HADMÉRNÖK

VIII. Évfolyam 3. szám - 2013. szeptember

Kovács Zoltán
zkovacs@nbsz.gov.hu

FELHŐ ALAPÚ RENDSZEREK TÖRVÉNYES ELLENŐRZÉSI MÓDSZEREI VIZSGÁLATA I.

Absztrakt

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 ensures 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 for 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, összehasonlítani 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 FELHŐ ALAPÚ RENDSZEREK TÖRVÉNYES ELLENŐRZÉSI KIHÍVÁSAI

A felhő alapú rendszerek törvényes ellenőrzése minden ország nemzetbiztonsági és rendvédelmi szervét kihívások elé állítja. Az elektronikus úton folytatott kommunikáció ma már jóval tágabb értelemben értelmezhető fogalom, mint a hagyományos hírközlés, hiszen lehetőségei, a kommunikációs formák száma messze meghaladják ez utóbbiét. Ennek következtében rengeteg olyan új rendszer, technológia jelent, jelenik meg, amelyek törvényes ellenőrzését az arra feljogosított szolgálatoknak meg kell, vagy legalábbis meg kellene oldani. Az új technológiák megjelenése mellett egy jól kivehető átalakulási folyamat is zajlik a hírközlés, vagy pontosabban fogalmazva az elektronikus úton folytatott kommunikáció

területén. A klasszikus hírközlési szolgáltatói modellt egyre inkább felváltja egy specializált infrastruktúra-, alkalmazás-, és tartalomszolgáltatói (ez utóbbival jelen cikk nem foglalkozik) modell, és ez a tendencia a jövőben várhatóan tovább erősödik. Az új modell legjelentősebb hatása a hírközlésre, hogy az infrastruktúraszolgáltató a hírközlési hálózatot – vagy célszerűbb megfogalmazással Internet elérést – biztosítja, míg az alkalmazásszolgáltató gondoskodik a tényleges kommunikációs szolgáltatásról.

Az új technológiák megjelenése önmagukban is arra késztetik a kommunikáció törvényes ellenőrzésével foglalkozó szervezeteket, hogy figyeljék a trendeket, kövessék a sokak által használt technológiák fejlődését, és biztosítsák azok törvényes ellenőrzését. Legalább ugyan ilyen mértékű kényszerítő erőt jelent, hogy a fenti bekezdésekben vázolt felhasználói változások okán a hagyományosnak mondható kommunikációs formák és rendszerek (pl. telefónia) jelentősége a felhasználók – ezáltal a potenciális célszemélyi kör, így a törvényes ellenőrzést végző szolgálatok – számára csökken.

A törvényes ellenőrzést végző szervezeteknek alapvetően az a feladata, célja, hogy a kijelölt célszemélyek kommunikációját lehetőség szerint teljes mértékben ellenőrizzék, függetlenül annak formájától, az általuk használt technológiától, eszközöktől, alkalmazásoktól. Az egyik legnagyobb feladat tehát, hogy pontosan meghatározzuk azt, hogy mit kell, mit célszerű ellenőrizni, majd ehhez ki kell alakítani a megfelelő technikai és jogszabályi környezetet.

Az elektronikus úton folytatott kommunikáció változásában nagy szerepük van a PC/SaaS felhő alapú rendszereknek, ahol is alkalmazásszolgáltatók biztosítják azokat a szolgáltatásokat, amelyeken keresztül – a lehető legkülönfélébb módon – elektronikus kommunikációt lehet folytatni. Ezen rendszerek törvényes ellenőrzésének megteremtése tehát kiemelt feladat az arra feljogosított szervek számára, ugyanakkor a feladat ellátását több probléma is nehezíti.

Az egyik probléma a jogi szabályozás hiányosságaiban keresendő. A rohamosan fejlődő technológiával, az ezen belül gyökeresen átalakuló kommunikációs módokkal, valamint az Internet szabadságával egyelőre nehezen birkózik meg a jogi világ. A hatályos jogszabályok nem, nem teljes mértékben vagy csak erős „beleértéssel” teszik lehetővé a PC/SaaS felhő alapú rendszerek ellenőrzését.

A másik problémát a technikai megoldások hiánya jelenti. Az új technológia új ellenőrző eszközöket kíván, kívánhat, ez pedig beruházást igényel. Sokszor azonban még nincsenek meg azok a technikai eszközök, amelyekkel az új technológiák törvényes ellenőrzését egyáltalán végre lehet hajtani. Ráadásul az eltérően felépített szolgáltatói infrastruktúrák miatt ez akár szolgáltatónként eltérő megoldásokat igényelhet, ami igen költséges.

A harmadik nagy problémát az okozza, hogy a hírközlés ellenőrzésnél régóta kialakult és elfogadott rend, miszerint az infrastruktúrával és szolgáltatással az adott országban egyaránt jelen lévő szolgáltató együttműködik a nemzetbiztonsági és bűnüldöző szervekkel, ebben az esetben nem, vagy nem teljes mértékben működik.

