Belépő a tudás közösségébe

Szakköri segédanyagok tanároknak

Informatikai biztonságtudatosság

Törley Gábor

A kiadvány „A felsőoktatásba bekerülést elősegítő készs
lesztő és kommunikációs programok megvalósítása, val
az MTMI szakok népszerűsítése a felsőoktatásban” (EFOP-
16-2017-006) című pályázat keretében készült 2019-ben.

Eötvös Loránd Tudományegyetem
Informatikai Kar

SZÉCHENYI 2020
MAGYARORSZÁG KORMÁNYA
Európai Unió
Európai Szociális Alap
BEFEKTETÉS A JÖVŐBE

Informatikai biztonságtudatosság

Szerző

Törley Gábor

Felelős kiadó

ELTE Informatikai Kar
1117 Budapest, Pázmány Péter sétány 1/C.

ISBN szám

ISBN 978-963-489-148-2

A kiadvány „A felsőoktatásba bekerülést elősegítő készségfejlesztő és kommunikációs programok megvalósítása, valamint az MTMI szakok népszerűsítése a felsőoktatásban” (EFOP-3.4.4-16-2017-006) című pályázat keretében készült 2017-ben.

Tartalomjegyzék

1. Fogalmi bevezetés: informatikai védelem, informatikai biztonság

Általában a biztonság alatt egy rendszer állapotát értjük. Olyan **kedvező állapotot**, amellyel szemben elvárható, hogy a fenyegetések **bekövetkezésének lehetősége**, valamint az esetlegesen bekövetkező fenyegetés által **okozott kár a lehető legkisebb legyen**. Ahhoz azonban, hogy teljes legyen ez a biztonság az szükséges, hogy **minden valós fenyegetésre valamilyen védelmet nyújtson**, ugyanakkor **körkörös legyen**, vagyis **minden támadható ponton biztosítson** valamilyen akadályt a támadó számára. Mindezek mellett elvárható, hogy **folyamatosan** létezzen[1]. Ahhoz, hogy ezt az állapotot elérjük és fenntartsuk, védelemre van szükségünk, azaz jogi, műszaki, technikai, szervezési, stb. intézkedésekre és eljárások együttes rendszerére.

A biztonság és a védelem, így, cél – eszköz viszonyban áll egymással. A védelem célja a biztonság kedvező állapotának megteremtése és fenntartása és minél hatékonyabb a védelem, annál hatékonyabb és tartósabba biztonság.

Legyen szó bármilyen szervezetről, intézményről, a biztonság állapota számos összetevővel, működési tényezővel kapcsolatban felmerülhet. Így például beszélhetünk a szervezeti felépítés és a szervezeti működés biztonságáról, ha a szervezet kialakítása a hatékony és stabil működés irányába hat. Nincs túl sok vagy túl kevés bürokratikus szint, és a szervezet képes alkalmazkodni – különösebb megrázkódtatás nélkül – a környezetből vagy az újabb feladatokból adódó változásokhoz. A szervezeti felépítés és működés biztonságának megteremtése irányába ható védelmi intézkedések például a szervezeti felépítés pontos megtervezése, a humánerőforrás-stratégia kialakítása, a megfelelően működtetett minőségbiztosítás, stb.

Egy másik biztonsági kategória a gazdasági-pénzügyi biztonság. Ez akkor áll fenn, ha rendelkezésre állnak a működéshez szükséges megfelelő anyagi és tárgyi források. E nélkül a szervezet kényszerpályára kerülhet, például az informatikai erőforrások rendszerbe állítása, alkalmazása és védelme terén is. A gazdasági-pénzügyi biztonság megteremtésére irányuló védelmi intézkedéseket számos külső tényező is befolyásolja, így nehéz lenne azt állítani, hogy a szigorú gazdálkodás, mint védelmi eszköz eredménye lenne a gazdasági-pénzügyi biztonság, bár kétség kívül hozzájárul annak megteremtéséhez. A pénzügyi biztonság megteremtésére irányuló védelmi intézkedéseket alapvetően befolyásolja a működési környezet, illetve az ehhez kapcsolódó biztonsági kategória, a működési környezet biztonsága. Ez alatt, profitorientált szervezet esetén a gazdasági biztonságot, a gazdasági folyamatok kiszámíthatóságát értjük. Nem profitorientált, végrehajtó szervezetek esetén, mint amilyen a közigazgatási szervek többsége, a gazdasági környezetnél jelentősebb és közvetlenebb befolyásoló hatással bír a – felépítést, működést, feladatmegosztást alapvetően meghatározó – jogszabályi háttér biztonsága. Látszik, hogy ennek a biztonsági kategória megvalósítása érdekében kifejtett védelem részben a szervezeteken kívül esik, így a védelmi intézkedéseket a működési környezetben, és az azt befolyásoló szervezeteknél kell keresnünk.

A vagyonbiztonság fogalmának meghatározásával közelebb kerülünk az információs rendszerekhez. Ez azt jelenti, hogy a szervezet céljának megvalósításához szükséges vagyoni erőforrások (épületek, berendezési tárgyak, vagyonvédelmi eszközök, munkaeszközök, az információs rendszerek fizikai összetevői) bizalmasságának, sértetlenségének és rendelkezésre állásának fenyegetettsége minimális, azaz csekély esélye van annak, hogy a kedvező állapot megváltozzon[2], tehát a vagyoni erő-

[1] Muha Lajos (szerk.): Az informatikai biztonság kézikönyve – Budapest: Verlag Dashöfer, 2000-2005.

[2] Horváth László, dr. Lukács György, dr. Tuzson Tibor, Vasvári György: Informatikai biztonsági rendszerek, BMF Kandó Kálmán Villamosmérnöki Kar, Budapest, 2001., 6. oldal

forrásokat csak az arra illetékesek használhatják (például az épületekbe, helyiségekbe csak a jogosultak léphetnek be), a vagyoni erőforrások megfelelnek az eredeti állapotuknak (sértetlenek, ide nem értve persze a szükségszerűen bekövetkező amortizációt) és adott időben, adott helyen rendelkezésre állnak, használhatók, szolgáltatásokat nyújthatnak.

Végül, de nem utolsó sorban, a biztonsági kategóriák közé sorolhatjuk az informatikai biztonságot. A fogalom meghatározásához az informatika definíciójából kell kiindulnunk. Az informatika az adatok rögzítésével, kezelésével, rendszerezésével, továbbításával foglalkozik[3], és nem kizárólag a számítógéppel történő információkezelést és feldolgozást öleli fel: vannak technológia független részei, elvei, szabályai, eszközei is. Általában ismerjük azt a kijelentést, miszerint „minden információ adat, de nem minden adat információ". Ebből megállapíthatjuk azt, hogy hogy az informatika központi fogalma az információ, illetve az ezt is tartalmazó tágabb kategória: az adat. Az informatika az információ és az adat köré csoportosítja interdiszciplináris és sokszor technológia független eszközeit, elveit.

Ezzel meg is érkeztünk a fő témánkhoz, az adat kezeléséhez, feldolgozásához, védelméhez és biztonságához. Az informatikai biztonság is technológia független és interdiszciplináris fogalom[4]. Technológia független azért, mert adatot, információt kezelni nem csak számítógéppel vagy kommunikációs eszközökkel lehet, hanem papír alapon is. Interdiszciplináris azért, mert az információs és a kommunikációs technológiák eszközein kívül felöleli a szervezés- és vezetéstan, a jogtudomány, a szociológia, a pénzügytan, a közgazdaságtan és egyéb tudományok bizonyos területeit.

Ez a tananyag – kiindulva az Európai Unió általános adatvédelmi rendeletéből (GDPR[5]) –, azokat az elsősorban számítástechnikai és kommunikációs technológiákkal megvalósuló módszereket és eszközöket mutatja be, amelyek segítségével az adatalany érdekében az adatot meg lehet védeni.

Az informatikai biztonság és az informatikai védelem fogalma legalább két nézőpontból közelíthető meg. Ez azt jelenti, hogy az embert a középpontjába állító jogi oldal és az adatot a középpontjába állító műszaki, technikai oldal folyamatos versenyben van egymással, ugyanakkor egymást kiegészítve működnek. A rendszerváltás előtt az informatikai védelem megvalósítását és szabályozását tekintve a technikai oldalra helyeződött nagyobb hangsúly. A rendszerváltást követően azonban az embert a középpontba állító, emberi jogi gondolkodás és az individuum érdekében megvalósított adatvédelem (a szó szoros értelmében) lett az uralkodó irányzat. Ma tehát az informatikai védelem két oldala, egymást kiegészítve, az adatalany érdekében lép fel: egyrészt védi az egyént, a személyiséget (jogi szabályokkal és garanciákkal), és ennek érdekében az adatot (műszaki, technikai eszközökkel). Ez a szemléletmód Nyugat-Európában a II. világháború után fokozatos fejlődés nyomán bontakozott ki, míg Magyarországon csak a rendszerváltás után.

Az informatikai biztonság tehát kétféle megközelítésben írható le:

- Jogilag – az embert, az adatalanyt (az érinttetet) a középpontba állítva: pl. jogi eszközök (törvények): az információs szabadságjogok (információs önrendelkezési jog és információszabadság), valamint az egyéb emberi és személyhez fűződő jogok (pl. az emberi méltósághoz való jog)

[3] Dr. Horváth Katalin – Dr. Kőnig Balázs – Dr. Orbán Anna – Törley Gábor: A közigazgatási informatika alapjai Szerk.: Dr. Orbán Anna Budapest, FÁMA Zrt. – Nemzeti Közszolgálati és Tankönyv Kiadó Zrt. ISBN 978-615-5344-08-4 Budapest, 2013.

[4] Törley Gábor: Adatbiztonság a közigazgatásban, FÁMA Zrt. – Nemzeti Közszolgálati és Tankönyv Kiadó Zrt. ISBN 978-615-5344-05-3 Budapest, 2013. 139 p. (elektronikus jegyzet)

[5] Az Európai Parlament és a Tanács (EU) 2016/679 rendelete, General Data Protection Regulation

- Műszaki, technikai értelemben – az adatalany érdekében az adatot a középpontba állítva: az a kedvező állapot, amikor a szervezet, információs rendszer informatikai erőforrásai bizalmasságának, sértetlenségének és rendelkezésre állásának fenyegetettsége minimális, azaz csekély a kedvező állapot megváltozásának a valószínűsége[6].

Az informatikai védelem az informatikai biztonság megteremtésének eszköze, és az informatikai biztonság az informatikai védelem eredménye. A cél és az eszköz megjelölését követően azonban a terminológiában némi fogalmi zavar keletkezhet[7]. Az informatikai védelem két oldalának az angol tükörfordítása ugyanis nem egészen igazodik a tartalomhoz. Az informatikai védelemnek az embert, az adatalanyt a középpontjába állító vetülete az adatvédelem (data protection). Ez azonban valójában nem az adat, hanem az adatalany védelmét jelenti (tehát a jogi oldalról szól). Az informatikai védelemnek az adatot a középpontjába állító vetülete az adatbiztonság (data security). Ez azonban valójában nem biztonsági, hanem védelmi kategória, nem cél, hanem eszköz: az adatalany védelme érdekében az adat védelmének műszaki, technikai eszköze. A fogalom e pontos meghatározása mutatja az adatalany védelméhez képest alárendelt szerepét is. (Sajnos, a fogalom téves elnevezése és ezért sokszor téves értelmezése folytán az adatbiztonságot sok szakember célnak és nem eszköznek tekinti még ma is.)

Fontosnak tartom, hogy élesebben el kellene különíteni az *adatvédelemnek* és az *adatok védelmének* jelentését. Míg az *adatvédelem* „a személyes adatok jogszerű kezelését, az érintett személyek védelmét biztosító alapelvek, szabályok, eljárások, adatkezelési eszközök és módszerek összességét" jelenti[8], addig az *adatok védelme* alatt azokat a védelmi módszereket értem, amelyeket az érintett, valamint az adatkezelő védelme érdekében az adatokon hajtanak végre. Az adatvédelem központi szereplője az adatalany, az adatok védelmének fő fókuszában pedig az adat áll. Tehát az informatikai biztonság fogalmát két oldalról, jogi és műszaki oldalról is meg lehet közelíteni, és valójában ugyanaz a célja a két megközelítésnek: az adatalany adatai legyenek biztonságban. Ezt az egységes megközelítést érdemes átadni a középiskolában (és egyetemen is).

2. Adatvédelem

Az adatvédelmi szabályozás célja a magánélet védelme, ilyen módon az információs szabadságjogokat, vagy más néven az adatvédelmi jogot az emberi méltóság védelmének sajátos aspektusaként is felfoghatjuk. Az információs technológia elterjedésének köszönhetően az állampolgár kiszolgáltatottsága egyre nő. Nem csak az állam tárol rólunk adatokat, hanem a piaci szereplők is áhítoznak arra, hogy minél többet megtudjanak rólunk, hiszen így tudják hatékonyabbá tenni marketingpolitikájukat.

Az adatvédelmi jog másik célja, hogy az állampolgár alanya és ne célja legyen az adatkezelésnek. Általában (kivéve, ha a jogszabályok másként rendelkeznek) az állampolgárnak joga van tudni azt, hogy ki, milyen adatokat kezel róla, mit csinál vele, meddig tárolja azokat. Így csökken az adatalany kiszolgáltatottsága.

---

[6] Horváth László, dr. Lukács György, dr. Tuzson Tibor, Vasvári György: Informatikai biztonsági rendszerek, BMF Kandó Kálmán Villamosmérnöki Kar, Budapest, 2001., 6. oldal

[7] Törley Gábor: Adatbiztonság a közigazgatásban, FÁMA Zrt. – Nemzeti Közszolgálati és Tankönyv Kiadó Zrt. ISBN 978-615-5344-05-3 Budapest, 2013. (elektronikus jegyzet)

[8] Nemzeti Adatvédelem és Információszabadság Hatóság: Adatvédelmi értelmező szótár - http://www.naih.hu/adatvedelmi-szotar.html - Letöltve: 2019.05.02.

Magyarország alapjogként ismeri el a személyes adatok védelméhez és a közérdekű adatok megismerhetőségéhez fűződő jogot.

Az Alaptörvény 6. cikke szól az információs önrendelkezési jogról és az információszabadságról.

Alaptörvény VI. cikk:

(1) Mindenkinek joga van ahhoz, hogy magán- és családi életét, otthonát, kapcsolattartását és jó hírnevét tiszteletben tartsák.

(2) Mindenkinek joga van személyes adatai védelméhez, valamint a közérdekű adatok megismeréséhez és terjesztéséhez.

(3) A személyes adatok védelméhez és a közérdekű adatok megismeréséhez való jog érvényesülését sarkalatos törvénnyel létrehozott, független hatóság ellenőrzi.

Ahogy azt fentebb láttuk, az adatvédelem az informatikai biztonság jogi megközelítése. Ma ezt az Európai Parlament és a Tanács (EU) 2016/67 rendelete[9] (a továbbiakban: GDPR) szabályozza. Ennek a fejezetnek nem célja a jogi normaszöveg elemzése, alapvetően fontos elveket fogok kiragadni belőle. Fontos szó szerint idézni a Rendelet indoklását (38), ugyanis jól összefoglalja, miért van szükség erről a témáról tanítani a közoktatásban: *„A gyermekek személyes adatai különös védelmet érdemelnek, mivel ők kevésbé lehetnek tisztában a személyes adatok kezelésével összefüggő kockázatokkal, következményeivel és az ahhoz kapcsolódó garanciákkal és jogosultságokkal. Ezt a különös védelmet főként a gyermekek személyes adatainak olyan felhasználására kell alkalmazni, amely marketingcélokat, illetve személyi vagy felhasználói profilok létrehozásának célját szolgálja, továbbá a gyermekek személyes adatainak a közvetlenül a részükre nyújtott szolgáltatások igénybevétele során történő gyűjtésére. A közvetlenül a gyermek részére nyújtott megelőzési és tanácsadási szolgáltatások esetében nincs szükség a szülői felügyelet gyakorlójának hozzájárulására.”*

Fontos tisztában lennünk a személyes adat fogalmával. A GDPR 4. cikk 1. szerint személyes adat: *„azonosított vagy azonosítható természetes személyre („érintett”) vonatkozó bármely információ; azonosítható az a természetes személy, aki közvetlen vagy közvetett módon, különösen valamely azonosító, például név, szám, helymeghatározó adat, online azonosító vagy a természetes személy testi, fiziológiai, genetikai, szellemi, gazdasági, kulturális vagy szociális azonosságára vonatkozó egy vagy több tényező alapján azonosítható”*

Ki kell emelnem azt a szót, hogy azonosít*ható*. Egy illegális „adatgyűjtő” számára (aki akár lehet egy troll vagy egy szexuális ragadozó), nem probléma, ha az első néhány adatmorzsából nem tudja azonosítani a célszemélyt, sokszor az is elég, hogy a megszerzett információkból valamilyen másik, akár szenzitív adatra, tulajdonságra következtessen, ami akár eljuttathatja őt a teljes azonosításig.

