HADMÉRNÖK

XII. Évfolyam „KÖFOP” szám – 2017. október

A FELHASZNÁLÓK DIGITÁLIS LÁBNYOMÁNAK, ANONIMITÁSÁNAK VIZSGÁLATA TECHNIKAI SZEMPONTBÓL I. RÉSZ - SZEMÉLYI SZÁMÍTÓGÉPEK

DEMONSTRATING USER ANONYMITY AND DIGITAL FOOTPRINT WITH TECHNICAL TOOLS PART I. PERSONAL COMPUTERS

SZABÓ ANDRÁS

szabo.andras@uni-nke.hu

Absztrakt

Jelen cikksorozat a felhasználói kiberhigéniás szokások és gyakorlatok bemutatásával foglalkozik. A felhasználókra leselkedő fenyegetések bemutatása mellett javaslatokat tesz azok csökkentésére, a védelem fokozására. Mindennap használjuk, mégis ritkán vizsgáljuk meg, hogyan is működnek számítógépeink és okos eszközeink. Jelen cikksorozat a biztonságos számítógép használatra hívja fel a figyelmet, illetve a felhasználók személyes adatainak védelme érdekében az anonim internetezés lehetőségeit mutatja be. Napjainkban a felhasználók internetelérésre kétféle eszközt használnak: a klasszikus személyi számítógépeket, és a mobil eszközöket. Ez a két eszközcsoport eltérő megközelítést igényel, így a cikksorozat első része a „klasszikus” személyi számítógépekkel foglalkozik, majd a második rész pedig a mobil eszközökre fókuszál. A mű a KÖFOP-2.1.2-VEKOP-15-2016-00001 azonosítószámú, „A jó kormányzást megalapozó közszolgálat-fejlesztés” elnevezésű kiemelt projekt keretében működtetett Ludovika Kiemelt Kutatóműhely keretében, a Nemzeti Közszolgálati Egyetem felkérésére készült.

Kulcsszavak: *biztonságtudatosság, Informatikai biztonság, digitális lábnyom, anonimitás*

Abstract

This article deals with the Internet user's habits and practices. In addition to presenting threats to the users, I made some suggestion to reduce them and increase the security awareness of the reader. We use our computers and smart devices day by day, but we rarely look at how they really work. This article focuses on to use of computers securely, and also how to access the Internet anonymously to protect personal information. Recommendations include practical advice and technical examples. Nowadays users are accessing the Internet using two main types of devices: computers (desktop and portable), and mobile devices (smartphones, tablets, and wearable devices). These two sets of devices require different approaches, so the first article in this series deal with "classical" personal computers, and the second focuses on the mobile devices. The work was created in commission of the National University of Public Service under the priority project KÖFOP-2.1.2-VEKOP-15-2016-00001 titled „Public Service Development Establishing Good Governance” in the Ludovika Workshop.

Keywords: *security awareness, IT security, digital footprint,* anonymity

A kézirat benyújtásának dátuma (Date of the submission): 2017.10.02.
A kézirat elfogadásának dátuma (Date of the acceptance): 2017.11.02.

BEVEZETÉS

Jelen cikksorozat a felhasználói kiberhigéniás szokások és gyakorlatok bemutatásával foglalkozik. A felhasználói fenyegetések bemutatása mellett javaslatokat tesz azok csökkentésére, és a védelem fokozására. Ez napjainkban mindenki számára fontos, a közszolgálatban dolgozók pedig kiemelten érintettek lehetnek magánemberként, és a szervezetük IT felhasználójaként is.

Érdekes megfigyelni, hogy a fizikai biztonságukra még mindig jobban ügyelnek az emberek, mint az informatikai biztonságra. Azonban a bűnözési statisztikák alapján[1] a kibertérben már nagyobb valószínűséggel leszünk áldozata egy bűncselekménynek, mint a fizikai valóságban. Ez alapján pedig mindenképpen fokoznunk kell a védelmünket, mint ahogy arra több tanulmány is felhívta a figyelmet [1] [2].

Az Egyesült Államokban a közszolgálatban dolgozókat külföldi kiküldetés előtt felkészítik a fogadó országban várható fenyegetésekre [3] [4]. Ilyen jellegű felkészítést napjainkban a kibertér használatával kapcsolatban is tartani kellene, hiszen az ott található fenyegetések nem ismerik az országhatárokat, így bármelyik felhasználót fenyegethetik. Jelen munkámmal egy ilyen jellegű anyagot kívántam összeállítani, mely praktikus tanácsokkal készíti fel az olvasókat a biztonságos internetezésre, és az „okos" eszközeik tudatos használatára.

Napjainkban a felhasználók internetelérésre kétféle eszközt használnak: a klasszikus személyi számítógépeket (asztali és hordozható kivitelűeket), és a mobil eszközöket (okostelefonokat, tableteket és a viselhető okos eszközöket). Ez a két eszközcsoport eltérő megközelítést igényel, így a cikksorozat első részében a „klasszikus" személyi számítógépekkel, majd a második részben a mobil eszközökkel foglalkozom.

DIGITÁLIS LÁBNYOM: BARÁT VAGY ELLENSÉG?

Az informatika körülvesz minket, az IT eszközök használata már a mindennapok részét képezik, függetlenül, hogy fiatalok vagyunk vagy idősek, tanulunk, dolgozunk, közlekedünk, épp nyaralunk, esetleg hivatalos ügyeinket intézzük. Ezeken keresztül informálódunk a világ eseményeiről, vásárlunk, tartjuk a kapcsolatot ismerőseinkkel, keresünk párt magunknak. Ha ennyi mindenre használjuk, felmerül a kérdés, hogy mennyire biztonságos, illetve esetenként, hogy mennyire anonim a szolgáltatások igénybevétele.

A mindennapi életünk során nyomot hagyunk közösségünkben, és környezetünkben, ezt lehet mérni, például, hogy milyen aktív társasági életet élünk (~mekkora az ismerősi körünk, és milyen aktívan kommunikálunk velük), mennyi szemetet termel háztartásunk, mennyi energiát és vizet fogyasztunk nap, mint nap (~mekkora az ökológiai lábnyomunk). Ezek mellett a kézzelfogható „nyomok" mellett, a mindennapi életünknek is van digitális vetülete, melyet digitális lábnyomnak (digital footprint-nek [5]) hívunk. Az, hogy a digitális lábnyomunk mekkora, az nagyrészt tőlünk függ. A meggondolatlan internetezés következtében azonban ez általunk kontrollálhatatlan méreteket ölthet.

[1] Pl.: Az Egyesült Királyságban 2015-ben már meghaladta a kiberbűnözés a valós világban elkövetett bűncselekményeket Forrás: https://www.scmagazineuk.com/cyber-crime-overtakes-physical-crime-in-the-uk/article/535247/

Azt is fontos megjegyezni, hogy az anonimitás nem mindenkinek célja és érdeke (pl.: hírességek és gondolatvezérek számára fontos a markáns digitális jelenlét), azonban a mások által megismerhető lábnyomunk alakítása mindannyiunk érdekében áll[2].

Még ha kerüljük is az online perszónánk használatát, akkor is visszaérhetnek vele (mint, ahogy az a NATO Szövetséges Erők európai főparancsnokának nevében létrehozott hamis facebook fiókkal tették 2012-ben [6]).

MAGÁNSZFÉRA VÉDELME, ANONIMITÁS ÉS ONLINE BIZTONSÁG

A magánszféra védelme alatt azt értjük, hogy a személyes adatainkat csak az általunk jóváhagyott félnek adjuk át, annak is csak a feltétlenül szükséges adatokat, és ő csak a szükséges mértékig tárolja (azokat harmadik félnek nem adja át).

Anonimitás alatt azt értjük, hogy a felhasználók névtelenül képesek hozzáférni a világhálóhoz, és felhasználni az azon keresztül elérhető szolgáltatásokat. Számtalan oka lehet, hogy névtelenek szeretnénk maradni, például:

- a személyes adataink védelme miatt,
- böngészési szokásaink védelme érdekében,
- célzott spam-ek csökkentése céljából.

