HADMÉRNÖK

VIII. Évfolyam 3. szám - 2013. szeptember

Kovács Zoltán
zkovacs@nbsz.gov.hu

FELHŐ ALAPÚ RENDSZEREK TÖRVÉNYES ELLENŐRZÉSI MÓDSZEREI VIZSGÁLATA II.

Absztrakt

A napjaink kommunikációs szokásait nagymértékben meghatározzák az Internetes kommunikációt biztosító felhő alapú rendszerek. Ezek azok a mindenki számára elérhető, akár csekély számítástechnikai tudással is használható, olcsón, sokszor ingyenesen igénybe vehető rendszerek, szolgáltatások, amelyek ma már szerves részét képezik mindennapi életünknek (pl. Facebook, gmail, Dropbox, Twitter, Skype stb.) Ezen rendszerek törvényes ellenőrzésének igénye a felhasználás ütemével arányosan nő. A cikksorozat első része áttekinti az említett rendszerek törvényes ellenőrzésének kihívásait, majd publikus forrásokból elérhető információkra alapozva jellemző példákat mutat be külföldi nemzetbiztonsági szolgálatok és rendvédelmi szervek által használt módszerekre. A második rész megvizsgálja a törvényes ellenőrzéshez rendelkezésre álló technikai lehetőségeket, felállítja az ezek elemzéséhez szükséges szempontrendszert, majd az így kialakított szempontrendszer alapján elvégzi azok elemzését.

The habits of recent communication have been dramatically determined by cloud computing which ensure communication via Internet. These systems and services, which have become the part of your everyday life, are available for everyone and can be used with slight IT knowledge at a low price or free (e.g. Facebook, gmail, Dropbox, Twitter, Skype, etc.). The requirement of lawful monitoring of these cloud computing systems has been growing proportionally to the growth of using. The first part of this article series is reviewing the problems appearing in lawful monitoring of cloud computing systems mentioned above, and then presenting representative lawful monitoring methods used by foreign national security services and law enforcement agencies based on public sources. The second part of this article series is analysing the possible technical solutions of lawful monitoring, setting up criteria which needed to analyse them, then doing the analysis of technical solutions by this criteria.

Kulcsszavak: *felhő alapú rendszerek, törvényes ellenőrzés, Skype ~ cloud computing, lawful monitoring, Skype*

BEVEZETÉS

A kommunikáció formái, lehetőségei az Internet és az azt kihasználó alkalmazások fejlődésével ugrásszerűen változnak, bővülnek. A változások ütemét tovább növeli a felhő alapú rendszerek egyre nagyobb mértékű felhasználása, azon belül is a nyilvános számítási felhő (Public cloud) telepítési modell szerint működő, elsősorban szoftver, mint szolgáltatás (Cloud Software as a Service (SaaS)) szolgáltatási modell típusú rendszereké (továbbiakban: PC/SaaS felhő alapú rendszerek). Egyszerűbben fogalmazva ezek azok a mindenki számára – a meglévő személyi használatú eszközök (pl. notebook, okostelefon stb.) felhasználásával, akár csekély számítástechnikai tudással is használható, olcsón, sokszor ingyenesen – igénybe vehető rendszerek, szolgáltatások (mint pl. Facebook, gmail, Dropbox, Twitter, Skype stb.) amelyek ma már szerves részét képezik mindennapi életünknek, kommunikációnknak.

A PC/SaaS felhő alapú rendszerek törvényes ellenőrzésének igénye a felhasználás ütemével arányosan nő, hiszen a (potenciális) célszemélyi kör is ezt használja leginkább. A „Felhő alapú rendszerek törvényes ellenőrzési problémái" című cikk bemutatta az Internet és az azt felhasználó alkalmazások fejlődésével ugrásszerűen változó, bővülő kommunikációs formák, lehetőségek hatásait, áttekintette az elektronikus úton folytatott kommunikáció és a hírközlés viszonyát, e kettő változásait, valamint a PC/SaaS felhő alapú rendszerek törvényes ellenőrzése kapcsán felmerült problémákat. Az összefoglalás és a következtetések részben a törvényes ellenőrzés hatékony kialakítása érdekében teendő továbblépéshez újabb elvégzendő feladatokat fogalmazott meg. Ezek közül az egyik a következő: *„… célszerű áttekinteni, összehasonlítása a törvényes ellenőrzésre jelenleg rendelkezésre álló technikai eszközöket és módszereket, azok előnyeivel, hátrányaival együtt."*. Jelen cikksorozat ezzel a foglalkozik részletesen.

A cikksorozat első része áttekinti a PC/SaaS felhő alapú rendszerek törvényes ellenőrzésének kihívásait, majd ezt követően publikus forrásokból elérhető információkra alapozva jellemző példákat mutat be külföldi nemzetbiztonsági szolgálatok és rendvédelmi szervek által használt módszerekre. A példák ismertetésénél főként a Skype-ot használja mintának. Egyrészt azért, mert ennek a rendszernek a lehallgatása minden országban megoldandó, de problémás feladatként jelentkezett, másrészt pedig azért, mert jól példázza, hogy egy új infokommunikációs rendszer törvényes ellenőrzése kapcsán a különböző országok képesek gyökeresen eltérő irányokba elindulni.

