

ความลับในวิชาชีพในยุคดิจิทัล

เมื่อการสื่อสารระหว่างมืออาชีพและลูกค้าเกิดขึ้นผ่านช่องทางที่ไม่เหมาะสมทางเทคนิค ความลับจะไม่ได้ถูกทำลายในวันที่ข้อมูลรั่วไหล แต่มันถูกทำลายไปนานแล้วตั้งแต่วันที่เลือกใช้เครื่องมือนั้น

ปัญหาที่เกือบไม่มีใครมองเห็น

ทนายความได้รับเอกสารลับจากลูกค้าผ่านโทรศัพท์ แพทย์ปรึกษาอาการป่วยที่ละเอียดอ่อนกับเพื่อนร่วมงาน นักจิตวิทยาประสานงานการรักษาคนไข้กับจิตแพทย์ ที่ปรึกษาด้านภาษีส่งข้อมูลการยื่นแบบแสดงรายการภาษีที่รอการตรวจสอบ ทุกคนทำผ่านการส่งข้อความทันที และแทบไม่มีใครหยุดคิดว่าข้อความเหล่านั้นไปสิ้นสุดลงที่ใดจริงๆ

คำตอบในหลายกรณีเหมือนกันหมด: ไปยังเซิร์ฟเวอร์ที่มีมืออาชีพไม่ได้ควบคุม ในประเทศที่กฎหมายอาจจะไม่คุ้มครอง บริหารจัดการโดยบริษัทที่มีโมเดลธุรกิจคือการสะสมข้อมูล ข้อความอาจถูกเข้ารหัสระหว่างการส่ง แต่ทันทีที่ถึงเซิร์ฟเวอร์ มันคือสำเนาที่ถูกเก็บไว้ในโครงสร้างพื้นฐานของบุคคลภายนอก ขึ้นอยู่กับการตัดสินใจเชิงปฏิบัติการ กฎหมาย และการค้าของบุคคลภายนอกนั้น ไม่ใช่การตัดสินใจของมืออาชีพ

สิ่งที่กฎหมายระบุไว้

กฎระเบียบการคุ้มครองข้อมูลทั่วไปของยุโรปมีความชัดเจนในมาตรา 32: ใครก็ตามที่ประมวลผลข้อมูลส่วนบุคคลต้องดำเนินการมาตรการทางเทคนิคและองค์กรที่ "เหมาะสม" เพื่อรับประกันระดับความปลอดภัยที่สอดคล้องกับความเสี่ยง ความเหมาะสมของมาตรการไม่ได้วัดจาก "สิ่งที่แอปพลิเคชันบอกว่าทำ" แต่วัดจากความเสี่ยงที่แท้จริง หากข้อมูลลูกค้าไปสิ้นสุดที่เซิร์ฟเวอร์ซึ่งเขตอำนาจศาลไม่รับประกันระดับการคุ้มครองที่เทียบเท่ากับเขตเศรษฐกิจยุโรป ผู้ควบคุมข้อมูลหรือมืออาชีพรายนั้น กำลังแบกรับความเสี่ยงที่เขาอาจจะไม่รู้ตัวเลย

และไม่ใช่แค่ GDPR เท่านั้น ความลับในวิชาชีพซึ่งมีการควบคุมเป็นพิเศษสำหรับทนายความ แพทย์ นักจิตวิทยา ผู้สอบบัญชี ผู้สื่อข่าว และอื่นๆ กำหนดให้การสื่อสารกับลูกค้าต้องเป็นความลับ ไม่ใช่ "เป็นความลับเท่าที่จะเป็นไปได้" แต่เป็นความลับโดยไม่มีเงื่อนไข หากช่องทางทางเทคนิคที่ใช้ไม่สามารถรับประกันสิ่งนี้ได้ มืออาชีพรายนั้นกำลังรับความเสี่ยงที่จรรยาบรรณวิชาชีพของเขาไม่อนุญาตให้ทำ

ความอ่อนแอคือความเสี่ยงนั้นมองไม่เห็น ไม่มีใครตรวจสอบการส่งข้อความในสำนักงาน ไม่มีใครขอสัญญาการประมวลผลข้อมูลจากผู้ให้บริการแขก ความเสี่ยงจะปรากฏขึ้นเมื่อสายเกินไปเท่านั้น: ข้อมูลรั่วไหล การละเมิดความปลอดภัยที่ถูกเผยแพร่ หรือคำสั่งศาลที่ดำเนินการในทวีปอื่นโดยไม่มีการแจ้งให้ผู้ใช้ทราบ