A személyes felhasználású IT rendszerek biztonságos használata esetén a felhasználók az eszközeiket, és a rajtuk keresztül elérhető hálózati szolgáltatásokat a megkívánt bizalmassággal, a kezelt információt sértetlenül, és a kívánt időben rendelkezésre állva tudják igénybe venni.

Az, hogy biztonság egy rendszer, nem feltétlenül jelenti, hogy anonim módon használható is egyben (sőt sok esetben ezek kizárja egymást, pl.: az webmail szolgáltatók a kétfaktoros azonosítás érdekében elkérik telefonszámunkat). Ugyancsak tévedés azt hinni, hogy ha titkosítást használunk, akkor névtelenek is maradunk. Erre példa, hogy ha egy webmail szolgáltatást[3] a titkosított https protokoll segítségével vesszük igénybe, akkor is ismert lesz külső megfigyelő (pl. a csatlakozásra használt hálózat tulajdonosa) számára, hogy ki, mikor, mely szolgáltatást vette igénybe. Ugyancsak megfigyelhető lesz a látogatási szokásunk (pl.: milyen gyakran nyitjuk meg, mennyi ideig maradunk a weblapon). A szolgáltató ezen felül pedig azt is be tudja azonosítani, hogy melyik felhasználója honnan jelentkezett be (sőt, ezt még össze is tudja kötni, hogy mely más felhasználókkal kommunikált, illetve ők honnan jelentkeztek be).

SZÁMÍTÓGÉP BIZTONSÁGA

Számtalan leírás (pl. [7] [8] [9] [10]) foglalkozik a személyes használatú számítógépek biztonságának fokozásával, ezért csak felsorolás jelleggel említem a feltétlenül szükséges védelmi intézkedéseket, melyek hozzásegítenek minket a biztonságos és anonim interneteléréshez. Hasznos tananyagot állított össze ebben a témában a Neumann János Számítógép-tudományi Társaság [11].

---

[2] (több híresség is kellemetlen helyzetbe került már a meggondolatlanul feltöltött tartalmak miatt Lásd:http://www.foxnews.com/entertainment/2016/12/20/biggest-celebrity-social-media-mistakes-2016.html , vagy a média által hirtelen híressé vált személyek múltjából előkerülő titkok miatt pl.:http://www.scenariomagazine.com/your-digital-footprint/)

[3] Lásd: https://gmail.com

BIOS, UEFI BIZTONSÁG

A számítógépünk boot sorrendje, és a hardver specifikus beállítások lezárása érdekében célszerű a BIOS[4]-t, vagy újabb számítógépek esetén az UEFI[5]-t jelszavazni, és ha nincs szükség rá, akkor megtiltani a külső eszközről való rendszerbetöltést (pl.: CD vagy USB-ről).

A BIOS / UEFI frissen tartása (un. update-elése) is lényeges, de azt célszerű hozzáértő szakemberrel bízni, mert hiba esetén a számítógépünk működésképtelenné válhat. A frissítések telepítésére nem csak a számítógépek, hanem az un. beágyazott rendszerek (pl.: routerek, vezetéknélküli hozzáférési pontok, okos TV-k, IP kamerák stb.) esetén is figyelni kell.

KIJELZŐ FÓLIÁK ÉS BETEKINTÉS ELLENI VÉDELEM

A kijelző védelme az érintőkijelzővel ellátott mobil IT eszközök korában kiemelten fontos. Jellemzően a sérülések elkerülése miatt használjuk ezeket, azonban más fenyegetésekre is érdemes készülni, hiszen az információvédelem is fontos szempont lehet. Nemcsak a tárolt és továbbított, hanem a megjelenített adatokat is védenünk kell. A betekintés elleni fóliákkal[6] a képernyőn megjelenő bizalmas információkat szűrhetjük az illetéktelen tekintetek elől. Így ha kávézóban, repülőtéri váróban, konferencián használjuk eszközünket, mások elől rejthetjük képernyőnk tartalmát. Ettől függetlenül a billentyűzeten bevitt információkat megfigyelhetik (pl.: kamerával). A laptopokba beépített mikrofonok és kamerák hardveres kikapcsolása a BIOS/UEFI-ből nem túl életszerű (viszont biztonságos lehet), hiszen a felhasználók többsége rendszeresen használja (pl.: videóhívások alkalmával), így célszerű azokat letakarni (ezt lehet egy egyszerű matricával, vagy vannak olyan megoldások, melyekkel szükség esetén használni is tudjuk a kamerát[7]).

INGYENES (?) ÉS ILLEGÁLIS SZOFTVEREK HASZNÁLATA

Az "ingyenes"-nek hirdetett szoftverek sokszor mégis kérnek valamit használatukért cserébe. Jobb esetben csak kéretlen reklámokkal bombáznak (pl.: mert regisztráltunk a letöltés érdekében), vagy a felhasználói szokásainkról gyűjtenek adatot. Így használatukért sokszor a személyes adatainkkal és anonimitásunkkal fizetünk [12].

A nem megbízható forrásból, illegálisan letöltött és használt szoftvereknek az a veszélye, hogy kártékony kódokat is tartalmazhatnak, melyek a hirdetett funkcionalitás biztosítása mellett (vagy helyett) információt gyűjthetnek, illetve egyéb módon kompromittálhatják rendszerünket (pl. távoli hozzáférést tesznek lehetővé). Sajnos napjainkban a megbízhatónak vélt gyártóktól is érkezhet kártékony kódot tartalmazó telepítő csomag vagy frissítés (2017 augusztusában pl. a hivatalos honlapon található CCleaner telepítő kódját ismeretlenek megváltoztatták, és kártékony tartalommal látták el[8]).

---

[4] Basic Input Output System, mely a számítógép hardvere és az operációs rendszer közti kommunikációt biztosítja

[5] Universal Extensible Firmware Interface, az újabb számítógépekbe már a BIOS-t leváltotta, több funkcióval rendelkezik, és biztonságosabb működést biztosít.

[6] További információ erről a technológiáról:http://www.3m.com/3M/en_US/privacy-screen-protectors-us/ és https://www.3m.com.au/3M/en_AU/privacy-screen-protectors-au/visualprivacy/news/full-story-page/?storyid=7221901b-b698-4f01-a234-6802f143684f és https://ftp.hp.com/pub/caps-softpaq/cmit/whitepapers/HPSureViewWhitepaper.pdf

[7] Pl.:https://twitter.com/itsthechampagne/status/727563423404412930

[8] Továábi részletek olvashatóak: https://www.piriform.com/news/blog/2017/9/18/security-notification-for-ccleaner-v5336162-and-ccleaner-cloud-v1073191-for-32-bit-windows-users

FÁJLRENDSZER TITKOSÍTÁS

A tárolt adatok védelme is fontos, hiszen ha mások is hozzáférnek a számítógépünkhöz (pl. amikor az irodánkban vagy a hotelszobában felügyelet nélkül hagyjuk a gépet), akkor az azon tárolt információk megszerzése mellett kártékony szoftvereket (pl.: billentyűzet leütés naplózót, vagy távoli hozzáférést biztosító alkalmazást) is telepíthetnek. A legtöbb operációs rendszer rendelkezik fájlrendszer szintű titkosítással (pl.:Windows rendszereknél a Bitlocker, Linux rendszereken pedig több, ingyenes lehetőségünk is van[9]). Vannak továbbá olyan felső kategóriás számítógépek, melyek BIOS/UEFI-je is képes titkosítani az adattároló eszközöket. A hordozható médiák (pl.: külső merevlemez és pendrive-ok) titkosítása is fontos lehet, vannak olyan gyártók, akik hardveres titkosítással látják el eszközeiket. A titkosítással nem rendelkező hordozható médiák szoftveres védelmét például a Veracrypt nevű alkalmazással tudjuk biztosítani.

