Az információbiztonság alapjai: a hálózatok

Bevezetés

Az infokommunikációs hálózatokban az információbiztonság megteremtése mindig is nagy kihívást jelentett a számítógépek, a rádiótelefonok megjelenése óta, és különösen nagy figyelmet kell fordítanunk rá az internet, a globális telefonhálózatok elterjedése és az általunk használt eszközök (okostelefonok, táblagépek, számítógépek, IoT-eszközök) világméretű hálózatba kapcsolása óta. Ezt a folyamatot kiválóan foglalja össze Muha Lajos doktori értekezésének bevezetőjében, amikor a következőket írja:

> „A modern állam, annak minden szervezete és polgára kiszolgáltatottá vált a számítógépekből, kommunikációs eszközökből és automata rendszerekből álló bonyolult, többszörösen összetett információs infrastruktúrának. Napjainkban ezen eszközök nélkül életünk elképzelhetetlenné vált. Vezetékes és mobil telefonon tartjuk szeretteinkkel a kapcsolatot, ha pénzre van szükségünk, a bankjegykiadó automatához (ATM) fordulunk, amelynek a lényege egy személyi számítógép, ami vezetékes telefonvonalon keresztül a bankunk vagy az elszámoló központ számítógépére csatlakozik, és digitális kommunikációjuk dönti el, hogy kaphatunk-e készpénzt az automatából vagy sem. Munkahelyünkön a munkánkhoz szükséges adatok jelentős része a számítógépen van tárolva. A legtöbb esetben már nem is a saját asztali számítógépünkön, hanem távol, néha több száz vagy ezer kilométerre lévő központi számítógépeken. Ezek a számítógépeken tárolt adatok teszik lehetővé, hogy például a villamosenergia-szolgáltatónk átlássa, hol mennyi áramra van szükség, és honnét tudja azt beszerezni. Ha ezekben a rendszerekben bárhol, bármilyen hiba adódik, máris elindul egy dominóhatás. Villamos energia nélkül más számítógépek is leállnak, sötétség lesz, de még hideg is, mert az elektromosan vezérelt gázfűtésünk is leáll. Ha nem működnek a bankjegykiadó automaták, akkor még a vésztartalék petróleumlámpával világító üzletben sem tudjuk alapvető létszükségleti cikkeinket beszerezni. Ez olyan káoszba torkollhat, amelynek kimenetele nehezen jósolható meg.
> Tudomásul kell vennünk, hogy információs rendszereink egyre gyakrabban szembesülnek az igen sokféle forrásból származó biztonsági fenyegetéssel, többek között gazdasági hírszerzéssel, ipari kémkedéssel, számítógépes csalással, szabotázzsal, vandalizmussal, tűzzel vagy árvízzel. A szándékos károkozások olyan formái, mint a számítógépvírusok, a számítógépes betörések vagy a szolgáltatás-megtagadásra vezető támadások egyre gyakoribbá, általánosabbá válnak, ugyanakkor ezek egyre vakmerőbbek és egyre bonyolultabbak is. Egyre nagyobb fenyegetést jelent sérülékeny információs rendszereinkre

https://doi.org/10.36250/01004_03

a hadviselés új formája, az információs hadviselés, de még inkább a békeidőkben is állandóan fenyegető terrorizmus számítógépes változata, a kiberterrorizmus."[43]

Napjainkban jellemzően a terheléses támadások végrehajtásához szükséges botnetvírusok, illetve a zsarolóvírusok *(ransomware)* a jellemző veszélyforrások.[44]

Éppen az itt leírtak okán célszerű megvizsgálni, hogy az infokommunikációs hálózatokban melyek az információvédelem alapelvei, milyen védelmi megoldásokkal találkozhatunk, miket alkalmazhatunk a napi gyakorlatban, mik a szolgáltató és mik a felhasználó felelősségi körébe tartozó feladatok. Ezek alapján pedig az is körülhatárolható, hogy melyek lehetnek a kibernyomozók számára releváns információk forrásai.

Az információbiztonság alapjai

Mindenekelőtt azt érdemes tisztázni, hogy mit értünk információbiztonság alatt. Ez ugyanis nem egyezik meg az adatvédelemmel vagy az informatikai biztonság fogalmával, ugyanakkor ezek között nyilvánvalóan szoros kapcsolat áll fenn.

Le kell azonban itt szögezni, hogy a fogalmi kérdések meghatározásánál alapelvként kell kezelni, miszerint „a terminológiai kérdések vizsgálata során a megnevezéssel szemben a tartalomnak van elsődlegessége".[45] Ez már csak azért is fontos, mert – mint a későbbiekben látható lesz – mára számtalan olyan elnevezés került be a gyakorlati életbe (például informatikai biztonság, elektronikus információbiztonság, de akár még az információbiztonság is), amelyeket sokszor vállalatoknál, intézményeknél is pontatlanul, olykor egymás szinonimájaként is használnak. A kibernyomozó számára azért is fontos a tartalom megismerése, ezek tisztázása, mert egy nyomozás során meg kell találja azokat az egyéneket, csoportokat, akik a számára releváns kérdéseket meg fogják tudni válaszolni.

Az előző fejezetben már ismertetett fogalmi különbségek mellett meg kell jegyeznünk, hogy az adat és információ megnevezés sokszor még a szakirodalomban is együtt, akár egymás szinonimájaként jelenik meg, vagy pontosabban

[43] Muha Lajos: *A Magyar Köztársaság kritikus információs infrastruktúráinak védelme.* PhD-értekezés. Budapest, ZMNE, 2007b. 4–5, 127.

[44] Mezei Kitti – Nagy Zoltán András: A zsarolóvírus és a botnet mint napjaink két legveszélyesebb számítógépes vírusa. In Gaál Gyula – Hautzinger Zoltán (szerk.): *Szent Lászlótól a modern kori rendészettudományig.* Pécs, Pécsi Határőr Tudományos Közlemények, 19. kötet. (2017). 163–168.

[45] Munk Sándor: Információbiztonság vs. informatikai biztonság. *Hadmérnök,* Különszám. Robothadviselés 7. Tudományos Szakmai Konferencia 2007. november 27.

fogalmazva adott témák szempontjából nem feltétlenül tesznek a szerzők különbséget a két fogalom között. (Például az Ibtv.-ben sem, bár az értelmező rendelkezésekben megjelenik a két fogalom definíciója, a törvényben együtt használatos az adat és az információ, ami tudományosan helytelen.) Így például, amikor egy infokommunikációs rendszerben tárolásról, továbbításról, feldolgozásról beszélünk, akkor annak technikai eszközei és módszerei nagyrészt függetlenek lehetnek attól, hogy adatról vagy információról beszélünk-e. Erre egy példa, amikor adatok, információk tárolásának, megosztásának, titkosításának technikai aspektusairól beszélünk. Ennek megfelelően jelen fejezet a továbbiakban nem választja szét ezeket, hiszen a következőkben ismertetendő témák mind az adatok, mind az információk tekintetében egyaránt helytállók.

