DOI azonosító: 10.17625/NKE.2015.021

- 2015 -

NEMZETI KÖZSZOLGÁLATI EGYETEM
KATONAI MŰSZAKI DOKTORI ISKOLA

Kovács Zoltán

Az infokommunikációs rendszerek nemzetbiztonsági kihívásai

Doktori (PhD) Értekezés

Témavezető:
Prof. Dr. Kovács László ezredes (PhD)
egyetemi tanár

BUDAPEST, 2015.

DOI azonosító: 10.17625/NKE.2015.021

Tartalomjegyzék

DOI azonosító: 10.17625/NKE.2015.021

DOI azonosító: 10.17625/NKE.2015.021

DOI azonosító: 10.17625/NKE.2015.021

DOI azonosító: 10.17625/NKE.2015.021

Bevezetés

Az elmúlt évtizedekben az infokommunikációs rendszerek rohamosan fejlődtek, és úgy tűnik, hogy ennek lendületét még a gazdasági válságok sem képesek megtörni. A mobil kommunikációs rendszerek és az internet világméretű elterjedése, a rendelkezésünkre álló adatátviteli sávszélesség folyamatos növekedése, és a felhasználási lehetőségek gyarapodása azt eredményezte, hogy mára a gyors és nagy tömegű adatcsere életünk szerves részévé vált. Az elterjedt technológiák alkalmazásával olcsón, gyorsan és hatékonyan vagyunk képesek ellátni munkahelyi feladatainkat és 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, a rézkábelek folyamatos kiváltása üvegszálakra az egyéni felhasználóknál, vagy a(z IP[2] alapú, sokszor ingyenes) kommunikációt lehetővé tévő alkalmazások gyors terjedése (pl. Facebook, Skype, Viber stb.), akkor egyértelműen kijelenthető, hogy az említett tendencia a következő években, évtizedekben is folytatódni fog. Különösen igaz ez a felhő alapú rendszerekre, amelyekre ma úgy tekinthetünk, mint az infokommunikációs rendszerek fejlődésének egyik meghatározó mozgatórugójára. Ezek előnyei ugyanis minden szereplő számára kézzel foghatóak, hogy csak az egyik legfontosabbat említsem, 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, az pedig egyre jelentősebb fejlesztésre sarkallja a gyártókat, szolgáltatókat.

A tudományos probléma

Napjaink két, az infokommunikációt jelentősen meghatározó trendje a felhő alapú rendszerek előretörése, valamint a mobil eszközök és az azokon futó alkalmazások piaci részesedésének a 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 felhő alapú rendszereket veszünk igénybe, akár munkánkhoz, akár magánéletünk elintézendő dolgaihoz.

A felhő alapú rendszerek robbanásszerű növekedését már az évtized elején, az iparág

[1] LTE: Long Term Evolution (tükörfordításban hosszú távú fejlődés) rövidítése, amely egy negyedik generációs mobil adatátviteli szabvány.
[2] IP: Internet Protocol (Internet Protokoll) csomagkapcsolt átvitelt megvalósító hálózati réteg protokoll.

DOI azonosító: 10.17625/NKE.2015.021

kilátásairól közzétett prognózisok előrevetítették. A Visiongain 2011-ben elvégzett kutatása a felhő alapú rendszerek az évi 77 milliárd US dolláros piacának 2016-ra 240 milliárd US dollárra történő növekedését jósolta, [1] a Gartner ugyanebben az esztendőben adott előrejelzése szerint pedig 2016 év végére a világ 1000 legjelentősebb vállalatának több mint a fele fogja érzékeny ügyféladatait is nyilvános felhőben tárolni. [2] Mára az előrejelzéseik helyességét olyan adatok támasztják alá, mint például a Microsoft negyedéves jelentései, amelyekben rendre a felhős szolgáltatásaik ugrásszerű növekedését mutatták be. 2014-re ugyanis már sorozatban a második évben sikerült megduplázniuk a kereskedelmi felhőből származó bevételeiket, így az elmúlt év végére 4,4 milliárd dollárnál álltak ebben az üzletágban. [3] De hasonló növekedésről számolt be az SAP is, ahol 2015. júliusi adatok szerint a 20 %-os bevételnövekedésük jelentős részét éppen a felhő alapú szolgáltatásoknak köszönhetik. Ez utóbbi ugyanis az előző év azonos időszakához képest 129 %-os növekedést produkálva 555 millió euró bevételt hozott a német cégnek. [4] 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 internetelérással, amelyből 53 %-uk, közel 2 milliárd ember, felhő alapú tárolóhelyet (is) igénybe fog venni. [5]

A mobil eszközök és a rájuk írt alkalmazások elterjedése kapcsán hasonló növekedést tapasztalhatunk és várhatunk. Az Emarketer 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. [6] A táblagépek eladása, ha lassuló mértékben is, de szintén tovább növekszik. Csak az Egyesült Államokban a 2010-ben 10,8 millió, 2014-ben pedig már 53,2 millió darabot adtak el belőlük, 2016-ra pedig 60,3 millió darab eladását várják a szakemberek. [7] De nem csak a hordozható eszközök, hanem a rájuk írt alkalmazások esetében is jelentős a növekedés. Egy átlagos amerikai felhasználó ma 8,8 alkalmazást tölt le havonta, a mobil alkalmazásokat áruló boltok bevétele pedig a 2011-es 8,32 milliárd US dollárról 2017-re várhatóan 76,52 milliárdra emelkedik. [8]

Ebben a szegmensben a magyarországi felmérések is hasonló tendenciákat mutatnak. Az eNet felmérései szerint már 2013-ban 2,4 millió okostelefonja volt a 18 éven felüli lakosságnak, [9] 2014 januárjában az internetezők 21 %-a táblagépet is használt, 26 %-uk tervezte annak megvételét, [10] és 2015 januárjára már az okostelefon felhasználók 62 %-a rendelkezett internetelérással is a készülékén. [11] Ráadásul ezek fő felhasználói a fiatalabb korosztály

DOI azonosító: 10.17625/NKE.2015.021

tagjai, akiknél az internethasználat kapcsán jellemző, hogy a közösségi oldalak felhasználása abszolút domináns, de az online tartalomfogyasztás is már messze megelőzi a hagyományos (TV, rádió, újság) médiumokon keresztülit. [12]

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 ezeknek a szerveknek az új technológiák esetében is meg kell oldani a hatáskörükbe tartozó törvényes ellenőrzést.**

A kettős kihívás kettős problémát is jelent. Az első, felhasználóként a megfelelő biztonság garantálása, amely két nagy szegmensre bontható.

Szervezeti felhasználóként a nemzetbiztonsági és a rendvédelmi szerveknek meg kell győződnie 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 magukban hordozzák azokat a hibákat, hibalehetőségeket, amelyek kihasználásával sérülhet az adatok bizalmassága, sértetlensége, rendelkezésre állása. Ám nem csak a véletlen hibákkal, hanem például a szándékosan beépített hátsó kapukkal, vagy akár ellenérdekelt felek, de akár a szolgáltató általi információgyűjtésre, adatszerzésre irányuló törekvésekkel is számolni kell is.

A biztonságot ugyanakkor nem csak a szervezetszerű felhasználáskor, hanem – megfelelő mértékben – a szolgálatok által információbiztonsági szempontból védett állami, kormányzati szervek vezetői által használt eszközök, rendszerek esetében is vizsgálni, a biztonsági résekből adódó hiányosságokat tudatosítani, a biztonságos használathoz szükséges tudnivalókat pedig oktatni kell. Erre azért van szükség, mert jellemzően ezek a vezetők szívesen használnak új, sok esetben prémium kategóriás készülékeket (pl. okostelefon, táblagép), ezekkel pedig internet technológiára épülő szolgáltatásokat, ráadásul mindezt vegyes, hivatali és magánhasználatban. Ezek tiltását, korlátozását ma jellemzően ezek a vezetők nehezen, vagy egyáltalán nem fogadják el, akárcsak a biztonságot fokozó, de a használhatóságot korlátozó szoftver és/vagy hardver elemek használatát. Ugyanakkor esetükben az információbiztonság – hangsúlyozottan első lépésként (!) – már jelentős mértékben emelhető az említett eszközök és szolgáltatások biztonságtudatos használatával,

DOI azonosító: 10.17625/NKE.2015.021

amelyre azonban az említett vezetőket fel kell készíteni.

Jelenleg azonban nem létezik olyan egységes ajánlás, amely megmutatja, hogy milyen kritériumokat kell vagy célszerű megvizsgálni egy teljes körű biztonsági elemzéshez felhő alapú rendszer szervezeti szintű felhasználása esetén, mint ahogy nincs egységes ajánlás arra nézve sem, hogy mit kell vagy célszerű oktatni a kiemelt, védett vezetőknek egy információbiztonság-tudatossági felkészítés keretében.

Törvényes ellenőrzést végzőként más problémák merülnek fel. Az új technológiák megjelenése magával hozza a régiek, például hagyományos telefónia leértékelődését, az újak felértékelődését a célszemélyek, és ez által 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 igényelnek technikai, jogi és adminisztratív oldalról a jogalkotóktól, az érintett nemzetbiztonsági és rendvédelmi szervektől, valamint a szolgáltatóktól egyaránt.

Jelenleg azonban nem található olyan összehasonlító elemzés, amely a szolgálatokat segítendő bemutatná az új technológiák törvényes ellenőrzésére jelenleg alkalmas technikai módszereket, összehasonlítaná azokat előnyeikkel, hátrányaikkal együtt, mitahogy nem található olyan egységes szempontrendszer sem, amellyel akár egy már megévő, akár egy új módszer adott feladatra alkalmassága megvizsgálható. Hiányként merül fel továbbá, hogy jogszabályba illeszthető fogalmi meghatározása csupán a hagyományos hírközlési szolgáltatóknak van, az új tipusú, újonnan megjelent szolgáltatóknak viszont nincs, és ez ma már jelentősen akadályozza a hatékony törvényes ellenőrzést.

Kutatási célkitűzések

A fentiek alapján kutatásom célja is kettős. Egyfelől felhasználói, másfelől törvényes ellenőrzési szempontból vizsgálom meg a korszerű infokommunikációs rendszerek közül az internet-technológiára épülő szolgáltatásokat, azon belül pedig kiemelten a **felhő alapú rendszereket.**

Felhasználói szempontból két fő célom van. Egyrészt egy olyan biztonsági követelményrendszer megalkotása, amellyel az említett rendszerek, kiemelten a **felhő alapú rendszerek vizsgálhatóak**, azok használatának, alkalmazásának kockázatai felmérhetőek, másrészt pedig ezen rendszerek használatához kapcsolódóan egy lehetséges biztonságtudatossági felkészítés tartalmi elemeinek kidolgozása védett vezetők számára.

DOI azonosító: 10.17625/NKE.2015.021

Törvényes ellenőrzési szempontból pedig célom egy olyan keretrendszer felállítása, amely megmutatja az említett rendszerek törvényes ellenőrzésének lehetőségeit, azok előnyeit, hátrányait, kockázatait, és ajánlásokat fogalmaz meg kialakításukkal, kialakíthatóságukkal kapcsolatban, valamint – akár jogszabályba illeszthető módon – fogalmi meghatározást ad az újonnan megjelent szolgáltatókra.

Ezek tudományos jelentősége az, hogy az említett rendszerek biztonságának számos területe kevéssé, vagy még egyáltalán nem kidolgozott. Az újonnan megjelenő technológiákat sok esetben úgy kínálják használatra a szolgáltatók, az ügyfelek pedig már úgy veszik igénybe azokat, hogy sok esetben az alapvető biztonsági kérdéseket nem vizsgálták, a törvényes ellenőrzés pedig nem biztosított. Jelenleg a nemzetbiztonsági és rendvédelmi szervek részére nem áll rendelkezésre egy olyan, a gyakorlatban is hasznosítható eljárásrend, amelynek segítségével az említett rendszerek biztonsága egységesen vizsgálható, mérhető, és egy olyan egységes keretrendszer, amely bemutatná a törvényes ellenőrzés lehetőségeit.

Céljaimat a fejlett országok nemzeti és nemzetközi szervezetei által megalkotott elérhető ajánlások, az iparági szabványok és bevált gyakorlatok, valamint a törvényes ellenőrzésről nyiltan rendelkezésre álló információk felhasználásával és továbbfejlesztésével, valamint a nemzetbiztonsági és rendvédelmi szervek igényeihez történő hozzáigazításával kívánom elérni. A kutatási területek kiválasztásánál azokra a részfeladatokra koncentrálok, melyek világszerte kidolgozatlan és megoldatlan problémaként jelentkeznek a nemzetbiztonsági és a rendvédelmi szervek számára.

Kutatásommal hozzá kívánok járulni egyrészt a nemzetbiztonsági és a rendvédelmi szervek és az általuk védett állami, kormányzati vezetők által használt információk továbbítására szolgáló rendszereken és alkalmazásokon folyó kommunikáció védelmi szintjének, másrészt a releváns infokommunikációs rendszerek törvényes ellenőrzése hatékonyságának emeléséhez.

A kutatási célkitűzéseimet a következő részcélokra bontott kutatómunkával valósítom meg:

1. **A felhő alapú rendszerek biztonsági vizsgálatához szükséges követelményrendszer megalkotása**

   A fejlett országok érintett nemzeti-, és a nemzetközi szervezetei által megalkotott, elérhető biztonsági ajánlásainak tanulmányozása és összehasonlítása adhat alapot arra, hogy a kialakítható legyen egy követelményrendszer, amely lehetővé teszi az infokommunikációs rendszerek egységes és teljes körű vizsgálatát. Jelenleg nyilvánosan nem érhető el olyan összehasonlító tanulmány, amely erre a területre vonatkozna. Kutatómunkám során az elérhető ajánlások, valamint az iparági szabványok és bevált gyakorlatok felhasználásával, továbbgondolásával és –

DOI azonosító: 10.17625/NKE.2015.021

fejlesztésével, valamint azok magyarországi (elsősorban jogi) viszonyokra, valamint a rendvédelmi szervek sajátosságaira szabásával felállítok egy olyan szempontrendszert, amellyel a probléma teljes körűen vizsgálható, majd megalkotok egy olyan követelményrendszert, amellyel a címben szereplő rendszerek alapvető biztonsági elemzése egységes keretek között végrehajtható. Egy ilyen, bármely nemzetbiztonsági vagy rendvédelmi szerv által szabadon elérhető és felhasználható „biztonsági elemző sablon" véleményem szerint hiánypótló.

2. **Információbiztonsági felkészítés tartalmi elemeinek kidolgozása védett vezetők számára**

   A védett vezetők ellen irányuló támadások elhárítását nem csak fizikailag, hanem információvédelem szempontjából is próbálják garantálni az érintett szervek. Ugyanakkor ma már nem elégséges az iroda, lakás, autó stb. „poloskátlanítása", hiszen sokkal könnyebben és kockázatmentesebben lehet információhoz jutni pl. egy postafiók feltörésével, vagy egy iPadbe történő bejutással. A védett személyek által is használt rengeteg infokommunikációs eszköz és szolgáltatás számos biztonsági kockázatot rejt, amelyet megfelelő információbiztonság-tudatossági képzéssel jelentősen csökkentetni lehet. Ugyanakkor jelenleg nem létezik olyan tematika, amely egységes keretben, komplett leírást adna arról, hogyan is kell(ene) a védett vezetőket felkészíteni arra, hogy normál kommunikációs szokásaikkal ne okozzanak nemzetbiztonsági kockázatot. Ezt az infokommunikációs rendszerek biztonsági vizsgálatával és a védett vezetők speciális helyzetének figyelembevételével felállított keretrendszer felhasználásával alakítom ki.

3. **Az internet-technológiára épülő szolgáltatások törvényes ellenőrzési lehetőségei elvi kialakítása, előírásainak megfogalmazása**

   Az információk továbbítására szolgáló rendszereken és alkalmazásokon folyó kommunikáció és azok kísérőadatainak törvényes ellenőrzése feladataik okán alapvető érdeke minden rendvédelmi és nemzetbiztonsági szervnek. A technológiák sokszínűsége és az egyes országok törvényeinek eltérő volta miatt ennek elvégzésére számos megoldás létezik, de sok problémával is küzdenek az érintett szervek. Jelenleg nem létezik olyan elemzés, amely jogi és technikai összefüggésében bemutatná ezeket az ellenőrzési lehetőségeket, leírva előnyeiket, hátrányaikat, korlátaikat, kockázataikat.

   A jelenleg hatályos, törvényes ellenőrzést lehetővé tevő jogszabályok – megalkotásuk ideje okán – alapvetően a hang alapú kommunikációt biztosító telefóniára koncentrálnak. A mai, kommunikációt biztosító technológiákra ezek nem, vagy csak

DOI azonosító: 10.17625/NKE.2015.021

nagy nehézségekkel értelmezhetők, húzhatók rá. Ugyanakkor a technológiai változás nem csak jogi, hanem technikai problémákat is okoz a törvényes ellenőrzés során. Ma már az elsődlegesen érintett szereplők (nemzetbiztonsági és rendvédelmi szervek, szolgáltatók) találkoztak ezekkel a gondokkal, és várhatóan a közeljövőben a törvényalkotók is szembesülnek vele. Jelenleg nem létezik olyan egységes keretrendszer, amely összefoglalja a törvényes ellenőrzés lehetőségeit, jogi és technikai ajánlásokat tesz annak teljes körű kialakításához, és végeredményeként – akár jogszabályba illeszthető módon – ajánlásokat tesz.

Kutatómunkám során ezeket alkotom meg, kidolgozok egy, a törvényes ellenőrző módszerek vizsgálatához általánosan használható szempontrendszert, felállítom a jelenlegi hírközlési modellt potenciálisan felváltó új modellt, valamint ajánlást teszek az újonnan megjelent szolgáltatók olyan fogalmi meghatározása, amelyek beilleszthetőek a törvényes ellenőrzésről szóló jogszabályokba.

Az értekezés felépítése

A fentieknek megfelelően az értekezésemet az alábbi négy fejezet szerint építem fel:

Az **első fejezet**ben a felhő alapú rendszerek értelmezésével foglalkozom, szolgáltatási -, és telepítési modellek szerint csoportosítva megvizsgálom azok tulajdonságait, előnyeit, hátrányait. Elemzem, hogy mi a különbség a felhő alapú rendszerek és a virtualizáció, a kiszervezés, valamint az internet-technológiára épülő szolgáltatások között. Megvizsgálom, hogy ma értelmezhető-e a kormányzati és a rendvédelmi felhő fogalma, valamint bemutatom, hogy a nemzetbiztonsági szolgálatoknak és a rendvédelmi szerveknek érdemes és kell is foglalkozniuk a felhő alapú rendszerekkel.

A **második fejezet**ben nemzetbiztonsági szolgálatok és a rendvédelmi szervek szempontjából elemzem és értékelem a felhő alapú rendszerekkel foglalkozó nemzeti és nemzetközi szervezetei által megalkotott, nyíltan elérhető, a dolgozat célkitűzése szempontjából releváns biztonsági ajánlásokat, majd felállítok egy, az említett rendszerek komplex vizsgálatához alkalmazható új szempontrendszert. Ennek segítségével, az elemzett ajánlásokat összefoglalva, kiegészítve, elkészítek egy, a felhő alapú rendszerek biztonsági elemzését a rendvédelmi szervek számára egységes keretek között lehetővé tevő sablont.

A **harmadik fejezet**ben elemzem a védett vezetők információbiztonsági felkészítésének főbb kérdéseit, bemutatom a védett vezetők információbiztonsági védelme kiterjesztésének szükségességét az általuk használt kibertérre. Az előző fejezetben felállított szempontrendszer segítségével elemzem az általuk leggyakrabban használt internet-technológiára épülő

DOI azonosító: 10.17625/NKE.2015.021

szolgáltatások és személyi használatú hordozható infokommunikációs eszközök jellemzőit, azok veszélyeit, majd a védett vezetőkre szabott keretrendszer segítségével összeállítom a biztonságtudatos használatra történő felkészítés egy lehetséges módszerét.

A **negyedik fejezet**ben az internet-technológiára épülő szolgáltatások törvényes ellenőrzési lehetőségeit veszem górcső alá. Nyíltan elérhető forrásokból származó nemzetközi példákon keresztül bemutatom, hogy a törvényes ellenőrzésére milyen lehetőségek állnak rendelkezésre, milyen technikai és jogi problémák merülnek fel alkalmazásuk kapcsán. Ezeket felhasználva felállítok 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 javaslatot teszek egy, a mára már elavult hírközlési modellt potenciálisan felváltani képes új modellre úgy, hogy jogszabályokba illeszthető fogalmi meghatározást is adok annak egyes szereplőire.

Kutatási hipotézisek megfogalmazása

A tudományos probléma és a kutatási célkitűzések megfogalmazása után az alábbi hipotéziseket állítom fel:

- A felhő alapú rendszerek használata iránti igény előnyeik, különösen költségcsökkentő hatásuk okán már a közeljövőben jelentősen megnő a rendvédelmi szférában is. Ezen rendszerek felhasználásának azonban éppen a biztonsággal kapcsolatos problémák gátat is szabnak. Feltételezésem szerint a rendvédelmi szervek egyébként is az átlagnál magasabb információbiztonsági igénye sokkal jobban érvényesíthető, ha pontosan tisztázottak a használatból eredő, számukra releváns kockázatok. Ilyen összegzett tanulmány jelenleg nyíltan nem elérhető, ám feltételezem, hogy ennek kidolgozásához a nagy nemzetközi és nemzeti szervezetek ajánlásai megfelelő segítséget adnak.
- A védett vezetők által használt hordozható infokommunikációs eszközök és internet-technológiára épülő szolgáltatások információbiztonsági szempontból nem kellően védettek. Feltételezem, hogy ezen jelentősen és hatékonyan lehet javítani egy személyükre szabott biztonságtudatossági képzéssel, amely gyorsan és egyszerű eszközökkel lebonyolítható.
- A modern infokommunikációs, ezen belül kiemelten a felhő alapú rendszerek jelentősen átalakították mindennapjainkat, ezen belül kommunikációs szokásainkat. Ezek törvényes ellenőrzése azonban jelenleg jogilag és technikailag is problémákba ütközik. Feltételezem, hogy hogy ennek egyik legfőbb oka a törvényi alapot képező

DOI azonosító: 10.17625/NKE.2015.021

hírközlési modell elavultsága. Egy új jogszabályi környezet kialakítását mind jogi, mind technikai oldalról jelentősen segítheti egy, a mai viszonyokhoz illeszkedő modell megalkotása, az abban azonosított szereplők pontos meghatározása.

- Léteznek olyan eszközök és módszerek, amelyek a modern infokommunikációs, ezen belül a felhő alapú rendszerek törvényes ellenőrzésére kapcsán a titkos információgyűjtésben és titkos adatszerzésben érintett szervezetek rendelkezésre állnak. Ezek azonban a jogi vagy a technikai korlátaik okán nem alkalmasak teljes mértékben az információigények kielégítésére. Feltételezem, hogy ezek az eszközök és módszerek kategorizálhatók, tulajdonságaik rendszerezhetők, és kialakítható egy olyan szempontrendszer, amelynek segítségével egy adott feladatra való alkalmasságuk megítélhető.

Kutatási módszerek

Az értekezésem elkészítéséhez az alábbi kutatási módszereket alkalmaztam:

- irodalomkutatás: a vonatkozó releváns nemzetközi és hazai szakirodalom, jogszabályok és egyéb dokumentumok kutatása, tanulmányozása, feldolgozása,
- összehasonlító elemzés;
- általánosítás, mint vizsgálati módszer;
- kutatások másodelemzése: korábbi, a témában készült kutatási eredmények elemzése feldolgozása,
- logikai elemzés: a feltárt adatok feldolgozása, elemzése, értékelése, ebből következtetések levonása után javaslatok megfogalmazása
- empirikus kutatások: saját megszerzett szakmai tapasztalatok felhasználása, leírása
- konferenciákon, konzultációkon, rendezvényeken való részvétel, jogszabályi javaslatok kidolgozása, projektekben való részvétel
- eredmények publikálása: kutatási eredmények feldolgozása, cikkek, egyetemi jegyzet fejezetek formájában történő publikálása, valamint konferenciákon és oktatásban történő előadása.

DOI azonosító: 10.17625/NKE.2015.021

1. Felhő alapú rendszerek értelmezése

A ’90-es évek közepétől a számítástechnika és a kommunikáció egyre jobban összefonódott, integrálódott, létrejöttek az infokommunikációs (ICT)[3] hálózatok. [13] Az infokommunikáció fogalmát – bár pontos, mindenki által elfogadott meghatározása nincs és jelentéséről a mai napig is sok vita folyik [14] – az információtechnológia (IT)[4] kiterjesztett szinonimájaként is használják, beleértve olyan hardver és szoftver elemeket, tárolókat, middleware-t, tárolókat, audio-vizuális rendszereket stb. is, amelyek az információk előállításához, tárolásához, használatához, megosztásához, archiválásához és törléséhez szükségesek. [15] Elfogadva ezt a megközelítést, értekezésemben én is így használom az infokommunikáció fogalmát, olyan helyeken is ezt alkalmazva, ahol a különböző dokumentumok készítői IT rendszereket írtak (pl. a felhő alapú rendszerekkel foglalkozó szervezetek anyagai). Ennek oka pedig az, hogy véleményem szerint is 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 infokommunikációs egyre felkapottabb és ma már talán legdivatosabb fogalma a „felhő”. Felhő alapú megoldásokról, felhőben tárolt adatokról hallunk, de olvashatunk felhő alapú 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, itt ismertetve elképzeléseiket, ötleteiket, új, folyamatban lévő, vagy éppen tervezett fejlesztéseiket, felvázolva, hogyan képzelik a – nem is oly távoli – jövőt. Mindeközben folyamatosan sulykolják a felhő-technológia olyan előnyeit, mint a gyors, igény szerinti erőforrás-kiszolgálás, a mindig naprakész technológiai környezet, a koncentrált erőforrásokból adódó előnyök, beleértve az ICT szakemberekét is, és nem utolsó sorban a már rövidtávon is jelentkező, de hosszú távon is 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

[3] ICT: Information and Communications Technology (információ- és kommunikációtechnológia vagy infokommunikács technológia)

[4] IT: Infomation technology (információtechnológia vagy informatika)

DOI azonosító: 10.17625/NKE.2015.021

szerveket is – szempontjából lényegesnek tűnő kérdést. Mit is jelent pontosan a felhő alapú 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 azok használatát a jövőben? Amennyiben egy rendvédelmi szerv felhő alapú rendszert kíván használni, van-e lehetősége a sokkal szigorúbb biztonsági követelmények elfogadtatására, az ezeknek megfelelő rendszer megteremtésére? A rendvédelmi szervek mellett a kiemelt, minden szempontból védendő állami vezetők esetében hogyan lehet biztosítani, hogy az általuk igénybe vett felhő alapú rendszereknek már önmagukban a használata ne okozzon nemzetbiztonsági kockázatot? Meg lehet-e teremteni a nemzetbiztonsági szolgálatok törvényben foglalt kötelezettségét és alapfeladatát jelentő törvényes ellenőrzést a felhő alapú rendszereknél?

Az első fejezetben értékelem a felhő alapú rendszerek sajátosságait, az egyes típusok előnyeit, hátrányait, meghatározom mi tekinthető és mi nem felhő alapú rendszernek, lehet-e ezek között éles határt meghúzni, valamint, hogy az iparági tendenciák alapján kell-e a nemzetbiztonsági szolgálatoknak és a rendvédelmi szerveknek komolyan foglalkoznia a felhővel.

1.1. Példák felhő alapú rendszerekre

A felhő alapú 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. [16]

DOI azonosító: 10.17625/NKE.2015.021

1. ábra. A felhő alapú rendszer ábrázolása.[5]

Ebben a mondatban a „valahol” a kulcsszó, hiszen nevét is innen kapta ez a technológia. Ezen rendszerek működését bemutató ábrákon ugyanis az 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.

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, lelhetővé téve, hogy képeinket, dokumentumainkat, zenéinket is interneten tároljuk, ezáltal csökkenthetjük a saját eszközeinkben a háttértárak méretét és bárhonnan (ahol internet elérés biztosított), bármilyen arra megfelelő eszközzel (tehát nem kizárólag a saját számítógépünkkel), bármikor hozzáférhetünk adatainkhoz. Ez a 2010-es évek elejére már annyira elterjedt, hogy pl. 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 eszközökkel 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

[5] Szerkesztette a szerző. Forrás: [290]

DOI azonosító: 10.17625/NKE.2015.021

olyan népszerű alkalmazásokból, mint a Facebook és a Gmail. [17] De hasonló szolgáltatásokat kínált a Windows 7 és a Windows Live kombináció is. [18]

Nem csak adatokat érhetünk így el, hanem komplett alkalmazásokat is. Ilyen pl. a Microsoft Office csomagjának online verziója, az ún. Office 365, amely a felhasználóknak a megszokott együttműködési és irodai eszközöket kínálja, felhőalapú szolgáltatások formájában. [19]

A kínálat nem áll meg itt. Már olyan alkalmazásokat is „felhősítettek", mint a víruskeresők (például a Panda Cloud Antivirus, amely felhő alapú szolgáltatásának köszönhetően kis méretével és erőforrásigényével kíván nagy népszerűségre szert tenni [20]), de találkozhatunk felhő alapú (hoszting) szolgáltatással a NEXON-tól, amelyben a cég online elérést kínál HR szoftvereihez [21], vagy mobil és felhő alapú nyomtatási szolgáltatásokkal az Epsontól [22].

Az operációs rendszerek fejlesztői is elindultak a felhő alapú, online szolgáltatásként nyújtott forma irányába. Gondoljunk itt a Google régóta dédelgetett tervére a Google Chrome OS-re [23], amely végül 2011 nyarára készült el, és az első kifejezetten erre fejlesztett notebookokkal együtt került forgalomba [24] [25], vagy akár az Ubuntu 11.04-es verziójának telepítés nélkül, online, böngészőből kipróbálható verziójára. [17]

1.2. A felhő alapú rendszerek tulajdonságai, csoportosításai, előnyei, hátrányai

Hosszasan lehetne sorolni a példákat, kiegészítve a listát, bővítve azon szolgáltatások körét, amelyeket felhő alapú szolgáltatás keretében vehetünk igénybe, mégis lehetne még újabbakat találni, és másnapra szinte biztosan megjelenik egy olyan, amelyre még csak nem is gondoltunk. Ugyanakkor lehet rendszerezni is ezeket a szolgáltatásokat, mint ahogyan azt a NIST (National Institute of Standards and Technology) Információtechnológiai Laboratóriuma (Information Technology Laboratory) is megtette. [26] Az alábbiakban az általuk közzétett rendszerezést követve csoportosítom a felhő alapú rendszerek, hiszen szinte minden felhő alapú információtechnológiával foglalkozó szakmai anyag, publikáció e szerint a logika szerint teszi meg ugyanezt. Véleményem szerint mindamellett, hogy korlátai az újonnan megjelenő szolgáltatások és a technológiák konvergenciája okán már érezhetőek, ma is ez adja a legátfogóbb, legelfogadottabb csoportosítási rendszert. Hozzá kell azonban tenni azt, hogy a NIST munkatársai szerint is egy jelentősen fejlődő technológiáról van szó, ahol a definíciók is idővel fejlődni, változni, finomodni fognak. [27]

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

DOI azonosító: 10.17625/NKE.2015.021

- 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 szerver idő, hálózati tárolók stb.
- Jó hálózati hozzáférés (Broad network access)

  Hálózaton, szabványos mechanizmusokon keresztül, heterogén eszközökkel (legyen akár vékony vagy vastag kliens pl. mobiltelefonok, laptopok, PDA-k stb.) elérhetőek a szolgáltatások.
- Erőforrás készletek (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 (pl. ország, állam/megye, adatközpont)
- Teljes rugalmasság (Rapid elasticity)

  A fogyasztónak felkínált kapacitások gyorsan és rugalmasan változtathatóak, fel-, és leskálázhatóak az aktuális igények szerint, a felhasználó számára úgy tűnik, mintha korlátlan mennyiségben állna rendelkezésre.
- Mért szolgáltatások (Measured Service)

  A felhő alapú rendszerek automatikusan, a kívánt szolgáltatások típusának megfelelően képesek vezérelni és optimalizálni a rendelkezésre álló erőforrásokat (pl. tárolás, feldolgozás, sávszélesség, aktív felhasználói fiókok). Az erőforrások megfigyelhetőek, ellenőrizhetőek, használatuk pontosan mérhető, így biztosítva mind a használt szolgáltatás fogyasztója és üzemeltetője számára az átláthatóságot (pontos, mindkét fél számára elfogadott számlázási lehetőséget). [28]

A NIST szakemberei szerint ezek azok a tulajdonságok, amelyek az adott rendszerhez felhasznált – és később ismertetésre kerülő – szolgáltatási és telepítési modelltől függetlenül jellemzik a felhő alapú rendszereket.

A BSI[6] is teljes mértékben elfogadja és átveszi a NIST meghatározását, azonban a felhő alapú rendszerekre, szolgáltatásokra saját definíciót is alkot. E szerint: *„A számítási felhő megnevezés igény alapú és hálózaton keresztül elérhető, dinamikus ellátott, felhasznált és számlázott IT szolgáltatásokat takar. Ezek a szolgáltatások csak meghatározott technikai*

[6] BSI: Bundesamtes für Sicherheit in der Informationstechnik (angolul: Federal Office for Information Security) Német Szövetségi Információbiztonsági Hivatal

DOI azonosító: 10.17625/NKE.2015.021

interfészeken és protokollokon keresztül érhetők el. A számítási felhőként nyújtott szolgáltatások köre lefedi a teljes informatikai spektrumot, és magában foglalja az infrastruktúrákat (pl. feldolgozási teljesítmény, tárolók), platformokat, és szoftvereket."[7] [29]
Ez azonban lényegében nem tér el a NIST definíciójától, annak egyszerűbben, rövidebben megfogalmazott változata, amely röviden tartalmazza a következőkben ismertetésre kerülő szolgáltatási modelleket, de nem foglalkozik a telepítési modellekkel.
Több cikkben, internetes publikációban találkozhatunk olyan megjelölt tulajdonságokkal, amelyekkel a felhő alapú rendszereket próbálják jellemezni. Ilyenek pl. a rendelkezésre állás, a kiszolgálás gyorsasága, a megbízhatóság, a skálázhatóság, a teljesítmény, a biztonság, a karbantartás, a költség stb.. Egy adott felhő alapú rendszer pontos leírásánál véleményem szerint rendkívül fontos a figyelembe veendő tényezők és 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 értékelésénél figyelembe venni az adott tulajdonságot.
Ahhoz azonban, hogy a felhő alapú rendszereket csoportosíthassuk, egy ilyen elven működő rendszert pontosan besorolhassunk, szükség van a már említett két modell csoport – a szolgáltatási és a telepítési – kategóriáinak ismeretére is, előnyeikkel, hátárnyaikkal együtt.

1.2.1. 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 kliens felületen pl. web böngészőn elérhetőek. (ilyen pl. a webmail szolgáltatás). A felhasználó néhány felhasználó-specifikus alkalmazás korlátozott konfigurációs beállítási lehetőségétől eltekintve semmilyen ráhatással sincs a mögöttes infrastruktúrára, hálózatra, szerverekre, operációs rendszerekre, a tárolás módjára, vagy akár egyedi alkalmazások képességére.
  Előnyei: gyorsan bevezethető, azonnal használható, a felhasználói oldalról használható eszközök rendkívül széleskörűek, nem igényel nagy beruházást, a legnagyobb költséget kitevő ICT üzemeltetési költség jelentősen csökkenthető, a használt szoftverek mindig naprakészek, az alapvető, általános biztonsági funkciókat a

[7] [29] p. 13.

DOI azonosító: 10.17625/NKE.2015.021

szoláltató biztosítja (pl. vírusvédelem), alkalmazásváltás alacsony költséggel, gyorsan végrehajtható.

Hátrányai: nincs testre szabás vagy egyedi igény 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, szervereket, operációs rendszereket, vagy a tárolókat, de kontrollálja a telepített szolgáltatásokat és az azok fogadására szolgáló környezet konfigurációját.

  Előnyei: egyedi, akár saját készítésű szoftverek használhatóak, ezért a bevezetése gyors és egyszerű, a heterogén szoftverkörnyezet bizonyos mértékben homogenizálódik, 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 szoftver komponensek (operációs rendszer) korlátolja, ezért gondos választás esetén is kompromisszumos megoldás születhet, 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 csökkenthetőek, 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, amelyre, és amelyen tetszőleges szoftvereket telepíthet és futtathat, beleértve az operációs rendszereket és alkalmazásokat. A felhasználó nem képes menedzselni vagy ellenőrizni a mögöttes

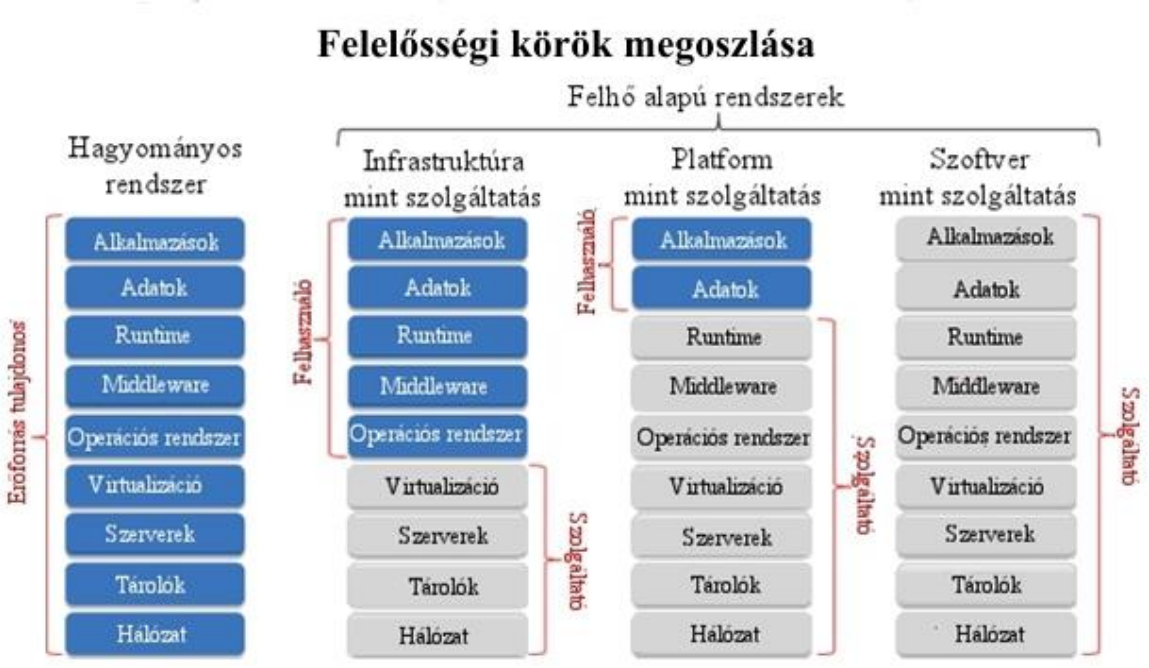
DOI azonosító: 10.17625/NKE.2015.021

felhő infrastruktúrát, de kontrollálni tudja az operációs rendszereket, tárhelyeket, telepített alkalmazásokat, és esetleg korlátozott ráhatása lehet a hálózati elemek (pl. 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 csökkenthetőek legkevésbé az korábbi ICT költségek. [30]

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 ezek között nem található.



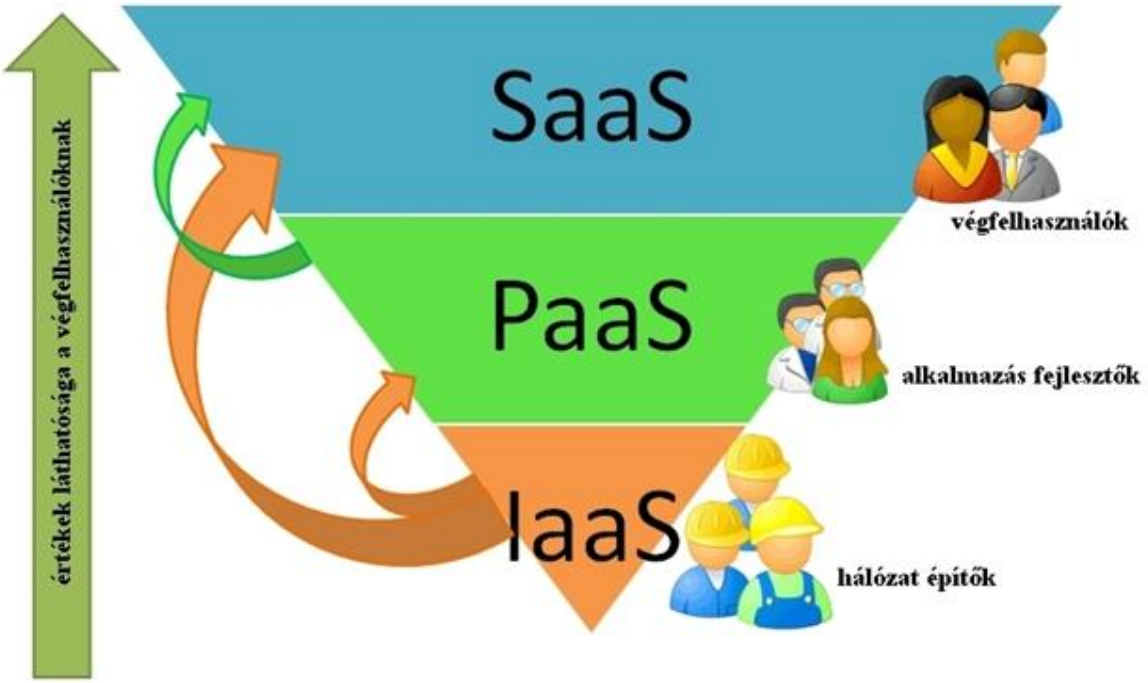
2. ábra. Felelősségi körök megoszlása a szolgáltatási modellekben.[8]

[8] Szerkesztette a szerző. Forrás: [287]

DOI azonosító: 10.17625/NKE.2015.021

A szolgáltatási modelleket már többen, többféleképpen megpróbálták kiegészíteni (mint ahogy már utaltam rá, a NIST szakemberei is hasonló fejlődési folyamatot várnak). Megjelentek az olyan fogalmak, mint a Desktop as a service (DaaS) [31] (amely vékonykliensek kiszolgálására használt desktop rendszerek virtualizációját jelenti) vagy a PRaaS (Process as a service) [32] (amely szerint a teljes folyamat egy komplett, felhőben futó megoldás, úgy, hogy a felhasználónak nincs szüksége semmilyenfajta ICT szakember beavatkozására). De amíg a fent kifejtett 3 modellt teljes mértékben mindenki – beleértve az ipari szereplőket is – elfogadja és – ha úgy tetszik – kvázi-szabványként használja, addig az utóbbiak (és az itt fel nem soroltak is) vagy nem ismertek, vagy nem elfogadottak és megkérdőjelezik a létjogosultságukat. [33]

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



3. ábra. A szolgáltatási modellek előnyeinek értékelői.[9]

1.2.2. Telepítési modellek (Deployment Models)

- Magán számítási felhő (Private cloud)

  A felhő infrastruktúra kizárólag egy szervezet számára működik. Ezt akár a felhasználó szervezet, de akár egy másik fél is menedzselheti, fizikailag lehet akár a felhasználó telephelyén, akár azon kívül.

[9] Szerkesztette a szerző. Forrás: [288]

DOI azonosító: 10.17625/NKE.2015.021

Előnyei: a teljes rendszer kézben tartott, a biztonság itt garantálható a legjobban, meglévő rendszerek, rendszerelemek felhasználhatóak.

Hátrányai: korlátozott erőforrások, csúcsterhelésre kell tervezni, kevésbé skálázható, a korábbi ICT-re fordított költségek csökkentése itt érhető el a 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 (pl. 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 szóltam, ez tekinthető ma a legismertebb telepítési modellnek.

  Előnyei: teljes felhasználói mobilitás biztosított, jól skálázható, 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 adatvisszaállítással, 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,

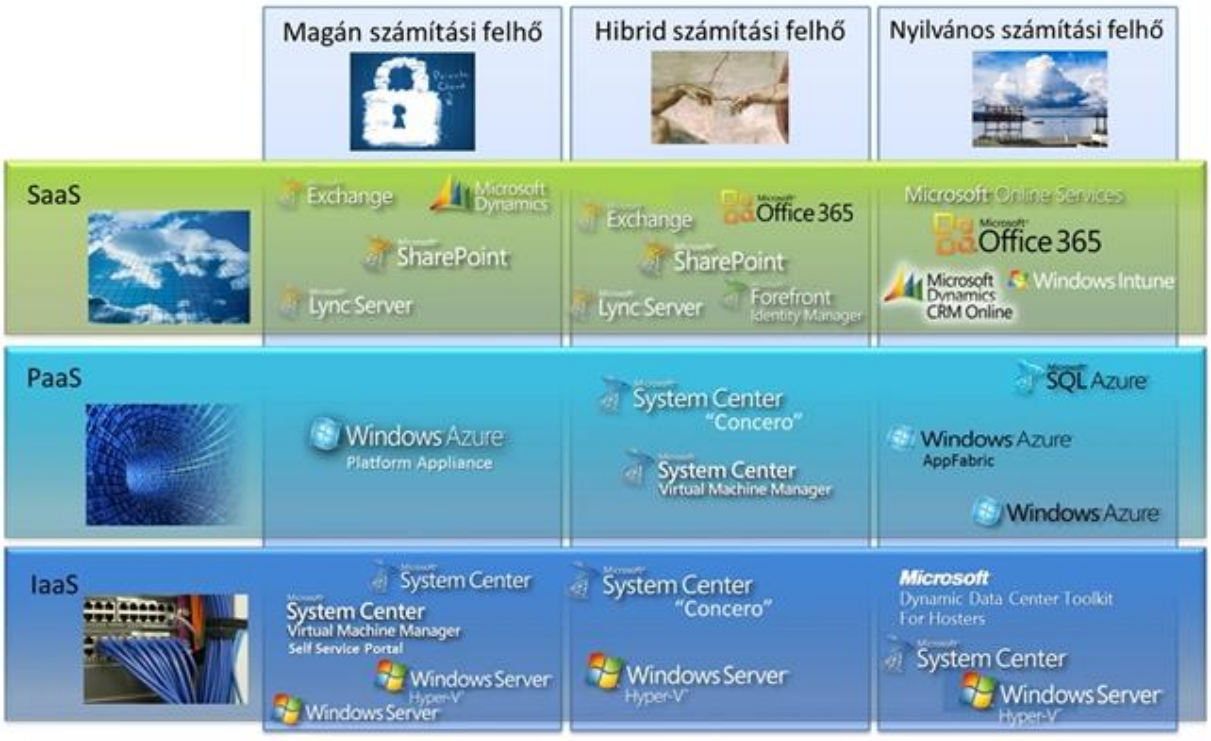
DOI azonosító: 10.17625/NKE.2015.021

azokat szabványosított vagy szabadalmazott technológiák kötik össze, lehetővé téve az adatok és alkalmazások hordozhatóságát (pl. cloudbursting technológia a felhők közötti terhelés-kiegyenlítésre, amikor a magán felhőben rendelkezésre álló erőforrások elfogynak és azokat más, tipikusan nyilvános felhőben meglévőkkel pótolják ki [34]).

Előnyei: alapvetően kézben tartott rendszer, amely egyedi igények szerint épül fel, az átlagterhelés feletti szükséges plusz kapacitásokat 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 adatvisszaállítás és a biztonság, nem, vagy csak korlátozottan rendelkezünk ismeretekkel a saját rendszeren kívüli többi erőforrás fizikai helyét, összetételét, biztonságát stb. illetően. [35]

A szolgáltatási és a telepítési modellekből egyfajta mátrix képezhető. Ebben a mátrixban kell megtalálnia a felhasználónak, hogy hová helyezi saját (meglévő vagy tervezett) hálózatát, és ennek 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 mátrixban.[10]

[10] Szerkesztette a szerző. Forrás: [59]

DOI azonosító: 10.17625/NKE.2015.021

1.3. A kormányzati felhő fogalma

Az általános meghatározások után érdemes elemezni, hogy mit is takar a kormányzati felhő fogalma. Már csak azért is, mert ennek meghatározása, valamint ez alapján a felhő alapú rendszerek bizonyos tulajdonságainak a megfeleltetése főleg a biztonsággal összefüggő szigorúbb kormányzati feltételeknek, jelentősen előre viheti a rendvédelmi szféra tagjainak is megfelelő felhő-követelmények kialakítását.

Az ENISA[11] a „Good Practice Guide for Securely Deploying Governmental Clouds" [36] című dokumentumában külön próbálja meghatározni a kormányzati felhő (gov-Cloud)[12] fogalmát. A készítő szakemberek ehhez alapnak elfogadják a NIST felhő definícióját, amelyből három telepítési modellt, a nyilvánost, a magánt és a közösségit emeli ki, mint lehetséges kormányzati felhő megoldást, míg a szolgáltatási modellek tekintetében mindhármat alkalmasnak tekintik ilyen célú felhasználásra.

A kormányzati felhőre jelenleg nincs elfogadott pontos meghatározás, csupán elfogadott megközelítések vannak. 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).”*[13] [36]

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 és szolgáltatási szintek mellett lehet olyan alapvető szolgáltatásokat nyújthatni a kormányzati szerveknek, minisztériumoknak, amelyek segítik azok belső működését, lehetővé teszi számukra e-kormányzati szolgáltatások nyújtását

[11] ENISA: European Union Agency for Network and Information Security (eredeti nevén: European Network and Information Security Agency) Európai Hálózat- és Információbiztonsági Ügynökség.
[12] gov-Cloud: governmental Cloud computing, kormányzati felhő
[13] [36] p. 5.

DOI azonosító: 10.17625/NKE.2015.021

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 felhő technológiából adódó új kockázatokat is.

Az ENISA az áttekintést követően végül a következő meghatározást adja a kormányzati felhő fogalmára: *„a kormányzati felhő olyan felhő alapú rendszer (infrastruktúra, platform és alapvető szolgáltatások csoportja), amelyik általában megfelel a következőknek:*

A. *olyan magán (egyedi bérlő), közösség (megegyezés alapján bérlők csoportja) vagy nyilvános (több bérlő) felhő modellben 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;*
B. *egy sor olyan többször használható szolgáltatási elemet biztosít, amelyek segítségével létrehozhatók e-kormányzati szolgáltatások a közigazgatás, a polgárok és a magánvállalatok számára;*
C. *lehet központi kormányzati, de lehet külső szolgáltató vagy szerv tulajdonban és irányítás alatt, de a végfelelősség a felhasználóé, azaz a központi kormányzaté vagy a helyi szervezeteké (főleg a magán és a közösségi felhő esetében);*
D. *egy olyan üzleti modell, amely lehetővé teszi az infrastruktúrát, platform és a szolgáltatások működtetését olyan módon, hogy garantálja a hatékonyságot és a méretgazdaságosságot;*
E. *az infrastruktúra, a platform és a szolgáltatások megfelelnek országok kormányai és az EU jogszabályoknak az információbiztonság és az ellenálló képesség terén (függetlenül a kormányzati felhő tényleges fizikai elhelyezkedésétől.”*[14] [36]

Az idézett szöveg véleményem szerint nem tekinthető definíciónak, sokkal inkább körbeírása annak, mikor beszélhetünk – az ENISA szerint – kormányzati felhőről. A hatékonyság és méretgazdaságosság megjelenítését sem tartom megfelelőnek, ezek velejárói lehetnek vagy kellenek, 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 felhő struktúrára váltani. Ugyanígy nem értek egyet a kormányzati és az EU szabályozásnak megfelelés kiemelésével, mert azokat alapkövetelménynek tekintem, ráadásul nem csak a

[14] [36] p. 6.

DOI azonosító: 10.17625/NKE.2015.021

kormányzati, hanem minden az EU-ban szolgáltatást nyújtó felhő rendszer esetében is. (Ezek betartása a valóságban azonban már más kérdés.)

Joggal merül fel a kérdés, érdemes-e egyáltalán meghatározni a kormányzati felhő fogalmát. Véleményem szerint igen. Már csak azért is, mert a kormányzati felhasználású felhő rendszerekre 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, vagy akár hacktivistáknak is. Ugyanakkor ebből a meghatározásból kiindulva, még szigorúbb biztonsági és ellenálló képességi szabályokat alkalmazva juthatunk el a rendvédelmi szervek által is használható felhő alapú rendszerhez.

A kormányzati felhőre kevés meghatározást lehet találni. Azokban a dokumentumokban, amelyek adott országok kormányzati felhőjének kialakításával foglalkoznak, inkább leírásokat, követelményeket találhatunk, felhő definícióként pedig elfogadják és átveszik a NIST meghatározását. Ilyen például az Egyesült Királyság G-Cloud programja [37], de említhetjük a Fülöp-szigetek Intergrated Government Phillippines (iGovPhil) [38] projektjét is.

Az ENISA-n kívüli kevés meghatározások egyikét a technopedia.com adja. E szerint a *„GovCloud kifejezés vonatkoztatható az összes olyan számítási felhőre 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”*. [39]

Az Amazon saját GovCloud megoldását, az AWS[15] GovCloud-ot úgy határozza meg, mint egy kifejezetten az Egyesült Államok kormányzati szervei, és azok szerződő partnerei és ügyfelei számára 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. [40]

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

[15] AWS: Amazon Web Services Amazon web szolgáltatások

DOI azonosító: 10.17625/NKE.2015.021

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 véleményem szerint 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 ez oly módon képes segíteni a kormányzati és rendvédelmi szervek munkáját, hogy a számukra megfelelő felhő alapú 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.

DOI azonosító: 10.17625/NKE.2015.021

1.4. Felhő és nem felhő alapú rendszerek megkülönböztetése

Az előző fejezetek ismertették, hogy mit takar a felhő alapú rendszer kifejezés, milyen kategóriákba oszthatjuk őket és azok milyen tulajdonságokkal jellemezhetőek. Felmerülhet azonban az a kérdés, hogy mi a különbség a felhő és a nem felhő alapú rendszerek között, hogyan lehet ezeket egyértelműen megkülönböztetni egymástól, vagy egyáltalán meglehet-e ezt tenni? Ahhoz, hogy a felhő alapú rendszereket pontosan meg lehessen határozni és el lehessen őket helyezni az „ICT világ-térképén", mindenképpen célszerű megpróbálni megtenni ezt az elhatárolást.

A dolgozatomban tárgyalt témák szempontjából véleményem szerint azt a három dolgot érdemes tisztázni, hogy mi a különbség egyrészt a felhő alapú rendszerek és a hagyományos ICT rendszerek virtualizációja, másrészt a felhő alapú rendszerek és a kiszervezett ICT rendszerek és szolgáltatások, harmadrészt a felhő alapú rendszerek és az internet-technológiára épülő szolgáltatások között. Az első kettő a nemzetbiztonsági szolgálatok és a rendvédelmi szervek számára a felhő alapú rendszerek (esetleges) használata, a harmadik pedig elsősorban a törvényes ellenőrzés kialakítása, valamint védett vezetők információbiztonsági védelmének emelése miatt lehet érdekes.

1.4.1. Virtualizáció vs. felhő

A virtualizáció és a felhő alapú rendszerek között lényeges különbségek vannak. Ezek használata során jelentkező előnyökről, hátrányokról külön tanulmányok készültek, kiemelve mikor melyik megoldást érdemes használni. [41] 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. [42] [43]

Miért erőforrásokat említettem? A mai – elterjedt – technológiákat tekintve és rendkívül leegyszerűsítve a dolgot azt mondhatnánk, hogy virtualizáció az, amikor egy adott hardveren több virtuális rendszert működtetünk. [44] Ennél azért jóval többről van szó, hiszen a virtualizációt az adatközponttól a munkaállomásig az informatika minden rétegére lehet alkalmazni. [42] Az 5. ábra jól szemlélteti a teljesen „hagyományos" informatika és a teljesen virtualizált közötti technikai különbségeket, minden rétegre vonatkozóan.

DOI azonosító: 10.17625/NKE.2015.021

5. ábra. A „hagyományos” és a virtualizált informatika közötti különbségek.[16]

A felhő alapú rendszerekhez hasonlóan a virtualizált környezetben sem tudja a felhasználó megmondani, hogy az általa futtatott alkalmazások milyen fizikai hardveren futnak, vagy éppen az adatai hol kerültek tárolásra. 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 hardverelemek ugyanúgy a felhasználó telephelyen kerülnek elhelyezésre, ugyanúgy a felhasználó üzemelteti azokat, és valószínűleg ezek az eszközök ugyanúgy a felhasználó tulajdonában is vannak, mint hagyományos megoldások esetében. A felhő alapú rendszerek esetében mindig virtualizált környezetről beszélhetünk, ha úgy tetszik, akkor a felhő alapú rendszerek bizonyos szempontból részhalmazát képezik a virtualizált hálózatoknak. Ám a felhő alapú 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 felhő alapú rendszer használata esetén, ahol ezt a problémát a felhő alapú rendszer szolgáltatója átveszi a felhasználótól.

[16] Szerkesztette a szerző. Forrás: [42]

DOI azonosító: 10.17625/NKE.2015.021

A virtualizáció is – a felhő alapú rendszerekhez hasonlóan – lehetővé teszi az erőforrások a „hagyományos” informatikai megoldásokhoz képesti jobb kihasználását, ám amíg a virtualizáció esetében azok elosztásához, újraosztásához mindig a felhasználó ICT szakemberinek beavatkozás szükséges, addig a felhő alapú rendszerek esetében ez automatikusan, akár emberi beavatkozás nélkül képes megtörténni. [45] 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 nem csak az emberi beavatkozás szükségességét vetíti elénk, hanem azt is, hogy a felhő alapú rendszerekben az erőforrások felhasználása hatékonyabb, újraosztása gyorsabb, a kritikus leállások – pl. erőforráshiány miatt – száma kevesebb lehet.

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

1.4.2. Kiszervezés vs. felhő

Az ICT rendszerek, szolgáltatások kiszervezése már jóval régebben elkezdődött, mint ahogy a felhő alapú rendszerek, szolgáltatások megjelentek. Egy felhő alapú rendszer használata azonban többet jelenthet, mint a kiszervezés, hiszen nem csak 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 felhő alapú rendszer esetében a legtöbbször több felhasználós 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 felhő alapú 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. [46] Yigitbasioglu, Mackenzie és Low megközelítésében a felhő egy olyan ICT kiszervezés, ahol az olyan erőforrásokat, mint hardver, szoftver, platform, interneten keresztül lehet elérni és a legtöbb esetben használat alapú fizetés ellenében. [47] Katzan és Dowling megfogalmazásában a kiszervezés a meglévő funkciók kihelyezését jelenti, míg a felhő esetében a felhőben lévő alkalmazás motiválja az adott funkció kihelyezését. [48] Marston és munkatársai további különbséget tesznek a kiszervezés és a

DOI azonosító: 10.17625/NKE.2015.021

felhő között, a szerződés időtartama alapján. Véleményük szerint ez a hagyományos kiszervezés esetén általában hosszabb, hiszen a felhő szolgáltatóval 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 kéréseket az ügyfél közel azonnal megteheti, az erre alkalmas szoftveren keresztül. [49] GetCloudServices szerint a fentieken kívül figyelembe lehet venni az ellenőrzés mértékét is. Egy hagyományos kiszervezés esetén a felhasználónak nagyobb kontrollja marad(hat) az adatai felett, mintha felhőt használna. [50]

Nagyobb szervezetek is foglalkoztak a kérdéssel. Az ENISA azt tekinti felhő alapú rendszernek, amely megfelel a NIST definíciójában leírtaknak, míg a nem felhő alapú 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. [51] A kiszervezés és a felhő alapú 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, pl. ITIL[17]-ben.

A BSI szerint a klasszikus kiszervezés és a felhő alapú 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 fel-, és leskálázás lehetősége, a felhasználók saját maguk általi erőforrás-menedzselhetősége, a földrajzilag jobban elosztott hálózat, valamint a személyre szabottabb szolgáltatások. [29]

A fentiekből látszik, hogy a kiszervezés és a felhő megkülönböztetése nem teljesen egyértelmű, az elhatárolás bizonyos esetekben (pl. magán felhő) pedig szinte lehetetlen. Az egyes megközelítések nagyban függnek attól, hogy milyen telepítési-, és szolgáltatási modellt vizsgál a szerző. Véleményem szerint a felhőre úgy lehet tekinteni, mint a kiszervezés egy

[17] ITIL: Information Technology Infrastructure Library informatikai rendszerek üzemeltetésére és fejlesztésére szolgáló módszertan, illetve ajánlás gyűjtemény.

DOI azonosító: 10.17625/NKE.2015.021

formájára, azaz a felhő alapú rendszerek használata az ICT kiszervezések részhalmazát képezik.

1.4.3. Internet-technológiára épülő szolgáltatások vs. felhő

Katzan és Dowling cikkében úgy tekint a számítási felhőre, mit egy internet alapú eszközre, interneten keresztüli hozzáférhetőséggel. [48] Ebből a megfogalmazásból is látszik, hogy az internet-technológiára épülő valamint a felhő alapú szolgáltatások elhatárolása még nehezebb, mint a kiszervezés és a felhő közöttié. Bár az általam elemzett szakirodalom ezzel egyáltalán nem foglalkozik, én ennek elvégzését a tárgyalt témák szempontjából mégis fontosnak tartom, mert véleményem szerint a felvetett tudományos problémák közül az infokommunikációs rendszerek törvényes ellenőrzési lehetőségei, előírásai, valamit információbiztonsági felkészítés tartalmi elemeinek kidolgozása védett személyek számára megértésében és megoldásában is segíthet.

Ahhoz, hogy az említett két témakör kapcsán valóban segítséget nyújtson az internet-technológiára épülő valamint a felhő alapú szolgáltatások elhatárolása, a felhő alapú rendszerek esetén tovább lehet és célszerű szűkíteni a vizsgálandó kört. Az „átlagfelhasználók” ugyanis elsősorban a nyilvános számítási felhő (Public cloud (PC)) és szoftver, mint szolgáltatás (Cloud Software as a Service (SaaS)) típusú rendszereket (továbbiakban: PC/SaaS felhő alapú rendszerek) használják leggyakrabban. Egyszerűbben fogalmazva ezek azok a mindenki számára – a meglévő személyi használatú infokommunikációs eszközök (pl. notebook, okostelefon stb.) felhasználásával, akár csekély számítástechnikai tudással is használható, olcsón, sokszor ingyenesen – igénybe vehető rendszerek, szolgáltatások (mint pl. Facebook, Gmail, Dropbox, Twitter, Skype stb.) amelyek ma már szerves részét képezik mindennapi életünknek, kommunikációnknak. Ez pedig több szempont miatt is érdekli a nemzetbiztonsági szolgálatokat és a rendvédelmi szerveket. Egyrészt célszemélyi körük nagy része, másrészt az általuk védett vezetők is akár magán, akár hivatalos célokra is ezeket a rendszereket, szolgáltatásokat használják (pl. választókkal, szimpatizánsokkal való kapcsolattartásra, gondolataik gyors, széles rétegekhez történő eljuttatására [52] [53] [54]).

A PC/SaaS rendszerek mindenképpen az internet-technológiára 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. [27] Hozzá kell azonban tenni azt,

DOI azonosító: 10.17625/NKE.2015.021

hogy NIST munkatársai szerint is egy jelentősen fejlődő technológiáról van szó, ahol a definíciók is idővel fejlődni, változni, finomodni fognak. A NIST definíciója a lehető legáltalánosabban kívánja megfogalmazni a felhő alapú rendszerek alapvető tulajdonságait (igény szerinti önkiszolgálás, jó hálózati hozzáférés, erőforrás készletek, teljes rugalmasság, mért szolgáltatások), így azután lehetséges, hogy egy adott szolgáltatási-, vagy telepítési modellre rendkívüli módon jellemző tulajdonság nem, vagy csak korlátozott mértékben igaz a többire. A NIST definíciójában a szolgáltatási-, és a telepítési modelleken belül leírtak is a lehető legszélesebb értelemben próbálják átfogni a felhő alapú rendszerek egyes típusait, ám minden valós rendszer más és más, bizonyos jellemzők teljes mértékben igazak, mások viszont nem vagy csak kis mértékben jellemzőek az adott rendszerre. Az újonnan megjelenő funkciók, lehetőségek, az egy alkalmazás használatával elérhető többféle szolgáltatás, pedig tovább nehezíti a besorolást. Gondoljunk például a Google szolgáltatásaira (pl. Gmail, YouTube, Térkép, Naptár, Fordító, Dokumentumok stb.). [55] Ezek egy része tisztán értelmezhető felhő alapú szolgáltatásként, egy másik része kis jóindulattal, egy harmadik része pedig szinte egyáltalán nem.

Éppen ezért, sokszor nagyon nehéz megmondani, hogy internet-technológiára épülő szolgáltatással, vagy az annak részhalmazát képező PC/SaaS rendszerrel van-e dolgunk. Véleményem szerint 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.

A dolgozatban sokszor kitekintek a felhő alapú rendszerekből, hiszen az infokommunikációs rendszerek törvényes ellenőrzési lehetőségei, előírásai, valamit az információbiztonsági felkészítés tartalmi elemeinek kidolgozása védett személyek számára témakör sem tárgyalható érdemben úgy, hogy a vizsgálatot csupán ezekre leszűkítve végzem el. Az első esetében figyelembe kell venni az olyan internet-technológiára épülő szolgáltatásokat is, amelyek – jelenleg legalábbis – nem érthetők bele a PC/SaaS rendszerek fogalmába, de a második eset sem lehet figyelmen kívül hagyni a személyi használatú infokommunikációs eszközöket, és azok tulajdonságait. Éppen ezért a dolgozat céljának eléréséhez, amikor szükséges, akkor a kiterjesztőbb értelmű internet-technológiára épülő szolgáltatások megfogalmazást használom, de egyértelműen beleértve és kiemelten kezelve a PC/SaaS rendszereket.

DOI azonosító: 10.17625/NKE.2015.021

1.5. Nemzetbiztonsági szolgálatok, rendvédelmi szervek és a felhő

A felhő alapú rendszerek ismertetését követően érdemes megnézni, hogy a felvetett tudományos probléma valóban megoldandó-e, azaz szükséges-e a nemzetbiztonsági szolgálatoknak és a rendvédelmi szerveknek foglalkozniuk ezekkel a rendszerekkel. Tekintsük ezt akár a felhasználás, akár a védett vezetők információbiztonságának emelése, akár a törvényes ellenőrzés végrehajtása szempontjából. Ehhez nem csak a jelen, hanem 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. Nézzük meg először a globálisan tendenciákat, azaz azt, hogy mit jósoltak korábban és mi várható a felhő alapú rendszerekkel kapcsolatban.

Az IDC szerint a felhő alapú rendszerek és a hozzájuk kapcsolódó szolgáltatások szegmense átlagosan évi 28 százalékkal nő majd, így a 2011-ben mintegy 21,5 milliárd dolláros piac 2015-re 73 milliárd dollárosra bővül. De nem csak ezt, hanem a teljes ICT iparág átalakulását, átrendeződését is jósolják az IDC szakértői, véleményük szerint ez a technológia – összefonódva az egyre okosodó és terjedő mobil eszközökkel, valamint közösségi hálózatokkal – adja majd az iparág harmadik nagy platformját és hozza el a mainframe-ek és a PC-k utáni a harmadik nagy növekedési hullámot. [56]

Egy másik elemzésben a Gartner piacelemző cég szerint 2012-re a legnagyobb, Fortune 1000 soraiba tartozó vállalatok 80 százaléka igénybe fog venni valamilyen felhőalapú szolgáltatást. [57]

A Cisco Connected World Report című 2010. december 8-án megjelentetett nemzetközi tanulmánysorozat harmadik részében 13 országra kiterjedő vizsgálat adatait tették közzé – többek között – a felhő alapú rendszerek jelenlegi felhasználásával, valamint azok tervezett bevezetésével kapcsolatosan. A válaszok szerint a megkérdezettek 18% már használ valamilyen felhőalapú megoldást, 34% pedig tervezi bevezetését. 92% vélekedett úgy, hogy a következő három évben adataihoz és alkalmazásaihoz bizonyos részben privát vagy nyilvános felhőrendszert vesz majd igénybe. [58]

Az ipar szereplői is komolyan veszik a felhő alapú rendszereknek jósolt kiemelkedő jövőt. Senki sem szeretne lemaradni, a jelenlegi nagyok meg kívánják őrizni vezető szerepüket, a kihívók, vagy új piaci szereplők pedig ebben látják a nagy lehetőséget az előrelépésre. Számos példát ismerünk arra, hogyan bukhatnak, vagy maradhatnak le a nagyok, ha korábbi sikeres termékeiket, technológiájukat erőltetik, azokkal akarják megtartani pici előnyüket (pl. IBM [59], Nokia [60]).

DOI azonosító: 10.17625/NKE.2015.021

Jó példa a vezető szerep megtartására való törekvésre a Microsoft, amely – Steve Ballmer a Microsoft vezérigazgatója szerint – 2012-ig közel 10 milliárd dollárt fektetett a felhő alapú rendszerek kutatásába és fejlesztésébe. [61] Ennek folytatásaként a Microsoft két iparági elsőséget is begyűjtött. 2014-ben elsőként kapta meg azt a tanúsítványt, hogy felhőalapú nagyvállalati szolgáltatásai megfelelnek az EU legmagasabb szintű elvárásainak, [62] 2015-ben pedig elismerten az övék volt a világon az első olyan felhő alapú rendszert, amely megfelelt az ISO/IEC 27018-as elsősorban adatkezelési ajánlásokat tartalmaz, különös tekintettel a biztonsági kockázatok megfelelő kezelésére. [63]

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. Nem mehetnek el e mellett az állami intézmények, így a rendvédelmi szervek sem. A felhő alapú rendszerek előnyei (költség megtakarítás, skálázhatóság, könnyebb üzemeltetés stb.), valamint az elhúzódó gazdasági válság államra gyakorolt hatása (pl. állam fenntartására fordítható kiadások csökkenése) olyan hívószavak, amelyek tovább erősítik az iparági tendenciákat és e hatékonyabb technológia felhasználása irányába hatnak.