Külföldi utazás[10] előtt célszerű elgondolkodni, hogy szükséges-e az adott számítógépet, és az azon tárolt adatot magunkkal vinni. Ha nélkülözhetetlennek ítéltük, akkor a felesleges adatok törlésével (biztonságos módszerekkel[11]), vagy titkosítás használatával a tárolt adatok biztonságát fokozhatjuk.

KÁRTÉKONY TARTALMAK ELLENI VÉDELEM

A kártékony tartalmak ellen célszerű valamilyen Antivirus szoftverrel védekezni, jellemzően ezek már komplex védelmet biztosítanak, és a fájlok ellenőrzése mellett figyelik a böngészőinket, és a levelező kliensünket is. Ennek következtében ezek a szoftverek is megoszthatják böngészési, levelezési szokásainkat. Meg kell még jegyezni, hogy ezek a szoftverek az ismert támadási módok ellen képesek hatékonyan védekezni, és az eddig nem azonosított sérülékenységek kihasználása ellen nem nyújtanak megfelelő védelmet. Erre is szükség van, azonban sokszor az eddig nem látott támadások ellen is védekezni kell valahogy (sajnos az eddig ismeretlen un. 'zero day' támadások ellen még csak nagyvállalati megoldások léteznek, otthoni felhasználóknak ezek nagyrészt elérhetetlenek, vagy mély műszaki ismereteket igényelnek).

Ha nem vagyunk biztosak a fájlok megbízhatóságában (és nincs telepítve Antivirus szoftver a számítógépünkre) akkor több lehetőségünk is van a feltételezett kártékony tartalom ellenőrzésére.

Az egyik lehetőség, hogy felhőszolgáltatásokat veszünk igénybe az ellenőrzésre (pl.: a Virustotal[12] fájlok és URL-ek ellenőrzésére használható cloud szolgáltatást, mely 64 Antivirus motorral ellenőrzi a feltöltött fájlokat). E mellett vannak más hasonló szolgáltatások, melyeket Lenny Zeltser malware elemző gyűjtött össze[13]).

Végső megoldásként online alkalmazásokkal is megnyithatjuk a gyanús fájt, ezzel is minimalizálva a számítógépünk fertőzésének lehetőségét (pl. a Google docs[14] vagy az Office Online[15] segítségével). Ezek használata esetén azonban kerülni kell a bizalmas dokumentumok feltöltését. Telepítő csomagok és futtatható állományok esetén a gyártó

---

[9] Lásd: https://wiki.archlinux.org/index.php/Disk_Encryption#Comparison_table
[10] Forrás: https://www.theguardian.com/technology/2008/may/15/computing.security
[11] A magánhasználatú eszközök (mobil és asztali platformok) szanizálásáról olvashatunk a Stanford University ajánlásában: https://uit.stanford.edu/security/data-sanitization
[12] Forrás: https://www.virustotal.com/
[13] Forrás: https://zeltser.com/lookup-malicious-websites/
[14] Lásd:https://www.google.com/docs/about/
[15] Lásd:https://products.office.com/hu-hu/office-online/documents-spreadsheets-presentations-office-online

honlapjáról való letöltés során ügyeljünk, hogy biztonságos (https) kapcsolaton keresztül történjen, illetve célszerű ellenőrizni a letöltött állomány digitális aláírását[16].

FRISSÍTÉSEK

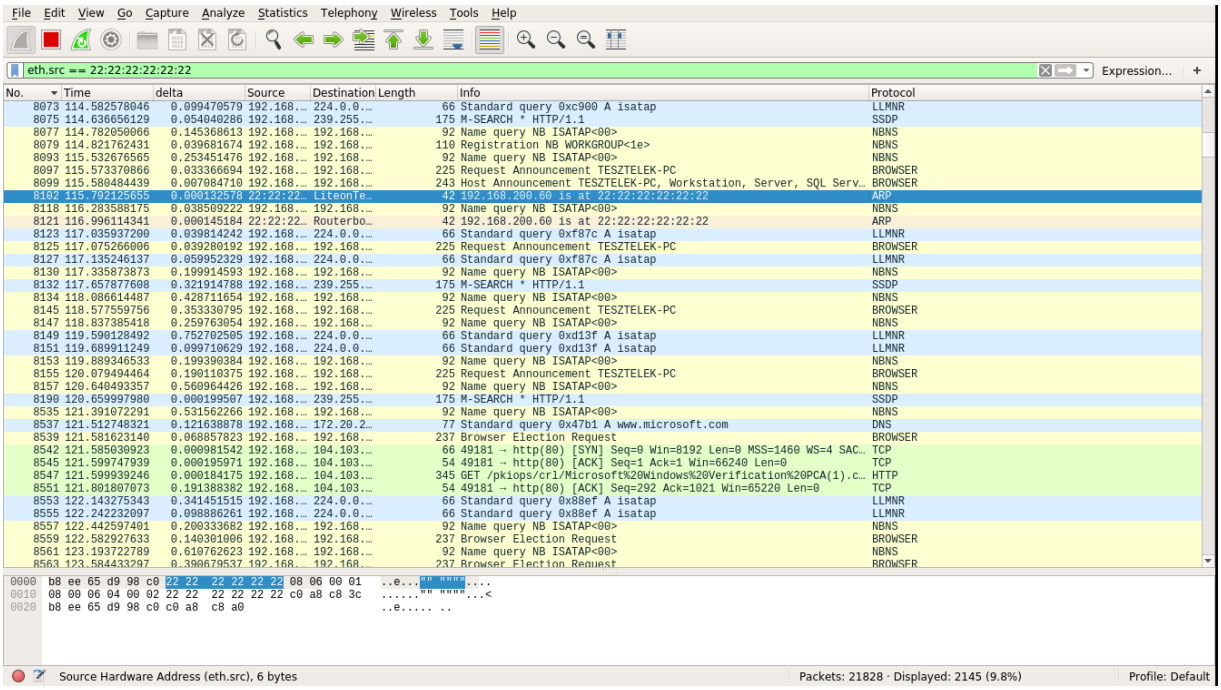
A kiberbiztonsági incidensek jelentős része az elavult, ismert sérülékenységgel bíró operációs rendszerek és programok használata miatt következik be[17]. Épp ezért a legtöbb operációs rendszer automatikusan, a felhasználó tudta nélkül, a háttérben frissíti önmagát. A felhasználói szoftverek általában telepítésnél megkérdezik, hogy kívánjuk-e az automatikus frissítés keresést bekapcsolni (ha ezt nem jelzik, akkor feltételeznünk kell, hogy nem frissítenek automatikusan).

Ezek bekapcsolása javasolt, valamint időszakosan célszerű ellenőrizni a frissítések állapotát (pl.: sok esetben a frissítések érvénybe lépése újraindítást követel, és egyesek a laptopjukat csak alvó üzembe helyezik, így csak ritkán indítják újra, ezáltal a frissítések nem lépnek érvénybe).

Komolyan növelhetjük online biztonságunkat, ha „frissen” tartjuk rendszereinket, azonban az anonimitás szempontjából ennek is vannak árnyoldalai. Mivel a névtelenség szempontjából a túl gyakori frissítések is árulkodóak lehetnek (eláruljuk, hogy milyen operációs rendszert használunk, azon milyen programok futnak), és hozzásegíthetnek másokat az identitásunk megismeréséhez. Az alábbi ábrán egy Windows operációs rendszer hálózati forgalmának olyan pillanatképét láthatjuk, amikor a felhasználó nem használta a számítógépet (az egyes sorok egy-egy hálózati csomagot jelentenek). A Windows rendszereken automatikusan bekapcsolt hálózati szolgáltatások generálják ezt a háttérforgalmat, mint például a fájlmegosztás szolgáltatás a 8077. csomagnál, vagy a frissítés szolgáltatás miatt kezdeményezett névfeloldás a 8537. csomagnál). Érdemes megfigyelni az info oszlopban megjelenő „TESZT ELEK” nevet, mely utal a felhasználónkra (nyílt hálózaton ugyanígy gyűjthetnek információt a felhasználókról).

