जब बीच में कोई न हो

सर्वर के माध्यम से जो गुजरता है उसे एन्क्रिप्ट करना सामग्री की सुरक्षा करता है। बीच में सर्वर न होने से प्रश्न ही समाप्त हो जाता है। वे एक ही बात नहीं हैं।

दो लोग, एक बातचीत

जब दो लोग एक कमरे में आमने-सामने बात करते हैं, तो किसी को यह वादा नहीं करना पड़ता कि उन्होंने कुछ नहीं सुना। उन्होंने नहीं सुना क्योंकि वे वहां नहीं थे। जब दो लोग एक हाथ से दूसरे हाथ में कागज पास करते हैं, तो बीच में किसी को कसम नहीं खानी पड़ती कि उन्होंने इसे नहीं पढ़ा है। बीच में कोई नहीं है।

रोजमर्रा की जिंदगी में ज्यादातर चीजें इसी तरह काम करती हैं। हम अपनी आवाज प्रसारित करने वाली हवा के साथ, या हमारे द्वारा पकड़े गए कागज के साथ गोपनीयता समझौतों पर हस्ताक्षर नहीं करते हैं। बातचीत की गोपनीयता किसी मध्यस्थ के वादे पर टिकी नहीं होती है, क्योंकि कोई मध्यस्थ नहीं होता है। निजी होने का यह सबसे मजबूत रूपों में से एक है: इसलिए नहीं कि कुछ या कोई अच्छा व्यवहार करता है, बल्कि इसलिए कि वहां कुछ या कोई है ही नहीं।

जब बातचीत डिजिटल चैनल पर चली जाती है, तो यह डिफ़ॉल्ट रूप से बदल जाती है। सामान्य मॉडल इस प्रकार है: दो लोग एक सर्वर से जुड़ते हैं, सर्वर संदेश प्राप्त करता है, इसे एन्क्रिप्ट करता है या इसे एन्क्रिप्टेड रखता है, और इसे प्राप्तकर्ता को वितरित करता है। सर्वर बीच में है। सर्वर ईमानदार हो सकता है। इसका ऑडिट किया जा सकता है। यह अनुकूल अधिकार क्षेत्र और सख्त गोपनीयता नीति के तहत काम कर सकता है। यह सब सच हो सकता है। लेकिन सर्वर बीच में है।

एन्क्रिप्ट करने और एकत्र न करने के बीच का अंतर (दूसरा भाग)

इसी श्रृंखला के पिछले लेख में हम तर्क देते हैं कि सामग्री को एन्क्रिप्ट करना और मेटाडेटा एकत्र न करना एक ही बात नहीं है। एक और कदम है जिसे स्पष्ट रूप से तैयार किया जाना चाहिए: सर्वर के माध्यम से जो गुजरता है उसे एन्क्रिप्ट करना और सर्वर न होना भी एक ही बात नहीं है।

पहला मॉडल — बीच में सर्वर, एन्क्रिप्टेड सामग्री — सर्वर ऑपरेटर, उसके रखरखाव कर्मचारियों, सिस्टम से समझौता करने वाले बाहरी हमलावर से सामग्री की सुरक्षा करता है। और यह महत्वपूर्ण है। लेकिन यह सर्वर को खत्म नहीं करता है। सर्वर अभी भी वहीं है। यह मेटाडेटा को संसाधित करना जारी रखता है। यह अभी भी एक ऐसा बिंदु है जो न्यायिक आवश्यकता, कानूनी हस्तक्षेप, राजनीतिक दबाव या सुरक्षा उल्लंघन प्राप्त कर सकता है। यह अभी भी एक ऐसा बिंदु है जिसके लिए किसी पर भरोसा करने की आवश्यकता होती है।

दूसरा मॉडल — दो सिरों के बीच कोई सर्वर नहीं होना — एन्क्रिप्टेड सामग्री को बेहतर सुरक्षा नहीं देता है: यदि क्रिप्टोग्राफी ठोस है, तो सामग्री दोनों मामलों में सुरक्षित है। सामग्री क्या नहीं बदलती है। जो बदलता है वह यह है कि प्रश्न *"सर्वर का क्या होता है?"* अब प्रासंगिक नहीं रह जाता है, क्योंकि प्रश्न पूछने के लिए कोई सर्वर ही नहीं है।

विश्वास, अनुपस्थिति, और दोनों के बीच का अंतर

विश्वास अच्छी तरह से रखा जा सकता है। ईमानदार कंपनियां मौजूद हैं। कठोर ऑडिटर मौजूद हैं। उपयोगकर्ता के अनुकूल कानून मौजूद हैं। गंभीर सेवाएं जो उपरोक्त सभी का ईमानदारी से पालन करती हैं, मौजूद हैं। विश्वास, जब किसी ऐसे ऑपरेटर को दिया जाता है जो इसका हकदार है, तो यह कोई बुरा समझौता नहीं है।