A következőben két idézetet hozok. Az egyik Steve Ballmer a Microsoft akkori vezérigazgatója által 2010. november 18-án írt cikkből való: *„Az üzleti élet mellett a közigazgatás szereplői is felismerték az új technológia előnyeit. Európa kormányaival és állami intézményeivel együttműködve azon dolgozunk, hogy kitaláljuk, miként növelhető a hatékonyság a felhő alapú megoldásokkal, miként nyújthatók jobb szolgáltatások, illetve hogyan fokozható a növekedés. Látható, hogy a felhő alapú számítástechnikának köszönhetően Európa polgárai mára hatékonyabb és gyorsabb közigazgatási szolgáltatásokban részesülnek, s a közszférában is teret nyer a vállalkozói szellem, a dinamizmus és a kísérletező kedv."* [61]

A másik Kalotay Balázs, a Fujitsu Technology Solutions Kft. szakértőjének az „Új típusú IT funkciók az új gazdasági környezethez" címmel Budapesten megrendezett IDC Hosting Konferencián tett megállapítása: *„Minden korábbinál nagyobb szükségük van a magyar önkormányzatoknak, valamint a kis- és középvállalatoknak a felhő alapú számítástechnikai szolgáltatásokra. A válság időszakában ugyanis a magyar gazdaság legtöbb szereplőjének nem áll rendelkezésére elegendő fejlesztési forrás informatika rendszerük színvonalának szinten tartására a hagyományos módon. Ebben a helyzetben a megoldást az infrastruktúra beruházások költségét minimalizáló és a működési kiadásokat csaknem megfelező felhő*

DOI azonosító: 10.17625/NKE.2015.021

szolgáltatások igénybevétele jelentheti. Számos városi és járási (kistérségi) önkormányzat, valamint jó néhány vállalat már felismerte ezt a lehetőséget…" [64]

2011 tavaszán arról is jelent meg publikáció, hogy Magyarországon elsőként Veszprém, másodikként Fejér megye csatlakozott a felhő alapú szolgáltatásokhoz. [65] Ez jól mutatja, hogy a 2010-es évek elején az állami szférában Magyarországon is megkezdődött a „felhő korszak".

A fenti adatok a 2010-es évek elejének előrejelzéseit mutatták, a növekedésről szóló jóslatok jelentős részét az eltelt idő alá is támasztotta. Az iparági előrejelzések hasonló fejlődéssel számolnak az 2010-es évek második felére is. A Forbes 2013-ban többek között a hibrid felhő megoldások további terjedését, a PaaS piac akkori 3,8 milliárd $-ról 2017-re 14 milliárd $-ra növekedésével számoltak. A felhő rendszerek további kiterjedést jósolták a saját tulajdonú, munkában is használat eszközök (BYOD)[18] és ehhez kapcsolódóan a vállalati ICT rendszerben létrehozott személyes felhők egyre gyakoribb használatával. [66] 2015-re vonatkozóan megerősítették ezeket az előrejelzésüket, hiszen ezzel szinte teljesen megegyező trendeket vázoltak fel [67], amelyekre az ITBusinessEdge ráerősített. [68] A theguardian által megkérdezett szakértők 2014-re hasonlókat vetítettek elő. Vállalati oldalról elsősorban a nem a nyilvános, hanem a hibrid felhő rendszerek fejlődésével számoltak. Volt, aki szerint a Gartner előrejelzése, amely szerint 2017-re a nagyvállalatok több mint fele hibrid felhőt fog használni, nem helytálló, mert azok sokkal hamarabb elérik ezt a szintet. [69] A Gartner szerint a felhő növekedését a közeljövőben elsősorban a több (mobil) eszköz használatával jelentkező, alkalmazások és tartalmak szinkronizálásának igénye fogja meghatározni. [70] Az Information Management pedig egyenesen azzal számol 2015-re, hogy a Microsoft felhő megoldásainak bevételei már meg fogják haladni a tradicionális, nem felhő alapú megoldások értékesítéséből származókét. [71]

A fentiek alapján kijelenthető hogy rendvédelmi szektor kapcsán sem az a kérdés, az ide tartozó szervezetek igénybe fognak-e venni a felhő alapú rendszereket, szolgáltatásokat, sőt még csak nem is az, hogy ezt minden szervezet megteszi-e. Látva az iparági tendenciákat, ezekre a válasz már megszületett, ráadásul ezen szervezetek egy része már ma is használ ilyen rendszereket. [72] [73] [74] A kérdés sokkal inkább az, hogy mikortól, milyen formában, milyen modellek és milyen 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,

[18] BYOD Bring Your Own Device, azaz Hozd a saját eszközöd. A munkavállalók saját eszközeiket használják a mindennapi munkavégzés során.

DOI azonosító: 10.17625/NKE.2015.021

önkormányzati felhasználás esetén, másrészt a biztonság kérdése ma a felhő alapú rendszerek egyik legfőbb problémája. A felhő alapú rendszerek biztonságos használata az EU-ban állami szinten is megoldandó probléma, oly annyira, hogy az ENISA szakemberei a „Security Framework for Governmental Clouds" [75] című dokumentumukban megállapították, hogy 2014 szeptemberében is csupán alig néhány EU tagállamnak volt erre olyan kidolgozott felhő megközelítése, amely jól definiált biztonsági stratégián alapult. Márpedig ez egyértelműen kihat a rendvédelmi szervek ilyen irányú lehetőségeire, törekvéseire is.

Biztonsági kérdések megfogalmazás persze egy rendkívül nagyvonalú egyszerűsítés a felhő alapú rendszerek kapcsán. Itt olyan kérdéseket kell megvizsgálni a hagyományos ICT biztonsági kérdéseken belül, mint például az üzemeltetés, sérülékenység-menedzsment, személyazonosság-kezelés azon kívül esők közül pedig olyanokat, mint az adatvédelem, megfelelőség, jogi és szerződési kérdések. [76] Meg kell határozni, hogy ezek közül melyek azok, amelyeket egy felhő alapú rendszer felhasználásával kapcsolatban vizsgálni szükséges, azokat pontosan definiálni kell, át kell tekinteni, hogy ezek közül 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 felhő alapú rendszerek lehetséges felhasználása mellett a nemzetbiztonsági szolgálatoknak és a rendvédelmi szerveknek azt is el kell dönteni, hogy a védett vezetők információbiztonságának emelése és a törvényes ellenőrzés biztosítása érdekében kell-e ezekkel a rendszerekkel foglalkozniuk. Ennek kapcsán elmondható, hogy a növekedés az internet-technológiára épülő szolgáltatások, azon belül is a PC/SaaS rendszerek esetében is markánsan kimutatható. A Facebook felhasználók száma 2008. III. negyedévében mért 100 millióról 2014. III. negyedévében 1350 millióra ugrott. [77] A Dropbox 2014. év közepére 200 országban volt elérhető 19 nyelven, szolgáltatásaikat 300 millióan vették igénybe, [78] mindezt úgy, hogy a 2013 novemberében közzétett 200 milliós felhasználói számhoz képest csupán fél év alatt nyertek meg újabb 100 millió ügyfelet. [79] A Skype napi aktív felhasználóinak száma 2013-ban 2,7 millióról 4,9 millióra, azaz 82 %-kal növekedett. [80] Az ilyen típusú rendszerek használatát jól jellemzi, hogy egy szintén 2013-ban készült felmérés szerint a Facebookon 41 ezer post jelenik meg másodpercenként, a Twitteren 278 ezer üzenet percenként, az Instagramra 3600 fotót töltenek fel ugyanennyi idő alatt, és egyetlen perc elég ahhoz is, hogy az interneten 204 millió levelet küldjenek el. [81]

Hosszan lehetne még sorolni a felhő alapú 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

DOI azonosító: 10.17625/NKE.2015.021

szerveknek a felhő alapú rendszerekkel a lehetséges felhasználás mellett akár a védett vezetők információbiztonságának emelése, akár a törvényes ellenőrzés biztosítása okán is foglalkozniuk kell.

Összegzés, következtetések

Az első fejezetben több példát is bemutattam a felhő alapú rendszerekre, meghatároztam, hogy mit is jelent pontosan a felhő alapú informatika, milyen elfogadott modellek léteznek, azok mentén hogyan csoportosíthatóak az ilyen elven működő rendszerek, ezeknek melyek a sajátosságai, milyen jellemezőkkel írhatóak le. A szolgáltatási és telepítési modellek esetében meghatároztam az egyes típusok előnyeit, hátrányait, úgy, hogy **egységesen összefoglaltam a szakirodalomban található, meglehetősen heterogén, sokszor hiányos és nem konzekvens felsorolásokat, amelyet kiegészítettem saját gondolataimmal**. Ez így már véleményem szerint **kellő alapot ad arra**, hogy a szolgáltatási és telepítési modellekből képezhető mátrixban **elhelyezzünk egy kínált szolgáltatást**, vagy **kiválasszuk** az igényeinknek **leginkább megfelelő modellt**.

A rendvédelmi szervek – főleg biztonság szempontjából – magasabb követelményei miatt fontosnak tartom az általános meghatározásokon túlmenő, a szűkebb, rájuk szabott felhő alapú rendszerek pontosabb definiálását. Ennek érdekében először **értékeltem a kormányzati felhőre adott meghatározásokat**, hiszen ezeknél már figyelembe vették a specializált felhasználást és az átlagosnál magasabb biztonsági követelményeket. **Megállapítottam, hogy jelenleg nincs egységesen elfogadott meghatározás a kormányzati felhőre**. A létező definíciók pedig sokkal inkább körülírják ezt a fogalmat, sem mint pontos meghatározást adnak rá, ráadásul a meglévő definíciók esetében több tényező megjelenítésével nem értek egyet. Éppen ezért **saját meghatározást adtam először a kormányzati felhő, majd ebből kiindulva a rendvédelmi felhő fogalmára**.

A fejezetben **tisztáztam** azt is, hogy **mi a különbség egyrészt a felhő alapú rendszerek és a hagyományos ICT rendszerek virtualizációja**, másrészt a felhő alapú rendszerek és **a kiszervezett ICT rendszerek és szolgáltatások**, harmadrészt a felhő alapú rendszerek és **az internet-technológiára épülő szolgáltatások között**. Ennek kapcsán rámutattam, hogy a hagyományos ICT rendszerek virtualizációjára úgy tekinthetünk, mint egy közbenső állomásra a hagyományos rendszerek és a felhő alapú rendszerek használata között. Ha már használjuk ezt a technológiát, akkor az első lépést megtettük a felhő alapú rendszerek alkalmazása felé, ám ez utóbbiak összes előnyét még nem élvezhetjük. Megállapítottam, hogy a felhőre úgy lehet tekinteni, mint a kiszervezés egy formájára, azaz a felhő alapú rendszerek

DOI azonosító: 10.17625/NKE.2015.021

használata az ICT kiszervezések részhalmazát képezik. **Megállapítottam** azt is, **hogy jelenleg nem lehet éles határvonalat húzni az internet-technológiára épülő szolgáltatások és az annak részhalmazát képező PC/SaaS rendszerek között**. Sőt, 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.

Már itt előrebocsátom, hogy **a dolgozatban** bár **a felhő alapú rendszerekre fókuszálok**, mégis **többször kitekintek a szűken vett felhő alapú rendszerekből**. Ennek oka, hogy sem az infokommunikációs rendszerek törvényes ellenőrzési lehetőségei, előírásai, sem az információbiztonsági felkészítés tartalmi elemeinek kidolgozása védett személyek számára témaköre nem tárgyalható érdemben úgy, hogy ne a tágabb értelmű internet-technológiára épülő szolgáltatásokról beszéljünk, valamint a személyi használatú infokommunikációs eszközöket, és azok tulajdonságait ne vegyük figyelembe. Éppen ezért a dolgozat céljának eléréséhez, amikor szükséges, akkor a kiterjesztőbb értelmű internet-technológiára épülő szolgáltatások megfogalmazást használom, de egyértelműen beleértve és kiemelten kezelve a PC/SaaS rendszereket.

A felhő alapú rendszerek pontos meghatározására, megkülönböztetésére a további fejezetek érdemi tárgyalása miatt volt szükség, hiszen az első kettő a nemzetbiztonsági szolgálatok és a rendvédelmi szervek számára a felhő alapú rendszerek lehetséges felhasználásához, míg a harmadik elsősorban a felhő alapú rendszerek törvényes ellenőrzésének kialakíthatóságához, valamint védett vezetők információbiztonsági védelmének emeléséhez ad a későbbiekben segítséget.

Márpedig ezen feladatok elvégzésére szükség van, hiszen a fejezet utolsó részében az iparági tendenciák és előrejelzések figyelembevételével **bizonyítottam, hogy a nemzetbiztonsági szolgálatoknak, a rendvédelmi szerveknek a felhő alapú rendszerekkel akár a lehetséges felhasználás, akár a védett vezetők információbiztonságának emelése, akár a törvényes ellenőrzés biztosítása okán foglalkozniuk kell**.

Összefoglalásként elmondható, hogy **a felhő alapú informatikai rendszerek** megjelenése és **használata megkerülhetetlennek tűnik a rendvédelmi szervek esetében**. A fent említett nagy iparági beruházások nyomán kialakult, kialakuló sok fajta és széles szolgáltatási palettát kínáló felhő alapú informatika az eddigieknél olcsóbban képes a jelenlegi számítástechnikai igények kielégítésére, vagy akár a meglévőknél több, újabb feladat ellátására. Ez és a rendvédelmi szervek rendelkezésére álló, behatárolt ICT-re fordítható költségvetés olyan hívószavak, amelyek miatt a felhő alapú rendszerek bevezetése biztosra vehető. Ugyanakkor

DOI azonosító: 10.17625/NKE.2015.021

ez a szimpla megállapítás újabb kérdéseket vet fel (pl. biztonság tekintetében), amelyeket meg kell válaszolni, mielőtt megkezdjük egy ilyen rendszer tervezését, bevezetését.

A lehetséges használat kapcsán át kell tekinteni, hogy a felhő alapú rendszerek milyen biztonsági jellemzőkkel írhatók le, azokat csoportosítani és pontosan definiálni kell. Ezek után kell meghatározni a rendvédelmi szervek számára relevánsakat, majd a szolgáltatási-telepítési modell mátrixból kiválasztani azt, amely biztosítja, hogy a kívánt ICT szolgáltatásokhoz a megfelelő biztonság mellett a jelenleginél olcsóbban jussunk hozzá. A kiválasztás után pontosítani kell az elvárt üzem-, és adatbiztonsági kritériumokat, és azokat olyan technikai és jogi megoldásokkal körülbástyázni, amely lehetővé teszi, hogy egy adatot az, és csak az érhessen el, aki arra jogosult, ő viszont midig, amikor szükséges, az adat teljes életciklusában. Különös tekintettel kell lenni arra, hogy harmadik fél illetéktelenül ne férhessen hozzá az adatokhoz (és ez sokszor nem, vagy nem csak a szolgáltató feladata), ugyanakkor adott esetekben a törvényes ellenőrzést biztosítani kell.

A védett vezetők információbiztonságának emelése kapcsán át kell tekinti a védett vezetők információbiztonsági védelmének főbb kérdéseit, körülhatárolni a veszélyek szempontjából vizsgálandó személyi használatú hordozható infokommunikációs eszközöket, valamint internet-technológiára épülő szolgáltatásokat, majd számba venni az elemezendő biztonsági kategóriákat. Az így megadott kritériumok alapján össze kell foglalni az említett eszközök és szolgáltatások használata során jelentkező veszélyeket, ez alapján lehet pontosítani a személyre szabott felkészítés keretrendszerét, majd felállítani egy lehetséges, az említett eszközök és szolgáltatások használatára vonatkozó biztonságtudatossági felkészítés módszerét.

A törvényes ellenőrzés biztosítása kapcsán meg kell vizsgálni a hírközlés és a kommunikáció viszonyát, a jelenleg is zajló strukturális változásokat, valamint az ezek kapcsán a törvényes ellenőrzés végrehajtásában jelentkező problémákat. Ezt követően át kell tekinti az említett rendszerek törvényes ellenőrzésének kihívásait, majd meg kell vizsgálni a törvényes ellenőrzéshez rendelkezésre álló technikai lehetőségeket, felállítani az ezek elemzéséhez szükséges szempontrendszert, és az így kialakított szempontrendszer alapján elvégezni azok elemzését. A kommunikáció strukturális változása indukálja a vonatkozó törtvények módosítását is, az elvégzett elemzések alapján javaslatot lehet tenni az ezeknek és a törvényes ellenőrzés szempontjainak is megfelelő, akár jogszabályba is illeszthető új szolgáltatói kör meghatározására.

DOI azonosító: 10.17625/NKE.2015.021

2. A felhő alapú rendszerekkel kapcsolatos biztonsági ajánlások összehasonlítása és a biztonsági vizsgálatukhoz szükséges követelményrendszer megalkotása

A felhő alapú rendszerek terjedése új kihívásokkal állítják szembe a rendvédelmi szerveket, amelyekből az egyik a használathoz kapcsolódó biztonság kérdése. Ez azért lényeges számukra, mert – ahogy azt az első fejezetben bemutattam – a felhő alapú 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, [82] fenntartva kiemelt igényüket a magas szintű biztonság iránt.

Azonban a felhő alapú 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 [83] nem fedik le teljes mértékben az újonnan jelentkező problémákat, az ott alkalmazott megoldások pedig nem vagy nem teljes mértékben használhatók a felhő alapú 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 felhő alapú 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 célszerűnek tartom egy olyan elsődleges biztonsági vizsgálattal kezdeni, amely egységes elvek mentén, egy átfogó kérdéssor segítségével képes tisztázni, hogy 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 szervezet specifikus, részletes felmérés, amely már azt hivatott megmondani, hogy 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 elsődleges biztonsági vizsgálat kialakításához első lépéseként szükségesnek tartom egy egységes alapkövetelmény-lista elkészítését. Ennek érdekében elemezni kell, hogy a felhő

DOI azonosító: 10.17625/NKE.2015.021

alapú rendszerek milyen kockázatokat rejtenek, milyen biztonsági jellemzőkkel írhatók le, azokat csoportosítani kell, majd ezekből a rendvédelmi szervek számára relevánsakat kiválasztva és az egyéb szükséges elemekkel kiegészítve kell meghatározni az ebben a szektorban elfogadható és használható alapkövetelmény-listát.

A második fejezetben ennek érdekében elemzem és értékelem a fejlett országok felhő alapú rendszerekkel foglalkozó nemzeti-, és a nemzetközi szervezetei által megalkotott, nyíltan elérhető, releváns biztonsági ajánlásokat, majd ezek felhasználásával, továbbgondolásával és –fejlesztésével kidolgozok egy olyan sablont, amellyel a felhő alapú rendszerek elsődleges biztonsági elemzése egységes keretek között és teljes körűen végrehajtható.

2.1. Biztonsági kérdések – alapok

A felhő alapú 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 felhő alapú 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 célszerűnek tartom 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 biztonsági követelményrendszer, amellyel a felhő alapú rendszerek elsődleges vizsgálata elvégezhető, azok használatának, alkalmazásának kockázatai felmérhetőek.

Az egyes szervezetek nem egységesen, és főleg nem a rendvédelmi szervek szempontjából közelítik meg a felhő alapú rendszerek biztonsági kérdéseit. 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 sablon elkészítéséhez is, hiszen az ott megfogalmazottak megfelelő újragondolással és átalakítással felhasználhatók ahhoz.

A továbbiakban, a biztonsági kockázatok feltárását, azonosítását a középpontban tartva, a felhő technológiában 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.

DOI azonosító: 10.17625/NKE.2015.021

2.1.1. A Cloud Security Alliance fontosabb ajánlásai

A Cloud Security Alliance (CSA) az iparági szakemberek, vállalatok és más érintettek széles koalíciója által vezetett non-profit szervezet. Küldetése egyrészt, hogy támogassa a felhő alapú 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 fehérkönyvüket 2009-ben tették közzé. [84]

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 felhő alapú rendszerek biztonságával kapcsolatban. Ahogyan a felhő alapú rendszerek meghatározásánál és kategorizálásánál a NIST Információtechnológiai Laboratóriuma a „The NIST Definition of Cloud Computing" [27] címen kiadott tanulmánya egy általánosan elfogadottnak és kvázi-szabványnak tekinthető, úgy a biztonság kapcsán a CSA „Security Guidance for Critical Areas of Focus in Cloud Computing" [85] című kiadványáról mondható el ugyanez.

A dokumentumban a felhő alapú rendszerekkel kapcsolatos biztonsági kérdéseket alapvetően 13 területre osztják, amelyeket 2 fő részbe csoportosítanak: irányításiba és üzemeltetésibe. Az irányítás részben az általuk stratégiainak, míg az üzemeltetési részben a taktikainak tartott biztonsági kérdésekre koncentrálnak. A CSA által definiált területeket és azok rövid leírását az alábbi, 1. és 2. táblázat tartalmazza:

TERÜLETEK	LEÍRÁS
Irányítás és vállalati kockázat kezelés	A szervezet azon képességéről szól, amely segíti, hogy irányítsa és mérje azokat a vállalati kockázatokat, amelyeket a felhő alapú rendszer bevezetése jelent. Olyan elemeket tartalmaz, mint a szerződés megszegésének jogesete, 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 az, hogy a nemzetközi határok hogyan hatnak ezekre a kérdésekre.
Jogi kérdések: szerződések és elektronikus felderítés	Lehetséges jogi kérdésekről szól a felhő alapú rendszerek használatakor. Ennek a résznek a kérdései érintik az információ és a számítógépes rendszerek védelmének követelményeit, biztonsági események közzétételének törvényi előírásait, egyéb szabályozási követelményeket, adatvédelmi követelményeket, nemzetközi törvényeket stb.

DOI azonosító: 10.17625/NKE.2015.021

TERÜLETEK	LEÍRÁS
Megfelelőség és audit	A megfelelőség fenntartásáról és növeléséről szól a felhő alapú 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.
Információmenedzsment és adatbiztonság	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. Említésre kerülnek olyan egyéb tényezők is, mint az, hogy ki a felelős az adatok bizalmasságáért, sértetlenségéért és rendelkezésre állásáért.
Hordozhatóság és interoperabilitás	Az adatok, szolgáltatások egyik szolgáltatótól a másikhoz, vagy adott esetben a felhasználó szervezethez történő visszamozgatásának képességéről szól. Ezeket együtt tárgyalja a szolgáltatók közötti interoperabilitás kérdéseivel.

1. táblázat. A CSA által definiált irányítási területek.[19]

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 felhő alapú rendszerek hol segíthetnek csökkenteni az aktuális kockázatokat és mely területeken növelik azokat.
Adatközpont működés	Arról szól, hogyan lehet értékelni a szolgáltató adatközpontjának architektúráját és működését. Segít azonosítani az adatközpontok közös jellemzőit, amelyek károsan hatnak az éppen futó szolgáltatásokra, vagy melyek azok a jellemzők, amelyek alapvetően meghatározóak a hosszú távú stabilitáshoz.
Incidenskezelés, riasztások, kárelhárítás	Megfelelő incidensérzékelésről, reagálásról, értesítésről és kármentésről szól. Tartalmazza azokat az elemeket, amelyek 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, or IaaS).

[19] Szerkesztette a szerző. Forrás: [85] p. 23.

DOI azonosító: 10.17625/NKE.2015.021

TERÜLETEK	LEÍRÁS
Titkosítás és kulcskezelés	A megfelelő tikosítás használatról és a megfelelő, skálázható kulcsmenedzsment azonosításáról szól.
Azonosítás és hozzáférés kezelés	Azonosítók és az azonosításhoz szükséges szolgáltatások menedzselése a hozzáférés-szabályozás biztosítása érdekében. A terület olyan kérdésekre fókuszál, amelyek segítségével megállapítható a szervezet felkészültsége a felhő alapú azonosítás, jogosultság és hozzáférés-kezelés menedzselésére.
Virtualizáció	A virtualizációs technológia használatáról szól a számítási felhőben. A terület olyan kérdéseket taglal, mint a több-felhasználós környezet kockázatai, a virtuális gépek izolációja, hypervisor sérülékenységek stb., azaz a fókuszában a rendszer és hardver virtualizáció biztonsági kérdései állnak.
Biztonság, mint szolgáltatás (Security as a Service)	A felhasználónak egy külső fél nyújtotta, biztonságot szavatoló, incidenskezelési, megfelelőség igazolási, valamint azonosítás és hozzáférés-szabályozási funkciók szolgáltatásáról szól. A biztonság, mint szolgáltatás az észlelésnek, a kármentésnek, és a biztonsági infrastruktúra irányításának az átruházása egy megfelelő eszközökkel és szakértelemmel rendelkező, megbízható harmadik félre.

2. táblázat. A CSA által definiált üzemeltetési területek.[20]

A CSA 2009 áprilisában adta ki először fent említett dolgozatát, amelynek V3.0 változatát 2011-ben tette közzé. Ez utóbbiban már újdonságként megjelent a Biztonság, mint szolgáltatás azaz Security as a Service (SecaaS) fogalma is (2. táblázat utolsó területe). Ennek bevezetésére a szerzők szerint azért van szükség, mert míg a felhő alapú rendszerek biztonságról szóló fejtegetések túlnyomóan arra fókuszálnak, hogyan migráljunk felhőbe, hogyan biztosítsuk a bizalmasságot, 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 Group-ja a „Defined Categories of Service 2011" [86] című tanulmányt, 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:

[20] Szerkesztette a szerző. Forrás: [85] p. 24-25.

DOI azonosító: 10.17625/NKE.2015.021

KATEGÓRIÁK	LEÍRÁS
1. kategória: azonosítás, jogosultság és hozzáférés-kezelés (IAM)[21]	Az azonosítás, jogosultság és hozzáférés-kezelésnek biztosítania kell a kontrollt az azonosítók és a hozzáférés-menedzsment felett.
2. kategória: 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. kategória: web biztonság	A web biztonság a felhasználó telephelyén telepített és futtatott szoftver, alkalmazás segítségével, vagy a teljes web-forgalom felhőszolgáltatóhoz történő átirányításával és ott történő ellenőrzésével valósít meg valós idejű védelmet.
4. kategória: email biztonság	Az email biztonság kontrollt biztosít a bejövő és a 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. kategória: biztonságértékelés	A biztonságértékelés a felhőszolgáltatások harmadik fél általi auditja, vagy a felhasználó telephelyén lévő rendszerek értékelése iparági szabványokon alapuló felhőszolgáltató megoldásokon keresztül.
6. kategória: behatolás-kezelés	A behatolás-kezelés 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.

[21] IAM: Identity and Access Management azonosítás és hozzáférés-kezelés

DOI azonosító: 10.17625/NKE.2015.021

KATEGÓRIÁK	LEÍRÁS
7. kategória: Biztonsági információs és eseménykezelő rendszer (SIEM[22])	Biztonsági információs és eseménykezelő rendszerek (push vagy pull mechanizmus segítségével) fogadják a naplóadatokat és eseményinformációkat. Ezeket az információkat korreláltatják 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 azok manipulálását és így azok felhasználhatók legyenek bizonyítékként a későbbi nyomozás során.
8. kategória: titkosítás	A titkosítás egy kriptográfiai algoritmust felhasználó adatkódolási folyamat, amelynek eredményeképpen titkosított adatok jönnek létre.
9. kategória: üzletmenet-folytonosság és katasztrófa-elhárítás	Az üzletmenet-folytonosság és katasztrófa-elhárítás olyan intézkedéseket takar, amelyek tervezésével és végrehajtásával biztosítható a működés rugalmassága bármilyen szolgáltatás megszakadása, szünetelése esetén.
10. kategória: hálózatbiztonság	A hálózatbiztonság olyan biztonsági szolgáltatásokból áll, mint a hozzáférések kiosztása, ellenőrzése és a szolgáltatás-erőforrások védelme. Architektúrálisan, a hálózatbiztonság olyan szolgáltatásokat nyújt, amelyek a hálózatok biztonsági kontrolljával foglalkoznak az egyedi hálózatok mögöttes erőforrásainak egyedi vagy összevontan történő figyelembe vételével.

3. táblázat. A CSA által definiált SecaaS kategóriák.[23]

Ebben a két dokumentumban is jól megfigyelhető, hogy átfedések vannak az alapdokumentumban megadott területek és a „Security as a Service" területnél leírt kategóriák között (pl. azonosítás és hozzáférés menedzsment, titkosítás stb.). Ezek az átfedések több dolgot is jeleznek. Egyrészt, hogy a hagyományos ICT biztonsági elemek egy része a felhő alapú rendszerek esetében is használható, másrészt, hogy a felhő alapú rendszerek biztonsági

[22] SIEM Security information and event management Biztonsági információs és eseménykezelő (szoftver) rendszer
[23] Szerkesztette a szerző. Forrás: [86]

DOI azonosító: 10.17625/NKE.2015.021

problémái mennyire újszerűek, és még nincsenek teljesen egzakt elhatárolások, definíciók, standardok. Ezen utóbbiak kimunkálásán dolgoznak az iparág szereplői, beleértve olyan szervezeteket is, mint a CSA, az ETSI[24] vagy az ITU.[25]

Mivel a SecaaS akár egy, a felhasználó által igénybe vett felhő alapú 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" címűben leírtakat.

A két dokumentum kapcsán az is megállapítható, hogy a CSA ezekben a gazdasági társaságokra koncentrálva, iparági megközelítéssel, a szolgáltató szempontjából dolgozza fel a felhő alapú rendszerek biztonsági kérdéseit. Így ezek ugyan sok hasznos információt tartalmaznak az egyik kutatási célkitűzés eléréséhez, azaz a rendvédelmi szervek szempontjából összeállítandó követelményrendszer kialakításához, de nyilvánvalóan ezen szervezetek sokkal szigorúbb feltételeit nem veszik, nem vehetik figyelembe. Véleményem szerint pontosan ezen, sokkal szigorúbb biztonsági igény miatt más, és nem a CSA által leírt csoportosítást érdemes majd a kritériumrendszer felállításakor használni. Itt már ugyanis figyelembe lehet és kell venni a hatályos szabályozókból valamint a gazdasági társaságoktól jelentősen eltérő működési rendből adódó specialitásokat, így a jelenlegi szervezeti és működési folyamatokhoz jobban illeszkedő biztonsági elemző sablon állítható össze.

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

Az előző dokumentumok hasznos kiegészítőjeként szolgál a CSA Top Threats Working Group-ja által összeállított „The Notorious Nine Cloud Computing Top Threats in 2013" [87] című felmérése, amelyben azokat a legveszélyesebb felhőbiztonsági fenyegetéseket rangsorolják, amelyek a felhő rendszerek megosztott igény szerinti kiszolgálás természetéből adódnak. Ezekhez rövid leírást, értékelést, és olyan egyéb hasznos információkat is adnak, mint például, hogy melyik szolgáltatási modell érintett, vagy, hogy az adott veszéllyel hol foglalkoztak a korábban említett két dokumentumban. Az általuk azonosított legveszélyesebb fenyegetések sorrendben a következők:

[24] ETSI: European Telecommunications sztenders Institute Európai Távközlési Szabvány Intézet
[25] ITU: International Telecommunication Union Nemzetközi Távközlési Egyesület

DOI azonosító: 10.17625/NKE.2015.021

1. adatszivárgás,
2. adatvesztés,
3. azonosítók megszerzése,
4. nem biztonságos API[26]-k,
5. DoS[27] (túlterheléses támadás), DDoS[28] (elosztott túlterheléses támadás)
6. rosszindulatú belső munkatárs,
7. visszaélés a felhőszolgáltatással (például illegális jelszótörésre),
8. nem megfelelő átvilágítás, gondosság felhőszolgáltatás választásakor,
9. megosztott technológiából adódó sérülékenységek.

A dokumentumban leírt veszélyeket, valamint azok javasolt kezelési módjait célszerűnek tartom figyelembe venni a rendvédelmi szervek használata kapcsán felmerülő biztonsági elemzéskor is.

A felhő kockáztok felmérésében, értékelésében iparági alapdokumentumnak tekinthető CSA „Cloud Controls Matrix" táblázata [88] a hozzá tartozó információs lappal együtt [89]. Ez ugyan alapvetően a szolgáltatók számára készített útmutató, ha úgy tetszik, egy biztonsági ellenőrző lista, 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 felhő alapú rendszer használatához, harmadrészt pedig segítséget nyújt a felhő alapú rendszerek, valamint ezek szolgáltatóinál felmerülő kockázatok értékelésében. A „Cloud Controls Matrix" további nagy előnye, hogy 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, akár saját rendszerei biztonságával kapcsolatban. Éppen ezért, a „Cloud Controls Matrix"-ot, természetesen a megfelelő, a felhasználó oldalára történő átalakítással, megfeleltetéssel, de mindenképpen célszerű felhasználni a rendvédelmi szervek számára készítendő biztonsági elemző sablonhoz.

[26] API: application programming interface alkalmazásprogramozási felület. API segítségével lehetséges egy programrendszer szolgáltatásait használni anélkül, hogy annak belső működését ismerni kellene.
[27] DoS: Denial of Service, szolgáltatásmegtagadással járó támadás, vagy más néven túlterheléses támadás.
[28] DDoS: Distributed Denial of Service, elosztott szolgáltatásmegtagadással járó támadás, vagy más néven elosztott túlterheléses támadás.

DOI azonosító: 10.17625/NKE.2015.021

2.1.2. A NIST fontosabb ajánlásai

A NIST az Egyesült Államok legrégibb fizikai kutató laboratóriuma, amely ma a Kereskedelmi Minisztérium alatt, szövetségi ügynökségként dolgozik. 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 itt élő emberek életminősége. Elért eredményeiket számos területen kamatoztatják, így az egészségügyi nyilvántartásoktól kezdve az atomórákon és nanoanyagokon át a számítógépes chipekig számtalan termék és szolgáltatás használja a NIST által kidolgozott technológiákat, szabványokat. A szervezet meghatározó szerepet játszik a felhő alapú rendszerekkel kapcsolatos szabványok és ajánlások kidolgozásában is. [90]

Ez utóbbi kapcsán a NIST számos dokumentumot készített, amelyek nemcsak a felhő alapú rendszerek definiálásakor, hanem a kritikus biztonsági elemek azonosításában is segítenek. A felhő alapú rendszerekkel kapcsolatban megjelentetett dokumentumait a szervezet alapvetően három kategóriába sorolja:

- NIST Special Publication 500 Series, amelyben a különböző szabványokhoz és referencia architektúrákhoz kapcsolódó anyagokat teszik közzé,
- NIST Special Publication 800 Series, amelyben a biztonsági kérdésekkel foglalkozó anyagok találhatóak,
- NIST Cloud Computing Research Papers, amelyben kutatási anyagaikat publikálják. [91]

Ezek közül a dolgozat célkitűzése szempontjából a legfontosabb a NIST 800-144 „Guidelines on Security and Privacy in Public Cloud Computing” [92] című, 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 több-felhasználós 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 felhő alapú rendszer bevezetéséhez, hiszen bemutatja azokat a fontosabb lépéseket, amelyeket ennek kapcsán meg kell tenni,

DOI azonosító: 10.17625/NKE.2015.021

egyben felhívja a figyelmet azokra a biztonsági kockázatokra és tényezőkre is, amelyeket az egyes lépések során mindenképpen elemezni és értékelni kell.

A NIST 800-144 számú dokumentuma összefoglalja a nyilvános felhő veszélyeit, technológiai kockázatait, azok kezelését. Az itt megfogalmazottak szerint egy felhő alapú 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.

A biztonsági lehetőségek értékeléséhez kockázat alapú megközelítés szükséges, amelyhez pontosan meg kell érteni a felajánlott felhőkörnyezetet, azaz a szolgáltatói által kínált technikai kontrollokat, eljárásokat és előírásokat, valamint a rendszer architektúráját. Ha szükséges, akkor 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, szerződésből való kilépés lehetőségei, titkosítás, törvényeknek megfelelés stb.

Természetesen a felhasználónak más teendői is vannak, hiszen meg kell győződnie arról is, hogy a felhő alapú rendszer felhasználó oldali környezete is megfelel a szervezet biztonsági előírásainak. Itt olyanokat is vizsgálni kell, mint az eléréshez használt böngésző sérülékenységei, a beágyazott mobil alkalmazások biztonsága, stb.

A teljes – a felhő alapú 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, és veszélyek kezeléséről, a kockázatértékelés és –kezelés menetéről, az ott használt kvalitatív és kvantitatív faktorokról, valamint arról, hogy a teljes rendszer képes biztosítani az adatok bizalmasságát.

A felhő alapú rendszer bevezetését 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 bír, bírhat akár a hagyományos ICT rendszerekkel szemben is. Ilyenek az erre specializálódott szakembergárda megléte a szolgáltatónál, az erős egységes, a speciális előírásokat is sok

DOI azonosító: 10.17625/NKE.2015.021

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, és 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, több-felhasználós környezet, a szintén könnyen támadható interneten keresztüli szolgáltatás-elérés, 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 nem csak a sokféle elem támadhatóságától, hanem azok egymás közötti interakcióitól is függ.

A NIST által azonosított, a nyilvános felhő alkalmazáskor kulcsfontosságúnak tekintett biztonsági és adatvédelmi kérdéseket 4. számú táblázat tartalmazza.

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.
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 (ESI)[29] 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

[29] ESI: Electronically Stored Information elektronikusan tárolt információk

DOI azonosító: 10.17625/NKE.2015.021

TERÜLETEK	LEÍRÁS
	meg kell, hogy legyen a bizalom a szolgáltató felé, ugyanakkor a felhasználó szervezet 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 (pl.: SaaS szolgáltatás nyújtása, más szolgáltató IaaS, vagy PaaS rendszerére alapozva), alvállalkozói kérdések, • az átláthatósághoz és a folyamatos ellenőrzéshez biztosított eszközöket, módszereket, • a kiegészítő adatok védelmét (pl.: felhasználói tevékenység adataiét, vagy mondjuk a bejelentkezési adatok lopás, phising elleni védelmét), • kockázatkezelést.
architektúra:	az alábbi vizsgálandó kérdéseknél tekintettel kell lenni a szoftver-, és a hardver környezetre, valamint a szolgáltatási modellre is: • a virtualizált környezetből adódó új támadási felületek (pl. új API-k, új csatornák, új adatfajták), • a virtuális hálózatok védelme (pl. virtuális gépek egymás közötti kommunikációjának védelme, biztonsági beállítások és adminisztrátori jogosultságok szétválasztása), • a virtuális gépek rendszermásolatai (image) (pl. ezek napra készen tartása, sérülékenységek és új szoftververziók miatt), • a kliens oldal védelme (pl. kliens oldali fizikai és

DOI azonosító: 10.17625/NKE.2015.021

TERÜLETEK	LEÍRÁS
	logikai védelem, használt web böngésző plug-in-ek, közösségi oldalak használatának engedélyezése).
azonosítás és hozzáférés menedzsment:	itt elsősorban a meglévő hagyományos rendszer és a felhő alapú rendszernél alkalmazott eljárások azonossá tételének vagy egyformára alakításának az előnyeit, hátrányait kell számba venni, az alábbiak tekintetében: • hitelesítés (pl. használt protokollok, mint SAML,[30] az ezeket kihasználó támadási lehetőségek, mint az „XML[31] wrapping attack”, azonosítási szolgáltató használata, azonosító adatok cseréje felhő alapú rendszer és a meglévő hagyományos hálózat között), • hozzáférés szabályozás (pl. SAML mellett használt hozzáférés-szabályozó protokollok, mint XACML,[32] az ezeket kihasználó támadási lehetőségek, mint az ismétléses, vagy visszajátszásos támadás).
szoftver-elválasztás:	a több felhasználós környezet megköveteli a felhasználók szétválasztását, amelyeket az alábbiak mentén célszerű vizsgálni: • hypervisor komplexitása (pl. futó folyamatokat felügyelő szoftverek tulajdonságai), • lehetséges támadási vektorok (pl. hypervisor fertőzése virtuális gépből, közbeékelődéses támadás (MitM),[33] memóriatartalom módosítása).
adatvédelem:	a több felhasználós környezetbe vitt (érzékeny) adatoknak a többi felhasználóval szembeni védelmét az alábbiak szerint érdemes vizsgálni:

[30] SAML: Security Assertion Markup Language
[31] XML: eXtensible Markup Language
[32] XACML: eXtensible Access Control Markup Language
[33] MitM: Man in the Middle, azaz közbeékelődéses támadás

DOI azonosító: 10.17625/NKE.2015.021

TERÜLETEK	LEÍRÁS
	• az értékkoncentrációból adódó direkt és indirekt támadási lehetőségek (pl. exploitok, rendszergazdák által használt közösségi oldalak támadása és indirekt módon hozzáférési jogosultság-szerzés, DoS támadás, fizikai támadás), • adatizoláció (számtalan kérdéskört kell megvizsgálni ennek kapcsán pl. 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" [93] alapján), • adatmegsemmisítés (pl. felülírás, hardver megsemmisítés lehetőségei, szerződéses feltételek).
rendelkezésre állás:	a hagyományos ICT rendszerekhez hasonlóan az alábbiakat célszerű vizsgálni: • átmeneti leállások (pl. szerződésben rögzített rendelkezésre állásból adódó kieső idő, tervezett karbantartások ideje, biztonsági mentések, katasztrófa utáni visszaállítás, esetleg másik felhőszolgáltatóra átállás), • hosszantartó és folyamatos leállás (pl. szolgáltató leállása, csődje, létesítmény elvesztése, katasztrófaterv), • DoS támadás (pl. külső támadás esélye, belső támadás lehetősége, mind szándékos, mind véletlen támadás esetén)
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 (pl. nem

DOI azonosító: 10.17625/NKE.2015.021

TERÜLETEK	LEÍRÁS
	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 (pl. nyomozati másolat készítése incidens után, támadási vektor azonosítása, a történtek rekonstruálása, gyors helyreállítás, incidenskezelési felelősségek, bizonyítékgyűjtési lehetőségek és hiányosságok, jelentési kötelezettségek a CERT[34] felé, azok tartalma).

4. táblázat. A NIST által meghatározott kulcs biztonsági és adatvédelmi kérdések.[35]

A felhő alapú rendszer bevezetése kapcsán a szerzők további számos, a rendvédelmi szervek részére készítendő biztonsági elemző sablonhoz is hasznos, biztonsági kockázatra és tényezőre hívják fel a figyelmet. Így a fenti, a felhő alapú 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,*
- *fizikai és logikai hozzáférés-szabályozás,*
- *hálózati hozzáférés-szabályozás, kapcsolat és szűrés,*
- *adatvédelem,*
- *rendszerkonfiguráció és a javítócsomagok kezelése,*
- *biztonsági mentés és visszaállítás,*

[34] CERT: Computer Emergency Readiness Team vagy számítógépes katasztrófa-elhárító csoport
[35] Szerkesztette a szerző. Forrás: [92]

DOI azonosító: 10.17625/NKE.2015.021

- *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".*[36]

A biztonság lehető legteljesebb körű megteremtéséhez a szolgáltatóval tisztázni kell a felelősség körök megosztását, amely nagyban függ szolgáltatási modelltől. Meg kell tőle követelni és ellenőrizni kell a katasztrófa-elhárítási és 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 elvégezni a biztonsági és adatvédelmi szempontú kockázatértékelést, amelynek az alapja a szolgáltatási modell, a szolgáltatás célja, hatálya, a hozzáférés típusa, szintje, a szolgáltató és 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, ott csupán általánosságban foglalkozik a kormányzati szervekkel. Amennyiben az értékelést követően előálló kockázati szint túl magas, akkor 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:

[36] Szerkesztette a szerző. Forrás: [92] p. 43.

DOI azonosító: 10.17625/NKE.2015.021

- *„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.*”[37]

A dokumentum készítői kiemelik, hogy felhő rendszereknél 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, hogy a biztonsági és adatvédelmi kontroll korrektül, az elvárásinak megfelelően működik. Ugyanakkor ügyelni kell arra, hogy – a kockázatalapú megközelítésnek megfelelően – a biztonsági és adatvédelmi megoldások és a használhatóság között megmaradjon az egyensúly, a felhő előnyei ne vesszenek el, az hatékonyan használható maradjon. Ha ez már nem biztosítható, akkor nem szabad felhő alapú rendszert használni.

A NIST ezen dokumentumának több érdeme is kiemelhető. Egyrészt a biztonsági és adatvédelmi problémák a nyilvános felhőben jelentkeznek a legerősebben. Ennek megfelelően az itt végiggondolt elemek jól használhatóak 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 felhasználáskor 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

[37] Szerkesztette a szerző. Forrás: [92] p. 48.

DOI azonosító: 10.17625/NKE.2015.021

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 ott honos és 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, a CSA ajánlásai kapcsán már megfogalmazott megfelelő átalakításokat ebben az esetben is szükségesnek és elkerülhetetlennek tartom.

2.1.3. 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 weboldalt [94] az Egyesült Államok kormánya hozta létre FedRAMP[38] (Federal Risk and Authorization Management Program) [95] nevű program keretében. Ez egy kormányzati szintű program, amely a felhő szolgáltatások biztonsági értékeléséhez és ellenőrzéséhez kínál szabványosított megközelítést. Mindezt a "csináld egyszer, használd sokszor" megközelítés jegyében, azaz a kormányhivataloknak nem kell külön-külön összeszedni a felhő alapú rendszerek biztonságos használatához szükséges kritériumokat, követelményeket, azt elkészítik és elérhetővé teszik számukra a kormányprogram keretében.

Ennek kapcsán meg kell jegyezni, hogy a FedRAMP nagyban támaszkodik a program egyik kulcsszervezeteként megjelölt NIST dokumentumaira. Ugyanakkor bár maga a FedRAMP, valamint a cloud.cio.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 weboldal tematikusan végigvezeti az érdeklődőket a legfontosabb témákon, így megismertet a felhő alapú rendszerekkel kapcsolatos legszükségesebb tudnivalókkal, bemutatja a felhőszolgáltatásokat, végigvezet a kiválasztott szolgáltatások felhőbe helyezésén, ismerteti, hogyan menedzselhetjük a felhőnket, majd elemzi azok biztonsági kérdéseit. Ennek kapcsán itt is több, a rendvédelmi szervek részére készítendő biztonsági elemző sablonhoz is felhasználható információt, szempontot, kockázatot ismerhetünk meg. Így például a felhőszolgáltató értékelése, kiválasztása kapcsán megjelenők közül az alábbiakat:

[38] FedRAMP Federal Risk and Authorization Management Program (Szövetségi Kockázat és Jogosultságkezelési Program)

DOI azonosító: 10.17625/NKE.2015.021

- a szolgáltatás robusztussága (ellenálló képesség, redundancia, megbízhatóság, rendelkezésre állás, szolgáltatási szint, adatközpontok helye, biztonsági mentések és adat-helyreállítás, katasztrófa-elhárítás, üzletmenet-folytonossági terv stb.),
- a kínált és szükséges biztonsági intézkedések (hozzáférési pontok, biztonsági értékelések és jogosultságok, folyamatos ellenőrzés, biztonsági ellenőrzések implementálása stb.),
- megfelelőség biztosítása (törvényi, iratkezelési, adatvédelmi, elektronikus felderítési stb.),
- adatokkal kapcsolatos biztonsági meggondolások (tulajdonjog, adatok migrációja, adatok biztonsága és adatvédelem, biztonsági tesztelések célja és hatálya, hibajavítások, adatmegőrzés és törlés, interoperabilitás, stb.),
- a szolgáltató stabilitása (pénzügyi stabilitás és a szolgáltató múltbeli pénzügyi teljesítménye, ismeretlen tényezők és kockázatok elfogadása, harmadik fél bevonása, igazolások stb.).

A cloud.cio.gov oldalon található, az általuk azonosított felhő alapú rendszerek biztonsági kihívásai közül a következőket érdemes biztonsági elemző sablonhoz figyelembe venni:

- az adatok diszperziója és ehhez kapcsolódóan a nemzetközi adatvédelmi törvények,
- a szolgáltatási szint garantálásának problémái,
- biztonságos hypervisor-októl való függés,
- a kormányzat által használt felhő alapú rendszer vonzó célpontja a hackereknek,
- a felhőben használt virtuális operációs rendszerek biztonsága,
- titkosítás szükségessége a felhő használatához, a felhő erőforrások felügyeletét szabályozó interfész, operációs rendszerek, alkalmazások, adatok eléréséhez,
- adatok tulajdonjoga,
- több-felhasználós környezet problémái, izoláció,
- naplózási kérdések,
- adatmegőrzési kérdések,
- az adatok kitetté válhatnak külföldi kormányoknak és hatósági eljárásoknak.

A felhő alapú rendszerek kormányzati szervezetek általi használatának bevezetésekor a legnagyobb kihívást éppen az általuk megkövetelt biztonsági szabványok és protokollok előírásaiban foglaltak elérése és betartása jelenti. Éppen ezért ebben az esetben kiemelt szerepe van a kockázatelemzésnek. A FedRAMP szakemberei által megfogalmazott talán egyik legfontosabb gondolat ezzel kapcsolatban az, hogy az elemzés eredményeként előálló

DOI azonosító: 10.17625/NKE.2015.021

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, az jobb költséghatékonyságot negligálhatja. A kockázatok értékelésénél a következőket javasolják a készítők alaposan megvizsgálni:

- milyen típusú felhőszolgáltatást választottunk,
- hogyan érjük el a felhőt,
- hogyan feleltethető meg a szervezet saját, meglévő biztonsági és adatvédelmi követelményeinek,
- hogyan lehet a felhőbe vitt adatok és alkalmazások tekintetében a számon kérhetőséget fenntartani.

Ezeket pedig szintén célszerűnek tartom biztonsági elemző sablon elkészítéséhez figyelembe venni. Ugyanakkor kiemelendő, hogy a kockázatok mélyebb elemzéshez, értékeléshez a FedRAMP szakemberei a – korábban már bemutatott – NIST 800-144 számú, „Guidelines on Security and Privacy in Public Cloud Computing" [92] című anyagát javasolják tanulmányozni.

Az amerikai kormányzati program kapcsán közzétett anyagokból további, egy felhő alapú 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 (pl. személyes adat, érzékeny adat stb.), valamint annak az országnak az 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 (pl. szolgáltató alvállalkozója) is akár teljes hozzáférése lehet az ide kivitt adatokhoz. Ugyancsak a szerződésben célszerű tisztázni, hogy mi a teendő incidens, vagy külföldi hatóság adatszolgáltatási megkeresése esetén, és itt kell rögzíteni az ezekhez kapcsolódó reagálási és értesítési időket is.

Nagy hangsúlyt kell helyezni a biztonságtudatossági képzésekre is. Ezeket kötelezővé kell tenni a felhőbe történő kihelyezéskor, majd periodikusán ismételve mindenki – felhasználó és a szolgáltató szakemberei – számára, akik érzékeny vagy személyes adattal kapcsolatba kerülnek. Előre rögzíteni kell a képzésben résztvevők körét, a képzési kategóriákat, azok gyakoriságát, a képzések igazolásának módját, valamint tisztázni kell az ezzel kapcsolatos költségek megosztását is.

DOI azonosító: 10.17625/NKE.2015.021

A felhőtechnológia okán megjelenő új kockázatok miatt folyamatos ellenőrzésre van szükség. 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. A folyamatos ellenőrzéshez a FedRAMP egy három lépésből álló – 1. működési átláthatóság vizsgálata, 2. változások ellenőrzése, 3. incidensreagálás – kockázatkezelési eljárását ajánlj.
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 és szabályai egyformák legyenek a teljes helyszíni-, és felhő-infrastruktúra tekintetében egyaránt. Ehhez meg kell állapodni, hogy a szervezeteknek és a szolgáltatónak milyen szabályokat és törvényeket kell alkalmaznia, valamint milyen gyorsan kell reagálni, detektálni, csökkenteni a kárt, visszaállítani az eredeti állapotot és jelenteni az eseményt. Ehhez célszerű, ha a szolgáltató SIEM rendszert használ.
A FedRAMP szakemberei hangsúlyosan kiemelik, hogy bár bizonyos felelősségek átruházhatók, vagy megoszthatók, azonban az adatok bizalmasságának, sértetlenségének, és rendelkezésre állásának a teljes felelősségét mindig a kormányzati szerv viseli.
A weboldal nagyon sok hasznos információval szolgál olyan, kifejezetten kormányzati szerveknek, amelyek felhő alapú szolgáltatást kívánnak igénybe venni. Ezekhez olyan kulcsfontosságú dokumentumokat és sablonokat is biztosít, mint az alkalmazandó szabályozókat és szabványokat is tartalmazó „Security Assessment Framework” [96], a folyamatos ellenőrzést részletesen leíró „Continuous Monitoring Strategy & Guide” [97] című dokumentumok, vagy a rendszer biztonsági tervezését segítő „System Security Plan (Template)” [98] sablon. Rendkívül fontosnak tartom azt a gondolatot, hogy minden kormányzati szerv egységes megközelítés alapján tudja értékelni a felhő alapú rendszereket, azok biztonsági kockázatait. Ez azért is lényeges, mert így nem adódhat elő az a hiba, hogy valamit éppen kifelejt a kockázatelemzéssel foglalkozó szakember. Mindemellett bizonyítja a kutatási célkitűzésem helyességét is. A másik itt is visszatérő és nagyon fontos elem maga a kockázatértékelés. A biztonság ugyanis pénzbe kerül és az adatokat, rendszereket mindig kockázat alapon kell védeni, legyen szó akár felhő, akár fizikailag a felhasználónál lévő rendszerekről, adatokról.
Ugyanakkor a weboldalon leírtak kapcsán figyelembe kell venni, hogy az az Egyesült Államokban lévő kormányzati szerveknek szól, ahol más szabályozások, előírások vannak, ráadásul az esetek többségében az ország területén működő, ott alapított és ott székelő

DOI azonosító: 10.17625/NKE.2015.021

felhőszolgáltató választható a szervezet által kitűzött célok eléréséhez. Ez ma nemhogy Magyarországon, de még Európában sincs így, ráadásul a szabályozási környezet is jóval hiányosabb, ráadásul országonként is eltérő. Ezeket pedig mind figyelembe kell venni egy felhő alapú rendszer esetleges használatának tervezésekor, különösen a sok személyes és érzékeny, sokszor akár minősített adatot is kezelő rendvédelmi szerveknek.

2.1.4. A BSI fontosabb ajánlásai

A BSI (Bundesamtes für Sicherheit in der Informationstechnik), azaz 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. [99]

A felhő alapú rendszerek biztonságával kapcsolatban, a 2011-ben közreadott, „Security Recommendations for Cloud Computing Providers” [29] fehér könyvük tekinthető irányadónak. A dokumentum közvetlen célja az, hogy ezen 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 felhő alapú 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. 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.

DOI azonosító: 10.17625/NKE.2015.021

A német szakemberek által javasolt metodológia szerint a szolgáltatóknak az olyan normák szerint kell kiépíteni a számítási felhőben a biztonsági rendszereket, mint az ISO 27001,[39] vagy a BSI 100-2 IT-Grundschutz Methodology.[40] Ehhez a szolgáltatóknak el kell készíteniük a kockázatelemzést, amelynek 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 felhő alapú 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 kategóriába sorolták:

- „Category B" (alapkövetelmények): ebben a kategóriában a minden szolgáltató számára érvényes alapkövetelmények találhatóak,
- „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, és hogy az adott terület melyik szolgáltatási modellre értelmezhető, vagy nem értelmezhető.

[39] ISO 27001: az információbiztonsági irányítási rendszerek követelményszabványa.

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

DOI azonosító: 10.17625/NKE.2015.021

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 az elemzése,
- az ICT rendszerek, alkalmazások és adatok védelmi követelményének meghatározása,
- adatok, alkalmazások, rendszerek és felhő szolgáltatások 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. 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. felhasználói kontroll lehetőségek,
5. monitoring and biztonsági események kezelése,
6. üzletmenet-folytonosság menedzsment,
7. hordozhatóság és interoperabilitás,
8. biztonsági tesztelés és audit,
9. személyi követelmények,
10. megállapodás kidolgozása, ezen belül
    10.1. átláthatóság,
    10.2. szolgáltatási szint megállapodás (SLA),[41]
11. adatvédelem és megfelelőség, ezen belül:
    11.1. adatvédelem,
    11.2. megfelelőség.

[41] SLA: Service Level Agreements szolgáltatási szint megállapodás

DOI azonosító: 10.17625/NKE.2015.021

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

A dokumentum bár alapvetően a szolgáltatóknak készült, de kiemelten hasznos az állami a felhasználók részére is. Ugyan véleményem szerint 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 részükre 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. [100] Ez megmutatja, hogy milyen védelmi megoldásra milyen veszély esetén van szükség a felhő alapú rendszerek esetében, és ezekhez hozzárendeli, hogy az életciklus melyik szakaszában kell értelmezni (pl. tervezés, működés stb.) azokat. Megadja a hozzájuk tartozó besorolási szintet (pl. belépő, azaz kötelező, tanúsításhoz szükséges, járulékos stb.) is. Véleményem szerint ezt a táblázatot kiegészítőként is lehet használni a felhőkockázatok felméréshez alapdokumentumnak tekinthető CSA „Cloud Controls Matrix” [88] táblázathoz, mindamellett, hogy a kettő célja és részletezettsége sem azonos.

2.1.5. Az ENISA fontosabb ajánlásai

Az ENISA, azaz az Európai Hálózat- és Információbiztonsági Ügynökség, a tagállamok és intézmények érdekében tevékenykedő, azokkal együttműködő szakértői központ, amely 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-, ás információbiztonsághoz kapcsolódó jogszabály előkészítő és fejlesztő munkáját. [101]

DOI azonosító: 10.17625/NKE.2015.021

Az említett feladatok ellátása kapcsán természetesen a felhő alapú rendszerekkel és kifejezetten azok biztonságával kapcsolatban is tettek közzé anyagokat. Ezek közül a kutatási téma célkitűzéseiben megfogalmazottak elérésének érdekében 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" [102] című dokumentumot érdemes áttekinteni.
A dokumentum készítői – a korábban bemutatott szervezetek szakembereihez hasonlóan – rámutatnak arra, hogy a felhő alapú rendszerek biztonsági szempontból kettős arcot mutatnak. Egyrészről, elsősorban az adatok koncentráltsága okán, vonzó célpontjai a támadásoknak, másrészről viszont általában sokkal robosztusabb védelemmel rendelkezik, mint a hagyományos ICT rendszerek. E kettősséget figyelembe véve, a dokumentum együtt értékeli a felhő előnyeit és biztonsági kockázatait, és mindemellett biztonsági útmutatót ad a felhasználóknak. Mindezt úgy, hogy a hálózat-, és információbiztonság, az adatvédelem szempontjából megközelítve technikai, eljárásmódbeli, és jogi következtetéseket von le, majd konkrét ajánlásokat tesz a kockázatok csökkentésére és az előnyök maximalizálására. A felhő biztonság értékelését 3 forgatókönyvön keresztül mutatja be:

1. kis-, középvállalati migráció felhőbe,
2. a számítási felhő hatása a szolgáltatás rugalmasságára, ellenálló képességére,
3. felhő az e-kormányzatban (pl. 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 felhő alapú rendszerek használatát. Az Európai Bizottságot az adatvédelemmel, felhőszolgáltatók kötelezettségeivel, – különösen az 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 a hatása,
    - végpont-végpont közötti titkosítás a felhőben, és azon túl,
    - magasabb biztonságú felhők, virtuális privát felhők, stb.,

DOI azonosító: 10.17625/NKE.2015.021

- nagyméretű, szervezeteken átnyúló rendszerek adatvédelme:
    - nyomozati és bizonyítékgyűjtési mechanizmusok,
    - incidenskezelés - monitoring és visszakövethetőség,
    - a vonatkozó nemzetközi előírások különbségei, beleértve az adatvédelmet,
- nagyméretű számítógépes rendszerek tervezése:
    - erőforrás izolációs mechanizmusok (pl. adatok, feldolgozás, memória, naplók),
    - felhőszolgáltatók közötti interoperabilitás,
    - felhőszolgáltatások rugalmasságának, ellenálló képességének növelése.

Ez a javaslat rávilágít a felhő alapú rendszerek legjelentősebb biztonsági kockázataira, amelyek sarkalatosak a rendvédelmi szervek számára is, ezért ezeket a biztonsági elemző sablon kidolgozásához mindenképpen célszerűnek tartom 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 felhő alapú rendszerek használatában, azonban több aktuális problémával is szembesülnek. Jelenleg sok jogi és szabályozási előírás, így például a személyes adatok kezelésének előírásai, is akadályozzák például e-kormányzati feladatok felhőbe költöztetését, ugyanakkor a belső szabályzóktól. előírásoktól függetlenül, vagy éppen azok ellenére is, sok alkalmazott használ felhő alapú szolgáltatásokat. A különböző szolgáltatási modellek (IaaS, PaaS, SaaS) esetében az előnyök és a kockázatok is jelentősen eltérnek, eltérhetnek egymástól, így a szolgáltatás típusát, mint az egyik legfontosabb tényezőt, az elemzésnél, 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. felhő szolgáltatás alkalmazásának kockázat értékelése,
2. különböző felhőszolgáltatók ajánlatainak összehasonlítása,
3. 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 felhő technológia miatt megjelenő új elemek, kockázatok kezelésében nyújtanak segítséget. A megfogalmazottak szerint a biztonsági feladatokat egyértelmű delegálása mellett kiemelt figyelmet kell fordítani

DOI azonosító: 10.17625/NKE.2015.021

a felek jogaira és kötelezettségeire, különös tekintettel a biztonsági szabályok megsértésére, az adatok átvitelére, a származékos művek alkotására, az kontroll változására, valamint a rendvédelmi szervek részére az adathozzáférés biztosítására.

A felhő alapú rendszerek biztonsági kockázatainak értékelését az ENISA szakértői az ISO 27005:2008 előírásain alapuló, 8 fokozatú 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 3. táblázat szerint ábrázolták.

	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

5. táblázat. Felhő alapú rendszerek kockázatértékelési táblázata ISO 27005:2008 alapján.[42]

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 felhő alapú rendszerek kockázatait mindig a hagyományos ICT megoldások kockázatával kell összehasonlítani. Másodszor, hogy a kockázatok szintje felhő típusonként 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

[42] Szerkesztette a szerző. Forrás: [102] p. 22.

DOI azonosító: 10.17625/NKE.2015.021

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 az 5. táblázatban bemutatottak szerinti szintjét.

Az alábbi, 6. táblázat bemutatja az ENISA által azonosított kockázatokat, azok általuk történt csoportosítását, valamint az egyes elemek értékelését.

KOCKÁZATOK				
MEGNEVEZÉS		**SZINT**		
		valószí-nűség	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

DOI azonosító: 10.17625/NKE.2015.021

KOCKÁZATOK					
MEGNEVEZÉS			SZINT		
			valószí-nűség	hatás	teljes kockázati szint
Technikai kockázatok:					
R.8	erőforrások kimerülése (alultervezés vagy túligénylés miatt),	R.8a plusz kapacitások tekintetében	közepes	alacsony/ közepes	közepes
		R.8b szerződésben foglalt kapacitások tekintetében	alacsony	magas	
R.9	izolációs hiba,	R.9a magán felhő 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 szolgáltatás-megtagadásos támadások,[43]		közepes	magas	közepes
R.16	gazdasági szolgáltatás-megtagadásos támadás, vagy erőforrás-felhasználás,		alacsony	magas	közepes
R.17	titkosító kulcs elvesztése,		alacsony	magas	közepes

[43] az ENISA dokumentumban található értékek közül a felhasználó szemszögéből adott értéket vettem figyelembe

DOI azonosító: 10.17625/NKE.2015.021

KOCKÁZATOK				
MEGNEVEZÉS		**SZINT**		
		valószí-nűség	hatás	teljes kockázati szint
R.18	rosszindulatú hálózat-feltérképezések,	közepes	közepes	közepes
R.19	szolgáltatás motor szoftverének kompromittálódása,	alacsony	nagyon magas	közepes
R.20	konfliktus a felhasználó biztonságot szolgáló megerősítő tesztelési eljárásai és a felhő környezet 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
Nem felhő-specifikus kockázatok				
R.25	hálózat leállás	alacsony	nagyon magas	közepes
R.26	hálózat kezelési problémák (pl. 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[44] típusú támadások	közepes	magas	közepes
R.30	üzemeltetési naplóállomány elvesztése vagy kompromittálódása	alacsony	közepes	közepes

[44] A social engineering, vagy 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, főnök megszemélyesítése, nemlétező felhatalmazásra hivatkozás, „fordított szúrás” (reverse social engineering) és az adathalászat különböző módszerei. [293]

DOI azonosító: 10.17625/NKE.2015.021

KOCKÁZATOK				
MEGNEVEZÉS		SZINT		
		valószí-nűség	hatás	teljes kockázati szint
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

6. táblázat. Az ENISA által azonosított kockázatok felhő alapú rendszerek vizsgálatához.[45]

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. (7. táblázat)

[45] Szerkesztette a szerző. Forrás: [102]

DOI azonosító: 10.17625/NKE.2015.021

	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;	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;

7. táblázat. A felhő alapú rendszerek ENISA által azonosított kockázatainak eloszlása.[46]

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,

[46] Szerkesztette a szerző. Forrás: [102] p. 24.

DOI azonosító: 10.17625/NKE.2015.021

- R.11 kezelőfelület kompromittálódása,
- R.23 adatvédelmi kockázatok,
- R.14 adatok nem teljes vagy nem biztonságos törlése,
- R.10 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, amelynek okára a dokumentumban nem találtam magyarázatot.

Ugyancsak eltéréseket tapasztaltam az ENISA által megadott egyes kockázathoz tartozó értékek és az ezek alapján készített, a „Cloud Computing: Benefits, risks and recommendations for information security" [102] című dokumentumban eredetileg közzétett kockázat-eloszlási táblázat adatai között is. Ez utóbbit azonban egyértelműen szerkesztési hibának vélem, így az általam közölt 7. számú táblázatot az eredeti dokumentumban az egyes kockázatoknál megadott értékeknek megfelelően szerkesztettem át. Így az R.1, az R9a, és azR.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 [103] [104] vagy a szolgáltatás megszűnésére, [105] alapvető megváltozására, [106] ezért én ezeket közepes kockázatúnak soroltam be.

A kockázatelemzésnél 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" [102] című dokumentum 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 és kiegészítésével – egyértelműen felhasználható a rendvédelmi szervek számára kialakítandó biztonsági sablon elkészítéséhez.

A felhő alapú 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

DOI azonosító: 10.17625/NKE.2015.021

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 felhő alapú rendszerek törvényes ellenőrzésének problémájával a későbbiekben részletesen foglalkozom, ebben a fejezetben ezeket a rendszereket a nemzetbiztonsági szolgálatok és a rendvédelmi szervek oldaláról kizárólag a felhasználás szemszögéből közelítem meg. Mindamellett még felhasználói oldalról nézve is, véleményem szerint az említett szerveknek figyelembe venniük, hogy adott esetben biztosítani, biztosíttatni kell a saját országuk bizonyos szervei részére a törvényes ellenőrzés és az adathozzáférés lehetőségét. Hazánkban tipikusan ilyen szerv lehet például az NVSZ.[47]

Az ENISA második kiemelést érdemlő dokumentuma a „Security & Resilience in Governmental Clouds - Making an informed decision”. [51] Ez deklaráltan az előzőekben áttekintett anyagra épít, sőt, szerzői ajánlása szerint azzal együtt kell használni.

A felhő alapú 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 felhő-architektúra kiválasztásában.

A dokumentum fő célja bemutatni a magán, közösségi és 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 3 lehetséges felhőhasználati forgatókönyvön alapul:

[47] NVSZ: Nemzeti Védelmi Szolgálat

DOI azonosító: 10.17625/NKE.2015.021

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

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

Az ENISA szakértői megállapítják, hogy végeredményben a felhő alapú 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 EU-n kívülre vitelét. Mindemellett a dokumentum sürgeti a tagállami és az EU ez irányú jogszabályi kereteinek a felülvizsgálatát annak érdekében, hogy az adatok külföldre vitelét megengedőbb módon kezeljék, és ezáltal a felhő használatából származó előnyöket kihasználhassák az állami szervezetek anélkül, hogy ezzel veszélyeztetnék az állampolgárok személyes adatainak a biztonságát, vagy sértenék a nemzetbiztonsági, vagy akár a gazdasági érdekeket. A rendvédelmi szervek kapcsán véleményem szerint kijelenthető, hogy adataik nagy része fokozottabban védendő, mint más állami szervé, ezért egy, az ENISA által sürgetett adatkezelési liberalizáció valószínűleg csak kis mértékben érintené őket.

