult.

A DRM-vezérelt tartalom, ami Adobe Flash vagy Microsoft Silverlight NPAPI beépülő modulokat igényel, továbbra is lejátszódik, ha a Firefox telepítve van és engedélyezve van.

media.gmp-widevinecdm.enabled = false

Letiltja a Google Inc. által biztosított Widevine tartalom visszafejtési modult, amelyet DRM-vezérelt HTML5 tartalom lejátszására használnak.

media.navigator.enabled = false

Ezzel a beállítással letilthatjuk, hogy a webhelyek nyomon követhessék a számítógépünk mikrofonjának és webkamerájának állapotát.

network.cookie.cookieBehavior = 1

Sütik kikapcsolása

- 0 = Alapértelmezés szerint fogadjon el minden sütit
- 1 = Csak az eredeti webhelyről fogadjon el (blokkolja a harmadik féltől származó sütiket)
- 2 = Alapértelmezés szerint tiltsa le az összes sütit

webgl.disabled = true

Ezzel a beállítással letilthatjuk a WebGL-t, amely egy potenciális biztonsági kockázat.

beacon.enabled = false

Ezzel a beállítással letilthatjuk a böngésző által a webhelyek felé küldött további információkat."[64]

[64] Privacy Guides [é. n.].

## ÖSSZEFOGLALÁS

A fejezetben igyekeztünk olyan gyakorlati tanácsokat megfogalmazni, amelyek segítségével nemcsak biztonságtudatosabban internetezhet az Olvasó, de csökkentheti annak a kockázatát, hogy támadás áldozatává váljon. Ennek érdekében szükséges volt azoknak a fő fogalmaknak az ismertetése, amelyek segítenek komplexen értelmezni a kibertérből leselkedő fenyegetéseket. Remélhetőleg a fejezet eloszlatta azokat a gyakori tévhiteket, amelyek az emberekben a kiberbiztonsággal kapcsolatban élnek. Az egyik ilyen tévhit, hogy „nem vagyok érdekes", „miért lennék én célpont?". Ahogy Kim Philby és társainak példája igazolta, sosem lehet tudni, kiből mi lesz az életében, mikor kerül olyan pozícióba, amikor valakinek értékes lehet. Egy védett informatikai rendszerhez való hozzáférésben nem csupán a rendszergazda, de akár egy takarító, biztonsági őr is segíthet, ha megtévesztik, megzsarolják. Mindenki célpont lehet, ha másért nem, hogy rajta keresztül jussanak el egy harmadik személyhez. Szintén káros az a tévhit, hogy az internetes oldalak használata ingyenes. Meg kell érteni mindenkinek, hogy soha semmi nem ingyenes. Ha egy szolgáltatáshoz ingyen férünk hozzá, ott minden bizonnyal mi, az adataink vagyunk az áru. Őszintén reméljük, hogy a tisztelt Olvasó hasznosnak találta az itt leírtakat, és megfogadja a fejezetben megfogalmazott ajánlásokat. Biztonságos internetezést!

## FOGALMAK

- adatvédelem
- anonimizálás
- darknet
- dolgok internete
- hacktivizmus
- incidensmenedzsment
- infokommunikációs technológiák
- információbiztonság
- kiberbiztonság
- kiberbűnözés
- kiberfenyegetettség
- kiberhadviselés
- kiberkémkedés
- kibertér
- kiberterrorizmus
- kockázat
- kockázatelemzés
- közösségi média
- *malware*
- nyílt forrású információgyűjtés
- privát szférát erősítő technológiák
- *social engineer*ing
- titkosítás
- virtuális magánhálózat

## ÁTTEKINTŐ KÉRDÉSEK

1. Véleménye szerint napjainkban mi a legnagyobb kiberbiztonsági kockázat az állami szervezeteket illetően?
2. Milyen humán alapú *social engineer*ing támadásokat ismer? Ismertesse az egyes támadástípusokat röviden!
3. Milyen IT-alapú *social engineer*ing támadásokat ismer? Ismertesse az egyes támadástípusokat röviden!
4. Milyen motivációk azonosíthatók a kibertámadások mögött? Jellemezze az egyes kategóriákat!
5. Milyen jellegű oktatást tartana fontosnak az adat- és információbiztonsági tudatosság növelésére az állami szervezetek esetében?
6. Milyen jellegű támadások azonosíthatók a kiberbűnözés kapcsán? Ismertesse az egyes támadástípusokat röviden!
7. Milyen védelmi megoldásokat javasolna a szüleinek, hogy nagyobb biztonságban internetezhessenek?
8. Véleménye szerint mi a legnagyobb veszély, ami Önre leselkedik az interneten?

