Adatvédelem és információszabadság

Tartalom

Bioszkript

- A „bioszkript" olyan technológia, amely nem egyetlen felhasználói tevékenységtípus védelmére irányul; alkalmazható például a személyazonosító adatok és más személyes adatok ideiglenes szétválasztására, ún. „anonim adatbázisok" felépítésére; használható az elektronikus levelezésben vagy az elektronikus kereskedelmi szolgáltatásokban. A bioszkript létrehozásához két kiinduló adatra: egy biometrikus és egy nem biometrikus adatra van szükség. A biometrikus adat célszerűen egy ujjlenyomat digitális képe, a nem biometrikus pedig egy kriptográfiai kulcs, egy azonosító kód vagy egy mutató (pointer), de akár egy haiku is lehet. A két adat összekódolásából jön létre a bioszkript, amelyet a biometrikus adattal, mint afféle kulccsal lehet felnyitni, és így lehet hozzáférni a további alkalmazáshoz szükséges nem-biometrikus adathoz. A gyakorlatban a biometrikus adat ismételt produkálása az ujjlenyomat újbóli leolvasását jelenti, s így biztosítható, hogy az alkalmazás az érintett személyek jelenlétében és feltételezett hozzájárulásukkal történjék.

Kapcsolati kód

- A kapcsolati kód szerepe az, hogy az adatalanyokat egyértelműen azonosítsa két adatkezelés (vagy egy adatkezelés két szegmense) közötti kapcsolatban, ugyanakkor szegmentálja a személyesadat-köröket, amelyeket az egyes adatkezelők megismerhetnek. A kapcsolati kód alkalmazását egyébként a nagy állami nyilvántartások közötti adatkapcsolatban törvény is elrendeli Magyarországon,"' de szervezeten belüli alkalmazásuk is hasznos lehet, például a személyazonosító adatoknak a többi személyes adatról való leválasztására. Az egyik adatállományban például a nevek és az egyedi kapcsolati kódok szerepelhetnek, a másikban csak a kapcsolati kódok és az érdemi adatok - így a túloldalon látszólag anonimizált egyedi adatsorokhoz juthatunk, amelyek személyes volta ugyan a kapcsolati kód segítségével bármikor helyreállítható, azonban személyes mivoltuktól ideiglenesen megfosztott formájukban alkalmasak arra, hogy kezelésük garanciákat nyújtson a személyes adatok „szükségtelen", „nemkívánatos" vagy „jogellenes" kezelése ellen.

Anonim remailer

- Ugyancsak a legelterjedtebb internetes tevékenységek közé tartozik a személyközi üzenetváltás, elsősorban az e-mail. Kevés internethasználó van tudatában annak, hogy az e-mailes üzenetküldés bizalmassági szintje közel áll a nyílt levelezőlapéhoz; és bár vannak az üzenet illetéktelen elolvasását nehezítő megoldások, a főnök vagy a rendszergazda általában nem tartozik az elektronikus levelek tartalmához nehezen hozzáférők közé. De nemcsak az üzenet tartalma, hanem a kommunikáló felek kiléte, üzenetváltásuk időpontja, gyakorisága, sorrendje, sőt néha a terjedelme is értékes információt nyújthat a lehallgatónak. Az anonim remailerek ezeknek az információknak az illetéktelenek előli elfedését célozzák. Olyan üzenet-továbbküldő szolgáltatásokról van szó, amelyek akár a címzett elől is elfedik a küldő kilétét; ez a hatalom kritikájának ókori formája, a tömegből való „bekiabálás" modern megfelelőjeként funkcionálhat az internetes környezetben. Többnyire azonban a címzett ismeri a feladót, kettejük kapcsolatából csak a harmadik feleket kívánják kizárni. A remailerek és a lehallgatásukra kifejlesztett technológiák fejlődése az elmúlt két évtizedben rabló-pandúr játékra emlékeztetett. A legelső, ún. Cypherpunk típusú remailerek csak a továbbítandó üzenet fejlécét cserélték le, s ezt a - szabadon reklámozott, tehát mindenki által ismert - remailer bemenetének és kimenetének figyelésével könnyen vissza lehetett állítani. A védekezésül bevezetett késleltetési időt (az üzenetek „pufferolását") a támadók a saját üzeneteikkel való elárasztással próbálták ellensúlyozni, amire a fejlettebb remailerek véletlenszerű sorrendben történő üzenettovábbítással reagáltak. A támadók által végzett üzenetsokszorozás ellen a remailereknek fel kellett ismerniük az azonos üzeneteket, és csak egy példányt volt szabad elfogadniuk belőlük - ez egyébként hasznos volt a remailerekkel való visszaélés egyik formája, a korai „levélszemét" (spam) kiszűrésére is. Az útvonalfigyelés megnehezítésére a remailereket láncba fűzték, méghozzá oly módon, hogy minden remailer csak a láncban utána következő remailer címét ismerte, a címzettét nem. Éppen ez a technika adott még egy lehetőséget a támadóknak: az ismeretlen tartalmú és címzésű üzeneteknek a remailerláncon való áthaladásuk során megjósolható mértékben csökkent a mérete, hiszen a továbbításra vonatkozó „elhasznált" parancsokat törölték a továbbított üzenetből. A csökkenő méretű üzenetek követése végül elvezethetett a címzetthez. E probléma megoldására jött létre a szabványos méretű és formátumú - ún. Mixmaster típusú - anonim üzenetcsomag; továbbfejlesztett, harmadik generációs típusukat MixMinion névvel illetik. A remailerek használata - lényegükből fakadóan - ingyenes; hiszen ha a szolgáltató díjat akarna szedni a felhasználóktól, akkor neki is ismernie kellene kilétüket, ez pedig a remailerek kompromittálhatóságát eredményezné. A remailer szolgáltatás használatakor először le kell kérdezni az éppen aktív remailerek listáját, a felhasználónak választania kell egy programot; az üzenetküldő lánc már automatikusan alakul ki. Tekintettel az olykor jelentős - szándékos - késleltetésekre, a remailerek nem a sürgős üzenetküldés, hanem a biztonságos és bizalmas kommunikáció eszközei.

