DISSERTATIONES DOCTORALES

Az infokommunikációs rendszerek nemzetbiztonsági kihívásai

KOVÁCS ZOLTÁN

LUDOVIKA
EGYETEMI KIADÓ

Kovács Zoltán

Az infokommunikációs rendszerek nemzetbiztonsági kihívásai

Dissertationes Doctorales

Sorozatszerkesztő
Padányi József

Kovács Zoltán

AZ INFOKOMMUNIKÁCIÓS RENDSZEREK NEMZETBIZTONSÁGI KIHÍVÁSAI

Ludovika Egyetemi Kiadó ❖ Budapest, 2021

A mű a KÖFOP-2.1.2-VEKOP-15-2016-00001
„A jó kormányzást megalapozó közszolgálat fejlesztés”
című kiemelt projekt keretében jelent meg.

Szerző
Kovács Zoltán

Szakmai lektor
Kovács László

Tartalom

Bevezetés

Az elmúlt évtizedekben az infokommunikációs rendszerek rohamosan fejlődtek, és úgy tűnik, ennek lendületét még a gazdasági válságok sem képesek megtörni. A mobilkommunikációs rendszerek és az internet világméretű elterjedése, a rendelkezésünkre álló adatátviteli sávszélesség folyamatos növekedése, valamint a felhasználási lehetőségek gyarapodása azt eredményezte, hogy mára a gyors, továbbá nagy tömegű adatcsere életünk szerves részévé vált. Az elterjedt technológiák alkalmazásával olcsón, gyorsan és hatékonyan vagyunk képesek ellátni munkahelyi feladatainkat, illetve megoldani hétköznapi problémáinkat egyaránt. A fejlődés azonban láthatóan nem áll meg. Ha csak olyan tényekre gondolunk, mint az LTE[1]-technológia 2012. év eleji bevezetése és az IoT-t[2] előtérbe helyező, az LTE-hálózatoknál kisebb késleltetéssel, gyorsabban több eszközt kiszolgálni képes 5G hálózat[3] fejlesztése, a rézkábelek folyamatos kiváltása üvegszálakra[4] az egyéni felhasználóknál, vagy a(z IP[5]-alapú, sokszor ingyenes) kommunikációt lehetővé tévő alkalmazások gyors terjedése (például Facebook, Skype, Viber stb.), akkor egyértelműen kijelenthető, hogy az említett tendencia a következő években, évtizedekben is folytatódni fog.

---

1 Long Term Evolution – tükörfordításban: hosszú távú fejlődés, amely egy negyedik generációs mobil adatátviteli szabvány.

2 Internet of Things, azaz a dolgok internete, amely olyan hálózatba kötött intelligens eszközöket takar, amelyek képesek felismerni bizonyos lényegi információkat és azokat internetalapú hálózaton másik eszközök felé kommunikálni.

3 5G – 5. generációs mobil távközlési hálózat.

4 Az üvegszál előnyei a rézkábelekkel szemben a magasabb átviteli sebesség (üvegszál: akár 100 Gb/s, rézkábel: CAT7 10Gb/s), a kisebb csillapítás, ennek megfelelően a kevesebb szükséges ismétlő elem (üvegszál: kb. 30km-enként, rézkábel: kb. 5 km-enként), nem érzékeny az áramimpulzusokra, az elektromágneses zavarokra és az elektromos hálózati kimaradásokra, vékonyabb és sokkal könyebb. (Tanenbaum–Wetherall, 2016)

5 Internet Protocol – internetprotokoll: csomagkapcsolt átvitelt megvalósító hálózatiréteg-protokoll.

Különösen igaz ez a felhőalapú rendszerekre, amelyekre ma úgy tekinthetünk, mint az infokommunikációs rendszerek fejlődésének egyik meghatározó mozgatórugójára. Ezek előnyei ugyanis minden szereplő számára kézzelfoghatók, hogy csak az egyik legfontosabbat említsük, a felhasználóknál költségmegtakarítást, a szolgáltatóknál és a gyártóknál pedig a hagyományos technológiával operáló versenytársakkal szemben piaci térnyerést, így bevételnövekedést eredményez. A kettő egymást erősítve bővülő felhasználást indukál, így egyre jelentősebb fejlesztésre sarkallja a gyártókat, szolgáltatókat.

Napjaink két, az infokommunikációt jelentősen meghatározó trendje a felhőalapú rendszerek előretörése, valamint a mobil eszközök és az azokon futó alkalmazások piaci részesedésének növekedése. Ez a kettő egymásra épülve folyamatosan növekvő szerepet tölt be mindennapjainkban, hiszen az egyre gyorsabb, egyre nagyobb számítási teljesítményű mobil eszközökkel és az azokra írt egyre fejlettebb alkalmazásokkal mind gyakrabban éppen felhőalapú rendszereket veszünk igénybe akár munkánkhoz, akár magánéletünk elintézendő dolgaihoz.

A felhőalapú rendszerek robbanásszerű növekedését már az évtized elején előrevetítették az iparág kilátásairól közzétett prognózisok. A Visiongain 2011-ben elvégzett kutatása a felhőalapú rendszerek évi 77 milliárd amerikai dolláros (USD) piacának 2016-ra 240 milliárd USD-re történő növekedését jósolta (visiongain.com, 2016), a Gartner ugyanebben az esztendőben adott előrejelzése szerint pedig 2016 év végére a világ 1000 legjelentősebb vállalatának több mint fele fogja érzékeny ügyféladatait is nyilvános felhőben tárolni (Gartner, 2011). Előrejelzéseik helyességét mára olyan adatok támasztják alá, mint például a Microsoft negyedéves jelentései, amelyekben rendre felhős szolgáltatásaik ugrásszerű növekedését mutatták be. 2014-re ugyanis már sorozatban a második évben sikerült megduplázniuk kereskedelmi felhőből származó bevételeiket, így ez év végére 4,4 milliárd dollárnál álltak ebben az üzletágban (blogs.microsoft.com, 2014), 2015-ben már 8,2 milliárd dollár évesített bevételről számoltak be (Clarke, 2015), 2016-ban és 2017-ben, a negyedéves eredménybeszámolókban rendre a felhőszolgáltatást emelték ki mint meghatározó húzóágazatot (Clarke, 2016; 2017). Hasonló növekedésről számolt be az SAP is, ahol 2015. júliusi adatok szerint 20%-os bevételnövekedésük jelentős részét éppen a felhőalapú szolgáltatásoknak köszönhetik. Ez utóbbi ugyanis az előző év azonos időszakához képest 129%-os növekedést produkálva 555 millió euró bevételt hozott a német cégnek (CIB, 2015). 2017-ben is hasonló eredményekről számoltak be,

ahol az SAP bővülésének hajtómotorjaként a felhőszolgáltatások 49%-os növekedését jelölték meg, amely éves alapon az innen származó bevételek 34%-os növekedését eredményezte (bitport.hu, 2017). Napjaink előrejelzései szerint a növekedés a közeljövőben sem áll meg. A CISCO szerint 2018-ra az adatközpontok forgalma közel megháromszorozódik (2013-hoz képest), a világ lakosságának fele rendelkezni fog otthoni interneteléréssel, amelyből 53%-uk, közel 2 milliárd ember felhőalapú tárolóhelyet (is) igénybe fog venni (Cisco, 2014). Egy 2016-os Gartner-előrejelzés szerint pedig a 2017-re jósolt 89,78 milliárd dolláros piacméret 2020-ra 162,08 milliárd dollárosra növekszik (Coles, s.d.).

A mobil eszközök és a rájuk írt alkalmazások elterjedése kapcsán hasonló növekedést tapasztalhatunk és várhatunk. Az Emarketer 2014-es kutatása szerint 2016-ra a világon több mint 2 milliárd okostelefon lesz a felhasználók birtokában. A legjelentősebb felhasználó ebből Kína, az ázsiai országban már 2014-ben is közel 520 millió darab okostelefont használtak, ám a kutatók 2018-ra csak ebben az országban már több mint 704 millió eladott készüléket prognosztizálnak (Ghosh, 2014). A 2016 év végi adatok igazolták a korábbi prognózist, hiszen e szerint az okostelefon-használók száma 2,1 milliárd körül alakult, ugyanakkor a 2017-ben elkészített előrejelzés szerint ez a szám 2020-ra 2,87 milliárdra nő majd (Statista, 2017a).

A táblagépek eladása 2014-ig szintén növekedett, majd lassú csökkenés után stagnálásba fordult. Világviszonylatban 2010-ben 19 milliót, 2012-ben 145 milliót, majd 2014-ben már 230,1 milliót adtak el belőle, míg 2016-ban már csak 174,9 milliót. 2019-re, valamint 2020-ra mintegy 180 millió eszköz eladásával számolnak a szakemberek (Statista, 2017b). A 2016–2026 közötti időszakra pedig a globális táblagéppiacon 9,1%-os átlagos éves növekedést prognosztizálnak a mennyiség tekintetében (PRNewswire, 2017).

Ám nemcsak a hordozható eszközök, hanem a rájuk írt alkalmazások esetében is jelentős a növekedés. Egy átlagos amerikai felhasználó 2015-ben 8,8 alkalmazást töltött le havonta, a mobilalkalmazásokat áruló boltok bevétele pedig a 2011-es 8,32 milliárd amerikai dollárról 2017-re várhatóan 76,52 milliárdra emelkedik (Cohen, 2015). A globális piacon a mobilalkalmazásokból származó bevételek 2016-ban elérték a 88,3 milliárd dolláros szintet, és a várakozások szerint ez az érték 2020-ra 188,9 milliárd dollárra nő (Statista, 2017c).

Ebben a szegmensben a magyarországi felmérések is hasonló tendenciákat mutatnak. Az eNet felmérései szerint a 18 éven felüli lakosságnak már 2013-ban 2,4 millió okostelefonja volt (eNet, 2013), 2017-re pedig ez a szám

elérte 4,5 milliót (Habók, 2017). 2014 januárjában az internetezők 21%-a táblagépet is használt, 26%-uk tervezte annak megvételét (eNet, 2014), és 2015 januárjára az okostelefon-használók 62%-a rendelkezett már internetelléréssel is a készülékén (eNet, 2015a). 2017-re pedig már 79%-uk (Habók, 2017). Ráadásul ezek fő felhasználói a fiatalabb korosztály tagjai, akiknél az internethasználat kapcsán jellemző, hogy a közösségi oldalak alkalmazása abszolút domináns, de az online tartalomfogyasztás is már messze megelőzi a hagyományos (tévé, rádió, újság) médiumokon keresztülit (eNet, 2015b).

A felvázolt trendek a nemzetbiztonsági és a rendvédelmi szerveket kettős kihívás elé állítják. Egyrészről az új technológiák egy részét felhasználóként igénybe fogják venni (akárcsak az általuk védett állami, kormányzati szervek és azok vezetői), hiszen így vagy már meglévő feladataikat tudják hatékonyabban (olcsóbban, gyorsabban, kiterjesztett képességekkel) ellátni, vagy adott esetben újakat képesek megoldani. Másrészről e szerveknek az új technológiák esetében is meg kell oldaniuk a hatáskörükbe tartozó törvényes ellenőrzést.

A kettős kihívás kettős problémát is jelent. Az első: felhasználóként a megfelelő biztonság garantálása. Szervezeti felhasználóként a nemzetbiztonsági és a rendvédelmi szerveknek meg kell győződniük arról, hogy az adott rendszer kielégíti az általuk meghatározott – sokszor igen magas – biztonsági követelményeket, ugyanakkor tisztában kell lenniük azok minden fennmaradó biztonsági kockázatával is. Márpedig napjainkban a feszes, sokszor előre meghirdetett ütemű fejlesztési ciklusok, az egyre-másra megjelenő új technológiák kiforratlansága mind magában hordozza azokat a hibákat, hibalehetőségeket, amelyek kihasználásával sérülhet az adatok bizalmassága, sértetlensége, rendelkezésre állása. Ám nemcsak a véletlen hibákkal, hanem például a szándékosan beépített hátsó kapukkal vagy ellenérdekelt felek, de akár a szolgáltató általi információgyűjtésre, adatszerzésre irányuló törekvésekkel is számolni kell.

A második, hogy biztosítani kell a törvényes ellenőrzést. Az új technológiák megjelenése magával hozza a régiek, például a hagyományos telefónia leértékelődését, az újak felértékelődését a célszemélyek, ezáltal a törvényes ellenőrzést végző szolgálatok szemében. Ugyanakkor, amíg a hagyományos rendszerek ellenőrzése mind technikai, mind jogi szempontból kiforrott, addig ezen új technológiákról ugyanez nem mondható el. Az újfajta rendszerek ellenőrzése újfajta gondolkodásmódot és újfajta megoldásokat igényel technikai, jogi, valamint adminisztratív oldalról a jogalkotóktól, az érintett

nemzetbiztonsági, továbbá rendvédelmi szervektől, illetve a szolgáltatóktól egyaránt.

A fentiek alapján a monográfia célja is kettős. Egyfelől felhasználói, másfelől törvényes ellenőrzési szempontból megvizsgálni a korszerű infokommunikációs rendszerek közül az internettechnológiára épülő szolgáltatásokat, azon belül pedig kiemelten a felhőalapú rendszereket.

A fentieknek megfelelően jelen kötet az alábbi három fejezetben vizsgálja a kérdéskört:

a) az *első fejezet* a felhőalapú rendszerek értelmezésével foglalkozik, szolgáltatási és telepítési modellek szerint csoportosítva megvizsgálja tulajdonságaikat, előnyeiket, hátrányaikat. Elemzi, mi a különbség a felhőalapú rendszerek és a virtualizáció, a kiszervezés, valamint az internettechnológiára épülő szolgáltatások között. Megvizsgálja, értelmezhető-e ma a kormányzati és a rendvédelmi felhő fogalma, valamint bemutatja, hogy a nemzetbiztonsági szolgálatoknak és a rendvédelmi szerveknek érdemes és kell is foglalkozniuk a felhőalapú rendszerekkel;

b) a *második fejezet* a nemzetbiztonsági szolgálatok és a rendvédelmi szervek szempontjából elemzi és értékeli a felhőalapú rendszerekkel foglalkozó nemzeti és nemzetközi szervezetek által megalkotott, nyíltan elérhető, a téma szempontjából releváns biztonsági ajánlásokat, kiemelve az említett szervezetek számára a felhőalapú rendszerek biztonsági értékelésekor felhasználható, felhasználandó elemeket;

c) a *harmadik fejezet* az internettechnológiára épülő szolgáltatások törvényes ellenőrzési lehetőségeit veszi górcső alá. Nyíltan elérhető forrásokból származó nemzetközi példákon keresztül mutatja be, milyen lehetőségek állnak rendelkezésre a törvényes ellenőrzésre, milyen technikai és jogi problémák merülnek fel alkalmazásuk kapcsán. Ezeket felhasználva felállít egy, a törvényes ellenőrző módszerek vizsgálatához általánosan használható szempontrendszert, amellyel az erre feljogosított szervek képesek akár a meglévő, akár a jövőben megjelenő új módszerek adott célra való megfelelőségét is megvizsgálni. Mindemellett bemutatja a mára már elavult hírközlési modellt potenciálisan felváltani képes új modellt.

Vákát oldal

1. fejezet
Felhőalapú rendszerek értelmezése

A 90-es évek közepétől a számítástechnika és a kommunikáció egyre jobban összefonódott, integrálódott, létrejöttek az infokommunikációs (ICT)[6] hálózatok (Haig et al., 2013). Az infokommunikáció fogalmát – bár pontos, mindenki által elfogadott meghatározása nincs, és jelentéséről a mai napig is sok vita folyik (Munk, 2009) – az információtechnológia (IT)[7] kiterjesztett szinonimájaként is használják, beleértve olyan hardver- és szoftverelemeket, tárolókat, middleware-t, audiovizuális rendszereket stb. is, amelyek az információk előállításához, tárolásához, használatához, megosztásához, archiválásához és törléséhez szükségesek (Sallai, 2012). Elfogadva ezt a megközelítést, az infokommunikáció fogalma alatt a továbbiakban is ez a definíció értendő, olyan helyeken is ezt alkalmazva, ahol a különböző dokumentumok készítői IT-rendszereket írtak (például a felhőalapú rendszerekkel foglalkozó szervezetek anyagai). Ennek oka pedig az, hogy az IT az ICT részhalmazát képezi, annak kiterjesztett szinonimájaként használható, ugyanakkor ma nagyon nehéz, sokszor képtelenség meghatározni, mikor van szó „csupán" IT-rendszerről, így az ICT fogalma pontosabban, teljeskörűbben lefedi ezeket a rendszereket.

Az infokommunikáció egyre felkapottabb, ma már talán legdivatosabb fogalma a *felhő.* Felhőalapú megoldásokról, felhőben tárolt adatokról hallunk, de olvashatunk felhőalapú operációs rendszerről is. Sorra jelennek meg az így működő szolgáltatások, a nagy gyártók ezeket támogató hardveres és szoftveres megoldásai. Neves cégek konferenciákat, előadásokat tartanak róla, ismertetve elképzeléseiket, ötleteiket, új, folyamatban lévő vagy éppen tervezett fejlesztéseiket, felvázolva, hogyan képzelik a – nem is oly távoli – jövőt. Mindeközben folyamatosan sulykolják a felhőtechnológia olyan előnyeit, mint a gyors, igény szerinti erőforrás-kiszolgálás, a mindig naprakész technológiai környezet, a koncentrált erőforrásokból

---

6 Information and Communications Technology (információ- és kommunikációtechnológia vagy infokommunikációs technológia).

7 Infomation technology (információtechnológia vagy informatika).

adódó előnyök, beleértve az ICT-szakemberekét is, és nem utolsósorban a már rövid távon is jelentkező, de hosszú távon jóval olcsóbb költségek. Márpedig ezek olyan hívószavak, amelyek cégek és magánemberek tömegei mellett az állami szféra, ezen belül pedig a nemzetbiztonsági, rendvédelmi ágazat szakembereire és döntéshozóira is hatnak.

Éppen ezért érdemes elemezni, majd megválaszolni – vagy legalábbis megpróbálni megválaszolni – néhány, az állami szervezetek – beleértve a rendvédelmi, nemzetbiztonsági szerveket is – szempontjából lényegesnek tűnő kérdést. Mit is jelent pontosan a felhőalapú informatika? Milyen előnyei, hátrányai vannak? Kell-e, lehet-e használni a rendvédelmi szférában ezt a technológiát? Vagy inkább úgy kell feltennünk ezt a kérdést, hogy meg lehet-e kerülni használatukat a jövőben? Amennyiben egy rendvédelmi szerv felhőalapú rendszert kíván használni, van-e lehetősége a sokkal szigorúbb biztonsági követelmények elfogadtatására, az ezeknek megfelelő rendszer megteremtésére? Meg lehet-e teremteni a nemzetbiztonsági szolgálatok törvényben foglalt kötelezettségét és alapfeladatát jelentő törvényes ellenőrzést a felhőalapú rendszereknél?

Az első fejezet értékeli a felhőalapú rendszerek sajátosságait, az egyes típusok előnyeit, hátrányait, meghatározza, mi tekinthető felhőalapú rendszernek, és mi nem, lehet-e ezek között éles határt húzni, valamint hogy az iparági tendenciák alapján kell-e a nemzetbiztonsági szolgálatoknak és a rendvédelmi szerveknek komolyan foglalkozniuk a felhővel.

Példák felhőalapú rendszerekre

A felhőalapú infokommunikációs rendszerek lényege, hogy olyan adatokkal, szoftverekkel dolgozunk, amelyek egy része vagy akár teljes egésze nem saját infokommunikációs eszközünkön, hálózatunkon található, hanem valahol az interneten (intermatrix.hu, 2011).

Ebben a mondatban a „valahol” a kulcsszó, hiszen nevét is innen kapta ez a technológia. Az e rendszerek működését bemutató ábrákon ugyanis az a hely és az az infrastruktúra, ahol adatainkat, használt alkalmazásainkat stb. tárolják, elérhetővé teszik, számunkra ismeretlen, ezért felhővel szokták ábrázolni (helyettesíteni), mint ahogy azt az 1. ábra is mutatja.

1. ábra

A felhőalapú rendszer ábrázolása

Forrás: a szerző szerkesztése a tutorialspoint.com, s.d. alapján

Már régóta használunk webes elektronikus levelezési szolgáltatásokat, amelyek ugyanezen az elven működnek, ez nem szokatlan számunkra. Az utóbbi időben megjelentek a webes tárhelyet kínáló szolgáltatások, szolgáltatók, lehetővé téve, hogy képeinket, dokumentumainkat, zenéinket is az interneten tároljuk, ezáltal csökkenthetjük saját eszközeinken a háttértárak méretét, és bárhonnan (ahol az internetelérés biztosított), bármilyen arra megfelelő eszközzel (tehát nem kizárólag a saját számítógépünkkel), bármikor hozzáférhetünk adatainkhoz. Ez a 2010-es évek elejére már annyira elterjedt, hogy például a Linux-alapú Ubuntu operációs rendszerben a 11.04-es, fejlesztői kódnevén a Natty Narwhal változattól már beágyazottan elérhető volt az Ubuntu One, amely az előzőekhez hasonló szolgáltatásokat kínál. A bárhonnan, bármilyen eszközzel elérhetőség kritériumát pedig az Ubuntu One szolgáltatója iPhone-, Android-, valamint Windows-kliens kiadásával tervezte lefedni, sőt a még rugalmasabb használat érdekében lehetővé tették a névjegyek importálását olyan népszerű alkalmazásokból, mint a Facebook és a Gmail (ubuntu.hu, 2011). De hasonló szolgáltatásokat kínált már a Windows 7 és a Windows Live kombináció is (windows.microsoft.com, s.d.).

Nemcsak adatokat érhetünk így el, hanem komplett alkalmazásokat is. Ilyen például a Microsoft Office csomagjának online verziója, az úgynevezett Office 365, amely a felhasználóknak a megszokott együttműködési és irodai eszközöket kínálja felhőalapú szolgáltatások formájában (Microsoft, s.d.a).

A kínálat nem állt meg itt. Már olyan alkalmazásokat is „felhősítettek", mint a víruskeresők, például a Panda Cloud Antivirus, amely felhőalapú szolgáltatásának köszönhetően kis méretével és erőforrásigényével kíván nagy népszerűségre szert tenni (Harangi, 2011). Találkozhattunk felhőalapú (hoszting) szolgáltatással a NEXON-tól, amelyben a cég online elérést kínált HR-szoftvereihez (nexon.hu, 2011), illetve mobil és felhőalapú nyomtatási szolgáltatásokkal az Epsontól is (hirek.prim.hu, 2011).

Az operációs rendszerek fejlesztői is elindultak a felhőalapú, online szolgáltatásként nyújtott forma irányába. Gondoljunk itt a Google régóta dédelgetett tervére, a Google Chrome OS-re (googleblog.blogspot.hu, 2009), amely végül 2011 nyarára készült el, és az első kifejezetten erre fejlesztett notebookokkal együtt került forgalomba (Bodnár, 2010; google.com/chromebook, s.d.), vagy az Ubuntu 11.04-es verziójának telepítés nélkül, online, böngészőből kipróbálható verziójára (ubuntu.hu, 2011).

A felhőalapú rendszerek tulajdonságai, csoportosításai, előnyei, hátrányai

Hosszasan lehetne sorolni a példákat, kiegészítve a listát, bővítve azon szolgáltatások körét, amelyeket felhőalapú szolgáltatás keretében vehetünk igénybe, mégis lehetne még újabbakat találni, és másnapra szinte biztosan megjelenik egy olyan, amelyre még csak nem is gondoltunk. Ugyanakkor ezeket a szolgáltatásokat rendszerezni is lehet, mint ahogyan azt a National Institute of Standards and Technology (NIST) Információtechnológiai Laboratóriuma (Information Technology Laboratory) is megtette (NIST, s.d.a). Az alábbiakban az általuk közzétett rendszerezést követve csoportosítjuk a felhőalapú megoldásokat, hiszen szinte minden felhőalapú információtechnológiával foglalkozó szakmai anyag, publikáció e szerint a logika szerint teszi meg ugyanezt. Mindamellett, hogy korlátai az újonnan megjelenő szolgáltatások és a technológiák konvergenciája okán már érezhetők, ma is ez adja a legátfogóbb, legelfogadottabb csoportosítási rendszert. Hozzá kell azonban tenni azt, hogy a NIST munkatársai szerint is a felhőalapú rendszerek esetében egy jelentősen fejlődő technológiáról van szó, ahol a definíciók is idővel fejlődni, változni, finomodni fognak (Mell–Grance, 2009).

Először tekintsük át, mely tulajdonságok megléte esetén mondhatjuk, hogy felhőalapú szolgáltatással van dolgunk:

- *Igény szerinti önkiszolgálás (On-demand Self Service)*
  A felhasználók szükségleteik szerint, a szolgáltatónál történő emberi beavatkozás nélkül képesek változtatni az igényelt számítási kapacitásokat, mint például szerveridő, hálózati tárolók stb.
- *Jó hálózati hozzáférés (Broad Network Access)*
  Hálózaton, szabványos mechanizmusokon keresztül, heterogén eszközökkel (legyen akár vékony vagy vastag kliens, például mobiltelefonok, laptopok, PDA-k stb.) érhetők el a szolgáltatások.
- *Erőforráskészletek (Resource Pool)*
  A szolgáltató készletezett erőforrásokat ajánl fel a fogyasztók számára a több-bérlős modell szerint, a fogyasztói kereslet szerint dinamikusan kiosztva és újraosztva a fizikai és virtuális erőforrásokat. A felhasználó általában nem ismeri vagy nem tudja kontrollálni a biztosított erőforrások pontos helyét, csak valamilyen magasabb szinten (például ország, állam/megye, adatközpont).
- *Teljes rugalmasság (Rapid Elasticity)*
  A fogyasztónak felkínált kapacitások gyorsan és rugalmasan változtathatók, fel- és leskálázhatók az aktuális igények szerint, a felhasználó számára úgy tűnik, mintha korlátlan mennyiségben állna rendelkezésre.
- *Mért szolgáltatások (Measured Service)*
  A felhőalapú rendszerek automatikusan, a kívánt szolgáltatások típusának megfelelően képesek vezérelni és optimalizálni a rendelkezésre álló erőforrásokat (például tárolás, feldolgozás, sávszélesség, aktív felhasználói fiókok). Az erőforrások megfigyelhetők, ellenőrizhetők, használatuk pontosan mérhető, így biztosítva mind a használt szolgáltatás fogyasztója, mind üzemeltetője számára az átláthatóságot (pontos, mindkét fél számára elfogadott számlázási lehetőséget) (Lepenye, 2011a).

A NIST szakemberei szerint ezek azok a tulajdonságok, amelyek az adott rendszerhez felhasznált – később még ismertetendő – szolgáltatási és telepítési modelltől függetlenül jellemzik a felhőalapú rendszereket.

A Bundesamtes für Sicherheit in der Informationstechnik (BSI)[8] is teljes mértékben elfogadja és átveszi a NIST meghatározását, azonban a felhőalapú rendszerekre, szolgáltatásokra saját definíciót is alkot. E szerint:

> *„A számítási felhő megnevezés igényalapú és hálózaton keresztül elérhető, dinamikus, ellátott, felhasznált és számlázott IT-szolgáltatásokat takar. Ezek a szolgáltatások csak meghatározott technikai interfészeken és protokollokon keresztül érhetők el. A számítási felhőként nyújtott szolgáltatások köre lefedi a teljes informatikai spektrumot, és magában foglalja az infrastruktúrákat (például feldolgozási teljesítmény, tárolók), platformokat és szoftvereket"* (Federal Office for Information Security, 2011: 13).

Ez azonban lényegében nem tér el a NIST definíciójától, de annak egyszerűbben, rövidebben megfogalmazott változata, amely röviden tartalmazza a következőkben ismertetett szolgáltatási modelleket, ugyanakkor nem foglalkozik a telepítési modellekkel.

Több cikkben, internetes publikációban találkozhatunk olyan megjelölt tulajdonságokkal, amelyekkel a felhőalapú rendszereket próbálják jellemezni. Ilyenek például a rendelkezésre állás, a kiszolgálás gyorsasága, a megbízhatóság, a skálázhatóság, a teljesítmény, a biztonság, a karbantartás, a költség stb. Egy adott felhőalapú rendszer pontos leírásánál rendkívül fontos a figyelembe veendő tényezők, valamint a meghatározó jellemzők pontos kiválasztása, így azokat a (leendő) felhasználónak mindig az adott esethez, saját igényeihez, elvárásaihoz célszerű összeválogatnia és melléjük fontossági sorrendet felállítania. Akár úgy, hogy az egyes tényezők mellé előre megadja, hány százalékban kívánja a végső értékelésnél figyelembe venni az adott tulajdonságot.

Ahhoz azonban, hogy a felhőalapú rendszereket csoportosíthassuk, egy ilyen elven működő rendszert pontosan besorolhassunk, szükség van a már említett két modellcsoport – a szolgáltatási és a telepítési – kategóriáinak ismeretére is, előnyeikkel, hátrányaikkal együtt.

---

[8] Német Szövetségi Információbiztonsági Hivatal (angolul: Federal Office for Information Security).

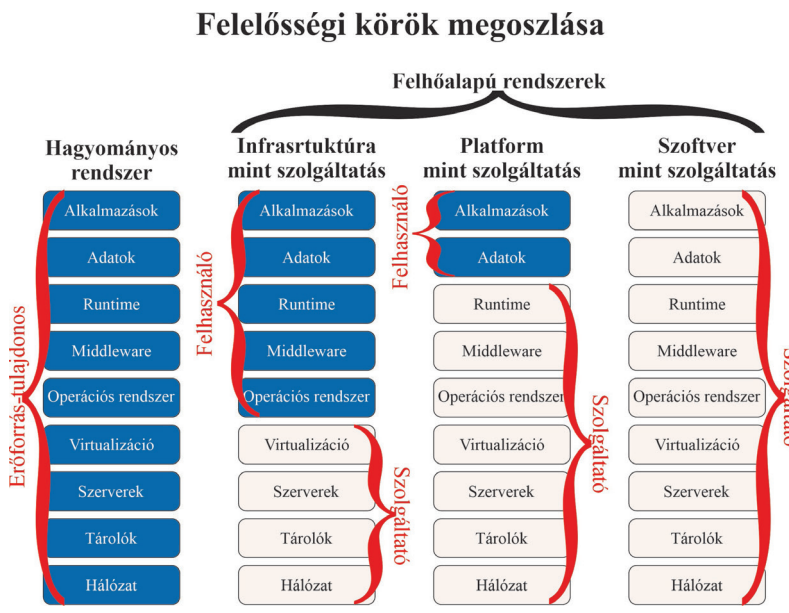
Szolgáltatási modellek (Service Models)

- *Szoftver mint szolgáltatás (Cloud Software as a Service – SaaS)*
  A felhasználó számára nyújtott képességeket a felhő-infrastruktúrában futó szolgáltatói alkalmazások biztosítják. Az alkalmazások különböző eszközökön, vékony kliensfelületen, például webböngészőn elérhetők (ilyen például a webmailszolgáltatás). A felhasználó néhány felhasználóspecifikus alkalmazás korlátozott konfigurációs beállítási lehetőségétől eltekintve semmilyen ráhatással sincs a mögöttes infrastruktúrára, hálózatra, szerverekre, operációs rendszerekre, a tárolás módjára vagy akár az egyedi alkalmazások képességére.
  Előnyei: gyorsan bevezethető, azonnal használható, a felhasználói oldalról használható eszközök rendkívül széles körűek, nem igényel nagy beruházást, a legnagyobb költséget kitevő ICT-üzemeltetési költség jelentősen csökkenthető, a használt szoftverek mindig naprakészek, az alapvető, általános biztonsági funkciókat a szolgáltató biztosítja (például vírusvédelem), alkalmazásváltása alacsony költséggel, gyorsan végrehajtható.
  Hátrányai: nincs testre szabás vagy egyediigény-kiszolgálás, minimális konfigurálási lehetőség áll rendelkezésre, az alkalmazások képességei adottak, új funkció fejlesztése, beillesztése teljes mértékben a szolgáltatótól függ, bevezetéséhez sok betanításra lehet szükség.
- *Platform mint szolgáltatás (Cloud Platform as a Service – PaaS)*
  Ebben az esetben a szolgáltató által támogatott programnyelveken és eszközökkel a fogyasztó által készített vagy megszerzett alkalmazásokat a szolgáltató telepíti egy felhő-infrastruktúrára. A felhasználó itt sem képes menedzselni vagy ellenőrizni a mögöttes felhő-infrastruktúrát, beleértve a hálózatot, a szervereket, az operációs rendszereket vagy a tárolókat, de kontrollálja a telepített szolgáltatásokat és a fogadásukra szolgáló környezet konfigurációját.
  Előnyei: egyedi, akár saját készítésű szoftverek használhatók, ezért bevezetése gyors és egyszerű, a heterogén szoftverkörnyezet bizonyos mértékben homogenizálódik, az ICT-beruházásokra fordított kiadások jelentős mértékben csökkennek, hiszen nem kell rövid idejű csúcsterhelésre méretezett rendszereket vásárolni,

karbantartani, a felhasználói oldalon eddig használt eszközök nagy része továbbra is használható.
Hátrányai: felhasználó által telepített alkalmazások naprakészen tartása továbbra is a felhasználó feladata, a telepíthető alkalmazásokat a szolgáltató által biztosított hardver- és szoftverkomponensek (operációs rendszer) korlátolják, ezért gondos választás esetén is kompromisszumos megoldás születhet, a szolgáltatónál történő változások (hardver, szoftver egyaránt) nem tervezett fejlesztéseket indukálhatnak, a felhasználói oldalon magasabb fokú ICT-háttértámogatást igényel a felhasználó részéről, ezért az ICT-karbantartásra fordított költségek (beleértve a béreket is) kevésbé csökkenthetők, mint a SaaS-megoldás esetében, a felhasználó által biztosított alkalmazásokat – már amennyiben egyáltalán lehet vagy gazdaságos – át kell írni ahhoz, hogy a PaaS-megoldás előnyeit valóban kiaknázhassuk.

- *Infrastruktúra mint szolgáltatás (Cloud Infrastructure as a Service – IaaS)*
  A felhasználó számára ebben az esetben olyan számítási, tárolási, hálózati és egyéb alapvető informatikai erőforrásokat biztosít a szolgáltató, amelyekre és amelyeken tetszőleges szoftvereket telepíthet és futtathat, beleértve az operációs rendszereket és az alkalmazásokat. A felhasználó nem képes menedzselni vagy ellenőrizni a mögöttes felhő-infrastruktúrát, de kontrollálni tudja az operációs rendszereket, tárhelyeket, telepített alkalmazásokat, és esetleg korlátozott ráhatása lehet a hálózati elemek (például tűzfalak) kiválasztására.
  Előnyei: a teljes, megszokott, már testre szabott szoftverkörnyezet átültethető, így betanítás nélkül, a régi eszközökkel használható, könnyen bevezethető, az összes szoftver teljes kontrollja biztosítható (kivéve a virtualizációt biztosítót, de ez talán a legkevésbé kritikus), új szoftverkomponens, funkció bevezetése kizárólag a felhasználótól függ.
  Hátrányai: a teljes szoftverkörnyezet kialakítása, karban- és napra készen tartása a felhasználót terheli, felhasználói oldalon szinte ugyanazt az informatikai szervezetet fenn kell tartani, mint korábban, konzerválódhat a régi, elavult, heterogén szoftverkörnyezet, a három modell közül ezzel csökkenthetők legkevésbé a korábbi ICT-költségek (Lepenye, 2011b).

Az egyes modelleknél a felhasználó és a szolgáltató felelősségi körébe tartozó feladatokat jól szemlélteti a 2. ábra. Az interneten ezzel a kérdéskörrel foglalkozó szakmai anyagok, publikációk vagy ugyanezt a felosztást, vagy ehhez nagyon hasonlót használnak, de lényeges eltérés nem található közöttük.



2. ábra

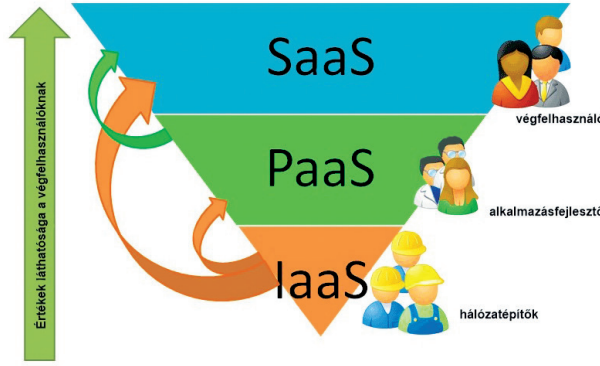
Felelősségi körök megoszlása a szolgáltatási modellekben

Forrás: a szerző szerkesztése a *blogs.cisco.com, s.d.* alapján

A szolgáltatási modelleket már többen, többféleképpen megpróbálták kiegészíteni (ahogy azt már említettük, a NIST szakemberei is hasonló fejlődési folyamatot várnak). Megjelentek az olyan fogalmak, mint a Desktop as a service (DaaS) – ez vékony kliensek kiszolgálására használt desktop-rendszerek virtualizációját jelenti (DePaolis, 2009), a Process as a service (PRaaS) – e szerint a teljes folyamat egy komplett, felhőben futó megoldás úgy, hogy a felhasználónak nincs szüksége ICT-szakember beavatkozására (Naugès, 2009) vagy a Database as a Service (DBaaS) – amely hardverek és szoftverek telepítése és konfigurálása nélkül kínálja az adatbázishoz való

hozzáférés valamilyen formáját (techopedia.com, s.d.a). Amíg azonban a fent kifejtett három modellelemet teljes mértékben mindenki, beleértve az ipari szereplőket is, elfogadja, és – ha úgy tetszik – kvázi szabályként használja, addig az utóbb említett, továbbá az itt fel nem sorolt újabb, kiegészítésnek szánt meghatározások vagy nem ismertek kellően, vagy nem elfogadottak, ráadásul megkérdőjelezik azok létjogosultságát (Kusnetzky, 2009).

A 3. ábrán láthatjuk, kik értékelik, látják igazán az adott szolgáltatási modellek előnyeit.



3. ábra

A szolgáltatási modellek előnyeinek értékelői

Forrás: a szerző szerkesztése a *saasblogs.com, 2009* alapján

Telepítési modellek (Deployment Models)

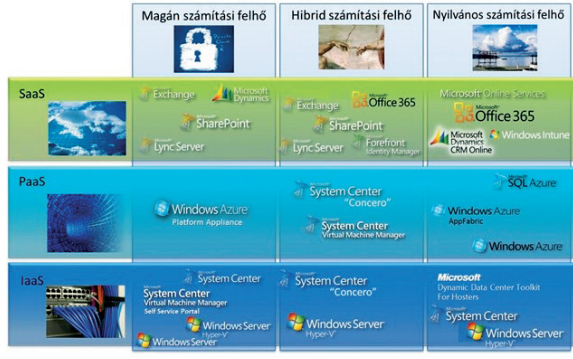
- *Magán számítási felhő (Private Cloud)*
  A magán számítási felhő esetében a felhő-infrastruktúra kizárólag egy szervezet számára működik, amelyet akár a felhasználó szervezet, de akár egy másik fél is menedzselhet, fizikailag pedig akár a felhasználó telephelyén, akár azon kívül is elhelyezkedhet. Előnyei: a teljes rendszer kézben tartott, a biztonság itt garantálható a legjobban, a meglévő rendszerek, rendszerelemek felhasználhatók.

Hátrányai: korlátozott erőforrások, csúcsterhelésre kell tervezni, kevésbé skálázható, a korábbi ICT-re fordított költségek csökkentése itt érhető el legkevésbé.

- *Közösségi számítási felhő (Community Cloud)*
  Ebben az esetben a felhő-infrastruktúrát több szervezet megosztottan használja úgy, hogy az az adott közösség közös érdekeit támogassa (például közös küldetés, biztonsági követelmények, előírások, megfelelőségi szempontok). Ezt menedzselheti akár a felhasználó szervezet, akár egy másik fél is, fizikailag lehet akár a felhasználó telephelyén, akár azon kívül.
  Előnyei: a közös érdekek okán az adott feladatokra jól skálázható, jelentős költség takarítható meg, hiszen az erre fordítandó ICT-költségek megoszlanak, a biztonság megfelelően garantálható, a közös érdekek szerinti kritériumoknak tökéletesen megfeleltethető.
  Hátrányai: közös érdekek mellett is lehetnek egyedi igények, ezek bizonyos esetekben csak kompromisszumokkal vagy egyáltalán nem teljesülnek, limitált skálázhatóság (közös érdekeknél azonos időben jelentkezhetnek csúcsterhelések, ami kritikus lehet, vagy éppen a költségcsökkenési előnyt veszíthetjük el), adott esetben az addig használt szoftverek, alkalmazások cseréje szükséges.
- *Nyilvános számítási felhő (Public Cloud)*
  A felhő-infrastruktúra ebben a modellben bárki (a nagyközönség vagy egy nagy [ipari] csoport) számára elérhető, de a felhőszolgáltatást nyújtó szervezet tulajdonában van. A példákról szóló fejezetben szinte csak ilyenekről esett szó, ez tekinthető ma a legismertebb telepítési modellnek.
  Előnyei: biztosított a teljes felhasználói mobilitás, jól skálázható, a legtöbb költség itt takarítható meg, csak annyit kell fizetni, amennyit fogyasztunk, a felhasználó számára szinte karbantartásmentes, itt szükséges a legkisebb létszámú ICT-csapat a felhasználónál.
  Hátrányai: problémák lehetnek az elérhetőséggel, az adat-visszaállítással, a kiszolgálással, nem ismert az infrastruktúra fizikai elhelyezkedése, a biztonság itt garantálható a legkevésbé.
- *Hibrid számítási felhő (Hybrid Cloud)*
  A felhő-infrastruktúra ekkor több, az előző modellek szerint felépülő rendszer (magán, közösségi, nyilvános) keveréke, ahol

a felhők megtartják egyedi jellegzetességeiket, azokat szabványosított vagy szabadalmazott technológiák kötik össze, lehetővé téve az adatok és alkalmazások hordozhatóságát (például cloudbursting technológia a felhők közötti terheléskiegyenlítésre, amikor a magánfelhőben rendelkezésre álló erőforrások elfogynak, amelyeket más, tipikusan nyilvános felhőben meglévőkkel pótolnak [Chandrasekhar, 2011]).
Előnyei: alapvetően kézben tartott rendszer, amely egyedi igények szerint épül fel, az átlagterhelés feletti szükséges pluszkapacitásokat igény szerinti mértékben és időtartamban kell csak megvásárolni, a nem csúcsra méretezett ICT-rendszerek okán költségek takaríthatók meg.
Hátrányai: összekapcsoláskor nem biztosított homogén módon a rendelkezésre állás, az adat-visszaállítás és a biztonság, nem vagy csak korlátozottan rendelkezünk ismeretekkel a saját rendszeren kívüli többi erőforrás fizikai helyét, összetételét, biztonságát stb. illetően (Lepenye, 2011c).

A szolgáltatási és a telepítési modellekből egyfajta mátrix képezhető. Ebben a mátrixban kell megtalálnia a felhasználónak, hová helyezi saját (meglévő vagy tervezett) hálózatát, és az ennek a mezőibe pozícionált termékek közül tudja kiválasztani a számára megfelelőket. Egy ilyen termékpozicionálást mutat a 4. ábra, itt most a Microsoft termékeire.



4. ábra

Termékpozicionálás a szolgáltatási-telepítési modell mátrixában
Forrás: a szerző szerkesztése Lepenye, 2011d alapján

A kormányzati felhő fogalma

Az általános meghatározások után érdemes elemezni, mit is takar a kormányzati felhő fogalma. Már csak azért is, mert ennek meghatározása, valamint ez alapján a felhőalapú rendszerek bizonyos tulajdonságainak megfeleltetése főleg a biztonsággal összefüggő szigorúbb kormányzati feltételekkel jelentősen előreviheti a rendvédelmi szféra tagjainak is a megfelelő felhőkövetelmények kialakítását.

A European Network and Information Security Agency (ENISA)[9] *Good Practice Guide for Securely Deploying Governmental Clouds* (ENISA, 2013) című dokumentumában külön próbálja meghatározni a kormányzati felhő (gov-Cloud)[10] fogalmát. A készítő szakemberek ehhez alapnak elfogadják a NIST felhődefinícióját, amelyből három telepítési modellt, a nyilvánosat, a magánt és a közösségit emelik ki mint lehetséges kormányzatifelhő-megoldást, míg a szolgáltatási modellek tekintetében mindhármat alkalmasnak tekintik ilyen célú felhasználásra.

Az ENISA szakemberei szerint a kormányzati felhőre jelenleg nincs elfogadott pontos meghatározás, csupán elfogadott megközelítések vannak rá. Ezek viszont több nézőpontból írják le a fogalmat, az alábbiak szerint:

> *„A gov-Cloud egy olyan környezet, ahol a futó szolgáltatások megfelelnek a kormányzati és EU-szabályozásoknak az információbiztonság és az ellenálló képesség terén (ez a* mi? *kérdésre ad választ).*
> *A gov-Cloud a közintézmények, kormányzatok által működtetett szolgáltatások futtatásának (magán vagy nyilvános felhőben) egy biztonságos és megbízható módja (ez a* hogyan? *kérdésre ad választ).*
> *A gov-Cloud egy telepítési modell, amelyet arra építettek, hogy szolgáltatásokat nyújtsanak állami szervek (belső szolgáltatások nyújtása), polgárok és vállalkozások (külső szolgáltatások nyújtása a társadalom számára (ez a* kinek? *kérdésre ad választ)"* (ENISA, 2013: 5).

A kormányzati felhő nem tekinthető csupán egy olyan centralizált, virtualizált ICT-környezetnek, amelyen e-kormányzati alkalmazások futnak. Annál jelentősen több, hiszen itt közös alapok, például egységesített szolgáltatások

---

9 Eredeti nevén: European Network and Information Security Agency (Európai Hálózat- és Információbiztonsági Ügynökség).

10 gov-Cloud: governmental Cloud computing (kormányzati felhő).

és szolgáltatási szintek mellett lehet olyan alapvető szolgáltatásokat nyújthatni a kormányzati szerveknek, minisztériumoknak, amelyek segítik belső működésüket, lehetővé teszi számukra e-kormányzati szolgáltatások nyújtását az állampolgárok, vállalatok részére. Ilyenek lehetnek például a hitelesítési szolgáltatások, adatok tárolása, dokumentumkezelés. Ráadásul mindezeket úgy lehet biztosítani, hogy megmaradjon a felhő legnagyobb előnyének mondott költséghatékonyság, és közösen, akár kormányzati szinten lehet kezelni a felhőtechnológiából adódó új kockázatokat is.

Az ENISA az áttekintést követően végül a következő meghatározást adja a kormányzati felhő fogalmára:

> *„A kormányzati felhő olyan felhőalapú rendszer (infrastruktúra, platform és alapvető szolgáltatások csoportja), amely általában megfelel a következőknek:*
> - *olyan magán (egyedi bérlő), közösség (megegyezés alapján bérlők csoportja) vagy nyilvános (több bérlő) felhőmodellben nyújtott felhőszolgáltatás, amely alkalmas folyamatok futtatására és/vagy adatok tárolására, e-kormányzati szolgáltatások futtatására, és az állami szervezet ezt helyi vagy központosított módon ellenőrizheti/felügyelheti;*
> - *egy sor olyan többször használható szolgáltatási elemet biztosít, amelyek segítségével létrehozhatók e-kormányzati szolgáltatások a közigazgatás, a polgárok és a magánvállalatok számára;*
> - *lehet központi kormányzati, de lehet külső szolgáltató vagy szerv tulajdonában és irányítása alatt, de a végfelelősség a felhasználóé, azaz a központi kormányzaté vagy a helyi szervezeteké (főleg a magán- és a közösségi felhő esetében);*
> - *egy olyan üzleti modell, amely lehetővé teszi az infrastruktúrát, a platform és a szolgáltatások működtetését olyan módon, hogy garantálja a hatékonyságot és a méretgazdaságosságot;*
> - *az infrastruktúra, a platform és a szolgáltatások megfelelnek az országok kormány- és az EU-jogszabályoknak az információbiztonság és az ellenálló képesség terén (függetlenül a kormányzati felhő tényleges fizikai elhelyezkedésétől)*" (ENISA, 2013: 6).

Az idézett szöveg nem tekinthető definíciónak, sokkal inkább körbeírása annak, mikor beszélhetünk – az ENISA szerint – kormányzati felhőről. A hatékonyság és a méretgazdaságosság megjelenítése sem megfelelő, ezek

velejárói lehetnek vagy kellene hogy legyenek a felhő használatának, nem pedig definícióba illő tényezői. Nem ez alapján dől el, hogy az-e vagy sem, hanem ez egy olyan tényező, amely miatt érdemes felhőstruktúrára váltani. Ugyanígy nem érthető a kormányzati és az EU-szabályozásnak való megfelelés kiemelése, mert ezek alapkövetelmények, ráadásul nemcsak a kormányzati, hanem minden, az EU-ban szolgáltatást nyújtó felhőrendszer esetében is. (Ezek betartása a valóságban azonban már más kérdés.)

Joggal merül fel a kérdés, érdemes-e egyáltalán meghatározni a kormányzati felhő fogalmát. A válasz erre: igen. Már csak azért is, mert a kormányzati felhasználású felhőrendszerre mindenképpen magasabb biztonsági követelményeket kell meghatározni, mint az egyéb rendszerekre. Egyrészt azért, mert ebben sok olyan érzékeny, személyes adatot kezelnek, amelyek kiemelt védelmet kell, hogy élvezzenek, másrészt egy ilyen rendszer, szolgáltatás mindig kiemelt célpontja akár a bűnözőknek, akár ellenérdekelt országok titkosszolgálatainak, akár hacktivistáknak is. Ugyanakkor ebből a meghatározásból kiindulva még szigorúbb biztonsági és ellenálló-képességi szabályokat alkalmazva juthatunk el a rendvédelmi szervek által is használható felhőalapú rendszerhez.

A kormányzati felhőre kevés meghatározást lehet találni. Azokban a dokumentumokban, amelyek adott országok kormányzati felhőjének kialakításával foglalkoznak, inkább leírásokat, követelményeket találhatunk, felhődefinícióként pedig elfogadják és átveszik a NIST meghatározását. Ilyen például az Egyesült Királyság G-Cloud programja (Gov.uk, 2013), de említhetjük a Fülöp-szigetek Intergrated Government Phillippines (iGovPhil); (iGov, 2014) projektjét is.

Az ENISA-n kívüli kevés meghatározások egyikét a technopedia.com adja. E szerint a *„GovCloud kifejezés vonatkoztatható az összes olyan számítási felhőre [sic!], valamint virtualizációs termékekre és megoldásra, amelyet kifejezetten a kormányzati szervezetek és intézmények fejlesztettek”*. De ugyanitt rögtön egy másik meghatározást is megadnak, amely szerint a *„GovCloud egy globális kezdeményezés, hogy világszerte az IT-szükségleteknek és a kormányok stratégiai, pénzügyi és operatív célkitűzéseinek megfelelő felhőszolgáltatásokat tervezzenek”* (techopedia.com, s.d.b).

Az Amazon saját GovCloud megoldását, az Amazon Web Services (AWS)[11] GovCloudot úgy határozza meg, mint egy kifejezetten az Egyesült Államok kormányzati szervei és azok szerződő partnerei, ügyfelei számára

[11] Amazon webszolgáltatások.

tervezett rendszert, amelybe bevihetik érzékeny folyamataikat, tárolhatják, feldolgozhatják ilyen jellegű, az akár erős szabályozás alá eső vagy az akár védelmi vonatkozású adataikat is. Ezt a szolgáltatást fizikailag és logikailag is kizárólag az Egyesült Államok állampolgárai és jogi személyei érhetik el (aws, s.d.).

A fentieket figyelembe véve a kormányzati felhő fogalmára az alábbi meghatározás adható:

> *A kormányzati felhő a kifejezetten kormányzati szervek számára ajánlott, fejlesztett vagy akár épített felhő-infrastruktúra és/vagy -szolgáltatás, amely garanciákkal biztosítja számukra az érzékeny, védendő alkalmazások, adatok teljes körű, az üzleti rendszereknél elvárthoz képest magasabb szintű biztonságát és azok biztonságos menedzselését a szerződés teljes időtartama alatt, annak összes fázisában, valamint szerződő partnereik és ügyfeleik részére a számukra szükséges adatok és folyamatok biztonságos elérését. A kormányzati felhő fogalma szempontjából nem releváns az adott felhő telepítési és szolgáltatási modellje, valamint annak tényleges tulajdonosa sem, ugyanakkor az adatok tekintetében a végfelelősség mindig megmarad az azt kezelő, felhasználó kormányzati szervnél.*

A rendvédelmi szervek által használható felhőre vagy, ha úgy tetszik, a rendvédelmi felhőre hasonló meghatározás adható, amelyben még hangsúlyosabbá kell tenni a biztonság kérdését:

> *A rendvédelmi felhő a kifejezetten rendvédelmi szervek számára ajánlott, fejlesztett vagy akár épített felhő-infrastruktúra és/vagy -szolgáltatás, amely garanciákkal biztosítja számukra az érzékeny, védendő alkalmazások, adatok még kormányzati rendszereknél elvárthoz képest is magasabb szintű, teljes körű biztonságát és azok biztonságos menedzselését a szerződés teljes időtartama alatt, annak összes fázisában, valamint szerződő partnereik és ügyfeleik részére a számukra szükséges adatok és folyamatok biztonságos elérését. A rendvédelmi felhő fogalma szempontjából nem releváns az adott felhő telepítési és szolgáltatási modellje, valamint annak tényleges tulajdonosa sem, ugyanakkor az adatok tekintetében a végfelelősség mindig megmarad az azt kezelő, felhasználó rendvédelmi szervnél. A rendvédelmi felhőben található*

> *adatokhoz, szolgáltatásokhoz szigorú hozzáférés és jogosultságkezelés alapján fizikailag és logikailag is kizárólag az adott ország állampolgárai és jogi személyei, kizárólag a számukra szükséges és meghatározott mértékben férhetnek hozzá, azokhoz hozzáférést külföldi állampolgár vagy jogi személy részére kizárólag egyedi engedély alapján lehet adni.*

Az így megalkotott fogalmakat felhasználva a szolgáltatók – egyfajta címkeként – megjelölhetik a magasabb biztonsági követelményeket kielégítő rendszereiket. Amennyiben ez kellő mértékben elterjed, akkor oly módon képes segíteni a kormányzati és rendvédelmi szervek munkáját, hogy a számukra megfelelő felhőalapú rendszer kiválasztása során elég lehet csak azokat a rendszereket megvizsgálniuk, amelyek rendelkeznek a fenti megjelöléssel. Ez pedig jelentősen leszűkítheti, így nagyban egyszerűsítheti a kiválasztási folyamatot.

Felhő- és nem felhőalapú rendszerek megkülönböztetése

Az előző alfejezetek bemutatták, mit takar a *felhőalapú rendszer* kifejezés, milyen kategóriákba oszthatjuk ezeket, és milyen tulajdonságokkal jellemezhetők. Felmerülhet azonban a kérdés, mi a különbség a felhő- és a nem felhőalapú rendszerek között, hogyan lehet egyértelműen megkülönböztetni őket egymástól, vagy egyáltalán meg lehet-e ezt tenni. Ahhoz, hogy a felhőalapú rendszereket pontosan meg lehessen határozni, és el lehessen őket helyezni az *ICT-világtérképen,* mindenképpen célszerű megpróbálni megtenni ezt az elhatárolást.

A monográfiában tárgyalt témák szempontjából azt a három dolgot érdemes tisztázni, hogy mi a különbség egyrészt a felhőalapú rendszerek és a hagyományos ICT-rendszerek virtualizációja, másrészt a felhőalapú rendszerek, illetve a kiszervezett ICT-rendszerek, valamint szolgáltatások, harmadrészt pedig a felhőalapú rendszerek, továbbá az internettechnológiára épülő szolgáltatások között. Az első kettő a nemzetbiztonsági szolgálatok és a rendvédelmi szervek számára a felhőalapú rendszerek (esetleges) használata, a harmadik pedig elsősorban a törvényes ellenőrzés kialakítása miatt lehet érdekes.

Virtualizáció vs. felhő

A virtualizáció és a felhőalapú rendszerek között lényeges különbségek vannak. Az ezek használata során jelentkező előnyökről, hátrányokról külön tanulmányok készültek, kiemelve, mikor melyik megoldást érdemes használni (rackspace.com, 2012). A téma szempontjából azonban csupán az az érdekes, hogy mi a különbség a felhő és a ma szintén oly divatos virtualizáció között.

Összefoglalóan azt mondhatjuk, hogy virtualizációról akkor beszélhetünk, ha egy olyan infrastruktúrát hozunk létre, ahol az erőforrások elosztását rugalmasan, a szükségleteknek megfelelően végezhetjük el oly módon, hogy az adott informatikai erőforrást a többi erőforrástól elkülönítetten vagy leválasztottan kezeljük (Microsoft, s.d.b; Vasvári, 2008).

Miért erőforrásokat említünk? A mai – elterjedt – technológiákat tekintve és rendkívül leegyszerűsítve a dolgot azt mondhatnánk, hogy virtualizáció az, amikor egy adott hardveren több virtuális rendszert működtetünk (Kvint-R, s.d.). Ennél azért jóval többről van szó, hiszen a virtualizációt az adatközponttól a munkaállomásig az informatika minden rétegére lehet alkalmazni (Microsoft, s.d.b). Az 5. ábra jól szemlélteti a teljesen „hagyományos" informatika és a teljesen virtualizált közötti technikai különbségeket, minden rétegre vonatkozóan.

5. ábra

A „hagyományos" és a virtualizált informatika közötti különbségek

Forrás: a szerző szerkesztése a *Microsoft, s.d.b* alapján

A felhőalapú rendszerekhez hasonlóan a virtualizált környezetben sem tudja megmondani a felhasználó, hogy az általa futtatott alkalmazások milyen fizikai hardveren futnak, vagy éppen az adatai hol tárolódnak. Akkor mi a különbség a felhő és a virtualizáció között? Ha most is egyszerűen akarjuk megfogalmazni, akkor a felhasználó oldaláról megközelítve a kérdést, talán két markáns tényező emelhető ki. Az egyik a hardverelemek fizikai elhelyezkedése és tulajdonjoga. A hagyományos ICT-infrastruktúra virtualizálásakor a hardverelemeket ugyanúgy a felhasználó telephelyén helyezik el, ugyanúgy a felhasználó üzemelteti azokat, és valószínűleg ezek az eszközök ugyanúgy a felhasználó tulajdonában is vannak, mint a hagyományos megoldások esetében. A felhőalapú rendszerek esetében mindig virtualizált környezetről beszélhetünk, ha úgy tetszik, akkor a felhőalapú rendszerek bizonyos szempontból részhalmazát képezik a virtualizált hálózatoknak. Ám a felhőalapú rendszerek esetében az eszközök nem a felhasználó telephelyén vannak, nem a felhasználó üzemelteti azokat, és nem is az ő tulajdonát képezik az eszközök. A másik markáns különbség az emberi beavatkozás szükségessége. Egy virtualizált rendszer beállításához, felügyeletéhez, ellenőrzéséhez, karbantartásához a felhasználónál nagyobb informatikai háttér szükséges, mint felhőalapú rendszer használata esetén, ahol ezt a problémát a felhőalapú rendszer szolgáltatója átveszi a felhasználótól.