Az európai szervezet szakértői azt is megállapítják, hogy éppen az érzékeny alkalmazásoknak és adatoknak köszönhetően a magán és a közösségi felhő modellek felelnek meg legjobban az állami feladatoknak, még akkor is, ha a méretbeli előnyök javarésze 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 felhő alapú rendszerek kockázatainak azonosításához közvetlenül nem tartozó, mégis a nemzetbiztonsági szolgálatok és a rendvédelmi szervek számára fontos, egyéb

DOI azonosító: 10.17625/NKE.2015.021

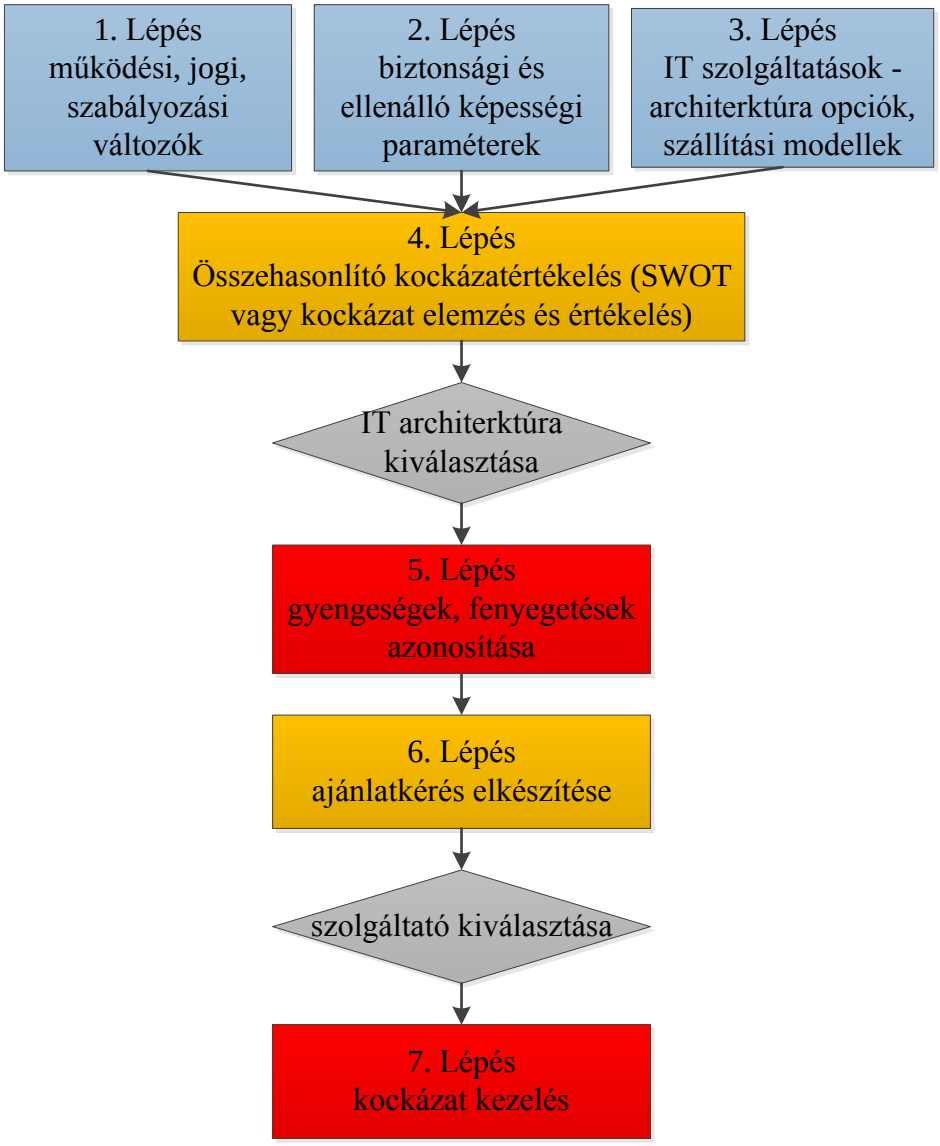
gondolatokat is felvetnek a készítők. Így például az ENISA szakemberei a kormányoknak szóló javaslatokban megfogalmazzák, hogy a felhő alapú rendszerek alkalmazását lépcsőzetesen érdemes bevezetni, amibe előre be kell tervezni az adott lépcsőről történő visszalépés lehetőségét is. A bevezetés tervezésekor 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 felhő alapú rendszerek milyen szerepet játszhatnak a létfontosságú infrastruktúrák védelme kapcsán, különösen az interdependencia nemzeti és nemzetközi hatásait kell elemezni a teljes ellátási láncban. E mellett 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 felhő alapú rendszerek bevezetésének elősegítésére az állami szerveknek célszerű elkészíteniük:

- egy pontos, egyértelmű kockázatértékelés és követelmény-meghatározást beleértve az emberi tényezők és jogi keretek vizsgálatát,
- a jelenlegi biztonsági rendszer átültetésének, támogatási lehetőségének a vizsgálatát,
- az adatbiztonság és a szolgáltatás ellenálló képesség 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 felhő alapú rendszer kiválasztásában. Ugyanakkor az egyes lépések elemzése kapcsán azonosítják is azokat a biztonsági kockázatokat, amelyek a felhő alapú rendszerek bevezetése vagy használata során felmerülhetnek.

DOI azonosító: 10.17625/NKE.2015.021



6. ábra. Az ENISA döntési modellje felhő alapú rendszer kiválasztásához.[48]

1. Lépés: A működési, jogi, szabályozási változók 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 (kapacitás fluktuáció, hosszú távú (fel és le) skálázhatóság)

[48] Szerkesztette a szerző. Forrás: [51] p. 27.

DOI azonosító: 10.17625/NKE.2015.021

- 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.

2. Lépés: A biztonsági és ellenálló képességi paraméterek kapcsán az alábbiakat célszerű megvizsgálni:

Az ENISA szakemberei itt definiálják, hogy pontosan mit is értenek biztonság és ellenálló képesség alatt. Ezek szerint:

„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.”[49]

„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 reagálásnak és a visszaállításnak a képessége."[50]

[49] Szerkesztette a szerző. Forrás: [51] p. 29.
[50] Szerkesztette a szerző. Forrás: [51] p. 29.

DOI azonosító: 10.17625/NKE.2015.021

Ezek a meghatározások véleményem szerint is 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 [107] 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 4 csoportba sorolták be, az alábbiak szerint:

1. 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, sérülékenység értékelés 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 felelősségre vonhatóság (naplóadatok rendelkezésre állásának szintje, nyilvánossága),
   - A5 ellátási lánc (végrehajtott audit típusa, úgymint belső, harmadik fél általi független, esetleg saját értékelés, annak hatóköre, metodikája.

2. 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.

DOI azonosító: 10.17625/NKE.2015.021

- 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.[51]
- B2 skálázhatóság és rugalmasság (kapacitás-fluktuáció, 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.

3. reagálás és helyreállítás:

Ez a csoport a hibák és incidensek reagálásához szükséges rendszerképességek mérésére szolgáló kritériumokat tartalmazza.

- C1[52] RTO[53] és RPO[54] meghatározása
- C2[55] 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.

4. 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).

[51] a jitter itt csomagkésleltetési eltéréseket, ingadozásokat takar.
[52] Az eredeti dokumentumban ez a jelölés nem szerepel, azt csupán én alkalmazom a jobb érthetőség miatt.
[53] RTO recovery time objective visszaállítási időtartam
[54] RPO recovery point objective visszaállítási időpont
[55] Az eredeti dokumentumban ez a jelölés nem szerepel, azt csupán én alkalmazom a jobb érthetőség miatt.

DOI azonosító: 10.17625/NKE.2015.021

3. Lépés: Az ICT szolgáltatások, architektúra-opciók, szállítási modellek esetén vizsgálandó kritériumokkal kapcsolatban csupán azt elemzik a dokumentumban, hogy mikor tekinthető és mikor nem felhőszolgáltatásnak valami, ehhez kapcsolódó kockázatokat itt nem azonosítanak a készítők.

4. Lépés: Az összehasonlító kockázatértékelés kapcsán az ENISA szakértői SWOT elemzést készítettek a nyilvános, a magán, és a közösségi felhőre. Ezeket rendre a 8. 9. és 10. táblázatok mutatják.

NYILVÁNOS FELHŐ	
ERŐSSÉGEK • rendelkezésre állás és megbízhatóság • tűrőképesség és rugalmasság • javítócsomag-menedzsment • reagálási idő • üzletment-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 támadásának a veszélye meglehetősen nagy • izolációs hiba • a követelmények és a vagyonosztályozás gyenge meghatározása • többszörös joghatóság • a szolgáltató irányításában bekövetkező változás • az alkalmazott adatformátum ellehetetlenítheti a szolgáltató váltást

8. táblázat. Az ENISA nyilvános felhő SWOT elemzése.[56]

[56] Szerkesztette a szerző. Forrás: [51]

DOI azonosító: 10.17625/NKE.2015.021

MAGÁN FELHŐ	
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 magán felhő 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 geo-redundancia 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 • nem megfelelő részletességű szerződés az abban foglaltak teljesítésének ellenőrizhetőségét csökkentheti

9. táblázat. Az ENISA magán felhő SWOT elemzése.[57]

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 magán felhőhöz képest)	**GYENGESÉGEK** • a közös célok miatt a partnerek között versengés van az erőforrásokért • a magán felhőhöz képest még vonzóbb célpontja a támadásoknak • a magán felhőhöz képest gyengébb hozzáférés szabályozás és jogosultságkezelés • a rossz összeköttetés miatti gyengébb teljesítmény csökkentheti a szolgáltatás szintjét

[57] Szerkesztette a szerző. Forrás: [51]

DOI azonosító: 10.17625/NKE.2015.021

LEHETŐSÉGEK	FENYEGETÉSEK
• növelt biztonsági előírások, alapkövetelmények és standardok, közös kockázatelemzési és -értékelési gyakorlat, naplózás és monitoring • közös, megosztott incidenskezelési rendszer • információk megosztása a közösségi tagjai között (legjobb-gyakorlatok, múltbeli incidensek tapasztalatai stb.) • szigorúbb biztonságot eredményezhet, hogy a felhőt csak a tagok használják	• 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

10. táblázat. Az ENISA közösségi felhő SWOT elemzése.[58]

A SWOT analízissel kapcsolatban két dolog mindenképpen kiemelést érdemel. Az egyik, hogy az ebben az esetben a szolgáltatási modelltől függetlenül készült, így egy konkrét vizsgálatnál az aktuális szolgáltatási modell (IaaS, PaaS, SaaS) figyelembe vételével módosulhat. Másrészt a felhasználó ebben a lépésben más módszert, például kockázatelemzést, -értékelést is alkalmazhat a SWOT analízis 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 11. táblázat.

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

[58] Szerkesztette a szerző. Forrás: [51]

DOI azonosító: 10.17625/NKE.2015.021

PARAMÉTEREK	
MEGNEVEZÉS	**LEHETSÉGES ÉRTÉKEK**
• 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
Azonosítás, hitelesítés és hozzáférés-kezelés (AAA)[59]	
• azonosítás-kezelés	belső (saját), külső (szolgáltató), mindkettő
• felhasználók ellátása engedélyekkel	belső (saját), külső (szolgáltató), mindkettő
• szabály alapú hozzáférés-kezelés (RBAC)[60]	igen, nem
• hitelesítés erőssége	erős, közepes, 2 faktoros, jogi követelmény jelszavas, opcionális
• államilag megkövetelt	igen, nem
Titkosítás	
• titkosítás	igen útközben, opcionális, javasolt útközben
• hozzáférés a kulcsokhoz	-
• adminisztrátori hozzáférés engedélyezése	a szolgáltató biztosítja bejelentkezési és hitelesítési adatokat az adminisztrátori 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[61]), a szabály alapú hozzáférés-kezelés (RBAC), vagy ezek kombinációja
• felelősségre vonhatóság (naplóadatokat a bíróság elfogadhatja)	igen, nem
• hozzáférés digitális személyazonosító-kártya használatával	igen, nem
• digitális aláírás	igen, nem, lehet, kell
• egyszeres bejelentkezés (SSO)[62]	opcionális

[59] AAA: authentication, authorization, and accounting hitelesítés, engedélyezés, hozzáférés-kezelés
[60] RBAC: Role-based access control szabály alapú hozzáférés-kezelés
[61] MAC: Mandatory Access Control kötelező hozzáférés-védelem.

DOI azonosító: 10.17625/NKE.2015.021

PARAMÉTEREK	
MEGNEVEZÉS	**LEHETSÉGES ÉRTÉKEK**
• 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

11. táblázat. ENISA szolgáltatások értékelésének szempontjai.[63]

Az ENISA szakemberei végezetül 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 [108] vagy a CSA Cloud Controls Matrix [88].

A dokumentum, akárcsak a korábban elemzett másik ENISA anyag, véleményem szerint kiemelkedően hasznos a rendvédelmi szervek felhő alapú rendszerek használatával kapcsolatban megfogalmazandó követelménylista elkészítéséhez. A döntési modell segíthet a megfelelő felhő alapú rendszer kiválasztásában, a javasolt biztonsági és ellenálló képességi paraméterek, azok értékelésének szempontjai, valamint a különböző telepítési modellű felhő rendszerek SWOT elemzésénél leírtak pedig – a megfelelő kiegészítésekkel – jól használhatóak a rendvédelmi szervek szigorú biztonsági követelményrendszerének kialakításához. Mindemellett a dokumentum egyedülálló módon hívja fel a figyelmét az állami szerveknek a nemzetbiztonsági érdekek figyelembevételére a felhő alkalmazásakor. Ez pedig a rendvédelmi alkalmazás során – tekintettel az érzékeny adatokra – kiemelt jelentőséggel bír.

Az anyag fontos üzenetének tartom, hogy bár az elején még csak feltételes módban beszél arról, hogy a sok érzékeny adatot használó szervezek számára a nyilvános felhő, bizonyos biztonsági előnyei ellenére sem megfelelő alternatíva, addig a dokumentum végére ezt már-

[62] SSO: single sign-on egyszeres bejelentkezés, amely után a rendszer minden erőforrásához és szolgáltatásához további autentikáció nélkül hozzá lehet férni.
[63] Szerkesztette a szerző. Forrás: [51] p. 62-67.

DOI azonosító: 10.17625/NKE.2015.021

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 számomra 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 felhő alapú rendszerek milyen szerepet játszhatnak a létfontosságú infrastruktúrák védelmével összefüggésben. Ezzel a gondolattal más szervezet anyagaiban nem találkoztam, ugyanakkor ez itt sem kerül részletesen kibontásra, csupán a gondolatfelvetés szintjén marad meg.

A témában a fenti két kiemelt dokumentumon kívül további hasznos információkat ad az ENISA felhő alapú rendszerekkel, azok biztonságával foglalkozó weboldala [109], valamint az itt található, általam korábban már említett „Good Practice Guide for Securely Deploying Governmental Clouds" [36], és a „Security Framework for Governmental Clouds" [75] című anyagok is.

2.2. Biztonsági kérdések – a rendvédelmi szervek szempontjából

Megállapítható, hogy a felhő alapú rendszerek terén vezető szerepet játszó nemzeti és a nemzetközi szervezetek, az előző részben általam feldolgozott 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 pedig 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 felhő alapú rendszerek kockázatainak azonosításához – és így a készítendő biztonsági elemző sablon kidolgozásához is, - ám véleményem szerint nekik, speciális helyzetükből adódóan, az említett dokumentumokat felhasználva, ám azoktól eltérő módon csoportosítva, helyenként kiegészítve, módosítva érdemes ugyanezt a kéréskört megvizsgálni.

2.2.1. A felhő alapú rendszerek komplex biztonsági vizsgálatának szempontjai

Álláspontom szerint a nemzetbiztonsági szolgálatoknak és a rendvédelmi szerveknek a felhő alapú rendszerek komplex biztonsági vizsgálatát az alábbi négy dimenzió mentén célszerű lefolytatni:

DOI azonosító: 10.17625/NKE.2015.021

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 felhő alapú rendszerek biztonsági problémái kapcsán valóban komplex, minden releváns tárgykörre választ adó vizsgálatot tudnak lefolytatni. Ugyanakkor egy adott kérdés megválaszolásához lehet, és célszerű is szűkíteni az elemezendő kérdéseket. A következőkben a fejezet közvetlen célját, a biztonsági elemző sablon kidolgozását szem előtt tartva haladok végig az említett négy dimenzión, és teszem meg a további vizsgálathoz általam szükségesnek és célszerűnek gondolt szűkítéseket.

1. 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.

DOI azonosító: 10.17625/NKE.2015.021

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 felhő alapú megoldást, hogy a törvényes ellenőrzést elkerülhesse).
A törvényes ellenőrzés lehetőségeivel később foglalkozom, ebben a fejezetben kizárólag a felhasználói szerepkörből közelítem meg a kérdést.

2. Telepítési modellek:

A telepítési modellek definícióját, részletes leírását az első fejezetben is meg lehet találni, így ezek bemutatásával itt nem foglalkozom. Az egyszerűsítés okán élhetünk azzal a feltételezéssel, hogy a rendvédelmi szervek felhasználóként – a korábbi megállapításomnak megfelelően – közösségi számítási felhőt fognak igénybe venni, míg a törvényes ellenőrzés kapcsán elsősorban a nyilvános számítási felhőkre koncentrálnak. Felhasználóként ekkor a vizsgálatok lényegesen egyszerűsödnek, amelyre már érdemes és lehet biztonsági elemző sablont kidolgozni, amelyet több rendvédelmi szerv is fel tud majd használni.

3. Szolgáltatási modellek:

A szolgáltatási modellek definícióját, részletes leírását ugyancsak az első fejezet tartalmazza, így ezek bemutatásával itt szintén nem foglalkozom. 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 modell szerint működő számítási felhőkre koncentrálnak, ám felhasználóként mindhárom modell alkalmazása egyaránt reális lehet.
Meg kell jegyezni, hogy amennyiben az általam tett első három dimenzióra vonatkozó feltevések egy adott esetre nem igazak, akkor természetesen az adott szerepkör, telepítési-, és szolgáltatási modell sajátosságait figyelembe véve újra kell gondolni a sablonban leírtakat és vizsgálni a biztonsági kérdéseket.

4. 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 felhő alapú rendszerek biztonságával kapcsolatos témákban, vagy éppen hívják fel egy addig kevéssé ismertre a figyelmet. [110] [111] [112] [113] [114] [115] [116] [117] [118] [119] [120] [121] [122] A nagyobb piaci szereplők is különböző tanulmányokat adnak ki bizonyos biztonsági kérdéseket reflektorfénybe helyezve, persze nem

DOI azonosító: 10.17625/NKE.2015.021

titkoltan azzal a szándékkal, hogy saját termékeikkel egyfajta megoldást kínáljanak ezekre. [123] [124] [125] [126] [127]

Véleményem szerint a vizsgálandó biztonsági kérdéseket az előző fejezetben ismertetett dokumentumokra alapozva, az imént említett internetes anyagokat is felhasználva, azoktól mégis eltérő módon az alábbi 4 fő csoportba célszerű sorolni:

4.1. üzembiztonság

4.2. adatbiztonság

4.3. egyéb (jogi, fizikai stb.) biztonság

4.4. törvényes ellenőrzés.

Ebben az esetben a csoportosítás önkényes, általam alkotott. Gyakorlati tapasztalatom azt mutatja, hogy – természetesen a 4.4. pontot kivéve – az állami, kormányzati szervezeteknél, különösen a rendvédelmi szerveknél különböző emberek, jobb esetben csoportok vagy szervezeti egységek foglalkoznak ezekkel a kérdéskörökkel és véleményem szerint ezt erősítik a különböző vonatkozó jogszabályok, előírások is. Ugyanakkor a szakirodalomban találkozhatunk az általam felállítotthoz hasonló megközelítéssekkel, így például felosztásában közel azonos jellegűt lehet találni a BSI,[64] és szinte teljesen megegyezőt az ENISA[65] korábban elemzett anyagában.

Az általam választott csoportok elnevezései az azokat ellátó személyekre vagy szervezetekre utalnak. Miután a felhő alapú rendszerek biztonsága kapcsán a technikai jellegű kérdések a dominánsak, ezért azokat kettébontva, külön címkével ellátva szerepeltetem, míg a többi kérdéskör ellátóit – bár azok jól elkülönülnek minden szervezetnél – egy kategóriába, az egyéb biztonságiban fogtam össze. Ez utóbbinak az alábontását a biztonsági sablonban elvégeztem, így álláspontom szerint egy vizsgálat során ott is egyértelműen delegálhatók a megválaszolandó kérdések, feladatok.

4.1. Üzembiztonság:

Az üzembiztonság kérdése a felhő alapú 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 (pl. Androidos táblagépek), meghatározott helyekről (pl. bárhonnan, ahol internet kapcsolat van) meghatározott rendelkezésre állással (pl. 95%, de a szolgáltatás kiesés nem hosszabb, mint 30 perc) érjük el

[64] [29] p. 17.
[65] [51] p. 6.

DOI azonosító: 10.17625/NKE.2015.021

a szolgáltatást, de ide tartozik az adataink biztonsági mentése, a redundáns tárolás, a katasztrófa utáni adat-visszaállítás stb. is.

Az üzembiztonsági kérdések gyakorlatilag tisztán technikai úton kezelhetőek, 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, függetlenül a szolgáltatási modelltől (SaaS, PaaS, IaaS).

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

4.2. Adatbiztonság

Adatbiztonsági kérdésnek tekinthetünk minden olyan tényezőt, amelyek a felhasználók adataihoz való biztonságos hozzáférés (kezelés, használat stb.), valamint az illetéktelen hozzáférések megakadályozása kapcsán felmerül. 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 felhő alapú rendszerekre (pl. vírusvédelem), egy része pedig teljesen új megoldásokat kíván (pl. adatszegregáció, felhő alapú rendszerekben használt virtualizációt kihasználó támadások elleni védekezés). [116] Az adatbiztonsági kérdések közül vannak (technikailag) egyszerűen megoldhatók (pl. a felesleges, ezáltal a sérülékenységek miatt biztonsági kockázatot jelentő alkalmazások kikapcsolása) és bonyolult technikai, sőt akár jogi megoldásokat igénylők (pl. a szolgáltató – beleértve annak rendszergazdáit is – ne férhessen hozzá az adatainkhoz [115] [122].

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, [117] vagy az adatok teljes törlésének [119] a kérdésköre.

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

DOI azonosító: 10.17625/NKE.2015.021

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 az 7. ábra szemléltet.

7. ábra. Az adatok életciklusa.[66]

Az adatok életciklusának 6 állomását véleményem szerint biztonsági szempontból 2 fő csoportra bonthatjuk, az adatmozgással járó és az adatmozgással nem járó műveletekre.

- Adatmozgással járó műveletek: előállítás, használat, megosztás, törlés.
- Adatmozgással nem járó műveletek: tárolás, archiválás.

Ezt a bontás azért célszerű megtenni, mert a felhő alapú 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.

[66] Szerkesztette a szerző. Forrás: [289]

DOI azonosító: 10.17625/NKE.2015.021

4.3. Egyéb (jogi, fizikai stb.) biztonság

Ebbe a kategóriába tartozik minden olyan biztonsági kérdéskör, amelyeket nem technikai úton kezelünk, és akár egy harmadik fél is bevonásra kerülhet (pl. audit). Ide soroljuk 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 is, de ugyanebbe a csoportba tartoznak az adatközpontok fizikai védelmét, a szolgáltató személyi-, gazdasági vagy dokumentumbiztonságot szavatoló tényezők is.

Az ebbe a kategóriába tartozó kérdésre kizárólag jogi eszközökön keresztül lehet ráhatása a felhasználónak. Ez a jogi kérdések esetében egyértelmű, de ugyanez igaz a többi, például fizikai biztonságra vagy a 3. 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 kategóriába eső kérdésekre szélsőségek között változhat, így például akár a szerződés tartalmára is. Amíg egy nyilvános SaaS megoldásnál ez leredukálódhat a szolgáltató által megírt szerződés és kialakított egyéb feltételek elfogadása vagy elvetése, addig egy magán IaaS megoldásnál a szerződés tartalmát és az egyéb feltételeket a felhasználó a szolgáltatóval folytatott közvetlen tárgyaláson befolyásolhatja, határozhatja meg.

A felelősségi körök itt talán 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.

4.4. Törvényes ellenőrzés

Ebbe a kategóriába tartoznak a törvényes lehallgatással, az adatmegőrzéssel és a nyomozati (forensics) eszközök használatával kapcsolatos kérdések. Amint említettem, a törvényes ellenőrzéssel később foglalkozom, ez a biztonsági ellenőrző sablon kidolgozása szempontjából irreleváns. Röviden azonban itt is célszerű foglalkozni vele. Egyrészt azért, mert ez is eleme a felhő alapú rendszerek 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 felelősség megoszlásokat. 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

DOI azonosító: 10.17625/NKE.2015.021

formák, amelyek a klasszikus hírközlési hálózatoknál már kialakultak és elfogadottak (pl. törvényes lehallgatás), és azok is, amelyek kifejezetten számítástechnikai rendszereknél alakultak ki (pl. számítógépes nyomozás vagy angol nevén computer forensics).

A törvényes ellenőrzés kategóriájába tartozó kérdések technikai és jogi úton rendezhetőek, ám ezek pillanatnyilag a legproblémásabbak 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 és a felhasználó között, mint a többi biztonsági kérdésnél. Ám amíg a hírközlési hálózatoknál egy kialakult, minden szereplő által elfogadott és a demokratikus államokban hasonló jellegű törvényekre alapozott törvényes ellenőrzésről beszélhetünk, addig a felhő alapú 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 felhő alapú 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 (pl. olyan eszközök 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 szolgáltató szerződést köt.

Ahogyan a CSA fent említett dokumentumaiban megjelent a Security as a Service fogalma, úgy a törvényes ellenőrzéshez is megjelenhet a Lawful Monitoring as a Service (LMaaS) (vagy valami hasonló) 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.

2.2.2. Biztonsági elemző sablon felhő alapú rendszerek értékeléséhez

A korábban elemzett ajánlások ismeretében és a fentiek figyelembe vételével már kidolgozható a rendvédelmi szervek számára egy, a felhő alapú rendszerek biztonsági értékelésére használható elemző sablon. Annak érdekében, hogy ez valóban használható, és

DOI azonosító: 10.17625/NKE.2015.021

jól használható legyen, a kidolgozás előtt érdemes tisztázni és pontosan meghatározni a sablon elkészítésének és felhasználásának a célját.

Jelenleg magyar nyelven nincsenek olyan sablonok, amelyeket akár kormányzati, akár rendvédelmi szervek fel tudnának használni a felhő alapú rendszerek bevezetése előtt azok biztonsági kockázatainak feltárásához, értékeléséhez. Ehhez, a FedRAMP-hoz hasonlóan több sablont is érdemes elkészíteni, úgy, hogy az általuk lefedett területek és az adott területen a vizsgálatok mélysége eltérjen egymástól. Kiindulásként azonban egy olyannal érdemes kezdeni, amely mintegy 0. lépésként azt segít tisztázni, hogy a kínált vagy kinézett felhő alapú rendszer megfelel-e azoknak a minimális biztonsági követelményeknek, amelyek teljesítése nélkül a rendszert nem szabad használni. Ehhez meglátásom szerint egy olyan sablont célszerű elkészíteni, amely az alap biztonsági kérdéseket teljes körűen felölelő módon, igen/nem elvárt válaszok megadásával biztosítja ezt.

Az ilyen formában kidolgozott sablon alapján eldönthető, hogy az adott felhő alapú 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 felhő alapú rendszer megfelel a felhasználó biztonsági követelményeinek, csupán azt, hogy nincs kizáró tényező, azaz érdemes további vizsgálatokat elvégezni. Jelen állapotban amellett, hogy még egyáltalán nincsenek a téma egy-egy területére koncentráló, mélységi elemzést lehetővé tevő sablonok, azért is egy ilyen jellegűt érdemes először kidolgozni, mert a további lépésekhez a felhasználónak ez még nagy szabadságfokot biztosít. Ezt követően ugyanis már a konkrét felhő alapú rendszer adottságainak (pl. szolgáltatási-, telepítési modell stb.), a szervezet meghatározott feladatainak, céljainak, az általa kezelt adatok érzékenységének, valamint az ott már bevezetett biztonsági standardoknak megfelelően képesek a felhasználó kijelölt szakemberei további vizsgálatokat lefolytatni.

Ezeknek az irányelveknek megfelelően dolgoztam ki a rendvédelmi szervek számára a felhő alapú rendszerek biztonsági értékelésére használható elemző sablont. Ez a korábban felfektetett felosztásnak megfelelően három főcsoportból áll: üzembiztonsági, adatbiztonsági és egyéb biztonságiból. Ezeket az 1., 2., 3. és 4. számú melléklet tartalmazza.

A sablon kitöltéséhez az általam alkotott szabályok a következők:

- A sablon 3 főcsoportra bomlik, minden főcsoport kitöltése kötelező, azok közül egyik sem hagyható el.
- Az egyes főcsoportokon belül további alcsoportok találhatóak, ezek kitöltése szintén kötelező, azok közül egyik sem hagyható el.

DOI azonosító: 10.17625/NKE.2015.021

- Minden alcsoporthoz tartozik egy vagy több, szürke színnel kiemelt fő vagy összegző kérdés, azok kitöltése kötelező, azok közül egyik sem hagyható el.
- Minden alcsoporthoz több, fehér színnel jelzett kérdés tartozik, azok közül a felhasználó döntése alapján egy vagy akár több is elhagyható.
- Az egyes kérdésekhez igen/nem válaszok adhatók, ezek közül kizárólag az egyik jelölhető meg.
- A kérdésekre mindenhol az igen válasz jelenti a pozitív eredményt.
- A fehérrel jelölt alcsoporti kérdések esetében a nemleges válasz még nem jelenti automatikusan azt, hogy a vizsgált felhő alapú rendszer nem felel meg a megkívánt biztonsági követelményeknek. Ugyanakkor azt az összegző kérdésnél mindenképpen, a szervezet számára képviselt súlyának megfelelően, figyelembe kell venni.
- A szürkével jelölt összegző, vagy fő kérdések esetében a nemleges válasz automatikusan azt jelenti, hogy a vizsgált felhő alapú rendszer nem felel meg a megkívánt biztonsági követelményeknek, annak használatától el kell tekinteni.

Az általam kidolgozott sablonra úgy tekintek, mint egy alapra, amelyre rá lehet építeni a többi, a felhő alapú rendszerek biztonsági kérdéseinek egy-egy területére koncentráló, mélységi elemzést lehetővé tevő sablont. Remélem, hogy ilyen sablonok már a közeljövőben készülni fognak.

Kiemelendőnek tartom továbbá, hogy az általam kidolgozott sablont nem tekintem véglegesnek. Egyrészt kiegészítéseket generálhat hozzá egy adott szervezet speciális igénye, de akár egy olyan, általános érvényű szempont is, amely az adott szervezet számára fontos, ám azt nem szerepeltettem a sablonban. Másrészt a felhő alapú rendszerek fejlődése kapcsán megjelenő új technológiák, szolgáltatások, a szintén egyre fejlődő, finomodó technikai és jogi szabályozások, szabványosítások kapcsán is a sablon változását várom. Ezekre azonban úgy tekintek, mint természetes evolúciós folyamatokra, hiszen ugyanez történt, történik a nagy szervezetek hasonló jellegű kiadványaival. Gondoljunk itt például a CSA „Cloud Controls Matrix” táblázatára, [88] amely 2015 év elején éppen a 3.0.1 verziónál jár, vagy akár a FedRAMP „System Security Plan (Template)” [98] sablonjára, amelynek 2014. 06. 06-án adták ki a 2.0-ás változatát.

Összegzés, következtetések

A második fejezetben **elemeztem és értékeltem** a fejlett országok felhő alapú rendszerekkel foglalkozó **nemzeti és nemzetközi szervezetei** által megalkotott, nyíltan elérhető, a dolgozat célkitűzése szempontjából **releváns biztonsági ajánlásokat**.

DOI azonosító: 10.17625/NKE.2015.021

Megállapítottam, hogy **a CSA** az általam feldolgozott dokumentumaiban alapvetően a gazdasági társaságokra koncentrálva, iparági megközelítéssel, a szolgáltató szempontjából dolgozza fel a felhő alapú rendszerek biztonsági kérdéseit. Ugyanakkor **ezen dokumentumokban leírtak megfelelő átalakítással, a szigorúbb követelményeknek és előírásoknak történő megfeleltetéssel jól használhatóak a célkitűzésben megfogalmazott, a rendvédelmi szervek számára készítendő biztonsági elemző sablon elkészítéséhez**. Különösen igaz ez az egyébként is iparági alapdokumentumnak tekinthető „Cloud Controls Matrix" című anyagra.

A NIST általam kiemelt és elemzett anyaga kapcsán rámutattam, hogy számos, a rendvédelmi szervek részére készítendő biztonsági elemző sablonhoz is hasznos információt tartalmaz, hiszen **a kormányzati szervek szempontjából közelíti meg** a nyilvános felhő szolgáltatási modellű rendszer felhasználásának biztonsági problémáit. Márpedig napjainkban ez hordozza a legnagyobb biztonsági kihívást. Ugyanakkor ennek felhasználása során mindenképpen figyelembe kell venni, hogy egyrészt a rendvédelmi szervek az állami szervekhez képest nagyobb mennyiségű magasabb szintű biztonságot igénylő, jobban védendő adatot kezelnek, másrészt a dokumentum **az Egyesült Államok jogi, technikai lehetőségeinek figyelembevételével készül**, amely jelentősen eltér az Európai Unió országaiétól. Ennek megfelelően, a CSA ajánlásai kapcsán már megfogalmazott megfelelő **átalakításokra ebben az esetben is szükség van**.

Feltártam, hogy **a FedRAMP**, és az ennek keretében működtetett cloud.cio.gov weboldal éppen annak okán, hogy kifejezetten kormányzati szerveknek készült felhő alapú rendszerek bevezetésének, használatának biztonságosabbá tétele érdekében rengeteg hasznos információval szolgál az ilyen típusú feladatoknál akár a rendvédelmi szervek számár is. Az előzőekben vizsgált szervezetek anyagaihoz képest ezek már a dolgozat céljához jobban illeszkedő, ahhoz jobban fókuszált megközelítést biztosítanak. Ráadásul a program keretében, szintén a dolgozat célkitűzései között szereplő biztonsági elemző sablonhoz hasonló sablonokat is közzétesznek, amely bizonyítja kutatási célkitűzésem helyességét. Ugyanakkor a FedRAMP dokumentumaiban megfogalmazottak kapcsán két dolgot is figyelembe kell venni. Egyrészt a kormányzati és a rendvédelmi szervek információi közötti különbségeket, másrészt, hogy ezek a dokumentumok kifejezetten az Egyesült Államok kormányzati szerveinek szólnak. Így ezekre ugyanúgy igazak az előző két szervezet anyagai kapcsán megfogalmazottak, azaz **egy európai rendvédelmi szerv csupán a megfelelő átalakítások után tudja érdemben használni** az ott leírtakat.

DOI azonosító: 10.17625/NKE.2015.021

Megállapítottam, hogy a **BSI általam elemzett dokumentumai** bár alapvetően a szolgáltatóknak készültek és **nem teljes mértékben fedik le a rendvédelmi szervek igényeit, mégis kiemelten hasznos számukra**. A felhő alapú rendszerek biztonsági kérdéseit új csoportosításban közelítik meg, hasznos kiegészítésekkel szolgálva a korábban ismertetett anyagokhoz. Ráadásul egy minden téren vezetőnek számító európai ország kormányzati információbiztonságért felelős szervezete készítette, amely a hazaihoz hasonló jogi, szabályozási, technikai és szolgáltatói környezetben működik, ezért az anyagai könnyebben adaptálhatók a magyarországi viszonyokra, mint az Egyesült Államok szervezeteinek hasonló témában készített dokumentumai.

Rámutattam, hogy bár az **ENISA ajánlásai** nem kizárólag kormányzati szerveknek szólnak, az azokban azonosított kockázatok, a megfelelőek kiválasztásával és kiegészítésével, **egyértelműen felhasználhatók a rendvédelmi szervek számára kialakítandó biztonsági sablon elkészítéséhez**. További nagy előnye az anyagaiknak, hogy azok az Európában jellemző, az Egyesült Államokétól jelentősen eltérő, ráadásul a tagországokat tekintve is rendkívül heterogén technikai és szabályozási környezet szemszögéből történő megközelítéssel készültek, így az ott feltárt kockázatok és azok megállapított mértékei hazánk mai realitásához sokkal jobban illeszkednek, mint az amerikai szervetek által meghatározottak. Az ENISA dokumentumok kiemelendő pozitívumának tartom azt is, hogy egyedülálló módon hívják fel az állami szervek figyelmét a felhő alapú rendszerek alkalmazása kapcsán a nemzetbiztonsági érdekek figyelembevételére.

A különböző szervezetek ajánlásaiban megfogalmazott, az összes telepítési modell előnyeire, hátrányaira vonatkozó következtetések megismerését követően megállapítottam, hogy napjainkban, felhasználóként, a rendvédelmi szervek számára a közösségi felhő jelentheti az optimális megoldást.

A felhő alapú rendszerek biztonsági kérdéseinek rendvédelmi szervek szemszögéből történő **komplex vizsgálatához felállítottam egy új szempontrendszert**. Az ebben felvázolt „a rendvédelmi szerv szerepe – telepítési modellek – szolgáltatási modellek – vizsgálandó biztonsági kérdéscsoportok” 4 dimenziós térben bemutattam, hogyan lehet egy adott célnak megfelelően a kívántakra leszűkíteni a vizsgálandó kritériumokat. A „vizsgálandó biztonsági kérdéscsoportoknál” szintén egy új kategorizálást vezettem be, az „üzembiztonság – adatbiztonság – egyéb (jogi, fizikai stb.) biztonság – törvényes ellenőrzés” csoportosítást. Tettem ezt azért, mert gyakorlati tapasztalatom azt mutatja, hogy az állami, kormányzati szervezeteknél, különösen pedig a rendvédelmi szerveknél különböző emberek, jobb esetben csoportok vagy szervezeti egységek foglalkoznak ezekkel a kérdéskörökkel, és ezért a

DOI azonosító: 10.17625/NKE.2015.021

biztonsági vizsgálatokat is célszerűnek tartom az ő feladatköreiknek megfelelően delegálni és elvégezni. Meghatároztam, hogy mit tekintek üzembiztonsági, adatbiztonsági, egyéb (jogi, fizikai stb.) biztonsági, valamint törvényes ellenőrzési kategóriába tartozó kérdésnek, azok milyen úton (technikai, jogi) oldhatók meg, valamint a felhasználó és a szolgáltató érdekei és felelősségi körei hogyan viszonyulnak egymáshoz.

A fejezetben elemeztem a felhő technológiában vezető szerepet játszó nagy nemzetközi szervezetek dolgozatom szempontjából releváns ajánlásait, és ezekben feltártam a biztonság értékeléséhez szükséges kockázatokat. Ezeket összefoglalva, kiegészítve, az általam alkotott új csoportosításnak megfelelően **megalkottam a rendvédelmi szervek számára használható biztonsági elemző sablont**, valamint annak használati útmutatóját. Meglátásom szerint ez megfelelő alapot ad az egyes részterületeket mélyebben vizsgáló további sablonok előállításához. Rávilágítottam ugyanakkor, hogy az általam kialakított sablon természetesen 1.0 verziónak tekinthető, és mint minden, az iparágban megjelenő hasonló kiadvány, ez is továbbfejleszthető, továbbfejlesztendő. Egyrészt kiegészíthető azokkal a követelményekkel, amelyek adott esetben egy-egy szervezet részére olyan jelentőséggel bírnak, hogy azokat mindenképpen meg kell jeleníteni, másrészt a technikai környezet változásával, a felhő alapú rendszerek fejlődésével jöhetnek olyan újabb elemek, amelyeket célszerű ebbe beépíteni.

Feltártam és **leszögeztem** azt is, hogy a törvényes ellenőrzés kapcsán **célszerű lenne bevezetni és szabványosítani a Lawful Monitoring as a Service (LMaaS)** (vagy valami hasonló) **fogalmát.** Ennek keretében ugyanis a szolgáltató szolgáltatásként, standardizáltan biztosíthatná az ellenőrzést végző szervek számára a szükséges információkat, kiküszöbölve rengeteg, napjainkban meglévő technikai és jogi problémát. Ez ugyan nem kötődik közvetlenül a fejezet célkitűzéséhez, de a dolgozat összes célját tekintve mégis rendkívül fontos megállapításnak tartom.

Véleményem szerint a fejezet kidolgozásának egyik további eredménye, hogy az összegyűjtötten mutatja be a felhő alapú rendszerekkel foglalkozó nagy nemzeti és nemzetközi szervezetek által megalkotott, biztonsági kockázatok azonosítását, kezelését ismertető ajánlásokat, valamint feltárja, hogy ilyen jellegű, magyar nyelvű dokumentum jelenleg nem elérhető.

DOI azonosító: 10.17625/NKE.2015.021

3. Információbiztonsági felkészítés tartalmi elemei védett vezetők számára

A címben szereplő védett vezetők alatt értekezésemben nem a védett személyek és a kijelölt létesítmények védelméről szóló 160/1996. (XI. 5.) Korm. rendeletben meghatározott szűk körre értem, hiszen ez a kormányrendelet is kifejezetten az abban meghatározott vezetők fizikai védelméről, életének és testi épségének megóvásáról, nem pedig információik védelméről szól. Dolgozatomban jóval szélesebb értelemben veszem a védett vezető fogalmát, beleértve minden olyan állami vezetőt, akiknél az információbiztonság növelése és az információszivárgás megakadályozása érdekében az arra jogosult szolgálatok technikai elhárítást tartanak, tarthatnak.

A védett vezetők mindennapi tevékenységéhez szorosan hozzátartozik a kommunikáció és az ezekhez szükséges hordozható infokommunikációs eszközök (pl. okostelefon, táblagép, hordozható számítógép) használata. Gyorsan, egyszerűen, és nem utolsó sorban olcsón akarnak beszélni másokkal, adatokat, információkat elérni, cserélni, továbbítani. Sokszor mindezt úgy, hogy az érzékeny információkat csak az a néhány ember ismerhesse meg, akinek feltétlenül szükséges, az általuk közétenni kívánt információkhoz viszont az emberek széles köre is gyorsan, egyszerűen hozzáférhessen. Ez utóbbihoz sok esetben mindenki által elérhető, sokszor ingyenes internet-technológiára épülő szolgáltatásokat, ezen belül is főleg PC/SaaS felhő alapú rendszereket használnak fel vagy kívánnak felhasználni. Ráadásul a hivatali és magánjellegű kommunikációt, az érzékeny és a széles körnek szánt információk továbbítását lehetőleg egyazon eszköz segítségével akarják lebonyolítani. Ez azonban jelentős veszélyeket rejt magában.

Az elektronikus úton folytatott kommunikációs és adattovábbítási lehetőségek, az internet-technológiára épülő, ezen belül is a felhő alapú szolgáltatások rohamos fejlődése új, korábban nem ismert kihívások elé állította, állítja az illetékeseket, döntéshozókat és a szakembereket egyaránt. [128] A kibertérben ma minden felhasználót a veszélyek egész sora fenyegeti, a kiberbűnözéstől az idegen titkosszolgálatok adatszerző tevékenységéig. [129] Fokozottan igaz ez a védett vezetőkre, akik mindig is kiemelt célpontjai voltak az információszerző támadásoknak. Ráadásul külön problémakánt jelentkezik, hogy a védett személyek által használt eszközök – hordozhatóságuk és személyhez rendeltségük okán – általában vegyes felhasználásúak, azaz hivatali és magáncélokat egyaránt szolgálnak.

Éppen ezért fontos megvizsgálni, hogy mit is tehetünk a védett vezetők információinak – azon belül is legfőképpen elektronikus információinak – megvédése, biztonságának garantálása

DOI azonosító: 10.17625/NKE.2015.021

érdekében. Az internet-technológiára épülő szolgáltatások, és a személyi használatú hordozható infokommunikációs eszközök[67] esetében a védekezés egyik leghatékonyabb módszere biztonságtudatos használata. A védelemre fordítható összegek ugyanis korlátozottak, ráadásul a megfelelő biztonság technikailag sokszor nem, vagy csak irreálisan magas költségek mellett lenne a megfelelő szinten kialakítható.

A biztonságtudatos használatra fel lehet készíteni a védett vezetőket, amelyhez érdemes egy személyükre szabott, általános jellemzőiket figyelembe vevő felkészítési módszerét kidolgozni. Ehhez az első lépés a lehetséges veszélyek felmérése. Ennek érdekében elemezni kell a védett vezetők információbiztonsági védelmének főbb kérdéseit, körülhatárolni a veszélyek szempontjából vizsgálandó személyi használatú hordozható infokommunikációs eszközöket, valamint internet-technológiára épülő szolgáltatásokat, majd számba venni az elemezendő biztonsági kategóriákat. Az így megadott kritériumok alapján lehet összefoglalni az említett eszközök és szolgáltatások használata során jelentkező veszélyeket, majd ennek alapján meghatározni a személyre szabott felkészítés keretrendszerét és felállítani egy lehetséges, az említett eszközök és szolgáltatások használatára vonatkozó biztonságtudatossági felkészítés módszerét.

A fentiek alapján látható, hogy a nemzetbiztonsági szolgálatok és rendvédelmi szervek szerepe ebben az esetben eltér az előző fejezetben vizsgáltaktól. Míg ott közvetlen felhasználóként jelentek meg, addig itt – mivel a védett vezetők védelmét ilyen téren is biztosítaniuk kell – mintegy harmadik félként, belépve a felhasználó és a szolgáltató közé. Ha úgy tetszik, ebben a szerepkörben a CSA „Security Guidance for Critical Areas of Focus in Cloud Computing” [85] című dokumentumában megjelenő Biztonság, mint szolgáltatás kapcsán leírtakhoz hasonló módon, a felhasználónak egy külső félként nyújtanak biztonságot szavatoló „szolgáltatásokat”. Ennek azonban több következménye is van. Egyrészt az előző fejezetben kizárólag a felhasználó szemszögéből elemeztem a felhő alapú rendszerek szolgáltatóval szemben felállítandó biztonsági kérdéseit, nem foglalkozva a felhasználói oldal

[67] A személyi használatú hordozható infokommunikációs eszköz fogalmára nincs egységesen elfogadott definíció. A dolgozatban ebbe a fogalomba azokat az eszközöket értem bele, amelyek rendelkeznek a következő tulajdonságokkal. Egyrészt személyhez kötötten használtak, azaz egy dedikált személy számára biztosítottak, és a működési idő jelentős részében valóban ő is használja azokat. Az egyéb személy általi felhasználásuk nem jelentős. Másrészt hordozhatóak, azaz viszonylagos kis méretük és tömegük, beépített adat be-, és kiviteli eszközeik (pl. érintőképernyő), csatolófelületei (pl. WiFi, LTE stb.) és áramellátási rendszerük lehetővé teszi azok nem helyhez kötött alkalmazását akár több féle kommunikációs hálózatra való felcsatlakoztatása mellett. Harmadrészt pedig infokommunikációs lehetőségeket biztosítanak, azaz kiépítettségüktől függően különböző mértékben és lehetőségekkel alkalmasak hang és adat alapú kommunikációra akár az internet elérésével, akár más hálózat felhasználásával, egyéb, nem kommunikációra fejlesztett program futtatására stb. Ma jellemzően ilyen eszközök az okostelefonok, a notebookok és a táblagépek, ám az általam leírtak vonatkoznak minden más, a fenti tulajdonságokkal bíró meglévő és a jövőben megjelenő eszközre is.

DOI azonosító: 10.17625/NKE.2015.021

hasonló kérdéseivel. Itt viszont nem a nemzetbiztonsági szolgálatok és rendvédelmi szervek a közvetlen felhasználók, így most a felhasználó helyett kell bizonyos biztonsági követelményt szabni, sőt – és ebben tér el lényegesen az előző fejezetben taglaltaktól – megának a felhasználónak is. Másrészt éppen az eltérő szerepkör miatt nem is lehet kizárólag a felhő alapú rendszerekre fókuszálni. Az érdemi, valóban felhasználható eredmény eléréséhez az elemzés során figyelembe kell venni azokat az internet-technológiára épülő szolgáltatásokat, amelyeket a védett vezetők használnak, és nem tartoznak a szűken vett felhő alapú rendszerek közé, másrészt vizsgálatokat ki kell terjeszteni a személyi használatú hordozható infokommunikációs eszközökre is. Álláspontom szerint csak ezek együttes vizsgálata ad megfelelő alapot az információbiztonsági felkészítés tartalmi elemeinek kidolgozásához.

3.1. A védett vezetők információbiztonsági védelmének szükségessége a kibertérben

Napjainkban az információ védelme egyre nagyobb hangsúlyt kap, és különösen igaz ez a kibertérre. Katonai, állami szempontból értékes adatokat az érintettek mindig is megpróbálták a kor technikai színvonalának és az anyagi lehetőségeknek megfelelően, a lehető legjobban megvédeni. Az üzleti információkat is folyamatosan védték, védik tulajdonosaik, hiszen ehhez alapvető anyagi érdekük fűződik. Ám ezekben a szegmensekben az elektronikus úton folytatott kommunikációs és adattovábbítási lehetőségek, az internet-technológiára épülő szolgáltatások rohamos fejlődése új, korábban nem ismert kihívások elé állította, állítja az illetékeseket, döntéshozókat és a szakembereket. Azonban éppen ennek a technikai fejlődésnek köszönhetően adataink védelme a privát szférában is alaposan felértékelődött.

Az, hogy az élet szinte minden területén kiemelt szerepet kapott az információbiztonság, több tényezőnek köszönhető. Az egyik, a kibertér veszélyeinek ugrásszerű, minden felhasználót érintő növekedése, a másik az elektronikus kommunikációs és adattovábbítási lehetőségek, az internet-technológiára épülő szolgáltatások, valamint a személyi használatú hordozható infokommunikációs eszközök rohamos fejlődése, elterjedése.

A technológiák fejlődése és a felhasználási szokások nem választhatók szét egymástól. Egyfajta összefonódó spirált képezve, egymást is erősítve, gerjesztve hozták létre a mai népszerű kommunikációs formákat, adattárolási -továbbítási lehetőségeket és egyéb internet-technológián alapuló szolgáltatásokat. A szélessávú és mobil internet elérések elterjedése, a hordozható eszközök (pl. ultrabookok, tabletek, okostelefonok stb.) hihetetlen mértékű fejlődése, a közösségi oldalak népszerűségének ugrásszerű növekedése, a különböző kommunikációs lehetőségeket biztosító internet-technológián alapuló szolgáltatások, felhő alapú rendszerek (mint pl. Facebook, Gmail, Dropbox, Twitter, Skype stb.), valamint az ezek

DOI azonosító: 10.17625/NKE.2015.021

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. [130] Ez a megállapítás a védett vezetőkre is igaz, hiszen ők is használják ezeket az eszközöket, technológiákat. [52] [53] [54] [131] [132]

A kibertérben ma minden felhasználót a veszélyek egész sora fenyegeti, a kiberbűnözéstől (pl. banki adatok megszerzése után pénz leemelése a bankszámláról), [133] [134] [135] egészen az idegen titkosszolgálatok adatszerző tevékenységéig (pl. Prism ügy).[68] [136] [137] Fokozottan igaz ez a védett vezetőkre, akik mindig is kiemelt célpontjai voltak az információszerző támadásoknak. [138] Éppen ezért fontos megvizsgálni, hogy mit is tehetünk a védett vezetők információinak – azon belül is legfőképpen elektronikus információinak – megvédése, biztonságának garantálása érdekében. A védekezés egyik leghatékonyabb módszere az internet-technológiára épülő szolgáltatások, és a személyi használatú hordozható infokommunikációs eszközök biztonságtudatos használata. A védelemre fordítható összegek ugyanis korlátozottak, ráadásul a megfelelő biztonság technikailag sokszor nem, vagy csak irreálisan magas költségek mellett lenne kialakítható a megfelelő szinten. [139]

A biztonságtudatos felhasználásért azonban tennünk kell, hiszen a védett vezetők sokszor tudatában sincsenek a veszélyeknek, így azt sem tudják, hogyan kellene használniuk eszközeiket és az igénybevett szolgáltatásokat, hogy a használat már önmagában ne okozzon nemzetbiztonsági kockázatot. Ennek tudatosításában a leggyorsabb út a felkészítés.

Az elérendő eredmények ugyanakkor megfelelő adaptációval mások – akár magánemberek – számára is segítséget adhatnak az internet-technológiára épülő szolgáltatások és az azokat elérő személyi használatú eszközök kockázatmentesebb használatához.

3.2. Védett vezetők információbiztonsági felkészítése

Az alap célkitűzés tehát az, hogy kidolgozásra kerüljön a védett vezetők számára egy testreszabott, különleges helyzetüket, időbeosztásukat, stb. figyelembe vevő biztonságtudatossági felkészítési módszer. Egyrészt azért, mert a Snowden-ügy[69] kapcsán megjelent hírek, [136] a 2013-ban elfogadott kiberbiztonsági stratégia, [140] valamint a 2013.

[68] A PRISM ügy**:** Az Egyesült Államok technikai hírszerző szolgálata, az NSA (National Security Agency – Nemzetbiztonsági Ügynökség) által folytatott nagyszabású Internet ellenőrző projekt, amelynek keretében többek között a kilenc vezető internetes alkalmazásszolgáltató (Microsoft, Yahoo, Google, Facebook, PalTalk, AOL, Skype, YouTube, Apple) rendszerein tárolt és azokon átfolyó adatokhoz (pl. beszélgetések, video-chat, fényképek stb.) – szolgáltatónként változó formában és mélységben – férnek hozzá. [128]

[69] Edward Joseph Snowden, az NSA volt alkalmazottja rengeteg, közöttük minősített iratokat csempészett ki az Ügynökségtől, amelyeket különböző újságokban nyilvánossá tett. Így derült fény az Egyesült Államok nagyszabású, a kibertér teljes ellenőrzését, az ott folyó kommunikáció totális lehallgatását célzó projektjeire (pl. PRISM), valamint arra, hogy az Egyesült Államok világszerte széles körben, szűrő-kutató és készletező adatgyűjtő jelleggel monitorozta az emberek Internetes tevékenységét és hallgatta le mobiltelefonjait. [136]

DOI azonosító: 10.17625/NKE.2015.021

évi L. törvény az állami és önkormányzati szervek elektronikus információbiztonságáról [141] mind az információk fokozottabb védelme irányába mutatnak. Másrészt azért, mert védett vezetőknél hagyományosnak tekinthető információvédelmi módszert, azaz a technikai elhárítást célszerű lenne kiterjeszteni a kibertér általa használt régióira is, és ennek egyik alapvető részét kellene képeznie a biztonságtudatossági felkészítésnek.

A védett vezetők teljes körű, ezen belül az információbiztonságot is garantáló védelme meglehetősen összetett feladat. Ennek az egyik speciális részét képezi technikai elhárítás, mint a védett vezetők információbiztonsági védelmének egy jól körülhatárolható, és önállóan is működtethető része. A fejezet ez utóbbinak a szempontjából közelíti meg a biztonságtudatossági képzés kérdését, és nem foglalkozik a védett vezetők egyéb védelmi kérdéseivel.

A biztonságtudatossági felkészítés tartalmi elemeinek kidolgozáshoz szükséges vizsgálat és annak eredményéül előálló felkészítési módszer azonban megfelelő adaptációval máshol, a gazdasági vagy akár a magánszférában is felhasználható. A probléma megoldásával így több – fontos és indokoltan megoldandó – célt is elérhetünk.

Ráadásul az internet-technológiára épülő szolgáltatások, valamint a személyi használatú hordozható infokommunikációs eszközök használatánál az információvédelem kapcsán hasonló problémákkal, veszélyekkel és jelenségekkel találkozunk akár a védett állami vezetőket, akár a nagyvállalatok vezetőit, akár a magánembereket tekintjük.

Erre egy tipikus példa, hogy a védett vezetők személyi használatú hordozható infokommunikációs eszközei esetében is vegyes (hivatali és magán) használatra kerül sor. Az ennek kapcsán felmerülő problémák és veszélyek nagyban hasonlítanak a saját tulajdonú eszközök munkában történő felhasználása (BYOD) esetében felmerülő problémákhoz, veszélyekhez [142] [143] [144] [145] azzal a különbséggel, hogy míg ott a dolgozó saját eszközét viszi munkába, addig itt (javarészt) hivatalból biztosított eszközöket használják fel magáncélra is. Az eredmény azonban hasonló, mindkét esetben a vegyes felhasználás miatt információbiztonsági problémákba ütközünk, még akkor is, ha a nem felhasználói tulajdonú eszközök talán kissé jobban védhetők, például rezsimszabályokkal.

A legszigorúbb, mindenre kiterjedő védelmet a védett vezetőknek kell megkapniuk, így a számukra kidolgozott biztonságtudatos felhasználói felkészítés tartalma (például a szükségtelen részek elhagyásával) könnyebben átültethető az élet többi területére, mint fordítva.

DOI azonosító: 10.17625/NKE.2015.021

3.3. A technikai elhárítás változása, kiterjesztett értelmezése

Annak érdekében, hogy az állami szempontból fontos információkat a lehető legjobban meg lehessen védeni, az illetékes szervek rendszeresen végeznek technikai elhárítást a védett vezetők által használt helyiségekben. Ekkor – többek között – olyan megfigyelő, lehallgató stb. eszközöket keresnek, amelyekkel illetéktelenek megismerhetik a szobában zajló eseményeket, hozzájuthatnak az elhangzó beszélgetések tartalmához, vagy egyéb információkhoz. Természetesen a technikai elhárítás kiterjedhet a védett vezető által használt magánhelyiségekre (pl. saját lakás), vagy szállodai szobákra is.

A technikai elhárítás feladata, hogy feltárja és ezáltal megakadályozza az illetéktelenek által folytatott információgyűjtést, felderítse a támadható, gyenge pontokat, sérülékenységeket, valamint felfedje az esetlegesen régebben végrehajtott információszerzés bizonyítékait (pl. mikrofon-fészek, falban maradt kábel stb.). Ma már azonban nem elégséges az iroda, lakás, stb. „poloskátlanítása", hiszen sokkal könnyebben és kockázatmentesebben lehet információhoz jutni például. egy postafiók feltörésével, vagy egy táblagépbe történő bejutással. Éppen ezért a lehető legteljesebb körű védelem kialakításához az információvédelem komplex megközelítésére van szükség. Azért, hogy megérthessük, hogy a komplex megközelítés mit takar, először érdemes tanulmányozni, hogy milyen vizsgálatokkal célszerű kiterjeszteni a klasszikus értelemben vett technikai elhárítást annak érdekében, hogy a védett vezetők személyes (beleértve a hivatali és magán) életterében az információbiztonságot garantálni lehessen.

3.3.1. A klasszikus technikai elhárítás kérdései

Ebbe a kategóriába a technikai elhárítás hagyományos értelmezése szerinti feladatok tartoznak, mint például mikrofonok, kamerák, vagy adattovábbításra alkalmas eszközök keresése. Azaz egyszerűen fogalmazva és a jelen esetre nézve, a védett személy által használt és vizsgálatra kijelölt, magánlakásnak minősülő helyiségek átvizsgálása történik, oda telepített audio vagy vizuális megfigyelő, lehallgató eszközök felderítése érdekében. (Ennek pontosabb behatárolása, felsorolása túlmutat a dolgozat keretein.) Ezek a feladatok természetesen és egyértelműen a technikai elhárítást végző szervezet felelősségi körébe tartoznak.

Álláspontom szerint magát a „technikai elhárítás" fogalmát ma már célszerűbb lenne kizárólag a fentebb vázolt és a fejezet következő pontjaiban részletesebben megadottak szerinti kiterjesztett értelemben használni. A szakirodalomban található meghatározások is ezt támasztják alá, hiszen azok is kiterjesztőbb jelleggel közelítenek a témához. Az egyik definíció szerint a technikai elhárítás jelentése a következő:

DOI azonosító: 10.17625/NKE.2015.021

„A TSCM vizsgálat egy szakképzett személyzet által nyújtott szolgáltatás technikai megfigyelőeszközök (helyiséglehallgató vagy más információszerző eszközök) jelenlétének és egyéb információbiztonsági veszélyek kimutatására, valamint azon technikai és kommunikációs biztonsági hiányosságok, sérülékenységek azonosítására, amelyek lehetőséget adhatnak a védett helyiségben történő technikai információszerzésre." [146]

Ez a megfogalmazás már láthatóan bőven túlmutat a helyiséglehallgató és –megfigyelő eszközök keresésén, ám még mindig a védett helyiségekre koncentrál.

Álláspontom szerint a technikai elhárítás (TSCM)[70] meghatározásaként alapvetően elfogadhatjuk az USA Department of Defence által 2006-ban kiadott 5240.05 számú dokumentumban található definíciót, amely így szól:

„Olyan módszerek és intézkedések, amelyek felderítik, semlegesítik és/vagy kihasználják a minősített vagy érzékeny adatokhoz való illetéktelen hozzáférésre irányuló különféle (szervezett) bűnözői vagy külföldi titkosszolgálati információszerzési kísérleteket."[71] [147]

Ez, az előzőt is jelentősen kibővítve és egy általános megközelítést adva, időt állóan adja a fogalom meghatározását. Ezt támasztja alá, hogy a meghatározás a 2014. április 3-án, ugyanazon a referenciaszámon kiadott frissített változatban[72] is ugyanez maradt, pedig a 2006 óta eltelt idő alatt a technológia sokat változott, az elektronika, az infokommunikáció azóta is rengeteget fejlődött, és ez az (illegális) információszerző lehetőségek bővülését is magával hozta.

Ezt a megfogalmazást ugyanakkor már túl általánosnak tartom a védett vezetők információbiztonságát célzó, kiterjesztetten értelmezett technikai elhárítás feladatainak egyértelmű azonosításához. Ennek pontos meghatározása szintén túlmutat a dolgozat keretein, ám egy új, kifejezetten erről szóló definíció esetleges későbbi elkészítéséhez segítségül, valamint a célkitűzésben foglaltak eléréséhez érdemes áttekinteni, hogy melyek azok a feladatok, amelyeket mindenképpen bele kell érteni a kiterjesztett értelmezésbe. Ezeket az általam ide sorolt feladatokat mutatják be a következő részek.

3.3.2. Munkahelyi számítástechnikai eszközök biztonsági kérdései

A cím itt sem véletlen, ebbe a kategóriába kizárólag a munkahelyen található, nem hordozható számítástechnikai eszközöket (pl. asztali számítógép) értem. A védett vezetők személyes használatában ugyanis lehet(nek) az irodájában elhelyezett és a helyi hálózatba kötött (esetleg

[70] TSCM: Technical Surveillance Countermeasurestechnikai elhárítás
[71] Forrás: [147] p. 21.
[72] (http://www.dtic.mil/whs/directives/corres/pdf/524005_2014.pdf megtekintve: 2015.03.14.)

DOI azonosító: 10.17625/NKE.2015.021

azon keresztül az internetet is elérő) számítógép(ek). Természetesen ezeket is infokommunikációs eszközöknek tekintem, ám a védelmükkel kapcsolatos – főleg a technikai elhárítást érintő – feladatok és lehetőség szempontjából élesen el kívánom határolni őket mind a személyi használatú hordozható infokommunikációs eszközöktől, mind az egyéb, az irodában található kommunikációs eszköztől (pl. belső telefon).

A védett vezető munkahelyi számítástechnikai eszközeinek a védelme is az információbiztonsági feladat részét képezi, ugyanakkor ezek védelmét ketté kell választani.

Az általános ICT biztonsági feladatok (pl. jogosultságok, biztonsági beállítások, vírusvédelem stb.) alapvetően a helyi biztonsági vezető és informatikáért felelős szervezet feladata és felelősségi köre.[73] Az említett hálózatok, eszközök hardveres manipulálásának, esetlegesen ide elhelyezett információszerző (pl. lehallgató) eszközök keresése, felfedése azonban már a technikai elhárítás feladatkörébe tartozik. Hasonló kettősség mondható el az úgynevezett gyenge pontok kereséséről. A hagyományos értelemben vett ICT sérülékenység-vizsgálat a helyi biztonsági vezető és informatikáért felelős szervezet feladata és felelősségi köre, míg a többi sebezhető pont feltárása már a technikai elhárítóké.

Mindent egybevéve az irodai számítástechnikai eszközök védelme is hozzátartozik a védett vezető információbiztonságának megteremtéséhez, így bele kell érteni a technikai elhárítás kiterjesztett értelmezésébe.

3.3.3. Személyi használatú hordozható infokommunikációs eszközök információbiztonsági kérdései

A védett vezetők mindennapi tevékenységéhez szorosan hozzátartozik a kommunikáció, az információk cseréje vagy adott esetben csupán azok gyors elérése. Ennek érdekében életük szerves részét képezi a személyi használatú, hordozható infokommunikációs eszközök használata. Ma már elképzelhetetlen, hogy az irodában rendelkezésre álló infokommunikációs eszközök, mint például az asztali számítógép, vagy a vezetékes (belső) telefon mellett ne használjanak mobiltelefont, hordozható számítógépet, vagy táblagépet. Ráadásul a technológiai konvergencia okán ezek egyre inkább egybeolvadnak, így biztosítva egy, kisméretű, hosszú üzemidejű készülékben a hang-, és adatkommunikációt. Ebbe a kategóriába kizárólag a hordozható eszközöket értjük (hordozható számítógép, táblagép, okostelefon, stb.), amelyek sok esetben kettős célt (hivatali és személyes használat) szolgálnak. [148]

[73] A feladatokat és a felelősségi köröket a vonatkozó jogszabályok (pl. 1995. évi CXXV. törvény a nemzetbiztonsági szolgálatokról, 2013. évi L. törvény az állami és önkormányzati szervek elektronikus információbiztonságáról stb.) valamint a helyi szabályzatok, előírások tartalmazzák részletesen.

DOI azonosító: 10.17625/NKE.2015.021

Az információvédelem teljes körű megteremtéséhez, így a technikai elhárítás komplex értelmezéséhez ma már feltétlenül hozzátartozik a személyi használatú hordozható infokommunikációs eszközök, valamint az azokról igénybe vett internet-technológiára épülő szolgáltatások vizsgálata. Egyrészt azért, mert ma lényegesen egyszerűbb, veszélytelenebb bejutni egy védett vezető által használt infokommunikációs eszközbe, mint a fizikailag jól védett irodájába, ráadásul az információszerzés ezen formájánál jóval kisebb a felfedezés veszélye is. És még ha ki is derül a támadás ténye, akkor is nehezebb a támadót azonosítani, mint a helyiséglehallgatás esetén. Másrészt pedig azért, mert bizonyos szolgáltatások használatával „önként" ad meg magáról lényeges adatokat a felhasználó. Gondoljunk csak arra, amikor egy ingyenes alkalmazás letöltésekor elfogadjuk, hogy a szoftver gyűjtse, és a készítőhöz továbbítsa pl. az aktuális pozíciónkat, vagy akár a telefonkönyvünk tartalmát. Nem nehéz belátni, hogy ez is nem kívánt információszivárgáshoz vezet.

Ezen a területen a védelem kialakítását az is nehezíti, hogy kevés a megfelelő eszköz, szoftver, gyenge a szabályozás és ez utóbbi okán a területnek nincs is kijelölt felelőse.

A fentiekből látható, hogy a védett vezetők információinak biztonsága érdekében a technikai elhárítást kiterjesztett értelemben kell használni, és a komplex információbiztonsági ellenőrzésnek ki kell terjednie a védett vezető által használt személyi használatú hordozható infokommunikációs eszközökre és internet-technológia alapú szolgáltatásokra is. Ahhoz azonban, hogy hatékonyan védekezni lehessen az itt felmerülő veszélyek ellen, először fel kell mérni, majd csoportosítani azokat.

3.4. A veszélyek szempontjából vizsgálandó személyi használatú hordozható infokommunikációs eszközök, valamint internet-technológiára épülő szolgáltatások

A védett vezetők biztonságtudatossági felkészítésének elemeit, mint minden felkészítési módszert, csak megfelelő általánosítást és csoportosítást követően lehet kialakítani. Nem lehet teljesen személyre szabott (vagy pontosabban fogalmazva: teljesen, az éppen használt eszközökre és szolgáltatásokra szabott) felkészítési módszert kidolgozni. Egyrészt azért, mert a védett vezetők száma is elég nagy, így sok tematikát és azokhoz számtalan tartalmat kellene kidolgozni, oktatni. Másrészt pedig, az új eszközök, alkalmazások piacra kerülésének üteme miatt is célszerű inkább általánosított jelenségekre, veszélyekre fókuszálni annak érdekében, hogy a jövőben megjelenő eszközök, szolgáltatások és fenyegetések esetében is használható ismeretekkel rendelkezzenek a felkészítésben részesítettek.

A fejezetben kitűzött cél eléréséhez az internet-technológiára épülő szolgáltatások, ezeken belül is kiemelten a felhő alapú rendszereket kell alaposabban megvizsgálni. A felhő alapú

DOI azonosító: 10.17625/NKE.2015.021

rendszerek esetében tovább lehet szűkíteni a kört, hiszen az „átlagfelhasználók” elsősorban a nyilvános számítási felhő és szoftver, mint szolgáltatás, azaz a PC/SaaS típusú rendszereket használják leggyakrabban. De nem csak ők, hiszen ezek azok a szolgáltatások, amelyek bárki számára olcsón, sokszor ingyenesen elérhetők, azokat a védett vezetők is akár magán, akár hivatalos célokra (pl. választókkal, szimpatizánsokkal való kapcsolattartásra, gondolataik gyors, széles rétegekhez történő eljuttatására) [52] [53] [54] is használják.

Amint azt az 1.4.3. alfejezetben is bemutattam, a PC/SaaS rendszerek mindenképpen az internet-technológiára épülő szolgáltatások részhalmazának tekinthetők, ám a határvonalat, hogy mi tekinthető egyértelműen PC/SaaS rendszernek, nagyon nehéz meghúzni. Éppen ezért - az ott leírtak alapján - a dolgozat céljának eléréséhez, a fejezetben a kiterjesztőbb értelmű internet-technológiára épülő szolgáltatások megfogalmazást használom, de egyértelműen, sőt kiemelten beleértem a PC/SaaS rendszereket is.

