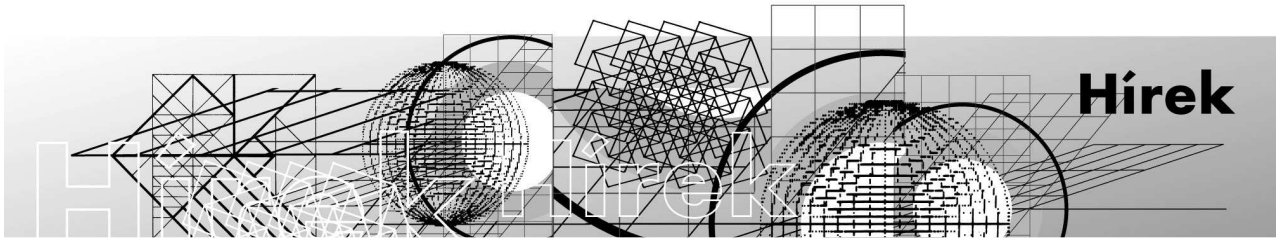

Az IBM kutatói megújították a személyes adatok védelmét

Mind több online szolgáltatás követeli meg valamely személyes adat – név, lakcím, esetleg bankkártyaszám – megadását, ezek azonban könnyen rossz kezekbe is kerülhetnek. Az IBM kutatói Identity Mixer néven olyan felhőmegoldást dolgoztak ki, amelynek segítségével a felhasználók maguk határozhatják meg, hogy mikor, kinek, mely adataikat szolgáltatják ki az interneten. Kifinomult kriptográfiai algoritmusra épülő felhőmegoldást dolgoztak ki az IBM kutatói, hogy megvédjék a felhasználókat a személyes adataikkal való visszaélésektől. Az online szolgáltatások terjedése miatt minden korábbinál fontosabbá váltak az adatvédelemi kérdések – legyen szó közösségi oldalakról, videómegosztókról, online vásárlásról vagy éppen a bankolásról. Mind több alkalmazás igényli a személyes adatok bizonyos körének megadását, a felhasználóknak azonban eddig gyakorlatilag nem volt ráhatásuk arra, hogy mi történik – a gyakran a szükségesnél jóval többet elárulóadatbázisokkal.

Az IBM felhőalapú Identity Mixer technológiájának célja, hogy a felhasználók személyes adatai az online szolgáltatások használatakor ne kerüljenek illetéktelen kezekbe. A hiteles adatokat ennek érdekében a rendszer titkosítja, lehetővé téve, hogy az ügyfél mindig csak annyit osszon meg magáról egy harmadik féllel, amennyi feltétlenül szükséges. A probléma mind nagyobb súlyát jelzi, hogy a comScore adatai szerint egy átlagos felhasználó havi 25 órát tölt az internet előtt, és ez alatt tucatnyi olyan online szolgáltatással találkozik, amelyhez személyes felhasználói fiókot kell létrehoznia, vagyis különböző adatokat kell megadnia. Az ilyen szolgáltatók természetesen maguk is törekednek a biztonságra, adatvédelmi szempontból azonban általában nem nyújtják a legmagasabb szintű védelmet, ami komoly költségekkel is járhat, ha az adatbázis „rossz kezekbe” kerül.

Előfordulhat például, hogy egy videostreaming szolgáltatás csak életkori és földrajzi korlátozással vehető igénybe, ilyenkor a felhasználónak pontos születési dátumát és lakcímét is meg kell adnia. Mindezek a szükségesnél már önmagukban jóval szélesebb adatkört jelentenek. Az Identity Mixer ebben az esetben azonban csak annyit igazol visszaa szolgáltató felé – pontos dátum nélkül –, hogy az adott egyén már betöltötte a minimális életkort, illetve nem részletezve jelzi, hogy tartózkodási helye megfelel-e a kívánt régiónak. Ha pedig bankkártyával vásárolna filmet az ügyfél, a szolgáltató csak annyit nyerhetne ki a központi felhőből, hogy a plasztik érvényes és a bank elfogadta-e a tranzakciót – a kártyaszám és a lejárati dátum nem kerülne a szervereire. Az adatbázisban így csak az „igen” kerül a felhasználó neve mellé, a valódi személyes adatokat pedig a biztonságos felhő tartalmazza. Ezek akkor sem kerülhetnek illetéktelenekhez, ha például a regisztrációt kérő portál szerverét feltörik.

Az Identity Mixer tehát kriptografikus algoritmusokkal titkosítja a felhasználó – akár harmadik fél, például az állam által hitelesített – adatait, az adatokat hitelesítő tanúsítványt kiadó szervezet pedig természetesen nem kap arról információt, hogy hogyan és mikor használják fel az adatokat. A technológia előnyös a felhasználóknak, hiszen pontosan kontrollálhatják, hogy mikor, kivel, milyen adatokat osztanak meg. Nyerhetnek vele azonban a szolgáltatók is, hiszen jelentősen csökkenthetik az online aktivitást esetleg akadályozó kockázatokat, növelhetik az ügyfélbizalmat. Mindezt ráadásul felhőalapon, ami nagyban megkönnyíti a fejlesztők dolgát a technológia saját alkalmazásaikba integrálásakor.

Az Identity Mixer tesztelésére tavasztól nyílik mód az IBM Bluemix felhőplatformján, a fejlesztők így saját platformjaikba ágyazva próbálhatják ki a megoldást, mind asztali, mind mobil felhasználási területen.

A rendszer potenciálját természetesen már ez megelőzően is tesztelték. A Német Vöröskereszt-

nél például az otthoni sürgősségi és szociális ellátásban alkalmazták sikerrel a technológiát. Ebben az esetben a központi szerver a tesztprogramban résztvevő gondozottakra szerelt szenzorok – fizikai állapotra és aktivitásra vonatkozó – adatainak rögzítésével és elemzésével döntötte el, hogy kinek van éppen szüksége segítségre, és ezen belül is milyen jellegűre. Az adatkezelés itt értelemszerűen kulcskérdés, hiszen számos, betegségekkel, orvosi leletekkel, gyógyszerekkel és a rokonok elérhetőségeivel összefüggő érzékeny információt kell kezelni a megfelelő döntésekhez és intézkedésekhez.

/Forrás: ***http://sg.hu/cikkek/110576/az-ibm-kutatoi-megujitottak-a-szemelyes-adatok-vedelmet***/

(F. Iné)