Fontos fogalmi elem az is, hogy a személyes adatot nem kell rögzíteni (leírni, tárolni) ahhoz, hogy teljes védelemben részesüljön, hiszen a magánszférával is ugyanez a helyzet.

Lényegében bármit tekinthetünk személyes adatnak (adott esetben akár a gyermek szüleinek autójának rendszámát is), amely alapján el lehet jutni az adatalanyhoz. Emiatt fontos tudatosítani a tanulókban, hogy olyan adatok/információk, mint pl.

- név,
- életkor,
- iskola és osztály, ahova jár (beleértve a korábbi iskolákat is),
- lakhely,

[9] https://eur-lex.europa.eu/legal-content/HU/TXT/HTML/?uri=CELEX:32016R0679 – Letöltve 2019.05.16.

- szülők neve,
- diákigazolvány száma,

személyes adatok, és nem tartoznak akárkire.

Léteznek olyan személyes adatok, amelyeket a jogszabályok külön védelemben részesítenek, ezek az úgynevezett különleges adatok. Ilyenek pl. az egészségügyi állapotra, kóros szenvedélyre, vallásra, bőrszínre, nemzetiségi hovatartozásra, pártprefenciára, büntetett előéletre, szexuális életre vonatkozó személyes adatok.

A különleges adatok kezelésénél még óvatosabban kell eljárni, hiszen itt különösen nagy sérelmet lehet okozni az érintettnek. A következmények az enyhe kellemetlenségtől az élet teljes ellehetetlenítéséig is terjedhetnek, gondoljunk csak a közösségi hálózatokra, illetve az internetes zaklatásra.

Az adatvédelemhez fűződő egyik fontos jog az önrendelkezés joga. Ez azt jelenti, hogy alapesetben, ha bárki kezelni akarja a személyes adatokat, ahhoz be kell szerezni az érintett hozzájárulását. A jogszabály szerint **16 éves kor felett bárki** dönthet arról, hogy milyen esetben járul hozzá ahhoz, hogy mások kezeljék a személyes adatait. Gyakorlatilag a nagykorúság határa 16 év az adatvédelem esetében. 16 éves kor alatt a szülők hozzájárulása szükséges az adatok kezeléséhez. Különleges adatok esetén mindenképpen írásbeli hozzájárulásra van szükség.

Adatkezelésnek minősül, ha valakinek a fényképét kiteszem a közösségi hálózatra. A fénykép személyes adat, mivel felismerhető és azonosítható a rajta levő személy. Tehát akkor és csak akkor publikálhatom valaki más fényképét, ha rendelkezem a hozzájárulásával.

Léteznek olyan kivételes esetek, amikor nem kell vagy lehetetlen megkapni az adatalany hozzájárulását. Tipikus példák: körözés kiadása, bűnügyi érdek, a gyermek egészségének az érdeke, illetve ha törvény rendeli el az adatkezelést (pl. választások, népszámlálás, egészségügyi adatok kezelése).

Ha a természetes személy kizárólag személyes célra végez adatfeldolgozást, abban az esetben nem vonatkoznak rá az adatkezelői kötelezettségek. Tehát ha valaki eltárolja a barátai telefonszámát a saját telefonjában, nem válik a jog szerint adatkezelővé, és nyilvánvalóan nem kell az érintettek hozzájárulását kérni ehhez (egyébként, lényegében megkapta ezt a hozzájárulást, amikor az érintett megadta a telefonszámát). Ezt az esetet nevezzük úgy, hogy „háztartási kivétel", azaz a GDPR-t nem kell alkalmazni olyan esetekben, amikor az adatok kezelését a *„természetes személyek kizárólag személyes vagy otthoni tevékenységük keretében végzik"*[10]

Az egyik legfontosabb garanciája az adatvédelemnek a **célhoz kötöttség**. Személyes adatok gyűjtése csak meghatározott, egyértelmű és jogszerű célból történhet, és azokat nem kezelhetik ezekkel a célokkal össze nem egyeztethető módon. Ilyen jogszerű cél, pl. a tanulók adatainak nyilvántartása vagy pl. egy kirándulás utaslistája. Azonban, ha az adatkezelés elérte a célját, akkor attól kezdve az adatokat nem lehet már kezelni. Ebből következik, hogy „csak úgy" senkiről sem lehet adatokat tárolni (az adatok puszta tárolása is adatkezelés). Másik következménye ennek az elvnek, hogy amikor hozzájárulásomat adom adataim kezeléséhez, akkor tisztában kell lennem annak céljával.

Eddig több szó esett az adatkezelés jogalanyáról, tehát az érintettről. Az adatainkat kezelő személyt vagy jogi személyt adatkezelőnek hívjuk, pontos definíció szerint az adatkezelő *„az a természetes vagy jogi személy, közhatalmi szerv, ügynökség vagy bármely egyéb szerv, amely a személyes adatok kezelésének céljait és eszközeit önállóan vagy másokkal együtt meghatározza"*

[10] Adatvédelmi rendelet 2. cikk (2) c)

Az adatkezelőnek kötelessége megteremtenie azokat a feltételeket, amelyek biztosítják az adatalany jogait. Adatkezelő lehet az iskola, a webáruház mögött levő cég, az adott közösségi hálózatot üzemeltető cég, stb.

Az érintettek fontos joga a tájékozódáshoz való jog. Ez azt jelenti, hogy bárki informálódhat egy konkrét adatkezelőnél arról, hogy

- milyen adatait ismeri (adatok köre);
- azok honnan vannak meg neki (adatok forrása);
- miért vannak azok nála és mit csinál velük (adatkezelés célja);
- mióta vannak meg neki az adatok és meddig kívánja azokat felhasználni;
- és a fentieken túlmenően bármilyen egyéb, az adatkezeléssel kapcsolatos kérdés feltehető.

A fenti kérdésekre 25 napon belül választ kell kapnia a kérelmezőnek. Amennyiben a kérelmező nem kap választ a megadott határidőn belül vagy úgy gondolja, hogy az adatkezelés nem jogszerű, akkor a Nemzeti Adatvédelem és Információszabadság Hatósághoz (NAIH) fordulhat az úgy kivizsgálásáért.

Amennyiben kiderül, hogy az adatalanyról tárolt adatok nem felelnek meg a valóságnak, akkor kérni lehet ezek javítását az adatkezelőtől.

Azokban az esetekben, amikor nem jogszabály írja elő az adatkezelést, hanem az kizárólag az érintett hozzájárulásán alapul, az adatalanynak jogában áll a hozzájárulást visszavonni, és a róla tárolt adatokat töröltetni. Erre jó példa, amikor megszüntetem a regisztrációmat egy e-mail szolgáltatónál, a szolgáltatónak törölnie kell a személyes adataimat. Másik példa a hírlevélről való leiratkozás. Fontos tudni, hogy maga a leiratkozás nem vonja automatikusan maga után a személyes adatok törlését, ezt külön kell kérvényezni az adatkezelőtől

A Világháló lehetőségei, szolháltatásai nagy kihívást adnak annak, aki tudatosan szeretné kezelni az adatait. Ami egyszer kikerül az Internetre, ott is marad. A posztokon, feltöltött képeken túl figyelni kell a regisztrációkor megadott adatokra is.

Az adatvédelmi jog másik pillére az **információszabadság**. Ez a jog lehetővé teszi, hogy az állampolgárok megismerhessék az állami szervek működésével, a közpénzek elköltésével kapcsolatos információka, hiszen egy demokráciában fontos alapelv, hogy az emberek az őket érintő döntések hátteréről, az általuk választott döntéshozók eljárásáról minél megbízhatóbb képet kaphassanak.

Ilyen állami szerv pl. az adóhatóság, a hulladékszállító cég, az iskola, a közműszolgáltatók, az iskolai érkeztetést biztosító cég, de ilyen egy állami üdülő vagy tábor is. Ebbe a körbe személyek is tartoznak: pl. polgármester, miniszter, iskolaigazgató, országgyűlési képviselő. A fenti szerveknek és személyeknek kötelességük, hogy rendszeresen, önmaguktól és kérés esetén külön is beszámoljanak tevékenységükről.

Az állami vagy helyi önkormányzati feladatot, valamint jogszabályban meghatározott egyéb közfeladatot ellátó szerveknek és személyeknek rendszeresen elektronikusan vagy más módon közzé, illetve hozzáférhetővé kell tenniük a tevékenységükkel kapcsolatos adatokat. Az elektronikus közzététel esetén *„a közérdekű adatokat internetes honlapon, digitális formában, bárki számára, személyazonosítás nélkül, korlátozástól mentesen, kinyomtatható és részleteiben is adatvesztés és -torzulás nélkül kimásolható módon,*

a betekintés, a letöltés, a nyomtatás, a kimásolás és a hálózati adatátvitel szempontjából is díjmentesen kell hozzáférhetővé tenni".[11]

Közérdekű adat megismerése iránt bárki igényt nyújthat be, akár szóban, akár írásban, akár elektronikus úton. Az adatigénylésnek a közérdekű adat kezelője köteles eleget tenni legkésőbb az igény tudomására jutásától számított 15 napon belül. A válaszadást csak kivételesen, törvényi indokokra hivatkozva lehet elutasítani (pl. ha magyar katonai titkokat sértene, vagy bűncselekmények felderítését akadályozná).

Közérdekű adatnak minősül az, hogy pl. az állami szerv / cég tevékenysége, működése; mennyi fiatal jár iskolába egy településen, mennyit fizet a fenntartó az iskolának, mennyit költ az iskola tornaszerre, általában mennyi ösztöndíjat ad az önkormányzat, stb. Ha nem kapunk választ adatigénylésünkre, akkor a NAIH-hoz lehet fordulni.

A NAIH feladata, hogy őrködjön az adatvédelmi jogok felett. Itt jogász és nem jogász adatvédelmi szakértők, tanácsadók és informatikusok köztisztviselőként dolgoznak és ingyen, bármikor, bármilyen formában (e-mailen is) kérni lehet egy esetleges adatvédelemmel vagy információszabadsággal kapcsolatos panasz kivizsgálását.

Fontosnak tartom kiemelni, hogy a NAIH a honlapján[12] bíztatja a fiatalokat a tudatos joggyakorlásra, azaz ha csak kérdés merülne fel az adatvédelemmel kapcsolatban, akkor is várja a megkereséseket.

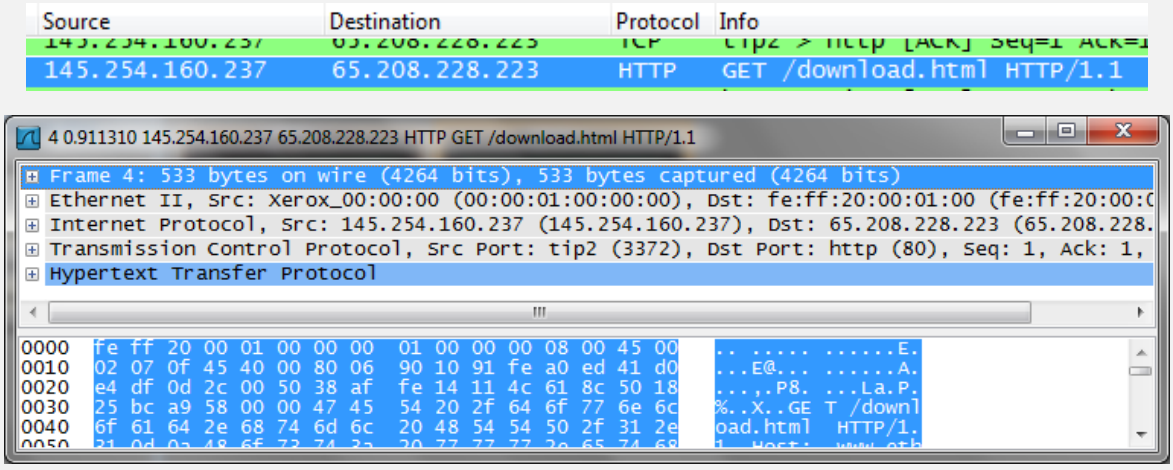
Panasz benyújtása esetén kérni lehet, hogy a kérelmező adatai ne jussanak az vizsgálat alá került adatkezelő tudomására, tehát lehetőség van teljes anonimitásra a kérelmező szemszögéből nézve. Viszont létezhetnek olyan esetek, ahol az adatkezelő rájöhet arra, hogy ki volt a panaszbejelentő. Ekkor sem jogszerű, ha hátrány éri a panaszost. Ha mégis olyan történne, hogy egy adatvédelmi bejelentés miatt hátrány éri a panaszost, akkor a NAIH segít megtalálni a megfelelő fórumot a jogorvoslat érdekében.

A Hatóság minden esetben választ ad az információs jogokkal kapcsolatos kérdéseke és kivizsgálja a panaszt, amit, ha jogosnak ítél, akár még komoly bírságot is kiszabhat az adatkezelőre.

3. Csatlakozás a világhálóhoz

Ahhoz, hogy megértsük, hogyan is lehet biztonságosan csatlakozni a világhálóhoz, meg kell ismernünk az Internetes kommunikáció alapjait. Az adatforgalom alapegysége a csomag, tehát egy letöltött fájlt így is el lehet képzelni: csomag + csomag + csomag… Az adatforgalom bizonyos szabályok szerint zajlik, ezeket a szabályokat a protokollok határozzák meg. Például az Internet Protocol (IP) írja le, hogyan kerülnek az egyes csomagok egyik számítógépről a másikra. Minden hálózaton levő számítógépnek van IP címe: pl. 192.101.32.156 (IPv4 szabvány szerint). A csomag így ezekből a részekből áll: forrás IP cím, cél IP cím, adathalmaz részlete (lásd 1. ábra). Az IP-nek az a hátránya, hogy nem jelzi vissza azt, hogy a csomagok rendben megérkeztek-e.

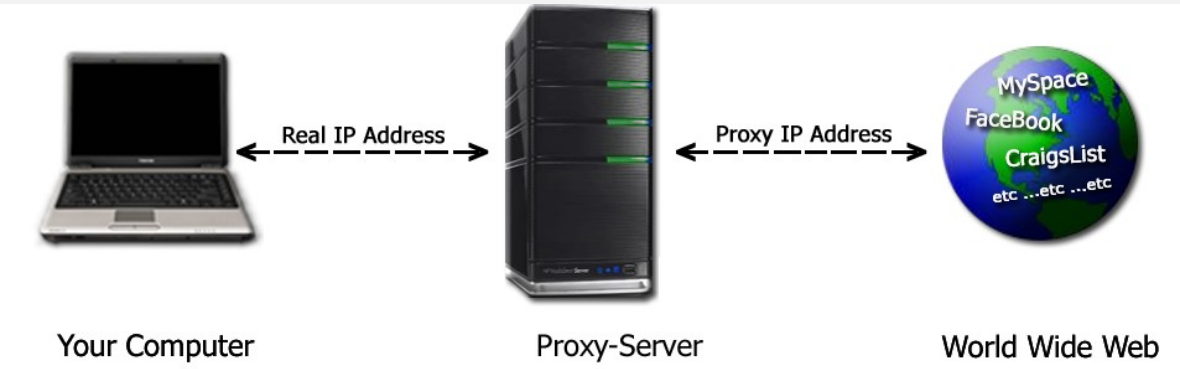
[11] 2011. évi CXII. törvény az információs önrendelkezési jogról és az információszabadságról (Infotv.) 33. § (1)
[12] NAIH: Kulcs a net világához: http://naih.hu/adatvedelemr-l-fiataloknak--kulcs-a-net-vilagahoz--projekt.html - Letöltve: 2019.05.17.



1. ábra Példa egy hálózati csomagra és tartalmára

A Transmission Control Protocol (TCP) sorszámot ad minden csomagnak – így tudjuk, hány csomag lesz, illetve meggyőződik arról, hogy csomagok célt értek-e. Minden protokoll vagy alkalmazás úgynevezett kapukat (portokat) használ az egyes számítógépekhez való csatlakozás során, pl. http – 80 vagy 8080-as port, https – 443-as port.