Az adatok (információk) életciklusát az 1. ábra mutatja be.

1. ábra: Az adatok életciklusa

Forrás: Rich: Data Security Lifecycle 2.0. *Securosis. Blog.* 2011. szeptember 6.

Az adatok (információk) életciklusának 6 állomását biztonsági szempontból 2 fő csoportra bonthatjuk, az *adatmozgással járó* (előállítás, használat, megosztás, törlés) *és az adatmozgással nem járó* (tárolás, archiválás) műveletekre.

Ezt a bontást azért célszerű megtenni, mert napjainkban, amikor egyre több felhőalapú rendszert használunk, ha a felhasználó egy ilyen rendszer használatakor 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. Ezekről a későbbiekben még részletesebben lesz szó.

A következőkben pedig vizsgáljuk meg az adatvédelem, az informatikai biztonság, a kiberbiztonság és az információbiztonság fogalmát, azok tartalmát, a közöttük lévő különbségeket és adott esetben az azonos tartalmi részeket!

Mindenekelőtt azonban érdemes tisztázni az egyes rendszerek, így az informatikai rendszer, az infokommunikációs rendszer és az elektronikus információs rendszer közötti különbséget. Amíg például az 1990-es években még nagyon markánsan szét lehetett választani például egy analóg rádióhálózatot egy lokális számítógép-hálózattól, addig mára a funkcióbeli különbségek eltűntek, a technológiai konvergencia okán ma sokkal inkább infokommunikációs rendszerekről vagy – a jogszabályokban található terminológia szerint – elektronikus információs rendszerekről beszélünk, beszélhetünk. Mára a szakemberek is sokszor egymás szinonimájaként használják az említett fogalmakat, és valljuk meg, nagyon nehéz is közöttük különbséget tenni. Ma már nem nagyon létezik olyan számítógép-hálózat, amely ne kapcsolódna más hálózatokhoz (például interneten keresztül), ne lenne benne elérhető elektronikus levelezés, de például az okostelefonunk is sokkal többre alkalmas, mint pusztán telefonálásra vagy sms-küldésre/fogadásra. Éppen ezek miatt, szem előtt tartva jelen mű fő témáját, itt nem (vagy inkább már itt sem) érdemes különbséget tenni ezen rendszerek között. Ennek megfelelően a továbbiakban az informatikai rendszer, az infokommunikációs rendszer és az elektronikus információs rendszer alatt ugyanazt értjük.

A vizsgálatot az információbiztonsággal érdemes kezdeni.

Az információbiztonság fogalma

Az információbiztonságon komplex, az alábbi három dimenzió mindegyikében megvalósuló védelmet kell értenünk:

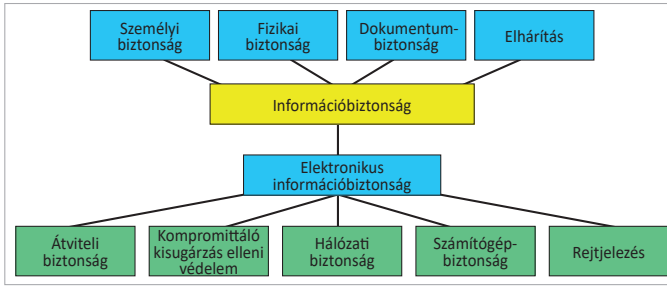
- *fizikai dimenzió:* az információbiztonság kapcsán ez a különböző információs infrastruktúrák, infokommunikációs rendszerek elemei elleni, többnyire úgynevezett „kemény típusú” *(hard kill)* támadásokat, valamint azok fizikai védelmét jelenti;
- *információs dimenzió:* az információbiztonság kapcsán ez a különböző információs folyamatok, adatszerzés, adatfeldolgozás, kommunikáció stb.

elleni, többnyire elektronikus úton történő, „lágy típusú” *(soft kill)* támadásokat, valamint azok többnyire logikai védelmét jelenti;
– *tudati dimenzió:* az információbiztonság kapcsán a közvetlenül az emberi gondolkodás – észlelés, érzékelés, értelmezés, vélemény, vélekedés – elleni támadásokat, valamint azok védelmét jelenti.

Az információbiztonság megvalósítása során tehát komplex és integrált védelmet kell kialakítani annak érdekében, hogy mindhárom dimenzióban megvédhessük a kritikus információkat. Kritikusnak tekintendő minden olyan információ, amelyet a támadó felhasználhat a saját érdekei érvényesítésében és/vagy döntési folyamataiban, vagy kárt okozhat számunkra, akadályozhatja, esetleg ellehetetlenítheti a saját döntési folyamatainkat.

Az információbiztonság, így a kritikus információk védelme, főleg az alábbi biztonsági komponensekre, az itt alkalmazható védelmi megoldásokra kell hogy kiterjedjen:
– a személyi biztonság;
– a fizikai biztonság;
– a dokumentumbiztonság;
– az elhárítás (vagy felderítés elleni tevékenység);
– az elektronikus információbiztonság.

Ezt, valamint a könyv témájának szempontjából leglényegesebb információbiztonsági részterületet, az elektronikus információbiztonság alterületeit mutatja be a 2. ábra.



2. ábra: A komplex információbiztonság elemei

Forrás: Haig Zsolt: Az információbiztonság komplex értelmezése. Robothadviselés 6. Tudományos Szakmai Konferencia 2006. november 22. *Hadmérnök.* Különszám.

Az információbiztonság részterületei az alábbiak szerint jellemezhetők:

A *személyi biztonság:* az érzékeny adatokhoz, kritikus információkhoz való hozzáférés engedélyezéséhez szükséges biztonsági követelmények összessége. Ezen adatokhoz, információkhoz csak azok a személyek férhetnek hozzá, akik igazoltan megfelelnek bizonyos követelményeknek, előírásoknak, és a munkájukhoz az adatok, információk megismerésére ténylegesen szükség van. A személyi biztonságra legjellemzőbb példa, hogy a nemzeti minősített adatok megismeréséhez szükséges a kockázatmentes nemzetbiztonsági ellenőrzés megléte, az ezek alapján kiállított személyi biztonsági tanúsítvány, valamint az aláírt titoktartási nyilatkozat is.

A *fizikai biztonság:* azon szabályzatok, fizikai akadályok, jelzőrendszerek (például sorompók, falak, beléptetőrendszerek, riasztórendszerek, behatolásjelzők, tűzjelzők stb.) összessége, amelyek megakadályozzák az illetékteleneket a kritikus információkhoz, az azokat tartalmazó dokumentumokhoz, eszközökhöz való hozzáférésben, a számukra nem engedélyezett épületekbe, épületrészekbe, helyszínekre történő bejutásban, valamint meggátolják az ezek elleni fizikai támadást. A fizikai biztonságra jellemző példa az élőerős őrség felállítása a bejáratoknál, a kamerarendszer és az úgynevezett proximity kártyaalapú beléptető használata az épületeken belül.