A második rész megvizsgálja a törvényes ellenőrzéshez rendelkezésre álló technikai lehetőségeket, majd felállítja az ezek elemzéséhez szükséges szempontrendszert. Az így kialakított szempontrendszer alapján elvégzi a felsorolt technikai megoldások elemzését, csoportosítva azok előnyeit, hátrányait. Végezetül a következtetések levonása után – illeszkedve a „Felhő alapú rendszerek törvényes ellenőrzési problémái" című cikk összegzésében leírtakhoz – további, a PC/SaaS felhő alapú rendszerek törvényes ellenőrzésének hatékony kialakítása érdekében végrehajtandó feladatokat fogalmaz meg.

A TÖRVÉNYES ELLENŐRZÉS TECHNIKAI LEHETŐSÉGEI

Mint ahogy azt a cikksorozat első részéből kitűnik, az arra felhatalmazott nemzetbiztonsági és rendvédelmi szerveknek jelenleg több technikai megoldás is a rendelkezésére áll ahhoz, hogy a PC/SaaS felhő alapú rendszereket törvényes ellenőrzés alá vonják. Az összehasonlító elemzés elvégzése előtt azonban érdemes áttekinteni ezeket a módszereket, megoldásokat, és összefoglalni azok főbb jellemzőit, tulajdonságait.

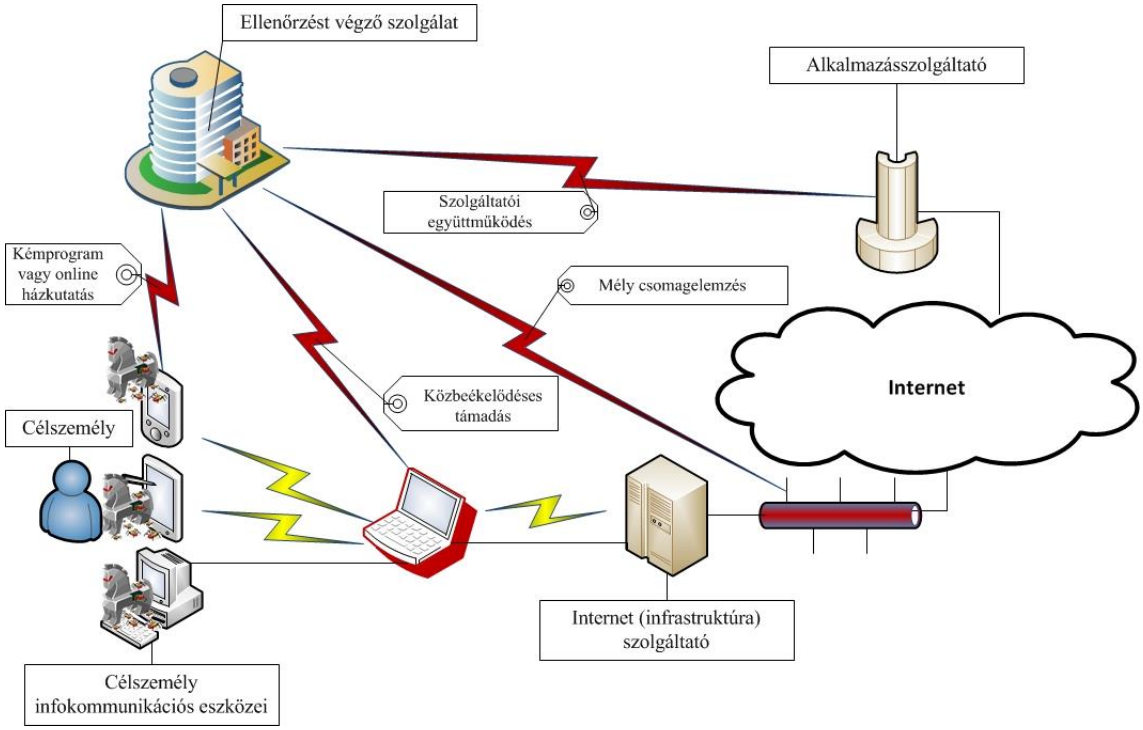
A cikknek nem célja az egyes módszereket minden részletet felölelően ismertetesse, azokat csupán általánosítva, csak az összehasonlítási szempontrendszer felállításához és a végkövetkeztetések levonásához szükséges mértékben tárgyalja.

A PC/SaaS felhő alapú rendszerek törvényes ellenőrzésre alapvetően az alábbi négy módszert használhatják az arra felhatalmazott szolgálatok:

1. aktív támadó eszköz vagy kémprogram (spyware),
2. közbeékelődéses támadás (Man in the middle),
3. mély csomagvizsgálat (Deep Packet Inspection (DPI)),
4. együttműködés a szolgáltatóval.

A módszerek elnevezései önkényesek. Valódi, mindenki által elfogadott magyar megfelelőik vagy nem alakultak ki, vagy az ezekről szóló szakirodalom is többféle megnevezéssel használja azokat.

A fenti módszerekre rendkívül jellemző az alkalmazásakor használt adatszerző, elfogó eszközök (ebbe bele kell érteni a hardver és szoftver elemeket egyaránt) távolsága a célszemélytől. Ezt jól szemlélteti az 1. ábra.