A tűzfalak az Internethez való biztonságos csatlakozás eszközei. Ezzel kapcsolatban számos védelmi feladat ellátására alkalmasak. Egyrészt elősegítik a név nélküli Internet-használatot. Ugyanis az, hogy az Interneten milyen lapokat, milyen gyakorisággal látogatunk meg, személyes adatnak minősül, ilyen típusú érdeklődésünk a magánszféra védendő része. Az anonimitást biztosító tűzfalakat proxy kiszolgálóknak (angolul proxy server) hívjuk, amelyeknek az a feladatuk, hogy a felhasználó megbízásából, őt helyettesítve végezzék az internet-kapcsolatok (TCP) fel- illetve leépítését.[13] Ez annyit jelent, hogy a webszerver(ek) és a felhasználó közé egy harmadik fél, a proxy kiszolgáló kerül. A felhasználó (böngészője) által kért weblapokat a proxy kiszolgáló tölti le és továbbítja a felhasználónak. Így a felhasználó csak a proxy kiszolgáló számára azonosítható (IP cím alapján), de az Internet tartalmát szolgáltató webszerverek számára nem (lásd 2. ábra).



2. ábra Proxykiszolgáló működése[14]

A tűzfalak másik feladata annak megakadályozása, hogy a számítógépről információ jusson ki az Internetre, illetve, hogy onnan rosszindulatú programok jussanak be a felhasználó számítógépébe.[15] A tűzfalak védelme olyan, mintha „fallal", „kerítéssel" vennénk körbe a számítógépet (személyes

[13] Othmar Kyas: Számítógépes hálózatok biztonságtechnikája, Kossuth Kiadó, Budapest, 2000., 195. oldal
[14] http://www.elite-proxy-server.com/image-files/elite-proxy-server-diagram.png - Letöltve: 2011.11.18.
[15] Andrew S. Tanenbaum: Számítógéphálózatok, PANEM Könyvkiadó, Budapest, 2004., 829. oldal

tűzfalak), illetve egy egész hálózati szegmenset (hardver alapú tűzfalak, amelyek útválasztókba vannak beépítve): az információs rendszer és a külvilág (Internet) közötti ki- és bemenő (adat)forgalmat egyetlen (vagy néhány) jól őrizhető kapun keresztül bonyolítja. Tehát a tűzfal azt figyeli, hogy

- melyek azok az engedélyezett portok (kapuk), amelyeken keresztül kapcsolódni lehet.
- melyek azok a helyek (IP cím), ahonnan lehet vagy nem lehet csomagot (adatot) fogadni és melyek azok a címek, ahova engedélyezett vagy tilos az adatküldés,
- melyek azok a szoftverek, amelyek kommunikálhatnak a világhálóval.

Tűzfalprogramokból sok fajta található a piacon.

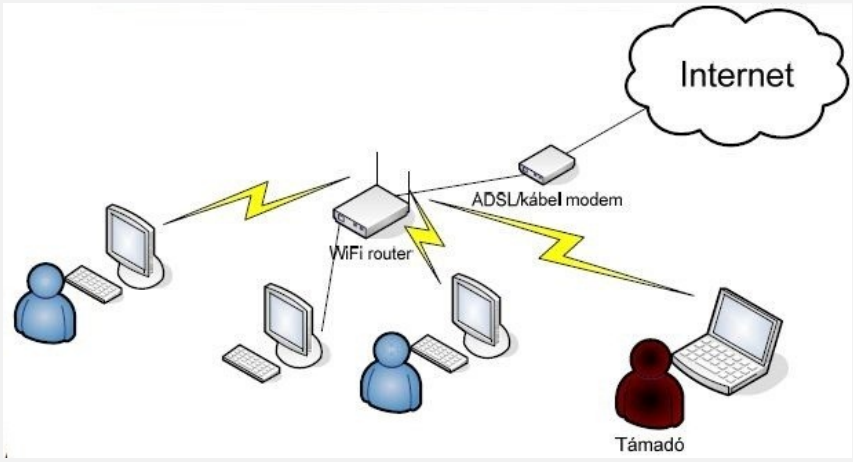
Léteznek olyan szoftverek is, amelyek komplex védelmet nyújtanak, tehát antivírus programot, kémprogram-írtót és személyes tűzfalat is tartalmaznak.

Egy személyi számítógép védelmének az alappillérei tehát a következők:

- Mindig friss adatbázissal futó antivírus program
- Tűzfal program
- Mindig friss adatbázissal futó kémprogram-írtó
- Legyenek fent az operációs rendszer és az alkalmazói programok frissítései
- Felhasználói tudatosság

3.1. Vezeték nélküli hálózatok biztonsága

Az elmúlt tízenöt évben váltak egyre olcsóbbá és ennek okán népszerűbbé a vezeték nélküli technológiák, így a vezeték nélküli hálózatok. Előnyei mellett (pl. sok kábellel kevesebb van a szobában) valós veszélyeket is rejt magában ez a technológia (gondolok itt különösen a nyílt wifi hálózatokra). Egyszerű példaként nézzünk egy tipikus otthoni hálózatot (lásd 3. ábra)!



3. ábra Tipikus otthoni hálózat[16]

[16] Szentgyörgyi Attila: WiFi hálózatok biztonsági kérdései, http://hte.tmit.bme.hu/root/club_ppt/201005/eloadas_szgyi_wifi_hte.pdf - Letöltve: 2019.05.30.

Egy ilyen otthoni hálózatnak két gyenge pontja lehet: az egyik a felhasználó, a másik pedig a biztonsági protokollok minősége. A vezeték nélküli hálózatok természetüknél fogva kevésbé biztonságosak, mint jobban kiérlelt, nagyobb múlttal rendelkező vezetékes testvéreik. Mivel a vezeték nélküli hálózati kártyák adatközvetítő közege a levegő, így jobban ki vannak téve annak, hogy illetéktelenek is hozzáférjenek az adatokhoz. A „hálózatszaglászók" a WLAN esetében könnyebben követhetik figyelemmel és lophatják el az adatokat, mint a vezetékeseken, hiszen a behatoláshoz nincs szükségük fizikai kapcsolatra, így könnyebb dolguk van. A leendő hackernek csak egy vezeték nélküli csatolókártyára van szüksége, valamint ismernie kell az aktuális hálózat biztonsági réseit, így akár „ház előtt, az autóban ülve" is be tud jutni a hálózatba.

Ha a vezeték nélküli hálózaton nincs kódolás, a rajta áthaladó adatok, gyakorlatilag, bárki számára elérhetőek, a 4. ábrán látni lehet a csomagok forrás- és a célállomás IP címeit és a tartalmukat is.

Protocol	Src MAC	Dest MAC	Src IP	Dest IP	Src Port
IP/TCP	GemtekTe...	Intel:96:0...	192.168.0.4	192.168.0.1	micros...
IP/UDP	GemtekTe...	01:00:5E:...	192.168.0.4	239.255.2...	1900
IP/UDP	GemtekTe...	33:33:00:...	158.22.250.0	0.0.0.12	1900

4. ábra Mi látszik egy nyílt vezeték nélküli hálózaton

A vezeték nélküli hálózati szabvány (IEEE[17] 802.11, 1997.) tervezői már a kezdettől fogva fontosnak tartották a biztonságot. Már a szabvány korai verziója is tartalmazott biztonsági mechanizmusokat, melynek célja az volt, hogy a vezeték nélküli hálózat legalább rendelkezzen azokkal a biztonsági tulajdonságokkal, mint vezetékes testvére, így ezt vezetékes ekvivalencia protokollnak (wired equivalency protocol = WEP) nevezték el. Elméletben ez a protokoll biztosítja a hálózati adatok titkosságát, valamint másodlagos funkcióként megakadályozza, hogy illetéktelenek hozzáférhessenek magához a hálózathoz. 2001-ben számos kutató vizsgálata megmutatta, hogy a WEP nem tölti be e két funkcióját.[18] A főbb problémák: Az IEEE 802.11-es szabvány egyik hiányossága, hogy nem rendelkezik a megosztott kód kezeléséről. A legtöbb vezeték nélküli hálózat esetén ez mindössze egyetlen kód, melyet kézzel állítanak be minden csomóponton és az Access Pointon (AP) is. Gyenge a kódolás (rövid kulcs) és túl hosszú ideig használja a hálózat, így egy passzív lehallgatással néhány perc alatt elég csomagot lehet elfogni ahhoz, hogy azokból visszafejtsék a kulcsot.

A WEP hibáit felismerve az IEEE új biztonsági megoldást dolgozott ki, amelyet a 802.11i szabvány tartalmaz. Ennek része a WPA (Wireless Protected Access), amely a TKIP (Temporal Key Integrity Protocol) kulcskiosztást használja. A titkos kulcsot az AES (Advanced Encryption Standard) algoritmussal titkosítják. Az új módszerrel hitelesített eszközök esetében, a forgalmazott adatcsomagokban dinamikusan képes váltogatni a titkosítást szolgáló kulcsokat, azaz hiába szerzi meg a támadó az éppen használt kulcsot a forgalom lehallgatásával összegyűjtött adatokból, a TKIP-nek elég 5 percenként változtatni a kulcson, a betörni szándékozó már kezdheti is elölről munkáját, sőt a TKIP adatcsomagonként is képes új kulcsot generálni.[19]

A WPA két működési módban alkalmazható. Otthoni felhasználóként a vezeték nélküli AP beállításánál a WPA-PSK (Wireless Protected Access – Preshared Key) beállítást érdemes választani. a WPA-PSK-nak egy jelszóra van szüksége, ebből áll elő a hozzáférési pont kódolási kulcsa.[20] Ez első látásra megegyezik a WEP módszerével, a WPA azonban a kapcsolódást követően folyamatosan változtatja a titkos kulcsot, így szinte lehetetlen az éppen érvényben lévőt megfejteni. Újabb

[17] Institute of Electrical and Electronic Engineers

[18] http://hu.wikipedia.org/wiki/WEP - Letöltve: 2019.05.30.

[19] http://torpospapa.weboldala.net/vezetek_nelkuli_halozat_otthon_-_ii.html - Letöltve: 2011.11.18.

[20] Andrew Conry - Murray, Vincent Weafer: Internetes biztonság otthoni felhasználóknak, Kiskapu Kiadó, Budapest, 2006., 161. oldal

kapcsolódás esetén ismét az eredeti kulcsot kell megadni, tehát csak arra kell figyelnünk, hogy titkos kulcsunkat senki ne ismerje meg rajtunk kívül.

A WPA másik működési módja az úgynevezett Enterprise mód, amely nagyvállalatok számára nyújt biztonságos megoldást. Otthoni alkalmazása körülményes. Ez a mód az EAP -ot (Extensible Authentication Protokol) használja, amellyel kiterjeszthető a hitelesítés, pl. egy felhasználó a vállalati azonosító adataival lép be valójában a vezeték nélküli hálózatba, így, gyakorlatilag, dupla hitelesítésen megy át a felhasználó. Az Enterprise mode továbbá alkalmas többszintű felhasználói jogosultság kezelésére is, azaz (egyszerűen fogalmazva) meghatározható, hogy a hálózaton ki milyen erőforrásokat érhet el, például ki férhet hozzá csak az internethez és ki férhet hozzá egyéb információkhoz is.

A WPA2 már a 802.11i biztonsági szabvány végelegesítése után jött létre, amely annyiban különbözik a WPA-tól, hogy erősebb kódolást használ és kötelezően az AES algoritmussal titkosít.

Amennyiben titkosítjuk vezeték nélküli hozzáférési pontunk forgalmát, a külső támadó már csak kódolt adatokat lát (lásd 5. ábra). Vessük össze az előző ábrán látottakkal!

No	Protocol	Src MAC	Dest MAC	Src IP	Dest IP	Src Port
1	MNGT/BEAC...	D-Link:B2:22:A4	Broadcast	? N/A	? N/A	N/A
2	MNGT/BEAC...	D-Link:B2:22:A4	Broadcast	? N/A	? N/A	N/A
3	MNGT/BEAC...	06:22:B0:B2:22:...	Broadcast	? N/A	? N/A	N/A
4	MNGT/BEAC...	06:22:B0:B2:22:...	Broadcast	? N/A	? N/A	N/A
5	MNGT/BEAC...	D-Link:B2:22:A4	Broadcast	? N/A	? N/A	N/A

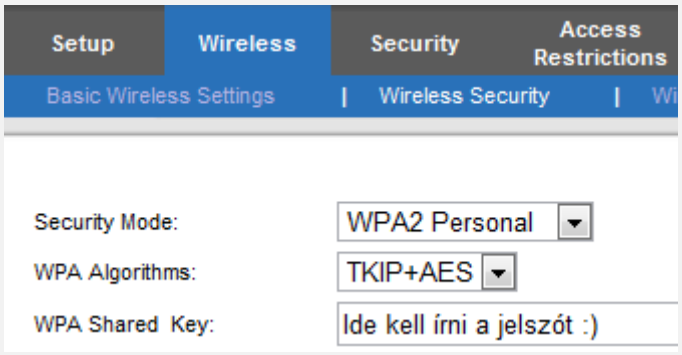
5. ábra Kódolt vezeték nélküli hálózat „látványa”

Amikor új vezeték nélküli routert vásárolunk, és beüzemelem, néhány dolgot érdemes figyelembe venni[21]:

- A router neve gyári
- A router jelszava gyári
- A router IP-címe gyári
- A router SSID[22]-ja gyári
- A router WiFi interfésze titkosítatlan, azaz nyílt
- vagy ha mégis titkosított, akkor gyári jelszóval van ellátva!

A router MAC címéből ki lehet találni, hogy melyik cég gyártotta a routert és innentől kezdve a világhálóról meg lehet tudni bármelyik routernek a gyári adatait. Tehát ezeket az adatokat érdemes a beüzemelést követően azonnal megváltoztatni. Fontos, hogy a router biztonsági beállításainál a WPA2-PSK-t vagy a WPA2-PSK+AES-t válasszuk (lásd 6. ábra)! Természetesen, a hozzáférési pont jelszavánál vegyük figyelembe a jelszavak biztonságáról korábba tanultakat!

[21] Szentgyörgyi Attila: WiFi hálózatok biztonsági kérdései, http://hte.tmit.bme.hu/root/club_ppt/201005/eloadas_szgyi_wifi_hte.pdf - Letöltve: 2019.05.30.
[22] Ez a vezeték nélküli hozzáférési pont neve



6. ábra Vezeték nélküli router helyes beállítása

Azért is érdemes a WPA2-t használni, ugyanis 2009-ben japán tudósok feltörték a WPA-TKIP titkosítását.[23]

Vannak olyan biztonsági lehetőségek, amelyeket ma már könnyű kijátszani:

- Kiszűrjük azokat a MAC címeket, amelyek hozzáférhetnek a hálózathoz
  - A MAC címet lehet klónozni, átállítani, illetve a hálózatot figyelve könnyű kideríteni, melyek a „legitim" MAC címek, aztán már csak meg kell várni, míg a legitim felhasználó eltűnik az éterből…
- Elrejtjük a hozzáférési pont nevét (SSID)
  - ha valaki kommunikál, az SSID már lehallgatható

Sok negatív következménnyel kell számolnia annak, akinek rákapcsolódnak a hálózatára:

- hozzáférnek a belső hálózathoz,
- operációs rendszer biztonsági réseit kihasználva adatot lehet lopni,
- kéretlen leveleket (spam) küldhetnek a hálózatból, Internetes bűncselekményeket hajthatnak végre, és a nyomok a feltört hálózathoz fognak vezetni,
- sávszélességet foglalnak, így lassabb lesz a hálózat,
- egyéb illegális tevékenységet végezhetnek mindenféle kockázat nélkül,
- Németországban már pénzbüntetés jár a nem védett WiFi hálózatért.[24]

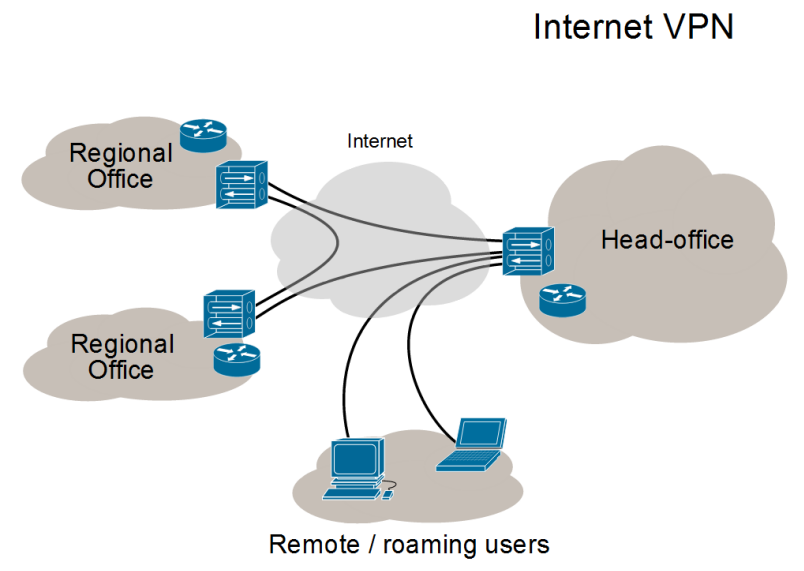
Mivel az otthoni hozzáférési pontok általában nem naplóznak, jó eséllyel nem lehet megtalálni azt, aki betört az otthoni hálózatunkba.

