



עדכון לקוחות לעניין ניהול סיכוני אבטחת מידע בשימוש בקוד פתוח

לקוחות נכבדים,

נבקש להביא לידיעתכם כי ביום 10.4.2024 פרסמה הרשות להגנת הפרטיות גילוי דעת בדבר ניהול סיכוני אבטחת מידע בעת שימוש בקוד פתוח. כפי שיפורט להלן, שימוש בקוד פתוח במערכות מאגרי מידע, ללא ניהול ותחזוקה ראויים, עשוי להכיל חולשת אבטחה ולגרום לחשיפה של מידע אישי רגיש.

רקע

קוד פתוח (Open Source) הינו מודל לפיתוח תוכנה בשיתוף פעולה המוני. בקוד פתוח, קוד המקור ומסמכי התייעוד שלו זמינים באופן חופשי לציבור הרחב לשימוש, עריכת שינויים והפצה על פי תנאי הרישיון. קוד פתוח או תוכנה חופשית, מוטמעת בכ-96% ממוצרי התוכנה המסחריים, בשיעור ממוצע של 76% מתכולת הקוד בתוכנה מסחרית. במקביל לכך, מתקפות סייבר המנצלות חולשות בקוד פתוח הולכות ומתרבות.

הטמעת קוד פתוח על ידי בעל מאגר מידע, מביאה עימה סיכונים, בהם סיכונים לפגיעה בפרטיות.

על פי חוק הגנת הפרטיות התשמ"א-1981 על בעל מאגר מידע, מחזיק במאגר או מנהל מאגר חלה חובת אחריות לאבטחת המידע שבמאגר המידע. מכוח חוק הגנת הפרטיות הותקנו תקנות הגנת הפרטיות (אבטחת מידע), התשע"ז-2017 שמטרתן להבטיח כי מאגרי מידע ומערכות החומרה והתוכנה שלהם יאובטחו כראוי. אי-מתן מענה הולם בהיבטי אבטחת מידע לסיכונים הכרוכים בשימוש בקוד פתוח, עלול לעלות כדי הפרה של הוראות החוק או התקנות.

עמדת הרשות להגנת הפרטיות על פי גילוי הדעת מיום 10.4.2024

חובות מרכזיות בעת שימוש בקוד פתוח:

1. **תקנה 5(א) לתקנות אבטחת מידע**, אשר קובעת כי בעל מאגר מידע יחזיק רשימת מצאי מעודכנת של מערכות המאגר, חלה גם ביחס לרכיבי המערכת שהם מבוססי קוד פתוח, **ויש לוודא כי רשימת המצאי מאפשרת להבין באופן ברור אילו חלקי תוכנה מבוססים על רכיבי קוד פתוח.**
2. **תקנה 13(ג) לתקנות**, דורשת שלא יעשה שימוש במערכות שהיצרן לא תומך בהיבטי האבטחה שלהן. על כן, אין להשתמש בספריית קוד פתוח שאינה נתמכת ומתוחזקת בידי קהילת הקוד הפתוח או בידי גוף אחר אשר תומך בהיבטי האבטחה של הספרייה.
3. **תקנה 14(א) לתקנות**, קובעת כי בעל מאגר לא יחבר את מערכות המאגר לרשת האינטרנט או לרשת ציבורית אחרת, בלא התקנת אמצעי הגנה מתאימים. **אחריות זו חלה גם כאשר אמצעי ההגנה שהותקנו מכילים קוד פתוח.**

תקנה 15(א)(1) לתקנות, קובעת כי במקרה של מיקור חוץ, בעל מאגר יבחן לפני ביצוע התקשרות עם הגורם החיצוני המסוים את סיכוני אבטחת המידע הכרוכים בהתקשרות. **מיקור חוץ של שירות או מוצר יכול שיהיה גם קוד פתוח, והסכמה לתנאי רישיון של שירות או מוצר, או חתימה על חוזה להתקשרות לשם קבלת שירות או מוצר, מטילה על בעל המאגר חובה לבחון את כל סיכוני האבטחה (למשל קוד פתוח עם המאפשר למפתח להפעיל קוד מרוחק בדדון וכיו"ב).**