Az arra feljogosított szerveknek azonban addig is, amíg kialakul a mindenki által elfogadott, letisztult jogi környezet és az összes igényt kielégítő technikai háttér, a törvényes ellenőrzést – valamilyen formában – biztosítaniuk kell. Ehhez a korábban már kialakult kelléktárat és a hatályos jogszabályokat alapul véve próbálnak más és más megoldást alkalmazni. Még a fejlett demokráciával és ipari háttérrel rendelkező országok esetében is kiépítő, vagy nem is demokratikusnak tekintett országokról. Érdemes – a nyíltan elérhető anyagok alapján – megvizsgálni, hogy milyen módszerek állnak a titkos információgyűjtést végző szervezetek rendelkezésére, és azok alkalmazása során milyen buktatókba ütköztek. [1]

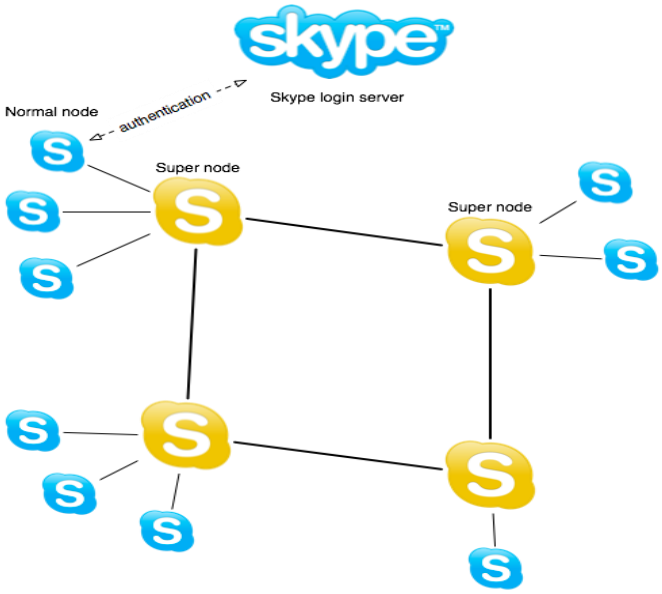
NEMZETKÖZI PÉLDÁK

Skype, mint „állatorvosi ló”:

A Skype esetét célszerű példaként, különállóan vizsgálni. 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 még a fejlett demokráciával rendelkező országok is képesek gyökeresen eltérő irányokba elindulni, nem beszélve a demokráciát még éppen kiépítő, vagy nem is demokratikusnak tekintett országokat.

A rendkívül népszerű Skype első béta verziója 2003 augusztusában jelent meg, míg 2011-re átlagban 20 millió felhasználó használta egyidejűleg. [2] Az új technológiák megjelenése önmagukban is arra késztetik a kommunikáció törvényes ellenőrzésével foglalkozó szervezeteket, hogy figyeljék a trendeket, kövessék a sokak által használt technológiák fejlődését, és biztosítsák azok törvényes ellenőrzését. Legalább ugyan ilyen mértékű kényszerítő erőt jelent, hogy a fenti bekezdésekben vázolt felhasználói változások okán a hagyományosnak mondható kommunikációs formák és rendszerek (pl. telefónia) jelentősége a felhasználók – ezáltal a potenciális célszemélyi kör, így a törvényes ellenőrzést végző szolgálatok – számára csökken. [1] A Skype pedig szinte minden nemzetbiztonsági és bűnüldöző szerv prioritási listájának az élén áll.

Röviden érdemes áttekinteni, hogy mi is okozza a problémát ennek a rendszernek az ellenőrzése kapcsán. Az egyik maga a rendszer felépítése. (Ennek sematikus elrendezése az 1. ábrán látható.)



1. ábra. Skype topológiája
Forrás: http://crypto.stanford.edu/cs294s/projects/skype.html (letöltve: 2013.03.26.)

A működés leegyszerűsítve úgy történik, hogy a korábban már regisztrált felhasználó (a regisztrációhoz csupán egy érvényes email címre van szükség!) bejelentkezik felhasználói nevével a Skype központi szerverére, ahol a jelszava alapján megtörténik a hitelesítése. A hitelesített felhasználó lekérdezheti kontaktlistáját, felhasználó adatait, más felhasználókat kereshet stb. A tényleges kommunikáció közvetlen (a kommunikáló felek (Node) közvetlen összeköttetésben áll egymással), vagy közvetett (a kommunikáló felek Supernode-okon keresztül állnak összeköttetésben egymással) kapcsolaton keresztül zajlik, de nem folyik át egy központon. [3] [4] Éppen ezért már az egy felhasználóhoz tartozó kommunikáció elfogása

is – figyelembe véve a felhasználók mobil eszközökkel bárhonnan használhatják a szolgáltatást – rendkívül nehéz.

A másik problémát a felhasznált magas szintű titkosítás (RSA és AES-256) okozza. [5] Azaz, ha sikerül is „útközben" elfogni a kommunikációt, annak tényleges tartalmához csak a használt titkosítás visszafejtése után lehetséges hozzáférni. Az ehhez szükséges számítási kapacitás és időigény meglehetősen nagy, a tömeges méretű ellenőrzést ez meglehetősen megnehezíti, vagy inkább teljes mértékben kizárja.

További problémát okoz a korábban már említett regisztráció, amelyhez csupán egy érvényes email címre van szükség. Emiatt a törvényes ellenőrzés feladatrendszerébe beleértett – és hagyományos hírközlési szolgáltatók esetében hatékonyan alkalmazható – felhasználói/előfizetői adatok szolgáltatása [1] ebben az esetben nehézkesen és főleg hiányosan valósul meg.