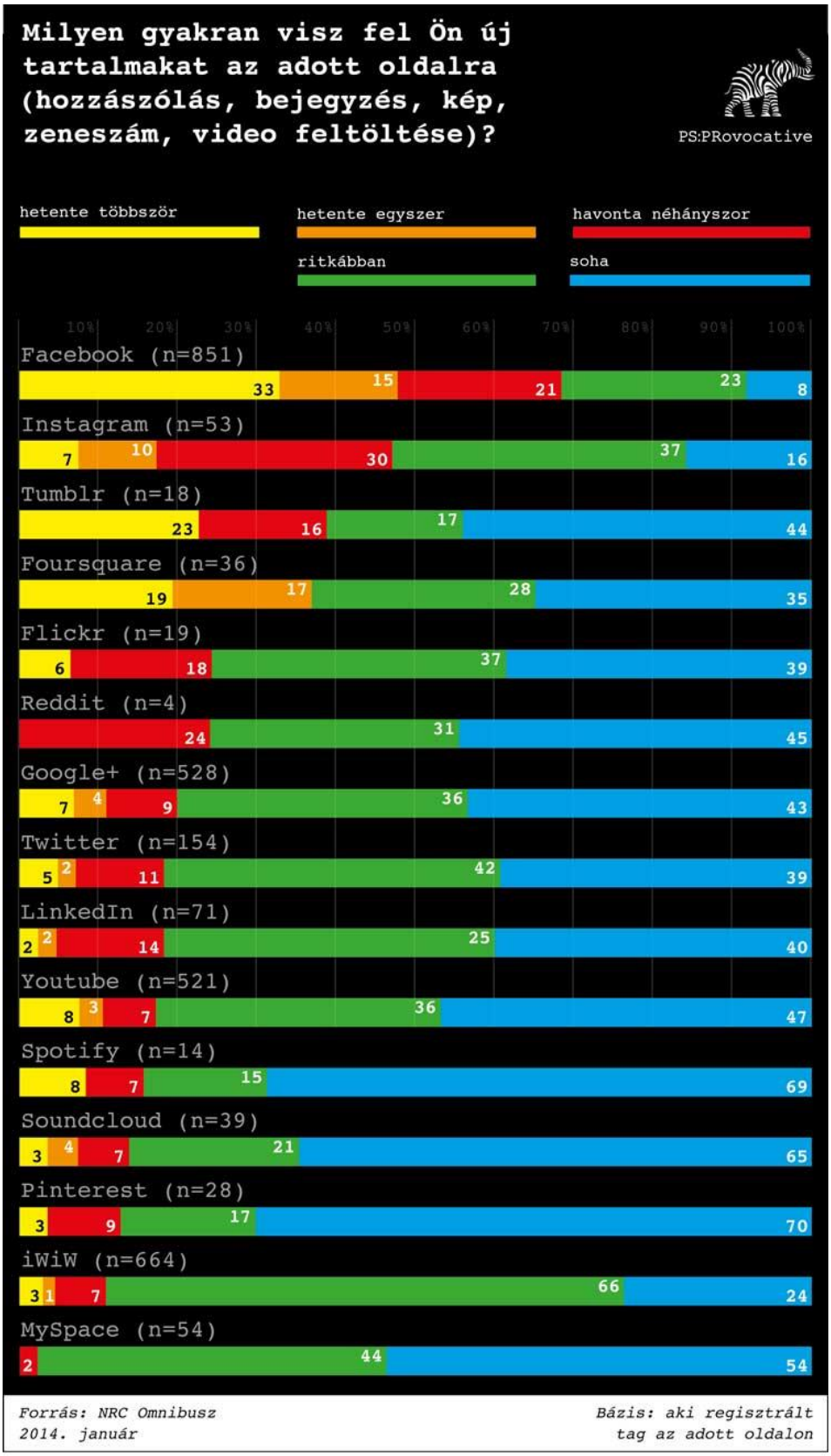
3.4.1. A leggyakrabban használt internet-technológiára épülő szolgáltatások jellemzői

Megszámlálhatatlan az internet-alapú szolgáltatások száma, ráadásul szinte minden nap jelennek meg újak, amelyek között gyakran találkozhatunk teljesen új koncepción alapuló, vagy új igényeket kielégítő megoldásokkal. Éppen ezért rendkívül nehéz összefoglalni az említett szolgáltatások jellemzőit.

Véleményem szerint a védett vezetőknek kialakítandó biztonságtudatossági képzés okán az „átlagfelhasználók” által is leggyakrabban használt szolgáltatásokat érdemes megvizsgálni. Egyrészt azért, mert a védett vezetők felhasználói szokásairól nem elérhető kimutatás vagy statisztika, másrészt pedig azért, mert azzal a feltételezéssel élek, hogy azok ma nem térnek el jelentősen az „átlagfelhasználók” szokásaitól.

A leggyakrabban használt internet-alapú szolgáltatások pedig a PC/SaaS legjellemzőbb tulajdonságaival bírnak, azaz a bárki által elérhető és igénybe vehetőek, használatukhoz a szükséges szoftvert a szolgáltató biztosítja például böngészőben futtatott alkalmazás, vagy letölthető kliensprogram formájában. [149] Ezek közül pedig, a kialakítandó képzés célját és az internet-alapú szolgáltatások népszerűségét tekintve, elsősorban a valamiféle elektronikus úton folytatott kommunikációt [130] (pl. közösségi oldalak, levelezés, blogok, stb.) és a különféle adatok tárolását, megosztását lehetővé tevő szolgáltatásokat (pl. YouTube, Dropbox stb.) kell figyelembe venni. [150] [151] [152] Igaz ez a magyar viszonyokra is, mint ahogy azt egy, a közösségi oldalak magyarok általi használatát vizsgáló felmérés is bizonyította. [153] Erre mutat jellemző adatokat az 8. és a 9. ábra.

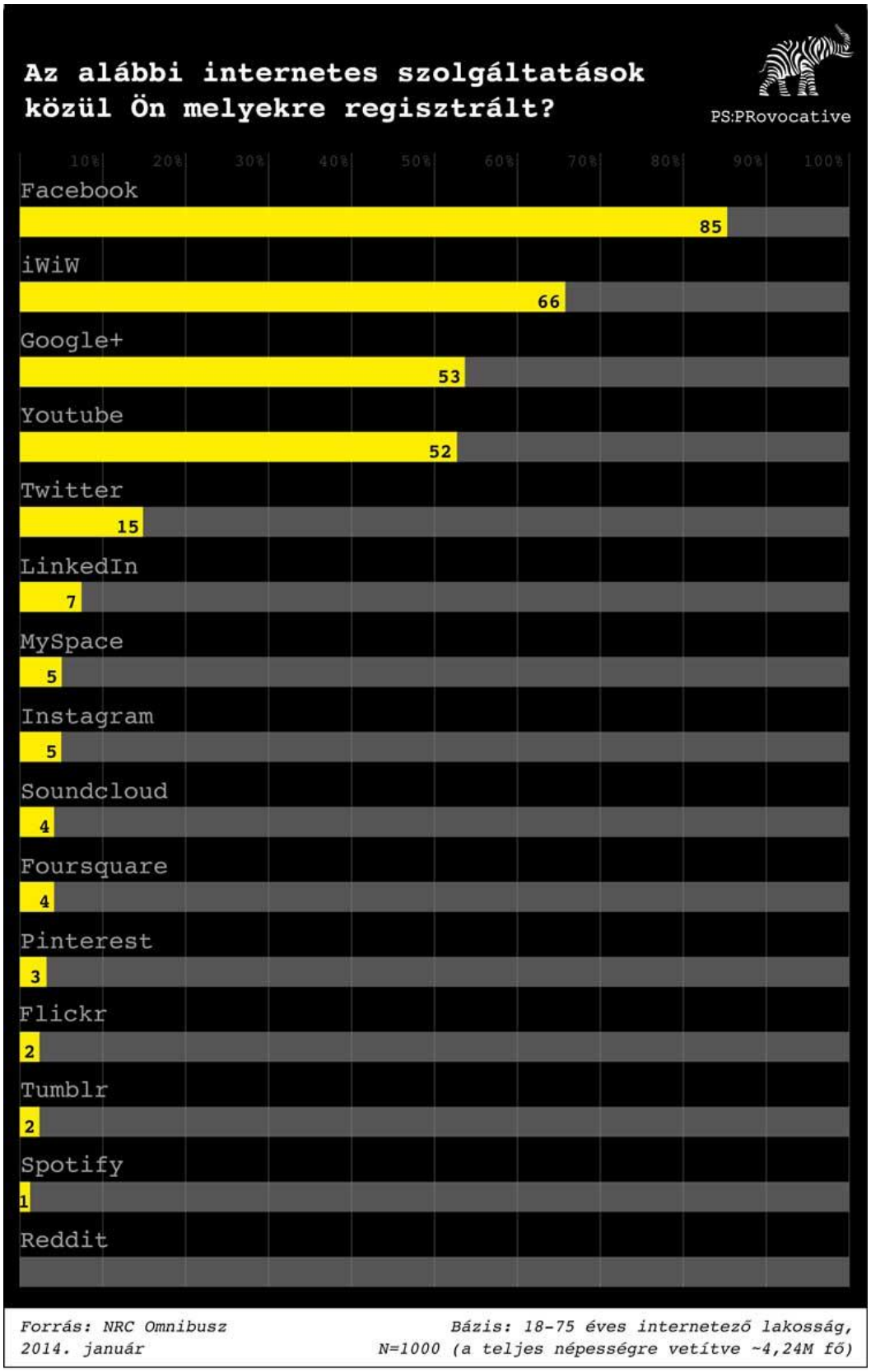
DOI azonosító: 10.17625/NKE.2015.021



8. ábra. Tartalomfeltöltési szokások.[74]

[74]Forrás: [153]

DOI azonosító: 10.17625/NKE.2015.021



9. ábra. Internetes szolgáltatások használati szokásai.[75]

[75] Forrás: [153]

DOI azonosító: 10.17625/NKE.2015.021

3.4.2. A leggyakrabban használt személyi használatú hordozható infokommunikációs eszközök jellemzői

Ma a leggyakrabban használt személyi használatú, hordozható infokommunikációs eszközöknek az okostelefonokat, a táblagépeket és a notebookokat tekinthetjük. [154] [155] Természetesen az elmúlt évek (évtizedek) tendenciája, a technológiák konvergenciája ebben a szegmensben is – ráadásul egyre gyorsuló formában – megtalálható, így valószínű, hogy néhány év múlva az említett három – jelenleg még markánsan elkülöníthető – csoport helyett csupán egy lesz jellemző. [156]

Az eszközök eltérő kivitelük, operációs rendszerük, stb. mellett is rendelkeznek közös tulajdonságokkal. Ilyenek az internet nagy sebességű, vezeték nélküli csatolók (pl. LTE, WiFi)[76] alkalmazása, ezáltal az internet-technológiára épülő szolgáltatások elérése, a kis méretek, a könnyű hordozhatóság, és a viszonylag nagy (akár tíz óra feletti) üzemidő. [157] [158] [159]

Miután a védett vezetők is a fenti három kategória valamelyik (vagy akár mindegyik) eszközét használják, [131] [132] [160] ezért érdemes a veszélyek szempontjából is a három kategóriát együtt, azok közös jellemzői alapján vizsgálni.

3.5. A releváns biztonsági kategóriák elemezése

Az internet-technológián alapuló szolgáltatások esetében az elemezendő biztonsági kategóriák meghatározása elvégezhető a 2.2.1. alfejezetben a „Vizsgálandó biztonsági kérdéscsoportok” kapcsán leírt, a felhő alapú rendszereknél általam már alkalmazott csoportosítás szerint. [139] [161] Természetesen a törvényes ellenőrzés vizsgálata a veszélyek feltárásához és a biztonságtudatos használat felkészítési módszerének kialakításához nem releváns, így attól itt eltekintek. Ugyanakkor az ott használt csoportosítás többi része felhasználható nemcsak az internet-technológiára épülő szolgáltatások, hanem a személyi használatú infokommunikációs eszközök biztonsági elemzésénél is. Ennek két oka is van. Az egyik, hogy az elérendő cél, azaz a védett vezető információbiztonságának garantálása a személyi használatú infokommunikációs eszközök, valamint az általa használt internet-technológia alapú szolgáltatások esetén szorosan összefügg, és nem érdemes az egyiket a másik nélkül vizsgálni. A másik pedig az, hogy a személyi használatú hordozható infokommunikációs eszközökre is értelmezhetőek ezek a kategóriák.

[76] WiFi: Az engedélt nélkül használható 2,4 és az 5 GHz-es frekvenciasávban működő vezeték nélküli helyi hálózat (WLAN) kialakítására szolgáló, széles körben elterjedt szabvány (IEEE 802.11)

DOI azonosító: 10.17625/NKE.2015.021

Így átvéve és elfogadva a 2.2.1. alfejezetben leírtakat, a vizsgálandó biztonsági kérdéseket az alábbi 3 csoportba sorolom:

1. üzembiztonság,
2. adatbiztonság,
3. egyéb (jogi, fizikai stb.) biztonság.

1. üzembiztonság

Üzembiztonság kérdése itt is azokat a jellemzőket foglalja össze, amelyek a rendszerek megbízható, üzemszerű működésével függnek össze. Ilyenek lehetnek például:

- elérhetőség: a tárolt adatok hozzáférhetősége onnan és akkor, ott és akkor, amikor a felhasználó szeretné;
- folyamatos szolgáltatás/rendelkezésre állás: internet-alapú szolgáltatásnál a szerződésben előírtak szerint (pl. 95%, de a szolgáltatás-kiesés nem hosszabb, mint 30 perc), eszközök esetén kicsit másképp, de szintén értelmezhető kategória;
- katasztrófa utáni visszaállítás: terv a lehető leggyorsabb, és lehetőleg adatvesztés nélkül történő adat-visszaállításra;
- hordozhatóság/interoperabilitás: adatok, átvitele egyik szolgáltatótól a másikhoz, vagy egyik eszközről a másikra megoldható legyen, ha szolgáltatót vagy eszközt kívánunk váltani;
- redundancia: magas rendelkezésre állás biztosítása a teljes infrastruktúra és a kapcsolódó eszközök tekintetében egyaránt.
- adatformátum: milyen formátumban állíjuk elő, tároljuk, továbbítjuk, stb. adatainkat, hiszen az adatkonverzió sok időbe és pénzbe kerülhet.

2. adatbiztonság

Ebben az esetben is adatbiztonsági kérdésnek tekinthetünk minden olyan tényezőt, amelyek a felhasználók adataihoz való biztonságos hozzáférés (kezelés, használat stb.), valamint az illetéktelen hozzáférések megakadályozása kapcsán felmerülnek. Ilyenek lehetnek például:

- adatszegregáció: többfelhasználós környezet lévén biztosítani kell, hogy az egyes felhasználók csak a saját adataikhoz férjenek hozzá.
- szolgáltatói adathozzáférés: internet-alapú szolgáltatás esetén számolni kell azzal, hogy a szolgáltató (és emberei) hozzáfér(het)nek a felhasználó adataihoz, legyen szó akár a munkájához kapcsolódó, akár szándékos (rosszindulatú) adatelérésről. (Eszközök esetében kicsit másképp, de szintén értelmezhető kérdés.)

DOI azonosító: 10.17625/NKE.2015.021

- (nem biztonságos, vagy nem teljes) törlés: meg kell oldani, hogy ha a felhasználó töröl egy adatot, az biztosan törlődjön (a biztonsági mentések és a redundáns tárolás ellenére is), visszaállíthatatlanul, mindenhonnan.
- alkalmazásbiztonság: a használt, futó alkalmazások sérülékenységei is lehetőséget teremthetnek a felhasználó adataihoz való illetéktelenek általi hozzáférésére, ezért ilyen szempontból is vizsgálni, tesztelni kell a szolgáltatásokat, eszközöket.
- titkosítás és kulcskezelés: internet-alapú szolgáltatásnál adataink a „felhőben" utaznak, ott tárolódnak, így elemi kérdés, hogy azokat a védelem érdekében tikosítsuk. (Eszközök esetében kicsit másképp, de szintén értelmezhető kérdés.)
- azonosítás és jogosultság-kezelés: alapvető feltétel, hogy a bejelentkezőt nagy biztonsággal azonosítani lehessen, és csak azokhoz a szolgáltatásokhoz és adatokhoz férjen hozzá, amelyhez jogosultsággal rendelkezik.
- virtualizáció: a virtualizált környezet kapcsán új, korábban a „hagyományos" informatikában nem ismert támadások jelentek meg (pl. másik felhasználó adatainak elérése a közös fizikai memóriából), amelyekre fel kell készülni.

Az adatbiztonság kéréskörét ebben az esetben is az adatok életciklusán (amelyet az 7. ábra szemléltet) keresztül érdemes megvizsgálni. A vizsgált kérdések közül elsősorban az internet-alapú szolgáltatások használata miatt az adatok életciklusának 6 állomását biztonsági szempontból itt is 2 fő csoportra célszerű bontani: az adatmozgással járó és az adatmozgással nem járó műveletekre. Ezt pedig azért célszerű megtenni, mert ha internet-alapú szolgáltatásokról beszélünk, akkor, ha a felhasználó bármilyen aktív műveletet végez, az az adatok mozgásával fog járni. Márpedig amennyiben ezt figyelembe vesszük, akkor a felhasználó és a szolgáltató felelősségi körét, ezáltal a felhasználó ráhatását veszélyekre, kockázatokra így jobban szét tudjuk választani.

3. egyéb (jogi, fizikai stb.) biztonság

A meghatározás itt sem változott, ebbe a kategóriába tartozik minden olyan biztonsági kérdéskör, amelyeket nem technikai úton kezelünk, és akár egy harmadik fél is bevonásra kerülhet (pl. audit). Ide soroljuk azokat a jogi garanciákat, amelyek adott kérdésköröket egyértelműen rendeznek, beleértve az üzembiztonsági és adatbiztonsági kérdéseknél felmerült, ilyen módon megoldandó feladatokat is, de például a fizikai védelmet is. Ilyenek lehetnek:

- audit: internet-alapú szolgáltatásoknál ezt egy 3. cég bevonásával lehet végrehajtani, ha a szerződés egyáltalán lehetővé teszi, a készülékek esetében ez nem értelmezhető.

DOI azonosító: 10.17625/NKE.2015.021

- hagyományos (fizikai) biztonság: hogyan gondoskodik a szolgáltató az adatközpontjai, vagy a felhasználó saját készülékei fizikai védelméről.
- adatok hosszú távú elérhetősége: internet-alapú szolgáltatásoknál értelmezhető, és azt tartalmazza, hogy hozzájuthatunk-e adatainkhoz akkor is, ha a szolgáltató csődbe megy, vagy felvásárolja egy másik cég.
- különféle naplóállományok és statisztikák tulajdonjoga: szintén az internet-alapú szolgáltatásoknál értelmezhető, alapvetően a felhasználási szerződés tartalmazhat kitételeket arról, hogy a szolgáltató mire használhatja az általa készített, ám érzékeny információkat is tartalmazó statisztikákat, naplóállományokat.
- szolgáltató általi szándékos adatlopás: kizárólag jogi úton kezelhető, de a használat megkezdése előtt gondolni kell erre is.
- alvállalkozók kérdése: az internet-alapú szolgáltatás üzemeltetője (pl. hardver eszközei karbantartásához), de a hordozható infokommunikációs eszköz gyártója (pl. szervizeléshez) alvállalkozókat is bevonhat a munkájába, akik adott esetben szintén hozzáférhetnek a felhasználó adataihoz, ám rájuk a szolgáltató és a felhasználó között megkötött szerződések nem feltétlenül érvényesek.
- (nem biztonságos, vagy nem teljes) törlés: az internet-alapú szolgáltatások esetében ez jogi kérdés is, hiszen főként így szabályozható, a hordozható infokommunikációs eszközök esetében azonban teljesen a felhasználó hatás-, és felelősségi köre.

3.6. Személyi használatú hordozható infokommunikációs eszközök, és azok használatával igénybe vett internet-technológiára épülő szolgáltatások veszélyei

A védett vezetők információbiztonsági védelme összetett feladat. Ebbe ma már szorosan beletartozik az általuk használt hordozható infokommunikációs eszközök, valamint az azokkal folytatott kommunikáció védelme is. [162] Ahhoz, hogy az információbiztonságot ebben a szegmensben is teljes körűen ki lehessen alakítani, több szervezet, sőt, a védett vezető aktív közreműködése is szükséges. Amint arra az előző alfejezet is rámutatott, a védett vezetők információbiztonságának garantálásához az információbiztonság komplex megközelítése szükséges. Ennek érdekében a technikai elhárítást ki kell terjeszteni a védett vezetők által használt kibertérre is, azon belül pedig kiemelten kell kezelni az elterjedt személyi használatú hordozható infokommunikációs eszközöket és az internet-technológiára épülő szolgáltatásokra. Ugyanakkor megítélésem szerint két dolog kijelenthető. Az egyik, hogy a védelemnek ez csak az egyik szegmense, másrészt a teljes körű védelem csupán technikai eszközökkel nem, vagy csak irreálisan magas költségekkel valósítható meg.

DOI azonosító: 10.17625/NKE.2015.021

A személyi használatú hordozható infokommunikációs eszközök és az internet-technológiára épülő szolgáltatások esetében a védekezés egyik leghatékonyabb módszere a biztonságtudatos használat, amelyre a védett vezetőket is fel lehet, fel kell készíteni. Ehhez viszont személyre szabott felkészítési módszert célszerű kialakítani, amelyhez a kellő alapot a lehetséges veszélyek áttekintése adhatja meg. A biztonsági kategóriák csoportosítását követően már célirányosan meg lehet vizsgálni, hogy az egyes kategóriákban milyen veszélyekkel találkozhat a felhasználó, és ezek közül melyek azok, amelyek biztonságtudatos felhasználással elkerülhetők, vagy legalábbis a kockázat mértéke csökkenthető. Ez azért lényeges, mert azokat, amelyekre nincs ráhatása a felhasználónak, tudomásul kell venni és arról kell dönteni, hogy használja-e vagy sem az adott eszközt, szolgáltatást, míg azoknál, amelyeknél van ráhatása, ott ismertetni kell a veszélyeket és oktatni a kockázatok csökkentésének módjait. Egyszerűbben szólva ezek alapján lehet majd – természetesen a védett vezetőkre vonatkozó egyéb speciális keretfeltételek figyelembevételével – kidolgozni egy hatékony biztonságtudatossági képzés módszerét.

3.6.1. Üzembiztonsági veszélyek

Az üzembiztonsági veszélyek gyakorlatilag két részre oszthatók: a felhasználó, mint üzemeltető által kontrollálható tényezőkre és a szolgáltatók által biztosított üzembiztonsági kérdésekre.

Az első csoportba tehát a felhasználó, mint üzemeltető által kontrollálható tényezők tartoznak. Az üzemeltető meghatározás ebben az esetben nem elírás. A felhasználónak ugyanis a hordozható infokommunikációs eszközök használatával vannak „üzemeltetői” feladatai és felelősségei is. Ilyenek lehetnek például az eszközei rendelkezésre állásának biztosítása (pl. akkumulátor feltöltése, kímélő használat stb.), a készülékein tárolt adatok biztonsági mentése, vagy azok redundáns tárolása. Ezek azonban ismertnek tekinthetőek, hiszen egyrészt egyértelműek (pl. akkumulátor feltöltése), másrészt jelentős részük (pl. biztonsági mentés) az asztali számítógépek kapcsán már minden felhasználó számára nyilvánvalónak feltételezhető.

A második csoport a szolgáltatók által biztosított üzembiztonság kérdése szintén egyszerűen rendezhető. A hordozható infokommunikációs eszközök esetében ez a gyártó által kínált garanciális és szervizelési feltételeket jelenti, amelyet a készülék vásárlásával a felhasználó elfogad. Mivel a védett vezetők számára a hivataluk biztosítja a hordozható infokommunikációs készülékeket, ezért ebben az esetben számukra ez már adott tényként kezelhető, erre ráhatásuk nincs.

DOI azonosító: 10.17625/NKE.2015.021

A készülékekkel elért legnépszerűbb – és így a védett vezetők által is leggyakrabban használt – internet-alapú szolgáltatások (pl. közösségi oldalak, levelezőrendszerek, tárhelyek stb.) igénybevételekor a szolgáltató által megírt, és minden felhasználó számára egyforma felhasználási feltételek – beleértve az üzembiztonsági (pl. rendelkezésre állás, redundáns tárolás stb.) kérdéseket – elfogadásáról vagy adott esetben elutasításáról dönthet a felhasználó. Itt egyedi szerződések megkötésére, egyedi feltételek kialakítására nincs lehetőség.
Összességében tehát megállapítható, hogy a fent leírtak okán, az üzembiztonsági kérdésekkel a védett vezetőknek szóló biztonságtudatossági képzés során nem célszerű foglalkozni.

3.6.2. Adatbiztonsági veszélyek

Az adatbiztonság témaköre az adatokhoz való biztonságos hozzáférés (kezelés, használat stb.), valamint az illetéktelen hozzáférések megakadályozása kapcsán felmerülő problémákat tartalmazza. A három kategóriát összehasonlítva ez az, amelyre a felhasználónak a legnagyobb ráhatása van, függetlenül a felhasznált eszköz vagy szolgáltatás típusától, valamint az elfogadott felhasználói szerződés tartalmától. Ennek okán érdemes áttekinteni, hogy a védett vezetők adatai milyen veszélyeknek vannak kitéve hordozható infokommunikációs eszközök és internet-alapú szolgáltatások igénybevétele során. Alapvetően négy kategóriába sorolhatjuk ezeket a veszélyeket:

- illegális adatszerzés;
- nem valós adatok feltöltése;
- nyílt forrású információgyűjtés;
- egyéb veszélyek.

Az illegális adatszerzés talán a legismertebb kategória, ez az, amire általában mindenki gondol. Ma a kibertérben az illegális információgyűjtésére, azok kereskedelmére komplett iparág alakult. Például egy ügyfél adatait tartalmazó, ellopott banki adatcsomagot 50 Fontért lehet értékesíteni. [163] De nem csak a bűnözőktől, hanem az idegen titkosszolgálatoktól, ellenérdekelt felektől is tartani kell. A Snowden által közzétett anyagok [136] megmutatták, hogy bizonyos titkosszolgálatok számára ma már gyakorlatilag bármely „átlagfelhasználó” levelezése, tárolt adatai megszerezhetőek, ha használja az internetet és az arra épülő népszerű szolgáltatásokat.
A nem valós adatok feltöltésének veszélye már nem mindenki számára ennyire nyílván való, pedig ez egy egyre jobban megfigyelhető jelenség. [164] Ebben az esetben egy megszerzett azonosítót, egy feltört honlapot, Facebook fiókot stb. nem információszerzésre használnak a támadók, hanem épp ellenkezőleg, hamis információk közlésére. Egy saját honlapot ért

DOI azonosító: 10.17625/NKE.2015.021

„deface”[77] támadás inkább csak kellemetlen, de egy saját blogban vagy Facebook fiókban történt bejegyzés már akár magyarázkodásra késztetheti a politikust, [165] adott esetben egy védett vezetőt. Ráadásul az incidens végén mindenkiben ott marad a kétely, hiszen a bejegyzés valódi feltöltőjének kiléte – főleg hosszabb idő elteltével – nagyon ritkán határozható meg egyértelműen. [166]

A nyílt forrású információgyűjtés veszélyei talán a legkevésbé ismertek. Ezt a technikát fel lehet használni az adott személyről elérhető információk összegyűjtéséhez (pl. profil elkészítéséhez), kapcsolati rendszerének feltérképezéséhez, vagy egy esetleges későbbi, akár kibertámadás előkészítéshez szükséges információk megszerzéséhez. A nyílt forrású információk között a támadóknak talán azok a leghasznosabbak, amelyeket a felhasználó saját maga tölt fel (ráadásul önként!) a különböző közösségi oldalakra, blogokra.

Az egyéb veszélyekbe tartozó problémák ugyan kapcsolódnak az előzőekhez, de mégis kilógnak a fenti három kategóriából. Ilyen például az adatok törlése az internetről. Egy korábban feltöltött információt ugyan eltávolíthat a gazdája, de – főleg a mindenki által hozzáférhető, pl. közösségi oldalak esetén – semmi sem garantálja, hogy azt másvalaki már nem mentette le, és töltötte fel máshová. Erre szokták mondani, hogy „az internet nem felejt!” Ugyancsak az egyéb veszélyek közé tartozik a blogok, közösségi oldalak kommentjeinek témája, ahol a látogatók, követők le tudják írni a véleményüket a bejegyzésekről (is). Egy politikus, védett vezető esetén itt célzott kommentekkel egyszerűen indíthatók lejáratókampányok, vagy félrevihetők az eredeti kommentek irányai ellehetetlenítve az eredeti témáról a vélemények kifejtését, vagy akár el is riasztva a szimpatizánsok egy részét azok olvasásától.

Az említett veszélyek az „átlagfelhasználó” esetén is fennállnak, de a védett vezetők esetén – akik mindig is kiemelt célpontot jelentettek az ellenérdekelt felek számára – még fokozottabban igazak. A veszélyek általános áttekintése után célszerű megkeresni azokat a pontokat, amelyekre a felhasználónak, így adott esetben a védett vezetőnek is van, lehet ráhatása.

Az adatok elérésének egyik sarkalatos pontja az azonosítás. A leggyakrabban használt internet-alapú szolgáltatások esetében ez a bejelentkezési névre és a jelszóra korlátozódik. Veszélyt jelent az azonosítók mások általi megszerzése, vagy kitalálása, hiszen így a támadók teljes jogosultsággal hozzáférhetnek a felhasználói fiókhoz, annak adataihoz. Ez ellen a felhasználó tehet bizonyos lépéseket. A már bejelentkezéskor biztonságos kapcsolatot

[77]Deface (vagy defacement): általában weboldalak feltörését és tartalmának, kinézetének megváltoztatását jelenti. (További információ pl.: http://www.techopedia.com/definition/4870/defacement)

DOI azonosító: 10.17625/NKE.2015.021

használó (pl. HTTPS)[78] szolgáltatások használatával jelentősen csökkenthető az azonosítók lehallgatás útján történő megszerzése, így amennyiben lehetséges, célszerű ilyet választani. A jelszó feltörése (pl. bruteforce[79] módszerrel) ellen is védekezhet a felhasználó, ha a jelszógenerálás alapvető szabályait (legalább 8 karakter, kisbetű, nagybetű, szám, esetleg speciális karakterek vegyesen) betartja, és annak megfelelően gyakori cseréjét elvégzi. Fontos megjegyezni, hogy a szolgáltató hálózatára a felhasználónak nincs ráhatása, így például az ellen nem tehet óvintézkedéseket, hogy ha szolgáltató rendszeréből szerzik meg az támadók az azonosító-adatokat. A hordozható eszközök esetében már több lehetősége van a felhasználónak. Itt gyakoriak és elterjedtek a különböző gyárilag beépített azonosító eljárások (pl. PIN[80] kódok, képernyő-feloldó, ujjlenyomat azonosító). Ehhez plusz védelmet adhat a felhasználó, például a teljes háttértárat titkosító alkalmazás használatával, amelynél szintén a megfelelő jelszó beírása szükséges az adatok eléréséhez, az eszköz rendeltetésszerű használatához.

A jogosultságkezeléssel – ráhatás híján – a leggyakrabban használt internet-alapú szolgáltatások esetében nem kell foglalkozni. Ennek ugyanakkor már van jelentősége a hordozható infokommunikációs eszközök esetében. Bizonyos rendszerek esetében (pl. Windows) a jogosultságok beállíthatók, így korlátozhatók bizonyos adatokhoz, szoftverekhez való hozzáférések, vagy szoftvertelepítési jogosultságok. Ez pedig segíthet megelőzni rosszindulatú szoftverek telepítését (települését) vagy az adatokhoz való hozzáférést, esetleg azok módosítását.

Internet-alapú szolgáltatásnál adataink a „felhőben” utaznak, ott tárolódnak, így elemi kérdés, hogy azokat lehallgatás és akár szolgáltatói hozzáférés elleni védelem érdekében tikosítsuk Eszközök esetében kicsit másképp, de szintén értelmezhető kérdés. Ott például az azonosítás kapcsán már említett teljes háttértárat titkosító megoldások alkalmazásával védhetőek adataink. Ez a védelem akkor is hatásos lehet, ha például az eszközt ellopják.

Hordozható eszközök tekintetében a fentieken túl további lehetőségek is a felhasználó rendelkezésére állnak arra, hogy az elektronikus úton történő illetéktelen adathozzáférés veszélyét csökkentse. Ezek között vannak olyanok, amelyek már mindenki számára ismertnek tekinthetőek, ilyenek például a biztonsági szoftverek használata (pl. vírusirtók, internet-

[78] HTTPS: Secure Hypertext Transfer Protocol, egy biztonságos információátviteli protokoll elosztott információs rendszerekhez.

[79] Bruteforce vagy nyers erő módszere, ahol a támadó az összes lehetséges jelszót végigpróbálgatva keresi meg a valódit. (További információ pl.: Biztonságos jelszavak és a gyenge jelszavak feltöréseshttp://iesb.hu/logikai-biztonsag/biztonsagos-jelszavak-es-a-gyenge-jelszavak-feltorese/

[80] PIN: Personal Identification Number, magyarul személyi azonosító szám, egy számjegyekből álló kód, amellyel általában különféle személyes jellegű adatokat, szolgáltatásokat védenek.

DOI azonosító: 10.17625/NKE.2015.021

biztonsági programcsomagok). Fontos ezek naprakészen tartása és az ellenőrzések rendszeres elvégzése. Szintén ilyen a felhasználói szoftverek naprakészen tartása, folyamatos frissítése. Ezzel ugyanis legalább a már ismert és javított sérülékenységek befoltozhatók. Vannak azonban olyanok, amelyek már nem ennyire értelemszerűek minden felhasználó számára.

Az egyik, hogy csak a feltétlenül szükséges szoftvereket telepítsük. Ennek több oka is van. Egyrészt minden szoftver tartalmaz(hat) olyan – publikusan még nem ismert – sérülékenységet, amelyet kihasználva a támadók hozzáférhetnek az eszközön tárolt adatokhoz vagy telepíthetnek más rosszindulatú programokat. Másrészt vannak olyanok, amelyek telepítésével a felhasználó elfogadja, és önként veti alá magát annak, hogy adatihoz a készítők hozzáférjenek. Ma a legtöbb – főleg ingyenesen – Android és iOS alkalmazás szerződési feltételei tartalmazzák ezt. Harmadrészt pedig vannak olyanok, amelyekbe kifejezetten adatszerzési szándékkal írtak bele bizonyos kódrészleteket. [167]

A másik kevésbé ismert veszélyforrás a hardver sérülékenységek kihasználhatósága. Egyfelől bizonyos hardver elemek támadhatóak, így akár a velük folytatott kommunikáció lehallgatható (pl. Bluetooth, WiFi), akár rajtuk keresztül az eszköz feletti ellenőrzés is átvehető. [162] Ezek elkerülése érdekében egyrészt kerülni lehet bizonyos eszközök használatát (pl. Bluetooth billentyű), másrészt bizonyos beállítások használatával fokozni lehet a biztonságot. Ez utóbbira egy példa lehet a WiFi-csatoló letiltása és csak szükség esetén történő használata. Ekkor ugyanis csökkenthető egyrészt az ezen keresztüli támadás, másrészt az általa bekapcsolásakor szórt információk (ugyanis azonnal keresni kezdi azokat a hálózatokat, amelyekre korábban már felkapcsolódott és ezek azonosítóit sugározza) lehallgatásának kockázata.

Összességében tehát megállapítható, – bár a fenti felsorolás korántsem teljes, már így is bizonyítja, – hogy az adatbiztonsági kérdésekkel a védett vezetőknek szóló biztonságtudatossági képzés során kiemelten célszerű foglalkozni. Ez az a terület, ahol a felhasználó – ebben az esetben a védett vezető – a legtöbbet tehet elektronikus információinak biztonsága érdekében. Ezek egy részét (pl. WiFi-csatoló kikapcsolása) ő maga képes elvégezni, míg más részében szakemberek (pl. egyéb biztonsági beállítások, biztonsági szoftverek telepítését az üzemeltető rendszergazdája, a hordozható eszközök átvizsgálását lehallgató eszközök, kémszoftverek megtalálása érdekében nemzetbiztonsági szakemberek) lehetnek, lesznek a segítségére. Ezen lehetőségek oktatása és fontosságuk tudatosítása a védett vezetők számára megkerülhetetlen.

DOI azonosító: 10.17625/NKE.2015.021

3.6.3. Egyéb (jogi, fizikai, stb.) biztonsági veszélyek

Az egyéb biztonsági kategóriába tartozó tényezőket a veszélyek szempontjából szintén aszerint érdemes áttekinteni, hogy azok elkerülésére, csökkentésére a felhasználóknak van-e bármilyen ráhatása.

A fizikai biztonságot kivéve, az ebbe a kategóriába eső biztonsági tényezőkre a felhasználónak nincs ráhatása. A hordozható infokommunikációs eszközök esetében nincsenek olyan jogi garanciák, amelyek az üzembiztonságon túlmutatnának, auditról, vagy esetleg más harmadik fél bevonását illető, nem technikai úton rendezendő kérdésről pedig nem beszélhetünk az említett készülékeknél.

Az említett eszközökkel elérhető internet-alapú szolgáltatásoknál már kicsit összetettebb, ám végeredmény szempontjából mégis hasonló a helyzet. A korábban említett, valamiféle elektronikus úton folytatott kommunikációt és a különféle adatok tárolását, megosztását lehetővé tevő szolgáltatásokra szűkített értelemben vett rendszerek használata esetén a felhasználónak – így a védett vezetőknek – is csupán a szolgáltató által kínált szerződés elfogadására, az abban megfogalmazott jogi lehetőségek igénybevételére van módjuk. Ráadásul, mivel a szolgáltatók a leggyakrabban külföldi telephellyel rendelkeznek és Magyarországon sem bejelentési, sem engedélyeztetési, sem egyéb (pl. hatósági felügyelet elfogadási, adófizetési stb.) kötelezettségük nincs, így probléma esetén még az országban hatályos jogi garanciák kikényszerítése is szinte lehetetlen. Auditról, vagy bármilyen más harmadik fél bevonását igénylő, nem technikai úton rendezendő kérdésről pedig itt sem beszélhetünk.

A fizikai biztonság esetében azonban már kettős képet kapunk. Egyfelől az internet-alapú szolgáltatásoknál a fizikai biztonságra, – hasonlóan a jogi kérdésekhez – a felhasználónak nincs ráhatása, nem szabhatja meg, vagy kérheti számon a szolgáltatót, hogyan és hány emberrel, milyen technikai berendezésekkel, vasráccsal stb. őrzi az adatközpontjait.

Másfelől a hordozható infokommunikációs eszközök esetében a fizikai védelem teljes egészében a felhasználó feladata, így arra teljes mértékű ráhatása van. Ráadásul több veszélyt is megelőzhet, vagy azok kockázatát csökkentheti, ha felelősen végzi ezt a tevékenységet. Megakadályozhatja a készülék eltulajdonítását, így egyrészt elkerülhet egyfajta információvesztést, másrészt azt, hogy illetéktelenek hozzáférjenek az adataihoz. A fizikai felügyeletnek azonban nem csak a készülék elvesztése, eltulajdonítása és az ezzel járó anyagi-, és információveszteség miatt van jelentősége. A néhány percre, órára magára hagyott eszköz lehetőséget biztosíthat illetéktelenek számára az eszközön lévő adatokhoz való hozzáférésre, azok lemásolására, vagy valamilyen rosszindulatú szoftver telepítésére is. Ez utóbbival pedig

DOI azonosító: 10.17625/NKE.2015.021

nem csak a készüléken éppen fent lévő adatokhoz, hanem a felhasználó – ez esetben a védett vezető – későbbiekben folytatott kommunikációjához, felvitt adataihoz, mozgási (hely) adataihoz stb. is hozzáférhetnek a támadók. [167] [168]

Problémát jelenthet családtagok (pl. gyerek) hozzáférése is a védett vezető hordozható infokommunikációs eszközeihez. Egyrészt, akár véletlenül is feltölthet valamilyen oldalra olyan adatokat, amelyeknek nem lenne szabad kikerülniük (gondoljunk itt például egy véleményezés alatt lévő törvényjavaslatra vagy beruházási tervre), másrészt pedig – a védett vezető tudta nélkül – telepíthet olyan programot, amely kártékony kódokat is tartalmazhat. [167] (Ezek veszélyeiről az adatbiztonság rész bővebben szól.)

Összességében tehát megállapítható, hogy az egyéb biztonsági kérdések közül a védett vezetőknek szóló biztonságtudatossági képzés során csupán a hordozható infokommunikációs eszközök fizikai biztonságának kérdéseivel célszerű foglalkozni, azzal viszont feltétlenül szükséges.

3.7. A személyre szabás keretrendszere

A védett vezetők személyre szabott információbiztonsági felkészítési módszer kidolgozásának egyik alapfeltétele a lehetséges veszélyek felmérése, amelyet az előző alfejezetben megtettem. Az ott leírtak pedig már megfelelő alapot teremt az felkészítés tartalmi elemeinek kidolgozásához. A másik alapfeltétel a személyre szabáshoz a védett vezetők speciális helyzetének felmérése. Figyelembe kell venni ugyanis az élethelyzetükből, munkájukból, elfoglaltságukból adódó feltételeket, amelyek egyfajta keretrendszert, feltételrendszert képzenek az információbiztonsági felkészítési módszeréhez.

Bár kifejezetten a védett vezetők felhasználói szokásairól nem készült felmérés a személyi használatú hordozható infokommunikációs eszközök valamint az internet-technológiára épülő szolgáltatások használata kapcsán, ám feltételezésem szerint a normál felhasználói szokásokból lehet általánosítani és ide vonatkozó következtetéseket levonni.

Véleményem szerint a figyelembe veendő feltevések, megállapítások a következőek:

- Használnak személyi infokommunikációs eszközöket.

Az első egy értelemszerű, de fontos megállapítás.

- Hordozzák ezeket az eszközöket.

Szintén értelemszerű megállapítás, ám fontos tényező a kialakítandó biztonság szempontjából. Az eszközök hordozása ugyanis olyan plusz kockázatokat rejt, amelyeket már érdemes, vagy inkább be kell építeni a biztonságtudatos képzésbe. Ilyenek lehetnek az előző alfejezetben és a "Hordozható infokommunikációs eszközök használatának veszélyei a védett vezetők

DOI azonosító: 10.17625/NKE.2015.021

biztonságtudatossági képzésének szempontjából" [169] című cikksorozatban megtalálható veszélyek, mint például az eszközök felügyelete, mások általi hozzáférése, kapcsolódás más hálózatokhoz, stb.

- Az eszközök jórészt normál kereskedelmi forgalomból származó, kommersz eszközök.

Ez azt jelenti, hogy ezek jellemzően nem rendelkeznek egyéni biztonsági funkcióval, vagy ha mégis, azok más országok által gyártottak. Ugyanakkor a világméretű elterjedtség, ismertség okán számos ismert sebezhetőséget, valamint akár a gyártó által beépített, esetleg ki is használt, információszivárgást okozó „funkciót" is tartalmaznak.

- Vegyes (részben magán, részben hivatali) jellegű használat a jellemző.

A személyi használatú, hordozható infokommunikációs eszközöket a védett vezetők általában hivatalból kapják, de – teljesen szabályos módon – magáncélra is használják, használhatják. Ez azonban nem csak a kommunikáció tartalma miatt, hanem a felhasznált internet-technológiára épülő szolgáltatások, ezáltal a készülékek ellenőrzése és a biztonságtudatossági képzés tartalma okán is figyelembe veendő tény. De éppen ezért az ellenőrzéshez és a biztonságtudatossági képzéshez is egészen más lehet a védett vezetők hozzáállása, mint egy tisztán hivatali célra igénybevett eszköz esetén.

- Mások (pl. családtagok) is hozzáférhetnek az eszközökhöz, sőt használhatják is azokat.

A magánjellegű használatból eredő kockázatot fokozza ez a kitétel, hiszen az eszközök egy részénél nehezen, vagy egyáltalán nem megvalósítható a jogosultságkezelés, a családtagok letölthetnek, telepíthetnek alkalmazásokat, esetleg véletlenül is feltölthetnek fájlokat az eszközről valamilyen oldalra. Ez pedig olyan, amelynek kockázatait és azok csökkentésének lehetőségeit szintén ismertetni kell a képzés során.

- Iskolai végzettségük (diplomáik szakterületei) óriási szórást mutat (pl. közgazdász, jogász, agrármérnök, bölcsész stb.)

A képzés kialakítása szempontjából ez egy meghatározó tényező, hiszen mindenki számára érthetően, sőt a későbbiekben alkalmazható módon kell az felkészítés tartalmi elemeit kialakítani.

- Jellemzően nem mély számítástechnikai, informatikai, kommunikációs és információbiztonsági ismeretekkel rendelkeznek, sőt ez a tudás csekélynek tekinthető

Az előző ponthoz szorosan kapcsolódó, de a felkészítés tartalmi elemeinek kialakítására nézve önállóan is fontos megállapítás.

- Jellemzően az érdeklődés a normál használat iránt is vegyes.

A védett vezetők egy része szereti „nyomkodni” a telefonját, táblagépét, más részük normál felhasználónak tekinthető, míg vannak köztük olyanok is, akik csak akkor használják, amikor feltétlenül szükséges. Ez hatással van a felhasználói ismeretekre, de a védendő információk mennyiségére is.

- A "megszokott" felhasználási módokat keresik, a biztonságosabb használat miatti korlátozásokat, nehezen fogadják el.

Minden olyan elem, amely a biztonságot emeli, várhatóan korlátozza a felhasználót és/vagy nehezíti a használatot. Ezt pedig akárcsak az „átlagfelhasználók” általában, a védett vezetők is nehezen fogadják, viselik el.

- Bonyolult azonosítási, felhasználási eljárások a védett vezetőket elriasztják a használattól, vagy keresik az elkerülő lehetőségeket.

Adott esetben a magasabb biztonsággal járó, bonyolultabb azonosítási eljárások okozta kényelmetlenségek ilyen reakciókat is kiválthatnak a védett vezetőkből. Ennek megelőzésében nem csupán az eljárások gondos megválogatása, hanem a biztonságtudatos képzés is sokat segíthet.

- Egy részük szereti, sőt akár presztízskérdésnek fogja fel az új mobil infokommunikációs eszközök birtoklását.

Az új eszközök új technikai lehetőségeket, ezáltal új biztonsági előnyöket és kockázatokat egyaránt jelentenek. A felkészítésnek figyelembe kell vennie és a lehetőségekhez mérten fel kell készítenie a védett vezetőt egy új készülék használatából adódó biztonsági kockázatokra és lehetőségekre.

- Számolni kell a személyes infokommunikációs eszközök elvesztésével, ellopásával.

A felkészítés során ki kell térni az ebből adódó kockázatokra, valamint azok csökkentésére vonatkozó lehetséges ellenlépésekre is. Tudatosítani kell, hogy mi a felhasználó feladata és felelőssége, és mi az rendszergazdáké.

- Jellemzően rendelkeznek közösségi oldalon, oldalakon profillal, és azt, azokat aktívan használják is.

A közösségi oldalakkal kapcsolatos veszélyek részint tartalmazzák az egyéb internet-technológiára épülő szolgáltatásokkal kapcsolatos kockázatokat, ugyanakkor máshol nem, vagy legalábbis nem ilyen formában jelentkező veszélyeket is. Az felkészítés során ezekre is fel kell hívni a figyelmet.

- Jellemzően használnak egyéb felhő alapú szolgáltatásokat levelezésre, adattárolásra stb. (pl. Gmail, Dropbox).

DOI azonosító: 10.17625/NKE.2015.021

A közösségi oldalak mellett a felhő alapú rendszerek használata is rejt speciális, csak ezekre jellemző veszélyeket. Ezekkel a jellegzetes problémákkal, kockázatokkal ugyanúgy foglalkozni kell az felkészítés során, mint a közösségi oldalak esetében.

- Jellemzően töltenek le és telepítenek újabb alkalmazásokat eszközeikre.

Ma már a legegyszerűbb alkalmazások is szinte minden esetben teljes hozzáférést kének adatainkhoz, telefonkönyvünkhöz, pozíciónkhoz stb., a szerződés elfogadásával pedig a felhasználó saját maga járul hozzá ezek átadásához. Ráadásul, mint minden szoftver, ezek is tartalmaznak, tartalmazhatnak olyan sérülékenységeket, netán tudatosan beépített hátsó kapukat, amelyet kihasználva a támadók szintén hozzáférhetnek a felhasználó minden adatához. A biztonságtudatos használat egyik alappillére, hogy a védett vezető ezekkel a kockázatokkal is tisztában legyen.

- Jellemzően a letöltött és telepített alkalmazások egy része, vagy akár egésze ingyenes.

A fentiek kiemelten igazak abban az esetben, ha a kiválasztott alkalmazás ingyenes. Ekkor ugyanis jóval több hozzáférést kell engedélyezni a szerződés elfogadásakor, mint fizetős társaiknál. Különösen jól megfigyelhető ez azoknál a szoftvereknél, ahol fizetős és ingyenes verzió is létezik ugyanabból a verzióból.

- Jellemzően kevés idővel rendelkeznek, amelyet felkészítésre, biztonságtudatosság növelésére lehet fordítani.

Lényeges szempont a felkészítés tartalmi elemeinek összeállításánál egy időkorlát meghatározása. Ez természetesen azt is jelenti, hogy nem csak a képzés anyagát kell nagyon gondosan megválogatni és tömören, de érthetően előadni, hanem azt is, hogy az összeállított módszer egyfajta alapképzés lehet, amelyet a későbbiekben lehetőség és igény szerint további, akár hosszabb oktatásokkal kell kiegészíteni.

- Az információbiztonság fontos számukra.

Szintén egyértelmű tény, hogy a védett vezetők tisztában vannak azzal, hogy sokszor kezelnek érzékeny információkat, amelyek megvédése fontos számukra. Ezáltal fogékonyabbnak tekinthetők az információbiztonság területén jelentkező problémák megértésére, mint az „átlagfelhasználók”. Ennek elősegítésére érdemes olyan példákat hozni az felkészítésben, amelyek ismertek, éppen ezért az információszerzés miatt kiemelt személyekkel kapcsolatosan mutatnak rá a lehetséges veszélyekre.

- A védett vezetőknél technikai elhárítás is segíti az információbiztonságot.

A védett vezetőknél az információbiztonság teljes körű garantálásának érdekében rendszeresen tartanak technikai elhárítást is. Az előző alfejezetben és a „Hordozható infokommunikációs eszközök használatának veszélyei a védett vezetők biztonságtudatossági

DOI azonosító: 10.17625/NKE.2015.021

képzésének szempontjából” [169] című cikksorozatban megtalálható a technikai elhárítás kiterjesztett értelmezése. Az ebben megfogalmazottak szerint ennek ki kell terjednie a védett vezetők hordozható infokommunikációs eszközeire is. Ez pedig nagyobb fokú biztonságot garantál, amelyet meg kell ismertetni a védett vezetőkkel.

3.8. A felkészítés tartalmi elemei

A feltárt veszélyeket, valamint a fenti feltételeket és feltevéseket figyelembe véve már kidolgozhatók a védett vezetők számára a személyükre szabott felkészítéshez szükséges tartalmi elemek.

A fent leírtak alapján a védett vezetőknek szóló, a személyi használatú hordozható infokommunikációs eszközök valamint internet-technológiára épülő szolgáltatások igénybevétele kapcsán jelentkező biztonságtudatos használatának alap felkészítési módszerénél a következőkből célszerű kiindulni:

- A képzést célszerű a – kiterjesztett értelemben vett és végrehajtott – technikai elhárítással összekötni, azzal párhuzamosan végrehajtani. Ekkor ugyanis átvizsgálásra kerülnek a védett vezető eszközei, és feltérképezésre kerülnek az esetleges információszivárgási csatornák, lehetséges információbiztonsági veszélyek.
- Az felkészítés megtartását célszerű a technikai elhárítást végző szervre bízni. Itt ugyanis a megfelelő időben rendelkezésre állnak a megfelelő ismerettel rendelkező szakemberek.
- Az felkészítés időtartamát célszerű körülbelül 60 percben meghatározni. Az egyedi felkészítés kapcsán ugyanis a védett vezetőknek várhatóan nem lesz több erre fordítható ideje, ennyi viszont feltétlenül szükséges a megfelelő információ átadásához.

Mindent egybevetve véleményem szerint a következő tartalmi elemeinek alapján célszerű elvégezni a felkészítést:

A felkészítés célja: A felkészítés keretében a védett vezető ismerje meg a személyi használatú hordozható infokommunikációs eszközök valamint internet-technológiára épülő szolgáltatások igénybevétele kapcsán jelentkező veszélyeket, azok elhárítása vagy legalábbis csökkentése érdekében általa elvégzendő teendőket, a biztonságtudatos használatot.

DOI azonosító: 10.17625/NKE.2015.021

A felkészítés tartalma:

1.	Veszélyek bemutatása példákkal
	a. Illetéktelen hozzáférés, lehallgatás
	i. A Snowden-ügy tanulságai
	ii. Egy pénzlopási ügy rövid bemutatása
	iii. Egy híres ember adatai illetéktelen megszerzésének és felhasználásának esete, rövid bemutatása
	b. Másodlagos adatok fontossága
	i. OSINT[81] bemutatása példával
	ii. Helymeghatározás bemutatása példával
	c. Adatvesztés bemutatása - Cryptolocker-példa [82]
	d. Nem valós adatfeltöltés, lejáratás bemutatása példával
2.	A biztonság megteremtésének módjai, beállítások, biztonságtudatos használat
	a. Üzembiztonsághoz kapcsolódó lehetőségek
	i. Felhő alapú rendszerek – szerződés elfogadás/elutasítás
	ii. Eszköz - biztonsági mentés
	b. Egyéb biztonsághoz kapcsolódó lehetőségek
	i. Jogi lehetőségek - korlátozott lehetőségek bemutatása
	ii. Fizikai védelem - tudatos viselkedés bemutatása példákkal
	c. Adatbiztonsághoz kapcsolódó lehetőségek
	i. Adatkészítés - biztonságos környezet kérdésköre
	1. Frissítések fontosságának bemutatása
	2. Minimalizált szoftverkörnyezet fontosságának bemutatása
	3. Új szoftvertelepítések elkerülésének fontossága
	4. Biztonsági szoftverek naprakészen tartásának fontossága
	5. Felhasználók kezelése, jogosultságok fontossága
	ii. Adattovábbítás kérdésköre
	1. Kapcsolódó(tt) hálózatok veszélyei beleértve a hardveres eszközöket pl. BT[83] billentyűzet is
	2. Távoli, passzív lehallgatás veszélyei
	3. Titkosítás fontosságai, korlátai
	iii. Bejelentkezés, adatmegadás, jelszó kérdésköre
	iv. Törlés, megsemmisítés, fióktörlés kérdésköre
	v. Social engineering veszélyei
3.	Ellenőrzés lehetőségei, fontossága
4.	Összefoglalás, kérdések

Elvárt eredmények:

A védett vezető:

- megértse a veszélyeket és elfogadja a biztonság fontosságát,

[81] OSINT. Open Source Intelligence nyílt forrású információgyűjtés
[82] A Cryptolocker egy, a merevlemezen lévő adatokat titkosító, majd a visszaállításért pénzt követelő vírus.
[83] BT: Bluetooth rövid hatótávolságú vezeték nélküli adatcseréhez használt szabvány

DOI azonosító: 10.17625/NKE.2015.021

- megértse és elfogadja a technikai elhárítás keretein belül a személyi használatú hordozható infokommunikációs eszközeinek vizsgálatát,
- megértse egy hosszabb idejű képzés fontosságát, a részvételhez érdeklődéssel és készségesen álljon hozzá,
- támogassa a felkészítés és a vizsgálat kiterjesztését közvetlen munkatársaira és családtagjaira,
- az általa használt személyi használatú hordozható infokommunikációs eszközeit valamint internet-technológiára épülő szolgáltatásokat a képzést követően a korábbiaknál sokkal nagyobb biztonságtudatossággal legyen képes használni.

Ütemezés: a technikai elhárítás alkalmával, kb. 60 perc időtartamban.

Irodalom és további információk:

- Az oktatók által elkészített 2-3 oldalas anyag, a személyi használatú hordozható infokommunikációs eszközök valamint internet-technológiára épülő szolgáltatások biztonságtudatos használatához szükséges legfontosabb információkkal.
- Az oktatók által elkészített 2-3 oldalas anyag, a személyi használatú hordozható infokommunikációs eszközök biztonságtudatos használatához szükséges legfontosabb beállításokkal kapcsolatos információkkal.
- Az oktatók által elkészített rövid, 10-15 perces flash[84] animáció, a személyi használatú hordozható infokommunikációs eszközök biztonságtudatos használatához szükséges legfontosabb beállításokkal kapcsolatos információkkal.
- Egy kontaktszemély adatainak átadása, akit a későbbiekben felmerülő kérdésekkel akár telefonon, akár e-mailben megkereshet.

A felkészítés tartalmi elemei alapján a tényleges, teljes ismeretanyag kidolgozása, annak naprakészen tartása már a képzést tartó szervezet szakembereinek, vezetőinek a feladata.

3.9. A továbblépés lehetőségei

A felkészítés tartalmi elemeinek meghatározása természetesen csak az első lépés a védett vezetők információbiztonságának minél magasabb szintű megteremtéséhez a személyi használatú hordozható infokommunikációs eszközök valamint internet-technológiára épülő szolgáltatások használata során. Bár nyilvánvalóan 100 %-os védelmet nem lehet kialakítani, de mindenképpen törekedni kell rá. A jelen fejezetben is már rámutattam, hogy a felvázolt

[84] Az Adobe Flash az Adobe Systems által gyártott professzionális multimédiás tartalomfejlesztő szoftver, például webes alkalmazások, játékok fejlesztésére.

DOI azonosító: 10.17625/NKE.2015.021

felkészítési elemek tartalommal való megtöltése, és a felkészítés végrehajtása mellett is vannak további feladatok, amelyek végrehajtásával a biztonsági szint tovább emelhető.

Ezek közül az első csoportba azok a feladatok tartoznak, amelyek minden, a cikkekben említett szereplőkön (védett vezető, technikai elhárítók, helyi biztonsági vezető, rendszergazdák) túlmutató, magasabb szintű megközelítést igényelnek. Ilyen például a megfelelő jogszabályi háttér kialakítása új jogszabályok létrehozásával és a meglévők szükséges mértékű átalakításával, ezeken belül pedig bizonyos biztonsági elemek kötelezővé tétele. Ilyen kötelező elem lehet(ne) a kiterjesztett értelemben vett technikai elhárítás előírása bizonyos vezetői szintig, meghatározott biztonságtudatossági felkészítésen, oktatáson való kötelező részvétel, vagy a hordozható infokommunikációs eszközök esetében, azok teljes életciklusára (fejlesztés, beszerzés, rendszerbe állítás, használat, kivonás stb.) vonatkoztatva kötelező biztonsági előírások kialakítása, betartatása, és hatósági ellenőrzése. Szintén a jogszabályi háttér kialakításakor kell gondolni a védett vezetők környezetében lévő személyekre, a technikai elhárítás rájuk történő kiterjesztésére is (pl. családtagok, közvetlen munkatársak, titkárság stb.). Ez azért is fontos, mert sokszor ők is kezelik a védett vezetőhöz kapcsolódó információkat, így az érzékeny adatok szivárgását náluk is meg kell előzni, akadályozni.

De ugyan ebbe a csoportba tartozik a védett vezetők felhasználási szokásainak felmérése is. Ilyen célzott felmérés ugyanis még nem készült, márpedig ez segítheti a specifikus kockázatelemzést. Bár a jelen fejezetben bemutatott alap biztonságtudatossági képzéshez ez nem elengedhetetlenül szükséges, a hosszabb, például 1 napos képzések tematikájának kialakításában, valamint a szükséges biztonsági szintek meghatározásában nagy segítséget nyújthat. A felmérés során választ kell kapni azokra a kérdésekre, hogy ki, milyen személyi használatú hordozható infokommunikációs eszközöket valamint internet-technológiára épülő szolgáltatásokat használ, és azokat mikor, hol, hogyan és mire. A felmérés természetesen – a lehetőségekhez mérten – lehet anonim, a „ki” kérdésnél sokkal érdekesebb a vezetési szint. Elsősorban azért, hogy meg lehessen állapítani, van-e statisztikailag is kimutatható markáns különbség az egyes vezetési szinteken lévő vezetők felhasználói szokásaiban.

A második csoportba a védett vezető által megtehető további feladatok tartoznak. Ilyen lehet a korábban említett további, hosszabb biztonságtudatossági képzésen való önkéntes részvétel, az önképzés, az egyéb lehetőségek, például konzultációs lehetőségek kiaknázása a biztonsági szakemberekkel, vagy a kiterjesztett értelemben vett technikai elhárítás aktív, segítő támogatása.

DOI azonosító: 10.17625/NKE.2015.021

A harmadik csoportba sorolhatóak az eszközök üzemeltetéséért, biztonságáért permanensen felelős helyi biztonsági vezető, a rendszergazda és munkatársaik feladatai. Ide tartoznak a felhasználási előírások megalkotása, betartatása, a meghajtó programok és a feltelepített alkalmazások naprakészen tartása, az eszközök biztonságos működéséhez szükséges beállítások megtétele, ismert, de javítatlan biztonsági rések esetén az adott szoftver esetleges cseréje hasonló tudásúra, a felesleges, ezáltal biztonsági kockázatot jelentő szoftverek eltávolítása, az incidensek kivizsgálását elősegítő alkalmazások telepítése, beállítások megtétele.

A negyedik csoportba sorolható további feladatok a technikai elhárításért felelős szervezetek felelősségi körébe tartoznak. Míg a helyi szervezetek feladata a permanens biztonság megteremtése, addig a technikai elhárítóké egy mélyebb biztonsági pillanatkép felvétele. Ebbe beletartozik a helyiségek mellett a hordozható infokommunikációs eszközök átvizsgálási metodikájának kidolgozása majd gyakorlati megvalósítása, a védett vezető munkahelyén érvényes helyi előírások áttekintése, azok megvalósításának ellenőrzése, valamint az általa használt eszközök speciális – hardver sebezhetőségi, kémszoftverek elleni – vizsgálata. Szintén ide sorolható a védett vezetők által leggyakrabban használt internet-technológiára épülő szolgáltatások, ezen belül is a felhő alapú rendszerek folyamatos vizsgálata, majd ezek alapján a figyelmük felhívása az említett rendszerek ismert sérülékenységeire, kockázataira.

A teendők részletes kibontása és az egyes szereplők közötti megosztása túlmutat a dolgozat keretein, ugyanakkor néhány fontos, már a közeljövőben megoldandó és elvégezendő, a felkészítéshez szorosan kapcsolódó feladatot már itt érdemes leszögezni.

Először is a fent leírt felkészítési módszert tartalommal kell kitölteni, amely a képzést tartó szervezet szakembereinek, vezetőinek a feladata. Ugyancsak az ő felelősségük az felkészítéshez kapcsolódó anyagok (2-3 oldalas leírások, flash animáció, stb.) elkészítése. Ezekhez bizonyos fajta segítséget nyújthatnak az általam a „Védett vezetők hordozható infokommunikációs eszközeinek védelme a rádiófrekvenciás tartományban” című cikkben megfogalmazottak. [170]

Szintén az ő feladatuk, hogy a későbbiekben figyelemmel kísérjék a technológiai változásokat, az új eszközök új tulajdonságait, a megjelenő új internet-technológiára épülő szolgáltatásokat, az azokból eredő új veszélyeket, és ezeknek megfelelően – ha szükséges – javítsanak, módosítsanak, változtassanak, frissítsenek a képzés tartalmán, vagy adott esetben magán a tematikán is.

DOI azonosító: 10.17625/NKE.2015.021

Célszerű további elméleti kutatásokat végezni és a technikai elhárításra, annak kiterjesztett értelmezése szerint egy új, pontos definíciót adni. Ennek kapcsán kell részletezni, pontosítani és elhatárolni a technikai elhárítók valamint a helyi, elektronikus biztonságért felelő személyek, szervezetek feladatait, hatáskörét.

Mihamarabb szükséges kidolgozni egy, az alap felkészítésnél jóval többet adó, az elektronikus információk védelmét előíró jogszabályokkal összhangban lévő, hosszabb időtartamú képzés tematikáját. Ennek fontos pontja az alap felkészítéshez hasonlóan az alábbiak:

- veszélyek bemutatása,
- biztonság megteremtésének módjai, beállítások, biztonságtudatos használat,
- ellenőrzés.

Ezt a lehető leghamarabb el kell indítani, még azelőtt, hogy azt jogszabályban kötelezővé tennék az érintett vezetői körnek.

Bár a továbblépés lehetőségeinél már szerepel, de kiemelést érdemel, hogy ugyancsak a lehető leghamarabb célszerű jogszabályi javaslatot megfogalmazni a hordozható infokommunikációs eszközök teljes életciklusát átfogó hatósági felügyeletére. Ebbe bele kell foglalni a beszerzendő eszközök engedélyezésétől kezdve, a használathoz kapcsolódó biztonsági előírások jóváhagyásán keresztül, a kivonáskor a használt adathordozók megsemmisítésének ellenőrzéséig minden olyan feladatot, amely hatósági eszköztárral segíti az elektronikus információbiztonság további emelését.

Összegzés, következtetések

A harmadik fejezetben **elemeztem a védett vezetők információbiztonsági felkészítésének főbb kérdéseit**. Ennek kapcsán **rávilágítottam**, hogy **a védett vezetők személyi használatú hordozható infokommunikációs eszközei esetében is vegyes (hivatali és magán) használatra kerül sor**, amelynél a felmerülő veszélyek nagyban hasonlítanak a BYOD, azaz a saját tulajdonú eszközök munkában történő felhasználása során jelentkező problémákra. Ebben az esetben talán annyival jobb a helyzet, hogy a nem felhasználói tulajdonú eszközök kissé jobban védhetők, például rezsimszabályokkal.

Rámutattam, hogy **a védett vezetők információbiztonságának garantálásához az információbiztonság komplex megközelítése szükséges**. Ennek érdekében **a technikai elhárítást ki kell terjeszteni a védett vezetők által használt kibertérre is**, így a klasszikusnak tekinthető helyiséglehallgató és –megfigyelő eszközök keresésén felül az ellenőrzés során vizsgálni kell a védett vezetők által használt munkahelyi számítástechnikai

DOI azonosító: 10.17625/NKE.2015.021

eszközöket, a személyi használatú hordozható infokommunikációs eszközöket és internet-technológiára épülő szolgáltatásokat is.

Megállapítottam azt is, **hogy csak technikai úton az információbiztonsági védelmet nem lehet, vagy irreálisan drága kialakítani**, ezért ez utóbbi eszközök és szolgáltatások tekintetében **az információk megvédésének egyik leghatékonyabb** – és nem utolsó sorban **legolcsóbb** – **módja a biztonságtudatos használat.** Ennek kialakításához viszont személyre szabott felkészítési módszert célszerű megalkotni, amelyhez először azonosítani kell a releváns veszélyeket.

Leszögeztem, hogy a kitűzött cél eléréséhez az internet-technológiára épülő szolgáltatásokat, ezeken belül is kiemelten az „átlagfelhasználók" által leggyakrabban használt PC/SaaS típusú rendszereket kell alaposabban megvizsgálni. Ám amint azt az 1.4.3. alfejezetben is bemutattam, a PC/SaaS rendszerek az internet-technológiára épülő szolgáltatások részhalmazának tekinthetők, de a határvonalat nagyon nehéz meghúzni. Éppen ezért, a fejezetben a kiterjesztőbb értelmű internet-technológiára épülő szolgáltatások megfogalmazást használtam.

Ezen szolgáltatások esetében a védett vezetők felhasználói szokásairól nem elérhető kimutatás, ezért azzal a feltételezéssel éltem, hogy azok ma nem térnek el jelentősen az „átlagfelhasználók" szokásaitól. Az utóbbiakkal kapcsolatban egy 2014-ben készült magyarországi felmérés alapján megállapítottam, hogy elsősorban a valamiféle elektronikus úton folytatott kommunikációt (pl. közösségi oldalak, levelezés, blogok, stb.) és a különféle adatok tárolását, megosztását lehetővé tevő szolgáltatásokat célszerű vizsgálat alá vonni.

A leggyakrabban használt személyi használatú, hordozható infokommunikációs eszközöknek a védett vezetők esetében is az okostelefonokat, a táblagépeket és a notebookokat azonosítottam.

Az így behatárolt személyi használatú, hordozható infokommunikációs eszközök és internet-technológiára épülő szolgáltatások kapcsán, a 2.2.1. alfejezetben általam már használt kategorizálás mentén **bemutattam**, hogy **az üzembiztonság, az adatbiztonság és az egyéb biztonság kategóriák esetében milyen releváns veszélyek állnak fenn**, ezek közül melyikre és milyen mértékű ráhatása lehet a felhasználónak.

Rámutattam arra is, hogy a feltárt veszélyek mellett a személyre szabott információbiztonsági felkészítés tartalmi elemeinek kidolgozásához **a védett vezetők speciális helyzetének figyelembevételére** szintén szükség van. Ennek kapcsán **felállítottam egy keretrendszert**, amelyben rögzítettem azokat a feltételezéseket, amelyekkel a felhasználói szokásaik, technikai ismereteik, az említett eszközökhöz, szolgáltatásokhoz és az

DOI azonosító: 10.17625/NKE.2015.021

információbiztonsághoz való viszonyulásuk kapcsán a védett vezetők esetében éltem. Aláhúztam, hogy ebben az esetben is a normál felhasználói szokásokból, attitűdökből indultam ki.

