עקרונות לניהול סיכוני אבטחת מידע בשימוש בקוד פתוח

מבוא

מהו קוד פתוח? קוד פתוח (Open Source) הינו מודל מבוזר לפיתוח תוכנה בשיתוף פעולה המוני באופן שקוד המקור ומסמכי התיעוד זמינים באופן חופשי לציבור הרחב לשימוש, עריכת שינויים ולהפצתו מחדש. המודל נוצר מטעמי כדאיות כלכלית וטכנולוגית, וכתגובה למגבלות קניניות על הקוד, כאשר "תכנה חופשית" (Free Software), נולדה כתפיסה חברתית. לעיתים הביטויים קוד פתוח ותכנה חופשית מופיעים יחד – "תוכנת קוד חופשי ופתוח" (FOSS - Free and Open Source Software).

בעל מאגר מידע אפשר שיפתח קוד בעצמו, שיטמיע קוד פתוח בעצמו, או שירכוש מוצר תוכנה שמטמיע קוד פתוח, תחת כל רישיון שימוש.[1] הטמעת קוד פתוח שוכנת תחת המטריה של פיתוח קוד מאובטח, ומביאה עימה סיכונים, בהם סיכונים לפרטיותנו. זאת, כאשר הקוד אינו מתוחזק כראוי, ועשוי להכיל חולשות אבטחה שאינן זוכות לתיקון וללא הצבתן של בקרות מפצות, באופן שעשוי לאפשר ניצולן לפגיעה במערכות, וחשיפה של מידע אישי רגיש, פרטי או מסחרי.

במסמך זה, תפרט הרשות להגנת הפרטיות את **העקרונות החלים** בעת שימוש בקוד פתוח במערכות המאגר מכוח הוראותיו של חוק הגנת הפרטיות, התשמ"א-1981 (להלן: חוק הגנת הפרטיות) ומכוחן של תקנות הגנת הפרטיות (אבטחת מידע), התשע"ז-2017 (להלן: תקנות אבטחת מידע).

שימוש בקוד פתוח ועמידה בהוראות תקנות הגנת הפרטיות (אבטחת מידע), התשע"ז-2017

סעיף 17 לחוק הגנת הפרטיות קובע כי "בעל מאגר מידע, מחזיק במאגר מידע או מנהל מאגר מידע, כל אחד מהם אחראי לאבטחת המידע שבמאגר המידע". מכוח החוק הותקנו תקנות אבטחת מידע, שמטרתן להבטיח כי מאגרי מידע ומערכות החומרה והתוכנה שלהם יאובטחו כראוי.

עיבוד מידע אישי במאגר מידע כפוף לעמידה בהוראות חוק הגנת הפרטיות ובהוראות התקנות שהותקנו מכוחו, וזאת גם כאשר מערכות המאגר מבוססות במידה רבה או חלקית על שימוש בקוד פתוח. אי-מתן מענה הולם בהיבטי אבטחת מידע לסיכוני אבטחת מידע הכרוכים בשימוש בקוד פתוח, עלול לעלות כדי הפרה של הוראות החוק או התקנות. לנוכח היבטי אבטחת מידע ייחודים הכרוכים בשימוש בקוד פתוח, הרשות תתייחס להלן לחובות המרכזיות בתקנות אבטחת מידע אשר יש לתת עליהן את הדעת בעת שימוש בקוד פתוח:

- תקנה 5(א) לתקנות אבטחת מידע קובעת כי בעל מאגר מידע יחזיק רשימת מצאי מעודכנת של מערכות המאגר, ובכלל זה מערכות התוכנה המשמשות להפעלת מאגר המידע, לניהול המאגר ולתחזוקתו, לתמיכה בפעילותו, לניטור שלו ולאבטחתו; תוכנות וממשקים המשמשים לתקשורת אל מערכות המאגר ומהן; תאריך העדכון האחרון של המסמך ושל רשימת המצאי ועוד.

[1] ראה: https://spdx.org/licenses/

ppa@justice.gov.il | 073-3928529 | *3103
קרית הממשלה, ת.ד. 33503, תל-אביב 6133401 | www.go.gov.il/ppa

החובה האמורה חלה גם ביחס לרכיבי המערכת שהם מבוססי קוד פתוח, ויש לוודא כי רשימת המצאי מאפשרת להבין באופן ברור אילו חלקים ממערכות התוכנה מבוססים על רכיבי קוד פתוח, כאמור.