A fentiek okán célszerű tehát – természetesen a publikusan elérhető információk korlátozott volta miatt – a teljesség igénye nélkül megvizsgálni, hogy melyik ország, hogyan ellenőrzi (vagy hogyan próbálja ellenőrizni) a Skype rendszert. Bár a példák elsősorban azt szolgálják, hogy az ellenőrzésre szolgáló elveket, technológiákat, valamint a használatuk kapcsán felmerült jogi, technikai problémákat áttekinthessük, emellett arra is megfelelnek, hogy analógiaként felhasználhatók legyenek majd más PC/SaaS felhő alapú rendszerek ellenőrzési kérdéseinek vizsgálatakor.

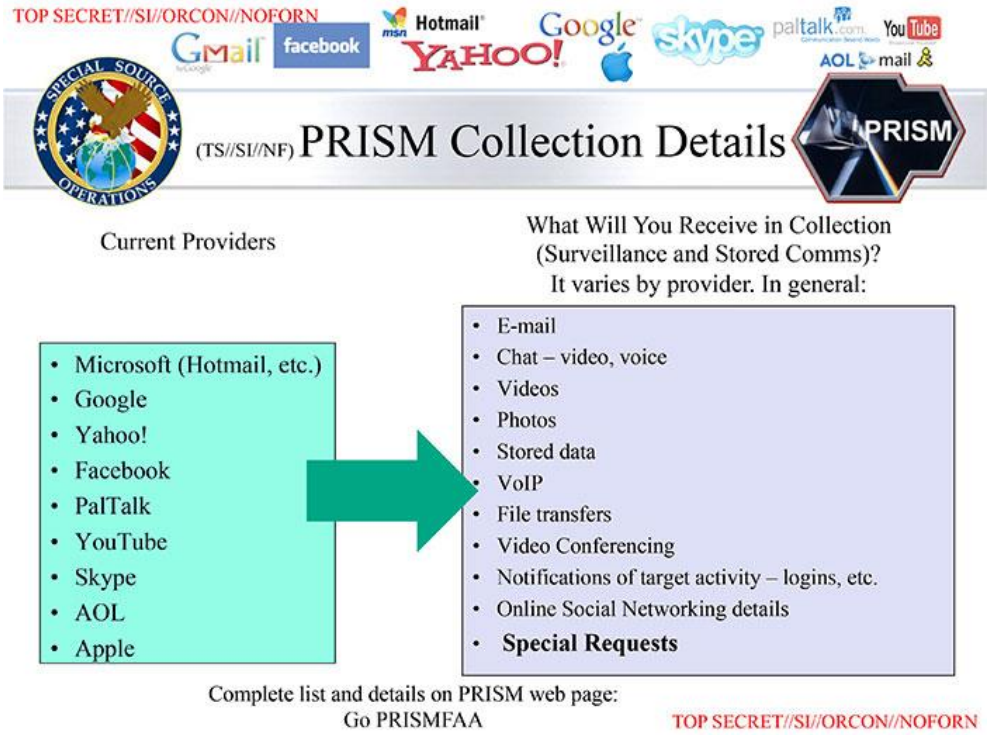
USA és a Skype:

A nyíltan elérhető források alapján arra lehet következtetni, hogy az USA a „Skype-probléma" megoldására a szolgáltatóval való együttműködést választotta. 2011 májusában már tényként könyvelték el, hogy a nagyhírű redmondi cég 8,5 Mrd USD-ért felvásárolta a Skype-ot.[6] Az ügyletet az Európai Unió versenyjogi végrehajtó szerve, az Európai Bizottság még az év októberében jóváhagyta, így elhárult minden akadály a fúzió elől. A felvásárlás már csak azért is „érdekes" volt, mert a Skype üzleti szempontból nem volt éppen sikertörténet. 2010-ben 7 millió dolláros nettó veszteséget könyvelhettek el amellett, hogy ugyanebben az évben december 31-én a társaság hosszú távú adósságállománya 686 millió dollár volt. [7]

A szaksajtóban már a felvásárlás bejelentésekor elindultak a találgatások, hogy miért is kell, kellhet a Skype a Microsoftnak. [8] [9] Az ott felvetetteken kívül nem kell túl nagy fantázia ahhoz, hogy az addig a titkosítás és a peer-to-peer struktúra miatt nagy nehézségekbe ütköző törvényes ellenőrzést is felírjuk a listára, alighanem az első helyre. Ennek megvalósítása az USA nemzetbiztonsági és bűnüldöző szervei számára ugyanis sokkal egyszerűbben kivitelezhető, ha egy egyesült államokbeli cég a tulajdonos, aki együttműködik az említett hatóságokkal, szervezetekkel. Ezt a feltételezést erősítik azok az információk is, hogy a felvásárlást követően a Microsoft megkezdte a Skype infrastruktúrájának átalakítását és egy központosítottabb hálózatot kezdett kiépíteni. A változás az addig rotációban a felhasználók között kiosztott un. Supernode-oknál indult el. Egyrészt számukat jelentősen csökkentették (több mint 48 ezerről kb. 10 ezerre), másrészt az új Supernode-ok már nem lehetnek felhasználók gépei, hanem csak és kizárólag a Microsoft/Skype központjába telepített eszközök. [10] Mára már az is bizonyított, hogy a Microsoft minden írott üzenethez hozzáfér, a továbbított üzenetekben pedig szűrést is végez. Ez a képesség pedig lehetőséget teremt arra is, hogy az üzenetek tartalmát hozzáférhetővé tegye a titkos információgyűjtésre feljogosított szervek számára. [11] [12] [13]

