عندما لا يوجد أحد في المنتصف

تشفير ما يمر عبر خادم يحمي المحتوى. عدم وجود خادم في المنتصف يلغي السؤال. إنهما ليسا نفس الشيء.

ببساطة: عندما تتحدث وجهًا لوجه مع شخص ما، لا يحتاج أي شخص آخر إلى أن يعدك بأنه لم يستمع. لم يستمع لأنه لم يكن هناك. هذه هي أقوى نسخة من الخصوصية: ليست وعدًا من وسيط يتصرف بشكل جيد — بل غياب الوسيط.

شخصان، محادثة واحدة

عندما يتحدث شخصان وجهًا لوجه في غرفة، لا يحتاج أي شخص آخر إلى أن يعد بأنه لم يسمع شيئًا. لم يسمع لأنه لم يكن هناك. عندما يمرر شخصان ورقة من يد إلى أخرى، لا يحتاج أحد في المنتصف إلى القسم بأنه لم يقرأها. لا يوجد أحد في المنتصف.

معظم الأشياء في الحياة اليومية تعمل بهذه الطريقة. نحن لا نوقع اتفاقيات سرية مع الهواء الذي ينقل صوتنا، ولا مع الورق الذي نمسكه. خصوصية المحادثة لا تعتمد على وعد وسيط، لأنه لا يوجد وسيط. هذا أحد أقوى أشكال الخصوصية الموجودة: ليس لأن شيئًا أو شخصًا ما يتصرف بشكل جيد، بل لعدم وجود شيء أو شخص.

عندما تنتقل المحادثة إلى قناة رقمية، يتغير هذا افتراضيًا. النموذج المعتاد هو كالتالي: يتصل شخصان بخادم، يتلقى الخادم الرسالة، يشفرها أو يحفظها مشفرة، ويسلمها إلى المستلم. الخادم موجود في المنتصف. قد يكون الخادم صادقًا. قد يكون مدققًا. قد يعمل في ولاية قضائية مواتية وتحت سياسة خصوصية صارمة. كل هذا قد يكون صحيحًا. لكن الخادم في المنتصف.

الفرق بين التشفير وعدم الجمع (الجزء الثاني)

في مقال سابق من هذه السلسلة نفسها، زعمنا أن تشفير المحتوى وعدم جمع البيانات الوصفية (metadata) ليسا نفس الشيء. هناك خطوة أبعد يجدر صياغتها بوضوح: تشفير ما يمر عبر خادم وعدم وجود خادم ليسا نفس الشيء أيضًا.

النموذج الأول — خادم في المنتصف، محتوى مشفر — يحمي المحتوى من مشغل الخادم، ومن موظفي الصيانة، ومن مهاجم خارجي يخترق النظام. وهذا أمر مهم. لكنه لا يلغي الخادم. لا يزال الخادم هناك. لا يزال يعالج البيانات الوصفية. لا يزال نقطة يمكن أن تتلقى طلبًا قضائيًا، أو تدخلًا قانونيًا، أو ضغطًا سياسيًا، أو خرقًا أمنيًا. لا يزال نقطة تتطلب وضع الثقة في شخص ما.

النموذج الثاني — عدم وجود خادم بين الطرفين — لا يحمي المحتوى المشفر بشكل أفضل: إذا كان التشفير قويًا، فسيكون المحتوى محميًا في كلتا الحالتين. ما يتغير ليس المحتوى. ما يتغير هو أن السؤال «*ماذا يحدث مع الخادم؟*» لم يعد له موضوع، لأنه لا يوجد خادم للسؤال عنه.

الثقة، الغياب، والفرق بينهما

قد تكون الثقة في محلها. توجد شركات صادقة. يوجد مدققون صارمون. توجد تشريعات مواتية للمستخدم. توجد خدمات جادة تلتزم بدقة بكل ما سبق. الثقة، عندما تُمنح لمشغل يستحقها، ليست ترتيبًا سيئًا.