A feltárt veszélyeket, valamint a fenti feltételeket és feltevéseket figyelembe véve **kidolgoztam a védett vezetők számára a személyükre szabott biztonságtudatos használathoz kapcsolódó alap felkészítési módszert**, egyben **javaslatot tettem** arra, **hogy a felkészítés végrehajtására a technikai elhárítással egy időben, az elhárítást végző csapat munkatársai által kerüljön sor**.

Mindeközben **olyan általánosításokat tettem, amely lehetővé teszi, hogy az oktatott anyag** nem csak a védett vezető által éppen aktuálisan használt eszközre és szolgáltatásra legyen megfelelő, hanem azokat **a védett vezetők képesek legyenek alkalmazni** például egy **új szolgáltatás vagy eszköz igénybe vétele esetén is**.

Megállapítottam, hogy ez a felkészítés csupán az első lépés, önmagában nem elégséges, ezért **bemutattam a továbblépés lehetőségeit** négy kategóriában: a magasabb szintű megközelítést igénylő, a védett vezető által megtehető, az üzemeltetést végző személyek által megvalósítható, valamint a technikai elhárítást végzők által elvégezhető feladatok esetében. Bár ezek kibontása meghaladja a dolgozat kereteit, ugyanakkor rögzítettem néhány fontos, már a közeljövőben megoldandó és elvégezendő, az alap felkészítéshez szorosan kapcsolódó feladatot.

Megállapítottam azt is, hogy **az általam feltárt veszélyek és az információbiztonsági felkészítés tartalmi elemei** – megfelelő adaptációval – **más területeken** (pl. gazdasági, magán) **is felhasználhatók**.

DOI azonosító: 10.17625/NKE.2015.021

4. Az internet-technológiára 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 internet-technológiára épülő szolgáltatásoknak, ezeken belül pedig a PC/SaaS típusú felhő alapú rendszereknek. Ezek azok a mindenki számára elérhető, meglévő eszközeivel (pl. notebook, okostelefon stb.), akár csekély számítástechnikai tudással is használható, olcsón, sokszor ingyenesen igénybe vehető rendszerek, szolgáltatások (mint pl. Facebook, Gmail, Dropbox, Twitter, Skype stb.), amelyek ma már szerves részét képezik mindennapi életünknek, kommunikációnknak.

Ráadásul az internet-technológiára épülő szolgáltatások nemcsak kommunikációs szokásainkra hatnak, hanem 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, hanem 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 legtöbb esetben nem is tudnak egymásról, nincsenek semmilyen kapcsolatban egymással.

Az internet-technológiára épülő szolgáltatások, azokon belül is a felhő alapú rendszerek törvényes ellenőrzésének igénye a felhasználás ütemével arányosan nő, ugyanakkor a törvényes ellenőrzést végző szervek több – jogi és technikai – problémával is szembesülnek.

A fejezetben elemzem a hírközlés és a kommunikáció viszonyát, a jelenleg is zajló strukturális változásokat valamint az ezek kapcsán a törvényes ellenőrzés végrehajtásában jelentkező problémákat. Felállítok egy új modellt, amely véleményem szerint alkalmas a jelenlegi struktúra leírására, ráadásul úgy, hogy ebbe a modellbe nem csak a kommunikációt lehetővé tevő internet-technológiára épülő szolgáltatások, szolgáltatók illeszthetők be. Feltárom ezen rendszerek törvényes ellenőrzésnek jelenlegi lehetőségeit, problémáit, majd publikus forrásokból elérhető információkra alapozva jellemző példákat mutatok be külföldi nemzetbiztonsági szolgálatok és rendvédelmi szervek által használt módszerekre úgy, hogy közben megvizsgálom azok technikai és jogi megfelelőségét, elfogadottságát is.

DOI azonosító: 10.17625/NKE.2015.021

Felállítok egyfajta csoportosítást a törvényes ellenőrzéshez rendelkezésre álló technikai lehetőségek kategorizálására, amely ugyan nem teljes körű, azonban alkalmas egy általános összehasonlítási szempontrendszer felállítására és az összehasonlító elemzés elvégzésére. Megalkotom az ezek elemzéséhez szükséges szempontrendszert, és az így kialakított szempontrendszer alapján elvégzem a felsorolt technikai megoldások elemzését, csoportosítva azok előnyeit, hátrányait.

A megjelenő új technológiák mentén kialakult egy új szolgáltatói struktúra is, amelyhez a törvényes ellenőrzésnek is alkalmazkodnia kell. Bemutatom az elektronikus hírközlésről szóló 2003. évi C. törvény ezen okból történő módosításának szükségességét, áttekintem az új szolgáltatói modellben megtalálható tartalom-, infrastruktúra-, és alkalmazásszolgáltatók jelenleg elérhető definícióit, majd javaslatot tesz ezek új, a törvényes ellenőrzés szempontjából is megfelelő, akár jogszabályba is illeszthető meghatározására.

A fentiek alapján látható, hogy a nemzetbiztonsági szolgálatok és rendvédelmi szervek szerepköre ebben az esetben eltér az előző fejezetekben vizsgáltaktól. Míg a második fejezetben közvetlen felhasználóként, a harmadikban a védett vezetők védelmét ilyen téren is biztosító, mintegy harmadik félként jelentek meg, addig itt törvényes ellenőrzést végzőként kell feladataikat ellátniuk. Ez pedig azt jelenti, hogy a szolgáltatóval való viszonyuk, a felelősségi és érdekkörök megoszlása is – ahogy azt a 2.2.1. alfejezetben leírtam – jelentősen eltér az előzőekben említettektől.

Akárcsak az előző fejezetben, úgy most is kiemelendő, hogy a kitűzött célok eléréséhez, érdemi, valóban jól használható eredményekhez nem érdemes ebben az esetben sem leszűkíteni a vizsgálatot a felhő alapú rendszerekre. Amint azt az 1.4.3. alfejezetben is bemutattam, a PC/SaaS rendszerek mindenképpen az internet-technológiára épülő szolgáltatások részhalmazának tekinthetők, ám a határvonalat, hogy mi tekinthető egyértelműen PC/SaaS rendszernek, nagyon nehéz meghúzni. Éppen ezért - az ott leírtak alapján - a dolgozat céljának eléréséhez, a fejezetben a kiterjesztőbb értelmű internet-technológiára épülő szolgáltatások megfogalmazást használom, de egyértelműen, sőt kiemelten beleértem a PC/SaaS rendszereket is.

4.1. A kommunikáció változása

A kommunikáció formái, lehetőségei az internet, az internet-technológiára épülő szolgáltatások, azokon belül is kiemelten a PC/SaaS felhő alapú rendszerek valamint az ezek elérését biztosító eszközök fejlődésével ugrásszerűen változnak, bővülnek. Amint azt a 3.1.

DOI azonosító: 10.17625/NKE.2015.021

alfejezetben is megállapítottam, ezek egyfajta összefonódó spirált képezve, 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. [148] [129] 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 internet-technológiára 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,
- kommunikációellenőrzés,
- 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 és 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 vetnek fel a törvényes ellenőrzésre feljogosított szervezetek számára. [171] Álláspontom szerint elemezni kell a változások okait, tendenciáit, majd az azokból következő problémákat és lehetőségeket. Erre azért van szükség, mert a korábbi, jól működő, a törvényes ellenőrzésre feljogosított szervek számára tevékenységük

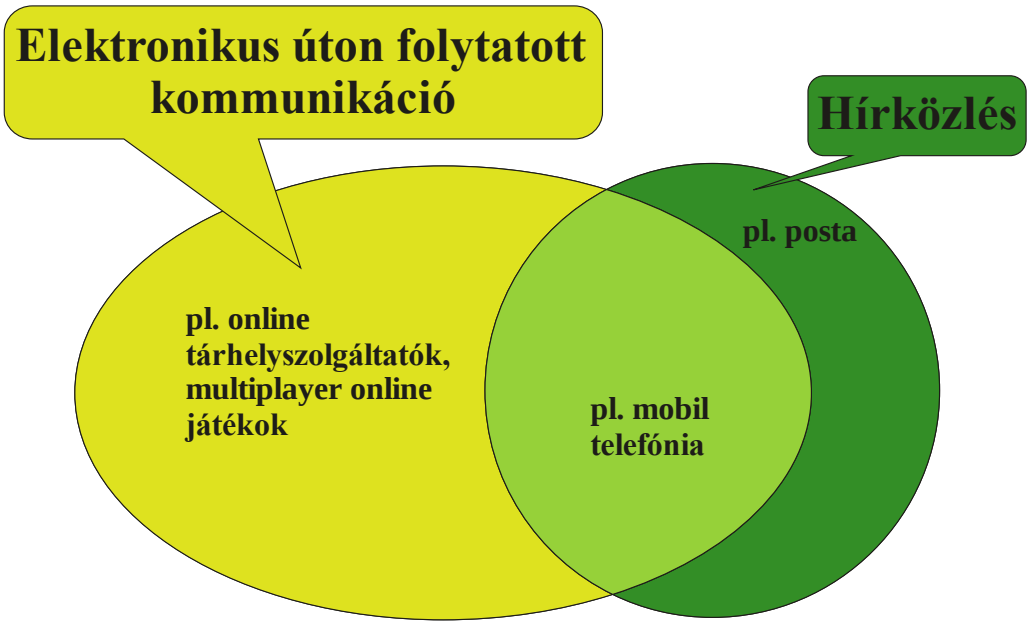
DOI azonosító: 10.17625/NKE.2015.021

ellátásához jelenleg rendelkezésre álló technikai és jogi eszközök ma már sok esetben nem teszik lehetővé a teljes körű, hatékony feladat-végrehajtást.

4.1.1. Elektronikus úton folytatott kommunikáció vs. hírközlés

Az elektronikus úton folytatott kommunikáció megnevezés teljesen tudatos szóhasználat. Napjainkban ugyanis az említett fogalom alatt nem csak 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 internet alapú 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 10. ábra megfelelően szemléltetné a kettő kapcsolatát. A területek nagyságával az egymáshoz képesti jelentőséget is szemléltetni kívántam.



10. ábra. Az elektronikus úton folytatott kommunikáció és a hírközlés viszonya.[85]

Ma az elektronikus úton folytatott kommunikáció lehetőségei messze meghaladják a hagyományos hírközlését. A végeredmény szempontjából ugyanis nincs különbség a között, hogy megírok és elküldök egy elektronikus levelet, vagy megírás után a piszkozatok közé teszem, de a másik félnek megadom a postafiók eléréséhez szükséges felhasználónevet és jelszót. Hiszen ez utóbbi esetben is hozzáfér, olvashatja ugyanazt az üzenetet. De itt még

[85] Szerkesztette a szerző.

DOI azonosító: 10.17625/NKE.2015.021

legalább a „levélszerűség” megvan, a „hagyományos” hírközlési forma fellelhető. Ha a továbbítani szánt információkat azonban egy felhő alapú tárhely szolgáltatónál kialakított fiókba helyezem el fájlként, majd ennek adom 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 feladata, célja, hogy a kijelölt célszemélyek kommunikációját lehetőség szerint teljes mértékben ellenőrizzék függetlenül annak formájától, a felhasznált technológiától. Az egyik legnagyobb feladat tehát, hogy az adott szervezetek pontosan meghatározzák azt, hogy mit kell ehhez ellenőrizniük, majd ehhez ki kell alakítani a megfelelő technikai és jogszabályi környezetet.

4.1.2. Az elektronikus úton folytatott kommunikáció változása

A fejezetben nem célom, hogy az elektronikus úton folytatott kommunikációs technológiák változásának okait, tendenciáit teljes vertikumukban bemutassam, csupán érzékeltetni kívánom, hogy miért kell foglalkozni vele, miért és milyen hatása van a törvényes ellenőrzésre.

A kommunikációs technológiák és szokások nem választhatók szét egymástól, egyfajta összefonódó spirált képezve, egymást is erősítve, gerjesztve hozták létre a mai népszerű kommunikációs formákat, lehetőségeket. A szélessávú és mobil internet elérések elterjedése, a hordozható eszközök (pl. ultrabookok, tabletek, okostelefonok stb.) hihetetlen mértékű fejlődése, a közösségi oldalak népszerűségének ugrásszerű növekedése, a különböző kommunikációs lehetőségeket biztosító internet-technológiára épülő szolgáltatások, ezen belül kiemelten a PC/SaaS felhő alapú rendszerek 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, használatra.

A technológia fejlődésének, a kommunikációs formák és lehetőségek rohamos bővülésének köszönhetően a felhasználói szokások nagymértékben megváltoztak az elmúlt években. Az un. Y (1980-1994 között születtek) és Z (1995-2009 között születtek) generáció [172] tagjai

DOI azonosító: 10.17625/NKE.2015.021

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. [173] A korábbi generációk hagyományos elektronikus kapcsolatteremtési formái (pl. telefónia, SMS) helyett számukra sokkal fontosabbak az internet alapú kommunikációs lehetőségek, azok használatát játszi könnyedséggel sajátítják el, a kibővített funkciókat természetesen és teljes körűen 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 jelentik az ikonikus technológiákat, szemben például az X (1965-1979 között születtek) generáció tagjaival, akiknek ugyanezt a kazettás videomagnó, a walkman és az IBM PC testesítették meg. [172]

Az új technológiák megjelenése önmagukban is arra késztetik 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 (pl. telefónia) jelentősége a felhasználók – ezáltal a potenciális célszemélyi kör, így a törvényes ellenőrzést végző szolgálatok – számára csökken.

4.1.3. A hírközlés változása

A megfizethető havidíjú, korlátlan adatforgalmat biztosító szélessávú 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, akik elektronikus hírközlő hálózatot üzemeltetnek és ezen hírközlő szolgáltatást nyújtanak. A hangsúly a

DOI azonosító: 10.17625/NKE.2015.021

klasszikus szolgáltatók esetében az „és”-en van, azaz a két szolgáltatási tevékenységet együtt végzik. Ilyenek pl. a hagyományos (vezetékes és mobil) telefonszolgáltatást biztosító cégek.

Az elektronikus hírközlésről szóló 2003. évi C. törvény (Eht.), [174] így annak a 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 következőek:

„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.”

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 volt elérhető!), míg 2011-re átlagban 20 millió felhasználó használta egyidejűleg. [175] Másik példa a Facebook, amely 2004. február 4-én debütált, tehát a törvény hatályban lépésekor (2004. január 1-én) [174] 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. [176] [177]

A Skype mellett számtalan jelenleg kisebb vagy nagyobb jelentőséggel bíró internet alapú 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, és ez a tendencia a jövőben várhatóan tovább erősödik. Az új modell legjelentősebb hatása a hírközlésre, hogy az infrastruktúraszolgáltató a hírközlési hálózatot – vagy célszerűbb megfogalmazással internet

DOI azonosító: 10.17625/NKE.2015.021

elérést – biztosítja, míg az alkalmazásszolgáltató gondoskodik a tényleges kommunikációs szolgáltatásról.

Az infrastruktúra-, alkalmazás-, és tartalomszolgáltatói modell pontos leírását a fejezet utolsó részében adom meg. Itt csak olyan mértékben említem, amennyire a törvényes ellenőrzés problémáinak felvetéséhez és lehetőségeinek vizsgálatához szükséges, és éppen ezért a tartalomszolgáltatókkal itt egyáltalán nem foglalkozom.

Az alkalmazásszolgáltató elnevezést nem csak azért célszerű használni a hírközlési szolgáltató helyett, hogy megkülönböztessük 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. Erre mutattunk be egy példát szerzőtársammal a „Felhő alapú új pénzügyi tranzakciós lehetőségek és azok veszélyei" című cikkünkben. [178] Ennek pedig véleményem szerint a törvényes ellenőrzés jogi eszközeinek átalakítása során is nagy jelentősége lesz.

A hírközlési szolgáltatók specializált szolgáltatókra történő szétválása nemcsak a törvényes ellenőrzés tekintetében jelent problémát. Amint azt már a fejezet elején is bemutattam, a szélessávú, 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 mobil internetről is elmondható – megfizethető, nem túlságosan magas fix havi díjért, korlátlan vagy az átlag felhasználói szokások okán annak tekinthető adatforgalommal nagyon sok ember számára elérhető. Ha kifejezetten a mobil kommunikációt 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 internet alapú kommunikációs szolgáltatásoknak csupán egy része ingyenes, más részük igénybevételéért (pl. vezetékes vagy mobiltelefon hívása esetén) viszont fizethetnünk kell. De még az ingyenes szolgáltatások esetében is jelentős reklámbevételek keletkeznek. Ez természetes, hiszen ezekből a bevételekből fedezi az alkalmazásszolgáltató a költségeit, és a megmaradó profit az, amiért érdemes ezt a tevékenységet folytatnia. Ám a profit csak nála és nem az internet szolgáltatónál – aki ez esetben infrastruktúraszolgáltatóvá avanzsált – képződik. Ugyanez elmondható nem csak 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 havidíjak összegét. Ez a mobil internetet nyújtó, infrastruktúrát is üzemeltető

DOI azonosító: 10.17625/NKE.2015.021

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 és nem utolsó sorban a hirdetőktől befolyó jóval magasabb összegeknek köszönhetik.

Ezt a jelenséget az egyre inkább infrastruktúraszolgáltatóvá váló hírközlési cégek is kezdik felismerni és próbálnak valamit tenni a helyzet megváltoztatása érdekében. Erre az egyik legjobb példa az Orange cég esete, akinek sikerült elérnie, hogy a nagy költséggel járó infrastrukturális fejlesztéseihez a hálózatát – természetesen a felhasználói kérések által – leginkább használó Google pénzügyileg hozzájáruljon. [179] [180] Erre korábban is voltak már – sikertelen – kezdeményezések, [181] a francia szolgáltató sikeres akciója azonban precedenst teremtett. Lépésével várhatóan egy folyamat indul el, átalakul az internet korábbi, sérthetetlennek tűnő üzleti modellje. [179]

4.1.4. Az internet-technológiára 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 internet-technológiára 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 általam vázolt modell szerint itt ugyanis sokkal inkább különálló infrastruktúra-, alkalmazás-, és tartalomszolgáltatókkal találkozunk, nagyon ritka az az eset, amikor a felhasznált infrastruktúrát és alkalmazást egyazon szolgáltató biztosítja. Márpedig a hatályos magyar jogszabályok alapján csak ez utóbbi esetében lenne vitán felül állóan hírközlési szolgáltatónak tekinthető és így a törvényes ellenőrzés kapcsán együttműködésre kötelezhető bármely szolgáltató. Ugyanakkor a jelenleg érvényben lévő jogszabályainkban az infrastruktúra-, alkalmazás-, és tartalomszolgáltatók nem vagy nem megfelelő módon vannak

DOI azonosító: 10.17625/NKE.2015.021

definiálva, a törvényes ellenőrzés kapcsán felmerülő kötelezettségeik pedig szintén nem vagy jó esetben is csak részlegesen olvashatók ki ezekből.

Az ellenőrzéshez használt technikai eszközök kapcsán ugyancsak problémákkal szembesülnek a felhatalmazott szolgálatok. Egyrészt az új technológia új ellenőrző eszközöket kíván, kívánhat, ráadásul ezek akár szolgáltatónként eltérő megoldásúak lehetnek. Ez pedig meglehetősen költséges beruházásokat indukálhat. Másrészt a hírközlés szolgáltatókkal ellentétben, akik – a törvényi kötelezettségek okán - együttműködnek a nemzetbiztonsági és bűnüldöző szervekkel, az új nem vagy nem teljes mértékben twszik 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”*. [174] Ilyenfajta kötelezettsége azonban jelenleg nincs az alkalmazásszolgáltatóknak Magyarországon, de ennek előírása az Európai Unió más országainak, sőt a világ többi államának is komoly problémákat okoz.

Jelenleg nincs olyan szabályozás, amely európai szinten irányadó lenne a kérdésben, és amely rövid időn belül, nagyobb szolgáltatói ellenállás nélkül átemelhető lenne a magyar törvényekbe. Ez pedig két gondot okoz. Az első, hogy az alkalmazásszolgáltatók hajlandóságán múlik, hogy engedi-e ellenőrző eszköz telepítését, esetleg saját eszközeivel egyfajta törvényes ellenőrzés, mint szolgáltatást (LMaaS)[86] [139] nyújt a szolgálatok számára, vagy teljesen elutasítja az együttműködést. Ez utóbbira – sajnos negatív – példa a Google esete, aki nem, hogy nem működik együtt, de átláthatósági jelentéseiben még közzé is teszi, hogy 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 jelenleg hatályos törvényi feltételeket. [182] 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 internet-technológiára épülő szolgáltatások ellenőrzésére elsősorban egyedi problémákat megoldó eszközöket tudnak csak szállítani. Ez pedig drágává, bonyolulttá és esetivé teszi az ellenőrzéseket.

Véleményem szerint a megoldás első lépését a törvényi háttér kialakítása jelentheti. Ebben az egyik legfontosabb feladat, hogy pontosan definiáljuk az infrastruktúra-, alkalmazás-, és

[86] LMaaS: Lawful Monitoring as a Service, törvényes ellenőrzés, mint szolgáltatás

DOI azonosító: 10.17625/NKE.2015.021

tartalomszolgáltatók fogalmát, meghatározzuk, mit kell ellenőrizni és annak megfelelően kell kialakítani a megfelelő jogszabályi környezetet. Amint az előző alfejezet végén az Orange cég példáján keresztül bemutattam, 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 a hazai infrastruktúrával nem rendelkező, internetes alkalmazást nyújtó cégek működési jogai, kötelezettségei Magyarországon.

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 nem mondható el. Ez utóbbi szolgáltatók egy része csak bizonyos jogértelmezéssel lenne az Eht. hatálya alá tartozónak tekinthető, más részük pedig még úgy sem. Az NMHH által közzétett, „Elektronikus hírközlési szolgáltatások hatósági osztályozása" alatt megtalálható „Szolgáltatás típusok" [183] és „Szolgáltatás leírása" [184] dokumentumok sem segítenek a probléma feloldásában, hiszen azok is kifejezetten a klasszikus hírközlési szolgáltatásokra koncentrálnak. Ezt bizonyítja az is, hogy az „Egyéb előfizetői adatátviteli szolgáltatás" címke alatti leírásnál – ahová talán beleérthetőek lennének az alkalmazásszolgáltatók – a következő példa szerepel: *„Ide tartozik például az önálló elektronikus hírközlési szolgáltatásként nyújtott MMS szolgáltatás."* Az viszont egységesen elmondható, hogy az alkalmazásszolgáltatók szankcionálására egyrészt eddig nem volt példa, másrészt az egyébként is rendkívül nehezen kivitelezhető.

Így fordulhat elő, hogy a korábban már említett eset szerint a Google bár Magyarországon szolgáltat, ki tud bújni a hatályos jogszabályok alól és az érvényes törvényeknek megfelelő adatszolgáltatási kérést vissza tudja utasítani. [182] Ez a hagyományos postai és klasszikus elektronikus hírközlési szolgáltatók esetében elképzelhetetlen lenne. Ráadásul a Google-nak, és a többi hasonló alkalmazásszolgáltatónak még azok a törvényes ellenőrzéshez kapcsolódó költségeket sem kell viselnie, amit a hírközlési szolgáltatók a magyarországi piacra lépésükkel vállalnak.

DOI azonosító: 10.17625/NKE.2015.021

A felhő alapú – így a PC/SaaS – rendszerek törvényes ellenőrzésének szabványosításán többek között az ITU és az ETSI is dolgozik. Ám 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. Véleményem szerint a megoldást egy új – akár átmenetinek is tekinthető – hazai jogi szabályozás kialakítása jelentheti.

4.2. Az internet-technológiára 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 szerintem tökéletesen 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 célszerűnek tartom megvizsgálni és összehasonlítani a törvényes ellenőrzésre jelenleg rendelkezésre álló technikai eszközöket és módszereket azok előnyeivel, hátrányaival együtt. Ez egyrészt lehetőséget ad majd a szolgálatoknak arra, hogy kiválaszthassák egy adott feladathoz leginkább megfelelőnek és hatékonynak tartott, törvényesen felhasználható módszert, másrészt segít rávilágítni, hol vannak olyan törvényi hiányosságok, amelyeket az új jogszabályi környezetben mindenképp le kell fedni. Álláspontom szerint ezt követően lehet a jogi szabályozás kialakítása érdekében pontosan definiálni az infrastruktúra-, alkalmazás- és tartalomszolgáltatók fogalmát.

Ennek érdekében viszont először elemezni kell az internet-technológiára 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. Én ehhez a példák ismertetésénél főként a Skype-ot használom mintának. Egyrészt azért, mert ennek a rendszernek a 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.

DOI azonosító: 10.17625/NKE.2015.021

4.2.1. Az internet-technológiára épülő szolgáltatások törvényes ellenőrzési kihívásai

Az internet-technológiára épülő szolgáltatások, ezen belül is a kiemelten a felhő alapú rendszerek törvényes ellenőrzése minden ország nemzetbiztonsági és rendvédelmi szervét kihívások elé állítja. Amint azt az 4.1. alfejezetben is bemutattam, 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 oldani, hiszen alapvető feladatuk az, hogy a kijelölt célszemélyek 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 (pl. 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, a kiválasztott rendszerek ellenőrzésének technikai megoldása pedig 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 internet-technológiára épülő szolgáltatásoknak, azon belül pedig a PC/SaaS felhő alapú rendszereknek, ahol is alkalmazásszolgáltatók biztosítják azokat a szolgáltatásokat, amelyeken keresztül – a lehető legkülönfélébb módon – elektronikus kommunikációt lehet folytatni. Ezen rendszerek törvényes ellenőrzésének megteremtése tehát kiemelt feladat az arra feljogosított szervek számára, ugyanakkor a feladat ellátását több probléma is nehezíti.

Az egyik probléma 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 internet-technológiára épülő szolgáltatások ellenőrzését.

A másik problémát a technikai megoldások hiánya jelenti. Az új technológia új ellenőrző eszközöket kíván, kívánhat, ez pedig jelentős beruházásokat igényel. Ráadásul az eltérően felépített szolgáltatói infrastruktúrák miatt ez akár szolgáltatónként eltérő megoldásokat

DOI azonosító: 10.17625/NKE.2015.021

igényelhet, ami igen költséges. Sokszor azonban még nagyobb problémát 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 és 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, hogy egyáltalán milyen módszerek állnak a titkos információgyűjtést végző szervezetek rendelkezésére, és azok alkalmazása során milyen buktatókba ütköztek.

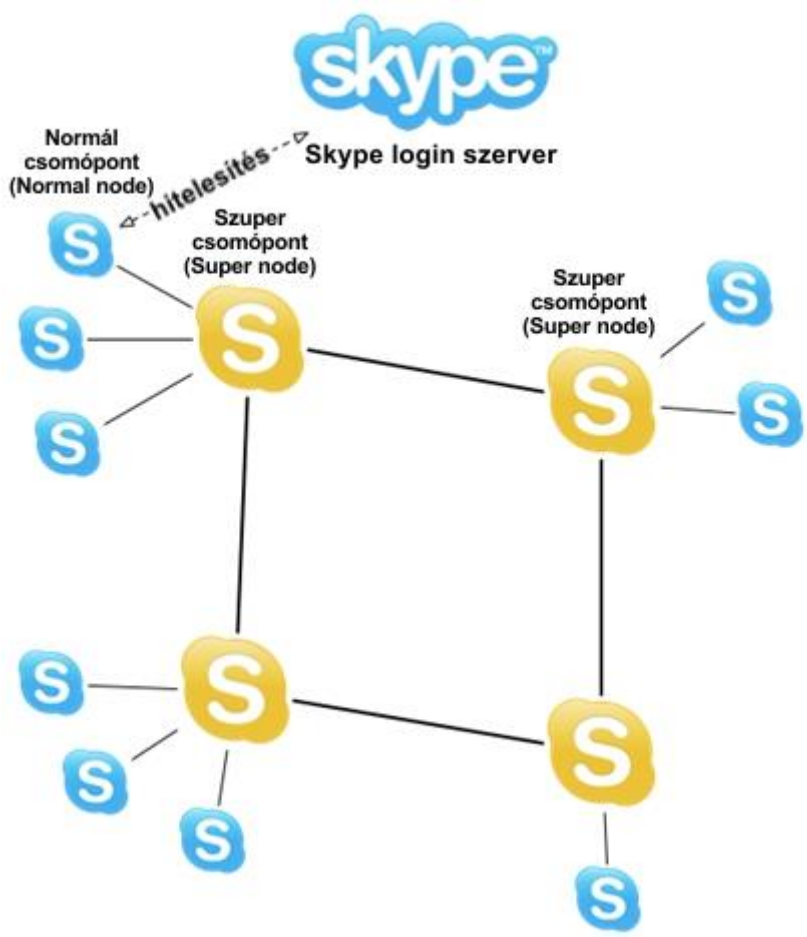
4.2.2. Nemzetközi példák I. - Skype, mint „állatorvosi ló”

A korábban leírtaknak megfelelően a Skype esetét különállóan, olyan példaként vizsgálom, amely alapján sok általános következtetést le lehet vonni.

A rendkívül népszerű Skype első béta verziója 2003 augusztusában jelent meg, ám 2013-ban már átlagban, percenkén összesen 1,4 millió percnyi összeköttetést létesítettek vele a felhasználói. [81] Ez kiválóan szemlélteti a felhasználói szokások változását, hiszen jól mutatja, hogy míg a hagyományosnak mondható kommunikációs formák és rendszerek (pl. telefónia) jelentősége a felhasználók – ezáltal a potenciális célszemélyi kör, így a törvényes ellenőrzést végző szolgálatok – számára csökken, addig az új rendszereké sokszor robbanásszerűen nő. [130] A Skype pedig szinte minden nemzetbiztonsági és bűnüldöző szerv prioritási listájának az élén áll.

Röviden érdemes áttekinteni, hogy mi is okozza a problémát ennek a rendszernek az ellenőrzése kapcsán. Az egyik maga a rendszer felépítése. Ennek sematikus elrendezése a 11. ábrán látható.

DOI azonosító: 10.17625/NKE.2015.021



11. ábra. Skype topológiája.[87]

A működés leegyszerűsítve úgy történik, hogy a korábban már regisztrált felhasználó (a regisztrációhoz csupán egy érvényes email 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 áll egymással – vagy közvetetten – a kommunikáló felek Supernode-okon keresztül állnak összeköttetésben egymással – zajlik, de nem folyik át egy központon. [185] [186] 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. [187] Azaz, ha sikerül is „útközben” elfogni a teljes kommunikációt, annak tényleges tartalmához csak a használt titkosítás visszafejtése után lehetséges hozzáférni. Az ehhez szükséges

[87] Szerkesztette a szerző. Forrás: [292]

DOI azonosító: 10.17625/NKE.2015.021

számítási kapacitás és időigény meglehetősen nagy, a tömeges méretű ellenőrzést ez meglehetősen megnehezíti, vagy inkább teljes mértékben kizárja.

További problémát okoz a korábban már említett regisztráció, amelyhez csupán egy érvényes email címre van szükség. Emiatt a törvényes ellenőrzés feladatrendszerébe beleértett – és hagyományos hírközlési szolgáltatók esetében hatékonyan alkalmazható – felhasználói/előfizetői adatok szolgáltatása [130] ebben az esetben nehézkesen és főleg hiányosan valósul meg.

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

- 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. [188] 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. [189]

A szaksajtóban már a felvásárlás bejelentésekor elindultak a találgatások, hogy miért is kell, kellhet a Skype a nagyhírű redmondi cégnek. [190] [191] Az ott felvetetteken kívül nem kell túl nagy fantázia ahhoz, hogy az addig a titkosítás és a peer-to-peer[88] (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, akinek a 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

[88] P2P peer-to-peer kapcsolat lényege, hogy az informatikai hálózatvégpontjai kitüntetett központi csomópont nélkül, közvetlenül egymással kommunikálnak.

DOI azonosító: 10.17625/NKE.2015.021

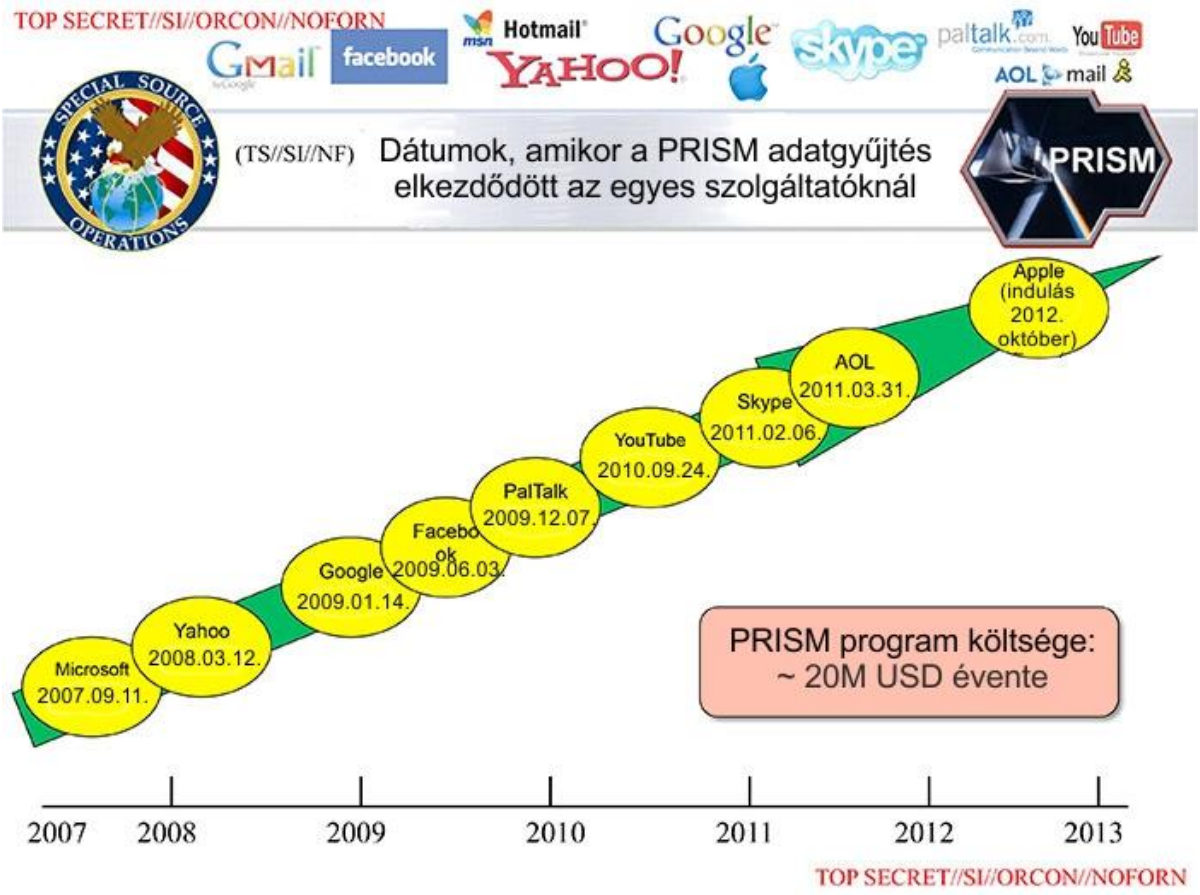
kiépíteni. A változás az addig rotációban a felhasználók között kiosztott un. Supernode-oknál indult el. Egyrészt számukat jelentősen csökkentették (több mint 48 ezerről kb. 10 ezerre), másrészt az új Supernode-ok már nem lehetnek felhasználók gépei, hanem csak és kizárólag a Microsoft/Skype központjába telepített eszközök. [192] 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. [193] [194] [195]

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 (pl. beszélgetések, video-chat, fényképek stb.) (12. ábra) – szolgáltatónként változó formában és mélységben – fér hozzá az NSA (National Security Agency – Nemzetbiztonsági Ügynökség), az FBI (Federal Bureau of Investigation – Szövetségi Nyomozó Iroda) és az NSA-n keresztül az angol GCHQ (UK Government Communications Headquarters – Kormányzati Kommunikációs Központ). [196] A Skype-ot a kiszivárgott információk szerint 2011. 02. 06-án kapcsolták be a programba. (13. ábra.)

12. ábra. A Prism programban szereplő szolgáltatók és az általuk – különböző mértékben – biztosított adatok.[89]

[89] Forrás: [240]

DOI azonosító: 10.17625/NKE.2015.021



13. ábra. A Prism programban résztvevő szolgáltatók és csatlakozásuk időpontja.[90]

- Oroszország és a Skype:

Oroszország is a szolgáltatókkal történő együttműködést választotta, csak annak egy másik változatát. Az FSZB (Федеральная служба безопасности Российской Федерации (angolul Federal Security Service of the Russian Federation) – Orosz Szövetségi Biztonsági Szolgálat) 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 ellenőrizhetetlen azok tartalma. Ez pedig biztonsági kockázatot jelent. [197] 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. [198] [199] A lehallgatás, sőt a felhasználók pontos tartózkodási helyének meghatározási képességét orosz lapértesülésre hivatkozva a szaksajtó ma már tényként kezeli. [200]

[90] Forrás: [240]

DOI azonosító: 10.17625/NKE.2015.021

- 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 internet szolgáltató cég) és a Microsoft által alapított vegyesvállalat adott ki TOM-Skype néven. A szoftver feltörése után bizonyítottá vált, hogy kínai hatóságok ezen keresztül ellenőrzik a kommunikációt, az azonnali üzenetküldések esetében több ezer szavas szótár alapú kulcsszavas keresést használnak, és találat esetén rögzítik a teljes chatelést, vagy adott esetben blokkolják a forgalmat. [201]

- 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 hírközlési hatóság, az ARCEP[91] 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 utolsó sorban – az arra feljogosított szervek számára biztosítania kell a törvényes ellenőrzést is. [202] [203]

4.2.3. Nemzetközi példák II. - más példák

Természetesen nem csak a Skype az, amit a hatóságok ellenőrizni kívánnak, és természetesen a fent említett módszerekkel nem csak a Skype, hanem más alkalmazásszolgáltatók rendszerein küldött és tárolt információk is ellenőrizhetők. A következő példákban is többnyire megjelenik a Skype ellenőrzése, de e mellett a más rendszerekből származó információk megszerzése a korábbiaknál sokkal hangsúlyosabban jelenik meg, így ezeket célszerűnek tartom külön csoportban vizsgálni. Már csak azért is érdemes így tenni, mert a következő példák jól mutatatják, 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, használhat.

- 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.

[91] 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

DOI azonosító: 10.17625/NKE.2015.021

A módszer törvénybe iktatása, ezáltal a használat kereteinek kialakítása már régóta szerepelt a német parlament napirendjén. [204] Többszöri elutasítást [205] [206] követően a szövetségi alkotmánybíróság végül úgy foglalt állást, hogy a módszer használható, de szigorú keretek között, kizárólag kommunikáció ellenőrzésére – azaz gyakorlatilag az internetes telefon (pl. Skype) lehallgatására. Egy német hackercsoport a Chaos Computer Club (CCC) azonban analizálta a német hatóságok által használt, a szintén német DigiTask által gyártott „maleware"-t, és megállapította, hogy annak képességei messze túlmutatnak a fent említett, szövetségi bíróság által megszabott kereteken. [207] [208]

Ezt követően a német hatóságok egy saját eszköz kifejlesztése mellet döntöttek, amelyet a BKA (Bundeskriminalamt – Szövetségi Bűnügyi Hivatal) berkein belül felállítandó un. 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 un. „FinFisher/FinSpy IT intrusion software kit"-et használják. [209] [210]

A kémprogramok használata nem csak 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, [211] Franciaország, [212] Ausztria, [213] Hollandia [214] és természetesen az USA [215] [216] és az Egyesült Királyság [217] vonatkozásában is.

Az online házkutatásra alkalmas eszközök, azaz kémprogramok természetesen jóval több információt tudnak biztosítani a célszemélyek számítógépéről (pl. tárolt fájlok), a számítógép technikai eszközein keresztül a célszemély tevékenységéről (pl. webkamera képek), mint amit 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 [218] és a fent említett német Eleman/Gamma Group terméke is. [219]

DOI azonosító: 10.17625/NKE.2015.021

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, akkor 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. [220]

- Egyesült Királyság (UK) és a mély csomagelemzés:

Egy másik módszer a törvényes ellenőrzést végzők kezében az un. mély csomagelemzés (DPI)[92] módszere. Ennek lényege, hogy adott helyen átfolyó adatforgalom minden csomagjának a tartalmát vizsgálat alá veszik. Ezt a technológiát használják fel például a behatolás-érzékelő és –védelmi rendszerek, (IDS/IPS)[93] [221] [222] de internetszolgáltatók is előszeretettel alkalmazzák bizonyos – általuk károsnak vélt vagy tartott tartalmak, forgalmak (pl. VoIP,[94] peer-to-peer) – blokkolására. [223] Ugyanakkor ez a technológia a törvényes ellenőrzést végző szolgálatok számára is lehetőséget teremt, hogy információhoz jussanak. [222] [224] 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 (pl. HTTPS Everywhere). [222]

E korlát ellenére az angol GCHQ ezt a módszert használja „TEMPORA" nevű, a „PRISM"-hez 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 – a kinyert tartalmat és a kísérő un. metaadatokat egyaránt. [225] [226] Az NSA hasonló, „Upstream" fedőnevű tevékenységét a 14. ábra szemlélteti, amelyből jól látszik, hogy a Prism csak egy része az USA lehallgató rendszerének.

[92] DPI: Deep Packet Inspection mély csomag elemzés
[93] IDS/IPS: Intrusion Detection System/ Intrusion Prevention Systems behatolás-érzékelő és –védelmi rendszerek
[94] VoIP: Voice over IP Internet Protokoll alapú hangátvitel

DOI azonosító: 10.17625/NKE.2015.021

14. ábra. Az Upstream és a Prism program viszonya, felhasználhatósága.[95]

- Németország és a felhő alapú rendszerek titkosításainak törése:

Németországban az online házkutatás (vagy inkább a kémprogramok) használata mellett felmerült a felhő alapú 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 a BfV (Bundesamt für Verfassungsschutz – Alkotmányvédelmi Hivatal) által működtetett SFZ TK (Strategie- und Forschungszentrum Telekommunikation – Távközlési Stratégiai és Kutatóközpont) nevű intézet azt a feladatot kapta az illetékes szervektől, hogy vizsgálja meg a felhő alapú rendszereknél használt titkosításokat valamint azt, hogy azok megfejtésén keresztül hogyan lehet hozzáférni a felhasználói adatokhoz, fájlokhoz. [227]

- 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

[95] Forrás: [240]

DOI azonosító: 10.17625/NKE.2015.021

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. [228] 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, [229] ráadásul a törvényi szabályozás azt is garantálná, hogy minden szolgáltató bekényszeríthető legyen a rendszerbe. Ugyanakkor az USA-ban a már létező jogszabályok (Protect America Act (2007), FISA (Foreign Intelligence Surveillance Act) Amendments Act (2008)) is kötelezettségeket rónak a magáncégekre a törvényes ellenőrzés tekintetében. [196]

4.2.4. A törvényes ellenőrzés technikai lehetőségei

Az általam hozott 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 dolgozatomban tehát elsősorban a technikai lehetőségek áttekintésére és bizonyos problémák felvetésére, valamint arra szolgált, hogy megteremtse az alapot az ellenőrzéshez felhasználható módszerek rendszerezésére, elemzésére. Ezen tapasztalatok megismerését követően lehet ugyanis az internet-technológiára épülő szolgáltatások hatékony ellenőrzésének kialakítása felé tett következő lépésként elvégezni a törvényes ellenőrzésre jelenleg rendelkezésre álló technikai eszközök és módszerek leírását, összehasonlítását azok előnyeinek, hátrányainak meghatározásával együtt. Ezen vizsgálatok elvégzése ugyanis szükséges és elengedhetetlen feltétele annak, hogy az arra felhatalmazott szolgálatok megtehessék a szükséges lépéseket az internet-technológiára épülő szolgáltatások ellenőrzésének hatékony kialakítása érdekében.

A fent említett módszereket azonban még ki kell egészíteni a közbeékelődéses támadás elvén alapuló un. közbeékelődéses ellenőrzéssel (MitM)[96], amire ugyan a fentiekben nincs példa, de ez is fontos eleme a törvényes ellenőrzést végző szervezetek módszertárának.

[96] A továbbiakban a közbeékelődéses ellenőrzés esetében is a közbeékelődéses támadásnál alkalmazott angol rövidítést, a „MitM”-et használom.

DOI azonosító: 10.17625/NKE.2015.021

A vizsgálat elvégzéséhez először is érdemes számba venni a törvényes ellenőrzéshez rendelkezésre álló technikai lehetőségeket, majd felállítani az ezek elemzéséhez 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 internet-technológiára épülő szolgáltatások törvényes ellenőrzésének hatékony kialakítása érdekében végrehajtandó feladatok is.

Mint ahogy a fejezet előző részében rámutattam, az arra felhatalmazott nemzetbiztonsági és rendvédelmi szerveknek jelenleg több technikai megoldás is a rendelkezésére áll ahhoz, hogy az internet-technológiára épülő szolgáltatásokat törvényes ellenőrzés alá vonják. Az összehasonlító elemzés elvégzése előtt azonban érdemesnek tartom összefoglalóan csoportosítani ezeket a rendelkezésre álló módszereket, megoldásokat, és összefoglalni azok főbb jellemzőit, tulajdonságait.

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

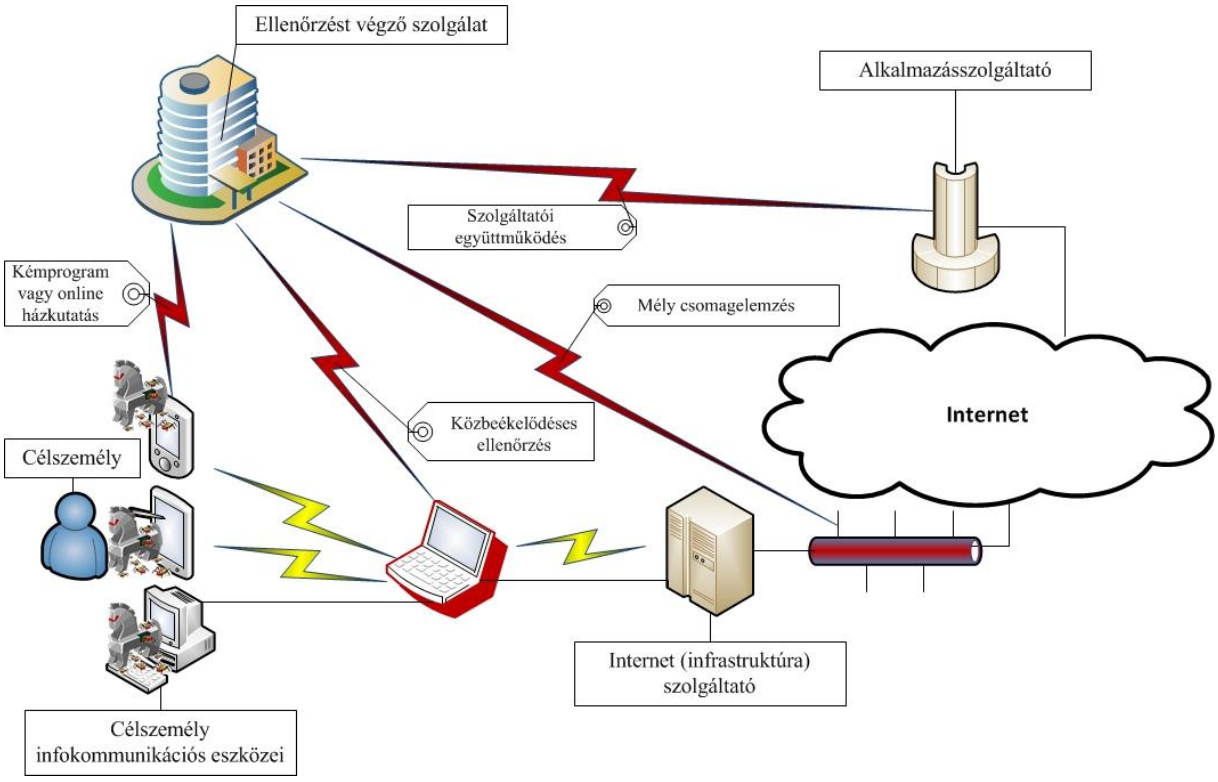
Az internet-technológiára épülő szolgáltatások törvényes ellenőrzésére alapvetően az alábbi négy módszert használhatják az arra felhatalmazott szolgálatok:

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 azokat. [230] [207]

A fenti módszerekre rendkívül jellemző az alkalmazásukkor használt adatszerző, elfogó eszközök – ebbe bele kell érteni a hardver és szoftver elemeket egyaránt – távolsága a célszemélytől. Ezt jól szemlélteti a 15. ábra.

DOI azonosító: 10.17625/NKE.2015.021



15. ábra. Az adatszerző, elenőrző eszközök távolsága a célszemélytől.[97]

a) Aktív ellenőrző eszköz:

Az aktív ellenőrző eszközök, vagy közismertebb, a fejezet első részében említett nevükön kémprogramok vagy online házkutatási eszközök esetében a célszemély infokommunikációs eszközére, eszközeire (pl. 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.

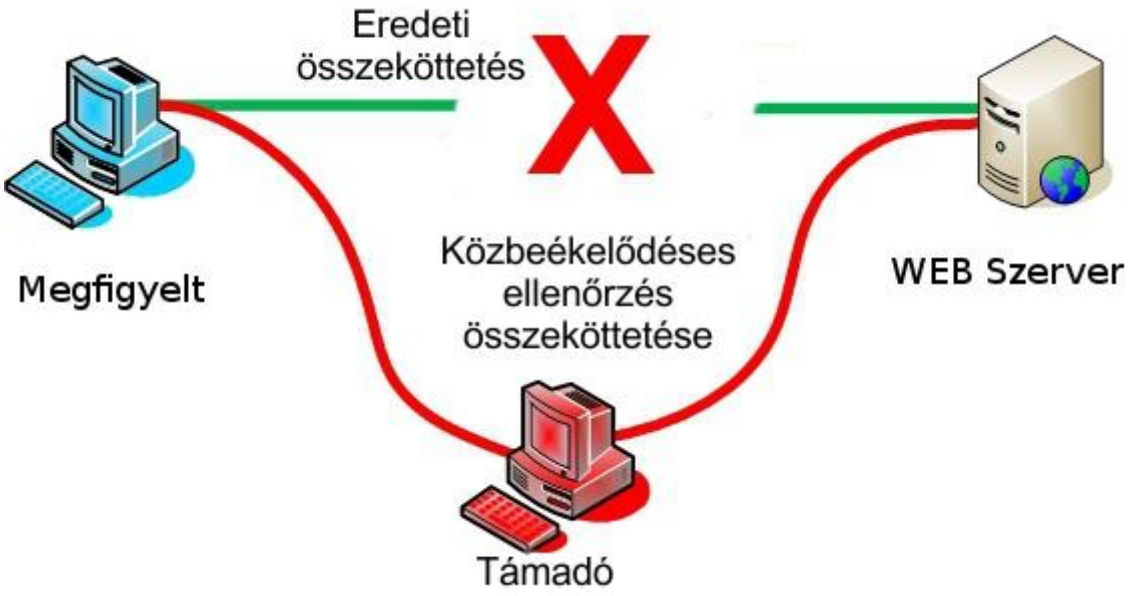
Az aktív ellenőrző eszköz bejuttatása a célszemély eszközére többféle módszerrel is lehetséges, hasonlóan a kiberbűnözők által használt módozatokhoz (pl. elektronikus levél csatolmányaként, fertőzött weboldal segítségével, 0. napi sebezhetőség kihasználásával stb.). A működés során ezek képesek az online 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. [208] [218] [219] [231] [232]

[97] Szerkesztette a szerző.

DOI azonosító: 10.17625/NKE.2015.021

b) 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 16. ábra.



16. ábra. Közbeékelődéses ellenőrzés.[98]

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 17. ábra.

[98] Szerkesztette a szerző. Forrás: [291]

DOI azonosító: 10.17625/NKE.2015.021

17. ábra. Példa HTTPS kommunikáció ellenőrzésére.[99]

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. [233] [234] [235] [236] [237] [238]

c) 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 attól. [239]

A mély csomagvizsgálatot leggyakrabban három esetben szokták alkalmazni. Az első eset a behatolást észlelő és behatolás-védelmi rendszerekben (IDS/IPS) történő felhasználás. Ezek a rendszerek a csomagok elemzésekor speciális bitmintákat (ismert támadókódokat) keresnek erre dedikált eszközök segítségével, majd a felismert, rosszindulatú kódot tartalmazó csomagokat kiszűrik. [221] A második a hírközlési, internetszolgáltatók rendszereiben történő alkalmazás. Itt az internet protokoll alapú hangátviteli szolgáltatások (VoIP) és a peer-to-peer kapcsolaton alapuló fájlcsere forgalmának blokkolására használják a technológiát. [223] A harmadik a törvényes ellenőrzés, ahol a csomagok vizsgálata alapján dönthető el, hogy az az ellenőrzést végző számára érdekes-e (pl. adott célszemélyhez tartozik-e az email), vagy sem. Itt a szűrés azonban nem a kiválasztott csomagok blokkolását szolgálja, hanem azoknak az ellenőrzést végző szolgálathoz (is) történő eljuttatását. [222] [224] [240] [225]

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 (pl. HTTPS Everywhere) jelentősen megnehezíthetik vagy akár el is lehetetlenítik az ellenőrzést. [241]

[99] Szerkesztette a szerző. Forrás: [236]

DOI azonosító: 10.17625/NKE.2015.021

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 (pl. 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. [240]

4.2.5. A törvényes ellenőrzési módszerek vizsgálati, összehasonlítási szempontjai

Az eddigiekből tehát látható, hogy az internet-technológiára épülő szolgáltatások törvényes ellenőrzésére több lehetőség, módszer is a felhatalmazott szolgálatok rendelkezésére áll. Ezek a módszerek azonban jelentősen – mondhatni minden paraméterükben – eltérnek egymástól, akár a technikai megvalósításukat, akár a hatékonyságukat, vagy akár a 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, hogy melyiket (melyikeket) kívánja megvasalósítani és munkájában felhasználni.

A módszer kiválasztásakor álláspontom szerint 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 – annak újszerűsége miatt – sem kizáró, sem engedélyező szabályozó sincs a jogrendben.

DOI azonosító: 10.17625/NKE.2015.021

- *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 teljes körűsége:*

Fontos tényező, hogy a célszemély online forgalmát teljes egészében vagy csak részlegesen biztosítja az adott módszer. Ennek a kérdésnek a 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 (pl. 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 fellépnek, felléphetnek, amelyekkel komolyan számolni kell az alkalmazást megelőzően. Ilyenek lehetnek pl. az együttműködőknek fizetendő díjak, a betanítás vagy éppen speciális ismeretekkel rendelkező (pl. 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, férhet még hozzá. Ez ugyanis nagymértékben növelheti a

DOI azonosító: 10.17625/NKE.2015.021

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 (pl. szolgáltató szakemberei) vizsgáljuk.)

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

4.2.6. A törvényes ellenőrzés módszereinek vizsgálata

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

1. **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 (pl. webkamerával képkészítés) is kínál.
- *Online kommunikációhoz való hozzáférés teljes körűsége:* nem ad teljes körű hozzáférést, hiszen csak 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 un. 0. napi sebezhetőségek költségesek.

DOI azonosító: 10.17625/NKE.2015.021

- *Egyéb költségek:* magas, a módszer alkalmazásához speciális (hacker) tudással rendelkező szakemberek szükségesek.
- *Célszemélyek adataihoz harmadik fél hozzáférése:* ennek lehetősége minimális.

2. 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 teljes körűsége:* nem ad teljes körű hozzáférést, hiszen csak azon az eszközön bonyolított kommunikációt képes elfogni, amelyik forgalma „átfolyik” az ellenőrző (17. 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.

3. 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.

DOI azonosító: 10.17625/NKE.2015.021

- *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 teljes körűsége:* 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 (pl. infrastruktúraszolgáltató beruházásai) a helyi jogszabályoknak megfelelően esetleg fizetni kell.
- *Célszemélyek adataihoz harmadik fél hozzáférése:* ennek lehetősége minimális.

4. 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 hajlandóak 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 teljes körűsége:* az alkalmazásszolgáltatón keresztül lebonyolított kommunikációhoz teljes körű hozzáférést ad.

DOI azonosító: 10.17625/NKE.2015.021

- *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 plusz eszközt.
- *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 (pl. célszemély adatai) – általában – külföldi szolgáltató hazai biztonsági ellenőrzésen át nem esett emberei férhetnek hozzá a kérő szerv szemszögéből kontrollálatlanul.

Annak érdekében, hogy az arra felhatalmazott szervek számára az internet-technológiára épülő szolgáltatások törvényes ellenőrzésére jelenleg rendelkezésre álló módszereket össze tudjuk hasonlítani, célszerű azok előnyeit, hátrányit is összefoglalni. Ezt tartalmazza a következő táblázat.

DOI azonosító: 10.17625/NKE.2015.021

MÓDSZER	ELŐNYÖK	HÁTRÁNYOK
aktív ellenőrző eszköz	• nem csak 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 (pl. vírusirtó, tűzfal) • működése azonnali utasítással nem megszakítható • alapos előkészületek ellenére a képességet egy egyszerű (pl.: vírusellenőrző) 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 (pl. 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

DOI azonosító: 10.17625/NKE.2015.021

MÓDSZER	ELŐNYÖK	HÁTRÁNYOK
mély csomagvizsgálat (DPI)	• tömeges – egyszerre több célszemély forgalma is ellenőrizhető • teljesen passzív • tartalom alapú 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 • 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 • teljes információkör elérhető, a használt eszközöktől, interneteléréstől függetlenül • nem csak az éppen folyó forgalmat, hanem a szolgáltatónál tárolt minden adatot (pl. 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 szolgáltató is megismeri – titoktartási, konspirációs gondot okozhat • több szolgáltatót használó célszemélyeknél mindegyikkel együtt kell működni

12. táblázat. Az internet-technológiára épülő szolgáltatások törvényes ellenőrzésére jelenleg rendelkezésre álló módszerek előnyei, hátrányai.[100]

Ahogy azt bemutattam, az internet-technológiára épülő szolgáltatások, ezen belül pedig kiemelten a PC/SaaS felhő alapú 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 véleményem szerint 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

[100] Szerkesztette a szerző.

DOI azonosító: 10.17625/NKE.2015.021

szolgáltatáshoz kapcsolódó teljes információkör elérhető az adott szolgálat számára, függetlenül a célszemély(ek) által használt eszközöktől és interneteléréstől. Ez pedig az egyik leghatékonyabb és legköltség-takarékosabb ellenőrzési formává teszi.

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

A törvényes ellenőrzés hatékonyságának növelése érdekében az új Európai Uniós irányelvek, valamint a hazai jogi szabályozás kialakításához mindenképpen definiálni kell az alkalmazásszolgáltató fogalmát. Véleményem szerint ezt, a korábban általam már felvázolt infrastruktúra-, alkalmazás-, és tartalomszolgáltatói modell szerint érdemes megtenni, a másik két szolgáltató meghatározásával egyetemben. Ez ugyanis egyrészt lehetőséget biztosít a többi általam elemzett vagy bármilyen más, akár teljesen új módszer törvényi szabályozásának kialakításában, másrészt teljes körűen 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, [178] útvonaltervek stb.

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

A fejezet előző részeiben bemutattam az internet és az azt felhasználó alkalmazások fejlődésével ugrásszerűen változó, bővülő kommunikációs formák, lehetőségek hatásait, elemeztem az elektronikus úton folytatott kommunikáció és a hírközlés viszonyát, e kettő változásait, valamint az internet-technológiára épülő szolgáltatások, azon belül pedig a PC/SaaS felhő alapú rendszerek törvényes ellenőrzése kapcsán felmerült problémákat. Megállapítottam, 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 szolgáltatató biztosítja. Ennek kapcsán felállítottam egy új, specializált infrastruktúra-, alkalmazás-, és tartalomszolgáltatói modellt, amely véleményem szerint teljes körűen leírja a jelenlegi struktúrát és az érintett szereplőket.

DOI azonosító: 10.17625/NKE.2015.021

Az internet-technológiára épülő szolgáltatások, azon belül pedig a PC/SaaS felhő alapú rendszerek természetesen nem csak kommunikációt, hanem sok egyéb online szolgáltatást is biztosítanak a felhasználók számára. Igénybe vehetünk banki szolgáltatásokat, [242] fizethetünk web boltokban, [243] játszhatunk, [244] szerkeszthetjük dokumentumainkat, [245] képeinket, [246] tárolhatjuk, megoszthatjuk adatainkat, [149] készíthetünk útvonaltervet, [247] és még nagyon hosszan lehetne folytatni a felsorolást. Ugyanakkor a korábban említett hármas tagozódásba (infrastruktúra-, alkalmazás-, és tartalomszolgáltatók) nem csak az elektronikus úton folytatott kommunikációt lehetővé tevő rendszerek, hanem az itt említettek is beleérthetők, beleértendők. Akárcsak a többi internet-technológiára épülő szolgáltatás.

Fel kell azonban tenni a kérdést, hogy mit is takarnak az infrastruktúra-, alkalmazás-, és tartalomszolgáltató fogalmak. Ezekre ugyanis számos megfogalmazás létezik, azok 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 ilyen fogalmak a jelenlegi magyar jogi szabályozásokban nem találhatóak. Ez pedig megnehezíti a hatékony törvényes ellenőrzés végrehajtását.

Az internet-technológiára épülő szolgáltatások, azon belül pedig a PC/SaaS felhő alapú rendszerek törvényes ellenőrzésének igénye azok felhasználásával arányosan nő. Azonban ennek kapcsán – mint, ahogy a fejezet előző részében bemutattam – az erre feljogosított szervezetek számos jogi és technikai problémával küzdenek. Ezek közül az egyik kiemelkedő a fent említett szolgáltatói definíciók hiánya.

4.3.1. Az elektronikus hírközlésről szóló törvény módosításának szükségessége

Az infrastruktúra-, alkalmazás- és tartalomszolgáltatók definícióinak kialakítása előtt célszerűnek tartom értékelni, hogy a jelenleg érvényes jogszabályok megfelelő keretet biztosítanak-e az említett szolgáltatók, szolgáltatások törvényes ellenőrzéséhez.

Jelenleg a hírközlés törvényes ellenőrzését a hatályos törvényeink két, párhuzamosan alkalmazott szabályrendszer szerint teszi lehetővé. Ezek közül az egyik a titkos információgyűjtést és titkos adatszerzést szabályozó ágazati normák, mint például a nemzetbiztonsági szolgálatokról szóló 1995. évi CXXV. (továbbiakban: Nbtv.), [248] a büntetőeljárásról szóló 1998. évi XIX. (Be.), [249] a Rendőrségről szóló 1994. évi XXXIV. (Rtv.), [250] az ügyészségről szóló 2011. évi CLXIII. (Ütv.), [251] valamint a Nemzeti Adó-

DOI azonosító: 10.17625/NKE.2015.021

és Vámhivatalról szóló 2010. évi CXXII. (NAVtv.) [252] törvények. A másik az elektronikus hírközlésről szóló 2003. évi C. törvény, [174] 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. [253]

De nem csak 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 [130] 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, tehát a törvény megalkotásakor még nem volt elérhető, míg a Facebook, amely 2004. február 4-én debütált, tehát a törvény hatályban lépésekor (2004. január 1-én) még el sem indult! Márpedig ezeket a változásokat a törvény nem követte.

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

DOI azonosító: 10.17625/NKE.2015.021

megjelenő kevesebb szereplő miatt könnyebb az esetleges későbbi változtatásokat átvezetni, harmadrészt, azokat a szolgáltatókat (tipikusan alkalmazásszolgáltatók) 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 már elkészült egy hasonló megfontolásokon alapuló törvény. [254]

A javasolt két új törvénnyel kapcsolatban viszont kiemelendőnek tartom, hogy álláspontom szerint célszerű mindkettőben ugyanazokat a meghatározásokat használni és a meglévő, bizonyos területeket most is lefedő hírközlési szolgáltató mellett megjeleníteni és bevezetni az infrastruktúra-, alkalmazás- és tartalomszolgáltatók fogalmát is.

4.3.2. 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 (pl. 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 (továbbiakban: 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, szélessávú, 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.” [255]

DOI azonosító: 10.17625/NKE.2015.021

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 [256] a sajtószabadságról és a médiatartalmak alapvető szabályairól szóló 2010. évi CIV. törvény (a továbbiakban: Smtv.), [257] valamint a médiaszolgáltatásokról és a tömegkommunikációról szóló 2010. évi CLXXXV. törvény (a továbbiakban: Mttv.) [258] 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, így a dolgozatomban ezzel nem foglalkozom.)

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 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. Véleményem szerint ugyanis van 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 tartalom kerül közlésre, annak tartalmát a fogyasztó nem tudja befolyásolni.

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

DOI azonosító: 10.17625/NKE.2015.021

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 videó üzeneteket 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-t nevezi meg. [259]

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*”. [260] A British & World English verzióban ugyanez a meghatározást közlik, de már leszűkítve szervezetre, a személy megjelölése nélkül. [261]

Az előzőeknél bővebben leírt, ezáltal szűkebben, pontosabban értelmezhető definíciókat is közreadtak. A Gartner meghatározása szerint a tartalomszolgáltató „*egy vállalkozás információ-alapú (értsd: tartalom-alapú) termékekkel, amely tartalmazza az információelérési és -kezelési szolgáltatásokat is*”. [262]

Hasonló meghatározást ad közre a Dictionary.com is, azzal a különbséggel, hogy abban személy vagy csoport, valamint honlapok vagy elektronikus média szerepel. [263]

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. [264]

A TheFreeDictionary 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 szoftver alapú termékek számára*”. Megjegyzendő, hogy a tartalom eléréséhez szükséges szoftver biztosítását a tartalomszolgáltató számára lehetőségként, de nem szükségszerűségként említik meg. [265]

DOI azonosító: 10.17625/NKE.2015.021

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

Saját meghatározás

A magyar és a külföldi definíciókat áttekintve, valamint figyelembe véve a technológiai fejlődés irányait, a tartalomszolgáltató törvényes ellenőrzés szempontú meghatározáshoz álláspontom szerint az alábbiakat kell figyelembe venni:

- bármilyen információt (textuális, numerikus, képi, hangos, multimediális) közzé tehet,
- 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 azok akár nyomtatottak (pl. újság, könyv stb.), akár elektronikusak (pl. CD, DVD, Blue-ray Disc stb.) – a téma szempontjából nem relevánsak.]

A fentiek alapján, véleményem szerint 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,

DOI azonosító: 10.17625/NKE.2015.021

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.

4.3.3. 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 pl. nyomtatott sajtó, analóg vagy digitális tv műsorszórás, stb. – több évtizede végeznek ilyen tevékenységet, így a tevékenységi körüket leíró meghatározások kialakultak, tehát az IP alapú szolgáltatásokkal történő megfeleltetése is viszonylag egyszerűen elvégezhető volt. Ugyanez nem mondható el az alkalmazás-, és infrastruktúraszolgáltatókról, 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 járom körbe.

Az alkalmazásszolgáltató elnevezést nem csak 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 cikk [178] is bemutatta – szintén érdekesek lehetnek a törvényes ellenőrzést végző szolgálatok számára. Meglátásom szerint, éppen ezért ez a törvényes ellenőrzés jogi eszközeinek átalakítása során is nagy jelentőséggel bír majd.

DOI azonosító: 10.17625/NKE.2015.021

Magyar meghatározások

Az „E-önkormányzati stratégiakészítési ajánlás kistérségek és önkormányzatok számára” című dokumentum v1.1 változatában a következőként definiálják az alkalmazásszolgáltatókat: *„Alkalmazásszolgáltató, ASP[101]: 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.”* [266]

A szakmai körökben is mérvadónak számító PC Fórum.hu oldal szótárában a következő meghatározást találjuk:

„Alkalmazás-szolgáltató: 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, web hosting tömeges SMS küldés.” [267]

A Humansoft oldalán található leírás az előzőeknél is szűkebb értelmezést tesz lehetővé, hiszen az alkalmazásszolgáltatókat a „szoftver, mint szolgáltatás” szolgáltatási modell szerint működő felhő alapú szolgáltatókkal teszi egyenlővé. Az általuk használt megfogalmazás szerint *„az ügyfél a szolgáltató szerverein futó programokat egy kommunikációs csatornán keresztül bérleti díj fejében használja”*. [268]

A fentiek mellett mindenképpen figyelembe kell venni az elektronikus kereskedelmi szolgáltatások, valamint az információs társadalommal összefüggő szolgáltatások egyes kérdéseiről szóló 2001. évi CVIII. törvény [269] meghatározásait. Ez a törvény hasonló problémákat vet fel, mint amelyek az Eht. kapcsán már megfogalmaztam, definícióival azonban nagyban segítheti a dolgozat célkitűzésében megfogalmazott új meghatározás kialakítását. A törvény többek között azt is kimondja, hogy előírásait a Magyarország területére irányuló információs társadalommal összefüggő szolgáltatások esetében szintén alkalmazni kell. 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”*. Ez a megfogalmazás az alkalmazásszolgáltatókra, de akár a tartalomszolgáltatókra is értelmezhető,

[101] ASP: Application Service Provider, magyarul alkalmazásszolgáltató

DOI azonosító: 10.17625/NKE.2015.021

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”*. Ezek – megfelelő kiegészítésekkel – felhasználhatóak az alkalmazás-, és tartalomszolgáltatók definíciójának kialakításához is. A Magyarországra irányuló szolgáltatás alatt a törvény értelmező rendelkezései között a következőket találjuk: *„minden olyan szolgáltatás, melyről a használt nyelv, a pénznem és egyéb körülmények alapján valószínűsíthető, hogy magyarországi igénybe vevők számára kívánják elérhetővé tenni”*. Ez a megfogalmazás álláspontom szerint 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. Ám egyrészt ilyen szolgáltatásokat használnak Magyarországról is, másrészt a globális piac, a szabad valutahasználat, az angol nyelv használatának terjedése stb. okán véleményem szerint nem is szükséges előfeltételezésekkel élni.