[23] Index: Egy perc alatt feltörhető a wifi: http://index.hu/tech/2009/08/28/egy_perc_alatt_feltorheto_a_wifi - Letöltve: 2019.05.30.
[24] Szentgyörgyi Attila: WiFi hálózatok biztonsági kérdései, http://hte.tmit.bme.hu/root/club_ppt/201005/eloadas_szgyi_wifi_hte.pdf - Letöltve: 2019.05.30.

Amennyiben nincs más lehetőségünk, mint nyílt vezeték nélküli hálózaton barangolni vagy egyszerűen kódoltan szeretnénk az „éterbe” küldeni az adatfolyamunkat, jó megoldás a virtuális magánhálózat használata.

A virtuális magánhálózat (Virtual Private Network, VPN) egy számítógép hálózat fölött kiépített másik hálózat. „Magán” jellegét az adja, hogy a VPN-en keresztülmenő adatok nem láthatók az eredeti hálózaton, mivel titkosított adatcsomagokba vannak becsomagolva. A titkosítás általánosan használt szolgáltatása a VPN-nek, de titkosítás nélkül is használható, a különböző adatfolyamok elkülönítésére, vagy a hálózat logikai felépítésének egyszerűsítésére.[25]

A VPN-t gyakran arra használják, hogy a munkatársak távolról hozzáférjenek munkahelyük hálózatához. Az Interneten keresztül biztonságos csatorna építhető ki a munkahelyen kívüli számítógép és a vállalat központjában működő VPN forgalomirányító között. Így bár a felhasználó fizikailag távol van, logikailag a vállalati hálózatban lesz benne a gépe (lásd 7. ábra).

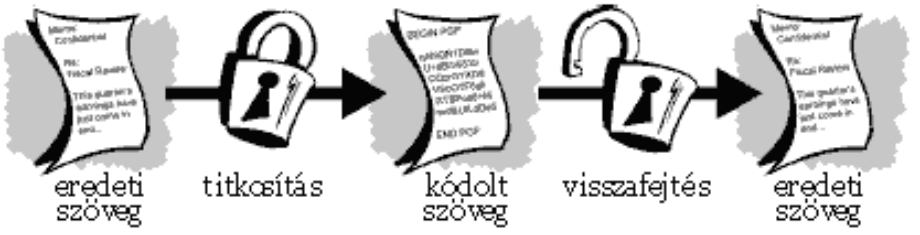


7. ábra Virtuális magánhálózat[26]

3.2 HTTP vs. HTTPS

Napjainkban két fajta titkosítási módszert alkalmaznak: a szimmetrikus kulcsú és az aszimmetrikus kulcsú titkosítást. A titkosítás olyan matematikai eljárás, melynek során egy üzenetet aképpen változtatunk meg felismerhetetlenül, hogy abból az eredeti üzenet csak valamilyen, kizárólag a küldő és a címzett által ismert eljárás segítségével fejthető vissza.[27] (Lásd: 8. ábra)

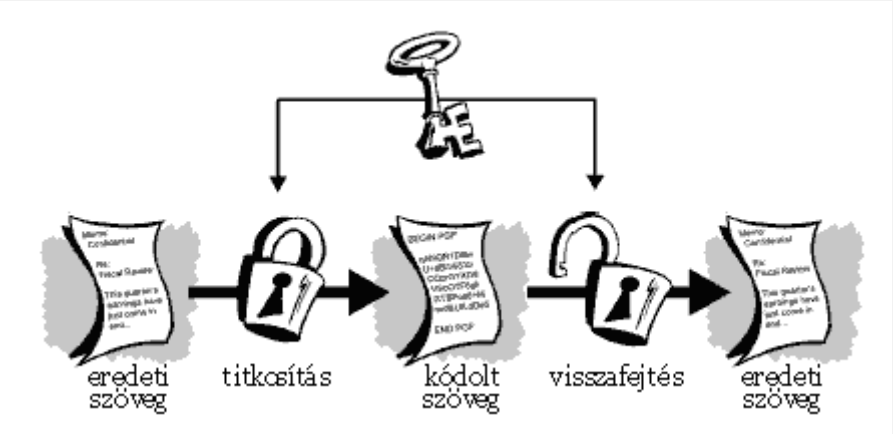
[25] http://hu.wikipedia.org/wiki/Virtu%C3%A1lis_mag%C3%A1nh%C3%A1l%C3%B3zat – Letöltve 2019.05.30.
[26] http://hu.wikipedia.org/wiki/Virtu%C3%A1lis_mag%C3%A1nh%C3%A1l%C3%B3zat – Letöltve 2019.05.30.
[27] http://www.agr.unideb.hu/~agocs/informatics/05_h_ecdl/ECDLweb/ecdlweb.uw.hu/m7-15.html – Letöltve: 2019.05.30.



8. ábra Titkosítás[28]

A titkosítás és visszafejtés során használt eljárás két részből áll: az egyik a titkosító/visszafejtő algoritmus (cipher), a másik pedig ennek az algoritmusnak egy vagy több paramétere, a kulcs (key). A művelet során a titkosító algoritmusnak két bemenete van: a titkosítandó adat és a kulcs, az eljárás kimenete pedig a titkosított információ. A visszafejtésnél ez utóbbi és a kulcs lesz a bemenet, a visszafejtett szöveg pedig a kimenet. Az algoritmus/kulcs jellege alapján különböztetjük meg a szimmetrikus kulcsú, illetve az aszimmetrikus, vagy más néven nyilvános kulcsú (public key) titkosítási eljárásokat.

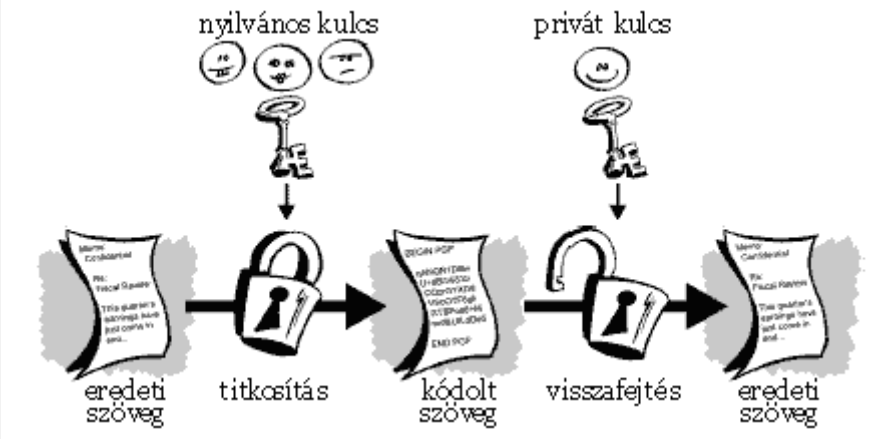
A szimmetrikus titkosításnál a kódoláshoz és a visszafejtéshez használt kulcs megegyezik, vagy egyik könnyen kiszámolható a másikból. (Lásd: 9. ábra) Ilyen algoritmusokra példa a DES, Triple-DES, AES (Rijndael), Blowfish, CAST, IDEA, Twofish, MARS.



9. ábra Szimmetrikus titkosítás[29]

Mint láttuk, a szimmetrikus eljárás gyenge pontja a titkosítás kulcsa, amit valamilyen megbízható módon kell a címzettel tudatnunk. Ezt a problémát a nyilvános kulcsú titkosító algoritmusok oldják meg, melyek egy összetartozó kulcspárt használnak. Az egyik neve privát, vagy más néven titkos kulcs (private key), ezt - mint a neve is mutatja - titokban tartjuk. A másik, nyilvános kulcsot (public key) pedig szabadon elérhetővé tesszük bárki számára. (Lásd 10. ábra)

[28] http://www.agr.unideb.hu/~agocs/informatics/05_h_ecdl/ECDLweb/ecdlweb.uw.hu/m7titk1.gif - Letöltve: 2019.05.30.
[29] http://www.agr.unideb.hu/~agocs/informatics/05_h_ecdl/ECDLweb/ecdlweb.uw.hu/m7titk2.gif - Letöltve: 2019.05.30.



10. ábra Aszimmetrikus titkosítás[30]

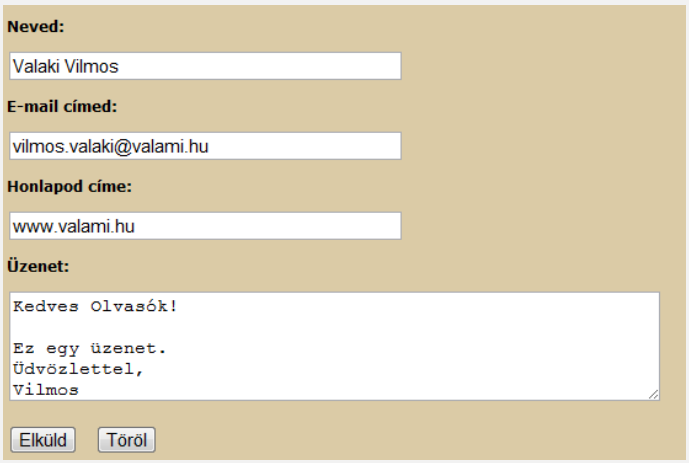
Fontos, hogy a privát kulcsból könnyen elő lehet állítani a nyilvános kulcsot, azonban ez fordítva már nem, vagy nagyon nehezen lehetséges. Ez tehát azt jelenti, hogy a kellően biztonságosnak ítélt titkosítási eljárással létrehozott rejtjelezett szöveg visszafejtése a jelenleg elérhető komputeres számítási kapacitással legalább néhány emberöltőig eltartana. Legismertebb algoritmusok: Diffie-Hellmann, RSA, DSA.

A HTTP (HyperText Transfer Protocol) a világháló általános átviteli protokollja, egy kérés-válasz alapú protokoll kliensek és szerverek között.[31] A kommunikációt mindig a kliens kezdeményezi (a mi szempontunkból nézve ez általában a számítógépünk webböngészője). Amikor beírjuk a http://valami.hu címet a böngészőprogramunkba, akkor ezt a protokollt használjuk. Ezen lépés után a kapcsolat felépítése a szerverrel úgy történik, hogy egy TCP-összeköttetés (Transmission Control Protocol) jön létre a kiszolgáló gépének 80-as portjával.

A HTTP 1.0-ban az összeköttetés kiépítése után csak egyetlen kérést lehetett elküldeni, amire csal egyetlen válasz érkezhetett. Ezután a TCP-összeköttetést lebontották a felek. Ez teljesen meg is felelt az akkori oldalaknál (a HTTP 1.0 1990-ben jött létre), azonban az új, több média adatot tartalmazó (pl. képek) oldalaknál ez már nem volt elégséges megoldás. Ez vezetett a HTTP 1.1-hez, ami már támogatja a tartós kapcsolatokat. Ezáltal lehetővé vált az, hogy egy kiépített TCP összeköttetésen belül több kérést küldjünk el egymás után, és ezekre válaszokat kapjunk. Ezzel jelentősen csökkenteni lehet a TCP-re eső terhelést (és az oldalak betöltési idejét).

Az egyik fontos HTTP művelet a GET, amely egy weboldal letöltését kezdeményezi. Amikor a HTTP protokollt használjuk, egyáltalán nem vagyunk biztonságban, ugyanis a GET által lekért adatokat bárki elolvashatja, aki az átvitel közben hozzáfér. A 11. ábra egy adatbekérő honlap részletét tartalmazza (ez akár lehetne egy webes e-mail kliens is). A 12. ábrán látható, hogy a kommunikáció olvasható az azt lehallgatók számára, így hozzájuthatnak olyan személyes adatokhoz, mint pl. az e-mail cím.

[30] http://www.agr.unideb.hu/~agocs/informatics/05_h_ecdl/ECDLweb/ecdlweb.uw.hu/m7titk3.gif - Letöltve: 2019.05.30.
[31] http://iesb.hu/logikai-biztonsag/protokollok-ftpsftp-http-https-ssl – Letöltve: 2011.11.24.



11. ábra Egy adatbekérő űrlap

```
Line-based text data: application/x-www-form-urlencoded
  nev=Valaki+Vilmos&e-mail=vilmos.valaki%40valami.hu&honlap=www.valami.hu&uzenet=Kedves+Olvas%F3k%21%0D
```

12. ábra Olvashatóak az adatok HTTP kapcsolaton keresztül

Ezen hiba elhárítására lett bevezetve a HTTPS (Hypertext Transfer Protocol over SSL) protokollt, ami szintaktikailag majdnem teljesen megegyezik a HTTP-vel (a 80-as port helyett a 443-ast használja), azonban jelzi a webszervernek hogy az SSL réteget is használni kell az adatátvitel során. Ez a megoldás akkor is működik, ha csak az egyik oldal hitelesített. Így van ez a HTTP protokoll esetében is (általában csak a szerver hitelesített, a böngésző nem).

Az előbb megemlített SSL (Secure Socket Layer – biztonságos csatlakozóréteg) egy protokoll réteg, amely a TCP/IP rétege és a HTTP rétege között helyezkedik el. Böngészésnél az SSL teszi lehetővé a biztonságos kommunikációt a böngésző és a webszerver között. A hitelesítéshez digitálisan aláírt tanúsítványokat használ, a kommunikáció titkosítva zajlik. Az SSL kapcsolat-felépítés során a böngésző és a szerver közösen megegyeznek egy kulcsban. Ez általában egy véletlenszerű számsorozat. Ebből generálják azután – az egy kapcsolat erejéig használatos – kulcsot, és ezt használják valamely szimmetrikus titkosító algoritmussal (pl. DES, AES).[32]

```
Encrypted Application Data: 8e2b7d9d20121849f82965f551711155a8411c
```

13. ábra HTTPS kapcsolaton keresztül már kódolt az üzenet

A másik protokoll, amelyet az SSL utódjának is nevezek, a TLS (Transport Layer Security). A protokoll elsődleges célja a titkosság és az adatintegritás biztosítása a két egymással kommunikáló alkalmazás között.[33] A kapcsolódás azzal indul, hogy a kliens egy TLS-el ellátott szerverhez kérelmet küldve próbál biztonságos kapcsolatot létesíteni, és egy listát biztosít a szerver számára a felhasználható kriptográfiai algoritmusokkal és hash függvényekkel. Majd ebből a listából a szerver kiválasztja a legerősebbet, azaz a legnehezebben feltörhetőet. Aztán a szerver elküldi a digitális aláírását, ami a szerver nevéből, egy tanúsítványból és a szerver nyilvános kulcsából áll. A kliens ezután már képes csatlakozni, és elkészít munkafolyamat-azonosító kulcsot (session key). Egy ilyen kulcs előállításához a kliens vesz egy véletlen számot, amit titkosít a szerver nyilvános kulcsával együtt és ennek eredményét visszaküldi a szerver számára, amit kizárólag a szerver képes dekódolni a titkos kulcsa segítségével.

[32] http://iesb.hu/logikai-biztonsag/protokollok-ftpsftp-http-https-ssl – Letöltve: 2011.11.24.
[33] http://wiki.hup.hu/index.php/TLS - Letöltve: 2019.05.30.

3.3 Biztonságos elektronikus levelezés

Az elektronikus levelezést széles körben alkalmazzák a hivatalos kommunikáció során – már csak azért is, mert ezzel sok papírt és pénzt lehet megtakarítani. Az elektronikus üzenetküldés, az e-mail, azonnali üzenetküldés, vagy az on-line konferenciák egyre fontosabb szerepet játszanak az üzleti információcserében. Az elektronikus üzenetküldésnek a papír alapú adatközléstől jelentősen eltérő kockázatai vannak. A KIB 25. ajánlása a következő kockázatokat sorolja fel:[34]

a) Az üzenetek illetéktelen elérésének vagy módosításának, illetve a szolgáltatás megtagadásának veszélye.
b) Emberi hibákból eredő veszélyeztető tényezők, például rossz címzés vagy irányítás.
c) Bizalmas adatok továbbításának lehetősége és ennek veszélyei, pl. nem titkosított kapcsolat használata.
d) A feladó és címzett hitelesítési problémák (könnyű a feladó e-mail címét meghamisítani), illetve a levél átvételének bizonyítása.
e) A kívülről hozzáférhető címjegyzékek tartalmával való visszaélési lehetőségek.
f) Távolról bejelentkező felhasználó biztonsági problémái.
g) Rosszindulatú program forrása lehet az elektronikus üzenet: vagy az üzenet csatolmánya, vagy maga az üzenet, ha az html-ben készült, ugyanis ilyenkor rosszindulatú kódot lehet beleírni.