[16] A futtatható állományok a weblapokhoz hasonló módon hitelesíthetőek a készítőik elektronikus aláírásával. A Microsoft Sigcheck szoftverével ezt mi magunk is ellenőrizni tudjuk. További részletek: https://docs.microsoft.com/en-us/sysinternals/downloads/sigcheck

[17] Az Avast felmérése alapján az alábbi címen elérhető szoftverek frissítéséről feledkezünk meg leggyakrabban https://betanews.com/2017/03/28/outdated-programs-cause-security-incidents/



1. ábra Windows hálózati forgalom "nyugalmi állapotban" (saját szerkesztés)

Mérlegelnünk kell tehát, és a használt hálózat biztonsága és megbízhatósága alapján kell eldöntenünk, hogy kívánunk-e frissíteni, vagy sem (jellemzően manapság ezt kézzel nehéz állítani).

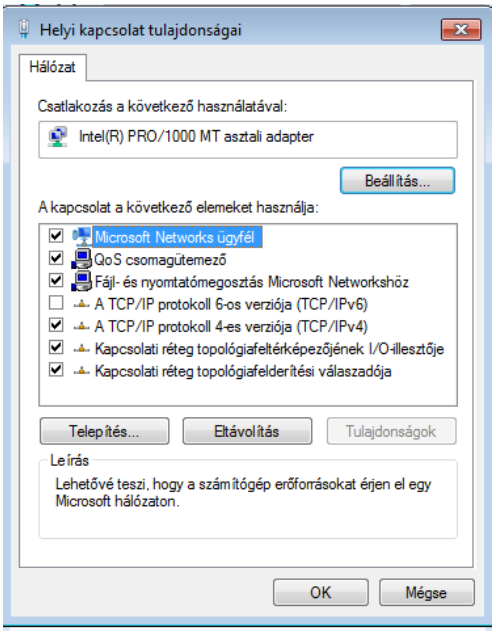
Ha külföldre utazunk, vagy más okból tudjuk előre, hogy publikus, titkosítatlan vezeték nélküli internetelérést fogunk használni, célszerű még előtte frissítenünk a szoftvereinket.

FELESLEGES SZOLGÁLTATÁSOK KIKAPCSOLÁSA

Főként a nem használt hálózati szolgáltatások kikapcsolásával javíthatjuk a rendszerünk biztonságát és csökkenthetjük a digitális lábnyomunkat.

A Windows rendszerek esetén az automatikusan bekapcsolt IPv6-os hálózati stack is egyenes utat nyit a támadásoknak [18]. Ezt igen egyszerűen, az IPv6-os stack letiltásával meg tudjuk előzni.

[18] Például a Responder nevű script számára, mely a Windows rendszerek sérülékeny automatikus beállításait használja ki További információ: https://github.com/SpiderLabs/Responder és https://www.trustwave.com/Resources/SpiderLabs-Blog/Introducing-Responder-1-0/



2. ábra Windows IPv6 stack letiltása (saját szerkesztés)

Másik jellemző támadási forma az irodai alkalmazásokat célozza és az azokban elérhető script funkciókat használja ki. Ha ezeket nem használjuk (pl.: makrókat az Office csomagban, vagy a javascriptet a pdf olvasó programban), akkor célszerű kikapcsolni, ezzel is csökkentve a támadók lehetőségeit. Mindenki más és más szoftvereket használ, így ajánlásom nem lehet teljes körű, azonban célszerű rászánni néhány percet, és a kedvenc keresőnk segítségével megnézni, hogy az adott szoftverre milyen fenyegetések várhatóak, és hogyan lehet azok ellen védekezni.

A korábban csatlakozott Wifi hálózatok automatikus keresése, a látható Bluetooth kapcsolatok, és egyéb vezeték nélküli kapcsolatok is elárulhatnak minket (merre jártunk, mely hálózatokra léptünk fel korábban). A Defcon konferencián az un. '*Wall of sheep'*-en kijelzik[19], a nyílt hálózaton, titkosítás nélkül küldött jelszavakat és felhasználóneveket (Lásd 3. ábra). Más konferenciákon az RFID kártyák veszélyeire hívják fel a figyelmet [13], vagy épp a Bluetooth és Wifi hálózatokat monitorozzák, hogy bemutassák, milyen hálózatokhoz szeretnénk automatikusan csatlakozni. Ez egy személetes módja, hogy felhívjuk a figyelmet a nyílt hálózatok és a vezeték nélküli kapcsolatok veszélyeire.

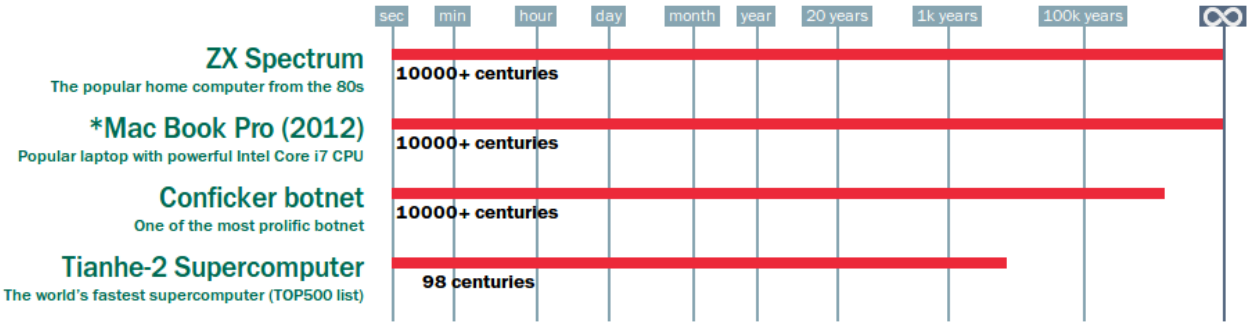
[19] További részlet: https://www.wallofsheep.com/pages/wall-of-sheep

3. ábra Szégyenfal a Defcon konferencián[20]

JELSZAVAK GENERÁLÁSA ÉS TÁROLÁSA

Az alábbi linuxos egysoros paranccsal megbízható jelszavakat tudunk generálni (a megbízhatóság relatív, és mindig a lehetséges támadási módok, a kor technológia színvonala, a támadó számára rendelkezésére álló számítási kapacitás határozza meg).

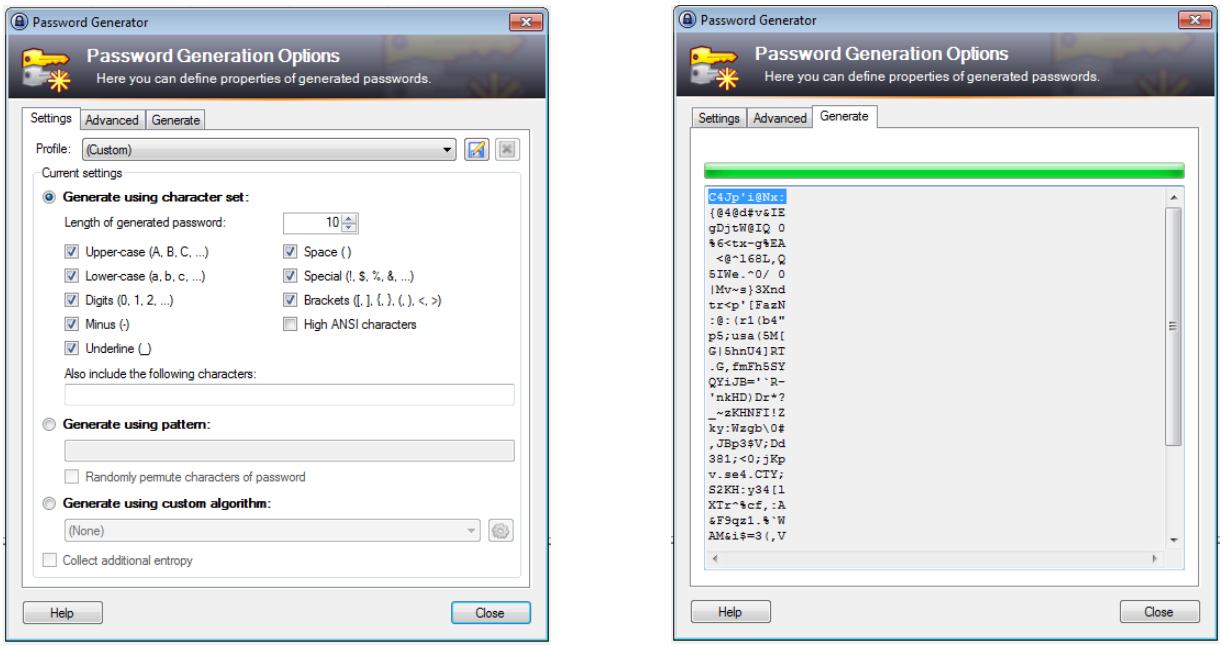
```
NCHARS=20; head -c 500 /dev/urandom | tr -dc 'a-zA-Z0-9~!@#$%^&*_-' | fold -w $NCHARS | head -n 1
```



