Bí mật nghề nghiệp trong kỷ nguyên số

Khi việc liên lạc giữa chuyên gia và khách hàng diễn ra qua một kênh không phù hợp về mặt kỹ thuật, bí mật không bị phá vỡ vào ngày rò rỉ. Nó đã bị phá vỡ từ trước đó rất lâu, ngay vào lúc lựa chọn công cụ.

Một vấn đề mà hầu như không ai nhìn thấy

Một luật sư nhận được một tài liệu bảo mật từ khách hàng trên điện thoại của mình. Một bác sĩ thảo luận với đồng nghiệp về một chẩn đoán tế nhị. Một nhà tâm lý học phối hợp với bác sĩ tâm thần về việc điều trị cho bệnh nhân. Một chuyên gia tư vấn thuế gửi dữ liệu của một tờ khai đang chờ kiểm tra. Tất cả đều thực hiện qua tin nhắn tức thời. Và hầu như không ai dừng lại để suy nghĩ xem những tin nhắn đó thực sự kết thúc ở đâu.

Câu trả lời trong hầu hết các trường hợp đều giống nhau: trên một máy chủ mà chuyên gia không kiểm soát, ở một quốc gia mà luật pháp họ không nhất thiết phải biết, được quản lý bởi một công ty có mô hình kinh doanh – xét theo các thuật ngữ kinh tế trực tiếp – là tích lũy dữ liệu. Tin nhắn có thể được mã hóa khi truyền tải. Nhưng một khi nó đến máy chủ, nó là một bản sao được lưu trữ trong cơ sở hạ tầng của bên thứ ba, chịu sự chi phối của các quyết định vận hành, pháp lý và thương mại của bên thứ ba đó. Chứ không phải của chuyên gia.

Luật pháp quy định gì

Quy định chung về bảo vệ dữ liệu của Châu Âu rất rõ ràng trong Điều 32: bất kỳ ai xử lý dữ liệu cá nhân phải thực hiện các biện pháp kỹ thuật và tổ chức "thích hợp" để đảm bảo mức độ bảo mật tương xứng với rủi ro. Tính thích hợp của các biện pháp không được đo lường bằng "những gì ứng dụng tuyên bố sẽ làm", mà bằng rủi ro thực tế. Nếu dữ liệu khách hàng kết thúc trên một máy chủ có quyền tài phán không đảm bảo mức độ bảo vệ tương đương với Khu vực Kinh tế Châu Âu, thì bên kiểm soát dữ liệu – tức là chuyên gia – đang gánh chịu một rủi ro mà có lẽ họ không nhận thức được đầy đủ.

Và không chỉ có GDPR. Bí mật nghề nghiệp, được quy định cụ thể cho luật sư, bác sĩ, nhà tâm lý học, kiểm toán viên, nhà báo và những người khác, yêu cầu việc liên lạc với khách hàng phải được bảo mật. Không phải là "bảo mật nhất có thể". Mà là bảo mật vô điều kiện. Nếu kênh kỹ thuật được sử dụng không thể đảm bảo điều này, chuyên gia đang chấp nhận một rủi ro mà đạo đức nghề nghiệp của họ không cho phép.

Nghịch lý là ở chỗ rủi ro đó vô hình. Không ai kiểm tra việc nhắn tin của văn phòng. Không ai yêu cầu hợp đồng xử lý dữ liệu từ nhà cung cấp dịch vụ trò chuyện. Rủi ro chỉ lộ ra khi đã quá muộn: một vụ rò rỉ, một lỗ hổng được công bố, một lệnh tòa án được thực thi ở một châu lục khác mà không có thông báo cho người dùng.

Chuyên gia cần gì về mặt kỹ thuật

Những gì một người có nghĩa vụ giữ bí mật cần, xét từ góc độ yêu cầu, thực sự đơn giản một cách đáng ngạc nhiên:

- Một kênh mà tin nhắn đi thẳng từ thiết bị của người gửi đến thiết bị của người nhận, không qua một máy chủ trung gian lưu trữ bản sao.

- Một cơ sở hạ tầng có quyền tài phán và các chính sách phù hợp với GDPR ngay từ khâu thiết kế, chứ không phải qua tuyên bố.
- Một cách thức để nhận diện với người đối thoại mà không cần phải bàn giao các liên hệ chuyên môn (tên khách hàng, số điện thoại, danh bạ) cho bên thứ ba.
- Một hệ thống có thể xác minh được – không dựa trên lời nói của nhà cung cấp – để xác nhận rằng tin nhắn đã đến đúng người.

Đây không phải là một danh sách đòi hỏi quá cao. Thực tế, đó là những gì được coi là hiển nhiên trong giao tiếp chuyên môn trước kỷ nguyên số. Một bức thư bảo đảm đã đáp ứng được tất cả các tiêu chí này. Một cuộc gọi điện thoại từ tổng đài của văn phòng đến tổng đài của khách hàng cũng vậy. Điều kỳ lạ không phải là những đảm bảo này được yêu cầu ngày nay: điều kỳ lạ là chúng đã bị mất đi khi chuyển sang kênh kỹ thuật số mà không ai nhận ra.

