DOI: 10.38146/BSZ.2018.5.3

KOVÁCS ZOLTÁN – MIKÓ ZOLTÁN – SÁGI GÁBOR

A biztonság mint szolgáltatás megteremtésének lehetőségei az állami, önkormányzati elektronikus információs rendszerek esetében II.

A cikksorozat első része[1] összefoglalta Magyarország kibervédelmének főbb elemeit, bemutatva a téma szempontjából legfontosabb stratégiát, jogszabályokat és szervezeteket. Ez után ismertette az állami, önkormányzati infokommunikációs rendszerek konszolidálása okán létrejött szolgáltató-felhasználói modellt, és annak hatását a kibervédelemre. Eközben, mint a téma szempontjából az egyik leglényegesebb elemre, rámutatott, hogy a jelenleg hatályos, a kibervédelmet szavatolni kívánó jogszabályok csupán említik, de nem rögzítik egyértelműen a szolgáltató-felhasználói modellből fakadó feladat- és felelősségelhatárolást. Rávilágított arra is, hogy a hazánkban létrehozott központi szolgáltató, a NISZ Zrt. jogszabályokban leírt feladatainak ellátását úgy tudja elvégezni, hogy alapvetően felhőalapú szolgáltatásokat nyújt, ezért összefoglalta a felhőalapú rendszerek tulajdonságait, csoportosításukat. Bemutatta azt is, hogy a nagy nemzetközi szervezetek ezek közül melyeket ajánlják az állami intézmények számára és a NISZ Zrt. melyben szolgáltat.

Ezt követően célszerű elemezni a biztonság mint szolgáltatás alapelveit, majd megvizsgálni, hogy hazánkban az állami és önkormányzati szférában a bevezethetőségnek milyen alapfeltételei, esetleg nehézségei vannak.

A biztonság mint szolgáltatás alapelvei és alapdokumentumai

A biztonság mint szolgáltatás alapelveit a felhőalapú rendszerek biztonságával foglalkozó, iparági szakemberek, vállalatok és más érintettek széles koalíciója által vezetett nonprofit szervezet, a Cloud Security Alliance (CSA) által közzétett dokumentumokból célszerű megismerni és átvenni.

1 Megjelent a Belügyi Szemle 2018/4. számában.

Ahogyan ugyanis a felhőalapú rendszerek meghatározásánál és kategorizálásánál a NIST Információtechnológiai Laboratóriuma által kiadott tanulmány[2] általánosan elfogadottnak és kváziszabványnak tekinthető, úgy a biztonság kapcsán a CSA kiadványáról[3] mondható el ugyanez.

A dokumentumban a felhőalapú rendszerekkel kapcsolatos biztonsági kérdéseket a CSA szakemberei alapvetően tizennégy területre osztják, ezeket két fő részbe csoportosítják: irányításiba és üzemeltetésibe. Az irányítási

1. számú táblázat

A CSA által definiált irányítási területek

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

Szerkesztette: Kovács Zoltán

Forrás: Security Guidance for Critical Areas of Focus in Cloud Computing V3.0. 2011. https://cloudsecurityalliance.org/guidance/csaguide.v3.0.pdf

2 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

3 Security Guidance for Critical Areas of Focus in Cloud Computing V3.0. 2011. https://cloudsecurityalliance.org/guidance/csaguide.v3.0.pdf

részben az általuk stratégiainak, míg az üzemeltetési részben az operatívnak tartott biztonsági kérdésekre koncentrálnak. A CSA által definiált területeket és azok rövid leírását az *1.* és a *2. számú táblázat* tartalmazza.

A CSA 2009 áprilisában adta ki először az említett tanulmányát, V4.0 változatát 2017-ben tette közzé. A V3.0 változatban újdonságként már megjelent a biztonság mint szolgáltatás, azaz Security as a Service (SecaaS) fogalma is

2. számú táblázat

A CSA által definiált üzemeltetési területek

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

Biztonság mint szolgáltatás (Security as a Service)
A felhasználónak egy külső fél nyújtotta, biztonságot szavatoló, incidenskezelési, megfelelőségigazolási, valamint azonosítás- és hozzáférés-szabályozási funkciók szolgáltatásáról szól. A biztonság mint szolgáltatás az észlelésnek, a kárenyhítésnek, és a biztonsági infrastruktúra irányításának az átruházása egy megfelelő eszközökkel és szakértelemmel felvértezett, megbízható harmadik félre.
Kapcsolódó technológiák
Már létező, és kialakulóban lévő technológiák, amelyek szoros kapcsolatban vannak a felhőalapú rendszerekkel, beleértve a big datát, a tárgyak internetét (IoT) és a mobil számítástechnikát.

Szerkesztette: Kovács Zoltán

Forrás: Security Guidance for Critical Areas of Focus in Cloud Computing V3.0. 2011, pp. 24–25. https://cloudsecurityalliance.org/guidance/csaguide.v3.0.pdf

(a *2. számú táblázat* utolsó előtti területe). Ennek bevezetésére a szerzők szerint azért van szükség, mert míg a felhőalapú rendszerek biztonságáról szóló fejtegetések túlnyomóan arra fókuszálnak, hogyan migráljunk felhőbe, hogyan gondoskodjunk a bizalmasságról, sértetlenségről és a rendelkezésre állásról, és hogyan védjük az adatok tárolását, feldolgozását szavatoló helyszíneket, addig a SecaaS egy teljesen új területet jelent, hiszen a vállalati biztonságot közelíti meg a felhőből nézve.

Szintén 2011-ben jelentette meg tanulmányát[4] a Cloud Security AllianceSM Security as a Service Working Groupja, ez 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 tíz kategóriát különböztet meg a biztonság mint szolgáltatás (Security as a Service) területen belül *(3. számú táblázat)*.

A CSA már megkezdte egy *Defined Categories of Service v2.0* című dokumentum kidolgozását is, amelyben az előbbiek mellett várhatóan két új kategória is megjelenik: a folyamatos felügyelet és a sérülékenységvizsgálat. A folyamatos felügyeletről már 2016-ban meg is jelentették a még nem végleges, előzetes dokumentumukat, amelyben a kategóriák leírása résznél a két új témakör definiálása kapcsán a következőket találjuk *(4. számú táblázat)*.