A fenti definíciók ugyan nagyban segítik egy megfelelő meghatározás kialakítását, de nem adnak teljesen elfogadható definíciót. Egyrészt, adott esetben nem teljes mértékben fedik le a törvényes ellenőrzésbe bevonni célszerű szolgáltatásokat, szolgáltatókat, másrészt bizonyos, a törvényes 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 felhasználás alapú fizetési modell szerint”*. [270] Meghatározásuk szerint az ASP piac olyan szolgáltatók keverékéből áll, mint a hálózat és telekommunikációs szolgáltatók, független szoftverforgalmazók, vagy olyan egyéb szolgáltatók, akik ICT kiszervezéssel vagy web üzemeltetéssel 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”*. Példának pedig a Google-t és a Yahoo-t említik. [271]

A Techterms.com-on található meghatározás szerint az alkalmazásszolgáltató *„egy olyan szervezet vagy vállalat, amely szoftveres alkalmazásokat biztosít a felhasználóknak az interneten”*. A definíció további részében az alkalmazásszolgáltatókat itt is egyenlővé teszik a

DOI azonosító: 10.17625/NKE.2015.021

„szoftver, mint szolgáltatás” szolgáltatási modell szerint működő felhő alapú szolgáltatókkal. [272]

A Bussinessdictionary.com leírása alapján az alkalmazásszolgáltató *„egy cég, amely interneten keresztüli elérésű számítógépes szoftverekhez árul hozzáférést”*. 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 használat alapú díjat fizet. [273]

Az előzőhöz hasonlóan definiálja a Dictionary.com is az alkalmazásszolgáltatót, hiszen szerintük az *„egy cég, amely egyéni vagy üzleti felhasználóknak nyújt specializált szoftverekhez és más számítástechnikához kapcsolódó szolgáltatáshoz elérhetőséget az interneten keresztül”*. [274]

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. [275]

Álláspontom szerint a törvényes ellenőrzés szempontjából a külföldi meghatározások sem adnak teljes körűen elfogadható definíciókat, amelynek okai megegyeznek a magyar meghatározások kapcsán leírtakkal. Ugyanakkor célszerűnek tartom még megvizsgálni az ún. „Over-the-Top” (OTT)[102] szolgáltatókra, szolgáltatásokra adott megfogalmazásokat is.

„Over-the-Top” szolgáltató meghatározások

Véleményem szerint a törvényes ellenőrzés szempontjainak megfelelő, általános és a szolgáltatást nyújtókat pontosan leíró meghatározások kialakításakor azért célszerű az ún. Over-the-Top szolgáltatásokat, valamint az azokat biztosító szolgáltatókra adott definíciókat is figyelembe kell 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”*. 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

[102] OTT: Over-the-Top az Interneten, mint mások által biztosított közegen nyújtott szolgáltatások, tartalmak, amelyekre az internetszolgáltatónak nincs befolyása.

DOI azonosító: 10.17625/NKE.2015.021

szolgáltatók és az OTT szolgáltatók között, hiszen az OTT szolgáltatók a hagyományos szolgáltatók piacából hasítanak ki részeket. [276]

A Pace.com szűkebb értelemben említi az OTT szolgáltatásokat, hiszen e fogalom alatt a dedikált és menedzselt saját IPTV[103] hálózat helyett az internetet, mint átviteli közeget használó tv, video és – talán egy kicsit kiterjesztő kitétellel – egyéb szolgáltatásokról beszél. Ugyanakkor lényeges elemként említi, hogy az OTT a fogyasztó internet hozzáférés-szolgáltatójától függetlenül, infrastruktúra-beruházások nélkül biztosítja szolgáltatásait. [277]

Az Imediaconnection.com szerint az OTT egy, a távközlési vagy több rendszert üzemeltető (pl. kábel tv, műholdas tv) szolgáltató nélkül biztosított hang-, video-, és adatszolgáltatás. Példának többek között az okostévék által közvetlenül elért YouTube-t említi. [278]

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 pl.: Skype, Gmail, az alkalmazásszolgáltatásokat, mint pl.: Facebook, LinkedIn, Twitter, valamint a tartalomszolgáltatásokat, mint pl.: Netfix, YouTube. Megállapítják, hogy az OTT szolgáltatók ráépülnek a fizikai infrastruktúrát üzemeltető internet szolgáltatókra, 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. [279]

Saját meghatározás

A fenti definíciókat áttekintve, valamint figyelembe véve az technológiai fejlődés irányait, az alkalmazásszolgáltató törvényes ellenőrzés szempontú meghatározáshoz 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 ide értve a közösségi oldalakat, a kommunikációs, pénzügyi, geo-információs, szórakozási, valamint tárhelyet biztosító szolgáltatásokat,
- az elérést specifikus szoftveren vagy webes felületen keresztül biztosítja,

[103] IPTV: Internet Protocol Television Internet Protokoll segítségével általában szélessávú interneten keresztül nyújtott digitális televíziós műsorszolgáltatás

DOI azonosító: 10.17625/NKE.2015.021

- a kínált szolgáltatás(ok) online, elektronikus úton, elsősorban az interneten keresztül hozzáférhető(ek),
- 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(ek), legyen 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 azok egy csoportja),
- amely a hozzáférés során nem kell, hogy egyértelműen azonosítható legyen,

Véleményem szerint 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

DOI azonosító: 10.17625/NKE.2015.021

ide értve a közösségi oldalakat, a kommunikációs, pénzügyi, geo-információs, szórakozási, valamint tárhelyet biztosító szolgáltatásokat. Alkalmazásszolgáltatás esetében az információáramlás többirányú, a felhasználó aktív, tevékeny résztvevő, az információk adattartalmára befolyással rendelkezik.

4.3.4. Infrastruktúraszolgáltatók fogalmi meghatározása

Az infrastruktúraszolgáltató meghatározására jelenleg nem igazán találni a fejezetben vizsgált értelemben vett, a törvényes ellenőrzés szempontjából is megfelelő definíciókat. Ennek az az oka, hogy az infrastruktúraszolgáltató alatt ma elsősorban a felhő alapú rendszerek osztályozásánál a szolgáltatási modellek szerinti csoportosításban szereplő infrastruktúra, mint szolgáltatást (IaaS) biztosító szolgáltatókat írják le ezen címke alatt. Ebbe a modellbe pedig azok a szolgáltatók tartoznak, amelyek a felhasználó számára olyan számítási, tárolási, hálózati és egyéb alapvető informatikai erőforrásokat biztosítanak, amelyre és amelyen 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 (pl. tűzfalak) kiválasztására. Márpedig ez jóval kevesebb tartalommal bír, mint a fejezet elején, valamint a „Felhő alapú rendszerek törvényes ellenőrzési problémái” című cikkben [130] bemutatott hármas tagozódásban szereplő infrastruktúraszolgáltató.

A dolgozat céljának eléréséhez 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 internet elérést biztosít”*. [280] 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-mail-ezési lehetőség biztosításával egészítették ki a megfogalmazást, valamint azzal, hogy a szolgáltatások havidíj ellenében vehetők igénybe. [281] 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(tv), DSL, optikai. Ilyenek például a Pcmag.com, az Investopedia.com, [282] vagy az About.com [283] meghatározásai. A Dictionary.com-on említett e-mail-ezési lehetőség mellett, az egyéb kapcsolódó szolgáltatásokra utalást is tartalmaznak egyes meghatározások, így például a Searchwindevelopment.techtarget.com oldalán fellelhető leírás is, amely példálózva weboldalak készítését és üzemeltetését említi. [284]

DOI azonosító: 10.17625/NKE.2015.021

Meglátásom szerint a fenti meghatározások sem felelnek meg teljesen a fejezet elején bemutatott hármas tagozódásban szereplő infrastruktúraszolgáltató 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 célszerűnek látom a jelenlegi hírközlési szolgáltató, és e mellett a hírközlő hálózat definícióját is áttekinteni. Ez az Eht. [174] szerint a következő:

„14. Elektronikus hírközlési szolgáltató: elektronikus hírközlő hálózat üzemeltetője, valamint elektronikus hírközlési szolgáltatást nyújtó természetes, illetőleg jogi személy.”

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.”

Szintén érdemesnek tartom figyelembe venni az elektronikus kereskedelmi szolgáltatások, valamint az információs társadalommal összefüggő szolgáltatások egyes kérdéseiről szóló törvény közvetítő szolgáltató 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);”.

DOI azonosító: 10.17625/NKE.2015.021

Ez a meghatározás szintén segíti a dolgozat céljának 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.

Saját meghatározás

A fenti definíciókat áttekintve, valamint figyelembe véve az technológiai fejlődés irányait, az infrastruktúraszolgáltató törvényes ellenőrzés szempontú meghatározáshoz véleményem szerint az alábbiakat kell figyelembe venni:

- elektronikus hírközlési, infokommunikációs hálózatot üzemeltet és/vagy internetelérést biztosít,
- több felhasználó számára,
- időben korlátozott vagy korlátlan módon,
- havi-, vagy használat alapú 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,[104]
- a szolgáltató lehet bármilyen természetes vagy jogi személy (cég, személy, vagy azok egy csoportja),
- amely a hozzáférés során nem kell, hogy egyértelműen azonosítható legyen.[105]

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

Infrastruktúraszolgáltató:

Online infrastruktúraszolgáltató 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 használat alapú ellenszolgáltatás fejében vagy ingyenes formában. Online infrastruktúraszolgáltatónak 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 infrastruktúraszolgáltatók közé értjük azokat a szolgáltatókat is, akik más

[104] például egy mesterséges holdon keresztül nyújtott Internet elérés lehet olyan, amelynél szolgáltató nincs Magyarországon letelepedve, sőt bejelentve sem.

[105] például egy nyílt WiFi szolgáltatás esetén nem mindig azonosítható a szolgáltató egyértelműen.

DOI azonosító: 10.17625/NKE.2015.021

szolgáltatótól vásárolt internetelériéshez biztosítanak harmadik félnek (feleknek) hozzáférést.

4.3.5. Vegyes szolgáltatások értelmezése

Természetesen előfordulhat, hogy valamely cég vegyes szolgáltatást nyújt. Ma például egy internetszolgáltató internetelérést és például e-mail-ezési lehetőséget is biztosíthat, vagy egy online tartalomszolgáltatással foglalkozó cégnél, például egy internetes újságnál pedig lehetőséget biztosíthatnak kommentek írására, ezen keresztül pedig kommunikáció megvalósítására is. Ezekben az esetek is kezelhetőek a fejezet elején, valamint a „Felhő alapú rendszerek törvényes ellenőrzési problémái" című cikkben [130] bemutatott hármas tagozódásban szereplő tartalom-, alkalmazás-, és infrastruktúraszolgáltató modellel.

A törvényes ellenőrzés kapcsán a három szolgáltatónak eltérő kötelezettségei származnak. Míg a tartalomszolgáltatónak alig, az infrastruktúra szolgáltatónak korlátozott (elsősorban előfizetői adatszolgáltatási), addig az alkalmazásszolgáltatóknak – a hagyományos hírközlési szolgáltatóhoz 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, chat, útvonal tervezési adatok stb.) információ-, és adatelérést kell biztosítania az arra felhatalmazott szervezetek számára.

Amennyiben egy cég vegyes szolgáltatást nyújt, akkor álláspontom szerint 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 venni. Ugyanez igaz az online újság esetében is, ahol a fórumok, kommentek esetén már az alkalmazásszolgáltatókra kirótt kötelezettségeket kell teljesíteniük.

Érdemesnek tartom megvizsgálni a mai hírközlési szolgáltatók helyzetét is. Esetükben a problémakör két részre bontható. Amennyiben internet-szolgáltatást is végeznek, akkor a fent leírtak alapján lehet eljárni. Amennyiben a hagyományos – például vezetékes telefon – szolgáltatásokat nézzük, akkor ott 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.

Meglátásom szerint ezek alapján megállapítható, hogy a tartalom-, alkalmazás-, és infrastruktúraszolgáltató modellbe minden szolgáltató egyértelműen besorolható, így

DOI azonosító: 10.17625/NKE.2015.021

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 célszerűnek tartom 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 és normarendszer szerint történik.

Ez utóbbi azonban például az alkalmazásszolgáltatókról nem mondható el, mint, ahogy a fejezet elején, valamint a „Felhő alapú rendszerek törvényes ellenőrzési problémái" és a Felhő alapú rendszerek törvényes ellenőrzési módszerei vizsgálata I.-II." című cikkekben [130] [167] [168] bemutattam, ezért álláspontom szerint a tartalom-, alkalmazás-, és infrastruktúraszolgáltató modell mielőbbi bevezetése rendkívül fontos.

4.3.6. A törvényes ellenőrzés kialakítását elősegítő lehetőségek

Fontos megjegyezni, hogy az infrastruktúraszolgáltatót 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. 06. 12-én érkeztetett T/264 számú, az egyes pénzügyi tárgyú törvények módosításáról szóló javaslat, [285] amelyet „2014. évi XXXIII. törvény az egyes pénzügyi tárgyú törvények módosításáról" [254] címmel az Országgyűlés azóta már jóváhagyott és hatályba is léptetett, többek között kitér az általam említett szolgáltatások adóztatására is.

Ebben a dolgozat 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 igénybevevő nem adóalany letelepedett, letelepedés hiányában pedig, ahol lakóhelye vagy szokásos tartózkodási helye van:

a) telekommunikációs szolgáltatások;

DOI azonosító: 10.17625/NKE.2015.021

b) rádiós és audiovizuális médiaszolgáltatások;

c) elektronikus úton nyújtott szolgáltatások.

(2) E § alkalmazásában elektronikus úton nyújtott szolgáltatás különösen:

a) e1ektronikus 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, változás-bejelentésre, 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,

DOI azonosító: 10.17625/NKE.2015.021

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.…" [285]

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, 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 teremtenek az internet-technológiára épülő szolgáltatások, azon belül pedig a PC/SaaS rendszerek „bekényszerítésére" a magyar jogrendbe. Az adóztatás lehet az első lépés, de ezt kihasználva tovább lehet, sőt, kell vinni a szabályozási folyamatot a törvényes ellenőrzésre is. Ott is ki kell kényszeríteni a bejelentési és az együttműködési kötelezettséget, akárcsak az adóztatás esetén és ugyanúgy, mint ahogyan a törvényes ellenőrzés oldaláról nézve jelenleg a hagyományos hírközlési szolgáltatók esetében fennáll.

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 az alól kibújókat. Erre lehet példa az interneten nyújtott sportfogadások, szerencsejátékok esete. Itt a NAV[106] már blokkoltatja azokat az online fogadási szolgáltatást nyújtó oldalakat, amelyek nem tesznek eleget a magyar jogszabályokban megfogalmazottaknak. [286] Ugyanakkor meg kell jegyezni, hogy a szankcionálás kérdése az adózás esetében még nem kristályosodott ki. Ez ugyanilyen problémát vet fel a törvényes ellenőrzés kapcsán is.

Összegzés, következtetések

Bemutattam az internet és az azt kihasználó alkalmazások fejlődésével ugrásszerűen változó, bővülő kommunikációs formák, lehetőségek hatásait, majd ebből levezettem, hogy az itt

[106] NAV: Nemzeti Adó- és Vámhivatal

DOI azonosító: 10.17625/NKE.2015.021

jelentkező **technológiai konvergencia a törvényes ellenőrzés feladatainak konvergenciáját is indukálja**. Meglátásom szerint ez alapvető változásokat indít el ebben a feladatkörben is.

Rámutattam, hogy az elektronikus úton folytatott kommunikáció egy sokkal szélesebben értelmezhető fogalom, mint a hírközlés, ráadásul jobban le is fedi a jelenlegi technikai környezetet, lehetőségeket. **Rávilágítottam** arra is**, hogy a hagyományos hírközlési formák egyre inkább veszítenek jelentőségükből a felhasználók, így a törvényes ellenőrzést végzők számára is**. Ennek okaként a felhasználói szokások jelentős változását jelöltem meg, amelyet a generációk változása is alapvetően befolyásol.

Bizonyítottam, hogy a jelenlegi – törvényi szabályozásban is alapnak tekintett – **hírközlési szolgáltatói modell már nem felel meg a mai viszonyoknak**, ezért **felállítottam az azt potenciálisan felváltó új, infrastruktúra-, alkalmazás-, és tartalomszolgáltatói modellt**. Ez véleményem szerint alkalmas a jelenlegi struktúra pontos leírására, ráadásul úgy, hogy egyrészt ebbe a modellbe nem csak a kommunikációt lehetővé tevő internet-technológiára épülő szolgáltatások, szolgáltatók illeszthetők be, másrészt alkalmas a törvényes ellenőrzés jogi problémáinak feloldására is.

Bemutattam azt is**, hogy az elektronikus úton folytatott kommunikáció változásában nagy szerepük van az internet-technológiára épülő szolgáltatásoknak, ezen belül pedig kiemelten a PC/SaaS felhő alapú rendszereknek, ám ezek törvényes ellenőrzése jogi és technikai problémákba ütközik**. Véleményem szerint a törvényes ellenőrzés hatékonyságának növelése érdekében az új hazai jogi szabályozás kialakítását – akár átmeneti jelleggel is – mi hamarabb meg kell tenni, azzal nem célszerű megvárni a feltehetően még évekig húzódó szabványosítási és Európai Uniós irányelvek kialakítását. Ennek során olyan, jelenleg sérthetetlennek tűnő dolgokhoz kell hozzányúlni (szabályozni és adott esetben szankcionálni!), mint a hazai infrastruktúrával nem rendelkező, internetes alkalmazást nyújtó cégek működési jogai, kötelezettségei Magyarországon.

Feltártam az internet-technológiára épülő szolgáltatások törvényes ellenőrzésének kihívásait, amelyeket a jogi szabályozás hiányosságaira, a megfelelő technikai megoldások hiányára, valamint az alkalmazásszolgáltatók együttműködési hajlandóságának a hiányára vezettem vissza.

Nemzetközi kitekintést adtam a tekintetben, hogy különböző országok hogyan valósítják meg, vagy legalábbis hogyan próbálják megvalósítani az említett rendszerek **törvényes ellenőrzés**ét. Bár a lehetséges módszereket a teljesség igénye nélkül ismertettem, ám véleményem szerint ez még így is megfelelő alapot biztosít azok későbbi csoportosítására és jellemző tulajdonságainak feltárására. Rámutattam, hogy a nem teljes körű kitekintésnek

DOI azonosító: 10.17625/NKE.2015.021

egyrészt az az oka, hogy csak publikus információkra lehet támaszkodni, azok pedig – az ügy jellegére tekintettel – meglehetősen korlátozottak, másrészt pedig az, hogy a törvényes ellenőrzésre felhatalmazott szervek részére rendelkezésre álló módszerek ismertetéséhez, elemzéséhez erre egyébként sincs szükség.

A nemzetközi példákat felhasználva, azt kiegészítve **csoportosítottam** az internet-technológiára épülő szolgáltatások, ezen belül pedig kiemelten a PC/SaaS felhő alapú rendszerek **törvényes ellenőrzésére jelenleg rendelkezésre álló jellemző módszereket**, ismertetve azok jellemzőit. **Felállítottam egy, a törvényes ellenőrző módszerek vizsgálatához általánosan használható szempontrendszert**, amelyben megadtam az egyes szempontok értékelésének feltételét. **Ezt a szempontrendszert felhasználva elemeztem** az általam megadott korábbi csoportosításnak megfelelően **a jelenleg rendelkezésre álló módszereket**, majd táblázatos formában összegeztem azok főbb előnyeit, hátrányait.

Megállapítottam, hogy a titkos információgyűjtésre felhatalmazott szervek az elemzést követően már nem csak **az adott módszer bevezetéséről, rendszeresítéséről képesek dönteni**, hanem arról is, hogy egy adott ügyben, adott körülmények között **melyik ellenőrző metódus használata a legcélravezetőbb**. Ugyanakkor a felállított **szempontrendszer** alapján bármilyen más, **akár teljesen új ellenőrzési módszer elemzése is elvégezhető**, így az egyfajta univerzális sablonként szolgálhat.

Bizonyítottam, hogy jelenleg több, egymástól technikailag és működés szempontjából is gyökeresen eltérő **megoldás áll** az arra feljogosított szervezetek **rendelkezésére**, hogy az internet-technológiára épülő szolgáltatásokat, azon belül pedig a PC/SaaS felhő alapú rendszerek kapcsán felmerülő törvényes ellenőrzési feladataikat végrehajtsák. Rámutattam ugyanakkor arra is, hogy **ezen megoldások** használata kapcsán az érintett szervezetek **jogi problémákkal is szembesülnek**. Ezek a technikai megoldások ugyanis annyira újak a törvényes ellenőrzés eszközrendszerében, hogy azok használata sok országban egyáltalán nincs jogilag szabályozva, más országokban frissen kidolgozott szabályzókkal – sokszor vitatottan, vagy éles bírálatok közepette – vezetik be az új, vagy legitimizálják a már működő rendszereket, megint más országokban pedig a meglévő jogszabályokba próbálják több-kevesebb sikerrel beleérteni, beleerőltetni a korábban még nem alkalmazott eszközöket és módszereket.

Egyértelműen megállapítottam, hogy az internet-technológiára épülő szolgáltatások, azon belül pedig a PC/SaaS felhő alapú rendszerek ellenőrzése minden ország törvényes ellenőrzést végző szervei számára kihívást jelentenek, amelynek egyik oka, hogy **a módszerek egyike sem nyújt teljes körű megoldást az igényelt adatok megszerzéséhez**, a másik oka pedig a

DOI azonosító: 10.17625/NKE.2015.021

meglévő jogi szabályozás hiányosságai. Álláspontom szerint az egyik legnagyobb gondot az jelenti, hogy jelenleg nincsen olyan általánosan elfogadott jogi szabályozás, amelyhez bármely országnak, így akár Magyarországnak is igazodni lehetne.

Aláhúztam, hogy a meglévő jogi és technikai problémák okán, a törvényes ellenőrzésre felhatalmazott szervezeteknek – alkalmazkodva a törvényi keretekhez, a célszemély által használt eszközökhöz, szolgáltatásokhoz, a célszemély kommunikációs szokásaihoz, a műveleti helyzethez és az egyéb (pl. infrastruktúraszolgáltató által használt) technikai feltételekhez – több, esetleg minden ellenőrzési módra fel kell készülniük és az azokhoz szükséges eszközöket be kell szerezniük. **Bizonyítottam** azt is, **hogy az alkalmazásszolgáltatóval való együttműködés kikerülhetetlen**. Ugyanakkor rámutattam, hogy bár ez az egyik leghatékonyabb és legköltség-takarékosabb ellenőrzési forma, **ám éppen ennek jogi szabályozottságában lelhető fel a legtöbb hiány**.

A jogi hiányosság feloldásában **elkerülhetetlen**nek látom az érintett piaci szereplők, azaz **a szolgáltatók új**, a törvényes ellenőrzés szempontjából is megfelelő **meghatározásának kialakítás**át. Ez véleményem szerint az általam felállított infrastruktúra-, alkalmazás-, és tartalomszolgáltatói modell szerint megtehető, amely amellett, hogy teljes körűen lefedi az összes jelenlegi szereplőt és egyértelműsíti az ellenőrzési kötelezettségeknek kitett szolgáltatói kört, több más lehetőséget is biztosít, így például segítséget nyújthat bármilyen más, akár teljesen új ellenőrzési módszer törvényi szabályozásának kialakításában valamint bármely, a nemzetbiztonsági szolgálatok és a rendvédelmi szervek számára érdemi információt nyújtó szolgáltatás ellenőrzését lehetővé teszi.

Értékeltem a törvényes ellenőrzést Magyarországon jelenleg szabályozó jogi keretrendszert és ennek kapcsán **javaslatot tettem az Eht. módosítására, kettéválasztására**. Ennek egyik okaként a technikai fejlődés követését, másik okaként pedig a törvényes ellenőrzéshez kapcsolódó és az érintett szereplők minden más feladatát, kötelezettségét előíró részek szétválasztásából adódó előnyöket, valamint a későbbiekben az említett két ok miatt történő egyszerűbb változtathatóságának lehetőségét jelöltem meg.

A törvényes ellenőrzés szemszögéből **elemeztem az infrastruktúra-, alkalmazás- és tartalomszolgáltatók jelenleg elérhető hazai és külföldi fogalmi meghatározásait**, amelyben kiemelt figyelmet fordítottam a hazai jogszabályokban megtalálható definíciókra. Az így megszerzett információkat értékeltem majd megadtam azokat a szempontokat, amelyeket megítélésem szerint az egyes szolgáltatók meghatározásánál figyelembe kell venni. Ezt követően **fogalmi meghatározást adtam az infrastruktúra-, alkalmazás- és tartalomszolgáltatók fogalmára** oly módon, hogy azok megfeleljenek a törvényes ellenőrzés

DOI azonosító: 10.17625/NKE.2015.021

szempontjainak is, így véleményem szerint alkalmasak az ilyen tárgyú törvényekbe és egyéb jogszabályokba történő beillesztésre. További előnye a meghatározásoknak, hogy azok meglátásom szerint nem kizárólag a törvényes ellenőrzéssel szóló, hanem bármilyen más, például a szolgáltatásokkal, szolgáltatók kötelezettségeivel vagy akár az adóztatásukkal kapcsolatos jogszabályokban is problémamentesen felhasználhatók.

Rávilágítottam, hogy az általam felállított modellben minden szolgáltató, szolgáltatás elhelyezhető és kezelhető. Ennek kapcsán példákat mutattam vegyes szolgáltatásokra, valamint azok törvényes ellenőrzés szempontjából történő kezelésére. **Leszögeztem, hogy a hírközlési szolgáltató és szolgáltatás fogalmát a továbbiakban is célszerűnek tartom fenntartani**, mert így például a hagyományos hírközlési szolgáltatások a jelenlegi szabályoknak megfelelően a továbbiakban is egyszerűen, mindenki számára vita nélkül elfogadott módon kezelhetők.

Feltártam, hogy már a magyar jogrendben és hivatali gyakorlatban is vannak olyan precedens értékű példák, amelyek felhasználása elősegíti a törvényes ellenőrzés kialakítását az említett szolgáltatókra.

DOI azonosító: 10.17625/NKE.2015.021

Összegzett következtetések

Az infokommunikációs rendszerek rohamosan fejlődése újabb és újabb, ráadásul többrétű kihívás elé állítja a nemzetbiztonsági szolgálatokat és a rendvédelmi szerveket egyaránt. Történik mindez egyrészt azért, mert az újonnan megjelenő technológiákat feladataik gyorsabb, hatékonyabb ellátása érdekében használni kívánják, ráadásul úgy, hogy az átlagnál jóval magasabb biztonsági igényeik ne sérüljenek, az általuk készített, kezelt érzékeny, személyes vagy adott esetben akár minősített adatok biztonságát az új rendszerek, szolgáltatások ne veszélyeztessék. Másrészt azért, mert az általuk védett állami, kormányzati szervek és azok vezetői szintén használják ezeket a rendszereket, akinél, amelyeknél a biztonságot, azon belül az információbiztonságot ezen a téren is meg kell teremteniük és fenn kell tartaniuk. Harmadrészt pedig azért, mert a célszemélyi körük is igénybe veszi az új infokommunikációs lehetőségeket, így ezek esetében meg kell oldaniuk a törvényes ellenőrzést. A nemzetbiztonsági szolgálatokat és a rendvédelmi szervek számára ezek a feladatok külön-külön is komoly kihívást jelentenek, a mai infokommunikációs rendszereknél azonban sok esetben mindhárom feladat egy időben jelenik meg egy-egy adott rendszer kapcsán. Ilyenek például a felhő alapú rendszerek is.

Értekezésem elkészítése során **a felhő alapú rendszerek nemzetbiztonsági kihívásaira koncentráltam**, ugyanakkor figyelembe vettem azt a tényt, hogy **ezek a rendszerek önállóan nem vizsgálhatóak**. Ahogyan már a felhasználás során is számba kell venni például a kapcsolathoz szükséges infokommunikációs csatornák, valamint a felhasználói oldal eszközeinek, rendszereinek tulajdonságait, sérülékenységeit, úgy a védett vezetők esetében sem alakítható ki megfelelő szintű biztonság az általuk igénybe vett egyéb internet-technológiára épülő szolgáltatások és személyi használatú hordozható infokommunikációs eszközök vizsgálata nélkül. De a törvényes ellenőrzés kapcsán is elmondható, hogy annak hatékony ellátása érdekében az internet-technológiára épülő szolgáltatások szélesebb körét, és nem pusztán az annak részhalmazát jelentő felhő alapú rendszereket kell górcső alá venni. Mindezek mellett dolgozatom fókuszpontjában a felhő alapú rendszerek álltak.

Az első fejezetben bemutattam a felhő alapú rendszereket, azok meghatározásait, az elfogadott modelleket, sajátosságaikat, jellemezőiket. Az egyes szolgáltatási és telepítési modelleknél meghatároztam azok előnyeit, hátrányait, egységesen összefoglalva és kiegészítve a szakirodalomban található, meglehetősen heterogén, sokszor hiányos és nem konzekvens felsorolásokat. Ez így már véleményem szerint kellő alapot ad arra, hogy a

DOI azonosító: 10.17625/NKE.2015.021

szolgáltatási és telepítési modellekből képezhető mátrixban bárki elhelyezzen egy kínált szolgáltatást, vagy kiválassza az igényeinek leginkább megfelelő modellt.

Áttekintettem **a kormányzati felhőre** adott meghatározásokat, és **megállapítottam,** hogy erre jelenleg **nincs egységesen elfogadott definíció**. Miután véleményem szerint **ennek gyakorlati haszna is lenne, ezért saját meghatározást adtam először a kormányzati felhő, majd ebből kiindulva a rendvédelmi felhő fogalmára**.

Tisztáztam azt is, hogy mi a különbség a felhő alapú rendszerek és egyrészt a hagyományos ICT rendszerek virtualizációja, másrészt a kiszervezett ICT rendszerek és szolgáltatások, harmadrészt az internet-technológiára épülő szolgáltatások között. Az értekezés szempontjából az elemzésemnek talán az volt legfontosabb megállapítása, hogy jelenleg nem lehet éles határvonalat húzni az internet-technológiára épülő szolgáltatások és az annak részhalmazát képező PC/SaaS rendszerek között, sőt és az új szolgáltatások megjelenésének ütemét, az általuk kínált, a korábbiaktól sokszor merőben eltérő új funkcióikat, lehetőségeket figyelembe véve, ezt jó ideig még nem is lehet egyértelműen megtenni. Ez önmagában is megerősíti, hogy vizsgálatokat nem célszerű a felhő alapú rendszerekre leszűkítve elvégezni, a dolgozat céljainak elérése és az eredmények hatékony alkalmazhatósága pedig kiemeli azt.

Az iparági tendenciák és előrejelzések figyelembevételével **bizonyítottam, hogy a nemzetbiztonsági szolgálatoknak és a rendvédelmi szerveknek a felhő alapú rendszerekkel a lehetséges felhasználás, a védett vezetők információbiztonságának emelése és a törvényes ellenőrzés biztosítása okán is mindenképpen foglalkozniuk kell**.

A második fejezetben **elemeztem és értékeltem a fejlett országok felhő alapú rendszerekkel foglalkozó nemzeti-, és a nemzetközi szervezetei által megalkotott, nyíltan elérhető, a dolgozat célkitűzése szempontjából releváns biztonsági ajánlásokat**, így a CSA, a NIST, a FedRAMP, a BSI, valamint az ENISA illeszkedő dokumentumait, és ezekben feltártam a biztonság értékeléséhez szükséges kockázatokat**. Megállapítottam, hogy az egyes szervezetek heterogén módon vizsgálják az adott kérdést**, ahol három alapvető kiindulásbeli különbség azonosítható. Az első, hogy a **szolgáltató vagy a felhasználó oldaláról** közelítik-e meg a kérdést, a második, hogy **a megcélzott felhasználó civil vagy kormányzati szervezet, esetleg magánember**-e, a harmadik pedig, hogy az ajánlást készítő szervezet **az Egyesült Államok vagy az Európai Unió jelenlegi technikai és jogi környezetéből indul**-e ki. **Megállapítottam** azt is, hogy bár **egyik sem a rendvédelmi szervek szemszögéből vizsgálódott**, ezek ellenére a dokumentumokban megfogalmazottak megfelelő újragondolással és átalakítással felhasználhatók akár egy, a hazánk rendvédelmi szerveinek szóló biztonsági sablon elkészítéséhez.

DOI azonosító: 10.17625/NKE.2015.021

A különböző szervezetek ajánlásaiban a telepítési modellek előnyeiről, hátrányairól leírtak alapján azt a következtetetést vontam le, hogy a rendvédelmi szervek számára napjainkban felhasználóként a közösségi felhő jelentheti az optimális megoldást.

A felhő alapú rendszerek biztonsági kérdéseinek rendvédelmi szervek szemszögéből történő komplex vizsgálatához egy új szempontrendszert állítottam fel. Ez egy olyan 4 dimenziós tér, amelynek „a rendvédelmi szerv szerepe – telepítési modellek – szolgáltatási modellek – vizsgálandó biztonsági kérdéscsoportok" az elemei. Ebben a „vizsgálandó biztonsági kérdéscsoportoknál" szintén egy új kategorizálásban vezettem be, az „üzembiztonság – adatbiztonság – egyéb (jogi, fizikai stb.) biztonság – törvényes ellenőrzés" csoportosítást. Ez utóbbiaknál meghatároztam, hogy mit tekintek üzembiztonsági, adatbiztonsági, egyéb (jogi, fizikai stb.) biztonsági, valamint törvényes ellenőrzési kategóriába tartozó kérdésnek, ezek technikai vagy jogi úton oldhatók-e meg, valamint, hogy a felhasználó és a szolgáltató érdekei és felelősségi körei itt hogyan viszonyulnak egymáshoz. Ennek segítségével az említett szervek bármely feladatuk kapcsán, komplex módon haladhatnak végig egy adott rendszer vizsgálatán.

A fentiek felhasználásával **megalkottam a rendvédelmi szervek számára egy, a felhő alapú rendszerek minimálisan elvárt biztonsági szintjének megállapítására szolgáló elemző sablont**, valamint annak használati útmutatóját. Rávilágítottam, hogy ez egyrészt a technikai fejlődésnek és az egyéb igényeknek köszönhetően akár önmagában is továbbfejleszthető, másrészt ezt alapként használva, a vizsgálati szint kibővíthető az egyes biztonsági részterületeket mélyebben elemző újabb sablonok előállításával.

Feltártam és leszögeztem, hogy a törvényes ellenőrzés kapcsán célszerű lenne bevezetni és szabványosítani a Lawful Monitoring as a Service (LMaaS) (vagy valami hasonló) fogalmát, amelynek keretében a szolgáltató szolgáltatásként, egységes megközelítés és feltételek mellett biztosíthatná az ellenőrzést végző szervek számára a szükséges és a különböző jogszabályok által igényelhető információkat.

A harmadik fejezetben a védett vezetők információbiztonsági védelmének főbb kérdéseit elemeztem. Rámutattam, hogy ennek emelése érdekében a technikai elhárítást ki kell terjeszteni a védett vezetők által használt kibertérre is, azaz az ellenőrzés során vizsgálni kell az általuk használt személyi használatú hordozható infokommunikációs eszközöket és internet-technológiára épülő szolgáltatásokat is. Megállapítottam azt is, hogy **csak technikai úton az információbiztonsági védelmet nem lehet, vagy irreálisan drága kialakítani, ugyanakkor az információk megvédésének egyik leghatékonyabb és legolcsóbb módja a**

DOI azonosító: 10.17625/NKE.2015.021

biztonságtudatos használat. Ennek kialakításához viszont személyre szabott felkészítési módszert célszerű megalkotni.

Azzal a feltételezéssel éltem, hogy a védett vezetők felhasználói szokásai nem térnek el jelentősen az átlagtól, így a leggyakrabban használt személyi használatú, hordozható infokommunikációs eszközök és internet-technológiára épülő szolgáltatások, ezeken belül is kiemelten a PC/SaaS típusú rendszerek kockázatait elemeztem. A korábban már használt kategorizálás mentén bemutattam, hogy az üzembiztonság, az adatbiztonság és az egyéb biztonság kategóriák esetében milyen releváns veszélyek állnak fenn, ezek közül melyikre és milyen mértékű ráhatása lehet a felhasználónak. Felállítottam továbbá egy keretrendszert, amelyben rögzítettem azokat a feltételezéseket, amelyekkel a védett vezetők speciális helyzetét figyelembe tudtam venni.

A feltárt veszélyek, valamint a fenti keretrendszer segítségével kidolgoztam a védett vezetők számára a személyükre szabott biztonságtudatos használathoz kapcsolódó alap információbiztonsági felkészítési módszert, úgy, hogy az ne csak az éppen aktuálisan használt eszközre és szolgáltatásra legyen megfelelő, hanem akár egy új szolgáltatás vagy eszköz igénybe vétele esetén is. Az általam megalkotott információbiztonsági felkészítési tematika megfelelő adaptációval, más területeken (pl. gazdasági, magán) is felhasználható. Megállapítottam, hogy ez az oktatás szükséges, de önmagában nem elégséges. A továbblépést négy kategóriában tartom célszerűnek: a magasabb szintű megközelítést igénylő, a védett vezető által megtehető, az üzemeltetést végző személyek által megtehető, valamint a technikai elhárítást végzők által megtehető feladatok esetében.

A negyedik fejezetben az internet-technológiára épülő szolgáltatások, ezen belül pedig kiemelten a PC/SaaS felhő alapú rendszerek törvényes ellenőrzési lehetőségeit elemeztem. Ennek kapcsán bemutattam, hogy az infokommunikációs eszközökben, szolgáltatásokban jelentkező technológiai konvergencia a törvényes ellenőrzés feladatainak konvergenciáját is indukálja, amely alapvető változásokat indít el ebben a feladatkörben is.

Bizonyítottam, hogy az elektronikus úton folytatott kommunikáció egy sokkal szélesebben értelmezhető fogalom, mint a hírközlés, ráadásul a hagyományos hírközlési formák egyre inkább veszítenek jelentőségükből a felhasználók, így a törvényes ellenőrzést végzők számára is. Ennek okaként a felhasználói szokások jelentős változását jelöltem meg. Mivel meglátásom szerint **a jelenlegi**, a törvényi szabályozásban is alapnak tekintett **hírközlési szolgáltatói modell már nem felel meg a mai viszonyoknak, ezért felállítottam az azt felváltó új, infrastruktúra-, alkalmazás-, és tartalomszolgáltatói modellt**. Ez úgy alkalmas a jelenlegi struktúra pontos leírására, hogy egyrészt minden internet-technológiára

DOI azonosító: 10.17625/NKE.2015.021

épülő, így a kommunikációt lehetővé tevő szolgáltatás, szolgáltató beilleszthető, másrészt megfelelő a törvényes ellenőrzés jogi problémáinak feloldására is.

Bemutattam azt is, hogy **az elektronikus úton folytatott kommunikáció változásában nagy szerepük van az internet-technológiára épülő szolgáltatásoknak**, ezen belül pedig kiemelten a PC/SaaS felhő alapú rendszereknek, **ám ezek törvényes ellenőrzése jogi és technikai problémákba ütközik.** Nyílt forrásokból merítve nemzetközi kitekintést adtam a jelenleg rendelkezésre álló jellemző lehetőségekről, módszerekről, majd ezt felhasználva, tulajdonságaikat is ismertetve, csoportosítottam azokat.

Felállítottam egy, a törvényes ellenőrző módszerek vizsgálatához általánosan használható új szempontrendszert, majd az itt megadott értékelési feltételek figyelembe vételével elemeztem a jelenleg rendelkezésre álló módszereket és táblázatos formában összegeztem azok főbb előnyeit, hátrányait. **Ennek segítségével a felhatalmazott szervek amellett, hogy képesek dönteni egy adott módszer bevezetéséről, bármilyen más, akár teljesen új ellenőrzési módszer elemzését is elvégezhetik**.

Egyértelműen megállapítottam, hogy az internet-technológiára épülő szolgáltatások törvényes ellenőrzése minden ország érintett szerve számára kihívást jelent, amelynek egyik oka, hogy egyik módszer sem nyújt teljes körű megoldást az igényelt adatok megszerzéséhez, a másik oka pedig a meglévő jogi szabályozás hiányosságai. **Bizonyítottam azt is, hogy az alkalmazásszolgáltatóval való együttműködés kikerülhetetlen, ugyanakkor éppen ennek jogi szabályozottságában lelhető fel a legtöbb hiány**. **A jogi hiányosság feloldásában elkerülhetetlennek látom az érintett piaci szereplők, azaz a szolgáltatók új, a törvényes ellenőrzés szempontjából is megfelelő meghatározásának kialakítását**. Ez véleményem szerint az általam felállított infrastruktúra-, alkalmazás-, és tartalomszolgáltatói modellben megtehető. A jelenleg elérhető hazai és külföldi fogalmi meghatározások elemzését követően **meghatározást adtam az infrastruktúra-, alkalmazás- és tartalomszolgáltatók fogalmára** oly módon, hogy azok beilleszthetők legyenek a velük foglalkozó, így a törvényes ellenőrzési tárgyú törvényekbe és egyéb jogszabályokba is.

Rávilágítottam, hogy az általam felállított modellben minden szolgáltató, szolgáltatás elhelyezhető, és ennek demonstrálására példákat mutattam vegyes szolgáltatásokra, valamint azok törvényes ellenőrzés szempontjából történő kezelésére. Ugyanakkor leszögeztem, hogy a hírközlési szolgáltató és szolgáltatás fogalmát a továbbiakban is célszerűnek tartom fenntartani, mert így a hagyományos hírközlési szolgáltatások ellenőrzése a jelenlegi szabályoknak megfelelően, a továbbiakban is egyszerűen, mindenki számára vita nélkül elfogadott módon megoldhatók.

DOI azonosító: 10.17625/NKE.2015.021

Új tudományos eredmények

1. **A felhő alapú rendszerek használatához kapcsolódó** biztonsági kérdések rendvédelmi szervek szemszögéből történő **komplex vizsgálatához új szempontrendszert dolgoztam ki.**
2. **Megalkottam a rendvédelmi szervek számára a felhő alapú rendszerek biztonsági értékeléséhez** szabadon **felhasználható elemző sablont**, valamint annak használati útmutatóját.
3. **Kidolgoztam a védett vezetők számára a személyükre szabott biztonságtudatos használathoz kapcsolódó alap információbiztonsági felkészítési módszert**.
4. **Kidolgoztam egy, a törvényes ellenőrző módszerek vizsgálatához általánosan használható szempontrendszert**, amelyben megadtam az egyes szempontok értékelésének feltételét.
5. A jelenlegi hírközlési szolgáltatói modell helyett **kidolgoztam** az azt potenciálisan felváltó **új, infrastruktúra-, alkalmazás-, és tartalomszolgáltatói modellt**, valamint **fogalmi meghatározást adtam az infrastruktúra-, alkalmazás- és tartalomszolgáltatók fogalmára**.

DOI azonosító: 10.17625/NKE.2015.021

Ajánlások

Az értekezésben megfogalmazottak további hasznosíthatóságát az alábbiakban látom:

1. Felhasználható a Nemzeti Közszolgálati Egyetem oktatási tevékenysége során, kiemelten a Hadtudományi és Honvédtisztképző Kar nemzetbiztonsági alap és mesterképzésén, valamint a Nemzetbiztonsági Intézet által oktatott tárgyak esetében, akár önálló oktatási anyagrészenként, akár forrásmunkaként, akár ajánlott irodalomként.
2. Az egyes fejezetek következtetési részében leírtaknak megfelelően további tudományos vizsgálatok, kutatások alapját képezheti, így például a technikai elhárítás kiterjesztett értelmezése, a védett vezetők felhasználói szokásainak felmérése során.
3. Bizonyos, például az internet-technológiára épülő szolgáltatások, azon belül kiemelten a felhő alapú rendszerek, valamint a személyi használatú, hordozható infokommunikációs eszközök biztonsági kockázatait leíró részei felhasználhatók a Kormányzati Eseménykezelő Központ (GovCERT) tudatosító tevékenysége során.
4. A „Biztonsági sablon felhőszolgáltató megfelelőségének ellenőrzésére” című dokumentum megfelelő adaptációval más kormányzati, nem rendvédelmi szervnek szóló hasonló biztonsági elemző sablon alapját képezheti, de felhasználható akár a magánszférában is, például egy kritikus infrastruktúrát üzemeltető vállalatnál, ahol a szokásosnál szigorúbb információbiztonsági feltételeket kell kialakítani.
5. A „Biztonsági sablon felhőszolgáltató megfelelőségének ellenőrzésére” című dokumentum a technikai fejlődés és az egyéb igények okán önmagában is továbbfejleszthető, de ezt alapként használva további, az egyes biztonsági részterületeket mélyebben vizsgáló elemző sablon is kidolgozható.
6. A védett vezetőknek szóló biztonságtudatossági felkészítés módszere, tartalma megfelelő adaptációval más területeken, így például a gazdasági vagy akár a magán szférában is felhasználható.
7. Kiindulási alapként szolgálhat a védett vezetők által használt személyi használatú, hordozható infokommunikációs eszközökkel és internet-technológiára épülő szolgáltatásokkal összefüggő információbiztonság emelésével kapcsolatos magasabb szintű megközelítést igénylő, a védett vezető által megtehető, az üzemeltetést végző személyek által megtehető, valamint a technikai elhárítást végzők által megtehető feladatok meghatározásához.

DOI azonosító: 10.17625/NKE.2015.021

8. Felhasználható a titkos információgyűjtésre és titkos adatszerzésre feljogosított szervezetek számára, például az internet-technológiára épülő szolgáltatások, ezen belül kiemelten a felhő alapú rendszerek törvényes ellenőrzése kapcsán egy adott feladathoz a megfelelő módszer kiválasztása, valamint bármilyen más, akár új módszer elemzése során.
9. A megalkotott szolgáltatói modell és definíciók felhasználhatók az új jogszabályi környezet kialakításához.

DOI azonosító: 10.17625/NKE.2015.021

A témakörben megjelent publikációim

Lektorált folyóiratban megjelent cikkek

1. Kovács Zoltán: Felhő alapú informatikai rendszerek potenciális alkalmazhatósága a rendvédelmi szerveknél. Hadmérnök. VI. Évfolyam 4. szám - 2011. december, pp. 176-188. ISSN 1788-1919 Online: http://hadmernok.hu/2011_4_kovacsz.php
2. Kovács Zoltán: Cloud Security in Terms of the Law Enforcement Agencies. Hadmérnök. VII. Évfolyam 1. szám - 2012. március, pp. 144-156. ISSN 1788-1919 Online: http://hadmernok.hu/2012_1_kovacsz.pdf
3. Kovács Zoltán: Felhő alapú rendszerek törvényes ellenőrzési problémái. Hadmérnök. VIII. Évfolyam 1. szám - 2013. március, pp. 233-241. ISSN 1788-1919 Online: http://hadmernok.hu/2013_1_kovacsz.pdf
4. Kovács Zoltán: „Electronic Written Tasking Order System" Accomplished Within the Project „Secure Electronic Communication" I. Hadmérnök. VIII. Évfolyam 3. szám - 2013. szeptember, pp. 171-183. ISSN 1788-1919 Online: http://hadmernok.hu/133_17_kovacsz_1.pdf
5. Kovács Zoltán: Felhő alapú rendszerek törvényes ellenőrzési módszerei vizsgálata I. Hadmérnök. VIII. Évfolyam 3. szám - 2013. szeptember, pp. 184-197. ISSN 1788-1919 Online: http://hadmernok.hu/133_18_kovacsz_2.pdf
6. Kovács Zoltán: Felhő alapú rendszerek törvényes ellenőrzési módszerei vizsgálata II. Hadmérnök. VIII. Évfolyam 3. szám - 2013. szeptember, pp. 198-210. ISSN 1788-1919 Online: http://hadmernok.hu/133_19_kovacsz_3.pdf
7. Kovács Zoltán: „Electronic Written Tasking Order System" Accomplished Within the Project „Secure Electronic Communication" II. Hadmérnök. VIII. Évfolyam 4. szám - 2013. december, pp. 201-209. ISSN 1788-1919 Online: http://hadmernok.hu/134_17_kovacsz.pdf
8. Kovács Zoltán: „Electronic Written Tasking Order System" Accomplished Within the Project „Secure Electronic Communication" III. Hadmérnök. IX. Évfolyam 1. szám - 2014. március, pp. 199-208. ISSN 1788-1919 Online: http://hadmernok.hu/141_19_kovacsz.pdf
9. Gazdag Tibor – Kovács Zoltán: Felhő alapú új pénzügyi tranzakciós lehetőségek és azok veszélyei. Nemzetbiztonsági Szemle. II. Évfolyam 2. szám - 2014. június, pp. 36-57.

ISSN 2064-3756 Online: http://uni-nke.hu/uploads/media_items/gazdag-tibor-kovacs-zoltan-felho-alapu-uj-penzugyi-tranzakcios-lehetosegek-es-azok-veszelyei.original.pdf

10. Kovács Zoltán: Hordozható infokommunikációs eszközök használatának veszélyei a védett vezetők biztonságtudatossági képzésének szempontjából I. Hadmérnök. IX. Évfolyam 2. szám - 2014. június, pp. 277-289 ISSN 1788-1919 Online: http://hadmernok.hu/142_26_kovacsz_1.pdf
11. Kovács Zoltán: Hordozható infokommunikációs eszközök használatának veszélyei a védett vezetők biztonságtudatossági képzésének szempontjából II. Hadmérnök. IX. Évfolyam 2. szám - 2014. június, pp. 290-296 ISSN 1788-1919 Online: http://hadmernok.hu/142_27_kovacsz_2.pdf
12. Kovács Zoltán: Hordozható infokommunikációs eszközök használatához kapcsolódó biztonságtudatossági képzési tematika védett vezetők számára. Hadmérnök. IX. Évfolyam 3. szám - 2014. szeptember, pp. 182-190 ISSN 1788-1919 Online: http://www.hadmernok.hu/143_14_kovacsz.pdf
13. Kovács Zoltán: Infrastruktúra-, alkalmazás- és tartalomszolgáltatók fogalmi meghatározása a törvényes ellenőrzés szemszögéből. Nemzetbiztonsági Szemle. II. Évfolyam 4. szám - 2014. december, pp. 3-28 ISSN 2064-3756 Online: http://uni-nke.hu/uploads/media_items/nemzetbiztonsagi-szemle-2014-4-2.original.pdf (2014.11.27.)
14. Kovács Zoltán: Védett vezetők hordozható infokommunikációs eszközeinek védelme a rádiófrekvenciás tartományban. Bolyai Szemle. XXIII. Évfolyam 2014/4. szám, pp. 58-75 ISSN 1416-1443 Online: http://uni-nke.hu/downloads/kutatas/folyoiratok/bolyai_szemle/Bolyai_Szemle_2014_04_elektron.pdf

Konferencia kiadványban megjelent cikkek

15. Kovács Zoltán: Felhő-alapú informatikai rendszerek, mint nemzetbiztonsági kihívás. Hadtudomány XXIII. Évfolyam 1-2. szám - 2013. március, pp. 5-12 ISSN 1215-4121 Online: http://mhtt.eu/hadtudomany/2013/1_2/HT_2013_1-2_mhtt.pdf

Konferencia kiadványban megjelent kivonatok

16. Kovács Zoltán: Hordozható infokommunikációs eszközök használatához kapcsolódó biztonságtudatossági képzési tematika védett vezetők számára. In: A haza szolgálatában 2014 konferencia rezümékötet. Szerk.: Kiss Dávid, Orbók Ákos. Nemzeti Közszolgálati Egyetem. Budapest 2014. pp. 160-161. ISBN:978-615-5491--88-7

DOI azonosító: 10.17625/NKE.2015.021

Egyetemi jegyzet fejezetek:

17. Dobák Imre - Kovács Zoltán: Új technológiák hatása a hírszerzésre. In: A nemzetbiztonság általános elmélete. Szerk.: Dobák Imre. Nemzeti közszolgálati Egyetem Nemzetbiztonsági Intézet. Budapest 2014. pp. 206-220. ISBN: 978-615-5305-49-8

DOI azonosító: 10.17625/NKE.2015.021

Felhasznált irodalom

Irodalomjegyzék

[1] The Mobile Cloud Computing Market Will Generate 45 Billion Dollars in Revenues by 2016, Says the Latest VISIONGAIN Report. 2011. 12. 16. https://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. Letöltés ideje: 2015. 08. 01.

[2] Gartner Reveals Top Predictions for IT Organizations and Users for 2012 and Beyond. 2011. 12. 01. http://www.gartner.com/newsroom/id/1862714. Letöltés ideje: 2015. 08. 01.

[3] Microsoft sees huge gains in commercial cloud revenue. 2014. 07. 22. https://blogs.microsoft.com/firehose/2014/07/22/microsoft-sees-huge-gains-in-commercial-cloud-revenue/ Letöltés ideje: 2015. 08. 01.

[4] CIB Bank - eBroker - Vállalatok. 2015. 07. 21. http://www.cib.hu/ebroker/hirportal/tozsde_vallalatok/index?id=P217204 Letöltés ideje: 2015.. 08. 01.

[5] Cisco Global Cloud Index: Forecast and Methodology, 2013–2018 - Whitepaper. 2014. http://www.cisco.com/c/en/us/solutions/collateral/service-provider/global-cloud-index-gci/Cloud_Index_White_Paper.pdf. Letöltés ideje: 2015. 08. 01.

[6] 204M Smartphone Users In India By 2016. Will Surpass US: EMarketer. 2014. 12. 23. http://trak.in/tags/business/2014/12/23/smartphone-users-india-global-growth-chart/ Letöltés ideje: 2015. 08. 01.

[7] Chart of the day: How many Tablet PCs have been sold in US since 2010. 2015. 03. 13. http://www.onlinemarketing-trends.com/2015/03/chart-of-day-how-many-tablet-pcs-have.html Letöltés ideje: 2015. 08. 01.

[8] Cohen, Heidi: 15 Mobile Facts That Should Change Your 2015 Marketing. 2015. 02. 02. http://heidicohen.com/mobile-app-trends-2015/ Letöltés ideje: 2015. 08. 01.

[9] Már okostelefon-felhasználó a magyar lakosság több mint ¼-e. 2013. 05. 17. http://www.enet.hu/hirek/mar-okostelefon-felhasznalo-a-magyar-lakossag-tobb-mint-%C2%BC-e/?lang=hu Letöltés ideje: 2015. 08. 02.

[10] Minden ötödik internetező kezében ott a tablet. 2014. 08. 26. http://www.enet.hu/hirek/minden-otodik-internetezo-kezeben-ott-a-tablet/?lang=hu Letöltés ideje: 2015. 08. 02.

[11] Áttörés a mobilnet használatban: a magyar internetezők fele zsebében tartja a világhálót. 2015. 03. 04. http://www.enet.hu/hirek/attores-a-mobilnet-hasznalatban-a-magyar-internetezok-fele-zsebeben-tartja-a-vilaghalot/?lang=hu Letöltés ideje: 2015.. 08. 02.

[12] Médiatartalmat inkább online! – kérik a fiatalok. 2015. 01. 17. http://www.enet.hu/hirek/mediatartalmat-inkabb-online-kerik-a-fiatalok/?lang=hu Letöltés ideje: 2015.. 08. 02.

[13] Haig Zsolt – Kovács László – Munk Sándor – Ványa, László: Az infokommunikációs technológia hatása a hadtudományokra. Budapest : Nemzeti Közszolgálati Egyetem, 2013. ISBN 978-615-5305-02-3.

[14] Munk, Sándor: A kommunikáció fogalomrendszerének keretei az integrálódó információs technológiák korában. In: Kommunikáció 2009. Budapest. ZMNE, 2009. pp. 51-64. ISBN 978-963-7060-70-0

[15] Sallai Gyula: Defining Infocommunications and Related. Acta Polytechnica Hungarica. 9. Évfolyam 6. szám – 2012. pp. 5-15. ISSN 1785-8860

[16] Cloud – számítási felhő, az internet jövője? 2011. 04. 25. http://intermatrix.hu/clouds. Letöltés ideje: 2011. 10. 04.

[17] toros: Az Ubuntu megváltoztatja a számítógép által nyújtott élményt. 2011. 04. 28. http://ubuntu.hu/ubuntu1104/press. Letöltés ideje: 2011. 10. 22.

[18] http://windows.microsoft.com/hu-HU/windows/cloud. Letöltés ideje: 2011. 10. 22.

[19] http://www.microsoft.com/hu-hu/office365/how-office365-works.aspx. Letöltés ideje: 2011. 10. 21.

[20] Harangi László: Hogyan szerezzünk felhő-alapú vírusírtót, tűzfallal? 2011. 09. 16. http://pcworld.hu/hogyan-szerezzunk-felho-alapu-virusirtot-tuzfallal-20110916.html. Letöltés ideje: 2011. 10. 04.

[21] http://www.nexon.hu/felho-alapu-hoszting-szolgaltatas. Letöltés ideje: 2011. 10. 07.

[22] Továbbfejlesztett mobil és felhő alapú nyomtatási szolgáltatások az Epsontól. 2011. 09. 14. http://hirek.prim.hu/cikk/2011/09/14/tovabbfejlesztett_mobil_es_felho_alapu_nyomtatasi_szolgaltatasok_az_epsontol. Letöltés ideje: 2011. 10. 07.

[23] Releasing the Chromium OS open source project. http://googleblog.blogspot.hu/2009/11/releasing-chromium-os-open-source.html. Letöltés ideje: 2011. 10. 21.

[24] Bodnár Ádám: 2011 közepén jön a Google Chrome OS. 2010. 12. 08. http://www.hwsw.hu/hirek/45786/google-chrome-os-web-store-bongeszo-operacios-rendszer-notebook-netbook.html. Letöltés ideje: 2011. 10. 21.

[25] http://www.google.com/chromebook/. Letöltés ideje: 2011. 10. 21.

[26] NIST Cloud Computing Program. http://www.nist.gov/itl/cloud/index.cfm. Letöltés ideje: 2011. 10. 21.

[27] Mell, Peter – Grance, Timothy: The NIST Definition of Cloud Computing Version 15. 2010. 10. 07. www.nist.gov/itl/cloud/upload/cloud-def-v15.pdf. Letöltés ideje: 2011. 10. 21.

[28] Lepenye Tamás: Számítási felhő – egyszerűen. 2011. 06. 15. http://lepenyet.wordpress.com/2011/06/15/szmtsi-felho-egyszeruen/. Letöltés ideje: 2011. 10. 21.

[29] Security Recommendations for Cloud Computing Providers (Minimum information security requirements) White Paper. 2011. 06. 22. https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Publications/Minimum_information/SecurityRecommendationsCloudComputingProviders.html. Letöltés ideje: 2014. 09. 21.

[30] Lepenye Tamás: Számítási felhő – egyszerűen (2. rész). 2011. 06. 16. http://lepenyet.wordpress.com/2011/06/16/szmtsi-felho-egyszeruen-2-rsz/. Letöltés ideje: 2011. 10. 21.

[31] DePaolis, Enrico: Types of Cloud Computing. 2009. 07. 25. http://cloudcomputing.sys-con.com/node/1048046. Letöltés ideje: 2011. 10. 09.

[32] Naugès, Louis: PRaaS, Process as a Service. 2009. 08. 30. http://nauges.typepad.com/my_weblog/2009/08/praas-process-as-a-service.html. Letöltés ideje: 2011. 10. 22.

[33] Kusnetzky, Dan: Fourth type of cloud computing. 2009. 10. 05. http://www.zdnet.com/blog/virtualization/fourth-type-of-cloud-computing/1346. Letöltés ideje: 2011. 10. 09.

[34] Chandrasekhar, Bharath: What is Cloudbursting? 2011. 03. 15. http://cloudsecurity.trendmicro.com/what-is-cloudbursting/. Letöltés ideje: 2011. 10. 22.

[35] Lepenye Tamás: Számítási felhő – egyszerűen (3. rész). 2011. 06. 17. http://lepenyet.wordpress.com/2011/06/17/szmtsi-felho-egyszeruen-3-rsz/. Letöltés ideje: 2011. 10. 22.

[36] Good Practice Guide for Securely Deploying Governmental Clouds. 2013. 11. 15. https://www.enisa.europa.eu/activities/Resilience-and-CIIP/cloud-computing/good-practice-guide-for-securely-deploying-governmental-clouds. Letöltés ideje: 2014. 11. 15.

[37] Guidance - G-Cloud service definitions. 2013. 11. 01. https://www.gov.uk/government/publications/g-cloud-service-definitions. Letöltés ideje: 2015. 01. 31.

[38] GovCloud. http://i.gov.ph/govcloud/wp-content/uploads/2014/03/GovCloud-Year-Ender_December-12-2013.pdf. Letöltés ideje: 2015. 01. 31.

[39] GovCloud. http://www.techopedia.com/definition/28218/govcloud. Letöltés ideje: 2015. 01. 31.

[40] AWS GovCloud (US) Region FAQs. http://aws.amazon.com/govcloud-us/faqs/. Letöltés ideje: 2015. 01. 31.

[41] Virtualization is Not the Cloud. 2012. 09. 12. http://www.rackspace.com/knowledge_center/whitepaper/virtualization-is-not-the-cloud. Letöltés ideje: 2015.. 01. 10.

[42] http://www.microsoft.com/hun/virtualization/promise.mspx. Letöltés ideje: 2011. 10. 28.

[43] Vasvári György: AZ IT VIRTUALIZÁCIÓ (AJÁNLÁS 4.0). 2008. www.infota.org/biztmen/docs/A_VIRTUALIZACIO_Ajanlas_4.doc. Letöltés ideje: 2011. 10. 28.

[44] http://www.kvint-r.hu/termekek_szolgaltatasok/57/virtualizacio_vmware. Letöltés ideje: 2011. 10. 28.

[45] Makk Attila: VMware a felhőkben. 2009. 05. 21. http://computerworld.hu/vmware-a-felhokben.html. Letöltés ideje: 2011. 10. 28.

[46] Barker, Colin: Cloud computing and outsourcing: Where does one end and the other begin? 2013. 07. 30. http://www.zdnet.com/article/cloud-computing-and-outsourcing-where-does-one-end-and-the-other-begin/. Letöltés ideje: 2015. 01. 10.

[47] Yigitbasioglu, Ogan M. – Mackenzie, Kim – Low, Rouhshi: Cloud Computing: How does it differ from IT outsourcing and what are the implications for practice and research? 2013., The International Journal of Digital Accounting Research, 13. pp. 99-

121. http://www.uhu.es/ijdar/10.4192/1577-8517-v13_4.pdf. ISSN: 2340-5058. Letöltés ideje: 2015. 03. 02.

[48] Katzan, Harry – Dowling, William A.: Software-As-A-Service Economics. The Clute Institute, 2010. First Quarter, Review of Business Information Systems, 14. pp. 27-38. http://www.cluteinstitute.com/ojs/index.php/RBIS/article/view/500/487. ISSN 2157-9547. Letöltés ideje: 2015. 03. 02.

[49] Marston, Sean R. – Li, Zhi – Bandyopadhyay, Subhajyoti – Ghalsasi, Anand – Zhang, Juheng: Cloud Computing: The Business Perspective. 2011. 04., Decision Support Systems, Volume 51, Issue 1, pp. 176-189. ISSN: 0167-9236.Letöltés ideje: 2015. 01. 10.

[50] Cloud Computing vs. Outsourcing. 2013. 01. 15. https://www.getcloudservices.com/blog/cloud-computing-vs-outsourcing. Letöltés ideje: 2015. 01. 10.

[51] Daniele Catteddu (szerk.): Security & Resilience in Governmental Clouds. 2011. 01. http://www.enisa.europa.eu/activities/risk-management/emerging-and-future-risk/deliverables/security-and-resilience-in-governmental-clouds. Letöltés ideje: 2014. 11. 18.

[52] https://www.facebook.com/orbanviktor. Letöltés ideje: 2014. 02. 22.

[53] https://www.facebook.com/gyurcsanyf. Letöltés ideje: 2014. 02. 22.

[54] https://twitter.com/FerencGyurcsany. Letöltés ideje: 2014. 02. 22.

[55] https://www.google.hu/. Letöltés ideje: 2014. 02. 22.

[56] Gálffy Csaba: Publikus felhőre költik az új IT-kiadások felét. 2011. 06. 23. http://www.hwsw.hu/hirek/46921/felho-cloud-idc-piac.html. Letöltés ideje: 2011. 10. 22.

[57] http://www.isidorcloud.hu/cloud-computing-felhoalapu-szamitastechnika.html. Letöltés ideje: 2011. 10. 07.

[58] http://newsroom.cisco.com/dlls/2010/ts_101910.html. Letöltés ideje: 2011. 10. 28.

[59] Lepenye Tamás: A számítási felhők hatása az IT versenyhelyzetekre. 2011. 06. 29. http://lepenyet.wordpress.com/2011/06/29/a-szmtsi-felhok-hatsa-az-it-versenyhelyzetekre/. Letöltés ideje: 2011. 10. 23.]

[60] Csökkent a Nokia piaci részesedése. 2011. 08. 11. http://www.168ora.hu/buxa/csokkent-a-nokia-piaci-reszesedese-80570.html. Letöltés ideje: 2011. 10. 23.

[61] Steve Ballmer a felhő alapú számítástechnikában rejlő lehetőségekről: Európa felett az ég. 2010. 11. 18. http://www.microsoft.com/hun/news/rolunkirtak/101118_01.aspx. Letöltés ideje: 2011. 10. 09.

[62] Privacy authorities across Europe approve Microsoft's cloud commitments. 2014. 04. 10. http://blogs.microsoft.com/blog/2014/04/10/privacy-authorities-across-europe-approve-microsofts-cloud-commitments/. Letöltés ideje: 2015. 02. 17.

[63] Smit, Brad: Microsoft adopts first international cloud privacy standard. 2015. 02. 16. http://blogs.microsoft.com/on-the-issues/2015/02/16/microsoft-adopts-first-international-cloud-privacy-standard/. Letöltés ideje: 2015. 02. 17.

[64] Megoldás a forráshiányra: felhő alapú IT szolgáltatás. 2010. 10. 14. http://hirek.prim.hu/cikk/79490/. Letöltés ideje: 2011. 10. 07.

[65] Tiger Szabolcs: Felhő alapú szolgáltatás. 2011. 03. 30. http://www.naplo-online.hu/kronika/20110330_felho_szolgaltatas. Letöltés ideje: 2011. 10. 07.

[66] Sreedhar, Suhas: Seven Cloud Computing Trends In 2014. 2013. 12. 10. http://www.forbes.com/sites/sungardas/2013/12/10/seven-cloud-computing-trends-in-2014/. Letöltés ideje: 2015.. 01. 11.

[67] Wirthman, Lisa: How The Top 5 Cloud Trends Of 2014 Will Impact The Enterprise In 2015. 2015. 01. 08. http://www.forbes.com/sites/centurylink/2015/01/08/how-the-top-5-cloud-trends-of-2014-will-impact-the-enterprise-in-2015/. Letöltés ideje: 2015. 01. 11.

[68] Five Cloud Computing Trends Affecting Cloud Strategy Through 2015. http://www.itbusinessedge.com/slideshows/show.aspx?c=95261. Letöltés ideje: 2015. 01. 11.

[69] Davidi, Adam: Experts outline key cloud computing trends for 2014. 2013. 12. 09. http://www.theguardian.com/media-network/media-network-blog/2013/dec/09/experts-cloud-computing-trends-2014. Letöltés ideje: 2015.. 01. 11.

[70] Gartner Identifies the Top 10 Strategic Technology Trends for 2015. 2014. 10. 08. http://www.gartner.com/newsroom/id/2867917. Letöltés ideje: 2015. 01. 11.

[71] Top 9 Cloud Computing Predictions for 2015. http://www.information-management.com/gallery/Cloud-Computing-Predictions-2015-Forrester-10026294-1.html. Letöltés ideje: 2015. 01. 11.

[72] Kovács Zoltán: „Electronic Written Tasking Order System" Accomplished Within the Project „Secure Electronic Communication" I.. 2013. szeptember, Hadmérnök, VIII. Évfolyam 3. szám. pp. 171-183. ISSN 1788-1919.

[73] Kovács Zoltán: „Electronic Written Tasking Order System” Accomplished Within the Project „Secure Electronic Communication” II.. 2013. december, Hadmérnök, VIII. Évfolyam 4. szám. pp. 201-209. ISSN 1788-1919.

[74] Kovács Zoltán: „Electronic Written Tasking Order System” Accomplished Within the Project „Secure Electronic Communication” III.. 2014. március, Hadmérnök, IX. Évfolyam 1. szám. pp. 199-208. ISSN 1788-1919.

[75] Security Framework for Governmental Clouds. 2014. 12. 12. https://www.enisa.europa.eu/activities/Resilience-and-CIIP/cloud-computing/govenmental-cloud-security/security-framework-for-govenmental-clouds. Letöltés ideje: 2015. 01. 23.

[76] Wang, Chenxi: Cloud Security Front And Center. 2009. 11. 18. http://blogs.forrester.com/security_and_risk/2009/11/cloud-security-front-and-center.html. Letöltés ideje: 2011. 10. 23.