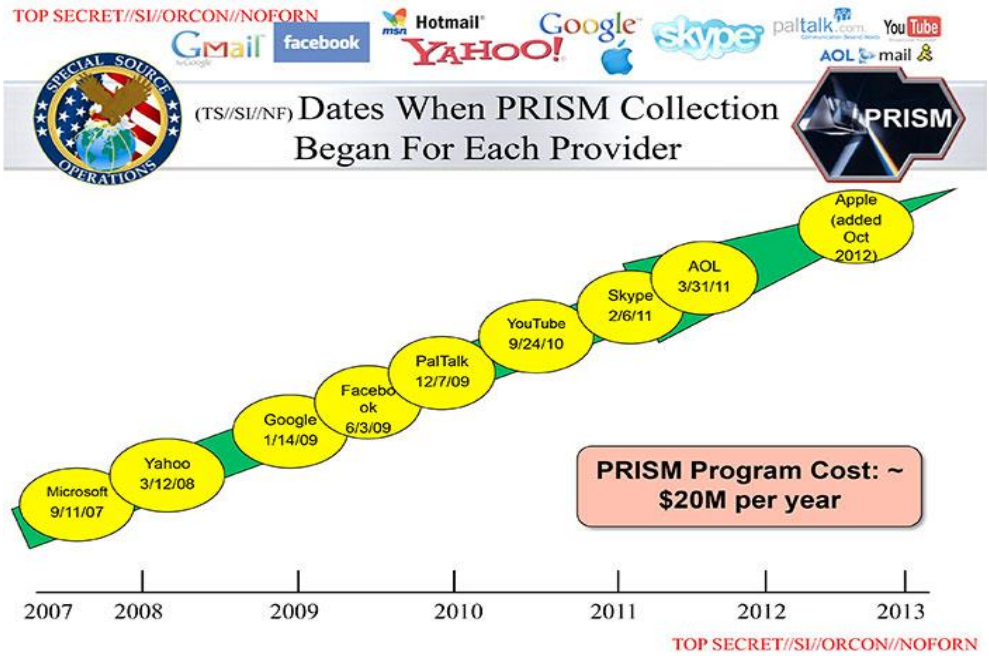
A Prism programról közzétett adatokból az is nyilvánosságra került, hogy a kilenc vezető internetes alkalmazás szolgáltató (Microsoft, Yahoo, Google, Facebook, PalTalk, AOL, Skype, YouTube, Apple) rendszerein tárolt és azokon átfolyó adatokhoz (pl. beszélgetések, video-chat, fényképek stb.) (2. ábra) – szolgáltatónként változó formában és mélységben – fér

hozzá az NSA (National Security Agency – Nemzetbiztonsági Ügynökség), az FBI (Federal Bureau of Investigation – Szövetségi Nyomozó Iroda) és az NSA-n keresztül az angol GCHQ (UK Government Communications Headquarters – Kormányzati Kommunikációs Központ). [14] A Skype-ot a kiszivárgott információk szerint 2011. 02. 06-án kapcsolták be a programba. (3. ábra.)



2. ábra. A Prism programban szereplő szolgáltatók és az általuk – különböző mértékben – biztosított adatok

Forrás: http://www.washingtonpost.com/wp-srv/special/politics/prism-collection-documents/ (letöltve: 2013.07.02.)



3. ábra. A Prism programban résztvevő szolgáltatók és csatlakozásuk időpontja

Forrás: http://www.washingtonpost.com/wp-srv/special/politics/prism-collection-documents/ (letöltve: 2013.07.02.)

Oroszország és a Skype:
Oroszország is a szolgáltatókkal történő együttműködést választotta, csak annak egy másik változatát. Az FSZB 2011-ben vetette fel, hogy be kellene tiltani a Skype, a Gmail és a Hotmail működését Oroszországban, mert azok ismeretlen algoritmusokat használnak a titkosításra, így ellenőrizhetetlen azok tartalma. Ez pedig biztonsági kockázatot jelent. [15] A Microsoft a felvásárlást követően bejelentette, hogy – a korábban más szoftvereinél alkalmazott gyakorlatának megfelelően – kész átadni a Skype forráskódját és titkosítási algoritmusát az orosz szolgálatnak, ezáltal elkerülheti annak betiltását. [16] [17] A lehallgatás, sőt a felhasználók pontos tartózkodási helyének meghatározási képességét orosz lapértesülésre hivatkozva a szaksajtó ma már tényként kezeli. [18]

Kína és a Skype:
A szolgáltatók Kínában is együttműködnek a törvényes ellenőrzést végző hatóságokkal. Az ázsiai országban a Skype egy speciális változatát használják, amelyet a – többségi tulajdonos – TOM Online (egy kínai Internet szolgáltató cég) és a Microsoft által alapított vegyesvállalat adott ki TOM-Skype néven. A szoftver feltörése után bizonyítottá vált, hogy kínai hatóságok ezen keresztül ellenőrzik a kommunikációt, az azonnali üzenetküldések esetében több ezer szavas szótár alapú kulcsszavas keresést használnak, és találat esetén rögzítik a teljes chatelést, vagy adott esetben blokkolják a forgalmat. [19]