Az említett két, már hivatalosan kiadott dokumentumban is jól megfigyelhető, hogy átfedések vannak a CSA által alapként megadott irányítási és üze-

4 Defined Categories of Service 2011. https://cloudsecurityalliance.org/wp-content/uploads/2011/09/SecaaS_V1_0.pdf

3. számú táblázat

A CSA által definiált SecaaS-kategóriák

1. kategória: azonosítás, jogosultság- és hozzáférés-kezelés (IAM)[5]
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, továbbítása, mozgása és használata közben a felhőben és a telephelyen egyaránt.
3. kategória: webbiztonság
A webbiztonság a felhasználó telephelyén telepített és futtatott szoftver, alkalmazás segítségével, vagy a teljes webforgalom felhőszolgáltatóhoz történő átirányításával és ott történő ellenőrzésével valósít meg valós idejű védelmet.
4. kategória: e-mail-biztonság
Az e-mail-biztonság kontrollt ad 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 szavatoló 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: behatoláskezelés
A behatoláskezelés egy mintázatfelismerésen alapuló folyamat, amely segít a statisztikailag szokatlan események érzékelésében és a reagálásban. Ez magában foglalja a rendszerkomponensek valós idejű újrakonfigurálását is egy behatolás megállítása, megakadályozása érdekében.
7. kategória: biztonsági információs és eseménykezelő rendszer (SIEM[6])
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 lehessenek bizonyítékként a későbbi vizsgálat során.
8. kategória: titkosítás
A titkosítás egy kriptográfiai algoritmust felhasználó adatkódolási folyamat, amelynek eredményeképpen titkosított adatok jönnek létre.

5 IAM: Identity and Access Management = azonosítás és hozzáférés-kezelés.

6 SIEM: Security information and event management = biztonsági információs és eseménykezelő (szoftver) rendszer.

9. kategória: üzletmenet-folytonosság és katasztrófaelhárítás
Az üzletmenet-folytonosság és katasztrófaelhárítás olyan intézkedéseket takar, amelyek tervezésével és végrehajtásával szavatolható 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. Architekturálisan a hálózatbiztonság olyan szolgáltatásokat nyújt, amelyek a hálózatok biztonsági kontrolljával foglalkoznak az egyedi hálózatok mögöttes erőforrásainak egyedi vagy összevontan történő figyelembevételével.

Szerkesztette: Kovács Zoltán

Forrás: Defined Categories of Service 2011.
https://cloudsecurityalliance.org/wp-content/uploads/2011/09/SecaaS_V1_0.pdf

4. számú táblázat

A CSA által várhatóan definiálandó új kategóriák

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

Szerkesztette: Kovács Zoltán

Forrás: Defined Categories of Security as a Service (Preview) – Continuous Monitoring as a Service
https://downloads.cloudsecurityalliance.org/assets/research/security-as-a-service/csa-categories-securities-prep.pdf

meltetési területek és az üzemeltetési terület részét képező Security as a Service területnél leírt kategóriák között (például azonosítás és hozzáférés-menedzsment, titkosítás stb.). Ezek az átfedések több dolgot is jeleznek. Egyrészt, hogy a hagyományos ICT biztonsági elemek egy része a felhőalapú rendszerek esetében is használható, másrészt, hogy a felhőalapú rendszerek biztonsági problémái még mindig mennyire újszerűek, és még mindig nincsenek teljesen egzakt elhatárolások, definíciók, standardok. Utóbbiak kimunkálásán dolgoznak az iparág szereplői, beleértve olyan szervezeteket is, mint a CSA, az Európai Távközlési Szabvány Intézet *(European Telecommunications Standards Institute; ETSI)* vagy a Nemzetközi Távközlési Egyesület *(International Telecommunication Union; ITU)*.

Mivel a SecaaS akár egy a felhasználó által igénybe vett felhőalapú rendszer biztonsági kontrollját is jelentheti felhőből nyújtott ilyen irányú szolgálta-

tással, 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*ben leírtakat.

A felhőalapú rendszerek kockázatainak felmérésében, értékelésében szintén iparági alapdokumentumnak tekinthető a CSA táblázata[7] (a továbbiakban: CCM) a hozzá tartozó információs lappal együtt[8]. Ez alapvetően a szolgáltatók számára készített útmutató, ha úgy tetszik, egy biztonsági ellenőrző lista a megvalósítandó biztonságikontroll-funkciókról. A CCM a téma szempontjából kiemelendő tulajdonságai, hogy egyrészt az ebben leírt biztonsági elemek, kockázatok megfeleltetését is megadja szinte minden, széles körben használt szervezet, szabvány által azonosított biztonsági elemhez, kockázathoz (például BSI, COBIT, FedRAMP, ISO/IEC 27001 stb.), másrészt pedig megadja, hogy ezek közül melyik elem kinek (a szolgáltatónak vagy a felhasználónak) a felelősségi körébe tartozik. Ez pedig alapvető adatokkal segíti a téma, azaz a biztonság mint szolgáltatás bevezetése feltételeinek meghatározásához szükséges felelősségelhatárolás elvégzését.

A SecaaS bevezetésének alapfeltételei

A biztonság mint szolgáltatás bevezetésének alapfeltétele a szolgáltató és a felhasználó közötti felelősség pontos és egyértelmű elhatárolása. Így van ez a normál piaci alapú szolgáltatás esetében is, ahol a menedzselt biztonsági szolgáltatók (MSSP[9]) közzéteszik szolgáltatási katalógusukat, és a felelősségi köröket az általános szerződési feltételek (ÁSZF) mellett az egyedileg kötött szerződésekben rögzítik. Ebben az esetben a kiberbiztonságot kiszervező cég általában maga dönt – az iparági jó gyakorlatok és az esetleg meglévő anyavállalati és/vagy hatósági előírások alapján – arról, hogy milyen biztonsági kontrollokat kíván megvalósítani, és azok közül melyeket szervezi ki az MSSP-hez, és melyeket látja el saját maga.

---

7 Cloud Controls Matrix v3.0.1. 2014. 07. 11. https://cloudsecurityalliance.org/research/ccm/#_downloads

8 Cloud Controls Matrix v3.0.1 Info Sheet. 2014. 07. 29. https://cloudsecurityalliance.org/download/cloud-controls-matrix-v3-0-1-info-sheet/

9 MSSP: managed security service provider = menedzselt biztonsági szolgáltató. Működési területe a kiszervezett biztonsági feladatok ellátása a felhasználó igénye szerint, beleértve a tanácsadást és támogatást, hálózat-, alkalmazás- és végpontbiztonsági elemek kiépítését, működtetését, a felügyelt rendszerek biztonsági állapotának nyomon követését és kiértékelését, a biztonsági incidensek kezelését, a

Magyarországon a kormányzati, önkormányzati rendszerek esetében *az állami és önkormányzati szervek elektronikus információbiztonságáról* szóló 2013. évi L. törvény[10] (a továbbiakban: Ibtv.), és *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 végrehajtáshoz szükséges szabályozók* című 41/2015. (VII. 15.) BM rendelet[11] egyértelműen előírja a megvalósítandó biztonsági kontrollokat. Ezek a kontrollok a NIST 800-53[12] előírásain alapulnak. Mindamellett a hazai jogszabályok egyértelműen arra a modellre épülnek, amikor az elektronikus információs rendszer teljes egészében az azt használó szervezeté, akárcsak az abban kezelt adatok és azok kezelésének, feldolgozásának összes folyamata is. Ennek megfelelően az ezekben a jogszabályokban előírt információbiztonsági kontrollok megvalósítását is egységesen kezeli, a felelősség elhatárolásának a gondolata megjelenik ugyan a szövegben, ám azok tényleges, egyértelmű szétválasztása már nem történt meg.