1. ábra. Az adatszerző, elfogó eszközök távolsága a célszemélytől
Forrás: saját

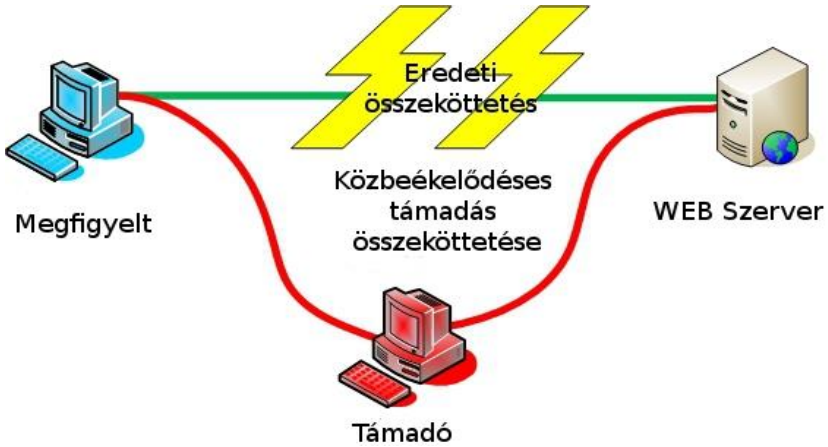
Aktív támadó eszköz (kémprogram vagy online házkutatás):

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

A kémprogram bejuttatása a célszemély eszközére több féle módszerrel is lehetséges, hasonlóan a kiberbűnözők által használt módozatokhoz (pl. elektronikus levél csatolmányaként, fertőzött weboldal segítségével, „0 day” sebezhetőség kihasználásával stb.). A működés során ezek képesek az online kommunikáció elfogására, de billentyűzetleütések tárolására, vagy akár – ha van – a webkamerával képek készítésére is. Az információkat azután összegyűjtve küldik el az aktív támadó eszköz tulajdonosának. [1] [2] [3] [4] [5]

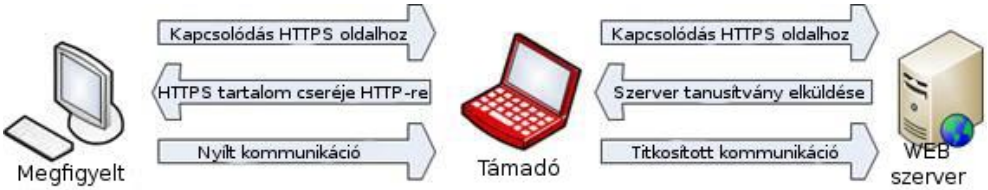
Közbeékelődéses támadás (Man in the Middle):

Leegyszerűsítve a dolgot, a közbeékelődéses támadás esetében a támadó (ellenőrzést végző szolgálat) úgy hallgatja le a két fél között zajló kommunikációt, hogy a kommunikációs csatornát megszakítja (legyen az vezetékes vagy vezeték nélküli), majd abba, a két kommunikáló fél közé „beállva" mindkettőjük számára a másik félnek adja ki magát. A kapcsolat ezáltal mindkét fél számára zavartalannak tűnik, valójában azonban a teljes forgalom „átfolyik" a támadó eszközén, amellyel az itt zajló kommunikációt lehallgathatja, ahhoz teljes mértékben hozzáfér. Ezt szemlélteti a 2. ábra.



2. ábra. Közbeékelődéses támadás
Forrás: https://www.owasp.org/index.php/Man-in-the-middle_attack (letöltve: 2013.07.16.)

A sikeres közbeékelődéses támadáshoz több feltételnek is teljesülnie kell. A támadónak hozzá kell férnie a kommunikációs csatornához, képesnek kell lennie annak megszakítására (legyen az vezetékes vagy vezeték nélküli kapcsolat) oly módon, hogy megakadályozza, hogy az üzenetek eljussanak a valódi címzetthez, majd le kell tudni lehallgatni a rajta küldött üzeneteket. Ez titkosítás nélküli kommunikáció esetében viszonylag egyszerű, de bizonyos esetekben, kis szerencsével és a valódi kommunikáló fél (felek) figyelmetlenségével akár titkosított kommunikáció esetén is megvalósítható. Ezt szemlélteti a 3. ábra.



3. ábra. Példa HTTPS kommunikáció lehallgatására
Forrás: http://www.windowsecurity.com/articles-tutorials/authentication_and_encryption/Understanding-Man-in-the-Middle-Attacks-ARP-Part4.html (letöltve: 2013.07.16.)

Sikeres közbeékelődéses támadás akkor hajtható végre viszonylag egyszerű eszközökkel és nagy valószínűséggel, ha a célszemélyhez (azaz az egyik kommunikáló félhez) a támadó a lehető legközelebb helyezkedik el. [6] [7] [8] [9] 10] [11]

Mély csomagvizsgálat (Deep Packet Inspection (DPI)):

A mély csomagvizsgálat azt jelenti, hogy az adatcsomagoknak nemcsak a fejlécét, hanem azok adattartalmát is vizsgálat alá vetik, majd az adattartalom alapján kiszűrik az „érdekes" adatcsomagokat. A szűrés jellege a mély csomagvizsgálat felhasználásának céljától függ, a csomagvizsgálati módszerek azonban technikailag függetlenek attól. [12]

A mély csomagvizsgálatot leggyakrabban három esetben szokták alkalmazni. Az első eset a behatolást észlelő és behatolásvédelmi rendszerekben (Intrusion Detection Systems (IDS),