## FELHASZNÁLT IRODALOM

1139/2013. (III. 21.) Korm. határozat Magyarország Nemzeti Kiberbiztonsági Stratégiájáról. Online: https://njt.jog.gov.hu/jogszabaly/2013-1139-30-22.1

1089/2025. (III. 31.) Korm. határozat Magyarország Kiberbiztonsági Stratégiájáról. Online: https://njt.jog.gov.hu/jogszabaly/2025-1089-30-22

2012. évi CCV. törvény a honvédek jogállásáról. Online: https://njt.jog.gov.hu/jogszabaly/2012-205-00-00

2013. évi L. törvény az állami és önkormányzati szervek elektronikus információbiztonságáról. Online: https://njt.jog.gov.hu/jogszabaly/2013-50-00-00

2015. évi XLII. törvény a rendvédelmi feladatokat ellátó szervek hivatásos állományának szolgálati jogviszonyáról. Online: https://njt.jog.gov.hu/jogszabaly/2015-42-00-00

2024. évi LXIX. törvény Magyarország kiberbiztonságáról. Online: https://njt.jog.gov.hu/jogszabaly/2024-69-00-00

Bányász Péter (2018): Social engineering és közösségi média. *Nemzetbiztonsági Szemle,* 5(1), 59–77.

Bányász Péter (2019): *A közösségi média lehetőségei és kihívásai a védelmi szférában.* PhD-disszertáció. Nemzeti Közszolgálati Egyetem Katonai Műszaki Doktori Iskola.

Bányász Péter – Bóta Bettina – Csaba Zágon (2019): A *social engineer*ing jelentette veszélyek napjainkban. In Zsámbokiné Ficskovszky Ágnes (szerk.): *Biztonság, szolgáltatás, fejlesztés, avagy új irányok a bevételi hatóságok működésében.* Budapest: Magyar Rendészettudományi Társaság Vám- és Pénzügyőri Tagozat, 12–37. Online: https://doi.org/10.37372/mrttvpt.2019.1.1

BERKI Gábor (2013): A kibertéri konfliktusok változásai. *Hadmérnök,* 8(1), 173–185. Online: http://hadmernok.hu/2013_1_berkig.pdf

BLUMLER, Jay G. – KATZ, Elihu (1974): *The Uses of Mass Communications. Current Perspectives on Gratifications Research. Sage Annual Reviews of Communication Research Volume III.* Beverly Hills, California: Sage Publications.

BUZAN, Barry – WÆVER, Ole – DE WILDE, Jaap (1997): *Security. A New Framework for Analysis.* Boulder, Colorado: Lynne Rienner Publishers.

CARTWRIGHT, Madison (2018): Who Cares About Reddit? Historical Institutionalism and the Fight Against the Stop Online Piracy Act and the PROTECT Intellectual Property Act. *Policy Studies,* 39(4), 383–401. Online: https://doi.org/10.1080/01442872.2018.1472757

DAVIS, Fred D. (1989): Perceived Usefulness, Perceived Ease of Use, and User Acceptance of Information Technology. *MIS Quarterly,* 13(3), 319–340. Online: https://doi.org/10.2307/249008

FARKAS Zoltán (2013): A társadalmi tőke fogalma és típusai. *Szellem és Tudomány,* 4(2), 106–133.

HAIG Zsolt (2015): *Információ – társadalom – biztonság*. Budapest: NKE.

HEAVEN, Douglas (2018): The Internet Knows You All Too Well. *New Scientist,* 237(3168), 42–43. Online: https://doi.org/10.1016/S0262-4079(18)30444-5

HEFFERNAN, Michael (2015): The Interrogation of Sándor Radó: Geography, Communism and Espionage between World War Two and the Cold War. *Journal of Historical Geography,* 47, 74–88. Online: https://doi.org/10.1016/j.jhg.2014.12.004

JAKOBI Ákos (2002): A virtuális világ terei. Reflexiók Mészáros Rezső A kibertér társadalomföldrajzi megközelítése című tanulmányához. *Magyar Tudomány,* 47(11) 1482–1491.

