כשאין אף אחד באמצע

הצפנת מה שעובר דרך שרת מגינה על התוכן. אי-קיום שרת באמצע מבטל את השאלה. אלו אינם דברים זהים.

שני אנשים, שיחה אחת

כששני אנשים מדברים פנים אל פנים בחדר, אף אחד לא צריך להבטיח שהוא לא שמע כלום. הוא לא שמע כי הוא לא היה שם. כששני אנשים מעבירים נייר מיד ליד, אף אחד באמצע לא צריך להישבע שהוא לא קרא אותו. אין אף אחד באמצע.

רוב הדברים בחיי היומיום פועלים כך. איננו חותמים על הסכמי סודיות עם האוויר המעביר את קולנו, ולא עם הנייר שאנו מחזיקים. פרטיות השיחה אינה נשענת על הבטחה של מתווך, כי אין מתווך. זוהי אחת הצורות החזקות ביותר של פרטיות הקיימות: לא בגלל שמשהו או מישהו מתנהג יפה, אלא בגלל שאין משהו או מישהו.

כאשר השיחה עוברת לערוץ דיגיטלי, זה משתנה כברירת מחדל. המודל הרגיל הוא הבא: שני אנשים מתחברים לשרת, השרת מקבל את ההודעה, מצפין אותה או שומר אותה מוצפנת, ומוסר אותה לנמען. השרת נמצא באמצע. השרת יכול להיות ישר. ניתן לבצע בו ביקורת. הוא יכול לפעול בתחום שיפוט נוח ותחת מדיניות פרטיות קפדנית. כל זה יכול להיות נכון. אבל השרת נמצא באמצע.

ההבדל בין הצפנה לבין אי-איסוף (חלק שני)

במאמר קודם בסדרה זו טענו שהצפנת התוכן ואי-איסוף מטא-נתונים אינם אותו דבר. ישנו צעד נוסף שכדאי לנסח בבירור: הצפנת מה שעובר דרך שרת ואי-קיום שרת אינם אותו דבר גם כן.

המודל הראשון — שרת באמצע, תוכן מוצפן — מגן על התוכן מפני מפעיל השרת, צוות התחזוקה שלו, או תוקף חיצוני שיפרוץ למערכת. וזה חשוב. אבל זה לא מבטל את השרת. השרת עדיין שם. הוא ממשיך לעבד מטא-נתונים. הוא נשאר נקודה שיכולה לקבל דרישה שיפוטית, התערבות משפטית, לחץ פוליטי או פרצת אבטחה. הוא נשאר נקודה שדורשת מתן אמון במישהו.

המודל השני — אי-קיום שרת בין שני הקצוות — אינו מגן טוב יותר על התוכן המוצפן: אם הקריפטוגרפיה חזקה, התוכן מוגן בשני המקרים. מה שמשתנה אינו התוכן. מה שמשתנה הוא שהשאלה *"מה קורה עם השרת?"* מפסיקה להיות רלוונטית, כי אין שרת לשאול עליו.

אמון, היעדרות, וההבדל ביניהם

האמון יכול להיות מונח במקומו. חברות ישרות קיימות. מבקרים קפדניים קיימים. חקיקות לטובת המשתמש קיימות. שירותים רציניים הממלאים בקפידה אחר כל האמור לעיל קיימים. אמון, כאשר הוא ניתן למפעיל שראוי לו, אינו הסדר רע.

אבל אמון, מוצק ככל שיהיה, נשאר אמון. זהו פתרון חברתי, לא פתרון טכני. חברה יכולה להחליף ידיים. תחום שיפוט יכול להחליף ממשלה. צו שיפוטי יכול להגיע מחר. פגיעות חדשה יכולה להתגלות בחודש הבא. שום דבר מזה לא קורה מחוסר תום לב. זה קורה כי המפעיל קיים, וכל מה שקיים כפוף למקריות של העולם.

היעדר מפעיל אינו כפוף לאותן מקריות. צו שיפוטי אינו יכול לבקש נתונים משרת שאינו קיים. תוקף אינו יכול לפרוץ לשרת שאינו קיים. שינוי במדיניות של חברה אינו יכול להשפיע על נתונים שחברה זו מעולם לא החזיקה. משפט המפתח הוא

פשוט: נתונים שאינם קיימים לא יכולים ללכת לאיבוד.

על הטיעון הלגיטימי מצד השרת

מי שמציע שירות מסרים מקצועי עם שרת באמצע מנסח בדרך כלל שלושה טיעונים תקפים לחלוטין. ראשית, שהשרת נחוץ כדי להבטיח מסירה כשהנמען אינו מחובר. שנית, שהצפנת התוכן חזקה ולכן המפעיל אינו יכול לקרוא אותו. שלישית, שהשירות עומד בחקיקה האירופית ושהנתונים מוגנים על פי חוק.