A *dokumentumbiztonság:* azon szabályzatok, előírások és intézkedések összessége, amelyek segítségével az összes dokumentumot azok minősítése, azaz a bennük lévő információk érzékenysége szerint tudjuk védeni. Fontos kitétel, hogy az érzékeny adatokat, kritikus információkat tartalmazó dokumentumokhoz csak azok férjenek hozzá, akiknek ez feltétlenül szükséges, az ő számukra azonban a hozzáférés biztosított legyen. Miután valamennyi elektronikus adathordozó egyben dokumentumnak is minősül, az információbiztonság többi részterületével ellentétben a dokumentumbiztonság közvetlen módon is kapcsolódik az elektronikus információbiztonsághoz. A dokumentumbiztonságra jellemző példa a nemzeti minősített adatoknál használandó titkos ügykezelés (TÜK).

Az *elhárítás* (vagy felderítés elleni tevékenység): azon védelmi jellegű módszerek és tevékenységek összessége, amelyek ellenérdekelt felek (például ellenérdekelt hírszerző szolgálatok, [kiber]bűnözők, [kiber]terroristák, hacktivisták, ártó szándékú belső munkatársak és/vagy külső közreműködők stb.) tevékenységének felderítésére és kivédésére irányul. Az elhárításra jellemző példa az infokommunikációs rendszerek védelme érdekében használt úgynevezett fenyegetettségekkel kapcsolatos hírszerzési tevékenység *(cyber threat intelligence).* Ez az adott védendő objektumra (szervezet, információk stb.)

a kibertérből potenciálisan fenyegetést jelentő támadók, támadási formák felderítésére és a lehetséges támadások megelőzésére, valamint a már megtörtént, de a szervezet által még fel nem ismert támadásokból származó információk – elsősorban a dark weben történő – felkutatására és a kárenyhítéshez szükséges intézkedés előkészítésére szolgáló tevékenység.

Az *elektronikus információbiztonság* fogalma:

> „a biztonsági rendszabályok alkalmazása a kommunikációs, információs és más elektronikus rendszerekben a feldolgozott, tárolt vagy továbbított információ bizalmasságának, sértetlenségének vagy rendelkezésre állásának véletlen vagy szándékos elvesztése ellen, és e rendszerek sértetlenségének vagy rendelkezésre állásának elvesztése ellen".[46]

Az elektronikus információbiztonság alterületei:

- *Átviteli biztonság:* azon szabályzatok, intézkedések és tevékenységek összessége, amelyek jelentősen megnehezítik, vagy akár el is lehetetlenítik az információk átvitele során az átviteli folyamatba történő illetéktelen beavatkozást, így különösen azok megváltoztatását, törlését, lehallgatását. Jellemző példa a rejtjelző eszközök alkalmazása az átvitel során.
- *Kompromittáló kisugárzás elleni védelem:* olyan aktív és passzív védelmi intézkedések és eszközök alkalmazása, amelyek jelentősen megnehezítik, vagy akár el is lehetetlenítik, azt, hogy az elektronikai eszközök, berendezések másodlagos sugárzásának elemzésével illetéktelenek hozzáférjenek a védendő információkhoz. Jellemző példa a berendezések és az azoknak helyet adó helyiségek árnyékolása.
- *Hálózati biztonság:* azon szabályzatok, intézkedések és tevékenységek összessége, amelyek védik a hálózatba kötött eszközöket és a hálózati szolgáltatásokat az azokon elérhető szolgáltatások szintjének csökkenése vagy ellehetetlenülése ellen, valamint jelentősen megnehezítik, vagy akár el is lehetetlenítik, illetéktelenek számára az azokban kezelt, tárolt, feldolgozott stb. adatok, információk megismerését, megváltoztatását vagy megsemmisítését. A hálózatok összekapcsolásának védelmi feladatai is ebbe a csoportba tartoznak. Jellemző példa a kiberbiztonsági operatív központ működtetése (amelynek feladata többek között a hálózatban elhelyezett speciális védelmi eszközökből és a hálózatban lévő alapműködést

[46] Muha Lajos: Az informatikai biztonság egy lehetséges rendszertana. *Bolyai Szemle,* 17. (2008), 4. 137–156.

szolgáló eszközökön futtatott védelmi szoftverekből kapott jelzések alapján a hálózatot érő támadások felismerése, kezelése), vagy a folyamatos kockázatelemzés végrehajtása (a kockázatok feltárása, értékelése, a feltárt kockázatok hatásainak elfogadható mértékűre csökkentése stb.).

– *Rejtjelzés:* a védendő információk olyan átalakítása (titkosítása), amely jelentősen megnehezíti, vagy akár el is lehetetleníti azt, hogy illetéktelenek megismerjék azokat. A rejtjelzés része az információk eredeti formátumúvá történő visszaalakítása is. A rejtjelzést az adatéletciklus (előállítás, tárolás, használat, megosztás, archiválás, törlés) több szakaszában is lehet használni. Jellemző példa a számítógépek, okostelefonok háttértárának teljes titkosítása (például Windows operációs rendszer esetén a BitLocker használatával), így azokon minden adatot, információt titkosítottan tárolnak.
– *Számítógép-biztonság:* azon szabályzatok, intézkedések és tevékenységek összessége, amelyek védik az egyes infokommunikációs eszközöket az azokon elérhető szolgáltatások szintjének csökkenése vagy ellehetetlenülése ellen, valamint jelentősen megnehezítik, vagy akár el is lehetetlenítik, illetéktelenek számára az azokban kezelt, tárolt, feldolgozott stb. adatok, információk megismerését, megváltoztatását vagy megsemmisítését. Ma már jobbára a hálózati biztonsággal együtt kezelik, egyrészt az egyedi, hálózatba nem kötött számítógépek alacsony száma miatt, másrészt annak okán, hogy egyedi gépeknél alkalmazott védelmi szoftverek csupán részhalmazát képezik a hálózati biztonság kapcsán a hálózati végponti eszközökön használt védelmi szoftverek halmazának. Jellemző példa a vírusirtó szoftverek használata.[47]

Az információbiztonság tehát komplex védelmet jelent, amely „a szóban, rajzban, írásban, a kommunikációs, informatikai és más elektronikus rendszerekben, vagy bármilyen más módon kezelt információk védelmére vonatkozik”.[48]

[47] Vö. Haig (2006): i. m.

[48] Muha Lajos – Krasznay Csaba: *Az elektronikus információs rendszerek biztonságának menedzselése.* Budapest, Nemzeti Közszolgálati Egyetem, 2018.

Adatvédelem

A Nemzeti Adatvédelmi és Információszabadság Hatóság (NAIH) honlapján található Adatvédelmi Értelmező Szótár szerint az „adatvédelem: a személyes adatok jogszerű kezelését, az érintett személyek védelmét biztosító alapelvek, szabályok, eljárások, adatkezelési eszközök és módszerek összessége”.[49] Azaz az adatvédelem kizárólag a személyes adatok védelmére vonatkozik, a személyiségi jogokkal összefüggő tevékenység. Ennek okán nem fedi le az összes információt, hanem annak csak egy bizonyos részét. Így az adatvédelem jelen fejezet témája szempontjából az információbiztonság egy – speciális – részhalmazának tekinthető. Erről a témáról bővebb információk jelen könyv adatvédelmi ismeretekről szóló fejezetében érhetők el.