Ma Magyarországon azonban teljesen más a valós helyzet. A magasabb színvonalú, korszerűbb és olcsóbb infokommunikációs rendszerek biztosítása miatt kialakult az a fajta szolgáltatói modell, ahol a NISZ Zrt. mint központi kormányzati infokommunikációs szolgáltató kínálja az egyes intézmények működéséhez szükséges elektronikus információs rendszerek egy részét (például hálózatot, tárolókat, szervereket, virtualizációt stb.), az adott intézmény pedig a többit. Mindemellett a NISZ Zrt. adatfeldolgozói szerepkörben van[13], azaz az adatokhoz való hozzáférése és az azokon, általa elvégezhető műveletek lehetősége, a releváns jogszabályok alapján korlátozott, azok élesen elválnak az adatkezelői feladatoktól.

A hazai viszonyokat tovább bonyolítja, hogy vannak olyan rendszerek is, amelyekben nem csupán két, hanem három, vagy akár több szereplő is található. Az ilyen rendszerek esetében az első kapcsolat a NISZ Zrt. és egy másik

---

sérülékenység- és fenyegetettségmenedzsmentet. From the Gartner IT Glossary: What is an MSSP? http://www.gartner.com/it-glossary/mssp-managed-security-service-provider/

10 https://net.jogtar.hu/jr/gen/hjegy_doc.cgi?docid=a1300050.tv

11 https://net.jogtar.hu/jr/gen/hjegy_doc.cgi?docid=a1500041.bm

12 Security and Privacy Controls for Federal Information Systems and Organizations NIST Special Publication 800-53 Revision 4. 2013. 04. http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf

13 A cikk nem foglalkozik a NISZ Zrt. által a saját működése érdekében létesített és fenntartott rendszerekkel, ahol adatkezelői szerepköre van. A téma szempontjából kizárólag azok a rendszerek érdekesek, amelyeket a NISZ Zrt. szolgáltatásként biztosít az ügyfelei számára, ám ezek esetében a NISZ Zrt. adatfeldolgozói szerepkört lát el.

intézmény között jön létre, ahol a NISZ Zrt. infrastruktúra-szolgáltatást nyújt a második szereplőnek. A második szereplő azonban a NISZ Zrt. által biztosított infrastruktúrán már SaaS szolgáltatást nyújt a harmadik szereplőnek. Ebben a felállásban a NISZ Zrt. és a második szereplő is adatfeldolgozói, míg a harmadik szereplő adatkezelői szerepkörben található, azaz a felelősségelhatárolás ily módon, csupán a korábban a jogszabályokban rögzített adatkezelő, adatfeldolgozó definíciókat felhasználva nem írható le egyértelműen. Célszerű tehát itt is már a szolgáltató-felhasználó modellt alkalmazni, hiszen az így elvégzett felelősségelhatárolás egyértelmű lesz az ilyen szituációkban is, és függetlenné válik az adatkezelői, -feldolgozói szerepköröktől. Amennyiben ugyanis egyértelműen szétválasztódnak az egyes felhőalapú szolgáltatások kapcsán (IaaS, PaaS, SaaS) a 41/2015. (VII. 15.) BM rendelet által előírt, megvalósítandó egyes biztonsági kontrollok kialakításának és működtetésének kötelezettségei a szolgáltató és a felhasználó között, akkor az említett példában a NISZ Zrt. és a második szereplő között az IaaS szerinti szolgáltató-felhasználó felelősségelhatárolást lehet majd alkalmazni, míg a második és a harmadik szereplő között a SaaS szerinti szolgáltató-felhasználó felelősségelhatárolás lesz felhasználható. A szolgáltatói-felhasználói modell alkalmazásával tehát minden eset – függetlenül a résztvevők számától és adatkezelői, adatfeldolgozói szerepkörétől – egyértelműen és pontosan leírhatóvá válik.

Mindazonáltal jelenleg még sehol nincs ténylegesen szabályozva az információbiztonsági kontrollok kialakításának felelőssége és felelősségi határai, azazhogy egy adott esetben melyek a szolgáltató, és melyek a felhasználó által elvégzendő feladatok, a szereplők közül ki melyik kontrollt valósítja meg. Ez pedig amellett, hogy problémát okoz a jogszabály által előírt információbiztonsági kontrollok teljes körű kialakításánál, a biztonság mint szolgáltatás bevezetését gyakorlatilag el is lehetetleníti. Amíg ugyanis vita tárgyát képez(het)i, hogy mely kontrollokat kell például egy infrastruktúra mint szolgáltatás esetében a szolgáltatónak kötelező módon biztosítania, és melyek a felhasználó által megteendő intézkedések, addig az is vitatott lesz, hogy melyek – ez utóbbira építhető – a biztonság mint szolgáltatás körébe tartozók, azaz melyek azok, amelyekre külön díjszabás mellett lehet külön szerződést kötni.

Az elektronikus információk biztonságát szavatoló kontrollok szolgáltató és felhasználó közötti felosztását érdemes a felhőalapú rendszerek esetén használt és általánosan elfogadottnak tekinthető felelősségi körök elhatárolására alapozni.[14]

14 Lásd a tanulmány első részében látható 4. számú ábrát!

Az elhatárolást azért is érdemes erre alapozni, mert – ahogy a cikksorozat első részében bemutattuk – a NISZ Zrt. is gyakorlatilag felhőszolgáltatónak tekinthető. Az esetek többségében ugyanis infrastruktúra, platform vagy szoftver mint szolgáltatást nyújt, teljesítve azokat a kritériumokat, amelyek alapján a NIST definíciója szerint felhőalapúnak nevezhetjük az adott szolgáltatást. Az ezekből kilógó, de a téma miatt az ezekhez szorosan kapcsolódó és a tanulmány első részében szintén ismertetett szolgáltatások (hosting, menedzselt munkaállomás-szolgáltatás) esetén pedig vagy némi módosítással szintén jól alkalmazhatók lesznek a kidolgozott felelősségi elhatárolások, vagy pedig más szolgáltatások esetén már ismert és elfogadott felelősségi elhatárolások lesznek egyszerűen alkalmazhatók. Így például amíg a hosting szolgáltatás esetén az iparági jó gyakorlatnak megfelelő, mindenki által elfogadott felelősségelhatárolás felhasználható, addig például azon rendszerek esetében, amelyeknél a NISZ Zrt. nem csupán szoftver mint szolgáltatást, de a felhasználói végkészüléket is biztosítja, ott a szoftver mint szolgáltatásnál alkalmazott felelősségelhatárolás további kiterjesztése lehet a megoldás. Ezt az állami, önkormányzati rendszerek esetében alkalmazandó, alapvető felelősségelhatárolási mátrixot mutatja az *5. számú táblázat.* A táblázat elemei a szolgáltató szemszögéből rögzítik a kötelező vagy éppen szolgáltatásként nyújtható elemeket.