4. ábra Egy generált jelszó (#uP7b^SU3DInV!57qyjX) feltöréséhez szükséges idő különböző számítógép architektúrákon[21]

[20] További információ: http://www.thesecurityblogger.com/what-is-the-wall-of-sheep-at-def-con-my-experience-as-a-speaker-volunteer-and-dj/

Windows rendszereken az alapértelmezetten telepített programok nem képesek jelszógenerálásra, így sajnos csak telepített programok segítségével lehet hasonló véletlenszerű jelszavakat létrehozni (lásd: 5. ábra). A biztonság egyik része a nehezen kitalálható jelszavak használata (amivel elég rosszul állunk, ha megnézzük a tömeges jelszólopások alapján publikált statisztikákat[22]). Az a probléma a nehezen kitalálható jelszavakkal, hogy általában nehezen is jegyezhetőek meg (és nagy valószínűséggel vétünk hibát a begépelésüknél). Ezért használjunk inkább jelszó menedzsment programokat. Például a Windows rendszereken használható Keepass rendelkezik jelszó generátor funkcióval is, megkönnyítve a véletlenszerű jelszavak létrehozását.



5. ábra A KeePass jelszógenerátorának paraméterezése (bal oldalt látható), és a generált jelszavak, melyek közül tetszőlegest kiválaszthatunk (jobb oldalt látható) (saját szerkesztés)

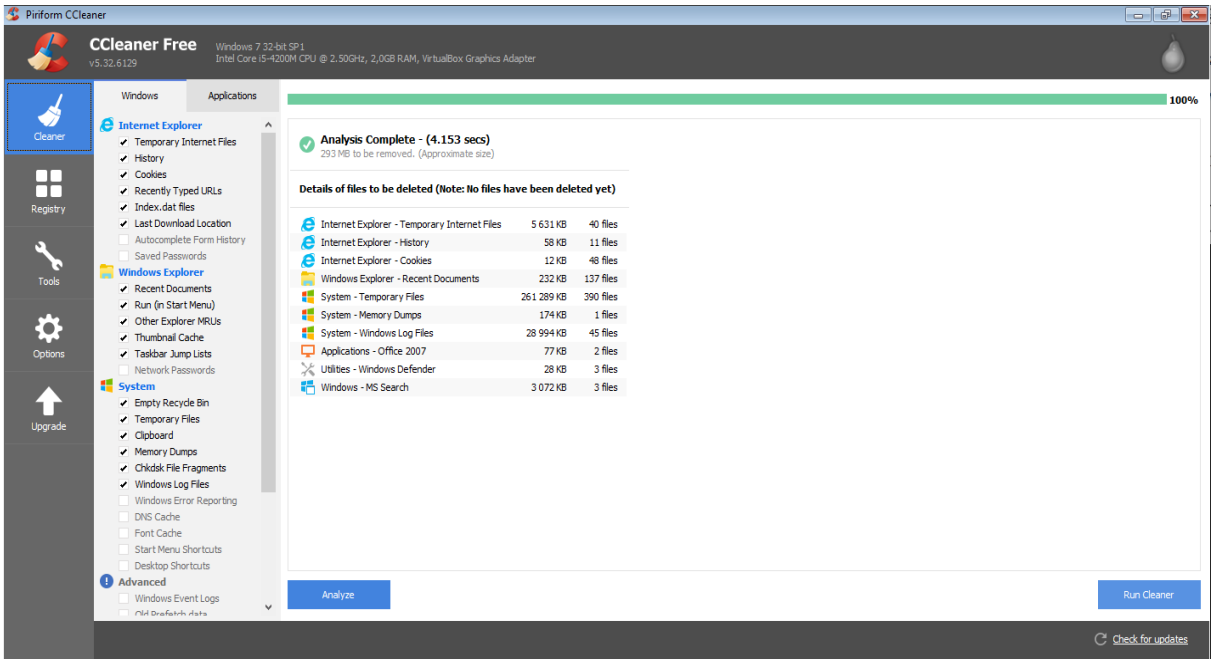
BÖNGÉSZŐ BIZTONSÁG

Az internet használata során a felhasználók főként a böngészőjükön keresztül látják a világhálót. Ezáltal a böngésző, és annak kiegészítői elsődleges célpontjai lehetnek a kártékony tartalmaknak és eszközök a felhasználók böngészési szokásainak követéséhez.

A legtöbb böngészőprogram támogat valamiféle anonim böngészési módot. Pl.: Firefox esetén a „privát böngészés” mód vagy Chrome-nál az „incognito” mód), mely használata esetén a munkamenet bezárása után a böngészés során összegyűlt metainformációkat (böngészési előzmények, sütik, automatikus űrlapkitöltési adatok, mentett felhasználónevek és jelszavak, stb.) a program törli. Célszoftverekkel még lehetőség van a böngészési előzmények törlése mellett az operációs rendszer időszakos fájljainak törlésére is (pl.: Windows-on a népszerű CCleaner[23], vagy a Windows-on, Linux-on és Mac OS X-en is

[21] a https://password.kaspersky.com/ kimutatása alapján
[22] Például az alábbi linken: https://nakedsecurity.sophos.com/2016/09/02/and-the-worst-passwords-from-the-last-fm-hack-are/
[23] Letölthető: https://www.piriform.com/ccleaner

futtatható BleachBit[24]). Azonban tudni kell, hogy az internetszolgáltatóknál (pl. publikus Wifi üzemeltetőknél) és a meglátogatott weblapok üzemeltetőinél is megmaradnak előzményeink



6. ábra A CCLEANER működés közben (saját szerkesztés)

Ezen felül a kártékony oldalak számos információt szerezhetnek rólunk, miközben meglátogatjuk azokat. Szemléletes példák voltak erre a felhasználó nemét kikövetkeztető weboldalak[25]. Megláthatjuk milyen információkat szolgáltat ki rólunk a böngészőnk, ha meglátogatjuk a Browserspy weboldalát (http://browserspy.dk/browser.php) vagy a Browserleaks (https://browserleaks.com/) lapját.

Célszerű több böngészőt is telepíteni, melyeket más-más célra használunk (pl.: Internet Explorer-t az online banki ügyintézésre, Chrome-ot az általános böngészésre, és Firefox-ot a webes levelezésre). Ennél a módszernél elegánsabb és nagyobb védelmet nyújt a QubesOS megoldása, mellyel a Live CD-k és virtualizáció fejezetnél részletesen is megismerkedhet az olvasó.

A TOR Projekt[26] használata esetén a titkosított forgalom több relé állomáson keresztül éri el a végcélt, és a forgalmazás során ezeknek a köztes állomásoknak a sorrendje változik, így a teljes forgalom nem áll össze egyetlen állomáson sem (a kilépő ponton viszont látszódnak az egyes csomagok). A TOR böngésző[27] segítségével automatikusan tudunk csatlakozni a TOR hálózathoz, így böngészésünk során folyamatosan változik az internetelérésre használt „kilépő” IP címünk.