A virtualizáció is – a felhőalapú rendszerekhez hasonlóan – lehetővé teszi az erőforrások „hagyományos" informatikai megoldásokhoz képesti jobb kihasználását, ám amíg a virtualizáció esetében azok elosztásához, újraosztásához mindig a felhasználó ICT-szakembereinek beavatkozása szükséges, addig a felhőalapú rendszerek esetében ez automatikusan, akár emberi beavatkozás nélkül képes megtörténni (Makk, 2009). A virtualizált környezet kezdeti beállításánál bizonyos mennyiségű erőforrást rendelünk adott alkalmazásokhoz, majd, ha valamelyik erőforrásigénye egy kritikus szintet elér, akkor ismételt emberi beavatkozással rendelhetünk hozzá újabb erőforrásokat. Ez nemcsak az emberi beavatkozás szükségességét vetíti elénk, hanem azt is, hogy a felhőalapú rendszerekben az erőforrások felhasználása hatékonyabb, újraosztása gyorsabb, a kritikus leállások – például erőforráshiány miatt – száma kevesebb lehet.

A virtualizációra tehát úgy tekinthetünk, hogy ha már használjuk ezt a technológiát, akkor az első lépést megtettük a felhőalapú rendszerek alkalmazása felé, ám ez utóbbiak összes előnyét még nem élvezhetjük.

Kiszervezés vs. felhő

Az ICT-rendszerek, -szolgáltatások kiszervezése már jóval régebben elkezdődött, mint ahogy a felhőalapú rendszerek és szolgáltatások megjelentek. Egy felhőalapú rendszer használata azonban többet jelenthet, mint a kiszervezés, hiszen nemcsak a meglévő folyamatok kihelyezését, hanem bizonyos ahhoz kapcsolódó folyamatok automatizálását is lefedheti. Egy másik különbség, hogy a hagyományos kiszervezés esetében mindig a felhasználóra szabott ICT-rendszerről beszélünk, míg felhőalapú rendszer esetében a legtöbbször többfelhasználós környezetre tervezett ICT-rendszerről van szó. Ugyanakkor ebben a logikában a magán számítási felhőt még mindig nehezen lehet megkülönböztetni a kiszervezéstől.

A fellelhető szakirodalmat segítségül hívva több további kisebb-nagyobb különbség és hasonlóság is felfedezhető a kiszervezés és a felhőalapú rendszerek használata között.

Barker szerint a kiszervezés és a felhő ugyanannak a kérdésnek a más árnyalatú válasza: erőforrásokat és felelősséget kihelyezni másnak, aki hatékonyabban tudja elérni a lehető legjobb eredményt. (Barker, 2013) Yigitbasioglu, Mackenzie és Low (2013) megközelítésében a felhő egy olyan ICT-kiszervezés, ahol az olyan erőforrásokat, mint hardver, szoftver, platform, az interneten keresztül lehet elérni, és a legtöbb esetben használatalapú fizetés ellenében. Katzan és Dowling (2010) megfogalmazásában a kiszervezés a meglévő funkciók kihelyezését jelenti, míg a felhő esetében a felhőben lévő alkalmazás motiválja az adott funkció kihelyezését. Marston és munkatársai további különbséget tesznek a kiszervezés és a felhő között a szerződés időtartama alapján. Véleményük szerint ez a hagyományos kiszervezés esetén általában hosszabb, hiszen a felhőszolgáltatóval akár néhány óra időtartamú szerződést is lehet kötni. Így a felhő nagyobb rugalmasságot és kevesebb elkötelezettséget jelent az ügyfélnek. A felhőben az erőforrások fel- és leskálázása, valamint új szolgáltatási kérések az ügyfél részéről szinte azonnal megtehetők az erre alkalmas szoftveren keresztül (Marston et al., 2010). A GetCloudServices szerint a fentieken kívül figyelembe lehet venni az ellenőrzés mértékét is. Egy hagyományos kiszervezés esetén a felhasználónak nagyobb kontrollja marad(hat) adatai felett, mintha felhőt használna (GetCloudServices, 2013).

Nagyobb szervezetek is foglalkoztak a kérdéssel. Az ENISA azt tekinti felhőalapú rendszernek, amely megfelel a NIST definíciójában leírtaknak, míg a nem felhőalapú rendszerek esetében két alcsoportot különböztet meg: a teljesen

saját tulajdonban lévő és így menedzselt, valamint a kiszervezett rendszereket. A saját tulajdonú rendszerek esetében olyan infrastruktúrán és platformon keresztül biztosítják a szervezet számára szükséges ICT-szolgáltatásokat, amely tulajdonosa, üzemeltetője és felhasználója ugyanaz az entitás. Kiszervezés esetén az ICT-szolgáltatások felhasználója és annak biztosítója, az ehhez szükséges infrastruktúra és platform üzemeltetője – sok esetben tulajdonosa – szétválik, a szervezet számára szükséges ICT-szolgáltatásokat a felhasználó számára annak szolgáltatója szerződés alapján biztosítja (Catteddu, 2011). A kiszervezés és a felhőalapú rendszerek különbsége az itt található leírásból nem egyértelmű. Ezt a szerzők is érezhették, mert azt javasolják, hogy a tipikus nem felhő ICT-szolgáltatások, architektúrák mélyebb leírásának az érdeklődő nézzen utána más szakirodalomban, például az Information Technology Infrastructure Library-ban (ITIL)[12].

A BSI szerint a klasszikus kiszervezés és a felhőalapú rendszerek igénybevétele között azonban vannak bizonyos különbségek, amelyeket a választás során figyelembe kell venni. A felhőre ugyanis sokkal inkább jellemző a gazdasági okokból megosztott infrastruktúra használata, a gyorsabb felés leskálázás lehetősége, a felhasználók saját maguk általi erőforrás-menedzselhetősége, a földrajzilag jobban elosztott hálózat, valamint a személyre szabottabb szolgáltatások (Federal Office for Information Security, 2011).

A fentiekből látszik, hogy a kiszervezés és a felhő megkülönböztetése nem teljesen egyértelmű, az elhatárolás bizonyos esetekben (például magánfelhő) pedig szinte lehetetlen. Az egyes megközelítések nagyban függnek attól, milyen telepítési és szolgáltatási modellt vizsgál a szerző. Összegzésként azt mondhatjuk, hogy a felhőre úgy lehet tekinteni, mint a kiszervezés egy formájára, azaz a felhőalapú rendszerek használata az ICT-kiszervezések részhalmazát képezik.

Internettechnológiára épülő szolgáltatások vs. felhő

Katzan és Dowling cikkében úgy tekint a számítási felhőre, mint egy internetalapú eszközre, interneten keresztüli hozzáférhetőséggel (Katzan–Dowling, 2010). Ebből a megfogalmazásból is látszik, hogy az internettechnológiára épülő, valamint a felhőalapú szolgáltatások elhatárolása még

[12] Informatikai rendszerek üzemeltetésére és fejlesztésére szolgáló módszertan-, illetve ajánlásgyűjtemény.

nehezebb, mint a kiszervezés és a felhő közöttié. Bár a fellelt és a monográfia elkészítéséhez elemzett szakirodalmak ezzel az elhatárolással egyáltalán nem foglalkoznak, ennek elvégzése a tárgyalt témák szempontjából azért fontos, mert elősegíti az infokommunikációs rendszerek törvényes ellenőrzési lehetőségeinek, előírásainak megértését és megoldását.

Ahhoz, hogy az említett témakör kapcsán valóban segítséget nyújtson az internettechnológiára épülő, valamint a felhőalapú szolgáltatások elhatárolása, a felhőalapú rendszerek esetén tovább lehet és célszerű szűkíteni a vizsgálandó kört. Az átlagfelhasználók ugyanis elsősorban a nyilvános számítási felhő (Public Cloud – PC) és a szoftver mint szolgáltatás (Cloud Software as a Service – SaaS) típusú rendszereket (továbbiakban: PC/SaaS felhőalapú rendszerek) használják leggyakrabban. Egyszerűbben fogalmazva ezek azok a mindenki számára – a meglévő személyi használatú infokommunikációs eszközök (például notebook, okostelefon stb.) felhasználásával, akár csekély számítástechnikai tudással is használható, olcsón, sokszor ingyenesen – igénybe vehető rendszerek, szolgáltatások (mint például Facebook, Gmail, Dropbox, Twitter, Skype stb.), amelyek ma már szerves részét képezik mindennapi életünknek, kommunikációnknak. Ez pedig azért érdekli a nemzetbiztonsági szolgálatokat és a rendvédelmi szerveket, mert célszemélyi körük egyre nagyobb része is ezeket a rendszereket, szolgáltatásokat használja.

A PC/SaaS-rendszerek mindenképpen az internettechnológiára épülő szolgáltatások részhalmazának tekinthetők, ám a határvonalat, hogy mi tekinthető PC/SaaS-rendszernek is, nagyon nehéz egyértelműen meghúzni. A PC/SaaS-rendszerek meghatározásához most is a NIST Információtechnológiai Laboratóriuma által felállított, és mára már kvázi szabványként elfogadott definíciót és besorolást hívhatjuk segítségül (Mell–Grance, 2009). Két dolgot azonban ki kell emelni, amely megnehezíti ezt. Az első, hogy a NIST definíciója a lehető legáltalánosabban kívánja megfogalmazni a felhőalapú rendszerek alapvető tulajdonságait (igény szerinti önkiszolgálás, jó hálózati hozzáférés, erőforráskészletek, teljes rugalmasság, mért szolgáltatások), így már a NIST-dokumentumon belül is előfordul, hogy az ezek közül egy adott szolgáltatási vagy telepítési modellre rendkívüli módon jellemző tulajdonság nem vagy csak korlátozottan igaz a többire. Példaként említhető, hogy az erőforráskészleteknél leírt több-bérlős modell, illetve a felhasználó által nem ismert vagy nem kontrollált erőforrások helye egyáltalán nem vagy

csak részben igaz egy magánfelhő esetében. A második nehezítő tényező pedig az, hogy a NIST definíciójában a szolgáltatási és a telepítési modelleken belül leírt tulajdonságok is a lehető legszélesebb értelemben próbálják jellemezni a felhőalapú rendszerek egyes típusait, ám éppen ezért teljes körű megfeleltetésük a valós rendszerekkel már sokszor problémát okoz. Ugyanis minden rendszer más és más, így egy adott rendszerre lehet, hogy bizonyos, a NIST által leírt jellemzők teljes mértékben igazak, más tulajdonságok viszont nem vagy csupán kismértékben. Olyan pedig, amelyre minden leírt tulajdonság tökéletesen illene, talán nincs is. Az egy adott alkalmazás használatával elérhető egyre többféle funkció és szolgáltatás pedig tovább árnyalja a képet, és még jobban megnehezíti a besorolást. Gondoljunk például a Google szolgáltatásaira (például Gmail, YouTube, Maps [térkép], naptár, fordító, dokumentumok stb.); (Google, s.d.d.), ahol ezek egy része a NIST-definíciók alapján tisztán értelmezhető felhőalapú szolgáltatásként, másik része kis jóindulattal, harmadik része pedig szinte egyáltalán nem. A fentiek mellett is a NIST definícióját célszerű használni, hiszen mindenki ezt fogadja el, így nekünk is ezt célszerű tennünk. (Ugyanakkor ismét ki kell emelni, hogy a NIST munkatársai szerint is egy jelentősen fejlődő technológiáról van szó, ahol a definíciók is idővel fejlődni, változni, finomodni fognak.)

A fentiek okán sokszor nagyon nehéz megmondani, hogy internettechnológiára épülő szolgáltatással vagy az annak részhalmazát képező PC/SaaS-rendszerrel van-e éppen dolgunk. A határvonal itt a legelmosódottabb, az elhatárolás itt a legnehezebb, és az új szolgáltatások megjelenésének ütemét, az általuk kínált, a korábbiaktól sokszor merőben eltérő új funkcióikat, lehetőségeket figyelembe véve még jó ideig ezt nem is lehet egyértelműen megtenni.

E kötetben is ki kell tekinteni a szűken vett felhőalapú rendszerekből, hiszen az infokommunikációs rendszerek törvényes ellenőrzési lehetőségei, előírásai témakör nem tárgyalható érdemben úgy, hogy a vizsgálatot csupán ezekre leszűkítve végezzük el. Itt ugyanis figyelembe kell venni az olyan internettechnológiára épülő szolgáltatásokat is, amelyek – jelenleg legalábbis – nem érthetők bele a PC/SaaS-rendszerek fogalmába. Éppen ezért, amikor szükséges, a kiterjesztőbb értelmű internettechnológiára épülő szolgáltatások megfogalmazása került a szövegbe, de egyértelműen beleértve és kiemelten kezelve a PC/SaaS-rendszereket.

Nemzetbiztonsági szolgálatok, rendvédelmi szervek és a felhő

A felhőalapú rendszerek ismertetését követően érdemes megnézni, szükséges-e foglalkozniuk a nemzetbiztonsági szolgálatoknak és a rendvédelmi szerveknek ezekkel a rendszerekkel. Tekintsük ezt akár a felhasználás, akár a törvényes ellenőrzés végrehajtása szempontjából. Ehhez nemcsak a jelen, hanem a várható fejlődési irányokat, trendeket is figyelembe kell venni.

Nehéz megjósolni a jövőt, de az ICT-ipar tendenciáiból, az erre szakosodott cégek előrejelzéséből viszonylag jó következtetéseket lehet levonni. A bevezetőben bemutatott, többek között a Microsofttól (Clarke, 2016; 2017), a Gartnertől (Gartner, 2011; Coles, s.d.) vagy a CISCO-tól (Cisco, 2014) származó elemzések és előrejelzések jól mutatták a felhőalapú rendszerek rohamos elterjedését, továbbá azok közeljövőben várható töretlen növekedését.

Tovább lehetne sorolni a példákat, kiegészítve más elemzésekkel, újabb piaci szereplőkről szóló adatokkal, de már ez is plasztikusan mutatja, hogy a 2010-es évek az ICT világában a felhőről szólnak és fognak szólni. A Gartner szerint 2020-ig az informatikai kiadások terén 1 trillió dollárt közvetlenül vagy közvetve érinteni fog a felhőre való átállás (Stamford, 2016), a Forbes szerint pedig a teljes felhőpiac 2020-ra elérheti a 411 milliárd dollárt (Columbus, 2017). Nem mehetnek el e mellett az állami intézmények, így a rendvédelmi szervek sem. A felhőalapú rendszerek előnyei (költségmegtakarítás, skálázhatóság, könnyebb üzemeltetés stb.), valamint az esetleges gazdasági válság államra gyakorolt hatása (például az állam fenntartására fordítható kiadások csökkenése) olyan hívószavak, amelyek tovább erősítik az iparági tendenciákat, és e hatékonyabb technológia felhasználása irányába hatnak.

A hazai, az állami és az önkormányzati szféra ICT-tendenciái azt is alátámasztják, hogy a felhőalapú rendszerek használatával minden állami szereplőnek számolnia kell. Hazánkban 2014-ben elindult a Kormányzati Felhő (KOF), amelynek fő célja a magas színvonalú, biztonságos és hatékony működtetést biztosító infrastruktúra-szolgáltatás nyújtása a közszféra intézményei számára (Egov Hírlevél, 2014; kof.hu, s.d.). 2015-ben átadták (Belügyminisztérium, 2015), majd 2017-ben kibővítették az önkormányzati

„Application Service Provider" (ASP-)[13] rendszert, amely az önkormányzatok számára egységes felületen, felhőalapú szolgáltatásként nyújtja a feladataik ellátásához és ügyfeleik kiszolgálásához szükséges alkalmazásokat (Egov Hírlevél, 2017a). A KOF tapasztalataira alapozva, amelyek bizonyították a felhőalapú rendszer használatának előnyeit a kormányzatban és a közigazgatásban, 2017-ben megkezdődött a Kormányzati Adatközpont (KAK) létrehozása is. Ez pedig amellett, hogy megteremti az egységes, hatékonyan üzemeltethető állami informatikai rendszerekhez szükséges alapinfrastruktúrát, és kapacitásbővítést biztosít, további szolgáltatások bevezetését is lehetővé teszi (Egov Hírlevél, 2017b).

A fentiek alapján kijelenthető, a rendvédelmi szektor kapcsán sem az a kérdés, hogy az idetartozó szervezetek igénybe fognak-e venni felhőalapú rendszereket, szolgáltatásokat, sőt még csak nem is az, hogy ezt minden szervezet megteszi-e. Látva az iparági tendenciákat, ezekre a válasz már megszületett, ráadásul e szervezetek egy része már ma is használ ilyen rendszereket (Kovács, 2013a, 2013b, 2014). A kérdés sokkal inkább az, hogy mikortól, milyen formában, milyen modellek és feltételek mellett lehet ezt úgy megtenni, hogy azokat biztonságosan lehessen használni. Ez azért fontos, mert egyrészt a rendvédelmi szervek általi felhasználás esetén a biztonság sokkal kritikusabb tényező, mint a magán vagy más állami, önkormányzati felhasználás esetén, másrészt a biztonság kérdése ma a felhőalapú rendszerek egyik legfőbb problémája. A felhőalapú rendszerek biztonságos használata az EU-ban állami szinten is megoldandó probléma, olyannyira, hogy az ENISA szakemberei a *Security Framework for Governmental Clouds* című dokumentumukban (ENISA, 2014) megállapították, 2014 szeptemberében is csupán alig néhány EU-tagállamnak volt erre olyan kidolgozott felhőmegközelítése, amely jól definiált biztonsági stratégián alapult. Márpedig ez egyértelműen kihat a rendvédelmi szervek ilyen irányú lehetőségeire, törekvéseire is.

A biztonsági kérdések megfogalmazása persze rendkívül nagyvonalú egyszerűsítés a felhőalapú rendszerek kapcsán. Itt olyan kérdéseket kell megvizsgálni a hagyományos ICT-biztonsági kérdéseken belül, mint például

[13] ASP – Application Service Provider (alkalmazásszolgáltató), ebben az esetben ASP-rendszer, amely az önkormányzatok működéséhez szükséges szoftverek elérését biztosítja felhőalapon.

az üzemeltetés, a sérülékenységmenedzsment, a személyazonosság-kezelés, valamint olyanokat, mint az adatvédelem, a megfelelőség, a jogi és szerződési kérdések (Wang, 2009). Meg kell határozni, hogy ezek közül melyek azok, amelyeket egy felhőalapú rendszer felhasználásával kapcsolatban vizsgálni szükséges; pontosan definiálni kell őket, át kell tekinteni, közülük melyek és milyen mértékben relevánsak a rendvédelmi szervezetek számára.

A fent citált elemzések, előrejelzések kifejezetten a vállalati jellegű felhasználás kapcsán mutattak be trendeket, tendenciákat. A felhőalapú rendszerek lehetséges felhasználása mellett a nemzetbiztonsági szolgálatoknak és a rendvédelmi szerveknek azt is el kell dönteniük, hogy a törvényes ellenőrzés biztosítása érdekében kell-e ezekkel a rendszerekkel foglalkozniuk. Ennek kapcsán elmondható, hogy a növekedés az internettechnológiára épülő szolgáltatások, azon belül is a PC/SaaS-rendszerek esetében is markánsan kimutatható. A Facebook-felhasználók száma a 2008 III. negyedévében mért 100 millióról 2014 III. negyedévében 1350 millióra, 2017 II. negyedévében pedig 2006 millióra ugrott (Statista, 2015). A Dropbox szolgáltatásait 2014. év közepére 300 millióan vették igénybe (Essers, 2014), 2017. július végére pedig már 500 millió felhasználóval büszkélkedhettek (Smith, 2017a). A Skype napi aktív felhasználóinak száma a 2013. év eleji 2,7 millióról (Hegman, 2014) 2017-re 300 millióra növekedett (Statista, 2017d). 2017 augusztusában a WhatsAppnak 1200, a Facebook Messsengernek szintén 1200, a WeChatnek pedig 938 millió aktív felhasználója volt (Statista, 2017d).

Az ilyen típusú rendszerek használatát jól jellemzi, hogy egy szintén 2013-ban készült felmérés szerint már ekkor 41 ezer poszt jelent meg másodpercenként a Facebookon, a Twitteren 278 ezer üzenet küldtek percenként, az Instagramra 3600 fotót töltöttek fel, az interneten pedig 204 millió levelet küldtek el ugyanennyi idő alatt (Woollaston, 2013). Egy 2017-es, hasonló felmérés azt mutatta, hogy ebben az évben egy perc alatt átlagosan 900 ezren jelentkeznek be a Facebookra, a Twitterre 452 ezer, az Instagramra pedig 46 200 üzenetet küldenek szintén ugyanennyi idő alatt, és ugyancsak 60 másodpercenként átlagosan 342 ezer alkalmazást töltenek le a két legnagyobb alkalmazás-áruházból. Meg kell említeni, hogy a küldött e-mailek száma viszont visszaesett: 2017-ben már „csak" 156 millió volt percenként (Desjardins, 2017). Ezekből a felmérésekből két fontos következtetést kell még levonni. Az első, hogy a 2017-es felmérésben már megjelentek újabb, a 2013-asban még nem szereplő alkalmazások (például Tinder, Netflix), és eltűntek korábban egy ilyen felmérésből kihagyhatatlannak tűnők (például Tumblr, Pinterest, de még a Skype is). A másik következtetés pedig az, hogy

ezek a felmérések jól mutatják a kommunikációs szokások változását is. Erre éppen az új alkalmazások megjelenése és erősödése mellett a küldött e-mailek számának jelentős visszaesése a jellemző példa, ami plasztikusan igazolja a hagyományos kommunikációs formák jelentőségének csökkenését.

Hosszan lehetne még sorolni a felhőalapú rendszerek, az internet-technológiára épülő szolgáltatások, azon belül is a PC/SaaS-rendszerek növekedéséről szóló példákat, de már a fentiek is plasztikusan bizonyítják, hogy a nemzetbiztonsági szolgálatoknak és a rendvédelmi szerveknek a felhőalapú rendszerekkel a lehetséges felhasználás mellett a törvényes ellenőrzés biztosítása okán is foglalkozniuk kell.

Vákát oldal

2. fejezet
Biztonsági ajánlások a felhőalapú rendszerekhez

A felhőalapú rendszerek terjedése új kihívásokkal állítja szembe a rendvédelmi szerveket, amelyekből az egyik a használathoz kapcsolódó biztonság kérdése. Ez azért lényeges számukra, mert – ahogy azt az első fejezet bemutatta – a felhőalapú rendszerek használata ebben a szektorban is elkerülhetetlennek tűnik. A hatékonyság és az alacsonyabb költségek miatt előbb vagy utóbb ezek a szervezetek is használni fognak ilyen rendszereket (Kovács, 2011), fenntartva kiemelt igényüket a magas szintű biztonság iránt.

Azonban a felhőalapú számítástechnika mint nemrég megjelent és folyamatosan, gyors ütemben fejlődő, változó technológia jelenlegi legnagyobb kihívása éppen a teljes körű biztonság megteremtése. A hagyományos ICT-biztonsági módszertanok (Muha, 2008) nem fedik le teljes mértékben az újonnan jelentkező problémákat, az ott alkalmazott megoldások pedig nem vagy nem teljes mértékben használhatók a felhőalapú rendszerek esetében. Ráadásul olyan új biztonsági kockázatok jelentek meg, amelyeket újszerű módon kell megoldani. Ezt tetézi, hogy a felhasználó és a szolgáltató érdekei – a biztonság megteremtése kapcsán felmerülő költségek, a felelősségi körök megosztása stb. okán – akár egymással ellentétesek is lehetnek. Éppen ezért a rendvédelmi szerveknek mint (leendő) felhasználóknak pontosan tisztában kell lenniük a felhőalapú rendszerek biztonsági kockázataival, kihívásaival, és képesnek kell lenniük felmérni és eldönteni, hogy az ajánlott vagy kiválasztott rendszer megfelel-e az általuk támasztott biztonsági követelményeknek.

A felmérést célszerű egy olyan elsődleges biztonsági vizsgálattal kezdeni, amely egységes elvek mentén, egy átfogó kérdéssor segítségével képes tisztázni, az adott rendszer megfelel-e a minimálisan elvárt, de a civil vagy akár a kormányzati szféráénál már magasabb szintű biztonsági követelményeknek. Ezt követheti majd a szervezetspecifikus, részletes felmérés, amely már azt hivatott megmondani, hol vannak azok az erősebb szintű követelmények, amelyeket az adott rendszer még nem teljesít. Várhatóan ugyanis a követelmények magasabb szintűek lesznek, mint a szolgáltató

által nyújtott képességek. De ezt már majd egyénileg, technikai és jogi eszközökkel kell lekezelniük a feleknek.

Az ehhez a többszintű vizsgálathoz szükséges követelményrendszer felállításához nyújthatnak segítséget a fejlett országok felhőalapú rendszerekkel foglalkozó nemzeti és a nemzetközi szervezetei által megalkotott, nyíltan elérhető, releváns biztonsági ajánlásai. Jelen fejezet ezeket veszi számba.

Biztonsági kérdések – alapok

A felhőalapú rendszerek biztonsági kérdéseivel több nagy szervezet is foglalkozik. Ezek időnként közzétesznek olyan dokumentumokat, amelyek segítik a leendő – de akár a meglévő – felhasználókat, hogy saját igényeik felmérése után azonosíthassák kritikus adataikat, folyamataikat, megismerhessék a felhőalapú rendszerek használatából adódó kockázatokat, majd ezek mentén választhassák ki a számukra legmegfelelőbb szolgáltatási és telepítési modellt, valamint tisztázhassák a szolgáltatóval a technikai és szerződéses feltételeket. Éppen ezért célszerű a rendvédelmi szervek szigorú biztonsági követelménye szempontjából elemezni és értékelni ezeket a dokumentumokat, hiszen ezek továbbgondolásával megalkotható egy olyan, a rendvédelmi szervek számára is megfelelő biztonságikövetelmény-rendszer, amellyel a felhőalapú rendszerek vizsgálata elvégezhető, használatuk, alkalmazásuk kockázatai felmérhetők.

A felhőalapú rendszerek biztonsági kérdéseivel foglalkozó szervezetek nem egységesen és főleg nem a rendvédelmi szervek szempontjából közelítik meg a kérdést. Jelentős különbségeket okoz, hogy a szolgáltató vagy a felhasználó oldaláról vizsgálják-e az adott kérdést, hogy a megcélzott felhasználó civil vagy kormányzati szervezet, esetleg magánember-e, de az is, hogy az ajánlást készítő szervezet az Egyesült Államok vagy az Európai Unió jelenlegi technikai és jogi környezetéből indul-e ki. Ugyanakkor ezek mégis hasznosak akár egy, a hazánk rendvédelmi szerveinek szóló biztonsági követelményrendszer elkészítéséhez is, hiszen az ott megfogalmazottak megfelelő újragondolással és átalakítással felhasználhatók hozzá.

A továbbiakban a biztonsági kockázatok feltárását, azonosítását a középpontban tartva a felhőtechnológiában vezető szerepet játszó nagy nemzetközi szervezetek releváns ajánlásait mutatom be, kiindulva az Egyesült Államok adottságait figyelembe vevő, civil felhasználókra koncentráló ajánlásoktól egészen az Európai Unió kormányzati szerveinek szólókig.

A Cloud Security Alliance fontosabb ajánlásai

A Cloud Security Alliance (CSA) az iparági szakemberek, vállalatok és más érintettek széles koalíciója által vezetett nonprofit szervezet. Küldetése egyrészt, hogy támogassa a felhőalapú rendszerek biztonságát szavatoló legjobb gyakorlatok terjesztését és felhasználását, másrészt, hogy a felhő felhasználásával kapcsolatos képzéseket biztosítson, ezzel is elősegítve az infokommunikáció minden más formájának biztonságát. A CSA koncepciójának gondolata 2008 novemberében merült fel, és még azon év decemberében hivatalosan is megalakult. Első fehér könyvüket 2009-ben tették közzé (CSA, s.d.).

Az interneten a témában fellelhető tanulmányok, publikációk sokféle megközelítésben, hol a teljességre törekedve, hol egy-egy témakört kiragadva keresnek válaszokat, vagy próbálnak definíciókat, tanácsokat adni a felhőalapú rendszerek biztonságával kapcsolatban. Ahogyan a felhőalapú rendszerek meghatározásánál és kategorizálásánál a NIST Információtechnológiai Laboratóriuma a *The NIST Definition of Cloud Computing* címen kiadott tanulmánya (Mell–Grance, 2009) általánosan elfogadottnak és kvázi szabványnak tekinthető, úgy a biztonság kapcsán a CSA *Security Guidance for Critical Areas of Focus in Cloud Computing* című kiadványáról (CSA, 2011a) mondható el ugyanez.

A dokumentumban a felhőalapú rendszerekkel kapcsolatos biztonsági kérdéseket alapvetően 14 területre osztják, amelyeket 2 fő részbe csoportosítanak: irányításiba és üzemeltetésibe. Az irányítási részben az általuk stratégiainak, míg az üzemeltetési részben az operatívnak tartott biztonsági kérdésekre koncentrálnak. A CSA által definiált területeket és azok rövid leírását az alábbi, 1. és 2. táblázat tartalmazza.

1. táblázat
A CSA által definiált irányítási területek

Területek	Leírás
Irányítás és vállalatikockázat-kezelés	A szervezet azon képességéről szól, amely segíti, hogy irányítsa és mérje azokat a vállalati kockázatokat, amelyeket a felhőalapú rendszer bevezetése jelent. Olyan elemeket tartalmaz, mint a szerződés megszegésének esete, a felhasználó szervezet azon képessége, hogy megfelelően értékelni tudja a felhőszolgáltató kockázatait, az érzékeny adatok védelmének felelőssége, amikor a felhasználó és a szolgáltató is hibás lehet, valamint azt, hogy a nemzetközi határok hogyan hatnak ezekre a kérdésekre.
Jogi kérdések: szerződések és elektronikus felderítés	Lehetséges jogi kérdésekről szól a felhőalapú rendszerek használatakor. E rész kérdései érintik az információ és a számítógépes rendszerek védelmének követelményeit, biztonsági események közzétételének jogszabályi előírásait, egyéb szabályozási követelményeket, adatvédelmi követelményeket, nemzetközi normákat stb.
Megfelelőség- és auditmenedzsment	A megfelelőség fenntartásáról és növeléséről szól a felhőalapú rendszerek használatakor. A kérdéskör annak értékelésével foglalkozik, hogy a számítási felhő hogyan hat a szervezet belső biztonsági előírásoknak való megfelelésére, a különböző szabályozási, jogi és egyéb megfelelési követelményekre. A terület az audit kapcsán a megfelelőség emelésére is iránymutatásokat tartalmaz.
Információirányítás	Azon adatok menedzseléséről szól, amelyeket a felhőben helyeztünk el. A kérdéskör a felhőben lévő adatok azonosítását és kontrollját, a fizikai kontroll elvesztése miatti kompenzációs kontroll lehetőségeket tárgyalja. Említ olyan egyéb tényezőket is, mint az, hogy ki a felelős az adatok bizalmasságáért, sértetlenségéért és rendelkezésre állásáért.

Forrás: a szerző szerkesztése a *CSA, 2011a: 24* alapján

2. táblázat
A CSA által definiált üzemeltetési területek

Területek	Leírás
Hagyományos biztonság, üzletmenet-folytonosság, katasztrófa utáni visszaállítás	Arról szól, hogyan hat a számítási felhő azokra a működési folyamatokra és eljárásokra, amelyeket jelenleg használ a szervezet a biztonság, az üzletmenet-folytonosság és a katasztrófa utáni visszaállítás megvalósításához. Ez a rész segít azonosítani, hogy a felhőalapú rendszerek hol segíthetnek csökkenteni az aktuális kockázatokat, és mely területeken növelik azokat.
Menedzsmentterv és üzletmenet-folytonosság	A használt menedzsmenttervek és adminisztratív interfészek biztosítása a felhő elérése során, beleértve a webkonzolokat és az API-kat. Az üzletmenet folytonosságának biztosítása felhő telepítéseknél.
Infrastruktúra-biztonság	A mag-felhőinfrastruktúra biztonsága, beleértve a hálózatépítést, a terhelésbiztonságot és a hibridfelhő-szempontokat. Ez a tartomány magában foglalja a magánfelhők biztonsági alapjait is.
Virtualizáció és konténerizáció	Hiperfelügyelők (hypervisor), konténerek és szoftveresen meghatározott hálózatok biztonságát írja le.
Incidenskezelés, riasztások, kárelhárítás	Megfelelő incidensérzékelésről, reagálásról, értesítésről és kárenyhítésről szól. Tartalmazza azokat az elemeket, amelyeket mind a szolgáltató, mind a felhasználó oldalán célszerű alkalmazni a megfelelő incidenskezeléshez, bizonyítékgyűjtéshez, a rendkívüli események feltárásához.
Alkalmazásbiztonság	A felhőben futó vagy oda tervezett és fejlesztés alatt álló alkalmazások biztonságosságának megteremtéséről szól. Olyan kérdésekre válaszol, hogy vajon egy alkalmazás megfelelő-e a felhőbe migrálásra, vagy hogy oda egyáltalán tervezhető-e ilyen alkalmazás, és ha igen, akkor arra melyik szolgáltatási modell a legmegfelelőbb (SaaS, PaaS vagy IaaS).
Adatbiztonság és titkosítás	A megfelelő adatbiztonság és titkosítás használatról, valamint a megfelelő, skálázható kulcsmenedzsment azonosításáról szól.

Területek	Leírás
Hitelesítés, engedélyezés, hozzáférés-kezelés	Azonosítók és a hitelesítéshes szükséges szolgáltatások menedzselése a hozzáférés-szabályozás biztosítása érdekében. A terület olyan kérdésekre fókuszál, amelyek segítségével megállapítható a szervezet felkészültsége a felhőalapú azonosítás, jogosultság és hozzáférés-kezelés menedzselésére.
Biztonság mint szolgáltatás (Security as a Service)	A felhasználónak egy külső fél nyújtotta, biztonságot szavatoló, incidenskezelési, megfelelőségigazolási, valamint azonosítás- és hozzáférés-szabályozási funkciók szolgáltatásáról szól. A biztonság mint szolgáltatás az észlelésnek, a kárenyhítésnek és a biztonsági infrastruktúra irányításának átruházása egy megfelelő eszközökkel és szakértelemmel rendelkező, megbízható harmadik félre.
Kapcsolódó technológiák	Már létező és kialakulóban lévő technológiák, amelyek szoros kapcsolatban állnak a felhőalapú rendszerekkel, beleértve a Big Datát, a tárgyak internetét (IoT) és a mobil számítástechnikát.

Forrás: a szerző szerkesztése a CSA, 2011a: 25 alapján

A CSA 2009 áprilisában adta ki először fent említett dolgozatát, amelynek V4.0 változatát 2017-ben tette közzé. A V3.0 változatban újdonságként már megjelent a biztonság mint szolgáltatás, azaz Security as a Service (SecaaS) fogalma is *(2. táblázat utolsó előtti területe).* Ennek bevezetésére a szerzők szerint azért van szükség, mert míg a felhőalapú rendszerek biztonságáról szóló fejtegetések túlnyomóan arra fókuszálnak, hogyan migráljunk felhőbe, hogyan biztosítsuk a bizalmasságot, a sértetlenséget és a rendelkezésre állást, és hogyan védjük az adatok tárolását, feldolgozását biztosító helyszíneket, addig a SecaaS egy teljesen új területet jelent, hiszen a vállalati biztonságot közelíti meg a felhőből nézve.

Szintén 2011-ben jelentette meg a Cloud Security Alliance^{SM} Security as a Service Working Groupja a *Defined Categories of Service 2011* című tanulmányt (CSA, 2011b), amely az alapdokumentum előbb említett témakörét dolgozza fel részletesebben. E szerint a Security as a Service fogalom a biztonsági alkalmazások és szolgáltatások nyújtását jelenti felhőszolgáltatáson keresztüli, felhőszolgáltatásra vonatkozó vagy felhőszolgáltatásból a felhasználó telephelyén lévő rendszerekre.

Az alapdokumentumban leírtaknak megfelelően itt is 10 kategóriát különböztet meg a biztonság mint szolgáltatás (Security as a Service) területen belül a 3. táblázat szerint:

3. táblázat

A CSA által definiált SecaaS-kategóriák

Kategóriák	Leírás
1. Hitelesítés, engedélyezés, hozzáférés-kezelés	Az hitelesítés, engedélyezés, hozzáférés-kezelés biztosítania kell a kontrollt az azonosítók és a hozzáférés-menedzsment felett.
2. Adatszivárgás-megelőzés	Az adatszivárgás-megelőzés az adatok biztonságának monitorozása, védelme és ellenőrzése azok tárolása, utazása, mozgása és használata közben a felhőben és a telephelyen egyaránt.
3. Webbiztonság	A webbiztonság a felhasználó telephelyén telepített és futtatott szoftver, alkalmazás segítségével vagy a teljes webforgalom felhőszolgáltatóhoz történő átirányításával és ott történő ellenőrzésével valósít meg valós idejű védelmet.
4. E-mail-biztonság	Az e-mail-biztonság kontrollt biztosít a bejövő és kimenő elektronikus levelek felett, így védve a szervezetet az adathalászat, a rosszindulatú csatolmányok ellen, erősítve és betartatva az olyan szervezeti előírásokat, mint a kéretlen levelek kezelése vagy az üzletmenet-folytonosságot biztosító lehetőségek kihasználása.
5. Biztonságértékelés	A biztonságértékelés a felhőszolgáltatások harmadik fél általi auditja, vagy a felhasználó telephelyén lévő rendszerek értékelése iparági szabványokon alapuló felhőszolgáltató megoldásokon keresztül.
6. Behatoláskezelés	A behatoláskezelés egy mintázat felismerésen alapuló folyamat, amely segít a statisztikailag szokatlan események érzékelésében és lereagálásában. Ez magában foglalja a rendszerkomponensek valós idejű újrakonfigurálását is egy behatolás megállítása, megakadályozása érdekében.

Kategóriák	Leírás
7. Biztonsági információs és eseménykezelő rendszer[14]	Biztonsági információs és eseménykezelő rendszerek (push vagy pull mechanizmus segítségével) fogadják a naplóadatokat és eseményinformációkat. Ezeket az információkat korrelláltatják és elemzik, majd ezek alapján valós idejű jelentéseket és riasztásokat állítanak elő azokról az incidensekről és eseményekről, amelyek beavatkozást igényelhetnek. A naplóállományokat oly módon kell megőrizni, hogy közben megakadályozzák manipulálásukat, és így azok felhasználhatók legyenek bizonyítékként a későbbi nyomozás során.
8. Titkosítás	A titkosítás egy kriptográfiai algoritmust felhasználó adatkódolási folyamat, amelynek eredményeképpen titkosított adatok jönnek létre.
9. Üzletmenet-folytonosság és katasztrófaelhárítás	Az üzletmenet-folytonosság és katasztrófaelhárítás olyan intézkedéseket takar, amelyek tervezésével és végrehajtásával biztosítható a működés rugalmassága bármilyen szolgáltatás megszakadása, szünetelése esetén.
10. Hálózatbiztonság	A hálózatbiztonság olyan biztonsági szolgáltatásokból áll, mint a hozzáférések kiosztása, ellenőrzése és a szolgáltatás-erőforrások védelme. Architekturálisan a hálózatbiztonság olyan szolgáltatásokat nyújt, amelyek a hálózatok biztonsági kontrolljával foglalkoznak az egyedi hálózatok mögöttes erőforrásainak egyedi vagy összevontan történő figyelembevételével.

Forrás: a szerző szerkesztése a CSA, 2011b alapján

A CSA már 2014-ben megkezdte egy *Defined Categories of Service v2.0* című dokumentum kidolgozását is, amelyben a fentiek mellett várhatóan két új kategória is meg fog jelenni: a folyamatos felügyelet és a sérülékenységvizsgálat. A folyamatos felügyeletről már 2016-ban meg is jelentették

[14] Security Information and Event Management – SIEM.

a még nem végleges, előzetes dokumentumukat, amelyben a kategóriák leírása résznél a két új témakör definiálása kapcsán az alábbiakat találjuk.

4. táblázat

A CSA által definiálandó új kategóriák

Kategóriák	Leírás
Sérülékenységvizsgálat	A sérülékenységvizsgálat a célinfrastruktúra vagy célrendszer biztonsági réseit keresi nyilvános hálózaton keresztül.
Folyamatos felügyelet	A folyamatos felügyelet a folyamatos kockázatkezelés funkciót takarja, amely megmutatja a szervezet jelenlegi biztonsági pozícióját.

Forrás: a szerző szerkesztése a CSA, 2016a alapján

A fent említett két, már hivatalosan kiadott dokumentumban, azaz a *Security Guidance for Critical Areas of Focus in Cloud Computing V4.0* és a *Defined Categories of Service 2011* címűekben is jól megfigyelhető, hogy átfedések vannak az alapdokumentumban megadott területek és a *Security as a Service* területnél leírt kategóriák között (például azonosítás és hozzáférés-menedzsment, titkosítás stb.). Ezek az átfedések több dolgot is jeleznek. Egyrészt, hogy a hagyományos ICT-biztonsági elemek egy része a felhőalapú rendszerek esetében is használható, másrészt, hogy a felhőalapú rendszerek biztonsági problémái még mindig mennyire újszerűek, és még mindig nincsenek teljesen egzakt elhatárolások, definíciók, standardok. Ez utóbbiak kimunkálásán dolgoznak az iparág szereplői, beleértve olyan szervezeteket is, mint a CSA, az Európai Távközlési Szabvány Intézet[15] vagy a Nemzetközi Távközlési Egyesület[16].

Mivel a SecaaS akár egy, a felhasználó által igénybe vett felhőalapú rendszer biztonsági kontrollját is jelentheti felhőből nyújtott ilyen irányú szolgáltatással, ezért az itt leírt kategóriák újabb fontos támpontot adnak arra vonatkozóan, hogy a CSA szakemberei mit tekintenek fontosnak az említett rendszerek biztonsága kapcsán. Ugyanakkor meg is erősítik a CSA által kiadott más dokumentumokban, így például a *Security Guidance for Critical Areas of Focus in Cloud Computing* című útmutatóban leírtakat.

15 European Telecommunications Standards Institute – ETSI.

16 International Telecommunication Union – ITU.

A két dokumentum kapcsán az is megállapítható, hogy a CSA ezekben a gazdasági társaságokra koncentrálva, iparági megközelítéssel, a szolgáltató szempontjából dolgozza fel a felhőalapú rendszerek biztonsági kérdéseit. Így ezek ugyan sok hasznos információt tartalmaznak a rendvédelmi szervek szempontjából összeállítandó követelményrendszer kialakításához, de nyilvánvalóan e szervezetek minden, akár például egy állami vagy önkormányzati szervezettől is szigorúbb feltételeit nem veszik, nem vehetik figyelembe.

A CSA anyagai az Egyesült Államok jogi, technikai környezetén, adottságain, lehetőségein alapulnak, amelyek jelentősen eltérnek az Európai Unióétól, ezáltal Magyarországétól is. Ezeket a különbségeket is mindenképpen figyelembe kell venni e dokumentumok felhasználása során.

Az előző dokumentumok hasznos kiegészítőjeként szolgál a CSA Top Threats Working Groupja által összeállított *The Treacherous 12 Cloud Computing Top Threats in 2016* című felmérés (CSA, 2016b), amelyben azokat a legveszélyesebb felhőbiztonsági fenyegetéseket rangsorolják, amelyek a felhőrendszerek megosztott igény szerinti kiszolgálása természetéből adódnak. Ezekhez rövid leírást, értékelést és olyan egyéb hasznos információkat is adnak, mint például, hogy melyik szolgáltatási modell érintett, az adott veszéllyel hol foglalkoztak a korábban említett két dokumentumban, de megadják például – a későbbiekben ismertetett – *Cloud Controls Matrix*ban érintett biztonságikontroll-pontokat is. Az általuk azonosított legveszélyesebb fenyegetések sorrendben a következők:

1. adatszivárgás,
2. gyenge azonosítás, jogosultság és hozzáférés-kezelés,
3. nem biztonságos *application programming interface*-ek (API)[17],
4. rendszerek és alkalmazások sérülékenységei,
5. azonosítók megszerzése,
6. rosszindulatú belső munkatárs,
7. folyamatosan fennálló fejlett fenyegetések,[18]
8. adatvesztés,
9. nem megfelelő átvilágítás, gondosság felhőszolgáltatás választásakor,
10. a felhőszolgáltatással történő visszaélés és annak rosszindulatú felhasználása (például illegális jelszótörésre),

[17] Alkalmazásprogramozási felület, amely segítségével lehetséges egy programrendszer szolgáltatásait anélkül használni, hogy annak belső működését ismerni kellene.

[18] Advanced Persistent Threat – APT.

11. Denial of Service (DoS)[19], Distributed Denial of Service (DDoS)[20],
12. megosztott technológiából adódó sérülékenységek.

A dokumentumban leírt veszélyeket, valamint azok javasolt kezelési módjait célszerű figyelembe venni a felhőalapú rendszerek rendvédelmi szervek által történő felhasználása kapcsán felmerülő biztonsági elemzéskor is.

A felhőkockáztok felmérésében, értékelésében iparági alapdokumentumnak tekinthető CSA *Cloud Controls Matrix* táblázata (CSA, 2014a) a hozzá tartozó információs lappal együtt (CSA, 2014b). Ez alapvetően a szolgáltatók számára készített útmutató, ha úgy tetszik, egy biztonsági ellenőrző lista a megvalósítandó biztonságikontroll-funkciókról, de a felhasználók számára is értékes információkkal szolgál. Egyrészt ennek alapján ők is átemelhetnek tételeket a saját követelményrendszerükbe, másrészt ennek felhasználása elősegítheti a felhasználó saját oldali felkészülését, a már meglévő biztonsági szint ellenőrzését, megfeleltetését a felhőalapú rendszer használatához, harmadrészt pedig segítséget nyújt a felhőalapú rendszerek, valamint ezek szolgáltatóinál felmerülő kockázatok értékelésében. A *Cloud Controls Matrix* további kiemelendő tulajdonságai, hogy egyrészt az ebben leírt biztonsági elemek, kockázatok megfeleltetését is megadja szinte minden, széles körben használt szervezet, szabvány által azonosított biztonsági elemhez, kockázathoz (például BSI, COBIT, FedRAMP, ISO/IEC 27001-2013 stb.), ez pedig nagyban segítheti a felhasználót, ha valamelyiket már alkalmazza saját rendszerei biztonságával kapcsolatban, másrészt pedig megadja, hogy az egyes biztonsági kontrollok közül melyik elem kinek (a szolgáltatónak vagy a felhasználónak) a felelősségi körébe tartozik. Éppen ezért a *Cloud Controls Matrixot,* természetesen a megfelelő, a felhasználó oldalára történő átalakítással, megfeleltetéssel, de mindenképpen célszerű felhasználniuk a rendvédelmi szerveknek is a felhőalapú rendszerek kockázatelemzéséhez.

A NIST fontosabb ajánlásai

A NIST az Egyesült Államok legrégibb fizikai kutatólaboratóriuma, amely ma a Kereskedelmi Minisztérium alatt szövetségi ügynökségként dolgozik.

---

19 Szolgáltatásmegtagadással járó támadás vagy más néven túlterheléses támadás.

20 Elosztott szolgáltatásmegtagadással járó támadás, vagy más néven elosztott túlterheléses támadás.

A honlapjukon is közzétett küldetésük az, hogy támogassák az Egyesült Államok beruházásait és ipari versenyképességét olyan tudományok, szabványok és technológiák fejlesztésével, amelyek segítségével javul az ország gazdaságbiztonsága és az ott élő emberek életminősége. Elért eredményeiket számos területen kamatoztatják, így az egészségügyi nyilvántartásoktól kezdve az atomórákon és nanoanyagokon át a számítógépes csipekig számtalan termék és szolgáltatás használja a NIST által kidolgozott technológiákat, szabványokat. A szervezet meghatározó szerepet játszik a felhőalapú rendszerekkel kapcsolatos szabványok és ajánlások kidolgozásában is (NIST, s.d.b). Ez utóbbi kapcsán a NIST számos dokumentumot készített, amelyek nemcsak a felhőalapú rendszerek definiálásakor, hanem a kritikus biztonsági elemek azonosításában is segítenek. A felhőalapú rendszerekkel kapcsolatban megjelentetett dokumentumait a szervezet alapvetően négy kategóriába sorolja:

- *NIST Special Publication 500 Series,* amelyben a különböző szabványokhoz és referenciaarchitektúrákhoz kapcsolódó anyagokat teszik közzé,
- *NIST Special Publication 800 Series,* amelyben a biztonsági kérdésekkel foglalkozó iránymutatások, ajánlások és referenciaanyagok találhatók,
- *NIST Special Publication 1800 Series,* amelyben a kiberbiztonsági kérdésekkel foglalkozó gyakorlatias, felhasználóbarát útmutatók, anyagok találhatók:ezt 2015-ben indították a 800-as sorozat kiegészítéseként, jelenleg még kidolgozás alatt lévő (Draft) dokumentumokat tartalmaz csupán,
- *NIST Cloud Computing Research Papers,* amelyben kutatási anyagaikat publikálják (NIST, s.d.c).

Ezek közül a téma szempontjából a legfontosabb a *NIST 800–144 Guidelines on Security and Privacy in Public Cloud Computing* című (Jansen–Grance, 2011), amely az egyik legtöbbet idézett dokumentum a felhőbiztonsági szakirodalomban. Ebben a készítők a biztonsági kérdéseket a nyilvános-felhő-telepítési modell szerint felépülő rendszerek esetében vizsgálják, ahol az infrastruktúra és a számítási erőforrások üzemeltetése és tulajdonjoga egy külső fél kezében van, a szállított szolgáltatások pedig nyilvánosak és többfelhasználós környezetben futnak. Külön érdeme az anyagnak, hogy a vizsgálatot a kormányzati szervezetek mint felhasználók szemszögéből is végzik, ami azért érdekes, mert ezek számára a többi modellhez képest

mindenképpen a nyilvános felhő hordozza a legnagyobb biztonsági kockázatot. A dokumentum egyfajta útmutatóként is szolgál az említett felhőalapú rendszer bevezetéséhez, hiszen bemutatja azokat a fontosabb lépéseket, amelyeket ennek kapcsán meg kell tenni, egyben felhívja a figyelmet azokra a biztonsági kockázatokra és tényezőkre is, amelyeket az egyes lépések során mindenképpen elemezni és értékelni kell (Jansen–Grance, 2011).

A NIST 800–144 számú dokumentuma összefoglalja a nyilvános felhő veszélyeit, technológiai kockázatait, azok kezelését. Az itt megfogalmazottak szerint egy felhőalapú rendszer használatának megkezdése előtt a felhasználó részéről gondos biztonsági és adatvédelmi tervezés szükséges, hiszen a bevezetésre tervezett rendszernek meg kell felelnie az összes releváns szervezeti előírásnak és szabályozónak, amelyek mentén olyan biztonságossá kell tenni, amennyire csak lehet (Jansen–Grance, 2011).

A biztonsági lehetőségek értékeléséhez kockázatalapú megközelítés szükséges, amelyhez pontosan meg kell érteni a felajánlott felhőkörnyezetet, azaz a szolgáltató által kínált technikai kontrollokat, eljárásokat és előírásokat, valamint a rendszer architektúráját. Ha szükséges, az ajánlott architektúráról, szolgáltatásokról, szolgáltatási szintekről stb. tárgyalni kell a szolgáltatóval, hogy azok valóban kielégítsék a szervezet biztonsági és adatvédelmi követelményeit. A megállapodás eredményét a szerződésben rögzíteni kell, ahogy olyan tényezőket is, mint az adatok, naplóállományok tulajdonjoga, a szerződésből való kilépés lehetőségei, a titkosítás, a törvényeknek megfelelés stb.

Természetesen a felhasználónak más teendői is vannak, hiszen meg kell győződnie arról is, hogy a felhőalapú rendszer felhasználóoldali környezete is megfelel a szervezet biztonsági előírásainak. Itt olyanokat is vizsgálni kell, mint az eléréshez használt böngésző sérülékenységei, a beágyazott mobilalkalmazások biztonsága stb.

A teljes – a felhőalapú és a hozzá kapcsolódó felhasználói – rendszer tekintetében biztosítani kell a biztonsággal és az adatvédelemmel kapcsolatos elszámoltathatóságot a felhőbe vitt alkalmazások és adatok tekintetében. Az ehhez szükséges folyamatos információbiztonsági ellenőrzések kapcsán meg kell győződni a meglévő biztonsággal és adatvédelemmel kapcsolatos biztonságtudatossági felkészültségről, a sérülékenységek, illetve veszélyek kezeléséről, a kockázatértékelés, továbbá -kezelés menetéről, az ott használt kvalitatív és kvantitatív faktorokról, valamint arról, hogy a teljes rendszer képes biztosítani az adatok bizalmasságát.

A felhőalapú rendszer bevezetését és felhasználását alapjaiban meghatározza, hogy milyen – és kiemelten milyen biztonsági – előnyökkel és hátrányokkal, kockázatokkal rendelkezik, az előnyöket hogyan tudja a felhasználó kiaknázni, a kockázatokat pedig elfogadható mértékűre csökkenteni.

A biztonság és adatvédelem szempontjából a nyilvános felhő határozott előnyökkel jellemezhető, akár a hagyományos ICT-rendszerekkel szemben is. Ilyenek az erre specializálódott szakembergárda megléte a szolgáltatónál, az erős, egységes, a speciális előírásokat is sok esetben kielégítő hardver, amely jól skálázható és magas rendelkezésre állást biztosító rendszert ad, a magas szintű biztonsági mentési és adat-visszaállítási lehetőségek, az akár a tárolt adatok hozzáférésének korlátozását is lehetővé tévő mobil végpontok alkalmazhatósága, illetve a karbantartást és feldolgozást is jelentősen megkönnyítő adatkoncentráció.

Ugyanebből a szempontból nézve azonban számos hátránnyal is rendelkezik a nyilvános felhő. Ilyenek például a támadható, csak logikai elválasztást biztosító, megosztott, többfelhasználós környezet, a szintén könnyen támadható interneten keresztüli szolgáltatáselérés, valamint akár a rendszer, akár az adatok feletti fizikai és/vagy logikai irányítás elvesztésének kockázata. Erre a modellre az egyik legjellemzőbbek a rendszer komplexitásából adódó veszélyek, hiszen a biztonság nemcsak a sokféle elem támadhatóságától, hanem azok egymás közötti interakcióitól is függ.

A NIST által azonosított, a nyilvános felhő alkalmazásakor kulcsfontosságúnak tekintett biztonsági és adatvédelmi kérdéseket az 5. táblázat tartalmazza.

5. táblázat

A NIST által meghatározott biztonsági és adatvédelmi kulcskérdések

Területek	Leírás
Irányítás	Kontroll és felügyelet az ICT-szolgáltatásokhoz és alkalmazásfejlesztésekhez használt szervezeti előírások, eljárások, valamint a telepített és alkalmazott szolgáltatásokhoz alkalmazott tervezés, megvalósítás, tesztelés, használat és ellenőrzés felett.

Területek	Leírás
Megfelelőség	A vonatkozó biztonsági és adatvédelmi törvényeknek, szabályzóknak, szabványoknak és specifikációnak megfelelés a szerződés, a rendszer és a működés tekintetében, ezen belül vizsgálandó és rögzítendő kérdések: • a vonatkozó törvények és szabályozók pontos jegyzéke, • az adatok (tárolási, feldolgozási) helye, • elektronikai felderítés (az elektronikusan tárolt információk[21] azonosítása, gyűjtése, előállítása és feldolgozása egy peres eljárás kezdeti szakaszában, vagy más szabályozókhoz, audithoz vagy akár az információs önrendelkezés megfelelőségéhez).
Bizalom, megbízhatóság	A közvetlen irányításról és kontrollról való lemondás miatt meg kell hogy legyen a bizalom a szolgáltató felé, ugyanakkor a felhasználószervezet felelőssége marad, hogy az adatok jogosulatlan hozzáférése, felhasználása, közzététele, módosítása, illetve megsemmisítése kockázatának és a kár nagyságának arányában megfelelő védelmet alakíttasson ki, amelyhez vizsgálni kell: • a belsősök adathozzáférési lehetőségeit, • az adatok tulajdonjogát, • az összetett, harmadik félen alapuló szolgáltatásokat (például SaaS-szolgáltatás nyújtása más szolgáltató IaaS- vagy PaaS-rendszerére alapozva), alvállalkozói kérdéseket, • az átláthatósághoz és a folyamatos ellenőrzéshez biztosított eszközöket, módszereket, • a kiegészítő adatok védelmét (például felhasználói tevékenység adataiét vagy, mondjuk, a bejelentkezési adatok lopás, phising elleni védelmét), • kockázatkezelést.

[21] Electronically Stored Information – ESI.

Területek	Leírás
Architektúra	Az alábbi vizsgálandó kérdéseknél tekintettel kell lenni a szoftver- és hardverkörnyezetre, valamint a szolgáltatási modellre is: • a virtualizált környezetből adódó új támadási felületek (például új API-k, új csatornák, új adatfajták), • a virtuális hálózatok védelme (például virtuális gépek egymás közötti kommunikációjának védelme, biztonsági beállítások és adminisztrátori jogosultságok szétválasztása), • a virtuális gépek rendszermásolatai (image) (például ezek napra készen tartása, sérülékenységek és új szoftververziók miatt), • a kliensoldal védelme (például kliensoldali fizikai és logikai védelem, használt webböngésző plug-inek, közösségi oldalak használatának engedélyezése).
Hitelesítés, engedélyezés, hozzáférés-kezelés	Itt elsősorban a meglévő hagyományos rendszer és a felhőalapú rendszernél alkalmazott eljárások azonossá tételének vagy egyformára alakításának előnyeit, hátrányait kell számba venni az alábbiak tekintetében: • hitelesítés (például használt protokollok, mint *Security Assertion Markup Language* [SAML], az ezeket kihasználó támadási lehetőségek, mint az *Extensible Markup Language* [XML] *wrapping attack*, azonosítási szolgáltató használata, azonosítóadatok cseréje felhőalapú rendszer és a meglévő hagyományos hálózat között), • hozzáférés-szabályozás (például SAML mellett használt hozzáférés-szabályozó protokollok, mint az *Extensible Access Control Markup Language* [XACML], az ezeket kihasználó támadási lehetőségek, mint az ismétléses vagy visszajátszásos támadás).

