DOI: 10.38146/BSZ.2018.4.3

KOVÁCS ZOLTÁN – MIKÓ ZOLTÁN – SÁGI GÁBOR

A biztonság mint szolgáltatás megteremtése az állami, önkormányzati elektronikus információs rendszereknél I.

Magyarországon az állami és önkormányzati elektronikus információs rendszerek biztonságának javítása érdekében az elmúlt években fontos lépések történtek, jellemzőik alapján ezek a következő három csoportba sorolhatók. Az első, hogy elkészültek a fő irányokat tartalmazó stratégiák, a második, hogy kiadták a végrehajtás kereteit szabályozó jogszabályokat, végül a harmadik, hogy kialakították azokat a szervezeteket, amelyek mind stratégiai, mind operatív szinten képesek biztosítani az említett dokumentumokban megfogalmazottak megvalósítását.

A fő keretek és a struktúra kialakítását, kialakulását követően minden szinten megindultak az állami és önkormányzati elektronikus információs rendszerek kiberbiztonságának növelését elősegítő tevékenységek. Jelen tanulmány szempontjából ezek közül kiemelendő, hogy megkezdődtek az egyes elektronikus információs rendszerek biztonsági osztályba sorolásai, valamint az érintettek megindították a biztonsági szint emeléséhez szükséges fejlesztéseket is.

Mindezekkel párhuzamosan Magyarországon megkezdődött egy másik folyamat is, amely nagy hatással van az említett tevékenységekre is. Ez pedig az a központosítási folyamat, amelyet annak érdekében indítottak el, hogy a korábbi széttagolt, ezáltal rendkívül drágán fenntartható, ráadásul mind eszközparkjában, mind biztonsági elemeiben rendkívül heterogén, sőt sok esetben a pénzhiány miatt elavult állami, önkormányzati infokommunikációs rendszereket konszolidálják, és egységes, megfelelő szolgáltatási – és nem utolsósorban – biztonsági szintű szolgáltatást nyújtsanak minden érintett számára. (Erre pedig a központosított informatikai és elektronikus hírközlési szolgáltatások ellátására kijelölt központi szolgáltatóként a NISZ Nemzeti Infokommunikációs Szolgáltató Zrt.-t [a továbbiakban: NISZ Zrt.] jelölték ki.[1])

1 309/2011. (XII. 23.) kormányrendelet a központosított informatikai és elektronikus hírközlési szolgáltatásokról. https://net.jogtar.hu/jr/gen/hjegy_doc.cgi?docid=a1100309.kor

Ám éppen az említett, az elektronikus információs rendszerek biztonságát szavatolni kívánó jogszabályok gyakorlatba történő átültetése, valamint az infokommunikációs rendszerek üzemeltetésének, fejlesztésének központosítása együttesen egy olyan hatást keltett, amely miatt a hatályos szabályozást és gyakorlatot felül kell vizsgálni és hozzá kell igazítani a valós helyzethez. A kibervédelmet szavatolni kívánó jogszabályok ugyanis nem erre, a mára kialakult szolgáltató-felhasználói modellre illesztve készültek el, ennek megfelelően az egyes kiberbiztonságot szavatoló kontrollok kialakítása és működtetése kapcsán a felelősségek elhatárolása nem történt meg, így a szabályzókban foglaltak megvalósítása ebben a működési modellben nehézségbe ütközik. Ez pedig alapvetően befolyásolja a biztonság mint szolgáltatás bevezethetőségét is. Akkor lehet ugyanis a kiberbiztonság területén is megvalósítani a szolgáltató-felhasználó modellt, ha egyértelmű, hogy mi az, amit a szolgáltatónak és mi az, amit a felhasználónak kell megvalósítania, és ebből egyértelműen levezethető, hogy mi az, amit biztonság mint szolgáltatás keretében egy szolgáltató nyújthat, kínálhat a felhasználóknak.

Magyarország kibervédelmének főbb elemei

Jelen tanulmánynak nem központi eleme a hazai kibervédelmi rendszer részletes ismertetése, azonban a téma vizsgálatához a következő főbb elemeket mindenképpen érdemes megemlíteni – tartva az említett stratégia–jogszabályok–szervezetrendszer típusú tagolást.