Informatikai biztonság

Az *informatikai biztonság* a biztonsági kérdéseket az adott rendszerben létrehozott, tárolt, feldolgozott, továbbított stb. információk mellett kiterjeszti az azokat kezelő rendszerekre is. Az Informatikai Tárcaközi Bizottság 1994-ben kiadott 8. számú ajánlásában, majd különösen a Miniszterelnöki Hivatal Informatikai Tárcaközi Bizottsága 1996-ban kiadott 12. számú ajánlásában az informatikai biztonság (az adatoknak és információknak az informatikai rendszerekben történő biztonságos kezelése) öt alapkövetelménye között határozta meg az információk rendelkezésre állását, sértetlenségét, bizalmasságát, hitelességét és a teljes informatikai, illetve információs rendszer működőképességét.[50] Később ez módosult a mára már általánosan elfogadott és a hatályos hazai jogszabályokban (például Ibtv.) is megjelenő három alapkövetelményre (bizalmasság, sértetlenség, rendelkezésre állás).

Az informatikai biztonság teljes egészében az információbiztonság részének tekinthető, hiszen minden intézkedést, tevékenységet, amelyet az informatikai biztonság érdekében teszünk, az adott rendszerekben tárolt adatok, információk bizalmasságának, sértetlenségének és rendelkezésre állásának az érdekében

[49] Vö. *Adatvédelmi Értelmező Szótár.*

[50] Vö. Munk (2007): i. m; Bodlaki Ákos et al.: *Informatikai rendszerek biztonsági követelményei.* Budapest, Miniszterelnöki Hivatal Informatikai Tárcaközi Bizottsága (MeH ITB), 12. számú ajánlása. 1996.

tesszük. Mára, ahogy azt fentebb kifejtettük, az informatikai rendszert, az infokommunikációs rendszert és az elektronikus információs rendszert azonosnak tekinthetjük, ezért az informatikai biztonságot (informatikai rendszerek biztonságát), az infokommunikációs rendszerek biztonságát és az elektronikus információs rendszerek biztonságát is azonosnak tekinthetjük.

Az elektronikus információs rendszer biztonsága

Az Ibtv. 1. § (1) bekezdés 15. pontja megfogalmazza az elektronikus információs rendszer biztonságának definícióját:

> „az elektronikus információs rendszer olyan állapota, amelyben annak védelme az elektronikus információs rendszerben kezelt adatok bizalmassága, sértetlensége és rendelkezésre állása, valamint az elektronikus információs rendszer elemeinek sértetlensége és rendelkezésre állása szempontjából zárt, teljes körű, folytonos és a kockázatokkal arányos".

Ennek megfelelően az elektronikus információs rendszer biztonsága felfogható az előbbiekben tárgyalt informatikai biztonság pontosabb, napjaink fogalmait jobban lefedő megfogalmazásának is.

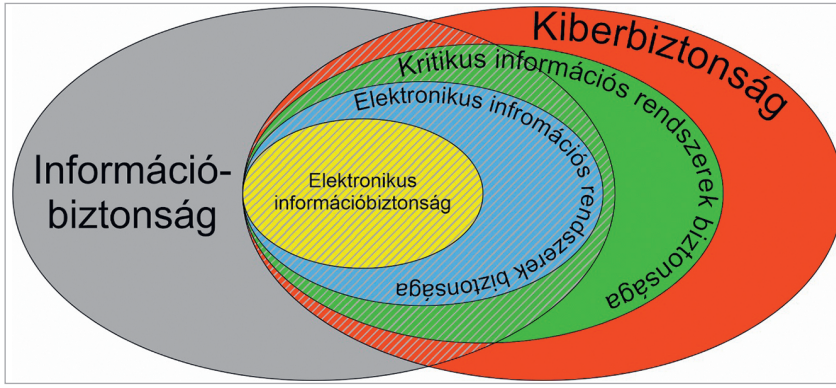
Kiberbiztonság

Az Ibtv. 1. § (1) bekezdés 26. pontja szerint a

> „kiberbiztonság: a kibertérben létező kockázatok kezelésére alkalmazható politikai, jogi, gazdasági, oktatási és tudatosságnövelő, valamint technikai eszközök folyamatos és tervszerű alkalmazása, amelyek a kibertérben létező kockázatok elfogadható szintjét biztosítva a kiberteret megbízható környezetté alakítják a társadalmi és gazdasági folyamatok zavartalan működéséhez és működtetéséhez."

Ennek megfelelően a kiberbiztonság tág fogalom, amely az információk védelmén kívül még nagyon sok mindenre kiterjed. Így a kiberbiztonság és az információbiztonság is egymást részben átfedő fogalmak, amelyek viszonyát szintén lehetne ábrázolni. (Fontos megemlíteni, hogy a halmazok nagysága ebben az esetben nem reprezentálja a benne lévő elemek számosságát.) A kiberbiztonság és az informatikai biztonság viszonyát tekintve az informatikai biztonság

a kiberbiztonság részének tekinthető, így a továbbiakban mindenhol a kiberbiztonság fogalmat használja a fejezet. A fent említettek kapcsolatát és egymáshoz való viszonyát mutatja be a 3. ábra.



3. ábra: Az információbiztonság, a kiberbiztonság, a kritikus információs rendszerek biztonsága, az elektronikus információs rendszerek biztonsága és az elektronikus információbiztonság egymáshoz való viszonya

Forrás: a szerző szerkesztése Muha–Krasznay (2018): i. m. alapján

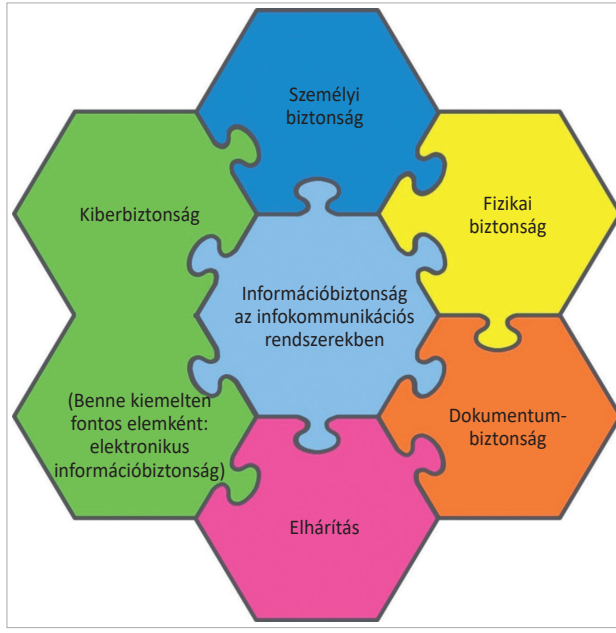
A kritikus (vagy a vonatkozó jogszabályokban használt terminológiával élve létfontosságú) információs infrastruktúrák biztonságát jelen mű keretei és témája okán most nem érdemes elemezni.