Intrusion Prevention Systems (IPS)) történő felhasználás. Ezek a rendszerek a csomagok elemzésekor speciális bitmintákat (ismert támadókódokat) keresnek erre dedikált eszközök segítségével, majd a felismert, rosszindulatú kódot tartalmazó csomagokat kiszűrik. [13] A második a hírközlési/Internet szolgáltatók rendszereiben történő alkalmazás. Itt az internet protokoll alapú hangátviteli szolgáltatások (VoIP) és a peer-to-peer (P2P) kapcsolaton alapuló fájlcsere forgalmának blokkolására használják a technológiát. [14] A harmadik a törvényes ellenőrzés, ahol a csomagok vizsgálata alapján dönthető el, hogy az ellenőrzést végző számára érdekes-e (pl. adott célszemélyhez tartozik-e az email), vagy sem. Itt a szűrés azonban nem a kiválasztott csomagok blokkolását szolgálja, hanem azoknak az ellenőrzést végző szolgálathoz (is) történő eljuttatását. [15] [16] [17] [18]

Titkosítás nélküli kommunikáció esetén a lehallgatás viszonylag egyszerűen, sőt – ebben az esetben, ellentétben a közbeékelődéses támadással – tömegesen is megvalósítható. Ugyanakkor titkosított kommunikáció esetén a tartalomhoz való hozzáféréshez feltétlenül szükséges a titkosítás feltörése, ez pedig is hosszadalmas, nagy számítástechnikai eszközparkot igénybe vevő folyamat. Ráadásul a kommunikáló felek akár a nyílt forgalmaknál is egyszerű – és ingyenesen rendelkezésre álló – titkosító szoftver eszközök használatával (pl. HTTPS Everywhere) jelentősen megnehezíthetik, vagy akár el is lehetetlenítik az ellenőrzést. [15]

Együttműködés a szolgáltatóval:

A szolgáltatóval való együttműködés a hagyományos hírközlési szolgáltatóknál már jól ismert és bevált modell szerint működik. Ekkor az ellenőrzést végző szerv eljuttatja a célszemélyhez kapcsolódó releváns adatokat (pl. felhasználói név) a szolgáltató rendszerébe, majd a szolgáltató automatikusan (emberi beavatkozás nélkül) vagy egyedi kiszolgálással (emberi beavatkozással) biztosítja a – rendszerében rendelkezésre álló – kért adatokat, információkat, vagy akár a rajta átfolyó kommunikáció tartalmát is. [17]

A TÖRVÉNYES ELLENŐRZÉSI MÓDSZEREK VIZSGÁLATI, ÖSSZEHASONLÍTÁSI SZEMPONTJAI

Az eddigiekből tehát látható, hogy a PC/SaaS felhő alapú rendszerek törvényes ellenőrzésre több lehetőség, módszer is a felhatalmazott szolgálatok rendelkezésére áll. Ezek a módszerek azonban jelentősen – mondhatni minden paraméterükben – eltérnek egymástól, akár a technikai megvalósításukat, akár a hatékonyságukat, vagy akár a jogi szabályozottságukat vesszük figyelembe. Annak érdekében, hogy az egyes módszereket össze tudjuk hasonlítani, először fel kell állítani egy, a vizsgálatukra megfelelő szempontrendszert. Ennek tartalmaznia kell minden olyan lényeges szempontot, amely alapján a titkos információgyűjtésre és a titkos adatszerzésre felhatalmazott szerv dönteni tud arról, hogy melyiket (melyikeket) kívánja megvasalósítani és munkájában felhasználni.

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

- *Az egy időben ellenőrizhető célszemélyek száma:* Ebben a kérdéskörben nem elsősorban a tényleges számadatot kell megvizsgálni, hanem azt, hogy egyedi vagy tömeges ellenőrzést tesz-e lehetővé a módszer.
- *Az ellenőrző eszköz működési módja:* Fontos kérdés, hogy az eszköz aktív vagy passzív módon működik-e. Ennek ugyanis meghatározó jelentősége van egyrészt az ellenőrzés célszemély általi felfedezhetőségében (dekonspiráció), másrészt a módszer alkalmazására, alkalmazhatóságára vonatkozó jogi háttér vizsgálatakor (meglévő törvényi szabályozás keretei).

- *A módszer jogi hátterének rendezettsége:* Ennek keretében kell megvizsgálni, hogy az adott módszer egyáltalán alkalmazható-e az adott ország jogrendszere szerint, és ha igen, milyen keretek között. Az is elképzelhető, hogy bizonyos ellenőrzési metódusokra – annak újszerűsége miatt – sem kizáró, sem engedélyező szabályozó sincs a jogrendben.
- *Az ellenőrző eszköz célszemélyhez való közelsége:* A dekonspiráció veszélyének a felméréséhez meg kell vizsgálni, hogy telepítéskor, működés közben, leállításkor és eltávolításkor (törvényes ellenőrzés megszüntetésekor), milyen távolságban (jobban érzékeltetné a problémát, a távolság helyett a közelség megfogalmazás) kell lenni a célszemélytől, hogy a módszert alkalmazni lehessen.
- *A módszer alkalmazásának technikai problémái:* Itt a telepítéskor, működés közben, leállításkor és eltávolításkor (törvényes ellenőrzés megszüntetésekor) felmerülő technikai problémákat kell számba venni.
- *A hozzáférhető adatok köre:* A döntés szempontjából lényeges elem, hogy az adott módszerrel milyen információkhoz (csak az online átfolyó vagy a tárolt adatok is) jut hozzá az törvényes ellenőrzést végző szervezet.
- *Online kommunikációhoz való hozzáférés teljes körűsége:* Fontos tényező, hogy a célszemély online forgalmát teljes egészében vagy csak részlegesen biztosítja az adott módszer. Ennek a kérdésnek a vizsgálatakor nem vesszük figyelembe, hogy a kommunikáció titkosított-e vagy sem, csak azt, hogy a célszemély minden kommunikációja összes bitjének elfogását biztosítja-e az adott módszer.
- *A módszer alkalmazásának problémái titkosított adatkommunikáció esetén:* Az ellenőrzési módszer hatékonyságát nagymértékben befolyásolja, hogy képes-e, és ha igen, milyen esetekben és mértékben a titkosított kommunikációból az eredeti tartalmat (pl. üzeneteket, képeket, beszédet stb.) biztosítani a titkos információgyűjtést végző szerv számára.
- *Beruházási igény:* Az sem elhanyagolható szempont, hogy az adott módszer alkalmazásához szükséges eszközrendszer mennyibe kerül.
- *Egyéb költségek:* Olyan egyéb járulékos költségek is fellépnek, felléphetnek, amelyekkel komolyan számolni kell az alkalmazást megelőzően. Ilyenek lehetnek pl. az együttműködőknek fizetendő díjak, a betanítás vagy éppen speciális ismeretekkel rendelkező (pl. hacker) szakemberek (tovább)képzési vagy megvásárlási költségei.
- *Célszemélyek adataihoz harmadik fél hozzáférése:* Lényeges kérdés az is, hogy a célszemély adataihoz a törvényes ellenőrzést végző szolgálat munkatársain kívül ki fér, férhet még hozzá. Ez ugyanis nagymértékben növelheti a dekonspiráció veszélyét. (Itt nem vizsgáljuk az eszköz alkalmazása során, a működés miatt fellépő dekonspirációt, azaz azt, amikor a célszemély, vagy annak közvetlen környezete szerez tudomást az alkalmazásról. Ebben az esetben kizárólag harmadik fél hozzáférését (pl. szolgáltató szakemberei) vizsgáljuk.)