[24] Lásd: https://www.bleachbit.org/
[25] Lásd:
https://www.researchgate.net/profile/Tu_Phuong2/publication/278399485_Gender_Prediction_Using_Browsing_History/links/5587f22b08ae7bc2f44d7a35/Gender-Prediction-Using-Browsing-History.pdf
https://www.ghacks.net/2008/07/28/male-or-female-your-browsers-history-might-tell/
http://www.mikeonads.com/2008/07/13/using-your-browser-url-history-estimate-gender/
[26] Lásd: https://www.torproject.org/
[27] Lásd: https://www.torproject.org/projects/torbrowser.html.en

Szólni kell arról, hogy több támadás is érte ezt a hálózatot [14], és vannak módszerek, melyek segítségével a böngészés továbbra is követhető [15].

A böngésző kiegészítőkkel is fokozni tudjuk a biztonságot, és az anonimitást, például a *Noscript*[28], mely az aktív tartalmak (pl.: JavaScript, Java, Flash) automatikus betöltését akadályozza meg, a *Ghostery*[29], mely a weblapok felhasználó követési technikáit blokkolja, vagy az Adblock Plus[30] reklám szűrők segítségével.

Felmerülhet a kérdés, hogy van-e különbség, ha a világ más pontjáról böngésszük az internetet? Erre a választ megkaphatjuk a Geopeeker oldalon keresztül:

https://www.geopeeker.com/fetch/?url=cnn.com

A fenti weblap segítségével ellenőrizhetjük, hogy pl.: a "cnn.com" vagy a "bbc.com" esetleg a "www.bbc.co.uk/weather/" mennyiben eltérő tartalmat szolgáltat annak függvényében, hogy épp hol vagyunk a világban.

A Geolokáció megtévesztése is lehetséges[31] a *Location guard* és a *Fake location*[32] kiegészítőkkel.

A *User Agent switcher*[33] kiegészítő is hozzásegíthet az anonim böngészéshez, mivel segítségével váltogatni tudjuk a böngészőnk típusát (legalábbis másnak adja ki magát a böngésző a http kérések user-agent mezőjében). Itt ügyelni kell, hogy bizonyos beállításoknál nem megfelelően fognak megjelenni a weblapok (pl.: ha mobil eszköznek adjuk ki magunkat).

Fontos azonban kiemelni, hogy ezeket a kiegészítőket is biztonságos forrásból telepítsük, mivel ezek is tartalmazhatnak kártékony kódokat.

A felhasználói profilkészítést a teljes képernyő használatának mellőzésével, és más-más méretre állított képernyőfelbontással, vagy átméretezett böngészőablakkal tudjuk fokozni.

DNS BIZTONSÁG

Böngészés során a webszolgáltatásokat jellemzően nem IP cím (pl.:172.217.6.68), hanem, URL cím (pl.: *google.com)* alapján érjük el. Ez fordítást igényel, mivel a számítógépek útvonalválasztása IP címek alapján történik. Ezt a DNS (Domain Name Service), más néven névfeloldó szolgáltatás végzi. Jellemzően a felhasználók alapértelmezetten szokták hagyni, mely esetén a hálózat saját DNS szerverét fogja használni (pl.: internet szolgáltató, publikus Wifi, stb. saját DNS szervere). Mivel minden keresés előtt a meglátogatni kívánt weblap IP címéért ehhez a DNS szerverhez fordulunk, így a böngészési szokásunkat a DNS szerver üzemeltetője látni fogja. Ha a biztonság az elsődleges célunk, akkor érdemes olyan szervert használni, mely reputáció alapú szűrést is alkalmaz, így a kártékony tartalmak elleni védelem első lépcsője a DNS lesz. Ilyen például a Cisco Umbrella által üzemeltetett OpenDNS[34] (ennek a DNS szervernek az IP címei: [208.67.222.222], [208.67.220.220]) vagy a Comodo

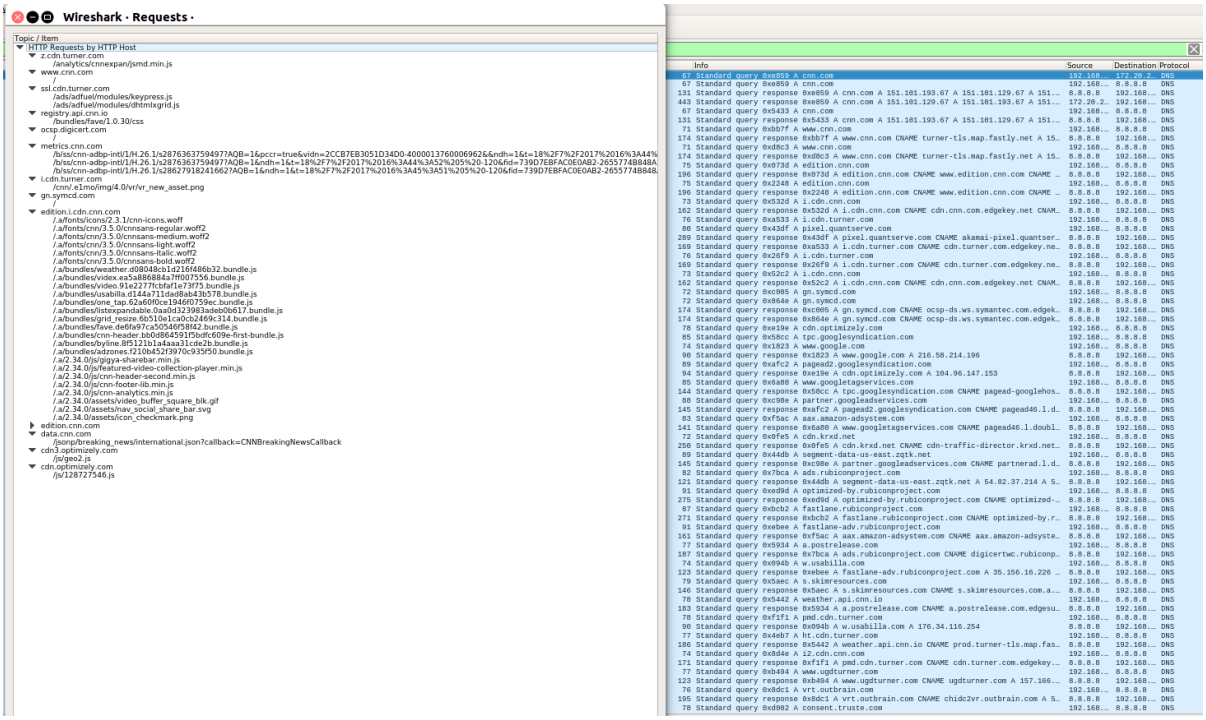
[28] Lásd: https://noscript.net/
[29] Lásd: https://www.ghostery.com/
[30] Lásd: https://adblockplus.org/
[31] amennyiben a geolokáció az eszközökbe épített GPS vevő alapján működik
[32] Lásd: https://addons.mozilla.org/hu/firefox/addon/location-guard/ és https://addons.mozilla.org/en-US/firefox/addon/fake-location/
[33] Lásd: http://useragentswitcher.org/
[34] Lásd:https://www.opendns.com/cisco-opendns/

SecureDNS[35] szolgáltatása a [8.26.56.26,8.20.247.20] [156.154.70.22, 156.154.71.22] IP címeken.

Az operációs rendszerekben lehetőség van egy un. host fájlt létrehozni, amiben kézzel állítjuk be a IP cím – URL cím összerendezéseket. Ebben lehetőség van a nem kívánt weblapok szűrésére (pl. felnőtt tartalmak szűrése szülői felügyelet céljából), illetve támogathatja az anonim böngészést azáltal, hogy a gyakran használt weboldalak IP címét nem kell lekérnünk a DNS szervertől.