Az információbiztonság magában foglalja az elektronikus információs rendszerek biztonságát és az elektronikus információbiztonságot teljes egészében, illetve egészen kis szeleteket a kritikus információs infrastruktúrák biztonságából és a kiberbiztonságból is.

Információbiztonság az infokommunikációs rendszerekben

Az előző alfejezetben részletesen bemutattuk a különböző fogalmakat, amelyek az információk biztonsága kapcsán napjainkban felmerülhetnek, valamint ezek összefüggéseit, egymáshoz való viszonyukat is. A fentiek alapján elmondható, hogy a kritikus információk védelmét az infokommunikációs hálózatokon csak komplex módszerekkel lehet hatékonyan biztosítani, amelynek

az információbiztonság mellett a kiberbiztonságnak az információbiztonságon kívül eső elemeit is tartalmaznia kell. Ezt mutatja be a 4. ábra.



4. ábra: Az információbiztonság elemei az infokommunikációs rendszerekben
Forrás: a szerző szerkesztése

Az ábrán az egyes elemeket szimbolizáló puzzle-darabok mérete ebben az esetben sem mutatja azok tényleges, a többi elemhez viszonyított mértékét. Az infokommunikációs hálózatokban a leghangsúlyosabbnak a kiberbiztonság, ezen belül pedig az elektronikus információbiztonság tekinthető, amelyeket itt – a fent leírtak okán – a 3. ábra szerint egy közös elemként ábrázoltunk.

Amikor infokommunikációs rendszerekben lévő információk kapcsán beszélünk információbiztonságról, akkor biztonság alatt egy olyan állapotot értünk, amelyben az érintett számára kielégítő módon valósul meg az adott rendszer *zárt, teljes körű, folytonos és a kockázatokkal arányos védeleme.* Ezek alatt – az Ibtv. alapján – az alábbiakat értjük:

– „zárt védelem: az összes számításba vehető fenyegetést figyelembe vevő védelem;
– teljes körű védelem: az elektronikus információs rendszer valamennyi elemére kiterjedő védelem;
– folytonos védelem: az időben változó körülmények és viszonyok között is megszakítás nélkül megvalósuló védelem;
– kockázatokkal arányos védelem: az elektronikus információs rendszer olyan védelme, amelynek során a védelem költségei arányosak a fenyegetések által okozható károk értékével."

Ezt a zárt, teljes körű, folytonos és a kockázatokkal arányos védelmet úgy lehet kialakítani, hogy az előző alfejezetben ismertetett, és a 4. ábrán bemutatott, az infokommunikációs rendszerekben elvárt komplex információbiztonsághoz szükséges összes elemmel foglalkozunk. Mielőtt azonban erre rátérnénk, még egy kérdést fontos tisztázni.

Amikor jelen esetben infokommunikációs rendszerekről beszélünk, akkor – a korábban leírtak szerint – az Ibtv.-ben meghatározott elektronikus információs rendszereket értjük.

„1. § (1) […] 14b. elektronikus információs rendszer:
a) az elektronikus hírközlésről szóló törvény szerinti elektronikus hírközlő hálózat;
b) minden olyan eszköz vagy egymással összekapcsolt vagy kapcsolatban álló eszközök csoportja, amelyek közül egy vagy több valamely program alapján digitális adatok automatizált kezelését végzi; vagy
c) az *a)* és *b)* pontban szereplő elemek által működésük, használatuk, védelmük és karbantartásuk céljából tárolt, kezelt, visszakeresett vagy továbbított digitális adatok."

Ezt a meghatározást a 2018. évi CXXI. törvény 111. § (3) bekezdése módosította.

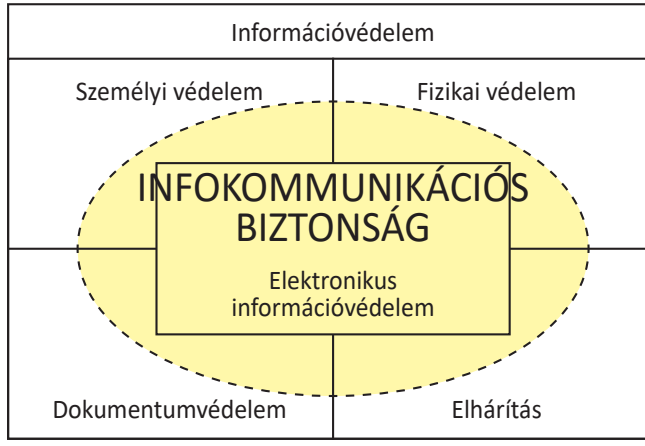
A korábbi, 2013. évi L. tv. 1. § 2. pontja a következő, kevésbé általános – ám jelen téma megértését talán jobban szolgáló – meghatározást használta az elektronikus információs rendszerek fogalmának meghatározására: „Elektronikus információs rendszer az adatok, információk kezelésére használt eszközök (környezeti infrastruktúra, hardver, hálózat és adathordozók), eljárások (szabályozás, szoftver és kapcsolódó folyamatok), valamint az ezeket kezelő személyek együttese."

A fenti definíciót alapul véve a Muha–Krasznay szerzőpáros leírása szerint

„az elektronikus információs rendszerekhez tartoznak:
1. a számítástechnikai rendszerek és hálózatok;
2. a helyhez kötött, mobil és egyéb rádiófrekvenciás, valamint műholdas elektronikus hírközlési hálózatok, szolgáltatások;

3. a rádiós vagy műholdas navigáció;
4. az automatizálási, vezérlési és ellenőrzési rendszerek (vezérlő és adatgyűjtő, távmérő, távérzékelő és telemetriai rendszerek stb.);
5. a fentiek felderítéséhez, lehallgatásához vagy zavarásához használható rendszerek."[51]

Az információvédelem, az infokommunikációs biztonság és az elektronikus információvédelem kapcsolatát mutatja az 5. ábra.



5. ábra: Az infokommunikációs biztonság, az elektronikus információvédelem és az információvédelem kapcsolata
Forrás: Muha (2007b): i. m.

Mivel a téma szempontjából – ahogy azt már feljebb is kifejtettük – az elektronikus információs rendszerek és az infokommunikációs rendszerek között nincs számottevő különbség, sőt ma már azonosnak tekinthetők, az egyszerűség kedvéért a továbbiakban elektronikus információs rendszerek biztonsága alatt az infokommunikációs rendszer biztonságát, az elektronikus információs rendszerek alatt pedig infokommunikációs rendszereket is értünk.

