A web bug technológia — barát vagy ellenség?

Hullám Gábor*

Budapesti Műszaki és Gazdaságtudományi Egyetem
Gazdaság- és Társadalomtudományi Kar
Információ- és Tudásmenedzsment Tanszék
1111 Budapest, Sztoczek u. 2. St. ép. I. em. 117.
Telefon: (36 1) 463-1832, Fax: (36 1) 463-4035
e-mail: hgabor@bakats.tvnet.hu

Absztrakt

A gazdasági életben az üzleti érdekek és az agresszív marketing egyre inkább igényli a vásárlók magánéletébe való behatolást, míg a vásárlók természetesen ennek megóvásában érdekeltek. E miatt az alapvető érdekellentét miatt számos csatát vívott a két oldal egymással mind az offline, mind az online világban. A web bug kezdetben nem volt más, mint egy több fronton bevethető, új fegyver az online marketing oldalán, ám idővel az internetes felhasználók adatainak tömegesen alkalmazott, ellenőrizhetetlen, jogilag és etikailag egyaránt kifogásolható megfigyelő eszközévé vált. Mára megszülettek azok az irányelvek, szabályozások, amelyek kijelölték és részben megteremtették a web bug etikus felhasználásához szükséges korlátozásokat. Az alábbiakban a lehetséges felhasználási módok ismertetése mellett ezen irányelvek bemutatására is sor kerül, érintve a már tisztázott jogi és etikai kérdéseket, valamint azokat a területeket, amelyek még további figyelmet igényelnek.

1. Mi az a web bug?

Már a neve is egy kissé félrevezető, hiszen nem a weboldalakon található hibákról van szó, mint ahogyan azt a szaknyelvben sűrűn alkalmazott 'bug' szócska sugalmazza. A *web bug*[1] egy — tipikusan 1x1 pixeles — grafika weboldalon vagy e-mailben elrejtve, amelynek elsődleges feladata az adott weboldalt vagy e-mailt olvasó felhasználók nyomonkövetése. De hogyan képes egy grafika, akkor is, ha csak egyetlen képpontról van szó, nyomkövetésre, megfigyelésre? A megoldás meglepően egyszerű, ha közelebbről megvizsgáljuk egy átlagos weboldal felépítését.

* Hullám Gábor műszaki informatikus, a BME GTK Információ- és Tudásmenedzsment Tanszék tudományos diákköri pályázója.

[1] A szaknyelvben más elnevezései is léteznek, mint a „Web beacon" vagy a „clear GIF".

A hozzáértők szemszögéből a weboldal meghatározott formai építőelemekből, úgynevezett HTML[2] címkékből, valamint az ezeket kitöltő tartalmi elemekből álló együttes. Az egyszerű felhasználó számára azonban a weboldal egyet jelent annak megjelenített részével. Az egyes bekezdések tagolása, a betűk színének, méretének, stílusának beállítása, táblázatok létrehozása, linkhozzáadás és számtalan más beállítási lehetőség pusztán láthatatlan formai összetevő.

Az egységes egészként megjelenő weboldal általában számos részből épül fel. Ezek lehetnek képek, grafikonok, szövegrészek, a legkülönfélébb objektumok, melyek egy-egy külön fájlban tárolódnak. Ezeket a felhasználó számára láthatatlan kapocs láncolja az oldalhoz. Egy kép beszúrásához mindössze egy „kép címkét" (IMG tag-et) kell beillesztenünk az oldal kódjába. Ebben a címkében specifikálni kell a képet tartalmazó fájl helyét[3] és a megjelenítés néhány paraméterét. Ezáltal az oldalhoz láncolódik az a képfájl, ami a beillesztendő képet tartalmazza, vagyis az oldal betöltése esetén maga a kép is betöltődik (alapértelmezett, hibamentes működés esetén). Egy címke beillesztése alapvető HTML-ismerettel rendelkezők számára nem jelent nehézséget, akár egy egyszerű szövegszerkesztővel is elvégezhető. Annak az ellenőrzése pedig, hogy az oldalon milyen címkék vannak, még ennél is egyszerűbb, mivel a teljes kód megjeleníthető a legtöbb manapság használatos böngésző segítségével.

Tételezzük fel, hogy adott egy egyszerű weboldal, amely egy kis méretű képet és egy féloldalnyi szöveget tartalmaz. Legyen ez a kép egy egyszerű reklám. Az esetek többségében elmondható, hogy a reklámot egy harmadik fél szolgáltatja, aki a weblap tulajdonosával, vagy a webszerver üzemeltetőjével köt valamilyen megállapodást. Fő célja a figyelemfelkeltés, amit élénk színekkel, animációval, hangeffektusokkal és egyéb elemekkel ér el. A reklám akkor sikeres, ha a felhasználó rákattint, és ezáltal a reklám tárgyát tartalmazó oldalra kerül. Az, hogy ezt követően pontosan mi történik az adott oldalon, a vizsgált téma szempontjából érdektelen. A kiemelendő tény az, hogy ilyen esetben a felhasználó önként lép be a marketing praktikák ördögi tárházába, ahol sokféleképpen rávehetik személyes információnak kiadására.

Mi történik akkor, ha az ember a saját tudomása nélkül vesz részt egy felmérésben? Alapesetben, ha az ember olyan ajánlatot, hirdetést kap, ami számára nem hordoz pozitív töltést, vagyis nem kelti fel érdeklődését vagy éppenséggel bántónak, sértőnek találja, akkor

[2] HyperText Markup Language: A World Wide Webhez létrehozott leíró nyelv hipermédia dokumentumok készítéséhez . A HTML állományokban < > karakterek közé zárt szöveges címkék, ún. „tag"-ek jelzik a dokumentum szerkezetét, színeket, beágyazott képek helyét, hiperlinkeket, stb.

[3] Az interneten a URL (Uniform Resource Locator) szabvány használatos a hely meghatározására. Lehetővé teszi az információforrások típusának és helyének megjelölését .

elutasítja azt. Tehát nem tölti ki a kérdőívet, nem küldi vissza a levelet, vagyis megszakítja a felé irányuló kommunikációs csatornát (nem válaszol). Hasonlóan zajlik mindez a webes világban is. Ha egy hirdetés nem tetszetős, nem kattint rá az ember. Ugyanígy, ha nem akarunk részt venni egy adatgyűjtésben, ha nem akarjuk, hogy adatainkat különféle célokra felhasználják, megtehetjük, hogy nem szolgáltatunk adatot. Éppen ezért, ha egy kereskedelmi site-on egy speciális embléma arról tanúskodik, hogy az oldalon történő vásárlások adatai (vásárló neve, címe, vásárolt termékek darabszáma, ára) egy központi adatbázisba kerülnek, amihez más kereskedők is hozzáférnek, lesznek felhasználók, akik emiatt nem vásárolnak az adott oldalon. Természetesen mindez egyéni ízlésen, és ami még fontosabb, egyéni döntésen alapszik. A web bugok esetében azonban más a helyzet, mert nem dönthetünk afelől, amit nem látunk. Ekkor ugyanis a megfigyelést, adatgyűjtést jelző embléma láthatatlan.

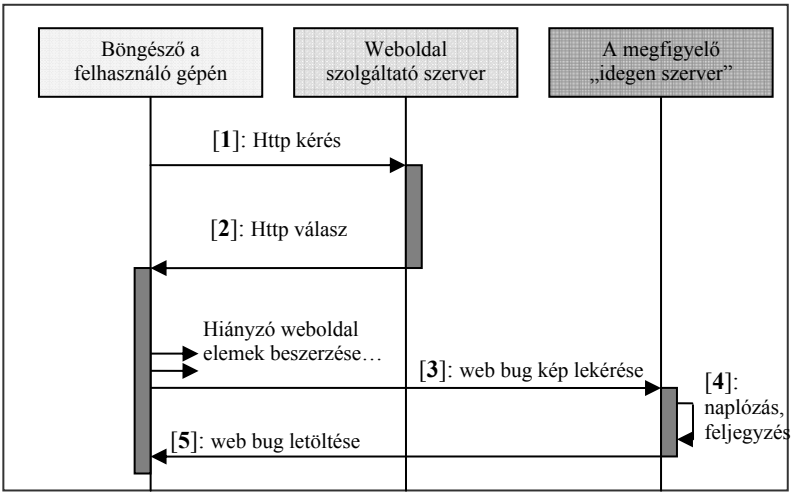
A web bugok az esetek többségében 1x1 pixeles áttetsző, egydimenziós képek,[4] tehát ugyanúgy beilleszthetőek, mint akármelyik másik kép. Így gyakorlatilag észrevétlenül meglapulhatnak egy weboldal tetszőleges részén. Természetesen ez a megjelenített felületre vonatkozik, mert a kódban mindenképpen szerepelnie kell, ha egyszer az oldal része. A problémát az jelenti, hogy eddig, ha olyasmivel találkozott a felhasználó, ami számára nem volt szimpatikus, akkor kikerülhette, letilthatta, kiszűrhette. De ebben az esetben akarva- akaratlan betölti a web bugot, és még csak tudomást sem szerez róla. Tehát az egyszerű felhasználó nem képes észlelni a potenciális veszélyforrást, így dönteni sem áll módjában, hogy hajlandó-e eltűrni, avagy sem. Tulajdonképpen ezért jogos a „bug" elnevezés, hiszen ez egyúttal lehallgatáshoz, nyomonkövetéshez használt eszközt is jelent angolul.[5]