A reklámoldalak és a kártékony tartalmak megnyitását is ilyen szűrőlistákkal, az un. Blacklist-ekkel tudjuk kivédeni. Lenny Zeltser, malware kutató összegyűjtött néhány ingyenes letölthető szűrőlistát weblapján (https://zeltser.com/malicious-ip-blocklists/).

Sokszor nem is tudjuk, hogy egy-egy weblap megnyitása során hány másik weblapról töltünk le tartalmat (ahonnan hirdetéseket, képeket vagy videókat tölt be a meglátogatott lap). Ezért célszerű a gyakrabban használt weblapjaink megnyitása során egy hálózati forgalomelemző alkalmazással (pl.:wireshark) megnézni, hogy mely más weblapokról is kér le információt böngészőnk (és felvenni a szűrőlistára a nemkívánatos oldalakat).



7. ábra A *ccn.com* betöltése során generált DNS lekérdezések (saját szerkesztés)

A fenti pillanatkép a Wireshark hálózati forgalomelemzését mutatja, miközben a böngészővel a cnn.com weboldalra navigáltam. Jobb oldalt soronként láthatóak azok a weblapok, melyekre hivatkozott a cnn.com (ezekről képeket, reklámokat, és egyéb, a megjelenítéshez szükséges tartalmakat töltött be a böngésző). Mivel ezeknek a hivatkozásoknak is ismernünk kell az IP címét, így az operációs rendszerünk minden egyes külső hivatkozásra kezdeményez egy DNS lekérdezést (Lásd: 7. ÁBRA jobb oldala).

Ha VPN kapcsolaton keresztül böngésszük az internetet, vagy a TOR hálózatot használunk, akkor is célszerű ellenőrizni a DNS beállításokat, mert információt szivárogtathat

[35] Lásd: https://www.comodo.com/secure-dns/

rólunk, ha nem megfelelően konfiguráljuk. Ezt az ellenőrzést a DNSleaktest.com oldal segítségével végezhetjük el.

KERESŐSZOLGÁLTATÁSOK ÉS AZ ANONIMITÁS

A legtöbb ember, ha számára ismeretlen, újszerű dologgal találkozik, az első dolga, hogy rákeres arra az interneten. Épp ezért a felhasználók nagy része a Google keresőn keresztül éri el a világhálót (a statisztikai elemzések 67-87% közé teszik ezt az arányt) [16] [17] [18] [19] [36].

Az internetezés 93% -ban egy keresőszolgáltatás használatával kezdődik [4]. Így ezek a rendszerek digitális lábnyomunkat megőrzik. Szokásaikról, kedvenc oldalainkról információt gyűjt, hogy a felhasználói élmény fokozása (és a fizetett reklámok) miatt célzott ajánlatokat tegyen későbbi böngészéseink során. Egyén függő, hogy ezt kényelmi funkcióként, vagy a „Nagy testvér" kéretlen gondoskodásaként fogja fel.

Ha nem szeretnénk, hogy a keresési előzményeinket egy keresőszolgáltató tárolja, akkor felváltva használjuk a keresőket, és a duckduckgo[37]-hoz hasonló anonimitást támogató szolgáltatásokat vegyünk inkább igénybe. Ha több keresőt is felhasználunk, akkor nagyobb mennyiségű, és remélhetőleg pontosabb találatok előnyét is élvezhetjük, mivel a különböző keresők más-más adatbázisból dolgoznak.

LEVELEZÉS BIZTONSÁGA

Ha az elektronikus levelezésre gondolunk, a hitelesség és a bizalmasság az, ami egyből eszünkbe juthat. A kliens és a levelező szerver között jellemzően biztonságos kapcsolat alakítható ki (pl.: https csatorna), azonban a levelező szerverek között titkosítás nélkül kerülnek továbbításra a levelek.

Több megoldás is létezik a levelezés védelmének fokozására. A bizalmasság érdekében titkosítást alkalmazhatunk, azonban az csak a tartalmat (a levél szövegét és a csatolmányokat) védi, a feladó és címzett, tárgy mezők továbbra is nyílt szövegként kerülnek továbbításra (mivel a szervereknek azokat fel kell dolgozniuk).

A hitelesség érdekében elektronikus aláírást használhatunk, melyre magáncélú alkalmazás esetén a PGP az egyik legjobb választás.

Sokszor az anonim levélküldésre is szükségünk lehet, melyben az alábbi oldalak tudnak segíteni, ideiglenes email fiókokkal. A nagyobb webes levelezőrendszerek közül a Yahoo-n lehet személyes adatok (és másik email vagy telefonszám) megadása nélkül regisztrálni. Vannak azonban egyirányú levelező szolgáltatók (csak küldésre, vagy csak fogadásra). Ilyen például a Tempinbox[38] (mely ingyenes, csak nyílt http protokollt használó, egyirányú, csak fogadásra használható levelező), MailNull[39] (mely időszakos email címet biztosít, lehetséges továbbítani a bejövő leveleket egy másik címre), Mailinator[40] (amely a beérkező levelek címzettjének kreál egy időszakos fiókot, nem szükséges regisztrálni, de így bárki megnézheti a bejövő levelünket), Jetable[41] (időszakos levelező cím létrehozására használható, a

[36] A fenti statisztikákat a google, a bing, a yahoo, és a duckduckgo keresők első 12 találata alapján választottam ki.
[37] Lásd: https://duckduckgo.com/
[38] http://www.tempinbox.com/
[39] https://mailnull.com/create.html
[40] https://www.mailinator.com/
[41] https://www.jetable.org/en/index

beérkezett leveleket továbbítja a valós címünkre), Sneakemail[42] (egy hónapig ingyenesen használható, szintén csak fogadásra használható levelezőfiók).

Vannak un. Remailer-ek[43] [44], melyek segítségével anonimen tudunk levelet küldeni.

A biztonságos kommunikáció érdekében például a ProtonMail[45]-t használhatjuk, mely segítségével végponttól végpontig titkosított levelezhetünk, és képes még a TOR hálózaton keresztül is működni[46] (így a hozzáférést anonimizálni).

Sok esetben a levelező rendszer fájlméret korlátai miatt a nagyobb méretű fájlokat egy felhőtárba töltjük fel, ebben az esetben csak a linket kell elküldenünk a címzetteknek. Célszerű ebben az esetben is titkosítást alkalmazni (még a feltöltés előtt, és a titkosításra használt kulcsot biztonságosan, más csatornán, vagy személyesen megosztani).

KÖZÖSSÉGI OLDALAK ÉS A BIZTONSÁG

A közösségi oldalak egyik lényege, hogy ismerőseinkkel információt osszunk meg a mindennapi életünkről. Paradox lenne ezeken az oldalakon az anonimitásra törekedni. Másrészt viszont a biztonság egyre fontosabbá válik. Az egyre gyakoribb adatbiztonsági incidensek, tömeges adatlopások korában azon is célszerű elgondolkodni, hogy milyen jellegű információkat osztunk meg az egyes oldalakon. Illetve azon is célszerű regisztráció előtt elgondolkodni, hogy hosszútávon akarjuk-e használni az oldalt, esetleg a későbbiekben kellemetlenséget okoz, ha kiszivárog, hogy milyen oldalakat látogattunk [47].

Érdekesség, hogy a Facebook is elérhető már a Tor hálózaton[48] keresztül az alábbi címen: https://facebookcorewwwi.onion/ .

A közösségi hálózatok biztonságos felhasználásáról többet tudhatunk meg a NATO által készített Biztonságtudatossági[49], és a Közösségi média[50] tanfolyamokból.

LIVE CD-K ÉS A VIRTUALIZÁCIÓ

A Tails[51] (The Amnesic Incognito Live System) egy debian alapú live operációs rendszer, mely telepítés nélkül is használható. Célja, hogy minél kevesebb nyomot hagyjunk böngészésünk során. Vannak más hasonló szoftverek is pl.: JonDo[52], vagy az Anonym.OS (utóbbi fejlesztése jelenleg szünetel).