Muha meghatározása szerint:

> „Az elektronikus információs rendszer biztonsága az elektronikus információs rendszer olyan – az érintett számára kielégítő mértékű – állapota, amelyben annak védelme

[51] Vö. Muha–Krasznay (2018): i. m.

az elektronikus információs rendszerben kezelt adatok bizalmassága, sértetlensége és rendelkezésre állása, valamint az elektronikus információs rendszer elemeinek sértetlensége és rendelkezésre állása szempontjából zárt, teljes körű, folytonos és a kockázatokkal arányos."[52]

Ahol az Ibtv. 1. § 19) bekezdése szerint:

- „bizalmasság: az elektronikus információs rendszer azon tulajdonsága, hogy a benne tárolt adatot, információt csak az arra jogosultak és csak a jogosultságuk szintje szerint ismerhetik meg, használhatják fel, illetve rendelkezhetnek a felhasználásáról; (8. pont)
- rendelkezésre állás: annak biztosítása, hogy az elektronikus információs rendszerek az arra jogosult személy számára elérhetőek és az abban kezelt adatok felhasználhatóak legyenek; (38. pont)
- sértetlenség: az adat tulajdonsága, amely arra vonatkozik, hogy az adat tartalma és tulajdonságai az elvárttal megegyeznek, ideértve a bizonyosságot abban, hogy az az elvárt forrásból származik (hitelesség) és a származás ellenőrizhetőségét, bizonyosságát (letagadhatatlanságát) is, illetve az elektronikus információs rendszer elemeinek azon tulajdonságát, amely arra vonatkozik, hogy az elektronikus információs rendszer eleme rendeltetésének megfelelően használható; (39. pont)."[53]

A továbbiakban ezeket átvéve és elfogadva vizsgáljuk meg az elektronikus információs rendszerekben a szolgáltató és a felhasználó feladatait, felelősségét, valamint a kibernyomozó számára releváns információk forrásait.

A szolgáltató és a felhasználó feladatai, felelőssége, valamint a kibernyomozó számára releváns információk forrásai

A fentiek bemutatása és értelmezése után azt kell tisztázni, hogy az elvárt zárt, teljes körű, folytonos és a kockázatokkal arányos védelmet ki és hogyan tudja biztosítani egy infokommunikációs (elektronikus információs) rendszerben. Minden ilyen rendszer általában két szereplőre, a szolgáltatóra és a felhasználóra bontható. (Léteznek természetesen speciális esetek is, amikor például valamely vállalat önmagában a rendszer szolgáltatója [ebben az esetben üzemeltetője] és felhasználója is, akkor azonban minden védelmi elemről neki magának kell gondoskodnia.)

[52] Vö. Muha–Krasznay (2018): i. m.
[53] Ibtv. 1. §.

A következőkben a felhőalapú rendszerek kapcsán vezetjük végig a szolgáltató és a felhasználó felelősségét az információvédelemben. Egyrészt azért, mert napjainkra talán ezek a legjellemzőbb infokommunikációs szolgáltatások; másrészt azért, mert az összes lehetséges eset vizsgálatára jelen mű keretei szűkek; harmadrészt pedig azért, mert a téma szempontjából, azaz a kibernyomozók számára nagy valószínűséggel ennek az esetnek a vizsgálata a legfontosabb, azaz ezekkel a kérdésekkel fog a leggyakrabban találkozni.

Ahhoz, hogy az információbiztonsági feladatok említett szétválasztását elvégezhessük, először is célszerű áttekinteni a felhőalapú rendszereket, azok tulajdonságait.

A felhőalapú rendszerek rövid összefoglalása

A NIST *(National Institute of Standards and Technology Information Technology Laboratory)* által *The NIST Definition of Cloud Computing* címen kiadott és mára kvázi szabványnak tekinthető tanulmány szerint akkor beszélhetünk felhőalapú szolgáltatásról, ha az alábbi tulajdonságok egy rendszerben (részben vagy egészben) fellelhetők:

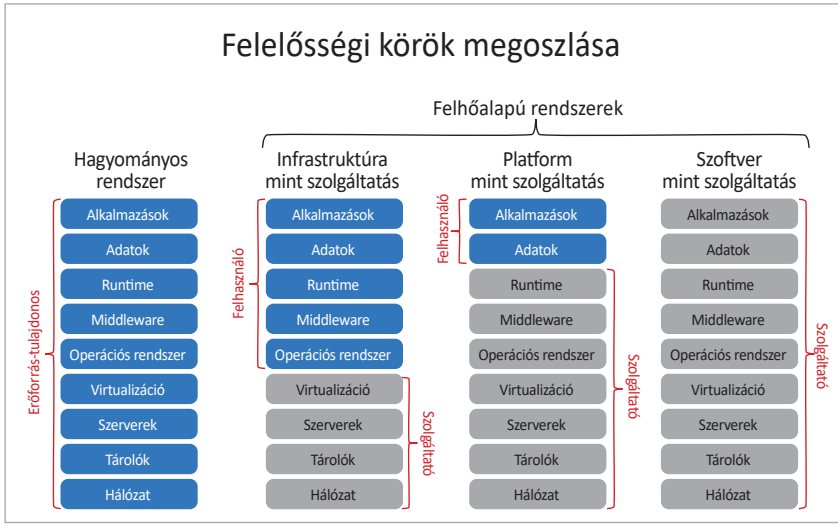
- igény szerinti önkiszolgálás *(on-demand self-service):* a felhasználók szükségleteik szerint képesek változtatni az igényelt számítási kapacitásokat;
- jó hálózati hozzáférés *(broad network access):* hálózaton, szabványos mechanizmusokon keresztül, heterogén eszközökkel elérhetők a szolgáltatások;
- 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.

A felhőalapú rendszereket az alábbi szolgáltatási és telepítési modellek szerint csoportosítják.

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.



6. ábra: Felelősségi körök megoszlása a szolgáltatási modellekben

Forrás: a szerző szerkesztése Zaid Kartit et al.: *Network Issues in cloud computing and countermeasures.* 2014. 4. alapján.

Infrastruktúra mint szolgáltatás (*cloud infrastructureas a service* – IaaS): a felhasználó számára ebben az esetben olyan számítási, tárolási, hálózati és egyéb alapvető informatikai erőforrásokat kínál a szolgáltató, amelyekre és amelyeken tetszőleges szoftvereket telepíthet és futtathat, beleértve az operációs 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.

A hagyományos (azaz a felhasználó tulajdonában és üzemeltetésében lévő, valamint az egyes szolgáltatási modelleknél a felhasználó és a szolgáltató felelősségi körébe tartozó feladatokat jól szemlélteti a 6. ábra.

Telepítési modellek (deployment models)

Magánszámítási 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 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 *cloud bursting* technológia a felhők közötti terheléskiegyenlítésre, amikor a magánfelhőben rendelkezésre álló erőforrások elfogynak, és azokat más, tipikusan nyilvános felhőben meglévőkkel pótolják ki).