A felelősségi körök elhatárolásának egy potenciális módszertana

Annak érdekében, hogy az *5. számú táblázat*ban meghatározott felelősségelhatárolás a gyakorlatban is alkalmazható legyen, pontosan meg kell határozni, hogy melyek azok az információbiztonsági elemek, amelyeket a szolgáltatónak, azaz a NISZ Zrt.-nek IaaS, PaaS, vagy SaaS szolgáltatás esetén nyújtania kell. Ehhez a korábban már említett Ibtv.-ből és a 41/2015. (VII. 15.) BM rendeletből kell kiindulni, amely egyértelműen előírja a megvalósítandó biztonsági kontrollokat. Ugyanakkor két ok miatt célszerű figyelembe venni a korábban szintén említett CSA CCM táblázatot is. Az egyik ok az ugyanis, hogy a CCM amellett, hogy a szolgáltatók számára készített biztonsági ellenőrző listának tekinthető, egyrészt olyan oszlopokat is tartalmaz, amelyek megmutatják, hogy az egyes biztonsági kontrollok megvalósítását a szolgáltató mellett a felhasználó felelősségi körébe tartozónak is értékelték-e a CSA szakemberei, másrészt azt is, hogy az adott kontroll IaaS, PaaS, vagy SaaS

5. számú táblázat

Alapvető felelősségelhatárolási mátrix – a szolgáltató szemszögéből

		A szolgáltató által nyújtott biztonsági szolgáltatás		
		IaaS-nak	PaaS-nak	SaaS-nak
		megfelelő információbiztonsági szolgáltatások		
A felhasználó által igénybe vett szolgáltatás	SaaS + végfelhasználói munkaállomások	kötelező	kötelező	kötelező + kötelező kiegészítő elemek
	SaaS	kötelező	kötelező	kötelező
	PaaS	kötelező	kötelező	szolgáltatás
	IaaS	kötelező	szolgáltatás	szolgáltatás
	hosting	kötelező + szolgáltatási elemek	szolgáltatás	szolgáltatás

Szerkesztette: Kovács Zoltán

esetén értelmezhető-e. A másik ok pedig az, hogy miután a CCM – a korábban említettek szerint – az iparági ajánlásokra épül, így feldolgozta és tartalmazza a 41/2015. (VII. 15.) BM rendelet alapjául szolgáló NIST 800-53 ajánlásban szereplő biztonsági kontrollokat is. Ráadásul mindezt úgy, hogy az általa definiált biztonsági kontrollokhoz egyértelműen megfelelteti, hogy az melyik ajánlás melyik kontrolljának felel meg.

A leírtakból kiindulva, a 41/2015. (VII. 15.) BM rendelet kontrollpontjait megfeleltetve a NIST 800-53 elemeinek, majd ezeket visszakeresve a CCM-ben, előállítható egy olyan lista, amely a CSA ajánlásán alapulva tételesen megadja az egyes információbiztonsági kontrollok felelőseit. A 41/2015. (VII. 15.) BM rendeletben megadott biztonsági kontrollok NIST 800-53-nak történő tételes megfeleltetése (visszafeleltetése) után ugyanis a CCM-ből kikereshető, hogy az egyes biztonsági kontrollpontoknál kit jelöltek meg felelősnek a CSA szakemberei.

A 41/2015. (VII. 15.) BM rendelet és a CCM összefuttatása után megkapott listából két dolog látszik.

Az első, hogy a CCM-ben maradtak olyan ajánlott biztonsági kontrollok, amelyek teljesítése a 41/2015. (VII. 15.) BM rendeletben nincsen előírva *(6. számú táblázat)*.

Ezek esetében úgy célszerű eljárni, hogy az előbbiekben leírt elemeket nem kötelező, hanem lehetőség szerint megvalósítandónak kell feltüntetni, és ezáltal – visszautalva az *5. számú táblázat*ban foglaltakra – a biztonság mint

6. számú táblázat

A nem kötelezően megvalósítandó biztonsági kontrollok listája

CCM V3.0.1 kontrollazonosító: DSI-02	**kontrollterület:** adatbiztonság és információéletciklus-menedzsment adatleltár/adatáramlás
Frissített kontroll-leírás, segédlet: A helyinek (állandó vagy ideiglenes jelleggel) minősülő adatok leltárba vételére, dokumentálására és az adatáramlás fenntartására a szolgáltatáshoz kapcsolódó földrajzilag elosztott (fizikai és virtuális) alkalmazások és az infrastruktúra hálózati és rendszerelemei között és/vagy azok harmadik felekkel történő megosztására szabályzatokat és eljárásokat kell létrehozni, és ezeket támogató üzleti folyamatokkal és technikai intézkedésekkel végrehajtatni, a szabályozási, jogszabályi vagy az ellátási láncra vonatkozó megállapodások (SLA) megfelelőségi hatásának megállapítása és egyéb, az adatokhoz kapcsolódó üzleti kockázatok kezelése érdekében. Igény esetén, a szolgáltató tájékoztatja az ügyfelet (bérlőt) a megfelelőségi hatásról és kockázatról, különösen, ha az ügyféladatokat a szolgáltatás részeként felhasználják.	
CCM V3.0.1 kontrollazonosító: DCS-01	**kontrollterület:** adatközpont-biztonság eszközmenedzsment
Frissített kontroll-leírás, segédlet: Az eszközöket be kell sorolni üzleti kritikusság, a szolgáltatásiszint-elvárások és a működési folytonossági követelmények alapján. Az összes telephelyen és/vagy földrajzi területen jelenlévő üzleti szempontból kritikus eszközről és azok használatáról teljes leltárt kell fenntartani és rendszeres időközönként aktualizálni, meghatározott szerepekkel és felelősségekkel tulajdonost kijelölni.	
CCM V3.0.1 kontroll azonosító: EKM-01	**kontrollterület:** titkosítás- és kulcsmenedzsment jogosultság
Frissített kontroll-leírás, segédlet: A kulcsoknak azonosítható tulajdonosaik kell, hogy legyenek (azonosítóhoz kötött kulcsok), és kell lenniük kulcskezelési szabályzatoknak is.	
CCM V3.0.1 kontrollazonosító: EKM-04	**kontrollterület:** titkosítás- és kulcsmenedzsment tárolás és hozzáférés
Frissített kontroll-leírás, segédlet: Meg kell követelni a platformnak és az adatoknak megfelelő titkosítást (például AES-256) nyílt/érvényesített formátumokban és szabványos algoritmusokban. A kulcsok nem tárolhatók a felhőben (azaz a kérdéses felhőszolgáltatónál), de karbantarthatók a felhő felhasználója vagy megbízható kulcsmenedzsment-szolgáltató által. A kulcskezelésnek és kulcshasználatnak elkülönített feladatkörnek kell lennie.	

