التشفير لا يعني الخصوصية: ماذا تقول البيانات الوصفية عنك

المحتوى المشفر والبيانات الوصفية المرئية شيئان مختلفان. عندما تتحدث خدمة ما عن "التشفير من طرف إلى طرف"، فإنها تروي نصف القصة فقط.

القفل الذي لا يحمي كل شيء

تعلن نسبة كبيرة من خدمات المراسلة اليوم عن تشفير من طرف إلى طرف. وهذا صحيح: محتوى الرسائل ينتقل مشفرًا، بحيث لا يستطيع أي شخص في الطريق – ولا حتى مزود الخدمة – قراءة النص أثناء نقله. حتى هنا، التصريح دقيق.

المشكلة هي أن المحتوى ليس سوى جزء من القصة. على الرغم من عدم تمكن أي شخص من قراءة ما تقوله، إلا أن الخدمة تعرف أشياء أخرى بدقة عالية جدًا: مع من تتحدث، وفي أي وقت، وكم مرة، ومن أي موقع تقريبي، وعلى أي جهاز، وكم عدد الرسائل التي ترسلها وكم عدد الرسائل التي تتلقاها، وكم عدد الملفات التي تشاركها. كل هذا يسمى البيانات الوصفية (metadata). والبيانات الوصفية، في كثير من الحالات، تقول الكثير بقدر ما تقوله الرسالة نفسها.

ما تكشفه البيانات الوصفية

لا يحتاج المرء لقراءة رسالة ليعرف أشياء كثيرة. إذا اتصل شخص أو كتب لطبيب أورام كل صباح ثلاثاء في الساعة التاسعة لمدة ستة أشهر، فليس من الضروري سماع المحادثة لتخمين ما يحدث. إذا تبادل شخصان مائة رسالة يوميًا وتوقفا فجأة، فلا داعي لقراءة أي منها لفهم ما حدث. إذا تلقى مستشار ضريبي عشرين رسالة متتالية من نفس العميل في ليلة ما قبل إغلاق ربع سنوي، فإن النمط يتحدث عن نفسه.

تكشف البيانات الوصفية عن أنماط سلوكية: من على علاقة بمن، وما هي جداول كل شخص، ومتى يكون مستيقظًا، ومتى ينام، ومتى يسافر، ومن هم العملاء الأكثر نشاطًا، ومن هي العلاقات المهنية الأكثر كثافة. يمكن للخادم الذي يجمع البيانات الوصفية بناء ملف تعريف مفصل للحياة الشخصية والمهنية لأي مستخدم دون قراءة كلمة واحدة مما يكتب.

هناك مثال تاريخي يوضح هذا بقسوة. صاغه المدير السابق لوكالة الأمن القومي (NSA)، مايكل هايدن، بصراحة في عام 2014: *"We kill people based on metadata"*. أشار التصريح إلى العمليات العسكرية الأمريكية ضد أهداف تم تحديدها حصريًا بناءً على أنماط اتصالاتهم. لا توجد رسالة واحدة مقروءة. فقط رسم بياني لجهات الاتصال والجداول الزمنية.

حقيقة أن الخدمة تجمع البيانات الوصفية لا تعني بالضرورة أنها ستستخدمها ضد مستخدميها. بل تعني أن لديها القدرة على القيام بذلك، وأن طرفًا ثالثًا لديه إمكانية الوصول إلى تلك البيانات – من خلال أمر قضائي، أو من خلال اختراق أمني، أو من خلال البيع لأطراف ثالثة إذا سمحت شروط الخدمة بذلك – لديه هذه القدرة أيضًا.

الوصول إلى دفتر العناوين

ناقل آخر يمر دون أن يلاحظه أحد تقريبًا: قائمة جهات الاتصال. تطلب نسبة كبيرة من خدمات المراسلة الوصول إلى دفتر عناوين الهاتف عند التسجيل. يقومون بتحميل جميع الأرقام إلى خادمهم لإظهار من يستخدم الخدمة أيضًا. ومنذ تلك اللحظة، تمتلك الشركة خريطة كاملة لعلاقات المستخدم، حتى لو لم يكتب رسالة واحدة لأي شخص.

بالنسبة للمهني الخاضع للسر المهني – محامٍ، طبيب، أخصائي نفسي، مستشار – يحتوي دفتر العناوين هذا على عملاء. إذا تم تحميل دفتر العناوين إلى خادم طرف ثالث، فإن أسماء العملاء توجد في بنية تحتية لا يتحكم المهني في ولايتها القضائية وسياساتها. لا يتم كسر السر المهني في اليوم الذي يسرب فيه شخص ما محادثة: لقد كسر قبل ذلك بكثير، في لحظة الموافقة على التحميل.

