INFINITI HÍRLEVÉL

Kollányi Bence

A mobilcégek mantrájától a kikerült radarokig

Erich Moechel médiakritikus és újságíró, többek között az ORF Futurezone *szerkesztője. A vele készült interjúban – egyebek mellett – a mobiltársaságok adatkezeléséről és a kormányok terrorizmus elleni harcának sajátosságairól kérdeztük.*

A linzi Ars Electronica fesztivál résztvevői évről évre a tudomány és művészet eszközeivel keresik a technológia és a társadalom átalakulása közben felmerült aktuális kérdésekre a választ. A hagyományoknak megfelelően minden évben hangzatos jelmondattal adják meg az esemény alaphangját. Az idén a résztvevők a magánszférától vettek búcsút... Ennek apropóján kérdeztük *Erich Moechelt.*

Kollányi Bence: Előadásában utalt arra, hogy a mobilcégek többsége folyamatosan elemzi az előfizetők kommunikációs szokásait. Példaként említette, hogy a felhasználók hívásainak analizálásával felismerhetők a társaság elhagyására készülő ügyfelek. Ugyanakkor az adatbázisok felépítése és elemzése a társaságok számára jelentős költségekkel jár. Ön szerint megéri a befektetés? Illetve milyen más hozadéka van az elemzéseknek?

Erich Moechelt: Ez elsősorban azért hasznos a szolgáltatóknak, mert a piacok telítődésével egyre nagyobb a verseny. Ha növekedni akarsz, nem teheted meg anélkül, hogy másoktól ne hódíts el ügyfeleket. Ezért a mobilszolgáltatók minden lehetséges, az előfizetők viselkedését előre jelző információt megpróbálnak kinyerni adatbázisaikból. Meghatározott alakzatok után kutatnak. Az alapvető kérdés pedig nem más, mint az, hogy „a felhasználó meg fogja-e változtatni telefonálási szokásait, hajlik-e arra, hogy elhagyja a társaságot". Erre jó példa, ha egy előfizető olyan szolgáltatásokat vesz igénybe, amelyeknek segítségével a hívások olcsóbb szolgáltatásokon keresztül futnak. Ez ugyanis ellenkezik a mobilcégek mantrájával. Tudja, mi az?

K. B.: Nem.

E. M.: ARPU, Average Revenue per User (egy előfizetőre jutó átlagbevétel), ez a mantrájuk. Ezt akarják növelni, ezért bármit hajlandók megtenni. Különböző okokból figyelik az előfizetőket. Az egyik, már a korábban is említett jelenség, hogy igyekeznek megtalálni azokat az ügyfeleket, akik a hívásaik alapján jó eséllyel el akarják hagyni a társaságot. Ezt követően üzletkötőket küldenek hozzájuk, akik ilyenkor rendszerint visszautasíthatatlan ajánlatot tesznek. Előbb ugyanis részletesen megvizsgálják az előfizető kommunikációs szokásait, csak ezután tesznek ajánlatot. Ahogy ez meg is történt Olaszországban a *Telecom Italia* esetében, de mindenhol hasonlóan működik a rendszer. Van továbbá egy másik adatbázis is minden mobilszolgáltatónál, amelynek segítségével a lehetséges visszaéléseket igyekeznek kiszűrni.

K. B.: Azokra a felhasználókra gondol, akik hatalmas tartozásokat halmoznak fel, és azt később nem fizetik meg?

E. M.: Igen. Ez az egyik legnagyobb problémája a szolgáltatóknak. Az egyes ügyek kivizsgálása mindenképpen veszteséget okoz a társaságnak. Ráadásul sok esetben akkor sem tudnak fizetni az ügyfelek, ha bebizonyították tartozásukat. Ezért a cégek igyekeznek minél korábban kiszűrni ezeket a felhasználókat, hogy a lehető leghamarabb közbeléphessenek, csökkentve ezzel veszteségeiket. Biztos vagyok, hogy ezen igyekezetük közben az európai adatvédelmi törvényeket napi rendszerességgel hágják át a mobilszolgáltatók. Az ok ismét ugyanaz, az egy előfizetőre jutó átlagbevétel növelése.

K. B.: Több adatbázist és elemzőszoftvert is említett, amelyeket a mobilszolgáltatók kiépítenek és alkalmaznak. Ennek ellenére, ha a kormányzat – például a terrorizmus elleni harcra hivatkozva – azt kéri a szolgáltatóktól, hogy tovább tárolják az előfizetők hívási adatait, a társaságok gyakran arra hivatkoznak, hogy ez jelentős többletköltséggel jár. Az Ön elmondása szerint azonban a szolgáltatók maguk is érdekeltek az előfizetői adatok minél hosszabb ideig tartó tárolásában.