Területek	Leírás
Szoftverelválasztás	A többfelhasználós környezet megköveteli a felhasználók szétválasztását, amelyeket az alábbiak mentén célszerű vizsgálni: • hypervisor komplexitása (például futó folyamatokat felügyelő szoftverek tulajdonságai), • lehetséges támadási vektorok (például hypervisor fertőzése virtuális gépből, közbeékelődéses támadás (Man in the Middle – MitM), memóriatartalom módosítása).
Adatvédelem	A többfelhasználós környezetbe vitt (érzékeny) adatok többi felhasználóval szembeni védelmét az alábbiak szerint érdemes vizsgálni: • az értékkoncentrációból adódó direkt és indirekt támadási lehetőségek (például ex-ploitok, rendszergazdák által használt közösségi oldalak támadása és indirekt módon hozzáférésijogosultság-szerzés, DoS-támadás, fizikai támadás), • adatizoláció (számtalan kérdéskört kell megvizsgálni ennek kapcsán, például hozzáférés-szabályozás, adatbázisok elszeparáltsága, interoperabilitás, adatok biztonsága használat, utazás és tárolás alatt, titkosítás, kulcsmenedzsment, ez utóbbi akár a kormányzati felhasználásra ajánlott *NIST Cryptographic Key Management Project* [NIST, s.d.d] alapján), • adatmegsemmisítés (például felülírás, hardvermegsemmisítés lehetőségei, szerződéses feltételek).
Rendelkezésre állás	A hagyományos ICT-rendszerekhez hasonlóan az alábbiakat célszerű vizsgálni: • átmeneti leállások (például szerződésben rögzített rendelkezésre állásból adódó kieső idő, tervezett karbantartások ideje, biztonsági mentések, katasztrófa utáni visszaállítás, esetleg másik felhőszolgáltatóra átállás), • hosszan tartó és folyamatos leállás (például szolgáltató leállása, csődje, létesítmény elvesztése, katasztrófaterv), • DoS-támadás (például külső támadás esélye, belső támadás lehetősége mind szándékos, mind véletlen támadás esetén).

Területek	Leírás
Incidensreagálás	Az incidens azonosítása, a támadás elemzése, az adatok, bizonyítékok gyűjtése, tárolása, a probléma közvetítése és a szolgáltatás visszaállítása kapcsán az alábbiakat célszerű áttekinteni: • adatok rendelkezésre állásának problémái (például nem megfelelő hozzáférés az erőforrásokhoz, sérülékenységek, nem megfelelő csatolófelületek az adatok eléréséhez és feldolgozásához, detektálási pontok elhelyezésének nehézségei, harmadik fél által jelentett visszaélések tudomásra hozási problémái), • incidenselemzés és értékelés (például nyomozati másolat készítése incidens után, támadási vektor azonosítása, a történtek rekonstruálása, gyors helyreállítás, incidenskezelési felelősségek, bizonyítékgyűjtési lehetőségek és hiányosságok, jelentési kötelezettségek a Computer Emergency • Readiness Team [CERT][22] felé, azok tartalma).

Forrás: a szerző szerkesztése a Jansen–Grance, 2011 alapján

A felhőalapú rendszer bevezetése kapcsán a szerzők további számos – a rendvédelmi szervek számára a biztonsági elemzéshez is hasznos – biztonsági kockázatra és tényezőre hívják fel a figyelmet. Így a fenti, a felhőalapú rendszerekhez kapcsolódó, kulcsfontosságúnak ítélt biztonsági és adatvédelmi kérdések mellett a NIST szakemberei további olyan elemeket is megneveznek, amelyek tapasztalataik alapján egy hagyományos informatikai kiszervezés kapcsán általános problémaként jönnek elő, de fontosak a felhőszolgáltató vagy -szolgáltatás kiválasztásához felállítandó követelményrendszer elkészítéséhez is. Ezek a következők:

- *„személyi feltételek, beleértve az engedélyeket, feladatokat és a felelősségeket,*
- *szabályozási előírások,*
- *a szolgáltatások rendelkezésre állása,*
- *problémák, incidensek jelentése, felülvizsgálata és értékelése,*
- *információkezelési és nyilvánosságra hozatali megállapodások és eljárások,*

[22] Számítástechnikai katasztrófaelhárító csoport.

- *fizikai és logikai hozzáférés-szabályozás,*
- *hálózati hozzáférés-szabályozás, kapcsolat és szűrés,*
- *adatvédelem,*
- *rendszerkonfiguráció és a javítócsomagok kezelése,*
- *biztonsági mentés és visszaállítás,*
- *adatmegőrzés és megsemmisítés,*
- *biztonsági és sérülékenységi vizsgálat,*
- *kockázatkezelés,*
- *incidensek jelentése, kezelése és lereagálása,*
- *üzletmenet-folytonosság,*
- *erőforrás-menedzsment,*
- *tanúsítványok és akkreditációk,*
- *biztosítási szintek,*
- *szolgáltatások független auditálása"* (Jansen–Grance 2011, 43. alapján a szerző fordítása).

A biztonság lehető legteljesebb körű megteremtéséhez a szolgáltatóval tisztázni kell a felelősségi körök megosztását, amely nagyban függ a szolgáltatási modelltől. Meg kell tőle követelni és ellenőrizni kell a katasztrófaelhárítási, továbbá üzletmenet-folytonossági terveket, valamint ki kell dolgozni a szolgáltató rossz teljesítésére vagy akár csődjére is vonatkozó kilépési stratégiát. Egyértelműen rögzíteni kell az elvárt szolgáltatási szinteket, a kapcsolódó szankciókat, a változások folyamatát, valamint a megfelelőségi követelményeket. Ez utóbbi esetében vannak országok, ahol egyértelmű előírások vannak; ahol pedig ilyen nincs, ott pontosan meg kell adni az irányadó jogszabályokat, különös tekintettel a biztonsági és adatvédelmi kérdésekre. A felhasználónak ezek tisztázása után kell elvégeznie a biztonsági és adatvédelmi szempontú kockázatértékelést, amelynek az alapja a szolgáltatási modell, a szolgáltatás célja, hatálya, a hozzáférés típusa, szintje, a szolgáltató, illetve a felhasználó számítási környezete közötti különbségek, a szolgáltatás időtartama, a kialakuló függőségek, a felajánlott biztonság erőssége, a szolgáltató telephelyeinek helyszínei, valamint a kezelt védendő vagy érzékeny adatok típusa. Kiemelést érdemel, hogy ez utóbbiak esetében a dokumentum külön kategóriában megemlíti a rendvédelmi szervek adatait is, bár az anyag többi részében ilyen jellegű kiemelés nincs, azoknál csupán általánosságban foglalkozik a kormányzati szervekkel. Amennyiben az értékelést követően előálló kockázati szint túl magas, a kontroll növelésével kell elfogadható

mértékűre csökkenteni. Amennyiben ez nem lehetséges, vagy már nem éri meg, akkor el kell tekinteni a felhő használatától.

Meg kell vizsgálni a felhőszolgáltató feladatra való alkalmasságát is, azaz képes-e, elkötelezett-e megvalósítani a biztonsági és adatvédelmi követelményeket. Ennek során a korábbiak mellett értékelni kell:

- *„a személyzet technikai szakértelmét és tapasztalatait,*
- *a személyzet átvilágítási folyamatát,*
- *a személyzetnek előírt biztonsági és adatvédelmi tudatosító képzések minőségét és gyakoriságát,*
- *a hozzáférés-szabályozási gyakorlatot és az elszámoltathatóságot,*
- *a biztosított biztonsági szolgáltatások és mögöttes mechanizmusainak jellegét és hatékonyságát,*
- *az új technológiák adaptálásának ütemét,*
- *a változásmenedzsmenti eljárásokat és folyamatokat,*
- *a felhőszolgáltató múltját,*
- *a felhőszolgáltató megfelelését a szervezet biztonsági és adatvédelmi politikájának, valamint a jogszabályi előírásoknak"* (Jansen–Grance 2011, 48. alapján fordította a szerző).

A dokumentum készítői kiemelik, hogy a felhőrendszereknél a magas biztonsági szint eléréséhez szükséges eszközök és módszerek egy része még kidolgozás alatt áll. Arra is felhívják a figyelmet, hogy a biztonsággal és adatvédelemmel kapcsolatos felelősségek a nyilvános felhő esetében nem delegálhatók a szolgáltatónak, azokért minden esetben a felhasználó felel. Éppen ezért ebből a szempontból a felhasználónak folyamatosan ellenőriznie kell a szolgáltató rendszerét, és meg kell győződnie arról, hogy a biztonsági, valamint az adatvédelmi kontroll korrektül, az elvárásinak megfelelően működik. Ugyanakkor ügyelni kell arra, hogy – a kockázatalapú megközelítésnek megfelelően – a biztonsági és adatvédelmi megoldások, továbbá a használhatóság között megmaradjon az egyensúly, a felhő előnyei ne vesszenek el, az hatékonyan használható maradjon. Ha ez már nem biztosítható, akkor nem szabad felhőalapú rendszert használni.

A NIST e dokumentumának (Jansen–Grance, 2011) több érdeme is kiemelhető. Egyrészt a biztonsági és adatvédelmi problémák a nyilvános felhőben jelentkeznek a legerősebben. Ennek megfelelően az itt végiggondolt elemek jól használhatók az állami szervek által inkább preferált

magán- vagy közösségi felhők biztonsági követelményeinek megfogalmazásakor. Másrészt a dokumentum sok kormányzati szerveknek szóló ajánlást és hivatkozott, a NIST által készített szakirodalmat tartalmaz, amely jól használható akár a rendvédelmi szervek számára is. Ugyanakkor a leírtak felhasználásakor két dolgot mindenképpen figyelembe kell venni. Az *egyik* kifejezetten a rendvédelmi szervekre vonatkozó megfontolás, miszerint ők az állami szervekhez képest nagyobb mennyiségű magasabb szintű biztonságot igénylő, jobban védendő adatot kezelnek. A *másik,* már általánosabb jellegű, az Egyesült Államok és az Európai Unió országai közötti jogi, technikai lehetőségek különbözősége. Míg az Egyesült Államokban könnyen találhatunk a teljes infrastruktúráját is ott üzemeltető szolgáltatót, addig ez ma az Európai Unió még nagyobb tagországaira sem jellemző. Így az ebből adódó problémákat mindenképpen kiemelten kell kezelni. Ennek megfelelően ezt a dokumentumot – a CSA ajánlásai kapcsán már megfogalmazott megfelelő átalakítások mellett – a rendvédelmi szerveknek is érdemes figyelembe venniük a felhőalapú rendszerek kockázatainak elemzéséhez.

A FedRAMP (a cloud.cio.gov weboldal) fontosabb ajánlásai

A NIST dokumentumaiban sok helyen foglalkoznak a kormányszervek információbiztonsági kérdéseivel, hol kifejezetten az ő igényeiket szem előtt tartva, hol pedig a gazdasági társaságok mellett külön megemlítve a rájuk vonatkozó szigorúbb előírásokat és információbiztonsági követelményeket. A *cloud.cio.gov* (cloud.cio.gov, s.d.a), majd az ezt felválltó *fedramp.gov* (FedRAMP, s.d.) weboldalt az Egyesült Államok kormánya hozta létre *Federal Risk and Authorization Management Program* (FedRAMP)[23] (cloud.cio.gov, s.d.b) nevű program keretében. Ez egy kormányzati szintű program, amely a felhőszolgáltatások biztonsági értékeléséhez és ellenőrzéséhez kínál szabványosított megközelítést. Mindezt a „csináld egyszer, használd sokszor" megközelítés jegyében, azaz a kormányhivataloknak nem kell külön-külön összeszedniük a felhőalapú rendszerek biztonságos használatához szükséges kritériumokat, követelményeket, ezeket elkészítik és elérhetővé teszik számukra a program keretében.

[23] Szövetségi Kockázat- és Jogosultságkezelési Program.

Ennek kapcsán meg kell jegyezni, hogy a FedRAMP szorosan együttműködik például az Egyesült Államok Belbiztonsági Minisztériumában, Nemzetvédelmi Minisztériumában, de akár magáncégeknél dolgozó kiberbiztonsági és felhőszakértőkkel is, így nagyban támaszkodik – többek között – a program egyik kulcsszervezeteként megjelölt NIST szakembereire és dokumentumaira is. Ugyanakkor bár maga a FedRAMP, valamint a fedramp.gov oldal és az itt található összes dokumentum kifejezetten kormányzati szerveknek szól, a hivatkozott NIST-dokumentumok egy része nem kizárólag vagy nem kifejezetten az említett szerveknek készült.

A program főbb céljai:

- *„az értékelések és engedélyek újrafelhasználásán keresztül gyorsítsa egy biztonságos felhőalapú rendszer bevezetését,*
- *növelje a felhőalapú rendszerek biztonságába vetett bizalmat,*
- *elfogadott szabványokon alapuló alapkövetelmények következetes betartásával biztosítsa a felhőtermékek biztonsági engedélyezését a FedRAMP-on belül és azon kívül is,*
- *biztosítsa a meglévő biztonsági gyakorlatok következetes alkalmazását,*
- *növelje a biztonsági értékelésbe vetett bizalmat,*
- *növelje az automatizálást és a közel valós idejű adatokat a folyamatos felügyelethez”* (A FedRAMP, s.d. alapján fordította szerző).

A program előnyei:

- *„növeli a meglévő biztonsági értékelések újbóli felhasználását az ügynökségek között,*
- *jelentős költséget, időt és erőforrást takarít meg – »csináld egyszer, használd sokszor«,*
- *javítja a valós idejű biztonsági átláthatóságot,*
- *a kockázatalapú menedzsmenthez egységes megközelítést biztosít,*
- *növeli az átláthatóságot a kormányzat és a felhőszolgáltatók között,*
- *javítja a szövetségi biztonsági engedélyezési eljárások megbízhatóságát, következetességét és minőségét”* (A FedRAMP, s.d. alapján fordította szerző).

A FedRAMP a célok eléréséhez és az előnyök biztosításához az alábbi, háromlépéses folyamatban engedélyezi a felhőalapú rendszereket:

> *„Biztonsági értékelés: a biztonsági engedélyek kiadásához használt biztonsági értékelési folyamat olyan szabványosított követelménycsomagokat alkalmaz, amelyek összhangban vannak a NIST 800–53 alapkövetelményeire épülő Federal Information Security Modernization Act (FISMA-)*[24] *elnevezésű törvényben megfogalmazottakkal.*
> *Felhasználás és engedélyezés: a szövetségi ügynökségek hozzáférnek a FedRAMP gyűjteményében található biztonsági engedélyezési csomagokhoz, és felhasználhatják azokat saját biztonsági engedélyeik kiadásához.*
> *Folyamatos értékelés és engedélyezés: az engedély megadását követően a biztonsági engedély fenntartásához folyamatos értékelési és engedélyezési tevékenységeket kell végrehajtani”* (A FedRAMP, s.d. alapján fordította szerző).

A FedRAMP korábbi és jelenlegi oldalán is több, a rendvédelmi szervek részére a felhőalapú rendszerek biztonsági értékeléséhez felhasználható információt, szempontot, kockázatot ismerhetünk meg.

A felhőalapú rendszerek kormányzati szervezetek általi használatának bevezetésekor a legnagyobb kihívást éppen az általuk megkövetelt biztonsági szabványok és protokollok előírásaiban foglaltak elérése, valamint betartása jelenti. Éppen ezért ebben az esetben kiemelt szerepe van a kockázatelemzésnek, ám figyelni kell arra, hogy az elemzés eredményeként előálló szintnek megfelelő biztonság megteremtését kell kitűzni célként, a túlzottan magas biztonsági szint ugyanis a költségeket is jelentősen emeli, ez pedig éppen a felhő egyik legvonzóbb tulajdonságát, a jobb költséghatékonyságot negligálhatja.

A felhőtechnológia okán megjelenő új kockázatok miatt folyamatos ellenőrzésre is szükség van. Ugyanakkor azt is vizsgálni kell, hogy a megkívánt és alkalmazott biztonsági eszközök és módszerek elég hatékonyak-e, azaz egyfajta periodikus kockázatelemzéssel kell segíteni azt a döntést, hogy megfelelő-e a jelenlegi biztonsági rendszer, vagy változtatások szükségesek-e.

---

[24] Szövetségi Információbiztonsági Korszerűsítési Törvény.

Az amerikai kormányzati program kapcsán közzétett anyagokból további egy, a felhőalapú rendszer bevezetését megelőzően akár a rendvédelmi szervek számára is hasznosítható, biztonsággal kapcsolatos megfontolást lehet megismerni. Ilyen például, hogy az adatok kihelyezése előtt mindig figyelembe kell venni azok típusát (például személyes adat, érzékeny adat stb.), valamint azon ország adatvédelmi és egyéb vonatkozó jogszabályait, amelyben a felhőszolgáltató szerverei találhatók. Mindemellett a szerződésben erős szabályokat szükséges megfogalmazni az adatvédelemre, felállítva a minimum biztonsági szinteket, hiszen adott esetben akár harmadik félnek (például a szolgáltató alvállalkozója) is teljes hozzáférése lehet az ide kivitt adatokhoz. Ugyancsak a szerződésben célszerű tisztázni, mi a teendő incidens vagy külföldi hatóság adatszolgáltatási megkeresése esetén, illetve itt kell rögzíteni az ezekhez kapcsolódó reagálási és értesítési időket is.

Biztonsági incidensek kezelése kapcsán előre és pontosan meg kell határozni az alkalmazott biztonsági kontrollokat, valamint, hogy a különböző események egyedüli vagy megosztott felelősséget indukálnak-e. Megosztott felelősség esetén ügyelni kell arra, hogy mindkét fél előírásai, eljárásai, illetve szabályai egyformák legyenek a teljes helyszíni és felhő-infrastruktúra tekintetében egyaránt. Ehhez meg kell állapítani, hogy a szervezeteknek és a szolgáltatónak milyen szabályokat, továbbá törvényeket kell alkalmaznia, valamint azt, milyen gyorsan kell reagálnia, detektálnia, csökkentenie a kárt, visszaállítania az eredeti állapotot, és jelentenie az eseményt.

A FedRAMP szakemberei hangsúlyozzák, hogy bár bizonyos felelősségek átruházhatók vagy megoszthatók, azonban az adatok bizalmasságának, sértetlenségének és rendelkezésre állásának teljes felelősségét mindig a kormányzati szerv viseli.

A weboldal nagyon sok hasznos információval szolgál olyan, kifejezetten kormányzati szerveknek, amelyek felhőalapú szolgáltatást kívánnak igénybe venni. Ezekhez a korábban engedélyezett vagy engedélyezés alatt lévő termékek listája mellett olyan kulcsfontosságú dokumentumokat és sablonokat is biztosít, mint az alkalmazandó szabályozókat és szabványokat is tartalmazó *Security Assessment Framework* (cloud.cio.gov, s.d.c), a folyamatos ellenőrzést részletesen leíró *Continuous Monitoring Strategy & Guide* című dokumentumok (FedRAMP, 2012a) vagy a rendszer biztonsági tervezését segítő *System Security Plan* (SSP-) sablonok (FedRAMP, 2012b). Rendkívül fontos az a gondolat, hogy minden kormányzati szerv egységes megközelítés alapján tudja értékelni a felhőalapú rendszereket, biztonsági kockázataikat. Ez azért is lényeges, mert így nem adódhat az a hiba, hogy

valamit éppen kifelejt a kockázatelemzéssel foglalkozó szakember. A másik, itt is visszatérő és nagyon fontos elem maga a kockázatértékelés. A biztonság ugyanis pénzbe kerül, és az adatokat, rendszereket mindig kockázati alapon kell védeni, legyen szó akár felhő-, akár fizikailag a felhasználónál lévő rendszerekről, adatokról.

Ugyanakkor a weboldalon leírtak kapcsán figyelembe kell venni, hogy azok az Egyesült Államokban lévő kormányzati szerveknek szólnak, ahol más szabályozások, előírások érvényesek, ráadásul az esetek többségében az ország területén működő, ott alapított és ott székelő felhőszolgáltató választható a szervezet által kitűzött célok eléréséhez. Ez ma nemhogy Magyarországon, de még Európában sincs így, ráadásul a szabályozási környezet is jóval hiányosabb és országonként is eltérő. Ezeket pedig mind figyelembe kell venniük egy felhőalapú rendszer esetleges használatának tervezésekor, különösen a sok személyes és érzékeny, sokszor akár minősített adatot is kezelő rendvédelmi szerveknek.

A Német Szövetségi Információbiztonsági Hivatal (BSI)[25] fontosabb ajánlásai

A Német Szövetségi Információbiztonsági Hivatal egy olyan állami szervezet, amelynek fő célja, hogy emelje az ICT-biztonságot és -biztonságtudatosságot Németországban. A gyakorlatban a BSI amellett, hogy ellátja a kormányzat központi ICT-biztonsági szolgáltatója szerepét, egyéni és üzleti, valamint ICT-cégeknek is nyújt szolgáltatásokat. Az általuk megfogalmazottak szerint egyrészt azért, hogy az azonos gondolkodásmód és felhasznált szabványok kialakításával elősegítse az együttműködést az említettek között; másrészt, mert az ICT-biztonság csak úgy teremthető meg, ha az érintettek együttműködnek, és ahhoz mindenki hozzáteszi a maga részét. A BSI éppen ezért ICT-felhasználással kapcsolatos biztonsági kockázatok kutatásával, értékelésével, a megelőzéshez szükséges eszközök kidolgozásával, valamint ICT-rendszerek biztonsági tesztelésével és értékelésével foglalkozik (Federal Office for Information Security, s.d.).

A felhőalapú rendszerek biztonságával kapcsolatban, a 2011-ben közreadott, *Security Recommendations for Cloud Computing Providers* című fehér könyvük (Federal Office for Information Security, 2011) tekinthető

[25] Bundesamtes für Sicherheit in der Informationstechnik.

irányadónak. A dokumentum közvetlen célja az, hogy az e rendszerek használatához kötődő biztonság kapcsán megteremtse az egységes alapot a szolgáltató és a felhasználó párbeszédéhez, távolabbi célja pedig az, hogy elősegítse olyan specifikus követelmények kidolgozását, amelyek mentén a magánszemélyek és a magáncégek is biztonságosan használhatják a felhőalapú rendszereket, szolgáltatásokat. A dokumentum azonban mégis alapvetően a szolgáltatóknak készült, célközönségének a szolgáltató (és a felhasználó) ICT-szakemberei tekinthetők, a megfogalmazott ajánlások pedig elsősorban a vállalatokat és a közintézményeket, és nem a magánfelhasználókat kiszolgáló felhőszolgáltatóknak szólnak (Federal Office for Information Security, 2011). Ahogy azt a NIST is megjegyezte saját dokumentumaival kapcsolatban, úgy a BSI is aláhúzza, hogy egy konkrét rendszer vizsgálata kapcsán, a gyors fejlődés okán mindig szükség van az ebben az anyagban leírtak újragondolására, az aktuális állapotoknak megfelelő kiegészítésére, felülvizsgálatára.

A német szakemberek által javasolt metodológia szerint a szolgáltatóknak az olyan normák szerint kell kiépíteniük a biztonsági rendszereket a számítási felhőben, mint az *ISO 2700I*[26] vagy a *BSI 100–2 IT-Grundschutz Methodology*[27]. Ehhez a szolgáltatóknak el kell készíteniük a kockázatelemzést, amely keretében azonosítják az általuk nyújtott szolgáltatásokkal kapcsolatos aktuális és releváns veszélyeket, és ehhez mérten kell dönteniük azok kezelésének módjáról, eszközeiről. Mindemellett a felhasználónak is értékelnie kell a kockázatokat, és döntenie az általa elfogadható biztonsági szintről. Akárcsak a FedRAMP szakemberei, a BSI munkatársai is kiemelik, hogy az elfogadható biztonsági szint elérése a kívánatos, hiszen a biztonság növelésével a költségek is jelentősen emelkednek.

A dokumentum a felhőalapú rendszereken tárolt, feldolgozott normáltól a magas védelmi szintet igénylő információk kapcsán felmerülő biztonsági kérdésekre fókuszál, de nem vizsgálja kifejezetten a nemzeti minősített adatok védelmét. A vizsgálatok kapcsán a bizalmasságot és a rendelkezésre állást kezelték kiemelten, a sértetlenség kérdése ebben az anyagban nem kapott kiemelt külön figyelmet. Ennek megfelelően az ajánlásokat is három csoportba sorolták:

---

[26] ISO 27001 – az információbiztonsági irányítási rendszerek követelményszabványa.

[27] BSI 100-2 IT-Grundschutz Methodology, vagyis IT alapvető védelmi módszertan a BSI által az információbiztonság hatékony menedzselése érdekében kifejlesztett módszertan, amely könnyen hozzáigazítható az egyes szervezetek speciális helyzetéhez.

- *Category B* (alapkövetelmények): ebben a kategóriában a minden szolgáltató számára érvényes alapkövetelmények találhatók,
- *Category C+* (magas bizalmasság): ebben a kategóriában az alapkövetelményekhez képest már további járulékos követelmények is megjelennek a magas bizalmassági szintű adatok miatt,
- *Category A+* (magas rendelkezésre állás): ebben a kategóriában az alapkövetelményekhez képest már további járulékos követelmények is megjelennek a magas rendelkezésre állású szolgáltatások miatt.

A BSI által azonosított, különböző kulcsfontosságú biztonsági területekhez – a nyilvános és a magán számítási felhőre vonatkoztatva – táblázatos formában adják meg a legfontosabb információkat. Ilyenek például, hogy az egyes területeket melyik fenti kategóriába (B, C+, A+) eső adat vagy szolgáltatás esetén kell megvizsgálni, hogy a két telepítési modellnél az adott terület veszélyszintje átlagos vagy magas-e, hogy melyek az adott terület kapcsán a konkrétan vizsgálandó kérdések, továbbá, hogy az adott terület melyik szolgáltatási modellre értelmezhető vagy nem értelmezhető.

A biztonsági kérdések vizsgálatához, a szolgáltatóval szemben támasztott, ehhez kapcsolódó követelmények kidolgozásához az alábbi lépéseket javasolják elvégezni:

- az összes interfész elhatárolása és azonosítása érdekében az ICT-rendszerek és -alkalmazások struktúrájának elemzése,
- az ICT-rendszerek, -alkalmazások és -adatok védelmi követelményének meghatározása,
- adatok, alkalmazások, rendszerek és felhőszolgáltatások védelmi követelmények szerinti kategorizálása,
- a meghatározó működési és jogi keretek tisztázása,
- a szolgáltatóval szemben támasztott konkrét biztonsági követelmények meghatározása.

A BSI a következő biztonsági fő- és részterületeket azonosította és vizsgálta:

1. a szolgáltató által biztosított biztonsági menedzsment,
2. biztonsági architektúra, ezen belül:
   2.1. adatközpont-biztonság,
   2.2. szerverbiztonság,
   2.3. hálózatbiztonság,
   2.4. alkalmazás- és platformbiztonság,
   2.5. adatbiztonság,
   2.6. titkosítás és kulcskezelés,

3. azonosítás és jogosultságkezelés;
4. felhasználóikontroll-lehetőségek,
5. monitoring és biztonsági események kezelése,
6. üzletmenet-folytonosság menedzsmentje,
7. hordozhatóság és interoperabilitás,
8. biztonsági tesztelés és audit,
9. személyi követelmények,
10. megállapodás kidolgozása, ezen belül:
    10.1. átláthatóság,
    10.2. szolgáltatásiszint-megállapodás,[28]
11. adatvédelem és megfelelőség, ezen belül:
    11.1. adatvédelem,
    11.2. megfelelőség.

A BSI dokumentuma a korábban elemzettekhez képest egy új csoportosításban közelíti meg a felhőalapú rendszerek biztonsági kérdéseit. Az itt leírtak ugyanakkor – érthető módon – sok átfedést mutatnak a korábban ismertetett anyagokkal, mégis több helyen kiegészíti azokat, vagy akár új adalékokkal is tud szolgálni.

A dokumentum bár alapvetően a szolgáltatóknak készült, kiemelten hasznos az állami felhasználók részére is. Ugyan nem teljes mértékben fedi le a rendvédelmi szervek igényeit, mégis számukra is felhasználható módon azonosítja az egyes kritikus biztonsági területeket, az ezeknél megjelölt vizsgálandó kérdések pedig nekik is jó útmutatóként szolgálhatnak. Az anyag további különösen jelentős előnye az, hogy egy – minden téren vezetőnek számító – európai ország kormányzati információbiztonságért felelős szervezete készítette, amely hasonló jogi, szabályozási és technikai, szolgáltatói környezetben; ráadásul a kormányzati szervek igényeit a fókuszban tartva fogalmazta meg az ebben leírt követelményrendszert. Emiatt pedig könnyebben adaptálható a hazai viszonyokra, mint az Egyesült Államok szervezeteinek hasonló témában készített anyagai.

További hasznos információt nyújt a BSI által 2013-ban közzétett *Cross Reference Table threats and safeguards for module cloud management* táblázat (Federal Office for Information Security, 2013). Ez megmutatja, milyen védelmi megoldásra milyen veszély esetén van szükség a felhőalapú rendszerek esetében, és hozzájuk rendeli, hogy az életciklus melyik szakaszában

[28] Service Level Agreements – SLA.

kell értelmezni (például tervezés, működés stb.) azokat. Megadja a hozzájuk tartozó besorolási szintet (például belépő, azaz kötelező, tanúsításhoz szükséges, járulékos stb.) is. Ezt a táblázatot kiegészítőként is lehet használni a felhőkockázatok felméréséhez alapdokumentumnak tekinthető CSA *Cloud Controls Matrix* (CSA, 2014a) táblázathoz mindamellett, hogy a kettő célja és részletezettsége sem azonos.

Az Európai Hálózat- és Információbiztonsági Ügynökség fontosabb ajánlásai

Az Európai Hálózat- és Információbiztonsági Ügynökség[29], azaz a tagállamok és intézmények érdekében tevékenykedő, azokkal együttműködő szakértői központ meghatározó szerepet tölt be az európai információbiztonság területén. Egyik legfontosabb feladata ezen a területen az ismeretek, a legjobb gyakorlatok terjesztése, valamint az információcsere biztosítása. Az ENISA mint az EU által felállított, Európai Ügynökségként dolgozó szakértői testület specifikus technikai és tudományos feladatokat is ellát, valamint segíti az Európai Bizottság hálózat- és információbiztonsághoz kapcsolódó jogszabály-előkészítő és -fejlesztő munkáját (ENISA, s.d.a).

Az említett feladatok ellátása kapcsán természetesen a felhőalapú rendszerekkel és kifejezetten azok biztonságával kapcsolatban is tettek közzé anyagokat. Ezek közül két dokumentumot érdemes kiemelni. Elsőként – az időrendben korábban elkészített, a második dokumentumban is kiindulási alapnak tekintett és sokszor hivatkozott – *Cloud Computing: Benefits, risks and recommendations for information security* című anyagot (Cloud Computing, 2009) érdemes áttekinteni.

A dokumentum készítői – a korábban bemutatott szervezetek szakembereihez hasonlóan – utalnak arra, hogy a felhőalapú rendszerek biztonsági szempontból kettős arcot mutatnak. Egyrészről, elsősorban az adatok koncentráltsága okán, vonzó célpontjai a támadásoknak, másrészről viszont általában sokkal robusztusabb védelemmel rendelkeznek, mint a hagyományos ICT-rendszerek. E kettősséget figyelembe véve a dokumentum együtt értékeli a felhő előnyeit és biztonsági kockázatait, mindemellett biztonsági útmutatót ad a felhasználóknak. Mindezt úgy, hogy a hálózat- és információbiztonság, az adatvédelem szempontjából megközelítve technikai,

[29] European Union Agency for Network and Information Security – ENISA.

eljárásmódbeli, valamint jogi következtetéseket von le, majd konkrét ajánlásokat tesz a kockázatok csökkentésére és az előnyök maximalizálására (Cloud Computing, 2009). A felhőbiztonság értékelését három forgatókönyvön keresztül mutatja be:

1. kis- és középvállalati migráció felhőbe,
2. a számítási felhő hatása a szolgáltatás rugalmasságára, ellenálló képességére,
3. felhő az e-kormányzatban (például e-egészségügy).

Ebből tisztán látszik, hogy a NIST-hez hasonlóan nem kizárólag a kormányzati szervek szemszögéből közelítik meg a kérdést, de velük is, vagy legalábbis egy bizonyos részükkel, érdemben foglalkoznak az anyagban. Ugyanakkor az Európai Bizottság és a fejlesztők számára is megfogalmaznak ajánlásokat, amelyek jól mutatják, hogy kontinensünkön milyen generális problémák nehezítik a felhőalapú rendszerek használatát. Az Európai Bizottságot az adatvédelemmel, felhőszolgáltatók kötelezettségeivel – különösen a felhasználók adataihoz fűződő biztonsági események és az elektronikus kereskedelemmel összefüggő közvetítőkre vonatkozó felelősség alóli felmentés kapcsán –, valamint a tagállamokban az egységes minimum adatvédelmi standardok kialakításával, támogatásával kapcsolatos kérdések tanulmányozására és tisztázására hívják fel. A fejlesztők számára pedig a felhőrendszerek biztonságának növeléséhez az alábbi kiemelt területeket javasolják kutatni, fejleszteni:

- bizalom kiépítése a felhőben:
  - biztonsági események bejelentése különböző formáinak hatása,
  - végpont-végpont közötti titkosítás a felhőben és azon túl,
  - magasabb biztonságú felhők, virtuális privát felhők stb.,
- nagyméretű, szervezeteken átnyúló rendszerek adatvédelme:
  - nyomozati és bizonyítékgyűjtési mechanizmusok,
  - incidenskezelés – monitoring és visszakövethetőség,
  - a vonatkozó nemzetközi előírások különbségei, beleértve az adatvédelmet,
- nagy méretű számítógépes rendszerek tervezése:
  - erőforrás-izolációs mechanizmusok (például adatok, feldolgozás, memória, naplók),
  - felhőszolgáltatók közötti interoperabilitás,
  - felhőszolgáltatások rugalmasságának, ellenálló képességének növelése.

Ez a javaslat rávilágít a felhőalapú rendszerek legjelentősebb biztonsági kockázataira, amelyek sarkalatosak a rendvédelmi szervek számára is, ezért ezeket a biztonsági elemzés során mindenképpen célszerű figyelembe venni.

A kormányzati szerveknek szóló elemzésekben az ENISA szakemberei egyértelműen megállapítják, hogy a költségcsökkentés és a képességek növelése okán a kormányzatok, állami intézmények érdekeltek a felhőalapú rendszerek használatában, azonban több aktuális problémával is szembesülnek. Jelenleg sok jogi és szabályozási előírás, így például a személyes adatok kezelésének előírásai is akadályozzák az e-kormányzati feladatok felhőbe költöztetését, ugyanakkor a belső szabályzóktól, előírásoktól függetlenül vagy éppen azok ellenére is sok alkalmazott használ felhőalapú szolgáltatásokat. A különböző szolgáltatási modellek (IaaS, PaaS, SaaS) esetében az előnyök és a kockázatok is jelentősen eltér(het)nek egymástól, így a szolgáltatás típusát mint az egyik legfontosabb tényezőt az elemzésnél, az értékelésnél és a szerződéskötésnél is mindig figyelembe kell venni. A felhőszolgáltatás bevezetését megelőző tervezéskor az alábbi, ellenőrzési lista formájában felépített dokumentumok megfelelő kiinduló eszközként szolgálhatnak a felhasználók számára:

1. felhőszolgáltatás alkalmazásának kockázatértékelése,
2. különböző felhőszolgáltatók ajánlatainak összehasonlítása,
3. a kiválasztott szolgáltatóknál elérhető biztonságot garantáló biztosítékok,
4. felhőszolgáltatók biztonsági terhének csökkentési lehetőségei.

A biztonsági ellenőrző listáknak a biztonsági követelmények teljes palettáját le kell fednie, beleértve a fizikai biztonságot, a szabályozási és technikai kérdéseket is.

A dokumentum jogi ajánlásai alapvetően a szerződéskötéshez, azon belül is főleg a hagyományos ICT-rendszereknél megszokottak mellett éppen a felhőtechnológia miatt megjelenő új elemek, kockázatok kezeléséhez nyújtanak segítséget. A megfogalmazottak szerint a biztonsági feladatok egyértelmű delegálása mellett kiemelt figyelmet kell fordítani a felek jogaira és kötelezettségeire, különös tekintettel a biztonsági szabályok megsértésére, az adatok átvitelére, a származékos művek alkotására, a kontroll változására, valamint a rendvédelmi szervek részére az adathozzáférés biztosítására.

A felhőalapú rendszerek biztonsági kockázatainak értékelését az ENISA szakértői az *ISO 27005:2008* előírásain alapuló, nyolcfokozatú skála segítségével végezték el, amely szerint:

- alacsony kockázat: 0–2,
- közepes kockázat: 3–5,
- magas kockázat: 6–8.

A kockázati szinteket azok üzleti hatása és a bekövetkezés valószínűsége alapján a 6. táblázat szerint ábrázolták.

6. táblázat

Felhőalapú rendszerek kockázatértékelési táblázata az ISO 27005:2008 alapján

	Incidens valószínűsége	**Nagyon valószínűtlen (nagyon alacsony)**	**Valószínűtlen (alacsony)**	**Lehetséges (közepes)**	**Valószínű (magas)**	**Nagyon valószínű (nagyon magas)**
Üzleti hatás	Nagyon alacsony	0	1	2	3	4
	Alacsony	1	2	3	4	5
	Közepes	2	3	4	5	6
	Magas	3	4	5	6	7
	Nagyon magas	4	5	6	7	8

Forrás: a szerző szerkesztése a Cloud Computing, 2009: 22 alapján

Az ENISA által azonosított kockázathoz tartozó valószínűségeket egy szakértői csapat állította össze, de volt olyan tényező, amelyhez nem adtak meg értéket. Az értékelés kapcsán a dokumentum készítői több dolgot is leszögeznek. Először is, hogy a felhőalapú rendszerek kockázatait mindig a hagyományos ICT-megoldások kockázatával kell összehasonlítani. Másodszor, hogy a kockázatok szintje felhőtípusonként változik, a dokumentum pedig általánosságban vizsgálódik, ezért mindig a konkrét esetre kell adaptálni a leírtakat. Harmadszor, hogy a kockázatok csökkentésének, elhárításának felelőssége némely esetben ugyan átruházható a szolgáltatóra, ám nem mindegyikben. Sőt, a legfontosabbak mindig a felhasználónál, azaz az adatok tulajdonosánál maradnak. Végül pedig, hogy a kockázatok értékelését a dokumentumban a felhasználó és nem a szolgáltató szemszögéből vizsgálták. A kockázatokhoz rövid ismertetőt csatoltak, sőt több esetben szolgáltatási modellenként elemezték az egyes modellekre vonatkozó

eltéréseket is. Minden kockázati elemet egységes, az összehasonlítást jól szolgáló táblázatban is bemutatnak, amely tartalmazza:

- a bekövetkezés valószínűségének és a kockázat hatásának szintjét (ahol értelmezhető, ott megadva, hogy ezek magasabbak, egyenlők vagy alacsonyabbak-e, mint a hagyományos ICT-rendszereknél),
- a kapcsolódó, hivatkozott sérülékenységeket,
- a kapcsolódó, hivatkozott érintett vagyonelemeket,
- a kockázat 6. táblázatban bemutatottak szerinti szintjét.

Az alábbi, 7. táblázat szemlélteti az ENISA által azonosított kockázatokat, azok általuk történt csoportosítását, valamint az egyes elemek értékelését.

7. táblázat

Az ENISA által azonosított kockázatok felhőalapú rendszerek vizsgálatához

Kockázatok					
Megnevezés			**Szint**		
			Valószínűség	**Hatás**	**Teljes kockázati szint**
Szabályozási és szervezeti kockázatok					
R.1	Adatok, szolgáltatások hordozhatóságának nehézségei (lock-in)		magas	közepes	magas
R.2	Irányítás elvesztése		nagyon magas	nagyon magas	magas
R.3	Megfelelőségi kihívások		nagyon magas	magas	magas
R.4	Üzleti reputációvesztés társfelhasználók tevékenysége miatt		alacsony	magas	közepes
R.5	Felhőszolgáltatás megszűnése vagy hibája		n. a.	nagyon magas	közepes
R.6	Felhőszolgáltató felvásárlása		n. a.	közepes	közepes
R.7	Ellátási lánc hibája		alacsony	közepes	közepes
Technikai kockázatok					
R.8	Erőforrások kimerülése (alultervezés vagy túligénylés miatt)	R.8a) pluszkapacitások tekintetében	közepes	alacsony/ közepes	közepes
		R.8b) szerződésben foglalt kapacitások tekintetében	alacsony	magas	

Kockázatok					
Megnevezés			Szint		
			Valószínűség	Hatás	Teljes kockázati szint
R.9	Izolációs hiba	R.9a) magánfelhő esetén	alacsony	nagyon magas	magas
		R.9b) nyilvános felhő esetén	közepes		
R.10	Felhőszolgáltató rosszindulatú belső munkatársa – visszaélés magas jogosultsággal		közepes	nagyon magas	magas
R.11	Kezelőfelület kompromittálódása		közepes	nagyon magas	közepes
R.12	Továbbított adatok lehallgatása (aktív módszerekkel)		közepes	magas	közepes
R.13	Adatszivárgás fel- és letöltéskor (passzív lehallgatás a felhasználó és a szolgáltató közötti úton)		közepes	magas	közepes
R.14	Adatok nem teljes vagy nem biztonságos törlése		közepes	nagyon magas	közepes
R.15	Elosztott szolgáltatásmegtagadásos támadások[30]		közepes	magas	közepes
R.16	Gazdasági szolgáltatásmegtagadásos támadás vagy erőforrás-felhasználás		alacsony	magas	közepes
R.17	Titkosító kulcs elvesztése		alacsony	magas	közepes
R.18	Rosszindulatú hálózatfeltérképezések		közepes	közepes	közepes
R.19	Szolgáltatásmotor szoftverének kompromittálódása		alacsony	nagyon magas	közepes
R.20	Konfliktus a felhasználó biztonságot szolgáló megerősítő tesztelési eljárásai és a felhőkörnyezet között		alacsony	közepes	közepes
Jogi kockázatok					
R.21	Elektronikus felderítés és bizonyítékgyűjtés		magas	közepes	magas
R.22	Illetékes igazságszolgáltatás változásából adódó kockázat		nagyon magas	magas	magas
R.23	Adatvédelmi kockázatok		magas	magas	magas
R.24	Licencelési kockázatok		közepes	közepes	közepes

[30] Az ENISA-dokumentumban található értékek közül a felhasználó szemszögéből adott értéket vettem figyelembe.

Kockázatok				
Megnevezés		Szint		
		Valószínűség	Hatás	Teljes kockázati szint
Nem felhőspecifikus kockázatok				
R.25	Hálózatleállás	alacsony	nagyon magas	közepes
R.26	Hálózatkezelési problémák (például torlódás, nem optimális használat, hibás kapcsolódás)	közepes	nagyon magas	magas
R.27	Hálózati forgalom módosítása	alacsony	magas	közepes
R.28	Túl magas jogosultságok	alacsony	magas	közepes
R.29	Social engineering[31] típusú támadások	közepes	magas	közepes
R.30	Üzemeltetési naplóállomány elvesztése vagy kompromittálódása	alacsony	közepes	közepes
R.31	Biztonsági naplóállomány elvesztése vagy kompromittálódása	alacsony	közepes	közepes
R.32	Biztonsági mentés elvesztése, ellopása	alacsony	magas	közepes
R.33	Illetéktelen hozzáférés telephelyekhez	nagyon alacsony	magas	közepes
R.34	Eszközök ellopása	nagyon alacsony	magas	közepes
R.35	Természeti katasztrófák	nagyon alacsony	magas	közepes

Forrás: a szerző szerkesztése a Cloud Computing, 2009 alapján

[31] A social engineering, más néven pszichológiai manipuláció lényege, hogy egy infokommunikációs rendszerhez nem technikai úton, hanem pszichológiai módszerekkel szerzi meg a támadó a jogosulatlan hozzáférést egy vagy több, ahhoz jogosultsággal rendelkező személytől. A jogosulatlan hozzáféréshez szükséges adatokhoz az arra jogosultaktól, azok emberi tulajdonságait, főként az emberek segítőkészségét, hiszékenységet, befolyásolhatóságot és konfliktuskerülő hajlamát kihasználva jut a támadó, általában sok apró lépéssel. A későbbiekben pedig az így megszerzett adatok és jogosultság felhasználásával hajtja végre a támadását a kiszemelt rendszer ellen. A social engineering során használt legjellemzőbb módszerek a segítség kérése, a „valamit adok valamiért" elv alkalmazása, a főnök megszemélyesítése, nem létező felhatalmazásra hivatkozás, „fordított szúrás" (reverse social engineering) és az adathalászat különböző módszerei (Oroszi, 2008).

A hatások és a bekövetkezési valószínűségek szintjét az esetek egy részében több értékkel vagy n. a., azaz nincs adat jelzéssel adták meg a szakértők. Ekkor olyan tényezőktől függ a tényleges érték, mint a felhő típusa, a felhasználó saját hálózata stb. Ez is alátámasztja a korábban már rögzített megállapítást, hogy a dokumentum általános jelleggel készült, annak tényleges felhasználásakor mindig az adott eszközöket, hálózatot és a tényleges felhasználói igényeket, követelményeket kell figyelembe venni.

Az azonosított kockázatok lehetséges bekövetkezését és hatását figyelembe véve elhelyezhetjük azokat a korábban említett kockázatértékelési táblázatban (8. táblázat).

8. táblázat

A felhőalapú rendszerek ENISA által azonosított kockázatainak eloszlása

	Incidens valószínűsége	**Nagyon valószínűtlen (nagyon alacsony)**	**Valószínűtlen (alacsony)**	**Lehetséges (közepes)**	**Valószínű (magas)**	**Nagyon valószínű (nagyon magas)**
Üzleti hatás	Nagyon alacsony	0	1	2	3	4
	Alacsony	1	2	3	4	5
	Közepes	2	3 R.7; R.20; R.30; R.31;	4 R.6; R.8a; R.18; R.24;	5 R.1; R.21;	6
	Magas	3 R.33; R.34; R.35;	4 R.4; R.8b; R.16; R.17; R.27; R.28; R.32;	5 R.12; R.13; R.15; R.29;	6 R.23;	7 R.3; R.22;
	Nagyon magas	4	5 R.9a; R.19; R.25;	6 R.5; R.9b; R.10; R.11; R.14; R.26;	7	8 R.2;

Forrás: a szerző szerkesztése a Cloud Computing, 2009: 24 alapján

Az ENISA szakemberei az általuk azonosított kockázatok közül a legkomolyabb kihívásoknak az alábbiakat tekintik:

- R.2 – irányítás elvesztése,
- R.1 – adatok, szolgáltatások hordozhatóságának nehézségei (lock-in),
- R.9 – izolációs hiba,

- R.3 – megfelelőségi kihívások,
- R.11 – kezelőfelület kompromittálódása,
- R.23 – adatvédelmi kockázatok,
- R.14 – adatok nem teljes vagy nem biztonságos törlése,
- R.10 – a felhőszolgáltató rosszindulatú belső munkatársa – visszaélés magas jogosultsággal.

A fent kiemelt kockázatok és a korábban szintén az ENISA szakemberei által magas besorolási szintet kapó kockázatok nem teljesen fedik egymást, amire a dokumentumban nem található magyarázat.

Ugyancsak eltérések tapasztalhatók az ENISA által megadott egyes kockázathoz tartozó értékek és az ezek alapján készített, a *Cloud Computing: Benefits, risks and recommendations for information security* című dokumentumban (Cloud Computing, 2009) eredetileg közzétett kockázateloszlási táblázat adatai között is. Ez utóbbi azonban egyértelműen szerkesztési hiba, így az itt közölt 8. táblázatot az eredeti dokumentumban az egyes kockázatoknál megadott értékeknek megfelelően szerkesztették át. Így az R.1, az R9a és az R.21 jelű kockázatok esetén a kockázatok értéke magasról közepesre, az R.5, az R.11 és az R.14 jelzésűek esetében közepesről magasra változott. Az eredeti táblázatban azokat a kockázati valószínűségeket, amelyeket a szakértők n. a. jelzéssel adtak meg, a táblázat szerkesztője nagyon alacsony besorolásúnak minősítette. Miután az elmúlt években több példát lehetett látni akár egy szolgáltató felvásárlására (Microsoft, 2011; Romanski, 2014), akár a szolgáltatás megszűnésére (Ulysses, 2014), alapvető megváltozására (cdn.wuala.com, s.d.), ezért ezeket közepes kockázatúként tartalmazza a táblázat.

A kockázatelemzésnél a különböző kapcsolódó hivatkozott sérülékenységeket és vagyonelemeket is összefoglalja a dokumentum. A sérülékenységek besorolásánál kiemelik, hogy a lista nem teljes körű, ugyanakkor az elemzéshez elegendőnek tartják.

A *Cloud Computing: Benefits, risks and recommendations for information security* című dokumentum (Cloud Computing, 2009) főleg a kis- és középvállalatokra koncentrál, de a kormányzatoknak és a nagyvállalatoknak is fogalmaz meg ajánlásokat. Ezek, valamint a kockázatok, sérülékenységek és a védendő vagyon listája – a megfelelők kiválasztásával, illetve kiegészítésével – egyértelműen felhasználható a rendvédelmi szervek számára kialakítandó biztonsági elemzéshez is.

A felhőalapú rendszerek esetében a rendvédelmi szervek részére a helyi jogszabályok által lehetővé tett törvényes ellenőrzés keretében biztosított

adathozzáféréssel kapcsolatban a korábban elemzett anyagok eddig kétféle megközelítést alkalmaztak; vagy egyáltalán nem említették, vagy pedig úgy, mint a FedRAMP esetében, ahol egy esetleges külföldi adatközpont esetén, a külföldi kormányzati és hatósági eljárásoknak kitettsége okán, kezelendő kockázatként tekintettek rá. Az ENISA dokumentumában ez egy jóval komolyabban kezelendő kockázatként jelenik meg, érezhetően más, az Európában jellemző, az Egyesült Államokétól eltérő, ráadásul a tagországokat tekintve is rendkívül heterogén technikai és szabályozási környezet szemszögéből történő megközelítéssel. Az európai felhasználók esetében ugyanis sokkal jellemzőbb, hogy vagy az adatközpont, vagy annak redundanciája, esetleg mindkettő külföldön található, így náluk magasabb szintű kockázatként kell kezelni adataik esetleges külföldi hatósági eljárásnak való kitettségét.

A felhőalapú rendszerek törvényes ellenőrzésének problémáját a későbbiekben részletesen bemutatjuk, jelen fejezet ezt a nemzetbiztonsági szolgálatok és a rendvédelmi szervek oldaláról kizárólag a felhasználás szemszögéből közelíti meg. Mindamellett még felhasználói oldalról nézve is, az említett szerveknek figyelembe kell venniük, hogy adott esetben biztosítaniuk, biztosíttatniuk kell saját országuk bizonyos szervei részére a törvényes ellenőrzés, továbbá az adathozzáférés lehetőségét. Hazánkban tipikusan ilyen szerv lehet például a Nemzeti Védelmi Szolgálat (NVSZ).

Az ENISA második kiemelést érdemlő dokumentuma a *Security & Resilience in Governmental Clouds – Making an informed decision* (Catteddu, 2011). Ez deklaráltan az előzőekben áttekintett anyagra épít, sőt szerzői ajánlása szerint azzal együtt kell használni.

A felhőalapú rendszerek bevezetésének kulcskérdése a kockázatok felmérése, megértése és kezelése, valamint a döntési folyamatok újragondolása. Ennek elősegítésére állítottak össze az ENISA szakemberei egy olyan modellt, amely segít a működési, jogi és információbiztonsági követelmények összeállításában, valamint a szervezet számára legjobban illeszkedő felhőarchitektúra kiválasztásában.

A dokumentum fő célja bemutatni a magán-, a közösségi és a nyilvános felhő információbiztonsági és ellenálló-képességi előnyeit, hátrányait, valamint segíteni a közintézményeket az ezekkel kapcsolatos követelmények meghatározásában. Ugyanakkor az anyag, szintén e tekintetben, indirekt módon segíti a tagállamokat nemzeti felhőstratégiájuk kialakításában.

Akárcsak az előzőekben ismertetett ENISA-dokumentumnál, ebben az esetben is az elvégzett elemzés három lehetséges felhőhasználati forgatókönyvön alapul:

1. az egészségügyin,
2. a helyi közigazgatásin,
3. az üzleti inkubátorként szolgáló állami tulajdonú felhőn.

Ebből látszik, hogy bár a megcélzott felhasználók itt sem közvetlenül a rendvédelmi szervek, ennek ellenére az előző anyagokhoz hasonlóan, ez is hasznos információkat hordoz számukra a felhőalapú rendszerek bevezetésének előkészítéséhez, kockázatainak azonosításához.

Az ENISA szakértői megállapítják, hogy végeredményben a felhőalapú rendszerek ki tudják elégíteni a közigazgatás legtöbb információbiztonsági és ellenálló-képességi követelményét, ennek eléréséhez a bevezetés előtt azonban mindenképpen alapos kockázatelemzés és -értékelés szükséges. Ráerősítenek arra – a korábban elemzett dokumentumban már megfogalmazott megállításukra –, hogy a hagyományos ICT-rendszereknél alkalmazott kockázatelemzés itt nem elég, hiszen a felhő új kockázatokat is hoz. Ugyanakkor figyelni kell a jogszabályi előírásokra is, hiszen több EU-tagállam nemzeti szabályozása tiltja bizonyos adatok külföldre, főleg az EU-n kívülre vitelét. Mindemellett a dokumentum sürgeti a tagállami és az EU ez irányú jogszabályi kereteinek felülvizsgálatát annak érdekében, hogy az adatok külföldre vitelét megengedőbb módon kezeljék, ezáltal a felhő használatából származó előnyöket kihasználhassák az állami szervezetek anélkül, hogy ezzel veszélyeztetnék az állampolgárok személyes adatainak biztonságát, vagy sértenék akár a nemzetbiztonsági, akár a gazdasági érdekeket. A rendvédelmi szervek kapcsán kijelenthető, hogy adataik nagy része fokozottabban védendő, mint más állami szervé, ezért egy, az ENISA által sürgetett adatkezelési liberalizáció valószínűleg csak kismértékben érintené őket.

Az európai szervezet szakértői azt is megállapítják, hogy éppen az érzékeny alkalmazásoknak és adatoknak köszönhetően a magán- és a közösségifelhő-modellek felelnek meg legjobban az állami feladatoknak még akkor is, ha a méretbeli előnyök java része ebben az esetben eltűnhet. Ez utóbbi viszont szintén fontos szempont, hiszen a biztonsági és ellenálló képességi előnyök egy része nem realizálható, amíg a felhő mérete nem éri el a „kritikus tömeget". A nyilvános felhő az előzőekhez képest jobb rendelkezésre állást és nagyobb költséghatékonyságot biztosít, mindezt kielégítő adatbiztonsággal, ám ezek használatát az érzékeny adatok vagy a már említett jogszabályok korlátozhatják, kizárhatják. Mindenesetre az esetleges bevezetésre, alkalmazásra jól átgondolt stratégiát és követelményrendszert kell

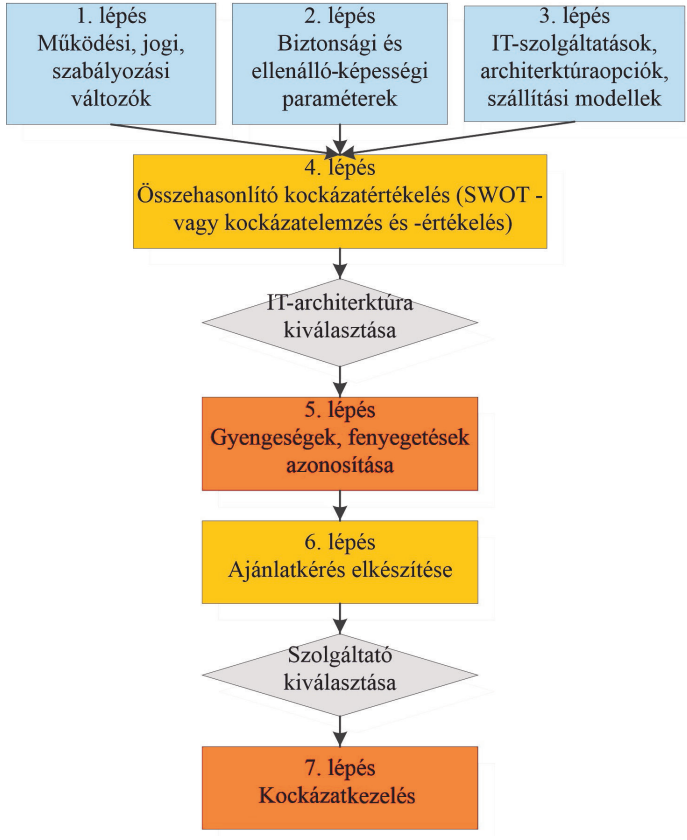
megfogalmazni, amely részletesen taglalja a szerződés megszüntetése, tehát a felhőből való kilépés feltételeit is.

Az anyagban a felhőalapú rendszerek kockázatainak azonosításához közvetlenül nem tartozó, mégis a nemzetbiztonsági szolgálatok és a rendvédelmi szervek számára fontos, egyéb gondolatokat is felvetnek a készítők. Így például az ENISA szakemberei a kormányoknak szóló javaslatokban megfogalmazzák, hogy a felhőalapú rendszerek alkalmazását lépcsőzetesen érdemes bevezetni, amelybe előre be kell tervezni az adott lépcsőről történő visszalépés lehetőségét is. A bevezetés tervezésekor az új veszélyek miatt új kockázatértékelést kell készíteni és alkalmazni, amelyben a kölcsönös függőségeket, a dinamikusan változó technikai környezetet, az ebből adódó lehetséges támadásokkal és sérülékenységekkel kapcsolatos hiányos ismereteket is figyelembe kell venni. Minden tagállam részére legalább 10 évre szóló felhőstratégia kidolgozását javasolják, amelyben hangsúlyosan figyelembe kell venni a nemzetbiztonsági és a nemzeti gazdasági érdekeket is. Ehhez vizsgálni kellene azt is, hogy a felhőalapú rendszerek milyen szerepet játszhatnak a létfontosságú infrastruktúrák védelme kapcsán, különösen az interdependencia nemzeti és nemzetközi hatásait kell elemezni a teljes ellátási láncban. Emellett célszerű lenne egységes EU-megközelítést alkalmazni az interoperabilitás megteremtéséhez, valamint a biztonság egységes megközelítéséhez, és EU-szinten kellene vizsgálni a kormányzati felhő koncepcióját, amelyet harmonizált jogszabályokkal kellene támogatni.

A felhőalapú rendszerek bevezetésének elősegítésére az állami szerveknek célszerű elkészíteniük:

- egy pontos, egyértelmű kockázatértékelés- és követelmény-meghatározást, beleértve az emberi tényezők, illetve jogi keretek vizsgálatát,
- a jelenlegi biztonsági rendszer átültetésének, támogatási lehetőségének vizsgálatát,
- az adatbiztonság és a szolgáltatás ellenálló képességének minimum elfogadható szintjét is részletes leírással tartalmazó, lehetőség szerint mérhető értékekkel operáló egyértelmű szolgáltatási szint meghatározását,
- egyéb, harmadik felet érintő kérdések alapos vizsgálatát (mint például az üzletmenet-folytonossági tervek ellenőrzése a teljes ellátási láncban, egy esetleges leállást követő szolgáltatás-újraindításnál a prioritási sorrend megtárgyalása a szolgáltatóval, vagy a szükséges távközlési infrastruktúra megléte stb.).

Az ENISA szakemberei a 6. ábrán látható folyamatábrának megfelelő lépések szerint ismertetik azokat a döntési folyamathoz kapcsolódó legfontosabb gondolatokat, követelményeket, kockázatokat és lehetőségeket, amelyek segítik a döntéshozókat a megfelelő felhőalapú rendszer kiválasztásában. Ugyanakkor az egyes lépések elemzése kapcsán azonosítják is azokat a biztonsági kockázatokat, amelyek a felhőalapú rendszerek bevezetése vagy használata során felmerülhetnek.