A nem titkosított kapcsolat használatának veszélyeiről már szó volt a HTTP-protokoll kapcsán. A levelezés azért érzékenyebb, mert minden egyes kapcsolódáskor, azaz, a levelek fogadásakor és elküldésekor hitelesítés történik és a hitelesítés összes információja (tehát a jelszó is) – nem titkosított kapcsolat esetén – olvasható a hálózaton (lásd 34. ábra). Ilyen protokoll a POP3 (Post Office Protocol version 3) protokoll, melynek segítségével az e-mail kliensek egy meglévő TCP/IP kapcsolaton keresztül letölthetik az elektronikus leveleket a kiszolgálóról.

No.	r	Source	Destination	Protocol	Info
1	(	CHADWICK	www.packet-	TCP	2232 > pop3 [SYN] Seq=4110545907 Ack=0 Win=
2	(	www.packet-	CHADWICK	TCP	pop3 > 2232 [SYN, ACK] Seq=1552009928 Ack=4
3	(	CHADWICK	www.packet-	TCP	2232 > pop3 [ACK] Seq=4110545908 Ack=155200
4	(	www.packet-	CHADWICK	POP	Response: +OK POP3 [161.58.73.170] v2000.70
5	(	CHADWICK	www.packet-	POP	Request: USER lchappell
6	(	www.packet-	CHADWICK	TCP	pop3 > 2232 [ACK] Seq=1552009977 Ack=411054
7	(	www.packet-	CHADWICK	POP	Response: +OK User name accepted, password
8	(	CHADWICK	www.packet-	POP	Request: PASS seetheCleartextpassword?
9	(	www.packet-	CHADWICK	TCP	pop3 > 2232 [ACK] Seq=1552010018 Ack=411054
10	3	www.packet-	CHADWICK	POP	Response: -ERR Bad login
11	3	CHADWICK	www.packet-	TCP	2232 > pop3 [FIN, ACK] Seq=4110545955 Ack=1
12	3	www.packet-	CHADWICK	TCP	pop3 > 2232 [ACK] Seq=1552010034 Ack=411054
13	3	www.packet-	CHADWICK	TCP	pop3 > 2232 [FIN, ACK] Seq=1552010034 Ack=4
14	3	CHADWICK	www.packet-	TCP	2232 > pop3 [ACK] Seq=4110545956 Ack=155201

[34] A KIB 25. számú ajánlása.

14. ábra A 8. csomagnál olvasható a jelszó[35]

A következő védelmi módszereket alkalmazhatjuk elektronikus leveleink biztonságának megőrzése érdekében:[36]

Az egyik védekezési módszer a levelek titkosítása, rejtjelezése. Ilyenkor a lehallgatás ellen szeretnénk védekezni, tehát, még mielőtt elhagyja a számítógépünket a levél, már kódolva kell lennie és majd a fogadó félnek a saját gépén kell visszafejtenie a levelet. Az a cél, hogy a külvilág mindenképp a kódolt levelet „lássa". Titkosítási módszerként olyan algoritmust kell használni, ami garantálja azt, hogy a levelet csak a címzett tudja dekódolni és elolvasni. Ezeknek előfeltétele az, hogy a küldő és a címzett számítógépe biztonságos, „tiszta" legyen. Ezt az állapotot a korábban tárgyalt antivírus és tűzfal programokkal érhetjük el.

A levelek titkosítására a legegyszerűbb mód titkosított kapcsolatot használni a levél küldésénél és fogadásánál. Itt a kapcsolat a korábban említett TLS vagy SSL protokollt használja.

A másik védelmi módszer a levelek ellátása elektronikus aláírással, amellyel két veszélyforrás ellen védekezhetünk: az elektronikus levelek illetéktelen módosítása a kézbesítés során, illetve a levelek vagy azok küldőjének hamisítása. A digitális aláírás garantálja a levél tartalmi hitelességét és a küldő fél személyazonosságát. Az elektronikus aláírástól elvárjuk, hogy legyen egyedi és személyhez köthető (hasonlóan a hagyományos aláíráshoz), ne lehessen hamisítani, szorosan kötődjön az elektronikus üzenethez, dokumentumhoz (az üzenet megváltoztatása esetén veszítse érvényét), ne lehessen hitelesen másolni (tehát egyik dokumentumról a másikra átrakni úgy, hogy a másik is hitelesen aláírt dokumentum legyen), illetve, hogy bárki ellenőrizni tudja a hitelességét.

A harmadik védelmi módszer a levelek tartalmán keresztül indított támadások (vírusok, férgek, rosszindulatú programok) ellen nyújt segítséget. Egyrészt ismét a korábban említett vírusirtó és tűzfal programok segítenek, illetve minden levelező programban és/vagy antivírus programban be lehet állítani, hogy a html-ben kapott leveleket mindig szövegesen jelenjenek meg, ugyanis így az esetleges rosszindulatú kód nem fog lefutni. Ilyenkor a html megjelenítését kell letiltani. Ekkor azért fog a levelünk mégis helyesen megjelenni, mert a levél törzsében mindig tárolódik az üzenet szöveges változata. Ezek mellett sose indítsunk el csatolásként kapott futtatható programot, amelynek eredetéről és ártalmatlanságáról nem győződtünk meg.

3.4 Jelszóhasználat

A logikai védelem egyik legfontosabb és legtöbb veszélyforrást hordozó része a jelszó-rendszer. A jelszavas hitelesítés célja, hogy belépni szándékozó meggyőzze a rendszert, hogy jogosult a belépésre, tehát a belépő bizonyít, a rendszer pedig ellenőriz.[37] A jelszavas védelem két részből áll. Időben az első a bejelentkezési azonosító (logon id, felhasználónév) megadása. Ebben a fázisban a belépni szándékozó állít magáról, a saját személyéről valamit: egyrészt tudja a felhasználónevet, másrészt azt állítja, hogy ő egy olyan személy, aki jogosult a rendszer használatához, az adatok hozzáféréséhez. Ebben a fázisban történhet meg annak a végpontnak az azonosítása is, ahonnan a bejelentkezést kezdeményezik.

A jelszavas védelem időben második része a hitelesítés. Itt a belépni szándékozónak be kell bizonyítania, hogy ő valóban az, akinek az első fázisban mondta magát. Ez többféle módon, egy,

[35] http://support.novell.com/techcenter/articles/img/nc20042004_05tt5_01.gif - Letöltve: 2019.05.30.

[36] Nagy Sándor: Elektronikus leveleink védelme, ComputerBooks Kiadó, Budapest, 2005. 63-65. oldal

[37] Horváth László, dr. Lukács György, dr. Tuzson Tibor, Vasvári György: Informatikai biztonsági rendszerek c. könyvében található, BMF Kandó Kálmán Villamosmérnöki Kar, Budapest, 2001., 93. oldal

vagy több különböző fajta jelszó megadásával történhet. Ebben a fázisban a rendszer ellenőrző lép funkciója előtérbe és a megadott jelszót összehasonlítja az adatbázisában tároltakkal. Ha a belépni szándékozó által megadott jelszó létezik az adatbázisban, akkor megtörtént a hitelesítés, hiszen a belépő olyan személynek mondta magát, aki a belépésre jogosult és megadta a szükséges jelszót, vagy jelszavakat is.[38]

A következő alapelveket szükséges betartani a jelszavakkal kapcsolatban, a KIB 25. ajánlása szerint:[39]

a) A felhasználónak kötelezően alá kell írnia egy nyilatkozatot, melyben felelősséget vállal személyes, (esetleg csoportos jelszavainak) bizalmas kezelésére.
b) Belépéskor megkapott, illetve – például elfelejtés esetén – ideiglenes jelszó átadása csak biztonságos csatornán történhet, a felhasználó előzetes – például személyes – azonosítása után. Az ideiglenes jelszavak csak az adott munkanap végéig lehetnek érvényesek, megváltoztatásuk kötelező.
c) **Telefonon, illetve elektronikusan aláíratlan e-mailen-en történő kérésre jelszóváltoztatás nem kezdeményezhető**.
d) A felhasználónak minden esetben vissza kell igazolnia új jelszavának az átvételét ellenőrizhető úton (például e-mail), vagy személyesen.
e) A jelszónak minden felhasználó számára szabadon megváltoztathatónak kell lennie.
f) A felhasználói jelszavakkal kapcsolatban (amennyiben az adott rendszerben erre lehetőség van) biztosítani kell a következő követelmények teljesülését:
    a. minimális jelszóhossz megadása
    b. a jelszó egyediségét (történeti tárolás), tehát, jelszóváltoztatás esetén nem lehet már korábban használt jelszót felhasználni
    c. a központi jelszó megadás utáni első bejelentkezéskor a kötelező jelszó cseréjét,
    d. a jelszó maximális élettartamát, tehát mennyi az a legtöbb idő, amely után már mindenképp meg kell változtatni a jelszót
    e. a jelszó minimális élettartamát,
    f. a jelszó zárolását
    g. a jelszó képzési szabályainak megváltoztatását, pl. kell-e kisbetű, nagybetű, szám, nem alfanumerikus karakter, stb.
g) A számítógépes rendszerekben a jelszavakat **tilos nyílt formában tárolni**. A jelszófájlokat megfelelő rejtjelezési védelemmel kell ellátni.
h) A jelszavakat vagy a jelszófájlokat a hálózaton nyílt, olvasható formában továbbítani tilos.

Jelszóhasználati szabályok:[40]

a) A jelszavakat bizalmasan kell kezelni

[38] Törley Gábor: Adatbiztonság a közigazgatásban, FÁMA Zrt. – Nemzeti Közszolgálati és Tankönyv Kiadó Zrt. ISBN 978-615-5344-05-3 Budapest, 2013. (elektronikus jegyzet), https://ludita.uni-nke.hu/repozitorium/handle/11410/10571 - Letöltve: 2019.05.30.

[39] A KIB 25. számú ajánlása, 161-162. oldal.

[40] A KIB 25. számú ajánlása, 164-165. oldal.

b) A jelszavakat nem szabad papíron tárolni (a biztonsági másolat kivételével, viszont azt megfelelően védett helyen, pl. széfben kell őrizni). Ha ez elkerülhetetlen, pl. a kezdeti jelszó esetén, akkor gondoskodni kell a zárt borítékban történő biztonságos tárolásáról.
c) Amennyiben felmerül a gyanú a felhasználóban, hogy jelszavát feltörték, azonnal le kell cserélnie
d) A jelszó hossza **haladja meg a 8 karaktert**, ne tartalmazzon egymást követő azonos karaktereket, vagy számokat, mert ez meglehetősen megkönnyíti a feltörhetőséget, pl. a brute force támadások esetében.
e) Kívülállók ne tudják könnyen kitalálni a jelszót, ne tartalmazzon a felhasználó személyére utaló információkat (például neveket, telefonszámokat, születési dátumokat), összefüggő szövegként ne legyen olvasható, ne legyen értelmes. Az érthetőség megkönnyíti a jelszó feltörését az úgynevezett szótár alapú támadások esetén.
f) A legnagyobb biztonságot a felhasználóhoz nem köthető, kis- és nagybetűkből és számokból álló, véletlenszerűen összeállított jelszavak garantálják.
g) A felhasználói jelszavakat rendszeresen (kb. 3 havonta) cserélni kell. Valamikor a rendszer automatikusan kötelezővé teszi. A korábbi jelszavak ciklikus vagy ismételt használatát kerülni kell.
h) A kiemelt jogosultságú felhasználók esetén (rendszergazda, szoftvertelepítő szakember) sokkal gyakrabban kell cserélni a jelszavakat.
i) Első bejelentkezéskor kötelezően le kell cserélni a kezdeti jelszót.
j) A biztonságos jelszóhasznált szabályait minden felhasználónak oktatni kell.
k) A felhasználóknak tudniuk kell, hogy minden olyan művelet, amely melyeket az ő azonosítójával és jelszavával mások hajtanak végre, az informatikai rendszer az ő „terhére" könyveli el, és azokért személyesen felel.

Jelszavak típusai: három típust különböztetünk meg: a többször használatos jelszót, az egyszer használatos jelszót, illetve a biometrikus jelszót.

A *többször használatos jelszó* valamilyen titkos információ tudására épül. Ez tehát a „mit tudsz?" elvén alapul[41]. Gyakorlatilag, a legtöbb esetben, ilyeneket használunk az e-mail fiókunkhoz, a számítógépünkbe való belépéskor, stb.

Miért érdemes olyan jelszavakat használni, amelyik kis- és nagybetűkből és számokból állnak, véletlenszerűen összekeverve? Az angol abc 25 kisbetűjét, 25 nagybetűjét, valamint a tízes számrendszer számjegyeit (0-9-ig), azaz összesen 60 karaktert figyelembe véve a lehetséges változatok száma igen magas, így brute force támadással nagyon sok időbe telnek feltörni a jelszót.

A brute force típusú jelszó-feltöréseket további intézkedésekkel szokták megnehezíteni. Ilyen védelmi intézkedés például az, hogy néhány – általában 3, 4, vagy 5 – rosszul megadott jelszó után megadott időre (30 perc, 60, perc, stb.), vagy végleg kitiltja a felhasználót a rendszer. A másik védelmi intézkedés a jelszó hossza. Egy hosszú jelszót ugyanis aránytalanul tovább tart feltörni, mint egy rövidet.

[41] Horváth László, dr. Lukács György, dr. Tuzson Tibor, Vasvári György: Informatikai biztonsági rendszerek, BMF Kandó Kálmán Villamosmérnöki Kar, Budapest, 2001., 94. oldal

Az *egyszer használatos jelszó* a „mi van a birtokodban?” elvén alapul[42]. Ez a jelszó a bejelentkezés folyamatában a felhasználói azonosító – és esetleg a többször használatos jelszó – helyes megadása után keletkezik. Ekkor a felhasználó birtokában van valamilyen algoritmus, amely segítségével a jelszót előállíthatja. Ez az algoritmus lehet pl. egy matematikai művelet is. A hitelesítés úgy történik, hogy a rendszer generál egy véletlen számot, amellyel el kell végezni az algoritmust, majd a belépni szándékozó válaszként visszaadja az algoritmus megoldását. A rendszer is megoldja az algoritmust és ha a felhasználó és a rendszer eredménye egyezik, akkor engedélyezésre kerül a belépés.

A *biometrikus jelszó* a „ki vagy?” elvén alapul. Ez alatt az ember fiziológiájából következő, a tényleges személyazonosságot igazoló egyedi azonosítókat értünk. Ilyen lehet például a hanglenyomat, az ujjlenyomat, a tenyérnyomat, a retina hártya mintázata, az íriszhártya mintázata, a DNS.

Azokban a rendszerekben, ahol biometrikus jelszavakat használnak, ilyen azonosításra általában csak az előző két azonosítási mód sikeressége után kerülhet sor[43].

Egyre több helyen lehet használni az ügynevezett két faktoros autentikációt. Ez a fajta módszer ötvözi a tudáson és a birtokláson alapuló jelszavak együttes használatát. Klasszikus példája a bakkártya. Ekkor a bakkártya jelenti a birtoklás alapú, míg a PIN-kód a tudás alapú hitelesítést. Valamilyen webes szolgáltatásba való belépés esetén a tudás alapú jelszavunkat követően egy újabb jelszót, általában egy számsort kér tőlünk a rendszer, amit vagy elküld a telefonunkra, vagy a telefonon futó hitelesítő alkalmazásból tudunk kinyerni. Így a tudás alapú jelszavunk önmagában nem lesz elég a hitelesítéshez.

Miért érdemes hosszú és bonyolult jelszót választani? Erre a választ az alábbi táblázat adja meg:

PASSWORD HACKING TIMES

LENGTH	LOWERCASE	+UPPERCASE	+NUMBERS & SYMBOLS
6 characters	10 minutes	10 hours	18 days
7 characters	4 hours	23 days	4 years
8 characters	4 days	3 years	463 years
9 characters	4 months	178 years	**44,530 years**

15. ábra Jelszavak feltörési ideje különböző paraméterek alapján[44]

Bonyolult és hosszú jelszavak esetén érdemes jelszószéfet használni.

[42] Horváth László, dr. Lukács György, dr. Tuzson Tibor, Vasvári György: Informatikai biztonsági rendszerek, BMF Kandó Kálmán Villamosmérnöki Kar, Budapest, 2001., 94. oldal

[43] Horváth László, dr. Lukács György, dr. Tuzson Tibor, Vasvári György: Informatikai biztonsági rendszerek, BMF Kandó Kálmán Villamosmérnöki Kar, Budapest, 2001., 95. oldal

[44] http://www.thesecuritysamurai.com/2012/01/12/in-this-edition-of-security-spot-new-year-new-password/ - Letöltve: 2019.05.30.