الفرق بين التشفير وعدم الجمع

التشفير هو حماية المحتوى. الخصوصية هي عدم جمع ما هو غير ضروري. هذه أشياء مختلفة، والفرق حاسم من الناحية التشغيلية. يمكن للخدمة تشفير جميع الرسائل بشكل مثالي وفي نفس الوقت معرفة كل شيء تقريبًا عن مستخدميها من خلال البيانات الوصفية. كلاهما متوافق تمامًا. في الواقع، هو نموذج العمل السائد في هذا القطاع.

السؤال الصحيح لتقييم الخصوصية الحقيقية لخدمة ما ليس *"هل تشفر المحتوى؟"*. هذا السؤال تمت الإجابة عليه منذ سنوات. السؤال الصحيح هو: *"ما هي البيانات الوصفية التي تولدها وأين يتم تخزينها؟"*. وقبل كل شيء: *"ما هي البيانات الوصفية التي لا تحتاج إلى توليدها؟"*.

بنية تحتية تقلل من البيانات الوصفية من خلال التصميم (privacy by design) – وليس من خلال الوعد، وليس من خلال السياسة الداخلية – هي أكثر خصوصية من الناحية الهيكلية من بنية تجمعها وتشفرها. لأن البيانات غير الموجودة لا يمكن تسريبها ولا بيعها ولا تسليمها لأمر قضائي ولا فقدانها في اختراق أمني.

للقارئ المهني

إذا كان نشاطك المهني يتضمن السرية أو الخصوصية أو مجرد احترام معلومات الأطراف الثالثة، فمن المفيد طرح الأسئلة بهذا الترتيب:

1. هل التطبيق الذي أستخدمه للاتصال يشفر المحتوى؟ (ربما نعم.)
2. هل يشفر البيانات الوصفية؟ (ربما لا.)
3. هل يولد بيانات وصفية *لا يحتاج إليها* للعمل؟ (من المؤكد تقريبًا نعم.)
4. أين يتم تخزين تلك البيانات الوصفية وتحت أي ولاية قضائية؟ (على الأرجح خارج المنطقة الاقتصادية الأوروبية.)
5. هل يعرف عميلي أو مريضي أن بياناته موجودة هناك؟

السؤال الأخير هو السؤال المزعج. لأن الإجابة الصادقة في معظم الحالات هي: لا.

هذا المقال هو الأول في سلسلة حول العمل الحقيقي لأدوات الاتصال المهنية. ستتناول الأعداد القادمة الامتثال لـ GDPR في المراسلة ومفهوم السر المهني في العصر الرقمي.

المصادر ومزيد من القراءة

- Hayden, M. – تصريح في جامعة جونز هوبكنز، 2014 ("We kill people based on metadata"). النصوص العامة متاحة.
- GDPR (لائحة الاتحاد الأوروبي 2016/679)، المادتان 4 و 5 – تعريف البيانات الشخصية ومبادئ المعالجة (البيانات الوصفية هي بيانات شخصية).
- المشرف الأوروبي لحماية البيانات و EDPB – آراء حول معالجة بيانات المرور والبيانات الوصفية في الاتصالات الإلكترونية (توجيه ePrivacy).

← السابقتاريخ موجز للختم الشمعيالتالي → السر المهني في العصر الرقمي

قراءات حديثة

- CUADERNOS_LIST_PREGUNTAS_TITLE
- CUADERNOS_LIST_SELFHOST_TITLE
- CUADERNOS_LIST_IDENTIDAD_TITLE

خذ هذا المقال معك أينما احتجت إليه.

↓ ماركداون ↓ نص عادي ↓ PDF

سيتم تنزيل الملف على جهازك. من هناك يمكنك حفظه، أو استيراده إلى Solo2 أو مشاركته أينما تريد. Cuadernos لا تقرر الوجهة نيابة عنك.

ختم شمعي · SHA-256 0b69208a2405efac52fca64fc3c7f395b3040d2d28708b367cff32c0fdf56a28

Cuadernos Lacre · منشور لشركة Menzuri Gestión S.L. ·
بقلم R.Eugenio · تحرير فريق Solo2.

هذا الموقع لا يستخدم ملفات تعريف الارتباط (cookies) ولا يحمل موارد من أطراف ثالثة. يستخدم عداد زيارات مجهول مستضاف ذاتيًا (Umami، على خادمنا الأوروبي) والحد الأدنى من JavaScript اللازم لتفضيل المظهر الفاتح/الداكن. لا يوجد متتبعون، لا يوجد تصنيف، لا توجد مشاركة بيانات. إذا كنت ترغب في متابعتنا: RSS.