עיקרון "עיצוב לפרטיות" (Privacy by Design) הרשות להגנת הפרטיות ממליצה לאמץ מודל "עיצוב לפרטיות", ובמסגרתו להתייחס לכל שימוש בקוד פתוח. ראשיתו של המודל היא כבר בשלבים מוקדמים של אפיון המערכת, המשכו בבקרה על הקוד שפותח ועדכנו. להטעמת העיקרון דרושה מודעות מכלל העוסקים במלאכה, לרבות מי שמאפיין את המערכת, מי שמעצב את הארכיטקטורה שלה, ולבסוף, מאת צוות הפיתוח, המיישם את דרישות האפיון, העיצוב והפיתוח, ומטמיע את הקוד הפתוח. טרם הטמעת קוד פתוח, חובה להיערך בהתאם ולנקוט בפעולות מקדימות, כגון, פרסום מסמך הגדרות מאגר, אשר בין היתר כולל התייחסות לסיכונים העיקריים הנובעים משימוש בקוד פתוח ואופן ההתמודדות עימם, הפעלת תוכנית הכשרה כשזו נדרשת, חלוקת תפקידים ברורה בין הגורמים האמונים על אבטחת המידע ועוד.

המלצות ויישום

לאור האמור, גיבשה הרשות להגנת הפרטיות מספר המלצות, אותן אנו מבקשים להביא בפניכם:

- יש להבטיח כי חובות האבטחה ביחס להטמעת קוד פתוח בארגון מיושמות. ניהול סיכונים אבטחת המידע וסקירתם היא חובתו של בעל מאגר המידע, לרבות במקרים של התקשרות במיקור חוץ.
- ככל שנעשה שימוש בקוד פתוח, קיימות בשוק מסגרות עבודה מוכרות ומקובלות, כגון:
 - ISO/IEC DIS 18974, OpenChain Security Assurance Specification
 - ISO/IEC 5230:2020, the International Standard for open-source compliance
 - Microsoft S2C2F
- מומלץ לאמץ מדיניות של "עיצוב לפרטיות" (privacy by design) ובמסגרתה להתייחס בין היתר, לכל שימוש בקוד פתוח.
- על בעל המאגר לזהות רכיבי תוכנה בקוד פתוח הנמצאים בשימוש, כולל אלו הנמצאים בשימוש עקיף; לקבוע ולנהל באיזה רישיון משתמש כל רכיב קוד פתוח; להגדיר ולנהל את נוהלי הקוד הפתוח ולוודא שהתחייבויות הרישוי מתקיימות בעת השימוש או בעת שחרור מוצר; לוודא סקירה כללית של תוכנית תאימות לקוד פתוח.
- מוצע לנהל מעקב הדוק אחר תוכנות קוד פתוח ולבחון את הסיכונים בשימוש בהן. אחת הדרכים לכך היא באמצעות שימוש בכלים כדוגמת VEX ו-SBOM.
- מוצע לאמץ גישה על פיה ישולב נושא האבטחה כבר בתחילת שלבי הפיתוח ולא לאחר סיומו. כך למשל יש לעשות, בין היתר, שימוש בכלי בדיקה אוטומטיים ובמבחני חדירה לאפליקציות, לאורך כל שלבי מחזור החיים בפיתוח תוכנה ובתהליכי תחזוקתה.

המסמכים שפורסמו על ידי הרשות להגנת הפרטיות זמינים [כאן](#).

נשמח לעמוד לרשותכם בכל עניין הנוגע לעדכון זה.

למידע נוסף ניתן לפנות אל:

03-6941320	adat@fbclawyers.com	עו"ד עמית דת
03-6941320	orachum@fbclawyers.com	עו"ד ד"ר עמרי רחום-טוויג
03-7428703	jamidor@fbclawyers.com	עו"ד ג'ודי עמידור
03-7428703	lzivoni@fbclawyers.com	עו"ד לני צבעוני

הכלול באגרת מידע זו הוא מידע כללי בלבד, הוא אינו חוות דעת משפטית או ייעוץ משפטי ואין להסתמך עליו. כל הזכויות שמורות לפישר (FBC & Co.). להירשם למייל זה או להסרה מרשימת התפוצה - newsletter@fbclawyers.com