4. Közösségi hálózatok biztonságos használata

Érdemes beszélni korunk egyik legnépszerűbb böngészési célpontjairól, a közösségi oldalakról, amelyek közül a Facebook-ot fogom kiemelni.

4.1 Facebook és az adatvédelem

„Ingyenes és az is marad" – így fogadja a Facebook oldala a látogatókat. Ugyanezt kiírhatná a Google is. A tény az, hogy semmi sincs ingyen. A Facebook szolgáltatásaiért a személyes adatainkkal fizetünk.

A Facebook-nak több, mint egymilliárd felhasználója van, ezzel ők a világ egyik legnagyobb, nem állami adatkezelője. Hatalmas mennyiségű adatot kezelnek, az alapvető személyes adatoktól (pl. név, születési hely és idő) a különleges adatokig (pl. vallás, politikai nézetek) olyan információk tudhatóak meg a felhasználókról, amelyeket önként adnak meg, növelve hitelességüket. Ezen felül az ismerősökön keresztül olyan kapcsolati háló rajzolható fel, amelyek csak komoly nyomozások után lennének felderíthetőek, nem véletlen, hogy a világ minden országában, ahol a szolgáltatása jelen van, az állami titkosszolgálatok rendszeresen megkeresik és együttműködését kérik (vagy megkövetelik).[45]

Nem könnyű olyan szolgáltatást nyújtani, mely megfelel minden olyan ország jogrendszerének, ahol a Facebook szolgáltat, nem beszélve ezen adatvédelmi jogszabályok szigorodásáról (pl. a GDPR az EU-ban).

Mint minden közösségi hálózat, a Facebook is a felületén elhelyezett reklámokból él. Ahhoz, hogy a reklámok minél személyesebb módon jussanak el a célközönséghez, *„a Facebook programozói készítettek egy matematikai algoritmust, mely megvizsgálja a felhasználó személyes adatait és a nyilvánosságra hozott információkat …, mely alapján az oldal megpróbálja megjósolni, hogy mi iránt érdeklődik, a korábbi preferenciáit megvizsgálva. A megoldás ahhoz hasonló, amikor a rendszer meghatározza, hogy a hírfolyamra olyan ismerőseink hírei kerüljenek rá vagy kerüljenek előre[46], akikkel gyakrabban tartunk kapcsolatot."*[47]

Ezt az algoritmust „News Feed Ranking Algorithm"-nak hívják (hírfolyam rangsorolásáért felelős algoritmus), mely több, mint százezer körülményt vesz figyelembe a hírek rangsorolásánál. A legfontosabb fogalom az „Edge", mely alatt „minden felhasználói tevékenységet" értünk (például személyes adat felöltése, kommentelés, likeolás, kép feltöltése, ismeretség létrejötte). Az algoritmus működése: az „Edge-ek" összessége, melyek súlyozva vannak a „rokonság" (a hírt létrehozó és a felhasználó rokonsági foka, azaz mennyire közeli kapcsolatban vannak egymással), „fontosság" (adott tevékenységre fordított idő) és „aktualitás" (az adott hír frissessége) alapján.

Korábban szó volt a „háztartási kivétel"-ről, illetve a GDPR preambuluma[48] meghatározza annak alkalmazását a közösségi hálózatokra vonatkozóan, amely alapján személyes vagy otthoni tevékeny-

[45] Mészáros János: Adatvédelem a XXI. században és az internet világában, PhD értekezés, Szegedi Tudományegyetem, Állam- és Jogtudományi Kar, Szeged, 2017.

[46] „Facebook programmers have created a mathematical algorithm that will examine the types of posts a person has chosen to give prominent placement to on his or her profile.... Whether food, movies or exercises logged into Facebook, the site will try to predict what you're most passionate about based on past choices, similar to how the system determines its news feed based partly on the people you contact most often"

[47] Mark Milian (January 19, 2012). 60 apps launch with Facebook auto-share. CNN. http://www.cnn.com/2012/01/18/tech/social-media/facebook-actions-apps/index.html - Letöltve: 2019.05.28.

[48] Adatvédelmi rendelet preambulum 18.

ségnek minősül például a levelezés, a címtárolás, valamint az említett személyes és otthoni tevékenységek keretében végzett, közösségi hálózatokon történő kapcsolattartás és online tevékenységek.

A Facebook adatkezelései jelentős részéhez jogalapként az érintett hozzájárulását használja fel, azonban a hozzájárulás alapvető követelményei (önkéntesnek, határozottnak, megfelelő tájékoztatáson alapulónak és félreérthetetlennek kell lennie) nem érvényesülnek maradéktalanul. Az egyik legjelentősebb probléma a Facebook egyes adatkezeléseinél, hogy a felhasználónak nincsen kontrollja felettük, mivel a Facebook „mindent vagy semmit" választási lehetőséget kínál csupán az érintettnek, aki így kénytelen vagy elfogadni azokat, vagy a regisztrációval, felhasználással felhagyni.[49]

A „mindent vagy semmit" választási „lehetőség" az adatalany hozzájárulásával kapcsolatban vet fel kérdéseket, mivel elképzelhető olyan eset, hogy nincsen alternatívája a Facebooknak.

Az önkéntességgel kapcsolatban merülnek fel problémák, mert a Facebook szabályzatának az elfogadása a partnereire, valamint azok szolgáltatásaira (pl. beépülő modulok) is kiterjed, így a felhasználó „kénytelen" azoknak az adatkezeléseihez is hozzájárulni a közösségi hálózat használatáért cserébe.

A személyes adatokon felül az alábbi adatokat tárolja felhasználóiról a Facebook (a teljesség igénye nélkül):

- Jellemzők – például az operációs rendszer, a hardver verziója, az eszközbeállítások, fájl- és szoftvernevek és -típusok, akkumulátor és jelerősség, valamint készülékazonosítók.
- Az eszközök helye – akár konkrét földrajzi helyadatokkal, például GPS-, Bluetooth- vagy WiFi-jelek alapján.
- Az internetkapcsolatra vonatkozó adatok – például mobilszolgáltató vagy internetszolgáltató neve, a böngésző típusa, nyelve, az időzóna, a mobiltelefonszám és az IP-cím.

A GDPR alapján a célhoz kötöttség elvének **az adatkezelés minden szakaszában érvényesülnie kell**, és nem világos, hogy a Facebook szolgáltatásainak nyújtásához (a cél eléréséhez) miért szükséges a készülék azonosítók, akkumulátor erőssége, mobiltelefonszám és az IP-cím elmentése. Valószínűleg a reklámozás hatékonyabbá tételéhez kellenek. A Facebook esetében az adatgyűjtés és az adatok felhasználása sem felel meg a célhoz kötöttségnek. Az adatkezelési szabályzat sok esetben általánosan és homályosan fogalmaz:

„Gyűjtünk olyan tartalmakat és információkat is, amelyeket mások osztanak meg szolgáltatásaink használata során, köztük rólad szóló információkat is – például amikor téged ábrázoló fényképet osztanak meg, üzenetet küldenek neked, illetve feltöltik, szinkronizálják vagy importálják az elérhetőségi adataidat.

Rólad és a Facebookon vagy azon kívül folytatott tevékenységeidről adatokat kapunk külső partnerektől – például olyan esetben, amikor egy partnerrel közösen kínálunk szolgáltatásokat, vagy hirdetőktől kaphatunk adatokat arról, milyen élményeid voltak velük, illetve milyen módon léptél érintkezésbe velük."

[49] Van Alsenoy Brendan, Verdoodt Valerie, Heyman Rob, Wauters Ellen, Ausloos Jef, Acar Günes - From social media service to advertising network: a critical analysis of Facebook's Revised Policies and Terms, Research Unit KU Leuven Centre for IT & IP Law (CiTiP), 2015. 9-10. http://www.law.kuleuven.be/citip/en/news/item/facebooks-revised-policies-and-terms-v1-2.pdf - Letöltve: 2019.05.28.

A helymeghatározással kapcsolatos adatkezelések esetén szintén szükséges a felhasználó előzetes hozzájárulásának megszerzése, mivel azok különösen érzékeny információkat szolgáltathatnak az érintettről: kórház vagy templom rendszeres látogatása alapján az érintett vallása és betegsége(i) könnyen kideríthetőek. Korábban láttuk, hogy ezek az adatok különleges adatok így ezek kezelése csak akkor lehetséges a GDPR alapján, ha ahhoz az érintett kifejezett hozzájárulását adta a „konkrét célból" történő kezeléséhez.

A hozzájárulás akkor tekinthető érvényesnek, ha az érintett megfelelően tájékoztatva lett annak megadása előtt. Az informálás akkor tekinthető megfelelőnek, ha az részletes, és a felhasználó számára érthető. A Facebook esetében regisztráció során nemhogy nem kell „végig görgetnie" az érintettnek a szabályzatot a regisztrációhoz, még rákattintani sem szükséges: elég csupán kipipálnia egy négyzetet. Meg kell azonban említeni, hogy a Facebook a „Privacy Basics" alatt egy átlátható és könnyen érthető tájékoztatást biztosít az adatok megosztásáról, és arról, hogy egyes felhasználók milyen adatokat láthatnak egymásról, azonban arról nem tesz említést, és nem ad meg beállítást, hogy pontosan milyen adatokat láthatnak és gyűjthetnek a Facebook partnerei. Amennyiben az alapbeállítás a személyes adatok megosztása, és a felhasználó csupán utólagosan dönthet úgy, hogy nem engedélyezi azok kezelését, nem beszélhetünk a hozzájárulás félreérthetetlenségéről. Ez azt jelenti, hogy általában a felhasználó aktív magatartása szükséges ahhoz, hogy az információ csupán szűkebb kör részére kerüljön megosztásra, ugyanez igaz a viselkedésalapú reklámozás beállításaira is. Alapértelmezés szerint ez a lehetőség be van kapcsolva.

Létezik egy adatvédelmi irányzat, amit „privacy by default"-nak, magyarul alapértelmezett adatvédelemnek hívnak. Ennek *„lényege, hogy személyes adatok gyűjtésére, kezelésére, illetve feldolgozására csak és kizárólag az adatalany kifejezett kérésére kerülhet sor. Az adatkezelők alapvető, „alapértelmezett" (angolul: by default) hozzáállása az kell, hogy legyen, hogy minden körülmények között figyelembe veszik az adatvédelmi szempontokat és ezeknek megfelelően járnak el az adatkezelési műveletek során."*[50] A GDPR szerint ennek célja, *„hogy a személyes adatok alapértelmezés szerint a természetes személy beavatkozása nélkül ne válhassanak hozzáférhetővé meghatározatlan számú személy számára"*.[51] A Facebook akkor követné ezt az elvet, ha a lehető legszigorúbb adatvédelmi beállítások lennének az alapértelmezettek. Ma nem ez a helyzet.

A Facebook adatbiztonsági szempontból igen veszélyes terület, ugyanis emberi tulajdonságok előtérbe helyezésével el lehet érni, hogy önként osszunk meg olyan adatot, amit valójában nem adnánk ki. Az egyik legegyszerűbb módszere a Facebook-nak, hogy ki lehet fejezni a tetszésünket többek között emberek, hozzászólások, fényképek iránt. Általában minden ember örül annak, ha valamilyen hozzá kapcsolódó dologról pozitív véleménnyel vannak az ismerősei, barátai. Ilyen módon személyes közösségi élményt-érzést (vagy ehhez hasonlót) lehet elérni, így bátran megosztunk magunkról olyan adatokat, amelyeket, ha pl. egy ügyintézés adatvédelmi hibája miatt kerülne ki, perrel fenyegetnénk az adott intézményt.

Azt tapasztalom, hogy sok felhasználó nem böngészi végig az adatvédelmi beállításokat. itt lehet szabályozni, hogyan tartjuk a kapcsolatot ismerőseinkkel: kik láthatják az adatlapunkat, név vagy kapcsolat alapján; kik küldhetnek nekünk ismerősnek jelölést vagy üzenetet; kik tehetnek közzé az üzenőfalunkon.

Az egyik legfontosabb adatvédelmi beállítás, hogy kik láthatják az üzenőfalunkat, a hozzászólásainkat, a képeinket és az alapadatainkat. Ezeket igen jól lehet ma már differenciálni, ugyanis lehetőségünk van csoportokat létrehozni az ismerőseink között (pl. barátok, család, évfolyam, stb.), és külön be tudjuk akár azt is állítani, hogy az adott csoport mit láthat és nem láthat az adataink közül. Ugyanez az elv igaz az alkalmazásokra is. Érdemes egyik alkalmazásnak sem engedni, hogy automatikusan hozzászólásokat tehessen az üzenőfalunkra.

[50] NAIH adatvédelmi szótár: https://www.naih.hu/adatvedelmi-szotar.html – Letöltve: 2019.05.28.
[51] Adatvédelmi Rendelet, 25. cikk (2)

Mi történhet, ha nem figyelünk oda ezekre? Megtörtént eset, hogy egy Facebook felhasználó kiírta lelkesen az üzenőfalára, hogy vett egy plazmatelevíziót, majd megosztotta országgal-világgal, hogy elmegy két hétre nyaralni külföldre, végül arra ért haza, hogy valaki feltörte a lakását és elvitt „valamit".

Mobil alkalmazásokkal és a Check in szolgáltatással, gyakorlatilag, minden egyes hozzászólásunkhoz meg lehet adni, hogy hol is vagyunk, ilyen módon, egy külső megfigyelő végig tudná kísérni az egész életünket, szokásainkat. Biztos, hogy megéri ennyi személyes adatot rábízni a Facebook-ra és közönségére?

A Facebook adatvédelme messze nem működik tökéletesen. 2011 őszén 250 gigabájtnyi személyes adatot bányásztak ki a Facebook-ból amerikai tudósok.[52] A vizsgálathoz programokat, úgynevezett socialbotokat, úgy tervezték, hogy az valódi felhasználónak álcázza magát. A kísérletben 102 socialbot és 1 ember vett részt. Azt várták a kutatók, hogy a Facebook ki fogja szűrni ezeket a robotokat, azaz programokat. Nem így történt. Igazából csak húszat zárt ki a rendszerből a közösségi oldal, de azokat is csak azért, mert más felhasználók blokkolták, illetve spam-nek jelölték őket.

Ezek a robotok több, mint 3000, valószínűleg valódi emberi barátra tettek szert, és így az ő személyes adataikra is, illetve, mivel rengeteg felhasználó a barátaik barátaival is megosztja érzékeny adatait, így a robotoknak kb. 1 millió ember személyes adatait sikerült beszerezni. Ez olyan, mintha valaki minden második budapesti ember személyes adatait ismerné. Ezzel kapcsolatban az a rossz hír, hogy nem kell sok pénz ahhoz, hogy valaki egy ilyen robotot megvásároljon a feketepiacon.

A fent említett socialbotok nem tudtak volna ennyi adatot megszerezni, ha a felhasználók megfelelően kezelik az adatvédelmi beállításokat, így belátható, hogy adataink védelmének megőrzése érdekében szükség van arra, hogy a minimális láthatóság elvét alkalmazzuk. Tehát csak annyit lásson a Facebook profilomból, idővonalamból, tevékenységeimből a külvilág (beleértve magát a Facebook-ot is), amit feltétlenül szükséges.

4.2 Pszichológiai vetület - röviden

Az Index készített egy interjút – többek között – a mobilfüggőségről Tari Annamária pszichológussal 2018-ban[53]. Ennek főbb megállapításai:

- Gyorsaságot és azonnaliságot ad: az azonnali érzelmi szükséglet kielégítésének a lehetőségét adja. A gyerekek azt vonják le ebből, hogy a valóság is ilyen ha valami elromlott, ha valamit meguntam kilépek és majd újra próbálkozok. Nem tapasztalja meg, hogy amit akar, azt nem kapja meg azonnal. Az információs korban azonban a reakcióidőnk egyre rövidül, mert az eszközökkel eljött az azonnali érzelmi szükségletkielégítés folyamatos lehetősége.
- Valójában mindenki egyedül van, miközben azt hiszi, hogy nem: ül egyedül a képernyője mögött, nincs valódi együttes élmény. Komplett világot kínál a közösségi média és hihetetlen lehetőséget ahhoz, hogy egymás életét megfigyeljük.

[52] Yazan Boshmaf, Ildar Muslukhov, Konstantin Beznosov, and Matei Ripeanu. The socialbot network: when bots socialize for fame and money. In Proceedings of the 27th Annual Computer Security Applications Conference (ACSAC'11), December 2011.