لكن الثقة، مهما كانت صلبة، تظل ثقة. إنها حل اجتماعي، وليست حلاً تقنيًا. يمكن لشركة أن تتغير ملكيتها. يمكن لولاية قضائية أن يتغير نظام حكمها. قد يصل أمر قضائي غدًا. قد يتم اكتشاف ثغرة جديدة الشهر المقبل. لا يحدث أي من هذا بسوء نية. يحدث لأن المشغل موجود، وكل ما هو موجود يخضع لتقلبات العالم.

غياب المشغل لا يخضع لتلك التقلبات نفسها. لا يمكن لأمر قضائي أن يطلب بيانات من خادم غير موجود. لا يمكن لمهاجم أن يخترق خادمًا غير موجود. لا يمكن لتغيير في سياسة شركة أن يؤثر على بيانات لم تمتلكها تلك الشركة أبدًا. الجملة المفتاحية بسيطة: البيانات غير الموجودة لا يمكن فقدانها.

حول الحجة المشروعة لجانب الخادم

من يقدم خدمة مراسلة مهنية مع خادم في المنتصف عادة ما يصيغ ثلاث حجج صالحة تمامًا. أولاً، أن الخادم ضروري لضمان التسليم عندما يكون المستلم غير متصل. ثانياً، أن تشفير المحتوى قوي وبالتالي لا يستطيع المشغل قراءته. ثالثاً، أن الخدمة تمتثل للتشريعات الأوروبية وأن البيانات محمية بموجب القانون.

الحجج الثلاث صحيحة. لا شيء منها يغير طبيعة الأمر. صحيح أن الخادم يسمح بتخزين الرسائل للتسليم المؤجل؛ صحيح أيضًا أن التسليم المؤجل يمكن حله بطريقة أخرى، من خلال بروتوكولات التواصل المباشر بين الأجهزة التي تم صقلها منذ عقود وتعمل اليوم. صحيح أن تشفير المحتوى أثناء النقل قوي في الخدمات الجادة. وصحيح أن التشريعات الأوروبية تحمي المستخدمين أكثر من العديد من الأماكن الأخرى.

المسألة ليست ما إذا كانت الخدمات التي تحتوي على خادم في المنتصف قانونية، ولا ما إذا كانت آمنة، ولا ما إذا كانت تحمي المحتوى. يمكن أن تكون كذلك، وهي قانونية، وعادة ما تكون آمنة. المسألة هي أن وجود خادم في المنتصف هو خيار بنيوي، وليس فرضًا تقنيًا. ولكل خيار عواقب. البنية التي تحتوي على خادم في المنتصف تولد بالضرورة طرقًا يجب الوثوق به. البنية التي لا تحتوي على خادم في المنتصف لا تفعل ذلك.

ما يقوله القانون، وما تفعله البنية

لا يتطلب الـ RGPD نموذجًا بنيويًا محددًا. إنه يتطلب نتائج: تقليل البيانات، تحديد الغرض، الحماية من خلال التصميم وبشكل افتراضي، والقدرة على إثبات الامتثال. يمكن للخدمة التي تحتوي على خادم في المنتصف أن تلبي جميع هذه المتطلبات. الخدمة التي لا تحتوي على خادم في المنتصف تلبي العديد منها من خلال البناء، وليس من خلال التصريح. التقليل المطلق — عدم جمع أي شيء ليس ضروريًا تمامًا لتسليم الرسالة — هو أمر بديهي عندما لا يوجد خادم يمكنه جمع أي شيء.

للاستخدامات اليومية غير الحساسة، تعد البنية القائمة على خادم معقولة تمامًا، والثقة في مشغل جاد هي ترتيب صالح. للاستخدامات الأخرى — تلك التي تنطوي على سر مهني منظم، وتلك التي تترتب عليها مسؤولية أخلاقية، وتلك التي تمس معلومات حساسة بشكل خاص — فإن غياب نقطة الثقة ليس رفاهية، بل هو ميزة هيكلية.