สิ่งที่มืออาชีพต้องการในเชิงเทคนิค

สิ่งที่ผู้ที่มีภาระหน้าที่ในการรักษาความลับต้องการนั้น หากมองจากมุมมองของข้อกำหนดแล้ว จริงๆ แล้วมันง่ายอย่างน่าประหลาดใจ:

- ช่องทางที่ข้อความส่งตรงจากอุปกรณ์ของผู้ส่งไปยังอุปกรณ์ของผู้รับ โดยไม่ผ่านเซิร์ฟเวอร์กลางที่เก็บสำเนาไว้
- โครงสร้างพื้นฐานที่เขตอำนาจศาลและนโยบายสอดคล้องกับ GDPR โดยการออกแบบ ไม่ใช่โดยคำประกาศ
- วัตถุประสงค์ตนกับคู่สนทนาโดยไม่จำเป็นต้องส่งมอบรายชื่อติดต่อทางวิชาชีพ (ชื่อลูกค้า เบอร์โทรศัพท์ สมุดรายชื่อ) ให้กับบุคคลภายนอก
- ระบบที่ตรวจสอบได้ ไม่ใช่ขึ้นอยู่กับคำพูดของผู้ให้บริการ เพื่อยืนยันว่าข้อความส่งถึงบุคคลที่ต้องการ

นี่ไม่ใช่รายการที่เรียกร่องมากเกินไป จริงๆ แล้วมันคือสิ่งที่เคยถือว่าเป็นเรื่องปกติในการสื่อสารทางวิชาชีพก่อนยุคดิจิทัล จดหมายลงทะเบียยนตอบรับสามารถตอบใจทุกเกณฑ์เหล่านี้ได้ทั้งหมด การโทรศัพท์จากตู้สาขาของสำนักงานไปยังสำนักงานของลูกค้าก็เช่นกัน สิ่งที่แปลกไม่ใช่การเรียกร่องการรับประกันเหล่านี้ในปัจจุบัน แต่สิ่งที่แปลกคือการรับประกันเหล่านี้สูญหายไปในการเปลี่ยนผ่านสู่ช่องทางดิจิทัลโดยที่ไม่มีใครสังเกตเห็น

ความแตกต่างระหว่างการเข้ารหัสกับการไม่จัดเก็บข้อมูล

มีอุปมาอุปไมยที่เป็นประโยชน์ การเข้ารหัสข้อความและเก็บไว้ในเซิร์ฟเวอร์เทียบเท่ากับการนำเอกสารใส่ไว้ในตู้เซฟแล้วทิ้งตู้เซฟไว้ในบ้านของคนแปลกหน้า ตู้เซฟนั้นดี เอกสารไม่สามารถอ่านได้ในหลักการ แต่เอกสาร *ยังคงอยู่ในบ้านของคนอื่น* และคนคนนั้นอาจได้รับคำสั่งศาล ถูกโจมตีทางไซเบอร์ เปลี่ยนแปลงข้อกำหนดการให้บริการ ถูกซื้อโดยบริษัทอื่นที่มีจริยธรรมต่างออกไป หรืออาจหายไปในวันพรุ่งนี้ก็ได้

ทางเลือกเชิงโครงสร้าง ไม่ใช่เชิงกระบวนการ ไม่ใช่ขึ้นอยู่กับความไว้วางใจ คือเอกสารต้องไม่หลุดออกจากสำนักงาน เดินทางจากโต๊ะของมืออาชีพไปยังโต๊ะของลูกค้าโดยตรงโดยไม่ต้องมีคนกลางใดๆ นี่คือสิ่งที่การสื่อสารแบบ point-to-point ระหว่างอุปกรณ์ทำในเชิงเทคนิค: มันกำจัดคนกลางออกไป ไม่ใช่ว่าคนกลางนั้นชั่วร้าย แต่ในกรณีของความลับในวิชาชีพ คนกลางนั้น *ไม่จำเป็น* และสิ่งที่ไม่จำเป็นต้องถูกกำจัดออกไปเป็นหลักการในทุกๆ ระบบที่ต้องการความปลอดภัย