[53] Index: Interjú Tari Annamáriával, https://index.hu/tech/2018/01/31/mobilfuggoseg_kozossegi_media_tari_annamaria_kiskamasz_gyerek_pszichologus_gyerekneveles_facebook - Letöltve: 2019.05.30.

- Jean Twenge kutatásai szerint a 8-12 éves korosztálynak olyan érzelmeket kell átélniük, amiket régebben felnőtt érzelmeknek hívtunk. A szorongáskapacitásunk azonban a biológiai életkorunkhoz kötött. Ha az online térben ilyen kihívások érik a gyereket, azt nem tudja elviselni, mert életkoránál fogva nincsenek meg az érzelmi eszközei a feldolgozásukhoz.
- Nagyobb a transzparencia. Az online világban történő kiközösítést, cukkolást, bullyinget - ami persze korábban is megvolt - most nem húsz ember látja, hallja az osztályteremben vagy az iskolai folyosón, hanem rögtön több száz. Ez a nagyfokú transzparencia megnöveli a szorongás mértékét.
- A valóság lassú és nehézkes. Az online világban ezek a fogalmak nem léteznek, minden azonnali, gyors, színes és vibráló, de ez nem a valóság. Az online és offline világból kibejáró gyerekek összekeverik a kettőt és a valóságtól is azt várják el, amit az online térben tapasztalnak.
- Nem tapasztalják meg, hogy ha valami rossz történik velük, akkor majd valamikor a közeljövőben meg tudják osztani az élményt másokkal, miután feldolgozták, de addig is, főleg gyerekkorban, néhány óra szükséges ehhez. Ezt holdingnak nevezi a pszichológia, azaz a tartalmazás képességének. Ez ahhoz kell, hogy felnőttként majd legyenek érzelmi stratégiák, amik a konfliktusmegoldáshoz, a problémakezeléshez, a szorongástűréshez vagy a stresszkezeléshez szükségesek. Régen ez a holding több óra volt, ma pár másodperc. A holdingot meg kell tanulni és azt csak a való életben lehet, mert a személyesség a szemtől szembeni kapcsolat a lényege.

5. Internetes zaklatás – Cyberbulliyng

Ebben a fejezetben érdemes tisztába tenni, hogy mi is az az iskolai bántalmazás (angolul bulliyng). *„Iskolai bántalmazásnak, más néven bullyingnek vagy mobbingnak nevezzük azt, ha valaki hosszabb időn át ismétlődően szándékosan bánt valakit/valakiket. Fontos jellemzője továbbá, hogy az áldozatok és az elkövetők között kiegyenlítetlenek az erőviszonyok. Tehát általában az idősebb a fiatalabbat, az erősebb a gyengébbet vagy az egészséges a fogyatékost bántalmazza."*[54] Ennek változatos formái lehetnek: pl. verbális, fizikai, érzelmi, szexuális. A gyakorlatban verésként, ütésként, rugdosódásként, kiközösítésként, molesztálásként, pletykálkodásként stb. jelenhet meg. A Cyberbulliyng a fenti bántalmazásnak az internetes megjelenése. Tehát a bántalmazás nem csak a fizikai térben történhet meg, hanem akár ez a kibertérben is folytatódhat.

A zaklatást definiálja a Bűntető Törvénykönyv is (Btk. 222. § (1)): *„Aki abból a célból, hogy mást megfélemlítsen, vagy más magánéletébe, illetve mindennapi életvitelébe önkényesen beavatkozzon, őt rendszeresen vagy*

[54] https://gyermekpszichologus.blog.hu/2011/08/18/bullying_avagy_az_iskolai_bantalmazasrol – Letöltve: 2019.05.17.

tartósan háborgatja, ha súlyosabb bűncselekmény nem valósul meg, vétség miatt egy évig terjedő szabadságvesztéssel büntetendő" Véleményem szerint a „háborgatás" szó túl enyhe kifejezés a zaklatás definiálására.

Fontos megjegyezni, hogy jelentős az átfedés az offline és az online bullying elkövetői és áldozatai között, de vannak különbségek: a cyberbullying érzelmileg megterhelőbb – koncentrált megaláztatás és szégyen, ugyanis

- nehezebb elmenekülni előle, nem ér véget az iskola kapujánál – ott kezdődik,
- abban a közegben zajlik, ahol a gyerekek a legtöbb időt töltik, ahol az egymás közti kommunikáció és szórakozás legnagyobb része zajlik,
- legtöbbször anonim, vagy álnéven történik, ellentétben a „klasszikus" bántalmazással
- nagyobb a „színtér" – online nyilvánosság, tehát nem „csak" egy osztály előtt történik

A cyberbullying legalább olyan veszélyes, mint a személyesen elkövetett, mert sokszor nem derül ki, hogy ki a zaklató, a névtelenség álarca mögött gyakran durvább tettekre vetemednek a bántalmazók, mint szemtől szemben

Főbb típusok:[55]

- **Flaming** („**lánghábor**ú") – durva és agresszív nyelvhasználatú online veszekedés, támadó jellegű hozzászólások küldése valakiről nyilvános fórumra.
- **Harrassment (zaklatás)** – zaklató, igaztalan online üzenetek küldése.
- **Denigration (befeketítés)** – a reputációt romboló rosszindulatú pletykák és rémhírek küldése, kiposztolása, terjesztése.
- **Exclusion (kiközösítés)** – online közösség tagjának kirekesztése a csoportból.
- **Impersonation (személyiséglopás)** – egy másik személy online profiljában jelenik meg, veszélyeztetve az áldozatot és/vagy annak reputációját.
- **Outing** (**kibeszélés)** – titkok, pletykák vagy egyéb személyes információk engedély nélküli megosztása másokkal.
- **Trickery („trükközés", becsapás) –** személyes adatok megszerzése megtévesztéssel, majd az információ, adat megosztása.
- **Cyberstalking (online zaklatás)** – az áldozat online szokásainak megfigyelése, és támadó jellegű kijátszása
- **Cyberthreats (online fenyegetések)** – közvetlen fenyegetések vagy nyugtalanító kijelentések, amelyekből úgy tűnik, hogy a szerző érzelmileg felkavart, és fontolgatja, hogy valaki mást, vagy magát bántja, illetőleg öngyilkosságot követ el.

[55] http://hun.tabby.eu/mit-jelent-a-cyberbullying.html - Letöltve: 2019.05.20.

- **Sexting** (**szexting**) – a „text” (szöveg) és a szex szavak összevonása. Az elkövető szexuálisan provokatív, saját maga által készített meztelen képeket vagy nyíltan szexuális tartalmú szöveget küld el online. A legnagyobb figyelmet a meztelen képek küldése kapja, mert az ilyen felvételek további, széleskörű terjesztése sokkal valószínűbb, és a fiatalokat nagyobb kockázatnak teszi ki.

A gyakorlatban ez sokféle módon valósulhat meg:[56]

- Felzaklató tartalmú anonim üzenetek (szöveg, kép, videó) küldése e-mailben, SMS-ben, chaten vagy közösségi oldalon
- Személyes felhasználói fiókba (e-mail, közösségi oldal, stb.) való jogosulatlan belépés,
- Valaki más online személyiségével való visszaélés,
- Bármilyen privát információ megszerzése és annak beleegyezés nélküli elterjesztése,
- Személyes kép vagy videó szerkesztése úgy, hogy az azon szereplőt megalázó helyzetbe hozza vagy nevetségessé tegye, s ennek a terjesztése,
- Mobiltelefonra érkező anonim hívások,
- Honlap vagy blog létrehozása valakinek a lejáratása céljából,
- Személyes honlap, blog feltörése és módosítása,
- Internetes szolgáltató vagy a hatóságok valótlan tájékoztatása annak érdekében, hogy valakit hátrányos következmény érjen, például kizárják egy honlapról, vagy házkutatást tartsanak nála,
- Rosszindulatú pletykák terjesztése online eszközök segítségével,
- Online hozzáférés meggátlása – például jelszóváltoztatással,
- Kirekesztés, negligálás („levegőnek nézés”) online környezetben.

5.1 Agresszorok és áldozatok

Tanárként jó tisztában lenni azzal, hogy milyen tulajdonságaokkal rendlekeznek a (potenciális) áldozatok, illetve az agresszorok.

Révész szerint[57] az áldozatot több típusba sorolhatjuk: A *passzív áldozat* gyenge, védtelen, önalávető, akinek kevés barátja van, a fájdalomra érzékenységet mutat (ez mintegy megerősíti a bántalmazót), önvádló. Úgy érzi, hogy közel van a tanáraihoz, szüleihez, de nem hiszi, hogy bárki segíteni akarna

[56] http://mipszi.hu/cikk/110104-elektronikus-zaklatas-cyberbullying – Letöltve: 2019.05.20.
[57] Révész György: Erőszak az iskolában, In: Péley-Révész (Szerk.) 2007. Autonómia és identitás. Tanulmányok Kézdi Balázs 70. születésnapjára. Pécs, Pannónia Könyvek, 162-179. old.

rajta. Szorongó, visszahúzódó, agressziót elutasító, túlságosan is érzékeny, és sajnos, ez a túlzott érzékenysége lesz a legnagyobb sérülékenysége, mert vonzani fogja a zaklatásra hajlamos társait.

Az ún. „*idegesítő gyerek*" a megfigyelhető viselkedés szintjén bohóckodik, dicsekszik, stréber, viszont önértékelési gondokkal küzdenek a háttérben.

Végül a harmadik típusba tartoznak azok a gyerekek, akik szinte kiprovokálják társaik támadását lökdösődnek, „beszólnak", verekedést kezdeményeznek stb.

Beszélhetünk agresszív vagy provokatív áldozatról is. Ilyen esetben a gyerek bántalmaz másokat, de ő maga is támadások áldozata, erőszakos, impulzív, szegényes szociális és problémamegoldó képességgel. Az ebbe a típusba tartozó fiatalokat általában a szülők gyakran büntetik, a tanáraik sem kedvelik, illetve a társaik kiközösítik.

Összefoglalásképpen az áldozatok és potenciális áldozatok tulajdonságai:

- Szorongásos viselkedés
- Érzékeny
- Visszahúzódó
- Csendes
- Az énképük általában negatív
- Önértékelésük alacsony
- Csúnyának, butának, szerencsétlennek tartják magukat

Támadónak tekintjük azokat, akik ismétlődően megtámadják azokat, akik nem támadnak vissza, így a támadó élvezheti az erő, a felsőbbrendűség és a hatalom érzését. Fontos különbséget tenni egy agresszor, illetve egy erőszakos gyerek vagy rivalizáló kamasz között, ugyanis az utóbbiak tetteik során nem rendelkeznek a támadó definíciójához tartozó összes aspektussal: ismétlődés, sérülés okozása, szándékosság (egyenlőtlen erőviszonyok). Támadó gyerekek kevésbé kötődnek szüleihez, mint az átlag gyerekek, családjuk gyakran hideg, bántalmazó.

Az agresszorok tulajdonságai:

- Agresszívak
- Elfogadóak az agresszióval szemben
- Önértékelésük magas
- Énképük pozitív
- Empátiájuk átlag alatti – felmérések azt mutatják, hogy nincsenek tisztában azzal, hogy milyen szenvedéseket okoznak a másiknak.

Iskolai bántalmazást bárki elszenvedhet, ahogy bárki lehet elkövető is.

Fontos tudatosítani: nem csupán zaklatók és áldozatok állnak szemben egymással, többnyire ún. szemlélődők is részesei az eseményeknek. Ha nem tesznek ellene semmit, passzivitásukkal az erőszakot támogatják.

5.2 Következmények és a lehetséges segítség a bajban

Ha egy gyermek tartósan az áldozat szerepében marad, és nem kap segítséget, annak következményei lehetnek: súlyos pszichés és szociális következmények, könnyen depresszióssá válhatnak, szorongásos betegségek, poszttraumás stressz szindróma (PTSD), függés különböző kábítószerektől, súlyosabb esetben öngyilkosság. Az áldozatszerepnek pszichoszomatikus tünetei is lehetnek: fejfájás, hasi panaszok, álmatlanság, többet hiányoznak az iskolából, nehezebben megy nekik a tanulás, romlanak a jegyeik, falcolás (nem jut el addig, hogy megsemmisítse önmagát, de fájdalmat azért okozzon magának), nem beszélve az ilyen traumák felnőttkori hatásairól.

Mit tehetünk, ha már megtörtént a baj? Mindenképpen vegyük komolyan, a probléma lekicsinylése, vagy olyan típusú tanácsok, hogy „Üss vissza!" vagy „Szólj vissza!" vagy „Állj bosszút!" nem segítenek. Amikor baj van, akkor már nem lehet besöpörni a szőnyeg alá. Sokat segít a türelmes hallgatás ilyenkor, akár nap, mint nap, ha ilyen trauma után szóra lehet bírni az áldozatot. Fontos tudatosítani: ő áldozat, nem ő hibázott. Az sem jó, ha más (szülő, barát, tanár) áll bosszút az áldozatért.

A tanárokra is szükség van a helyzet megoldásában, különösen az osztályfőnökre! Sok függ az osztályban uralkodó légkörtől, azt pedig odafigyeléssel alakítani tudja az osztályfőnök.

Abban az esetben, ha mindent megpróbáltunk és úgy látjuk, hogy a helyzet nem változik, akkor érdemes pszichológus segítségét kérni. A gyerekpszichológusoknak rendelkezésre állnak mérőeszközök, melyek segítségével megállapítható, hogy a gyereket piszkálják-e vagy piszkálták-e korábban, és megfelelő terápiával szakszerűen tudnak segíteni Szükség lenne minden iskolában iskolapszichológusra.

Elengedhetetlen az olyan iskola, ahol

- demokratikus, egymást tiszteletben tartó szellemiség uralkodik,
- olyan osztálytermi légkör megteremtése a cél, ahol fontos a diákok véleménye,
- a szabályok egyértelműek, betarthatóak,
- senki nem tűri meg az iskolai zaklatást.

Véleményem szerint segítene a prevencióban, illetve az előforduló esetek feldolgozásában, ha lenne ilyen helyzetekre külön képzésük vagy továbbképzésük a tanároknak, valamint lennének rendszeresen kifejezetten a bullyingra/cyberbullyingra irányuló tudatosító órák, emiatt fontos a Saferinternet munkája. Az alábbi plakát (16. ábra) egy tatabányai iskola példája a tudatosításra:

16. ábra Tudatosító plakát egy iskolában

5.2 EU Kids online II. felmérés

Az EU Kids onlline II. felmérés[58] szerint a kutatásban résztvevő magyar gyerekek 19%-a nyilatkozott úgy, hogy a kérdezést megelőző egy évben érte kortársai részéről zaklatás. Az érintettek 11%-a majdnem minden nap, 20%-a egyszer-kétszer egy héten, 15%-a egyszer-kétszer egy hónapban, csaknem fele ennél ritkábban vált áldozatává ilyen cselekedetnek (17. ábra).

	N	% az érintettek körében	% a teljes korosztály-ban
Volt része kortárs zaklatásban	190	-	19%
naponta zaklatták	21	11%	2%
hetente zaklatták	38	20%	4%
havonta zaklatták	29	15%	3%
ritkábban zaklatták	90	47%	9%

17. ábra Zaklatással kapcsolatos tapasztalatok megadása

A zaklatások nem egyforma mértékben érintik az egyes demográfiai csoportokat, minél fiatalabb valaki annál valószínűbb, hogy ilyen cselekmény áldozatává válik. Az alacsony szocio-ökonómiai státuszú családokban felnövekvő gyerekek negyedének volt zaklatásban része, míg a közepes helyzetűeknél átlagos az arány, a legjobb körülmények között élők esetében pedig jóval átlag alatti.

[58] EU Kids Online II. A magyarországi kutatás eredményei. ITHAKA, 2011. Online: http://nmhh.hu/dokumentum/3886/ITHAKA_EU_KIDS_Magyar_Jelentes_NMHH_Final_12.pdf - Letöltve: 2019.05.24.

Az egyszülős családban élőknél még magasabb a zaklatás áldozatinak aránya (28%), szemben a kétszülős háztartásokban élő gyerekek körében mért valamivel átlag alatti aránnyal.

Az internetes zaklatás platformjai leginkább a közösségi hálózatok, illetve az azonnali üzenetküldő programok. Tartalmát tekintve leginkább bántó, zaklató üzeneteket jelent

A felmérés arra is rákérdezett, hogy a kérdezett maga viselkedett-e zaklatóan valakivel szemben a kérdezést megelőző egy év folyamán. A kérdésre a gyerekek 15%-a válaszolt igennel. A zaklatók aránya leginkább a korral és a szocio-ökonómiai helyzettel függ össze, bár meg kell jegyeznünk, hogy a csoportok közti eltérések igen kicsik. Érdekes, hogy a zaklatók 45%-a azon gyerekek soraiból kerül ki, akik maguk is áldozatai ennek a magatartásformának.