Franciaország és a Skype:
Franciaország törvényi alapon kíván együttműködést elérni törvényes ellenőrzés tekintetében a Skype szolgáltatójával, mégpedig úgy, hogy hagyományos hírközlési szolgáltatónak kívánja minősíteni azt. Ennek megállapítása érdekében a francia hírközlési hatóság, az ARCEP beadvánnyal fordult az ügyészséghez. Amennyiben ez sikerül, akkor ugyanazok a kötelezettségek vonatkoznak a Skype szolgáltatójára is, mint a hagyományos hírközlési szolgáltatókra, azaz lehetőséget kell teremtenie a hálózatán keresztül a segélyhívó rendszerek elérésére, adót kell fizetnie a francia államnak, és – nem utolsó sorban – az arra feljogosított szervek számára biztosítania kell a törvényes ellenőrzést is. [20] [21]

Más példák:
Természetesen nem csak a Skype az, amit a hatóságok ellenőrizni kívánnak, és természetesen a fent említett módszerekkel nem csak a Skype, hanem más alkalmazásszolgáltatók rendszerein küldött és tárolt információk is ellenőrizhetők. A következő példákban is többnyire megjelenik a Skype ellenőrzése, de e mellett a más rendszerekből származó információk megszerzése a korábbiaknál sokkal hangsúlyosabban jelenik meg, így ezeket célszerű külön csoportban vizsgálni. Már csak azért is érdemes így tenni, mert a következő példák jól mutatatják, hogy egyrészt a szolgáltatóval való együttműködésen (vagy együttműködésre történő kényszerítésen) túl is vannak lehetőségek a titkos információgyűjtésre feljogosított szervezetek kezében, másrészt egy ország több ellenőrző módszert is használ (használhat).

Németország és az online házkutatás:
Németországból szivárgott ki a legtöbb információ a törvényes ellenőrzések során használt – és sok más névvel is illetett pl. kémprogramok, trójai programok – online házkutatásról. A módszer törvénybe iktatása, ezáltal a használat kereteinek kialakítása már régóta szerepelt a német parlament napirendjén. [22] Többszöri elutasítást [23] [24] követően a szövetségi alkotmánybíróság végül úgy foglalt állást, hogy a módszer használható, de szigorú keretek között (kizárólag kommunikáció ellenőrzésére – azaz gyakorlatilag az internetes telefon (pl. Skype) lehallgatására). Egy német hackercsoport a Chaos Computer Club (CCC) azonban

analizálta a német hatóságok által használt, a szintén német DigiTask által gyártott „maleware”-t, és megállapította, hogy annak képességei messze túlmutatnak a fent említett, szövetségi bíróság által megszabott kereteken. [25] [26]

Ezt követően a német hatóságok egy saját eszköz kifejlesztése mellet döntöttek, amelyet a BKA (Bundeskriminalamt – Szövetségi Bűnügyi Hivatal) berkein belül felállítandó un. Információtechnikai Ellenőrzési Kompetenciaközpontban (Kompetenzzentrum für informationstechnische Überwachung CC ITÜ) kívánnak legkésőbb 2014-ig létrehozni. Mindeközben azonban, annak elkészültéig a korábban már említett és kompromittálódott DigiTask szoftvere helyett egy kereskedelmi forgalomban kapható eszközt, az – egyébként szintén német – Eleman/Gamma Group termékét, az un. „FinFisher/FinSpy IT intrusion software kit”-et használják. [27] [28]

A kémprogramok használata nem csak Németországra jellemző, hanem – mint bizonyos körülmények között rendkívül hatékony, vagy sokszor egyetlen alkalmazható eszközt – más országok titkos információgyűjtésre feljogosított szervei is használják, vagy legalábbis használni tervezik. Ilyen témájú hírek érkeztek Svájc [29], Franciaország [30], Ausztria [31], Hollandia [32] és természetesen az USA [33] [34] és az Egyesült Királyság [35] vonatkozásában is.

Az online házkutatásra alkalmas eszközök, azaz kémprogramok természetesen jóval több információt tudnak biztosítani a célszemélyek számítógépéről (pl. tárolt fájlok), a számítógép technikai eszközein keresztül a célszemély tevékenységéről (pl. webkamera képek), mint amit pusztán az elektronikus úton folytatott kommunikációt biztosító szolgáltató – a törvényi feltételek megléte és maximális segítőkész hozzáállás mellett – képes. Az ilyen jellegű kémprogramokat azonban időről időre felderítik és alaposan analizálják az erre szakosodott biztonsági szakemberek vagy hackerek, majd – a törvényes ellenőrzést végző szervezeteknek nem kis anyagi és erkölcsi veszteséget okozva – eredményeiket sokszor publikálják is az Interneten. Erre a sorsra jutott az olasz Hacking Team nevű cég szintén kifejezetten rendvédelmi szerveknek árusított eszköze [36], és a fent említett német Eleman/Gamma Group terméke is. [37]

Érdekes, hogy míg a korábban leírtak szerint a törvényhozók is azon gondolkodnak, vitatkoznak, hogy használhatják-e az arra feljogosított szervek egyáltalán ez a technológiát törvényes ellenőrzésre, és ha igen akkor milyen keretek között, addig egészen meglepő elképzelések is napvilágot látnak. Ilyen az is, hogy a Commission on the Theft of American Intellectual Property nevű Egyesült Államokbeli szórakoztatóipari szervezet is hasonló programokat telepítene a zenei albumok, a filmek és a PC-s játékok adathordozóira, hogy az elkövetett jogsértéseket felderítse. [38]

Egyesült Királyság (UK) és a DPI:

