

การเข้ารหัสไม่ได้หมายถึงความเป็นส่วนตัว: Metadata บอกอะไรเกี่ยวกับคุณบ้าง

เนื้อหาที่ถูกเข้ารหัสกับ Metadata ที่มองเห็นได้คือคนละเรื่องกัน เมื่อบริการหนึ่งพูดถึง "การเข้ารหัสแบบ end-to-end" นั้นเป็นเพียงครึ่งเดียวของเรื่องราวทั้งหมด

คุณแจที่ไม่ได้ปกป้องทุกอย่าง

บริการส่งข้อความส่วนใหญ่ในปัจจุบันโฆษณาเรื่องการเข้ารหัสแบบ end-to-end ซึ่งเป็นเรื่องจริงที่เนื้อหาข้อความจะถูกเข้ารหัสระหว่างการเดินทาง ทำให้ไม่มีใครในระหว่างทาง แม้แต่ผู้ให้บริการเอง ก็สามารถอ่านข้อความขณะที่มีการส่งได้ จนถึงจุดนี้ คำกล่าวนี้ถือว่าถูกต้อง

ปัญหาคือเนื้อหาเป็นเพียงส่วนหนึ่งของเรื่องราวเท่านั้น แม้ว่าจะไม่มีใครอ่านสิ่งที่คุณพูดได้ แต่บริการจะรู้สิ่งอื่นด้วยความแม่นยำสูงมาก: คุณคุยกับใคร เวลาไหน บ่อยแค่ไหน จากตำแหน่งที่ตั้งโดยประมาณใด บนอุปกรณ์อะไร คุณส่งและรับข้อความที่ข้อความ คุณแชร์ไฟล์ที่ไฟล์ ทั้งหมดนี้เรียกว่า Metadata และในหลายกรณี Metadata บอกข้อมูลได้เกือบเท่ากับตัวข้อความเอง

Metadata เปิดเผยอะไรบ้าง

ไม่จำเป็นต้องอ่านข้อความก็สามารถรู้สิ่งต่างๆ ได้มากมาย หากบุคคลหนึ่งโทรหรือส่งข้อความหาแพทย์เฉพาะทางด้านมะเร็งทุกเช้าวันอังคารเวลาเก้าโมงเช้าเป็นเวลาหกเดือน ก็ไม่จำเป็นต้องฟังการสนทนาก็พอจะเดาได้ว่าเกิดอะไรขึ้น หากคนสองคนแลกเปลี่ยนข้อความกันวันละร้อยข้อความแล้วหยุดกะทันหัน ก็ไม่จำเป็นต้องอ่านแม้แต่ข้อความเดียวเพื่อทำความเข้าใจว่าเกิดอะไรขึ้น หากที่ปรึกษาด้านภาษีได้รับข้อความยี่สิบข้อความติดต่อกันจากลูกค้ารายเดิมในคืนก่อนวันปิดงบไตรมาส รูปแบบนี้บอกเล่าเรื่องราวได้ด้วยตัวมันเอง

Metadata เปิดเผยรูปแบบพฤติกรรม: ใครมีความสัมพันธ์กับใคร ตารางเวลาของแต่ละคนเป็นอย่างไร ตื่นเมื่อไหร่ นอนเมื่อไหร่ เดินทางเมื่อไหร่ ลูกค้ารายใดมีความเคลื่อนไหวมากที่สุด ความสัมพันธ์ทางวิชาชีพใดมีความเข้มข้นที่สุด เซิร์ฟเวอร์ที่รวบรวม Metadata สามารถสร้างโปรไฟล์รายละเอียดเกี่ยวกับชีวิตส่วนตัวและหน้าที่การงานของผู้ใช้ทุกคนได้โดยไม่ต้องอ่านข้อความที่เขียนแม้แต่คำเดียว

มีตัวอย่างทางประวัติศาสตร์ที่แสดงให้เห็นเรื่องนี้อย่างชัดเจน อดีตผู้อำนวยการ NSA Michael Hayden เคยกล่าวไว้ในปี 2014 ว่า "We kill people based on metadata" คำกล่าวนี้อ้างถึงปฏิบัติการทางทหารของสหรัฐฯ ต่อเป้าหมายที่ระบุตัว

ตนได้จากรูปแบบการสื่อสารของพวกเขาเท่านั้น โดยไม่ได้อ่านข้อความเลยแม้แต่ข้อความเดียว มีเพียงกราฟการติดต่อ และตารางเวลาเท่านั้น