שלושת הטיעונים נכונים. אף אחד מהם לא משנה את מהות העניין. זה נכון ששרת מאפשר לאחסן הודעות למסירה דחויה; נכון גם שניתן לפתור מסירה דחויה בדרך אחרת, באמצעות פרוטוקולי תקשורת ישירה בין מכשירים ששוכללו במשך עשרות שנים ופעילים כיום. זה נכון שהצפנת התוכן במעבר חזקה בשירותים רציניים. וזה נכון שהחקיקה האירופית מגינה על משתמשים יותר מאשר במקומות רבים אחרים.

השאלה היא לא אם שירותים עם שרת באמצע הם חוקיים, או אם הם בטוחים, או אם הם מגינים על התוכן. הם יכולים להיות כאלה, הם חוקיים, ובדרך כלל בטוחים. השאלה היא שקיום שרת באמצע הוא בחירה ארכיטקטונית, לא אילוץ טכני. ולכל בחירה יש השלכות. ארכיטקטורה עם שרת באמצע מייצרת בהכרח גורם שצריך לבטוח בו. ארכיטקטורה ללא שרת באמצע — לא.

מה שהחוק אומר, ומה שהארכיטקטורה עושה

ה-GDPR אינו דורש מודל ארכיטקטוני ספציפי. הוא דורש תוצאות: מזעור נתונים, מטרה מוגבלת, הגנה מראש ובידי מחדל, ויכולת להוכיח עמידה בדרישות. שירות עם שרת באמצע יכול לעמוד בכל הדרישות הללו. שירות ללא שרת באמצע מקיים כמה מהן מעצם בנייתו, ולא על ידי הצהרה. מזעור מוחלט — אי-איסוף של דבר שאינו נחוץ בהחלט למסירת ההודעה — הוא טריוויאלי כשאין שרת שיכול לאסוף משהו.

לשימושים יומיומיים שאינם רגישים, ארכיטקטורה עם שרת היא סבירה לחלוטין, ואמון במפעיל רציני הוא הסדר תקף. לשימושים האחרים — אלה הנושאים סודיות מקצועית מוסדרת, אלה הכרוכים באחריות אתית, אלה הנוגעים למידע רגיש במיוחד — היעדר נקודת אמון אינו מותרות, אלא יתרון מבני.

לקורא המקצועי

השאלות שכדאי לשאול אל מול שירות תקשורת מקצועי, המוכרות כבר ממאמרים קודמים בסדרה זו, מושלמות בשאלה ארכיטקטונית אחת נוספת:

1. האם הוא מצפין את התוכן במעבר? (כנראה שכן.)
2. האם הוא מייצר ומאחסן מטא-נתונים על עם מי אני מדבר ומתי? (כנראה שכן.)
3. האם קיים שרת בדרך בין המכשיר שלי לזה של הנמען?
4. אם קיים: מי מפעיל אותו, באיזו סמכות שיפוט, ומה צריך לקרות כדי שהוא ימסור נתונים עלי?
5. אם לא קיים: לשאלות הקודמות אין רלוונטיות.

ההבדל בין שתי הקטגוריות אינו בדרגה, אלא בסוג. כשמגיע הזמן להסביר זאת ללקוח, למטופל או לעמית, הניסוח הכי כנה הוא גם הכי פשוט: באחד יש מישהו באמצע; בשני, לא.

מאמר זה חותם את המחזור הראשוני של Cuadernos Lacre. לאחר שדיברנו על הצפנה, מטא-נתונים וסודיות מקצועית, אנו משלימים את התמונה הארכיטקטונית: הצפנת התוכן ואי-קיום שרת באמצע הם דברים שונים. שניהם יכולים להיות חוקיים; רק אחד מבטל את נקודת האמון.

מקורות וקריאה נוספת

- Saltzer, J. H.; Reed, D. P.; Clark, D. D. — *End-to-end arguments in system design*, ACM TOCS, 1984. טקסט מכונן של העיקרון לפיו הערבויות של מערכת צריכות להיות מיושמות בקצוות, לא בערוץ הביניים.

- תקנה (איחוד אירופי) 2016/679, סעיף 25 — הגנת נתונים כבר מהעיצוב וכברירת מחדל.
- תקנה (איחוד אירופי) 2016/679, סעיף c.5.1 — עקרון מזעור הנתונים.
- Schneier, B. — *Data and Goliath: the hidden battles to collect your data and control your world* (2015), W. W. Norton. פרקים על ארכיטקטורות הממזערות את האיסוף על ידי בנייה.

← הקודם GDPR ותקשורת מקצועית: מדוע הרוב מפרים את הכללים מבלי לדעת זאת התבא
CUADERNOS_LIST_SCHREMS_TITLE →

קריאות אחרונות

- CUADERNOS_LIST_PREGUNTAS_TITLE
- CUADERNOS_LIST_SELFHOST_TITLE
- CUADERNOS_LIST_IDENTIDAD_TITLE

קחו את המאמר הזה אתכם לכל מקום שתצטרכו.

Markdown ↓ · טקסט פשוט ↓ · PDF ↓

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 efb9d60d379af9044b49a046baf6afe75b5fb1d22e0e5c19cd7aac7c98550a15

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