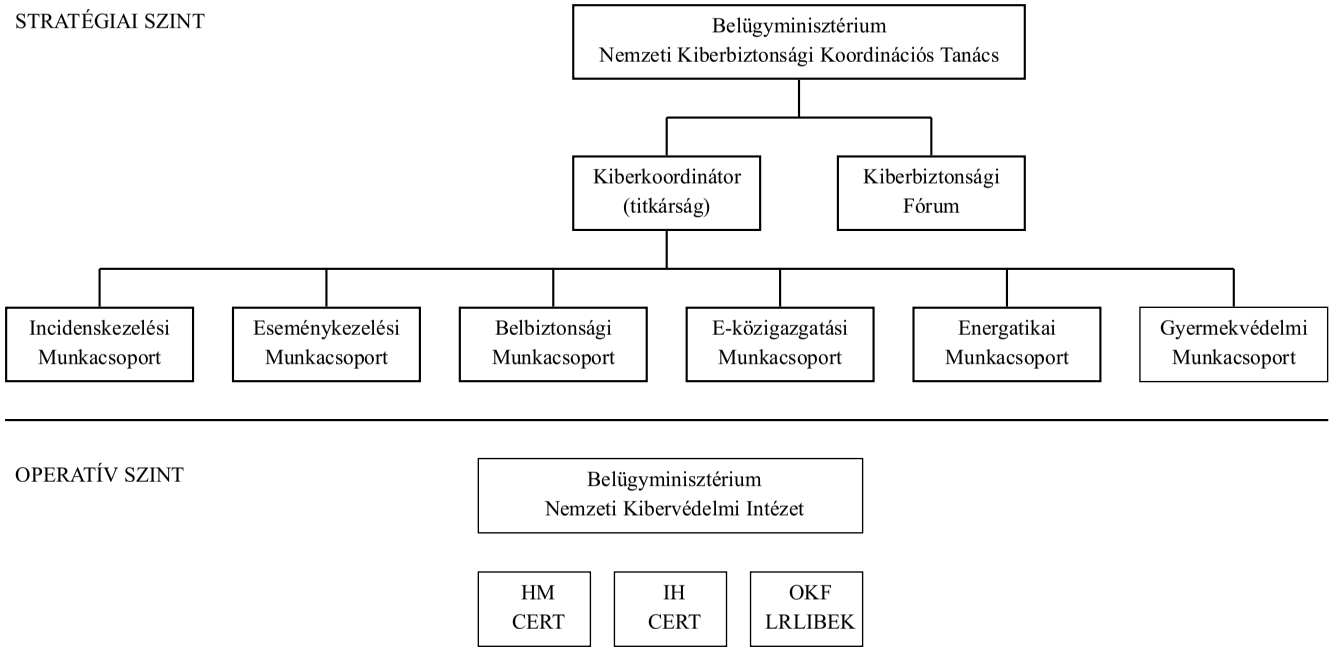
A stratégiai dokumentumok közül a téma szempontjából a legfontosabb Magyarország kiberbiztonsági stratégiája[2], amely 2013-ban jelent meg.

A vonatkozó jogszabályok közül a szintén ebben az évben elfogadott, *az állami és önkormányzati szervek elektronikus információbiztonságáról* szóló 2013. évi L. törvény[3] (a továbbiakban: Ibtv.), az ennek gyakorlati megvalósítását jelentősen elősegítő, az egyes biztonsági osztályba besorolt elektronikus információs rendszereknél kialakítandó védelmi intézkedéseket tételesen leíró, *az állami és önkormányzati szervek elektronikus információbiztonságáról szóló 2013. évi L. törvényben meghatározott technológiai biztonsági, valamint a biztonságos információs eszközökre, termékekre, továbbá a biztonsági osztályba és biztonsági szintbe sorolásra vonatkozó követelményekről* szó-

2 1139/2013. (III. 21.) kormányhatározat Magyarország Nemzeti Kiberbiztonsági Stratégiájáról.
3 https://net.jogtar.hu/jr/gen/hjegy_doc.cgi?docid=a1300050.tv

1. számú ábra

A hazai kibervédelmi struktúra 2015. július 16. után



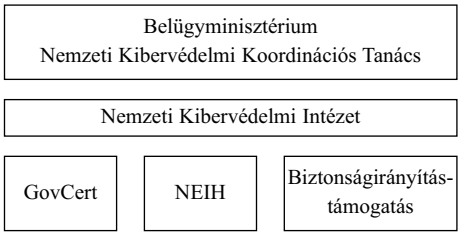
Forrás: Tikos Anita: Az NKI bemutatása (előadás). http://www.eoq.hu/szakb/11/inf170227.pdf

ló 41/2015. (VII. 15.) BM rendelet[4] és *a létfontosságú rendszerek és létesítmények azonosításáról, kijelöléséről és védelméről* szóló 2012. évi CLXVI. törvény[5], valamint ennek a végrehajtási rendeletei[6] emelendők ki.