כיום, קיימים בשוק כלי תוכנה שיכולים לסייע לבעל מאגר מידע למפות את תשתית התוכנה המשמשת את מערכות המאגר מקצה-אל-קצה. הרשות רואה בחיוב הסתייעות בכלי תוכנה, כאמור, לשם עמידה בתקנה 5 לתקנות אבטחת מידע.

- תקנה 13(א) לתקנות קובעת כי "בעל מאגר מידע יקפיד על ניהול ותפעול תקין של מערכות המאגר, לפי המקובל בהפעלת מערכות כאלה". בהמשך לכך, קובעת תקנה 13(ג) במפורש כי "**בעל מאגר מידע ידאג לכך שייערכו עדכונים שוטפים של מערכות המאגר**, לרבות חומר המחשב הנדרש לפעולתן;", בהמשך מובהר כי "לא ייעשה שימוש במערכות שהיצרן לא תומך בהיבטי אבטחה שלהן אלא אם כן ניתן מענה אבטחתי מתאים".

ייחודו של קוד פתוח נובע במידה רבה מעצם העובדה ששימוש בו מותנה בקבלת רישיון שימוש, אך אינו כרוך בהחזקה ברישיון מסחרי ופעמים רבות אין 'יצרן' אשר עומד מאחוריו. לכן, לשם עמידה בהוראות התקנות האמורות, **אין להשתמש בספריית קוד פתוח שאינה נתמכת ומתוחזקת** בידי קהילת הקוד הפתוח או בידי גוף אחר אשר תומך בהיבטי האבטחה של הספרייה, כפי שנדרש בתקנה 13(ג).

- תקנה 14(א) לתקנות, קובעת כי "בעל מאגר מידע לא יחבר את מערכות המאגר לרשת האינטרנט או לרשת ציבורית אחרת, בלא התקנת אמצעי הגנה מתאימים מפני חדירה לא מורשית או מפני תוכנות המסוגלות לגרום נזק או שיבוש למחשב או לחומר מחשב".

אחריותו של בעל מאגר המידע חלה גם כאשר אמצעי ההגנה שהותקנו על מנת להגן על המידע האישי בארגון, כגון חומת-אש ואנטי-וירוס, מכילים קוד פתוח. משמעות הדברים היא כי ייתכן שארגון אשר עושה שימוש ישיר בתוכנות או ספריות קוד פתוח, או במוצר מדף שמשתמש בספריית קוד פתוח, אשר עלולות לאפשר חדירה לא מורשית למאגרי המידע של הארגון או אפשרו פעולה זדונית באמצעות קוד זה, יפר את הוראת תקנה 14(א) לתקנות, ולא יעמוד בחובה המוטלת עליו מכוח סעיף 17 לחוק.

- במקרה של מיקור-חוץ, תקנה 15(א)(1) לתקנות קובעת במפורש, כי בעל מאגר "יבחן, לפני ביצוע ההתקשרות עם הגורם החיצוני המסוים כאמור, את סיכוני אבטחת המידע הכרוכים בהתקשרות".

מיקור-חוץ של שירות או מוצר, אפשר שיהיה שירות אחסון ענן, שירות זיהוי-פנים, מנוע בינה מלאכותית, ספרית קוד עם רישיון תוכנה, תוכנה חופשית או קוד פתוח ועוד. הסכמה לתנאי הרישיון, כל רישיון, של שירות או מוצר או חתימה על חוזה להתקשרות לשם קבלת שירות או מוצר, מטילה על בעל שליטה במאגר חובה לבחון את כל סיכוני האבטחה, כאמור בתקנה 15(א)(1).

בכל הנוגע לקוד פתוח, סיכוני אבטחת מידע כוללים, בין היתר: קוד פתוח ללא תחזוקה ותמיכה נאותים; קוד פתוח עם חולשה ידועה (חולשה המפורסמת לכל, כגון אלו המפורסמות באתר

ppa@justice.gov.il | 073-3928529 | *3103
קרית הממשלה, ת.ד. 33503, תל-אביב 6133401 | www.go.gov.il/ppa

NVD)[2] אשר עשויה לאפשר גישה לא-מבוקרת לבסיסי נתונים; קוד פתוח עם "דלת אחורית", שמאפשר למפתח זדוני להפעיל מרחוק קוד, שנשתל בספריה מלכתחילה ועוד.