Egy másik módszer a törvényes ellenőrzést végzők kezében az un. mély csomagelemzés (Deep Packet Inspection (DPI) módszere. Ennek lényege, hogy adott helyen átfolyó adatforgalom minden csomagjának a tartalmát vizsgálat alá veszik. Ezt a technológiát használják fel például a behatolás-érzékelő és –védelmi rendszerek (Intrusion Detection/Prevention Systems (IDS/IPS)) [39], [40], de Internetszolgáltatók is előszeretettel alkalmazzák bizonyos – általuk károsnak vélt vagy tartott tartalmak, forgalmak (pl. VoIP, peer-to-peer) – blokkolására. [41] Ugyanakkor ez a technológia lehetőséget teremt a törvényes ellenőrzést végző szolgálatok számára, hogy információhoz jussanak. [40] [42] Ez a hozzáférés azonban meglehetősen korlátozott, hiszen bár a nyíltan küldött adatok könnyen ellenőrizhetők, feldolgozhatók, a titkosított forgalmak esetében a titkosítást fel kell törni, ami időben hosszadalmas, nagy számítástechnikai eszközparkot igénybe vevő folyamat. Ráadásul a nyílt forgalmaknál is jelentősen megnehezíthető az ellenőrzés egy megfelelő – és

ingyenesen rendelkezésre álló – titkosító szoftver eszközök használatával (pl. HTTPS Everywhere). [40]

E korlát ellenére az angol GCHQ ezt a módszert használja „TEMPORA” nevű, a „PRISM”-hez hasonlóan nagyszabású, ám technikailag más alapokon nyugvó ellenőrző programjához. Itt – a kiszivárgott adatok szerint – 200 darab, egyenként 10 Gb/s adatátviteli sebességű optikai kábelen (ezek közül egy időben legalább 46-on) átfolyó összes információt kicsatolják és feldolgozzák a 2007 elején elindított „Mastering the Internet” projekt keretében. A programban öt ország (USA, UK, Kanada, Új Zéland és Ausztrália) titkosszolgálati szervei dolgoznak együtt és osztják meg egymás között az információkat – a kinyert tartalmat és a kísérő un. metaadatokat egyaránt. [43] [44] (Az NSA hasonló, „Upstream” fedőnevű tevékenységét a 4. ábra szemlélteti, amelyből jól látszik, hogy a Prism csak egy része az USA lehallgató rendszerének.)

4. ábra. Az Upstream program jól szemlélteti, hogy a Prism csak egy része az USA lehallgató rendszerének

Forrás: http://www.washingtonpost.com/wp-srv/special/politics/prism-collection-documents/ (letöltve: 2013.07.11.)

Németország és a felhő alapú rendszerek titkosításainak törése:

Németországban az online házkutatás (vagy inkább a kémprogramok) használata mellett felmerült a felhő alapú rendszerek másfajta ellenőrzésének kialakítása is. Erre azért van szükség, mert az említett módszernek – mint minden másiknak – megvannak a korlátai. Azokhoz az információkhoz, amelyekhez nem lehet a kémprogramok segítségével hozzáférni, azokat egy másik módszer alkalmazásával lehet megszerezni. Ennek érdekében a BKA és a BfV (Bundesamt für Verfassungsschutz – Alkotmányvédelmi Hivatal) által működtetett SFZ TK (Strategie- und Forschungszentrum Telekommunikation – Távközlési Stratégiai és Kutatóközpont) nevű intézet azt a feladatot kapta az illetékes szervektől, hogy vizsgálja meg a felhő alapú rendszereknél használt titkosításokat, valamint azt, hogy azok megfejtésén keresztül hogyan lehet hozzáférni a felhasználói adatokhoz, fájlokhoz. [45]

Törvényi szabályozások:

Mint, ahogy a Skype példáján keresztül is látszik, az ellenőrzés egyik leghatékonyabb formája a szolgáltatóval való együttműködés, amelyet törvényi előírásokkal garantálni lehet. Ebbe az irányba több ország is tett lépéseket. Németországban a törvényes ellenőrzés kialakíthatósága és hatékony alkalmazhatósága érdekében a telekommunikáció fogalmát kívánják kiszélesíteni minden online adatcserére (beleértve az ezekhez tartozó felhasználói adatokat is), és ezekre a hagyományos hírközléssel analóg rendelkezéseket alkotni az erről szóló jogszabályban. [46] Hasonló jogszabályváltozásokat akar az USA is bevezetni, amelyekkel kötelezheti az olyan szolgáltatókat, mint a Google vagy a Facebook, hogy tegyék lehetővé a rajtuk keresztül folytatott online kommunikáció törvényes ellenőrzését, [47] ráadásul a törvényi szabályozás azt is garantálja, hogy minden szolgáltató bekényszeríthető a rendszerbe. Ugyanakkor az USA-ban a már létező jogszabályok (Protect America Act (2007), FISA (Foreign Intelligence Surveillance Act) Amendments Act (2008) is kötelezettségeket rónak a magáncégekre a törvényes ellenőrzés tekintetében. [14]

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.

Jelen cikkből levonható következtetések:

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 felhozott külföldi példákból jól látszik, hogy – a technikai, jogi korlátok és a hatékony ellenőrzés okán – általában több módszert használnak a törvényes ellenőrzésre feljogosított szervezetek.