การที่บริการรวบรวม Metadata ไม่ได้หมายความว่าต้องนำไปใช้ในทางที่ผิดกับผู้ใช้เสมอไป แต่มันหมายความว่าพวกเขา มีความสามารถที่จะทำเช่นนั้นได้ และบุคคลภายนอกที่มีสิทธิ์เข้าถึงข้อมูลเหล่านั้น ไม่ว่าจะโดยคำสั่งศาล การละเมิดความปลอดภัย หรือการขายข้อมูลให้บุคคลภายนอกหากข้อกำหนดการให้บริการอนุญาต ก็มีความสามารถนั้นเช่นกัน

การเข้าถึงสมุดรายชื่อ

อีกปัจจัยหนึ่งที่มักถูกมองข้ามคือ รายชื่อติดต่อ บริการส่งข้อความส่วนใหญ่ขอเข้าถึงสมุดรายชื่อในโทรศัพท์เมื่อสมัครใช้งาน พวกเขาจะอัปโหลดเบอร์โทรศัพท์ทั้งหมดไปยังเซิร์ฟเวอร์เพื่อแสดงว่ามีใครอีกบ้างที่ใช้บริการ ตั้งแต่วันนั้น บริษัทจะมีแผนที่ความสัมพันธ์ของผู้ใช้อย่างสมบูรณ์ แม้ว่าผู้ใช้นั้นจะไม่เคยส่งข้อความหาใครเลยก็ตาม

สำหรับมืออาชีพที่มีภาระหน้าที่ในการรักษาความลับ เช่น ทนายความ แพทย์ นักจิตวิทยา ที่ปรึกษา สมุดรายชื่อนั้น ประกอบไปด้วยลูกค้า หากสมุดรายชื่อถูกอัปโหลดไปยังเซิร์ฟเวอร์ของบุคคลภายนอก ชื่อของลูกค้าจะไปอยู่ในโครงสร้างพื้นฐานที่มืออาชีพไม่สามารถควบคุมเขตอำนาจศาลและนโยบายได้ ความลับในวิชาชีพไม่ได้ถูกทำลายในวันที่ใครบางคน ทำบทสนทนารั่วไหล แต่มันถูกทำลายไปนานแล้วตั้งแต่วันที่ยินยอมให้อัปโหลดข้อมูล

ความแตกต่างระหว่างการเข้ารหัสกับการไม่รวบรวมข้อมูล

การเข้ารหัสคือการปกป้องเนื้อหา ความเป็นส่วนตัวคือการไม่รวบรวมสิ่งที่ไม่จำเป็น สองสิ่งนี้แตกต่างกัน และความแตกต่างนี้มีความสำคัญอย่างยิ่งในเชิงปฏิบัติการ บริการหนึ่งสามารถเข้ารหัสข้อความทั้งหมดได้อย่างสมบูรณ์แบบในขณะนี้ รู้เกือบทุกอย่างเกี่ยวกับผู้ใช้ผ่าน Metadata ทั้งสองสิ่งนี้เข้ากันได้อย่างสมบูรณ์ และในความเป็นจริง นี่คือโมเดลธุรกิจหลักในอุตสาหกรรมนี้

คำถามที่ถูกต้องในการประเมินความเป็นส่วนตัวที่แท้จริงของบริการไม่ใช่ "มีการเข้ารหัสเนื้อหาหรือไม่" เพราะคำถามนั้นมีคำตอบมานานหลายปีแล้ว คำถามที่ถูกต้องคือ "มีการสร้าง Metadata อะไรบ้างและเก็บไว้ที่ไหน" และที่สำคัญที่สุดคือ "มี Metadata อะไรบ้างที่ไม่มีความจำเป็นต้องสร้างขึ้น"

สถาปัตยกรรมที่ลด Metadata ให้เหลือน้อยที่สุดโดยการออกแบบ (privacy by design) ไม่ใช่โดยคำมั่นสัญญาหรือนโยบายภายใน จะมีความเป็นส่วนตัวเชิงโครงสร้างมากกว่าสถาปัตยกรรมที่รวบรวมและเข้ารหัสข้อมูล เพราะข้อมูลที่ไม่มีอยู่จริงย่อมไม่สามารถรั่วไหล ไม่สามารถถูกขาย ไม่สามารถถูกส่งมอบตามคำสั่งศาล และไม่สามารถสูญหายจากการละเมิดความปลอดภัยได้