Egy kép betöltése önmagában nem jelent nyomonkövetést, ehhez a háttérben egy jól olajozott gépezet működése szükséges, másfelől nem minden 1x1 pixeles áttetsző képpont web bug. A weboldalak szerkesztésénél bevett gyakorlatnak számít ilyen képek használata igazítási, elrendezési célból. A lényegi különbség a kettő között az, hogy míg a formai elemként szolgáló képpont a weblapot tartalmazó szerverről töltődik be, addig a web bug egy harmadik fél — a felhasználótól és az általa letöltött weboldal szolgáltatójától különböző — szerveréről. Ez könnyedén megvalósítható, hiszen a weblap, mint ahogy már a fentiekben is láthattuk, különféle elemekből áll össze, és nincs olyan megkötés, hogy minden részletnek azonos szerverről kell származnia. Tehát az oldal letöltésekor egyszerűen betöltődik a web bug is, úgy, mint a többi kép, csak máshonnan. Ez az egész mechanizmus kulcsmozzanata.

[4] Mivel tetszőleges grafika alkalmazható web bugként, ezét csak definíció kérdése, mit nevezünk annak. E tekintetben nincs egységes álláspont a szakmán belül.

[5] A magyar elnevezése éppen ezért: webpoloska.

A böngésző akkor szolgáltat ki adatot a felhasználóról, amikor a képet kéri le a harmadik fél szerverétől. Tekintsünk egy lehetséges lefutási módot egyszerű HTML oldal betöltése esetén: Első lépésben **[1]** a felhasználó megnyitja a weboldalt, vagyis a böngészőből egy HTTP kérést küld a megfelelő címre. Erre a kiszolgáló (hibamentes működés esetén) egy adott időn belül reagál és elküldi a kért HTML lap saját szerveren tárolt tartalmát **[2]**. Ekkor, ha valami még hiányzik, akkor azt a böngésző letölti a megfelelő további címről, vagyis esetünkben egy képet kér a harmadik fél szerverétől **[3].** Ezzel a kéréssel értesül az idegen szerver a felhasználó *IP céméről,*[6] a meglátogatott oldal URL céméről, valamint arról, hogy mikor hívta le a felhasználó az oldalt, és mindezt milyen típusú böngészővel tette. Az idegen szerver ezután a web bug céljától függően elvégzi a szükséges adminisztrációs tevékenységet **[4]**, például bejegyzést készít egy naplófájlba, vagy növel egy számlálót. Végül a kérést kiszolgálva megküldi az 1x1 pixeles képpontot **[5]**. A böngésző program legvégül összerakja és megjeleníti az elkészült oldalt. Tehát, ha valaki csak a legegyszerűbb web bug lehetőséget aknázza ki, akkor is azonosítani tudja, hogy egy buggal ellátott oldalt milyen időpontban, milyen személyek látogattak, anélkül, hogy az érintettek tudnának róla.



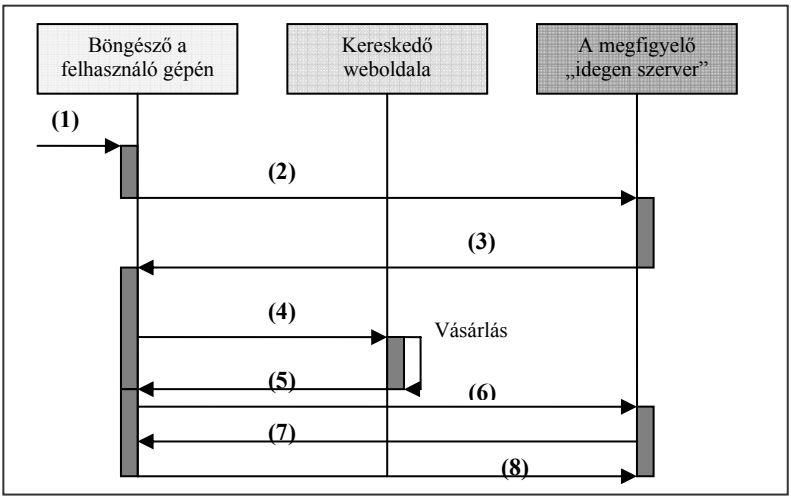
1. ábra: A web bug működési mechanizmusa

[6] A hálózati kommunikációban résztvevő, TCP/IP protokollt használó eszközök egyedi azonosítója.

Külön kell említeni a cookie-val összedolgozó web bugok működését. Ez azért fontos, mert a felhasználó azonosítása a gyakorlatban csak egy cookie segítségével lehetséges. De mi is valójában ez a cookie? Tulajdonképpen nem más, mint egy string, ami betöltődik a böngésző memóriájába. Létezésének célja, hogy dinamikát vigyen az egyébként állapotmentes HTTP protokoll által uralt világba. Állapotmentes esetben ugyanis minden látogatásunk ugyanolyan, mint az első, tehát a website nem jegyez meg rólunk semmit. A cookie-k teszik lehetővé azt az interaktivitást, és az egyéni beállítási lehetőségeket, amihez a jelenkor szörfözője már hozzászokott.

Felépítése egyszerű, pusztán négy paramétert tartalmaz: a cookie nevét (cookie name), egy értéket (cookie value), a lejárati időt (expiration date) és az érvényes elérési utat (path). A név és az érték egy-egy tetszőleges szöveges értéket tárolhat, például egy USERID-t, azaz felhasználó azonosítót. Fontos szerep jut a lejárati időnek is, mivel ettől függ, hogy a cookie elmentődik-e a merevlemezre későbbi használatra, vagy törlődik. Alapesetben csak a site-on tartózkodás ideje alatt él. Biztonsági szempontból azonban az elérési út a kritikus. Ugyanis csak olyan domainbe tartozó szerverek képesek kezelni a cookie-t , amelyek az elérési útban szerepelnek. Biztonsági okokból egy szerver mindig csak a saját domainjét állíthatja be, így csak a weblapot letöltő szerver és a vele egy domainben lévők képesek hozzáférni, idegen szerver nem. Itt lép képbe a web bug, ami képes cookie értéket átadni egy harmadik félnek, és ami még fontosabb, hogy a harmadik fél szervere, mivel a böngésző felvette vele a kapcsolatot, cookie-t küldhet a felhasználó gépére. Ezt pedig később lekérdezheti az idegen szerver, így amikor adatot szállít, a web bug felhasználóhoz tudja kötni a szerzett információt.

Példaként tekintsük azt az esetet, amikor egy reklámra kattintva a felhasználó egy kereskedelmi oldalra kerül, és ott vásárol valamit. Tegyük fel, hogy a felhasználó már betöltött egy tetszőleges oldalt, amin szerepel egy bizonyos reklám **(1).** A reklám betöltésénél a letöltésről egy web bug révén értesül az idegen szerver **(2),** és egy USERID-t tartalmazó cookie-t küld a felhasználó gépére **(3**). A reklámra kattintásnál a felhasználó átirányítódik **(4)** a kereskedő honlapjára. (Olyan megvalósítás is elképzelhető, ahol csak a reklámra kattintással kap cookie-t a felhasználó, ebben az esetben itt nincs szükség web bugra). Tegyük fel, hogy a vevő vásárol és fizet. Ezt követően megkapja a befizetést nyugtázó visszaigazolást **(5)**, amiben egy web bug található. A harmadik fél ezáltal értesül **(6)** a vásárlás adatairól. Ahhoz, hogy az így megszerzett adatokat hozzárendelhesse a megfelelő felhasználóhoz, lekérdezi a cookie eltárolt értékét **(7)**, amit a böngésző készségesen teljesít **(8)**. Így végeredményben az idegen fél képes megfeleltetni egymásnak a vásárolt árut és a vásárlót.