CCM V3.0.1 kontrollazonosító: IAM-04	**kontrollterület:** személyazonosság- és jogosultságkezelés irányelvek, eljárások
Frissített kontroll-leírás, segédlet: Szabályzatokat és eljárásokat kell létrehozni az azonosítási információ tárolására és kezelésére minden személyről, aki hozzáfér az IT-infrastruktúrához, továbbá a hozzáférési szintjeik megállapítására. Szintén szabályozni kell, felhasználói identitás alapon, a hálózati erőforrásokhoz való hozzáférést.	
CCM V3.0.1 kontrollazonosító: IAM-08	**kontrollterület:** személyazonosság- és jogosultságkezelés megbízható források
Frissített kontroll-leírás, segédlet: Szabályzatok és eljárások megállapítására kerül sor a hitelesítéshez használt azonosítók megengedett tárolásáról és hozzáféréséről, annak érdekében, hogy azok csak a legkisebb jogosultság elve és a replikációs korlátozások mellett legyenek elérhetők kizárólag azok számára, akiket egyértelműen meghatározott az üzleti igény.	
CCM V3.0.1 kontrollazonosító: IVS-02	**kontrollterület:** infrastruktúra- és virtualizációs biztonság változásészlelés
Frissített kontroll-leírás, segédlet: A szolgáltatónak biztosítania kell az összes virtuális gép lemezképének sértetlenségét. A virtuális gép lemezképein történő bármilyen változtatást naplózni kell, és a futási állapottól (például alvó, lekapcsolt, futó) függetlenül riasztani kell. Egy lemezkép változtatásának vagy mozgatásának eredményét és a lemezkép sértetlenségének ezt követő érvényesítését azonnal elérhetővé kell tenni az ügyfelek részére elektronikus úton (például portálok vagy riasztások segítségével).	
CCM V3.0.1 kontrollazonosító: IVS-05	**kontrollterület:** infrastruktúra- és virtualizációs biztonság sérülékenységkezelés
Frissített kontroll-leírás, segédlet: A kivitelezőknek biztosítaniuk kell, hogy a biztonságisérülékenység-értékelési eszközök vagy szolgáltatások magukban foglalják a használtban lévő virtualizációs technológiákat is (például a virtualizáció tudatosítása).	
CCM V3.0.1 kontrollazonosító: IVS-07	**kontrollterület:** infrastruktúra- és virtualizációs biztonság operációsrendszer-megerősítés és alapkontrollok
Frissített kontroll-leírás, segédlet: Minden operációs rendszert úgy kell megerősíteni, hogy csak az üzleti igényhez szükséges portokat, protokollokat és szolgáltatásokat nyújtsa, valamint már az alapszintű szabványra vagy sablonra épülő üzemüzemelés részeként is ki legyenek alakítva az olyan technikai támogató intézkedések, mint antivírus-, fájlsértetlenség-ellenőrzés, naplózás.	

CCM V3.0.1 kontrollazonosító: IVS-10	**kontrollterület:** infrastruktúra- és virtualizációs biztonság virtuálisgép-biztonság – adatvédelem
Frissített kontroll-leírás, segédlet: Biztonságos és titkosított kommunikációs csatornákat kell alkalmazni a fizikai szerverek, alkalmazások vagy adatok virtuális szerverekre történő áttelepítésekor, és ahol lehetséges, az ilyen áttelepítés a termelő hálózattól szeparált hálózaton történjen.	
CCM V3.0.1 kontrollazonosító: IVS-11	**kontrollterület:** infrastruktúra- és virtualizációs biztonság hiperfelügyelő-megerősítés
Frissített kontroll-leírás, segédlet: A hozzáférés minden hiperfelügyelő (hypervisor) menedzsmentfunkcióhoz vagy virtuális rendszert kezelő konzolfelülethez korlátozva kell, hogy legyen a legkisebb jogosultság elve szerint, és ezt technikai intézkedésekkel kell támogatni (például kétfaktoros hitelesítés, ellenőrző nyomvonalak, IP-cím-szűrés, tűzfalak, és a TLS zárt kommunikáció a konzolfelületekhez).	
CCM V3.0.1 kontrollazonosító: IVS-13	**kontrollterület:** infrastruktúra- és virtualizációs biztonság hálózati architektúra
Frissített kontroll-leírás, segédlet: Hálózati architektúradiagramoknak világosan meg kell határozniuk azokat a nagy kockázatú környezeteket és adatáramlásokat, amelyeknek jogi megfelelőségi hatásai lehetnek. Műszaki intézkedéseket kell bevezetni és mélységi védelmi technikákat kell alkalmazni (például mély csomagvizsgálat, a forgalom szabályozása és korlátozása) az abnormális be- vagy kimeneti forgalomhoz kapcsolódó hálózati támadások (például MAC címhamisítás, ARP mérgezéses támadás) vagy elosztott túlterheléses támadások DDoS) detektálására és az idejében történő reagálásra.	
CCM V3.0.1 kontrollazonosító: IPY-01	**kontrollterület:** átjárhatóság és hordozhatóság APIs
Frissített kontroll-leírás, segédlet: A szolgáltatónak nyílt és publikus alkalmazásprogramozási felületet (API) kell használnia az összetevők közötti interoperabilitás támogatása és az alkalmazások költözésének megkönnyítése érdekében.	
CCM V3.0.1 kontrollazonosító: IPY-02	**kontrollterület:** átjárhatóság és hordozhatóság adatok kérése
Frissített kontroll-leírás, segédlet: Minden strukturált és strukturálatlan adatnak elérhetőnek kell lennie az ügyfél számára, és kérésre szabványos formátumban (például .doc, .xls, .pdf, naplófájlok) át is kell adni neki.	

CCM V3.0.1 kontrollazonosító: IPY-03	**kontrollterület:** átjárhatóság és hordozhatóság irányelvek, eljárások, rendelkezések
Frissített kontroll-leírás, segédlet: Irányelveket, szabályzatokat, eljárásokat, és kölcsönösen elfogadott rendelkezéseket és/vagy feltételeket kell megállapítani, kialakítani, az ügyfelek (bérlők) alkalmazásprogramozási felületre (API), az információfeldolgozás interoperabilitására, az alkalmazások fejlesztésére és információcseréjére, használatára, valamint a sértetlenség fenntartására vonatkozó követelményeinek megfelelően.	
CCM V3.0.1 kontrollazonosító: IPY-04	**kontrollterület:** átjárhatóság és hordozhatóság szabványos hálózati protokollok
Frissített kontroll-leírás, segédlet: A szolgáltató csak biztonságos (például nem nyílt szöveget és hitelesítést használó) szabványosított hálózati protokollokat használhat az adatok importálására és exportálására a szolgáltatások menedzseléséhez és a fogyasztók (bérlők) rendelkezésére kell bocsátania (elérhetővé tennie) azokat a dokumentumokat, amelyek magukban foglalják, részletezik a vonatkozó interoperabilitási és hordozhatósági szabványokat.	
CCM V3.0.1 kontrollazonosító: IPY-05	**kontrollterület:** átjárhatóság és hordozhatóság virtualizáció
Frissített kontroll-leírás, segédlet: Az interoperabilitás biztosítása érdekében a szolgáltatónak az iparág által elismert virtualizációs platformot és szabványos virtualizációs formátumot (például OVF) kell alkalmaznia, hogy elősegítse az együttműködési képességet, és bármely hiperfelügyelőben végzett testre szabást dokumentálnia kell, és minden megoldásspecifikus virtualizációs megoldást az ügyfél rendelkezésére kell bocsátania.	
CCM V3.0.1 kontrollazonosító: MOS-01	**kontrollterület:** mobileszköz-biztonság[15] rosszindulatú programok elleni védelem
Frissített kontroll-leírás, segédlet: A mobil eszközökre vonatkozó kártékony szoftverek elleni küzdelemre vonatkozó tudatosságnövelő képzést fel kell venni a szolgáltató információbiztonsági tudatosság képzései közé.	
CCM V3.0.1 kontrollazonosító: MOS-02	**kontrollterület:** mobileszköz-biztonság alkalmazásboltok
Frissített kontroll-leírás, segédlet: Meg kell határozni azon jóváhagyott alkalmazásboltok dokumentált listáját, amelyek elfogadhatók, hogy azokról a mobil eszközökről elérjék őket, amelyekkel hozzáférnek a szolgáltató által kezelt vagy tárolt adatokhoz.	