Ahogy említettem, az elmúlt években kialakult a hazai kiberbiztonságért felelős szervezetrendszer is, amely alapvetően két szintre bontható, stratégiaira és operatívra. A stratégiai szinten a Kiberbiztonsági Fórum, a kiberkoordinátor, valamint az általa vezetett munkacsoportok találhatók, míg az operatív szintet – több esetben hatósági szerepekkel is kiegészülve – a Nemzetbiztonsági Szakszolgálat keretein belül működő Nemzeti Kibervédelmi Intézet (NKI), az Országos Katasztrófavédelmi Főigazgatóság szervezetében található Létfontosságú rendszerek és létesítmények informatikai biztonságiesemény-kezelő központ, a Honvédelmi Minisztérium és az Információs Hivatal saját CERT[7]-jei alkotják *(1. számú ábra).*

Az operatív szervezetek közül kiemelést érdemel a központi, vezető szerepet játszó Nemzeti Kibervédelmi Intézet, amely a Kormányzati Eseménykezelő Központot (GovCERT-Hungary), a Nemzeti Elektronikus Információbiztonsági Hatóságot (NEIH), valamint egy biztonságirányítás támogatásért felelős szervezeti egységet foglal magában *(2. számú ábra).*

2. számú ábra
Az NKI szervezeti egységei



Forrás: dr. Bencsik Balázs: Nemzeti Kibervédelmi Intézet (előadásanyag)
https://njszt.hu/sites/default/files/BencsikBalazs.pptx

Az NKI szervezeti egységeinek fő feladatai a *3. számú ábrá*n láthatók.
Az előbbiek alapján elmondható, hogy mára kialakult az állami és önkormányzati rendszerek kibervédelméért felelős struktúra, sor került a szükséges

4 https://net.jogtar.hu/jr/gen/hjegy_doc.cgi?docid=a1500041.bm
5 http://net.jogtar.hu/jr/gen/hjegy_doc.cgi?docid=A1200166.TV
6 Ezek gyűjteménye: http://www.katasztrofavedelem.hu/index2.php?pageid=lrl_szabalyozas
7 CERT: Computer Emergency Response Team, hálózatbiztonsági vészhelyzeteket elhárító csoport

3. számú ábra

Az NKI szervezeti egységei és fő feladataik

GovCert Incidenskezelő Osztály	– biztonsági események kezelése, – fenyegetésmenedzsment, – ügyeleti szolgálat, – elemzés/értékelés, – kibervédelmi gyakorlat, – képzés, tudatosítás
Nemzeti Elektronikus Információbiztonsági Hatóság (NEIH)	– ügyfelek és rendszerek nyilvántartása, – biztonsági osztályba és szintbe sorolás ellenőrzése, – követelmények teljesülésének ellenőrzése, – javaslat információbiztonsági felügyelő kirendelésére
Biztonságirányítási és Sérülékenységvizsgálati Osztály	– sérülékenységvizsgálat, – EMIR/FAIR-rendszerekkel kapcsolatos informatikai biztonsági feladatok ellátása, – IT-biztonsági tanácsadás

Forrás: Tikos Anita: Az NKI bemutatása (előadás). http://www.eoq.hu/szakb/11/inf170227.pdf

szabályozók kiadására, és ezek alapján zajlik ma hazánkban a kibervédelmi tevékenység. E tevékenység egyik, a tárgyalandó téma szempontjából mindenképp kiemelendő eleme, hogy az érintett intézmények megindították az egyes elektronikus információs rendszerek biztonsági osztályba sorolását, megkezdték a biztonsági szint emeléséhez szükséges fejlesztéseket, a Nemzeti Elektronikus Információbiztonsági Hatóság pedig végzi az ehhez kapcsolódó nyilvántartási, ellenőrzési feladatokat.

