رمزنگاری به معنای حریم خصوصی نیست: مِتادیتا درباره شما چه می‌گوید

محتوای رمزنگاری شده و متادیتاهای آشکار، دو مقوله متفاوت هستند. وقتی یک سرویس از «رمزنگاری سرتاسری» صحبت می‌کند، فقط نیمی از داستان را می‌گوید.

قفلی که از همه چیز محافظت نمی‌کند

بخش بزرگی از سرویس‌های پیام‌رسان امروزی رمزنگاری سرتاسری را تبلیغ می‌کنند. و این درست است: محتوای پیام‌ها به صورت رمزنگاری شده منتقل می‌شود، به طوری که هیچ‌کس در مسیر – حتی ارائه‌دهنده سرویس – نمی‌تواند متن را در حین انتقال بخواند. تا اینجا، این ادعا دقیق است.

مشکل اینجاست که محتوا فقط بخشی از داستان است. اگرچه هیچ‌کس نمی‌تواند آنچه را که می‌گویید بخواند، اما سرویس چیزهای دیگری را با دقت بسیار بالا می‌داند: با چه کسی صحبت می‌کنید، در چه زمانی، چند وقت یک‌بار، از چه مکان تقریبی، روی چه دستگاهی، چند پیام می‌فرستید و چند پیام دریافت می‌کنید، چه تعداد فایل به اشتراک می‌گذارید. به همه این‌ها مِتادیتا (metadata) یا فراداده گفته می‌شود. و متادیتا در بسیاری از موارد تقریباً به اندازه خود پیام حرف برای گفتن دارد.

آنچه متادیتا فاش می‌کند

نیازی به خواندن یک پیام برای دانستن بسیاری از چیزها نیست. اگر فردی به مدت شش ماه هر سه شنبه صبح ساعت نه با یک متخصص سرطان تماس بگیرد یا به او پیام بدهد، نیازی به شنیدن گفتگو نیست تا حدس بزنید چه خبر است. اگر دو نفر در روز صد پیام رد و بدل کنند و ناگهان متوقف شوند، نیازی به خواندن هیچ‌کدام برای درک اتفاقی که افتاده نیست. اگر یک مشاور مالیاتی در شب قبل از بستن حساب‌های فصلی، بیست پیام پشت سر هم از همان مشتری دریافت کند، این الگو خود گویای همه چیز است.

متادیتا الگوهای رفتاری را فاش می‌کند: چه کسی با چه کسی در ارتباط است، جدول زمانی هر فرد چیست، چه زمانی بیدار است، چه زمانی می‌خوابد، چه زمانی سفر می‌کند، کدام مشتریان فعال‌تر هستند، کدام روابط کاری فشرده‌تر هستند. سروری که متادیتا جمع‌آوری می‌کند، می‌تواند بدون خواندن حتی یک کلمه از آنچه کاربر می‌نویسد، یک پروفایل دقیق از زندگی شخصی و حرفه‌ای او بسازد.

یک مثال تاریخی وجود دارد که این موضوع را با صراحت نشان می‌دهد. مدیر سابق NSA، مایکل هایدن، در سال ۲۰۱۴ آن را بدون پرده‌پوشی بیان کرد: *«We kill people based on metadata»*. این جمله به عملیات نظامی ایالات متحده علیه اهدافی اشاره داشت که صرفاً بر اساس الگوهای ارتباطی آن‌ها شناسایی شده بودند. حتی یک پیام خوانده نشده. فقط نمودار مخاطبان و جداول زمانی.

اینکه یک سرویس متادیتا جمع‌آوری می‌کند، لزوماً به این معنی نیست که از آن‌ها علیه کاربرانش استفاده خواهد کرد. این به آن معناست که توانایی انجام این کار را دارد و شخص ثالثی که به آن داده‌ها دسترسی داشته باشد – از طریق حکم دادگاه، از طریق یک حفره امنیتی یا از طریق فروش به اشخاص ثالث در صورت اجازه شرایط سرویس – نیز این توانایی را خواهد داشت.

دسترسی به دفترچه تلفن

ناقل دیگری که تقریباً نادیده گرفته می‌شود: لیست مخاطبان. بخش بزرگی از سرویس‌های پیام‌رسان در هنگام ثبت‌نام درخواست دسترسی به دفترچه تلفن را دارند. آن‌ها تمام شماره‌ها را روی سرور خود آپلود می‌کنند تا نشان دهند چه کسانی دیگر از سرویس استفاده می‌کنند. از آن لحظه به بعد، شرکت یک نقشه کامل از روابط کاربر دارد، حتی اگر او هرگز پیامی برای کسی ننوشته باشد.

برای یک متخصص دارای تعهد به رازداری حرفه‌ای – وکیل، پزشک، روانشناس، مشاور – آن دفترچه تلفن حاوی مشتریان است. اگر دفترچه تلفن روی سرور شخص ثالث آپلود شده باشد، اسامی مشتریان در زیرساختی قرار می‌گیرد که متخصص بر حوزه قضایی و سیاست‌های آن کنترلی ندارد. رازداری حرفه‌ای در روزی که کسی یک گفتگو را لو می‌دهد فاش نمی‌شود: خیلی زودتر، در لحظه موافقت با آپلود، فاش شده است.