על בעל מאגר מידע לבחון את אופן יישום החובות בתחום אבטחת המידע, שהגורם החיצוני חייב בהן לפי תקנות אלה, וכן את אופן יישום ההנחיות הנוספות לעניין אמצעי אבטחת מידע שקבע בעל מאגר המידע, אם קבע. יודגש, כי בהתאם לתקנה 15(א)(2)(ז) אם התיר בעל מאגר מידע לגורם החיצוני לתת את השירות באמצעות גורם נוסף (קבלן משנה, צד שלישי וכדומה) **הגורם החיצוני מחויב** לכלול בהסכם עם הגורם הנוסף את כל הנושאים המפורטים בתקנה 15. המשמעות היא, שכדי שבעל המאגר והגורם החיצוני יעמדו בהוראות הדין, עליהם להבטיח שחובה זו מיושמת גם ביחס להטמעת קוד פתוח.

יצוין, כי הפרת הוראות התקנות המפורטות לעיל, עלולה אף להוביל לאי-עמידה של בעל מאגר המידע והמחזיק בחובות המוטלות עליהם מכוח סעיף 17 לחוק.

<u>מה ניתן לעשות?</u>

ידע ומידע העוסקים בכתיבת-קוד מאובטח קיימים ונגישים לכל. עם זאת, מספר אירועי אבטחת המידע המדווחים,[3] אשר נובעים מאי-יישום הנחיות בסיסיות לפיתוח-קוד מאובטח, הוא נרחב.[4] המשמעות היא למעשה שכל פיתוח קוד לא מאובטח יוצר איום ממשי לפגיעה בפרטיות.[5]

חוק הגנת הפרטיות ותקנות אבטחת מידע מטילים על בעל מאגר המידע אחריות לאבטחת המידע שבמאגר המידע, וכפועל יוצא מכך, מקימים חובות בהיבטי אבטחת המידע גם בעת שימוש בקוד פתוח.

על פי הוראות החוק ותקנות אבטחת מידע, בעל מאגר מידע חייב בניהול סיכוני אבטחת המידע ובסקירתם, לרבות בחינת רמת אבטחת המידע גם אצל הגורם החיצוני, שאתו בעל המאגר התקשר לשם מיקור-חוץ של שירות, וכך גם אם הגורם החיצוני מסתייע בגורם נוסף חלות חובות ביחס להסכם שייחתם עמו. מעשית, על כל אחד מהם להבטיח שחובות האבטחה ביחס להטמעת קוד פתוח מיושמות.

כאמור לעיל, בעל מאגר מידע אפשר שיפתח קוד בעצמו, שיטמיע קוד פתוח בעצמו, או שירכוש מוצר תוכנה שמטמיע קוד פתוח, תחת כל רישיון שימוש.[6] על בעל מאגר המידע מוטלת חובה לנהל ולתפעל את מערכות המאגר באופן תקין, כהוראת תקנה 13(א) לתקנות אבטחת מידע. עליו לעשות זאת בהתאם למקובל בתעשייה בכל הנוגע לפיתוח קוד מאובטח, להטמעת ספריית קוד או לרכישת מוצר תוכנה.

---

[2] ראה:
https://nvd.nist.gov/

[3] ראה על הפרצה בספריית log4j:
https://www.ynet.co.il/digital/technews/article/rjzatifck

[4] ראה:
https://www.gartner.com/en/newsroom/press-releases/2022-03-07-gartner-identifies-top-security-and-risk-management-trends-for-2022

[5] ראה המתקפה על אתר "למטיילי":
https://www.mako.co.il/news-digital/2021_q4/Article-b1ebccfac4fcd71027.htm

[6] ראה:
https://spdx.org/licenses/

ppa@justice.gov.il | 073-3928529 | *3103
קרית הממשלה, ת.ד. 33503, תל-אביב 6133401 | www.go.gov.il/ppa

הרשות להגנת הפרטיות רואה ערך רב בהקפדה על עדכון ותחזוקה של מערכות המאגר, בהגברת החוסן בהגנה על מאגרי מידע, ובשקיפות וניהול מיטבי של קוד. בעיקר, בעת התקשרות עם ספק לשם קבלת שירותים אשר כוללים רכיבי קוד פתוח. רכיבי קוד פתוח יכולים להיות מוטמעים גם בתוכנה מסחרית במסגרת מיקור-חוץ.

