

הרשות להגנת הפרטיות פרסמה מדריך בעניין שמירת קבצי תיעוד ולוגים

עדכוני לקוחות

ביום 29.09.2024 פרסמה הרשות להגנת הפרטיות ("הרשות"), [מדריך ליישום תקנה 10\(ד\) לתקנות הגנת הפרטיות \(אבטחת מידע\), תשע"ז-2017 \("התקנות"\)](#). המדריך עוסק בחובות לשמירת קבצי תיעוד (log) במאגרי מידע ברמת אבטחה בינונית וגבוהה. במאגרים אלה יש לנהל מנגנון תיעוד אוטומטי שיאפשר ביקורת על הגישה למערכות המאגר ולשמור את נתוני התיעוד שלו למשך שנתיים לפחות.

1. מטרה

לעמדת הרשות, לחובת התיעוד האוטומטי תחת תקנה 10(א) לתקנות מספר תכליות, לרבות ניטור שוטף של מערכות המאגר, בקרה על הפעילות ודגימת נתונים חריגים. בנוסף, יישום חובה זו נועד לאפשר שחזור נתונים לצורך בחינת אירועי אבטחה, זיהוי חולשות במערכת ומניעת הישנות של פרצות אבטחה.

2. תחולת התקנה

התקנה חלה על כל מאגרי המידע ברמת אבטחה בינונית או גבוהה, למשל מאגרים שכוללים מידע פיננסי או מידע רפואי. התקנה מחייבת בקרה ותיעוד אוטומטי של פעולות המשתמשים והממשקים, בין אם מדובר בגישה בידי משתמש אנושי או גישה באמצעות רכיב קוד.

3. טיב נתוני התיעוד ואופן שמירתם

לפי תקנה 10(ד), יש לשמור את נתוני התיעוד המתעדים את כל הפעולות המבוצעות במערכות האבטחה של המאגר לפרק זמן של שנתיים לפחות. יש לוודא שהלוגים נשמרים בצורה מאובטחת למניעת השחתה או מחיקה. התיעוד צריך לכלול פרטים כמו זהות הניגש (אנושי או ממשק), תאריך ושעת הגישה, הרכיב שבאמצעותו בוצעה הגישה, הרכיב אליו נעשתה הגישה (למשל, בסיס נתונים או מערכת קבצים), סוג הגישה (קריאה, כתיבה או שליפה), היקף הפעולה, והאם הגישה אושרה או נדחתה.

4. הבחנה בין סוגי מערכות

הרשות מבחינה בין סוגי מערכות: מערכות קריטיות לתפעול מאגר המידע ולאבטחתו וכאלו שאינן. לגישת הרשות, מערכות קריטיות מחויבות בתיעוד רציף, נגיש וזמין ועל כן יש לשמור את נתוני התיעוד מהן במערכות אחסון מקומיות למשך שנתיים לפחות. מערכות אלו כוללות למשל מערכות הפעלה, (Active Directory (AD לניהול רשתות, EDR- לתיעוד פעולות בתחנות קצה, NAC-לניטור גישות לרשת הארגונית, וחומות אש או WAF.

בכל הנוגע ללוגים ממערכות שאינן קריטיות, סבורה הרשות כי ניתן לשמור אותם במערכות אחסון מקומיות, למשך שישה חודשים לפחות, ובתום שישה חודשים ניתן להעבירם למשך לפחות 18 חודשים נוספים לאחסון במנגנון שימור ארוך טווח, דוגמת התקן אחסון המצוי מחוץ לחצרי הארגון (Backup Site Off).

יישום והמלצות

לשמירת לוגים ונתוני תיעוד ממגנוני תיעוד אוטומטי חשיבות רבה בהיבטי אבטחת מידע, בפרט בקרות אירוע סייבר. כדי לעמוד בדרישות תקנה 10(ד) חשוב להגדיר מנגנונים לשמירת לוגים ונתוני תיעוד כאמור ולוודא כי הם מיושמים כראוי, לרבות במסגרת ביקורות תקופתיות. נציין כי עם כניסתו לתוקף של תיקון 13 לחוק הגנת הפרטיות, בחודש אוגוסט 2025, תוכל הרשות להטיל עיצומים כספיים בגובה של 40,000-160,000 ש"ח בגין הפרה של הוראות תקנה 10 לתקנות.

נשמח לעמוד לרשותכם בכל שאלה בנושא.

* עדכון זה נועד לספק מידע כללי ותמציתי בלבד. הוא אינו מהווה ניתוח מלא או שלם של הסוגיות הנידונות, אינו מהווה חוות דעת משפטית או ייעוץ משפטי ואין להסתמך עליו.

אנשי קשר



מליסה פירון
עורכת דין



אסף הראל
שותף