2. ábra: A web bug működési mechanizmusa cookie-val

Hogy ki a felelős a web bug elhelyezéséért, azt gyakran nem egyszerű meghatározni. Az esetek többségében a site tulajdonosa megállapodik egy elektronikus reklámozó céggel, aki reklámot és vele együtt web bugot helyez el az oldalakon. Mindezért valamilyen díjszabás szerint fizet a reklámozó cég. Ebben az esetben egyértelműen az oldal tulajdonosának a felelőssége állapítható meg, ha erről nem tájékoztatja a látogatókat. Azonban a Cyveillance felmérése[7] szerint többször előfordult, hogy a reklámmal együtt, kéretlenül kaptak bugot az oldalak, tehát a tulajdonosok tudomása nélkül. Hasonló helyzetbe került számos személyes honlappal rendelkező felhasználó, akik oldalaikat közösségi webkiszolgálókon helyezték el, ahol a tárhely ingyenessége fejében a lapok egy része felett a kiszolgáló rendelkezik. A kiszolgáló üzemeltetője ugyanis a reklámozóval kötött megállapodás részeként ezeken az oldalakon a reklám mellett web bugot is elhelyezett a laptulajdonosok tudta nélkül. Ilyen esetben a reklámozó és a tárhely szolgáltatója is jogellenesen jár el.

Mindezidáig nem esett szó a web bug egy másik megjelenési formájáról, az e-mailekben elhelyezett kémkedő képekről. Gyakorlatilag minimális különbség van a két típus között. Az e-mailes változat is egy HTML kódban írt címke, amely egy kép letöltését kéri. Mivel a legtöbb levelező program értelmezni tudja a HTML kódot, a már megismert eljárás ezek esetében is működik, az idegen szerver a kép kérésével jut információhoz a felhasználóról.

[7] S. Olsen: Web bug swarm grows 500 per cent, CNET News.com, http://news.com.com

Aggályra ebben az esetben az adhat okot, hogy az egyéni azonosításra alkalmas e-mail cím már eleve egy harmadik fél kezében van.

2. Kik és milyen céllal használják a web bugot?

A web bugot a hálózati kereskedelemmel, reklámozással és hirdetéssel foglalkozó cégek alkalmazzák. Hogy ez mennyire elterjedt manapság, azt jól mutatja az előbbiekben említett felmérés, amely szerint egymilliós mintát véve alapul 16 százalékos az elterjedtség, vagyis az 50 legismertebb webhelyből 8 alkalmazza. Egy további, a Security Space által készített jelentés[8] részletesen taglalja, hogy melyik 100 domain jár a legjobban a kis kémek terjesztésével. Köztük nem egy nagynevű domain is szerepel, mint a yahoo, a paypal, a homestead, a tripod, a lycos, a google, az amazon és az aol. A jelentésben közölt számadatokból az előfordulások jól látható növekedése olvasható ki. Míg 2002-ben a legnagyobb web bug terjesztő mintegy 8 245 site-ot „fertőzött meg", addig 2003-ra ez a szám már elérte a 22 857-et. A web bugok elterjedtségéről további információval szolgál a WebBug Locator,[9] valamint a Privacy Foundation honlapja,[10] ahol további, bizonyítottan web bugot használó cégek listáját teszik közzé.

Mi mindenre jó egy web bug? Az alábbiakban ezen lehetőségek közül kerül néhány bemutatásra. Azonban fontos kiemelni azt a tényt, hogy egy részük valóban csak felhasználási lehetőség, vagyis nem minden esetre létezik gyakorlati példa.

Felhasználhatóság szempontjából alapvető a különbség a cookie nélküli és a cookie-val együttműködő változat között. Cookie nélkül a felhasználók nyomon követése csak nagy nehézségek árán lehetséges, ezért a magányos web bugokat általában olyan ártalmatlan célokra használják, mint egy adott weboldalt látogatók számának mérése, a használt internet böngésző típusának vizsgálata, egy adott reklám (banner[11]) letöltésének számlálása, vagy reklám (banner)-kampány hatékonyságának mérése.

A cookie-val együttműködő web bugok az előbbieknél összetettebb feladatok elvégzésére is képesek, mint például on-line áruházban történő vásárlás és a vásárlásra rávezető banner párosítása, felhasználói profil összeállítása a látogatott weboldalak alapján, egyedi felhasználói profil összeállítása website-on belül látogatott témacsoportok alapján. Ilyen web bugok használhatók továbbá felhasználó által begépelt keresési sztringek továbbadására egy internetes marketing cégnek, a honlap látogatóival összefüggésben

[8] Security Space: Web Bug Report, 2003. szeptember 1. http://www.securityspace.com/

[9] V. Capello: Webbug Locator, 2000. http://www.elfqrin.com/webbug_locator

[10] R. M. Smiths: FAQ: Web Bugs , Privacy Foundation http://www.privacyfoundation.org

[11] Álló vagy mozgó reklámszalag (eredeti jelentése: zászló).

demográfiai adatok (nem, kor, lakhely) gyűjtésére, a látogatók személyes adatainak internetes marketing cégekkel való közlésére. E két utóbbi eset csak abban az esetben lehetséges, ha a felhasználó kitölt valamilyen űrlapot. Az űrlap adatmezőinek értéke kerül a cookie-ban eltárolásra, majd egy későbbi lekérdezés alkalmával jut hozzá az idegen szerver.

A cookie-val együttműködő web bug alkalmas lehet még cookie-k háttérben történő összehangolására, valamint annak megállapítására, hogy egy adott felhasználó elolvasott-e egy adott üzenetet — elsősorban a hirdetésekkel teli úgynevezett junkmail-t –, avagy sem. További felhasználási lehetőségek: a felhasználó levelező programjának tesztelése, a banner betöltések számlálása a hírlevelekben, valamint az egyes reklám üzenetek elolvasásának száma a usenet hírcsoportokban.

Összességében azt mondhatjuk, hogy a web bug sokoldalúan felhasználható az internetes marketing területén. Csak az egyszerűbb alkalmazások figyelembe vétele esetén is kijelenthető, hogy a web bug alapú nyomkövetés a hatékonysági, valamint nézettségi mérések fontos komponense.

Egy oldal látogatottságának mérése egyszerűen megoldható, ebből pedig kiszámolható, hogy egy-egy hirdetés hány emberhez jut el. Ennél jóval fontosabb felhasználási mód az, ha a web bug a vásárlásra vezető reklám azonosításában játszik szerepet. Ebben az esetben közvetlen következtetéseket lehet levonni arra vonatkozóan, hogy a reklámok mely reklámpozíciókban a leghatékonyabbak, ez pedig egy-egy kampány egésze szempontjából nagyfokú hatékonyságnövekedéshez, költségoptimalizáláshoz vezethet.

Alkalmazásának egy következő lépcsőfoka a web alapú kereskedelemben betöltött adatgyűjtési funkció. Tekintsünk egy webes áruházat, ahol a vásárló kiválasztja egy kosárba az általa megvételre szánt termékeket. A fizetéskor megjelenő visszaigazolás betölt egy web bugot, minek révén a vásárlás adatai bekerülnek egy adatbázisba. A hagyományos papír alapú és az elektronikus kérdőívek helyett, amelyeket a vásárlók idő vagy érdeklődés hiányában nem mindig a valóságnak megfelelően töltenek ki (vagy ki sem töltenek), a web bug kézenfekvő megoldást kínál. Pontos adatokat szolgáltat és a vásárló idejét sem rabolja. Tehát a web bugok révén olyan adatok kinyerése lehetséges, amelyekből vásárlási minták, vásárlási kosarak összeállítása lehetséges. Ez utóbbi műveletekhez viszont már összetett adatbányászati algoritmusok szükségesek.