6. ábra

Az ENISA döntési modellje felhőalapú rendszer kiválasztásához

Forrás: a szerző szerkesztése a Catteddu, 2011: 27 alapján

A működési, jogi, szabályozási változók (1. lépés) kapcsán az alábbiakat célszerű megvizsgálni – működési tényezők tekintetében:

- adattípusok (személyes adatok, érzékeny adatok, minősített információk, összesített adatok),
- felhasználói profilok (felhasználói közösségek, felhasználók földrajzi eloszlása, ICT-műveltség és -biztonságtudatosság),
- skálázhatóság és kapacitásmenedzsment (kapacitásfluktuáció, hosszú távú „fel és le" skálázhatóság),
- interfészek interoperabilitása (interfészek interoperabilitása és komplexitása, adatformátumok cseréjének képessége, továbbító/kicserélő eszközök, azonosítási rendszerek, szabályozók interoperabilitása),
- rendszerek, szolgáltatások, platformok együttműködése (az entitások földrajzi szóródása, más szolgáltatási követelmények, az érintett ICT-rendszerek heterogenitása),
- költségek (működési költségek, beruházások, migráció költsége),
- tulajdonjogok (állami tulajdonú és általa nyújtott, állami tulajdonú és harmadik fél által nyújtott, államilag szponzorált, harmadik fél által nyújtott és államilag hivatkozott, partnerségi, megfelelőségi nyilatkozattal rendelkező).

Jogi, szabályozási tényezők tekintetében:

- általános jogi tényezők,
- kormányzati szuverenitás és adatok/információk feletti kontroll (rendvédelmi szervek hozzáférése, bizalmasság, szellemi tulajdon védelme),
- kormányzati beszerzések,
- adatvédelem, adatbiztonság,
- interoperabilitással, adatok visszaszolgáltatásával, valamint az adatok, szolgáltatások hordozhatóságának nehézségeivel (lock-in) kapcsolatos rendelkezések,
- szolgáltató szakmai gondatlansága,
- felhőszolgáltató alvállalkozói, valamint az irányításában történő változások.

A biztonsági és ellenálló-képességi paraméterek (2. lépés) kapcsán az alábbiakat célszerű megvizsgálni (az ENISA szakemberei itt definiálják, hogy pontosan mit is értenek biztonság és ellenálló képesség alatt):

> *„Az ellenálló képesség a rendszer (hálózat, szolgáltatás, infrastruktúra stb.) azon képessége, hogy elfogadható szintű szolgáltatást nyújtson és tartson fenn a különböző hibák és normál működési kihívások ellenére”* (Catteddu, 2011: 29 alapján fordította szerző).
>
> *„A biztonság az információk és az információs rendszerek jogosulatlan hozzáféréstől, használattól, közzétételétől, működésének zavarásától, módosításától, megsemmisítésétől való megvédésének, valamint hiba vagy rendkívüli esemény esetén a reagálás és a visszaállítás képessége”* (Catteddu, 2011: 29 alapján fordította szerző).

Ezek a meghatározások jól lefedik a fogalmakat, de természetesen figyelembe kell venni, hogy a dokumentumban ezek mentén vizsgálták meg az alábbi paramétereket:

- Végpont-végpont közötti biztonsági és ellenálló-képességi szolgáltatás a szolgáltatásoknak az ellátási lánc teljes hosszában, azaz a felhasználóktól, ügyfelektől kezdve a hálózaton, adatközpontokon át a nyilvános szolgáltatásokig, a rendszermenedzsment- és biztonsági szolgáltatásokig biztosítaniuk kell, hogy az adatok bizalmassági, sértetlenségi, rendelkezésre állási szintje és a szolgáltatások rendelkezésre állási és megbízhatósági szintje megfeleljen a követelményeknek, valamint a szolgáltatások megfeleljenek a vonatkozó jogszabályoknak.
- Biztonsági és ellenálló-képességi kiválasztási paraméterek:
  az ENISA *Metrics for resilience* nevű keretrendszere (ENISA, s.d.b) és az ennek kapcsán publikált dokumentumok alapján tekinti át, hogy mit kell a kormányszerveknek figyelembe venni a felhőszolgáltatás követelményeinek meghatározásához. Ezeket a kvantitatív és kvalitatív paramétereket négy csoportba sorolták be, az alábbiak szerint:
  - *Felkészültség*
    Ez a csoport az adatok bizalmasságának és sértetlenségének hatékony védelméhez szükséges szervezeti felkészülési szinthez tartozó paramétereket és kritériumokat tartalmazza:
    - A1 kockázatelemzés és -értékelés (ennek gyakorisága, sérülékenységértékelés kiterjedése és gyakorisága, biztonsági tesztelések gyakorisága),

- A2 megelőzés és detektálás (naplózott eseményekből és biztonsági riasztásokból készített jelentések gyakorisága, erőforrás-korlátozó mechanizmusok működésének megfelelősége),
- A3 javítócsomag-menedzsment (foltozások gyakorisága, átlagos ideje, javítócsomag-menedzsment kiterjedése),
- A4 hozzáférés-ellenőrzés és felelősségrevonhatóság (naplóadatok rendelkezésre állásának szintje, nyilvánossága),
- A5 ellátási lánc (végrehajtott audit típusa, úgymint belső, harmadik fél általi független, esetleg saját értékelés, annak hatóköre, metodikája).

– *Szolgáltatásnyújtás*
  Ez a csoport a fellépő hibák, váratlan események, rendszert érő támadások ellenére is az SLA-nak megfelelő, elfogadható szolgáltatási szint biztosítását garantáló képességek mérésére szolgáló kritériumokat tartalmazza:
  - B1 rendelkezésre állás, megbízhatóság (meghibásodások átlagos ideje, két meghibásodás közötti átlagos idő, teljes havi vagy napi rendelkezésre állás, incidensek aránya, rosszindulatú támadással szembeni tűrőképesség, redundancia, másolatok, automatikus antivírus-frissítések és -futtatások aránya, jelszószabályok ellenőrzésének aránya, titkosító kulcs hossza, sértetlenséget és letagadhatatlanságot ellenőrző algoritmusok, mint hasítókódok, ujjlenyomatok, ellenőrző összegek, sávszélesség, késleltetés, csomagvesztés, jitter)[32].
  - B2 skálázhatóság és rugalmasság (kapacitásfluktuáció, hosszú távú le- és felskálázhatóság, a maximális és a normál terhelés aránya, azaz a terheléstűrés, kiszámíthatatlan terhelések tűrése, mint DoS/DDoS-támadások, csúcs- és átlagterhelés különbsége, új hardverkomponensek beszerzési ideje, szolgáltatás teljesítésének időtartama).

– *Reagálás és helyreállítás*
  Ez a csoport a hibák és incidensek reagálásához szükséges rendszerképességek mérésére szolgáló kritériumokat tartalmazza:

[32] A jitter itt csomagkésleltetési eltéréseket, ingadozásokat takar.

- C1[33] visszaállítási időtartam (recovery time objective – RTO) és visszaállítási időpont (recovery point objective – RPO) meghatározása.
- C2[34] reagálási és hatékonysági stratégia mérése (incidens bekövetkezte és felfedezése között eltelt idő, az újraindítás szükségességének felismeréséhez szükséges átlagos időtartam, javításhoz szükséges átlagos időtartam, incidens utáni helyreállításhoz szükséges átlagos időtartam).

– *Jogi és szabályozási megfelelőség*
  Ez a csoport a jogi megfelelőség értékelésére szolgáló kritériumokat tartalmazza:
  - D1 nyomozati eszközök (szolgáltatónál található bizonyítékok gyűjtéséhez kapcsolódó követelmények, mint elektronikus felderítés, adatmegőrzés),
  - D2 adatmegőrzés és visszakövetés (adatmegőrzés minimum és maximum periódusa, naplóállományok megőrzésének minimum és maximum periódusa, adattárolás módja, naplóállományok tárolásának módja, visszaszolgáltatás időtartama),
  - D3 bizalmasság (nemzeti előírások a különböző kezelt adatok típusának megfelelően, titkosítás szükségessége, minimális előírt kulcshossz).

Az ICT-szolgáltatások, architektúraopciók, szállítási modellek (3. lépés) esetén vizsgálandó kritériumokkal kapcsolatban csupán azt elemzik a dokumentumban, hogy mikor tekinthető felhőszolgáltatásnak valami, és mikor nem, ehhez kapcsolódó kockázatokat itt nem azonosítanak a készítők.

Az összehasonlító kockázatértékelés (4. lépés) kapcsán az ENISA szakértői SWOT-elemzést készítettek a nyilvános, a magán- és a közösségi felhőre. Ezeket a 9., 10. és 11. táblázat mutatja.

---

33 Az eredeti dokumentumban ez a jelölés nem szerepel, azt csupán én alkalmazom a jobb érthetőség miatt.

34 Az eredeti dokumentumban ez a jelölés nem szerepel, csupán a jobb érthetőség miatt alkalmazzuk.

9. táblázat

Az ENISA nyilvános felhőre vonatkozó SWOT-elemzése

NYILVÁNOS FELHŐ	
ERŐSSÉGEK • rendelkezésre állás és megbízhatóság • tűrőképesség és rugalmasság • javítócsomag-menedzsment • reagálási idő • üzletmenet-folytonosság • fizikai biztonság • behatolás megelőzése és detektálása • más országok rendvédelmi szerveinek elektronikus felderítő és bizonyítékgyűjtő tevékenységének késleltetése	GYENGESÉGEK • ellátási lánc feletti kontroll hiánya • naplózási képességek • nyomozáshoz szükséges (forensic) adatok hozzáférésének nehézsége • a szükséges alkupozíció hiánya egyes állami szervezeteknél • jogi és szabályozási követelmények miatt az adatokat az ország területén belül kell tartani, ami csökkenti az üzletmenet-folytonosság szintjét • rossz minőségű összeköttetés miatt csökkenő teljesítmény • az adatközpontok elhelyezésére szolgáló terület korlátozott az Európai Unióban • adatvisszavétel nehézségei
LEHETŐSÉGEK • kockázatelemzés és -értékelés • biztonsági tesztelés • valós idejű biztonsági ellenőrzés • nyomozati tevékenység (forensics)	FENYEGETÉSEK • egy nagy, nyilvános felhő vonzó támadási célpont • egy belsős támadás veszélye meglehetősen nagy • izolációs hiba • a követelmények és a vagyonosztályozás gyenge meghatározása • többszörös joghatóság • a szolgáltató irányításában bekövetkező változás • az alkalmazott adatformátum ellehetetlenítheti a szolgáltatóváltást

Forrás: a szerző szerkesztése a Catteddu, 2011 alapján

10. táblázat

Az ENISA magánfelhőre vonatkozó SWOT-elemzése

MAGÁNFELHŐ	
ERŐSSÉGEK • kockázatértékelési gyakorlat • javítócsomagok telepítése • hozzáférés-szabályozás • naplózás • auditálás • kontroll a rendelkezésre állás, a megbízhatóság, a skálázhatóság és a rugalmasság felett • a kezelőfelület rendelkezésre állása • üzletmenet-folytonossági terv • jogi megfelelőség	GYENGESÉGEK • a magánfelhő méretgazdaságossága • a megfelelő méret hiánya kevesebb vagy gyengébb beépített biztonsági mechanizmust vonhat maga után • rosszindulatú támadásokkal szembeni gyengébb tűrőképesség • a váratlan csúcsigényekkel szembeni kisebb rugalmasság • alacsonyabb szintű redundancia-előírások • a georedundancia hiányosságai miatt a hiba utáni visszaállítás hosszabb lehet • a reputáció érzékenysége
LEHETŐSÉGEK • monitoring • további hozzáférés-szabályozási lehetőségek	FENYEGETÉSEK • politikailag motivált támadások • „Nagy testvér”-effektus • az erőforrás-kihasználás változékonysága és a nem várt csúcsterhelések kikényszeríthetik nyilvános felhő használatát is (hibrid felhő) • gyenge tervezés • a nem megfelelő részletességű szerződés az abban foglaltak teljesítésének ellenőrizhetőségét csökkentheti

Forrás: a szerző szerkesztése a Catteddu, 2011 alapján

11. táblázat

Az ENISA közösségi felhő SWOT-elemzése

KÖZÖSSÉGI FELHŐ	
ERŐSSÉGEK • közös követelmények, kikötések és kockázati profilok • a közös követelmények és kockázati profilok egyszerűsítik a külső és belső támadások ellen védő mechanizmusok és eszközök beállítását • a felhasználóknak jobb az alkupozíciója • a belépési kritériumok felállításának lehetősége • nagyobb méretek, jobb válaszok a csúcsigényekre (a magánfelhőhöz képest)	GYENGESÉGEK • a közös célok miatt a partnerek közötti versengés az erőforrásokért • a magánfelhőhöz képest még vonzóbb célpontja a támadásoknak • a magánfelhőhöz képest gyengébb hozzáférés-szabályozás és jogosultságkezelés • a rossz összeköttetés miatti gyengébb teljesítmény csökkentheti a szolgáltatás szintjét
LEHETŐSÉGEK • növelt biztonsági előírások, alapkövetelmények és standardok, közös kockázatelemzési és -értékelési gyakorlat, naplózás és monitoring • közös, megosztott incidenskezelési rendszer • információk megosztása a közösség tagjai között (legjobb gyakorlatok, múltbeli incidensek tapasztalatai stb.) • szigorúbb biztonságot eredményezhet, hogy a felhőt csak a tagok használják	FENYEGETÉSEK • megállapodás hiánya a biztonsági alapkövetelmények és biztonsági mechanizmusok tekintetében • a közösség túl gyorsan vagy túl lassan növekszik • az erőforrás-használatot nehezebb megjósolni • izolációs mechanizmus hibája • a jogosult személyeket nehéz azonosítani

Forrás: a szerző szerkesztése a Catteddu, 2011 alapján

A SWOT-analízissel kapcsolatban két dolog mindenképpen kiemelést érdemel. Az egyik, hogy a szolgáltatási modelltől függetlenül készült, így egy konkrét vizsgálatnál az aktuális szolgáltatási modell (IaaS, PaaS, SaaS) figyelembevételével módosulhat. Másrészt a felhasználó ebben a lépésben

más módszert, például kockázatelemzést és -értékelést is alkalmazhat a SWOT-elemzés helyett.

A készítők közzétesznek egy minta paraméterlistát, amely azonban jól tükrözi, hogy melyek azok a legfontosabb szempontok, amelyeket a kínált rendszerek, szolgáltatások kapcsán értékelni kell. A paraméterek mellett feltüntetik az általuk kitalált három forgatókönyvre vonatkoztatva, milyen lehetséges értékeket tartanak hozzájuk elképzelhetőnek. Ezt mutatja be összefoglaló jelleggel a 12. táblázat.

12. táblázat

ENISA-szolgáltatások értékelésének szempontjai

Paraméterek	
Megnevezés	**Lehetséges értékek**
Adatok érzékenysége	
• adatok típusa	• személyes adat, érzékeny adat, üzleti adat,
• információbiztonsági és ellenálló-képességi követelmények	• magas sértetlenség • magas bizalmasság • magas rendelkezésre állás
Skálázhatóság – igények kezelése	
• igények tartóssága	• alacsony, közepes, magas
• új szolgáltatások szükségessége	• igen, nem
• várható tárolási igények a következő öt évben	• megjósolható
• egyidejű felhasználók csúcsa	• alacsony, közepes, magas
• adatok aránya az aktív felhasználóknál	• alacsony, közepes, magas
• szükséges adminisztratív hozzáférés szintje (privilegizált felhasználó – ICT-szervezet)	• alacsony, közepes, magas
Szolgáltatások megbízhatósága, rendelkezésre állása és teljesítési szintje	
• rendelkezésre állás	• xx,x% (alacsony, közepes, magas)
• nem tervezett leállás	• nem több mint x óra
• valós idejű reagálás	• alacsony, közepes, magas
Együttműködés és interoperabilitás	
• más hatóságnak és/vagy közigazgatási szervnek el kell-e érnie a szolgáltatást	igen, nem

Paraméterek	
Megnevezés	**Lehetséges értékek**
Hitelesítés, engedélyezés, hozzáférés-kezelés (AAA)[35]	
• azonosításkezelés	• belső (saját), külső (szolgáltató), mindkettő
• felhasználók ellátása engedélyekkel	• belső (saját), külső (szolgáltató), mindkettő
• szabályalapú hozzáférés-kezelés (RBAC)[36]	• igen, nem
• hitelesítés erőssége	• erős, közepes, 2 faktoros, jogiköve-telmény-jelszavas, opcionális
• államilag megkövetelt	• igen, nem
Titkosítás	
• titkosítás	• igen útközben, opcionális, javasolt útközben
• hozzáférés a kulcsokhoz	–
• adminisztrátori hozzáférés engedé-lyezése	• a szolgáltató biztosítja a bejelentke-zési és hitelesítési adatokat az ad-minisztrátori hozzáféréshez
Jogi és megfelelőségi paraméterek	
• adatvédelem	• alkalmazható
• adatok helye és joghatóság	• mindkettőt meg kell adni (néhány országban a törvény előírja, hogy az adatok országon belül kell, hogy maradjanak)
• hozzáférés-szabályozás	• a kötelező hozzáférés-védelem (MAC)[37], a szabályalapú hozzá-férés-kezelés (RBAC) vagy ezek kombinációja
• felelősségre vonhatóság (a napló-adatokat a bíróság elfogadhatja)	• igen, nem
• hozzáférés digitális személyazono-sító kártya használatával	• igen, nem
• digitális aláírás	• igen, nem, lehet, kell

35 AAA – Authentication, Authorization and Accounting (hitelesítés, engedélyezés és hoz-záférés-kezelés).

36 RBAC – Role-Based Access Control (szabályalapú hozzáférés-kezelés).

37 MAC – Mandatory Access Control (kötelező hozzáférés-védelem).

Paraméterek	
Megnevezés	**Lehetséges értékek**
• egyszeres bejelentkezés (SSO)[38]	• opcionális
• letagadhatatlanság	• igen, nem
• elektronikus időbélyeg	• igen, nem, néhány dokumentumhoz kell
• egyedülálló jelszavak vagy egyedi felhasználónevek	• igen, nem
• a „need to know" elv kikényszerítése (alkalmazással)	• igen, nem
• ellátási lánc átláthatósága	• harmadik fél szolgáltatók elkerülése érdekében teljes átláthatóság szükséges
• ellátási lánc átvilágítása	• igen, nem

Forrás: a szerző szerkesztése a Catteddu, 2011: 62–67. alapján

Az ENISA szakemberei végezetül a 6. lépés, azaz az ajánlatkérés elkészítéséhez is adnak segítséget, ahol is azokat a kérdéseket foglalták össze felkészültség, szolgáltatásnyújtás, reagálás és helyreállítás, valamint jogi és szabályozási megfelelőség kérdéskörében, amelyek útmutatóként szolgálhatnak az ajánlattételi felhívás során. Ugyanakkor azt javasolják az érintett szervezeteknek, hogy akár az ajánlattételi felhíváshoz, akár a kockázatcsökkentési terv elkészítéséhez olyan más, ebben a témában készült keretrendszereket is használjanak fel, mint az *ENISA Information Assurance Framework* (ENISA, 2009) vagy a *CSA Cloud Controls Matrix* (CSA, 2014a).

A dokumentum, akárcsak a korábban elemzett másik ENISA-anyag, véleményem szerint kiemelkedően hasznos a rendvédelmi szervek felhőalapú rendszerek használatával kapcsolatban megfogalmazandó követelménylista elkészítéséhez. A döntési modell segíthet a megfelelő felhőalapú rendszer kiválasztásában, a javasolt biztonsági és ellenálló-képességi paraméterek, azok értékelésének szempontjai, valamint a különböző telepítési modellű felhőrendszerek SWOT-elemzésénél leírtak pedig – a megfelelő kiegészítésekkel – jól használhatók a rendvédelmi szervek szigorú biztonsági követelményrendszerének kialakításához. Mindemellett a dokumentum egyedülálló módon hívja fel az állami szervek figyelmét a nemzetbiztonsági

[38] SSO – Single Sign-On (egyszeres bejelentkezés, amely után a rendszer minden erőforrásához és szolgáltatásához további autentikáció nélkül hozzá lehet férni).

érdekek figyelembevételére a felhő alkalmazásakor. Ez pedig a rendvédelmi alkalmazás során – tekintettel az érzékeny adatokra – kiemelt jelentőségű.

A dokumentum fontos üzenete, hogy bár az elején még csak feltételes módban beszél arról, hogy a sok érzékeny adatot használó szervezet számára a nyilvános felhő, bizonyos biztonsági előnyei ellenére sem megfelelő alternatíva, addig a dokumentum végére ezt már-már tényként kezeli. Optimális megoldásként a közösségi felhő használatát javasolják számukra. Ez, a három kiemelt telepítési modell kapcsán elvégzett SWOT-elemzés eredménye, valamint a többi szervezet összes telepítési modell előnyeire, hátrányaira vonatkozó következtetések megismerése egyértelművé teszi, hogy a rendvédelmi szervek számára is valóban a közösségi felhő jelentheti az optimális megoldást.

Ugyancsak kiemelendő az az ötlet, miszerint vizsgálni kellene, hogy a felhőalapú rendszerek milyen szerepet játszhatnak a létfontosságú infrastruktúrák védelmével összefüggésben. Ezzel a gondolattal más szervezet anyagaiban nem találkozni, ugyanakkor ezt itt sem részletezzük, csupán a gondolatfelvetés szintjén marad meg.

A témában a fenti két kiemelt dokumentumon kívül további hasznos információkat ad az ENISA felhőalapú rendszerekkel, azok biztonságával foglalkozó weboldala (ENISA, s.d.c), valamint az itt található – általam korábban már említett – *Good Practice Guide for Securely Deploying Governmental Clouds* (ENISA, 2013) és a *Security Framework for Governmental Clouds* (ENISA, 2014) című anyag is.

A biztonsági követelmények elemzéséhez felhasználható az ENISA *Technical Guidelines for the implementation of minimum security measures for Digital Service Providers* (ENISA, 2016) című dokumentuma is. Ez *a hálózati és információs rendszerek biztonságának az egész unióban egységesen magas szintjét biztosító intézkedésekről* szóló Európai Parlament és Tanács (EU) 2016/1148 irányelvének 2016/1148 irányelv, 2016. július 6.) gyakorlati átültetését hivatott elősegíteni, többek között a felhőszolgáltatók számára, ám segítséget nyújthat a felhasználók számára is, elvárásaik megfogalmazásához.

Biztonsági kérdések – a rendvédelmi szervek szempontjából

A felhőalapú rendszerek terén vezető szerepet játszó nemzeti és a nemzetközi szervezetek előző részben bemutatott ajánlásai sokféle megközelítésből

foglalkoztak az említett rendszerek biztonsági kérdéseivel és kockázataival. Volt, amelyik a gazdasági társaságokra, volt, amelyik kifejezetten a kormányzati szervekre koncentrálva, és volt, amelyik vegyes megközelítést alkalmazva dolgozta fel a kérdést. A megközelítések másik tengelyét az adta, hogy a kockázatok azonosítását és csoportosítását a szolgáltató vagy a felhasználó szemszögéből végezték-e el az adott szervezetek. Ezek ugyan kiváló alapot biztosítanak a rendvédelmi szervek számára a felhőalapú rendszerek kockázatainak azonosításához – és így a biztonsági elemzés kidolgozásához is –, azonban nekik – speciális helyzetükből adódóan – az említett dokumentumokat felhasználva, azoktól azonban eltérő módon csoportosítva, helyenként kiegészítve, módosítva érdemes ugyanezt a kéréskört megvizsgálniuk.

A felhőalapú rendszerek komplex biztonsági vizsgálatának szempontjai

A nemzetbiztonsági szolgálatoknak és a rendvédelmi szerveknek a felhőalapú rendszerek komplex biztonsági vizsgálatát az alábbi *négy dimenzió* (és a bennük lévő területek) mentén célszerű lefolytatniuk:

1. A rendvédelmi szerv szerepe:
- felhasználó,
- törvényes ellenőrzést végző.

2. Telepítési modellek:
- magán számítási felhő (Private cloud),
- közösségi számítási felhő (Community cloud),
- nyilvános számítási felhő (Public cloud),
- hibrid számítási felhő (Hybrid cloud).

3. Szolgáltatási modellek:
- szoftver mint szolgáltatás (Cloud Software as a Service – SaaS),
- platform mint szolgáltatás (Cloud Platform as a Service – PaaS),
- infrastruktúra mint szolgáltatás (Cloud Infrastructure as a Service – IaaS).

4. Vizsgálandó biztonsági kérdéscsoportok:
- üzembiztonság,
- adatbiztonság,
- egyéb (jogi, fizikai stb.) biztonság,
- törvényes ellenőrzés.

A fenti négy dimenzió mentén az említett szervezetek a felhőalapú rendszerek biztonsági problémái kapcsán valóban komplex, minden releváns tárgykörre választ adó vizsgálatot tudnak lefolytatni. Ugyanakkor egy adott kérdés megválaszolásához, a biztonsági elemzés kidolgozását szem előtt tartva – a lentiekre figyelemmel – lehet és célszerű is szűkíteni az elemzendő kérdéseket.

A rendvédelmi szervek szerepkörei

A rendvédelmi szervek szerepe kettős lehet, egyrészt felhasználóként saját igényeiket elégíthetik ki az általuk meghatározott – sokszor igen magas – biztonsági követelményeiknek megfelelően, másrészt végre kell hajtaniuk a jogszabályokban megfogalmazott törvényes ellenőrzést. A kétféle szerep miatt a biztonsági kérdéseket is kettős szemszögből kell vizsgálni. Például a rendelkezésre állás vagy éppen az interoperabilitás kérdése felhasználóként nagyon fontos, míg ellenőrzést végzőként kevésbé releváns. Ugyanakkor adott esetben a felhasználói aktivitási adatok megőrzése ellenőrzést végző szervként fontosabb is lehet, mint felhasználóként.

A vizsgálatkor arra is figyelemmel kell lenni, hogy bizonyos esetekben a törvényes ellenőrzés követelményének érvényesítése ellentétes lehet mind a szolgáltató, mind a felhasználó érdekeivel (a szolgáltatónak pénzbe kerül annak kiépítése, fenntartása, míg a felhasználó adott esetben pont azért választ felhőalapú megoldást, hogy a törvényes ellenőrzést elkerülhesse).

Ebben a fejezetben kizárólag a felhasználói szerepkörből kiindulva vizsgálom meg a kérdést.

Telepítési modellek

A telepítési modellek definícióját, részletes leírását a *Szolgáltatási modellek (Service Models)* című rész tartalmazza, így ezek vizsgálatával itt nem foglalkozunk. A korábbi megállapításoknak megfelelően élhetünk azzal a feltételezéssel, hogy a rendvédelmi szervek felhasználóként közösségi számítási felhőt vesznek igénybe, míg a törvényes ellenőrzés kapcsán elsősorban a nyilvános számítási felhőkre koncentrálnak. Így a felhasználóként elvégzendő biztonsági vizsgálathoz szükséges követelményrendszer felállítása lényegesen egyszerűbbé válik.

Szolgáltatási modellek

A szolgáltatási modellek definíciójának részletes leírását a *Telepítési modellek (Deployment Models)* című rész a tartalmazza, így ezzel itt szintén nem foglalkozunk. Az egyszerűsítés ebben az esetben kicsit nehezebb, inkább csak a törvényes ellenőrzés kapcsán tehetünk ilyet. Ott feltételezhetjük, hogy a rendvédelmi szervek a szoftver mint szolgáltatás modellje szerint működő számítási felhőkre koncentrálnak, ám felhasználóként mindhárom modell alkalmazása egyaránt reális lehet.

Meg kell jegyezni, hogy amennyiben az első három dimenzióra vonatkozó feltevések egy adott esetre nem igazak, akkor természetesen az adott szerepkör, telepítési és szolgáltatási modell sajátosságait figyelembe véve kell vizsgálni a biztonsági kérdéseket.

Vizsgálandó biztonsági kérdések

A korábban már ismertetett nagy szervezetek ajánlásai mellett, az interneten a témában fellelhető tanulmányok, publikációk is sokféle megközelítésben foglalkoznak a témával. Hol a teljességre törekedve, hol egy-egy témakört kiragadva keresnek válaszokat, vagy próbálnak definíciókat, tanácsokat adni a felhőalapú rendszerek biztonságával kapcsolatos témákban, vagy éppen felhívni egy addig kevéssé ismert problémára a figyelmet.[39] A nagyobb piaci szereplők is különböző tanulmányokat adnak ki bizonyos biztonsági kérdéseket reflektorfénybe helyezve, persze nem titkoltan azzal a szándékkal, hogy saját termékeikkel egyfajta megoldást kínáljanak ezekre.[40]

A vizsgálandó biztonsági kérdéseket az előző részben ismertetett dokumentumokra alapozva, az imént említett internetes anyagokat is felhasználva, azoktól mégis eltérő módon az alábbi *négy fő csoportba* célszerű sorolni:

- üzembiztonság,
- adatbiztonság,
- egyéb (jogi, fizikai stb.) biztonság,
- törvényes ellenőrzés.

---

39 Lásd bővebben Silverston (2009); Cox (s.d.); Brodokin (2008); Cox (s.d.b); Gilbert (s.d.); Foran (s.d); Ristenpart et al. (2009); Chow et al. (2009); Chen et al. (2010); Jamil–Zaki (2011); Wang (2009); Preimesberger (2011); Jaeger et al. (2008).

40 Lásd bővebben TrendMicro (s.d.); GFS (s.d.); Intel (2015); TrendMicro (2011); Buecker et al. (2009).

Ez a csoportosítás önkényes, hiszen nem a mindenki által elfogadott bizalmasság–sértetlenség–rendelkezésre állás szerinti felosztás követi, hanem egy, az állami, kormányzati szervezeteknél, különösen a rendvédelmi szerveknél a gyakorlatban megvalósuló szervezeti felállást. Ott ugyanis különböző emberek, jobb esetben csoportok vagy szervezeti egységek foglalkoznak a fent leírt kérdéskörökkel. Ugyanakkor a szakirodalomban találkozhatunk az itt felállítotthoz hasonló megközelítéssekkel, így például ehhez a felosztáshoz közel azonos jellegűt lehet találni a BSI (Federal Office for Information Security, 2011: 17) és szinte teljesen megegyezőt az ENISA korábban elemzett anyagában (Catteddu, 2011: 6).

Az itt választott csoportok elnevezései az azokat ellátó személyekre vagy szervezetekre utalnak. Miután a felhőalapú rendszerek biztonsága kapcsán a technikai jellegű kérdések a dominánsak, ezért azok kettébontva, külön címkével ellátva szerepelnek, míg a többi kérdéskör ellátói – bár azok jól elkülönülnek minden szervezetnél – egy kategóriában, az egyéb biztonságiban találhatók. Ez utóbbi alábontását az elsődleges biztonsági vizsgálat során meg lehet tenni, így egyértelműen delegálhatók a megválaszolandó kérdések, feladatok.

Üzembiztonság

Az üzembiztonság kérdése a felhőalapú rendszerek esetében is nagyon hasonló, mint a hagyományos infokommunikációs rendszereknél, azokat a jellemzőket foglalja össze, amelyek a rendszerek megbízható, üzemszerű működésével függnek össze. Ilyenek lehetnek például, hogy a szerződésben meghatározott eszközökkel (például androidos táblagépek) meghatározott helyekről (például bárhonnan, ahol internetkapcsolat van) meghatározott rendelkezésre állással (például 95%, de a szolgáltatáskiesés nem hosszabb mint 30 perc) érjük el a szolgáltatást, de idetartozik adataink biztonsági mentése, a redundáns tárolás, a katasztrófa utáni adat-visszaállítás stb. is.

Az üzembiztonsági kérdések gyakorlatilag tisztán technikai úton kezelhetők, ahol a felhasználó és a szolgáltató érdekei nagyjából egybeesnek, hiszen a szolgáltató megbízható szolgáltatást kíván nyújtani, a felhasználó pedig kapni. A biztonságos szolgáltatás mértéke „csupán” pénz és megállapodás kérdése.

Üzembiztonságnál a felelősségi kérdések egyértelműnek tűnnek, alapvetően a szolgáltatóé az összes felelősség az általa üzemeltetett rendszerelemek tekintetében, függetlenül a szolgáltatási modelltől (SaaS, PaaS, IaaS).

A hagyományos ICT-megoldások esetében is már alkalmazott és elfogadott standardok tökéletesen jó kiindulási alapot biztosítanak a felhőalapú rendszerek üzembiztonsági kérdéseinek vizsgálatához.

Adatbiztonság

Adatbiztonsági kérdésnek tekinthetünk minden olyan tényezőt, amelyek a felhasználók adataihoz való biztonságos hozzáférés (kezelés, használat stb.), valamint az illetéktelen hozzáférések megakadályozása kapcsán felmerülnek. Ilyenek például az azonosító eljárások, a titkosítások használata vagy akár az adathalászat elleni védekezés. Ezek egy része a hagyományos ICT-rendszerek kapcsán már rendelkezésre áll, vagy könnyen átültethető felhőalapú rendszerekre (például vírusvédelem), egy részük pedig teljesen új megoldásokat kíván (például adatszegregáció, felhőalapú rendszerekben használt virtualizációt kihasználó támadások elleni védekezés) (Ristenpart et al., 2009). Az adatbiztonsági kérdések közül vannak (technikailag) egyszerűen megoldhatók (például a felesleges, ezáltal a sérülékenységek miatt biztonsági kockázatot jelentő alkalmazások kikapcsolása) és bonyolult technikai, sőt akár jogi megoldásokat igénylők (például a szolgáltató – beleértve annak rendszergazdáit is – ne férhessen hozzá az adatainkhoz) (Foran, s.d.; Jaeger et al., 2008).

Az adatbiztonság kérdésköre technikai, jogi és adminisztratív úton oldható meg, vannak olyan elemei, amelyek kizárólag technikai úton nem vagy csak irreálisan nagy ráfordítás mellett lennének megvalósíthatók. Ilyen például a szolgáltató szándékos adatszerzése kivédésének (Chow et al., 2009) vagy az adatok teljes törlésének (Jamil–Zaki, 2011) kérdésköre.

A biztonsági kérdések kapcsán a felhasználó és a szolgáltató érdekei eltérők (lehetnek). A szolgáltató alapvető érdeke az üzembiztos szolgáltatás, és csak másodsorban a felhasználó adatainak védelme, amely plusz-, továbbá az állandó fejlesztési kényszer miatt folyamatosan jelentkező, meglehetősen nagy mértékű, ráadásul a felhasználóra teljes mértékben nehezen áthárítható kiadásokat jelent számára. A felhasználóknak ugyanakkor kifejezetten érdekük, hogy adataik biztonságban legyenek.

A felelősségi körök itt megoszlanak a felhasználó és a szolgáltató között, a megosztás mértéke pedig nagyban függ a szolgáltatási modelltől. A SaaS-modellnél a felhasználónak kismértékű, míg az IaaS-modellnél jelentős mértékű a felelőssége.

Az adatbiztonság kéréskörét az adatok életciklusán keresztül érdemes megvizsgálni, amelyet a 7. ábra szemléltet.

7. ábra

Az adatok életciklusa

Forrás: a szerző szerkesztése a Securosis, 2011 alapján

Az adatok életciklusának hat állomását biztonsági szempontból két fő csoportra bonthatjuk, az adatmozgással járó és az adatmozgással nem járó műveletekre. Az adatmozgással járó műveletekbe beletartozik az előállítás, a használat, a megosztás, a törlés, míg az adatmozgással nem járó műveletek a tárolás és az archiválás.

Ezt a bontást azért célszerű megtenni, mert a felhőalapú rendszerek esetében, ha a felhasználó bármilyen aktív műveletet végez, akkor az az adatok mozgásával, utazásával fog járni. Márpedig ekkor olyan kockázatokat is kezelni kell, mint a felhasználó és a szolgáltató közötti adatforgalom passzív lehallgatása, közbeékelődéses támadások, visszajátszásos támadások stb. Ráadásul így a felhasználó és a szolgáltató felelősségi körét jobban szét lehet választani, hiszen az adatmozgással járó műveleteknél a felhasználónak nagyobb a felelősségi köre, mint az adatmozgással nem járó műveleteknél.

Egyéb (jogi, fizikai stb.) biztonság

Ebbe a kategóriába tartozik minden olyan biztonsági kérdéskör, amelyeket nem technikai úton kezelünk, és akár egy harmadik fél is bevonható (például audit). Idesoroljuk azokat az elsősorban szerződésbe foglalt vagy törvényileg szabályozott jogi garanciákat is, amelyek adott kérdésköröket egyértelműen rendeznek, beleértve az üzembiztonsági és adatbiztonsági kérdéseknél felmerült, ilyen módon megoldandó feladatokat, de ugyanebbe a csoportba tartoznak az adatközpontok fizikai védelmét, a szolgáltató személyi, gazdasági vagy a dokumentum biztonságát szavatoló tényezők is.

Az ebbe a kategóriába tartozó kérdésekre kizárólag jogi eszközökön keresztül lehet ráhatása a felhasználónak. Ez a jogi kérdések esetében egyértelmű, de ugyanez igaz a többi, például fizikai biztonságra vagy a harmadik fél bevonását igénylő auditra is. Ez azért is lényeges, mert ennél a kategóriánál a szolgáltató és a felhasználó érdeke szinte minden esetben eltér egymástól. Ráadásul a felhasználó ráhatása az ebbe a csoportba eső kérdésekre szélsőségek között változhat. Igaz ez például akár a szerződés tartalmára is, hiszen amíg egy nyilvános SaaS-megoldásnál ez leredukálódhat a szolgáltató által kialakított feltételek és az általa megírt szerződés elfogadására vagy elvetésére, addig egy magán IaaS-megoldásnál a szerződés tartalmát, valamint az egyéb feltételeket a felhasználó a szolgáltatóval folytatott közvetlen tárgyaláson befolyásolhatja, határozhatja meg.

A felelősségi körök talán itt a legegyértelműbbek, a felhasználó felelőssége arra terjed ki, hogy a szerződésben minden számára releváns kérdést tisztázzon, beleértve a leírt követelmények ellenőrzését is. A szerződésben foglaltak fizikai, technikai stb. megvalósítása pedig a szolgáltató felelősségi körébe tartozik.

Törvényes ellenőrzés

Ebbe a kategóriába tartoznak a törvényes lehallgatással, az adatmegőrzéssel és a nyomozati (forensics) eszközök használatával kapcsolatos kérdések. A törvényes ellenőrzés kérdéskörét később részletesen kifejtjük, azonban röviden itt is célszerű foglalkozni vele. Egyrészt azért, mert ez is eleme a felhőalapú rendszerek felhasználói szempontú, komplex biztonsági vizsgálatának, másrészt pedig azért, mert az előző kérdéskörökhöz hasonlóan ebben az esetben is célszerű tisztázni a szolgáltató és a felhasználó közötti

érdek- és felelősségmegoszlásokat. Ez utóbbi okán, az egységesség érdekében ezt itt érdemes megtenni.

Amíg a korábban vizsgált biztonsági kérdések alapvetően felhasználói, és csak kis mértékben törvényes ellenőrzést végzői szerepkörben érdekesek a rendvédelmi szervek számára, addig ennél a kérdéskörnél ez pont fordítva van.

Ebbe a csoportba tartoznak azok az ellenőrzési formák, amelyek a klaszszikus hírközlési hálózatoknál már kialakultak és elfogadottak (például törvényes lehallgatás), és azok is, amelyek kifejezetten számítástechnikai rendszereknél alakultak ki (például számítógépes nyomozás vagy angol nevén computer forensics).

A törvényes ellenőrzés kategóriájába tartozó kérdések technikai és jogi úton rendezhetők, ám ezek pillanatnyilag a legproblémásabb kérdések. Egyrészt a jogi kapcsolat ebben az esetben, általában törvényi kötelezettség alapján, a szolgáltató és a törvényes ellenőrzést végző között áll fenn, nem pedig a szolgáltató, illetve a felhasználó között, mint a többi biztonsági kérdésnél. Ám amíg a hírközlési hálózatoknál egy kialakult, minden szereplő által elfogadott, a demokratikus államokban hasonló jellegű törvényekre alapozott törvényes ellenőrzésről beszélhetünk, addig a felhőalapú rendszerek esetében ez nem mondható el. A jelenleg meglévő jogi szabályozás hiánya a törvényes ellenőrzés kapcsán problémákat okoz vagy akár meg is akadályozhatja azt. Másrészt a felhőalapú technológia meglehetősen új és rendkívül dinamikusan fejlődik. Ennek okán nem beszélhetünk még olyan kiforrott ellenőrző rendszerekről, mint amelyek például a telefónia esetében már rendelkezésre állnak.

Ennél a kategóriánál a szolgáltató és a felhasználó érdeke szinte azonos, ám ellentétes a törvényes ellenőrzést végző rendvédelmi szervével, mint ahogy erről már esett szó a rendvédelmi szerv szerepe kapcsán. Ez alól csak ritkán vannak kivételek: például olyan eszözök alkalmazása, amelyekkel bizonyítható vagy kizárható, hogy a felhőben tárolt adatokat biztosan a felhasználó állította-e elő, vagy valaki manipulálhatta-e azokat.

A felelősségi körök itt vagy egyértelműek, amennyiben van törvényi előírás, vagy egyértelművé tehetők, ha annak hiányában a rendvédelmi szerv és a szolgáltató szerződést köt.

Ahogyan a CSA fent említett dokumentumaiban megjelent *a Security as a Service* fogalma, úgy a törvényes ellenőrzés kapcsán is megjelenhet például a *Lawful Monitoring as a Service* (LMaaS) fogalma. Amennyiben ezt – a többi kérdéshez hasonlóan – sikerül szabványosítani, akkor ennek

keretében a szolgáltató egyfajta szolgáltatásként, standardizáltan biztosíthatja a törvényes ellenőrzést végző szervek számára a szükséges információkat, függetlenül a szereplők nemzeti hovatartozásától, az adatközpontok és egyéb technikai eszközök fizikai elhelyezkedésétől, valamint azoktól a kérdésektől, hogy mikor melyik ország jogrendszere szerint kell eljárni.

Elsődleges biztonsági elemzés a felhőalapú rendszerek értékeléséhez

A korábban elemzett ajánlások ismeretében és a fentiek figyelembevételével a rendvédelmi szervek már képesek kidolgozni a felhőalapú rendszerek biztonsági értékelésére használható szempontrendszert.

Ez történhet akár egy biztonsági elemzősablon-készlet elkészítésével is úgy, hogy az egyes sablonok által lefedett területek és az adott területen a vizsgálatok mélysége eltérjen egymástól. Továbbá a FedRAMP „csináld egyszer, használd sokszor" megközelítését alkalmazva adott esetben az így kidolgozott sablonkészletet több szervezet is felhasználhatja.

Kiindulásként egy olyan sablonnal érdemes kezdeni a vizsgálatokat, amely mintegy nulladik lépésként azt segít tisztázni, hogy a kínált vagy kinézett felhőalapú rendszer megfelel-e azoknak a minimális biztonsági követelményeknek, amelyek teljesítése nélkül a rendszert nem szabad használni. Ehhez egy olyan sablont célszerű felhasználni, amely az alap biztonsági kérdéseket teljeskörűen felöleli, de egyszerű elvárt válaszok (igen/nem) megadását várja a felhasználótól. Ennek kitöltése után eldönthető, hogy az adott felhőalapú rendszer biztonsági szempontból alkalmas-e a további, részletes vizsgálatra, vagy annak használatától mindenképpen el kell tekinteni. Ugyanakkor egy ilyen sablonra kapott pozitív válasz nem jelenti automatikusan azt, hogy a felhőalapú rendszer megfelel a felhasználó biztonsági követelményeinek, csupán azt, hogy nincs kizáró tényező, azaz érdemes további vizsgálatokat elvégezni. Ezután folytathatják a felhasználó kijelölt szakemberei már a konkrét felhőalapú rendszer adottságainak (például szolgáltatási, telepítési modell stb.), a szervezet meghatározott feladatainak, céljainak, az általa kezelt adatok érzékenységének, valamint az ott már bevezetett biztonsági standardoknak megfelelően a további vizsgálatokat.

Egy ilyen, nulladik lépésként felhasználható sablon megtalálható Kovács Zoltán *Az infokommunikációs rendszerek nemzetbiztonsági kihívásai* című PhD-értekezésének (Kovács, 2015) mellékletében. Erre úgy lehet tekinteni,

mint egy alapra, amelyre rá lehet építeni a többi, a felhőalapú rendszerek biztonsági kérdéseinek egy-egy területére koncentráló, mélységi elemzést lehetővé tevő sablont. Ugyanakkor kiemelendő, hogy ezt a sablont sem lehet véglegesnek tekinteni. Egyrészt kiegészítéseket generálhat hozzá egy adott szervezet speciális igénye, de akár egy olyan, általános érvényű szempont is, amely az adott szervezet számára fontos, ám az nem szerepel a sablonban. Másrészt a felhőalapú rendszerek fejlődése kapcsán megjelenő új technológiák, szolgáltatások, a szintén egyre fejlődő, finomodó technikai és jogi szabályozások, szabványosítások kapcsán is várható a sablon változása. Minderre azonban úgy tekintünk, mint természetes evolúciós folyamatra, hiszen ugyanez történt, történik a nagy szervezetek hasonló jellegű kiadványaival. Gondoljunk itt például a CSA *Cloud Controls Matrix* táblázatára (CSA, 2014), amely 2015. év elején éppen a 3.0.1 verziónál jár, vagy akár a FedRAMP *System Security Plan* sablonjára (FedRAMP, 2012b), amelynek 2014. június 6-án adták ki a 2.0-s változatát.

3. fejezet
Az internettechnológiára épülő szolgáltatások törvényes ellenőrzési lehetőségei

A kommunikáció formái, lehetőségei az internet és az azt kihasználó alkalmazások fejlődésével ugrásszerűen változnak, bővülnek. Ebben nagy szerepük van az internettechnológiára épülő szolgáltatásoknak, ezeken belül pedig a PC/SaaS-típusú felhőalapú rendszereknek. Ezek azok a mindenki számára elérhető, meglévő eszközökkel (például notebook, okostelefon stb.), akár csekély számítástechnikai tudással is használható, olcsón, sokszor ingyenesen igénybe vehető rendszerek, szolgáltatások (mint például Facebook, Gmail, Dropbox, Twitter, Skype stb.), amelyek ma már szerves részét képezik mindennapi életünknek, kommunikációnknak.

Továbbá az internettechnológiára épülő szolgáltatások nem csak kommunikációs szokásainkra hatnak, az élet minden más területén is – például vásárlás, pénzügyi szolgáltatások stb. – új lehetőségeket biztosítanak. Ezek pedig szintén jelentős mértékben befolyásolják, alakítják mindennapi tevékenységeinket.

Az említett rendszerek azonban nem csak a felhasználói szokásokat változtatták, változtatják meg alapjaiban, a hírközlés struktúráját is teljesen átformálják. Ennek talán a leglényegesebb eleme az, hogy a tényleges kommunikációs szolgáltatást, valamint az ahhoz szükséges infrastruktúrát – ellentétben például a hagyományos telefóniával – nem egyazon szervezet biztosítja a felhasználó számára. Sőt, ezek a szolgáltatók a legtöbb esetben nem is tudnak egymásról, nincsenek semmilyen kapcsolatban egymással. Éppen ezért célszerű megvizsgálni a hírközlés és a kommunikáció viszonyát, majd elemezni a jelenleg is zajló strukturális változásokat, valamint az ezek kapcsán a törvényes ellenőrzés végrehajtásában jelentkező problémákat. Az internettechnológiára épülő szolgáltatások, azokon belül is a felhőalapú rendszerek törvényes ellenőrzésének igénye ugyanis a felhasználás ütemével arányosan nő, ugyanakkor a törvényes ellenőrzést végző szervek több – jogi és technikai – problémával is szembesülnek.

Annak érdekében, hogy ezeket a problémákat feltárjuk, és megoldásokat is találjunk rájuk, először publikus forrásokból elérhető információkra alapozva célszerű elemezni a külföldi nemzetbiztonsági szolgálatok, valamint rendvédelmi szervek által az internettechnológiára épülő szolgáltatások törvényes ellenőrzésére használt módszereket, továbbá azok technikai és jogi megfelelőségét, elfogadottságát; majd ezt követően megvizsgálni a hazánkban kialakult jogszabályi környezetet, illetve annak hatásait. Ezekkel a kérdésekkel foglalkozik ez a fejezet oly módon, hogy figyelembe veszi, a nemzetbiztonsági szolgálatok és rendvédelmi szervek szerepköre ebben az esetben eltér az előző fejezetben vizsgáltaktól. Míg a második fejezetben közvetlen felhasználóként, addig itt törvényes ellenőrzést végzőként kell ellátniuk feladataikat. Ez pedig azt jelenti, hogy a szolgáltatóval való viszonyuk, a felelősségi és érdekkörök megoszlása is – ahogy az *A felhőalapú rendszerek komplex biztonsági vizsgálatának szempontjai* című alfejezetben megtalálható – jelentősen eltér a korábban vizsgáltakétól.

Azt is figyelembe kell venni, hogy az érdemi, valóban jól használható eredmények elérése érdekében nem érdemes leszűkíteni a vizsgálatot a felhőalapú rendszerekre. Amint azt az *Internettechnológiára épülő szolgáltatások vs. felhő* című alfejezet is bemutatta, a PC/SaaS-rendszerek mindenképpen az internettechnológiára épülő szolgáltatások részhalmazának tekinthetők, ám a határvonalat, hogy mi tekinthető egyértelműen PC/SaaS-rendszernek, nagyon nehéz meghúzni. Éppen ezért ez a fejezet a kiterjesztőbb értelmű internettechnológiára épülő szolgáltatások megfogalmazást használja, de egyértelműen, sőt kiemelten bele kell ezekbe érteni a PC/SaaS-rendszereket is.

A kommunikáció változása

A kommunikáció formái, lehetőségei az internet, az internettechnológiára épülő szolgáltatások, azokon belül is kiemelten a felhőalapú PC/SaaS-rendszerek, valamint az ezek elérését biztosító eszközök fejlődésével ugrásszerűen változnak, bővülnek. Az is megállapítható, hogy a technológiák fejlődése és a felhasználási szokások nem választhatók szét egymástól. Egyfajta összefonódó spirált képezve hozták létre a mai népszerű kommunikációs formákat, adattárolási, -továbbítási lehetőségeket és egyéb internettechnológián alapuló szolgáltatásokat. A szélessávú- és mobilinternet-elérések elterjedése, a hordozható eszközök (például ultrabookok,

tabletek, okostelefonok stb.) hihetetlen mértékű fejlődése, a közösségi oldalak népszerűségének ugrásszerű növekedése, a különböző kommunikációs lehetőségeket biztosító internettechnológián alapuló szolgáltatások, felhőalapú rendszerek (mint például Facebook, Gmail, Dropbox, Twitter, Skype stb.), valamint az ezek használatát biztosító alkalmazások megjelenése minden nagyobb platformra (Windows, iOS, Android) mind-mind növelték a felhasználás mértékét, egyre több emberben erősítették az igényt a csatlakozásra, a használatra (Kovács, 2013c). Ezek pedig egymást is erősítve, egyre nagyobb mértékű felhasználást gerjesztve növelik tovább a változások ütemét. Mindemellett markánsan megjelenik a technológiák konvergenciája, összeolvadása, amit az eszközöknél és az azokkal igénybe vett szolgáltatásoknál egyaránt megfigyelhetünk (Sallai–Abos, 2007; Haig, 2015). Az eszközök esetében láthatjuk, hogy ma már egy kisméretű eszköz biztosítja a hang- és adatkommunikációt, valamint szinte az összes, korábban dedikált számítógéppel ellátott funkciót. A szolgáltatások tekintetében pedig elmondható, hogy sokszor egy szolgáltatótól igénybe vehetünk például kommunikációs, tárhely- és csoportmunkával kapcsolatos szolgáltatásokat egyaránt.

Az internettechnológiára épülő szolgáltatások törvényes ellenőrzésének igénye a felhasználás ütemével arányosan nő. Természetesen ezek közül is a PC/SaaS-rendszerek emelhetők ki a törvényes ellenőrzést végzők szempontjából, hiszen a potenciális célszemélyi kör is ezeket használja leginkább. Ugyanakkor a fent említett technológiai konvergencia erre a tevékenységre is alapvető hatással van. A törvényes ellenőrzés feladatrendszerébe – a mai megközelítés szerint – ugyanis alapvetően az alábbi három tevékenységet értjük:

- adatszolgáltatás,
- kommunikáció-ellenőrzés,
- számítógépes nyomozati (forensic) tevékenység.

Ez azonban a korábbi ellenőrző tevékenységekhez képest egy eltérő, változó képet mutat. Míg az adatszolgáltatásról és a kommunikáció-ellenőrzésről elsősorban a klasszikus hírközlési hálózatoknál beszéltünk, addig a számítógépes nyomozati tevékenység eddig kifejezetten csak a számítástechnikai rendszerek vizsgálatára volt jellemző. Ma már a fejlett infokommunikációs rendszerek jellege, valamint az azokból kinyerhető, a nemzetbiztonsági, illetve a bűnüldözési feladatokat segítő információk köre miatt mindháromra egyaránt, és legtöbbször ma már egymás mellett, egyszerre van szükség. Ebből levonható tehát az a következtetés, hogy nemcsak a technológiák

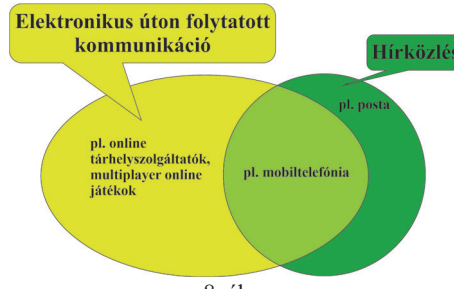
konvergenciája figyelhető meg napjainkban, hanem ennek kapcsán a törvényes ellenőrzési metódusok konvergenciája is.

A technikai fejlődés, a kommunikációs szokások változása, az informatikai és hírközlő rendszerek összeolvadása és az ezekből következő törvényes ellenőrzési metódusok konvergenciája komplex problémákat vet fel a törvényes ellenőrzésre feljogosított szervezetek számára (Kovács, 2011). A törvényes ellenőrzésre feljogosított szervek számára ugyanis a tevékenységük ellátásához jelenleg rendelkezésre álló, korábban jól működő technikai és jogi eszközök ma már sok esetben nem teszik lehetővé a teljes körű, hatékony feladatvégrehajtást.

Elektronikus úton folytatott kommunikáció vs. hírközlés

Az elektronikus úton folytatott kommunikáció megnevezés teljesen tudatos szóhasználat. Napjainkban ugyanis az említett fogalom alatt nemcsak a hírközlő rendszereken folytatott kommunikációt értjük, hanem minden olyan (kommunikációs) lehetőséget, formát, amely lehetővé teszi két – vagy adott esetben több – fél között információk, adatok áramlását, cseréjét. Ez pedig messze túlmutat nemcsak a hírközlés, de a kifejezetten kommunikáció céljából kifejlesztett, internetalapú rendszereken is.

Húsz évvel ezelőtt a hírközlés teljes egészében lefedte az elektronikus úton folytatott kommunikációt, ez utóbbi a hírközlés mintegy részhalmazát képezte. Mára ez a kép jelentősen megváltozott. Ha ábrázolnánk, akkor talán a 8. ábra megfelelően szemléltetné a kettő kapcsolatát. A területek nagysága az egymáshoz képesti jelentőséget is szemlélteti.



8. ábra

Az elektronikus úton folytatott kommunikáció és a hírközlés viszonya

Forrás: a szerző szerkesztése

Ma az elektronikus úton folytatott kommunikáció lehetőségei messze meghaladják a hagyományos hírközlését. A végeredmény szempontjából ugyanis nincs különbség a között, hogy megírunk és elküldünk egy elektronikus levelet, vagy megírás után a piszkozatok közé tesszük, de a másik félnek megadjuk a postafiók eléréséhez szükséges felhasználónevet és jelszót. Hiszen ez utóbbi esetben is hozzáfér, olvashatja ugyanazt az üzenetet. De itt még legalább a „levélszerűség" megvan, fellelhető a „hagyományos" hírközlési forma. Ha a továbbítani szánt információkat azonban egy felhőalapú tárhelyszolgáltatónál kialakított fiókba helyezzük el fájlként, majd ennek adjuk meg a belépéshez szükséges adatait a másik félnek, akkor a végeredmény ugyanaz: *A* felhasználótól *B* felhasználóhoz eljutott az információ. Ez a forma azonban már „nyomokban sem tartalmaz" hagyományos hírközlést. Ugyanilyen jellegű példa a multiplayer online játékok esete. Ezeket nem azért fejlesztették ki, hogy a felhasználók kommunikálni tudjanak egymással, az csak egy kiegészítője, hozadéka a játékoknak. Ugyanakkor tényszerűen vizsgálva, a végeredményt tekintve itt sincs különbség a játék során folytatott beszélgetések, chatelések és egy kifejezetten erre szakosodott hírközlő rendszeren folytatott beszélgetés vagy üzenetküldés között.

A törvényes ellenőrzést végző szervezeteknek alapvetően az a feladatuk, céljuk, hogy célszemélyeik kommunikációját lehetőség szerint teljes mértékben ellenőrizzék függetlenül annak formájától, a felhasznált technológiától. Az egyik legnagyobb feladat tehát, hogy az adott szervezetek pontosan meghatározzák azt, mit kell ehhez ellenőrizniük, majd ehhez ki kell alakítaniuk a megfelelő technikai és jogszabályi környezetet.

Az elektronikus úton folytatott kommunikáció változása

A fejezetnek nem célja, hogy az elektronikus úton folytatott kommunikációs technológiák változásának okait, tendenciáit teljes vertikumukban bemutassa, csupán érzékeltetni kívánja, miért kell foglalkozni vele, miért és milyen hatása van a törvényes ellenőrzésre.

A technológia fejlődésének, a kommunikációs formák és lehetőségek rohamos bővülésének köszönhetően a felhasználói szokások nagymértékben megváltoztak az elmúlt években. Az úgynevezett Y (1980–1994 között születtek) és Z (1995–2009 között születtek) generáció (mccrindle.com.au, 2012) tagjai abszolút meghatározó szerepet játszanak ebben. Ők azok, akik vagy már gyermekkorban találkoztak az internettel (Y generáció),

vagy már beleszülettek az internet uralta világba (Z generáció), így élen járnak az új kommunikációs lehetőségek használatában (intergeneracio.hu 2011). A korábbi generációk hagyományos elektronikus kapcsolatteremtési formái (például telefónia, SMS) helyett számukra sokkal fontosabbak az internetalapú kommunikációs lehetőségek, használatukat játszi könnyedséggel sajátítják el, a kibővített funkciókat természetesen és teljeskörűen használják. Okostelefonjaikkal vagy más mobil eszközeikkel évről évre növekvő mennyiségű adatforgalmat generálva bárhonnan, bármikor – az internetet használatával – kommunikálnak másokkal, kapcsolódnak a közösségi oldalakhoz, osztják meg életük pillanatait, töltik fel magukról a fényképeket, videókat. Emiatt a hagyományos kommunikációs lehetőségek túlságosan drágák és/vagy nem képesek biztosítani ugyanazokat a szolgáltatásokat számukra, így azokra egyre inkább csak kisegítő, tartalék rendszerként tekintenek. Jellemző, hogy a McCrindle Research kutatása szerint a Z generáció számára a MacBook, az iPad, a Google, a Facebook, a Twitter, a Wii, a PS3 és az Android jelenti az ikonikus technológiákat, szemben például az X (1965–1979 között születtek) generáció tagjaival, akiknek ugyanezt a kazettás videomagnó, a walkman és az IBM PC testesítette meg (mccrindle.com.au, 2012).