A biztonságosan és anonimitást támogató operációs rendszerek használata, azok iránti érdeklődés is felhívhatja a figyelmet ránk (pl.: Edward Snowden által kiszivárogtatott

---

[42] https://sneakemail.com/
[43] http://gilc.org/speech/anonymous/remailer.html
[44] Például: http://www.sendanonymousemail.net/
[45] https://protonmail.com/
[46] https://protonirockerxow.onion/
[47] 2015-ben az Ashley Madison online rendszerét törték fel hackerek, és szivárogtatták ki a felhasználók adatait https://digitalguardian.com/blog/timeline-ashley-madison-hack , 2016-ban pedig közel 400 millió, az Adult Friend Finder-re regisztrált felhasználó adat került nyilvánosságra https://www.wired.co.uk/article/adult-friend-finder-hacked-email-addresses-users
[48] További részletek: https://www.facebook.com/notes/protect-the-graph/making-connections-to-facebook-more- secure/1526085754298237?_fb_noscript=1
[49] Awareness e-Course https://ccdcoe.org/awareness-e-course.html
[50] Social Media Awareness https://innovationhub-act.org/content/five-lessons-social-media-awareness https://innovationhub-act.org/smcourse/course
[51] https://tails.boum.org/
[52] https://anonymous-proxy-servers.net/en/jondo.html

források alapján az NSA a Tails live CD felhasználóit is potenciális fenyegetésnek értékelte[53]).

Virtuális gépek használatával védhetjük a számítógépet, ha a nem megbízható oldalakat látogatunk, új szoftvereket telepítünk, vagy ismeretlentől kapott dokumentumokat szeretnénk megnyitni, mivel lehetőségünk van egy korábbi állapotra visszatölteni a virtuális gépünket.

Ennél a Qubes OS[54] koncepciója a napi életben hatékonyabban alkalmazható, mivel itt maga az operációs rendszerünk hoz létre szeparált munkakörnyezetet (pl.: a banki tranzakcióknak, a zenelejátszásnak, a munkahelyi levelezésnek és a magánjellegű chat-elésnek külön-külön).

KÖVETKEZTETÉSEK

A fentiekben ajánlott, az anonimitást és biztonságot elősegítő javaslataim nem igényelnek mély szakmai ismereteket, ez alapján felmerülhet a kérdés, hogy mégis miért nem alkalmazzák ezeket a felhasználók. A válasz egyszerű: jellemzően nincs igény a biztonságra, illetve mások a munka és magánéleti prioritások, így idő hiányában a kevésbé biztonságos (sokszor alapértelmezett) megoldásokat választják.

A másik ok, hogy sok felhőszolgáltatás kényelmessé tett minket, és a funkcionalitás miatt feláldoztuk az anonimitásunkat.

További veszély, melyre megpróbáltam felhívni a figyelmet, hogy nem ismerjük kellőképpen az általunk használt eszközöket, az azokban rejtőző funkciókat (melyek sokszor feleslegesek, de mégis aktiválva vannak). A biztonság-tudatos, vagy pontosabban a fenyegetés-tudatos magatartás hiánya sokszor a felhasználók tudatlansága (technikai lehetőségek és a fenyegetések ismeretének hiánya) miatt van. Remélem a fenti példák felébresztették az olvasóban az igényt a biztonságos internetezéshez, és „tudatos” felhasználókká válnak.

A cikksorozat következő részében a mobil és hordozható informatikai eszközök (un. Okos eszközök) biztonságos használatával ismerkedhetnek meg az olvasók.

FELHASZNÁLT IRODALOM

[1] ENISA - *Threat Landscape Report 2016*
Forrás: https://www.enisa.europa.eu/publications/enisa-threat-landscape-report-2016/at_download/fullReport (letöltve: 2017.08.10.)

[2] SANS - *SECURITY AWARENESS REPORT 2017*
Forrás:https://securingthehuman.sans.org/media/resources/STH-SecurityAwarenessReport-2017.pdf (letöltve: 2017.08.10.)

[3] Forrás: http://2016.trade.gov/jobs/forms/foreign-travel-briefing-training.pdf (letöltve: 2017.08.10.)

[4] US Food and Drug Administration Forrás: https://www.fda.gov/downloads/ICECI/Inspections/ForeignInspections/ucm113732.pdf (letöltve: 2017.08.10.)

53 Forrás: https://www.theregister.co.uk/2014/07/03/nsa_xkeyscore_stasi_scandal/
54 Forrás: https://www.qubes-os.org/

[5] INTERNETSOCIETY - *Digital Footprints* Forrás: https://www.internetsociety.org/sites/default/files/Digital%20Footprints%20-%20An%20Internet%20Society%20Reference%20Framework.pdf (letöltve: 2017.08.10.)

[6] KHETANI S. - *Spies Used A Fake Facebook Account For NATO's Supreme Commander To Get Private Personnel Information* Forrás: http://www.businessinsider.com/spies-used-a-fake-facebook-account-for-natos-supreme-commander-to-get-personnels-private-information-2012-3 (letöltve: 2017.08.10.)

[7] Microsoft Corporation - Security Hardening Tips and Recommendations Forrás: https://social.technet.microsoft.com/wiki/contents/articles/18931.security-hardening-tips-and-recommendations.aspx (letöltve: 2017.08.10.)

[8] Australian Signals Directorate - *Strategies to Mitigate Cyber Security Incidents* Forrás: https://www.asd.gov.au/infosec/mitigationstrategies.htm (letöltve: 2017.08.10.)

[9] Apple - *Mac OS X Security Configuration Guide* Forrás: http://www.apple.com/support/security/guides/ (letöltve: 2017.08.10.)

[10] Ubuntu - *Basic Ubuntu Security Guide, Desktop Edition* Forrás: https://wiki.ubuntu.com/BasicSecurity (letöltve: 2017.08.10.)

[11] ERDŐSI P. M., SOLYMOSI Á. - *IT biztonság közérthetően* Forrás: http://njszt.hu/sites/default/files/IT_biztonsag_kozerthetoen.pdf (letöltve: 2017.08.10.)

[12] Mark Hachman - *The price of free: how Apple, Facebook, Microsoft and Google sell you to advertisers* Forrás: http://www.pcworld.com/article/2986988/privacy/the-price-of-free-how-apple-facebook-microsoft-and-google-sell-you-to-advertisers.html (letöltve: 2017.08.10.)

[13] ZETTER, KIM - *Feds at DefCon Alarmed After RFIDs Scanned* Forrás: https://www.wired.com/2009/08/fed-rfid/ (letöltve: 2017.08.10.)

[14] FISHER, D. - *Researcher Finds Tor Exit Node Adding Malware to Binaries* Forrás: https://threatpost.com/researcher-finds-tor-exit-node-adding-malware-to-binaries/109008/ (letöltve: 2017.08.10.)

[15] SCHNEIER, B - *Attacking Tor: how the NSA targets users' online anonymity* Forrás: https://www.theguardian.com/world/2013/oct/04/tor-attacks-nsa-users-online-anonymity (letöltve: 2017.08.10.)

[16] *Desktop Search Engine Market Share* (online) Forrás: https://www.netmarketshare.com/search-engine-market-share.aspx?qprid=4&qpcustomd=0 (letöltve: 2017.07.21.)

[17] ALLEN, R. - *Search Engine Statistics 2017* (online) Forrás: http://www.smartinsights.com/search-engine-marketing/search-engine-statistics/ (letöltve: 2017.07.21.)

[18] *Worldwide desktop market share of leading search engines from January 2010 to July 2017* Forrás: https://www.statista.com/statistics/216573/worldwide-market-share-of-search-engines/ (letöltve: 2017.07.21.)

[19] Collage of Marketing - *Search Engine Usage Facts and Statistics*
Forrás: http://www.collegeofmarketing.com/seo-guide/search-engine-usage/ (letöltve: 2017.07.21.)