A web bugok marketing célú felhasználásának csúcsát a személyre szabott reklámozás jelentheti, vagyis az, amelynek eredményeképpen a felhasználóról gyűjtött adatok alapján mindig csak a számára vélhetően érdekes reklámok kerülnének megjelenítésre az internetes felületen. Egy jól működő rendszer esetén még előnye is származhat ebből a

felhasználónak, például kevesebbet kellene keresgélnie keresővel, mert adott számú keresés után megjelenne a reklámablakban a hőn áhított (és véletlenül éppen leértékelt) árucikk. A kérdés az, hogy milyen áron válik elérhetővé mindez, vagyis mennyi információt kell kiszolgáltatnunk magunkról egy kis kényelemért cserébe. Lesznek olyanok, akik számára ez az „üzlet" elfogadható lesz, míg mások orwelli kémkedésnek bélyegezve visszautasítják majd. A dolgot a másik oldalról megközelítve elmondható, hogy bár a marketing hatékonyságának újabb ugrásszerű növekedését jelentené, mégis a rendszer működtetéséhez szükséges erőforrások beszerzése és karbantartása óriási költségekkel járna. Követni minden egyes felhasználó útját, naplózni azt, hogy hol járt, az egyes helyeken mennyi időt töltött, rendszeresen jár-e oda vagy csak alkalmi esetről van szó, mindez hatalmas háttértár igénnyel és intenzív kommunikációval járna. A másik gondot a felhasználó egyértelmű azonosítása okozza. Igaz ugyan, hogy lehetséges egy cookie-ban tárolt egyedi azonosítóval követni valakit több site-on keresztül (cross-site tracking), de ehhez egyrészt minden site-nak ugyanazon reklámozó részére kellene adatot szolgáltatnia, másrészt ez csak a cookie élettartamának idején belül lenne lehetséges, hiszen annak lejártával vagy — valamely hiba következtében történő — törlődésével elveszne az azonosításra szolgáló információ, hacsak nem frissítené fel a reklámozó időben. Elméletileg az esetek egy részében megoldható az újraazonosítás az IP cím alapján, ám ez semmiképpen sem jelent optimális megoldást. A jelenlegi webes megoldások mellett tehát egy ilyen rendszer nagy valószínűséggel nem lenne annyival hatékonyabb, mint amennyivel a megvalósítása költségesebb.

3. A web bugok gazdasági jelentősége

Hogy valójában mekkora a web bug gazdasági jelentősége, azt jól mutatja az egyik gyakorlati alkalmazása, a HitBox[12] technológia, amit az 1996-ban alapított WebSideStory cég fejlesztett ki. Ez voltaképpen egy web bug és cookie együttesén alapuló megoldás, amit a cég 2002-ben sikeresen szabadalmaztatott. Mára havi 30 milliárd tranzakcióval és évi 4 millió elemzésével piacvezetővé vált. A siker titka kettős, egyrészt a HitBox reklámkövetési és számlálási módszerében, másrészt a begyűjtött adatok hatékony elemzésében rejlik.

A reklám bannerek követésére világszerte több különféle technológiát alkalmaznak. Bár az *IAB*[13] illetve az *IFABC WWW*[14] komoly erőfeszítéseket tett az egyes megoldások tökéletesítésére és egy egységes szabvány bevezetésére, ez mindezidáig nem valósult meg.

[12] A HitBox® a WebSideStory Inc. bejegyzett védjegye.
[13] Interactive Advertising Bureau.
[14] Federation of Audit Bureaux of Cirulations WWW.

Így a létező szabványok között zajlik a verseny, amelyek közül az egyik leghatékonyabb a HitBoxon alapuló Marketing ROI tracking.[15]

Ez egy összetett módszer, és ehhez mérten több információ is nyerhető vele. Az alapját egy CGI script képzi, amely a beérkező kérést kezeli, amikor a felhasználó egy reklámra kattint, és megérkezik a site-ra. Első lépésben a script az URL-ből megállapítja, hogy melyik reklám volt a kiindulási pont, és ezt az azonosítót elhelyezi a felhasználó gépén egy cookie-ban. Ezután a site megfelelő pontjára irányítja a felhasználót és beilleszti az oldal kódjába a HitBoxot, ami tartalmazza a reklám azonosítóját. Ezt követően az azonosító a cookie-ból bármely lapon beolvasható és az oldal betöltésekor egy web buggal elküldhető a nyomon követő szerverére, ezáltal pedig lehetővé válik a felhasználók mozgásának követése.

A más módszereknél gondot okozó web spiderek és botok[16] a HitBox esetében nem okoznak problémát, ugyanis ezek a mesterséges forgalmat keltő programok nem töltik le a képeket, így nem aktiválják a web bugot sem. Az átirányítás közben kilépő felhasználók pedig nem számítanak, ugyanis ez esetben nem töltődik be sem az oldal, sem pedig a web bug. Ezen tulajdonságok így jelentős előnyhöz juttatják ezt a módszert versenytársaival szemben.

A HitBoxon alapuló analízis a hagyományos naplófájl-analízishez képest a begyűjtött adatok elemzése terén is számos előnnyel rendelkezik. A hagyományos módszer esetében a szerver által tárolt, nagy terjedelmű, nem emberi áttekinthetőségre tervezett adathalmaz vizsgálatát kell lebonyolítani. Jellegéből fakadóan valamilyen elemző szoftver szükséges hozzá, aminek természetesen anyagi vonzata is van. Maga az elemzés idő- és erőforrás-igényes, ebből fakad a legnagyobb hátránya, hogy az így elkészült jelentés nem a pillanatnyi állapotot mutatja. Ezzel szemben a HitBox módszer esetében a forgalmi adatok nem az adott website-ot kiszolgáló szerveren kerülnek eltárolásra, hanem a web bug révén egy harmadik fél, a WebSideStory szerverén. Az elemzés valós időben történik, így a pillanatnyi állapot bármikor hozzáférhető. Nem szükséges hozzá külön szoftver és nagy számítási kapacitás. További előnye ennek a módszernek, hogy figyelembe veszi a manapság elterjedt weboldal *cachelés*t.[17] Ha a hagyományos módon a site-ot kiszolgáló szerver készít egy naplófájlt, akkor abban nem szerepelnek majd azok a felhasználók, akik

[15] ROI: Return On Investment — befektetés megtérülés.

[16] Olyan automatizált programok, melyek feltérképezik a weboldalak tartalmát általában valamelyik kereső program részére. Mivel nem emberek, nem szabad, hogy ott jártuk beleszámítson a látogatók számába.

[17] Hálózatok és kiszolgálógépek terhelésének csökkentését szolgáló eljárás, melynek lényege, hogy egyes weboldalakról másolatokat készítenek és azokat a világ számos pontján lévő speciális gyorsító (tároló) szervereken helyezik el.

az oldalt proxy szerverről[18] töltötték le, míg a HitBox módszer esetén a web bug így is, úgy is letöltődik, tehát valós képet ad a látogatók számáról.

A web bugot alkalmazó elemzési technológia fölényét a hagyományos naplófájl elemzéssel szemben számos gyakorlati kísérlet is bizonyítja. Az egyik ilyen kísérlet szerint a naplófájl analízis tévesen, nagyjából négyszer annyi találatot regisztrált, mint a HitBox megoldás. Ennek felderített okai között szerepel a HTML-keretek okozta eltérés, a botok és web spiderek által generált forgalom, melyekre az utóbbi módszer immunis.

4. Biztonsági kérdések

A web bug a legtöbb esetben szimpla számláló egységként működik, ami semmiféle személyes adat kezelésével nem jár együtt. Többnyire maguk a bannerek tartalmazzák, ahova maguk a hirdetők helyezik el azt. Célja általában annak az ellenőrizése, hogy egy adott hirdetést valóban annyian láttak-e, mint amennyit a website tulajdonosa állít. A web bug ily módon egy belépőket számoló forgóajtóhoz hasonlít.

Nem hagyható figyelmen kívül azonban, hogy web bugként gyakorlatilag bármilyen grafika, sőt tetszőleges link is felhasználható. Minden esetben, amikor szöveg- vagy képletöltés történik egy szerverről, sor kerül az összes olyan információ összegyűjtésére, ami az első fejezetben bemutatásra került. Ezek szerint a bugoknak önmagukban semmilyen különleges erejük nincs, azonban ha együttműködnek egy cookieval, akkor adatvédelmi szempontból veszélyes dolgokra is képesek.