Az új technológiák megjelenése önmagában is arra készteti a kommunikáció törvényes ellenőrzésével foglalkozó szervezeteket, hogy figyeljék a trendeket, kövessék a sokak által használt technológiák fejlődését, és biztosítsák azok törvényes ellenőrzését. Legalább ugyanilyen mértékű kényszerítő erőt jelent, hogy a fenti bekezdésekben vázolt felhasználói változások okán a hagyományosnak mondható kommunikációs formák és rendszerek (például telefónia) jelentősége a felhasználók – ezáltal a potenciális célszemélyi kör, így a törvényes ellenőrzést végző szolgálatok – számára csökken.

A hírközlés változása

A megfizethető havi díjú, korlátlan adatforgalmat biztosító széles sávú internet elterjedése, a sokszor ingyenesen elérhető és használható, elektronikus kommunikációt lehetővé tevő alkalmazások, valamint a mobil eszközök fejlődése alapjaiban változtatja meg a hírközlési piacot. Egy jól megfigyelhető folyamat zajlik le, amikor is a korábbi, klasszikus hírközlési szolgáltatók helyét specializált szolgáltatók veszik át.

Klasszikus hírközlési szolgáltatónak tekinthetők azok a szolgáltatók, amelyek elektronikus hírközlő hálózatot üzemeltetnek, amelyen hírközlő szolgáltatást nyújtanak. A hangsúly a klasszikus szolgáltatók esetében az *és*en van, azaz a két szolgáltatási tevékenységet együtt végzik. Ilyenek például a hagyományos (vezetékes és mobil) telefonszolgáltatást biztosító cégek.

Az elektronikus hírközlésről szóló 2003. évi C. törvény (Eht.) (2003. évi C. tv.), így annak törvényes ellenőrzéshez kapcsolódó részei is elsősorban a klasszikus hírközlési szolgáltatásokon és szolgáltatókon alapulnak. A törvény a 188. § (értelmező rendelkezések) alatt definiálja az elektronikus hírközlési szolgáltató és az elektronikus hírközlési szolgáltatás fogalmát. Ezek a következők:

> *„13. Elektronikus hírközlési szolgáltatás: olyan, más részére általában ellenszolgáltatásért végzett szolgáltatás, amely teljesen vagy nagyrészt jeleknek elektronikus hírközlő hálózatokon történő átviteléből és – ahol ez értelmezhető – irányításából áll, de nem foglalja magában az elektronikus hírközlő hálózatok és elektronikus hírközlési szolgáltatások felhasználásával továbbított tartalmat szolgáltató vagy ilyen tartalom felett szerkesztői ellenőrzést gyakorló szolgáltatásokat, valamint nem foglalja magában az információs társadalommal összefüggő, más jogszabályokban meghatározott szolgáltatásokat, amelyek nem elsősorban az elektronikus hírközlő hálózatokon történő jeltovábbításból állnak.”*
> *„14. Elektronikus hírközlési szolgáltató: elektronikus hírközlő hálózat üzemeltetője, valamint elektronikus hírközlési szolgáltatást nyújtó természetes, illetőleg jogi személy vagy jogi személyiséggel nem rendelkező gazdasági társaság”* [(2003. évi C. tv. 188. § (13), (14)].

A törvény 2003-as megalkotásakor számos, napjainkban már széleskörűen használt technológia még nem létezett. A probléma érzékeltetésére lássunk két példát. A rendkívül népszerű Skype első béta verziója 2003 augusztusában jelent meg (tehát a törvény megalkotásakor még nem is volt elérhető!), míg 2011-re átlagban 20 millió felhasználó használta egyidejűleg ezt a szolgáltatást (Molnár–Zalatnay, s.d.). Másik példa a Facebook, amely 2004. február 4-én debütált, tehát a törvény hatályba lépésekor (2004. január 1-én) (2003. évi C. tv.) még el sem indult! 2012. október 4-én az alapító saját Facebook-oldalán tette közzé, hogy havi szinten több mint 1 milliárd ember használta aktívan a közösségi oldal nyújtotta szolgáltatásokat (Facebook,

s.d.; Zuckerberg, 2012), 2017 novemberére pedig már több mint 2 milliárd (Noyes, 2017).

A Skype mellett számtalan jelenleg kisebb vagy nagyobb jelentőséggel bíró, internetalapú kommunikációs alternatíva létezik, amelyek megfelelnek az elektronikus hírközlési szolgáltatás definíciójának, de a Skype-hoz hasonlóan üzemeltetőjük – vagy Magyarországon, vagy egyáltalán – nem rendelkezik saját elektronikus hírközlési hálózattal.

A klasszikus hírközlési szolgáltatói modellt egyre inkább felváltja egy specializált infrastruktúra-, alkalmazás- és tartalomszolgáltatói modell; ez a tendencia a jövőben várhatóan tovább erősödik. Az új modell legjelentősebb hatása a hírközlésre, hogy az infrastruktúra-szolgáltató a hírközlési hálózatot – vagy célszerűbb megfogalmazással internetelérést – biztosítja, míg az alkalmazásszolgáltató gondoskodik a tényleges kommunikációs szolgáltatásról.

Az infrastruktúra-, alkalmazás- és tartalomszolgáltatói modell pontos leírása a fejezet utolsó részében olvasható, itt csak oly mértékben említjük, amennyire a törvényes ellenőrzés problémáinak felvetéséhez és lehetőségeinek vizsgálatához szükséges. Így például a tartalomszolgáltatókkal itt egyáltalán nem, csupán a fejezet végén foglalkozunk.

Az alkalmazásszolgáltató elnevezést nemcsak azért célszerű használni a hírközlési szolgáltató helyett, hogy megkülönböztessük a korábban együtt nyújtott két funkció (infrastruktúra- és kommunikációs [hírközlési] szolgáltatás) szétválasztását, hanem azért is, mert az alkalmazásszolgáltató kifejezés egy bővebb, tágabb értelmezésű fogalom, és nem csak a hírközlési szolgáltatást nyújtó alkalmazásokat érjük, érthetjük alatta. Erre lehet példát találni a *Felhő alapú új pénzügyi tranzakciós lehetőségek és azok veszélyei* című cikkben is (Gazdag–Kovács, 2014).

A hírközlési szolgáltatók specializált szolgáltatókra történő szétválása nem csak a törvényes ellenőrzés tekintetében jelent problémát. A széles sávú, mobilan bárhonnan elérhető internet arra ösztönzi a felhasználókat, hogy az erre alapuló, a korábbiaknál olcsóbb, több szolgáltatást biztosító kommunikációs formákat válasszák. Az internet – és ez ma már a mobilinternetről is elmondható – megfizethető, nem túlságosan magas fix havi díjért, korlátlan vagy az átlag felhasználói szokások okán annak tekinthető adatforgalommal nagyon sok ember számára elérhető. Amennyiben

kifejezetten a mobilkommunikációt nézzük, minden költséget összeadva olcsóbban lehet főleg külföldi viszonylatban kommunikálni a Skype vagy a Viber segítségével, mint hagyományos telefonszolgáltatással. Ugyanakkor az említett vagy a hasonló jellegű, internetalapú kommunikációs szolgáltatásoknak csupán egy része ingyenes, más részük igénybevételéért (például vezetékes vagy mobiltelefon hívása esetén) viszont fizethetnünk kell. De még az ingyenes szolgáltatások esetében is jelentős reklámbevételek keletkeznek. Ez természetes, ugyanis ezekből a bevételekből fedezi az alkalmazásszolgáltató a költségeit, és a megmaradó profit az, amiért érdemes ezt a tevékenységet folytatnia. Azonban a profit csak nála, és nem az internetszolgáltatónál –, aki ez esetben a korábbi hírközlési szolgáltatóból immár infrastruktúra-szolgáltatóvá avanzsált – képződik. Ugyanez elmondható nemcsak kommunikációs, hanem más alkalmazások esetén is.

Az internetszolgáltatók az éles piaci verseny, a sávszélesség és a szolgáltatások minőségének növelése okán óriási összegeket költenek technológiai fejlesztésekre, miközben időről időre csökkentik a havi díjak összegét. Ez a mobilinternetet nyújtó, infrastruktúrát is üzemeltető valódi, nem virtuális szolgáltatókra fokozottan igaz. Természetesen ez is termel profitot, de az igazán nagy nyereség nem náluk keletkezik, hanem az általuk üzemeltetett infrastruktúrán elérhető, internetet felhasználó alkalmazások szolgáltatóinál. Ráadásul ez utóbbiak sokkal kisebb kockázattal jutnak sokkal magasabb profithoz. Ezt pedig a jóval kisebb mértékű és értékű beruházási igényeknek, az alacsonyabb működési költségeknek, valamint a felhasználóktól, továbbá – nem utolsósorban – a hirdetőktől befolyó jóval magasabb összegeknek köszönhetik.

Ezt a jelenséget az egyre inkább infrastruktúra-szolgáltatóvá váló hírközlési cégek is kezdik felismerni, és próbálnak valamit tenni a helyzet megváltoztatása érdekében. Erre az egyik legjobb példa az Orange cég esete, amelynek sikerült elérnie, hogy nagy költséggel járó infrastrukturális fejlesztéseihez a hálózatát – természetesen a felhasználói szokások okán – leginkább használó Google pénzügyileg hozzájáruljon (Dajkó, 2013a; Gállfy, 2013). Erre korábban is voltak már – sikertelen – kezdeményezések (Koi, 2010), a francia szolgáltató sikeres akciója azonban precedenst teremtett. Lépésével várhatóan egy folyamat indul el, átalakul az internet korábbi, sérthetetlennek tűnő üzleti modellje (Dajkó, 2013a).

Az internettechnológiára épülő szolgáltatások törvényes ellenőrzésének problémái

A törvényes ellenőrzést végző szervezetek technikai és jogi eszközökkel rendelkeznek tevékenységük ellátásához. A napjainkban rendelkezésre álló eszközök alkalmazása, alkalmazhatósága és azok hatékonysága azonban több problémát is felvet.

Az internettechnológiára épülő szolgáltatások ellenőrzése esetén a jogi kapcsolat a szolgáltató és a törvényes ellenőrzést végző között áll fenn – ideális esetben – törvényi kötelezettség alapján. Problémaként jelentkezik azonban, hogy amíg a hírközlési hálózatoknál egy kialakult, minden szereplő által elfogadott és a demokratikus államokban hasonló jellegű törvényekre alapozott törvényes ellenőrzésről beszélhetünk, addig ebben az esetben nem mondható el ugyanez. A fent vázolt modell szerint itt ugyanis sokkal inkább különálló infrastruktúra-, alkalmazás- (és tartalom-) szolgáltatókkal találkozunk; nagyon ritka az az eset, amikor a felhasznált infrastruktúrát és alkalmazást egyazon szolgáltató biztosítja. Márpedig a 2016 előtti hatályos magyar jogszabályok alapján csak ez utóbbi esetében volt vitán felül állóan hírközlési szolgáltatónak tekinthető, és így a törvényes ellenőrzés kapcsán együttműködésre kötelezhető bármely szolgáltató. Ugyanakkor a 2016-ig hatályban lévő jogszabályainkban az infrastruktúra-, alkalmazás- és tartalomszolgáltatók nem vagy nem megfelelő módon voltak definiálva, a törvényes ellenőrzés kapcsán felmerülő kötelezettségeik pedig szintén nem vagy jó esetben is csak részlegesen voltak kiolvashatók ezekből.

Ez a probléma a mai napig fennáll a legtöbb országban, így a Magyarország számára jogrendszerében meghatározónak mondható országokban is (elsősorban az EU nagyobb államai, az Egyesült Államok), ahol még mindig az útkeresés zajlik az ellenőrzés szabályozása tekintetében. Erről és a 2016-ban hatályba lépett magyar szabályozásról, valamint annak hatásairól a fejezet végén még lesz szó.

Az ellenőrzéshez használt technikai eszközök kapcsán ugyancsak problémákkal szembesülnek a felhatalmazott szolgálatok. Egyrészt az új technológia új ellenőrző eszközöket kíván(hat) amelyek ráadásul akár szolgáltatónként eltérő megoldásúak lehetnek. Ezek pedig meglehetősen költséges beruházásokat indukálhatnak. Másrészt a hírközlés-szolgáltatókkal ellentétben, amelyek – a törvényi kötelezettségek okán – együttműködnek a nemzetbiztonsági és bűnüldöző szervekkel, az internetalapú kommunikációt biztosító alkalmazásszolgáltatók nem vagy nem teljes mértékben

teszik ugyanezt. A hírközlési szolgáltatók számára többek között kötelező a szolgáltatást bejelenteni és

> *„biztosítani az elektronikus hírközlő hálózatban továbbított küldemények, közlések, továbbá a szolgáltató által kezelt adatok titkos információgyűjtéssel, illetve titkos adatszerzéssel történő megismeréséhez szükséges eszközök és módszerek alkalmazási feltételeit”* (2003. évi C. tv.).

Ilyenfajta kötelezettsége azonban 2016 előtt nem volt az alkalmazásszolgáltatóknak Magyarországon, de ennek előírása az Európai Unió más országainak, sőt a világ többi államának ma is komoly problémákat okoz.

Jelenleg ugyanis nincs olyan szabályozás, amely európai szinten irányadó lenne a kérdésben, és amely rövid időn belül – nagyobb szolgáltatói ellenállás nélkül – átemelhető lenne az európai országok törvényeibe, vagy amelyhez – ha arra szükség lenne – igazítani lehetne a hatályos magyar jogszabályokat. Ez pedig két gondot generál. Az első, hogy az alkalmazásszolgáltatók hajlandóságán múlik, hogy engedik-e ellenőrző eszköz telepítését, esetleg saját eszközeikkel egyfajta törvényes ellenőrzést mint szolgáltatást (LMaaS)[41] (Kovács, 2012) nyújtanak a szolgálatok számára, vagy teljesen elutasítja az együttműködést. Ez utóbbira – sajnos negatív – példa a Google esete, amely nem hogy nem működik együtt, de átláthatósági jelentéseiben még közzé is teszi, melyik országból hány adatszolgáltatási kérést kapott, és abból mennyit, milyen minőségben teljesített. A cég Magyarországnak annak ellenére sem szolgáltatott információkat, hogy az azokra vonatkozó kérések teljes mértékben kielégítették a hazánkban hatályos törvényi feltételeket (Dajkó, 2013b). A 2016-ban hazánkban elfogadott új jogszabályok erre hazai viszonylatban már megoldást nyújtanak, ám az együttműködés kikényszeríthetősége már más kérdés. Erről is lesz még szó a fejezet végén. A másik gond, hogy míg a hagyományos hírközlés ellenőrzésénél a jól ismert törvényi és technikai háttér okán teljes értékű technikai megoldásokat kínálnak az erre szakosodott gyártók, addig az internettechnológiára épülő szolgáltatások ellenőrzésére elsősorban egyedi problémákat megoldó eszközöket tudnak csak szállítani. Ez pedig drágává, bonyolulttá és esetivé teszi az ellenőrzéseket.

---

41 Lawful Monitoring as a Service (törvényes ellenőrzés mint szolgáltatás).

A megoldás első lépését az egységes törvényi háttér kialakítása jelentheti. Ebben az egyik legfontosabb feladat, hogy pontosan definiáljuk az infrastruktúra-, alkalmazás- és tartalomszolgáltatók fogalmát; meghatározzuk, mit kell ellenőrizni, és annak megfelelően kell kialakítani a megfelelő jogszabályi környezetet. Amint az előző alfejezet végén az Orange cég példája mutatta, elindulhat egy folyamat, amely során átalakul az internet korábbi, sérthetetlennek tűnő üzleti modellje. Várhatóan hasonló változások következnek be a törvényes ellenőrzés területén is. Ahhoz ugyanis, hogy a nemzetbiztonsági és bűnüldözési munkát hatékonyan támogató ellenőrzést lehessen kialakítani, olyan, jelenleg szintén sérthetetlennek tűnő dolgokhoz kell hozzányúlni, szabályozni és adott esetben szankcionálni (!), mint az adott országban infrastruktúrával nem rendelkező, internetes alkalmazást nyújtó cégek működési jogai, kötelezettségei. Az erre precedenst teremtő hazai szabályozás részleteiről, tartalmáról és hatásairól a fejezet végén lesz szó.

A hírközlési szolgáltatók kontra alkalmazásszolgáltatók kapcsán korábban említett kettős helyzet rendezése a nemzetbiztonsági, bűnüldöző szerveken kívül a klasszikus hírközlési szolgáltatóknak is érdeke. Ugyanis amíg az infrastruktúrával is rendelkező, azokat üzemeltető hírközlési cégek kötelezettségeit (bejelentés, együttműködés a törvényes ellenőrzés kapcsán, adófizetés, frekvenciadíj stb.) a hatályos jogszabályok pontosan előírják, az erre feljogosított hatóság pedig szankcionálhatja, addig az infrastruktúrával nem rendelkező alkalmazásszolgáltatók esetében ez ma nemzetközi szinten általánosságban nem mondható el. A 2016-ban hatályba lépett hazai szabályozó is csupán a törvényes ellenőrzés kérdését rendezi. Hazánkban korábban a problémát az jelentette, és a törvényes ellenőrzésen kívül még ma is az jelenti, hogy az infrastruktúrával nem rendelkező alkalmazásszolgáltatók egy része csak bizonyos jogértelmezéssel lenne az Eht. hatálya alá tartozónak tekinthető, más részük pedig még úgy sem. A Nemzeti Média- és Hírközlési Hatóság (NMHH) által közzétett *Elektronikus hírközlési szolgáltatások hatósági osztályozása* alatt megtalálható *Szolgáltatástípusok* (NMHH, 2008) és *Szolgáltatás leírása* (Swisher, 2011) dokumentum sem segít a probléma feloldásában, ugyanis azok is kifejezetten a klasszikus hírközlési szolgáltatásokra koncentrálnak. Ezt bizonyítja az is, hogy az *Egyéb előfizetői adatátviteli szolgáltatás* címke alatti leírásnál – amelybe talán beleérthetők lennének az alkalmazásszolgáltatók – a következő példa szerepel: *„Ide tartozik például az önálló elektronikus hírközlési szolgáltatásként nyújtott MMS-szolgáltatás”* (NMHH, 2012, 2.). Az viszont egységesen elmondható,

hogy az alkalmazásszolgáltatók szankcionálására egyrészt eddig nem volt példa, másrészt az egyébként is rendkívül nehezen kivitelezhető.

Így fordulhatott elő, hogy a korábban már említett eset szerint a Google bár Magyarországon szolgáltatott, ki tudott bújni a hatályos jogszabályok alól, és az érvényes törvényeknek megfelelő adatszolgáltatási kérést vissza tudta utasítani. Ez a hagyományos postai és klasszikus elektronikus hírközlési szolgáltatók esetében elképzelhetetlen lenne. Ráadásul a Google-nak és a többi hasonló alkalmazásszolgáltatónak még azokat a törvényes ellenőrzéshez kapcsolódó költségeket sem kell(ett) viselnie, amelyeket a hírközlési szolgáltatók magyarországi piacra lépésükkel vállalnak. A 2016-ban hatályba lépett hazai szabályozás törvényes ellenőrzésének lehetőségeire gyakorolt hatásait, korlátait a fejezet végén még kifejtjük.

A felhőalapú – így a PC/SaaS- – rendszerek törvényes ellenőrzésének szabványosításán többek között az ITU és az ETSI is dolgozik. Azonban amíg ezek elkészülnek, és megjelennek – az akár ezekből levezetett – európai szintű jogszabályok, addig még várhatóan hosszú évek telnek el. További időt vesz igénybe az európai szabályzó átültetése a hazai jogi környezetbe, majd annak elfogadtatása és hatályba léptetése is. Ezt viszont nem célszerű megvárni. A megoldást egy új – de az egységesen elfogadott európai szabályozás megjelenéséig akár átmenetinek is tekinthető – hazai jogi szabályozás kialakítása jelentette 2016-ban, amelyről a fejezet végén részletesen lesz szó.

Az internettechnológiára épülő szolgáltatások törvényes ellenőrzési módszereinek vizsgálata

Az előző alfejezetben említett új jogszabályi – legyen az átmeneti vagy hosszú távú – környezet megalkotásának alapja, hogy pontosan meg kell határozni a szereplőket. Erre megfelel az infrastruktúra-, alkalmazás- és tartalomszolgáltatói modell. Ugyanakkor azt is meg kell vizsgálni, hogy ez szükséges és elégséges-e a törvényes ellenőrzés megfelelő jogszabályi alapjainak megteremtéséhez a mai viszonyok között. A kérdés eldöntéséhez célszerű megvizsgálni és összehasonlítani a törvényes ellenőrzésre jelenleg rendelkezésre álló technikai eszközöket és módszereket előnyeikkel, hátrányaikkal együtt. Ez egyrészt lehetőséget ad majd a szolgálatoknak arra, hogy kiválaszthassák egy adott feladathoz leginkább megfelelőnek és hatékonynak tartott, törvényesen felhasználható ellenőrzési módszert, másrészt segít

rávilágítani, hol vannak olyan törvényi hiányosságok, amelyeket a jogszabályi környezetben mindenképp le kell fedni. Ezek alapján lehet pontosan definiálni az infrastruktúra-, alkalmazás- és tartalomszolgáltatók fogalmát.

Ennek érdekében viszont először elemezni kell az internettechnológiára épülő szolgáltatások törvényes ellenőrzésének kihívásait, valamint – már amennyire ezek elérhetők – publikus forrásokból megszerezhető információkra alapozva a külföldi nemzetbiztonsági szolgálatok és rendvédelmi szervek által használt módszereket. Ehhez a példák ismertetésénél itt főként a Skype lesz a minta. Egyrészt azért, mert e rendszer lehallgatása minden országban megoldandó, de problémás feladatként jelentkezett az elmúlt időben, másrészt pedig azért, mert jól példázza, hogy egy új infokommunikációs rendszer törvényes ellenőrzése kapcsán a különböző országok képesek gyökeresen eltérő irányokba elindulni.

Az internettechnológiára épülő szolgáltatások törvényes ellenőrzési kihívásai

Az internettechnológiára épülő szolgáltatások, ezen belül is kiemelten a felhőalapú rendszerek törvényes ellenőrzése minden ország nemzetbiztonsági és rendvédelmi szervét kihívások elé állítja. Amint azt *A kommunikáció változása* című alfejezetben is láthattuk, az elektronikus úton folytatott kommunikáció ma már jóval tágabb értelemben értelmezhető fogalom, mint a hagyományos hírközlés, hiszen lehetőségei, a kommunikációs formák száma messze meghaladja ez utóbbiét. Rengeteg olyan új rendszer, technológia jelent, jelenik meg, amelyek törvényes ellenőrzését az arra feljogosított szolgálatoknak meg kell vagy legalábbis meg kellene oldania, hiszen alapvető feladatuk az, hogy célszemélyeik kommunikációját lehetőség szerint teljes mértékben ellenőrizzék, függetlenül annak formájától, az általuk felhasznált technológiától, eszközöktől, alkalmazásoktól. Éppen ezért a kommunikáció törvényes ellenőrzésével foglalkozó szervezeteknek figyelniük kell a technológiai trendeket, mert új kommunikációs formák megjelenésével és elterjedésével célszemélyeik, így az ő számukra is a hagyományos, korábban ellenőrzött kommunikációs formák és rendszerek (például telefónia) jelentősége csökken, míg az újonnan megjelenőké – relevanciájuk mértékben – nő.

Az említett szervezetek számára az egyik legnagyobb kihívás tehát éppen az, hogy pontosan meghatározzák, mely rendszereket, szolgáltatásokat kell,

célszerű ellenőrizni. Ez önmagában sem egyszerű; továbbá a kiválasztott rendszerek ellenőrzésének technikai megoldása még nehezebb feladat. Ha pedig a jogszabályi háttér adott technikai megoldásokat nem is támogat vagy kifejezetten tilt, akkor akár teljesen el is lehetetlenülhet az ellenőrzés.

Az elektronikus úton folytatott kommunikáció változásában nagy szerepük van az internettechnológiára épülő szolgáltatásoknak, azon belül pedig a PC/SaaS felhőalapú rendszereknek, ahol is alkalmazásszolgáltatók biztosítják azokat a szolgáltatásokat, amelyeken keresztül – a lehető legkülönfélébb módon – elektronikus kommunikációt lehet folytatni. E rendszerek törvényes ellenőrzésének megteremtése tehát kiemelt feladat az arra feljogosított szervek számára, ugyanakkor a feladat ellátását több probléma is nehezíti.

Az egyik gond a jogi szabályozás hiányosságaiban keresendő. A rohamosan fejlődő technológiával, az ezen belül gyökeresen átalakuló kommunikációs módokkal, valamint az internet szabadságával egyelőre nehezen birkózik meg a jogi világ. A hatályos jogszabályok egyáltalán nem, nem teljes mértékben vagy csak erős *beleértéssel* teszik lehetővé az internettechnológiára épülő szolgáltatások ellenőrzését.

A másik problémát a technikai megoldások hiánya jelenti. Az új technológia új ellenőrző eszközöket kíván(hat), ez pedig jelentős beruházásokat igényel. Ráadásul az eltérően felépített szolgáltatói infrastruktúrák miatt ez akár szolgáltatónként eltérő megoldásokat igényelhet, ami igen költséges. Sokszor azonban még nagyobb gondot jelent az, hogy még csak nem is állnak rendelkezésre azok a technikai eszközök, amelyekkel az új technológiák törvényes ellenőrzését egyáltalán végre lehet hajtani.

A harmadik nagy problémát az okozza, hogy a hírközlés-ellenőrzésnél régóta kialakult és elfogadott rend, miszerint az infrastruktúrával, valamint szolgáltatással az adott országban egyaránt jelen lévő szolgáltató együttműködik a nemzetbiztonsági és bűnüldöző szervekkel, ebben az esetben nem vagy nem teljes mértékben működik.

Az arra feljogosított szerveknek azonban addig is, amíg kialakul a mindenki által elfogadott, letisztult jogi környezet és az összes igényt kielégítő technikai háttér, a törvényes ellenőrzést – valamilyen formában – biztosítaniuk kell. Ehhez a már rendelkezésre álló technikai kelléktárat és a hatályos jogszabályokat alapul véve próbálnak a szolgálatok más és más megoldásokat alkalmazni. Még a fejlett demokráciával és ipari háttérrel rendelkező országok esetében is sokszor gyökeresen eltérő megoldásokat találhatunk, nem beszélve a demokráciát még éppen csak építő vagy nem is demokratikusnak

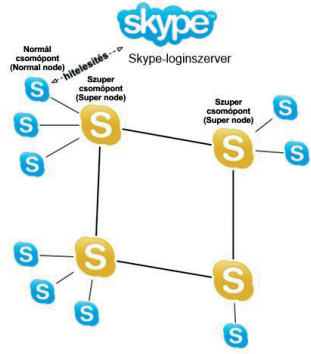
tekintett országokról. Annak érdekében, hogy a rendelkezésre álló ellenőrzési metódusokat elemezhessük és összehasonlíthassuk, először érdemes – a nyíltan elérhető anyagok alapján – megvizsgálni, egyáltalán milyen módszerek állnak a titkos információgyűjtést végző szervezetek rendelkezésére, és azok alkalmazása során milyen buktatókba ütköztek.

Nemzetközi példák I. – a Skype mint „állatorvosi ló”

A korábban leírtaknak megfelelően a Skype esetét célszerű különállóan vizsgálni, mert ebből sok általános következtetést le lehet vonni.

A rendkívül népszerű Skype első béta verziója 2003 augusztusában jelent meg (Woollaston, 2013), ám 2017 októberében már 300 millió aktív felhasználója volt, akik naponta átlagban 3 milliárd percnyi összeköttetést létesítettek vele (Smith, 2017b). Ez kiválóan szemlélteti a felhasználói szokások változását, hiszen jól mutatja, hogy míg a hagyományosnak mondható kommunikációs formák és rendszerek (például telefónia) jelentősége a felhasználók – ezáltal a potenciális célszemélyi kör, így a törvényes ellenőrzést végző szolgálatok – számára csökken, addig az új rendszereké sokszor robbanásszerűen nő (Kovács, 2013c). A Skype pedig szinte minden nemzetbiztonsági és bűnüldöző szerv prioritási listájának élén áll(t).

Röviden érdemes áttekinteni, mi is okozza a problémát e rendszer ellenőrzése kapcsán. Az egyik maga a rendszer felépítése. Ennek sematikus elrendezése a 9. ábrán látható.



9. ábra

A Skype topológiája

Forrás: a szerző szerkesztése a Stanford University, s.d. alapján

A működés leegyszerűsítve úgy történik, hogy a korábban már regisztrált felhasználó (a regisztrációhoz csupán egy érvényes e-mail-címre van szükség!) bejelentkezik felhasználói nevével a Skype központi szerverére, ahol a jelszava alapján megtörténik a hitelesítése. A hitelesített felhasználó lekérdezheti kontaktlistáját, felhasználói adatait, más felhasználókat kereshet stb. A tényleges kommunikáció közvetlenül – a kommunikáló felek (Node-ok) közvetlen összeköttetésben állnak egymással – vagy közvetetten – a kommunikáló felek Supernode-okon keresztül állnak összeköttetésben egymással – zajlik, de nem folyik át egy központon (Molnár–Perényi, 2010; Baset–Schulzrinne, 2006). Éppen ezért már az egy felhasználóhoz tartozó kommunikáció elfogása is – figyelembe véve, hogy a felhasználók mobil eszközökkel bárhonnan használhatják a szolgáltatást – rendkívül nehéz.

A másik problémát a felhasznált magas szintű titkosítás (RSA és AES–256) okozza (Microsoft, s.d.c). Azaz, ha sikerül is „útközben" elfogni a teljes kommunikációt, annak tényleges tartalmához csak a használt titkosítás visszafejtése után lehetséges hozzáférni. Az ehhez szükséges számítási kapacitás és időigény meglehetősen nagy, a tömeges méretű ellenőrzést ez meglehetősen megnehezíti vagy inkább teljes mértékben kizárja.

További gondot okoz a korábban már említett regisztráció, amelyhez csupán egy érvényes e-mail-címre van szükség. Emiatt a törvényes ellenőrzés feladatrendszerébe beleértett – és hagyományos hírközlési szolgáltatók esetében hatékonyan alkalmazható – felhasználói/előfizetői adatok szolgáltatása (Kovács, 2013c) ebben az esetben nehézkesen, illetve főleg hiányosan valósul meg.

A fentiek okán – természetesen a publikusan elérhető információk korlátozott volta miatt – a teljesség igénye nélkül célszerű megvizsgálni, melyik ország hogyan ellenőrzi (vagy hogyan próbálja ellenőrizni) a Skype-rendszert. Bár a példák elsősorban azt szolgálják, hogy az ellenőrzésre való elveket, technológiákat, valamint a használatuk kapcsán felmerült jogi, technikai problémákat áttekinthessük, emellett arra is jók, hogy analógiaként felhasználhatók legyenek majd más internettechnológiára épülő szolgáltatások ellenőrzési kérdéseinek vizsgálatakor.

Az USA és a Skype

A nyíltan elérhető források alapján arra lehet következtetni, hogy az USA a *Skype-probléma* megoldására a szolgáltatóval való együttműködést

választotta. 2011 májusában már tényként könyvelték el, hogy a Microsoft 8,5 Mrd USD-ért felvásárolta a Skype-ot (Swisher, 2011). Az ügyletet az Európai Unió versenyjogi végrehajtó szerve, az Európai Bizottság még az év októberében jóváhagyta, így elhárult minden akadály a fúzió elől. A felvásárlás már csak azért is „érdekes" volt, mert a Skype üzleti szempontból nem volt éppen sikertörténet. 2010-ben 7 millió dolláros nettó veszteséget könyvelhettek el amellett, hogy ugyanebben az évben, december 31-én a társaság hosszú távú adósságállománya 686 millió dollár volt (Origo, 2011).

A szaksajtóban már a felvásárlás bejelentésekor elindultak a találgatások, hogy miért is kell(het) a Skype a nagy hírű redmondi cégnek (Bodnár, 2011; Insider, 2011). Az ott felvetetteken kívül nem kell túl nagy fantázia ahhoz, hogy az addig a titkosítás és a *peer-to-peer*[42] (P2P) struktúra miatt nagy nehézségekbe ütköző törvényes ellenőrzést is felírjuk a listára, ott is alighanem az első helyre. Ennek megvalósítása az USA nemzetbiztonsági és bűnüldöző szervei számára ugyanis sokkal egyszerűbben kivitelezhető, ha egy olyan cég a tulajdonos, amely székhelye az Egyesült Államokban található, és együttműködik az említett hatóságokkal, szervezetekkel. Ezt a feltételezést erősítik azok az információk is, hogy a felvásárlást követően a Microsoft megkezdte a Skype infrastruktúrájának átalakítását, és egy központosítottabb hálózatot kezdett kiépíteni. A változás az addig rotációban a felhasználók között kiosztott úgynevezett Supernode-oknál indult el. Egyrészt számukat jelentősen csökkentették (több mint 48 ezerről kb. 10 ezerre), másrészt az új Supernode-ok már nem lehetnek felhasználók gépei, hanem csak és kizárólag a Microsoft/Skype központjába telepített eszközök (Expert: Miami, 2012). Mára már az is bizonyított, hogy a Microsoft minden írott üzenethez hozzáfér, a továbbított üzenetekben pedig szűrést is végez. Ez a képesség pedig lehetőséget teremt arra is, hogy az üzenetek tartalmát hozzáférhetővé tegye a titkos információgyűjtésre feljogosított szervek számára (The H Security, 2013; Schmidt, 2013; Solovjovs, 2013).

Ezt a teóriát erősítették a Prism programról nyilvánosságra került adatok is. Az ott leírtak szerint a Skype és a többi nyolc vezető internetes alkalmazásszolgáltató (Microsoft, Yahoo, Google, Facebook, PalTalk, AOL, YouTube, Apple) rendszerein tárolt és azokon átfolyó adatokhoz (például beszélgetések, videócsetek, fényképek stb., 10. ábra) – szolgáltatónként változó formában és mélységben – fér hozzá a Nemzetbiztonsági Ügynökség

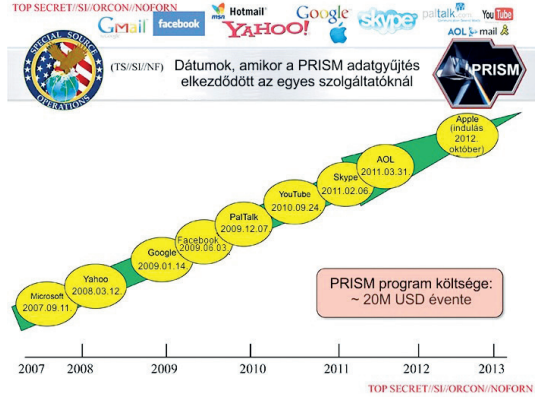
[42] A *peer-to-peer* kapcsolat lényege, hogy az informatikai hálózat végpontjai kitüntetett központi csomópont nélkül, közvetlenül egymással kommunikálnak.

(National Security Agency – NSA), a Szövetségi Nyomozó Iroda (Federal Bureau of Investigation – FBI) és az NSA-n keresztül az angol Kormányzati Kommunikációs Központ (UK Government Communications Headquarters – GCHQ); (POITRAS–GELLMAN, 2013). A Skype-ot a kiszivárgott információk szerint 2011. február 6-án kapcsolták be a programba. (11. ábra.)

10. ábra

A Prism programban szereplő szolgáltatók és az általuk – különböző mértékben – biztosított adatok

Forrás: a szerző szerkesztése a The Washington Post, 2013 alapján



11. ábra

A Prism programban részt vevő szolgáltatók és csatlakozásuk időpontja

Forrás: a szerző szerkesztése a The Washington Post, 2013 alapján

Oroszország és a Skype

Oroszország is a szolgáltatókkal történő együttműködést választotta, csak annak egy másik változatát. Az Orosz Szövetségi Biztonsági Szolgálat (Федеральная служба безопасности Российской Федерации – FSZB; angolul: Federal Security Service of the Russian Federation) 2011-ben vetette fel, hogy be kellene tiltani a Skype, a Gmail és a Hotmail működését Oroszországban, mert azok ismeretlen algoritmusokat használnak a titkosításra, így tartalmuk ellenőrizhetetlen. Ez pedig biztonsági kockázatot jelent (Sg.hu, 2011). A Microsoft a Skype felvásárlását követően bejelentette, hogy – a korábban más szoftvereinél alkalmazott gyakorlatának megfelelően – kész átadni annak forráskódját és titkosítási algoritmusát az orosz szolgálatnak, ezáltal elkerülheti annak betiltását (Fedorinova, 2011; Berta, 2011). A lehallgatás, sőt a felhasználók pontos tartózkodási helyének meghatározási képességét orosz lapértesülésre hivatkozva a szaksajtó ma már tényként kezeli (Berta, 2013a).

Kína és a Skype

A szolgáltatók Kínában is együttműködnek a törvényes ellenőrzést végző hatóságokkal. Az ázsiai országban a Skype egy speciális változatát használják, amelyet a – többségi tulajdonos – TOM Online (egy kínai internetszolgáltató cég) és a Microsoft által alapított vegyes vállalat adott ki TOM–Skype néven. A szoftver feltörése után bizonyítottá vált, hogy a kínai hatóságok ezen keresztül ellenőrzik a kommunikációt, az azonnali üzenetküldések esetében több ezer szavas szótáralapú kulcsszavas keresést használnak, és találat esetén rögzítik a teljes csetelést, vagy adott esetben blokkolják a forgalmat (Silver, 2013).

Franciaország és a Skype

Franciaország törvényi alapon kíván együttműködést elérni a törvényes ellenőrzés tekintetében a Skype szolgáltatójával, mégpedig úgy, hogy hagyományos hírközlési szolgáltatónak kívánja minősíteni azt. Ennek megállapítása érdekében a Francia Elektronikus Hírközlési és Postai Szabályozó Hatóság (Autorité de régulation des communications électroniques et des

postes – ARCEP; angolul: French Electronic Communications and Postal Regulatory Authority) beadvánnyal fordult az ügyészséghez. Amennyiben ez sikerül, akkor ugyanazok a kötelezettségek vonatkoznak a Skype szolgáltatójára is, mint a hagyományos hírközlési szolgáltatókra, azaz lehetőséget kell teremtenie a hálózatán keresztül a segélyhívó rendszerek elérésére, adót kell fizetnie a francia államnak, és – nem utolsósorban – az arra feljogosított szervek számára biztosítania kell a törvényes ellenőrzést is (Koi, 2013; ARCEP, 2013).

Nemzetközi példák II. – egyéb országok

Természetesen nem csak a Skype az, amelyet a hatóságok ellenőrizni kívánnak, illetve a fent említett módszerekkel nemcsak a Skype, hanem más alkalmazásszolgáltatók rendszerein küldött és tárolt információk is ellenőrizhetők. A következő példákban is többnyire fellelhető a Skype ellenőrzése, de e mellett a más rendszerekből származó információk megszerzése a korábbiaknál sokkal hangsúlyosabban jelenik meg, így ezeket célszerű külön csoportban vizsgálni. Már csak azért is, mert a következő példák jól mutatják, hogy egyrészt a szolgáltatóval való együttműködésen vagy együttműködésre történő kényszerítésen túl is vannak lehetőségek a titkos információgyűjtésre feljogosított szervezetek kezében, másrészt egy ország több ellenőrző módszert is használ(hat).

Németország és az online házkutatás

Németországból szivárgott ki a legtöbb információ a törvényes ellenőrzések során használt – és sok más névvel is illetett, például kémprogramok, trójai programok – online házkutatásról. A módszer törvénybe iktatása, ezáltal a használat kereteinek kialakítása már régóta szerepelt a német parlament napirendjén (Berta, 2008). Többszöri elutasítást (Dajkó, 2007; Dajkó, 2008) követően a szövetségi alkotmánybíróság végül úgy foglalt állást, hogy a módszer használható, de szigorú keretek között, kizárólag kommunikáció ellenőrzésére, azaz gyakorlatilag az internetes telefon (például Skype) lehallgatására. Egy német hackercsoport, a Chaos Computer Club (CCC) azonban analizálta a német hatóságok által használt, a szintén német DigiTask által gyártott *malware-t,* és megállapította, hogy annak képességei

messze túlmutatnak a fent említett, szövetségi bíróság által megszabott kereteken (Dajkó, 2011; CCC, 2011).

Ezt követően a német hatóságok egy saját eszköz kifejlesztése mellet döntöttek, amelyet a Szövetségi Bűnügyi Hivatal (Bundeskriminalamt – BKA) berkein belül felállítandó, úgynevezett Információtechnikai Ellenőrzési Kompetenciaközpontban (Kompetenzzentrum für Informationstechnische Überwachung – CC ITÜ) kívántak legkésőbb 2014-ig létrehozni. Mindeközben azonban annak elkészültéig a korábban már említett és kompromittálódott DigiTask szoftvere helyett egy kereskedelmi forgalomban kapható eszközt, az – egyébként szintén német – Eleman/Gamma Group termékét, az úgynevezett *FinFisher/FinSpy IT intrusion software kit-et* használják (Meister, 2013; Bundesministerium des Finanzen, 2012).

A kémprogramok használata nemcsak Németországra jellemző, hanem – mint bizonyos körülmények között rendkívül hatékony vagy sokszor egyetlen alkalmazható eszközt – más országok titkos információgyűjtésre feljogosított szervei is használják vagy legalábbis használni tervezik. Ilyen témájú hírek érkeztek Svájc (The H Security, 2006), Franciaország (Le Monde, 2008), Ausztria (Sg.hu, 2007), Hollandia (Berta, 2013b), természetesen az USA (McCullagh, 2007; politechbot.com, s.d.) és az Egyesült Királyság (Gardham, 2009) vonatkozásában is.

Az online házkutatásra alkalmas eszközök, azaz kémprogramok természetesen jóval több információt tudnak biztosítani a célszemélyek számítógépéről (például tárolt fájlok), a számítógép technikai eszközein keresztül a célszemély tevékenységéről (például webkameraképek), mint amennyit pusztán az elektronikus úton folytatott kommunikációt biztosító alkalmazásszolgáltató – a törvényi feltételek megléte és maximális segítőkész hozzáállás mellett – képes. Az ilyen jellegű kémprogramokat azonban időről időre felderítik és alaposan analizálják az erre szakosodott biztonsági szakemberek vagy hackerek, majd – a törvényes ellenőrzést végző szervezeteknek nem kis anyagi és erkölcsi veszteséget okozva – eredményeiket sokszor publikálják is az interneten. Erre a sorsra jutott az olasz Hacking Team nevű cég szintén kifejezetten rendvédelmi szerveknek árusított eszköze (Golovanov, 2013) és a fent említett német Eleman/Gamma Group terméke is (Marquis-Boire et al., 2013).

Érdekes, hogy míg a korábban leírtak szerint a törvényhozók is azon gondolkodnak, vitatkoznak, hogy használhatják-e az arra feljogosított szervek egyáltalán ez a technológiát törvényes ellenőrzésre, és ha igen, milyen keretek között, addig egészen meglepő elképzelések is napvilágot látnak.

Ilyen az is, hogy az Egyesült Államokban működő *Commission on the Theft of American Intellectual Property* nevű szórakoztatóipari szervezet is hasonló programokat telepítene a zenei albumok, a filmek és a PC-s játékok adathordozóira, hogy az elkövetett jogsértéseket felderítse (The IP Commission, 2013).

Az Egyesült Királyság (UK) és a mély csomagelemzés

Egy másik módszer a törvényes ellenőrzést végzők kezében az úgynevezett mély csomagelemzés[43] módszere. Ennek lényege, hogy adott helyen átfolyó adatforgalom minden csomagjának tartalmát vizsgálat alá veszik. Ezt a technológiát használják fel például a behatolásérzékelő és védelmi rendszerek[44] (Dubrawsky, 2010; Wawro, 2012a), de internetszolgáltatók is előszeretettel alkalmazzák bizonyos – általuk károsnak vélt vagy tartott – tartalmak, forgalmak (például VoIP[45] peer-to-peer) blokkolására (BEREC, 2012). Ugyanakkor ez a technológia a törvényes ellenőrzést végző szolgálatok számára is lehetőséget teremt, hogy információhoz jussanak (Wawro, 2012a; Messmer, 2013). Ez a hozzáférés azonban meglehetősen korlátozott, hiszen bár a nyíltan küldött adatok könnyen ellenőrizhetők, feldolgozhatók, a titkosított forgalmak esetében a titkosítást fel kell törni, ami időben hosszadalmas, nagy számítástechnikai eszközparkot igénybe vevő folyamat. Ráadásul a felhasználó még a szolgáltató által nem titkosított forgalmaknál is képes jelentősen megnehezíteni az ellenőrzést egy megfelelő – és sokszor ingyenesen rendelkezésre álló – titkosító szoftvereszköz használatával (például HTTPS Everywhere) (Wawro, 2012a).

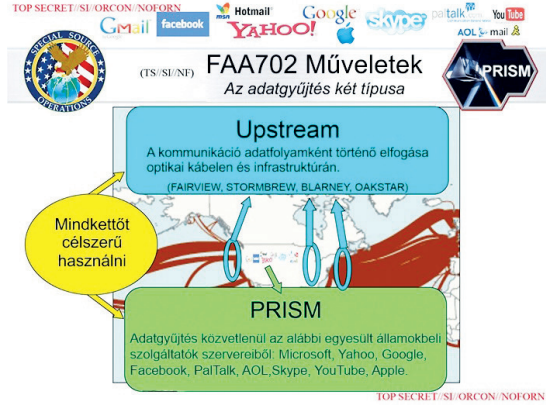
E korlát ellenére az angol GCHQ ezt a módszert használja *Tempora* nevű, a *Prismhez* hasonlóan nagyszabású, ám technikailag más alapokon nyugvó ellenőrző programjához. Itt – a kiszivárgott adatok szerint – 200 darab, egyenként 10 Gb/s adatátviteli sebességű optikai kábelen (ezek közül egy időben legalább 46-on) átfolyó összes információt kicsatolják és feldolgozzák a 2007 elején elindított *Mastering the Internet* projekt keretében. A programban öt ország (USA, UK, Kanada, Új-Zéland és Ausztrália) titkosszolgálati szervei dolgoznak együtt, és osztják meg egymás között az információkat,

43 DPI – Deep Packet Inspection.

44 IDS/IPS – Intrusion Detection System/Intrusion Prevention Systems.

45 VoIP – Voice over IP – internetprotokoll-alapú hangátvitel.

a kinyert tartalmat, valamint a kísérő, úgynevezett metaadatokat egyaránt (MacAskill et al., 2013a; MacAskill et al., 2013b). Az NSA hasonló, *Upstream* fedőnevű tevékenységét a 12. ábra szemlélteti, amelyből jól látszik, hogy a Prism csak egy része az USA lehallgatórendszerének.



12. ábra

Az Upstream és a Prism program viszonya, felhasználhatósága

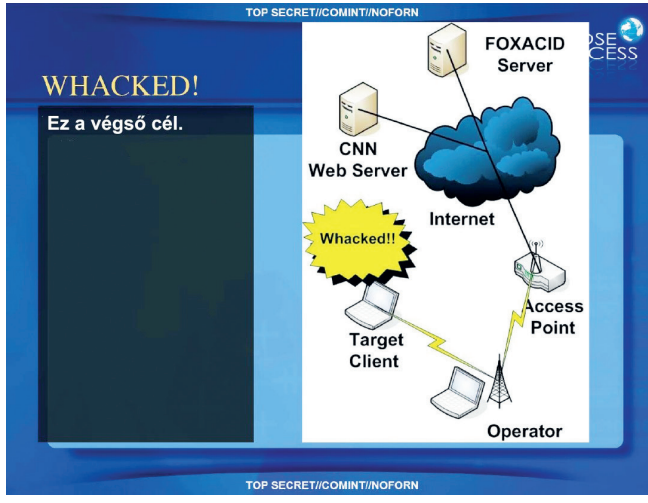
Forrás: a szerző szerkesztése a The Washington Post, 2013 alapján

Németország és a felhőalapú rendszerek titkosításainak törése

Németországban az online házkutatás (vagy inkább a kémprogramok) használata mellett felmerült a felhőalapú rendszerek másfajta ellenőrzésének kialakítása is. Erre azért van szükség, mert az említett módszernek – mint minden másiknak – megvannak a korlátai. Azokhoz az információkhoz, amelyekhez nem lehet a kémprogramok segítségével hozzáférni, egy másik módszer alkalmazásával lehet megszerezni. Ennek érdekében a BKA és az Alkotmányvédelmi Hivatal (Bundesamt für Verfassungsschutz – BfV) által működtetett Távközlési Stratégiai és Kutatóközpont (Strategie- und Forschungszentrum Telekommunikation –SFZ TK) nevű intézet azt a feladatot kapta az illetékes szervektől, hogy vizsgálja meg a felhőalapú rendszereknél használt titkosításokat, valamint azt, hogy megfejtésükön keresztül hogyan lehet hozzáférni a felhasználói adatokhoz, fájlokhoz (Berta, 2013c).

Az USA és a közbeékelődéses ellenőrzés (MitM)46

Érdekes, hogy amíg a többi módszer törvényes ellenőrzésre történő felhasználásáról sok konkrét információ szivárgott ki, addig a MitM-ről ez nem mondható el. Ugyanakkor a Snowden által kiszivárogtatott anyagokban található információ arra utal, hogy az Egyesült Államok szolgálatai használták ezt a technológiát is (Biddle, 2016). A közbeékelődéses ellenőrzéskor az ellenőrzést végző a célszemély infokommunikációs eszköze és az általa elért internetszolgáltató közötti kommunikációs csatornába áll be, megszakítva és a saját ellenőrző eszközén átfolyatva a célszemély készülékének teljes forgalmát, így biztosítva annak lehallgatását. Általában erre az átviteli csatorna rádiós részét használják. Erre mutat példát a 13. ábra. Az NSA-nál *BADDECISION* névre keresztelt program keretében használt közbeékelődéses ellenőrzéskor a kommunikáció lehallgatása mellett azt is megoldották, hogy a legális forgalomba illesztve kémprogramot juttassanak a célszemély infokommunikációs eszközére (Biddle, 2016).



13. ábra

Az NSA BADDECISION programja a közbeékelődéses ellenőrzésre épül

Forrás: Biddle, 2016

46 Angolul: Man in the Middle – MitM.

Törvényi szabályozások

Mint ahogy a Skype példáján keresztül is látszik, az ellenőrzés egyik leghatékonyabb formája a szolgáltatóval való együttműködés, amelyet törvényi előírásokkal garantálni lehet. Ilyen törvények kialakításának irányba több ország is tett lépéseket. Németországban a törvényes ellenőrzés megvalósíthatósága és hatékony alkalmazhatósága érdekében a telekommunikáció fogalmát kívánják kiszélesíteni minden online adatcserére, beleértve az ezekhez tartozó felhasználói adatokat is, és ezekre a hagyományos hírközléssel analóg rendelkezéseket alkotni az erről szóló jogszabályban (Berta, 2013d). Hasonló jogszabályváltozásokat akar az USA is bevezetni, amelyekkel kötelezheti az olyan szolgáltatókat, mint a Google vagy a Facebook, hogy tegyék lehetővé a rajtuk keresztül folytatott online kommunikáció törvényes ellenőrzését (Nakashima, 2013), ráadásul a törvényi szabályozás azt is garantálná, hogy minden szolgáltató bekényszeríthető legyen a rendszerbe. Ugyanakkor az USA-ban a már létező jogszabályok[47] is kötelezettségeket rónak a magáncégekre a törvényes ellenőrzés tekintetében (Poitras–Gellman, 2013).

A törvényes ellenőrzés technikai lehetőségei

A fenti nemzetközi példák bár széles, de nem teljes körű áttekintést adtak. Ennek egyrészt az az oka, hogy csak publikus információkra lehet támaszkodni, azok pedig – a problémakör jellegére tekintettel – meglehetősen korlátozottak, ráadásul szinte sohasem igazoltak, így nem lehetnek teljes körűek, másrészt pedig az, hogy a törvényes ellenőrzésre felhatalmazott szervek részére rendelkezésre álló módszerek ismertetéséhez, elemzéséhez egyébként sincs szükség teljes körű áttekintésre.

A nemzetközi tapasztalatok vizsgálata elsősorban a technikai lehetőségek áttekintésére és bizonyos problémák felvetésére, valamint arra szolgált, hogy megteremtse az alapot az ellenőrzéshez felhasználható módszerek rendszerezésére, elemzésére. E tapasztalatok megismerését követően lehet ugyanis az internettechnológiára épülő szolgáltatások hatékony ellenőrzésének kialakítása felé tett következő lépésként elvégezni a törvényes ellenőrzésre jelenleg rendelkezésre álló technikai eszközök és módszerek

[47] Protect America Act (2007), Foreign Intelligence Surveillance Act – FISA, Amendments Act (2008).

leírását, összehasonlítását előnyeinek, hátrányainak meghatározásával együtt. E vizsgálatok elvégzése ugyanis szükséges és elengedhetetlen feltétele annak, hogy az arra felhatalmazott szolgálatok megtehessék a szükséges lépéseket az internettechnológiára épülő szolgáltatások ellenőrzésének hatékony kialakítása érdekében.

A vizsgálat elvégzéséhez először is érdemes számba venni a törvényes ellenőrzéshez rendelkezésre álló technikai lehetőségeket, majd felállítani az elemzésükhöz szükséges szempontrendszert. Az így kialakított szempontrendszer alapján lehet elvégezni a felsorolt technikai megoldások elemzését, csoportosítva azok előnyeit, hátrányait. A kapott eredmények már alkalmasak lehetnek arra, hogy újabb, immár jóval teljesebb következtetéseket vonjunk le. Így amellett, hogy egyfajta útmutatóként szolgálhat ahhoz, hogy egy adott szervezet kiválassza, melyik módszert és mikor érdemes alkalmaznia, meghatározhatók belőle a további, az internettechnológiára épülő szolgáltatások törvényes ellenőrzésének hatékony kialakítása érdekében végrehajtandó feladatok is.

Mint ahogy a fejezet előző része rámutatott, az arra felhatalmazott nemzetbiztonsági és rendvédelmi szerveknek jelenleg több technikai megoldás is a rendelkezésükre áll ahhoz, hogy az internettechnológiára épülő szolgáltatásokat törvényes ellenőrzés alá vonják. Az összehasonlító elemzés elvégzése előtt azonban érdemes összefoglalóan csoportosítani ezeket a rendelkezésre álló módszereket, megoldásokat, és összefoglalni főbb jellemzőiket, tulajdonságaikat.

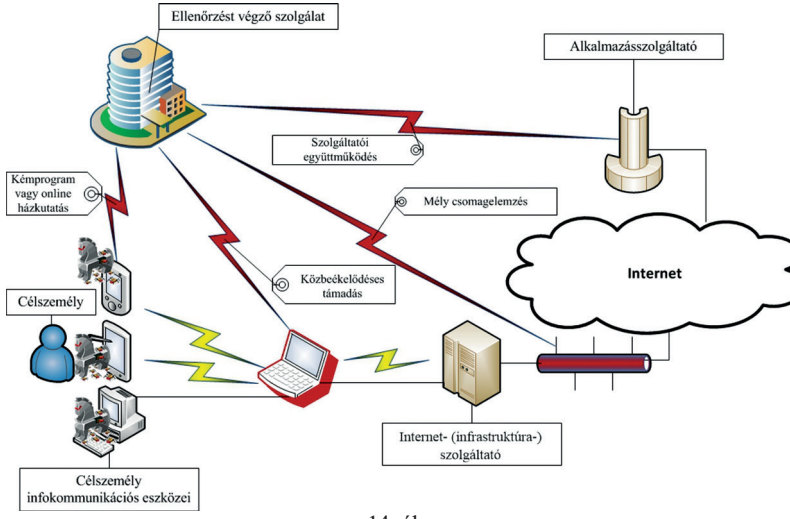
A fejezetnek nem célja, hogy az egyes módszereket minden részletet felölelően ismertesse, azokat csupán általánosítva, csak az összehasonlítási szempontrendszer felállításához és a végkövetkeztetések levonásához szükséges mértékben tárgyalja.

Az internettechnológiára épülő szolgáltatások törvényes ellenőrzésére alapvetően az alábbi négy módszert használhatják az arra felhatalmazott szolgálatok:

a) aktív ellenőrző eszköz,
b) közbeékelődéses ellenőrzés (MitM),
c) mély csomagvizsgálat (DPI),
d) együttműködés a szolgáltatóval.

A módszerek elnevezései önkényesek. Valódi, mindenki által elfogadott magyar megfelelőik vagy nem alakultak ki, vagy az ezekről szóló szakirodalom is többféle megnevezéssel használja őket (Berta, 2006; Dajkó, 2011).

A fenti módszerekre rendkívül jellemző az alkalmazásukkor használt adatszerző, elfogó eszközök – ebbe bele kell érteni a hardver- és szoftverelemeket egyaránt – távolsága a célszemélytől. Ezt jól szemlélteti a 14. ábra.



14. ábra

Az adatszerző, ellenőrző eszközök távolsága a célszemélytől

Forrás: a szerző szerkesztése

Aktív ellenőrző eszköz

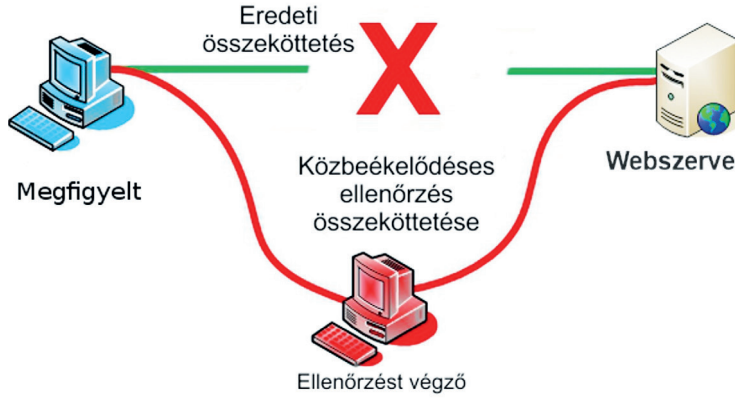
Az aktív ellenőrző eszközök – vagy közismertebb, a fejezet első részében említett nevükön kémprogramok, illetve online házkutatási eszközök – esetében a célszemély infokommunikációs eszközére, eszközeire (például számítógép, telefon, táblagép stb.) egy speciális, *kártékony* szoftvert telepít az ellenőrzést végző szolgálat. Ez sok hasonlóságot mutat a valódi kártékony szoftverekkel, de ebben az esetben ez törvényes célokat szolgál. Talán azt az analógiát lehetne erre alkalmazni, mint amikor egy lőfegyverről beszélünk, amely más értelmet nyer egy bűnöző és mást egy rendőr kezében.

