החיסיון המקצועי בעידן הדיגיטלי

כאשר התקשורת בין איש המקצוע ללקוח שלו מתבצעת בערוץ שאינו מתאים מבחינה טכנית, הסוד אינו נפרץ ביום ההדלפה. הוא נפרץ הרבה קודם לכן, ברגע בחירת הכלי.

בעיה שכמעט איש אינו רואה

עורך דין מקבל בטלפון שלו מסמך סודי מלקוח. רופא דן עם קולגה באבחנה רגישה. פסיכולוג מתאם עם פסיכיאטר את הטיפול במטופל. יועץ מס שולח נתונים של דוח הממתין לביקורת. כולם עושים זאת באמצעות הודעות מיידיות. וכמעט אף אחד לא עוצר לחשוב היכן ההודעות הללו באמת מסתיימות.

התשובה ברוב המקרים היא אותה תשובה: בשרת שאיש המקצוע אינו שולט בו, במדינה שאת חקיקתה הוא לא בהכרח מכיר, המנוהל על ידי חברה שהמודל העסקי שלה הוא – במונחים כלכליים ישירים – צבירת נתונים. ההודעה עשויה להיות מוצפנת בעת ההעברה. אך ברגע שהיא מגיעה לשרת, היא עותק המאוחסן בתשתית של צד שלישי, הכפוף להחלטות התפעוליות, המשפטיות והמסחריות של אותו צד שלישי. לא של איש המקצוע.

מה אומרת החקיקה

תקנת הגנת הנתונים הכללית האירופית (GDPR) היא חד-משמעית בסעיף 32 שלה: כל מי שמעבד נתונים אישיים חייב ליישם אמצעים טכניים וארגוניים "מתאימים" כדי להבטיח רמת אבטחה התואמת את הסיכון. התאמת האמצעים אינה נמדדת לפי "מה שהאפליקציה טוענת שהיא עושה", אלא לפי הסיכון האמיתי. אם נתוני לקוח מגיעים לשרת שסמכות השיפוט שלו אינה מבטיחה רמת הגנה המקבילה לזו של האזור הכלכלי האירופי, בעל השליטה בנתונים – כלומר איש המקצוע – לוקח סיכון שכנראה אינו מודע לו לחלוטין.

וזה לא רק ה-GDPR. החיסיון המקצועי, המוסדר באופן ספציפי עבור עורכי דין, רופאים, פסיכולוגים, רואי חשבון, עיתונאים ואחרים, דורש שהתקשורת עם הלקוח תהיה סודית. לא "סודית ככל האפשר". סודית ללא סייג. אם הערוץ הטכני שבו משתמשים אינו יכול להבטיח זאת, איש המקצוע לוקח סיכון שכללי האתיקה של המקצוע שלו אינם מתירים לו לקחת.

הפרדוקס הוא שהסיכון הוא בלתי נראה. אף אחד לא מבצע ביקורת על ההודעות במשרד. אף אחד לא מבקש את הסכם עיבוד הנתונים מספק הצ'אט. הסיכון מתגלה רק כשכבר מאוחר מדי: הדלפה, פרצת אבטחה שפורסמה, צו בית משפט שבוצע ביבשת אחרת ללא הודעה למשתמש.

מה איש מקצוע צריך מבחינה טכנית

מה שאדם בעל חובת חיסיון צריך הוא למעשה פשוט באופן מפתיע מנקודת המבט של הדרישות:

- ערוץ שבו ההודעות עוברות ישירות מהמכשיר של השולח למכשיר של המקבל, מבלי לעבור דרך שרת ביניים השומר עותקים.
- תשתית שסמכות השיפוט והמדיניות שלה תואמות את ה-GDPR מעצם תכנונה, ולא באמצעות הצהרה.
- דרך להזדהות מול בן השיח מבלי צורך למסור לצד שלישי אנשי קשר מקצועיים (שמות לקוחות, מספרי טלפון, ספר כתובות).
- מערכת ניתנת לאימות – שאינה מבוססת על המילה של הספק – לאישור שההודעה הגיעה לאדם הנכון.

זו אינה רשימה תובענית. זה למעשה מה שנחשב למובן מאליו בתקשורת המקצועית הקדם-דיגיטלית. מכתב רשום עמד בכל הקריטריונים הללו. שיחת טלפון ממרכזיית המשרד לזו של הלקוח גם כן. הדבר המוזר אינו שהערבויות הללו נדרשות היום: הדבר המוזר הוא שהן אבדו במעבר לערוץ הדיגיטלי, מבלי שאיש שם לב.