Tekintsük a lehetséges legrosszabb lehetőséget, ami egy web bug segítségével elkövethető. Ebben az esetben előzőleg bevitt személyes információ kerülhet egy harmadik félhez. A kulcsszó az előzőleg bevitt, ugyanis a web bug nem képes átkutatni egy rendszert olyan információ után, amit a felhasználó nem szándékozik megadni, és később sem küldi el azt titokban egy külső forrásnak. Ahhoz, hogy a baj bekövetkezzen, a felhasználónak önként kell megadnia az adatokat egy rossz szándékú site-nak. Némi óvatossággal azonban elkerülhető a baj. Olyan website-ok esetén, amelyek személyes információ megadását kérik, ajánlott elolvasni az adott site privacy policy-jét,[19] azaz személyesadat-kezelési irányelveit. Amennyiben ez tartalmaz olyan kitételt, miszerint a személyi azonosításra

[18] Több feladatot ellátó segédszerver, melynek egyik funkciója lehet bizonyos weboldalak másolatainak a tárolása, ezáltal gyorsítva a hozzáférést.

[19] A website a privacy policyban (személyesadat-kezelési irányelv) tájékoztatja a felhasználót arról, hogy adatait milyen szabályok szerint kezeli. Kötetünkben külön tanulmányok foglalkoznak a privacy policy témájával.

alkalmas információ megosztásra kerül üzleti partnerekkel, akkor valóban komoly veszélyt jelent az adatok megadása.[20]

Ahhoz, hogy a web bug segítségével személyes információk tényleges kezelésére kerüljön sor, a felhasználó közreműködése is szükséges. A marketing cégek nagy örömére az egyszerű felhasználó nagyon könnyen belesétál a legnyilvánvalóbb csapdákba is. Klasszikus példa a hírlevél regisztrálás esete, ahol mindig feltesznek egy olyan kérdést, hogy akar-e a felhasználó más izgalmas, érdekes ajánlatokat kapni a hírlevél mellett. Egy rossz kattintás, és a személyi azonosításra alkalmas e-mail címét máris elnyeli a marketing labirintus, s ezt követően kéretlen levelek százai bombázzák e-mail fiókját.

A biztonsági kockázatok számításánál különbséget kell tenni az adatbiztonság terén tudatos és az átlagos felhasználó között. A tudatos felhasználó számára a web bug minimális kockázatot jelent, akár cookie-val, akár anélkül. Amennyiben körültekintően bánik személyes adataival, és még letiltja a harmadik féltől származó cookie-kat is, akkor számára jogosan tűnhet a web bugoktól való félelem — Fred Langa IT biztonsági szakértő szavaival élve — „a tömeghisztéria egy formájának, amely a valós kockázattól nagyon távol van."[21] Valóban, e feltételek mellett a legérzékenyebb adat, amit egy web bug kifürkészhet, az az IP cím. Ez azonban nem a felhasználót azonosítja, hanem a gépet. Másrészt nem mindenki rendelkezik fix IP címmel, de ha mégis, és el akarja rejteni, akkor erre számos lehetőség kínálkozik. Vagyis annak az esélye, hogy egy website valakit csupán az IP cím alapján nyomonkövessen, minimális.[22] Aggodalomra az ad okot, ha egy az internetes marketing veszélyeire kevésbé felkészült felhasználó kerül szembe a web buggal. Mit sem sejtve arról, hogy milyen folyamatok zajlanak a háttérben, információt szolgáltat magáról mindenütt, ahol erre kérik. Egy ilyen felhasználó számára a web bug komoly kockázati tényező, bár itt is igaz, hogy nem önmagában a bug a veszélyes, hanem az adatok meggondolatlan kiszolgáltatása.

[20] A privacy policy sem feltétlenül nyújt megnyugtató megoldást, hiszen sok esetben nincs az oldalon privacy policy, vagy ha van is, nem tájékoztat a web bugok jelenlétéről. A BackcountryStore.com weboldala például alkalmazza a WebSideStory HitBox technológiáját. Ez utóbbi cég website-ján többszörösen is felhívják a figyelmet arra, hogy a HitBox technológiában web bugot alkalmaznak, és a klienseiktől is elvárják, hogy közzé tegyék ezt oldalaikon. A BackcountryStore.com oldalon azonban, bár szó esik cookie alapú adatgyűjtésről, a web bugot még csak meg sem említik.

[21] F. Langa: The Web-Bug Boondoggle, Information Week, 2001. jún.25. http://www.informationweek.com

[22] Ennek ellenére az EU adatvédelmi munkacsoportja (Article 29 WP) és a magyar adatvédelmi biztos is személyes adatnak tekinti az IP címet.

5. Védekezési módszerek

Az a kérdés, hogy érdemes-e bármilyen külön védekező intézkedést tenni a web buggal szemben, függ a felhasználó felkészültségétől. Tudatos felhasználók számára az egyéb óvintézkedések betartása mellett nagy valószínűséggel nem lesz rá szükség, míg mások esetben indokolt lehet.

Alapvetően kétfajta védekezési módszer között tehetünk különbséget, létezik ad hoc és szoftveres módszer. Az előbbi esetben a böngésző különféle beállításaival érhető el a web bug részleges vagy teljes kivédése, míg az utóbbi esetében valamilyen speciális szoftver segítségével detektálhatjuk vagy blokkolhatjuk a web bugot.

A web bug felfedezésének legegyszerűbb — ad hoc — módja az oldal kódjának analizálása. Ennek ugyanis tartalmaznia kell az idegen szerver URL-jét is. E módszer hátránya, hogy a kép címkék azonosítása ugyan egyszerű, a scriptben elrejtett web bugok feltárása viszont már nem az. További hátrány, hogy az átlagos felhasználótól nem várható el, hogy weboldal kódot ellenőrizzen annak érdekében, hogy megbizonyosodjon az oldal biztonságáról, ha egyáltalán van annyira jártas e témában, hogy ez a kérdés benne felmerüljön.

A következő — a bonyolultság tekintetében a második lépcsőfokot jelentő — módszer a böngésző opcióinak a megfelelő beállítása. Ehhez az adott böngészőprogram (gyakran alapos) ismerete szükséges. A web bugok veszélyességét nagyban lecsökkenti, ha részben vagy teljesen blokkoljuk a cookie-kat. Részleges blokkolás esetén a harmadik féltől származó *cookie*-kat[23] blokkolja a rendszer, a többi érintetlen marad. Ez azonban könnyen kijátszható, ha a meglátogatott weboldal és a megfigyelő szerver azonos domainben található. Teljes blokkolás estén viszont a jóindulatú cookie-k sem működnek, így az internet nyújtotta számos szolgáltatás csak részlegesen vagy egyáltalán nem működik. Mindezzel azonban csak a web bug segítőtársa iktatható ki, maga a kém nem, tehát a látogatásunk helye, időpontja valamint IP címünk ebben az esetben is idegen kézbe kerül.

A következő, az előzőeknél drasztikusabb megoldás a képek betöltésének teljes letiltása. Ennek hátránya, hogy az internet használata közben egyetlen kép sem fog betöltődni. Ez a mai, vizuális megjelenítésre koncentrált webtartalom korában igen komoly hátrány. További probléma, hogy léteznek nem kép alapú web bugok is, amelyekre ez a tiltás nincs

[23] Más néven third party cookie: a weblaptól eltérő, azaz nem látogatott domainből származó cookie.

hatással. Összességében elmondhatjuk, hogy az ad hoc módszerek nem kellően hatékonyak a web bugok megfékezésében.

A szakszerű szoftveres megoldásokat két nagy csoportra lehet osztani. Az első típusba tartoznak a bugdetektáló programok, míg a másikat a különböző reklám- és spamszűrők alkotják. A bugdetektálók — nevükhöz híven — a web bugok azonosításában játszanak szerepet.[24] Hátrányuk, hogy pusztán a web bug jelenétére hívják fel a figyelmet, a működését megakadályozni nem tudják. Az átlagos felhasználó számára azonban megfelelnek arra, hogy felkeltse a figyelmét egy potenciális biztonsági veszélyre. Az pedig már a felhasználó egyéni érzékenységén múlik, hogy hogyan reagál egy-egy riasztásra.

Ennél hatékonyabb megoldást spam, illetve reklámszűrők nyújtatnak,[25] amelyek a weboldalak betöltése előtt analizálják azok kódját, és letiltják a nem kívánatos elemek letöltését. Ezek segítségével a web bugok is blokkolhatók.