E. M.: Egészen addig tiltakoznak, ameddig meg nem kapják a kormányzattól a várt ellentételezést. A mobilszolgáltatók egyszerűen el akarják adni mindezt a kormányzatnak egyfajta szolgáltatásként, és megfelelő fizetséget akarnak kiharcolni. Ennek megfelelően elutasítják az első ingyenes ajánlatokat. Ha visszaemlékezünk, a kezdeti időkben a szolgáltatók nem is rendelkeztek az adatok elemzéséhez szükséges szoftverekkel, mert azon dolgoztak, hogy megalapozzák a hálózati infrastruktúrájukat. De mihelyt többé-kevésbé befejeződött a hálózatépítés, elsősorban az adatelemzésbe kezdtek el befektetni a társaságok. Rengeteg olyan szoftver és hardver létezik ma a piacon, amely kiszolgálja a telefontársaságok igényeit. Így beszerezhető visszaélés-előrejelző *(Fraud Management Tool)* vagy a már említett potenciális szolgáltatóváltást előrejelző megoldás is, továbbá ott vannak a kormányzati adatkéréseket kiszolgáló alkalmazások. Az elmúlt néhány évben ezek mélyen beépültek a mobilhálózatok struktúrájába, s a mobilhálózatok ennek megfelelően nyitottá váltak.

K. B.: Jól értem, hogy olyan kiskapukat építettek a hálózatba a szolgáltatók, melyek segítségével a kormányzati igényeket szolgálhatják ki? Tehát harmadik félnek adhatják ki az előfizetői információkat?

E. M.: Pontosan. Nézze, szükségük van egy olyan felületre, ahol adatokat tudnak szolgáltatni. Ez a felület nem jut más szerephez a mobilhálózatban. Ez valami furcsa, idegen elem a rendszerben, hiszen alapvetően az lenne a cél, hogy a hálózat minél zártabb legyen. Ennek a zárt hálózati logikának mond ellent az a fejlesztés, amelynek egyetlen célja, hogy kiemeljen a rendszerből bizonyos információkat egy harmadik fél számára. Ezek a felületek rettenetesen sérülékenyek, bárki, aki ismeri a működésüket, könnyedén betörhet a hálózatba. Nemrégiben Görögországban tört ki botrány, mivel olyan személyes adatokat és információkat árultak, amelyeket mobilhálózatok adatbázisaiból nyertek ki. Ezekre az adatokra pedig komoly kereslet van manapság.

K. B.: Mi a szerepe az egész folyamatban a sztenderdizációnak? Előadásában ezt a területet is érintette, de nem pontosan értettem a párhuzamot.

E. M.: Ez egyszerű. Minden nagyobb társaság, különösen a több országban hálózattal rendelkező társaságok érdekeltek abban, hogy az egész hálózatukon belül ugyanazt a technológiát alkalmazzák. Nézzük a *Deutsche Telekom* példáját: úgy tudom, ők rendelkeznek Magyarországon érdekeltségekkel, megvették a *Matávot*. Tehát a *Deutsche Telekom*, illetve a *T-mobile* érdekeltek abban, hogy ugyanazokat az eszközöket használják, azonos jogszabályi környezetben. Így olcsóbb a hardverek beszerzése, csökkennek a szoftverek fejlesztési költségei, kevesebbe kerül a rendszer fenntartása. Ezért a mobiltársaságok alapvetően érdekeltek a sztenderdizációban. Az ezzel foglalkozó bizottságokban természetesen a megfigyelési eszközöket gyártó cégek és a harmadik érdekelt csoport, a rendőrség és az állambiztonság képviselői is jelen kívánnak lenni – ők a technológia kínálta lehetőségeket akarják kihasználni. A modern hálózatokban központi hozzáféréssel lehet a leghatékonyabban hozzájutni az adatokhoz. Van persze más lehetőség is. Például egy személy követésekor erre szolgál az *IMSI (International Mobile Subscriber Identification) catcher*. Ez egy apró eszköz, amely mobil adótoronyként működik. Minden mobiltelefonnak van egyedi azonosítója (ez az *IMSI*), akár előfizetéses, akár kártyás készülékről beszélünk. Ha az *IMSI catcher* közeléből indít valaki hívást, elsőként a kis jeladót érzékeli a telefonja: ez a klasszikus *man in the middle (MITM) attack*. Ehhez persze a megfigyelést végző embernek ugyanabban a cellában kell lennie. Az *IMSI catcher* a telefon felé toronyként jelentkezik, a torony felé pedig mobiltelefonként viselkedik. Ez a mobiltársaság központjából sem látható. Egyébként, ha egy ilyen eszközt a parlament közelében helyezünk el, akkor az jelentős állambiztonsági kockázatot jelent.