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

A TÖRVÉNYES ELLENŐRZÉS MÓDSZEREINEK VIZSGÁLATA

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

Aktív támadó eszköz (kémprogram vagy online házkutatás):

- *Az egy időben ellenőrizhető célszemélyek száma:* egyedi ellenőrzést tesz lehetővé.
- *Az ellenőrző eszköz működési módja:* aktív módszer, a dekonspiráció veszélye magas.
- *A módszer jogi hátterének rendezettsége:* a módszerre nincsenek mindenki által elfogadott jogszabályok, több ország most próbálja a felhasználás, alkalmazás pontos jogi kereteit kialakítani.
- *Az ellenőrző eszköz célszemélyhez való közelsége:* a vizsgált módszerek közül a legközelebb működik a célszemélyhez.
- *A módszer alkalmazásának technikai problémái:* a közelség okán a telepítés, újratelepítés nehézkes lehet, az online kapcsolat megszakadásakor az eszköz „eltűnik” az ellenőrzést végző szervek elől, kikerül a felügyeletük alól.
- *A hozzáférhető adatok köre:* nemcsak az online forgalomhoz, hanem az adott eszközön tárolt minden fájlhoz elérést biztosít, sőt további ellenőrzési lehetőségeket (pl. web kamerával képkészítés) is kínál.
- *Online kommunikációhoz való hozzáférés teljes körűsége:* nem ad teljes körű hozzáférést, hiszen csak azon az eszközön bonyolított kommunikációt képes elfogni, amelyikre feltelepítették.
- *A módszer alkalmazásának problémái titkosított adatkommunikáció esetén:* a kommunikációt a titkosítást megelőzően képes elfogni, így a felhasznált titkosítástól függetlenül ellenőrizhetővé teszi a kommunikációt.
- *Beruházási igény:* közepes, az alkalmazott eszközök, a bejuttatáshoz esetleg használt un. „0 day” sebezhetőségek költségesek.
- *Egyéb költségek:* magas, a módszer alkalmazásához speciális (hacker) tudással rendelkező szakemberek szükségesek.
- *Célszemélyek adataihoz harmadik fél hozzáférése:* ennek lehetősége minimális.

Közbeékelődéses támadás (Man in the Middle):

- *Az egy időben ellenőrizhető célszemélyek száma:* egyedi ellenőrzést tesz lehetővé.
- *Az ellenőrző eszköz működési módja:* aktív módszer, a dekonspiráció veszélye magas.
- *A módszer jogi hátterének rendezettsége:* a módszerre nincsenek mindenki által elfogadott jogszabályok.
- *Az ellenőrző eszköz célszemélyhez való közelsége:* a módszer kizárólag a célszemély (infokommunikációs eszközének) közvetlen közelében működik.
- *A módszer alkalmazásának technikai problémái:* az alkalmazás teljes időtartamában kötelezően a célszemély (infokommunikációs eszközének) közelében kell tartózkodni. Ez pedig az egész alkalmazást nehézkessé, esetlegessé teszi, teheti.
- *A hozzáférhető adatok köre:* csak az online forgalomhoz biztosít elérést.
- *Online kommunikációhoz való hozzáférés teljes körűsége:* nem ad teljes körű hozzáférést, hiszen csak azon az eszközön bonyolított kommunikációt képes elfogni, amelyik forgalma „átfolyik” az ellenőrző (ábrán: támadó) eszközön.
- *A módszer alkalmazásának problémái titkosított adatkommunikáció esetén:* kis szerencsével és a célszemély figyelmetlenségével párosulva bizonyos titkosított forgalmaknál is lehetővé teszi a közlemények megismerését.

- *Beruházási igény:* alacsony, az ellenőrzés gyakorlatilag kommersz eszközökkel megvalósítható.
- *Egyéb költségek:* magas, a módszer alkalmazásához speciális (hacker) tudással rendelkező szakemberek szükségesek.
- *Célszemélyek adataihoz harmadik fél hozzáférése:* ennek lehetősége minimális.