6. Privacy és a web bug

A web bugok alkalmazásának számos módja közül egyesek nem jelentenek veszélyt a felhasználóra nézve, azaz nem sérülnek személyiségi jogai. Ebben az esetben az elhelyezett poloskák csupán hatékony, láthatatlan segédeszközök. Ám mások komoly visszaélésre adnak lehetőséget. Az alábbi megtörtént eset azt mutatja, hogy a web buggal kapcsolatos etikai aggályok nem csupán a jogvédők képzelgései, hanem sajnos valós alappal rendelkeznek.

2000 nyarán nagy felháborodást keltett Robert O'Harrow cikke, amelyben feltárta, hogy egy bostoni cég a gyógyszergyártó vállalatok részére készített feljegyzéseket a honlapjaikat látogatók tevékenységéről.[26] A Pharmatrak Inc. több ezer egészségüggyel, gyógyszerekkel és betegségekkel foglalkozó oldalon figyelte meg a felhasználókat és szolgáltatott róluk adatokat tizenegy gyógyszergyártó részére. A cég által kifejlesztett web bug és cookie alapú szoftver segítségével megállapítható, milyen információkat tölt le gyakran ugyanaz a gép, vagyis például töltött-e le ismertetőt a HIV-ről vagy az ellene alkalmazható terápiákról. A Pharmatrak szerint a szörfözők szokásainak a vizsgálata pusztán arra szolgál, hogy segítsék a gyógyszergyártókat a keresletnek megfelelő website-ok kialakításában, és hogy minél nagyobb áttekintést nyújtsanak arról, hogy hogyan viselkednek a website-juk látogatói a többi, konkurens oldallal összehasonlítva. Állításuk szerint nem gyűjtenek

[24] E kategóriába sorolható például a Privacy Foundation ingyenes, Bugnosis nevű diagnosztizáló programja.

[25] Ilyen komplex szoftver például a Privacy Foundation által ajánlott Guidescope, a WebWasher vagy az AdSubtract.

[26] R. O'Harrow: Firm tracking Consumers on Web for Drug Companies, *Washington Post,* Page E01, 2000. aug.15. http://www.washingtonpost..com

neveket, de azt azért meg tudják állapítani, hogy egy látogató fogyasztó, orvos, újságíró vagy tisztségviselő, abból, hogy honnan jött és mit nézett meg. Ugyanakkor azt is bejelentették, hogy a jövőben egy olyan szoftver elkészítését tervezik, amely úgy gyűjt adatot, hogy egy követési adatbázissal összevetve lehetővé teszi egyes egyéni látogatók azonosítását. Az ember egészségügyi állapotára vonatkozó adatok az érzékeny személyi információk közé tartoznak, ezért többen jogosan megengedhetetlennek tartották a Pharmatrak vezetőségének ezt az elképzelését.

Az ügyet tovább súlyosbította az a tény, hogy sem a Pharmatrak, sem a szolgáltatásait igénybevevők nem tettek közzé semmiféle tájékoztatást arról, hogy adatot gyűjtenek. Michigan állam főügyésze vádemelés előtti utolsó felszólításban részesítette a Pharmaciá-t, a Pharmatrak egyik megbízóját, hogy szüntesse be jogellenes magatartását. Válaszlépésként a cég kitette weboldalaira a privacy policyt, ellenben a Pharmatrak konkrét működéséről továbbra sem tájékoztatta a közönséget. Ugyanilyen felszólításban részesült az Ortho Biotech vállalat, amely HIV/AIDS, valamint a rák különféle gyógykezeléseit bemutató oldalain helyezett el web bugot, amin keresztül a DoubleClick gyűjtött információkat.

Ezen kívül számos esetben történt visszaélés a web bug technológia nyújtotta megfigyelési lehetőségekkel. Emiatt több személyiségi jogokat védő szervezet folytatott kampánytevékenységet a web bugok használatának megfelelő korlátok közé szorításáért. Közülük a Privacy Foundation tette meg a legnagyobb lépést azzal, hogy kidolgozott egy szabályozási tervezetet, amit 2000. szeptember 13-án ismertetett a Global Privacy Summit (Washington D.C., 2000.) alkalmával.

Később, több mint negyven szervezetnek — internetes hirdető cégeknek, e-mail hirdetőknek, a Federal Trading Committee-nek, valamint az internet szabványosító szervezeteknek — küldte el tervezetét. Ez az alábbi irányelveket tartalmazta :

1. A web bugot egy látható ikonnal kell megjeleníteni a képernyőn.
2. A web bugot elhelyező cég neve az ikon segítségével legyen azonosítható.
3. Az ikonra kattintva a felhasználó jusson hozzá a web bugot érintő információkhoz, úgymint:
   – milyen adatot gyűjt a web bug;
   – hogyan használják fel az összegyűjtött adatot;
   – milyen céghez vagy cégekhez kerül az adat;
   – milyen más adatokkal egyeztetik;
   – kapcsolódik-e cookie a web bughoz.

   Ez a tájékoztatás része lehet a privacy policy-nak vagy egy külön a web bugok használatát leíró nyilatkozatnak.

4. A felhasználónak mindig legyen lehetősége visszautasítani (opt-out[27]) bármilyen web bug által végzett adatgyűjtést.
5. A web bugokat ne lehessen felhasználni személyes információk gyűjtésére az „érzékeny szférába tartozó" oldalakról, úgymint:
   – gyermekeknek szánt oldalak;
   – egészségügyi állapotot érintő oldalak;
   – pénzügyi és állásügyi oldalak.

Hiába készült el a tervezet 2000-ben, nem követte hivatalos válasz egészen 2002-ig. A civil szervezetek, valamint a hatóságok nyomására a hirdetési szakmát képviselő NAI[28] kiadott egy átfogó dokumentumot, amelyben rögzítette a web bugok felhasználásának irányelveit.[29] Ez azonban elég messze állt attól a megoldástól, amit a jogvédő szerveztek javasoltak, mert az elektronikus kereskedelemmel és marketinggel foglalkozó cégek által preferált opt-out megközelítést juttatták érvényre, míg a személyiségi jog védői az opt-in[30] szemléletet akarták elfogadtatni.

A NAI dokumentuma bemutatja, hogy szerinte milyen részeket kell kötelezően tartalmaznia a web bugok használatáról szóló tájékoztatónak.

- A felhasználóval tudatni kell a web bugok használatának tényét.
- Ismertetni kell a web bugok használatának célját.
- A felhasználó tudomására kell hozni, ha személyi azonosítására alkalmas adatot gyűjtenek róla.
- Nyilatkozni kell arról, hogy az összegyűjtött adatot megosztják-e egy harmadik féllel.
- Tájékoztatni kell a felhasználót arról, ha az oldal üzemeltetőitől vagy harmadik féltől származó e-mailben web bugot helyez el.
- Ha a felhasználóról gyűjtött személyes azonosításra alkalmas adat megosztásra kerül egy harmadik féllel, akkor a felhasználónak meg kell adni a lehetőséget annak elutasítására (opt-out) abban az esetben, ha más céllal kerül felhasználásra, mint amiért eredetileg begyűjtötték.
- Ha a web bug egy felhasználóról érzékeny adatot továbbít egy harmadik félnek, akkor a felhasználó engedélyét kötelező kikérnie (opt-in).

[27] Opt-out — opting out: Lehetőség egy adott szolgáltatás lemondására/megszüntetésére.
[28] Network Advertising Initiative — Hálózati Hirdetési Kezdeményezés.
[29] NAI : Web beacons — Guidelines for Notice and Choice http://www.networkadvertising.org/
[30] Opt-in — opting in: A felhasználó közvetlen engedélyéhez kötött.

Ezek az irányelvek láthatóan azt a célt tűzték ki, hogy az online hirdetés hatékony maradjon. Részben tiszteletben tartják a felhasználók személyiségi jogait, de közel sem oly mértékben, mint ahogy azt a jogvédők tervezték. A NAI 2001 májusában kérte az irányelvek átvizsgálását az Federal Trading Commitee-től (Szövetségi Kereskedelmi Tanács). A bizottság szakvéleményében a szabványokhoz illeszkedő opt-out szemléletet támogatta, így elfogadta a javaslatot. Ennek megfelelően a NAI tagjainak álláspontja győzedelmeskedett a privacy jogvédőkével szemben. Ezt követően csak 2002 novemberében hozta nyilvánosságra a NAI az irányelveket.

