Analyse · 16 mei 2026

← Vorige·Volgende →

Versleutelen is niet hetzelfde als privé zijn: wat metadata over u vertelt

Versleutelde inhoud en zichtbare metadata zijn twee verschillende dingen. Wanneer een dienst spreekt over "end-to-end versleuteling", vertellen ze slechts het halve verhaal.

Het hangslot dat niet alles beschermt

Een groot deel van de huidige messaging-diensten adverteert met end-to-end versleuteling. En het is waar: de inhoud van de berichten reist versleuteld, zodat niemand onderweg – zelfs de dienstverlener niet – de tekst kan lezen terwijl deze in transit is. Tot zover is de bewering juist.

Het probleem is dat de inhoud slechts een deel van het verhaal is. Hoewel niemand kan lezen wat u zegt, weet de dienst wel andere dingen met een zeer hoge precisie: met wie u spreekt, hoe laat, hoe vaak, vanaf welke geschatte locatie, op welk apparaat, hoeveel berichten u verstuurt en hoeveel u ontvangt, hoeveel bestanden u deelt. Al dit wordt metadata genoemd. En metadata vertelt in veel gevallen bijna net zoveel als het bericht zelf.

Wat metadata onthult

U hoeft geen bericht te lezen om veel dingen te weten. Als iemand gedurende zes maanden elke dinsdagochtend om negen uur een oncoloog belt of schrijft, is het niet nodig om het gesprek te horen om te vermoeden wat er aan de hand is. Als twee mensen honderd berichten per dag uitwisselen en daar plotseling mee stoppen, hoef je er geen één te lezen om te begrijpen wat er is gebeurd. Als een belastingadviseur de avond voor een kwartaalafsluiting twintig berichten achter elkaar ontvangt van dezelfde klant, spreekt het patroon voor zich.

Metadata onthult gedragspatronen: wie met wie in relatie staat, wat de schema's van elk persoon zijn, wanneer ze wakker zijn, wanneer ze slapen, wanneer ze reizen, welke klanten het meest actief zijn, welke professionele relaties het meest intens zijn. Een server die metadata verzamelt, kan een gedetailleerd profiel opbouwen van het persoonlijke en professionele leven van elke gebruiker zonder ooit een enkel woord te hebben gelezen van wat hij schrijft.

Er is een historisch voorbeeld dat dit hard illustreert. De voormalige directeur van de NSA, Michael Hayden, formuleerde het in 2014 zonder omwegen: *"We kill people based on metadata"*. De uitspraak verwees naar Amerikaanse militaire operaties tegen doelen die uitsluitend werden geïdentificeerd aan de hand van hun communicatiepatronen. Geen enkel bericht gelezen. Alleen de contactgraaf en de schema's.

Dat een dienst metadata verzamelt, betekent niet dat deze tegen zijn gebruikers zal worden gebruikt. Het betekent dat hij de capaciteit heeft om dat te doen, en dat een derde partij met toegang tot die gegevens – door een gerechtelijk bevel, door een inbreuk op de beveiliging of door verkoop aan derden als de servicevoorwaarden dit toestaan – dat ook heeft.

Toegang tot de agenda

Een andere vector die bijna onopgemerkt blijft: de contactlijst. Veel messaging-diensten vragen bij het registreren toegang tot de agenda van de telefoon. Ze uploaden alle nummers naar hun server om te laten zien wie de dienst nog meer gebruikt. Vanaf dat moment heeft het bedrijf een volledige kaart van de relaties van de gebruiker, ook al heeft deze nooit een enkel bericht naar iemand gestuurd.

Voor een professional met een beroepsgeheim – advocaat, arts, psycholoog, adviseur – bevat die agenda klanten. Als de agenda is geüpload naar een server van derden, staan de namen van de klanten op een infrastructuur waarvan de professional de jurisdictie en het beleid niet controleert. Het beroepsgeheim wordt niet gebroken op de dag dat iemand een gesprek lekt: het werd al veel eerder gebroken, op het moment dat de upload werd geaccepteerd.

Het verschil tussen versleutelen en niet verzamelen

Versleutelen is de inhoud beschermen. Privé zijn is niet verzamelen wat niet nodig is. Dat zijn verschillende dingen, en het verschil is operatief cruciaal. Een dienst kan alle berichten perfect versleutelen en tegelijkertijd bijna alles over zijn gebruikers weten via metadata. De twee dingen zijn perfect compatibel. In feite is het het dominante bedrijfsmodel in de sector.

De juiste vraag om de werkelijke privacy van een dienst te evalueren is niet *"versleutelt het de inhoud?"*. Die vraag wordt al jaren als beantwoord beschouwd. De juiste vraag is: *"welke metadata genereert het en waar wordt het opgeslagen?"*. En vooral: *"welke metadata hoeft het niet te genereren?"*.

Een architectuur die metadata minimaliseert door ontwerp – niet door belofte, niet door intern beleid – is structureel meer privé dan een architectuur die ze verzamelt en versleutelt. Omdat gegevens die niet bestaan, niet kunnen worden gelekt, noch verkocht, noch overhandigd aan een gerechtelijk bevel, noch verloren gaan bij een inbreuk.

Voor de professionele lezer

Als uw professionele activiteit een beroepsgeheim, vertrouwelijkheid of simpelweg respect voor de informatie van derden inhoudt, is het raadzaam om de vragen in deze volgorde te stellen:

1. Versleutelt de applicatie die ik gebruik om te communiceren de inhoud? (Waarschijnlijk wel.)
2. Versleutelt het de metadata? (Waarschijnlijk niet.)
3. Genereert het metadata die het *niet nodig heeft* om te functioneren? (Bijna zeker van wel.)
4. Waar is die metadata opgeslagen en onder welke jurisdictie? (Waarschijnlijk buiten de Europese Economische Ruimte.)
5. Weet mijn klant of patiënt dat zijn gegevens daar staan?

De laatste vraag is de pijnlijke. Want het eerlijke antwoord is in de meeste gevallen: nee.

Dit artikel is het eerste in een reeks over de werkelijke werking van professionele communicatietools. Volgende afleveringen zullen ingaan op AVG-naleving in messaging en het concept van beroepsgeheim in het digitale tijdperk.

Bronnen und verdere lectuur

- Hayden, M. – Verklaring aan de Johns Hopkins University, 2014 ("We kill people based on metadata"). Openbare transcripties beschikbaar.
- AVG (EU-verordening 2016/679), art. 4 en 5 – definitie van persoonsgegevens en beginselen van verwerking (metadata zijn persoonsgegevens).

- EDPS en EDPB – adviezen over de verwerking van verkeersgegevens en metadata in elektronische communicatie (ePrivacy-richtlijn).

← VorigeEen korte geschiedenis van het lakzegelVolgende →Het beroepsgeheim in het digitale tijdperk

Recente artikelen

- CUADERNOS_LIST_PREGUNTAS_TITLE
- CUADERNOS_LIST_SELFHOST_TITLE
- CUADERNOS_LIST_IDENTIDAD_TITLE

Neem dit artikel mee naar waar u het nodig heeft.

↓ Markdown ↓ Platte tekst ↓ PDF

Het bestand wordt gedownload naar uw apparaat. Van daaruit kunt u het opslaan, importeren in Solo2 of delen waar u maar wilt. Cuadernos beslist niet voor u over de bestemming.

Lakzegel · SHA-256 9d622097c2173845fed119e92806308b3864c288a9408a9080e8fc41c6beea0f

Cuadernos Lacre · Een uitgave van Menzuri Gestión S.L. ·
geschreven door R.Eugenio · geredigeerd door het team van Solo2.