A szolgáltató-felhasználói modell az állami, önkormányzati infokommunikációs rendszereknél és hatása a kibervédelemre

Az említett változásokon túl azonban egy másik tényező is erős befolyást gyakorol/gyakorolt a hazai állami, önkormányzati szektor kibervédelmére. Ez pedig az a központosított informatikai és elektronikus hírközlési szolgáltató/szolgáltatások kialakítása érdekében zajló folyamat, amelyet azért indítottak el, hogy a korábbi széttagolt, drágán fenntartható, heterogén eszközrendszerű, sőt sok esetben elavult állami, önkormányzati infokommunikációs

rendszert konszolidálja, és egységes, megfelelő szolgáltatási és biztonsági szintű szolgáltatást nyújtson minden érintettnek.

A feladatra a NISZ Zrt.-t jelölte ki a kormány. A NISZ Zrt. működését meghatározó legfontosabb jogszabályok a már említett és hivatkozott 309/2011. (XII. 23.) kormányrendelet mellett a kormányzati célú hálózatokról szóló 346/2010. (XII. 28.) kormányrendelet[8], az egyes, az elektronikus ügyintézéshez kapcsolódó szervezetek kijelöléséről szóló 84/2012. (IV. 21.) kormányrendelet[9], az elektronikus ügyintézés részletszabályairól szóló 451/2016. (XII. 19.) kormányrendelet, valamint a központosított informatikai és elektronikus hírközlési szolgáltatásokat egyedi szolgáltatási megállapodás útján igénybe vevő szervezetekről, valamint a központi szolgáltató által üzemeltetett vagy fejlesztett informatikai rendszerekről szóló 7/2013. (II. 26.) NFM rendelet[10]. A NISZ Zrt. működését meghatározó szabályozók mellett a téma szempontjából fontos megemlíteni az információbiztonság feladatait rögzítő, a központosított informatikai és elektronikus hírközlési szolgáltató információbiztonsággal kapcsolatos feladatköréről szóló 186/2015. (VII. 13.) kormányrendeletet[11] is.

Az említett jogszabályok természetesen elsősorban a NISZ Zrt. által ellátandó feladatokról szólnak, ezáltal közvetetten az érintett szervezetek infokommunikációs rendszereinek konszolidálását irányozzák elő, e rendszerek egy részének, vagy adott esetben egészének központi szolgáltató által történő biztosításával – és adott esetben kiváltásával. Ez azonban az ezekben a rendszerekben tárolt, kezelt elektronikus információk biztonságát is érinti, hiszen az adott elektronikus információs rendszer azon részének, amelyet a NISZ Zrt. biztosít, neki kell megteremtenie az Ibtv. és a 41/2015. (VII. 15.) BM rendelet által előírt biztonsági kontrollok rá eső részét. Azaz akárcsak az elektronikus információs rendszer elemeinek tervezése, üzemeltetése, úgy a biztonság megteremtésének feladata, felelőssége is megoszlik a szolgáltató és a felhasználó között.

Ám éppen ez okozza a problémát. Az előző fejezetben említett, az elektronikus információs rendszerek biztonságát szavatolni kívánó jogszabályok gyakorlatba történő átültetése, valamint az infokommunikációs rendszerek üzemeltetésének, fejlesztésének központosítása együttesen egy olyan hatást

8 https://net.jogtar.hu/jr/gen/hjegy_doc.cgi?docid=A1000346.KOR
9 https://net.jogtar.hu/jr/gen/hjegy_doc.cgi?docid=a1200084.kor
10 https://net.jogtar.hu/jr/gen/hjegy_doc.cgi?docid=A1300007.NFM&timeshift=fffffff4&txtreferer=00000001.TXT
11 https://net.jogtar.hu/jr/gen/hjegy_doc.cgi?docid=a1500186.kor

teremtett, amely miatt a hatályos szabályozást pontosítani szükséges és azt hozzá kell igazítani a szolgáltató-felhasználó működési modellhez. Amíg ugyanis az infokommunikációs rendszerek üzemeltetésének, fejlesztésének központosítása kialakította a gyakorlatban a ma működő szolgáltató-felhasználói modellt, addig az elektronikus információk biztonságát garantálni kívánó jogszabályok nem rögzítik egyértelműen sem ezt a fajta működési modellt, sem az egyes szerepkörökhöz tartozó felelősségi köröket.