Általános megállapítás, hogy a zaklatások jelenleg nagyrészt offline módon valósulnak meg (áldozatok szemszögéből: 73%, támadók szemszögéből 80%).

Végül érdemes beszélni arról, hogy a kérdőív milyen eredményt adott a védekezési módszerekről és stratégiákról. A felmérés megkísérelte kideríteni, hogy azokban az esetekben, amikor a gyerekek olyasmit éltek át az interneten, ami kellemetlen, zavaró esetleg megrázó élményt jelentett, hogyan kezelték a helyzetet, mit tettek az így keletkezett ártalom csökkentése érdekében. Három stratégia rajzolódott ki:

- fatalista stratégia: a kellemetlen élményt átélt gyerek visszahúzódással, passzivitással válaszol az adott szituációra; Ennek a típusnak egy variációja, mikor valaki saját magát hibáztatja, bűntudatot érez a történtek miatt;
- kommunikációs stratégia: az érintett gyerek elmondta valakinek, ami vele történt;
- cselekvő stratégia: az érintett gyerek aktívan, internethasználói tudását felhasználva, lépéseket tesz a probléma megoldása és a hasonló szituációk megismétlődésének kivédése érdekében.

Nyilvánvaló, hogy a fatalista stratégia a legveszélyesebb a három közül, mert ekkor a probléma elnyomásra kerül, nem segíti a problémakezelési eszközök fejlődését és az sérülékenység csökkentését.

stratégia típusa	N	% az érintettek körében[17]
fatalista	34	42%
saját magát hibáztató	9	11%
kommunikációs	54	67%
cselekvő	54	67%

stratégia típusa	N	% az érintettek körében[18]
csak aktív válaszokat adott	32	40%
csak passzív válaszokat adott	8	10%
vegyes válaszokat adott	34	42%

18. ábra Védekezési stratégiák eloszlása (több válasz is lehetséges volt) és mintázata

A fenti ábra szerint a válaszadók többsége a cselekvő és/vagy a kommunikációs stratégiát választották, és örvendetes az, hogy csupán a minta 10%-a választotta a passzív stratégiát, mikor egy adott problémával találta szembe magát. Fontos kiemelni, hogy egy ilyen kérdőíves kutatás természetesen nem szolgáltathat elegendő információt ezeknek a konkrét eseteknek a valódi, komplex és hosszú távú hatásmechanizmusairól, így az adatok csupán jelezhetik azt, hogy a probléma jelen van, az arra adott reakciók pedig igen sokrétűek.

6. Mobil eszközök biztonságos használata

Napjainkban húzóágazattá vált a mobil számítástechnika, különösen az okostelefonok miatt. Gyakorlatilag az okostelefonok nem is igazán telefonok, hanem olyan kisméretű számítógépek, amelyek többek között telefonálásra is alkalmasak. Az elmúlt években már lényegében csak okostelefonokat lehet vásárolni. Ezt különösen elősegítette az Android platform megjelenése. A korábban említett közösségi hálózatok is nagyban hozzájárulnak ahhoz, hogy egyre több felhasználó vegyen okostelefont, hiszen így napjának szinte minden percét megoszthatja ismerőseivel. Ennek veszélyeiről már korábban említést tettem.

Az egyik probléma az, hogy egy vállalati (így akár az iskolai) hálózaton belül kényes szereplőkké válhatnak ezek a készülékek, ugyanis kívülről behozott computereknek minősülnek. Tehát, beengedjük-e őket a vállalati/iskolai hálózatra vagy sem? Vállalatok esetében, általában a top-menedzsereknek ilyen készülékeik vannak, és ezen keresztül akarnak elérni mindent, ezeken a készülékeken tárolnak/tárolhatnak bizalmas és személyes adatokat is. Ha mindenképpen szükséges, hogy a munkatársak elérjék a vállalat hálózati erőforrásait mobilkészüléken keresztül, akkor külön biztonsági politikát kell létrehozni az ilyen készülékeknek és elkülönítve kell kezelni a többi számítógéptől. Ebben a politikában érdemes letiltani a közösségi oldalak elérését. Egy ilyen típusú politika hasznos lehet az iskolában is, ahol az iskola tudja szabályozni azt, hogy a hálózatán levő okostelefonok mit és hogyan érhetnek el.

Mivel egy okostelefonon rengeteg személyes adatot tárolunk, annak ellopása/elvesztése óriási kockázatot jelent a tulajdonos számára. Ilyen esetre léteznek szoftverek, amelyek lehetővé teszik, hogy egy megadott számról küldött SMS üzenettel (azaz egy jelszóval) a telefon teljes tartalma törlődjön, ilyen módon meg lehet akadályozni, hogy illetéktelen kezekbe kerüljenek a készüléken tárolt adatok.

Az előző veszélyforrás miatt érdemes rendszeresen adatmentést végeznünk a telefonon tárolt adatokról. Sajnos a rendszeres mobil adatmentés fogalma a legtöbb helyen még ismeretlen, pedig, általában a telefon gyártójának szoftvere lehetőséget ad erre vagy be lehet szerezni külön erre a célra írt mobiltelefonos alkalmazásokat is.

A rosszindulatú programok jelenleg kisebb veszélyt mobiltelefonokra, mint a Windows operációs rendszert futtató számítógépekre. Viszont tudjuk, hogy a népszerűség vonzza a rosszindulatú programok íróit, így, véleményem szerint, idő kérdése, mikor fognak a hírek olyan „zombi" telefonokról szólni, amelyek felett már nem a tulajdonosuk bírja az irányítást. A nagy vírusirtó programot gyártó cégek is felismerték ezt az üzleti lehetőséget, így ma már vannak ingyenes és fizetős szoftverek, amellyel telefonunkat védhetjük a kívülről érkező veszélyektől.

A piacon két nagyobb operációs rendszer (platform) verseng a vevők kegyeiért: az IOS (az iPhoneok és iPad-ek rendszere) és az Android. Az iPhone vagy iPad készülékekre csak az Apple által működtetett App Store-ból lehet telepíteni alkalmazásokat. Ennek az az előnye, hogy az Apple mind az alkalmazást, mind az alkalmazás készítőjét le tudja ellenőrizni biztonsági szempontból. Természetesen ez sem nyújt 100%-os biztonságot, de ha az Apple úgy véli, hogy valamelyik szoftver fertőzött, azonnal letiltják a további elérést.

Az Android készülékek ebből a szempontból mások. Sokkal nagyobb szabadságot biztosítanak, így bárhonnan le tudunk tölteni egy alkalmazást. Természetesen ehhez vagy meg kell változtatnunk az alapbeállításokat, vagy külön telepítési jogot kell adjunk az alkalmazástelítőt futtató alkalmazásnak. Amennyiben nem engedélyeztük a külső forrásból való telepítést, és különleges jogot sem adtunk, akkor a rendszer meg fogja akadályozni a külső forrásból való telepítést. Telepítési jog megadása után mindenképp meg kell erősítenünk az installálást. Pontosan emiatt a nagyobb szabadság nagyobb felelőséggel is jár. Tanácsos csak a Google Play-ről alkalmazást telepíteni. A kockázatok elkerülése érdekében ne töltsünk le vadonatúj alkalmazásokat, amelyeket csak néhányan próbáltak ki, vagy csak nagyon kevés pozitív visszajelzéssel rendelkeznek. Minél régebb óta elérhető egy alkalmazás, vagy minél több pozitív visszajelzés van róla, annál valószínűbb, hogy megbízható alkalmazásról van szó. Továbbá csak olyan alkalmazást telepítsünk, amire tényleg szükségünk van, és használni is fogjuk.

Telepítés előtt érdemes megvizsgálni azt, hogy milyen engedélyeket kér, milyen adatokhoz kíván hozzáférni az alkalmazás. Vannak alkalmazások – ilyen pl. a Facebook is – amely indokolatlanul sok mindenhez kér engedélyt. Az Android 6.0 óta már lehetőségünk van személyre szabni valamennyire, hogy egy adott alkalmazás mihez férhet hozzá (korábban nem így volt).

Jó példa a nem 100%-os megbízhatóságra, hogy 2019-ben Több száz androidos alkalmazásban elrejtett kártevőre bukkantak a Check Point nevű kiberbiztonsági cég szakértői, amit összesen már több mint 150 millió alkalommal tölthettek le a Google Playből[59]. A cég kutatói által SimBadnek keresztelt malware úgy fertőzött meg más alkalmazásokat, hogy reklámszolgáltató platformnak adja ki magát, aztán telepítés után egy másik kártevőt rak az eszközre, kijátszva ezzel a Google biztonsági rendszerét. A malware aztán a háttérben fut, és folyamatosan weboldalakat böngészik, ezzel extra bevételeket generálva. A Google törölte az érintett alkalmazásokat.

Osztrák minőségellenőrök teszteltek 250 androidos antivírus applikációt[60] 2019-ben. Arra jutottak, hogy ezek közül 80 a legalapvetőbb kiberbiztonsági követelményeknek sem felelt meg. Néhány tesztelt androidos biztonsági szolgáltatás olyan kevés kártevő szoftver tudott csak azonosítani – néhány konkrétan egyetlenegyet sem – hogy valójában nem lehet őket vírusirtónak nevezni. Néhány alkalmazás minőségét az a tény is leírja, hogy még saját magukat is sikerült rosszindulatú programként detektálniuk. Az értékelések alapján a legtöbb négyes felett teljesített, ami sokkal többet elmond az alkalmazásértékelések megalapozottságáról, mint magukról a termékekről. A tesztelők szerint a legtöbben csak a felhasználói élmény alapján osztályoznak, miközben a vírusirtók valós hatékonyságáról fogalmuk sincs, és persze az sem ritka, hogy egy alkalmazás fejlesztői nyomják a felhasználóinak álcázott pozitív visszajelzéseket. Vírusírtó alkalmazás esetén amúgy is tanácsos a jól bejáratott márkákat választani. Érdemes ehhez meglátogatni az AV-Test oldalát[61].

Személyes adataink védelme érdekében érdemes biometrikus hitelesítést használni a telefonba való belépéshez (pl. ujjlenyomat), illetve a telefon háttértárát titkosítani.

Végül nézzünk egy 2011-es vállalati felmérést, amit a Symantec mobilbiztonsági készített. E szerint[62] a vállalatok az utazó munkatársaik hatékonysága, valamint a kollégák mobilitása érdekében egyre inkább alkalmaznak okostelefonokat és táblagépeket. A vállalatok 71%-a már használ céges okostelefont, és általában a dolgozóknak is vannak ilyen készülékeik.

[59] https://index.hu/techtud/2019/03/14/android-adware-app-kartevo/ - Letöltve: 2019.05.29.
[60] https://index.hu/techtud/2019/03/20/android_virusirto_antivirus_hatastalan/ - Letöltve: 2019.05.29.
[61] https://www.av-test.org/en/ - Letöltve: 2019.05.29.
[62] http://index.hu/tech/2011/10/16/vedtelenek_a_vallalati_mobilok_es_tabletek - Letöltve: 2019.05.30.

Annak ellenére, hogy a mobileszközök használata igen gyorsan terjed, a vizsgált vállalatok mindössze 40 százalékában ellenőrzik, hogy a kollégák milyen tevékenységeket végeznek, milyen alkalmazásokat futtatnak a mobilkészülékeiken. A vizsgálat rámutatott arra is, hogy csupán a cégek húsz százalékánál dolgozik informatikai biztonsági szakértő.

A vállalatok leginkább az adatvesztéstől tartanak (69 százalék). Megközelítően a felük az emberi tényezőt emelte ki kockázatként, beleértve a megfelelő ismeretek hiányát és a tiltott tartalmak letöltését is. A vírusfertőzés és a céges hálózat jogosulatlan használata a vállalatok 47 százalékánál szerepel a legnagyobb kockázatként, miközben az informatikai biztonságért felelős vezetők többsége nem tartja reálisnak egy esetleges mobilbiztonsági támadás bekövetkeztét.

Sajnos, csak minden második vállalat alkalmaz valamilyen megoldást a mobilkészülékek védelmére, és csupán a felhasználók negyede rendelkezik valamilyen szoftveres védelemmel. A védelmi megoldások közül a legelterjedtebb a programok telepítésének tiltása, valamint a pin-kód használata.

Ezek az egyszerű megoldások nem jelentenek teljes körű védelmet az összes vállalati mobileszközre, és nem felelnek meg a vállalatok komolyabb biztonsági előírásainak sem.

Felhasznált irodalom

2011. évi CXII. törvény az információs önrendelkezési jogról és az információszabadságról (Infotv.)

A Közigazgatási Informatikai Bizottság 25. számú ajánlása.

Andrew Conry - Murray, Vincent Weafer: Internetes biztonság otthoni felhasználóknak, Kiskapu Kiadó, Budapest, 2006.,

Andrew S. Tanenbaum: Számítógéphálózatok, PANEM Könyvkiadó, Budapest, 2004.

Az Európai Parlament és a Tanács (EU) 2016/679 rendelete, General Data Protection Regulation, https://eur-lex.europa.eu/legal-content/HU/TXT/HTML/?uri=CELEX:32016R0679 – Letöltve 2019.05.16.

EU Kids Online II. A magyarországi kutatás eredményei. ITHAKA, 2011. Online: http://nmhh.hu/dokumentum/3886/ITHAKA_EU_KIDS_Magyar_Jelentes_NMHH_Final_12.pdf - Letöltve: 2019.05.24.

Dr. Horváth Katalin – Dr. Kőnig Balázs – Dr. Orbán Anna – Törley Gábor: A közigazgatási informatika alapjai Szerk.: Dr. Orbán Anna Budapest, FÁMA Zrt. – Nemzeti Közszolgálati és Tankönyv Kiadó Zrt. ISBN 978-615-5344-08-4 Budapest, 2013.

Horváth László, dr. Lukács György, dr. Tuzson Tibor, Vasvári György: Informatikai biztonsági rendszerek, BMF Kan-dó Kálmán Villamosmérnöki Kar, Budapest, 2001.

Index: Interjú Tari Annamáriával, https://index.hu/tech/2018/01/31/mobilfuggoseg_kozossegi_media_tari_annamaria_kiskamasz_gyerek_pszichologus_gyerekneveles_facebook - Letöltve: 2019.05.30.

Mészáros János: Adatvédelem a XXI. században és az internet világában, PhD értekezés, Szegedi Tudományegyetem, Ál-lam- és Jogtudományi Kar, Szeged, 2017.

Muha Lajos (szerk.): Az informatikai biztonság kézikönyve – Budapest: Verlag Dashöfer, 2000-2005.

Nagy Sándor: Elektronikus leveleink védelme, ComputerBooks Kiadó, Budapest, 2005.

Nemzeti Adatvédelem és Információszabadság Hatóság: Adatvédelmi értelmező szótár - http://www.naih.hu/adatvedelmi-szotar.html - Letöltve: 2019.05.02.

Nemzeti Adatvédelem és Információszabadság Hatóság: Kulcs a net világához: http://naih.hu/adatvedelemr-l-fiataloknak--kulcs-a-net-vilagahoz--projekt.html - Letöltve: 2019.05.17.

Othmar Kyas: Számítógépes hálózatok biztonságtechnikája, Kossuth Kiadó, Budapest, 2000.

Révész György: Erőszak az iskolában, In: Péley-Révész (Szerk.) 2007. Autonómia és identitás. Tanulmányok Kézdi Ba-lázs 70. születésnapjára. Pécs, Pannónia Könyvek, 162-179. old.

Szentgyörgyi Attila: WiFi hálózatok biztonsági kérdései, http://hte.tmit.bme.hu/root/club_ppt/201005/eloadas_szgyi_wifi_hte.pdf - Letöltve: 2019.05.30.

Törley Gábor: Adatbiztonság a közigazgatásban, FÁMA Zrt. – Nemzeti Közszolgálati és Tankönyv Kiadó Zrt. ISBN 978-615-5344-05-3 Budapest, 2013. (elektronikus jegyzet), https://ludita.uninke.hu/repozitorium/handle/11410/10571 - Letöltve: 2019.05.30.

Van Alsenoy Brendan, Verdoodt Valerie, Heyman Rob, Wauters Ellen, Ausloos Jef, Acar Günes - From social media service to advertising network: a critical analysis of Facebook's Revised Policies and Terms, Research Unit KU Leuven Centre for IT & IP Law (CiTiP), 2015. 9-10.

Yazan Boshmaf, Ildar Muslukhov, Konstantin Beznosov, and Matei Ripeanu. The socialbot network: when bots socialize for fame and money. In Proceedings of the 27th Annual Computer Security Applications Conference (ACSAC'11), December 2011.