מאגרי מידע "עבשים": למה ניקוי מידע ישן הוא צעד קריטי בהגנת סייבר ופרטיות

הכותב: רועי בסר, CISO, DPO*

ארגונים נוטים לחשוב שככל שיש להם יותר מידע, כך הם "מוגנים" יותר מבחינה עסקית או משפטית. בפועל, המציאות הפוכה: מידע שאינו נדרש לפעילות השוטפת, אך נשמר במערכות הפעילות, הופך לעומס סיכון. הוא לא מייצר ערך יומיומי, אבל כן מגדיל את פוטנציאל הנזק בכל אירוע אבטחה.

עבור משרדי רו"ח ולקוחותיהם זו נקודה קריטית מאחר ועיקר המידע שמנוהל הוא אישי ורגיש למשל דוחות מס, שכר, מסמכים מזהים, פרטי חשבונות, ולעיתים גם מידע רגיש נוסף הנוגע למשפחה, בריאות או מצב כלכלי. כאשר מידע כזה "נגרר" שנים קדימה במערכת התפעולית, כל כשל או פריצה הופכים מאירוע נקודתי לאירוע רב - נפגעים. במילים פשוטות, ככל שבמאגר המידע הפעיל יש יותר נתונים, כך באירוע סייבר יש יותר מה שיכול להיפגע. דלף, שינוי, מחיקה, כופר או שיבוש. הנזק לא גדל בקו ישר; הוא גדל מעריכית, כי הוא משפיע על יותר אנשים, יותר תהליכים, ויותר חשיפה משפטית ומוניטינית.

אירוע סייבר לא חייב להיות "פריצה דרמטית". מספיק שמישהו עם הרשאה לא מתאימה יוריד קובץ, שמערכת גיבוי תשחזר גרסה שגויה, או ששגיאת תפעול תמחק תיקיות קריטיות. כשהמאגר מנופח, גם טעות קטנה יכולה להפוך לבעיה גדולה.

מעבר לכך, מאגר גדול אומר לרוב גם יותר מקומות שבהם המידע נמצא. גיבויים, העתקים, מערכות צד ג', קבצים מקומיים, מיילים, תיקיות "שיתוף", וענני פרטיים של עובדים. כלומר, לא רק שיש יותר מידע יש יותר "משטחים" שהוא עלול לברוח אליהם. ברגע האמת, קשה לדעת איפה הוא נמצא, מי נגע בו, ומה צריך לדווח.

לכן, צמצום המידע במאגר הפעיל הוא לא "סדר וארגון". זהו צעד שמקטין את היקף הפגיעה האפשרית מראש, ומפשט משמעותית את ההתמודדות אם וכאשר קורה אירוע.

אחת הטעויות השכיחות בארגונים היא לערבב בין מידע שנדרש לעבודה היומיומית לבין מידע שנשמר רק למקרה הצורך. מידע תפעולי פעיל הוא נתונים שבלעדיהם העסק לא עובד כמו לקוחות פעילים, תיקים פתוחים, תהליכי שכר נוכחיים. לעומתו, מידע היסטורי נועד בעיקר לצרכים של ביקורת, הגנה משפטית, או דרישות שמירה והוכחה. הבעיה מתחילה כשהמידע ההיסטורי נשאר באותה מערכת תפעולית עם אותן הרשאות, אותן אינטגרציות, ואותה נגישות. זה יוצר מצב שבו מידע שאף אחד לא באמת צריך ביום - יום, עדיין "נגיש בטעות" לעוד ועוד משתמשים, מערכות וספקים. כך נוצר פער תפיסתי כאשר הארגון חושב שזה ארכיון, אבל בפועל זה מאגר פעיל לכל דבר מבחינת חשיפה.

הפתרון הוא להפריד: מה שנדרש לפעילות נשאר נגיש, ומה שנדרש לשמירה עובר לארכיון מנוהל, מוגן, עם הרשאות מצומצמות ומדיניות גישה ברורה.

החוק לא מצפה מארגונים לשמור כל דבר לנצח, ובטח לא להשאיר הכל זמין ונגיש. העיקרון הבסיסי הוא שמידע אישי צריך להישמר למטרה לגיטימית, לפרק זמן סביר, ובהתאם לצורך. במקביל, ישנם תחומים שבהם קיימת חובת שמירה לתקופות מסוימות למשל בשל התיישנות, ניהול הליכים, או דרישות ביקורת.