Az aktív ellenőrző eszköz bejuttatása a célszemély eszközére többféle módszerrel is lehetséges, hasonlóan a kiberbűnözők által használt módozatokhoz (például elektronikus levél csatolmányaként, fertőzött weboldal segítségével, 0. napi sebezhetőség kihasználásával stb.). A működés során

ezek képesek az online kommunikáció elfogására, de billentyűzetleütések rögzítésére, a háttértárban található adatok megszerzésére vagy akár – ha van – a webkamerával képek készítésére is. Az információkat azután összegyűjtve küldik el az aktív ellenőrző eszköz tulajdonosának.[48]

Közbeékelődéses ellenőrzés (MitM)

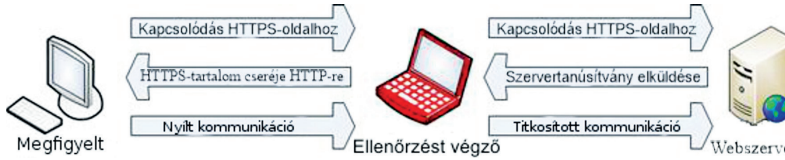
Leegyszerűsítve a dolgot, a közbeékelődéses ellenőrzés esetében az ellenőrzést végző szolgálat úgy hallgatja le a két fél között zajló kommunikációt, hogy a kommunikációs csatornát megszakítja, legyen az vezetékes vagy vezeték nélküli, majd abba, a két kommunikáló fél közé „beállva" mindkettőjük számára a másik félnek adja ki magát. A kapcsolat ezáltal mindkét fél számára zavartalannak tűnik, valójában azonban a teljes forgalom „átfolyik" az ellenőrzést végző eszközén, amellyel az itt zajló kommunikációt lehallgathatja, ahhoz teljes mértékben hozzáfér. Ezt szemlélteti a 15. ábra.



15. ábra
Közbeékelődéses ellenőrzés
Forrás: a szerző szerkesztése az OWASP, 2015 alapján

[48] Lásd bővebben CCC (2011); Golovanov (2013); Marquis-Boire et al. (2013); Rouse (2006); SpywareGuide (2003).

A sikeres közbeékelődéses ellenőrzéshez több feltételnek is teljesülnie kell. Az ellenőrzést végzőnek hozzá kell férnie a kommunikációs csatornához, képesnek kell lennie annak megszakítására (legyen az vezetékes vagy vezeték nélküli kapcsolat) oly módon, hogy megakadályozza az üzenetek eljutását a valódi címzetthez, majd le kell tudnia hallgatni a rajta küldött üzeneteket. Ez titkosítás nélküli kommunikáció esetében viszonylag egyszerű, de bizonyos esetekben, kis szerencsével és a valódi kommunikáló fél (felek) figyelmetlenségével akár titkosított kommunikáció esetén is megvalósítható. Ezt szemlélteti a 16. ábra.



16. ábra

Példa HTTPS-kommunikáció ellenőrzésére

Forrás: a szerző szerkesztése a Sanders, Chris (2010d) alapján

Sikeres közbeékelődéses ellenőrzés akkor hajtható végre viszonylag egyszerű eszközökkel és nagy valószínűséggel, ha a célszemélyhez (azaz az egyik kommunikáló félhez) az ellenőrzést végző a lehető legközelebb helyezkedik el.[49]

Mély csomagvizsgálat (DPI)

A mély csomagvizsgálat azt jelenti, hogy az adatcsomagoknak nemcsak a fejlécét, hanem azok adattartalmát is vizsgálat alá vetik, majd az adattartalom alapján kiszűrik az „érdekes" adatcsomagokat. A szűrés jellege a mély csomagvizsgálat felhasználásának céljától függ, a csomagvizsgálati módszerek azonban technikailag függetlenek tőle (Wawro, 2012b).

A mély csomagvizsgálatot leggyakrabban három esetben szokták alkalmazni. Az első eset a behatolást észlelő és behatolásvédelmi rendszerekben (IDS/IPS) történő felhasználás. Ezek a rendszerek a csomagok elemzésekor speciális bitmintákat (ismert támadókódokat) keresnek erre dedikált eszközök

[49] Lásd bővebben Sanders (2010a; 2010b; 2010c; 2010d); Fisher (2013); DuPaul (s.d.).

segítségével, majd a felismert, rosszindulatú kódot tartalmazó csomagokat kiszűrik (Dubrawsky, 2010). A második a hírközlési, internetszolgáltatók rendszereiben történő alkalmazás. Itt az internetprotokoll-alapú hangátviteli szolgáltatások (VoIP) és a peer-to-peer kapcsolaton alapuló fájlcsere forgalmának blokkolására használják a technológiát (BEREC, 2012). A harmadik a törvényes ellenőrzés, ahol a csomagok vizsgálata alapján dönthető el, hogy az az ellenőrzést végző számára érdekes-e (például adott célszemélyhez tartozik-e az e-mail), vagy sem. Itt a szűrés azonban nem a kiválasztott csomagok blokkolását szolgálja, hanem azoknak az ellenőrzést végző szolgálathoz (is) történő eljuttatását.[50]

Titkosítás nélküli kommunikáció esetén a lehallgatás viszonylag egyszerűen, sőt ebben az esetben, ellentétben a közbeékelődéses ellenőrzéssel, tömegesen is megvalósítható. Ugyanakkor titkosított kommunikáció esetén a tartalomhoz való hozzáféréshez feltétlenül szükséges a titkosítás feltörése, ez pedig hosszadalmas, nagy számítástechnikai eszközparkot igénybe vevő folyamat. Ráadásul a kommunikáló felek akár a nyílt forgalmaknál is egyszerű – és sokszor ingyenesen rendelkezésre álló – titkosító szoftvereszközök használatával (például HTTPS Everywhere) jelentősen megnehezíthetik vagy akár el is lehetetlenítik az ellenőrzést (Electronic Frontier Foundation, s.d.).

Együttműködés a szolgáltatóval

A szolgáltatóval való együttműködés a hagyományos hírközlési szolgáltatóknál már egy jól ismert és bevált modell szerint működik. Ekkor az ellenőrzést végző szerv eljuttatja a célszemélyhez kapcsolódó releváns adatokat (például felhasználónév) a szolgáltató rendszerébe, majd a szolgáltató automatikusan (emberi beavatkozás nélkül) vagy egyedi kiszolgálással (emberi beavatkozással) biztosítja a – rendszerében rendelkezésre álló – kért adatokat, információkat vagy akár a rajta átfolyó kommunikáció tartalmát is (The Washington Post, 2013).

[50] Lásd bővebben Wawro (2012a); Messmer (2013); The Washington Post (2013); MacAskill et al. (2013).

A törvényes ellenőrzési módszerek vizsgálati, összehasonlítási szempontjai

Az eddigiekből tehát látható, hogy az internettechnológiára épülő szolgáltatások törvényes ellenőrzésére több lehetőség, módszer is a felhatalmazott szolgálatok rendelkezésére áll. Ezek a módszerek azonban jelentősen – mondhatni, minden paraméterükben – eltérnek egymástól, akár technikai megvalósításukat, akár hatékonyságukat, akár jogi szabályozottságukat vesszük figyelembe. Annak érdekében, hogy az egyes módszereket össze tudjuk hasonlítani, először fel kell állítani egy, a vizsgálatukra megfelelő szempontrendszert. Ennek tartalmaznia kell minden olyan lényeges kritériumot, amely alapján a titkos információgyűjtésre és a titkos adatszerzésre felhatalmazott szerv dönteni tud arról, melyike(ke)t kívánja megvalósítani és munkájában felhasználni.

A módszer kiválasztásakor a következő szempontokat célszerű a törvényes ellenőrzésre felhatalmazott szervezeteknek megvizsgálnia, így a felállítandó vizsgálati szempontrendszernek tartalmaznia:

- *Az egy időben ellenőrizhető célszemélyek száma*
  Ebben a kérdéskörben nem elsősorban a tényleges számadatot kell megadni, hanem azt, hogy egyedi vagy tömeges ellenőrzést tesz-e lehetővé a módszer.
- *Az ellenőrző eszköz működési módja*
  Fontos kérdés, hogy az eszköz aktív vagy passzív módon működik-e. Ennek ugyanis meghatározó jelentősége van egyrészt az ellenőrzés célszemély általi felfedezhetőségében (dekonspiráció), másrészt a módszer alkalmazására, alkalmazhatóságára vonatkozó jogi háttér vizsgálatakor (meglévő törvényi szabályozás keretei).
- *A módszer jogi hátterének rendezettsége*
  Ennek keretében kell megvizsgálni, hogy az adott módszer egyáltalán alkalmazható-e az adott ország jogrendszere szerint, és ha igen, milyen keretek között. Az is elképzelhető, hogy bizonyos ellenőrzési metódusokra – újszerűségük miatt – sem kizáró, sem engedélyező szabályozó nincs.
- *Az ellenőrző eszköz célszemélyhez való közelsége*
  A dekonspiráció veszélyének felméréséhez meg kell vizsgálni, hogy telepítéskor, működés közben, leállításkor és eltávolításkor (törvényes ellenőrzés megszüntetésekor) milyen távolságban

(jobban érzékeltetné a problémát a távolság helyett a közelség megfogalmazás) kell lenni a célszemélytől, hogy a módszert alkalmazni lehessen.

- *A módszer alkalmazásának technikai problémái*
  Itt a telepítéskor, működés közben, leállításkor és eltávolításkor (törvényes ellenőrzés megszüntetésekor) felmerülő technikai problémákat kell számba venni.
- *A hozzáférhető adatok köre*
  A döntés szempontjából lényeges elem, hogy az adott módszerrel milyen információkhoz (csak az online átfolyó vagy a tárolt adatok is) jut hozzá a törvényes ellenőrzést végző szervezet.
- *Online kommunikációhoz való hozzáférés teljeskörűsége*
  Fontos tényező, hogy a célszemély online forgalmát teljes egészében vagy csak részlegesen biztosítja az adott módszer. E kérdés vizsgálatakor nem vesszük figyelembe, hogy a kommunikáció titkosított-e vagy sem, csak azt, hogy a célszemély minden kommunikációja összes bitjének elfogását biztosítja-e az adott módszer.
- *A módszer alkalmazásának problémái titkosított adatkommunikáció esetén*
  Az ellenőrzési módszer hatékonyságát nagymértékben befolyásolja, hogy képes-e, és ha igen, milyen esetekben és mértékben a titkosított kommunikációból az eredeti tartalmat (például üzeneteket, képeket, beszédet stb.) biztosítani a titkos információgyűjtést végző szerv számára.
- *Beruházási igény*
  Az sem elhanyagolható szempont, hogy az adott módszer alkalmazásához szükséges eszközrendszer mennyibe kerül.
- *Egyéb költségek*
  Olyan egyéb járulékos költségek is fellép(het)nek, amelyekkel komolyan számolni kell az alkalmazást megelőzően. Ilyenek lehetnek például az együttműködőknek fizetendő díjak, a betanítás vagy éppen speciális ismeretekkel rendelkező (például hacker) szakemberek (tovább)képzési vagy megvásárlási költségei.
- *Célszemélyek adataihoz harmadik fél hozzáférése*
  Lényeges kérdés az is, hogy a célszemély adataihoz a törvényes ellenőrzést végző szolgálat munkatársain kívül ki fér(het) még hozzá. Ez ugyanis nagymértékben növelheti a dekonspiráció veszélyét. (Itt nem vizsgáljuk az eszköz alkalmazása során,

a működés miatt fellépő dekonspirációt, azaz azt, amikor a célszemély vagy annak közvetlen környezete szerez tudomást az alkalmazásról. Ebben az esetben kizárólag harmadik fél hozzáférését [például szolgáltató szakemberei] vizsgáljuk.)

A fenti szempontok szerint megvizsgálva az egyes, korábban említett törvényes ellenőrzési módszereket, a titkos információgyűjtésre felhatalmazott szerv már nemcsak az adott módszer bevezetéséről, rendszeresítéséről képes dönteni, hanem arról is, hogy majd adott ügyben a körülményeknek megfelelően melyik ellenőrző metódus használata a legcélravezetőbb.

A törvényes ellenőrzés módszereinek vizsgálata

Vizsgáljuk meg tehát a korábban leírt négy módszert a fenti kritériumrendszer alapján.

a) Aktív ellenőrző eszköz

- *Az egy időben ellenőrizhető célszemélyek száma:* egyedi ellenőrzést tesz lehetővé.
- *Az ellenőrző eszköz működési módja:* aktív módszer, a dekonspiráció veszélye magas.
- *A módszer jogi hátterének rendezettsége:* a módszerre nincsenek mindenki által elfogadott jogszabályok, több ország most próbálja a felhasználás, alkalmazás pontos jogi kereteit kialakítani.
- *Az ellenőrző eszköz célszemélyhez való közelsége:* a vizsgált módszerek közül a legközelebb működik a célszemélyhez.
- *A módszer alkalmazásának technikai problémái:* a közelség okán a telepítés, újratelepítés nehézkes lehet, az online kapcsolat megszakadásakor az eszköz „eltűnik” az ellenőrzést végző szervek elől, kikerül a felügyeletük alól.
- *A hozzáférhető adatok köre:* nemcsak az online forgalomhoz, hanem az adott eszközön tárolt minden fájlhoz elérést biztosít, sőt további ellenőrzési lehetőségeket (például webkamerával képkészítés) is kínál.
- *Online kommunikációhoz való hozzáférés teljeskörűsége:* nem ad teljes körű hozzáférést, hiszen csak az azon az eszközön bonyolított kommunikációt képes elfogni, amelyikre feltelepítették.
- *A módszer alkalmazásának problémái titkosított adatkommunikáció esetén:* a kommunikációt a titkosítást megelőzően képes elfogni, így

a felhasznált titkosítástól függetlenül ellenőrizhetővé teszi a kommunikációt.

- *Beruházási igény:* közepes, az alkalmazott eszközök, a bejuttatáshoz esetleg használt, úgynevezett 0. napi sebezhetőségek költségesek.
- *Egyéb költségek:* magas, a módszer alkalmazásához speciális (hacker-) tudással rendelkező szakemberek szükségesek.
- *Célszemélyek adataihoz harmadik fél hozzáférése:* ennek lehetősége minimális.

b) Közbeékelődéses ellenőrzés (MitM)

- *Az egy időben ellenőrizhető célszemélyek száma:* egyedi ellenőrzést tesz lehetővé.
- *Az ellenőrző eszköz működési módja:* aktív módszer, a dekonspiráció veszélye magas.
- *A módszer jogi hátterének rendezettsége:* a módszerre nincsenek mindenki által elfogadott jogszabályok.
- *Az ellenőrző eszköz célszemélyhez való közelsége:* a módszer kizárólag a célszemély (infokommunikációs eszközének) közvetlen közelében működik.
- *A módszer alkalmazásának technikai problémái:* az alkalmazás teljes időtartamában kötelezően a célszemély (infokommunikációs eszközének) közelében kell tartózkodni. Ez pedig az egész alkalmazást nehézkessé, esetlegessé teszi, teheti.
- *A hozzáférhető adatok köre:* csak az online forgalomhoz biztosít elérést.
- *Online kommunikációhoz való hozzáférés teljeskörűsége:* nem ad teljes körű hozzáférést, hiszen csak az azon az eszközön bonyolított kommunikációt képes elfogni, amelyik forgalma „átfolyik" az ellenőrző (lásd a 16. ábrán: ellenőrzést végző) eszközön.
- *A módszer alkalmazásának problémái titkosított adatkommunikáció esetén:* kis szerencsével és a célszemély figyelmetlenségével párosulva bizonyos titkosított forgalmaknál is lehetővé teszi a közlemények megismerését.
- *Beruházási igény:* alacsony, az ellenőrzés gyakorlatilag kommersz eszközökkel megvalósítható.
- *Egyéb költségek:* magas, a módszer alkalmazásához speciális (hacker-) tudással rendelkező szakemberek szükségesek.
- *Célszemélyek adataihoz harmadik fél hozzáférése:* ennek lehetősége minimális.

c) Mély csomagvizsgálat (DPI)

- *Az egy időben ellenőrizhető célszemélyek száma:* tömeges ellenőrzést tesz lehetővé.
- *Az ellenőrző eszköz működési módja:* passzív módszer, a dekonspiráció veszélye alacsony.
- *A módszer jogi hátterének rendezettsége:* a hagyományos hírközlési szolgáltatókra vonatkozó jogszabályok szerint lehet eljárni.
- *Az ellenőrző eszköz célszemélyhez való közelsége:* a célszemélytől (infokommunikációs eszközeitől) távol működik.
- *A módszer alkalmazásának technikai problémái:* az óriási „átfolyó" adatmennyiség szűrése, feldolgozása nagy számítástechnikai hátteret és sok embert igényel, így gondot okozhat.
- *A hozzáférhető adatok köre:* csak az online forgalomhoz biztosít elérést.
- *Online kommunikációhoz való hozzáférés teljeskörűsége:* közel teljes körű hozzáférést adhat, hiszen az ellenőrző eszköz(ök) elhelyezésétől függően a célszemély akár több eszközén, akár több szolgáltató hálózatán keresztül lebonyolított kommunikációját képes elfogni.
- *A módszer alkalmazásának problémái titkosított adatkommunikáció esetén:* az elfogott titkosított forgalmak tartalmához kizárólag a titkosítás feltörését követően lehet hozzáférni.
- *Beruházási igény:* rendkívül magas, az összes vizsgált módszer esetében messze a legmagasabb.
- *Egyéb költségek:* közepes, a módszer alkalmazásához nem kellenek külön speciális tudással rendelkező szakemberek, de külső közreműködőket, azok költségeit (például infrastruktúra-szolgáltató beruházásai) a helyi jogszabályoknak megfelelően esetleg fizetni kell.
- *Célszemélyek adataihoz harmadik fél hozzáférése:* ennek lehetősége minimális.

d) Együttműködés a szolgáltatóval

- *Az egy időben ellenőrizhető célszemélyek száma:* tömeges ellenőrzést tesz lehetővé.
- *Az ellenőrző eszköz működési módja:* passzív módszer, a dekonspiráció veszélye alacsony.

- *A módszer jogi hátterének rendezettsége:* a módszerre nincsenek mindenki által elfogadott jogszabályok, az alkalmazásszolgáltatók általában nem hajlandók együttműködni.
- *Az ellenőrző eszköz célszemélyhez való közelsége:* a célszemélytől (infokommunikációs eszközeitől) távol működik.
- *A módszer alkalmazásának technikai problémái:* az alkalmazásszolgáltató tényleges együttműködése esetén problémamentes.
- *A hozzáférhető adatok köre:* csak az online forgalomhoz és a szolgáltatónál tárolt adatokhoz, információkhoz biztosít elérést.
- *Online kommunikációhoz való hozzáférés teljeskörűsége:* az alkalmazásszolgáltatón keresztül lebonyolított kommunikációhoz teljes körű hozzáférést ad.
- *A módszer alkalmazásának problémái titkosított adatkommunikáció esetén:* a szolgáltató által használt titkosítás ekkor nem jelent problémát, gondot kizárólag a felhasználó által esetleg használt egyedi titkosítás okozhat.
- *Beruházási igény:* alacsony, az összes többi módszernél is jelentkező feldolgozó terminálok kivételével alig igényel pluszeszközt.
- *Egyéb költségek:* közepes, a módszer alkalmazásához nem kellenek külön speciális tudással rendelkező szakemberek, de az alkalmazásszolgáltató beruházásait vagy adott esetben az adatszolgáltatását a helyi jogszabályoknak megfelelően esetleg fizetni kell.
- *Célszemélyek adataihoz harmadik fél hozzáférése:* magas, ma még sokszor emberi beavatkozással működik az adatszolgáltatás és a kommunikáció ellenőrizhetővé tétele is, ráadásul a kérésekben foglalt érzékeny vagy akár minősített adatokhoz (például célszemély adatai) – általában – külföldi szolgáltató hazai biztonsági ellenőrzésen át nem esett emberei férhetnek hozzá a kérőszerv szemszögéből kontrollálatlanul.

Annak érdekében, hogy az arra felhatalmazott szervek számára az internettechnológiára épülő szolgáltatások törvényes ellenőrzésére jelenleg rendelkezésre álló módszereket össze tudjuk hasonlítani, célszerű előnyeiket, hátrányaikat is összefoglalni. Ezt tartalmazza a következő táblázat.

13. táblázat

Az internettechnológiára épülő szolgáltatások törvényes ellenőrzésére jelenleg rendelkezésre álló módszerek előnyei, hátrányai

Módszer	előnyök	hátrányok
Aktív ellenőrző eszköz	• nemcsak az éppen folyó forgalmat, hanem a gépen tárolt minden adatot el lehet érni • titkosítás előtti elfogás – azaz a felhasznált titkosítástól függetlenül ellenőrizhető a forgalom	• egyedi ellenőrzés (egy trójai, egy eszköz) • a telepítés problémákba ütközhet • a célszemély minden eszközére kell telepíteni a teljes körű ellenőrzéshez • aktív, ezért működése adott esetben felfedezhető • működése, működő képessége nagymértékben függ a céleszköz beállításaitól, telepített szoftvereitől (például vírusirtó, tűzfal) • működése azonnali utasítással nem megszakítható • alapos előkészületek ellenére a képességet egy egyszerű (például: víruselleőrző) frissítés ellehetetlenítheti • jogszabályi háttere nem egyértelmű
Közbeékelődéses ellenőrzés (MitM)	• bizonyos titkosított forgalmaknál is lehetővé teszi a közlemények megismerését (általában SSL, https esetén)	• egyedi ellenőrzés (egy internetforgalomra) • más titkosított forgalmak problémát okozhatnak • viszonylag közel kell menni • több eszköz és netelérés esetén problémás (például vezetékes és mobil net) • adott esetben a tevékenység felfedezhető • csak az éppen folyó forgalmat lehet vele megismerni • titkosított forgalom esetében az alkalmazónak szükséges hiteles tanúsítvánnyal rendelkeznie • jogszabályi háttere nem egyértelmű

Módszer	előnyök	hátrányok
Mély csomagvizsgálat (DPI)	• tömeges – egyszerre több célszemély forgalma is ellenőrizhető • teljesen passzív • tartalomalapú szűrést tesz lehetővé • jogszabályi háttere egyértelmű	• nagy beruházási igény • az egyre növekvő sávszélesség miatt egyre gyorsabb, nagyobb sávszélességű elfogókat kell használni • a titkosítás problémákat okozhat • az adott „csatornán” átfolyó forgalmat elemzi, ha nem ott megy a célszemély forgalma, nem fogja el – nem teljes körű • csak az éppen folyó forgalmat lehet vele megismerni
Együttműködés a szolgáltatóval	• tömeges – egyszerre több célszemély is ellenőrizhető • a teljes információkör elérhető a használt eszközöktől, internetelérestől függetlenül • nemcsak az éppen folyó forgalmat, hanem a szolgáltatónál tárolt minden adatot (például piszkozatok) el lehet érni • a szolgáltató által alkalmazott titkosítás nem probléma	• a szolgáltatók nem mindig partnerek, csak jogszabályi alapon működik (hatékonyan) • külföldi szolgáltatók felhasználóinak ellenőrzése esetén ráadásul nemzetközi jogszabályok szükségesek • a célszemély adatait a szolgáltató is megismeri – titoktartási, konspirációs gondot okozhat • több szolgáltatót használó célszemélyeknél mindegyikkel együtt kell működni

Forrás: a szerző szerkesztése

Az internettechnológiára épülő szolgáltatások, kiemelten a PC/SaaS felhőalapú rendszerek törvényes ellenőrzésére technikailag jelenleg is többféle módszer áll az érintett szolgálatok rendelkezésre. Amennyiben tisztán technikai oldalról közelítjük meg az ellenőrzés lehetőségeit és hatékonyságát, akkor egyértelműen kijelenthető, hogy bár a fent leírt módszerek egyike sem nyújt teljes körű megoldást, az alkalmazásszolgáltatóval való együttműködés

kikerülhetetlen. Ez biztosítja ugyanis, hogy egyszerre több célszemély is ellenőrizhető úgy, hogy az adott szolgáltatáshoz kapcsolódó teljes információkör elérhető az adott szolgálat számára, függetlenül a célszemély(ek) által használt eszközöktől és interneteléréstől. Ez pedig az egyik leghatékonyabb és legköltségtakarékosabb ellenőrzési formává teszi.

Ugyanakkor éppen e módszer jogi szabályozottságában lelhető fel a legtöbb hiány, így ma gyakorlatilag a legtöbb ország esetében is kizárólag az alkalmazásszolgáltató jóindulatán múlik, együttműködik-e az ellenőrzést végző szervekkel, illetve teljesíti-e az egyébként teljesen legális, hatályos és például a hírközlési szolgáltatók számára (is) kötelező érvényű bírói végzésben foglaltakat.

A törvényes ellenőrzés hatékonyságának növelése érdekében, például az új Európai Uniós irányelvek vagy jogi szabályozás kialakításához mindenképpen definiálni kell az alkalmazásszolgáltató fogalmát. Ezt, a korábban már felvázolt infrastruktúra-, alkalmazás- és tartalomszolgáltatói modell szerint érdemes megtenni, a másik két szolgáltató meghatározásával egyetemben. Ez ugyanis egyrészt lehetőséget biztosít a többi elemzett vagy bármilyen más, akár teljesen új ellenőrzési módszer törvényi szabályozásának kialakításában, másrészt teljeskörűen lefedi az összes jelenlegi szereplőt, harmadrészt pedig nemcsak a kommunikációt biztosító, hanem bármely, a nemzetbiztonsági szolgálatok és a rendvédelmi szervek számára érdemi információt nyújtó szolgáltatás ellenőrzését lehetővé teszi. Ez utóbbiak lehetnek például a pénzügyi szolgáltatások (Gazdag–Kovács, 2014), útvonaltervek stb.

Infrastruktúra-, alkalmazás- és tartalomszolgáltatók fogalmi meghatározása a törvényes ellenőrzés szemszögéből

A fejezet előző részei bemutatták az internet és az azt felhasználó alkalmazások fejlődésével ugrásszerűen változó, bővülő kommunikációs formák, lehetőségek hatásait, elemezték az elektronikus úton folytatott kommunikáció és a hírközlés viszonyát, e kettő változásait, valamint az internettechnológiára épülő szolgáltatások, azok közül is a PC/SaaS felhőalapú rendszerek törvényes ellenőrzése kapcsán felmerült problémákat. Megállapítható, hogy a klasszikus hírközlési szolgáltatói modell egyre inkább eltűnik, helyét új szolgáltatói struktúra veszi át, és ez a tendencia a jövőben várhatóan tovább erősödik. Az új modell legjelentősebb hatása a hírközlésre az, hogy a hírközlési

hálózatot – vagy célszerűbb megfogalmazással internetelérést – és a tényleges kommunikációt más szolgáltató biztosítja. Ennek kapcsán felállítható egy új, specializált infrastruktúra-, alkalmazás- és tartalomszolgáltatói modell, amely teljeskörűen leírja a jelenlegi struktúrát és az érintett szereplőket.

Az internettechnológiára épülő szolgáltatások, azok közül is a PC/SaaS felhőalapú rendszerek természetesen nemcsak kommunikációt, hanem sok egyéb online szolgáltatást is biztosítanak a felhasználók számára. Igénybe vehetünk banki szolgáltatásokat (OTP, s.d.), fizethetünk webboltokban (PayPal, s.d.), játszhatunk (Blizzard, s.d.), szerkeszthetjük dokumentumainkat (Microsoft (s.d.d), képeinket (Adobe, s.d.), tárolhatjuk, megoszthatjuk adatainkat (Dropbox, s.d.), készíthetünk útvonaltervet (Google, s.d.) – és még nagyon hosszan lehetne folytatni a felsorolást. Ugyanakkor a korábban említett hármas tagozódásba (infrastruktúra-, alkalmazás- és tartalomszolgáltatók) nemcsak az elektronikus úton folytatott kommunikációt lehetővé tevő rendszerek, hanem az itt említettek is beleérthetők, beleértendők. Akárcsak a többi internettechnológiára épülő szolgáltatás.

Fel kell azonban tenni a kérdést, hogy mit is takarnak az infrastruktúra-, alkalmazás- és tartalomszolgáltató fogalmak. Ezekre ugyanis számos megfogalmazás létezik, amelyek hol szélesebben értelmezve, hol szűken, egy adott feladatra, problémára koncentrálva írják le, mit is értenek a fent említett fogalmak alatt. Törvényes ellenőrzés szempontjából azonban két problémába is ütközünk. Az egyik az, hogy ezek a definíciók nem fedik le teljes mértékben a fenti rendszereket, szolgáltatásokat, a másik pedig az, hogy a hatályos nemzetközi jogszabályokban az említett szolgáltatókra nincsenek megfelelő definíciók, a magyar szabályozókban is csupán az alkalmazásszolgáltatóra találunk ebből a szempontból megfelelőt. Ez pedig megnehezíti a hatékony törvényes ellenőrzés végrehajtását.

Az elektronikus hírközlésről szóló törvény módosításának szükségessége

Az infrastruktúra-, alkalmazás- és tartalomszolgáltatók definícióinak kialakítása előtt célszerű értékelni, hogy a 2016-ban hatályos jogszabályok megfelelő keretet biztosítottak-e az említett szolgáltatók, szolgáltatások törvényes ellenőrzéséhez. A 2016-ban elfogadott, az alkalmazásszolgáltatót definiáló és azok törvényes ellenőrzését meghatározó jogszabályról, valamint annak hatásairól a fejezet végén lesz szó.

A hírközlés törvényes ellenőrzését az akkor hatályos törvényeink két, párhuzamosan alkalmazott szabályrendszer szerint tették lehetővé[51]. Ezek közül az egyik a titkos információgyűjtést és titkos adatszerzést szabályozó ágazati normák, mint például *a nemzetbiztonsági szolgálatokról szóló 1995. évi CXXV.* (Nbtv.), *a büntetőeljárásról szóló 1998. évi XIX.* (Be.), a *Rendőrségről szóló 1994. évi XXXIV.* (Rtv.), *az ügyészségről szóló 2011. évi CLXIII.* (Ütv.), valamint a *Nemzeti Adó- és Vámhivatalról szóló 2010. évi CXXII.* (NAVtv.) törvény. A másik *az elektronikus hírközlésről szóló 2003. évi C. törvény* [138], valamint *az elektronikus hírközlési feladatokat ellátó szervezetek és a titkos információgyűjtésre, illetve titkos adatszerzésre felhatalmazott szervezetek együttműködésének rendjéről szóló 180/2004. (V. 26.) Korm. rendelet.*

Azonban nemcsak a szabályozást, hanem az Eht.-t is kettőségek jellemzik. Egyfelől a törvényt 2003-ban fogadták el, az akkori technikai, technológiai viszonyoknak megfelelően, így kizárólag az infrastruktúrával rendelkező és az ehhez kapcsolódó, erre ráépülő szolgáltatást egyszerre nyújtó hírközlési- és internetszolgáltatókról szól. Ez utóbbiak akkor még jelentős mértékben nyújtottak olyan szolgáltatásokat, amelyeket mára szinte teljesen átvettek a tőlük függetlenül működő alkalmazásszolgáltatók. Ilyen például az elektronikus levelezés. Ráadásul – mint ahogy a fejezet első része és a *Felhő alapú rendszerek törvényes ellenőrzési problémái* című cikk (Kovács, 2013c) is taglalja – az elektronikus úton folytatott kommunikáció is gyökeresen megváltozott. A törvény 2003-as megalkotásakor számos, napjainkban már széleskörűen használt technológia még nem létezett. Erre két jellemző példa a korábban már hivatkozott, az IP-alapú kommunikációban ma meghatározó Skype és Facebook. A rendkívül népszerű Skype első béta verziója 2003 augusztusában jelent meg, a Facebook pedig 2004. február 4-én debütált, így ezek a törvény megalkotásakor még nem voltak elérhetők. Az pedig kijelenthető, hogy a kommunikációs technológiák ilyen változását az Eht. nem követte.

Másfelől a törvény felépítését is kettősség jellemzi. Az Eht. megalkotásakor teljesen logikus lépés volt az érintettek hírközlési szolgáltatáshoz

---

[51] Ezek a szabályozók jelenleg is hatályban vannak. A parlament 2017-ben elfogadta A titkos információgyűjtés szabályainak az új büntetőeljárási törvénnyel összefüggő, továbbá a bírósági végrehajtás során *a sértettnek megítélt polgári jogi követelések kielégítési sorrendjére vonatkozó rendelkezések módosításáról szóló 2017. évi XCIII.*, és *a büntetőeljárásról szóló 2017. évi XC. törvényt*, ezek azonban a téma szempontjából lényeges elemeket nem módosították.

kapcsolódó feladatai és kötelezettségei mellett a törvényes ellenőrzéshez kapcsolódó kötelezettségek megjelenítése is. Mára ez azonban már minden szereplő számára akadályozó tényezővé vált. A törvényes ellenőrzési kitételek miatt a törvény vonatkozó része kétharmados, így az egyébként logikus és szükséges, nem a törvényes ellenőrzéshez kapcsolódó változtatásokat is sokkal nehezebben lehet elfogadtatni.

Éppen ezért célszerű lenne az Eht.-t kettébontani. Az egyik, továbbra is kétharmados törvény szabályozná a törvényes ellenőrzéshez kapcsolódó kötelezettségeket, de már az új, fent említett infrastruktúra-, alkalmazás- és tartalomszolgáltató struktúrának megfelelően. Ez jól kiegészíthetné a korábban említett ágazati törvényeket. A másik, immár normál feles törvény pedig, szintén az új struktúrának megfelelően, az érintett szereplők minden más feladatát, kötelezettségét írná elő.

A változtatásnak több előnye is lenne. Egyrészt a jelenlegi viszonyokhoz és a közeljövőhöz alkalmazkodó törvényi szabályozást lehetne létrehozni, másrészt az egyes törvények kapcsán megjelenő kevesebb szereplő miatt könnyebb az esetleges későbbi változtatásokat átvezetni, harmadrészt azokat a szolgáltatókat is be lehetne vonni minden tekintetben a törvényi szabályozás hatálya alá, akik eddig kívül estek azon. Erre más területen már történnek kísérletek, például az adózás kapcsán elkészült egy hasonló megfontolásokon alapuló törvény (2014. évi XXXIII. tv.).

A javasolt két új törvénnyel kapcsolatban viszont kiemelendő, hogy célszerű mindkettőben ugyanazokat a meghatározásokat használni, valamint a meglévő, bizonyos területeket most is lefedő hírközlési szolgáltató mellett megjeleníteni – illetve amelyik még nincs, bevezetni – az infrastruktúra-, alkalmazás- és tartalomszolgáltatók fogalmát is.

Tartalomszolgáltatók fogalmi meghatározása

A törvényes ellenőrzés szempontjából is teljes körű definíciók kialakítását érdemes a tartalomszolgáltatókkal kezdeni. Elsősorban azért, mert talán erre vannak a legátfogóbb, a törvényes ellenőrzés szempontjából is elfogadható meghatározások. Másodsorban azért, mert a hagyományos tartalomszolgáltatók (például újság, tv stb.) kapcsán a törvényes ellenőrzés metódusai kialakultak, és a demokratikus országokban hasonló elvek alapján elfogadottá váltak. Harmadsorban pedig azért, mert a törvényes ellenőrzés kapcsán ez kapja a legkisebb figyelmet.

Magyar meghatározások

A tartalomszolgáltató meghatározására a Magyarországi Tartalomszolgáltatók Egyesületének (MTE) a tartalomszolgáltatásra vonatkozó működési, etikai és eljárási szabályzatának 3. pontjában az alábbiakat találjuk:

> *„Internetes tartalomszolgáltatónak tekintünk minden olyan jogi vagy természetes személyt, illetve ezek bármilyen csoportját, amely/aki az internetfelhasználók összessége, vagy egy csoportja által elérhető módon, bármilyen (textuális, numerikus, képi, hangos, multimediális) információt tesz közzé időben korlátozott vagy korlátlan módon úgy, hogy a tartalomhoz hozzáférők által e jogi vagy természetes személy egyértelműen, a tartalomhoz való hozzáférés során azonosítható. Az internetes tartalomszolgáltatás fogalmába beleértjük a különböző hálózatokon elérhető WWW, mobil, széles sávú e-mailes információkat, mely technológiák ugyanakkor nem kizárólagosan alkotják a fogalom tartalmát. Nem tekintjük Tartalomszolgáltatónak azt a szolgáltatót, aki pusztán technológiai lehetőséget biztosít egy vagy több, egyszerűen azonosítható jogi vagy természetes személynek, információk közzétételére"* (MTE, 2009).

Ez a meghatározás a törvényes ellenőrzés szempontjából is iránymutatóan foglalja össze az internetes tartalomszolgáltató fogalmát, ugyanakkor érdemes megvizsgálni, hogy az általános – tehát nem csupán internetes – médiaszolgáltatások és sajtótermékek fogalmi meghatározásai alapján a fenti fogalomkört célszerű-e kiterjeszteni. A Nemzeti Média- és Hírközlési Hatóság által kiadott *A médiaszolgáltatás és a sajtótermék fogalma az új magyar médiaszabályozásban* című dokumentum (Koltay et al., s.d.), *a sajtószabadságról és a médiatartalmak alapvető szabályairól szóló 2010. évi CIV. törvény* (Smtv.), valamint *a médiaszolgáltatásokról és a tömegkommunikációról szóló 2010. évi CLXXXV. törvény* (Mttv.) alapján foglalja össze az említett fogalomrendszert.

A dokumentum az Smtv. és az Mttv. szerint megkülönbözteti a médiaszolgáltatást és a sajtóterméket. E kettőt a jogszabályok összefoglalóan médiatartalom-szolgáltatásnak nevezik, a két törvény hatálya pedig a Magyarországon letelepedett médiatartalom-szolgáltatókra terjed ki. A médiaszolgáltatásnak és a sajtótermékek kiadásának vannak közös jellemzőik. Mindkét esetben a szolgáltatók tájékoztatás, oktatás vagy szórakoztatás

céljából hoznak nyilvánosságra tartalmakat, amelyekért szerkesztői felelősséget viselnek, és ezeket elektronikus hírközlő hálózaton keresztül továbbítják. (A sajtótermék esetében a törvény e mellett a nyomtatott formára is kiterjed, de ez a téma szempontjából érdektelen.)

A dokumentum 2.1.3. részében pontosítja a fent említett tájékoztatás, oktatás és szórakoztatás fogalom tartalmát, amelyben kiemeli, hogy nem tekinthetők tartalomszolgáltatásnak a közösségi vagy fájlmegosztó oldalakon közzétett anyagok, mint ahogy a magáncélú vagy a szűk, határozott körben elérhető tartalmak sem.

Az említett dokumentumokban megjelenő definíciók a készítők saját feladatrendszerének megfelelően, ahhoz teljes mértékben illeszkedve fedik le a tartalomszolgáltatás fogalmát. A törvényes ellenőrzés szempontjából a fenti meghatározások ugyan szintén jó kiindulási alapot adnak, azonban még mindig nem teljes körűek. Van ugyanis néhány olyan sarkalatos pont, amelyet a pontos meghatározás érdekében még szükséges leszögezni.

Az első, hogy a hármas tagolás (infrastruktúra-, alkalmazás- és tartalomszolgáltató) tagjainak egyértelmű megkülönböztetése miatt fontos jellegzetesség, hogy a tartalomszolgáltató csak és kizárólag egyirányú kommunikációt tesz lehetővé. Az általa elkészített, szerkesztett tartalmat közlik, annak tartalmát a fogyasztó nem tudja befolyásolni.

A második, hogy tartalomszolgáltatónak kell tekinteni minden olyan szolgáltatót, amely szolgáltatása Magyarországon elérhető, igénybe vehető, és nem csak azokat, amelyek – a fenti törvények megfogalmazása szerint – hazánkban letelepedtek.

A harmadik, hogy – az internet jelenlegi lehetőségeit figyelembe véve – nem mindig lehet egyértelműen azonosítani a tartalomszolgáltatót mint jogi vagy természetes személyt, ettől azonban még tartalomszolgáltatásnak minősülhet a tevékenysége. Gondoljunk csak egy olyan blogra vagy internetes újságra, amely szöveges, képi és videóüzeneteket is tartalmaz, külföldi szerveren érhető el, a készítő(k) csupán álnevet használ(nak), de a közzétett tartalom bárki számára hozzáférhető.

Külföldi meghatározások

A magyar meghatározások után célszerű megvizsgálni néhány külföldi definíciót is annak reményében, hogy további hatékony segítséget nyújthatnak

a törvényes ellenőrzés ellátásához szükséges, törvénybe is illeszthető meghatározás kialakításában.

A Collins English Dictionary szerint a tartalomszolgáltató *„egy személy vagy cég, amely tartalmat szolgáltat egy honlap számára”,* és példaként az (azóta már megszűnt) MSN-t és a Freeserve-et nevezi meg (Collins, s.d.).

Hasonlóan rövid meghatározást közöl az Oxford Dictionaries is, amelynek US English verziója szerint a tartalomszolgáltató *„az a személy vagy szervezet, aki honlapokon történő felhasználáshoz információkat szolgáltat”* (Oxford Dictionaries, s.d.a). A British & World English verzióban ugyanezt a meghatározást közlik, de már leszűkítve szervezetre, a személy megjelölése nélkül (Oxford Dictionaries, s.d.b).

Az előzőeknél bővebben leírt, ezáltal szűkebben, pontosabban értelmezhető definíciókat is közreadtak. A Gartner meghatározása szerint a tartalomszolgáltató *„egy vállalkozás információalapú (értsd: tartalomalapú) termékekkel, amely tartalmazza az információelérési és -kezelési szolgáltatásokat is”* (Gartner, s.d.a).

Hasonló meghatározást ad közre a Dictionary.com is azzal a különbséggel, hogy abban személy vagy csoport, valamint honlapok vagy elektronikus média szerepel (Dictionary.com, s.d.a).

A BussinessDictionary.com már bonyolultabb megfogalmazást használ. Definíciójukban cégekről beszélnek, amelyek kiadványukat vagy honlapjukat teszik vonzóbbá vagy hasznosabbá olvasóik, látogatóik számára szövegek, grafikák, interjúk, új fejlesztések, új történetek – és a sort egy stb.-vel nyitva hagyják! – közlésével (BusinessDictionary, s.d.a).

A The Free Dictionary by Farlex megfogalmazásában már a magyar meghatározásokhoz közel álló definíciót találunk: *„egy szervezet vagy egyén, amely információs, oktatási vagy szórakoztató tartalmakat hoz létre az internet, CD-ROM-ok vagy szoftveralapú termékek számára”.* Megjegyzendő, hogy a tartalom eléréséhez szükséges szoftver biztosítását a tartalomszolgáltató számára lehetőségként, de nem szükségszerűségként említik meg (TheFreeDictionary, s.d.a).

A fenti meghatározásokat a törvényes ellenőrzés szempontjából értékelve elmondható, hogy azok bár szélesítik a korábban vizsgált magyar definíciókat, már a túlzott általánosság szintjén mozognak. Így segíthetnek ugyan egy megfelelő definíció kialakításában, de önmagában egyik sem alkalmas arra, hogy beilleszthető legyen egy törvénybe mint meghatározás.

Egy lehetséges meghatározás (szerzői javaslat)

A magyar és a külföldi definíciókat áttekintve, valamint figyelembe véve a technológiai fejlődés irányait, a tartalomszolgáltató törvényesellenőrzés-szempontú meghatározásához álláspontom szerint az alábbiakat kell figyelembe venni:

- bármilyen információt (textuális, numerikus, képi, hangos, multimediális) közzétehet,
- tájékoztatás, oktatás vagy szórakoztatás céljából,
- időben korlátozott vagy korlátlan módon,
- fizetős vagy ingyenes formában,
- amelyért szerkesztői felelősséggel tartozik,
- nem tekinthetők tartalomszolgáltatásnak a magáncélú vagy szűk, meghatározott körben elérhető tartalmak,
- kizárólag egyirányú kommunikációt szolgál, a felhasználó *passzív* fogyasztó,
- a szolgáltatás Magyarországon elérhető és igénybe vehető függetlenül attól, hogy a szolgáltató hazánkban letelepedett vagy egyáltalán bármilyen formában engedélyezett-e,
- a szolgáltató lehet bármilyen természetes vagy jogi személy (cég, személy vagy azok egy csoportja),
- amely a hozzáférés során nem kell, hogy egyértelműen azonosítható legyen,
- a tartalmakat online, elektronikus úton, elsősorban az interneten teszi hozzáférhetővé.

(Az offline elérhető tartalmak – legyenek akár nyomtatottak [például újság, könyv stb.], akár elektronikusak [például CD, DVD, Blue-ray Disc stb.] – a téma szempontjából nem relevánsak.)

A fentiek alapján az alábbi definíciót célszerű a törvényes ellenőrzéssel foglalkozó törvényben felhasználni:

> *Tartalomszolgáltató: online tartalomszolgáltató minden olyan jogi vagy természetes személy vagy jogi személyiséggel nem rendelkező gazdasági társaság, illetve ezek bármilyen csoportja, amely/aki infokommunikációs rendszeren – főként interneten – keresztül, elsősorban tájékoztatás, oktatás vagy szórakoztatás céljából, a felhasználók összessége vagy*

> *egy csoportja által elérhető módon bármilyen (textuális, numerikus, képi, hangos, multimediális) információt tesz közzé időben korlátozott vagy korlátlan módon, ingyenesen vagy ellenszolgáltatás fejében. Online tartalomszolgáltatónak kell tekinteni minden ilyen szolgáltatót, amennyiben szolgáltatása Magyarországon elérhető függetlenül attól, hogy a szolgáltató hazánkban letelepedett vagy egyáltalán bármilyen formában engedélyezett-e, valamint attól, hogy a tartalom hozzáférése során egyértelműen azonosítható-e. Tartalomszolgáltató esetén a közlések kizárólag egyirányúak, azok tartalmára a fogyasztónak semmilyen befolyása nincs, a szolgáltató a tartalomért szerkesztői felelősséggel tartozik.*

Alkalmazásszolgáltatók fogalmi meghatározása

Az alkalmazásszolgáltatókra már jóval kevesebb és jóval heterogénebb meghatározásokat lehet találni. Ennek több oka is van. A tartalomszolgáltatók jelentős része már régóta létezik, más médiumokon – mint például a nyomtatott sajtó, az analóg vagy digitális televíziós műsorszórás stb. – több évtizede végeznek ilyen tevékenységet, így a tevékenységi körüket leíró meghatározások kialakultak, tehát az IP-alapú szolgáltatásokkal történő megfeleltetésük is viszonylag egyszerűen elvégezhető volt. Ugyanez nem mondható el az alkalmazás- és az infrastruktúra-szolgáltatókról, amelyek jószerével csak az elmúlt években jöttek létre, alakultak ki. Ugyanakkor már mindkettőre lehet találni bizonyos definíciókat, ám ezek nem a törvényes ellenőrzés szempontjából készültek, így jelen formájukban nem alkalmasak arra, hogy az ezt szabályozó törvényben megjelenjenek. Ebben az alfejezetben az alkalmazásszolgáltató fogalmát járjuk körbe.

Az alkalmazásszolgáltató elnevezést nemcsak azért célszerű használni a hírközlési szolgáltató helyett, hogy megtehessük a korábban együtt nyújtott két funkció (infrastruktúra- és alkalmazásszolgáltatás) szétválasztását, hanem azért is, mert az alkalmazásszolgáltató kifejezés egy bővebb, tágabb értelmezésű fogalom, és nem csak a hírközlési szolgáltatást nyújtó alkalmazásokat érjük, érthetjük alatta. Gondoljunk csak egy banki háttérrel nem rendelkező pénzügyi tranzakciókat biztosító szolgáltatóra vagy, mondjuk, egy útvonaltervező szolgáltatásra, amelyek – ahogy azt a *Felhő alapú új pénzügyi tranzakciós lehetőségek és azok veszélyei* című közlemény (Gazdag–Kovács, 2014) is bemutatta – szintén érdekesek lehetnek

a törvényes ellenőrzést végző szolgálatok számára. Éppen ezért ez a törvényes ellenőrzés jogi eszközeinek kialakítása során is nagy jelentőségű.

Magyar meghatározások

Az *E-önkormányzati stratégiakészítési ajánlás kistérségek és önkormányzatok számára* című dokumentum v1.1 változatában a következőként definiálják az alkalmazásszolgáltatókat:

> *„Alkalmazásszolgáltató, ASP*[52]*: Az ASP modell lényege, hogy az alkalmazásszolgáltató üzemelteti a szoftvereket egy szerverhotelben vagy a saját telephelyén, a felhasználónak nyújtva az összes közös eszközt és kapcsolódó szolgáltatást (hardver, operációs rendszer, alkalmazási szoftverek, karbantartás, ügyfélszolgálat, biztonsági szolgáltatások stb.). A szolgáltatásokat igénybe vevő felhasználó az interneten keresztül kapcsolódik a távoli szerverekre, és használja az azokon futó alkalmazásokat"* (Közigazgatási Informatikai Bizottság, 2009).

A PC Fórum.hu oldal szótárában a következő meghatározást találjuk:

> *„Alkalmazásszolgáltató: Egy központi adatbázison vagy gépparkon alapuló hálózati szolgáltatásokat nyújtó cég. Az alkalmazás-szolgáltatók lehetővé teszik a cégek és magánemberek számára, hogy az ahhoz szükséges eszközök megvásárlása nélkül, bérleti vagy eseti díj ellenében vegyenek igénybe információs és feldolgozási szolgáltatásokat. A legismertebb ASP-megoldások: bérelt web-boltok, webhosting, tömeges SMS-küldés"* (PC-fórum, s.d.).

A Humansoft oldalán található leírás az előzőknél is szűkebb értelmezést tesz lehetővé, hiszen az alkalmazásszolgáltatókat a „szoftver mint szolgáltatás" szolgáltatási modell szerint működő felhőalapú szolgáltatókkal teszi egyenlővé. Az általuk használt megfogalmazás szerint *„az ügyfél a szolgáltató szerverein futó programokat egy kommunikációs csatornán keresztül bérleti díj fejében használja"* (HumanSoft, s.d.).

---

[52] ASP – Application Service Provider.

A fentiek mellett mindenképpen figyelembe kell venni *az elektronikus kereskedelmi szolgáltatások, valamint az információs társadalommal összefüggő szolgáltatások egyes kérdéseiről szóló 2001. évi CVIII. törvény* (Ekertv.) (2001. évi CVIII. tv.) meghatározásait.[53] Ez a törvény hasonló problémákat vet fel, mint amelyeket az Eht. kapcsán már megfogalmaztunk, definícióival azonban nagyban segítheti a meghatározás kialakítását. A törvény többek között azt is kimondja, hogy előírásait a Magyarország területére irányuló információs társadalommal összefüggő szolgáltatások esetében szintén alkalmazni kell. Az információs társadalommal összefüggő szolgáltatást a következőként határozza meg: *„elektronikus úton, távollevők részére, rendszerint ellenszolgáltatás fejében nyújtott szolgáltatás, amelyhez a szolgáltatás igénybe vevője egyedileg fér hozzá"* [2001. évi CVIII. tv. 2. § f]. Ez a megfogalmazás az alkalmazásszolgáltatókra, de akár a tartalomszolgáltatókra is értelmezhető, akárcsak maga a szolgáltató meghatározása, amelyet így fogalmaz meg a törvény: *„az információs társadalommal összefüggő szolgáltatást nyújtó természetes, illetve jogi személy vagy jogi személyiség nélküli szervezet"* [2001. évi CVIII. tv. 2. § k)]. Ezek – megfelelő kiegészítésekkel – felhasználhatók az alkalmazás- és tartalomszolgáltatók definíciójának kialakításához is. A Magyarországra irányuló szolgáltatás alatt a törvény értelmező rendelkezései között a következőket találjuk: *„minden olyan szolgáltatás, amelyről a használt nyelv, a pénznem és egyéb körülmények alapján valószínűsíthető, hogy magyarországi igénybe vevők számára kívánják elérhetővé tenni"* [2001. évi CVIII. tv. 2. § g]. Ez a megfogalmazás mindenképpen átalakításra szorul. Ma már rengeteg szolgáltatás létezik, amelyeket Magyarországról úgy lehet igénybe venni, hogy semmilyen előfeltétel nem utal arra, hogy kifejezett cél lett volna a magyar piac. Azonban egyrészt ilyen szolgáltatásokat használnak Magyarországról is, másrészt a globális piac, a szabad valutahasználat, az angol nyelv használatának terjedése stb. okán nem is szükséges előfeltételezésekkel élni.

A fenti definíciók ugyan nagyban segítik egy megfelelő meghatározás kialakítását, de nem adnak teljesen elfogadható meghatározást. Egyrészt adott esetben nem teljes mértékben fedik le a törvényes ellenőrzésbe bevonni célszerű szolgáltatásokat, szolgáltatókat, másrészt bizonyos, a törvényes

[53] 2016-ban éppen ez a törvény változott a téma szempontjából leginkább. Itt vezették be ugyanis az alkalmazásszolgáltató fogalmát, és ebben írták elő a törvényes ellenőrzésre vonatkozó kötelezettségeiket. Erről részletesen a fejezet végén lesz szó, itt a módosítás előtti állapotról van szó.

ellenőrzés szempontjából fontos kritériumokról, mint például hazai letelepedés, nem szólnak.

Külföldi meghatározások

Annak érdekében, hogy egy, a törvényes ellenőrzést jobban szolgáló, szélesebben értelmezhető meghatározást lehessen kialakítani, célszerű néhány külföldi meghatározást is áttekinteni.

A Gartner szerint az alkalmazásszolgáltató *„alkalmazásfunkciókat és hozzá kapcsolt szolgáltatásokat biztosít több felhasználó részére, megrendelés- vagy felhasználásalapú fizetési modell szerint"* (Gartner, s.d.b). Meghatározásuk szerint az ASP-piac olyan szolgáltatók keverékéből áll, mint a hálózat- és telekommunikációs szolgáltatók, független szoftverforgalmazók vagy olyan egyéb szolgáltatók, amelyek ICT-kiszervezéssel vagy webüzemeltetéssel foglalkoznak. Érdekes, hogy a Gartner *Tartalom és alkalmazásszolgáltató* címszóval is ad egy meghatározást, amely szerint ezen szolgáltatók *„elsődlegesen az információ- és médiaszolgáltatásokra, tartalom-, szórakozás- és alkalmazásszolgáltatásokra fókuszálnak"* (Gartner, s.d.c). Példának pedig a Google-t és a Yahoo-t említik (Gartner, s.d.c).

A Techterms.com-on található meghatározás szerint az alkalmazásszolgáltató *„egy olyan szervezet vagy vállalat, amely szoftveres alkalmazásokat biztosít a felhasználóknak az interneten"* (TechTerms, s.d.). A definíció további részében az alkalmazásszolgáltatókat itt is egyenlővé teszik a „szoftver mint szolgáltatás" szolgáltatási modell szerint működő felhőalapú szolgáltatókkal (TechTerms, s.d.).

A Bussinessdictionary.com leírása alapján az alkalmazásszolgáltató *„egy cég, amely interneten keresztüli elérésű számítógépes szoftverekhez árul hozzáférést"* (BusinessDictionary, s.d.b). További kritériumként határozzák meg, hogy a cég garantálja az alkalmazások folyamatos, problémamentes elérését, ehhez rendelkezik a szükséges hardver-, szoftver- és humán erőforrásokkal. Ezért az előfizető havi- vagy használatalapú díjat fizet (BusinessDictionary, s.d.b).

Az előzőhöz hasonlóan definiálja a Dictionary.com is az alkalmazásszolgáltatót, szerintük az *„egy cég, amely egyéni vagy üzleti felhasználóknak nyújt specializált szoftverekhez és más számítástechnikához kapcsolódó szolgáltatáshoz elérhetőséget az interneten keresztül"* (Dictionary.com, s.d.b).

A TheFreeDictionary.com-on szinte ugyanezt a meghatározást találhatjuk meg azzal az apró különbséggel, hogy az elérést valamilyen hálózati protokollon, tipikusan HTTP-n keresztülinek definiálja. Példaként fizetésre vagy rendelésre használt weboldalakat említ (TheFreeDictionary, s.d.b).

A törvényes ellenőrzés szempontjából a külföldi meghatározások sem adnak teljeskörűen elfogadható definíciókat, amelynek okai megegyeznek a magyar meghatározások kapcsán leírtakkal. Ugyanakkor célszerű még megvizsgálni az úgynevezett „Over-the-Top" (OTT-)[54] szolgáltatókra, -szolgáltatásokra adott megfogalmazásokat is.

„Over-the-Top"-szolgáltatói meghatározások

A törvényes ellenőrzés szempontjainak megfelelő, általános és a szolgáltatást nyújtókat pontosan leíró meghatározások kialakításakor azért célszerű az úgynevezett Over-the-Top-szolgáltatásokat, valamint az azokat biztosító szolgáltatókra adott definíciókat is figyelembe venni, mert ezek már annak megfelelően írják le ezeket a szolgáltatásokat, szolgáltatókat, hogy tekintettel vannak az internetet mint alap- és mások által biztosított infrastruktúrát csupán felhasználó és azokon alkalmazásokat szolgáltató modellre.

A Techopedia.com meghatározása szerint az OTT-alkalmazás *„egy olyan alkalmazás vagy szolgáltatás, amely lehetővé teszi egy termék elérését az interneten keresztül, kikerülve a hagyományos terjesztést"* (technopedia, s.d.). Példának a médiát és a kommunikációt hozza, legnagyobb előnyének pedig a hagyományoshoz képest alacsonyabb költségeket említi. Ugyanakkor a magyarázó részben megjegyzi, hogy ez bizony konfliktusokat okoz a hagyományos szolgáltatók és az OTT-szolgáltatók között, hiszen az OTT-szolgáltatók a hagyományos szolgáltatók piacából hasítanak ki részeket (technopedia, s.d.).

A Pace.com szűkebb értelemben említi az OTT-szolgáltatásokat, hiszen e fogalom alatt a dedikált és menedzselt saját Internet Protocol Television (IPTV-)[55] hálózat helyett az internetet mint átviteli közeget használó tévé-, videó- és – talán egy kicsit kiterjesztő kitétellel – egyéb szolgáltatásokról

---

54 Az interneten mint mások által biztosított közegen nyújtott szolgáltatások, tartalmak, amelyekre az internetszolgáltatónak nincs befolyása.

55 Az internetprotokoll segítségével általában széles sávú interneten keresztül nyújtott, digitális televíziós műsorszolgáltatás.

beszél. Ugyanakkor lényeges elemként említi, hogy az OTT a fogyasztó internethozzáférés-szolgáltatójától függetlenül, infrastruktúra-beruházások nélkül biztosítja szolgáltatásait (Arris, s.d.).

Az Imediaconnection.com szerint az OTT egy, a távközlési vagy több rendszert üzemeltető (például kábeltévé, műholdas tévé), szolgáltató nélkül biztosított hang-, videó- és adatszolgáltatás. Példának többek között az okostévék által közvetlenül elért YouTube-ot említi (Smith, 2007).