A szolgáltatási és a telepítési modellekből egyfajta mátrix képezhető. Ebben a mátrixban kell megtalálnia a felhasználónak a számára megfelelő szolgáltatást, ide kell elhelyeznie saját (meglévő vagy tervezett) hálózatát, majd ennek a mátrixnak a megfelelő mezőjébe pozicionált termékek közül kell kiválasztania a számára megfelelőket.[54]

A fentiek közül a téma szempontjából a nyilvános számítási felhő (*public cloud* – PC) és a szoftver mint szolgáltatás (*cloud software as a service* – SaaS) típusú rendszereket (PC/SaaS felhőalapú rendszerek) vizsgáljuk tovább. Ezek azok a mindenki számára – a meglévő személyi használatú infokommunikációs eszközök (például notebook, okostelefon stb.) felhasználásával, akár csekély számítástechnikai tudással is használható, olcsón, sokszor ingyenesen – igénybe vehető rendszerek, szolgáltatások (mint például Facebook, Gmail, Dropbox, Twitter, Skype stb.), amelyek ma már szerves részét képezik mindennapi életünknek, kommunikációnknak. Az „átlagfelhasználók" ezeket a rendszereket használják leggyakrabban, de nagyon jellemző ezek (akár még nagy-) vállalati alkalmazása is. Éppen ezért a kibernyomozók számára is ezek a legfontosabbak.

A következőkben az információbiztonság 4. ábra szerint bemutatott részterületeit vizsgáljuk meg a szolgáltatói és felhasználói felelősség oldaláról megközelítve, valamint azt is bemutatva, hogy a kibernyomozó honnan juthat számára releváns információkhoz.

A személyi biztonság a PC/SaaS felhőalapú rendszerekben

A szolgáltató felelőssége: A PC/SaaS felhőalapú rendszerekben a szolgáltatók felelőssége a saját rendszereikhez hozzáférő személyek (saját alkalmazottak, alvállalkozók) ellenőrzése, erre a felhasználónak nincs ráhatása, de még csak rálátása sem. A felhasználó nem szabhatja meg, vagy kérheti számon a szolgáltatót, hogy hogyan végzi ezt, mit követel meg az érintett emberektől. Éppen ezért az ilyen rendszerekben tárolt, kezelt stb. adatokat a felhasználónak ennek megfelelően kell védenie (például titkosítottan tárolni stb.) A kibernyomozó személyi biztonsággal kapcsolatos információkat csekély eséllyel kap a szolgáltatóktól, jellemzően ilyenek a hazai internet- és/vagy felhőszolgáltatóktól szerezhetők be. Ugyanakkor ezen információk nem is igazán relevánsak számára, hiszen sok

[54] Kovács Zoltán: *Az infokommunikációs rendszerek nemzetbiztonsági kihívásai*. Doktori értekezés. Budapest, Nemzeti Közszolgálati Egyetem, 2015.

esetben nem is lehet pontosan felmérni az adott adatokhoz a szolgáltatói oldalon esetlegesen hozzáférők körét (például technikai rendszer karbantartásáért felelős alvállalkozók, egy másik országba, de vállalaton belül kiszervezett, távoli eléréssel rendelkező helpdeskesek stb.).

A felhasználó felelőssége: A felhasználó ugyanakkor teljes ráhatással rendelkezik a szolgáltatások eléréséhez használt végponti eszköz, leggyakrabban a hordozható infokommunikációs eszközök felett, így afelett is, hogy azokhoz ki, milyen jogosultágokkal fér hozzá. Számukra az adatok, információk körének, minősítésének stb. megfelelően előírhatja a hozzáféréshez szükséges engedélyek körét, követelmények listáját. A kibernyomozó a felhasználótól érdemi információkhoz juthat ebben a kérdéskörben.

A fizikai biztonság a PC/SaaS felhőalapú rendszerekben

A szolgáltató felelőssége: A PC/SaaS felhőalapú rendszerekben a szolgáltatók felelőssége a saját rendszereik fizikai védelme, erre a felhasználónak nincs ráhatása, de még csak rálátása sem. Ugyanúgy, mint az ezen rendszerek eléréséhez használt internetszolgáltatás során használt infrastruktúrák esetében sem. A felhasználó nem szabhatja meg, vagy kérheti számon a szolgáltatót, hogyan és hány emberrel, milyen technikai berendezésekkel, vasráccsal stb. őrzi például az adatközpontjait. Éppen ezért az ilyen rendszerekben tárolt, kezelt stb. adatokat a felhasználónak ennek megfelelően kell védenie (például titkosítottan közlekedtetni, tárolni stb.) A kibernyomozó fizikai védelemmel kapcsolatos információkat csekély eséllyel kap a szolgáltatóktól, jellemzően ilyenek a hazai internet- és/vagy felhőszolgáltatóktól szerezhetők be. Ugyanakkor ezen információk nem is igazán relevánsak számára, hiszen például nem lehet pontosan tudni, hogy az adott adatok mely internetszolgáltatók milyen infrastruktúráján haladtak pontosan keresztül.

A felhasználó felelőssége: A felhasználó ugyanakkor teljes ráhatással rendelkezik a szolgáltatások eléréséhez használt végponti eszköz, leggyakrabban a hordozható infokommunikációs eszközök védelme felett. Így ezek fizikai védelme teljes egészében a felhasználó feladata, 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 nemcsak a készüléken éppen fent lévő adatokhoz, hanem a felhasználó későbbiekben folytatott kommunikációjához, felvitt adataihoz, mozgási (hely) adataihoz stb. is hozzáférhetnek a támadók. A kibernyomozó a felhasználótól érdemi információkhoz juthat ebben a témában.

A dokumentumbiztonság a PC/SaaS felhőalapú rendszerekben

A szolgáltató felelőssége: A PC/SaaS felhőalapú rendszerekben az esetek 99%-ában kizárólag elektronikus dokumentumokról beszélhetünk, hiszen még a felhasználói szerződést is így fogadják el a felhasználók. Ezek védelméről *Az elektronikus információbiztonság–kiberbiztonság a PC/SaaS felhőalapú rendszerekben* alfejezetben lesz szó. A kibernyomozó ezzel kapcsolatban releváns információkhoz a szolgáltatóktól ritkán juthat, talán még a hazai internet- és/vagy felhőszolgáltatóktól szerezhet be papíralapú szerződések védelmével kapcsolatos információkat – már ha vannak ilyenek egyáltalán.

A felhasználó felelőssége: A felhasználó ugyanakkor teljes ráhatással rendelkezik a saját dokumentumaival kapcsolatban. (Az elektronikus dokumentumok védelméről ebben az esetben is *Az elektronikus információbiztonság–kiberbiztonság a PC/SaaS felhőalapú rendszerekben* alfejezetben lesz szó.) A nála papíralapon (is) keletkező, a PC/SaaS felhőalapú rendszerekben felhasznált, feltöltött stb. dokumentumok védelmét a saját, valamint erre vonatkozó egyéb (például jogszabályi) előírások, szabályok szerint tudja kezelni. A kibernyomozó a felhasználótól ebben a témakörben is érdemi információkhoz juthat.

Az elhárítás a PC/SaaS felhőalapú rendszerekben

A szolgáltató felelőssége: A PC/SaaS felhőalapú rendszerekben a szolgáltatók felelőssége a saját rendszereikkel kapcsolatos elhárító tevékenység végzése, amelyet a legtöbbször valamilyen saját és/vagy vásárolt kibertérből származó fenyegetettségekkel kapcsolatos hírszerzési *(cyber threat intelligence)* szolgáltatás igénybevételével hajtanak végre. Erre a felhasználónak nincs ráhatása, de

még csak rálátása sem, nem szabhatja meg, vagy kérheti számon a szolgáltatót, hogyan és milyen módon végzi, vagy egyáltalán végzi-e ezt a fajta tevékenységet. A kibernyomozó ezzel kapcsolatban releváns információkhoz a szolgáltatóktól ritkán juthat, talán még a hazai internet- és/vagy felhőszolgáltatóktól szerezhet be ilyen jellegű információkat.