تفاوت بین رمزنگاری و عدم جمع‌آوری

رمزنگاری یعنی محافظت از محتوا. خصوصی بودن یعنی جمع‌آوری نکردن آنچه مورد نیاز نیست. این‌ها مقوله‌های متفاوتی هستند و تفاوت آن‌ها از نظر عملیاتی تعیین‌کننده است. یک سرویس می‌تواند تمام پیام‌ها را به طور کامل رمزنگاری کند و در عین حال تقریباً همه چیز را درباره کاربرانش از طریق متادیتا بداند. هر دو با هم کاملاً سازگار هستند. در واقع، این مدل تجاری غالب در این صنعت است.

سوال درست برای ارزیابی حریم خصوصی واقعی یک سرویس این نیست که «*آیا محتوا را رمزنگاری می‌کند؟*». سال‌هاست که به این سوال پاسخ داده شده است. سوال درست این است: «*چه متادیتاهایی تولید می‌کند و کجا ذخیره می‌شوند؟*». و فراتر از همه: «*چه متادیتاهایی را نیاز ندارد تولید کند؟*».

معماری‌ای که متادیتاها را از طریق طراحی (privacy by design) به حداقل می‌رساند – نه از طریق وعده، نه از طریق سیاست داخلی – به طور ساختاری خصوصی‌تر از معماری‌ای است که آن‌ها را جمع‌آوری و رمزنگاری می‌کند. زیرا داده‌هایی که وجود ندارند، نه می‌توانند لو بروند، نه فروخته شوند، نه به حکم دادگاه تسلیم شوند و نه در یک نفوذ امنیتی از دست بروند.

برای خواننده حرفه‌ای

اگر فعالیت حرفه‌ای شما شامل راز، محرمانگی یا صرفاً احترام به اطلاعات اشخاص ثالث است، ارزش دارد که سوالات را به این ترتیب بپرسید:

1. آیا اپلیکیشنی که برای ارتباط استفاده می‌کنم، محتوا را رمزنگاری می‌کند؟ (احتمالاً بله.)
2. آیا متادیتا را رمزنگاری می‌کند؟ (احتمالاً خیر.)
3. آیا متادیتاهایی تولید می‌کند که برای کار کردن به آن‌ها *نیاز ندارد*؟ (تقریباً به طور قطع بله.)
4. آن متادیتاها کجا و تحت کدام حوزه قضایی ذخیره می‌شوند؟ (احتمالاً خارج از منطقه اقتصادی اروپا.)
5. آیا مشتری یا بیمار من می‌داند که داده‌هایش آنجاست؟

سوال آخر همان سوال آزاردهنده است. زیرا پاسخ صادقانه در اکثر موارد این است: خیر.

این مقاله اولین مقاله از یک مجموعه درباره عملکرد واقعی ابزارهای ارتباطی حرفه‌ای است. شماره‌های بعدی به انطباق با GDPR در پیام‌رسانی و مفهوم رازداری حرفه‌ای در عصر دیجیتال خواهند پرداخت.

منابع و مطالعه بیشتر

- هایدن، م. – اظهارات در دانشگاه جانز هاپکینز، ۲۰۱۴ («We kill people based on metadata»). متن‌های عمومی موجود است.

- GDPR (مقررات اتحادیه اروپا 2016/679)، مواد ۴ و ۵ – تعریف داده‌های شخصی و اصول پردازش (متادیتا داده شخصی محسوب می‌شود).
- ناظر حفاظت از داده‌های اروپا و EDPB – نظرات درباره پردازش داده‌های ترافیکی و متادیتا در ارتباطات الکترونیک (دستورالعمل ePrivacy).

← السابقتاریخچه‌ای کوتاه از مهر و مومالتالي → رازداری حرفه‌ای در عصر دیجیتال

قراءات حديثة

- CUADERNOS_LIST_PREGUNTAS_TITLE
- CUADERNOS_LIST_SELFHOST_TITLE
- CUADERNOS_LIST_IDENTIDAD_TITLE

این مقاله را هر کجا که نیاز دارید همراه خود ببرید.

↓ مارک‌داون ↓ متن ساده ↓ PDF

فایل در دستگاه شما دانلود خواهد شد. از آنجا می‌توانید آن را ذخیره کنید، به Solo2 وارد کنید یا در هر کجا که می‌خواهید به اشتراک بگذارید. Cuadernos مقصد را برای شما تعیین نمی‌کند.

ختم شمعي · SHA-256 d8635721264d08e1af6d00908213b01f919f6871ab5b9778a3e5a19427c695ee

Cuadernos Lacre · نشريّة من Menzuri Gestión S.L. ·
كتبها R.Eugenio · حرّرها فريق Solo2.