

עקרונות ניהול סיכוני אבטחת מידע בשימוש בקוד פתוח

עדכוני לקוחות

ביום 10 באפריל 2024 פרסמה הרשות להגנת הפרטיות (להלן: "הרשות") [מסמך עקרונות](#) לניהול סיכוני אבטחת מידע בעת שימוש בקוד פתוח (Open Source) במערכות מאגר מידע, בהתבסס על הוראות חוק הגנת הפרטיות, התשמ"א – 1981 ("החוק") ותקנות הגנת הפרטיות (אבטחת מידע), התשע"ז-2017 ("התקנות").

"קוד פתוח" הוא מודל מבוסס לפיתוח תוכנה בשיתוף פעולה המוני, באופן שקוד המקור ומסמכי התיעוד זמינים לציבור הרחב לשימוש, עריכת שינויים ולהפצתו מחדש. כאשר הקוד הפתוח מוטמע ברוב המוחלט של מוצרי התוכנה המסחריים והשימוש בו חוצה תעשיות ומגזרים. לצד זאת, ישנה מגמה הולכת וגוברת של מתקפות סייבר המבקשות לנצל חולשות בקוד הפתוח.

לנוכח היבטי אבטחת מידע ייחודיים הכרוכים בשימוש בקוד פתוח, ריכזנו עבורכם את 5 הדרישות המרכזיות שלעמדת הרשות יש לתת עליהן את הדעת:

- 1. להחזיק ברשימת מצאי מעודכנת של מערכות המאגר ובכלל זה מערכות תוכנה המשמשות להפעלת מאגר המידע, לניהול, תחזוקתו, תמיכה בפעילותו, ניטורו ואבטחתו.** הרשות מבהירה כי החובה חלה גם ביחס לרכיבי המערכת המבוססים על קוד פתוח וכי בעל מאגר נדרש לוודא שרשימת המצאי מאפשרת להבין באופן ברור אילו חלקים ממערכות התוכנה מבוססים על רכיבי קוד פתוח. בהקשר זה, הרשות רואה בחיוב הסתייעות בכלי תוכנה שיכולים לסייע במיפוי תשתית התוכנה של מערכות המאגר.
- 2. לא להשתמש במערכות שהיצרן לא תומך בהיבטי האבטחה שלהן.** הרשות מבהירה כי אין להשתמש בספריית קוד פתוח שאינה נתמכת ומתוחזקת בידי קהילת הקוד הפתוח או בידי גוף אחר אשר תומך בהיבטי האבטחה של הספרייה.
- 3. לא לחבר את מערכות המאגר לרשת האינטרנט או לרשת ציבורית אחרת, ללא התקנת אמצעי הגנה מתאימים.** הרשות מבהירה כי חובה זו חלה גם כאשר אמצעי ההגנה שהותקנו מכילים קוד פתוח. כמו כן, לעמדת הרשות יש לוודא כי תוכנות קוד פתוח בהן עושה שימוש הארגון לא מאפשרות חדירה לא מורשית למאגרי המידע.
- 4. בחינת סיכוני אבטחת המידע בהתקשרות עם גורם חיצוני בטרם ההתקשרות.** יש לתת את הדעת לסיכונים הייחודיים שבהתקשרות עם ספק לשם קבלת שירותים אשר כוללים רכיבי קוד פתוח (כגון קוד פתוח עם "דלת אחורית" שמאפשר למפתח זדוני להפעיל מרחוק קוד או מכיל חולשה מוכרת אשר עלולה לאפשר גישה לא-מבוקרת לבסיסי נתונים). בהקשר זה, לעמדת הרשות יש להעדיף ספקי תוכנה המצהירים כי הם עומדים במסגרות עבודה מוכרות לניהול סיכונים הנובעים משימוש בקוד פתוח.
- 5. עיצוב לפרטיות (privacy by design).** הרשות ממליצה, כחלק מהעיצוב לפרטיות, להתייחס לכל שימוש של קוד פתוח החל בשלבים המוקדמים של אפיון המערכת, עיצובה ופיתוחה וכן בשלבים מאוחרים יותר של ביצוע בקרה על הקוד שפותח ועדכונו. הרשות מדגישה כי דרושה מודעות של כלל העוסקים במלאכה, לרבות גורמים המעורבים באפיון המערכת, עיצוב הארכיטקטורה ובפיתוח, וחלוקת תפקידים ברורה בין הגורמים האמונים על אבטחת המידע במאגר כך שיובהר מיהו הגורם האחראי לאבטחת מידע בהיבטי השימוש בקוד פתוח.

לסיכום, השימוש בקוד פתוח, לצד היתרונות הרבים הטמונים בו, עלול לחשוף את הארגון לסיכוני אבטחת מידע אשר מחייבים היערכות נאותה ונקיטת צעדים כדי להבטיח עמידה בדרישות החוק והתקנות.

אנו מזמינים אתכם לפנות אלינו לכל שאלה ו/או התייעצות בנושא.

עדכון זה הוכן בסיועה של מליסה פוירון.

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



אביטל חייטוביץ'
עורכת דין בכירה



אסף הראל
שותף