लेकिन विश्वास, चाहे वह कितना भी ठोस क्यों न हो, विश्वास ही बना रहता है। यह एक सामाजिक समाधान है, तकनीकी समाधान नहीं। कंपनी हाथ बदल सकती है। एक अधिकार क्षेत्र सरकार बदल सकता है। कल एक अदालती आदेश आ सकता है। अगले महीने एक नई भेद्यता का पता चल सकता है। इसमें से कुछ भी बुरी नीयत से नहीं होता है। यह इसलिए होता है क्योंकि ऑपरेटर मौजूद है, और जो कुछ भी मौजूद है वह दुनिया की आकस्मिकताओं के अधीन है।

ऑपरेटर की अनुपस्थिति उन समान आकस्मिकताओं के अधीन नहीं है। एक अदालती आदेश उस सर्वर से डेटा नहीं मांग सकता जो मौजूद नहीं है। एक हमलावर उस सर्वर से समझौता नहीं कर सकता जो मौजूद नहीं है। कंपनी की नीति में बदलाव उन डेटा को प्रभावित नहीं कर सकता जो उस कंपनी के पास कभी थे ही नहीं। मुख्य वाक्यांश सरल है: जो डेटा मौजूद नहीं है उसे खोया नहीं जा सकता।

सर्वर साइड के वैध तर्क के बारे में

जो बीच में सर्वर के साथ एक पेशेवर मैसेजिंग सेवा प्रदान करता है, वह आमतौर पर तीन पूरी तरह से वैध तर्क देता है। पहला, प्राप्तकर्ता के डिस्कनेक्ट होने पर डिलीवरी सुनिश्चित करने के लिए सर्वर आवश्यक है। दूसरा, सामग्री एन्क्रिप्शन मजबूत है और इसलिए ऑपरेटर इसे पढ़ नहीं सकता है। तीसरा, सेवा यूरोपीय कानून का पालन करती है और डेटा कानून द्वारा संरक्षित है।

तीनों तर्क सत्य हैं। इनमें से कोई भी मामले की प्रकृति को नहीं बदलता है। यह सच है कि सर्वर विलंबित डिलीवरी के लिए संदेशों को संग्रहीत करने की अनुमति देता है; यह भी सच है कि विलंबित डिलीवरी को किसी अन्य तरीके से हल किया जा सकता है, उपकरणों के बीच प्रत्यक्ष संचार प्रोटोकॉल के माध्यम से जो दशकों से परिष्कृत हैं और आज परिचालन में हैं। यह सच है कि गंभीर सेवाओं में पारगमन में सामग्री एन्क्रिप्शन मजबूत है। और यह सच है कि यूरोपीय कानून कई अन्य स्थानों की तुलना में उपयोगकर्ताओं की अधिक रक्षा करता है।

सवाल यह नहीं है कि बीच में सर्वर वाली सेवाएं कानूनी हैं या नहीं, या वे सुरक्षित हैं या नहीं, या वे सामग्री की रक्षा करती हैं या नहीं। वे हो सकते हैं, वे कानूनी हैं, और वे आमतौर पर सुरक्षित हैं। मुद्दा यह है कि बीच में सर्वर होना एक वास्तुकला संबंधी विकल्प है, तकनीकी थोपना नहीं। और प्रत्येक विकल्प के परिणाम होते हैं। बीच में सर्वर वाली वास्तुकला आवश्यक रूप से एक ऐसा अभिनेता उत्पन्न करती है जिस पर भरोसा किया जाना चाहिए। बीच में सर्वर के बिना वास्तुकला नहीं।

कानून क्या कहता है, और वास्तुकला क्या करती है

GDPR किसी विशिष्ट वास्तुकला मॉडल की मांग नहीं करता है। इसके लिए परिणामों की आवश्यकता होती है: डेटा न्यूनीकरण, सीमित उद्देश्य, डिजाइन द्वारा और डिफ़ॉल्ट रूप से सुरक्षा, अनुपालन प्रदर्शित करने की क्षमता। बीच में सर्वर वाली सेवा इन सभी आवश्यकताओं को पूरा कर सकती है। बीच में सर्वर के बिना सेवा निर्माण द्वारा उनमें से कई का अनुपालन करती है, घोषणा द्वारा नहीं। पूर्ण न्यूनीकरण — संदेश देने के लिए जो कड़ाई से आवश्यक है उसे छोड़कर कुछ भी एकत्र नहीं करना — तुच्छ है जब ऐसा कोई सर्वर नहीं है जो कुछ भी एकत्र कर सके।