A nemzetközi példák bár széles, de nem teljes körű áttekintést adtak. Ennek egyrészt az az oka, hogy csak publikus információkra lehet támaszkodni, azok pedig – a problémakör jellegére tekintettel meglehetősen korlátozottak, ráadásul szinte sohasem igazoltak, így nem lehetnek teljes körűek. Másrészt pedig az, hogy a törvényes ellenőrzésre felhatalmazott szervek részére rendelkezésre álló módszerek ismertetéséhez, elemzéséhez egyébként sincs szükség teljes körű áttekintésre.

A nemzetközi tapasztalatok vizsgálata elsősorban tehát a technikai lehetőségek áttekintésére és bizonyos problémák felvetésére szolgált. Ezen tapasztalatok megismerését követően lehet – a „Felhő alapú rendszerek törvényes ellenőrzési problémái” című cikkben javasolt, az említett rendszerek hatékony ellenőrzésének kialakítása felé tett következő lépésként – elvégezni a törvényes ellenőrzésre jelenleg rendelkezésre álló technikai eszközök és módszerek leírását, összehasonlítását, azok előnyeinek, hátrányainak meghatározásával együtt. A fent említett módszereket még ki kell egészíteni az un. közbeékelődéses támadással (Man-in-the-Middle), amire ugyan a fentiekben nincs példa, de ez is fontos eleme a törvényes ellenőrzést végző szervezetek módszertárának. Ezekkel foglalkozik a cikksorozat második része.

Felhasznált irodalom

[1] Kovács Zoltán: FELHŐ ALAPÚ RENDSZEREK TÖRVÉNYES ELLENŐRZÉSI PROBLÉMÁI Hadmérnök, VIII. Évfolyam 1. szám - 2013. március

[2] Molnár Gábor, Zalatnay Zsolt: Szolgáltatások és architektúrák Skype előadás www.tmit.bme.hu/dl239 (2013. 02. 13.)

[3] Sándor Molnár, Marcell Perényi: On the identification and analysis of Skype traffic INTERNATIONAL JOURNAL OF COMMUNICATION SYSTEMS 21 April 2010 in Wiley Online Library http://hsnlab.tmit.bme.hu/~molnar/files/ijcs2010.pdf (2013.06.18.)

[4] Salman A. Baset and Henning Schulzrinne: An Analysis of the Skype Peer-to-Peer Internet Telephony Protocol (2004. 09. 15.) http://www1.cs.columbia.edu/~library/TR-repository/reports/reports-2004/cucs-039-04.pdf (2013.06.18.)

[5] Does Skype use encryption? https://support.skype.com/en/faq/FA31/does-skype-use-encryption (2013. 07. 11.)

[6] Kara Swisher: Done Deal: Microsoft to Buy Skype for $8.5 Billion in Cash (2011. 05.10.) http://allthingsd.com/20110510/done-deal-microsoft-to-buy-skype-for-8-5-billion-in-cash/ (2013.06.17.)

[7] Az EU jóváhagyta a Microsoft Skype-felvásárlását (2011. 10. 07.) http://www.origo.hu/techbazis/20111007-az-europai-bizottsag-jovahagyta-a-microsoft-skypefelvasarlasat.html (2013.06.17.)

[8] Bodnár Ádám: A Microsoft megvette a Skype-ot (2011. 05. 10.) http://www.hwsw.hu/hirek/46667/microsoft-skype-voip-telefon-felvasarlas.html (2013.06.17.)

[9] Miért jó a Skype a Microsoftnak? http://insiderblog.hu/kulfold/2011/05/12/skype/ - (2013.06.17.)

[10] Skype does away with random supernodes (2012. 05. 01.) http://expertmiami.blogspot.hu/2012/05/skype-does-away-with-random-supernodes.html (2013.06.18.)

[11] Skype with care – Microsoft is reading everything you write (2013. 05. 14.) http://www.h-online.com/security/news/item/Skype-with-care-Microsoft-is-reading-everything-you-write-1862870.html (2013.06.18.)

[12] Jürgen Schmidt: Skype's ominous link checking: Facts and speculation (2013. 05. 17.) http://www.h-online.com/security/features/Skype-s-ominous-link-checking-Facts-and-speculation-1865629.html (2013.06.18.)

[13] Kirils Solovjovs: On Skype URL eavesdropping (3013. 05. 17.) http://seclists.org/fulldisclosure/2013/May/78 (2013.06.18.)

[14] Barton Gellman and Laura Poitras: U.S., British intelligence mining data from nine U.S. Internet companies in broad secret program (2013. 06. 07.) http://www.washingtonpost.com/investigations/us-intelligence-mining-data-from-nine-us-internet-companies-in-broad-secret-program/2013/06/06/3a0c0da8-cebf-11e2-8845-d970ccb04497_story.html (2013.06.28.)

[15] Betilthatják Oroszországban a Skype-ot, a Gmailt és a Hotmailt (2011. 04. 09.) http://www.sg.hu/cikkek/81250/betilthatjak_oroszorszagban_a_skype_ot_a_gmailt_es_a_hotmailt (2013.06.18.)

[16] Yuliya Fedorinova: Microsoft May Offer Skype Codes to Russia's FSB, Vedomosti Says (2011. 06. 09.) http://www.bloomberg.com/news/2011-06-09/microsoft-may-offer-skype-codes-to-russia-s-fsb-vedomosti-says.html?cmpid=yhoo (2013.06.18.)

[17] Lehallgathatják az oroszok a Skype-ot (2011. 06. 11.) http://www.sg.hu/cikkek/82579/lehallgathatjak_az_oroszok_a_skype_ot (2013.06.18.)