Sự khác biệt giữa mã hóa và không lưu trữ

Có một phép ẩn dụ hữu ích. Việc mã hóa một tin nhắn và lưu trữ nó trên máy chủ tương đương với việc để một tài liệu vào két sắt và để két sắt đó ở nhà một người lạ. Két sắt đó tốt. Tài liệu về nguyên tắc không thể đọc được. Nhưng tài liệu đó *vẫn đang ở trong nhà của người khác*. Và người đó có thể nhận được lệnh của tòa án, bị tấn công mạng, thay đổi các điều khoản dịch vụ, bị mua lại bởi một công ty khác với đạo đức khác, hoặc có thể biến mất vào ngày mai.

Giải pháp thay thế về mặt cấu trúc – không phải theo quy trình, không phải dựa trên sự tin tưởng – là tài liệu không bao giờ rời khỏi văn phòng. Nó di chuyển trực tiếp từ bàn làm việc của chuyên gia sang bàn làm việc của khách hàng mà không qua bất kỳ trung gian nào. Đó là những gì giao tiếp điểm-đối-điểm giữa các thiết bị thực hiện về mặt kỹ thuật: nó loại bỏ trung gian. Không phải vì trung gian là xấu. Mà chỉ đơn giản là trong trường hợp bí mật nghề nghiệp, trung gian là *không cần thiết*. Và những gì không cần thiết, trong bất kỳ hệ thống nào muốn an toàn, phải bị loại bỏ về mặt nguyên tắc.

Vấn đề trách nhiệm

Cuối cùng, câu hỏi mà mọi chuyên gia có nghĩa vụ giữ bí mật phải có thể trả lời bằng một từ "có" dứt khoát là:

> Nếu ngày mai một cuộc trò chuyện với một trong những khách hàng của tôi bị rò rỉ và tòa án hoặc hiệp hội nghề nghiệp hỏi tôi cách quản lý tính bảo mật, liệu tôi có thể chứng minh về mặt kỹ thuật rằng kênh tôi đã sử dụng không lưu trữ bản sao trong cơ sở hạ tầng của bên thứ ba không? Tôi có thể chứng minh rằng dữ liệu chưa bao giờ rời khỏi thiết bị của hai người tham gia cuộc trò chuyện không? Tôi có thể chứng minh tính bảo mật được đảm bảo bởi kiến trúc chứ không phải bằng một lời hứa, mà không cần dựa trên lời nói của một công ty từ châu lục khác không?

Nếu câu trả lời là không, thì vấn đề không cụ thể nằm ở công cụ đó. Vấn đề là một trách nhiệm đã được giao phó cho một công cụ mà công cụ đó không được thiết kế để hỗ trợ trách nhiệm đó. Giống như việc để các hồ sơ mật vào một phong bì trong suốt và tin rằng người đưa thư sẽ không nhìn vào bên trong.

Công cụ mà một chuyên gia chọn để liên lạc với khách hàng nói lên nhiều điều về cách họ trân trọng sự tin tưởng của khách hàng. Có những công cụ được thiết kế để sự tin tưởng đó không phụ thuộc vào những lời hứa, mà vào kiến trúc. Và có những công cụ không như vậy. Biết được sự khác biệt là một phần của công việc.

Khung pháp lý được trích dẫn

- Quy định (EU) 2016/679 (GDPR), đặc biệt là các Điều 5, 25 (bảo vệ dữ liệu ngay từ khâu thiết kế) và 32 (an ninh xử lý).
- Luật pháp Việt Nam về bí mật nghề nghiệp (ví dụ: Luật Luật sư Điều 25, Luật Khám bệnh, chữa bệnh Điều 8).

- Bộ luật Hình sự về việc xâm phạm bí mật nghề nghiệp.
- Quy tắc đạo đức của các hiệp hội nghề nghiệp liên quan đến tính bảo mật và bí mật nghề nghiệp.

← TrướcMã hóa không có nghĩa là quyền riêng tư: siêu dữ liệu nói gì về bạnTiếp theo →GDPR và tin nhắn chuyên nghiệp: tại sao hầu hết đang vi phạm mà không hề hay biết

Các bài đọc gần đây

- CUADERNOS_LIST_PREGUNTAS_TITLE
- CUADERNOS_LIST_SELFHOST_TITLE
- CUADERNOS_LIST_IDENTIDAD_TITLE

Tải bài viết này để sử dụng ở bất cứ đâu bạn cần.

↓ Markdown ↓ Văn bản thuần túy ↓ PDF

Tệp sẽ được tải xuống thiết bị của bạn. Từ đó, bạn có thể lưu trữ, nhập vào Solo2 hoặc chia sẻ ở bất cứ đâu. Cuadernos không quyết định điểm đến thay cho bạn.

Dấu sáp · SHA-256 a29ba03de1647a57116151337a1b22f761cbb82f3f3daf3f8da571fc451fe9d2

Cuadernos Lacre · Một ấn phẩm của Menzuri Gestión S.L. ·
viết bởi R.Eugenio · được biên tập bởi đội ngũ Solo2.