A titkosítás nem azonos a magánélettel: mit árulnak el Önről a metaadatok

A titkosított tartalom és a látható metaadatok két különböző dolog. Amikor egy szolgáltatás „végpontok közötti titkosításról” beszél, csak a történet felét meséli el.

A lakat, amely nem véd meg mindent

A mai üzenetküldő szolgáltatások nagy része végpontok közötti titkosítást hirdet. És ez igaz is: az üzenetek tartalma titkosítva utazik, így útközben senki – még a szolgáltató sem – tudja elolvasni a szöveget a továbbítás alatt. Eddig az állítás pontos.

A probléma az, hogy a tartalom csak a történet egy része. Bár senki sem tudja elolvasni, amit mond, a szolgáltató más dolgokat nagyon nagy pontossággal tud: kivel beszél, mikor, milyen gyakran, megközelítőleg honnan, milyen eszközről, hány üzenetet küld és hányat kap, hány fájlt oszt meg. Mindezt metaadatoknak hívják. És a metaadatok sok esetben majdnem annyit elárulnak, mint maga az üzenet.

Amit a metaadatok feltárnak

Nem kell elolvasni egy üzenetet ahhoz, hogy sok mindent megtudjunk. Ha valaki hat hónapon keresztül minden kedd reggel kilenckor felhív egy onkológust vagy ír neki, nem kell hallani a beszélgetést ahhoz, hogy sejtsük, mi történik. Ha két ember napi száz üzenetet vált, majd hirtelen abbahagyják, egyet sem kell elolvasni ahhoz, hogy megértsük, mi történt. Ha egy adótanácsadó a negyedéves zárás előtti éjszakán húsz üzenetet kap egymás után ugyanattól az ügyféltől, a minta önmagáért beszél.

A metaadatok viselkedési mintákat tárnak fel: ki kivel áll kapcsolatban, kinek milyen az időbeosztása, mikor van ébren, mikor alszik, mikor utazik, mely ügyfelek a legaktívabbak, mely szakmai kapcsolatok a legintenzívebbek. Egy metaadatokat gyűjtő szerver részletes profilt tud építeni bármely felhasználó magán- és szakmai életéről anélkül, hogy valaha is elolvasna egyetlen szót is abból, amit az illető ír.

Van egy történelmi példa, amely ezt keményen illusztrálja. Az NSA korábbi igazgatója, Michael Hayden 2014-ben kertelés nélkül fogalmazott: *„We kill people based on metadata”* (Metaadatok alapján ölünk embereket). A kijelentés azokra az amerikai katonai műveletekre utalt, amelyek során a célpontokat kizárólag kommunikációs mintáik alapján azonosították. Egyetlen elolvasott üzenet nélkül. Csak a kapcsolati háló és az időpontok alapján.

Az, hogy egy szolgáltatás metaadatokat gyűjt, nem feltétlenül jelenti azt, hogy azokat a felhasználói ellen fogja felhasználni. Azt jelenti, hogy megvan rá a képessége, és hogy egy harmadik félnek, aki hozzáfér ezekhez az adatokhoz – bírósági végzés, biztonsági rés vagy harmadik félnek történő értékesítés útján, ha a szolgáltatási feltételek ezt lehetővé teszik – szintén megvan rá a lehetősége.

A telefonkönyvhöz való hozzáférés

Egy másik vektor, amely szinte észrevétlen marad: a névjegyzék. Az üzenetküldő szolgáltatások nagy része regisztrációkor hozzáférést kér a telefon névjegyzékéhez. Minden számot feltöltenek a szerverükre, hogy megmutassák, ki használja még a szolgáltatást. Ettől a pillanattól kezdve a vállalatnak teljes térképe van a felhasználó kapcsolatairól, még akkor is, ha az illető soha egyetlen üzenetet sem írt senkinek.

Egy szakmai titoktartásra kötelezett személy – ügyvéd, orvos, pszichológus, tanácsadó – számára ez a névjegyzék ügyfeleket tartalmaz. Ha a névjegyzéket feltöltötték egy harmadik fél szerverére, az ügyfelek nevei egy olyan infrastruktúrába kerültek, amelynek joghatóságát és szabályozását a szakember nem ellenőrzi. A szakmai titok nem azon a napon törik meg, amikor valaki kiszivárogtat egy beszélgetést: már sokkal korábban, a feltöltés elfogadásának pillanatában megtört.