Juan José Ganuza és María Fernanda Viecens *Over-the-top (OTT) applications, services and content: implications for broadband infrastructure* című tanulmányukban többek között tisztázzák azt is, hogy mit is értenek OTT alatt. Ezt nem definíciószerűen teszik, hanem 3 fő OTT-szolgáltatást különítenek el: a kommunikációs szolgáltatásokat, mint például: Skype, Gmail; az alkalmazásszolgáltatásokat, mint például: Facebook, LinkedIn, Twitter; valamint a tartalomszolgáltatásokat, mint például: Netflix, YouTube. Megállapítják, hogy az OTT-szolgáltatók ráépülnek a fizikai infrastruktúrát üzemeltető internetszolgáltatókra, sőt paradox módon még veszteséget is okoznak nekik. Anélkül ugyanis, hogy azok részesednének a profitból, egyrészt részeket hasítanak ki az üzletükből, például a kommunikációs szolgáltatások terén, másrészt a generált nagyobb adatforgalom okán még infrastruktúra-fejlesztési beruházásokra is kényszerítik őket (Ganuza–Viecens, 2013).

Egy lehetséges meghatározás (szerzői változat)

A fenti definíciókat áttekintve, valamint figyelembe véve az technológiai fejlődés irányait, az alkalmazásszolgáltató törvényes ellenőrzés szempontú meghatározásához az alábbiakat kell figyelembe venni:

- valamilyen szoftverhez és/vagy hardverhez való hozzáférést, szoftveres alkalmazást, valamint kapcsolódó szolgáltatásokat biztosít a felhasználók számára,
- kiemelten, de nem kizárólagosan ideértve a közösségi oldalakat, a kommunikációs, pénzügyi, geoinformációs, szórakozási, valamint tárhelyet biztosító szolgáltatásokat,
- az elérést specifikus szoftveren vagy webes felületen keresztül biztosítja,
- a kínált szolgáltatás(ok) online, elektronikus úton, elsősorban az interneten keresztül hozzáférhető(k),

- a szolgáltató által üzemeltetett eszközökön futnak a kínált alkalmazások,
  - a szolgáltatás(ok) ráépül(nek) a fizikai infrastruktúrát üzemeltető – elsősorban internet-hozzáférést biztosító – szolgáltatók hálózatára,amelyek több felhasználó számára biztosítottak,
  - időben korlátozott vagy korlátlan módon,
  - havi vagy használat alapú fizetős vagy ingyenes formában,
- a kínált szolgáltatás(ok) bárki számára elérhető(k), legyen(ek) az természetes vagy jogi személy, magán vagy vállalati felhasználó,
- a használat során a felhasználó sosem „passzív" fogyasztó, hanem aktív, tevékeny résztvevő,aki a hozzáférés során nem kell, hogy egyértelműen azonosítható legyen,
- a szolgáltatás Magyarországon elérhető és igénybe vehető függetlenül attól, hogy a szolgáltató hazánkban letelepedett-e, vagy egyáltalán bármilyen formában engedélyezett-e,
- a szolgáltató lehet bármilyen természetes vagy jogi személy (cég, személy vagy ezek egy csoportja), amely a hozzáférés során nem kell hogy egyértelműen azonosítható legyen.

A fentiek alapján az alábbi definíciót célszerű a törvényes ellenőrzéssel foglalkozó törvényben felhasználni:

> *Alkalmazásszolgáltató: online alkalmazásszolgáltató minden olyan jogi vagy természetes személy, illetve ezek bármilyen csoportja, amely/aki valamilyen infokommunikációs rendszerre – elsősorban internetre – ráépülő, azon keresztül valamilyen szoftverhez és/vagy hardverhez való hozzáférést, szoftveres alkalmazást, valamint kapcsolódó szolgáltatásokat biztosít specifikus szoftveren vagy webes felületen, több felhasználó számára, időben korlátozott vagy korlátlan módon, havi- vagy használat alapú ellenszolgáltatás fejében vagy ingyenes formában. Online alkalmazásszolgáltatónak kell tekinteni minden ilyen szolgáltatót, amennyiben szolgáltatása Magyarországon elérhető függetlenül attól, hogy a szolgáltató hazánkban letelepedett, vagy egyáltalán bármilyen formában engedélyezett-e, valamint attól, hogy a hozzáférése során akár a szolgáltató, akár a felhasználó egyértelműen azonosítható-e. Online alkalmazásszolgáltatók közé értjük kiemelten, de nem kizárólagosan ide értve a közösségi oldalakat, a kommunikációs, pénzügyi, geoinformációs, szórakozási, valamint tárhelyet biztosító*

szolgáltatásokat. Alkalmazásszolgáltatás esetében az információáramlás többirányú, a felhasználó aktív, tevékeny résztvevő, az információk adattartalmára befolyással rendelkezik.

Infrastruktúra-szolgáltatók fogalmi meghatározása

Az infrastruktúra-szolgáltató meghatározására jelenleg nem igazán találni a törvényes ellenőrzés szempontjából is megfelelő definíciókat. Ennek az az oka, hogy az infrastruktúra-szolgáltató alatt ma elsősorban a felhőalapú rendszerek osztályozásánál a szolgáltatási modellek szerinti csoportosításban szereplő infrastruktúra mint szolgáltatást (IaaS) biztosító szolgáltatókat írják le. Ebbe a modellbe pedig azok a szolgáltatók tartoznak, amelyek a felhasználó számára olyan számítási, tárolási, hálózati és egyéb alapvető informatikai erőforrásokat biztosítanak, amelyekre és amelyeken a felhasználó tetszőleges szoftvereket telepíthet és futtathat, beleértve az operációs rendszereket és alkalmazásokat. Ugyanakkor ebben az esetben a felhasználó nem képes menedzselni vagy ellenőrizni a mögöttes felhő-infrastruktúrát, de kontrollálni tudja az operációs rendszereket, tárhelyeket, telepített alkalmazásokat, és esetleg korlátozott ráhatása lehet a hálózati elemek (például tűzfalak) kiválasztására. Márpedig ez jóval kevesebb tartalommal jellemezhető, mint a fejezet elején bemutatott hármas tagozódásban szereplő infrastruktúra-szolgáltató.

Ezeknél jobb megközelítést adnak az internetszolgáltatókra megtalálható definíciók. Ezek jelentős része a Pcmag.com-on megtalálható enciklopédiában fellelhető meghatározás magjához hasonlóan írja le az internetszolgáltatót, amely szerint ez *„egy vállalat, amely internetelérést biztosít”* (Encyclopedia, s.d.). A definíciók egy része megmarad ezen a szinten, az ennél bővebb meghatározások pedig ezt az alapot terjesztik ki különféle módokon. A Dictionary.com-on az e-mailezési lehetőség biztosításával egészítették ki a megfogalmazást, valamint azzal, hogy a szolgáltatások havi díj ellenében vehetők igénybe (Dictionary.com, s.d.c). A havi vagy használatarányos fizetési mód a már idézett Pcmag.com-meghatározásban is fellelhető. Több definícióban kitérnek az internetelérés lehetséges módjaira is, mint például ISDN, kábel(tévé), DSL, optikai. Ilyenek például a Pcmag.com, az Investopedia.com (Investopedia, s.d.) vagy az About.com (lifewire, s.d.) meghatározásai. A Dictionary.com-on említett e-mailezési lehetőség mellett az egyéb kapcsolódó szolgáltatásokra utalást is tartalmaznak egyes

meghatározások, így például a Searchwindevelopment.techtarget.com oldalán fellelhető leírás is, amely weboldalak készítését és üzemeltetését említi példaként (TechTarget, s.d.).

A fenti meghatározások sem felelnek meg teljesen a fejezet elején bemutatott hármas tagozódásban szereplő infrastruktúra-szolgáltató értelmezésének, és egyike sem ad a törvényes ellenőrzés kapcsán is felhasználható pontos definíciót. Egyrészt azért, mert több helyen olyan szolgáltatások biztosítása is megjelenik, amelyek a fejezet előző részeiben említett szerinti értelmezésben már az alkalmazásszolgáltatók feladatrendszerébe tartozik, másrészt a törvényes ellenőrzésnek tökéletesen megfelelő meghatározáshoz képest olyan irreleváns és egyáltalán nem időtálló elemeket is tartalmaznak, mint az internetelérés módja.

A fentiek okán célszerű a jelenlegi hírközlési szolgáltató, emellett a hírközlő hálózat definícióját is áttekinteni. Ez az Eht. szerint a következő: *„14. Elektronikus hírközlési szolgáltató: elektronikus hírközlő hálózat üzemeltetője, valamint elektronikus hírközlési szolgáltatást nyújtó természetes, illetőleg jogi személy”* (2003. évi C. tv.).

Elektronikus hírközlő hálózat alatt az Eht. pedig a következőket érti:

> *„19. Elektronikus hírközlő hálózat: átviteli rendszerek és – ahol ez értelmezhető – a hálózatban jelek irányítására szolgáló berendezések, továbbá más erőforrások – beleértve a nem aktív hálózati elemeket is –, amelyek jelek továbbítását teszik lehetővé meghatározott végpontok között vezetéken, rádiós, optikai vagy egyéb elektromágneses úton, beleértve a műholdas hálózatokat, a helyhez kötött és a mobil földfelszíni hálózatokat, az energiaellátó kábelrendszereket olyan mértékben, amennyiben azt a jelek továbbítására használják, a műsorszórásra használt hálózatokat és a kábeltelevíziós hálózatokat, tekintet nélkül a továbbított információ fajtájára”* (2003. évi C. tv.).

Szintén érdemes figyelembe venni *az elektronikus kereskedelmi szolgáltatások, valamint az információs társadalommal összefüggő szolgáltatások egyes kérdéseiről szóló törvény* közvetítőszolgáltató-meghatározását, amely a következőket mondja:

> *„l) Közvetítő szolgáltató: az információs társadalommal összefüggő szolgáltatást nyújtó szolgáltató, amely*

> *la) az igénybe vevő által biztosított információt távközlő hálózaton továbbítja, vagy a távközlő hálózathoz hozzáférést biztosít (egyszerű adatátvitel és hozzáférés-biztosítás);*
> *lb) az igénybe vevő által biztosított információt távközlő hálózaton továbbítja, és az alapvetően a más igénybe vevők kezdeményezésére történő információtovábbítás hatékonyabbá tételét szolgálja (gyorsítótárolás);*
> *lc) az igénybe vevő által biztosított információt tárolja (tárhelyszolgáltatás);*
> *ld) információk megtalálását elősegítő segédeszközöket biztosít az igénybe vevő számára (keresőszolgáltatás)"* (2001. évi CVIII. tv. 2. § l)]

Ez a meghatározás szintén segíti a cél elérését, ám az lc) és az ld) pontok alatt leírtak az alkalmazásszolgáltatók definíciójánál használható fel, az lb) pont esetében pedig tekintetbe kell venni a törvény megírása óta eltelt több mint 10 év technikai fejlődését.

Egy lehetséges meghatározás (szerzői változat)

A fenti definíciókat áttekintve, valamint figyelembe véve az technológiai fejlődés irányait, az infrastruktúra-szolgáltató törvényes ellenőrzés szempontú meghatározáshoz az alábbiakat kell figyelembe venni:

- elektronikus hírközlési, infokommunikációs hálózatot üzemeltet és/vagy internetelérést biztosít,
- több felhasználó számára,
- időben korlátozott vagy korlátlan módon,
- havi vagy használatalapú fizetős vagy ingyenes formában,
- a szolgáltatás Magyarországon elérhető és igénybe vehető függetlenül attól, hogy a szolgáltató hazánkban letelepedett-e vagy egyáltalán bármilyen formában engedélyezett-e,[56]
- a szolgáltató lehet bármilyen természetes vagy jogi személy (cég, személy vagy ezek egy csoportja),

[56] Például egy mesterséges holdon keresztül nyújtott internetelérés lehet olyan, amelynél a szolgáltató nincs Magyarországon letelepedve, sőt bejelentve sem.

- amely a hozzáférés során nem kell hogy egyértelműen azonosítható legyen.[57]

A fentiek alapján az alábbi definíciót célszerű a törvényes ellenőrzéssel foglalkozó törvényben felhasználni:

> *Infrastruktúra-szolgáltató: online infrastruktúra-szolgáltató minden olyan jogi vagy természetes személy, illetve ezek bármilyen csoportja, amely/aki valamilyen infokommunikációs rendszert üzemeltet, és azon keresztül internetelérést biztosít több felhasználó számára, időben korlátozott vagy korlátlan módon, havi vagy használatalapú ellenszolgáltatás fejében vagy ingyenes formában. Online infrastruktúra-szolgáltatónak kell tekinteni minden ilyen szolgáltatót, amennyiben szolgáltatása Magyarországon elérhető függetlenül attól, hogy a szolgáltató hazánkban letelepedett vagy egyáltalán bármilyen formában engedélyezett-e, valamint attól, hogy a hozzáférése során akár a szolgáltató, akár a felhasználó egyértelműen azonosítható-e. Online infrastruktúra-szolgáltatók közé értjük azokat a szolgáltatókat is, amelyek más szolgáltatótól vásárolt interneteléréshez biztosítanak harmadik félnek (feleknek) hozzáférést.*

Vegyes szolgáltatások értelmezése

Természetesen előfordulhat, hogy valamely cég vegyes szolgáltatást nyújt. Ma például egy internetszolgáltató internetelérést és e-mailezési lehetőséget is biztosíthat, vagy egy online tartalomszolgáltatással foglalkozó cégnél, például egy internetes újságnál pedig lehetőséget adhatnak kommentek írására, ezen keresztül pedig kommunikáció megvalósítására is. Ezek az esetek is kezelhetők a fejezet elején bemutatott hármas tagozódásban szereplő tartalom-, alkalmazás- és infrastruktúra-szolgáltató modellel.

A törvényes ellenőrzés kapcsán a három szolgáltatónak eltérő kötelezettségei származnak. Míg a tartalomszolgáltatónak alig, az infrastruktúra-szolgáltatónak korlátozott (elsősorban előfizetői adatszolgáltatási), addig az alkalmazásszolgáltatónak – a hagyományos hírközlési szolgáltatóhoz

[57] Például egy nyílt WiFi-szolgáltatás esetén nem mindig azonosítható a szolgáltató egyértelműen.

hasonlóan – szinte teljes körű (például az összes felhasználói adat, így bejelentkezési IP-címek, felhasználónevek, valamint az általa nyújtott szolgáltatás kapcsán keletkező tartalmak, így e-mailek, hangkommunikáció, cset, útvonaltervezési adatok stb.) információ- és adatelérést kell biztosítania az arra felhatalmazott szervezetek számára.

Amennyiben egy cég vegyes szolgáltatást nyújt, a szolgáltatásfajtáknak megfelelően kell a törvényes ellenőrzést lehetővé tennie. Maradva a fent említett példáknál, ha egy mai értelemben vett internetszolgáltató e-mail-lehetőséget is biztosít, akkor erre az alkalmazásszolgáltatóknál kialakítandó kötelezettségeket kell figyelembe vennie. Ugyanez igaz az online újság esetében is, ahol a fórumok, kommentek esetén már az alkalmazásszolgáltatókra kirótt kötelezettségeket kell teljesíteniük.

Érdemes megvizsgálni a mai hírközlési szolgáltatók helyzetét is. Esetükben a problémakör két részre bontható. Amennyiben internetszolgáltatást is végeznek, akkor a fent leírtak alapján lehet eljárni. Amennyiben a hagyományos – például vezetékestelefon- – szolgáltatásokat nézzük, ezeknél is megjelenik az infrastruktúra- és alkalmazásszolgáltatás, csak kizárólagosan egy, azonos és elválaszthatatlan infrastruktúrával és szolgáltatóval. Ebben az esetben is ugyanúgy kezelhető a probléma, mint a fent már leírt egyéb vegyes szolgáltatások esetében.

Ezek alapján megállapítható, hogy a tartalom-, alkalmazás- és infrastruktúra-szolgáltató modellbe minden szolgáltató egyértelműen besorolható, így törvényes kötelezettségeik is egyértelműen meghatározhatóvá válnak. Igaz ez a mai jogszabályokban leírt hírközlési és internetszolgáltatók esetében is.

Mindezek mellett a hírközlési szolgáltató és szolgáltatás fogalmát a továbbiakban is célszerű fenntartani, egyrészt azért, mert így például a hagyományos telefonszolgáltatások a jelenlegi szabályoknak megfelelően a továbbiakban is egyszerűen, mindenki számára vita nélkül elfogadott módon kezelhetők; másrészt pedig azért, mert a nemzetközi jogi szabályozásban ezek törvényes ellenőrzése egy mindenki által elfogadott meghatározás, illetve normarendszer szerint történik.

Ez utóbbi azonban például az alkalmazásszolgáltatókról nem mondható el, mint ahogy a fejezet első része, valamint a *Felhőalapú rendszerek törvényes ellenőrzési problémái,* valamint *a Felhőalapú rendszerek törvényes ellenőrzési módszereinek vizsgálata I–II.* című cikk (Kovács, 2013c; Kovács, 2013d; Kovács, 2013e) bemutattak, ezért a tartalom-, alkalmazás- és infrastruktúra-szolgáltató modell mielőbbi bevezetése rendkívül fontos.

A törvényes ellenőrzés kialakítását elősegítő lehetőségek

Fontos megjegyezni, hogy az infrastruktúra-szolgáltatót kivéve a másik két szolgáltató tud úgy – teljes körű! – szolgáltatást nyújtani, hogy az adott országban fizikailag nem jelenik meg, ott nincs bejelentve vagy az Smtv. és az Mttv. megfogalmazása szerint letelepedve. Éppen ezért a törvényes ellenőrzéssel kapcsolatos törvény hatályát úgy kell megfogalmazni, hogy minden Magyarországon elérhető, oda is irányuló vagy onnan igénybe vehető szolgáltatásra kiterjedjen. Ez azonban nem egyszerű feladat.

Ugyanakkor más aspektusból, például az adózás oldaláról is érdemes a kérdéskört megvizsgálni. Az ehhez kapcsolódó törvényeink a fentieknek megfelelő átalakításával ugyanis plusz adóbevételt is lehet teremteni. Erre már van is kezdeményezés, hiszen a 2014. június 12-én érkeztetett *T/264 számú, az egyes pénzügyi tárgyú törvények módosításáról szóló javaslat* (2014. évi T/264. tv. jav.), amelyet a *2014. évi XXXIII. törvény az egyes pénzügyi tárgyú törvények módosításáról* címmel (2014. évi XXXIII. tv.) az Országgyűlés azóta már jóváhagyott és hatályba is léptetett, többek között kitér a korábban már említett szolgáltatások adóztatására is.

Ebben a téma szempontjából legfontosabb kitételek a következők:

> *„45/A. § (1) A következő, nem adóalany részére nyújtott szolgáltatások esetében a teljesítés helye az a hely, ahol ezzel összefüggésben a szolgáltatást igénybe vevő nem adóalany letelepedett, letelepedés hiányában pedig, ahol lakóhelye vagy szokásos tartózkodási helye van:*
> *a) telekommunikációs szolgáltatások;*
> *b) rádiós és audiovizuális médiaszolgáltatások;*
> *c) elektronikus úton nyújtott szolgáltatások.*
> *(2) E § alkalmazásában elektronikus úton nyújtott szolgáltatás különösen:*
> *a) elektronikus tárhely rendelkezésre bocsátása, honlap tárolása és üzemeltetése, valamint számítástechnikai eszköz és program távkarbantartása,*
> *b) szoftver rendelkezésre bocsátása és frissítése,*
> *c) kép, szöveg és egyéb információ rendelkezésre bocsátása, valamint adatbázis elérhetővé tétele,*
> *d) zene, film és játék – ideértve a szerencsejátékot is – rendelkezésre bocsátása, valamint politikai, kulturális, művészeti, tudományos, sport*

és szórakoztatási célú médiaszolgáltatás, illetőleg ilyen célú események közvetítése, sugárzása,
e) távoktatás, feltéve, hogy a szolgáltatás nyújtása és igénybevétele globális információs hálózaton keresztül történik. A szolgáltatás nyújtója és igénybevevője közötti, ilyen hálózaton keresztüli kapcsolat felvétele és tartása – ideértve az ajánlat tételét és elfogadását is – azonban önmagában még nem elektronikus úton nyújtott szolgáltatás".

„3.1. teljesítési hely szerinti tagállam: az a tagállam, amelyet az általános forgalmi adóról szóló törvény szerint nem adóalany részére nyújtott távolról is nyújtható szolgáltatás teljesítési helyének kell tekinteni".
„4. Az Európai Közösség területén nem letelepedett adózókra vonatkozó különös szabályok:
4.1. Bejelentkezésre, bejelentésre, változásbejelentésre, nyilvántartásba vételre vonatkozó szabályok;
4.1.1. Az adózó az azonosítószám megállapítása céljából a távolról is nyújtható szolgáltatási tevékenységének az Európai Közösség bármely tagállamában történő megkezdését megelőzően az állami adóhatósághoz elektronikus úton bejelenti:
4.1.1.1. a vállalkozás nevét, cégneve(i)t amennyiben eltér(nek) a vállalkozás nevétől,
4.1.1.2. a teljes postai címét, e-mait címét, a cég elektronikus elérhetőségét (honlapját)
4.1.1.3. a székhelye szerinti adóazonosító számát, amennyiben ilyennel rendelkezik,
4.1.1.4. az adózó székhelye szerinti ország megnevezését,
4.1.1.5. az IBAN vagy OBAN bankszámlaszámot,
4.1.1.6. a BIC kódot,
4.1.1.7. az adóhatósággal történő kapcsolattartásra feljogosított személy (ún. kapcsolattartó) nevét, telefonszámát,
4.1.1.8. nyilatkozatot arról, hogy az Európai Közösség más tagállamának HÉA-nyilvántartásában nem szerepel,
4.1.1.9. a különös szabályozás hatálya alá eső tevékenység megkezdésének időpontját" [2014. évi (T/264) tv. jav.].

A törvényben megfogalmazottaknak három hatása van a fejezetben körüljárt témára nézve:

- Az első és talán legfontosabb, hogy már EU-s ajánlás szintjén is megfogalmazottak alapján bekényszeríti a magyar jogrend kereteibe

a Magyarországon nem, sőt sokszor az EU-ban sem letelepedett, az interneten, elektronikus úton szolgáltatást nyújtó cégeket. Ehhez bejelentési kötelezettségeket is kapcsol.
- A második, hogy az adóztatást a teljesítés helyéhez köti, és nem a szolgáltató székhelyéhez.
- A harmadik, hogy – ha más csoportosítás szerint is, de – az ott alkalmazott felsorolásokba beleérthetők az alkalmazás- és tartalomszolgáltatók egyaránt.

A törvényben megfogalmazottak alapot és precedenst teremtettek az internettechnológiára épülő szolgáltatások, azon belül pedig a PC/SaaS-rendszerek „bekényszerítésére" a magyar jogrendbe. Az adóztatás volt tehát az első lépés, de ezt kihasználva tovább lehetett, sőt kellett vinni a szabályozási folyamatot a törvényes ellenőrzésre is. Ott is ki kell(ett) kényszeríteni a bejelentési és az együttműködési kötelezettséget, akárcsak az adóztatás esetén, ráadásul olyan formában, ahogyan a törvényes ellenőrzés oldaláról nézve a hagyományos hírközlési szolgáltatók esetében már korábban is létezett és jelenleg fennáll.

Többek között ezekre alapozva született meg hazánkban 2016-ban az a jogszabályi háttér, amely az alkalmazásszolgáltatók számára mára már kötelezővé teszi az együttműködést a törvényes ellenőrzés végrehajtása kapcsán az arra feljogosított nemzetbiztonsági szolgálatokkal és rendvédelmi szervekkel. Azonban ebben az esetben is, ugyanúgy, mint ahogy az adóztatás szempontjából is, érdekes – és a későbbiekben megoldandó – feladatként jelentkezik a szankcionálás kérdése. Nagy kérdés ugyanis, milyen eszközökkel lehet kikényszeríteni az együttműködést, vagy hogyan lehet büntetni az alóla kibújókat. Erre lehet példa az interneten nyújtott sportfogadások, szerencsejátékok esete. Itt a Nemzeti Adó- és Vámhivatal (NAV) már blokkoltatja azokat az online fogadási szolgáltatást nyújtó oldalakat, amelyek nem tesznek eleget a magyar jogszabályokban megfogalmazottaknak (napi.hu, s.d.). Ugyanakkor meg kell jegyezni, hogy a szankcionálás és a kikényszeríthetőség kérdése még az adózás esetében sem kristályosodott ki teljesen, a törvényes ellenőrzés kapcsán pedig ugyanolyan problémákkal kell szembesülniük az érintett szerveknek.

Mindemellett célszerű megvizsgálni azt is, hogy a hazánkban bevezetett szabályozásnak milyen keretei és hatásai vannak, kikre vonatkozik, kikre nem, rontja-e a kommunikáció biztonságát, valamint azt is, hogy milyen jogi garanciákat biztosít az alkalmazásszolgáltatók számára. Ugyanakkor ki kell

emelni, hogy ez a szabályozás csupán az alkalmazásszolgáltatókra vonatkozik, a tartalom- és az infrastruktúra-szolgáltatókra nem. Amíg azonban az infrastruktúra-szolgáltatók, amelyek a modell szerint az internetelérést biztosítják, a hatályos Eht. alapján együttműködésre kötelezettek, addig a tartalomszolgáltatókra ilyen előírások jelenleg nem vonatkoznak, így az ő esetükben a jogszabályalkotási folyamatot célszerű továbbvinni.

A 2016-ban hatályba lépett magyarországi törvényi szabályozás és annak hatásai

A fentiekre alapozva bemutathatók a hazánkban 2016-ban elfogadott új szabályozás keretei és hatásai, megvizsgálható, hogy az új jogszabály milyen kötelezettségeket ró a felhasználókra, a gyártókra/fejlesztőkre, továbbá az alkalmazásszolgáltatókra, elemezhetők az általa biztosított jogi garanciák, valamint a betarthatósággal kapcsolatos kérdések is.

Az internetalapú szolgáltatások – ezek közül is kiemelten a kommunikációt lehetővé tevők – törvényes ellenőrzésében mérföldkőnek tekinthető a hazánkban 2016-ban hatályba lépett szabályozás. *A terrorizmus elleni fellépéssel összefüggő egyes törvények módosításáról szóló 2016. évi LXIX. törvény* (2016. évi LXIX. tv.) ugyanis többek között módosította az Ekertv.-t (2001. évi CVIII. tv.). Ennek keretében bevezette az alkalmazásszolgáltató fogalmát[58], definiálta a Magyarország területére irányuló szolgáltatásokat, valamint előírta a titkosított kommunikációt biztosító alkalmazásszolgáltatóknak, hogy megkeresés esetén tegyék lehetővé az erre feljogosított szervezetek számára a kommunikáció tartalmához és az annak kapcsán keletkező vagy kezelt metaadatokhoz való hozzáférést. Kötelezővé tette számukra továbbá a továbbított küldeményekkel, közlésekkel kapcsolatosan keletkező vagy kezelt metaadatok, azok keletkezésétől számított egy éven át történő megőrzését is. Az ehhez szorosan kapcsolódó, *a titkosított kommunikációt biztosító alkalmazásszolgáltatók és a titkos információgyűjtésre feljogosított*

[58] *„Alkalmazásszolgáltató: az a természetes, illetve jogi személy vagy jogi személyiséggel nem rendelkező más szervezet, aki vagy amely elektronikus hírközlő hálózat felhasználásával valamilyen szoftverhez vagy hardverhez való hozzáférést, szoftveres alkalmazást, valamint kapcsolódó szolgáltatásokat biztosít specifikus szoftveren vagy webes felületen több felhasználó számára, időben korlátozott vagy korlátlan módon, havi vagy használatalapú ellenszolgáltatás fejében vagy ingyenes formában”* [2001. évi CVIII. tv. 2. § m)].

szervezetek együttműködésének rendjéről szóló 185/2016. (VII. 13.) Korm. rendelet pedig rögzíti a szolgáltatók és a törvényes ellenőrzést végzők közötti együttműködés részletszabályait.

A szabályozás keretei és hatásai

A sajtóban a jogszabályok kihirdetése előtt számos találgatás látott napvilágot, majd a kihirdetés után is lehetett olvasni kissé félreértelmezett interpretálásokat a szolgáltatók, de akár a felhasználók szerepéről, kötelezettségeiről, sőt az ellenőrzés kialakítása okán a kommunikáció biztonságának csökkenéséről is. Éppen ezért érdemes áttekinteni, mire ad pontosan lehetőséget ez a szabályozás, mit tesz lehetővé, és mit nem, valamint, hogy miben jelent előrelépést a korábbiakhoz képest.

Először is az említett szabályozás nem vonatkozik a titkosított kommunikáció felhasználóira, azaz irányukba semmilyen kötelezettséget vagy büntetést nem eszközöl. Másodszor pedig a titkosított kommunikáció kapcsán is csupán a szolgáltatókkal – és nem a gyártókkal, fejlesztőkkel vagy eladókkal (!) – foglalkozik, azaz azokra érvényes, akik a kommunikáció felépítése és/vagy végrehajtása során érdemi tevékenységet látnak el. Így nem vonatkozik olyan gyártó és/vagy fejlesztő- és/vagy értékesítőcégekre sem, akik csupán végpont–végpont-titkosítást nyújtó szoftver- és/vagy hardvertermékeket biztosítanak a felhasználók részére. Ez utóbbi esetben ugyanis mindkét kommunikáló félnek ugyanazt a titkosító eszközt kell alkalmaznia, és ugyanazt – vagy legalábbis kompatibilis – harmadik fél által nyújtott kommunikációs csatornát kell igénybe vennie, a tikosított kommunikáció kapcsán pedig nincs központi azonosítás, azaz így a kommunikáció kizárólag úgy tud megvalósulni, hogy a felek azt előre egymással egyeztették.

Ugyanakkor ez a szabályozás vonatkozik minden olyan kommunikációs szolgáltatóra, amely központilag biztosítja a titkosított kommunikáció lehetőségét minden oda beregisztrált felhasználó számára, a felhasználáshoz pedig megfelelő azonosítás szükséges.

A kötelezettség ilyetén történő meghatározásának logikája megegyezik a jelenlegi hírközlési szolgáltatóknál alkalmazottal, amely előírja egyrészt a törvényes ellenőrzés biztosításának kötelezettségét, másrészt tiltja olyan új szolgáltatás bevezetését vagy a meglévők olyan átalakítását, amely azt ellehetetleníti, ugyanakkor engedi az egyedi, a felhasználó által alkalmazott végpont-végpont titkosítás használatát.

Ez az előírás viszont azt is jelenti, hogy azok a szolgáltatók, amelyek ma úgy nyújtanak titkosított kommunikációs szolgáltatást, hogy jelenleg nem biztosítják a kommunikáció tartalmához való hozzáférést, vagy át kell alakítaniuk működési struktúrájukat, vagy hazánkban nem nyújthatják szolgáltatásukat. Ez pedig amellett, hogy a hazánkban infrastruktúrával is jelen lévő hírközlési szolgáltatókkal e tekintetben versenyegyenlőséget teremt, lehetővé teszi a törvényes ellenőrzést az arra feljogosított szervek számára.

Érdemes ugyanakkor azt is megvizsgálni, hogy okozhatja-e ez a fajta új jogi szabályozás a kommunikáció biztonságának romlását a felhasználó szemszögéből. Ehhez először is elemezni kell az említett jogszabályok hatásait a kommunikáció biztonságára, majd ezeket össze kell vetni azon egyéb technikai lehetőségek hatásaival, amelyek adott esetben a törvényes ellenőrzést végzők rendelkezésére áll(hat)nak.

A szabályozás hatása a kommunikáció biztonságára

Nézzünk egy példát a klasszikus hírközlés világából. A rádiótelefonok hazai elterjedésekor az első telepített rendszer az NMT 450 volt. Ez a hangátvitelre titkosítás nélküli FM-modulált jelet használt (Ketterling, 2004), amely egy megfelelő vevő segítségével bárki által lehallgatható volt. Ilyen vevővel bármelyik rádióamatőr rendelkezhetett, de néhány tízezer forintnak megfelelő összegért bárki engedély nélkül megvásárolhatta ezeket, akár hazánkban is. Ehhez képest a mai GSM-hálózatok már erős (jobbára A5.1 vagy A5.3) titkosítást alkalmaznak a levegőinterfész lehallgatás elleni védelmére (GSM 2000 Joint GSMA TSG SA WG3 Working party, s.d.). Ezeket ma sokkal biztonságosabbnak tekintjük, mint a régi NMT-rendszert, pedig azzal is tisztában vagyunk, hogy a GSM-rendszerek esetében is biztosított a törvényes ellenőrzés lehetősége. Ez azt mutatja, hogy úgy lehetett növelni a kommunikáció biztonságát a felhasználó szempontjából, hogy ugyanakkor nem csorbult a törvényes ellenőrzéshez fűződő érdek sem.

Természetesen felmerülhet a kérdés, hogy a hazánkban bevezetett jogi szabályozásnak vannak-e negatív hatásai, azaz a felhasználó szemszögéből a kommunikáció továbbra is elég biztonságosnak tekinthető-e.

A felhőalapú rendszerek, így a kommunikációt (is) biztosítók esetében az egyik kiemelten kezelt probléma a szolgáltató kémkedése, valamint harmadik felek (például szolgáltató beszállítói, partnerei) hozzáférése a felhasználó adataihoz, információihoz (Chow et al., 2009). Sőt, e kérdés

vizsgálata kapcsán arra is külön érdemes kitérni, hogy – az általában külföldi – felhőszolgáltató hogyan és melyik ország szervei számára biztosítja még az ellenőrzés lehetőségét. Nézzük meg például a Gmail esetét. A Gmailt biztonságosnak tekintjük, hiszen már bejelentkezéstől erős SSL-titkosítást használ, és több eszközt is biztosít (például ki, mikor, milyen IP-címről, eszközről stb. fért hozzá utoljára a fiókunkhoz, figyelmeztető e-mailt küld, ha szokatlan bejelentkezést észlel például új mobil eszközről stb.), amellyel támogatja kommunikációnk biztonságát (Google, s.d.b). Ugyanakkor már a Google-lal kötött szerződésben is szerepel, hogy hozzáfér leveleinkhez, azokat – persze csupán a szolgáltatás fejlesztése érdekében – elemzi és felhasználja (Google, s.d.c). Ráadásul a Snowden által közzétett anyagokból azt is tudjuk, hogy 2009-ben a Google is csatlakozott az úgynevezett *Prism programhoz,* amelynek keretében – több más szolgáltatóval (például Microsoft, Facebook, Apple stb.) együtt biztosították az Egyesült Államok szolgálatai részére a hozzáférést a rendszereiken tárolt és azokon átfolyó adatokhoz (például beszélgetések, videócsetek, fényképek stb.); (Poitras–Gellman, 2013; The Washington Post, 2013). Joggal merülhet fel akkor a kérdés: a felhasználó szemszögéből nézve ez így mennyire biztonságos szolgáltatás? De úgy is feltehetjük a kérdést: ront-e bármit is a biztonságon az, ha az arra illetékes hazai szolgálat egyértelmű és szigorúan betartott, továbbá betartatott törvényi előírásoknak megfelelően fér hozzá az általa jogosan igényelt információkhoz?

Ehhez érdemes továbbvizsgálni a szolgáltatói együttműködés adta kereteket. Az egyik ilyen kitétel, hogy a hazai jogszabályok által előírtak mellett nincs szükség az átviteli út titkosításának kikényszerített gyengítésére. Ez azt jelenti, hogy nem kell olyan hátsó kaput, mesterkulcsot vagy gyengített titkosítást alkalmazni, amelyik lehetővé teheti a szolgálatok számára az információkhoz való hozzáférést a szolgáltatók bevonása nélkül is. Ez a megoldás ugyanis valóban adna egyfajta technikai megoldást az ellenőrzésre,[59] de ez azzal a veszéllyel is járna, hogy más, illetéktelen titkosszolgálatok, bűnözők, konkurens cégek stb. is könnyebben hozzáférhetnének a felhasználó adataihoz, információihoz, ami valóban jelentősen gyengíthetné a biztonságot.

A másik ilyen kitétel, hogy így nincs szükség a felhasználó által használt hardvereszközök (például okostelefon, notebook stb.) kikényszerített gyengítésére, hátsó kapu beépítésére. Ez szintén adhatna egyfajta technikai

[59] Lásd például mély csomagvizsgálat (DPI), közbeékelődéses ellenőrzés (MitM).

megoldást[60] a törvényes ellenőrzésre feljogosított szolgálatok részére, sőt nemcsak a kommunikáció tartalmához, hanem akár az eszközön tárolt egyéb adatokhoz is hozzáférést biztosítana, ugyanakkor ugyanúgy rendelkezne azokkal a hátrányokkal, mint a fenti megoldás. Azaz az eszköz elvesztése, ellopása, de akár távoli hozzáférése esetén mások is könnyen hozzájuthatnának ezekhez az információkhoz, vagy telepíthetnének rá kémprogramokat (Yadron, 2016).

A szolgáltató együttműködése így talán a legkisebb veszélyforrásnak tekinthető mindazok ellenére, hogy ily módon fennáll a veszélye a szolgáltató kémkedésének vagy egy partnere illetéktelen hozzáférésének. Ez ugyanis jogi és adminisztratív úton kezelhető, azaz előírhatók a szolgáltató számára olyan rendelkezések, amelyek ennek kizárását szolgálják. Ráadásul ezek betartása, valamint a betartás bizonyítása a szolgáltatók érdeke is. Azok a szolgáltatók ugyanis, amelyek elvégeztetnek egy erre vonatkozó auditot, tanúsítással rendelkeznek arról, hogy náluk szabályozott, valamint ellenőrzött módon zárták ki a fent említett problémát, és annak eredményeit közzé is teszik, versenyelőnyt szereznek azokkal szemben, akik nem tudnak hasonlót felmutatni. Ez a metódus a felhőalapú rendszerek esetében már elfogadottnak tekinthető, erre bevált formák és eljárások vannak, az auditorok pedig rendelkeznek a kellő tudással egy ilyen típusú átfogó vizsgálat elvégzéséhez. Ezért a szolgáltatók – a biztonság szem elé kerülésével – érdekeltek lesznek abban, hogy így járjanak el.

Arra, hogy a felhasználók számára valóban a szolgáltatók és a törvényes ellenőrzést végző szervezetek közötti együttműködés biztosítja a legkisebb kockázatot, további érvek is felsorakoztathatók.

Az első, hogy a felhasználó számára így ismert és tudott az együttműködés ténye, amely ráadásul a hírközlési szolgáltatók viszonylatában már elfogadott gyakorlat is. Korábban éppen a Snowden-botrány kapcsán derült fény arra, hogy például a legjelentősebb alkalmazásszolgáltatók

[60] Lásd például aktív ellenőrző eszközök (kémprogramok), valamint például FBI–Apple-vita. Ez utóbbi esetében két, az Iszlám Államm szimpatizáló terrorista 14 embert ölt meg egy egészségklinikán az egyesült államokbeli San Bernandinóban. A rendőrség által begyűjtött bizonyítékok között volt az egyik támadó jelkódos zárral védett iPhone 5C típusú mobiltelefonja, amelynek feltörését kérte az FBI az Apple-től. A cég ezt megtagadta, majd egy, az ügyön túlnövő vita alakult ki az adatvédelemről. Bár bírósági végzés is született arról, hogy az Apple-nek segítenie kell, végül egy – vélhetőleg – izraeli cég törte fel a telefont, és tette a rajta lévő adatokat elérhetővé az FBI számára (Nakashima, 2016).

tagadták vagy kerülték a válaszadást az egyesült államokbeli nemzetbiztonsági szolgálatokkal és rendvédelmi szervekkel való együttműködésre, mégis lehetőséget biztosítottak számukra a felhasználók adataihoz való hozzáférésre (Gyurkity, 2013).

A második, hogy azok a szolgáltatók, amelyek a korábban már jelzett auditot végrehajtják, és annak eredményeit közzéteszik, azt is bizonyítják a felhasználóknak, hogy csak azokkal az ellenőrzést végző szolgálatokkal állnak kapcsolatban, amelyekről a felhasználó is tud. A felhőalapú szolgáltatások esetében ugyanis mindig is kiemelten kezelendő kockázat volt, hogy a szolgáltató kivel osztja, oszthatja meg a felhasználó adatait, így például a szolgáltató honos országában vagy akár adatközpontjainak országában is. Amennyiben ez nem tisztázott a felhasználó számára, ez is csökkentheti kommunikációja biztonságát.

A harmadik, hogy arra egyébiránt sincs garancia, hogy egy szolgáltató vagy gyártó nem épít-e be tudatosan valamilyen hátsó kaput, amellyel akár saját maga, akár egy harmadik fél számára biztosíthatja a hozzáférést a felhasználó adataihoz. Erre több alkalommal is felmerült a gyanú olyan neves gyártók esetében, amelyek biztonságosnak hirdették termékeiket (Sullivan, 2014; Zetter, 2012; Afonin, 2016).

Kikényszeríthetőség

A hazai szabályozás kapcsán felmerült már a kérdés, hogy ki lehet-e egyáltalán kényszeríteni az alkalmazásszolgáltatók együttműködését. Erre talán az adózással és a szerencsejátékok szabályozásával kapcsolatos példákat érdemes megemlíteni. Az alkalmazásszolgáltatók adóztatására már 2014-ben, T/264 számon javaslat érkezett (2014. évi T/264. tv. jav.), amelyet az Országgyűlés még abban az évben el is fogadott (2014. évi XXXIII. tv.). Az így hatályosított törvényben megfogalmazottak alapot és precedenst teremtettek az internettechnológiára épülő szolgáltatások, így az alkalmazásszolgáltatók „bekényszerítésére" a magyar jogrendbe. Ugyanakkor az adóztatás szempontjából is érdekes – és a későbbiekben megoldandó – feladatként jelentkezik a szankcionálás kérdése. Nagy kérdés ugyanis, hogy milyen eszközökkel lehet kikényszeríteni az együttműködést, vagy hogyan lehet büntetni az alóla kibújókat. Erre lehet példa az interneten nyújtott sportfogadások, szerencsejátékok esete. Itt a NAV már blokkoltatja azokat az online fogadási szolgáltatást nyújtó oldalakat,

amelyek nem tesznek eleget a magyar jogszabályokban megfogalmazottaknak (napi.hu, s.d.). Megjegyzendő azonban, hogy az itt egyébként működő szankcionálási rendszert is meg kívánták erősíteni az illetékesek, amelynek érdekében törvényjavaslatot terjesztettek be (T/12250. tv. jav.), amelyet azóta az Országgyűlés el is fogadott, rendelkezései pedig már hatályba is léptek. Ennek főbb elemei, hogy a kiszabható pénzbírságot a tízszeresére emelték, valamint bevezették a pénzügyi blokkolást is. Ez utóbbi azt akadályozza meg, hogy az illegálisszerencsejáték-szervező bankszámlájára megérkezzen a játékos által átutalt összeg, az átutalást ebben az esetben ugyanis a pénzforgalmi szolgáltató nem teljesítheti.

A szankcionálásra a törvényes ellenőrzés kapcsán jelenleg az Ekertv. – ismételhető módon – pénzbírság kiszabását biztosítja. Ennek gyakorlati betarthatósága, esetlegesen más elemekkel – például a szerencsejátékokhoz hasonló módon blokkolással – történő kiegészítése még a jövő zenéje. Ugyanakkor meg kell jegyezni, hogy a szankcionálás kérdése az adózás esetében sem kristályosodott még ki teljesen, és ez ugyanúgy kérdéseket vet fel a törvényes ellenőrzés kapcsán is. Mindazok mellett, hogy az interneten nyújtott sportfogadások, szerencsejátékok esetében Magyarországon már kialakult egyfajta működő megoldás, célszerű egyrészt megvizsgálni a külföldi ilyen célú megoldásokat, másrészt egyeztetéseket folytatni arról, hogy magasabb, például EU-szinten hogyan lehet a kérdésben egységesen fellépni.

Jogi garanciák

További kérdésként merülhet fel, hogyan lehet, vagy lehet-e bármilyen garanciát adni arra, hogy a törvényes ellenőrzést végző szolgálatok csak ahhoz az információhoz férnek hozzá, amelyekre engedélyt kaptak. Erre jogi garanciát nyújt a nagyon szigorú hazai szabályozás. Ez már a hírközlési szolgáltatók esetében is kizárólag úgynevezett külső, azaz bírói vagy igazságügy-miniszteri engedély megléte esetén tette lehetővé a kommunikáció tartalmához való hozzáférést, valamint kizárta a szűrő-kutató jellegű ellenőrzés lehetőségét. A jelenlegi szabályozás ezt konzekvensen fenntartja. Ráadásul a *185/2016. (VII. 13.) Korm. rendelet* lehetőséget biztosít a szolgáltató számára, hogy jogi képviselőjével megvizsgáltassa az adatigénylés jogszabályok szerinti megfelelőségét. Ezek pedig megfelelő garanciális elemek mind a felhasználó, mind a szolgáltató számára.

Összességében megállapítható, hogy a Magyarországon 2016-ban életbe lépett jogi szabályozás mindenképpen előremutató, mondhatni példaértékű, hiszen mások csak most keresik a problémára a megfelelő megoldást. Jól mutatja ezt a német és a francia belügyminiszter által kiadott közös közlemény is, amelyben deklarálják, hogy a terrorizmus elleni küzdelem okán olyan megoldást kell találni a titkosított kommunikáció lehallgatására, amely biztosítja az adatokhoz való hozzáférést a felhasználók magánszférájának védelme mellett. Mindezt úgy, hogy a szabályozás minden szolgáltatóra egyforma kötelezettségekkel és feltételekkel terjedjen ki, függetlenül azok székhelyétől (Bundesministerium des Innern, für Bau und Heimat, s.d.). Azaz egyfajta, a magyar szabályozásnak megfelelő megoldást javasolnak, ám ennek tényleges megvalósításától még messze vannak.

Megállapítható az is, hogy az új hazai szabályozás teremtette lehetőség mindamellett, hogy a felhasználó szempontjából nézve a kommunikáció biztonságára a legkisebb veszélyforrásnak tekinthető, költséghatékonyan képes biztosítani a törvényes ellenőrzést. Ráadásul oly módon, hogy ahhoz megfelelő jogi garanciákat is csatol.

Ugyanakkor megállapítható az is, hogy a kikényszeríthetőség további megoldandó kérdéseket vet fel, amelyek hatékony megoldásához célszerű megvizsgálni egyrészt a hazai és a külföldi már kialakult és működő megoldásokat, másrészt egy magasabb, például EU-szintű egységes fellépés lehetőségét.

Felhasznált irodalom

Könyvek, forrásgyűjtemények, tudományos-szakmai közlemények

Adobe (s.d.): *Adobe Photoshop.* www.adobe.com/hu/products/photoshop.html (A letöltés ideje: 2013. 10. 27.)

Afonin, Oleg (2016): *iOS 10: Security Weakness Discovered, Backup Passwords Much Easier to Break.* http://blog.elcomsoft.com/2016/09/ios-10-security-weakness-discovered-backup-passwords-much-easier-to-break/ (A letöltés ideje: 2016. 09. 27.)

ARCEP (2013): *Skype Refuses to Register as an Operator.* http://arcep.fr/index.php?id=8571&tx_gsactualite_pi1%5Buid%5D=1593&tx_gsactualite_pi1%5Bannee%5D=&tx_gsactualite_pi1%5Btheme%5D=&tx_gsactualite_pi1%5Bmotscle%5D=&tx_gsactualite_pi1%5BbackID%5D=26&cHash=baebcd8ef257d3194065360ecec41a90&L=1 (A letöltés ideje: 2013. 06. 20.)

Arris (s.d.): *Over-the-Top Services (OTT).* www.pace.com/global/our-thinking/over-the-top-services-ott/ (A letöltés ideje: 2014. 06. 09.)

aws (s.d.): *AWS GovCloud (US) Region FAQs.* http://aws.amazon.com/govcloud-us/faqs/ (A letöltés ideje: 2015. 01. 31.)

Barker, Colin (2013): *Cloud computing and outsourcing: Where does one end and the other begin?* www.zdnet.com/article/cloud-computing-and-outsourcing-where-does-one-end-and-the-other-begin/ (A letöltés ideje: 2015. 01. 10.)

Baset, Salman A. – Schulzrinne, Henning (2006): *An Analysis of the Skype Peer-to-Peer Internet Telephony Protocol.* www1.cs.columbia.edu/~salman/publications/skype1_4.pdf (A letöltés ideje: 2013. 06. 18.)

Belügyminisztérium (2015): *Megkezdődött az ASP-rendszer átadása.* www.kormany.hu/hu/belugyminiszterium/hirek/megkezdodott-az-asp-rendszer-atadasa (A letöltés ideje: 2017. 09. 02.)

BEREC (2012): *BEREC preliminary findings on traffic management practices in Europe show that blocking of VoIP and P2P traffic is common, other practices vary widely.* http://berec.europa.eu/doc/2012/TMI_press_release.pdf (A letöltés ideje: 2013. 06. 28.)

Berta Sándor (2006): *Online házkutatásokat indítanának Németországban.* http://sg.hu/cikkek/49079/online_hazkutatasokat_inditananak_nemetorszagban (A letöltés ideje: 2013. 06. 24.)

Berta Sándor (2008): *Mindenki lehallgatható lenne Németországban.* http://sg.hu/cikkek/57484/mindenki_lehallgathato_lenne_nemetorszagban (A letöltés ideje: 2013. 06. 24.)

Berta Sándor (2011): *Lehallgathatják az oroszok a Skype-ot.* http://sg.hu/cikkek/82579/lehallgathatjak_az_oroszok_a_skype_ot (A letöltés ideje: 2013. 06. 18.)

Berta Sándor (2013a): *Évek óta lehallgatható Oroszországban a Skype.* http://sg.hu/cikkek/96074/evek_ota_lehallgathato_oroszorszagban_a_skype (A letöltés ideje: 2013. 06. 18.)

Berta Sándor (2013b): *Külföldi szervereket is megtámadhat a holland rendőrség.* http://sg.hu/cikkek/97134/kulfoldi_szervereket_is_megtamadhat_a_holland_rendorseg (A letöltés ideje: 2013. 06. 28.)

Berta Sándor (2013c): *Németország a felhőadatokat is ellenőrizné.* http://sg.hu/cikkek/96458/nemetorszag_a_felhoadatokat_is_ellenorizne (A letöltés ideje: 2013. 06. 28.)

Berta Sándor (2013d): *Szigorítanák a német távközlési törvényt.* http://sg.hu/cikkek/96798/szigoritanak_a_nemet_tavkozlesi_torvenyt (A letöltés ideje: 2013. 06. 28.)

Biddle, Sam (2016): *The NSA Leak is Real, Snowden Documents Confirm.* https://theintercept.com/2016/08/19/the-nsa-was-hacked-snowden-documents-confirm/ (A letöltés ideje: 2016. 09. 19.)

bitport.hu (2017): *A felhő tolta meg az SAP negyedévét.* 2017. 04. 25. http://bitport.hu/a-felho-tolta-meg-az-sap-negyedevet (A letöltés ideje: 2017. 08. 17.)

Blizzard (s.d.): *World of Warcraft.* http://eu.battle.net/wow/en (A letöltés ideje: 2013. 10. 27.)

blogs.cisco.com (s.d.): *Seperation of Responsibility in Cloud.* http://blogs.cisco.com/wp-content/uploads/Seperation-of-Responsibility-in-Cloud.png (A letöltés ideje: 2011. 10. 29.

blogs.microsoft.com (2014): *Microsoft sees huge gains in commercial cloud revenue.* https://blogs.microsoft.com/firehose/2014/07/22/microsoft-sees-huge-gains-in-commercial-cloud-revenue/ (A letöltés ideje: 2015. 08. 01.)

Bodnár Ádám (2010): *2011 közepén jön a Google Chrome OS.* www.hwsw.hu/hirek/45786/google-chrome-os-web-store-bongeszo-operacios-rendszer-notebook-netbook.html (A letöltés ideje: 2011. 10. 21.)

Bodnár Ádám (2011): *A Microsoft megvette a Skype-ot.* www.hwsw.hu/hirek/46667/microsoft-skype-voip-telefon-felvasarlas.html (A letöltés ideje: 2013. 06. 17.)

Brodkin, Jon (2008): *Gartner: Seven cloud-computing security risks.* www.infoworld.com/d/security-central/gartner-seven-cloud-computing-security-risks-853?page=0,0 (A letöltés ideje: 2012. 01. 02.)

Buecker, Axel – Lodewijkx, Koos – Moss, Harold – Skapinetz, Kevin – Waidner, Michael: *Cloud Security Guidance (IBM Recommendations for the Implementation of Cloud Security) Redpaper.* www.redbooks.ibm.com/redpieces/abstracts/redp4614.html?Open&pdfbookmar (A letöltés ideje: 2012. 01. 02.)

Business Dictionary (s.d.a): *content provider.* www.businessdictionary.com/definition/content-provider.html (A letöltés ideje: 2013. 08. 16.)

Business Dictionary (s.d.b): *Application Service Provider (ASP).* www.businessdictionary.com/definition/application-service-provider-ASP.html (A letöltés ideje: 2013. 08. 24.)

Catteddu, Daniele (2011) (ed.): *Security & Resilience in Governmental Clouds.* www.enisa.europa.eu/activities/risk-management/emerging-and-future-risk / deliverables/security-and-resilience-in-governmental-clouds (A letöltés ideje: 2014. 11. 18.)

CCC (2011): *Chaos Computer Club analyzes government malware.* http://ccc.de/en/updates/2011/staatstrojaner (A letöltés ideje: 2013. 06. 24.)

cdn.wuala.com (s.d.): *Termination of Free Storage.* https://cdn.wuala.com/files/termination_free_storage.pdf (A letöltés ideje: 2015. 01. 26.)

Chandrasekhar, Bharath (2011): *What is Cloudbursting?* http://cloudsecurity.trendmicro.com/what-is-cloudbursting/ (A letöltés ideje: 2011. 10. 22.)

Chen, Yanpei – Paxson, Vern – Katz, Randy H. (2010): *What's New About Cloud Computing Security? Technical Reports. Electrical Engineering and Computer Sciences University of California at Berkeley.* www.eecs.berkeley.edu/Pubs/TechRpts/2010/EECS-2010-5.pdf (A letöltés ideje: 2011. 11. 05.)

Chow, Richard – Golle, Philippe – Jakobsson, Markus – Shi, Elaine – Staddon, Jessica – Masuoka, Ryusuke – Molina, Jesus (2009): Controlling Data in the Cloud: Outsourcing Computation without Outsourcing Control. In *CCS '09 Proceedings of the 16th ACM conference on Computer and communications security.* New York: ACM, 85–90. www.parc.com/publication/2335/controlling-data-in-the-cloud.html (A letöltés ideje: 2011. 11. 05.)

CIB (2015): *CIB Bank – eBroker – Vállalatok*. cib.hu 2015. 07. 21. www.cib.hu/ebroker/hirportal/tozsde_vallalatok/index?id=P217204 (A letöltés ideje: 2015.. 08. 01.)

Cisco (2014): *Cisco Global Cloud Index: Forecast and Methodology, 2013–2018. – Whitepaper*. www.cisco.com/c/en/us/solutions/collateral/service-provider/global-cloud-index-gci/Cloud_Index_White_Paper.pdf (A letöltés ideje: 2015. 08. 01.)

Clarke, Steve (2015): *Commercial cloud annualized revenue run rate exceeds $8.2 billion as strong execution drives Microsoft first quarter results*. https://blogs.microsoft.com/firehose/2015/10/22/commercial-cloud-annualized-revenue-run-rate-exceeds-8-2-billion-as-strong-execution-drives-microsoft-first-quarter-results/ (A letöltés ideje: 2017. 08. 17.)

Clarke, Steve (2016): *Fourth quarter results highlight Microsoft Cloud strength*. https://blogs.microsoft.com/firehose/2016/07/19/fourth-quarter-results-highlight-microsoft-cloud-strength/ (A letöltés ideje: 2017. 08. 17.

Clarke, Steve (2017): *Fourth quarter results highlight Microsoft cloud strength*. https://blogs.microsoft.com/firehose/2017/07/20/fourth-quarter-results-highlight-microsoft-cloud-strength-2/ (A letöltés ideje: 2017. 08. 17.)

Cloud Computing (2009): *Benefits, risks and recommendations for information security*. www.enisa.europa.eu/activities/risk-management/files/deliverables/cloud-computing-risk-assessment (A letöltés ideje: 2014. 11. 12.)

cloud.cio.gov (s.d.a): *One Stop Source for Federal Cloud Computing Information*. http://cloud.cio.gov/ (A letöltés ideje: 2014. 10. 25.)

cloud.cio.gov (s.d.b): *FedRAMP. Home*. http://cloud.cio.gov/fedramp (A letöltés ideje: 2014. 10. 25.)

cloud.cio.gov (s.d.c): *FedRAMP. Security Assessment Framework*. cloud.cio.gov/sites/default/files/documents/files/FedRAMP%20Security%20Assessment%20Fra (A letöltés ideje: 2015. 01. 17.)

Cohen, Heidi (2015): *15 Mobile Facts That Should Change Your 2015 Marketing*. http://heidicohen.com/mobile-app-trends-2015/ (A letöltés ideje: 2015. 08. 01.)

Coles, Cameron (s.d.): *Overview of Cloud Market in 2017 and Beyond*. www.skyhighnetworks.com/cloud-security-blog/microsoft-azure-closes-iaas-adoption-gap-with-amazon-aws/ (A letöltés ideje: 2017. 08. 17.)

Collins (s.d.): *content provider*. www.collinsdictionary.com/dictionary/english/content-provider (A letöltés ideje: 2013. 08. 16.)

Columbus, Louis (2017): *Cloud Computing Market Projected To Reach $411B by 2020.* www.forbes.com/sites/louiscolumbus/2017/10/18/cloud-computing-market-projected-to-reach-411b-by-2020/#41cfc26178f2 (A letöltés ideje: 2017. 12. 02.)

Cox, Phil (s.d.a): *Intrusion detection in a cloud computing environment.* http://searchcloudcomputing.techtarget.com/tip/Intrusion-detection-in-a-cloud-computing-environment (A letöltés ideje: 2012. 01. 02.)

Cox, Phil (s.d.b): *Securing data in the cloud.* http://searchcloudcomputing.techtarget.com/tip/Securing-data-in-the-cloud (A letöltés ideje: 2012. 01. 02.)

CSA (2011a): *Security Guidance for Critical Areas of Focus in Cloud Computing V3.0.* https://cloudsecurityalliance.org/guidance/csaguide.v3.0.pdf (A letöltés ideje: 2012. 01. 05.)

CSA (2011b): *Defined Categories of Service 2011.* https://cloudsecurityalliance.org/wp-content/uploads/2011/09/SecaaS_V1_0.pdf (A letöltés ideje: 2012. 01. 05.)

CSA (2014a): *Cloud Controls Matrix v3.0.1.* https://cloudsecurityalliance.org/research/ccm/#_downloads (A letöltés ideje: 2014. 09. 17.)

CSA (2014b): *Cloud Controls Matrix v3.0.1 Info Sheet.* https://cloudsecurityalliance.org/download/cloud-controls-matrix-v3-0-1-info-sheet/ (A letöltés ideje: 2014. 09. 17.)

CSA (2016a): *Defined Categories of Security as a Service (Preview) – Continuous Monitoring as a Service.* https://downloads.cloudsecurityalliance.org/assets/research/security-as-a-service/csa-categories-securities-prep.pdf (A letöltés ideje: 2017. 08. 01.)