15 Amíg a mobil eszközök biztonsága kapcsán a CCM alapvetően a BYOD (Bring Your Own Device, azaz Hozd a saját eszközöd; a munkavállalók a saját eszközeiket használják a mindennapi munkavégzéskor) eszközökre és a mobiltelefonokra, okostelefonokra helyezi a hangsúlyt, addig a 41/2015. (VII. 15.) BM rendelet elsősorban a(z állami) cég által biztosított hordozható számítógépekre (notebook). Éppen ezért kerültek a CCM-ben leírt kontrollpontok ide, a választható kategóriába.

CCM V3.0.1 kontrollazonosító: MOS-03	**kontrollterület:** mobileszköz-biztonság jóváhagyott alkalmazások
Frissített kontroll-leírás, segédlet: A cégnek rendelkeznie kell dokumentált szabályzatokkal, irányelvekkel, amelyek tiltják a nem jóváhagyott alkalmazások telepítését vagy a jóváhagyott alkalmazások nem előre meghatározott forrásból történő letöltését.	
CCM V3.0.1 kontrollazonosító: MOS-04	**kontrollterület:** mobileszköz-biztonság jóváhagyott szoftverek BYOD-ra (saját mobil eszközre)
Frissített kontroll-leírás, segédlet: A BYOD-szabályzat és az ezt támogató tudatosságnövelő képzés világosan meghatározza a jóváhagyott alkalmazásokat, alkalmazás-áruházakat és az alkalmazáskiterjesztéseket és plugineket, amelyek használhatók BYOD alkalmazásakor.	
CCM V3.0.1 Kontroll azonosító: MOS-05	**kontrollterület:** mobileszköz-biztonság tudatosítás és képzés
Frissített kontroll-leírás, segédlet: A szolgáltatónak kell, hogy legyen dokumentált mobileszköz-szabályzata, amely tartalmazza a mobil eszközök dokumentált meghatározását, és az összes mobil eszköz elfogadható felhasználását és követelményeit. A szolgáltatónak közzé kell tennie és kommunikálnia kell a szabályzatot és követelményeket a vállalat biztonsági tudatossági és oktatási programjai keretében.	
CCM V3.0.1 kontrollazonosító: MOS-06	**kontrollterület:** mobileszköz-biztonság felhőalapú szolgáltatások
Frissített kontroll-leírás, segédlet: Előzetesen jóvá kell hagyatni minden felhőalapú szolgáltatást, amelyeket a cég üzleti adatainak felhasználására és tárolására használnak a vállalati mobil eszközökkel vagy BYOD-készülékekkel.	
CCM V3.0.1 kontrollazonosító: MOS-07	**kontrollterület:** mobileszköz-biztonság kompatibilitás
Frissített kontroll-leírás, segédlet: A cégnek kell, hogy legyen dokumentált alkalmazásérvényesítési folyamata, a mobil eszközök, operációs rendszerek és alkalmazáskompatibilitási problémáinak tesztelésére.	
CCM V3.0.1 kontrollazonosító: MOS-08	**kontrollterület:** mobileszköz-biztonság eszközjogosultság
Frissített kontroll-leírás, segédlet: A BYOD-szabályzat határozza meg a készülék- és jogosultsági követelményeket a BYOD használathoz.	

CCM V3.0.1 kontrollazonosító: MOS-09	**kontrollterület:** mobileszköz-biztonság eszközleltár
Frissített kontroll-leírás, segédlet: Az összes vállalati adat tárolásához és hozzáféréséhez használt mobil eszközről egy leltárt kell készíteni és fenntartani. Minden változást ezen eszközök állapotához képest szerepeltetni kell minden eszköz mellett a leltárban (például az operációsrendszer- és a patchszint, elveszett vagy forgalomból kivont állapot, és a készülék kinek van kiosztva vagy használatra engedélyezve (BYOD).	
CCM V3.0.1 kontrollazonosító: MOS-10	**kontrollterület:** mobileszköz-biztonság eszközmenedzsment
Frissített kontroll-leírás, segédlet: Egy központosított mobileszköz-menedzsment megoldást kell telepíteni az összes mobil eszközre, amelyen engedélyezett ügyféladatok tárolása, továbbítása vagy feldolgozása.	
CCM V3.0.1 Kontroll azonosító: MOS-11	**kontrollterület:** mobileszköz-biztonság titkosítás
Frissített kontroll-leírás, segédlet: A mobileszköz-szabályzat előírja a titkosítás használatát minden mobil eszközre, akár az egész készülékre, vagy az érzékenynek ítélt adatok tekintetében, és ezeket technológiai intézkedésekkel kell érvényesíteni.	
CCM V3.0.1 kontrollazonosító: MOS-12	**kontrollterület:** mobileszköz-biztonság mobil eszközök szoftveres feltörése (jailbreaking, rooting)
Frissített kontroll-leírás, segédlet: A mobileszköz-szabályzatnak meg kell tiltania a mobil eszközökbe épített biztonsági ellenőrzések megkerülését (például szoftveres feltörés jailbreaking, rooting), és érvényesítenie kell a tiltást az eszközökön nyomozati és megelőző kontrollok révén, vagy központi eszközkezelő rendszeren keresztül (például mobileszköz-menedzsment).	
CCM V3.0.1 kontrollazonosító: MOS-13	**kontrollterület:** mobileszköz-biztonság jogszabályok
Frissített kontroll-leírás, segédlet: A BYOD-szabályzatnak magában kell foglalnia a bizalmas adatok kezelésének nyelvezetét, a peresíthetőség feltételeit, az elektronikus felderítést, és az adatmegőrzési kötelezettségeket. A BYOD-szabályzatnak egyértelműen meg kell határoznia a vonatkozó elvárásokat a nem vállalati adatok elvesztésével kapcsolatban, ha az eszközön teljes törlés szükségessé válik.	