[77] Number of monthly active Facebook users worldwide from 3rd quarter 2008 to 3rd quarter 2014 (in millions). 2015. http://www.statista.com/statistics/264810/number-of-monthly-active-facebook-users-worldwide/. Letöltés ideje: 2015. 01. 11.

[78] Essers, Loek: Dropbox learns Dutch, Swedish, Danish and Thai in international expansion. 2014. 06. 14. http://www.pcworld.com/article/2364400/dropbox-learns-dutch-swedish-danish-and-thai-in-international-expansion.html. Letöltés ideje: 2015.. 01. 11.

[79] Hong, Kaylene: Dropbox reaches 300m users, adding on 100m users in just six months. 2014. 05. 29. http://thenextweb.com/insider/2014/05/29/dropbox-reaches-300m-users-adding-100m-users-just-six-months/. Letöltés ideje: 2015. 01. 11.

[80] Andras, Sonja Hegman: DataPoint: Microsoft’s Skype DAU has grown 82 percent in a year. 2014. 02. 03. http://www.insidefacebook.com/2014/02/03/datapoint-microsofts-skype-dau-gains-82-from-a-year-ago-mau-gains-just-1-25/. Letöltés ideje: 2015. 01. 11.

[81] Woollaston, Victoria: Revealed, what happens in just ONE minute on the internet: 216,000 photos posted, 278,000 Tweets and 1.8m Facebook likes. 2013. 07. 30. http://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. Letöltés ideje: 2015. 03. 09.

[82] Kovács Zoltán: Felhő alapú informatikai rendszerek potenciális alkalmazhatósága a rendvédelmi szerveknél. 2011. december, Hadmérnök, VI. Évfolyam 4. szám. pp. 176-188. ISSN 1788-1919.

[83] Muha Lajos: Az informatikai biztonság egy lehetséges rendszertana. 2008. Bolyai Szemle, XVII. évfolyam 4. szám. pp. 137-156. ISSN 1416-1443.

[84] Cloud Security Alliance: about. https://cloudsecurityalliance.org/about/. Letöltés ideje: 2015. 02. 21.

[85] Security Guidance for Critical Areas of Focus in Cloud Computing V3.0. 2011. https://cloudsecurityalliance.org/guidance/csaguide.v3.0.pdf. Letöltés ideje: 2012. 01. 05.

[86] Defined Categories of Service 2011. 2011. https://cloudsecurityalliance.org/wp-content/uploads/2011/09/SecaaS_V1_0.pdf. Letöltés ideje: 2012. 01. 05.

[87] The Notorious Nine Cloud Computing Top Threats in 2013. 2013. 02. https://downloads.cloudsecurityalliance.org/initiatives/top_threats/The_Notorious_Nine_Cloud_Computing_Top_Threats_in_2013.pdf. Letöltés ideje: 2014. 09. 21.

[88] Cloud Controls Matrix v3.0.1. 2014. 07. 11. https://cloudsecurityalliance.org/research/ccm/#_downloads. Letöltés ideje: 2014. 09. 17.

[89] Cloud Controls Matrix v3.0.1 Info Sheet. 2014. 07. 29. https://cloudsecurityalliance.org/download/cloud-controls-matrix-v3-0-1-info-sheet/. Letöltés ideje: 2014. 09. 17.

[90] National Institute of Standards and Technology. http://www.nist.gov/. Letöltés ideje: 2014. 09. 21.

[91] NIST Cloud Computing Related Publications. http://www.nist.gov/itl/cloud/publications.cfm. Letöltés ideje: 2014. 09. 21.

[92] Jansen, Wayne – Grance, Timothy: Guidelines on Security and Privacy in Public Cloud Computing. 2011. 12. http://csrc.nist.gov/publications/nistpubs/800-144/SP800-144.pdf. Letöltés ideje: 2014. 09. 21.

[93] Cryptographic Key Management Projekt. http://csrc.nist.gov/groups/ST/key_mgmt/. Letöltés ideje: 2015. 10. 15.

[94] cloud.cio.gov - One Stop Source for Federal Cloud Computing Information. http://cloud.cio.gov/. Letöltés ideje: 2014. 10. 25.

[95] FedRAMP. http://cloud.cio.gov/fedramp. Letöltés ideje: 2014. 10. 25.

[96] FedRAMP Security Assessment Framework. 2014. 06. 06. cloud.cio.gov/sites/default/files/documents/files/FedRAMP%20Security%20Assessment%20Fra. Letöltés ideje: 2015. 01. 17.

[97] FedRAMP Continuous Monitoring Strategy & Guide. 2014. 06. 06. http://cloud.cio.gov/document/continuous-monitoring-strategy-guide. Letöltés ideje: 2014. 10. 25.

[98] System Security Plan (Template). http://cloud.cio.gov/document/system-security-plan. Letöltés ideje: 2015. 01. 17.

[99] https://www.bsi.bund.de/EN/Home/home_node.html. Letöltés ideje: 2014. 09. 21.

[100] Cross Reference Table threats and safeguards for module cloud management. 2013. 12. 09. https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Grundschutz/download/PreliminaryVersions/Module_Cloud_Management_Cross_Reference_Table.html. Letöltés ideje: 2014.. 09. 21.

[101] ENISA. https://www.enisa.europa.eu/. Letöltés ideje: 2014. 11. 12.

[102] Cloud Computing: Benefits, risks and recommendations for information security. 2009. 11. https://www.enisa.europa.eu/activities/risk-management/files/deliverables/cloud-computing-risk-assessment. Letöltés ideje: 2014. 11. 12.

[103] Microsoft Officially Welcomes Skype. 2011. 10. 13. http://news.microsoft.com/2011/10/13/microsoft-officially-welcomes-skype/. Letöltés ideje: 2013. 06. 13.

[104] Romanski, Hilton: Cisco Announces Intent to Acquire Metacloud. 2014. 09. 17. http://blogs.cisco.com/news/cisco-announces-intent-to-acquire-metacloud. Letöltés ideje: 2015. 01. 26.

[105] Ulysses: Megszűnik az Ubuntu One szolgáltatás. 2014. 04. 02. http://ubuntu.hu/node/37398. Letöltés ideje: 2015. 01. 26.

[106] Termination of Free Storage. https://cdn.wuala.com/files/termination_free_storage.pdf. Letöltés ideje: 2015. 01. 26.

[107] Resilience Metrics. http://www.enisa.europa.eu/activities/Resilience-and-CIIP/Incidents-reporting/metrics/metrics. Letöltés ideje: 2014. 11. 18.

[108] Cloud Computing - Information Assurance Framework. 2009. 11. https://www.enisa.europa.eu/activities/risk-management/files/deliverables/cloud-computing-information-assurance-framework?searchterm=Information+Assurance+. Letöltés ideje: 2014. 11. 12.

[109] Cloud Computing. https://www.enisa.europa.eu/activities/Resilience-and-CIIP/cloud-computing/introduction-to-cloud-computing. Letöltés ideje: 2014. 11. 12.

[110] Silverstone, Ariel: Clear Metrics for Cloud Security? Yes, Seriously. 2009. 11. 17. http://www.csoonline.com/article/507823/clear-metrics-for-cloud-security-yes-seriously?page=1. Letöltés ideje: 2012. 01. 02.

[111] Cox, Phil: Intrusion detection in a cloud computing environment. http://searchcloudcomputing.techtarget.com/tip/Intrusion-detection-in-a-cloud-computing-environment. Letöltés ideje: 2012. 01. 02.

[112] Brodkin, Jon: Gartner: Seven cloud-computing security risks. 2008. 07. 02. http://www.infoworld.com/d/security-central/gartner-seven-cloud-computing-security-risks-853?page=0,0. Letöltés ideje: 2012. 01. 02.

[113] Cox, Phil: Securing data in the cloud. http://searchcloudcomputing.techtarget.com/tip/Securing-data-in-the-cloud. Letöltés ideje: 2012. 01. 02.

[114] Gilbert, Francoise: Ten key provisions in cloud computing contracts. http://searchcloudsecurity.techtarget.com/tip/Ten-key-provisions-in-cloud-computing-contracts. Letöltés ideje: 2012. 01. 02.

[115] Foran, Joseph: 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. Letöltés ideje: 2012. 01. 02.

[116] Ristenpart, Thomas – Tromer, Eran – Shacham, Hovav – Savage, Stefan: 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. ACM. New York, NY, USA 2009. pp. 199–212. ISBN: 978-1-60558-894-0 http://cseweb.ucsd.edu/~hovav/dist/cloudsec.pdf. Letöltés ideje: 2011. 11. 05.

[117] Chow, Richard – Golle, Philippe – Jakobsson, Markus – Shi, Elaine – Staddon, Jessica – Masuoka, Ryusuke – Molina, Jesus: Controlling Data in the Cloud: Outsourcing Computation without Outsourcing Control. In CCSW '09 Proceedings of the 2009 ACM workshop on Cloud computing security ACM. New York, NY, USA 2009. pp. 85-90. ISBN: 978-1-60558-784-4 http://www.parc.com/publication/2335/controlling-data-in-the-cloud.html. Letöltés ideje: 2011. 11. 05.

[118] Chen, Yanpei – Paxson, Vern – Katz, Randy H.: What's New About Cloud Computing Security? Technical Reports. Electrical Engineering and Computer Sciences University of California at Berkeley. 2010. 01. 20.. www.eecs.berkeley.edu/Pubs/TechRpts/2010/EECS-2010-5.pdf. Letöltés ideje: 2011. 11. 05.

[119] Jamil, Danish – Zaki, Hassan: Cloud Computing Security. International Journal of Engineering Science and Technology. Vol. 3 No. 4. 2011. 04. pp. 3478-3483. ISSN 0975-5462 www.ijest.info/docs/IJEST11-03-04-129.pdf. Letöltés ideje: 2011. 11. 05.

[120] Wang, Chenxi: Cloud Security Front And Center. 2009. 11. 18 http://blogs.forrester.com/security_and_risk/2009/11/cloud-security-front-and-center.html. Letöltés ideje: 2011. 10. 23.

[121] Preimesberger, Chris: Cloud Computing: Cloud Computing Security: 10 Ways to Enforce It. 2011. 07. 06. http://www.eweek.com/c/a/Cloud-Computing/Cloud-Computing-Security-10-Ways-to-Enforce-It-292589/. Letöltés ideje: 2011. 11. 05.

[122] Cloud Computing and Information Policy: Computing in a Policy Cloud? Jaeger, Paul T., Lin, Jimmy és Grimes, Justin M. 3, 2008., Journal of Information Technology & Politics, 5. pp. 269-283. ISSN 1933-169X.

[123] 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. Letöltés ideje: 2011. 11. 05.

[124] Securing Microsoft's Cloud Infrastructure. http://www.globalfoundationservices.com/security/. Letöltés ideje: 2011. 11. 05.

[125] Intel's Vision of the Ongoing Shift to Cloud Computing. http://charltonb.typepad.com/papers/Cloud Vision.pdf. Letöltés ideje: 2011. 12. 03.

[126] Virtualization and Cloud Computing: Security Best Practice. http://us.trendmicro.com/imperia/md/content/us/trendwatch/researchandanalysis/final_cloud_virt_best_practice.pdf. Letöltés ideje: 2011. 11. 05.

[127] Buecker, Axel – Lodewijkx, Koos – Moss, Harold – Skapinetz, Kevin – Waidner, Michael: Cloud Security Guidance (IBM Recommendations for the Implementation of Cloud Security) Redpaper. 2009. 11. 02. http://www.redbooks.ibm.com/redpieces/abstracts/redp4614.html?Open&pdfbookmar. Letöltés ideje: 2012. 01. 02.

[128] Dobák Imre - Kovács Zoltán: Új technológiák hatása a hírszerzésre. In: A nemzetbiztonság általános elmélete. Szerk.: Dobák Imre. Nemzeti közszolgálati Egyetem Nemzetbiztonsági Intézet. Budapest 2014. pp. 206-220. ISBN: 978-615-5305-49-8

[129] Haig Zsolt: Információ - társadalom - biztonság. Budapest. NKE Szolgáltató Kft., 2015. ISBN 978-615-5527-08-1

[130] Kovács Zoltán: Felhő alapú rendszerek törvényes ellenőrzési problémái. 2013. március, Hadmérnök, VIII. Évfolyam 1. szám. pp. 233 – 241. ISSN 1788-1919.

[131] IPadet kapnak a kormány tagjai. 2011. 04. 27. http://www.hir24.hu/belfold/2011/04/27/ipadet-kapnak-a-kormany-tagjai/?beuszo. Letöltés ideje: 2014. 02. 22.

[132] iPadet kapnak a brit képviselők. 2012. 03. 28. http://beszeljukmac.com/index.php/weblog/comments/ipadet_kapnak_a_brit_kepviselok/. Letöltés ideje: 2014. 02. 22.

[133] Hackertámadás érte a Bank Austriát. 2013. 05. 09. http://www.vg.hu/penzugy/hackertamadas-erte-a-bank-austriat-403251. Letöltés ideje: 2014. 02. 17.

[134] Kaszás Endre: Netbankolás közben jött a hackertámadás. 2013. 01. 09. http://www.bama.hu/baranya/kek-hirek-bulvar/netbankolas-kozben-jott-a-hackertamadas-478955. Letöltés ideje: 2014. 02. 17.

[135] Adathalász e-mailekkel támadják az OTP Bank ügyfeleit. 2014. 01. 30. http://hirek.prim.hu/cikk/102848/. Letöltés ideje: 2014. 02. 17.

[136] Macaskill, Ewen – Dance, Gabriel: NSA Files: Decoded. 2013. 11. 01. http://www.theguardian.com/world/interactive/2013/nov/01/snowden-nsa-files-surveillance-revelations-decoded#section/1. Letöltés ideje: 2014. 02. 17.

[137] Haig Zsolt – Kovács László: Kritikus infrastruktúrák és kritikus információs infrastruktúrák (Tanulmány). Nemzeti Közszolgálati Egyetem, 2012.

[138] Chorley, Matt: iPads banned from Cabinet meetings over fears Chinese spies could use them as covert bugs to listen in on ministers. 2013. 11. 04. http://www.dailymail.co.uk/news/article-2487026/iPads-banned-Cabinet-meetings-Chinese-spying-fears.html Letöltés ideje: 2014. 02. 17.

[139] Kovács Zoltán: Cloud Security in Terms of the Law Enforcement Agencies. 2012. március, Hadmérnök, VII. Évfolyam 1. szám. pp. 144 - 156. ISSN 1788-1919.

[140] 1139/2013. (III. 21.) Korm. határozat Magyarország Nemzeti Kiberbiztonsági Stratégiájáról. Magyar Közlöny 47. szám 2013. március 21. pp. 6338 – 6342http://www.kozlonyok.hu/nkonline/MKPDF/hiteles/MK13047.pdf. Letöltés ideje: 2014. 02. 17.

[141] 2013. évi L. törvény Az állami és önkormányzati szervek elektronikus információbiztonságáról. Magyar Közlöny 69. szám 2013. április 25. pp. 50241 –

50255. http://kozlonyok.hu/nkonline/MKPDF/hiteles/MK13069.pdf. Letöltés ideje: 2014. 02. 17.

[142] Kristóf Csaba: Kulcskérdés a BYOD összehangolása a biztonsággal. 2013. 07. 26. http://bitport.hu/kulcskerdes-a-byod-oesszehangolasa-a-biztonsaggal Letöltés ideje: 2014. 02. 17.]

[143] A Dell innovatív szoftverei a BYOD, a Big Data és az IT biztonság kérdéseire adnak választ. 2013. 12. 12. http://www.dell.com/learn/hu/hu/hucorp1/press-releases/2013-12-12-dell-sajtokozlemeny-dell-world-dsg. Letöltés ideje: 2014. 02. 17.

[144] Balogh B. Jenő: Világméretű probléma a BYOD biztonságának hiánya. 2014. 01. 24. http://biztonsagpiac.hu/vilagmeretu-problema-a-byod-biztonsaganak-hianya. Letöltés ideje: 2014. 02. 17.

[145] Balogh B. Jenő: Nagy biztonsági kockázat a BYOD. 2013. 07. 14. http://biztonsagpiac.hu/nagy-biztonsagi-kockazat-a-byod. Letöltés ideje: 2014. 02. 17.

[146] Heskett, Stephen: Technical Surveillance Countermeasures (TSCM) Frequently Asked Questions. http://www.msainvestigations.com/tscm-faqs/bug-sweep/eavesdropping-Fequently-asked-questions/new-york#subjectSpying. Letöltés ideje: 2014. 02. 18.

[147] Department of Defense Instruction. (Subject: Technical Surveillance Countermeasures (TSCM) Program). Number 5240.05, 2006. 02. 22. http://www.dtic.mil/whs/directives/corres/pdf/524005p.pdf. Letöltés ideje: 2014. 02. 18.

[148] Sallai Gyula – Abos Imre: A távközlés, információ- és médiatechnológia konvergenciája. Magyar Tudomány. Infokommunikációs hálózatok. 168. Évfolyam. 2007. július pp. 844-851. ISSN 1588-1245

[149] dropbox.com. https://www.dropbox.com/. Letöltés ideje: 2014. 03. 14.

[150] Smith, Craig: How Many People Use 415 of the Top Social Media, Apps & Tools? 2014. 03. http://expandedramblings.com/index.php/resource-how-many-people-use-the-top-social-media/#.UyKrEvl5Ph5. Letöltés ideje: 2014. 03. 14.

[151] Top 15 Most Popular Social Networking Sites | March 2014. 2014. 03. http://www.ebizmba.com/articles/social-networking-websites. Letöltés ideje: 2014. 03. 14.

[152] McGee, Matt: Google Is Most Visited Site Of 2013, Despite Big Drops In Desktop Traffic [Nielsen]. 2013. 12. 16. http://marketingland.com/google-is-most-visited-site-of-2013-despite-big-drops-in-desktop-traffic-nielsen-68235. Letöltés ideje: 2014. 03. 14.

[153] Petrányi-Széll András: Közösségi élet a Facebookon túl. 2014. 03. 06. http://psprovocative.com/kozossegi-elet-facebookon-tul/. Letöltés ideje: 2014. 03. 14.

[154] Tóth Balázs: Az asztali pc-nek befellegzett. 2012. 08. 19. http://index.hu/tech/2012/08/19/az_asztali_pc-nek_befellegzett/. Letöltés ideje: 2015. 04. 11.

[155] Bodnár Ádám: Alig vesz PC-t a magyar lakosság. 2014. 05. 07. http://www.hwsw.hu/hirek/52244/idc-pc-notebook-tablet-piac-asus-lenovo-hp-dell-acer-concorde-samsung-apple.html. Letöltés ideje: 2015. 04. 11.

[156] A Sony bemutatta legújabb tablet-notebook eszközeit. 2013. 10. 30. http://androbit.net/news/3877/a_sony_bemutatta_legujabb_tablet_notebook_eszkozeit.html. Letöltés ideje: 2014. 02. 22.

[157] http://www.apple.com/hu/ipad-air/specs/. Letöltés ideje: 2014. 02. 22.

[158] http://www.samsung.com/hu/consumer/mobile-phone/mobile-phones/galaxy-note/SM-N9005ZKEXEH-spec. Letöltés ideje: 2014. 02. 22.

[159] http://www.asus.com/hu/Notebooks_Ultrabooks/TAICHI_31/#specifications. Letöltés ideje: 2014. 02. 22.

[160] Gruman, Galen: The real reason Obama can't swap his BlackBerry for an iPhone. 2013. 12. 12. http://www.infoworld.com/d/mobile-technology/the-real-reason-obama-cant-swap-his-blackberry-iphone-232525. Letöltés ideje: 2014. 02. 22.

[161] Kovács Zoltán: Felhõ-alapú informatikai rendszerek, mint nemzetbiztonsági kihívás. 2013. március, Hadtudomány, XXIII. Évfolyam 1-2. szám. pp. 5 – 12. ISSN 1215-4121.

[162] Haig Zsolt – Kovács László – Ványa László – Vass Sándor: Elektronikai hadviselés. Budapest. Nemzeti Közszolgálati Egyetem, 2014. ISBN 978-615-5305-87-0

[163] Ügyfelek tízezreinek adatait lopták el egy brit nagybanktól. 2014. 01. 20. http://sg.hu/cikkek/103209/ugyfelek-tizezreinek-adatait-loptak-el-egy-brit-nagybanktol. Letöltés ideje: 2014. 03. 24.

[164] Haig Zsolt – Várhegyi István: Információs Műveletek. II. kötet Információs műveletek tartalma. Budapest. Zrínyi Miklós Nemzetvédelmi Egyetem, 2004. Egyetemi jegyzet

[165] Balogh Artúrt Gavráék sem tolerálták. 2014. 02. 14. http://mno.hu/magyar_nemzet_belfoldi_hirei/balogh-arturt-gavraek-sem-toleraltak-1210883. Letöltés ideje: 2014. 03. 24.

[166] Kovács László – Illési Zsolt: Cyberhadviselés. In MHTT-KONFERENCIA - Az információs hadviselés és a hadtudomány. Hadtudomány, 2011. XXI. Évfolyam 1-2. szám. pp. 29-41. ISSN 1215-4121

[167] Kovács Zoltán: Felhő alapú rendszerek törvényes ellenőrzési módszerei vizsgálata I. 2013. szeptember, Hadmérnök, VIII. Évfolyam 3. szám. pp. 184 – 197. ISSN 1788-1919.

[168] Kovács Zoltán: Felhő alapú rendszerek törvényes ellenőrzési módszerei vizsgálata II. 2013. szeptember, Hadmérnök, VIII. Évfolyam 3. szám. pp. 198 – 210. ISSN 1788-1919.

[169] Kovács Zoltán: Hordozható infokommunikációs eszközök használatának veszélyei a védett vezetők biztonságtudatossági képzésének szempontjából I. 2014. június, Hadmérnök, IX. Évfolyam 2. szám. pp. 277 – 289. ISSN 1788-1919.

[170] Kovács Zoltán: Védett vezetők hordozható infokommunikációs eszközeinek védelme a rádiófrekvenciás tartományban. 2014. Bolyai Szemle, XXIII. Évfolyam 2014/4. szám. pp. 58-75. ISSN 1416-1443.

[171] Kovács László: Kiberháború? Internetes támadások a Wikileaks ellen és mellett. Nemzet és biztonság, 2011/1 szám. pp. 3-8. ISSN 1789-5286

[172] Generations Defined. McCrindle Research 2012. 2012. http://mccrindle.com.au/resources/Generations-Defined-Sociologically.pdf. Letöltés ideje: 2013. 02. 09.

[173] X, Y, Z: Generációk a világháló vonzásában 2011. 12. 18. http://www.intergeneracio.hu/2011/12/18/x-y-z-generaciok-a-vilaghalo-vonzasaban/. Letöltés ideje: 2013. 02. 07.

[174] 2003. évi C. törvény az elektronikus hírközlésről. http://net.jogtar.hu/jr/gen/hjegy_doc.cgi?docid=A0300100.TV. Letöltés ideje: 2013. 02. 09.

[175] Molnár Gábor – Zalatnay Zsolt: Szolgáltatások és architektúrák Skype előadás. www.tmit.bme.hu/dl239. Letöltés ideje: 2013. 02. 13.

[176] http://newsroom.fb.com/Timeline. Letöltés ideje: 2013. 02. 15.

[177] https://www.facebook.com/zuck/posts/10100518568346671. Letöltés ideje: 2013. 02. 15.

[178] Gazdag Tibor – Kovács Zoltán: Felhő alapú új pénzügyi tranzakciós lehetőségek és azok veszélyei. 2014. június, Nemzetbiztonsági Szemle, II. Évfolyam 2. szám. pp. 36-57. ISSN 2064-3756.

[179] Dajkó Pál: A Google fizet Franciaországban: megtört a netsemlegesség? 2013. 01. 22. http://itcafe.hu/hir/google_orange_netsemlegesseg.html. Letöltés ideje: 2013. 02. 09.

[180] Gálffy Csaba: A Google már fizet a francia internetszolgáltatónak. 2013. 01. 21. http://www.hwsw.hu/hirek/49670/google-france-telecom-orange-afrika-okostelefon-youtube-android.html. Letöltés ideje: 2013. 02. 09.

[181] Koi Tamás: Skype: az internet nem a mobilszolgáltatóké! 2010. 04. 26. http://www.hwsw.hu/hirek/44435/voip-skype-mobil-internet-halozat-mobiltelefon.html. Letöltés ideje: 2013. 02. 09.

[182] Dajkó Pál: A Google továbbra sem ad ki adatokat a magyar kormánynak 2013. 01. 24. http://itcafe.hu/hir/google_atlathatosag_transparency.html. Letöltés ideje: 2013. 02. 09.

[183] Elektronikus hírközlési szolgáltatások új hatósági osztályozása – lista 2012.02.13. 16:14 • Forrás: Szolgáltatásbejelentési osztály, Nyilvántartási és tájékoztatási főosztály. http://nmhh.hu/dokumentum/448/szolgaltatas_hierarchia_20081009.pdf. Letöltés ideje: 2013. 02. 19.

[184] Szolgáltatások osztályozása - fogalmak 2012.02.13. 16:13 • Forrás: Szolgáltatásbejelentési osztály, Nyilvántartási és tájékoztatási főosztály. http://nmhh.hu/dokumentum/448/szolgaltatas_hierarchia_20081009.pdf. Letöltés ideje: 2013. 02. 19.

[185] Molnár Sándor – Perényi Marcell: On the identification and analysis of Skype traffic. 2011. 1., International Journal of Communication Systems in Wiley Online Library, 24. pp. 94-117. http://hsnlab.tmit.bme.hu/~molnar/files/ijcs2010.pdf. ISSN: 1099-1131. Letöltés ideje: 2013. 06. 18.

[186] Baset, Salman A. – Schulzrinne, Henning: An Analysis of the Skype Peer-to-Peer Internet Telephony Protocol. IEEE, 2006. INFOCOM 2006. 25th IEEE International Conference on Computer Communications. Proceedings. pp.: 1-11. http://www1.cs.columbia.edu/~library/TR-repository/reports/reports-2004/cucs-039-04.pdf. ISSN 0743-166X; Print ISBN 1-4244-0221-2. Letöltés ideje: 2013. 06. 18.

[187] Does Skype use encryption? https://support.skype.com/en/faq/FA31/does-skype-use-encryption. Letöltés ideje: 2013. 07. 11.

[188] Swisher, Kara: Done Deal: Microsoft to Buy Skype for $8.5 Billion in Cash. 2011. 05. 10. http://allthingsd.com/20110510/done-deal-microsoft-to-buy-skype-for-8-5-billion-in-cash/. Letöltés ideje: 2013. 06. 17.

[189] Az EU jóváhagyta a Microsoft Skype-felvásárlását. 2011. 10. 07. http://www.origo.hu/techbazis/20111007-az-europai-bizottsag-jovahagyta-a-microsoft-skypefelvasarlasat.html. Letöltés ideje: 2013. 06. 17.

[190] Bodnár Ádám: A Microsoft megvette a Skype-ot. 2011. 05. 10. http://www.hwsw.hu/hirek/46667/microsoft-skype-voip-telefon-felvasarlas.html. Letöltés ideje: 2013. 06. 17.

[191] miskolczy_cs: Miért jó a Skype a Microsoftnak? 2011. 05. 12. http://insiderblog.hu/kulfold/2011/05/12/skype/. Letöltés ideje: 2013. 06. 17.

[192] Skype does away with random supernodes. 2012. 05. 01. http://expertmiami.blogspot.hu/2012/05/skype-does-away-with-random-supernodes.html. Letöltés ideje: 2013. 06. 18.

[193] djwm: Skype with care – Microsoft is reading everything you write. 2013. 05. 14. http://www.h-online.com/security/news/item/Skype-with-care-Microsoft-is-reading-everything-you-write-1862870.html. Letöltés ideje: 2013. 06. 18.

[194] Schmidt, Jürgen: Skype's ominous link checking: Facts and speculation. 2013. 05. 17. http://www.h-online.com/security/features/Skype-s-ominous-link-checking-Facts-and-speculation-1865629.html. Letöltés ideje: 2013. 06. 18.

[195] Solovjovs, Kirils: On Skype URL eavesdropping. 2013. 05. 17. http://seclists.org/fulldisclosure/2013/May/78. Letöltés ideje: 2013. 06. 18.

[196] Poitras, Laura – Gellman, Barton: U.S., British intelligence mining data from nine U.S. Internet companies in broad secret program. 2013. 06. 07. http://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. Letöltés ideje: 2013. 06. 28.

[197] Betilthatják Oroszországban a Skype-ot, a Gmailt és a Hotmailt. 2011. 04. 09. http://sg.hu/cikkek/81250/betilthatjak_oroszorszagban_a_skype_ot_a_gmailt_es_a_hotmailt. Letöltés ideje: 2013.. 06. 18.

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

[199] Berta Sándor: Lehallgathatják az oroszok a Skype-ot. 2011. 06. 11. http://sg.hu/cikkek/82579/lehallgathatjak_az_oroszok_a_skype_ot. Letöltés ideje: 2013. 06. 18.

[200] Berta Sándor: Évek óta lehallgatható Oroszországban a Skype. 2013. 03. 18. http://sg.hu/cikkek/96074/evek_ota_lehallgathato_oroszorszagban_a_skype. Letöltés ideje: 2013. 06. 18.

[201] Silver, Vernon: Cracking China's Skype Surveillance Software. 2013. 03. 08. http://www.bloomberg.com/bw/articles/2013-03-08/skypes-been-hijacked-in-china-and-microsoft-is-o-dot-k-dot-with-it. Letöltés ideje: 2013. 06. 20.

[202] Koi Tamás: Egyre nagyobb a nyomás Európában a Skype-on. 2013. 03. 13. http://www.hwsw.hu/hirek/49958/skype-microsoft-franciaorszag-arcep-voip.html. Letöltés ideje: 2013. 06. 20.

[203] Skype Refuses to Register as an Operator. 2013. 03. 12. 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. Letöltés ideje: 2013. 06. 20.

[204] Berta Sándor: Mindenki lehallgatható lenne Németországban. 2008. 01. 17. http://sg.hu/cikkek/57484/mindenki_lehallgathato_lenne_nemetorszagban. Letöltés ideje: 2013. 06. 24.

[205] Dajkó Pál: A német rendőröknek egyelőre tilos a hackelés. 2007. 02. 06. http://itcafe.hu/hir/a_nemet_rendoroknek_egyelore_tilos_a_hackeles.html. Letöltés ideje: 2013. 06. 24.

[206] Dajkó Pál: Új alkotmányos jog született: az IT-jog. 2008. 03. 01. http://itcafe.hu/hir/bundestrojaner_alkotmany_itjog.html. Letöltés ideje: 2013. 06. 24.

[207] Dajkó Pál: Lebukott az állami kémprogram. 2011. 10. 10. http://itcafe.hu/hir/chaos_computer_club_nemetorszag_bundestrojaner.html. Letöltés ideje: 2013. 06. 24.

[208] Chaos Computer Club analyzes government malware. 2011. 10. 08. http://ccc.de/en/updates/2011/staatstrojaner. Letöltés ideje: 2013. 06. 24.

[209] Meister, Andre: Secret Government Document Reveals: German Federal Police Plans To Use Gamma FinFisher Spyware. 2013. 01. 16. https://netzpolitik.org/2013/secret-government-document-reveals-german-federal-police-plans-to-use-gamma-finfisher-spyware/. Letöltés ideje: 2013. 06. 28.

[210] https://netzpolitik.org/wp-upload/BMI-Bericht-Sachstand-CC-TK%C3%9C.pdf. Letöltés ideje: 2013. 06. 28.

[211] ehe: Superintendent Trojan. 2006. 10. 09. http://www.h-online.com/security/news/item/Superintendent-Trojan-731613.html. Letöltés ideje: 2013. 06. 28.

[212] Cyberperquisitions. 2008. 02. 28. http://www.lemonde.fr/idees/article/2008/02/28/cyberperquisitions_1016773_3232.html Letöltés ideje: 2013. 06. 28.

[213] Ausztriában törvényes lesz az online házkutatás. 2007. 10. 18. http://sg.hu/cikkek/55658/ausztriaban_torvenyes_lesz_az_online_hazkutatas. Letöltés ideje: 2013. 06. 28.

[214] Berta Sándor: Külföldi szervereket is megtámadhat a holland rendőrség. 2013. 05. 06. http://sg.hu/cikkek/97134/kulfoldi_szervereket_is_megtamadhat_a_holland_rendorseg. Letöltés ideje: 2013. 06. 28.

[215] McCullagh, Declan: FBI remotely installs spyware to trace bomb threat. 2007. 06. 18. http://news.cnet.com/8301-10784_3-9746451-7.html. Letöltés ideje: 2013. 06. 28.

[216] http://www.politechbot.com/docs/fbi.cipav.sanders.affidavit.071607.pdf. Letöltés ideje: 2013. 06. 28.

[217] Gardham, Duncan: Government plans to extend powers to spy on personal computers. 2009. 01. 04. http://www.telegraph.co.uk/news/uknews/law-and-order/4109031/Government-plans-to-extend-powers-to-spy-on-personal-computers.html. Letöltés ideje: 2013. 06. 28.

[218] Golovanov, Sergey: Spyware. HackingTeam. 2013. 04. 23. http://securelist.com/analysis/publications/37064/spyware-hackingteam/. Letöltés ideje: 2013. 06. 28.

[219] Marquis-Boire, Morgan – Marczak, Bill – Guarnieri, Claudio – Scott-Railton, John: For their eyes only. 2013. 05. 01. https://citizenlab.org/storage/finfisher/final/fortheireyesonly.pdf. Letöltés ideje: 2013. 06. 28.

[220] The IP commission report. 2013. 05. http://ipcommission.org/report/IP_Commission_Report_052213.pdf. Letöltés ideje: 2013. 06. 28.

[221] Dubrawsky, Ido: Firewall Evolution - Deep Packet Inspection. 2010. 11. 02. http://www.symantec.com/connect/articles/firewall-evolution-deep-packet-inspection. Letöltés ideje: 2013. 06. 28.

[222] Wawro, Alex: A simple guide to Deep Packet Inspection. 2012. 02. 01. http://features.techworld.com/security/3334780/a-simple-guide-to-deep-packet-inspection/. Letöltés ideje: 2013. 06. 28.

[223] 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. Letöltés ideje: 2013. 06. 28.

[224] Messmer, Ellen: US government's use of deep packet inspection raises serious privacy questions. 2013. 04. 24. http://news.techworld.com/security/3444019/dhs-use-of-deep-packet-inspection-technology-in-new-net-security-system-raises-serious-privacy-questions/. Letöltés ideje: 2013. 06. 28.

[225] MacAskill, Ewen – Borger, Julian – Hopkins, Nick – Davies, Nick – Ball, James: GCHQ taps fibre-optic cables for secret access to world's communications. 2013. 06. 21. http://www.theguardian.com/uk/2013/jun/21/gchq-cables-secret-world-communications-nsa. Letöltés ideje: 2013. 07. 05.

[226] MacAskill, Ewen – Borger, Julian – Hopkins, Nick – Davies, Nick – Ball, James: Mastering the internet: how GCHQ set out to spy on the world wide web. 2013. 06. 21. http://www.theguardian.com/uk/2013/jun/21/gchq-mastering-the-internet. Letöltés ideje: 2013. 07. 05.

[227] Berta Sándor: Németország a felhőadatokat is ellenőrizné. 2013. 04. 07. http://sg.hu/cikkek/96458/nemetorszag_a_felhoadatokat_is_ellenorizne. Letöltés ideje: 2013. 06. 28.

[228] Berta Sándor: Szigorítanák a német távközlési törvényt. 2013. 04. 21. http://sg.hu/cikkek/96798/szigoritanak_a_nemet_tavkozlesi_torvenyt. Letöltés ideje: 2013. 06. 28.

[229] Nakashima, Ellen: Panel seeks to fine tech companies for noncompliance with wiretap orders. 2013. 04. 29. http://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. Letöltés ideje: 2013. 06. 28.

[230] Berta Sándor: Online házkutatásokat indítanának Németországban. 2006. 12. 08. http://sg.hu/cikkek/49079/online_hazkutatasokat_inditananak_nemetorszagban. Letöltés ideje: 2013. 06. 24.

[231] Rouse, Margaret: spyware. 2006. 10. http://searchsecurity.techtarget.com/definition/spyware. Letöltés ideje: 2013. 07. 16.

[232] Spyware. http://www.spywareguide.com/term_show.php?id=12. Letöltés ideje: 2013. 07. 16.

[233] Sanders, Chris: Understanding Man-in-the-Middle Attacks – ARP Cache Poisoning (Part 1). 2010. 03. 17. http://www.windowsecurity.com/articles-tutorials/authentication_and_encryption/Understanding-Man-in-the-Middle-Attacks-ARP-Part1.html. Letöltés ideje: 2013. 07. 16.

[234] Sanders, Chris: Understanding Man-In-The-Middle Attacks – Part2: DNS Spoofing. 2010. 04. 07. http://www.windowsecurity.com/articles-tutorials/authentication_and_encryption/Understanding-Man-in-the-Middle-Attacks-ARP-Part2.html. Letöltés ideje: 2013. 07. 16.

[235] Sanders, Chris: Understanding Man-In-The-Middle Attacks - Part 3: Session Hijacking. 2010. 05. 05. http://www.windowsecurity.com/articles-tutorials/authentication_and_encryption/Understanding-Man-in-the-Middle-Attacks-ARP-Part3.html. Letöltés ideje: 2013. 07. 16.

[236] Sanders, Chris: Understanding Man-In-The-Middle Attacks - Part 4: SSL Hijacking. 2010. 06. 09. http://www.windowsecurity.com/articles-tutorials/authentication_and_encryption/Understanding-Man-in-the-Middle-Attacks-ARP-Part4.html. Letöltés ideje: 2013. 07. 16.

[237] Fisher, Dennis: What is a Man-in-the-Middle Attack? 2013. 04. 10. http://blog.kaspersky.com/man-in-the-middle-attack/. Letöltés ideje: 2013. 07. 16.

[238] DuPaul, Neil: Man-in-the-Middle Tutorial: Learn About Man-in-the-Middle Attacks, Vulnerabilities and How to Prevent MITM Attacks. http://www.veracode.com/security/man-middle-attack. Letöltés ideje: 2013. 07. 16.

[239] Wawro, Alex: What Is Deep Packet Inspection? 2012. 02. 01. http://www.pcworld.com/article/249137/what_is_deep_packet_inspection_.html. Letöltés ideje: 2013. 07. 19.

[240] NSA slides explain the PRISM data-collection program. 2013. 06. 06. http://www.washingtonpost.com/wp-srv/special/politics/prism-collection-documents/. Letöltés ideje: 2013. 06 28.

[241] HTTPS Everywhere. https://www.eff.org/am/https-everywhere. Letöltés ideje: 2013. 06. 28.

[242] https://www.otpbank.hu/portal/hu/OTPdirekt/Home. Letöltés ideje: 2013. 10. 27.

[243] https://www.paypal.com/hu/webapps/mpp/home (2013. 10. 27.). Letöltés ideje: 2013. 10. 27.

[244] http://eu.battle.net/wow/en/. Letöltés ideje: 2013. 10. 27.

[245] http://office.microsoft.com/hu-hu/business/. Letöltés ideje: 2013. 10. 27.

[246] http://www.adobe.com/hu/products/photoshop.html. Letöltés ideje: 2013. 10. 27.

[247] https://maps.google.hu/maps?hl=hu&tab=wl. Letöltés ideje: 2013. 10. 27.

[248] 1995. évi CXXV. törvény a nemzetbiztonsági szolgálatokról. http://www.complex.hu/jr/gen/hjegy_doc.cgi?docid=99500125.TV. Letöltés ideje: 2013. 07. 01.

[249] 1998. évi XIX. törvény a büntetőeljárásról. http://www.complex.hu/kzldat/t9800019.htm/t9800019.htm. Letöltés ideje: 2013. 07. 01.

[250] 1994. évi XXXIV. törvény. a Rendőrségről. http://www.complex.hu/kzldat/t9400034.htm/t9400034_4.htm. Letöltés ideje: 2013. 07. 01.

[251] 2011. évi CLXIII. törvény az ügyészségről. http://net.jogtar.hu/jr/gen/hjegy_doc.cgi?docid=A1100163.TV. Letöltés ideje: 2013. 07. 01.

[252] 2010. évi CXXII. törvény a Nemzeti Adó- és Vámhivatalról. http://net.jogtar.hu/jr/gen/hjegy_doc.cgi?docid=A1000122.TV. Letöltés ideje: 2013. 07. 01.

[253] 180/2004. (V. 26.) Korm. rendelet az elektronikus hírközlési feladatokat ellátó szervezetek és a titkos információgyűjtésre, illetve titkos adatszerzésre felhatalmazott szervezetek együttműködésének rendjéről. http://www.complex.hu/jr/gen/hjegy_doc.cgi?docid=A0400180.KOR. Letöltés ideje: 2013. 07. 01.

[254] 2014. évi XXXIII. törvény az egyes pénzügyi tárgyú törvények módosításáról. http://www.complex.hu/kzldat/t1400033.htm/t1400033.htm#kagy1. Letöltés ideje: 2015. 03. 29.

[255] Magyarországi Tartalomszolgáltatók Egyesületének a tartalomszolgáltatásra vonatkozó működési, etikai és eljárási szabályzata. 2009. 10. 21. http://mte.hu/etikai-kodex/. Letöltés ideje: 2013. 08. 16.

[256] Koltay András – Mayer Annamária – Nyakas Levente – Pogácsás Anett: A médiaszolgáltatás és a sajtótermék fogalma az új magyar médiaszabályozásban. Nemzeti Média- és Hírközlési Hatóság Médiatanácsa és annak Médiatudományi Intézete). http://mediatanacs.hu/dokumentum/1786/1321010932mediaszolgaltatas.pdf. Letöltés ideje: 2013. 10. 27.

[257] 2010. évi CIV. törvény a sajtószabadságról és a médiatartalmak alapvető szabályairól. http://www.complex.hu/jr/gen/hjegy_doc.cgi?docid=A1000104.TV. Letöltés ideje: 2013. 11. 11.

[258] 2010. évi CLXXXV. törvény a médiaszolgáltatásokról és a tömegkommunikációról. http://net.jogtar.hu/jr/gen/hjegy_doc.cgi?docid=A1000185.TV. Letöltés ideje: 2013. 11. 11.

[259] http://www.collinsdictionary.com/dictionary/english/content-provider. Letöltés ideje: 2013. 08. 16.

[260] http://www.oxforddictionaries.com/definition/american_english/content-provider. Letöltés ideje: 2013. 08. 16.

[261] http://www.oxforddictionaries.com/definition/english/content-provider. Letöltés ideje: 2013. 08. 16.

[262] http://www.gartner.com/it-glossary/content-provider/. Letöltés ideje: 2013. 08. 16.

[263] http://dictionary.reference.com/browse/content+provider?s=t. Letöltés ideje: 2013. 08. 16.

[264] http://www.businessdictionary.com/definition/content-provider.html. Letöltés ideje: 2013. 08. 16.

[265] http://encyclopedia2.thefreedictionary.com/content+provider. Letöltés ideje: 2013. 08. 16.

[266] E-önkormányzati stratégiakészítési ajánlás kistérségek és önkormányzatok számára. változat: v1.1. 2009. 04. http://www.google.hu/url?sa=t&rct=j&q=alkalmaz%C3%A1sszolg%C3%A1ltat%C3%B3%20defin%C3%ADci%C3%B3&source=web&cd=1&cad=rja&ved=0CC8QFjAA&url=http%3A%2F%2Fwww.matisz.hu%2Ffileadmin%2Ftemplate%2Fdokumentumok%2Fmatisz%2Fimg%2Flogo%2Fpalyazat-projekt%2FeKozszol. Letöltés ideje: 2013. 08. 24.

[267] http://pcforum.hu/szotar/?term=Alkalmaz%E1s-szolg%E1ltat%F3. Letöltés ideje: 2013. 08. 24.

[268] http://www.humansoft.hu/Alkalmazas_szolgaltatas.html. Letöltés ideje: 2013. 08. 24.

[269] 2001. évi CVIII. törvény az elektronikus kereskedelmi szolgáltatások, valamint az információs társadalommal összefüggő szolgáltatások egyes kérdéseiről. net.jogtar.hu. http://net.jogtar.hu/jr/gen/hjegy_doc.cgi?docid=A0100108.TV. Letöltés ideje: 2014. 09. 07.

[270] http://www.gartner.com/it-glossary/asp-application-service-provider/. Letöltés ideje: 2014. 08. 24.

[271] http://www.gartner.com/it-glossary/casp-content-and-applications-service-provider/. Letöltés ideje: 2013. 08. 24.

[272] http://www.techterms.com/definition/asp. Letöltés ideje: 2013. 08. 24.

[273] http://www.businessdictionary.com/definition/application-service-provider-ASP.html. Letöltés ideje: 2013. 08. 24.

[274] http://dictionary.reference.com/browse/application%20service%20provider?&o=100074&s=t. Letöltés ideje: 2013. 08. 24.

[275] http://encyclopedia2.thefreedictionary.com/application+service+provider. Letöltés ideje: 2013. 08. 24.

[276] http://www.techopedia.com/definition/29145/over-the-top-application-ott. Letöltés ideje: 2014. 06. 09.

[277] http://www.pace.com/global/our-thinking/over-the-top-services-ott/. Letöltés ideje: 2014. 06. 09.

[278] http://www.imediaconnection.com/content/15893.asp#multiview. Letöltés ideje: 2014. 06. 09.

[279] Ganuza, Juan José – Viecens, María Fernanda: Over-the-top (OTT) applications, services and content: implications for broadband infrastructure. Universidad de San Andrés, Centro de Technología y Sociedad. 2013. 02. http://www.udesa.edu.ar/WP/GetFile.aspx?fid=654282. Letöltés ideje: 2014. 06. 09.

[280] http://www.pcmag.com/encyclopedia/term/45481/isp. Letöltés ideje: 2014. 07. 24.

[281] http://dictionary.reference.com/browse/isp. Letöltés ideje: 2014. 07. 24.

[282] http://www.investopedia.com/terms/i/isp.asp. Letöltés ideje: 2014. 07. 24.

[283] http://compnetworking.about.com/od/internetaccessbestuses/g/bldef_isp.htm. Letöltés ideje: 2014. 07. 24.

[284] http://searchwindevelopment.techtarget.com/definition/ISP. Letöltés ideje: 2014. 07. 24.

[285] http://www.parlament.hu/irom40/00264/00264.pdf. Letöltés ideje: 2014. 07. 01.

[286] Ezeket a szerencsejáték-oldalakat kapcsolta le a NAV. 2014. 06. 28. http://www.napi.hu/ado/ezeket_a_szerencsejatek-oldalakat_kapcsolta_le_a_nav.583212.html. Letöltés ideje: 2014. 07. 01.

[287] http://blogs.cisco.com/wp-content/uploads/Seperation-of-Responsibility-in-Cloud.png. Letöltés ideje: 2011. 10. 29.

[288] http://www.saasblogs.com/saas/demystifying-the-cloud-where-do-saas-paas-and-other-acronyms-fit-in/. Letöltés ideje: 2011. 10. 29.

[289] Data Security Lifecycle 2.0. https://securosis.com/blog/data-security-lifecycle-2.0. Letöltés ideje: 2012. 01. 05.

[290] Cloud Computing From the Home. http://www.tutorialspoint.com/shorttutorials/cloud-computing-from-the-home. Letöltés ideje: 2015. 04. 05.

[291] Man-in-the-middle attack. https://www.owasp.org/index.php/Man-in-the-middle_attack Letöltés ideje: 2013. 07. 16.

[292] CS294S Research Project in Computer Security: Skype Proxy (IP over Skype). Stanford University, Applied Cryptography Group. http://crypto.stanford.edu/cs294s/projects/skype.html. Letöltés ideje: 2013. 03. 26.

[293] Oroszi Eszter Diána: Social Engineering: Az emberi erőforrás, mint az információbiztonság kritikus tényezője. Budapesti Corvinus Egyetem Gazdálkodástudományi Kar Számítástudományi Tanszék – diplomamunka. 2008. http://krasznay.hu/presentation/diploma_oroszi.pdf. Letöltés ideje: 2015. 07. 19.

DOI azonosító: 10.17625/NKE.2015.021

Mellékletek

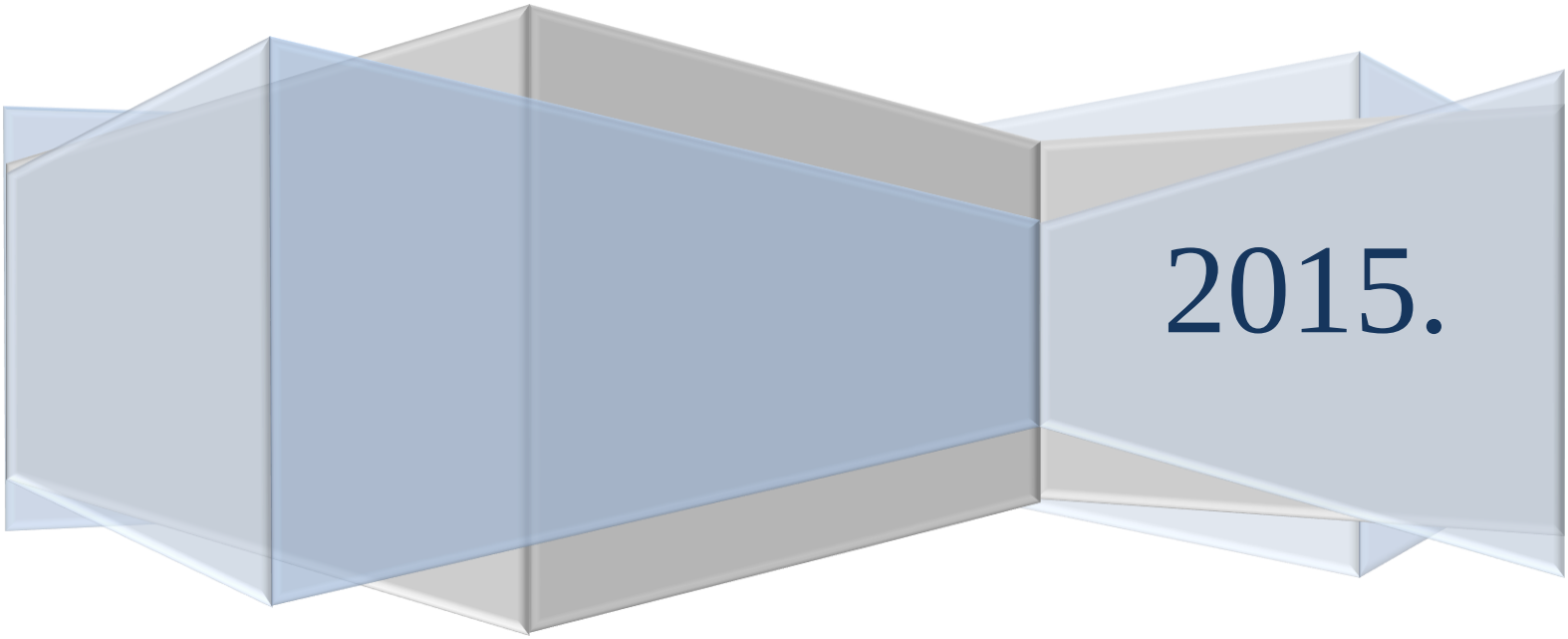
DOI azonosító: 10.17625/NKE.2015.021

1. számú melléklet: Biztonsági sablon felhőszolgáltató megfelelőségének ellenőrzésére – fedőlapok

Biztonsági elemző sablon felhő alapú rendszerek biztonsági értékeléséhez

- rendvédelmi szervek számára

1.0 verzió



DOI azonosító: 10.17625/NKE.2015.021

Sablon felülvizsgálati történet

DÁTUM	LEÍRÁS	VERZIÓSZÁM	SZERZŐ
2015. 03. 13.	Eredeti sablon	1.0	Kovács Zoltán

DOI azonosító: 10.17625/NKE.2015.021

Sablon kitöltési útmutató

- A sablon 3 főcsoportra bomlik, minden főcsoport kitöltése kötelező, azok közül egyik sem hagyható el.
- Az egyes főcsoportokon belül további alcsoportok találhatóak, ezek kitöltése szintén kötelező, azok közül egyik sem hagyható el.
- Minden alcsoporthoz tartozik egy vagy több, szürke színnel kiemelt fő, vagy összegző kérdés, azok kitöltése kötelező, azok közül egyik sem hagyható el.
- Minden alcsoporthoz több, fehér színnel jelzett kérdés tartozik, azok közül a felhasználó döntése alapján egy, vagy akár több is elhagyható.
- Amennyiben a vizsgált szolgáltató valamilyen elfogadott nemzetközi standardnak megfelel (pl. ISO/IEC 27001-2013), akkor a fehér színnel jelzett kérdések közül a standardban kezelt kérdések automatikusan igenlő válasszal beállíthatók, azokat külön nem kell vizsgálni. Ezek a kérdések erősen függnek a standardtól, ezért a megfeleltetés a kérdőív kitöltőjének felelőssége.
- Az egyes kérdésekhez igen/nem válaszok adhatók, ezek közül kizárólag az egyik jelölhető meg.
- A kérdésekre mindenhol az igen válasz jelenti a pozitív eredményt.
- A fehérrel jelölt alcsoporti kérdések esetében a nemleges válasz még nem jelenti automatikusan azt, hogy a vizsgált felhő alapú rendszer nem felel meg a megkívánt biztonsági követelményeknek. Ugyanakkor azt az összegző kérdésnél mindenképpen, a szervezet számára képviselt súlyának megfelelően, figyelembe kell venni.
- A szürkével jelölt összegző, vagy fő kérdések esetében a nemleges válasz automatikusan azt jelenti, hogy a vizsgált felhő alapú rendszer nem felel meg a megkívánt biztonsági követelményeknek, annak használatától el kell tekinteni.
- Amennyiben egy fehér színnel jelzett kérdésnél annak a szolgáltató csak részben felel meg, akkor a kérdőív kitöltőjének kell eldöntenie, hogy a hiányosság alkalmazást kizáró tényező-e. Amennyiben nem, akkor a kérdés kihagyható, és a későbbi vizsgálatok során kell tisztázni a szolgáltatóval annak kezelési módját.

DOI azonosító: 10.17625/NKE.2015.021

Biztonsági elemző sablon felhő alapú rendszerek értékeléséhez - rendvédelmi szervek részére

Készítő:

A dokumentumot készítő szerv adatai:		
	szervezet neve:	
	címe:	
	kapcsolattartó:	
	elérhetőségek:	

Értékelt szolgáltató:

Az értékelt szolgáltató adatai:		
	szervezet neve:	
	címe:	
	kapcsolattartó:	
	elérhetőségek:	

DOI azonosító: 10.17625/NKE.2015.021

Tartalomjegyzék:

DOI azonosító: 10.17625/NKE.2015.021

14. adatok elvesztése, ellopása
15. mobil eszközök kezelése

Egyéb (jogi, fizikai stb.) biztonság

1. jogi megfelelőség
2. fizikai biztonság
3. személyi biztonság
4. gazdasági biztonság
5. dokumentumbiztonság

DOI azonosító: 10.17625/NKE.2015.021

2. számú melléklet: Biztonsági sablon felhőszolgáltató megfelelőségének ellenőrzésére - üzembiztonság

Kategóriák vizsgálandó kérdései	**válaszok**	
	igen	**nem**
Üzembiztonság:		
1. közösségi felhő közös üzembiztonsági alapkövetelményei		
A felhasználó számára megfelelő és elfogadható a közösségi felhő felhasználói által kialakított közös üzembiztonsági alapkövetelmény rendszer?	☐	☐
2. hordozhatóság és interoperabilitás		
A szolgáltató által kínált eszközök, rendszerek és szolgáltatások biztosítják az adatok hordozhatóságát és a különböző (szolgáltató, felhasználó, harmadik fél) rendszereinek együttműködését?	☐	☐
A szolgáltató által kínált eszközök, rendszerek és szolgáltatások biztosítják az együttműködési képességet más, saját országbeli érintett hatóság vagy közigazgatási szervvel?	☐	☐
A szolgáltató által kínált eszközök, rendszerek és szolgáltatások biztosítják az együttműködési képességet más országok vagy EU érintett rendvédelmi szerveinek rendszereivel?	☐	☐
A szolgáltató nyilvános, publikált API-kat használ?	☐	☐
A szolgáltató által kínált interfészek interoperabilisak		
a felhasználó rendszereinek interfészeivel?	☐	☐
a felhasználó munkafolyamataihoz kapcsolódó harmadik felek rendszereinek interfészeivel?	☐	☐
más szolgáltató rendszereinek interfészeivel?	☐	☐
A szolgáltató által kínált interfészek komplexitása hordoz kockázatot?	☐	☐
A felhasználó által már használt rendszerek, szolgáltatások, platformok együttműködnek a szolgáltató által kínált rendszerrel, szolgáltatásokkal?	☐	☐
A szolgáltató által kínált feltételek mellett biztosított az adatformátumok cseréjének, elhordozásának képessége?	☐	☐

DOI azonosító: 10.17625/NKE.2015.021

A szolgáltató továbbító/kicserélő eszközei együttműködnek a felhasználó és az érintett harmadik felek rendszereivel?	☐	☐
A szolgáltató, a felhasználó és az érintett harmadik felek azonosítási rendszerei együtt tudnak működni?	☐	☐
Az adat importja/exportja és szolgáltatások menedzselése biztonságos standardizált hálózati protokollon keresztül biztosított, amelyhez teljes dokumentáció a felhasználó rendelkezésére áll?	☐	☐
A szolgáltató iparágilag elismert virtualizációs platformot és standard formátumokat használ, amelyhez teljes dokumentáció a felhasználó rendelkezésére áll, beleértve a lehetséges változtatási lehetőségek leírását is?	☐	☐
A felhasználói entitások földrajzi szóródása, elhelyezkedése lehetővé teszi az akadálymentes használatot?	☐	☐
Biztosított a szolgáltató és a felhasználó egymástól kért és kapott, strukturált és nem strukturált adatai iparági standard formátumban történő átadása?	☐	☐
A szolgáltató és a felhasználó vonatkozó szabályozói megfeleltethetők egymásnak?	☐	☐
A szolgáltató által bevont alvállalkozó, harmadik felek rendszerei, fejlesztései biztosítják a hordozhatóságot és az interoperabilitást a fenti pontok szerint?	☐	☐
3. üzletmenet-folytonosság		
A szolgáltató által kínált eszközök, rendszerek és szolgáltatások üzletmenet-folytonossága megfelelően biztosított?	☐	☐
A szolgáltató rendelkezik üzletmenet-folytonossági tervel, és a teljes dokumentáció a felhasználó rendelkezésére áll?	☐	☐
A szolgáltató megfelelő, rendszeres időközönként tart üzletmenet-folytonossági gyakorlatokat, teszteléseket, amelyről a teljes dokumentáció a felhasználó rendelkezésére áll?	☐	☐
Tisztázott és elfogadható-e az üzembiztonsági tesztelések célja és hatálya,		

DOI azonosító: 10.17625/NKE.2015.021

amelyeket a szolgáltató végez?	☐	☐
amelyeket harmadik féllel végeztet?	☐	☐
A szolgáltató biztosítja az adatközpont(ok) állapotellenőrzését (víz, áram, hőmérséklet, pára, telekommunikáció, internetkapcsolat), ezeket megfelelő, rendszeres időközönként teszteli és ezekről teljes dokumentáció a felhasználó rendelkezésére áll?	☐	☐
A szolgáltatónál rendelkezésre állnak a szükséges üzemeltetési dokumentációk (adminisztrátori, felhasználói utasítások, rendszerleírások konfiguráláshoz, installáláshoz, üzemeltetéshez, használathoz), és ezek teljes egészében a felhasználó rendelkezésére állnak?	☐	☐
A szolgáltatónál rendelkezésre állnak a szükséges karbantartási utasítások és eljárások, és ezek teljes egészében a felhasználó rendelkezésére állnak?	☐	☐
A szolgáltató rendelkezi-e bevezetett üzemeltetési módszertannal, és ehhez megfelelőségi tanúsítványokkal (pl. ITIL, COBIT)?	☐	☐
A szolgáltatónál bevezetett üzemeltetési módszertanhoz megvannak-e a szükséges előírások, a rendszeres képzések, és ezekről a teljes dokumentáció a felhasználó rendelkezésére áll?	☐	☐
A szolgáltatónál bevezetett üzemeltetési módszertan megfeleltethető-e a felhasználónál alkalmazottal?	☐	☐
Az adatközpontok elhelyezkedése megfelelő a környezeti és egyéb kockázatok szempontjából?	☐	☐
A szolgáltató megfelelő módon kiépítette a környezeti katasztrófák elleni fizikai védelmeket?	☐	☐
A szolgáltató felkészült az áramellátási biztosítására hálózat-kimaradás esetén?	☐	☐
A felhasználói hatáselemzés alapján, a szolgáltatóval egyeztetve, megfelelő módon és elfogadható eredménnyel megtörtént-e		
a kritikus szolgáltatások azonosítása?	☐	☐
a folyamatok, alkalmazások, partnerek, harmadik félként	☐	☐

DOI azonosító: 10.17625/NKE.2015.021

kapcsolódó szolgáltatók egymásra hatásának azonosítása?		
hibajavítás lefolyásának, a bevont személyeknek, szervezeteknek, az időtartamának stb. tisztázása?	☐	☐
visszaállítási prioritások meghatározása?	☐	☐
visszaállításhoz szükséges idő meghatározása?	☐	☐
a maximálisan tolerálható kiesőidő meghatározása?	☐	☐
az újrainduláshoz szükséges források becslése?	☐	☐
Tisztázott az üzembiztonsági események jelentési, és ezek tapasztalatainak megosztási kötelezettsége a felhasználóval?	☐	☐
4. rendelkezésre állás, ellenálló képesség, megbízhatóság:		
A szolgáltató által kínált eszközök, rendszerek és szolgáltatások rendelkezésre állása és ellenálló képessége, megbízhatósága megfelelő?	☐	☐
A szolgáltató több lehetséges szolgáltatási komponenst kínál-e, és azokból a felhasználónak van-e lehetősége választani?	☐	☐
A szolgáltató biztosítja-e az elvárt rendelkezésre állást, és ez szerződésben rögzíthető-e?	☐	☐
A szolgáltató képes-e leállásokra, üzemzavarokra valós időben reagálni?	☐	☐
Rendelkezik-e a szolgáltató adatokkal legalább az elmúlt egy év vonatkozásában adatokkal a nem tervezett leállások számáról, időtartamáról, és annak értékei megfelelőek a felhasználónak?	☐	☐
Rendelkezik-e a szolgáltató adatokkal legalább az elmúlt egy év vonatkozásában adatokkal az alábbiakról, és azok értékei megfelelőek a felhasználónak		
meghibásodások átlagos ideje?	☐	☐
két meghibásodás közötti átlagos idő?	☐	☐
teljes havi vagy napi rendelkezésre állás?	☐	☐
incidensek száma, aránya?	☐	☐
A felhasználó és a szolgáltató infrastruktúra közötti adatforgalom kapcsán a felhasználónak elfogadható-e a használt hálózat		
sávszélessége?	☐	☐

DOI azonosító: 10.17625/NKE.2015.021

késleltetése?	☐	☐
csomagvesztése?	☐	☐
csomagkésleltetések változása (jitter)?	☐	☐
A felhasználó számára elfogadható-e a szolgáltató által kínált		
rosszindulatú támadással szembeni tűrőképesség?	☐	☐
belső DoS, DDoS támadással szembeni tűrőképesség?	☐	☐
külső DoS, DDoS támadással szembeni tűrőképesség?	☐	☐
A szolgáltató az általa kínált eszközök, rendszerek és szolgáltatások megfelelő rendelkezésre állása és ellenálló képessége, megbízhatósága teljesítése érdekében rendelkezik-e elfogadható		
eszközállapot figyeléssel?	☐	☐
a visszaálláshoz szükséges lemezkép és konfigurációs másolatokkal?	☐	☐
átterhelési lehetőségekkel, eljárásrendekkel?	☐	☐
eszköz redundanciával?	☐	☐
tartalék telephellyel, telephelyekkel?	☐	☐
A szolgáltató által kínált, a nem tervezett leállásokra vonatkozó előírások és vállalások megfelelőek a felhasználónak?	☐	☐
A szolgáltató által kínált, az átmeneti leállásokra vonatkozó előírások és vállalások megfelelőek a felhasználónak?	☐	☐
A szolgáltató által kínált, a hosszantartó és folyamatos leállásokra vonatkozó előírások és vállalások megfelelőek a felhasználónak?	☐	☐
5. szolgáltatási szintek, azok garanciái		
A szolgáltató által kínált szolgáltatási megállapodás és azok garanciái megfelelők és elfogadhatók a felhasználó számára?	☐	☐
A szolgáltató által kínált feltételek megfelelők és elfogadhatók a felhasználó számára az alábbiakban		
szolgáltatási szintek (SLA[107])?	☐	☐
szolgáltatásszint-menedzsment (SLM[108])?	☐	☐

[107] SLA service level agreement szolgáltatási megállapodás

DOI azonosító: 10.17625/NKE.2015.021

szolgáltatásminőségi követelmény (SLR[109])?	☐	☐
szolgáltatásminőségi cél?	☐	☐
A szolgáltató által használt szolgáltatási szabályzatok és eljárásrendek megfelelőek, és azok teljes egészében a felhasználó rendelkezésére állnak?	☐	☐
A szolgáltató által használt folyamatba épített ellenőrzési rendszer átlátható a felhasználó számára, és azok dokumentációi a felhasználó rendelkezésére állnak?	☐	☐
6. skálázhatóság és erőforrás menedzsment		
A szolgáltató által kínált skálázhatóság és erőforrás menedzsment megfelelő a felhasználó számára?	☐	☐
A szolgáltató biztosítja-e a felhasználó számára szükséges fel-, és leskálázási erőforrás lehetőségeket?	☐	☐
A felhasználó számára elfogadható-e a szolgáltató által kínált rövid távú és hosszú távú le-, és felskálázhatósági lehetőségek?	☐	☐
Lehetséges-e a fel-, és leskálázás szolgáltatói beavatkozás nélkül?	☐	☐
A felhasználó számára elfogadható-e az automatizált folyamatok biztonsága (pl. lefoglalható erőforrások maximalizálása, erőforrás-megosztás kiegyensúlyozása plusz igények esetén)?	☐	☐
A felhasználó számára megfelelő és elfogadható a szolgáltató által biztosított erőforrások menedzselésével kapcsolatos		
felhasználói felügyeletet biztosító metódus és eszközrendszer?	☐	☐
szabályozó interfész?	☐	☐
A felhasználó számára megfelelő-e a szolgáltató által kínált fel-, és leskálázási prioritási sorrend a felhasználók között?	☐	☐
A szolgáltató rendelkezik-e adatokkal legalább az elmúlt egy év vonatkozásában adatokkal az alábbiakról, és annak értékei megfelelőek-e a felhasználónak		
a kapacitásigények fluktuációjáról, és azok teljesítéséről?	☐	☐
egyidejű felhasználók számának csúcsáról?	☐	☐

[108] SLM service level management szolgáltatásszint-menedzsment
[109] SLR service level requirement szolgáltatásminőségi követelmény

DOI azonosító: 10.17625/NKE.2015.021

az adatok arányáról az aktív felhasználók között?	☐	☐
csúcs és átlagterhelés különbségéről?	☐	☐
a maximális és normál terhelés arányáról (azaz a terheléstűrésről)?	☐	☐
a kiszámíthatatlan terhelésekről, azok kiszolgálásáról, (tűréséről), mint pl. DoS/DDoS támadások?	☐	☐
a növekvő igények kielégítéséhez szükséges új hardverkomponensek beszerzési idejéről?	☐	☐
A felhasználó számára átlátható, elfogadható a szolgáltató erőforrás gazdálkodása és tervezése az alábbiaknál		
felhasználók számának, igényeinek növekedési korlátai, tervezése?	☐	☐
erőforrások tervezése a szolgáltatónál?	☐	☐
felhőszolgáltatás tartalékképzési és tartalék felhasználási rendje és ennek felhasználói kontrollja?	☐	☐
erőforrások kimerülési lehetőségének tervezése?	☐	☐
erőforrások illetéktelen használata, gazdasági alapú DoS támadásból adódó erőforrások gazdálkodási lehetőségének tervezése?	☐	☐
A felhasználó számára elfogadható a kritikus alkalmazások, API-k, hálózati infrastruktúra-elemek, rendszerkomponensek és tartalékok tervezése		
a szolgáltatónál?	☐	☐
az alvállalkozóknál?	☐	☐
a megfeleltetés a felhasználó igényeinek, szerződésnek?	☐	☐
erőforrások kimerülési lehetősége	☐	☐
erőforrások illetéktelen használata, gazdasági alapú DoS	☐	☐
A felhasználó számára elfogadható a szolgáltató és a felhasználó által kölcsönösen biztosítandó, a felhőben használt szoftver és licenc leltár és licencgazdálkodás?	☐	☐
7. redundancia		