A felhasználó felelőssége: A felhasználó ugyanakkor teljes ráhatással rendelkezik a saját adatai, információi felett, így ezekkel, valamint saját magával és/vagy vállalatával kapcsolatban végezhet, végeztethet fenyegetettségekkel kapcsolatos hírszerzési tevékenységet. Ezt kritikus esetekben és jelentős megszorításokkal (amelynek jogi és a szolgáltatókkal kapcsolatos bizonyos információkhoz való korlátozott hozzáférés az oka), de kiterjesztheti a szolgáltatóra is. (Például keresheti, hogy a szolgáltatótól került-e ki bármilyen adat az elmúlt időszakban a dark webre.) Ugyanakkor – néhány nagyvállalattól eltekintve – ma még nem jellemző, hogy ilyen tevékenységet végeznének, végeztetnének cégek, főleg nem magánszemélyek. A kibernyomozó a felhasználótól ebben a témakörben is érdemi információkhoz juthat.

Az elektronikus információbiztonság–kiberbiztonság a PC/SaaS felhőalapú rendszerekben

A PC/SaaS felhőalapú rendszerekkel kapcsolatos információbiztonsági vizsgálatok során ez a legfontosabb témakör.

A szolgáltató felelőssége: A PC/SaaS felhőalapú rendszerekben az elektronikus információbiztonság–kiberbiztonság megteremtése a szolgáltatók felelőssége. Erre a felhasználónak nincs ráhatása, de még csak rálátása sem. A védelemmel kapcsolatos részletes adatok (például használt védelmi eljárások, eszközök, szoftverek pontos típusa stb.) – biztonsági okokból – a szolgáltatók egyik legféltettebb információi. Ugyanakkor bizonyos általános információkat a szolgáltatók jól felfogott üzleti megfontolások alapján megosztanak a felhasználókkal, érdeklődőkkel. Ilyen lehet például, hogy a szolgáltató milyen tanúsítványokkal (például ISO 27001) rendelkezik, vagy milyen egyéb biztonsági előírásoknak felel meg (például *NIST Cybersecurity Framework*). A kibernyomozó ezzel kapcsolatban releváns információkhoz legtöbb esetben a szolgáltatók honlapjain juthat, ennél bővebb információkat leginkább a hazai internet- és/vagy felhőszolgáltatóktól tud beszerezni.

A felhasználó felelőssége: A felhasználó ugyanakkor teljes ráhatással rendelkezik a saját adatai, információi és a PC/SaaS felhőalapú rendszerek által nyújtott szolgáltatások igénybevételéhez használt eszközök felett, így azok védelmét a saját, valamint erre vonatkozó egyéb (például jogszabályi) előírások, szabályok szerint tudja kezelni. A kibernyomozó a felhasználótól ebben a témakörben is érdemi információkat szerezhet be.

Ki kell emelni azt is, hogy Magyarországon, de akár külföldön működő kibervédelmi szervezetek – elsősorban a CERT-ek és CSIRT-ek – is szolgálhatnak a kibernyomozó számára releváns információkkal. Éppen ezért adott esetekben célszerű elsősorban a Nemzetbiztonsági Szakszolgálat keretein belül működő Nemzeti Kibervédelmi Intézetet (NKI), az Országos Katasztrófavédelmi Főigazgatóság szervezetében található Létfontosságú Rendszerek és Létesítmények Informatikai Biztonsági Eseménykezelő Központot (LRLIBEK), vagy a Honvédelmi Minisztérium saját hálózatbiztonsági vészhelyzeteket elhárító csoportját megkeresni. Segítségükkel, rajtuk keresztül kapcsolatot lehet teremteni külföldi kormányzati CERT-ekkel, CSIRT-ekkel is, akiktől a kibernyomozó szintén hasznos információkhoz juthat.

Összefoglalás

Jelen fejezet bemutatta az információbiztonság alapjait, részterületeit, tisztázta az ezzel kapcsolatos legfontosabb fogalmakat, valamint azok összefüggéseit. Ismertette, hogy az infokommunikációs hálózatokban hogyan lehet értelmezni az információbiztonság egyes részterületeit, majd a nyilvános számítási felhő és szoftver mint szolgáltatás típusú rendszereken (PC/SaaS felhőalapú rendszerek) keresztül bemutatta a szolgáltató és a felhasználó információbiztonsággal kapcsolatos feladatait és felelősségét, valamint azt, hogy a kibernyomozó a számára releváns információkat mely forrásokból gyűjtheti be.

Az egyes részeket olyan szintig mutattuk be, amely lehetővé tette a legfontosabb alapelvek és PC/SaaS felhőalapú rendszerek bizonyos működési sajátosságainak megértését, és az abból kinyerhető, a nyomozó számára fontos információk forrásainak bemutatását. Amennyiben a kibernyomozó a fentiekben leírtaktól eltérő infokommunikációs rendszerrel találkozik, akkor a fent leírtak megfelelő – az adott rendszer sajátosságainak figyelembevételével és az alapokat ismerve a megfelelő szakemberrel történt konzultációt követő – adoptálásával

a többi rendszerre ki tudja terjeszteni, át tudja alakítani, így a szükséges elemzést el tudja végezni.

Az infokommunikációs hálózatokkal kapcsolatos információbiztonsági nyomozói feladatok során a kibernyomozók a legritkább esetben találkoznak rutinszerű ügyekkel, feladatokkal. Ez azt jelenti, hogy egy adott ügy megoldásához kreativitás, a korábbiaktól eltérő információigénylési és -feldolgozási metodika, valamint ehhez az adott infokommunikációs rendszer bizonyos ismerete szükséges. Ennek megfelelően mindig érdemes és célszerű a lehetőségekről a felhasználó, de lehetőség szerint a szolgáltató erre a célra dedikált – általában biztonsági – szakembereivel konzultálni. Ugyancsak célszerű adott esetben a Nemzeti Kibervédelmi Intézetet (NKI), és/vagy a Létfontosságú Rendszerek és Létesítmények Informatikai Biztonsági Eseménykezelő Központot (LRLIBEK) és/vagy a Honvédelmi Minisztérium saját hálózatbiztonsági vészhelyzeteket elhárító csoportját megkeresni, akik a sok hasznos információ mellett lehetővé teszik a külföldön működő kibervédelmi szervezetek megkeresését, amelyek szintén szolgálhatnak a kibernyomozó számára releváns információkkal. Külföldi infokommunikációs szolgáltató esetén ugyanis a szükséges információk beszerzése sokszor nehézségekbe ütközik, ebben segíthetnek ezek a szervezetek.