Közadat-hozzáférést támogató rendszerek

Átlátszó.hu

- Az Átlátszó.hu internetes oknyomozó, tényfeltáró portál 2012-ben online közérdekűadat-igénylő szolgáltatást indított KiMitTud néven. Az igénylők egy előre elkészített levélsablonba írhatják kérdésük lényegét, kereshetnek az adatgazdák között; a rendszer figyeli a válasz törvényes határidejének leteltét, válasz híján automatikusan újraküldi az adatigénylést, valamint közzéteszi a feltett kérdéseket és a válaszokat. 2015 júliusáig mintegy 5.200 adatigénylést kezelt a szolgáltatás és 4.704 adatgazda kapcsolati adatait tette elérhetővé. Az

Átlátszó, tizenkilenc további országban működő testvér-szolgáltatásával közösen, az Alaveteli nevű, finn fejlesztésű, ingyenes és nyílt forráskódú, közadatkérést segítő szoftvert használja. Számos előnye mellett a szoftver kritikájaként említhető, hogy ugyan az, hogy az egyéni adatigénylők mit kérdeznek és arra a hatóságok mit válaszolnak, maga is közérdekű adat, de az, hogy ki kérdezi, az nem – az Alaveteli rendszer azonban ezt is nyilvánosságra hozza.

Egységes közadatkereső

- Az elektronikus közzétételre kötelezett adatgazdáknak regisztrálniuk kell a www.kozadattar.hu weboldalon, le kell tölteniük az ingyenes szoftvernek a saját rendszerükhöz illeszkedő nyelvű verzióját, majd pedig a közzétett közérdekű adatok és dokumentumok leíró adatait (metaadatait) – például a dokumentum típusát, keletkezésének időpontját, pontos webcímét – be kell írniuk egy egyszerű táblázatba, amit aztán az internetre kötött rendszer automatikusan „learat". A regisztrációs és adatfeltöltési fegyelem serkentésében és ellenőrzésében sem a korábbi adatvédelmi biztosok, sem a jelenlegi hatóság nem jeleskedtek, ezért a rendszer adattartalma hiányos. Ezzel együtt nyilvánvalók az előnyei az internetes keresőgépek találataival szemben: amíg az általános keresők találatainak relevanciája, időszerűsége és megbízhatósága kérdéses, addig a közadatkereső ellenőrizhető adatokat szolgáltat, az adatgazdák felelősségével.

PRIME architektúra

- A jelenleg futó legjelentősebb PET vonatkozású európai uniós projekt a 2004-ben indult PRIME (Privacy and Identity Management for Europe).
- A PRIME projektek végső célja, hogy az információs rendszerekbe egy middleware szerű, alkalmazás- és platform-független réteget építsenek bele, amely a felszín alatt elvégzi mindazokat a teendőket, amelyeket akár a jogszabályi előírások, akár az adatkezelő önszabályozása, akár az érintett adatalanyok egyéni preferenciái meghatároznak. Ha például egy adatot az adatkezelési cél teljesülésével törölni kell, a PRIME réteg automatikusan követi az adat sorsát a különböző adatkezelőknél és gondoskodik a törléséről. Amint a projekt elnevezése is utal rá, központi eleme az identitásmenedzselés. E kifejezés alatt általában azt értik használói, hogy miként tudja ügyfeleinek adatait minél jobban menedzselni az üzleti szolgáltató vagy a hatóság. A PRIME ezzel szemben felhasználó-központú identitásmenedzselést kíván megvalósítani, ahol – a jogszabályi korlátok között – maguk a felhasználók határozhatják meg adataik sorsát, és annak teljesítéséről automatikus rendszerek gondoskodnak.

Belső adatvédelmi felelős

- Az Adatvédelmi törvény 2004. január 1-én hatályba lépő – az EU szabályozásnak megfelelő – új rendelkezései szerint belső adatvédelmi (és nem adatbiztonsági) felelős kell kinevezni számos adatkezelőnél, s a törvény a felelősök feladatait is előírja. → adatvédelem: az, amivel a belső adatvédelmi biztosnak kell foglalkoznia 2004. január 1-től

Bejelentés az Adatvédelmi nyilvántartásba

- Bejelentés, adatszolgáltatás
    - Adatvédelmi nyilvántartás
        - egyszeri regisztráció a tevékenység megkezdése előtt
        - kötött forma, nyilvános adatok
        - változások jelentése

- Elutasított kérelmek bejelentése
    - évenkénti bejelentés
    - tájékoztatás a teljesített kérelmekről is
- Bejelentés
    - adatkezelő jelenti be
    - adatkezelést
    - adatkezelésenként
    - tevékenység megkezdése előtt
    - változást 8 napon belül
    - adatkezelési azonosító
- Belső szabályozás
    - Adatvédelmi szabályzat
    - Adatbiztonsági szabályzat
    - Privacy Policy

Nem követő keresőgépek

- SSL titkosítás
- Nem követi az IP címet
- Sütiket nem tárolja
- Keresési előzmények nincsenek tárolva
- Pl.: DuckDuckGo, start page, ixquick