Összehasonlítva azt, hogy mi valósult meg a NAI irányelveiben, és mit tartalmazott a Privacy Foundation eredeti tervezete, eléggé vegyes érzelmekkel nyilatkozhatunk. Az irányelvek azt jelzik, hogy megtörténtek a kezdő lépések a jó irányba, ám közel sem beszélhetünk teljes átlátszóságról, ha csak nem a web bug láthatatlanságáról van szó. Erről ugyanis nem esett szó az irányelvekben, pedig ez lett volna talán a legfontosabb. A bugot jelző kép nélkül az egyszerű felhasználó ezután sem fogja a megjegyzéseket keresve átvizsgálni az oldalakat, és nem fogja elolvasni minden egyes site privacy policyjét a web bugok alkalmazása után kutatva. Találóan azt mondhatjuk: hogyha nem jelez a fénysorompó, nem fogjuk megnézni, hogy milyen vonat jön.

Mindezek alapján kötelező információt nyújtani a web bug alkalmazásáról, pontos céljáról és arról, ha személyes információt osztanak meg harmadik személlyel, de arról, hogy pontosan kihez kerül és milyen célból, már nem. A másik érdekesség az, hogyha a website saját felhasználásra gyűjti az információt, azaz nem osztja meg egy harmadik féllel, akkor nem köteles (legalábbis a lefektetett elvek alapján) opt-outot, azaz visszautasítási lehetőséget biztosítani. Ez viszont ismét egy olyan kiskapu, amivel adott esetben vissza lehet élni. Ezek alapján a mindenkori opt-out lehetőség sem teljesül. Az utolsó pont szintén csak részlegesen valósult meg. Míg a Privacy Foundation azt kívánta elérni, hogy az érzékeny természetű adatokat egyáltalán ne lehessen begyűjteni, addig a NAI elvek ezt lehetővé teszik a felhasználó beleegyezésével (opt-in). Ezzel még talán nem lenne gond, ha nem lenne itt is egy kis kibúvó. Vagyis az opt-in csak akkor kötelező, ha harmadik féllel is megosztja a site az adatot. Ezek alapján az eredeti website tetszőlegesen, beleegyezés nélkül is gyűjthet személyes adatot, ami adott esetben jogi sérelmekhez vezethet.

Összességében elmondható, hogy a jogvédők javaslata és a gyakorlatban megvalósított elvek között jelentős különbség tapasztalható. Míg az előbbi egyértelműen a felhasználók érdekeit tartotta szem előtt, addig az utóbbi láthatóan az üzleti érdekeket szolgálja inkább. Ez abból a szempontból érthető, hogy mára a web bug az internetes marketing egy jelentős elemévé vált, alapvetően befolyásolva a hatékonyságot. Az érdekeltek vélhetően tartottak attól, hogy a bugok látható képpel való jelölése nem segítené elfogadásukat, inkább csak

sokkolná a látogatókat. Pedig a jelenlegi irányelvek szigorítása, elsősorban az érzékeny adatok gyűjtése és megosztása terén, a web bugok kockázati szintjét a jelenleginél jóval elfogadhatóbb szintre csökkentené, és könnyítené jelenlétük elfogadását.

7. Jogi szabályozás

A 2003 januárjában az USÁ-ban végül érvénybe lépett az új online privacy védelmi törvény,[31] ami a NAI elvek általánosított változatát tartalmazták. Az egyetlen különbség az, hogy a törvény szerint a felhasználó kérésére a szolgáltatónak tájékoztatást kell nyújtania arról hogy pontosan milyen típusú információt adott el illetve osztott meg más cégekkel. Ez a kötelezettség azonban nem terjed ki arra az esetre, ha a cég saját felhasználásra gyűjti az adatokat. Ebből látható, hogy a törvényben nagy előrelépés nem történt.

Mindezidáig az USÁ-ban alkalmazott irányelvekről, valamint egy törvényről esett szó. Érdemes azonban említést tenni az Európai Unió elektronikus privacy irányelvéről.[32] Az EU már 1998-ban lépéselőnyben volt a privacy védelme terén, azóta is fokozatosan fejlődik, és fejlettebb, mint az USÁ-ban. A különbség olyan szignifikáns volt, hogy az EU 1998-ban hatályba lépett adatvédelmi irányelve[33] első lépcsőjében a többi nem EU-s országgal együttesen az USÁ-t is a „nem megfelelő adatvédettségi szintet" nyújtó államok közé sorolta. Mivel az EU az irányelvben megtiltotta az adatforgalmazást minden olyan nem uniós tagállamba, amelynek törvényei nem biztosítanak megfelelő védettséget az adatoknak, ez azt jelentette volna, hogy az USA-beli vállalatok, szervezetek nem folytathatnak adatcserét az EU-n belül működő partnereikkel. Hosszas tárgyalások révén azonban megkötötték az úgynevezett „Safe Harbor" megállapodást, amivel — legalább is névlegesen — szavatolták az amerikaiak az adatok EU irányelveknek megfelelő szintű védelmét. Eszerint azok a szervezetek, amelyek az EU elvárásainak megfelelő önszabályozást valósítanak meg, folytathatnak adatcserét Európai Unión belüli partnereikkel.

A 2002 májusában elfogadott EU anti-spam és privacy irányelv sokkal markánsabban veszi védelmébe a felhasználók jogait, mint a már ismertetett újabb 2003. évi amerikai törvény. Az irányelv egyik legfontosabb eleme, hogy a website-on kötelező tájékoztatni a felhasználókat arról, hogy pontosan milyen cookie-kat használ és milyen célból. Emellett megadja a jogot a felhasználónak ahhoz, hogy bármilyen cookie-alapú adatgyűjtést

[31] Online Privacy Protection Act of 2003 [H.R.69,07/01/03].

[32] Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector.

[33] EC Directive 95/46 on the protection of individuals with regard to the processing of personal data and on the free movement of such data.

visszautasítsanak. Ez a jogvédőknek jó hír, hiszen a felhasználók követésére alkalmas web bugok voltaképpen mindig egy cookie-val játszanak össze. Ez az irányelv így épp a méregfoguktól fosztja meg a őket, így vetve véget az etikailag megkérdőjelezhető megfigyeléseknek.

Az irányelv másik újdonsága, hogy az e-mail alapú marketing tevékenységet opt-in metódushoz köti. Ez megsemmisítő csapás a kéretlen e-mailes web bugok számára, hiszen a reklámozónak először ki kell kérnie a felhasználó engedélyét a kereskedelmi célú levelek küldéséhez. Ekkor viszont tájékoztatnia kell arról, ha ő maga vagy egy harmadik fél web bugot helyez el benne. Ha összevetjük ezt a 2003. évi amerikai anti-spam törvénnyel,[34] akkor ismét csak azt tapasztaljuk, hogy a tengerentúlon a törvényhozás inkább a reklámozóknak kedvez, mivel az ottani szabályozásban az opt-out hozzáállás valósult meg.

Egy pillanatnyi kitérőt téve a magyar jogi szabályozásra, elmondhatjuk, hogy az összhangban van az EU irányelveivel. Már a csatlakozásnál jóval előbb, 2000-ben megkapta Magyarország az EU-tól az úgynevezett „adekvát" státust, amelyet megelőzött az *Európai Tanács adatvédelmi konvenciójának*[35] magyar részről történő ratifikálása. Ennek függvényében érthető, hogy a magyar *elektronikus kereskedelmi törvény*[36] is tiltja a kéretlen reklámot tartalmazó üzeneteket, vagyis csak opt-in jelleggel, a felhasználó beleegyezésével engedélyezettek.

Összegezve az a következtetés vonható le, hogy a web bugok által keltett aggályok feloldására, valamint általánosságban az online privacy problémáinak megoldására minőségileg jobb lépéseket tettek az EU irányelvei, mint az USA törvényei. Az előbbi nagyobb beleszólást enged a felhasználó számára, saját adatai védelmének érdekében. Kiemelendő, hogy a szigorúbb EU előírások nem gátolják a „jótékony" web bugok használatát, így változatlanul fontos szerepet játszhatnak a forgalomanalízisben.

8. Létezik-e „jó" web bug?

Ennek megítélése szubjektív dolog, hiszen a marketing szemszögéből a jelenleg használatos bugok is jók. Éppen ezért itt mindenképpen szükséges annak kimondása, hogy nem a web bug az, ami jó vagy rossz, hanem a felhasználásának a célja. Ez alapján „jó" web bug az, amelyik úgy fejti ki tevékenységét, hogy eközben semmilyen jogi, erkölcsi sérelmet nem

[34] Anti-Spam Act of 2003 [H.R.2515].