Mély csomagvizsgálat (Deep Packet Inspection (DPI)):

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

Együttműködés a szolgáltatóval:

- *Az egy időben ellenőrizhető célszemélyek száma:* tömeges ellenőrzést tesz lehetővé.
- *Az ellenőrző eszköz működési módja:* passzív módszer, a dekonspiráció veszélye alacsony.
- *A módszer jogi hátterének rendezettsége:* a módszerre nincsenek mindenki által elfogadott jogszabályok, az alkalmazásszolgáltatók általában nem hajlandóak együttműködni.
- *Az ellenőrző eszköz célszemélyhez való közelsége:* a célszemélytől (infokommunikációs eszközeitől) távol működik.
- *A módszer alkalmazásának technikai problémái:* az alkalmazásszolgáltató együttműködése esetén problémamentes.
- *A hozzáférhető adatok köre:* csak az online forgalomhoz és a szolgáltatónál tárolt adatokhoz, információkhoz biztosít elérést.
- *Online kommunikációhoz való hozzáférés teljes körűsége:* az alkalmazásszolgáltatón keresztül lebonyolított kommunikációhoz teljes körű hozzáférést ad.

- *A módszer alkalmazásának problémái titkosított adatkommunikáció esetén:* a szolgáltató által használt titkosítás ekkor nem jelent problémát, gondot kizárólag a felhasználó által esetleg használt egyedi titkosítás okozhat.
- *Beruházási igény:* alacsony, az összes többi módszernél is jelentkező feldolgozó terminálok kivételével alig igényel plusz eszközt.
- *Egyéb költségek:* közepes, a módszer alkalmazásához nem kellenek külön speciális tudással rendelkező szakemberek, de az alkalmazásszolgáltató beruházásait, vagy adott esetben az adatszolgáltatását a helyi jogszabályoknak megfelelően esetleg fizetni kell.
- *Célszemélyek adataihoz harmadik fél hozzáférése:* magas, ma még sokszor emberi beavatkozással működik az adatszolgáltatás és a kommunikáció ellenőrizhetővé tétele is, ráadásul a kérésekben foglalt érzékeny vagy akár minősített adatokhoz (pl. célszemély adatai) – általában – külföldi szolgáltató hazai biztonsági ellenőrzésen át nem esett emberei férhetnek hozzá, a kérő szerv szemszögéből kontrollálatlanul.

Annak érdekében, hogy az arra felhatalmazott szervek számára a PC/SaaS felhő alapú rendszerek törvényes ellenőrzésére jelenleg rendelkezésre álló módszereket össze tudjuk hasonlítani, célszerű azok előnyeit, hátrányit is összefoglalni. Ezt tartalmazza a következő táblázat.

Módszer	**előnyök**	**hátrányok**
aktív támadó eszköz (kémprogram vagy online házkutatás)	• nem csak az éppen folyó forgalmat, hanem a gépen tárolt minden adatot el lehet érni • titkosítás előtti elfogás – azaz felhasznált titkosítástól függetlenül ellenőrizhető a forgalom	• egyedi ellenőrzés (egy trójai, egy eszköz) • telepítés problémákba ütközhet • célszemély minden eszközére kell telepíteni a teljes körű ellenőrzéshez • aktív, ezért működése adott esetben felfedezhető • működése, működő képessége nagymértékben függ a céleszköz beállításaitól, telepített szoftvereitől (pl. vírusirtó, tűzfal) • működése azonnali utasítással nem megszakítható • alapos előkészületek ellenére a képességet egy egyszerű (pl.: vírusellenőrző) frissítés ellehetetlenítheti • jogszabályi háttere nem egyértelmű
közbeékelődéses támadás (Man in the Middle)	• bizonyos titkosított forgalmaknál is lehetővé teszi a közlemények megismerését (általában SSL, https esetén)	• egyedi ellenőrzés (egy netforgalomra) • más titkosított forgalmak problémát okozhatnak • viszonylag közel kell menni • több eszköz és netelérés esetén problémás (pl. vezetékes és mobil net) • adott esetben a tevékenység felfedezhető • csak az éppen folyó forgalmat lehet vele megismerni • titkosított forgalom esetében az alkalmazónak szükséges hiteles tanúsítvánnyal rendelkeznie • jogszabályi háttere nem egyértelmű
mély csomagvizsgálat (DPI)	• tömeges – egyszerre több célszemély forgalma is ellenőrizhető • teljesen passzív • tartalom alapú szűrést tesz lehetővé • jogszabályi háttere egyértelmű	• nagy beruházási igény • az egyre növekvő sávszélesség miatt egyre gyorsabb, nagyobb sávszélességű elfogókat kell használni • titkosítás problémákat okozhat • adott „csatornán” átfolyó forgalmat elemzi, ha nem ott megy a célszemély forgalma, nem fogja el – nem teljes körű • csak az éppen folyó forgalmat lehet vele megismerni

együttműködés a szolgáltatóval	• tömeges – egyszerre több célszemély is ellenőrizhető • teljes információkör elérhető, használt eszközöktől, neteléréstől függetlenül • nem csak az éppen folyó forgalmat, hanem a szolgáltatónál tárolt minden adatot (pl. piszkozatok) el lehet érni • szolgáltató által alkalmazott titkosítás nem probléma	• a szolgáltatók nem mindig partnerek, csak jogszabályi alapon működik (hatékonyan) • külföldi szolgáltatók felhasználóinak ellenőrzése esetén ráadásul nemzetközi jogszabályok szükségesek • célszemély adatait szolgáltató is megismeri – titoktartási, konspirációs gondot okozhat • több szolgáltatót használó célszemélyeknél mindegyikkel együtt kell működni