للقارئ المهني

الأسئلة التي يجدر طرحها أمام خدمة تواصل مهنية، والمألوفة بالفعل من المقالات السابقة في هذه السلسلة نفسها، تكتمل بسؤال بنيوي واحد إضافي:

1. هل يشفر المحتوى أثناء النقل؟ (على الأرجح نعم.)
2. هل يولد ويخزن بيانات وصفية (metadata) حول من أتحدث معه ومتى؟ (على الأرجح نعم.)
3. هل يوجد خادم في الطريق بين جهازي وجهاز المستلم؟
4. إذا كان موجودًا: من يشغله، وفي أي ولاية قضائية، وماذا يجب أن يحدث حتى يسلم بيانات عني؟
5. إذا لم يكن موجودًا: الأسئلة السابقة لا موضوع لها.

الفرق بين الفئتين ليس في الدرجة، بل في النوع. عندما يحين الوقت لشرح ذلك لعميل أو مريض أو زميل، فإن الصياغة الأكثر صدقًا هي أيضًا الأكثر بساطة: في واحدة يوجد شخص ما في المنتصف؛ في الأخرى، لا يوجد.

يختتم هذا المقال الدورة الأولية لـ Cuadernos Lacre. بعد التحدث عن التشفير والبيانات الوصفية والسر المهني، نكمل اللوحة البنيوية: تشفير المحتوى وعدم وجود خادم في المنتصف هما شيئان مختلفان. يمكن أن يكون كلاهما قانونيًا؛ واحد فقط يلغي نقطة الثقة.

ملاحظة هيئة التحرير: عندما تذكر هذه الـ Cuadernos شركات أو منتجات، فليس ذلك للاتهام. فالذين يبنونها يقومون بأعمال يستخدمها الملايين ويقدرونها. ما نشير إليه هو هيكلي — النموذج، وليس العلامة التجارية. تظهر العلامات التجارية كأمثلة لأنها التي يتعرف عليها القارئ.

المصادر ومزيد من القراءة

- سالتزر، ج. هـ.؛ ريد، د. ب.؛ كلارك، د. د. — *End-to-end arguments in system design*، ACM TOCS، 1984. النص التأسيسي للمبدأ الذي ينص على أن ضمانات النظام يجب أن تُنفذ في الأطراف، وليس في القناة الوسيطة.
- اللائحة (UE) 2016/679، المادة 25 — حماية البيانات من خلال التصميم وبشكل افتراضي.
- اللائحة (UE) 2016/679، المادة c.5.1 — مبدأ تقليل البيانات.
- شناير، ب. — *Data and Goliath: the hidden battles to collect your data and control your world* (2015)، W. W. Norton. فصول حول البنيات التي تقلل الجمع من خلال البناء.

← السابقGDPR والمراسلات المهنية: لماذا ينتهك معظم الناس القواعد دون علمهمالتالي → Schrems II، بعد مرور خمس سنوات

قراءات حديثة

- تحليل · ١٨ مايو ٢٠٢٦ الخصوصية الحقيقية مقابل الظاهرية: الأسئلة التي ينبغي طرحها
- تحليل · ١٨ مايو ٢٠٢٦ الاستضافة الذاتية كممارسة مهنية
- مفهوم · ١٨ مايو ٢٠٢٦ الـ 24 كلمة: ما هي الهوية التشفيرية

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 7674362364475107b7e6e02160ec82ed51ff3c735b60883d68e54d38310abe5f

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

هذا الموقع لا يستخدم ملفات تعريف الارتباط ولا يحمل موارد من جهات خارجية. يستخدم عداد زيارات مجهول مستضاف ذاتيًا (Umami، على خادمنا الأوروبي) والحد الأدنى من جافا سكريبت اللازم لعنصري التحكم في الرأس: المظهر الفاتح أو الداكن، ومحدد اللغة. بدون أدوات تتبع، بدون بروفايل، بدون مشاركة بيانات. إذا كنت تريد متابعتنا: RSS.