בכל הנוגע לניהול סיכונים[7] הנובעים משימוש בקוד פתוח, קיימות בשוק מסגרות עבודה (framework) מוכרות ומקובלות, כגון: ISO/IEC 5230 (identical to OpenChain specification 2.1); ISO/IEC DIS 18974[8] (identical to OpenChain security assurance specification 1.1); Microsoft S2C2F[9] ועוד.

אם נעשה שימוש בתוכנה קניינית או מסחרית, חובה לנהל אותה ולוודא כי אינה מכילה חולשות ידועות הניתנות לניצול (known exploitable vulnerabilities). ניתן לדרוש מהספק רשימת מצאי או להעדיף ספק תוכנה המצהיר כי הוא עומד במסגרת עבודה מוכרת ומקובלת.

הרשות ממליצה לאמץ "עיצוב לפרטיות" (privacy by design), ובמסגרתו להתייחס, בין היתר, לכל שימוש קוד פתוח. ראשיתו של "עיצוב לפרטיות" היא כבר בשלבים מוקדמים של אפיון המערכת, עיצובה ופיתוחה. המשכו בבקרה על הקוד שפותח ועדכונו. 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 במאגר כך שיובהר מיהו הגורם האחראי לאבטחת מידע בהיבטי השימוש בקוד פתוח וכן על הטמעתו בארגון (דוגמת Open Source Program Officer); לאחר הטמעת קוד פתוח, יש להיות ערניים לקוד שבמהלך השימוש בו מתברר כי אינו נתמך עוד. במצב שכזה יש להחליט האם לתחזק את הקוד עצמאית, או להחליפו.

כאמור, לפי תקנה 5 לתקנות אבטחת מידע, על בעל מאגר מידע למפות את מבנה מאגר המידע ולהחזיק רשימת מצאי מעודכנת של מערכות המאגר, לרבות תוכנות וממשקים. לשם כך 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; להקפיד על ביצוע הכשרה של כלל המעורבים בפיתוח ובניהול הקוד על פי הנדרש. אחת הדרכים שבהן ניתן לנהל מעקב הדוק אחר תוכנות קוד פתוח והסיכונים בשימוש בהן כתוצאה מחולשות ידועות היא באמצעות שימוש בכלים כדוגמת SBOM ו- VEX.[10]

---

[7] מפת הדרכים של אבטחת תוכנת קוד פתוח של CISA המפרט מטרות ויעדים ל 2024 – 2026:

[8] התקן אושר בדצמבר 2023 ראה:
https://www.openchainproject.org/security-assurance

[9] ראה:
https://www.microsoft.com/en-us/securityengineering/opensource

[10] ראה:
https://blog.adolus.com/what-is-vex-and-what-does-it-have-to-do-with-sboms
https://www.ntia.doc.gov/files/ntia/publications/ntia_sbom_framing_sharing_july9.pdf

ppa@justice.gov.il | 073-3928529 | *3103
קרית הממשלה, ת.ד. 33503, תל-אביב 6133401 | www.go.gov.il/ppa

לבסוף, הוראות החוק מטילות על בעל מאגר לבחון את אופן יישום החובות בתחום אבטחת המידע שהוא או המחזיק במאגר חייבים בהן לפי תקנות אלה, וכמו-כן, מטבע הדברים על בעל המאגר לבחון קיומן של הנחיות נוספות לעניין אמצעי אבטחת מידע שקבע, אם נקבעו על-ידי הרשות הנחיות נוספות. בעל מאגר מידע שהתיר לגורם חיצוני לתת שירות באמצעות גורם נוסף, אזי חובתו של הגורם החיצוני לכלול בהסכם עם הגורם הנוסף את כל הנושאים המפורטים בתקנה 15 לתקנות אבטחת מידע. כדי שבעל המאגר והגורם החיצוני יעמדו בהוראות החוק, עליהם להבטיח חוזית שהאחריות על הטמעת קוד פתוח תחלחל במורד שרשרת האספקה עד לספק האחרון בשרשרת האספקה.

בהמשך למסמך זה נספח הרחבה למסמך עקרונות לניהול סיכוני אבטחת מידע בשימוש בקוד פתוח.

ppa@justice.gov.il | 073-3928529 | *3103
קרית הממשלה, ת.ד. 33503, תל-אביב 6133401 | www.go.gov.il/ppa