Működési modell tekintetében az Ibtv. nem szolgáltatói és felhasználói, hanem adatgazdai, adatkezelői és adatfeldolgozói szerepköröket definiál, ám utóbbiak feladatainak és felelősségeinek egyértelmű meghatározása, lebontása sem az Ibtv.-ben, sem annak végrehajtási rendeleteiben nem történik meg. Ez tovább nehezíti a feladatok és felelősségek egyértelmű meghatározását, jelentősen hátráltatva a biztonság mint szolgáltatás bevezetését is.

Az említett jogszabályokban azonban mégis megtalálhatók a szolgáltató-felhasználói modell elemei. Azokban ugyanis megjelenik, hogy az egyes rendszereknél akár több felhasználó, akár több üzemeltető is lehet, valamint az is, hogy ezekben az esetekben is gondoskodni kell a teljes körű védelem kialakításáról, ám e feladatok megosztását, a felelősségi körök elhatárolását a két szervezet között megkötendő szerződésre bízzák [Ibtv. 11. § 1. k. és l., valamint 2., 3. bekezdései, 41/2015. (VII. 15.) BM rendelet 3. § 4., 5., 6. bekezdései]. Ez pedig amellett, hogy nem ad világos értelmezést a szolgáltató által kötelezően nyújtandó biztonságikontroll-elemekről, a felhasználó szervezetek „alkupozíciója", ezáltal az egyes szerződések különbözősége okán jelentős heterogenitáshoz is vezethet. Ez viszont jelentősen hátráltatja a biztonság mint szolgáltatás bevezethetőségét is, hiszen az a szolgáltató által nem kötelezően nyújtandó elemekre kell hogy alapuljon.

A szolgáltató és a felhasználók közötti feladat- és felelősségelhatároláshoz a 186/2015. (VII. 13.) kormányrendelet sem ad további iránymutatást.

Hazánkban az állami, önkormányzati szektorban kialakult szolgáltató-felhasználói modell esetében – ahogyan a következőkben lesz szó róla – a NISZ Zrt. gyakorlatilag felhőalapú szolgáltatásokat nyújt, amelynél az adott elektronikus információs rendszer egyes részeit szolgáltatóként ő nyújtja, míg más részeit felhasználóként az igénybe vevő szervezet. Márpedig – ahogy az okfejtésből látszik – ezt a fajta feladat- és felelősségelhatárolást a jelenleg hatályos, a kiberbiztonságot szavatolni kívánó szabályozók nem kezelik egyértelműen. Ezt a fajta felelősségelhatárolást az előbbiek mellett azért is meg kellene tenni, mert a biztonság mint szolgáltatás bevezetésének alapját is csak ez teremtheti meg.

A NISZ Zrt. a már említett jogszabályokban leírt feladatainak ellátását úgy tudja elvégezni, hogy alapvetően felhőalapú szolgáltatásokat nyújt. A téma okán ezért elsősorban ezekkel, a NISZ Zrt. által nyújtott felhőalapú szolgáltatásokkal foglalkozom, nem térek ki a NISZ Zrt. által nyújtott egyéb szolgáltatásokra (például hangalapú telekommunikációs szolgáltatások), de figyelembe veszem azokat, amelyek szorosan kapcsolódnak, kapcsolódhatnak a felhőalapú szolgáltatásokhoz, és így az elektronikus információs rendszerek biztonsági feladatainak elhatárolásához. Az első ilyen a hosting szolgáltatás, a második pedig a menedzselt munkaállomás szolgáltatás. Utóbbi azt jelenti, hogy a – későbbiekben részletesebben bemutatandó – szoftver mint szolgáltatás mellett a végfelhasználók munkaállomásait is a NISZ Zrt. biztosítja.

Ahhoz, hogy az elektronikus információs rendszerek biztonsági feladatainak említett elhatárolását elvégezhessük, célszerű áttekinteni a felhőalapú rendszereket, azok tulajdonságait.

A felhőalapú rendszerek rövid összefoglalása

Tulajdonságai, csoportosításai

A felhőalapú rendszerek, valamint azok tulajdonságainak leírását a *Felhő alapú informatikai rendszerek potenciális alkalmazhatósága a rendvédelmi szerveknél* című cikk[12] részletesen tartalmazza. E tanulmány csupán a téma tárgyalásához szükséges legfontosabb ismereteket foglalja össze.