CSA (2016b): *The Treacherous 12 Cloud Computing Top Threats in 2016.* https://downloads.cloudsecurityalliance.org/assets/research/top-threats/Treacherous-12_Cloud-Computing_Top-Threats.pdf (A letöltés ideje: 2017. 08. 01.)

CSA (s.d.): *Cloud Security Alliance: about.* https://cloudsecurityalliance.org/about/ (A letöltés ideje: 2015. 02. 21.)

Dajkó Pál (2007): *A német rendőröknek egyelőre tilos a hackelés.* http://itcafe.hu/hir/a_nemet_rendoroknek_egyelore_tilos_a_hackeles.html (A letöltés ideje: 2013. 06. 24.)

Dajkó Pál (2008): *Új alkotmányos jog született: az IT-jog.* http://itcafe.hu/hir/bundestrojaner_alkotmany_itjog.html (A letöltés ideje: 2013. 06. 24.)

Dajkó Pál (2011): *Lebukott az állami kémprogram.* http://itcafe.hu/hir/chaos_computer_club_nemetorszag_bundestrojaner.html (A letöltés ideje: 2013. 06. 24.)

Dajkó Pál (2013a): *A Google fizet Franciaországban: megtört a netsemlegesség?* http://itcafe.hu/hir/google_orange_netsemlegesseg.html (A letöltés ideje: 2013. 02. 09.)

Dajkó Pál (2013b): *A Google továbbra sem ad ki adatokat a magyar kormánynak.* http://itcafe.hu/hir/google_atlathatosag_transparency.html (A letöltés ideje: 2013. 02. 09.)

DePaolis, Enrico (2009): *Types of Cloud Computing.* http://cloudcomputing.syscon.com/node/1048046 (A letöltés ideje: 2011. 10. 09.)

Desjardins, Jeff (2017): *What Happens in an Internet Minute in 2017?* www.visualcapitalist.com/happens-internet-minute-2017/ (A letöltés ideje: 2015. 08. 18.)

Dictionary.com (s.d.a): *content provider.* http://dictionary.reference.com/browse/content+provider?s=t (A letöltés ideje: 2013. 08. 16.)

Dictionary.com (s.d.b): *asp.* http://dictionary.reference.com/browse/application%20service%20provider?&o=100074&s=t (A letöltés ideje: 2013. 08. 24.)

Dictionary.com (s.d.c): *ISP.* http://dictionary.reference.com/browse/isp (A letöltés ideje: 2014. 07. 24.)

Dropbox (s.d.): *Homepage.* www.dropbox.com/ (A letöltés ideje: 2013. 10. 27.)

Dubrawsky, Ido (2010): *Firewall Evolution – Deep Packet Inspection.* www.symantec.com/connect/articles/firewall-evolution-deep-packet-inspection (A letöltés ideje: 2013. 06. 28.)

DuPaul, Neil (s.d.): *Man-in-the-Middle Tutorial: Learn About Man-in-the-Middle Attacks, Vulnerabilities and How to Prevent MITM Attacks.* www.veracode.com/security/man-middle-attack (A letöltés ideje: 2013. 07. 16.)

Egov Hírlevél (2014): *Felhőszolgáltatás indul közigazgatási intézmények számára.* http://hirlevel.egov.hu/2014/02/21/felhoszolgaltatas-indul-kozigazgatasi-intezmenyek-szamara/ (A letöltés ideje: 2017. 09. 02.)

Egov Hírlevél (2017a): *Országossá válik az önkormányzati ASP-rendszer.* http://hirlevel.egov.hu/2017/06/24/orszagossa-valik-az-onkormanyzati-asp-rendszer/ (A letöltés ideje: 2017. 09. 02.)

Egov Hírlevél (2017b): *Új kormányzati adatközpont épül.* http://hirlevel.egov.hu/2017/04/30/uj-kormanyzati-adatko%CC%88zpont-epul/ (A letöltés ideje: 2017. 09. 02.)

Bundesministerium des Innern, für Bau und Heimat (s.d.): *Ein Beitrag zur Erhöhung der inneren Sicherheit in Europa.* www.bmi.bund.de/SharedDocs/Downloads/DE/Nachrichten/Kurzmeldungen/eckpunkte-der-europaeischen-zusammenarbeit-innere-sicherheit.pdf?__blob=publicationFile (A letöltés ideje: 2016. 08. 25.)

Electronic Frontier Foundation (s.d.): *HTTPS Everywhere.* www.eff.org/am/https-everywhere (A letöltés ideje: 2013. 06. 28.)

Encyclopedia (s.d.): *ISP.* www.pcmag.com/encyclopedia/term/45481/isp (A letöltés ideje: 2014. 07. 24.)

eNet (2013): *Már okostelefon-felhasználó a magyar lakosság több mint ¼-e.* www.enet.hu/hirek/mar-okostelefon-felhasznalo-a-magyar-lakossag-tobb-mint-%C2%BC-e/?lang=hu (A letöltés ideje: 2015. 08. 02.)

eNet (2014): *Minden ötödik internetező kezében ott a tablet.* www.enet.hu/hirek/minden-otodik-internetezo-kezeben-ott-a-tablet/?lang=hu (A letöltés ideje: 2015. 08. 02.)

eNet (2015a): *Áttörés a mobilnet használatban: a magyar internetezők fele zsebében tartja a világhálót.* www.enet.hu/hirek/attores-a-mobilnet-hasznalatban-a-magyar-internetezok-fele-zsebeben-tartja-a-vilaghalot/?lang=hu (A letöltés ideje: 2015. 08. 02.)

eNet (2015b): *Médiatartalmat inkább online! – kérik a fiatalok.* www.enet.hu/hirek/mediatartalmat-inkabb-online-kerik-a-fiatalok/?lang=hu (A letöltés ideje: 2015. 08. 02.)

ENISA (2009): *Cloud Computing – Information Assurance Framework.* www.enisa.europa.eu/activities/risk-management/files/deliverables/cloud-computing-information-assurance-framework?searchterm=Information+Assurance+ (A letöltés ideje: 2014. 11. 12.)

ENISA (2013): *Good Practice Guide for Securely Deploying Governmental Clouds.* www.enisa.europa.eu/activities/Resilience-and-CIIP/cloud-computing/good-practice-guide-for-securely-deploying-governmental-clouds (A letöltés ideje: 2014. 11. 15.)

ENISA (2014): *Security Framework for Governmental Clouds.* www.enisa.europa.eu/activities/Resilience-and-CIIP/cloud-computing/govenmental-cloud-security/security-framework-for-govenmental-clouds (A letöltés ideje: 2015. 01. 23.)

ENISA (2016): *Technical Guidelines for the implementation of minimum security measures for Digital Service Providers.* www.enisa.europa.eu/publications/minimum-security-measures-for-digital-service-providers (A letöltés ideje: 2017. 09. 02.)

ENISA (s.d.a): ENISA homepage. www.enisa.europa.eu/ (A letöltés ideje: 2014. 11. 12.

ENISA (s.d.b): *Resilience Metrics.* www.enisa.europa.eu/activities/Resilience-and-CIIP/Incidents-reporting/metrics/metrics (A letöltés ideje: 2014. 11. 18.)

ENISA (s.d.c): *Cloud Computing.* www.enisa.europa.eu/activities/Resilience-and-CIIP/cloud-computing/introduction-to-cloud-computing (A letöltés ideje: 2014. 11. 12.)

Essers, Loek (2014): *Dropbox learns Dutch, Swedish, Danish and Thai in international expansion.* www.pcworld.com/article/2364400/dropbox-learns-dutch-swedish-danish-and-thai-in-international-expansion.html (A letöltés ideje: 2015. 01. 11.)

Expert: Miami (2012): *Skype does away with random supernodes.* http://expert-miami.blogspot.hu/2012/05/skype-does-away-with-random-supernodes.html (A letöltés ideje: 2013. 06. 18.)

Facebook (s.d.): *Newsroom.* http://newsroom.fb.com/Timeline (A letöltés ideje: 2013. 02. 15.)

Fedorinova, Yuliya (2011): *Microsoft May Offer Skype Codes to Russia's FSB, Vedomosti Says.* www.bloomberg.com/news/articles/2011-06-09/microsoft-may-offer-skype-codes-to-russia-s-fsb-vedomosti-says?cmpid=yhoo (A letöltés ideje: 2013. 06. 18.)

FedRAMP (2012a): *FedRAMP. Continuous Monitoring Strategy & Guide.* http://cloud.cio.gov/document/continuous-monitoring-strategy-guide (A letöltés ideje: 2014. 10. 25.)

FedRAMP (2012b): *FedRAMP. System Security Plan (Template).* www.slideshare.net/kvjacksn/fedramp-system-security-plan-template-12840974 (A letöltés ideje: 2015. 01. 17.)

FedRAMP (s.d.): *Home.* www.fedramp.gov/ (A letöltés ideje: 2017. 08. 06.)

Fisher, Dennis (2013): What is a Man-in-the-Middle Attack? http://blog.kaspersky.com/man-in-the-middle-attack/ (A letöltés ideje: 2013. 07. 16.)

Foran, Joseph (s.d.): *Ten questions to ask when storing data in the cloud.* http://searchcloudcomputing.techtarget.com/tip/Ten-questions-to-ask-when-storing-data-in-the-cloud (A letöltés ideje: 2012. 01. 02.)

Gálffy Csaba (2013): *A Google már fizet a francia internetszolgáltatónak.* www.hwsw.hu/hirek/49670/google-france-telecom-orange-afrika-okostelefon-youtube-android.html (A letöltés ideje: 2013. 02. 09.)

Ganuza, Juan José – Viecens, María Fernanda (2013): *Over-the-top (OTT) applications, services and content: implications for broadband infrastructure.* Buenos Aires: Universidad de San Andrés, Centro de Technología y Sociedad. www.udesa.edu.ar/WP/GetFile.aspx?fid=654282 (A letöltés ideje: 2014. 06. 09.)

Gardham, Duncan (2009): *Government plans to extend powers to spy on personal computers.* www.telegraph.co.uk/news/uknews/law-and-order/4109031/Government-plans-to-extend-powers-to-spy-on-personal-computers.html (A letöltés ideje: 2013. 06. 28.)

Gartner (2011): *Gartner Reveals Top Predictions for IT Organizations and Users for 2012 and Beyond.* www.gartner.com/newsroom/id/1862714 (A letöltés ideje: 2015. 08. 01.)

Gartner (s.d.a): *Content Provider.* www.gartner.com/it-glossary/content-provider/ (A letöltés ideje: 2013. 08. 16.)

Gartner (s.d.b): *Application Service Provider (ASP).* www.gartner.com/it-glossary/asp-application-service-provider/ (A letöltés ideje: 2014. 08. 24.)

Gartner (s.d.c): *Content and Applications Service Provider.* www.gartner.com/it-glossary/casp-content-and-applications-service-provider/ (A letöltés ideje: 2013. 08. 24.)

Gazdag Tibor – Kovács Zoltán (2014): Felhő alapú új pénzügyi tranzakciós lehetőségek és azok veszélyei. *Nemzetbiztonsági Szemle,* II. évf. 2. sz., 36–57.

GetCloudServices (2013): *Cloud Computing vs. Outsourcing.* www.getcloudservices.com/blog/cloud-computing-vs-outsourcing (A letöltés ideje: 2015. 01. 10.)

GFS (s.d.): *Securing Microsoft's Cloud Infrastructure.* www.globalfoundationservices.com/security/ (A letöltés ideje: 2011. 11. 05.)

Ghosh, Mohul (2014): *204M Smartphone Users In India By 2016. Will Surpass US: EMarketer.* http://trak.in/tags/business/2014/12/23/smartphone-users-india-global-growth-chart/ (A letöltés ideje: 2015. 08. 01.)

Gilbert, Francoise (s.d.): *Ten key provisions in cloud computing contracts.* http://searchcloudsecurity.techtarget.com/tip/Ten-key-provisions-in-cloud-computing-contracts (A letöltés ideje: 2012. 01. 02.)

Golovanov, Sergey (2013): *Spyware. HackingTeam.* http://securelist.com/analysis/publications/37064/spyware-hackingteam/ (A letöltés ideje: 2013. 06. 28.)

Google (s.d.a): *Google Maps.* https://maps.google.hu/maps?hl=hu&tab=wl (A letöltés ideje: 2013. 10. 27.)

Google (s.d.b): *Biztonsági tippek a Gmail használatával kapcsolatban.* https://support.google.com/mail/answer/7036019?co=GENIE.Platform%3DDesktop&hl=hu (A letöltés ideje: 2016. 09. 25.)

Google (s.d.c): *Google Általános Szerződési Feltételek* (Utolsó módosítás: 2014. április 14.) www.google.com/intl/hu/policies/terms/ (A letöltés ideje: 2016. 09. 25.)

google.com/chromebook (s.d.): *The new Chromebooks are here.* www.google.com/chromebook/ (A letöltés ideje: 2011. 10. 21.)

Google (s.d.d): *Kezdőlap.* google.hu (A letöltés ideje: 2014. 02. 22.)

googleblog.blogspot.hu (2009): *Releasing the Chromium OS open source project.* http://googleblog.blogspot.hu/2009/11/releasing-chromium-os-open-source.html (A letöltés ideje: 2011. 10. 21.)

GSM 2000 Joint GSMA TSG SA WG3 Working party (s.d.): *GSM Association Specification for A5/3.* www.3gpp.org/ftp/tsg_sa/wg3_security/tsgs3_13_yokohama/docs/pdf/s3-000362.pdf (A letöltés ideje: 2016. 09. 25.)

Gyurkity Péter (2013): *Mindenki a megfigyelt felhőbe igyekszik*. https://sg.hu/cikkek/97838/mindenki-a-megfigyelt-felhobe-igyekszik (A letöltés ideje: 2016. 09. 25.)

Habók Lilla (2017): *Négy és fél millióan használnak okostelefont.* www.hwsw.hu/hirek/56731/enet-kutatas-felmeres-okostelefon-mobil-hasznalat-olvasas-zene-video.html (A letöltés ideje: 2017. 08. 17.)

Haig Zsolt – Kovács László – Munk Sándor – Ványa László (2013): *Az infokommunikációs technológia hatása a hadtudományokra.* Budapest: Nemzeti Közszolgálati Egyetem, 2013.

Haig Zsolt (2015): *Információ – Társadalom – Biztonság.* Budapest: NKE Szolgáltató Kft.

Harangi László (2011): *Hogyan szerezzünk felhő-alapú vírusírtót, tűzfallal?* http://pcworld.hu/hogyan-szerezzunk-felho-alapu-virusirtot-tuzfallal-20110916.html (A letöltés ideje: 2011. 10. 04.)

Hegman, Sonja (2014): *DataPoint: Microsoft's Skype DAU has grown 82 percent in a year.* www.insidefacebook.com/2014/02/03/datapoint-microsofts-skype-dau-gains-82-from-a-year-ago-mau-gains-just-1-25/ (A letöltés ideje: 2015. 01. 11.)

hirek.prim.hu (2011): *Továbbfejlesztett mobil és felhő alapú nyomtatási szolgáltatások az Epsontól.* http://hirek.prim.hu/cikk/2011/09/14/tovabbfejlesztett_mobil_es_felho_alapu_nyomtatasi_szolgaltatasok_az_epsontol (A letöltés ideje: 2011. 10. 07.)

HumanSoft (s.d.): *Alkalmazás szolgáltatás.* www.humansoft.hu/Alkalmazas_szolgaltatas.html (A letöltés ideje: 2013. 08. 24.)

iGov (2014): *GovCloud.* http://i.gov.ph/govcloud/wp-content/uploads/2014/03/GovCloud-Year-Ender_December-12-2013.pdf (A letöltés ideje: 2015. 01. 31.)

Insider (2011): *Miért jó a Skype a Microsoftnak?* http://insiderblog.hu/kulfold/2011/05/12/skype/ (A letöltés ideje: 2013. 06. 17.)

Intel (2015): *Intel's Vision of the Ongoing Shift to Cloud Computing.* www.intel.com/content/dam/www/public/us/en/documents/white-papers/cloud-computing-intel-cloud-2015-vision.pdf (A letöltés ideje: 2011. 12. 03.)

intergeneracio.hu (2011): *X, Y, Z: Generációk a világháló vonzásában.* www.intergeneracio.hu/2011/12/18/x-y-z-generaciok-a-vilaghalo-vonzasaban/ (A letöltés ideje: 2013. 02. 07.)

intermatrix.hu (2011): *Cloud – számítási felhő, az internet jövője?* http://intermatrix.hu/clouds (A letöltés ideje: 2011. 10. 04.)

Investopedia (s.d.): *ISP (Internet Service Provider).* www.investopedia.com/terms/i/isp.asp (A letöltés ideje: 2014. 07. 24.)

Jaeger, Paul T. – Lin, Jimmy – Grimes, Justin M. (2008): Cloud Computing and Information Policy: Computing in a Policy Cloud? *Journal of Information Technology & Politics,* Vol. 5, No. 3., 269–283.

Jamil, Danish – Zaki, Hassan (2011): Cloud Computing Security. *International Journal of Engineering Science and Technology,* Vol. 3, No. 4., 3478–3483. www.ijest.info/docs/IJEST11-03-04-129.pdf (A letöltés ideje: 2011. 11. 05.)

Jansen, Wayne – Grance, Timothy (2011): *Guidelines on Security and Privacy in Public Cloud Computing.* http://csrc.nist.gov/publications/nistpubs/800-144/SP800-144.pdf (A letöltés ideje: 2014. 09. 21.)

Katzan, Harry – Dowling, William A. (2010): Software-As-A-Service Economics. First Quarter, *Review of Business Information Systems,* Vol. 14, No. 1, 27–38. www.cluteinstitute.com/ojs/index.php/RBIS/article/view/500/487 (A letöltés ideje: 2015. 03. 02.)

Ketterling, Hans-Peter A. (2004): *Introduction to Digital Professional Mobile Radio.* Norwood: Artech House, 2004. https://books.google.hu/books?id=nZ5ISTkagOQC&pg=PA85&dq=nmt+450+modulation&hl=hu&sa=X&ved=0ahUKEwjPktaQuazPAhVI0xoKHY84APEQ6AEIVjAG#v=onepage&q=nmt%20450%20modulation&f=false (A letöltés ideje: 2016. 09. 25.)

kof.hu (s.d.): *Kormányzati Felhő.* http://kof.hu/informaciok (A letöltés ideje: 2017. 09. 02.)

Koi Tamás (2010): *Skype: az internet nem a mobilszolgáltatóké!* www.hwsw.hu/hirek/44435/voip-skype-mobil-internet-halozat-mobiltelefon.html (A letöltés ideje: 2013. 02. 09.)

Koi Tamás(2013): *Egyre nagyobb a nyomás Európában a Skype-on.* www.hwsw.hu/hirek/49958/skype-microsoft-franciaorszag-arcep-voip.html (A letöltés ideje: 2013. 06. 20.)

Koltay András – Mayer Annamária – Nyakas Levente – Pogácsás Anett (s.d.): *A médiaszolgáltatás és a sajtótermék fogalma az új magyar médiaszabályozásban.* Budapest: Nemzeti Média- és Hírközlési Hatóság http://mediatanacs.hu/dokumentum/1786/1321010932mediaszolgaltatas.pdf (A letöltés ideje: 2013. 10. 27.)

Kovács László (2011): Kiberháború? Internetes támadások a Wikileaks ellen és mellett. *Nemzet és Biztonság,* 1. sz., 3–8.

Kovács Zoltán (2011): Felhő alapú informatikai rendszerek potenciális alkalmazhatósága a rendvédelmi szerveknél. *Hadmérnök,* VI. évf. 4. sz., 176–188.

Kovács Zoltán (2012): Cloud Security in Terms of the Law Enforcement Agencies. *Hadmérnök,* VII. évf. 1. sz., 144–156.

Kovács Zoltán (2013a): „Electronic Written Tasking Order System" Accomplished Within the Project „Secure Electronic Communication" I. *Hadmérnök,* VIII. évf. 3. sz., 171–183.

Kovács Zoltán (2013b): „Electronic Written Tasking Order System" Accomplished Within the Project „Secure Electronic Communication" II. *Hadmérnök,* VIII. évf. 4. sz., 201–209.

Kovács Zoltán (2013c): Felhő alapú rendszerek törvényes ellenőrzési problémái. *Hadmérnök,* VIII. évf. 1. sz., 233–241.

Kovács Zoltán (2013d): Felhő alapú rendszerek törvényes ellenőrzési módszerei vizsgálata I. *Hadmérnök,* VIII. évf. 3. sz., 184–197.

Kovács Zoltán (2013e): Felhő alapú rendszerek törvényes ellenőrzési módszerei vizsgálata II. *Hadmérnök,* VIII. évf. 3. sz., 198–210.

Kovács Zoltán (2014): „Electronic Written Tasking Order System" Accomplished Within the Project „Secure Electronic Communication" III. *Hadmérnök,* IX. évf. 1. sz., 199–208.

Kovács Zoltán (2015): *Az infokommunikációs rendszerek nemzetbiztonsági kihívásai.* Budapest, Nemzeti Közszolgálati Egyetem Katonai Műszaki Doktori Iskola. (PhD-értekezés)

Kusnetzky, Dan (2009): *Fourth type of cloud computing.* www.zdnet.com/blog/virtualization/fourth-type-of-cloud-computing/1346 (A letöltés ideje: 2011. 10. 09.)

Kvint-R (s.d.): *Virtualizáció: VMWARE.* www.kvint-r.hu/termekek_szolgaltatasok/57/virtualizacio_vmware (A letöltés ideje: 2011. 10. 28.)

Le Monde (2008): *Cyberperquisitions.* www.lemonde.fr/idees/article/2008/02/28/cyberperquisitions_1016773_3232.html (A letöltés ideje: 2013. 06. 28.)

Lepenye Tamás (2011a): *Számítási felhő – egyszerűen.* http://lepenyet.wordpress.com/2011/06/15/szmtsi-felho-egyszeruen/ (A letöltés ideje: 2011. 10. 21.)

Lepenye Tamás (2011b): *Számítási felhő – egyszerűen (2. rész).* http://lepenyet.wordpress.com/2011/06/16/szmtsi-felho-egyszeruen-2-rsz/ (A letöltés ideje: 2011. 10. 21.)

Lepenye Tamás (2011c): *Számítási felhő – egyszerűen (3. rész).* http://lepenyet.wordpress.com/2011/06/17/szmtsi-felho-egyszeruen-3-rsz/ (A letöltés ideje: 2011. 10. 22.)

Lepenye Tamás (2011d): *A számítási felhők hatása az IT versenyhelyzetekre.* http://lepenyet.wordpress.com/2011/06/29/a-szmtsi-felhok-hatsa-az-it-versenyhelyzetekre/ (A letöltés ideje: 2011. 10. 23.)

lifewire (s.d.): *Internet Service Provider (ISP). What exactly does an internet service provider do?* http://compnetworking.about.com/od/internetaccessbestuses/g/bldef_isp.htm (A letöltés ideje: 2014. 07. 24.)

MacAskill, Ewen – Borger, Julian – Hopkins, Nick – Davies, Nick – Ball, James (2013a): *GCHQ taps fibre-optic cables for secret access to world's communications.* www.theguardian.com/uk/2013/jun/21/gchq-cables-secret-world-communications-nsa (A letöltés ideje: 2013. 07. 05.)

MacAskill, Ewen – Borger, Julian – Hopkins, Nick – Davies, Nick – Ball, James (2013b): *Mastering the internet: how GCHQ set out to spy on the world wide web.* www.theguardian.com/uk/2013/jun/21/gchq-mastering-the-internet (A letöltés ideje: 2013. 07. 05.)

Makk Attila (2009): *VMware a felhőkben.* http://computerworld.hu/vmware-a-felhokben.html (A letöltés ideje: 2011. 10. 28.)

Marquis-Boire, Morgan – Marczak, Bill – Guarnieri, Claudio – Scott-Railton, John (2013): *For their eyes only.* https://citizenlab.org/storage/finfisher/final/fortheireyesonly.pdf (A letöltés ideje: 2013. 06. 28.)

Marston, Sean R. – Li, Zhi – Bandyopadhyay, Subhajyoti – Ghalsasi, Anand – Zhang, Juheng (2010): Cloud Computing: The Business Perspective. *Decision Support Systems,* Vol. 51, No. 1., 176–189.

mccrindle.com.au (2012): *Generations Defined. McCrindle Research 2012.* http://mccrindle.com.au/resources/Generations-Defined-Sociologically.pdf (A letöltés ideje: 2013. 02. 09.)

McCullagh, Declan (2007): *FBI remotely installs spyware to trace bomb threat.* http://news.cnet.com/8301-10784_3-9746451-7.html (A letöltés ideje: 2013. 06. 28.)

Meister, Andre (2013): *Secret Government Document Reveals: German Federal Police Plans To Use Gamma FinFisher Spyware.* https://netzpolitik.org/2013/secret-government-document-reveals-german-federal-police-plans-to-use-gamma-finfisher-spyware/ (A letöltés ideje: 2013. 06. 28.)

Mell, Peter – Grance, Timothy (2009): *The NIST Definition of Cloud Computing Version 15.* www.nist.gov/itl/cloud/upload/cloud-def-v15.pdf (A letöltés ideje: 2011. 10. 21.)

Messmer, Ellen (2013): *US government's use of deep packet inspection raises serious privacy questions.* http://news.techworld.com/security/3444019/dhs-use-of-deep-packet-inspection-technology-in-new-net-security-system-raises-serious-privacy-questions/ (A letöltés ideje: 2013. 06. 28.)

Microsoft (2011): *Microsoft Officially Welcomes Skype.* http://news.microsoft.com/2011/10/13/microsoft-officially-welcomes-skype/ (A letöltés ideje: 2013. 06. 13.)

Microsoft (s.d.a): www.microsoft.com/hu-hu/office365/how-office365-works.aspx (A letöltés ideje: 2011. 10. 21.

Microsoft (s.d.b): www.microsoft.com/hun/virtualization/promise.mspx (A letöltés ideje: 2011. 10. 28.)

Microsoft (s.d.c): *Does Skype use encryption?* https://support.skype.com/en/faq/FA31/does-skype-use-encryption (A letöltés ideje: 2013. 07. 11.)

Microsoft (s.d.d): http://office.microsoft.com/hu-hu/business/ (A letöltés ideje: 2013. 10. 27.)

Molnár Gábor – Zalatnay Zsolt (s.d.): *Szolgáltatások és architektúrák.* Skype-előadás. www.tmit.bme.hu/dl239 (A letöltés ideje: 2013. 02. 13.)

Molnár Sándor – Perényi Marcell (2010): On the identification and analysis of Skype traffic. *International Journal of Communication Systems in Wiley Online Library,* No. 24., 94–117. http://hsnlab.tmit.bme.hu/~molnar/files/ijcs2010.pdf (A letöltés ideje: 2013. 06. 18.)

Muha Lajos (2008): Az informatikai biztonság egy lehetséges rendszertana. 2008. *Bolyai Szemle,* XVII. évf. 4. sz., 137–156.

Munk Sándor (2009): A kommunikáció fogalomrendszerének keretei az integrálódó információs technológiák korában. *In Kommunikáció 2009.* Budapest: ZMNE, 51–64.

Nakashima, Ellen (2013): *Panel seeks to fine tech companies for noncompliance with wiretap orders.* www.washingtonpost.com/world/national-security/proposal-seeks-to-fine-tech-companies-for-noncompliance-with-wiretap-orders/2013/04/28/29e7d9d8-a83c-11e2-b029-8fb7e977ef71_story.html (A letöltés ideje: 2013. 06. 28.)

Nakashima, Ellen (2016): *FBI paid professional hackers one-time fee to crack San Bernardino iPhone.* www.washingtonpost.com/world/national-security/fbi-paid-professional-hackers-one-time-fee-to-crack-san-bernardino-iphone/2016/04/12/5397814a-00de-11e6-9d36-33d198ea26c5_story.html (A letöltés ideje: 2016. 09. 25.)

napi.hu (s.d.): *Ezeket a szerencsejáték-oldalakat kapcsolta le a NAV.* www.napi.hu/ado/ezeket_a_szerencsejatek-oldalakat_kapcsolta_le_a_nav.583212.html (A letöltés ideje: 2014. 07. 01.)

Naugès, Louis (2009): *PRaaS, Process as a Service.* http://nauges.typepad.com/my_weblog/2009/08/praas-process-as-a-service.html (A letöltés ideje: 2011. 10. 22.)

nexon.hu (2011): *Felhő alapú hoszting szolgaltatás.* www.nexon.hu/felho-alapu-hoszting-szolgaltatas (A letöltés ideje: 2011. 10. 07.)

NIST (s.d.a): *NIST Cloud Computing Program.* www.nist.gov/itl/cloud/index.cfm (A letöltés ideje: 2011. 10. 21.)

NIST (s.d.b): *National Institute of Standards and Technology.* www.nist.gov/ (A letöltés ideje: 2014. 09. 21.)

NIST (s.d.c): *NIST Cloud Computing Related Publications.* www.nist.gov/itl/cloud/publications.cfm (A letöltés ideje: 2014. 09. 21.)

NIST (s.d.d): *Cryptographic Key Management Projekt.* http://csrc.nist.gov/groups/ST/key_mgmt/ (A letöltés ideje: 2015. 10. 15.)

NMHH (2008): *Elektronikus hírközlési szolgáltatások új hatósági osztályozása – lista.* Budapest: Nemzeti Média- és Hírközlési Hatóság, Nyilvántartási és Tájékoztatási Főosztály, Szolgáltatásbejelentési Osztály, 2012. http://nmhh.hu/dokumentum/448/szolgaltatas_hierarchia_20081009.pdf (A letöltés ideje: 2013. 02. 19.)

NMHH (2012): *Szolgáltatások osztályozása – fogalmak.* Budapest: Nemzeti Média- és Hírközlési Hatóság, Nyilvántartási és Tájékoztatási Főosztály, Szolgáltatásbejelentési Osztály http://nmhh.hu/dokumentum/447/szolgaltatas_leirasa.pdf (A letöltés ideje: 2013. 02. 19.)

Noyes, Dan (2017): *The Top 20 Valuable Facebook Statistics – Updated November 2017.* https://zephoria.com/top-15-valuable-facebook-statistics/ (A letöltés ideje: 2017. 12. 02.)

Origo (2011): *Az EU jóváhagyta a Microsoft Skype-felvásárlását.* www.origo.hu/techbazis/20111007-az-europai-bizottsag-jovahagyta-a-microsoft-skypefelvasarlasat.html (A letöltés ideje: 2013. 06. 17.)

Oroszi Eszter Diána (2008): *Social Engineering: Az emberi erőforrás, mint az információbiztonság kritikus tényezője.* Budapest: Budapesti Corvinus Egyetem Gazdálkodástudományi Kar Számítástudományi Tanszék, 2008. Diplomamunka. http://krasznay.hu/presentation/diploma_oroszi.pdf (A letöltés ideje: 2015. 07. 19.)

OTP (s.d.): *otpdirekt.* www.otpbank.hu/portal/hu/OTPdirekt/Home (A letöltés ideje: 2013. 10. 27.)

OWASP (2015): *Man-in-the-middle attack.* www.owasp.org/index.php/Man-in-the-middle_attack (A letöltés ideje: 2013. 07. 16.)

Oxford Dictionaries (s.d.a): *content provider.* www.oxforddictionaries.com/definition/american_english/content-provider (A letöltés ideje: 2013. 08. 16.

Oxford Dictionaries (s.d.b): *content provider.* www.oxforddictionaries.com/definition/english/content-provider (A letöltés ideje: 2013. 08. 16.)

PayPal (s.d.): *PayPal is for everyone who pays or gets paid.* www.paypal.com/hu/webapps/mpp/home (A letöltés ideje: 2013. 10. 27.)

PC-fórum (s.d.): *Szótár.* http://pcforum.hu/szotar/?term=Alkalmaz%E1s-szolg%E1ltat%F3 (A letöltés ideje: 2013. 08. 24.)

Poitras, Laura – Gellman, Barton (2013): *U.S., British intelligence mining data from nine U.S. Internet companies in broad secret program.* www.washingtonpost.com/investigations/us-intelligence-mining-data-from-nine-us-internet-companies-in-broad-secret-program/2013/06/06/3a0c0da8-cebf-11e2-8845-d970ccb04497_story.html (A letöltés ideje: 2013. 06. 28.)

politechbot.com (s.d.) www.politechbot.com/docs/fbi.cipav.sanders.affidavit.071607.pdf (A letöltés ideje: 2013. 06. 28.)

Preimesberger, Chris (2011): *Cloud Computing: Cloud Computing Security: 10 Ways to Enforce It.* www.eweek.com/c/a/Cloud-Computing/Cloud-Computing-Security-10-Ways-to-Enforce-It-292589/ (A letöltés ideje: 2011. 11. 05.)

PRNewswire (2017): *Global Tablet Market expected to reach US$ 596.61 Billion by 2026.* www.prnewswire.com/news-releases/global-tablet-market-expected-to-reach-us-59661-billion-by-2026-300462147.html (A letöltés ideje: 2017. 08. 17.)

rackspace.com (2012): *Virtualization is Not the Cloud.* www.rackspace.com/knowledge_center/whitepaper/virtualization-is-not-the-cloud (A letöltés ideje: 2015. 01. 10.)

Ristenpart, Thomas – Tromer, Eran – Shacham, Hovav – Savage, Stefan (2009): Hey, You, Get Off of My Cloud: Exploring Information Leakage in Third-Party Compute Clouds. In *CCS '09 Proceedings of the 16th ACM conference on Computer and communications security.* New York: ACM, 2009. 199–212. http://cseweb.ucsd.edu/~hovav/dist/cloudsec.pdf (A letöltés ideje: 2011. 11. 05.)

Romanski, Hilton (2014): *Cisco Announces Intent to Acquire Metacloud.* http://blogs.cisco.com/news/cisco-announces-intent-to-acquire-metacloud (A letöltés ideje: 2015. 01. 26.)

Rouse, Margaret (2006): *Spyware.* http://searchsecurity.techtarget.com/definition/spyware (A letöltés ideje: 2013. 07. 16.)

saasblogs.com (2009): *Demystifying the cloud where do SaaS paas and other acronyms fit in.* www.saasblogs.com/saas/demystifying-the-cloud-where-do-saas-paas-and-other-acronyms-fit-in/ (A letöltés ideje: 2011. 10. 29.)

Sallai Gyula – Abos Imre (2007): A távközlés, információ- és médiatechnológia konvergenciája. *Magyar Tudomány,* 168. évf. 1. sz., 844–851.

Sallai Gyula (2012): Defining Infocommunications and Related. *Acta Polytechnica Hungarica,* Vol. 9, No. 6., (2012), 5–15.

Sanders, Chris (2010a): *Understanding Man-in-the-Middle Attacks – ARP Cache Poisoning (Part 1).* www.windowsecurity.com/articles-tutorials/authentication_and_encryption/Understanding-Man-in-the-Middle-Attacks-ARP-Part1.html (A letöltés ideje: 2013. 07. 16.)

Sanders, Chris (2010b): *Understanding Man-In-The-Middle Attacks – Part2: DNS Spoofing.* www.windowsecurity.com/articles-tutorials/authentication_and_encryption/Understanding-Man-in-the-Middle-Attacks-ARP-Part2.html (A letöltés ideje: 2013. 07. 16).

Sanders, Chris (2010c): *Understanding Man-In-The-Middle Attacks – Part 3: Session Hijacking.* www.windowsecurity.com/articles-tutorials/authentication_and_encryption/Understanding-Man-in-the-Middle-Attacks-ARP-Part3.html (A letöltés ideje: 2013. 07. 16.)

Sanders, Chris (2010d): *Understanding Man-In-The-Middle Attacks – Part 4: SSL Hijacking.* www.windowsecurity.com/articles-tutorials/authentication_and_encryption/Understanding-Man-in-the-Middle-Attacks-ARP-Part4.html (A letöltés ideje: 2013. 07. 16.)

Schmidt, Jürgen (2013): *Skype's ominous link checking: Facts and speculation.* www.h-online.com/security/features/Skype-s-ominous-link-checking-Facts-and-speculation-1865629.html (A letöltés ideje: 2013. 06. 18.)

Securosis (2011): *Data Security Lifecycle 2.0.* https://securosis.com/blog/data-security-lifecycle-2.0 (A letöltés ideje: 2012. 01. 05.)

Sg.hu (2007): *Ausztriában törvényes lesz az online házkutatás.* http://sg.hu/cikkek/55658/ausztriaban_torvenyes_lesz_az_online_hazkutatas (A letöltés ideje: 2013. 06. 28.)

Sg.hu (2011): *Betilthatják Oroszországban a Skype-ot, a Gmailt és a Hotmailt.* http://sg.hu/cikkek/81250/betilthatjak_oroszorszagban_a_skype_ot_a_gmailt_es_a_hotmailt (A letöltés ideje: 2013.. 06. 18.)

Silver, Vernon (2013): *Cracking China's Skype Surveillance Software.* www.bloomberg.com/bw/articles/2013-03-08/skypes-been-hijacked-in-china-and-microsoft-is-o-dot-k-dot-with-it (A letöltés ideje: 2013. 06. 20).

Silverstone, Ariel (2009): *Clear Metrics for Cloud Security? Yes, Seriously.* www.csoonline.com/article/507823/clear-metrics-for-cloud-security-yes-seriously?page=1 (A letöltés ideje: 2012. 01. 02.)

Smith, Craig (2017a): *By the Numbers: 22 Staggering Dropbox Statistics (July 2017).* https://expandedramblings.com/index.php/dropbox-statistics/ (A letöltés ideje: 2017. 09. 02.)

Smith, Craig (2017b): *26 Amazing Skype Statistics and Facts (November 2017).* https://expandedramblings.com/index.php/skype-statistics/ (A letöltés ideje: 2017. 12. 02.)

Smith, David L. (2007): *How OTT Will Change Everything.* www.imediaconnection.com/content/15893.asp#multiview (A letöltés ideje: 2014. 06. 09.)

Solovjovs, Kirils (2013): *On Skype URL eavesdropping.* http://seclists.org/fulldisclosure/2013/May/78 (A letöltés ideje: 2013. 06. 18.)

SpywareGuide (2003): *Spyware.* www.spywareguide.com/term_show.php?id=12 (A letöltés ideje: 2013. 07. 16.)

Stamford, Conn (2016): *Gartner Says by 2020 "Cloud Shift" Will Affect More Than $1 Trillion in IT Spending.* www.gartner.com/newsroom/id/3384720 (A letöltés ideje: 2017. 12. 02.)

Stanford University (s.d.): *CS294S Research Project in Computer Security: Skype Proxy (IP over Skype).* Stanford: Stanford University, Applied Cryptography Group http://crypto.stanford.edu/cs294s/projects/skype.html (A letöltés ideje: 2013. 03. 26.)

Statista (2015): *Number of monthly active Facebook users worldwide from 3rd quarter 2008 to 3rd quarter 2014 (in millions).* www.statista.com/statistics/264810/number-of-monthly-active-facebook-users-worldwide/ (A letöltés ideje: 2015. 01. 11.)

Statista (2017a): *Number of smartphone users worldwide from 2014 to 2020 (in billions).* www.statista.com/statistics/330695/number-of-smartphone-users-worldwide/ (A letöltés ideje: 2017. 08. 17.)

Statista (2017b): *Shipment forecast of laptops, desktop PCs and tablets worldwide from 2010 to 2021 (in million units).* www.statista.com/statistics/272595/global-shipments-forecast-for-tablets-laptops-and-desktop-pcs/ (A letöltés ideje: 2017. 12. 02.)

Statista (2017c): *Worldwide mobile app revenues in 2015, 2016 and 2020 (in billion U.S. dollars).* www.statista.com/statistics/269025/worldwide-mobile-app-revenue-forecast/ (A letöltés ideje: 2017. 08. 17.)

Statista (2017d): *Most famous social network sites worldwide as of August 2017, ranked by number of active users (in millions).* www.statista.com/statistics/272014/global-social-networks-ranked-by-number-of-users/ (A letöltés ideje: 2017. 09. 02.)

Sullivan, Nick (2014): *How the NSA (may have) put a backdoor in RSA's cryptography: A technical primer.* http://arstechnica.com/security/2014/01/how-the-nsa-may-have-put-a-backdoor-in-rsas-cryptography-a-technical-primer/ (A letöltés ideje: 2016. 09. 27.)

Swisher, Kara (2011): *Done Deal: Microsoft to Buy Skype for $8.5 Billion in Cash.* http://allthingsd.com/20110510/done-deal-microsoft-to-buy-skype-for-8-5-billion-in-cash/ (A letöltés ideje: 2013. 06. 17.)

Tanenbaum, Andrew S. – Wetherall, David J. (2016): *Számítógép-hálózatok – Vezetékes átviteli közegek*. Digitális Tankönyvtár. www.tankonyvtar.hu/hu/tartalom/tamop412A/2011-0103_panem_szamhal/ch02s02.html (A letöltés ideje: 2017. 12 02.)

technopedia.com (s.d.): *Over-the-Top Application (OTT).* www.techopedia.com/definition/29145/over-the-top-application-ott (A letöltés ideje: 2014. 06. 09.)

techopedia.com (s.d.a): *Database as a Service (DBaaS).* www.techopedia.com/definition/29431/database-as-a-service-dbaas (A letöltés ideje: 2017. 08. 17.)

techopedia.com (s.d.b): *GovCloud.* www.techopedia.com/definition/28218/govcloud (A letöltés ideje: 2015. 01. 31.)

TechTarget (s.d.): *ISP (Internet service provider).* http://searchwindevelopment.techtarget.com/definition/ISP (A letöltés ideje: 2014. 07. 24.)

TechTerms (s.d.): *ASP.* www.techterms.com/definition/asp (A letöltés ideje: 2013. 08. 24.)

The H Security (2006): *Superintendent Trojan.* www.h-online.com/security/news/item/Superintendent-Trojan-731613.html (A letöltés ideje: 2013. 06. 28.)

The H Security (2013): S*kype with care – Microsoft is reading everything you write.* www.h-online.com/security/news/item/Skype-with-care-Microsoft-is -reading-everything-you-write-1862870.html (A letöltés ideje: 2013. 06. 18.)

The Washington Post (2013): *NSA slides explain the PRISM data-collection program.* www.washingtonpost.com/wp-srv/special/politics/prism-collection-do-cu ments/ (A letöltés ideje: 2013. 06 28.)

TheFreeDictionary (s.d.a): *content provider.* http://encyclopedia2.thefreedictionary.com/content+provider (A letöltés ideje: 2013. 08. 16.)

TheFreeDictionary (s.d.b): *Application Service Provider.* http://encyclopedia2.thefreedictionary.com/application+service+provider (A letöltés ideje: 2013. 08. 24.)

TrendMicro (2011): *Virtualization and Cloud Computing: Security Best Practice.* www.cio.in/whitepaper/virtualization-and-cloud-computing-security-best-practice (A letöltés ideje: 2011. 11. 05.)

TrendMicro (s.d.): *Virtualization and Cloud Computing: Security Threats To Evolving Data Centers.* http://us.trendmicro.com/imperia/md/content/us/trendwatch/researchandanalysis/final_cloud_virt_report.pdf (A letöltés ideje: 2011. 11. 05.)

tutorialspoint.com (s.d.): *Cloud Computing From the Home.* www.tutorialspoint.com/shorttutorials/cloud-computing-from-the-home (A letöltés ideje: 2015. 04. 05.)

ubuntu.hu (2011): *Az Ubuntu megváltoztatja a számítógép által nyújtott élményt.* http://ubuntu.hu/ubuntu1104/press (A letöltés ideje: 2011. 10. 22.)

Ulysses (2014): *Megszűnik az Ubuntu One szolgáltatás.* http://ubuntu.hu/node/37398 (A letöltés ideje: 2015. 01. 26.)

Vasvári György (2008): *Az IT virtualizáció. (Ajánlás 4.0)* infota.org/wp-content/uploads/2016/11/A_VIRTUALIZACIO_Ajanlas_4.doc (A letöltés ideje: 2011. 10. 28.)

visiongain.com (2016): T*he Mobile Cloud Computing Market Will Generate 45 Billion Dollars in Revenues by 2016. Says the Latest Visiongain Report.* www.visiongain.com/Press_Release/130/The-mobile-cloud-computing-market-will-generate-45-billion-dollars-in-revenues-by-2016-says-the-latest-visiongain-report (A letöltés ideje: 2015. 08. 01.)

Wang, Chenxi (2009): *Cloud Security Front And Center.* http://blogs.forrester.com/security_and_risk/2009/11/cloud-security-front-and-center.html (A letöltés ideje: 2011. 10. 23.)

Wawro, Alex (2012a): *A simple guide to Deep Packet Inspection.* http://features.techworld.com/security/3334780/a-simple-guide-to-deep-packet-inspection/ (A letöltés ideje: 2013. 06. 28.)

Wawro, Alex (2012b): *What Is Deep Packet Inspection?* www.pcworld.com/article/249137/what_is_deep_packet_inspection_.html (A letöltés ideje: 2013. 07. 19.)

windows.microsoft.com (s.d.): *Mentheti fájljait és fényképeit a OneDrive-ra, és bármilyen eszközről, bárhonnan hozzájuk férhet.* http://windows.microsoft.com/hu-HU/windows/cloud (A letöltés ideje: 2011. 10. 22.)

Woollaston, Victoria (2013): *Revealed, what happens in just ONE minute on the internet: 216,000 photos posted, 278,000 Tweets and 1.8 m Facebook likes.* www.dailymail.co.uk/sciencetech/article-2381188/Revealed-happens-just-ONE-minute-internet-216-000-photos-posted-278-000-Tweets-1-8m-Facebook-likes.html (A letöltés ideje: 2015. 03. 09.)

Yadron, Danny (2016): *Government keeping its method to crack San Bernardino iPhone 'classified'.* www.theguardian.com/technology/2016/mar/22/apple-fbi-san-bernardino-iphone-method-for-cracking (A letöltés ideje: 2016. 09. 25.)

Yigitbasioglu, Ogan M. – Mackenzie, Kim – Low, Rouhshi (2013): Cloud Computing: How does it differ from IT outsourcing and what are the implications for practice and research? *The International Journal of Digital Accounting Research,* Vol. 13 (2013), 99–121. www.uhu.es/ijdar/10.4192/1577-8517-v13_4.pdf (A letöltés ideje: 2015. 03. 02.)

Zetter, Kim (2012): *Secret Code Found in Juniper's Firewalls Shows Risk of Government Backdoors.* www.wired.com/2015/12/juniper-networks-hidden-backdoors-show-the-risk-of-government-backdoors/ (A letöltés ideje: 2016. 09. 27.)

Zuckerberg, Mark (2012): *Zuckerberg's post.* www.facebook.com/zuck/posts/10100518568346671 (A letöltés ideje: 2013. 02. 15.)

Jogszabályok és hivatalos dokumentumok

180/2004. (V. 26.) Korm. rendelet az elektronikus hírközlési feladatokat ellátó szervezetek és a titkos információgyűjtésre, illetve titkos adatszerzésre felhatalmazott szervezetek együttműködésének rendjéről.

185/2016. (VII. 13.) Korm. rendelet a titkosított kommunikációt biztosító alkalmazásszolgáltatók és a titkos információgyűjtésre feljogosított szervezetek együttműködésének rendjéről.

1994. évi XXXIV. törvény a Rendőrségről.

1995. évi CXXV. törvény a nemzetbiztonsági szolgálatokról.

1998. évi XIX. törvény a büntetőeljárásról.

2001. évi CVIII. törvény az elektronikus kereskedelmi szolgáltatások, valamint az információs társadalommal összefüggő szolgáltatások egyes kérdéseiről.

2003. évi C. törvény az elektronikus hírközlésről.

2010. évi CIV. törvény a sajtószabadságról és a médiatartalmak alapvető szabályairól.

2010. évi CLXXXV. törvény a médiaszolgáltatásokról és a tömegkommunikációról.

2010. évi CXXII. törvény a Nemzeti Adó- és Vámhivatalról. http://net.jogtar.hu/jr/gen/hjegy_doc.cgi?docid=A1000122.TV (A letöltés ideje: 2013. 07. 01.)

2011. évi CLXIII. törvény az ügyészségről.

2014. évi (T/264) törvény az egyes pénzügyi tárgyú törvények módosításáról. (javaslat)

2014. évi XXXIII. törvény az egyes pénzügyi tárgyú törvények módosításáról.

2016. évi LXIX. törvény a terrorizmus elleni fellépéssel összefüggő egyes törvények módosításáról.

Az Európai Parlament és a Tanács (EU) 2016/1148 irányelve (2016. július 6.) a hálózati és információs rendszerek biztonságának az egész Unióban egységesen magas szintjét biztosító intézkedésekről.

Bundesministerium des Finanzen (2012): *Bericht zur Nr. 10 des Beschlusses des Haushaltsausschusses des Deutschen Bundestages zu TOP 20 der 74. Sitzung am 10. November 2011.*

Federal Office for Information Security (2011): *White Paper. Security Recommendations for Cloud Computing Providers. (Minimum information security requirements).* Bonn: FOIS.

Federal Office for Information Security (2013): *Cross Reference Table threats and safeguards for module cloud management.* Bonn: FOIS.

Federal Office for Information Security (s.d.): *Taking advantage of opportunities – avoiding risks.* Bonn: FOIS.

GOV.UK (2013): *Guidance – G-Cloud service definitions.* www.gov.uk/government/publications/g-cloud-service-definitions (A letöltés ideje: 2015. 01. 31.)

Közigazgatás Informatikai Bizottság (2009): *E-önkormányzati stratégiakészítési ajánlás kistérségek és önkormányzatok számára. változat: v1.1.* https://ugyintezes.magyarorszag.hu/srv/letolt?id=47416978&lang=hu (A letöltés ideje: 2013. 08. 24.)

MTE (2009): *Magyarországi Tartalomszolgáltatók Egyesületének a tartalomszolgáltatásra vonatkozó működési, etikai és eljárási szabályzata.* http://mte.hu/etikai-kodex/ (A letöltés ideje: 2013. 08. 16.)

T/12250. számú törvényjavaslat egyes törvényeknek a tiltott szerencsejáték megakadályozásával összefüggő módosításáról. www.parlament.hu/irom40/12250/12250.pdf (A letöltés ideje: 2016. 09. 27.)

T/264. számú törvényjavaslat egyes pénzügyi tárgyú törvények módosításáról. www.parlament.hu/irom40/00264/00264.pdf (A letöltés ideje: 2014. 07. 01.)

The IP Commission (2013): *The IP commission report*. www.ipcommission.org/report/ip_commission_report_052213.pdf (A letöltés ideje: 2013. 06. 28.)

Ábrák jegyzéke

Táblázatok jegyzéke

Fogalomtár és rövidítések jegyzéke

5G	5th generation mobile networks or 5th generation wireless systems	5. generációs mobil távközlési hálózat
AAA	authentication, authorization, and accounting	hitelesítés, engedélyezés, hozzáférés-kezelés
API	application programming interface	alkalmazásprogramozási felület. Az API segítségével lehetséges egy programrendszer szolgáltatásait használni anélkül, hogy annak belső működését ismerni kellene.
ARCEP	Autorité de régulation des communications électroniques et des postes (angolul French Electronic communications and postal regulatory authority)	Francia Elektronikus Hírközlési és Postai Szabályozó Hatóság
AWS	Amazon Web Services Black-holing	Amazon webszolgáltatások hálózati be- és kimenő forgalom eldobása anélkül, hogy a forrás értesülne arról, hogy az adatok nem érték el a címzettet
BSI	Bundesamtes für Sicherheit in der Informationstechnik (angolul Federal Office for Information Security)	Német Szövetségi Információbiztonsági Hivatal
BT	Bluetooth	rövid hatótávolságú vezeték nélküli adatcseréhez használt szabvány
BYOD	Bring Your Own Device	„Hozd a saját eszközöd”

CERT	Computer Emergency Readiness Team	számítástechnikai katasztrófaelhárító csoport
CSA	Cloud Security Alliance	felhőalapú rendszerek biztonságával foglalkozó, iparági szakemberek, vállalatok és más érintettek széles koalíciója által vezetett nonprofit szervezet
DoS	Denial of Service	szolgáltatásmegtagadással járó támadás vagy más néven túlterheléses támadás
DDoS	Distributed Denial of Service	elosztott szolgáltatásmegtagadással járó támadás vagy más néven elosztott túlterheléses támadás
DPI	Deep Packet Inspection	mély csomagelemzés
ENISA	European Union Agency for Network and Information Security (eredeti nevén European Network and Information Security Agency)	Európai Hálózat- és Információbiztonsági Ügynökség
ESI	Electronically Stored Information	elektronikusan tárolt információk
ETSI	European Telecommunications Standards Institute	Európai Távközlési Szabvány Intézet
FedRAMP	Federal Risk and Authorization Management Program	Szövetségi Kockázat- és Jogosultságkezelési Program, az Egyesült Államok kormánya által létrehívott felhőbiztonsági program
FSZB	Федеральная служба безопасности Российской Федерации (angolul Federal Security Service of the Russian Federation)	Orosz Szövetségi Biztonsági Szolgálat
gov-Cloud	governmental Cloud computing	kormányzati felhő

HTTPS	Secure Hypertext Transfer Protocol,	egy biztonságos információátviteli protokoll elosztott információs rendszerekhez
IaaS	Cloud Infrastructure as a Service	infrastruktúra mint szolgáltatás
IAM	Identity and Access Management	azonosítás és hozzáférés-kezelés
ICT	Information and Communications Technology	információ- és kommunikációtechnológia vagy infokommunikációs technológia
IDS/IPS	Intrusion Detection System/Intrusion Prevention Systems	behatolásérzékelő és -védelmi rendszerek
IoT	internet of things	a dolgok internete, amely olyan hálózatba kötött intelligens eszközöket takar, amelyek képesek felismerni bizonyos lényegi információkat és azokat internetalapú hálózaton másik eszközök felé kommunikálni
IP	Internet Protocol	internetprotokoll: csomagkapcsolt átvitelt megvalósító hálózatiréteg-protokoll
IPTV	Internet Protocol Television	Az internetprotokoll segítségével általában széles sávú interneten keresztül nyújtott digitális televíziós műsorszolgáltatás
IT	Information technology	információtechnológia vagy informatika
ITIL	Information Technology Infrastructure Library	informatikai rendszerek üzemeltetésére és fejlesztésére szolgáló módszertan, illetve ajánlásgyűjtemény
ITU	International Telecommunication Union	Nemzetközi Távközlési Egyesület
KAK	–	Kormányzati Adatközpont
KOF	–	Kormányzati Felhő
LMaaS	Lawful Monitoring as a Service	törvényes ellenőrzés mint szolgáltatás

LTE	Long Term Evolution,	egy negyedik generációs mobil adatátviteli szabvány
MAC	Mandatory Access Control	kötelező hozzáférés-védelem
MitM	Man in the Middle	közbeékelődéses támadás
NAV		Nemzeti Adó- és Vámhivatal
NIST	National Institute of Standards and Technology	az Egyesült Államok legrégibb fizikai kutatólaboratóriuma
NSA	National Security Agency	Nemzetbiztonsági Ügynökség (Egyesült Államok)
NVSZ		Nemzeti Védelmi Szolgálat
OSINT.	Open Source Intelligence	nyílt forrású információgyűjtés
OTT	Over-the-Top	az interneten mint mások által biztosított közegen nyújtott szolgáltatások, tartalmak, amelyekre az internetszolgáltatónak nincs befolyása
PaaS	Cloud Platform as a Service	platform mint szolgáltatás
PIN	Personal Identification Number	magyarul személyi azonosítószám, egy számjegyekből álló kód, amellyel általában különféle személyes jellegű adatokat, szolgáltatásokat védenek
RBAC	Role-based access control	szabályalapú hozzáférés-kezelés
PC	Public cloud	nyilvános számítási felhő
PC/SaaS	Public cloud/Software as a Service	nyilvános számítási felhő/szoftver mint szolgáltatás
RPO	recovery point objective	visszaállítási időpont
RTO	recovery time objective	visszaállítási időtartam
SAML	Security Assertion Markup Language	XML-alapú, nyílt szabványú adatformátum hitelesítési és jogosultságkezelési eljárásokhoz
SaaS	Cloud Software as a Service	szoftver mint szolgáltatás
SIEM	Security information and event management	Biztonsági információs és eseménykezelő (szoftver) rendszer
SLA	service level agreement	szolgáltatási megállapodás
SLM	service level management	szolgáltatásszint-menedzsment

SLR	service level requirement	szolgáltatásminőségi követelmény
SSO	single sign-on	egyszeres bejelentkezés, amely után a rendszer minden erőforrásához és szolgáltatásához további hitelesítés nélkül hozzá lehet férni
TLS	Transport Layer Security	kliens-/szerveralapú alkalmazások számára készített, biztonságos kommunikációt biztosító protokoll
TSCM	Technical Surveillance Countermeasures	technikai elhárítás
VoIP	Voice over IP	internetprotokoll-alapú hangátvitel
WiFi		vezeték nélküli helyi hálózat (WLAN) kialakítására szolgáló, széles körben elterjedt szabvány (IEEE 802.11
WLAN	wireless local area network	vezeték nélküli helyi hálózat
XACML	eXtensible Access Control Markup Language	hozzáférés-szabályozáshoz használt nyelv
XML	eXtensible Markup Language	általános célú leíró nyelv elektronikus dokumentumok strukturálásához

Kiadja a Nemzeti Közszolgálati Egyetem
Ludovika Egyetemi Kiadó Iroda
Székhely: 1089 Budapest, Orczy út 1.
Kapcsolat: info@ludovika.hu

A kiadásért felel: Koltay András rektor
Felelős szerkesztő: Karácsony Fanni
Olvasószerkesztő: Simann Karola
Korrektor: Szarvas Melinda
Tördelőszerkesztő: Fehér Angéla

ISBN 978-963-531-065-4 (PDF)
ISBN 978-963-531-066-1 (ePub)

Az elmúlt évtizedekben az infokommunikációs rendszerek rohamosan fejlődtek, és úgy tűnik, ennek lendületét még a gazdasági válságok sem képesek megtörni. Különösen igaz ez a felhőalapú rendszerekre, amelyekre ma úgy tekinthetünk, mint az infokommunikációs rendszerek fejlődésének egyik mozgatórugójára. Mindez a nemzetbiztonsági és a rendvédelmi szerveket kettős kihívás elé állítja. Egyrészről az új technológiák egy részét igénybe fogják venni, így felhasználóként garantálni kell a megfelelő biztonságot. Másrészről az újfajta rendszerek ellenőrzése újfajta gondolkodásmódot és újfajta megoldásokat igényel technikai, jogi, valamint adminisztratív oldalról a jogalkotóktól, az érintett nemzetbiztonsági, továbbá rendvédelmi szervektől, illetve a szolgáltatóktól egyaránt.

A fentiek alapján a monográfia célja is kettős. Egyfelől felhasználói, másfelől törvényes ellenőrzési szempontból megvizsgálni a korszerű infokommunikációs rendszerek közül az internettechnológiára épülő szolgáltatásokat, azon belül pedig kiemelten a felhőalapú rendszereket.

A kiadvány a KÖFOP-2.1.2-VEKOP-15-2016-00001
„A jó kormányzást megalapozó közszolgálat-fejlesztés”
című projekt keretében jelent meg.