Kryptering är inte integritet: vad metadata berättar om dig

Krypterat innehåll och synlig metadata är två olika saker. När en tjänst talar om "totalsträckskryptering" berättar de bara halva historien.

Hänglåset som inte skyddar allt

En stor del av dagens meddelandetjänster utlovar totalsträckskryptering. Och det stämmer: innehållet i meddelandena färdas krypterat, så att ingen på vägen – inte ens tjänsteleverantören – kan läsa texten medan den är i transit. Så långt är påståendet korrekt.

Problemet är att innehållet bara är en del av historien. Även om ingen kan läsa vad du säger, vet tjänsten andra saker med mycket hög precision: vem du pratar med, när, hur ofta, från vilken ungefärlig plats, på vilken enhet, hur många meddelanden du skickar och hur många du tar emot, hur många filer du delar. Allt detta kallas metadata. Och metadata berättar i många fall nästan lika mycket som själva meddelandet.

Vad metadata avslöjar

Man behöver inte läsa ett meddelande för att veta mycket. Om en person ringer eller skriver till en onkolog varje tisdagsmorgon klockan nio under sex månader, behövs det inte höras vad som sägs för att ana vad som pågår. Om två personer utbyter hundra meddelanden om dagen och plötsligt slutar, behöver man inte läsa ett enda för att förstå vad som har hänt. Om en skatterådgivare får tjugo meddelanden i rad från samma kund kvällen före ett kvartalsskifte, talar mönstret för sig självt.

Metadata avslöjar beteendemönster: vem som umgås med vem, vilka tider varje person har, när de är vakna, när de sover, när de reser, vilka kunder som är mest aktiva, vilka yrkesmässiga relationer som är mest intensiva. En server som samlar in metadata kan bygga en detaljerad profil av varje användares personliga och yrkesmässiga liv utan att någonsin ha läst ett enda ord av vad som skrivits.

Det finns ett historiskt exempel som illustrerar detta med skärpa. Den tidigare chefen för NSA, Michael Hayden, formulerade det utan krusiduller 2014: *"We kill people based on metadata"*. Påståendet syftade på amerikanska militäroperationer mot mål som identifierats enbart genom deras kommunikationsmönster. Inte ett enda läst meddelande. Bara kontaktgrafen och tiderna.

Att en tjänst samlar in metadata innebär inte nödvändigtvis att den kommer att använda den mot sina användare. Det innebär att den har förmågan att göra det, och att en tredje part med tillgång till dessa data – genom domstolsbeslut, säkerhetsbrister eller försäljning till tredje part om användarvillkoren tillåter det – också har den.

Tillgången till kontaktboken

En annan vektor som nästan går obemärkt förbi: kontaktlistan. En stor del av meddelandetjänsterna ber om tillgång till telefonens kontaktbok vid registrering. De laddar upp alla nummer till sin server för att visa vilka andra som använder tjänsten. Från det ögonblicket har företaget en komplett karta över användarens relationer, även om denne aldrig har skrivit ett enda meddelande till någon.

För en yrkesutövare med tystnadsplikt – advokat, läkare, psykolog, rådgivare – innehåller den kontaktboken klienter. Om kontaktboken har laddats upp till en tredjepartsserver finns klienternas namn i en infrastruktur vars jurisdiktion och policyer yrkesutövaren inte kontrollerar. Tystnadsplikten bryts inte den dag någon läcker en konversation: den bröts långt tidigare, i det ögonblick uppladdningen accepterades.

Skillnaden mellan att kryptera och att inte samla in

Kryptering är att skydda innehållet. Integritet är att inte samla in det som inte behövs. Det är olika saker, och skillnaden är operativt kritisk. En tjänst kan kryptera alla meddelanden perfekt och samtidigt veta nästan allt om sina användare genom metadata. De två sakerna är fullt kompatibla. Faktum är att det är den dominerande affärsmodellen i branschen.

Den rätta frågan för att utvärdera en tjänsts verkliga integritet är inte *"krypterar den innehållet?"*. Den frågan har varit besvarad i åratal. Den rätta frågan är: *"vilken metadata genererar den och var lagras den?"*. Och framför allt: *"vilken metadata behöver den inte generera?"*.

En arkitektur som minimerar metadata genom design – inte genom löften eller interna policyer – är strukturellt mer privat än en arkitektur som samlar in och krypterar den. Eftersom data som inte finns inte kan läckas, säljas, lämnas ut vid ett domstolsbeslut eller förloras vid ett intrång.

För den professionella läsaren

Om din yrkesverksamhet innebär tystnadsplikt, konfidentialitet eller helt enkelt respekt för tredje parts information, är det värt att ställa sig frågorna i denna ordning:

1. Krypterar appen jag använder innehållet? (Sannolikt ja.)
2. Krypterar den metadata? (Sannolikt nej.)
3. Genererar den metadata som den *inte behöver* för att fungera? (Nästan säkert ja.)
4. Var lagras denna metadata och under vilken jurisdiktion? (Sannolikt utanför Europeiska ekonomiska samarbetsområdet.)
5. Vet min klient eller patient om att deras uppgifter finns där?

Den sista frågan är den obekväma. För det ärliga svaret är i de flesta fall nej.

Den här artikeln är den första i en serie om hur professionella kommunikationsverktyg fungerar i verkligheten. Kommande delar kommer att behandla GDPR-efterlevnad i messaging och konceptet tystnadsplikt i den digitala tidsåldern.

Källor och vidare läsning

- Hayden, M. – Uttalande vid Johns Hopkins University, 2014 ("We kill people based on metadata"). Offentliga transkriptioner finns tillgängliga.
- GDPR (EU-förordning 2016/679), art. 4 och 5 – definition av personuppgifter och principer för behandling (metadata är personuppgifter).
- EDPS och EDPB – yttranden om behandling av trafikuppgifter och metadata vid elektronisk kommunikation (ePrivacy-direktivet).

← FöregåendeEn kort historik om lacksigillNästa →Tystnadsplikten i den digitala tidsåldern

Senaste läsning

- CUADERNOS_LIST_PREGUNTAS_TITLE
- CUADERNOS_LIST_SELFHOST_TITLE
- CUADERNOS_LIST_IDENTIDAD_TITLE

Ta med dig den här artikeln dit du behöver den.

↓ Markdown ↓ Klartext ↓ PDF

Filen laddas ner till din enhet. Därifrån kan du spara den, importera den till Solo2 eller dela den var du vill. Cuadernos bestämmer inte destinationen åt dig.

Lacksigill · SHA-256 a957523d43aed67724f462814318442074c867edf133cd7bdb840d18e3333851

Cuadernos Lacre · En utgåva från Menzuri Gestión S.L. ·
skriven av R.Eugenio · redigerad av teamet bakom Solo2.