A felhőalapú rendszerek csoportosítását, jellemzőit az Egyesült Államok legrégibb fizikai kutató laboratóriuma, a NIST *(National Institute of Standards and Technology Information Technology Laboratory)* által *The NIST Definition of Cloud Computing*[13] címen kiadott tanulmányban foglaltakat alapul véve és elfogadva érdemes leírni. Ez a dokumentum ugyanis általánosan elfogadottnak és kváziszabványnak tekinthető, és ma ez adja a legátfogóbb és legelfogadottabb csoportosítási rendszert.

A NIST dokumentuma szerint a következő tulajdonságok megléte esetén beszélhetünk felhőalapú szolgáltatásról:

– Igény szerinti önkiszolgálás *(On-demand self service):* a felhasználók szükségleteik szerint képesek változtatni az igényelt számítási kapacitásokat.

12 Kovács Zoltán: Felhő alapú informatikai rendszerek potenciális alkalmazhatósága a rendvédelmi szerveknél. Hadmérnök, 2011/4., 176–188. o.

13 Peter Mell – Timothy Grance: The NIST Definition of Cloud Computing Version 15. 2010. 10. 07. www.nist.gov/itl/cloud/upload/cloud-def-v15.pdf

– Jó hálózati hozzáférés *(Broad network access):* hálózaton, szabványos mechanizmusokon keresztül, heterogén eszközökkel elérhetők a szolgáltatások.
– Erőforráskészletek *(Resource pool):* a szolgáltató több-bérlős modell szerint, a fogyasztói kereslet függvényében dinamikusan osztja ki és osztja újra az erőforrásokat, amelyek pontos helyét a felhasználó általában nem ismeri, vagy nem tudja kontrollálni.
– Teljes rugalmasság *(Rapid elasticity):* a felkínált kapacitások gyorsan és rugalmasan változtathatók, fel- és leskálázhatók az aktuális igények szerint.
– Mért szolgáltatások *(Measured Service):* a felhasznált erőforrások ellenőrizhetők, használatuk pontosan mérhető.[14]

A tanulmány témájának kifejtéséhez a szolgáltatási és telepítési modellek ismertetésére is szükség van.

Szolgáltatási modellek (Service Models)

– Szoftver mint szolgáltatás *(Cloud Software as a Service [SaaS]):* a felhasználó számára nyújtott képességeket a felhő-infrastruktúrában futó szolgáltatói alkalmazások teszik lehetővé. Az alkalmazások különböző eszközökön, vékony kliensfelületen, például webböngészőn elérhetők (ilyen például a webmail szolgáltatás). A felhasználó néhány felhasználóspecifikus alkalmazás korlátozott konfigurációs beállítási lehetőségétől eltekintve semmilyen hatással sincs a mögöttes infrastruktúrára, hálózatra, szerverekre, operációs rendszerekre, a tárolás módjára, vagy akár egyedi alkalmazások képességére.
– 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-infrastruktúrába. 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.
– Infrastruktúra mint szolgáltatás *[Cloud Infrastructure as a Service (IaaS)]:* a felhasználó számára ebben az esetben olyan számítási, tárolási, hálózati és egyéb alapvető informatikai erőforrásokat kínál a szolgáltató, amelyre és amelyen tetszőleges szoftvereket telepíthet és futtathat, beleértve az operá-

14 Lepenye Tamás: Számítási felhő – egyszerűen. 2011. 06. 15. http://lepenyet.wordpress.com/2011/06/15/szmtsi-felho-egyszeruen/

ciós rendszereket és alkalmazásokat. A felhasználó nem képes menedzselni vagy ellenőrizni a mögöttes felhő-infrastruktúrát, de kontrollálni tudja az operációs rendszereket, tárhelyeket, telepített alkalmazásokat, és esetleg korlátozott hatása lehet a hálózati elemek (például tűzfalak) kiválasztására.[15]