K. B.: Az emberek ezekről a veszélyekről mit sem tudnak. Hogyan látja Ön, mennyiben jelentheti a megoldást a felhasználók tájékoztatása? Az információk átadása mellett a jogszabályokat is módosíthatják, illetve olyan megoldásokat kínálhatnak, amelyek segítik a felhasználók anonimitását, elrejtőzését. Ön szerint a három lehetséges válasz közül melyiknek van a legnagyobb jelentősége?

E. M.: Nos, a jogszabályok jelenleg éppen az ellenkező irányban változnak, a helyzet egyre rosszabb. Ennyit a jogszabályokról, ehhez talán nincs is mit hozzáfűzni. A második kérdés az emberek tájékoztatása. Igen, ez lassan elkezdődött, az emberek kezdik megérteni, hogy nem a beszélgetéseik lehallgatása miatt vannak veszélyben. Viselkedési mintázataikat vizsgálják, ami, ha lehet, még rosszabb és többet árul el a személyről. Megtudhatjuk, hogy kiről van szó, kikkel kommunikál, milyen szociális háló veszi körül. Ez olyan veszély, amellyel még nem is számolnak az emberek. A kommunikációs szokások alapján profilokat alakítanak ki. Az anonimitásról és a titkosításról: mivel itt hívási adatokról van szó, azt kell mondanom, hogy a titkosítás nem sokat ér. Ha titkosítanánk a kommunikációnak ezt a részét, akkor a mobiltársaság nem tudná kapcsolni a hívott számot.

K. B.: Ezek szerint nem egyszerűen informálásról van szó, hanem a tudatosságot kell növelni az emberekben?

E. M.: Pontosan. Ezért van az, hogy a *Quintessenz* elnevezésű civil szabadságjogi mozgalom Bécsben ingyenes, megfigyelés nélküli internetkapcsolatot kínál. Ők nem hagyományos szolgáltatók, mivel nem számláznak, s ezért nem is kötelesek adatokat szolgáltatni a kormányzatnak. Aki valóban érdeklődik a technológia iránt, az könnyűszerrel kikerülheti a rendszert.

K. B.: Az Ön által említett szolgáltatást továbbgondolva, számolhatunk olyan pozitív forgatókönyvvel is, amely szerint az emberek fizetnek a magánszférájuk védelméért? Olyan virtuális szolgáltatókat, mobiltársaságokat vagy internetszolgáltatókat keresnek, amelyek nem gyűjtik és elemzik bizonyos módon az adataikat?

E. M.: A probléma az, hogy ezeket az alkalmazásokat azok az emberek fogják az elsők között elkezdeni használni, akiket meg akarnak figyelni, tehát ez az egész dolog: nagy hűhó semmiért. Csupán piti tolvajokat, buta csalókat, a technológiához nem értő balekokat fognak elkapni. Vagy olyan amatőr terroristákat, mint akik nemrég próbálkoztak Londonban, vagy akiket Skóciában kaptak el a hatóságok. Ezek dilettánsok voltak. A valódi veszélyt jelentő embereket nem lesznek képesek elfogni. Az egész rendszert a szervezett bűnözés, a komoly terroristák miatt találták ki, de – ismétlem – ők hagyják el a rendszert elsőként.

K. B.: Eszerint hiábavalóak a biztonság növelésére tett kísérletek?

E. M.: A terroristák amatőr rádióadókat, gyakran a Vöröskereszt munkatársaitól zsákmányolt rádió adóvevő készülékeket használnak. Ezeken kívül már csak egy-egy laptopra és áramellátásra, például egy autó akkumulátorára van szükségük. Az adatokat titkosítják a laptopon, és rádióhullámokon továbbítják. Nem tudják pontosan bemérni, hogy honnan indult a hívás, azt pedig különösen nem, hogy hova érkezik. Nincsen címzett, nincsen hálózat. Ez pont-pont típusú üzenetküldés, ráadásul rövid üzenetekről van szó, amelyek zajos csatornákon keresztül áramlanak.

K. B.: A terroristák ezek szerint a low-tech megoldásokkal képesek kivédeni a lehallgatásokat?

E. M.: Igen, egyszerűen a radarmezők alatt repülnek. A radarjaink az eget kémlelik, miközben a terroristák régi, már-már elfeledett technikákat használnak.