[18] Évek óta lehallgatható Oroszországban a Skype (2013. 03. 18.) http://www.sg.hu/cikkek/96074/evek_ota_lehallgathato_oroszorszagban_a_skype - (2013.06.18.)

[19] Vernon Silver: Cracking China's Skype Surveillance Software (2013. 03. 08.) http://www.businessweek.com/articles/2013-03-08/skypes-been-hijacked-in-china-and-microsoft-is-o-dot-k-dot-with-it (2013.06.20.)

[20] Koi Tamás: Egyre nagyobb a nyomás Európában a Skype-on (2013. 03. 13.) http://www.hwsw.hu/hirek/49958/skype-microsoft-franciaorszag-arcep-voip.html - (2013.06.20.)

[21] SKYPE REFUSES TO REGISTER AS AN OPERATOR (2013. 03. 12.) http://arcep.fr/index.php?id=8571&tx_gsactualite_pi1%5Buid%5D=1593&tx_gsactualite_pi1%5Bannee%5D=&tx_gsactualite_pi1%5Btheme%5D=&tx_gsactualite_pi1%5Bmotscle%5D=&tx_gsactualite_pi1%5BbackID%5D=26&cHash=baebcd8ef257d3194065360ecec41a90&L=1 (2013.06.20.)

[22] Mindenki lehallgatható lenne Németországban (2008. 01. 17.) http://www.sg.hu/cikkek/57484/mindenki_lehallgathato_lenne_nemetorszagban - (2013.06.24.)

[23] Dajkó Pál: A német rendőröknek egyelőre tilos a hackelés (2007. 02. 06.) http://itcafe.hu/hir/a_nemet_rendoroknek_egyelore_tilos_a_hackeles.html - (2013.06.24.)

[24] Dajkó Pál: Új alkotmányos jog született: az IT-jog (2008. 03. 01.) http://itcafe.hu/hir/bundestrojaner_alkotmany_itjog.html (2013.06.24.)

[25] Dajkó Pál: Lebukott az állami kémprogram (2011. 10. 10.) http://itcafe.hu/hir/chaos_computer_club_nemetorszag_bundestrojaner.html - (2013.06.24.)

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

[27] Andre Meister: Secret Government Document Reveals: German Federal Police Plans To Use Gamma FinFisher Spyware (2013. 01. 16.) https://netzpolitik.org/2013/secret-government-document-reveals-german-federal-police-plans-to-use-gamma-finfisher-spyware/ (2013.06.28.)

[28] https://netzpolitik.org/wp-upload/BMI-Bericht-Sachstand-CC-TK%C3%9C.pdf (2013.06.28.)

[29] Superintendent Trojan (2006. 10. 09.) http://www.h-online.com/security/news/item/Superintendent-Trojan-731613.html (2013.06.28.)

[30] Cyberperquisitions (2008. 02. 28.) http://www.lemonde.fr/idees/article/2008/02/28/cyberperquisitions_1016773_3232.html (2013.06.28.)

[31] Ausztriában törvényes lesz az online házkutatás (2007. 10. 18.) http://www.sg.hu/cikkek/55658/ausztriaban_torvenyes_lesz_az_online_hazkutatas - (2013.06.28.)

[32] Külföldi szervereket is megtámadhat a holland rendőrség (2013. 05. 06.) http://www.sg.hu/cikkek/97134/kulfoldi_szervereket_is_megtamadhat_a_holland_rendorseg (2013.06.28.)

[33] Declan McCullagh: FBI remotely installs spyware to trace bomb threat (2007. 06. 18.) http://news.cnet.com/8301-10784_3-9746451-7.html (2013.06.28.)

[34] http://www.politechbot.com/docs/fbi.cipav.sanders.affidavit.071607.pdf (2013.06.28.)

[35] Duncan Gardham: Government plans to extend powers to spy on personal computers (2009. 01. 04.) http://www.telegraph.co.uk/news/uknews/law-and-order/4109031/Government-plans-to-extend-powers-to-spy-on-personal-computers.html (2013.06.28.)

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

[37] 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.)

[38] The IP commission report (2013. május) http://ipcommission.org/report/IP_Commission_Report_052213.pdf (2013.06.28.)

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

[40] 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.)

[41] 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.)

[42] 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.)

[43] 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.)

[44] Ewen MacAskill, Julian Borger, Nick Hopkins, Nick Davies and James Ball: Mastering the internet: how GCHQ set out to spy on the world wide web (2013. 06. 21.) http://www.guardian.co.uk/uk/2013/jun/21/gchq-mastering-the-internet (2013.07.05.)

[45] Németország a felhőadatokat is ellenőrizné (2013. 04. 07.) http://www.sg.hu/cikkek/96458/nemetorszag_a_felhoadatokat_is_ellenorizne (2013.06.28.)

[46] Szigorítanák a német távközlési törvényt (2013. 04. 21.) http://www.sg.hu/cikkek/96798/szigoritanak_a_nemet_tavkozlesi_torvenyt (2013.06.28.)

[47] Ellen Nakashima: Panel seeks to fine tech companies for noncompliance with wiretap orders (2013. 04. 29.) http://www.washingtonpost.com/world/national-security/proposal-seeks-to-fine-tech-companies-for-noncompliance-with-wiretap-orders/2013/04/28/29e7d9d8-a83c-11e2-b029-8fb7e977ef71_story.html (2013.06.28.)

Ábrák jegyzéke