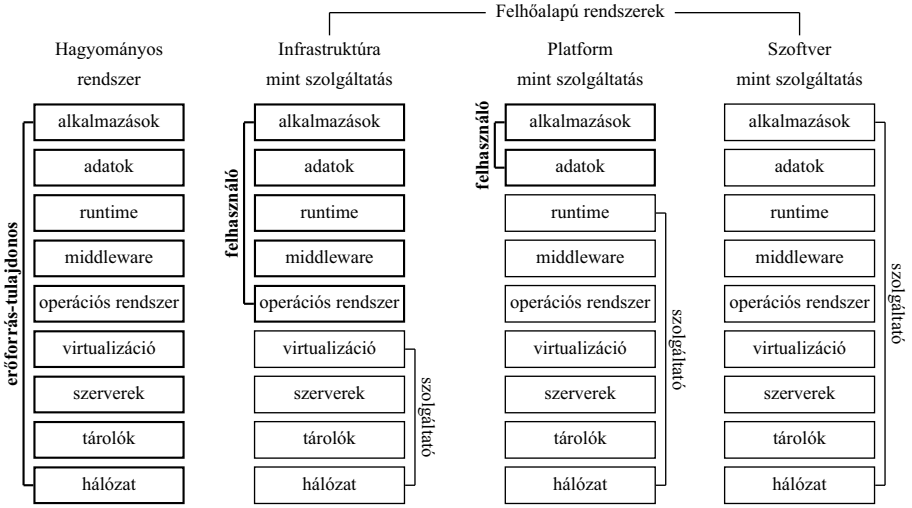
Az egyes modelleknél a felhasználó és a szolgáltató felelősségi körébe tartozó feladatokat jól szemlélteti a *4. számú ábra.*

Telepítési modellek (Deployment Models)

– Magán számítási felhő *(Private cloud):* a felhő-infrastruktúra kizárólag egy szervezet számára működik. Ezt a felhasználó szervezet, de akár egy másik fél is menedzselheti, fizikailag lehet akár a felhasználó telephelyén, akár azon kívül.
– Közösségi számítási felhő *(Community cloud):* ebben az esetben a felhő-infrastruktúrát több szervezet megosztottan használja úgy, hogy az az adott

4. számú ábra

Felelősségi körök megoszlása a szolgáltatási modellekben



Szerkesztette a szerző.

Forrás: http://blogs.cisco.com/wp-content/uploads/Seperation-of-Responsibility-inCloud.png

15 Lepenye Tamás: Számítási felhő – egyszerűen (2. rész). 2011. 06. 16. http://lepenyet.wordpress.com/2011/06/16/szmtsi-felho-egyszeruen-2-rsz/

közösség közös érdekeit támogassa (például közös küldetés, biztonsági követelmények, előírások, megfelelőségi szempontok). Ezt menedzselheti akár a felhasználó szervezet, akár egy másik fél is, fizikailag lehet a felhasználó telephelyén, akár azon kívül.

– 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. Ez tekinthető ma a legismertebb telepítési modellnek.
– Hibrid számítási felhő *(Hybrid cloud):* a felhő-infrastruktúra ekkor több, az előző modellek szerint felépülő rendszer (magán-, közösségi, nyilvános) keveréke, ahol a felhők megtartják egyedi jellegzetességeiket, azokat szabványosított vagy szabadalmazott technológiák kötik össze, lehetővé téve az adatok és alkalmazások hordozhatóságát (például cloudbursting technológia a felhők közötti terheléskiegyenlítésre, amikor a magánfelhőben rendelkezésre álló erőforrások elfogynak és azokat más, tipikusan nyilvános felhőben meglévőkkel pótolják ki.[16])

A szolgáltatási és a telepítési modellekből egyfajta mátrix képezhető. Ebben a mátrixban kell megtalálnia a felhasználónak a számára megfelelő szolgáltatást, azazhogy hová helyezi saját (meglévő vagy tervezett) hálózatát, és ennek mezőibe pozicionált termékek közül tudja kiválasztani a számára megfelelőket.

A téma szempontjából kiemelendő, hogy míg a fejlett országok felhőalapú rendszerekkel foglalkozó nemzeti és/vagy nemzetközi szervezetei a nagy tömegű érzékeny adattal dolgozó állami, kormányzati, önkormányzati szférában az információbiztonság szempontok okán a szolgáltatási modellek mindegyikét elfogadhatónak tartják, addig a telepítési modellek közül ez már nem mondható el mindegyikre. Az Európai Unió Hálózat- és Információbiztonsági Ügynöksége *(European Union Agency for Network and Information Security,* eredeti nevén: *European Network and Information Security Agency; ENISA)* szakértői megállapították, hogy éppen az érzékeny alkalmazásoknak és adatoknak köszönhetően a magán- és a közösségifelhő-modellek felelnek meg legjobban az állami feladatoknak, még akkor is, ha a méretbeli előnyök javarésze ebben az esetben eltűnhet.[17] Hasonlóan vélekednek a NIST szakem-