הנקודה החשובה היא זו: גם אם יש חובה לשמור, אין חובה שהמידע יישב במערכת הפעילה. ניתן לשמור מידע לאורך זמן בצורה מאובטחת יותר, עם נגישות מוגבלת, ובאופן שמקטין סיכון. כלומר, "שמירה" ו "זמינות תפעולית" הם לא אותו דבר, ומי שמבלבל ביניהם מגדיל חשיפה בלי לקבל ערך.

מבחינה ניהולית, מדובר בהחלטה של איזון - מתי ערך השמירה עולה על הסיכון, ומהם המנגנונים שיבטיחו שמירה בלי לייצר פצצה מתקתקת במאגר הפעיל.

יש נטייה לחשוב שניקוי מידע הוא נושא משפטי/ציות. בפועל, זהו צעד סייבר קלאסי של הפחתת משטח תקיפה והפחתת "Blast Radius". אם יש פחות מידע רגיש בסביבה הפעילה לא רק שיש פחות מה לדלוף, אלא גם יש פחות מה להצפין בכופר, פחות מה להשחית, ופחות מה לבלבל בתהליכי שחזור.

בנוסף, כשמאגרי מידע מנוהלים נכון, גם תגובת הארגון לאירוע הופכת מדויקת יותר. קל יותר לברר מה נחשף, למי, ובאיזה היקף. קל יותר לחסום, לשחזר ולהחזיר לפעילות. ובהרבה מקרים קל יותר לעמוד בחובות דיווח ולנהל את האירוע בלי "ערפל קרב" מידע.

זו בדיוק הסיבה שמדיניות שמירה ומחיקה (Retention & Disposal) נחשבת כיום לכלי ניהולי מרכזי בתחום הסייבר, ולא רק סעיף במדיניות הפרטיות השמורה בתיקייה שאף אחד לא פותח.

כדי להתחיל נכון, צריך קודם להכיר את סוגי המידע - איזה מידע באמת דרוש להפעלה השוטפת, איזה מידע נדרש לשמירה בגלל דין/התיישנות/ביקורת, ואיזה מידע נשמר "כי ככה התרגלנו". אחרי המיפוי מגיעה החלטה ניהולית של מה נשאר פעיל, מה עובר לארכיון מוגן, ומה נמחק.

השלב הקריטי הוא המדיניות - קובעים תקופות שמירה לפי סוג נתון (ולא "פעם בשנה נזכר לנקות"), מגדירים מי מאשר מחיקה, איך מתעדים, ואיך מבטיחים שהמחיקה אכן מתבצעת בכל המקומות (כולל גיבויים/העתקים/שירותי צד ג' לפי הצורך).

ובסוף תיעוד - מחיקה בלי תיעוד מייצרת פחד, אבל מחיקה מתועדת היא שכבת הגנה המוכיחה שהארגון ניהל סיכונים, פעל בצורה סבירה, וצמצם חשיפה במקום לצבור אותה.

ארגון לא נמדד רק לפי כמה "הוא מאובטח", אלא גם לפי כמה הוא מנהל נכון את המידע שבידיו. מאגרי מידע מנופחים, ישנים ולא רלוונטיים הם בדיוק המקום שבו אירוע קטן הופך לבעיה גדולה משפטית, תפעולית ומוניטינית. שמירה בגלל התיישנות היא עניין לגיטימי, אבל היא לא הצדקה להשאיר הכל במאגר הפעיל. ההחלטה הנכונה היא להבחין בין מידע שחייב להיות נגיש לבין מידע שחייב להיות שמור, ולבנות מנגנון שמגן על שניהם בצורה שונה.

בסופו של דבר, ניקוי מידע "עבש" הוא לא רק מהלך תאימות רגולטורית. זה מהלך של חוסן עסקי שמקטין נזק פוטנציאלי, מפשט תגובה לאירועים, ומשדר ללקוחות שמי שמחזיק את המידע שלהם מתייחס אליו בכבוד ובאחריות.

*רועי בסר, בעל 30 שנות ניסיון באבטחת מידע, יועץ ניהול סיכוני סייבר לרשות שוק ההון, ביטוח וחסכון.