KAPLAN, Andreas M. – HAENLEIN, Michael (2010): Users of the World, Unite! The Challenges and Opportunities of Social Media. *Business Horizons,* 53(1), 59–68. Online: https://doi.org/10.1016/j.bushor.2009.09.003

KISS Attila (2017): A biztonsági események és az adatvédelmi incidensek kezelésére vonatkozó előírások hazánk és az EU jogában. In BERZSENYI Dániel et. al.: *Incidensmenedzsment. Éves továbbképzés az elektronikus információs rendszer biztonságáért felelős személy számára.* Budapest: Dialóg Campus.

KRASZNAY Csaba (2012): A polgárok védelme egy kiberkonfliktusban. *Hadmérnök,* 7(4), 142–151.

LAKHANI, Aamir – MUNIZ, Joseph (2013): *Social Media Deception.* RSA Conference Europe, 2013. október 29. Online: https://itcafe.hu/dl/cnt/2013-11/102992/hum-w01-social-media-deception.pdf

LU, Tan – WANG, Neng (2010): Future Internet: The Internet of Things. In *2010 3rd International Conference on Advanced Computer Theory and Engineering(ICACTE).* 5:V5-376-V5-380. Online: https://doi.org/10.1109/ICACTE.2010.5579543

MÉSZÁROS Rezső (2001): A kibertér társadalomföldrajzi megközelítése. *Magyar Tudomány,* 46(7), 769–779.

MITNICK, Kevin D. – SIMON, William L. (2003a): *A legendás hacker. A megtévesztés művészete.* Ford. Lénárt Szabolcs. Budapest: Perfact-Pro Kft.

MITNICK, Kevin D. – SIMON, William L. (2003b): *The Art of Deception. Controlling the Human Element of Security.* Hoboken, New Jersey: Wiley.

MOUTON, Francois – LEENEN, Louise – VENTER, H. S. (2016): Social Engineering Attack Examples, Templates and Scenarios. *Computers & Security,* 59, 186–209. Online: https://doi.org/10.1016/j.cose.2016.03.004

Muha Lajos – Krasznay Csaba (2018): *Az elektronikus információs rendszerek biztonságának menedzselése.* Budapest: NKE.

Munk Veronika (2020): Sztárság, elméletben. *Médiakutató*, 2020. szeptember 27. Online: https://mediakutato.hu/cikk/2009_01_tavasz/01_sztarsag_elmeletben

Ngai, Eric W. T. et al. (2015): Social Media Models, Technologies, and Applications. An Academic Review and Case Study. *Industrial Management & Data Systems,* 115(5), 769–802. Online: https://doi.org/10.1108/IMDS-03-2015-0075

Oxford Dictionary [é. n.]: Social Media. Online: www.oxfordlearnersdictionaries.com/definition/english/social-media

Pléh Csaba – Boros Ottilia (2010): *Pszichológiai lexikon.* Akadémiai lexikonok A–Z. Budapest: Akadémiai.

Privacy Guides [é. n.]: The Collaborative Privacy Advocacy Community. Online: https://www.privacyguides.org/en/

Rajnai Zoltán – Fregan Beatrix (2017): Új alapokon a magyarországi kibervédelmi stratégia. *Műszaki Tudományos Közlemények,* 7. 351–354. Online: https://doi.org/10.33895/mtk-2017.07.80

Rolington, Alfred (2015): *Hírszerzés a 21. században. A mozaikmódszer.* Ford. Szabó Mihály. Budapest: Antall József Tudásközpont.

Snowden, Edward (2019): *Rendszerhiba.* Ford. Tomori Gábor, N. Kiss Zsuzsa. Budapest: 21. Század Kiadó.

Tajfel, Henri (2016): Social Identity and Intergroup Behaviour. *Social Science Information,* 13(2), 65–93. Online: https://doi.org/10.1177/053901847401300204

Venkatesh, Viswanath – Davis, Fred D. (2000): A Theoretical Extension of the Technology Acceptance Model: Four Longitudinal Field Studies. *Management Science,* 46(2), 2186–204. Online: https://doi.org/10.1287/mnsc.46.2.186.11926