16 Bharath Chandrasekhar: What is Cloudbursting? 2011. 03. 15. http://cloudsecurity.trendmicro.com/what-is-cloudbursting/ ; Lepenye Tamás: Számítási felhő – egyszerűen (3. rész). 2011. 06. 17. http://lepenyet.wordpress.com/2011/06/17/szmtsi-felho-egyszeruen-3-rsz/

17 Daniele Catteddu (ed.): 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

berei is, szerintük az állami szervek inkább a magán- vagy közösségi felhőt preferálják, éppen azért, mert a biztonsági és adatvédelmi problémák a nyilvános felhőben jelentkeznek a legerősebben.[18] A magyarországi helyzetről elmondható, hogy a NISZ Zrt. egyik fő feladata, hogy közösségifelhő-alapú szolgáltatást kínáljon az említett hazai szektor szereplőinek, amelyen belül IaaS, Paas és SaaS szolgáltatásokat is nyújt.

Összegzés, javaslatok

A tanulmányban összefoglaltam Magyarország kibervédelmének főbb elemeit, kiemelve a téma szempontjából legfontosabb stratégiát, jogszabályokat és szervezeteket. Ez után bemutattam az állami, önkormányzati infokommunikációs rendszerek konszolidálása okán létrejövő szolgáltató-felhasználói modellt, és annak hatását a kibervédelemre, amelynek kapcsán rámutattam, hogy a jelenlegi jogszabályok az ebből adódó feladat- és felelősségelhatárolást nem kezelik. Rávilágítottam, hogy a hazánkban kijelölt központi szolgáltató, a NISZ Zrt. említett jogszabályokban leírt feladatainak ellátását úgy végezheti el, hogy alapvetően felhőalapú szolgáltatásokat nyújt, ezért összefoglaltam a felhőalapú rendszerek tulajdonságait, csoportosításukat. Bemutattam azt is, hogy a nagy nemzetközi szervezetek ezek közül melyeket ajánlják az állami intézmények számára és a NISZ Zrt. melyben szolgáltat.

Ezek pedig már megteremtik az alapot arra, hogy megvizsgáljuk a biztonság mint szolgáltatás alapelveit és alapfeltételeit. Ezekről lesz szó a tanulmány második részében.

FELHASZNÁLT JOGSZABÁLYOK
(2017. augusztus 1-jei állapot)

346/2010. (XII. 28.) kormányrendelet a kormányzati célú hálózatokról

309/2011. (XII. 23.) kormányrendelet a központosított informatikai és elektronikus hírközlési szolgáltatásokról

84/2012. (IV. 21.) kormányrendelet egyes, az elektronikus ügyintézéshez kapcsolódó szervezetek kijelöléséről

2012. évi CLXVI. törvény a létfontosságú rendszerek és létesítmények azonosításáról, kijelöléséről és védelméről

18 Wayne Jansen – Timothy Grance: Guidelines on Security and Privacy in Public Cloud Computing. 2011. 12. http://csrc.nist.gov/publications/nistpubs/800-144/SP800-144.pdf

1139/2013. kormányhatározat Magyarország Nemzeti Kiberbiztonsági Stratégiájáról

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

7/2013. (II. 26.) NFM rendelet a központosított informatikai és elektronikus hírközlési szolgáltatásokat egyedi szolgáltatási megállapodás útján igénybe vevő szervezetekről, valamint a központi szolgáltató által üzemeltetett vagy fejlesztett informatikai rendszerekről

41/2015. (VII. 15.) BM rendelet az állami és önkormányzati szervek elektronikus információbiztonságáról szóló 2013. évi L. törvényben meghatározott technológiai biztonsági, valamint a biztonságos információs eszközökre, termékekre, továbbá a biztonsági osztályba és biztonsági szintbe sorolásra vonatkozó követelményekről

186/2015. (VII. 13.) kormányrendeletet a központosított informatikai és elektronikus hírközlési szolgáltató információbiztonsággal kapcsolatos feladatköréről

451/2016. (XII. 19.) kormányrendelet az elektronikus ügyintézés részletszabályairól