CCM V3.0.1 kontrollazonosító: MOS-14	**kontrollterület:** mobileszköz-biztonság képernyőzár
Frissített kontroll-leírás, segédlet: A BYOD és/vagy a vállalat tulajdonában lévő eszközökön automatikus képernyőzárat szükséges beállítani, és e követelményt technológiai intézkedésekkel kell érvényesíteni.	
CCM V3.0.1 kontrollazonosító: MOS-15	**kontrollterület:** mobileszköz-biztonság operációs rendszer
Frissített kontroll-leírás, segédlet: A mobil eszköz operációs rendszerén, patchszinteken és/vagy alkalmazásokon történő változástatásokat a vállalat változáskezelési folyamatán keresztül kell kezelni.	
CCM V3.0.1 kontrollazonosító: MOS-16	**kontrollterület:** mobileszköz-biztonság jelszavak
Frissített kontroll-leírás, segédlet: A mobil eszközökön alkalmazandó jelszószabályokat dokumentálni kell, és technológiai intézkedésekkel érvényesíteni kell minden vállalati eszközön és BYOD-használatra jóváhagyott eszközön, és tiltani kell a jelszó-/PIN-hossz- és hitelesítésikövetelmény-változtatást.	
CCM V3.0.1 Kontroll azonosító: MOS-17	**kontrollterület:** mobileszköz-biztonság irányelvek, eljárások
Frissített kontroll-leírás, segédlet: A mobileszköz-szabályzatnak elő kell írnia, hogy a BYOD-felhasználóknak az adatokról biztonsági másolatot kell készíteniük, és tiltania kell a nem jóváhagyott alkalmazás-áruházak használatát, valamint meg kell követelnie az anti-malware szoftver használatát (ahol támogatott).	
CCM V3.0.1 kontrollazonosító: MOS-18	**kontrollterület:** mobileszköz-biztonság távoli törlés
Frissített kontroll-leírás, segédlet: Minden, a vállalat BYOD-programjában engedélyezett vagy a vállalat által biztosított mobil eszköznél lehetővé kell tenni a távoli törlést a teljes eszköz vagy az összes vállalat által biztosított adat tekintetében a cég IT-részlege számára.	
CCM V3.0.1 kontrollazonosító: MOS-19	**kontrollterület:** mobileszköz-biztonság biztonsági frissítések
Frissített kontroll-leírás, segédlet: A vállalati hálózathoz kapcsolódó, vagy vállalati információt tároló vagy elérő mobil eszközök távoli szoftver verzió/patch érvényesítését engedélyezni kell. Minden mobil eszköznek rendelkeznie kell a legújabb biztonsági frissítés telepítésével, amelyet a gyártó vagy az eszköz használója kiadáskor telepít, vagy az erre meghatalmazott informatikai személyzetnek képesnek kell lennie ezeknek a frissítéseknek a távoli elvégzésére.	

CCM V3.0.1 kontrollazonosító: MOS-20	**kontrollterület:** mobileszköz-biztonság felhasználók
Frissített kontroll-leírás, segédlet: A BYOD-szabályzat meghatározza azokat a rendszereket és szervereket, amelyeket a BYOD-ként engedélyezett eszközökön használhatnak vagy azokról elérhetnek.	
CCM V3.0.1 kontrollazonosító: STA-01	**kontrollterület:** ellátásilánc-menedzsment, átláthatóság és elszámoltathatóság adatminőség és integritás
Frissített kontroll-leírás, segédlet: A szolgáltatók kivizsgálják, igazolják, és együttműködnek a felhőalapú ellátási láncban szereplő partnerekkel az adatminőségi hibák és az abból származó kockázatok kijavításában. A szolgáltatóknak olyan intézkedéseket kell tervezniük és végrehajtaniuk, amelyek csökkentik és kordában tartják a biztonsági kockázatokat a feladatok megfelelő szétválasztásával, szerepköralapú hozzáféréssel, és az ellátási lánc személyzetének a legkisebb jogosultságú hozzáférés biztosításával.	
CCM V3.0.1 kontrollazonosító: STA-02	**kontrollterület:** ellátásilánc-menedzsment, átláthatóság és elszámoltathatóság incidensjelentés
Frissített kontroll-leírás, segédlet: A szolgáltató a biztonsági eseményekkel kapcsolatos információkat minden érintett felhasználó és szolgáltató számára rendszeresen elektronikus formában (például portálokon keresztül) elérhetővé teszi.	
CCM V3.0.1 kontrollazonosító: STA-04	**kontrollterület:** ellátásilánc-menedzsment, átláthatóság és elszámoltathatóság szolgáltató belső értékelése
Frissített kontroll-leírás, segédlet: A szolgáltató köteles éves belső értékelést végezni a szabályzatai, folyamatai és az azokat támogató mértékek és mérőszámok megfelelőségéről és hatékonyságáról.	
CCM V3.0.1 Kontroll azonosító: STA-06	**kontrollterület:** ellátásilánc-menedzsment, átláthatóság és elszámoltathatóság ellátási lánc irányításának felülvizsgálata
Frissített kontroll-leírás, segédlet: A szolgáltatóknak felül kell vizsgálniuk a partnereik kockázatkezelési és -irányítási folyamatait, hogy a gyakorlatok következetesek és összehangoltak legyenek az adott partner felhőalapú ellátási láncának egyéb tagjaitól örökölt kockázatok figyelembevételekor.	

CCM V3.0.1 kontrollazonosító: STA-07	**kontrollterület:** ellátásilánc-menedzsment, átláthatóság és elszámoltathatóság ellátásilánc-mutatók
Frissített kontroll-leírás, segédlet: Szabályzatokat és eljárásokat kell létrehozni annak érdekében, hogy a szolgáltatók és az ellátási láncban (upstream/downstream) részt vevő ügyfelek (bérlők) közötti szolgáltatási szerződések (például SLA) következetes felülvizsgálatára kerüljön sor. A felülvizsgálatokat legalább évente kell elvégezni, és meg kell állapítani a nem megfelelőségeket a szerződési keretekhez képest. A felülvizsgálatoknak olyan cselekvési terveket kell eredményezniük, amelyekkel az eltérő beszállítói kapcsolatokból származó szolgáltatási szintű konfliktusokat vagy következetlenségeket kezelni lehet.	
CCM V3.0.1 kontrollazonosító: STA-08	**kontrollterület:** ellátásilánc-menedzsment, átláthatóság és elszámoltathatóság harmadik felek értékelése
Frissített kontroll-leírás, segédlet: Az éves értékelések elvégzésével a szolgáltatóknak észszerű információbiztonságot kell biztosítaniuk az információs ellátási lánc egészében. A felülvizsgálatnak ki kell terjednie az összes partnerre/harmadik fél szolgáltatóra, amelyektől az információ ellátási lánc függ.	