गैर-संवेदनशील रोजमर्रा के उपयोगों के लिए, सर्वर वाली वास्तुकला पूरी तरह से उचित है, और एक गंभीर ऑपरेटर में विश्वास एक वैध व्यवस्था है। अन्य उपयोगों के लिए — जो विनियमित व्यावसायिक गोपनीयता रखते हैं, जिनमें नैतिक जिम्मेदारी शामिल है, जो विशेष रूप से संवेदनशील जानकारी को छूते हैं — विश्वास बिंदु की अनुपस्थिति कोई विलासिता नहीं है, यह एक संरचनात्मक लाभ है।

पेशेवर पाठक के लिए

एक पेशेवर संचार सेवा का सामना करते समय पूछे जाने वाले प्रश्न, जो इस श्रृंखला के पिछले लेखों से पहले से ही परिचित हैं, एक और वास्तुशिल्प प्रश्न के साथ पूरे होते हैं:

1. क्या यह पारगमन में सामग्री को एन्क्रिप्ट करता है? (संभवतः हाँ।)
2. क्या यह इस बारे में मेटाडेटा उत्पन्न और संग्रहीत करता है कि मैं किससे और कब बात करता हूँ? (संभवतः हाँ।)
3. क्या मेरे डिवाइस और प्राप्तकर्ता के डिवाइस के बीच रास्ते में कोई सर्वर है?
4. यदि मौजूद है: इसे कौन संचालित करता है, किस अधिकार क्षेत्र में है, और मेरे बारे में डेटा देने के लिए क्या होना होगा?
5. यदि मौजूद नहीं है: पिछले प्रश्नों का कोई औचित्य नहीं है।

दो श्रेणियों के बीच का अंतर डिग्री का नहीं, बल्कि प्रकार का है। जब किसी ग्राहक, मरीज़ या सहकर्मी को इसे समझाने का समय आता है, तो सबसे ईमानदार सूत्रीकरण सबसे सरल भी होता है: एक में बीच में कोई होता है; दूसरे में, नहीं।

यह लेख Cuadernos Lacre के प्रारंभिक चक्र को समाप्त करता है। एन्क्रिप्शन, मेटाडेटा और व्यावसायिक गोपनीयता के बारे में बात करने के बाद, हम वास्तुशिल्प तस्वीर को पूरा करते हैं: सामग्री को एन्क्रिप्ट करना और बीच में सर्वर नहीं होना अलग चीजें हैं। दोनों कानूनी हो सकते हैं; केवल एक ही विश्वास बिंदु को समाप्त करता है।

स्रोत और आगे पढ़ने के लिए

- Saltzer, J. H.; Reed, D. P.; Clark, D. D. — *End-to-end arguments in system design*, ACM TOCS, 1984. उस सिद्धांत का मूलभूत पाठ जिसके अनुसार सिस्टम की गारंटी को सिरों पर लागू किया जाना चाहिए, मध्यवर्ती चैनल में नहीं।
- विनियमन (ईयू) 2016/679, कला। 25 — डिजाइन द्वारा और डिफ़ॉल्ट रूप से डेटा सुरक्षा।
- विनियमन (ईयू) 2016/679, कला। 5.1.c — डेटा न्यूनीकरण का सिद्धांत।
- Schneier, B. — *Data and Goliath: the hidden battles to collect your data and control your world* (2015), W. W. Norton. उन वास्तुकलाओं पर अध्याय जो निर्माण द्वारा संग्रह को कम करते हैं।

← पिछलाGDPR और पेशेवर संदेश सेवा: क्यों अधिकांश लोग अनजाने में नियमों का उल्लंघन करते हैंअगला
→CUADERNOS_LIST_SCHREMS_TITLE

हाल की रीडिंग

- CUADERNOS_LIST_PREGUNTAS_TITLE
- CUADERNOS_LIST_SELFHOST_TITLE
- CUADERNOS_LIST_IDENTIDAD_TITLE

इस लेख को अपने साथ ले जाएं जहाँ भी आपको इसकी आवश्यकता हो।

↓ मार्कडाउन ↓ सादा टेक्स्ट ↓ PDF

फ़ाइल आपके डिवाइस पर डाउनलोड हो जाएगी। वहां से आप इसे सहेज सकते हैं, Solo2 में आयात कर सकते हैं या जहां चाहें साझा कर सकते हैं। Cuadernos आपके लिए गंतव्य तय नहीं करता है।

मोहरबंद · SHA-256 aa226c174e2144665d3c4befe21c07bc565bc0dd0e5e8311b7feb0c06e99b2d1

Cuadernos Lacre · Menzuri Gestión S.L. का एक प्रकाशन ·
R.Eugenio द्वारा लिखित · Solo2 की टीम द्वारा संपादित।

आवश्यक न्यूनतम जावास्क्रिप्ट का उपयोग करती है। कोई ट्रैकर नहीं, कोई प्रोफाइलिंग नहीं, कोई डेटा साझाकरण नहीं। यदि आप हमें फॉलो करना चाहते हैं: RSS।