1. táblázat. A PC/SaaS felhő alapú rendszerek törvényes ellenőrzésére jelenleg rendelkezésre álló módszerek előnyei, hátrányai

ÖSSZEFOGLALÁS, KÖVETKEZTETÉSEK

A cikksorozat első része – a „Felhő alapú rendszerek törvényes ellenőrzési problémái” című cikkre alapozva – áttekintette a PC/SaaS felhő alapú rendszerek törvényes ellenőrzése kapcsán felmerült problémákat, majd – a teljesség igénye nélkül – megvizsgálta, hogy különböző országok hogyan valósítják meg, vagy legalábbis hogyan próbálják megvalósítani az említett rendszerek törvényes ellenőrzését. A nemzetközi példák bár széles, de nem teljes körű áttekintést adtak. Ennek egyrészt az az oka, hogy csak publikus információkra lehet támaszkodni, azok pedig – az ügy jellegére tekintettel meglehetősen korlátozottak, ráadásul szinte sohasem igazoltak, így nem lehetnek teljes körűek. A másrészt pedig az, hogy a törvényes ellenőrzésre felhatalmazott szervek részére rendelkezésre álló módszerek ismertetéséhez, elemzéséhez egyébként sincs szükség teljes körű áttekintésre.

A cikksorozat második része áttekintette a PC/SaaS felhő alapú rendszereket törvényes ellenőrzésre jelenleg rendelkezésre álló technikai lehetőségeket, majd felállította ezek vizsgálati, összehasonlítási szempontrendszerét. Ezt követően elvégezte a különböző módszerek vizsgálatát, megadta azok előnyeit, hátrányait, és megállapította, hogy a titkos információgyűjtésre felhatalmazott szervek az elemzést követően már nem csak az adott módszer bevezetéséről, rendszeresítéséről képesek dönteni, hanem arról is, hogy egy adott ügyben, adott körülmények között melyik ellenőrző metódus használata a legcélravezetőbb.

Összefoglalásként elmondható, hogy jelenleg több, egymástól technikailag és működés szempontjából is gyökeresen eltérő megoldás áll az arra feljogosított szervezetek rendelkezésére, hogy a PC/SaaS felhő alapú rendszerek kapcsán felmerülő törvényes ellenőrzési feladataikat végrehajtsák. Ezek a megoldások azonban annyira újak a törvényes ellenőrzés eszközrendszerében, hogy azok használata sok országban egyáltalán nincs jogilag szabályozva. Más országokban újonnan megjelenő szabályzókkal – sokszor vitatottan, vagy éles bírálatok közepette – vezetik be ezen ellenőrzési formákat, vagy legitimizálják a már működő rendszereket. Megint más országokban pedig a meglévő jogszabályokba próbálják több-kevesebb sikerrel beleérteni, beleerőltetni az új ellenőrzési formákat.

A cikksorozat alapján több következtetés is levonható:

1. A PC/SaaS felhő alapú rendszerek ellenőrzése minden ország törvényes ellenőrzést végző szervei számára kihívást jelentenek.
2. A törvényes ellenőrzést végzők számára több technikai megoldás is létezik a PC/SaaS felhő alapú rendszerek ellenőrzésére.
3. Ezen technikai megoldások jogi megítélése kétséges.
4. Nincsen olyan általánosan elfogadott jogi szabályozás a PC/SaaS felhő alapú rendszerek ellenőrzése kapcsán, amelyhez – akár Magyarországnak is – igazodni lehetne.
5. A fent leírt módszerek egyike sem nyújt teljes körű megoldást a nemzetbiztonsági és rendvédelmi szervek által törvényes ellenőrzés keretében igényelt adatok megszerzéséhez.
6. A törvényes ellenőrzésre felhatalmazott szervezeteknek – alkalmazkodva a törvényi keretekhez, a célszemély által használt eszközökhöz, szolgáltatásokhoz, a célszemély kommunikációs szokásaihoz, a műveleti helyzethez és az egyéb (pl. infrastruktúraszolgáltató által használt) technikai feltételekhez – több, esetleg minden ellenőrzési módra fel kell készülniük, és az azokhoz szükséges eszközöket be kell szerezniük.
7. Az alkalmazásszolgáltatóval való együttműködés az egyik leghatékonyabb és legköltség-takarékosabb ellenőrzési forma, így ez kikerülhetetlen, ugyanakkor ennek jogi szabályozottságában lelhető fel a legtöbb hiány. Így ma gyakorlatilag a legtöbb ország – így Magyarország – esetében is kizárólag az alkalmazásszolgáltató jóindulatán múlik, együttműködik-e az ellenőrzést végző szervekkel, és teljesíti-e – az egyébként teljesen legális, hatályos és pl. a hírközlési szolgáltatók számára (is) kötelező érvényű bírói végzésben foglaltakat.
8. A törvényes ellenőrzés hatékonyságának növelése érdekében az új hazai jogi szabályozás kialakítását – akár átmeneti jelleggel is – mi hamarabb meg kell tenni, azzal nem célszerű megvárni a feltehetően még évekig húzódó szabványosítási eljárásokat és – a várhatóan csak azt követő – Európai Uniós irányelvek kialakítását. Ennek során olyan, jelenleg sérthetetlennek tűnő dolgokhoz kell hozzányúlni (szabályozni és adott esetben szankcionálni!), mint a hazai infrastruktúrával nem rendelkező, Internetes alkalmazást nyújtó cégek működési jogai, kötelezettségei Magyarországon.