Szerkesztette: Kovács Zoltán

Forrás: Cloud Controls Matrix v3.0.1. 2014. 07. 11.
https://cloudsecurityalliance.org/research/ccm/#_downloads

szolgáltatás részének kell tekinteni függetlenül attól, hogy a felhasználó milyen szolgáltatást vesz igénybe. A felhasználó részére pedig azért előnyös e kontrollok megvalósítása, vagy szolgáltatótól történő igénylése, mert ezekkel még nagyobb biztonságot lehet garantálni, hiszen nem véletlenül kerültek be a CSA ajánlásába mint megvalósítandó tételek.

A másik, ami az összefuttatása után kapott listából látszik, hogy a CCM csupán annyit mutat be, hogy egy adott kontrollpont melyik szolgáltatói modellben értelmezhető, alkalmazható, és annak megvalósítása a szolgáltató mellett a felhasználónak is a felelőssége-e, ezért az csupán kiindulásként szolgálhat a tényleges elválasztási táblázat kidolgozásához. Egyrészt azért, mert a CCM szolgáltatóknak készült, így nem írja le azokat a kontrollokat, amelyek kizárólag a felhasználók felelősségi körébe tartoznak. Másrészt pedig azért, mert azoknál a kontrollpontoknál, amelyeknél a szolgáltató mellett a felhasználót is megjelöli felelősként, nem definiálja, hogy az adott pontot párhuzamosan (azaz egymástól függetlenül külön-külön, mindenki a saját részén, önállóan) kell, hogy megvalósítsák, vagy esetleg közösen együttműködve, valamilyen megállapodás szerint. Harmadrészt pedig azért, mert nem írja le tételesen, hogy IaaS, PaaS, vagy SaaS esetében melyek a csak a szol-

gáltató, csak a felhasználó, és melyek a mindkettőjük által (közösen, vagy párhuzamosan) megvalósítandó kontrollpontok. Főleg nem úgy, hogy az illeszthető legyen a biztonsági osztályba soroláshoz is.

Éppen ezért kiindulásként elfogadva a CCM-ből levezetett táblázatot, azt tovább kell bontani, hogy a leírtak szerint egyértelmű felelősségelhatárolást nyújtson az éppen aktuális szolgáltatói modellnek és biztonsági osztályba sorolásnak megfelelően, és egyértelműen rögzítse, melyek ezek közül a szolgáltató, melyek a felhasználó, és melyek a mindkettőjük által (közösen vagy párhuzamosan) megvalósítandó információbiztonsági kontrollok.

Ám ez már az előbbiek alapján megtehető és egy egzakt, az iparági szabványoknak és ajánlásoknak megfelelő, de a hazai érintett jogszabályokkal teljes mértékben harmonizáló felelősségelhatárolási táblázatot szül.

Összegzés, javaslatok

A cikksorozat első része összefoglalta Magyarország kibervédelmének főbb elemeit, bemutatta az állami, önkormányzati infokommunikációs rendszer konszolidálása okán létrejött szolgáltató-felhasználó modellt, és annak hatását a kibervédelemre, így rámutatott, hogy a jelenlegi jogszabályok az ebből adódó feladat- és felelősségelhatárolást nem kezelik. Rávilágított, hogy a hazánkban kijelölt központi szolgáltató, a NISZ Zrt. feladatainak ellátását úgy tudja elvégezni, hogy alapvetően felhőalapú szolgáltatásokat nyújt, ezért összefoglalta a felhőalapú rendszerek tulajdonságait, csoportosításukat. Bemutatta azt is, hogy a nagy nemzetközi szervezetek ezek közül melyeket ajánlják az állami intézmények számára, és a NISZ Zrt. melyben szolgáltat.

Jelen tanulmány ismertette a biztonság mint szolgáltatás alapelveit és alapvető szakmai dokumentumait, kiemelve azoknak a téma szempontjából legfontosabb részeit. Ez után bemutatta, hogy a SecaaS bevezetésének elengedhetetlen feltétele az Ibtv. és a 41/2015. (VII. 15.) BM rendelet által előírt, megvalósítandó biztonsági kontrollok feladat- és felelősségelhatárolásának rögzítése, amelyet a szolgáltató-felhasználó modell alkalmazásával célszerű megvalósítani. Bemutatott egy olyan potenciálisan alkalmazható módszertant, amely lehetővé teszi a feladat- és felelősségelhatárolást oly módon, hogy az egy egzakt, az iparági szabványoknak és ajánlásoknak megfelelő, de a hazai érintett jogszabályokkal teljes mértékben harmonizáló eredményre vezessen.

A tanulmány alapján a SecaaS kialakítása, hazai bevezetése kapcsán összegzésként, továbblépésként a következők fogalmazhatók meg:

1. A feladat elvégzéséhez alapként megfelelő mennyiségű és minőségű nemzetközi ajánlás áll rendelkezésre.
2. A bevezetés egyik alapfeltétele a megvalósítandó információbiztonsági kontrollok feladat- és felelősségelhatárolásának elvégzése és megfelelő szintű, minden szereplő számára egyértelmű deklarálása. Éppen ezért ki kell dolgozni és el kell fogadni, fogadtatni.
3. A feladat- és felelősségelhatárolás az alap ahhoz, hogy a szolgáltató által kötelezően nyújtandó biztonsági kontrollokon felüli tételek esetében a biztonság mint szolgáltatás igénybevételéről a felhasználók dönteni tudjanak, azazhogy a számukra előírt feladatok közül melyeket kívánják saját hatáskörben megvalósítani, és melyeket kívánják kiszervezni.
4. Az állami, önkormányzati szférában a sérülékenységvizsgálatnál alkalmazott jogszabályi korlátokhoz hasonlóan a biztonság mint szolgáltatás esetében is ki kell dolgozni a jogszabályi kereteket, egyértelműen rögzítve, hogy mely szolgáltatók milyen feltételek mellett működhetnek, az állami, önkormányzati szerveknek mikor kell vagy lehet adott esetben az Nemzeti Kibervédelmi Intézetet, mikor a NISZ Zrt.-t, és mikor külső gazdálkodó szervezetet mint menedzselt biztonsági szolgáltatót igénybe venniük, és ezt milyen feltételekkel tehetik meg. Egy nem állami kézben lévő menedzselt biztonsági szolgáltató igénybevétele ugyanis legalább olyan kockázatokat hordoz, mint a sérülékenységvizsgálatok kiszervezése.
5. A feladat- és felelősségelhatárolásra alapozva a szolgáltatóknak ki kell dolgozniuk egy szolgáltatáskatalógust, amelyben egyértelműen rögzítik a feladataikat, felelősségeiket, valamint olyan mérőszámokat (KPI[16]), amelyek alapján a szolgáltatás minősége és mennyisége egyértelműen mérhető és kimutatható mind a szolgáltató, mind a felhasználó számára.

FELHASZNÁLT JOGSZABÁLYOK (2017. augusztus 1-jei állapot)

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

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

16 KPI: Key Performance Indicators = Kulcsmutatók.