ประเด็นเรื่องความรับผิดชอบ

ท้ายที่สุด คำถามที่มืออาชีพทุกคนที่มีหน้าที่รักษาความลับควรจะตอบด้วยคำว่า "ใช่" ได้อย่างมั่นใจคือ:

หากพรุ่งนี้บทสนทนาด้านลูกค้ารายหนึ่งของฉันรั่วไหล และศาลหรือสภาวิชาชีพถามฉันว่าฉันจัดการเรื่องความลับอย่างไร ฉันสามารถพิสูจน์ทางเทคนิคได้หรือไม่ว่าช่องทางที่ฉันใช้ไม่ได้เก็บสำเนาไว้ในโครงสร้างพื้นฐานของบุคคลภายนอก ฉันสามารถพิสูจน์ได้หรือไม่ว่าข้อมูลไม่เคยออกจากอุปกรณ์ของคนสองคนที่ร่วมสนทนา ฉันสามารถพิสูจน์ได้หรือไม่โดยไม่ต้องพึ่งพาคำพูดของบริษัทจากทวีปอื่น ว่าความลับได้รับการรับประกันโดยสถาปัตยกรรม ไม่ใช่โดยคำสัญญา

หากคำตอบคือไม่ ปัญหาที่ไม่ใช่ตัวเครื่องมืออย่างเป็นทางการเป็นรูปธรรม ปัญหาคือมีการมอบหมายความรับผิดชอบให้กับเครื่องมือที่เครื่องมือไม่ได้ถูกออกแบบมาเพื่อรองรับ มันเหมือนกับ การใส่เพิ่มลับไว้ในซองจดหมายใสแล้วเชื่อว่าบุรุษไปรษณีย์จะไม่มองข้างใน

เครื่องมือที่มีอาชีพเลือกใช้สื่อสารกับลูกค้านั้นบอกอะไรได้มากมายเกี่ยวกับวิธีที่เขาให้คุณค่ากับความไว้วางใจ มีเครื่องมือที่ได้รับการออกแบบมาเพื่อให้ความไว้วางใจนั้นไม่ขึ้นอยู่กับคำมั่นสัญญา แต่ขึ้นอยู่กับสถาปัตยกรรม และมีเครื่องมือที่ไม่เป็นเช่นนั้น การรู้ถึงความแตกต่างเป็นส่วนหนึ่งของงาน

กรอบระเบียบข้อบังคับที่อ้างอิง

- ระเบียบ (EU) 2016/679 (GDPR) โดยเฉพาะมาตรา 5, 25 (การคุ้มครองข้อมูลโดยการออกแบบ) และมาตรา 32 (ความปลอดภัยในการประมวลผล)
- กฎหมายว่าด้วยความลับในวิชาชีพ (เช่น พ.ร.บ. ทนายความ, พ.ร.บ. วิชาชีพเวชกรรม, ข้อบังคับจรรยาบรรณวิชาชีพ)
- กฎหมายอาญาเกี่ยวกับการเปิดเผยความลับในวิชาชีพ
- ประมวลจริยธรรมของสมาคมวิชาชีพเกี่ยวกับการรักษาความลับและความลับในวิชาชีพ

[← ก่อนหน้าการเข้ารหัสไม่ได้หมายถึงความเป็นส่วนตัว: Metadata บอกอะไรเกี่ยวกับคุณบ้างถัดไป → GDPR และการส่งข้อความในระดับมืออาชีพ: ทำไมคนส่วนใหญ่ถึงละเมิดกฎโดยไม่รู้ตัว](#)

บทความล่าสุด

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

ดาวน์โหลดบทความนี้เก็บไว้เพื่อใช้งานได้ทุกที่ที่คุณต้องการ

[↓ Markdown](#) [↓ ข้อความรสรรมดา](#) [↓ PDF](#)

ไฟล์จะถูกดาวน์โหลดลงในอุปกรณ์ของคุณ คุณสามารถบันทึก นำเข้าสู่ Solo2 หรือแชร์ได้ทุกที่ตามต้องการ Cuadernos จะไม่กำหนดปลายทางแทนคุณ

ตราประทับครั้ง · SHA-256 8069c2337879aa5f6fb3c7595fd00343dba3a8650bc552d83eb3f541405526db

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](#)