Különbség a titkosítás és a nem-gyűjtés között

A titkosítás a tartalom védelmét jelenti. Privátnak lenni azt jelenti, hogy nem gyűjtjük azt, amire nincs szükség. Ezek különböző dolgok, és a különbség operatív szempontból döntő. Egy szolgáltatás tökéletesen titkosíthat minden üzenetet, miközben a metaadatokon keresztül szinte mindent tud a felhasználóiról. A kettő teljesen kompatibilis. Valójában ez a domináns üzleti modell az iparágban.

A megfelelő kérdés egy szolgáltatás valódi magánéletének értékeléséhez nem az, hogy *„titkosítja-e a tartalmat?”*. Erre a kérdésre évek óta tudjuk a választ. A helyes kérdés így hangzik: *„milyen metaadatokat generál, és hol tárolja azokat?”*. És mindenekelőtt: *„milyen metaadatokat nem kellene generálnia?”*.

Egy olyan architektúra, amely tervezésénél fogva (privacy by design) minimalizálja a metaadatokat – nem ígéretekkel, nem belső szabályzatokkal –, strukturálisan privátabb, mint egy olyan architektúra, amely gyűjti és titkosítja azokat. Mivel a nem létező adatok nem szivároghatnak ki, nem adhatók el, nem adhatók át bírósági végzésre, és nem veszhetnek el egy feltörés során.

A szakmai olvasó számára

Ha szakmai tevékenysége titoktartással, bizalmas kezeléssel vagy egyszerűen a harmadik felek információinak tiszteletben tartásával jár, érdemes a következő sorrendben feltenni a kérdéseket:

1. Titkosítja-e a tartalmat az az alkalmazás, amelyet kommunikációra használok? (Valószínűleg igen.)
2. Titkosítja-e a metaadatokat? (Valószínűleg nem.)
3. Generál-e olyan metaadatokat, amelyekre a működéséhez *nincs szüksége*? (Szinte biztosan igen.)
4. Hol tárolják ezeket a metaadatokat, és milyen joghatóság alatt? (Valószínűleg az Európai Gazdasági Térségen kívül.)
5. Tudja-e az ügyfelem vagy a páciensem, hogy az adatai ott vannak?

Az utolsó kérdés a kellemetlen. Mert az őszinte válasz a legtöbb esetben: nem.

Ez a cikk az első a professzionális kommunikációs eszközök tényleges működéséről szóló sorozatban. A következő számok a GDPR-megfelelőséggel és a szakmai titoktartás fogalmával foglalkoznak majd a digitális korban.

Források és további olvasnivalók

- Hayden, M. – Nyilatkozat a Johns Hopkins Egyetemen, 2014 („We kill people based on metadata”). Nyilvános leiratok elérhetők.
- GDPR (EU 2016/679 rendelet), 4. és 5. cikk – a személyes adatok meghatározása és az adatkezelés elvei (a metaadatok személyes adatok).
- Európai Adatvédelmi Biztos és EDPB – vélemények a forgalmi adatok és metaadatok kezeléséről az elektronikus hírközlésben (e-adatvédelmi irányelv).

← ElőzőA viaszpecsét rövid történeteKövetkező →A szakmai titoktartás a digitális korban

Legutóbbi olvasmányok

- CUADERNOS_LIST_PREGUNTAS_TITLE
- CUADERNOS_LIST_SELFHOST_TITLE
- CUADERNOS_LIST_IDENTIDAD_TITLE

Vigye magával ezt a cikket, ahová csak szüksége van rá.

↓ Markdown ↓ Egyszerű szöveg ↓ PDF

A fájl letöltődik az Ön eszközére. Onnan elmentheti, importálhatja a Solo2-be, vagy megoszthatja bárhol. A Cuadernos nem dönt Ön helyett a fájl sorsáról.

Viaszpecsét · SHA-256 39fb4446d5b0ed275f85d39e543ab32a17b2f42da99addeef533bdf6b27c7bdc

Cuadernos Lacre · A Menzuri Gestión S.L. kiadványa ·
írta R.Eugenio · szerkesztette a Solo2 csapata.