[35] Convention for the protection of individuals with regard to automatic processing of perdonal data, Council of Europe, Strassbourg, 1981. január 28. European Treaty Series No. 108.

[36] Az elektronikus kereskedelmi szolgáltatások, valamint az információs társadalommal összegfüggő szolgáltatások egyes kérdéseiről szóló 2001. évi CVIII. törvény.

okoz a felhasználóknak. Ez már egyértelműen kizárja a marketing célokra alkalmazott web bugok többségének említését.

Léteznek azonban más alkalmazási területek, amelyeknél szintén jelentős pozíciót tölthetnek majd be a web bugok, bár igaz, hogy e felhasználási módok még nem kiforrottak. Ezek között két jelentős terület az online biztonság és az online mikrofizetés.[37]

A web bugok biztonsági alkalmazására már létezik gyakorlati megvalósítás, mégpedig a Microsoft jóvoltából. A webes szerverén lévő korlátozott hozzáférésű területeket védi ezzel a technikával. Mindez úgy működik, hogy a védett oldalakon web bugot helyez el, aminek betöltésekor értesül a szerver arról, ha valaki az őrzött területre lép. Ekkor megvizsgálja a cookie-ban eltárolt azonosítót, és leellenőrzi, hogy a felhasználó megfelelő jogosultsággal rendelkezik-e. Nemleges esetben megteszi a szükséges lépéseket a behatoló eltávolítására. Ezzel a módszerrel az is megvizsgálható, hogy a felhasználó a megfelelő IP tartományból vagy címről jelentkezik-e be. Ennek a megkötésnek lehetnek biztonsági okai, például érzékeny céges információt ne töltsön le a felhasználó bárhonnan, csak a munkahelyéről, ahol megfelelő védelmi vonal van kiépítve. Ugyanez a technika segítséget nyújthat egy-egy eltulajdonított (kalózmásolat) dokumentum terjedésének nyomon követésében, esetleg a konkrét tettesek kézre kerítésében. E módszer hátránya, hogy alapvetően arra épít, hogy nem számítanak rá. Ebből kifolyólag egy felkészült szakembernek nem jelenthet nehézséget a hatástalanítása.

A biztonsági területtel szemben a web bug, mint mikrofizetési segédeszköz még csak egy elképzelés, amelynek még nem létezik gyakorlati alkalmazása. Ennek okai elsősorban a mikrofizetéssel fellépő gondok miatt adódnak. A webtartalomért való fizetés legnagyobb problémája a webes interakció sajátos voltából fakad A szörfözés gyorsasága és anonimitása megnehezíti egy gyorsan működő, biztonságos rendszer kiépítését. Másrészt az internet egy hatalmas erőforrás, melynél a webtartalmat egymástól független emberek milliói birtokolják, és szintén emberek milliói veszik igénybe, vagyis egy egységes fizetési rendszer felállítása komoly problémákba ütközne. Mindezek mellett a jelenlegi legnagyobb nehézség abból adódik, hogy a mikrofizetés alapját képző nagyon kis összegű befizetések gazdaságilag nem kifizetődők, mert a fizetés tranzakciós költségei a jelenlegi eszközökkel túl magasak. Ahhoz, hogy ebből az elképzelésből egy működőképes rendszer jöjjön létre, még sok gyakorlati próbát kell kiállnia, és ezek végeredményétől függ, hogy hosszútávon is életképes marad-e.

[37] Alacsony tranzakciós költségű kisösszegű online fizetési mód.

9. Végszó

A web bug tehát nemcsak a felhasználók magánéletének kifürkészése céljából bevetett fegyver lehet. Bár még mindig tapasztalható ilyenfajta használata, a jogi szabályozások révén megindult egy konszolidációs folyamat. A végcél az, hogy a bugok használata úgy maradjon gazdaságilag hatékony, hogy közben a felhasználók jogait ne sértse. A Privacy Foundation által javasolt irányelvek betartása mellett ez szavatolható lenne, ám sem az USA-ban újonnan meghozott törvények, sem azt megelőzően a NAI irányelvei nem biztosítottak ilyen mértékű védelmet a felhasználók számára. Így nem oszlatták el teljes egészében azokat az aggályokat, melyek jogosan felmerültek a web bugok alkalmazásával kapcsolatban. Ebben a tekintetben pozitív példát mutatott az Európai Unió szabályozása, mely az amerikai megfelelőjénél sokkal nagyobb védelemben részesítette a felhasználót a marketing cégekkel szemben. Fontos azt is látnunk, hogy a web bugok révén felmerült problémák orvoslására nem lehet megoldás a teljes betiltásuk, mivel az internetes marketing világában az etikusan használt alkalmazások kiemelkedő jelentőségűek, nagyban hozzájárultak az online vállalkozások egy jelentős részének gazdasági fellendüléséhez.

Zárásképpen kijelenthetjük, hogy ha a web bugok alkalmazásakor betartják a jog által diktált szabályokat és az etikai normákat, akkor széleskörű felhasználhatóságuk révén meghatározó és elfogadott eszközeivé válhatnak az internetes világnak.

Irodalom

ArentFox: Michigan Attorney General Cases Challanging the Use of Cookies, http://www.arentfox.com/additionalsites/e-privacy/e-privacynews/privacy-2000/

M. Campanelli: Bugged Out, *Entrepreneur magazine,* 2003. május http://www.Entrepreneur.com

M.J. Edwards: Your Web Browser is Bugged, *Windows Network & .Net Magazine,* InstantDoc #9543, 2000. július. 13. http://www.winnetmag.com

P. Festa – C. Barnes : Word documents susceptible to „web bug" infestation, *CNET News.com* http://news.com.com/2100-1023-245160.html

FindLaw Professionals: Cookies and Web Bugs, Michigan Web Bug Cases: Undisclosed Use of Web Bugs by Third Party Agents http://profs.lp.findlaw.com/privacy

T. J. Fitzgerald: Finding bugs in the cookies, *The Age,* 2003. június 26. http://www.theage.com.au

J. F. Harris – J. Schwartz: Anti-Drug Web Site Tracks Visitors, *Washington Post,* Page A23, 2000. június 22. http://www.washingtonpost.com

K. Hinckley: Security: „web bugs", email, and spammers, *Buzz Security,* 2003. szeptember 14. http://commons.somewhere.com/buzz/2000/Security.web.bugs.email.html

J. Hu: AOL Clears path to use web bugs, cookies, *CNET News.com* http://news.com.com

M. Kellner: The war on Spam continues, *JWR,* 2003. január 27. http://www.jewishworldreview.com

M. Marcum: Controlling Web Bugs – Online Advertisers Help Shape Guidelines, *EContent,* 2003. február 1. http://www.econtentmag.com

J. McCarthy: When Web Traffic Statistics Do Not Compute, *WebSideStory,* 2001. február 16. http://www.WebSideStory.com

J. McCarthy: Internet Intelligent Report Compliance, *WebSideStory,* 2001. február 26. http://www.WebSideStory.com

B. Morrissey: NAI Releases 'Web Bug' Guidelines, *InternetNews,* 2002.11.26.
http://www.internetnews.com

C. Saunders: EU OKs Spam Ban, Online Privacy Rules, *InternetNews,* 2002. május 31.
http://www.internetnews.com

R. M. Smith: New Proposal: Make Web Bugs Visible, *Privacy Foundation,* 2000. szeptember 13.
http://www.privacyfoundation.org/privacywatch

TechEncyclopedia, TechWeb: *The Business Technology Network*
http://www.techweb.com/tech

R. Yeargin: A Web Bug-based Micropayment Model, *Librenix,* 2003. január 13.
http://www.librenix.com

Webveil: Web Bug Demo, 2001. június
http://www.webveil.com

WebSideStory Inc.: Ad Tracking Disparities and Counting Methodologies
http://www.WebSideStory.com

WebSideStory Inc.: Case Study: HitBox Enterprise vs. Log File Analysis
http://www.WebSideStory.com

WebSideStory Inc.: The Future of Internet Intelligence
http://www.WebSideStory.com

E. Weise: 'web bugs' are still watching you, *USA Today,* 2000
http://www.usatoday.com/tech/columnist/cceli023.htm

D. Whalen: The Unofficial Cookie FAQ, *Cookie Central,* 2002. augusztus 6.
http://www.cookiecentral.com