ההבדל בין להצפין לבין לא לשמור

יש מטפורה מועילה. להצפין הודעה ולשמור אותה בשרת שווה ערך להנחת מסמך בכספת והשארת הכספת בביתו של זר. הכספת טובה. את המסמך עקרונית לא ניתן לקרוא. אבל המסמך *עדיין נמצא בבית של מישהו אחר*. ואותו מישהו יכול לקבל צו בית משפט, לסבול מהתקפת סייבר, לשנות את תנאי השירות שלו, להירכש על ידי חברה אחרת עם אתיקה אחרת, או להיעלם מחר.

החלופה המבנית – לא תהליכית, לא מבוססת אמון – היא שהמסמך לעולם לא יעזוב את המשרד. שהוא ייסע ישירות משולחנו של איש המקצוע לשולחנו של הלקוח, ללא כל מתווך. זה מה שתקשורת נקודה-לנקודה בין מכשירים עושה מבחינה טכנית: היא מבטלת את המתווך. לא שהמתווך הוא רע. זה פשוט שבמקרה של חיסיון מקצועי, המתווך הוא *מיותר*. ואת המיותר יש לבטל באופן עקרוני בכל מערכת השואפת להיות בטוחה.

שאלת האחריות

בסופו של דבר, השאלה שכל איש מקצוע עם חובת חיסיון צריך להיות מסוגל לענות עליה ב"כן" נחרץ היא הבאה:

> אם מחר תודלף שיחה עם אחד הלקוחות שלי ובית משפט או לשכה מקצועית ישאלו אותי איך אני מנהל את הסודיות, האם אוכל להוכיח טכנית שהערוץ שבו השתמשתי אינו שומר עותקים בתשתית של צדדים שלישיים? האם אוכל להוכיח שהנתונים לעולם לא עזבו את המכשירים של שני האנשים המעורבים בשיחה? האם אוכל, מבלי להסתמך על המילה של חברה מיבשת אחרת, להוכיח שהסודיות הייתה מובטחת על ידי הארכיטקטורה ולא על ידי הבטחה?

אם התשובה היא לא, הבעיה אינה הכלי הקונקרטי. הבעיה היא שלכלי הואצלה אחריות שהכלי לא תוכנן לתמוך בה. זה כמו לשים תיקים סודיים במעטפה שקופה ולסמוך על כך שהדוור לא יסתכל פנימה.

הכלי שבו בוחר איש מקצוע כדי לתקשר עם הלקוחות שלו אומר הרבה על האופן שבו הוא מעריך את האמון שלהם. ישנם כלים שתוכננו כך שהאמון הזה לא יהיה תלוי בהבטחות, אלא בארכיטקטורה. וישנם כלים שלא. הכרת ההבדל היא חלק מהעבודה.

מסגרת נורמטיבית מצוטטת

- תקנת האיחוד האירופי 2016/679 (GDPR), במיוחד סעיפים 5, 25 (הגנת נתונים כבר משלב התכנון) ו-32 (אבטחת העיבוד).
- חקיקה ישראלית בנושא חיסיון מקצועי (למשל חוק לשכת עורכי הדין סעיף 90, פקודת הראיות סעיף 48, פקודת הרופאים סעיף 24).
- חוק הגנת הפרטיות, התשמ"א-1981.
- כללי האתיקה המקצועית של לשכת עורכי הדין בעניין סודיות וחיסוי.

← הקודםלהצפין זה לא להיות פרטי: מה המטא-נתונים אומרים עליכםהבא → GDPR ותקשורת מקצועית: מדוע הרוב מפרים את הכללים מבלי לדעת זאת

קריאות אחרונות

- CUADERNOS_LIST_PREGUNTAS_TITLE
- CUADERNOS_LIST_SELFHOST_TITLE
- CUADERNOS_LIST_IDENTIDAD_TITLE

קחו את המאמר הזה אתכם לכל מקום שתצטרכו.

הקובץ יורד למכשיר שלכם. משם תוכלו לשמור אותו, לייבא אותו ל-Solo2 או לשתף אותו היכן שתרצו. Cuadernos לא מחליטה על היעד עבורכם.

חותם שעווה · SHA-256 c40316e1965cf9b8bce198df2aba6084ad0ba57ca482d474c9a3030192f7a9c8

Cuadernos Lacre · פרסום של Menzuri Gestión S.L. ·
נכתב על ידי R.Eugenio · נערך על ידי צוות Solo2.

אתר זה אינו משתמש בעוגיות (cookies) ואינו טוען משאבים מצד שלישי. הוא משתמש במונה ביקורים אנונימי באירוח עצמי (Umami, בשרת האירופי שלנו) ובמינימום ה-JavaScript הנדרש להעדפת ערכת הנושא הבהירה/כהה שלכם. ללא מעקבים, ללא פרופילינג, ללא שיתוף נתונים. אם תרצו לעקוב אחרינו: RSS.