Annak érdekében, hogy a PC/SaaS felhő alapú rendszerek törvényes ellenőrzési problémáit kezelni lehessen, a „Felhő alapú rendszerek törvényes ellenőrzési problémái” című cikk az összefoglalás és következtetés részben meghatározott néhány, további elvégzendő feladatot. Ezek közül jelen cikksorozat a másodikra ad választ, azaz áttekintette és összehasonlította az említett rendszerek törvényes ellenőrzésére jelenleg rendelkezésre álló technikai eszközöket és módszereket, azok előnyeivel, hátrányaival együtt. További feladatként, a jogi szabályozás kialakítása előtt, el kell végezi az infrastruktúra-, alkalmazás- és tartalomszolgáltatók fogalmának a definiálását. Majd ezt követően lehet meghatározni, hogy mit kell ellenőrzés alá vonni ahhoz, hogy a nemzetbiztonsági és a bűnüldözői munkát hatékonyan lehessen a támogatni, és ezek alapján célszerű a törvényi szabályozást átalakítani.

Felhasznált irodalom

[1] Chaos Computer Club analyzes government malware (2011. 10. 08.) http://ccc.de/en/updates/2011/staatstrojaner (2013.06.24.)

[2] Sergey Golovanov: Spyware. HackingTeam (2013. 04. 23.) http://www.securelist.com/en/analysis/204792290/Spyware_HackingTeam 2013.06.28.)

[3] Morgan Marquis-Boire - Bill Marczak - Claudio Guarnieri - John Scott-railton: For their eyes only (2013.05.01.) https://citizenlab.org/storage/finfisher/final/fortheireyesonly.pdf (2013.06.28.)

[4] DEFINITION: spyware (2006. október) http://searchsecurity.techtarget.com/definition/spyware (2013.07.16.)

[5] Spyware http://www.spywareguide.com/term_show.php?id=12 (2013.07.16.)

[6] Chris Sanders: Understanding Man-in-the-Middle Attacks – ARP Cache Poisoning (Part 1) (2010. 03. 17.) http://www.windowsecurity.com/articles-tutorials/authentication_and_encryption/Understanding-Man-in-the-Middle-Attacks-ARP-Part1.html (2013.07.16.)

[7] Chris Sanders: Understanding Man-In-The-Middle Attacks – Part2: DNS Spoofing (2010. 04. 07.) http://www.windowsecurity.com/articles-tutorials/authentication_and_encryption/Understanding-Man-in-the-Middle-Attacks-ARP-Part2.html (2013.07.16.)

[8] Chris Sanders: Understanding Man-In-The-Middle Attacks - Part 3: Session Hijacking (2010. 05. 05.) http://www.windowsecurity.com/articles-tutorials/authentication_and_encryption/Understanding-Man-in-the-Middle-Attacks-ARP-Part3.html (2013.07.16.)

[9] Chris Sanders: Understanding Man-In-The-Middle Attacks - Part 4: SSL Hijacking (2010. 06. 09.) http://www.windowsecurity.com/articles-tutorials/authentication_and_encryption/Understanding-Man-in-the-Middle-Attacks-ARP-Part4.html (2013.07.16.)

[10] Dennis Fisher: What is a Man-in-the-Middle Attack? (2013. 04. 10.) http://blog.kaspersky.com/man-in-the-middle-attack/ (2013.07.16.)

[11] Man-in-the-Middle Tutorial: Learn About Man-in-the-Middle Attacks, Vulnerabilities and How to Prevent MITM Attacks http://www.veracode.com/security/man-in-the-middle-attack (2013.07.16.)

[12] Alex Wawro: What Is Deep Packet Inspection? (2012. 02. 01.) http://www.pcworld.com/article/249137/what_is_deep_packet_inspection_.html (2013.07.19.)

[13] Ido Dubrawsky: Firewall Evolution - Deep Packet Inspection (2010. 11. 02.) http://www.symantec.com/connect/articles/firewall-evolution-deep-packet-inspection (2013.06.28.)

[14] BEREC preliminary findings on traffic management practices in Europe show that blocking of VoIP and P2P traffic is common, other practices vary widely http://berec.europa.eu/doc/2012/TMI_press_release.pdf (2013.06.28.)

[15] Alex Wawro: A simple guide to Deep Packet Inspection (2012. 02. 01.) http://features.techworld.com/security/3334780/a-simple-guide-to-deep-packet-inspection/ (2013.06.28.)

[16] Ellen Messmer : US government's use of deep packet inspection raises serious privacy questions (2013. 04. 24.) http://news.techworld.com/security/3444019/dhs-use-of-deep-packet-inspection-technology-in-new-net-security-system-raises-serious-privacy-questions/ (2013.06.28.)

[17] NSA slides explain the PRISM data-collection program (2013. 06. 29.) http://www.washingtonpost.com/wp-srv/special/politics/prism-collection-documents/ (2013.06.28.)

[18] Ewen MacAskill, Julian Borger, Nick Hopkins, Nick Davies and James Ball: GCHQ taps fibre-optic cables for secret access to world's communications (2013. 06. 21.) http://www.guardian.co.uk/uk/2013/jun/21/gchq-cables-secret-world-communications-nsa (2013.07.05.)

Ábrák jegyzéke