DOI azonosító: 10.17625/NKE.2015.021

A szolgáltató rendelkezik megfelelő, a felhasználó számára elfogadható üzembiztonságot garantáló redundanciával, és annak teljes dokumentációja a felhasználó számára hozzáférhető?	☐	☐
A szolgáltató rendelkezik megfelelő, a felhasználó számára elfogadható üzembiztonságot nyújtó redundanciával az alábbi elemekből	☐	☐
infrastruktúra elemek?		
tárolók?	☐	☐
mentések?	☐	☐
adatközpont, rendszerelemek hűtése?	☐	☐
áramellátás?	☐	☐
összeköttetés?	☐	☐
A szolgáltató megfelelő, a felhasználó számára elfogadható geo-redundanciát biztosít (elsősorban adatközpont és tárolt adatok esetében)?	☐	☐
A felhasználó számára biztosított a redundáns elemek menedzselésének átláthatósága, és annak megvalósítása elfogadható?	☐	☐
8. katasztrófa-elhárítási terv		
A szolgáltató rendelkezik megfelelő, a felhasználó számára elfogadható katasztrófa-elhárítási tervvel, és annak teljes dokumentációja a felhasználó rendelkezésére áll?	☐	☐
9. biztonsági mentés és visszaállítás:		
A szolgáltató által kínált biztonsági mentési és visszaállítási rendszer megfelelő és elfogadható a felhasználó számára?	☐	☐
A szolgáltató biztonsági mentési gyakorlata megfelelő a felhasználó számára az alábbiak tekintetében		
a mentés gyakorisága?	☐	☐
a mentett adatok, információk köre?	☐	☐
a mentések tárolási módja?	☐	☐
a mentések formátuma?	☐	☐
a mentések hozzáférhetősége a felhasználó számára?	☐	☐

DOI azonosító: 10.17625/NKE.2015.021

A visszaállítási időtartam (RTO[110]) és visszaállítási időpont (RPO[111]) a felhasználó számára egyértelmű és elfogadható?	☐	☐
A szolgáltató visszaállítási reagálási és hatékonysági stratégia mérése (incidens felfedezés időtartama, azaz a késés, az újraindítás szükségességének felismeréséhez szükséges átlagos időtartam, javításhoz szükséges átlagos időtartam, incidens utáni helyreállításhoz szükséges átlagos időtartam) rendszeres időközönként megtörténik és annak eredményei elfogadhatók a felhasználó számára?	☐	☐
10. életciklus kezelés és változásmenedzsment		
A szolgáltatónál alkalmazott életciklus kezelés és változásmenedzsment, beleértve új szolgáltatások bevezetési rendjét, a felhasználó számára megfelelő és elfogadható?	☐	☐
Rendelkezik a szolgáltató tervvel az új technológiák adaptálásának üteméről, ütemezéséről, valamint kimutatással a korábban végrehajtott fejlesztésekről, és ez megfelelő és elfogadható a felhasználó számára?	☐	☐
A szolgáltató szabályozott életciklus-kezelési és változásmenedzsment eljárásokkal és folyamatokkal rendelkezik?	☐	☐
A biztonsági alapkövetelményekben lefektetett konfigurációtól való eltérés		
engedélyeztetése megfelelően dokumentált, és arról megfelelő tájékoztatást kap a felhasználó?	☐	☐
magakadályozhatja a felhasználó, ha az súlyosan sérti vagy veszélyezteti az érdekeit?	☐	☐
A változások engedélyezése, nyomon követése, lezárása megfelelően dokumentált, és hozzáférhető a felhasználó részére az alábbiak esetén		
fejlesztések	☐	☐
adatok, hardver, szoftver más telephelyre áthelyezése?	☐	☐

[110] RTO recovery time objective visszaállítási időtartam
[111] RPO recovery point objective visszaállítási időpont

DOI azonosító: 10.17625/NKE.2015.021

A változások végrehajtását követően a szolgáltató által végzett minőség-ellenőrzés, tesztelés megfelelő a felhasználó számára?	☐	☐
A szolgáltatónál megfelelően kidolgozott a jogosulatlan szoftvertelepítések megakadályozásának rendszere, és ez elfogadható a felhasználó számára?	☐	☐
A szolgáltatónál van a kritikus alkalmazások, API-k, hálózati infrastruktúra-elemek, rendszerkomponensek változtatására külön engedélyeztetési, eljárási rend, és ez a felhasználó számára elfogadható?	☐	☐
A felhasználóval kapcsolatban álló, és a szolgáltató rendszerét elérő partnerek velőírásai változások kezelésére	☐	☐
Van lehetőség új szolgáltatás bevezetésére felhasználói igény alapján?	☐	☐
A felhasználói új igények befogadási, megvalósítási rendje, üteme megfelel a felhasználónak?	☐	☐
Van lehetősége a felhasználónak megakadályozni egy új szolgáltatás bevezetését, amennyiben az súlyosan sérti, vagy veszélyezteti az érdekeit?	☐	☐
A szolgáltatónak van bejelentési, értesítési kötelezettsége a nem a felhasználó által kezdeményezett új szolgáltatások bevezetése kapcsán?	☐	☐
Nem a felhasználó által kezdeményezett új szolgáltatások bejelentési, tesztelési, bevezetési rendje megfelel a felhasználónak?	☐	☐
A szolgáltatónál megtörténik a várható igények tervezése (pl. várható tárolási igények a következő öt évben) és azokat rendszeresen felülvizsgálják?	☐	☐
A szolgáltatónál megtörténik a szolgáltatási profil tervezése és azokat rendszeresen felülvizsgálják?	☐	☐
11. adatmigráció		
A szolgáltató megfelelő eszközöket biztosít és támogatást nyújt az	☐	☐

DOI azonosító: 10.17625/NKE.2015.021

adatok, alkalmazások migrálásához?		
12. adatformátum		
A szolgáltató által használt, biztosított adatformátum biztosítja a felhasználó számára	☐	☐
A szolgáltató iparági szabványoknak megfelelő, az iparágban elfogadott és széles körben használt adatformátumokat használ?	☐	☐
A szolgáltató által a szerződés megszűnésekor visszaszolgáltatott adatok formátuma lehetővé teszi azok további felhasználását a felhasználó saját rendszereiben?	☐	☐
A szolgáltató által a szerződés megszűnésekor visszaszolgáltatott adatok formátuma lehetővé teszi azok hordozhatóságát és használatát más szolgáltatók rendszereiben?	☐	☐
13. adatközpont működés, rendszer konfiguráció		
A felhasználó az adatközpont működéséről, a szolgáltató rendszereinek konfigurációjáról a számára szükséges mértékben, a megfelelő üzembiztonság megítéléséhez, rendelkezik információkkal, és az ehhez szükséges dokumentáció a rendelkezésére áll?	☐	☐
A szolgáltató rendelkezik a megfelelő mélységű alapkonfigurációs dokumentációval (tervek, tesztek, üzemelő konfigurációk teljes körűen dokumentációja)?	☐	☐
A szolgáltató rendelkezik konfiguráció nyilvántartással?	☐	☐
A szolgáltatónál megtörtént a hozzáférés-, és funkcionalitáskorlátozás (csak szükséges portok, protokollok, szolgáltatások engedélyezése, futtatása, többi tiltása)?	☐	☐
A szolgáltató alkalmaz megfelelő technikai kontrollt az állékonyság javítására, ellenőrzésére (pl. OS sértetlenség ellenőrzés)?	☐	☐
A szolgáltató által az adatközpontokban használt adatvagyon-kezelési eljárások (pl. adatkarbantartás, upgrade előírások, földrajzi redundancia) megfelelőek és elfogadhatóak a felhasználónak?	☐	☐
14. alkalmazásbiztonság:		

DOI azonosító: 10.17625/NKE.2015.021

A szolgáltatónál alkalmazott alkalmazásbiztonsági előírások és eljárásrendek megfelelőek és elfogadhatóak a felhasználó számára?	☐	☐
A szolgáltatónak van az alkalmazásbiztonsággal kapcsolatos szabályzata és eljárásrendje, mind a szolgáltató által, mind a felhasználó által fejlesztett, fejlesztetett, vásárolt és futatott vagy futtatni kívánt alkalmazásokra vonatkozóan, amelyek elfogadhatóak és megfelelnek a felhasználónak?	☐	☐
A szolgáltató által működtetett alkalmazásbiztonsági folyamatok és eljárásrendek a felhasználó számára megfelelően támogatják az adatai bizalmasságát, sértetlenségét és rendelkezésre állását?	☐	☐
A szolgáltatónál az alkalmazások tervezése, fejlesztése, telepítése, tesztelése az iparági szabványok szerint történik?	☐	☐
A szolgáltatónál megtörtént megfelelő adatintegritás ellenőrző rutinok implementálása az alkalmazásinterfészekbe és adatbázisokba a hibák, sérülékenységek megelőzésére?	☐	☐
A szolgáltatónál futó alkalmazások monitorozása (pl. teljesítés, hibák, frissítések) folyamatosan történik, és az eseményekről a felhasználó kellő időben és részletességgel kap jelentést?	☐	☐
A felhasználó számára megfelelő a szolgáltató által használt, segédprogramok használatának korlátozására, korlátozhatóságára (pl. túlzott erőforrás-felhasználás miatt, ezek a szoftverek hajlamosak túlterhelni a rendszert) vonatkozó eljárásrend?	☐	☐
15. javítócsomagok kezelése		
A javítócsomag kezelésének (előírásai, tesztelésének, telepítésének rendje, azok gyakorisága, dokumentáltsága) megfelelő és elfogadható a felhasználó számára?	☐	☐
16. ellátási lánc üzembiztonsága		
A szolgáltató által bevont alvállalkozók, kapcsolódó harmadok felek üzembiztonsága a szolgáltató által megfelelően kontrollált és elfogadható szintű a felhasználó számára?	☐	☐

DOI azonosító: 10.17625/NKE.2015.021

A szolgáltató rendszeresen elvégzi bevont alvállalkozók, kapcsolódó harmadok felek üzembiztonsági belső értékelését, mérését, és azok eredményeit értékeli?	☐	☐
A szolgáltató rendszeresen bekéri és megkapja a bevont alvállalkozók, kapcsolódó harmadok felek által elvégzett saját üzembiztonsági belső értékelési, mérési jelentéseket azok eredményeit értékeli?	☐	☐
17. üzembiztonsági kockázatcsökkentési terv:		
A szolgáltató rendelkezik üzembiztonsággal kapcsolatos kérdésekre vonatkozó kockázatcsökkentési tervvel, és annak teljes dokumentációja a felhasználó rendelkezésére áll?	☐	☐
A szolgáltató kockázatcsökkentési terve teljes körűen felöleli a korábban tárgyalt üzembiztonsági kockázatokat?	☐	☐
A szolgáltató kockázatcsökkentési szabályai, eljárásai teljes körűen dokumentáltak?		
A szolgáltató az érintett dolgozóinak rendszeresen oktatja az üzembiztonsággal kapcsolatos kockázatcsökkentési eljárási rendet, ellenőrzi és számon kéri oktatások	☐	☐

DOI azonosító: 10.17625/NKE.2015.021

3. számú melléklet Biztonsági sablon felhőszolgáltató megfelelőségének ellenőrzésére – adatbiztonság

Kategóriák vizsgálandó kérdései	**válaszok**	
	igen	**nem**
Adatbiztonság:		
1. közösségi felhő közös üzembiztonsági alapkövetelményei		
A felhasználó számára megfelelő és elfogadható a közösségi felhő felhasználói által kialakított közös adatbiztonsági alapkövetelmény rendszer?	☐	☐
2. irányítás:		
A szolgáltató adatbiztonsághoz kapcsolódó irányítási tevékenysége egyértelmű, átlátható, megfelelő és elfogadható a felhasználó számára?	☐	☐
A szolgáltatónál a biztonsági alapkövetelmények meghatározása a jogi, törvényi, szabályozási előírásoknak való megfeleléssel történt?	☐	☐
A szolgáltató rendelkezik az iparági információbiztonsági standardoknak való megfelelőségi tanúsítványokkal (pl. ISO 27001:2013)?	☐	☐
Ehhez a szolgáltatónál megvannak a szükséges előírások, a rendszeres képzések, és ezekről a teljes dokumentáció a felhasználó rendelkezésére áll?	☐	☐
A szolgáltatónál alkalmazott információbiztonsági standardok megfeleltethetők a felhasználónál alkalmazottal?	☐	☐
A szolgáltató által használt információbiztonsági irányelvek és eljárások megfelelően támogatják a felhasználó szervezeti céljait?	☐	☐
A szolgáltatónál vannak szankciókat is tartalmazó fegyelmi szabályozók az információbiztonsági előírások megsértőinek az információbiztonság kikényszerítése?	☐	☐
A felhasználó szolgáltatások feletti kontrollja megfelelően és a felhasználó számára elfogadhatóan biztosított?	☐	☐
A felhasználó alkalmazásfejlesztés feletti kontrollja megfelelően és a felhasználó számára elfogadhatóan biztosított?	☐	☐

DOI azonosító: 10.17625/NKE.2015.021

A szolgáltató és felhasználó számára a biztonsági tesztelések célja és hatálya egyértelmű, megfelelő és elfogadható, amikor is		
a szolgáltató végzi, végezteti?	☐	☐
a felhasználó végzi, végezteti?	☐	☐
a harmadik fél végzi, végezteti?	☐	☐
A szolgáltató működtet biztonságirányítási rendszert, ezt megfelelő dokumentumokkal igazolni tudja, és az megfelelő és elfogadható a felhasználó számára?	☐	☐
A szolgáltatónak van biztonságtervezési eljárásrendje és az megfelelő és elfogadható a felhasználó számára?	☐	☐
A szolgáltató rendelkezik az alábbi, a felhasználó számára megfelelő és elfogadható biztonsági szabályzatokkal, amelyek a felhasználó rendelkezésére állnak		
biztonságpolitika?	☐	☐
biztonsági irányelvek, szabályzatok?	☐	☐
biztonsági stratégia?	☐	☐
kockázatkezelési stratégia?	☐	☐
informatikai biztonsági szabályzat?	☐	☐
rendszerbiztonsági terv?	☐	☐
adatvédelmi szabályzat?	☐	☐
A szolgáltató rendelkezik a szükséges biztonsági szervezetekkel, és ezekben a megfelelő képzettségű személyekkel (pl. információbiztonsági felelős, adatvédelmi felelős stb.)	☐	☐
A szolgáltató és a felhasználó egyértelműen, a felhasználó számára átlátható, megfelelő és elfogadható módon megállapodott a felelősségek meghatározásában, szétválasztásában az alábbiak tekintetében		
szolgáltatói/felhasználói felelősségek?	☐	☐
a felelősök kijelölése?	☐	☐
a különböző biztonsági feladatok szétválasztása?	☐	☐
a „need to know” elv – alkalmazással történő – kikényszerítése?	☐	☐

DOI azonosító: 10.17625/NKE.2015.021

Az információbiztonsággal kapcsolatos dokumentálás (pl. rendszerekről, eseményekről, képzésekről, emberekről) rendszeres, hozzáférhető, megfelelő és elfogadható a felhasználónak?	☐	☐
Az információbiztonsághoz kapcsolódó eljárásrendek, szabályzatok, azok végrehajtása a szolgáltatónál a felhasználó számára megfelelő és elfogadható módon és gyakorisággal felülvizsgálatra kerül?	☐	☐
3. kockázatkezelés		
A szolgáltató adatbiztonsággal kapcsolatos kockázatkezelési rendje megfelelő és elfogadható a felhasználó számára?	☐	☐
A felhasználó számára megfelelő és elfogadható módon folyik a szolgáltatóknál az információbiztonsággal kapcsolatos kockázatok elemzése?	☐	☐
A szolgáltatónál és a felhasználónál megtörtént az érintett adatvagyon leltározása, osztályozása, és ez mindkét fél részére a számukra szükséges mértékben ismert és átlátható?	☐	☐
A szolgáltatónál megtörtént az információbiztonsági kockázatok értékelése az azonosított kockázatok hatása és valószínűsége szerint, ez rendszeresen felülvizsgálatra kerül, amelynek periódusideje, módszere és eredmény megfelelő és elfogadható a felhasználó számára?	☐	☐
A szolgáltatónál a kockázatelemzés adatközpontúan, az adatok feletti irányítás követelményeit kiemelten kezelő módon történik?	☐	☐
A szolgáltatónál az adatok nyilvántartási, címkézési, kezelési, biztonsági előírásai a felhasználó számára megfelelőek és elfogadhatóak?	☐	☐
A szolgáltatónál megtörténtek a biztosítási szintek kijelölése, a biztonsági osztályokba sorolás?	☐	☐
A szolgáltatónál teljes körűen megtörtént biztonsági állapot felmérése?	☐	☐
A szolgáltató által kínált rendszerek, szolgáltatások biztonsági	☐	☐

DOI azonosító: 10.17625/NKE.2015.021

besorolása, azok szintje megfeleltethető a felhasználó jelenlegi rendszerei biztonsági szintjének, és azok mértéke elfogadható a felhasználó számára?		
▯ A szolgáltató rendelkezik a felhasználó számára megfelelő és elfogadható kockázatkezelési és -csökkentési tervvel?	☐	☐
▯ A szolgáltató kockázatkezelési keretrendszere a felhasználó számára megfelelő és elfogadható módon biztosítja az azonosított kockázatok, a felhasználó által is jóváhagyott mérték-kockázati kritériumokon alapuló, elfogadható mértékűre csökkentését?	☐	☐
▯ A szolgáltató előírásai, szabályozói, valamint kockázatkezelési és –csökkentési terve egyen szilárdan biztosítja a kockázatok kezelését, bármilyen változtatás ezekben konzekvensen átvezetésre kerül?	☐	☐
▯ A szolgáltató használ Információbiztonsági Menedzsment Programot (ISMP)[112], amely kiterjed		
▯ a kockázatkezelésre?	☐	☐
▯ a biztonságpolitikára?	☐	☐
▯ az informatikai biztonsági szervezetre?	☐	☐
▯ az adatvagyon kezelésére?	☐	☐
▯ az emberi erőforrások biztonságára?	☐	☐
▯ a fizikai és környezeti biztonságra?	☐	☐
▯ az elektronikus kommunikáció és az üzemeltetés irányítására?	☐	☐
▯ a hozzáférés-szabályozásra?	☐	☐
▯ az információs rendszerek beszerzésére, fejlesztésére, és karbantartására?	☐	☐
4. azonosítás, hitelesítés jogosultságkezelés és hozzáférés szabályozás		
A szolgáltatónál használt és az általa kínált azonosítási, hitelesítési, jogosultságkezelési és hozzáférés-szabályozási rend megfelelő és elfogadható a felhasználó számára?	☐	☐
▯ A szolgáltatónál használt azonosítási, hitelesítési,		

[112] ISMP: Information Security Management Program Információbiztonsági Menedzsment Program

DOI azonosító: 10.17625/NKE.2015.021

jogosultságkezelési és hozzáférés-szabályozási eljárásrend a felhasználó számára megfelelő és elfogadható módon szabályozott és ezekről a teljes dokumentáció a felhasználó rendelkezésére áll az alábbiak tekintetében		
egyszeri bejelentkezés lehetősége több rendszer használatához?	☐	☐
többfaktoros azonosítás, bejelentkezés lehetősége, kötelezősége?	☐	☐
feladatok, szerepkörök, kötelezettségek?	☐	☐
felhasználói fiókok létesítése, megszüntetése, jogosultságváltozások szabályozása felhasználó, szolgáltató, vegyes (mindkettő) és harmadik fél esetében?	☐	☐
vészhelyzeti hozzáférés?	☐	☐
AAA[113] szabályok használata?	☐	☐
AAA szabályok engedélyezése, kontrolljának támogatása?	☐	☐
A szolgáltatónál az azonosításhoz, hitelesítéshez, jogosultságkezeléshez és hozzáférés-szabályozáshoz kapcsolódó tevékenységek, a felhasználó számára megfelelően és elfogadhatóan, engedélyeztetési eljáráshoz kötötten, a felhasználó kijelölt vezetőjével a hozzáférés biztosítása előtt jóváhagyatva, a magállapodás szerinti korlátozások, előírásoknak megfelelően történik?	☐	☐
A szolgáltató az azonosításhoz, hitelesítéshez, jogosultságkezeléshez és hozzáférés-szabályozáshoz kapcsolódóan a felhasználó számára megfelelő és elfogadható nyilvántartást, nyilvántartásokat vezet?	☐	☐
A szolgáltatónál engedélyek felülvizsgálata meghatározott időközönként, a felhasználó bevonásával, a számára megfelelő és elfogadható módon zajlik?	☐	☐
A szolgáltató bizonyos előre megjelölt személyek (pl. megjelölt harmadik fél) a felhasználót is érintő adatok, rendszerek, eszközök, szolgáltatások hozzáférésekor (pl. használat,	☐	☐

[113] AAA: authentication, authorization, and accounting hitelesítés, engedélyezés, hozzáférés-kezelés

DOI azonosító: 10.17625/NKE.2015.021

megosztás stb.) a felhasználó számára megfelelő és elfogadható módon és időben tájékoztatja a felhasználót?		
A szolgáltatónál a felhasználó számára megfelelően és elfogadhatóan, a felhasználói szabályok alapján, vagy azoknak megfeleltethető módon zajlik		
a hozzáférési szabályok megsértésének kezelése?	☐	☐
a kármentesítés?	☐	☐
az inaktív felhasználók észlelése, kezelése?	☐	☐
szabálytalan bejelentkezés kivizsgálása?	☐	☐
jogosultság visszavonása, módosítása?	☐	☐
A szolgáltató bizonyos előre megjelölt esetekben a felhasználó számára megfelelő és elfogadható módon és időben tájékoztatja a felhasználót jogosultság visszavonásáról, módosításáról (pl. ha azt megjelölt harmadik fél kéri)?	☐	☐
A szolgáltatónál a felhasználó számára megfelelő és elfogadható módon történik az azonosítók, hozzáférési adatok		
tárolása, kezelése?	☐	☐
a tárolt információk minimalizálása?	☐	☐
ezekhez a hozzáférések korlátozása legkisebb jogosultság alapján, valamint az adminisztrátori jogosultságok osztályozása, korlátozása?	☐	☐
azonosítók, hozzáférési adatok újrafelhasználásának tiltása, minimalizálása	☐	☐
A szolgáltatónál az azonosításhoz, hitelesítéshez, jogosultságkezeléshez és hozzáférés-szabályozáshoz (felhasználóé, szolgáltatóé, harmadik félé), valamint ezek ellenőrzéséhez kapcsolódó információk megosztásához az interoperabilitás a szolgáltató, a felhasználó és érintett harmadik felek esetén biztosított?	☐	☐
A szolgáltató a felhasználó számára átlátható, megfelelő és elfogadható módon alkalmaz fekete/fehér listákat az alábbiak tekintetében, és ezekről a szükséges dokumentáció a felhasználó		

DOI azonosító: 10.17625/NKE.2015.021

rendelkezésére áll		
▯ eszközök automatizált azonosítása?	☐	☐
▯ személyek azonosítása?	☐	☐
▯ hozzáférések?	☐	☐
▯ IP címek?	☐	☐
▯ felhasználás helyének automatizált azonosítása?	☐	☐
▯ A szolgáltatónál alkalmazott hitelesítési protokollok a felhasználó számára megfelelőek és elfogadhatóak?	☐	☐
▯ A szolgáltató és a felhasználó, a felhasználó számára megfelelő és elfogadható módon, megállapodott egyszeres hitelesítés után több rendszer használata lehetőségéről, ennek korlátozásáról vagy tiltásáról?	☐	☐
▯ Amennyiben engedélyezett az egyszeres hitelesítés után több rendszer használata, ennek kapcsán a szolgáltató és a felhasználó, a felhasználó számára megfelelő és elfogadható módon, megállapodott ennek részletszabályairól, valamint hogy ez		
▯ hitelesítési szolgáltatón keresztül történik?	☐	☐
▯ felhasználó hitelesítési rendszerével történik?	☐	☐
▯ A szolgáltató a felhasználó számára megfelelő és elfogadható sértetlenséget és letagadhatatlanságot ellenőrző algoritmusokat használ (pl. hasító kódok, digitális aláírások, ujjlenyomatok, ellenőrző összegek, elektronikus időbélyegek stb.)?	☐	☐
▯ A szolgáltatónál alkalmazott hitelesítés erőssége a felhasználó számára megfelelő és elfogadható?	☐	☐
▯ A szolgáltató a felhasználó számára megfelelő és elfogadható felmérte és alakított ki védelmet az azonosításhoz, hitelesítéshez, jogosultságkezeléshez és hozzáférés-szabályozáshoz kapcsolódó módszereket, protokollokat kihasználó támadások ellen (pl. visszajátszásos támadás)?	☐	☐
▯ A szolgáltatónál a felhasználó számára megfelelő és elfogadható módon történik az óraszinkronizálás (pl. külső időszinkronhoz) a naplózás, események kivizsgálása hitelességének érdekében?	☐	☐

DOI azonosító: 10.17625/NKE.2015.021

A hozzáférési szintek meghatározása a felhasználó számára megfelelő és elfogadható módon, a szolgáltató és a felhasználó megállapodása szerint, az adatkörök. adattípusok besorolása alapján történik?	☐	☐
A szolgáltatónál a felhasználó számára megfelelő és elfogadható módon szabályozott a logikai hozzáférés-védelem (pl. kötelező hozzáférés-védelem (MAC[114]), szabály alapú hozzáférés-kezelés (RBAC[115]), ezek kombinációja)?	☐	☐
A felhasználó számára megfelelő és elfogadható módon, a szolgáltató és a felhasználó megállapodása szerint történik a felhasználó, más felhasználó, a szolgáltató és egyéb harmadik felek hozzáféréseinek szétválasztása (pl. szabályok, eljárások, jogi, törvényi, üzleti kritikus folyamatok, vagyon és érzékeny adatok alapján)?	☐	☐
A felhasználó számára megfelelő és elfogadható módon, a szolgáltató és a felhasználó megállapodása szerint biztosított a szolgáltató, harmadik felek a felhasználó adatit, folyamatait érintő hozzáférésének minimalizálása a jogosulatlan vagy illetéktelen hozzáférés valószínűségének, üzleti hatásnak a figyelembevételével, valamint ezek monitorozása, mérése?	☐	☐
A felhasználó számára megfelelő és elfogadható módon, a szolgáltató és a felhasználó megállapodása szerint történik a fizikai hozzáférés-védelem kialakítása, kikényszerítése, ezek ellenőrzése szolgáltatói, felhasználói és érintett harmadik felek oldalán egyaránt az alábbiak esetében		
végpont hozzáférés-védelem (pl. ujjlenyomat, digitális azonosító-kártya, token)?	☐	☐
hozzáférési pontok helye?	☐	☐
A szolgáltatónál a felhasználó számára megfelelő és elfogadható módon történik a hálózati hozzáférés-szabályozás, és forgalomszűrés?	☐	☐

[114] MAC: Mandatory Access Control kötelező hozzáférés-védelem.
115 RBAC: Role-based access control szabály alapú hozzáférés-kezelés

DOI azonosító: 10.17625/NKE.2015.021

A szolgáltatónál a felhasználó számára megfelelő és elfogadható felhasználói portok konfigurálási, diagnosztikai lehetőségei, ezek korlátozásának metódusa?	☐	☐
A felhasználó számára megfelelő és elfogadható módon, a szolgáltató és a felhasználó megállapodása szerint történik az azonosításhoz, hitelesítéshez, jogosultságkezeléshez és hozzáférés-szabályozáshoz kapcsolódó események kapcsán		
naplózás, naplóelemzés?	☐	☐
riasztások kiadása?	☐	☐
korlátozások alkalmazása (pl. rossz adatmegadás esetén, feladat és szerepkör szétválasztás valamint a felhasználói érdekek alapján)?	☐	☐
elszámoltathatóság?	☐	☐
A felhasználó számára megfelelő és elfogadható módon, a szolgáltató és a felhasználó megállapodása szerint történik a jelszószabályok kialakítása, ezek ellenőrzése és ellenőrzésének aránya, különleges jelszavak kikényszerítése szolgáltatói, felhasználói és érintett harmadik felek oldalán egyaránt?	☐	☐
A felhasználó számára megfelelő és elfogadható módon, a szolgáltató és a felhasználó megállapodása szerint biztosított a hozzáférés a szolgáltató, valamint harmadik felek részére		
a felhasználó saját fejlesztésű szoftvereinek forráskódjához?	☐	☐
egyéb szellemi tulajdonhoz?	☐	☐
5. határvédelmi eszközök működtetése és ellenőrzése:		
A szolgáltatónál használt határvédelmi megoldások, azok működtetése és ellenőrzése átlátható, megfelelő és elfogadható a felhasználó számára és azok dokumentációja a felhasználó számára hozzáférhető?	☐	☐
A szolgáltató határvédelmi eszközeinek, rendszereinek tervezése, beállítása, üzemeltetése megfelel az iparági standardoknak és a felhasználó követelményeinek?	☐	☐
A szolgáltató által használt határvédelmi megoldások átláthatók, megfelelnek és elfogadhatók a felhasználó számára, és azok teljes		

DOI azonosító: 10.17625/NKE.2015.021

dokumentációja, beleértve a beállításokét is, a felhasználó rendelkezésére áll az alábbiak tekintetében		
tűzfalak?	☐	☐
távoli elérés, VPN?	☐	☐
behatolás érzékelő és megelőző rendszer (IDS/IPS)[116]?	☐	☐
tartalomszűrés (spamszűrés, vírusirtó, kártékony kódok szűrése, URL szűrés, ActiveX, JavaScript szűrés, kulcsszavas, web szűrés, web alkalmazások szűrése)?	☐	☐
antivírus megoldások, ezek automatikus frissítse és futtatások aránya?	☐	☐
központi védelmi megoldások (pl, kártékony kódok elleni védelem)?	☐	☐
adathordozók kezelése címkézés, tárolás, szállítás, törlés, megsemmisítés, elvesztés, találás?	☐	☐
adatszivárgás elleni védelem (DLP)?	☐	☐
rosszindulatú programok lefutásának megakadályozása (végpontokon, hálózati elemeken)?	☐	☐
különböző, megbízható (biztonságos) és nem megbízható (nem biztonságos) hálózatok között adat és szoftver cseréből eredő kódok lefutásának megakadályozása, amelyeket nem kifejezetten a címzett telepített vagy futtatott le?	☐	☐
rosszindulatú hálózat feltérképezések észlelése, jelentése?	☐	☐
6. folyamatos ellenőrzés		
A szolgáltató hálózatában a felhasználó számára megfelelő és elfogadható módon működik a folyamatos ellenőrzés?	☐	☐
A szolgáltató hálózatában a felhasználó számára megfelelőek és elfogadhatóak		
a beépített biztonsági ellenőrzések?	☐	☐
a valós idejű biztonsági ellenőrzési lehetőségek?	☐	☐
szolgáltató által biztosított biztonsági menedzsment?	☐	☐

[116] IDS/IPS: Intrusion Detection System/ Intrusion Prevention Systems behatolás-érzékelő és –védelmi rendszerek

DOI azonosító: 10.17625/NKE.2015.021

ezek felett a felhasználó kontroll lehetőségei?	☐	☐
A szolgáltató a felhasználó számára megfelelő és elfogadható folyamatos ellenőrzést lehetővé tevő folyamatot ajánlott fel és biztosít?	☐	☐
A szolgáltató hálózatában a felhasználó számára megfelelőek és elfogadhatóak az adatvédelmi ellenőrzések?	☐	☐
7. incidenskezelés		
A szolgáltatónál a felhasználó számára megfelelő és elfogadható módon szabályozott és működtetett az incidenskezelési rend?	☐	☐
A szolgáltatónál a felhasználó követelményeinek megfelelő, számára elfogadható módon működik az incidensek korai előrejelzése, megelőzése, észlelése, valamint az események kezelése, amely tartalmazza		
az eljárásrendet (pl. az incidensek osztályozásához szükséges leírásokat, a reagálási időket, értesítési sorrendet stb.)?	☐	☐
a felhasznált eszközöket?	☐	☐
az incidenskezelési gyakorlatokat?	☐	☐
naplóállományokkal kapcsolatos teendőket (elemzés, feldolgozás, ennek gyakorisága, hatóköre, mire kell kötelezően kiterjednie)?	☐	☐
A szolgáltató rendelkezik az incidensek jelentéséhez, kezeléséhez szükséges kapcsolati pontok listájával (beleértve a felhasználót, CERT-et, hatóságot, egyéb érintett szervezeteket), ezeket folyamatos frissíti, karbantartja?	☐	☐
A szolgáltató számára egyértelműen, a felhasználó követelményeinek megfelelően tisztázott és elfogadott az értesítések, riasztások rendje, az értesítési kötelezettségek paraméterei az alábbi szereplők tekintetében		
szolgáltató?	☐	☐
felhasználó?	☐	☐
alvállalkozó, érintett harmadik fél?	☐	☐
A szolgáltatónál a felhasználó számára megfelelő és elfogadható	☐	☐

DOI azonosító: 10.17625/NKE.2015.021

módon zajlik az incidensek felfedezése után a kárelhárítás?		
A szolgáltatónál a felhasználó számára megfelelő és elfogadható módon zajlik a szolgáltatás visszaállítása, beleértve ezek sorrendjét, prioritásait is?	☐	☐
A szolgáltató elfogadta a felhasználó által előírt,, az incidenskezelés kapcsán megszerzett információk, tapasztalatok megosztására vonatkozó kötelezettségeket?	☐	☐
A szolgáltató követelményeknek és előírásoknak, valamint a hatósági, bírósági eljárásban történő felhasználásra is alkalmas módon biztosítja az incidens utólagos elemzéséhez szükséges bizonyítékok gyűjtését, beleértve felhasználó ebbe a folyamatba bekapcsolódásának lehetőségét?	☐	☐
A szolgáltatónál az incidensek elemzése és értékelése az iparági, és CERT előírásoknak, ajánlásoknak, valamint a felhasználó követelményeinek megfelelően történik?	☐	☐
A szolgáltatónál a felhasználó számára megfelelő és elfogadható módon, azokat a felhasználóval megosztva, készít időszakos biztonsági jelentések, értékeléseket		
szolgáltatónál bekövetkezett eseményekről?	☐	☐
alvállalkozóknál, harmadik félnél bekövetkezett eseményekről?	☐	☐
A szolgáltatónál a felhasználó számára megfelelő és elfogadható módon működnek mechanizmusok az incidensek típusának, nagyságának és költségeinek figyelemmel kísérésére?	☐	☐
8. sérülékenység vizsgálat, kezelés		
A szolgáltatónál a felhasználó számára megfelelő és elfogadható módon szabályozott és működtetett a sérülékenységek kezelési rendje?	☐	☐
A szolgáltató a felhasználó számára megfelelő és elfogadható módon, rendszeres időközönként felméri rendszerei, szolgáltatásai elméleti sérülékenységeit, beleértve a kezelőfelület biztonságát, kompromittálódási lehetőségeit, a kiszolgáló szoftverek (op. rendszerek, szolgáltatási motor stb.) támadhatóságát is?	☐	☐

DOI azonosító: 10.17625/NKE.2015.021

A gyakorlati sérülékenység-vizsgálatok végrehajtásának körülményei, a felhatalmazott végrehajtók (szolgáltató, felhasználó, harmadik fél), a végrehajtás körülményei, időpontja, időtartama stb. minden érintett fél számára egyértelműen tisztázott és a felhasználó számára megfelelő és elfogadható?	☐	☐
A szolgáltató vagy a felhasználó által végrehajtott sérülékenység-vizsgálatok gyakorisága a felhasználó számára megfelelő és elfogadható?	☐	☐
A szolgáltató vagy a felhasználó által végrehajtott sérülékenység-vizsgálatokhoz kapcsolódó jogosultságok, korlátok, tilalmak minden érintett fél számára egyértelműen tisztázottak és a felhasználó számára megfelelőek és elfogadhatóak?	☐	☐
A szolgáltató, a felhasználó számára megfelelő és elfogadható módon tesz közzé figyelmeztetéseket, hajt végre tudatosítást a rendszerei, szolgáltatásai sérülékenységével kapcsolatban?	☐	☐
A szolgáltatónál felhasználó számára megfelelő és elfogadható módon történik a kapcsolódó biztonsági kontrollok hatékonyságának vizsgálata?	☐	☐
A szolgáltató, a felhasználó számára megfelelő és elfogadható módon tesz eleget a szolgáltató vagy alvállalkozók által azonosított sérülékenységek, időszakos és azonnali jelentési kötelezettségének?	☐	☐
9. titkosítás és kulcskezelés:		
A szolgáltató és a felhasználó megállapodott a szolgáltató, a felhasználó és kacsolódó harmadik felek által használható, használni kívánt titkosításról és az azokhoz tartozó kulcskezelésről, ez ezek a felhasználó számára megfelelőek és elfogadhatóak?	☐	☐
A szolgáltató és a felhasználó megállapodott a szolgáltató és/vagy a felhasználó általi kulcskezelési eljárásokról, előírásokról, azonosíthatóságról, jogosultságokról, kulcsgenerálásról a teljes életciklus alatt?	☐	☐
A szolgáltató és a felhasználó megállapodott a szolgáltatói és a	☐	☐

DOI azonosító: 10.17625/NKE.2015.021

felhasználói felelősségekről, feladatokról, értesítési, figyelmeztetési kötelezettségekről (pl. szolgáltatói titkosítás bármilyen változtatásakor)?		
A szolgáltató és a felhasználó megállapodott a szolgáltató és/vagy a felhasználó általi titkosítás használatóságáról vagy kötelező használatáról, annak szabályairól az alábbiakhoz kapcsolódóan	☐	☐
bejelentkezéskor?	☐	☐
a hozzáférés egyes fázisaiban?	☐	☐
az adatok használatkor, a memóriában?	☐	☐
az adatok közlekedtetésekor (rendszerinterfészeken, nyilvános hálózatokon, elektronikus üzenetekben)?	☐	☐
az adatok tárolása, archiválása esetén (fájl-szerveren, adatbázisban, felhasználó gépén)?	☐	☐
A szolgáltató és a felhasználó megállapodott a szolgáltató és/vagy a felhasználó általi titkosítás használatakor titkosító kulcs minimális hosszában?	☐	☐
A szolgáltató és a felhasználó megállapodott a szolgáltató és/vagy a felhasználó általi titkosítás használatakor a jogszabályi, törvényi, egyéb előírásoknak való megfelelésben?	☐	☐
A szolgáltatónál a felhasználó számára megfelelő és elfogadható módon szabályozott		
a kulcsokhoz való hozzáférés?	☐	☐
a kulcsok tárolása?	☐	☐
a kulcskezelés és használat szétválasztása?	☐	☐
az adminisztrátori hozzáférés engedélyezése?	☐	☐
A szolgáltató és a felhasználó megállapodott a szolgáltató és/vagy a felhasználó általi titkosítás használatakor kulcsmenedzsment szolgáltató bevonási lehetőségeiről?	☐	☐
A felhasználó számára megfelelő és elfogadható módon szabályozott a nyilvános hálózatok felé is továbbított adatok védelme módosítás, jogosulatlan nyilvánosságra hozatal vagy	☐	☐

DOI azonosító: 10.17625/NKE.2015.021

visszaélésekkel szemben?		
10. virtualizációból adódó biztonság kezelése:		
A szolgáltató a felhasználó számára megfelelő és elfogadható módon kezeli a virtualizációból adódó kockázatokat, és ezekről a szükséges dokumentumok a felhasználó rendelkezésére állnak?	☐	☐
A szolgáltató a felhasználó számára megfelelő és elfogadható módon felmérte a virtualizált környezetből adódó új támadási felületeket (pl. új API-k, új csatornák, új adatfajták), vektorokat (pl. hypervisor fertőzése virtuális gépből, közbeékelődéses támadás (MitM), memóriatartalom módosítása,) ezeket megfelelő gyakorisággal frissíti, és ennek megfelelően gondoskodik ezek biztonságáról?	☐	☐
A szolgáltató a felhasználó számára megfelelő és elfogadható módon gondoskodik a virtuális hálózatok védelméről (pl. virtuális gépek egymás közötti kommunikációjának védelme, biztonsági beállítások és adminisztrátori jogosultságok szétválasztása, virtuális tűzfalak üzemeltetése stb.), a virtuális gépken, hálózatokon bekövetkező változások érzékeléséről, a sértetlenség ellenőrzéséről és a riasztásról?	☐	☐
A szolgáltató a felhasználó számára megfelelő és elfogadható módon biztosítja a mozgó adatok védelmét a fizikai szerverek, adatok, alkalmazások virtuálisra migrálásakor, mozgatásakor?	☐	☐
A szolgáltató a felhasználó számára megfelelő és elfogadható módon gondoskodik a virtuális gépek rendszermásolatainak (image-ek) biztonságosságáról, beleértve ezek napra készen tartását a sérülékenységek és az új szoftververziók miatt?	☐	☐
A szolgáltató a felhasználó számára megfelelő és elfogadható módon gondoskodik a hypervisor megerősítéséről	☐	☐
menedzselési és adminisztrációs funkciók elérésének korlátozásával, a legkisebb jogosultság elv alapján?	☐	☐
több faktoros hitelesítés használatával?	☐	☐
ellenőrzési nyomvonalak megadásával?	☐	☐

DOI azonosító: 10.17625/NKE.2015.021

IP cím-szűréssel?	☐	☐
tűzfalak használatával?	☐	☐
biztonságos kapcsolat (pl. TLS[117]) használatával, még az adminisztratív felületekhez is?	☐	☐
A szolgáltató alkalmaz felügyelő szoftvereket a hypervisor és a futó folyamatokat ellenőrzésére, és ezek a felhasználó számára megfelelőek és elfogadhatóak?	☐	☐
A szolgáltató a felhasználó számára megfelelő és elfogadható módon biztosítja különböző felhasználók adatainak, folyamatainak izolációját?	☐	☐
11. kliensoldali védelem		
A szolgáltató által előírt kötelező kliensoldali védelem a felhasználó számára betartható, elfogadható, azt a szolgáltató megfelelően támogatja?	☐	☐
A szolgáltató pontos, átlátható, a felhasználó rendszereinek, eszközeinek, szoftvereinek megfelelő listát biztosít a kötelezően alkalmazandó kliensoldali védelmi elemekről (pl. kliens oldali fizikai és logikai védelem, használt web böngésző plug-in-ek, közösségi oldalak használatának engedélyezése stb.), és azok betarthatók és elfogadhatók a felhasználó számára?	☐	☐
A szolgáltató a felhasználó kérése esetén megfelelő módon képes segíteni a kliensoldali védelem kialakítását?	☐	☐
A szolgáltató és a felhasználó közös megállapodás alapján egyértelmű szabályokat tud alkalmazni azon, a felhasználó által az alkalmazottainak biztosított, vállalati eszközökre, szolgáltatásokra, amelyek magán célra történő használata is engedélyezett, és amelyek a szolgáltatót is érintik?	☐	☐
A szolgáltató és a felhasználó közös megállapodás alapján egyértelmű szabályokat tud alkalmazni a felhasználó alkalmazottai által használt azon saját tulajdonú eszközökre,	☐	☐

[117] TLS: Transport Layer Security kliens/szerver alapú alkalmazások számára készített, biztonságos kommunikációt biztosító protokoll

DOI azonosító: 10.17625/NKE.2015.021

amelyeken a felhasználó vállalati eszközeinek, szolgáltatásainak elérése, használata engedélyezett, és amely a szolgáltatót is érinti?		
12. vezeték nélküli hálózatok biztonsága		
A szolgáltatónál a felhasználó számára megfelelő és elfogadható módon szabályozottak, kezeltek és védettek a vezeték nélküli hálózatok és azok használata?	☐	☐
A szolgáltatónál a felhasználó számára megfelelő és elfogadható módon szabályozott a vezeték nélküli hálózat használata, tiltása		
a szolgáltató saját rendszereiben?	☐	☐
a szolgáltató telephelyeiről, adatközpontjaiból elérhető idegen hálózatok esetében?	☐	☐
a szolgáltató alkalmazottai által elért, a szolgáltató rendszereihez, eszközeihez, szolgáltatásaihoz történő kapcsolódáshoz használt hálózatok esetében?	☐	☐
A szolgáltatónál használt vezeték nélküli hálózatok esetén a felhasználó számára megfelelő és elfogadható módon szabályozott, és ezekről a dokumentáció a felhasználó rendelkezésére áll		
a tűzfal használata, beállítása?	☐	☐
biztonsági beállítások?	☐	☐
titkosítás azonosításra, hitelesítésre és kommunikációra?	☐	☐
nem hitelesített forgalom korlátozása, tiltása?	☐	☐
gyári beállítások kötelező cseréje?	☐	☐
felhasználók számának minimalizálása, korlátozása?	☐	☐
meghatározott eszközök engedélyezése, többi tiltása?	☐	☐
jogosulatlan eszközök érzékelése, kizárása?	☐	☐
13. biztonsági architektúra		
A szolgáltató architektúrája (pl. eszközei, rendszerei, szoftverei) az információbiztonsági iparági szabványoknak és a felhasználói követelményeknek megfelelően kerültek kialakításra, történik a rendszeres felülvizsgálata és frissítése, amelyek a felhasználó számára	☐	☐

DOI azonosító: 10.17625/NKE.2015.021

megfelelőek és elfogadhatóak?		
A szolgáltató által használt infrastruktúrák az információbiztonsági iparági szabványoknak és a felhasználói követelményeknek megfelelően kerültek kialakításra, azok megfelelőek és elfogadhatóak a felhasználó számára az alábbiak tekintetében		
adatközpont biztonság?	☐	☐
szerver biztonság?	☐	☐
alkalmazás és platform biztonság?	☐	☐
adatbiztonság?	☐	☐
A szolgáltató az információbiztonsági iparági szabványoknak és a felhasználói követelményeknek megfelelően alakította ki és működteti a hálózatbiztonsági elemeket, azok megfelelőek és elfogadhatóak a felhasználó számára az alábbiak tekintetében	☐	☐
hálózatok szegmentálása?	☐	☐
interfészek korlátozása?	☐	☐
hálózati forgalom naplózása?	☐	☐
a forgalom korlátozása biztonságos és nem biztonságos hálózatok között?	☐	☐
a hálózati beállítások, ezek áttekintése meghatározott időközönként, de legalább évente?	☐	☐
A szolgáltató és a felhasználó közösen elvégezte a magas kockázatú környezet, folyamatok, adatáramlások azonosítását, a szolgáltató megállapodásuk szerint, a felhasználó számára megfelelő és elfogadható módon végzi ezeknél a biztonság megteremtéséhez szükséges technikai eszközök telepítését, mélységi védelemi technológiák (defense-in-depth techiques) alkalmazását (pl. DPI[118], forgalom szabályozása, lezárása, black-holing[119])?	☐	☐
14. adatok elvesztése, ellopása:		
A szolgáltatónál a felhasználó számára megfelelő és elfogadható módon gondoskodik az adatok rendelkezésre állásáról, elvesztése, ellopása	☐	☐

[118] DPI: Deep Packet Inspection mély csomag elemzés
[119] black-holing: hálózati be-, és kimenő forgalom eldobása anélkül, hogy a forrás értesülne arról, hogy az adatok nem érték el a címzettet

DOI azonosító: 10.17625/NKE.2015.021

elleni védelemről (pl. biztonsági mentések, titkosítás alkalmazása stb.)		
15. mobil eszközök kezelése:		
A szolgáltatónál a felhasználó számára megfelelő és elfogadható módon gondoskodik saját alkalmazottai, alvállalkozói és más érintett harmadik felek vonatkozásában az általuk használt mobil eszközök biztonságáról?	☐	☐
A szolgáltató a felhasználó számára megfelelő és elfogadható szabályozási előírásokkal rendelkezik a mobil eszközök biztonságos használatával kapcsolatban, és az erről szóló dokumentumok a felhasználó rendelkezésére állnak?	☐	☐
A szolgáltató a felhasználó számára megfelelő és elfogadható technikai megoldásokat, korlátozásokat alkalmaz a mobil eszközök biztonságos használatának érdekében az alábbiak kapcsán		
személyes/vállalati adatok szétválasztása?	☐	☐
távoli törlés?	☐	☐
titkosítás?	☐	☐
eszköz-monitoring?	☐	☐
elérhető adatok, szolgáltatások meghatározása?	☐	☐
A szolgáltatónál a felhasználó számára megfelelő és elfogadható módon szabályozott a szolgáltató alkalmazottainak vállalati eszközök, szolgáltatások magán célra történő használata?	☐	☐
A szolgáltatónál a felhasználó számára megfelelő és elfogadható módon szabályozott a szolgáltató alkalmazottainak saját tulajdonú eszközeivel a szolgáltató rendszereinek, eszközeinek, szolgáltatásainak az elérése, használata?	☐	☐

DOI azonosító: 10.17625/NKE.2015.021

4. számú melléklet: Biztonsági sablon felhőszolgáltató megfelelőségének ellenőrzésére – egyéb biztonság

Kategóriák vizsgálandó kérdései	**válaszok**	
	igen	**nem**
Egyéb (jogi, fizikai stb.) biztonság		
1. jogi megfelelőség:		
A szolgáltató által nyújtott szerződési és jogi garanciák megfelelőek és elfogadhatóak a felhasználó számára, és a szolgáltató által kínált felhő alapú rendszerek és szolgáltatások megfelelnek a vonatkozó, valamint a felhasználó által megjelölt törvényeknek, jogi szabályozóknak, előírásoknak és követelményeknek?	☐	☐
• A szolgáltató rendelkezik a felhasználóval egyeztetett és a felhasználó által megfelelőnek és elfogadottnak tartott megfelelőségi listával (olyan keretrendszerrel, amely tartalmazza a releváns nemzetközi standardokat, szabályozásokat, jogi, törvényi előírásokat), amelye rendszeres időközönként, de legalább évente egyszer felülvizsgálatra és közös jóváhagyásra kerül?	☐	☐
• A szolgáltató által kínált felhő alapú rendszerek és szolgáltatások a megfelelőségi lista alapján – az ezekről szóló dokumentumok a felhasználó számára történő biztosításával, igazolható módon – megfelelnek az alábbiak tekintetében		
▯ vonatkozó hatályos magyar jogszabályoknak (pl. Ibtv., Mavtv. stb.)?	☐	☐
▯ vonatkozó EU előírásoknak?	☐	☐
▯ vonatkozó adatvédelmi előírásoknak?	☐	☐
▯ vonatkozó adatmegőrzési előírásoknak?	☐	☐
▯ hatósági bizonyítékgyűjtés megvalósítására és elősegítésére vonatkozó jogszabályi előírásoknak és iparági standardoknak?	☐	☐
▯ a felhasználó által peres eljáráshoz kért esetleges bizonyítékgyűjtési követelményeknek?	☐	☐
▯ különböző hatósági eljárásoknál a felhasználó adataihoz az adathozzáférés a vonatkozó jogszabályoknak?	☐	☐

DOI azonosító: 10.17625/NKE.2015.021

▯ külföldi rendvédelmi szerv vagy egyéb hatóság adatigénylése esetén a felhasználó adataihoz az adathozzáférés a vonatkozó jogszabályoknak és a szerződésben foglaltaknak?	☐	☐
• A szolgáltató által kínált felhő alapú rendszerek és szolgáltatások megfelelnek		
▯ az egyéb, általános jogi tényezőknek?	☐	☐
▯ a kormányzati beszerzésekről szóló rendelkezéseknek?	☐	☐
• A szolgáltató és a felhasználó közötti szerződésben a felhasználó számára megfelelően és elfogadhatóan szabályozható		
▯ a hatályos bíróság, joghatóság megállapítása?	☐	☐
▯ az információkezelési, titoktartási, nyilvánosságra hozatali megállapodások és eljárások?	☐	☐
▯ közösségi felhőnél az új felhasználók belépési feltételeinek a tisztázása?	☐	☐
▯ az információbiztonság kapcsán a felhasználó és a szolgáltató felelősségi körének pontos meghatározása?	☐	☐
▯ az adatok tárolási, feldolgozási helye, külföldre viteli korlátozások?	☐	☐
▯ a felhasználó számára az incidenskezeléshez lényeges adatmegőrzési és visszakövetési követelmények (pl. adatmegőrzés minimum és maximum periódusa, naplóállományok megőrzésének minimum és maximum periódusa, adattárolás módja, naplóállományok tárolásának módja, visszaszolgáltatás időtartama)?	☐	☐
▯ az adatok bizalmassághoz, sértetlenségéhez és rendelkezésre állásához szükséges előírások a különböző kezelt adatok típusának megfelelően (pl. titkosítás szükségesség, minimális előírt kulcshossz, API-k, adatok feldolgozása, interoperabilitás, hordozhatóság, alkalmazásfejlesztés, információk cseréje, használata stb.)?	☐	☐
▯ felhasználó mobil eszközkezelésével kapcsolatos, a szolgáltatót is érintő, de a felhasználót terhelő kérdések, szolgáltatói előírások		

DOI azonosító: 10.17625/NKE.2015.021

rosszindulatú programok elleni védekezés?	☐	☐
elfogadott/tiltott alkalmazásboltok?	☐	☐
elfogadott/tiltott más, párhuzamosan használható felhőszolgáltatások?	☐	☐
szoftverek telepítési rendje (elfogadott/tiltott jóváhagyott/nem jóváhagyott stb.)?	☐	☐
felhasználó előírásai, folyamatai mobil eszközökre (BYOD elfogadása/tiltása, mobil eszközök menedzselése, jailbreak, rooting tiltása stb.)?	☐	☐
szolgáltató mobil eszközökről szóló előírásainak elfogadhatósága	☐	☐
szolgáltató által elfogadott, kompatibilis eszközök listája?	☐	☐
szolgáltató által elfogadott, kompatibilis operációs rendszerek listája?	☐	☐
operációs rendszerek frissítésére vonatkozó szolgáltatói előírások, engedélyezési kötelezettség?	☐	☐
mobil eszközök leltárának kezelése, megosztása szolgáltatóval?	☐	☐
biztonsági javítócsomagok alkalmazásának feltételei, követelménye?	☐	☐
szolgáltató és alvállalkozók alkalmazottai mobil eszközkezelésével kapcsolatos, felhasználót is érintő kérdések tisztázása szerződésben (fentiek + biztonságtudatosság, képzések)		
rosszindulatú programok elleni védekezés?	☐	☐
elfogadott/tiltott alkalmazásboltok?	☐	☐
elfogadott/tiltott más, párhuzamosan használható felhőszolgáltatások?	☐	☐
szoftverek telepítési rendje (elfogadott/tiltott jóváhagyott/nem jóváhagyott stb.)?	☐	☐
a szolgáltató előírásai, folyamatai mobil eszközökre (BYOD elfogadása/tiltása, mobil eszközök menedzselése, jailbreak, rooting tiltása stb.)?	☐	☐

DOI azonosító: 10.17625/NKE.2015.021

szolgáltató mobil eszközökről szóló előírásainak elfogadhatósága?	☐	☐
az operációs rendszerek és telepített szoftverek frissítésére vonatkozó szolgáltatói előírások, engedélyezési kötelezettség?	☐	☐
biztonsági javítócsomagok alkalmazásának feltételei, követelménye?	☐	☐
egyéb adatbiztonsági előírások (pl. titkosítás lezáró képernyő alkalmazása, jelszóalkalmazás és követelmények, távoli törlés, felülírás, adatok tárolása eszközökön, más felhőben stb.)?	☐	☐
a felhasználó adatainak és egyéb vagyontárgyainak visszaszolgáltatása a szerződéses viszony bármilyen okból történő megszűnésekor, vagy a felhasználó kérésére?	☐	☐
a szolgáltató csődje, irányításbeli (tulajdonos) változásainak kezelése?	☐	☐
a szolgáltató szakembereinek szándékos adatlopása, rendszer működés akadályozása esetének szabályozása?	☐	☐
a szolgáltató szakmai gondatlanságából adódó problémák esetének szabályozása?	☐	☐
a szolgáltató embereinek és alvállalkozóinak a felhasználó adataihoz történő hozzáférés lehetőségeinek szabályozása?	☐	☐
a nem felügyelt munkamenetek szabályozása?	☐	☐
az átláthatósághoz és a folyamatos ellenőrzéshez biztosított eszközök, módszerek		
szolgáltatóra vonatkozóan?	☐	☐
teljes ellátási láncra vonatkozóan?	☐	☐
a tulajdonjogok kezelése az alábbiak tekintetében		
adatok, szolgáltatások besorolása tulajdonjog szempontjából (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 stb.)?	☐	☐
a licencelési kérdések kezelése?	☐	☐

DOI azonosító: 10.17625/NKE.2015.021

• Az auditálási tevékenység kapcsán a felhasználó számára átlátható, dokumentumokkal igazolható, megfelelő és elfogadható módon történik		
□ az auditálások tervezése?	☐	☐
□ a független auditáló kijelölése a felhasználóval közösen, a vállalhatatlan kockázatok elkerülése miatt?	☐	☐
□ a szolgáltató rendszereinek, tevékenységeinek, szolgáltatásainak adatbiztonságot és üzembiztonságot is felölelő rendszeres időközönként független szervezet(ek) általi auditálásra?	☐	☐
□ az egyéb tanúsítások megszerzése?	☐	☐
□ alvállalkozók információbiztonsági megfelelőségének igazolása (tanúsításokkal, auditokkal) legalább évente?	☐	☐
□ az audit eszközök korlátozása, információk szegmentálása az adatok, naplóállományok kompromittálódásának és visszaélések elkerülése miatt?	☐	☐
□ az audit naplózása, ezen naplóállományok kezelése, megtartása?	☐	☐
• Az alvállalkozók, összetett, harmadik félen alapuló szolgáltatások esetében a felhasználó számára átlátható, dokumentumokkal igazolható, megfelelő és elfogadható módon történik		
□ alvállalkozókkal szerződések megkötése?	☐	☐
□ adatbiztonsági kockázatok csökkentésére tett intézkedések, kontrollok az alvállalkozók felé (pl. feladatok szétválasztása, szabály-alapú hozzáférés, legkisebb jogosultság elve érvényesítése)?	☐	☐
□ a szerződések tárgya, hatálya, a harmadik fél által nyújtott szolgáltatások (pl. adatok cseréje, felhasználása, személyzeti és infrastrukturális elemek, támogatás, felelősségek, feladat és szerepkörök, földrajzi elhelyezkedés stb.)?	☐	☐
□ ésszerű információbiztonsági szint biztosítása a teljes ellátási láncban, ezek mérése, felülvizsgálata legalább évente?	☐	☐
□ felhasználó információbiztonsági követelményeinek teljesülése, ezek mérése?	☐	☐
□ felhasználót is érintő változások jelzése, engedélyeztetése?	☐	☐

DOI azonosító: 10.17625/NKE.2015.021

▯ szolgáltató – alvállalkozó szerződések lejártának kezelése a felhasználó szempontjából?	☐	☐
▯ az alvállalkozók kockázatkezelési és irányítási folyamatainak szolgáltató általi felülvizsgálata, így egységes gyakorlat és összehangolt felelősségre vonhatóság kialakítása?	☐	☐
▯ az SLA rendszeres felülvizsgálata ellátási lánc teljes hosszában, a következetlenségek korrigálása?	☐	☐
▯ a nem megfelelő teljesítések azonosítása és rendszeres (legalább évente történő) felülvizsgálata, korrigálása?	☐	☐
• A szolgáltató naplózási tevékenysége során a felhasználó számára egyértelműen tisztázott, megfelelő és elfogadható		
▯ a kötelezően gyűjtendő üzemeltetési és biztonsági naplóállományok köre?	☐	☐
▯ a szolgáltató által gyűjtött naplóadatok (beleértve a felhasználóhoz, annak tevékenységéhez kapcsolódó adatokat is) köre?	☐	☐
▯ a naplóállományok feldolgozására szolgáló előírások?	☐	☐
▯ a naplóadatok tulajdonjoga, felhasználhatósága?	☐	☐
• A felhasználó adatainak – beleértve a biztonsági mentéseket is – törlése egyértelműen, az előírásoknak, követelményeknek megfelelően, a felhasználó számára megfelelő és elfogadható módon, teljes körűen és visszaállíthatatlanul megtörténik	☐	☐
▯ a szerződés megszűnésekor?	☐	☐
▯ a felhasználó kérésére?	☐	☐
▯ a szolgáltató eszközeinek, adathordozóinak cseréjekor, főleg ha azokat máshol, más célra kívánja felhasználni?	☐	☐
2. fizikai biztonság:		
A szolgáltatónál kialakított fizikai biztonsági elemek és szabályozók megfelelő és elfogadható a felhasználó számára?	☐	☐
• A szolgáltatónál a felhasználó számára megfelelő és elfogadható módon történik a fizikai biztonsági kockázatelemzés, értékelés, és erről a megfelelő dokumentáció a felhasználó rendelkezésére áll?	☐	☐

DOI azonosító: 10.17625/NKE.2015.021

• A szolgáltatónál kialakított és működtetett fizikai biztonság elemek megfelelőek és elfogadhatóak a felhasználó számára az alábbiak tekintetében	☐	☐
□ a fizikai védelem kialakítása (kerítés, falak, kapuk, elektronikai jelzőrendszer, recepciós pult stb.)?	☐	☐
□ a látogatók ellenőrzése?	☐	☐
□ a fizikai biztonsági előírások, eljárásrendek?	☐	☐
□ a felhasználó és támogató személyzet fizikai hozzáférésének korlátozása?	☐	☐
□ beléptetés ellenőrzés, naplózás?	☐	☐
□ illetéktelen belépés megakadályozása, lehetséges belépési pontok folyamatos kontrollja?	☐	☐
□ biztonsági területek, zónák kialakítása, illetékes belépők ellenőrzési mechanizmusa?	☐	☐
□ a nem felügyelt munkaterületek védelme?		
□ be-, és kiszállítások ellenőrzési mechanizmusa, dokumentáltsága?	☐	☐
□ eszközök ellopás elleni mechanizmusa?	☐	☐
□ tűz-, víz-, pára-, füstérzékelők és beavatkozó rendszerek kialakítása, működtetése, hozzáférés és jogosultságok kezelése?	☐	☐
□ elektronikus behatolás-érzékelő és jelzőrendszer kialakítása, működtetése, hozzáférés és jogosultságok kezelése?	☐	☐
• A szolgáltatónál a felhasználó számára megfelelő és elfogadható módon történik a riasztások kezelése, a beavatkozás, valamint a szolgáltató rendelkezik a megfelelő élőerős védelemmel?	☐	☐
• A szolgáltatónál az elvárható gondossággal történik az eszközök tárolása, raktározása, és ez megfelelő és elfogadható a felhasználó számára?	☐	☐
• A szolgáltató megfelelő módon kiépítette a természeti katasztrófák elleni fizikai védelmeket?	☐	☐
3. személyi biztonság:		
A szolgáltatónál a felhasználó számára megfelelő és elfogadható a humán kockázat kezelése, a meglévő személyi biztonsági rendszer garantálja a felhasználó adatainak bizalmasságát, sértetlenségét és	☐	☐

DOI azonosító: 10.17625/NKE.2015.021

rendelkezésre állását?		
• Az érintett személyei rendelkezik a megfelelő átvilágítással és engedélyekkel (pl. személyi biztonsági tanúsítvány, nemzetbiztonsági ellenőrzés stb.)		
□ a szolgáltatónál?	☐	☐
□ a bevont alvállalkozóknál, harmadik feleknél?	☐	☐
• A szolgáltató végrehajt saját egyéb – az adatok osztályozásának, minősítésének megfelelő – átvilágítást		
□ a meglévő munkatársakra?	☐	☐
□ új felvételisekre?	☐	☐
• A szolgáltató felvételi követelményei, alkalmazási szerződése tartalmazza a biztonsági követelmények, információirányítás és biztonsági politika megismerését és elfogadását, amelyet a dolgozókkal még az alkalmazás megkezdése előtt aláíratnak?	☐	☐
• A szolgáltató rendelkezik informatikai biztonsági szervezettel, amely a felhasználó számára megfelelő és elfogadható az alábbiak tekintetében		
□ létszám?	☐	☐
□ felhalmozott képzettségek, tudás?	☐	☐
• A szolgáltatónál az érintett személyek esetében a munkakörök kapcsán egyértelműen, a felhasználó számára megfelelő és elfogadható módon tisztázott		
□ a munkakör betöltéséhez szükséges engedélyek, a munkakör biztonsági besorolása, követelményei?	☐	☐
□ a munkakörhöz kapcsolódó, felhasználót is érintő feladatok és a felelősségek?	☐	☐
□ az információbiztonsággal kapcsolatos jogok, kötelezettségek, feladatok meghatározása?	☐	☐
□ a fegyelmi eljárásrend?	☐	☐
• A szolgáltató szakemberei rendelkeznek a szükséges szakmai ismeretekkel, tapasztalattal és végzettséggel, amely a felhasználó számára megfelelően igazolható?	☐	☐
• A szolgáltatónál megfelelő gyakorisággal és megfelelően frissített	☐	☐

DOI azonosító: 10.17625/NKE.2015.021

tartalommal történnek képzések az alábbi témakörökben, és ezek elfogadhatóak a felhasználónak		
biztonságtudatossági, biztonsági és adatvédelmi tudatosító képzések?	☐	☐
szakmai képzések pl. rendszergazdáknak?	☐	☐
• A beszállítónál, érintett harmadik feleknél a szükséges biztonságtudatossági, biztonsági és adatvédelmi tudatosító és szakmai képzéseket a szolgáltató megfelelően igazolni tudja, és ez a felhasználó számára elfogadható?	☐	☐
• A szolgáltatónál a felhasználó számára megfelelő és elfogadható módon szabályozott a jogviszony-, és munkakörváltozás kezelése?	☐	☐
• A szolgáltatónál a felhasználó számára megfelelő és elfogadható módon szabályozott munkaviszony, szerződéses viszony megszűntekor	☐	☐
a felhasználót érintő adatok, folyamatok, erőforrások elérését lehetővé tevő eszközök és egyéb tulajdon visszaszolgáltatása?	☐	☐
titoktartási nyilatkozat további időszakra is?	☐	☐
egyéb, a felhasználó érdekeit érintő kötelezettségek meghatározása további időszakra is?	☐	☐
4. gazdasági biztonság:		
A felhasználó számára átláthatók és elfogadhatóak a szerződéskötéskor meglévő gazdasági keretek?	☐	☐
• A szolgáltatás igénybevételéhez kapcsolódó díjak tisztázottak, átláthatóak?	☐	☐
• A felhasználó számára a kapcsolódó költségek egyértelműek és elfogadhatóak az alábbiak tekintetében		
működési költségek?	☐	☐
a felhasználás kapcsán a felhasználót terhelő beruházások költségei?	☐	☐
migráció költsége?	☐	☐
• A szolgáltató gazdasági háttere, tulajdonosi struktúrája egyértelmű és átlátható a felhasználó számára?	☐	☐
• A szolgáltató gazdálkodási adatai, prosperitása egyértelmű és	☐	☐

DOI azonosító: 10.17625/NKE.2015.021

elfogadható a felhasználó számára?		
5. dokumentumbiztonság:		
A felhasználó számára megfelelő és elfogadható a szolgáltató által kialakított és működtetett papír alapú dokumentumok kezelésének rendszere?	☐	☐
• A szolgáltatónál alkalmazott kezelési rend elfogadható és megfelel a felhasználónak?	☐	☐
• Amennyiben van, a szolgáltatónál használt iratkezelési szabályzat megfelel a vonatkozó előírásoknak és törvényeknek?	☐	☐
• A szolgáltatónál alkalmazott papír alapú iratok tárolása elfogadható és megfelel a felhasználónak?	☐	☐
• A szolgáltatónál papír alapú iratok hozzáférés rendje, a hozzáférések engedélyeztetése elfogadható és megfelel a felhasználónak?	☐	☐
• Az érzékeny adatokhoz hozzáférő személyek engedélyének megadására vagy elutasítására a felhasználónak van ráhatása, különös tekintettel az alábbi	☐	☐
▯ szerződések	☐	☐
▯ felhasználó adatai,	☐	☐
▯ rendszerdokumentációk, leírások	☐	☐
• A papír alapú dokumentumok nyomon követhetősége elfogadható és megfelel a felhasználónak?	☐	☐

DOI azonosító: 10.17625/NKE.2015.021

Ábrák jegyzéke

DOI azonosító: 10.17625/NKE.2015.021

Táblázatok jegyzéke

DOI azonosító: 10.17625/NKE.2015.021

Fogalomtár és rövidítések jegyzéke

AAA	authentication, authorization, and accounting	hitelesítés, engedélyezés, hozzáférés-kezelés
API	application programming interface	alkalmazásprogramozási felület. 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	Amazon web szolgáltatások
	Black-holing	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	számítógépes katasztrófa-elhárító csoport
CSA	Cloud Security Alliance	felhő alapú rendszerek biztonságával foglalkozó, iparági szakemberek, vállalatok és más érintettek széles koalíciója által vezetett non-profit szervezet
DoS	Denial of Service	szolgáltatásmegtagadással járó támadás, vagy más néven túlterheléses támadás.
DDoS	Distributed Denial of Service	elosztott szolgáltatásmegtagadással járó

DOI azonosító: 10.17625/NKE.2015.021

		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 létrahívott 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	behatolás-érzékelő és –védelmi rendszerek
IP	Internet Protocol	Internet Protokoll: csomagkapcsolt átvitelt megvalósító hálózati réteg protokoll
IPTV	Internet Protocol Television	Internet Protokoll segítségével általában szélessávú interneten keresztül nyújtott digitális televíziós műsorszolgáltatás
IT	Information technology	információtechnológia vagy informatika

DOI azonosító: 10.17625/NKE.2015.021

ITIL	Information Technology Infrastructure Library	informatikai rendszerek üzemeltetésére és fejlesztésére szolgáló módszertan, illetve ajánlás gyűjtemény
ITU	International Telecommunication Union	Nemzetközi Távközlési Egyesület
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 kutató laboratóriuma
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 azonosító szám, egy számjegyekből álló kód, amellyel általában különféle személyes jellegű adatokat, szolgáltatásokat védenek
RBAC	Role-based access control	szabály alapú 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	XML alapú, nyílt szabványú adatformátum

DOI azonosító: 10.17625/NKE.2015.021

	Language	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/szerver alapú alkalmazások számára készített, biztonságos kommunikációt biztosító protokoll
TSCM	Technical Surveillance Countermeasures	technikai elhárítás
VoIP	Voice over IP	Internet Protokoll 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