สำหรับผู้อ่านระดับมืออาชีพ

หากกิจกรรมทางวิชาชีพของคุณเกี่ยวข้องกับความลับ การรักษาความลับ หรือเพียงแค่การเคารพข้อมูลของผู้อื่น เป็นเรื่องที่ต้องค่าแก่การตั้งคำถามในลำดับต่อไปนี้:

1. แอปพลิเคชันที่ฉันใช้สื่อสารมีการเข้ารหัสเนื้อหาหรือไม่ (น่าจะใช่)
2. มีการเข้ารหัส Metadata หรือไม่ (น่าจะไม่ใช่)
3. มีการสร้าง Metadata ที่ *ไม่จำเป็น* ต่อการทำงานหรือไม่ (เกือบจะแน่นอนว่าใช่)

4. Metadata เหล่านี้ถูกเก็บไว้ที่ไหนและอยู่ภายใต้เขตอำนาจศาลใด (มีโอกาสสูงที่จะอยู่นอกเขตเศรษฐกิจยุโรป)
5. ลुकค้าหรือผู้ใช้ของฉันรู้หรือไม่ว่าข้อมูลของพวกเขาอยู่ที่นั่น

คำถามสุดท้ายเป็นคำถามที่น่าอึดอัดใจ เพราะคำตอบที่แท้จริงในหลายกรณีคือ **ไม่รู้**

บทความนี้เป็นบทความแรกในชุดบทความเกี่ยวกับการทำงานที่แท้จริงของเครื่องมือสื่อสารระดับมืออาชีพ ฉบับต่อๆ ไป จะกล่าวถึงการปฏิบัติตาม GDPR ในการส่งข้อความ และแนวคิดเรื่องความลับในวิชาชีพในยุคดิจิทัล

แหล่งข้อมูลและการอ่านเพิ่มเติม

- Hayden, M. – คำแถลงที่ Johns Hopkins University, 2014 ("We kill people based on metadata") มีบันทึกสาธารณะเผยแพร่
- GDPR (ระเบียบ EU 2016/679), มาตรา 4 และ 5 – คำจำกัดความของข้อมูลส่วนบุคคลและหลักการประมวลผล (Metadata คือข้อมูลส่วนบุคคล)
- EDPS และ EDPB – ความเห็นเกี่ยวกับการประมวลผลข้อมูลการจราจรทางคอมพิวเตอร์และ Metadata ในการสื่อสารทางอิเล็กทรอนิกส์ (ePrivacy directive)

[← ก่อนหน้าประวัติย่อของตราประทับครั้งถัดไป](#) → [ความลับในวิชาชีพในยุคดิจิทัล](#)

บทความล่าสุด

- [CUADERNOS LIST PREGUNTAS TITLE](#)
- [CUADERNOS LIST SELFHOST TITLE](#)
- [CUADERNOS LIST IDENTIDAD TITLE](#)

ดาวน์โหลดบทความนี้เก็บไว้เพื่อใช้งานได้ทุกที่ที่คุณต้องการ

[↓ Markdown](#) [↓ ข้อความ RSS](#) [↓ PDF](#)

ไฟล์จะถูกดาวน์โหลดลงในอุปกรณ์ของคุณ คุณสามารถบันทึก นำเข้าสู่ Solo2 หรือแชร์ได้ทุกที่ตามต้องการ Cuadernos จะไม่กำหนดปลายทางแทนคุณ

ตราประทับครั้ง · SHA-256 a567381c7a50bbe713c0c7abfac63d6357701b107ebc4950f503bcb674237b06

Cuadernos Lacre · สิ่งพิมพ์ของ [Menzuri Gestión S.L.](#) ·

เขียนโดย R.Eugenio · เรียบเรียงโดยทีมงาน [Solo2](#)

เว็บไซต์นี้ไม่มีการใช้คุกกี้และไม่มีการโหลดทรัพยากรจากบุคคลภายนอก เราใช้ตัวนับผู้เข้าชมแบบไม่ระบุตัวตนที่โฮสต์เอง (Umami บนเซิร์ฟเวอร์ยุโรปของเรา) และใช้ JavaScript ขั้นต่ำที่จำเป็นสำหรับการเลือกธีมสว่าง/มืดเท่านั้น ไม่มีการติดตาม ไม่มีการทำโปรไฟล์ ไม่มีการแชร์ข้อมูล หากคุณต้องการติดตามเรา: [RSS](#)