אם אינך רואה מייל זה לחץ כאן

ניהול סיכוני אבטחת מידע בעת שימוש בקוד פתוח

14 באפריל, 2024

הרשות להגנת הפרטיות פרסמה ביום 8.4.24 מסמך שבו נקבע לראשונה כי שימוש בתוכנות קוד פתוח בלתי מאובטחות עשוי להוביל להפרת חוק הגנת הפרטיות ותקנות אבטחת המידע שמכוחו ("החוק", "התקנות").

כפי שיפורט להלן, קביעת הרשות בעניין זה היא קביעה חשובה לחברות טכנולוגיה ואחרות, נוכח השכיחות של השימוש מצדן בקוד פתוח והחובות האופרטיביות שהרשות קובעת בנושא.

כידוע, חברות תוכנה רבות מסתמכות על קוד פתוח בעת פיתוח מוצריהן, וארגונים אחרים מטמיעים מערכות מבוססות קוד פתוח[1] כדבר שבשגרה. בעלי מאגר מידע יכולים לפתח קוד פתוח בעצמם, להטמיע קוד פתוח, או לרכוש מוצר תוכנה שמוטמע בו קוד פתוח. עם זאת, כאשר הקוד אינו מנוהל ומתוחזק כראוי, הוא עשוי להכיל חולשות אבטחה אשר עלולות להוביל לאירועי אבטחת מידע ובהתאם, דורשות התייחסות וטיפול של בעל המאגר.

הרשות זיהתה מספר סיכונים מרכזיים בעת השימוש בקוד פתוח, לרבות:

- פרצות אבטחה הניתנות לניצול על-ידי גורמים זדוניים אשר עלולות להוביל לחשיפה של מידע אישי רגיש (ואף מידע סודי ומסחרי).
- אי ידיעה או הכרות מספקת עם רכיבי הקוד הפתוח;
- היעדר תחזוקה ותמיכה נאותים;
- חולשה ידועה (חולשה המפורסמת לכל) שעשויה לאפשר גישה לא מבוקרת לבסיסי נתונים;
- חולשת יום-אפס שאינה ידועה, "דלת אחורית", שמאפשרת למפתח זדוני להפעיל מרחוק קוד שנשתל בספריה מלכתחילה.

במסגרת המסמך, הרשות מציינת מספר היבטים ופעולות נדרשים על מנת לצמצם חשיפה בהיבט שימוש בתוכנות קוד פתוח ולצורך עמידה בדרישות החוק, ובכלל זה:

1. התייחסות לתוכנות קוד פתוח במסגרת רשימת מערכות המאגר הנדרשת במסגרת התקנות.
2. להימנע משימוש בתוכנות קוד פתוח שאינן נתמכות ומתוחזקות בידי קהילת הקוד הפתוח או בידי גוף אחר אשר תומך בהיבטי האבטחה של התוכנות, כנדרש ומפורט בתקנות.
3. בעת השימוש בקוד פתוח, אין לחבר את מערכות המאגר לרשת אינטרנט או לרשת ציבורית אחרת, ללא התקנת אמצעי הגנה מתאימים מפני חדירה לא מורשית.
4. במקרה של מיקור חוץ במסגרתו נעשה שימוש בקוד פתוח, על בעל המאגר להבטיח שחובות האבטחה ביחס להטמעת קוד פתוח מיושמות על ידי ספקיו החיצוניים, ואף על ידי ספקי המשנה של הספק על ידי ביצוע בדיקות מקדימות להתקשרות וכן הכללת התחייבויות חוזיות מתאימות.

בהתאם למסמך ועמדת הרשות, יש לוודא כי ככל שנעשה שימוש בתוכנות קוד פתוח במסגרת מאגרי מידע בהם מאוחסן מידע אישי, השימוש מתבצע בהתאם להוראות החוק והתקנות.

אנו ממליצים לפנות ולהתייעץ עם צוות הפרטיות במשרדנו ככל שהאמור רלוונטי לפעילותכם וכמובן באופן כללי כדי למפות את החובות שחלות על ארגונך ולבנות תכנית סדורה לעמידה בהן והפחתת סיכוני פרטיות ואבטחת מידע.

---

[1]קוד פתוח (Open Source) הוא מודל לפיתוח תוכנה בשיתוף פעולה המוני. בקוד פתוח, קוד המקור ומסמכי התיעוד שלו זמינים לציבור הרחב לשימוש, עריכת שינויים והפצה על פי תנאי הרישיון. מערכות מאגר רבות ואף מערכות אבטחה, מבוססות במידה מסוימת על שימוש בקוד פתוח, כשאי-יישום הנחיות בסיסיות לפיתוח וניהול קוד מאובטח, יוצר איום ממשי לפגיעה בפרטיות.

פרטי קשר

טלי יבין-סורסקי, שותפה
דיני פרטיות והגנת מידע
03-6103998
taliy@meitar.com

עדן אברהם, עו"ד
דיני פרטיות והגנת מידע
03-6144857
edena@meitar.com

שמשון מורפורגו, עו"ד
דיני פרטיות והגנת מידע

מתן שרף, עו"ד
דיני פרטיות והגנת מידע

03-6142642
matans@meitar.com

03-6103125
samsonm@meitar.com

למידע נוסף אודות מחלקת דיני פרטיות והגנת מידע במשרדנו, לחצו כאן.

מיתר | עורכי דין
דרך אבא הילל סילבר 16, רמת גן, 5250608, ישראל | 03-6103100