SECAUDIT
IT & CYBER AUDIT EXPERTS

אבטחת שרשרת האספקה

מאת: אורן שני, מנכ"ל משותף בחברת "סקאודיט"

אבטחת שרשרת האספקה היא נושא חשוב וקריטי בעידן בו חשיפה לסיכונים פוטנציאליים עשויים להביא לנזק כבד כלכלי, פיזי או בריאותי. העובדה כי ארגונים רבים הכניסו שימוש מאסיבי בשירותי גישה מרחוק למערכות המידע ומעבר לענן מייצרת סיכונים חדשים ואף מגדילה את "משטח התקיפה" של גורמים עוינים. נכונות הארגונים להתמודד עם סיכונים אלה התעוררה והתחזקה, והשקעת תשומות בנושא אבטחת שרשרת האספקה הינה קריטית בהבטחת קיום ותפעול חלק, שמירה על פרטיות הלקוחות והאינטרסים הכלכליים של הארגונים.

גורמים רגולטורים שונים, הפיצו דרישות להגנה מסיכוני סייבר בשרשרת האספקה כגון:

- בנק ישראל, כמו רשויות הרגולציה הפיננסית במדינות רבות בעולם, דורש מהבנקים והגורמים הפיננסיים המפוקחים על ידו עמידה בתקנות והנחיות בנוגע לאבטחת שרשרת האספקה, במסגרת הוראה 363, "ניהול סיכוני סייבר בשרשרת אספקה". זאת בכדי להבטיח את יציבותם ואמינותם של המערכות הפיננסיות, וכן להגן על הציבור והלקוחות מסיכונים שונים.
- מערך הסייבר הלאומי פרסם דגשים עבור "הגנת סייבר שרשרת אספקה" שמטרתו להציג מתודה סדורה, לניהול יעיל ולצמצום של איומי הסייבר אשר מקורם בשרשרת האספקה.
- הרשות להגנת הפרטיות: תקנה 15 לתקנות אבטחת מידע עוסקת בחובות החלות על בעל מאגר המתקשר עם גורם חיצוני לצורך קבלת שירות הכרוך במתן גישה למאגר מידע. הרשות פרסמה מספר הנחיות, לאורך השנים, המתייחסות לאופן ההתנהלות הנדרש מבעלי מאגר מידע בעת שימוש בשירותי מיקור חוץ.
- יה"ב - היחידה להגנת הסייבר האחראית להכוונה ולהנחיה המקצועית בתחום הגנת הסייבר עבור משרדי הממשלה פרסמה הנחיה בנושא שרשרת האספקה, המבוססת על המתודולוגיה של מערך הסייבר הלאומי.

למרבה הצער, בישראל קרו אירועי סייבר בשרשרת האספקה בשנים האחרונות. הדוגמא האחרונה כוללת פריצה של האקרים איראניים למערכות של מכללות רבות בישראל, כולל גניבת נתונים (פרטיים ואחרים) דרך פריצה לשרשרת האספקה, כאשר בפועל פרצו ההאקרים לחברה המספקת שירותים לאותם גופים אקדמאים. פורסם כי בין הגופים שנפרצו היו, על פי הצהרת ההאקרים, בסיסי הנתונים של מכללת אריאל, מכללת ספיר, בית ברל, דעת נסים, גור אשדוד, המכללה האקדמית חמדת, הקולג' הישראלי, מכללת המשטרה בבית שמש ועוד.

במצב בו הפריצה מתרחשת לגופים פיננסיים, גניבה של מידע רגיש (אישי או עסקי רגיש השייך לחברה) תיתכן ותגרום לפגיעה פיננסית מידית, פגיעה במוניטין ועד לפגיעה ביציבות המערכות הפיננסית. בהתייחס לגופים רפואיים או גופי תשתית קריטית, אזי מתקפת סייבר אל מול שרשרת האספקה עלולה להביא מעבר לאלה המצוינות מעלה לפגיעה ממשית בלחיי אדם, עד פגיעה בהיקף נרחב ומשמעותי.

למרבית הארגונים, פיננסיים, תשתיתיים, רפואיים ואחרים, יש צוותים מקצועיים שמטפלים באבטחת מידע ומערכות מידע, אולם ניכר כי נושא אבטחת שרשרת האספקה נופל פעמים רבות בין הכיסאות, תוך העברת אחריות לגוף שמספק השירות. עם זאת, לקוח קצה שנפגע מתקיפה כזו מכיר גורם אחד, את החברה ממנה רכש השירות, ואין לו עניין בגורמים הטכנולוגיים שמספקים את השירות ברקע.

דוח מבקר המדינה מציין כי מתוך הגופים שבדק, כ 60% מהגופים בממוצע מממשים הגנות חלקיות בלבד אל מול מתקפות מכיוון שרשרת האספקה, דבר המותיר גופים רבים חשופים למתקפות. בנוסף מציין הדוח כי 30% ממשרדי הממשלה וגופי התמ"ק (תשתיות קריטיות) דיווחו שחוו אירוע סייבר בשנים 2021 – 2022, שמקורו בשרשרת האספקה, מתוכם 60% לא קיבלו עדכון על המתקפה מהספק עצמו אלא מגורמים אחרים (כגון מערך הסייבר או אמצעי התקשורת).

פעמים רבות, חברות אינן מבצעות פעילות בחינה של ספקי שירות בתחום ה IT המהווים חלק משרשרת האספקה, בשל ההנחה כי הגוף מספק השירות הינו גוף רציני, מכובד וכזה המספק שירות לגופים גדולים אחרים, ויוצאים מתוך הנחה שהגוף מממש הגנות איכותיות, עליהן הם יכולים להסתמך. בפועל, במקרים רבים הדבר רחוק מהמציאות.

כיצד מתמודדים עם אבטחת שרשרת האספקה?

- רצוי כי תגובש מדיניות כתובה, ברורה ומגובה ע"י הנהלת החברה המגדירה מהן הפעולות המהותיות שיש לבצע בעת התקשרות עם ספק מהותי בשרשרת האספקה, מדיניות שתתורגם לנהלי עבודה ולמעשים בשטח.

- יש לבצע בחינת הפער הקיים בין המצב הרצוי למצב המצוי. בחינה זו אמורה לכלול סקירה אבטחתית של ספקי השירות המהותיים בשרשרת האספקה אל מול דרישות ייסוד של הארגון, דרישות חוקיות ורגולציה מובילה.
- יש לקבוע תהליכים סדורים של שילוב וגריעת ספקים מהותיים בתהליך כולל שילובם של גופים נוספים, מעבר לגוף הרכש ובכלל זה הייעוץ המשפטי, מחלקת אבטחת המידע והייעוץ הביטוחי, כולל שילובן של דרישות ברורות בעת חתימת חוזים עם ספקים מהותיים ביחס לפעילות שתבוצע טרם ההתקשרות ובמהלכה בנושא הגנת סייבר על ידי החברה, בחצרות הספק.

כמו כל תהליך אבטחתי בארגון, גם אבטחת סייבר בשרשרת האספקה הינה פעילות מתמשכת שעליה להתאים עצמה לסיכונים החדשים המתגלים, תוך פיקוח מתמיד ומעקב אחר הנעשה אצל ספקי המחשוב המשולבים בשרשרת האספקה הארגונית.

חברת סקאודיט מספקת שירותי ביקורת של אבטחת שרשרת האספקה, המאפשרים לחברות לנתח את המצב הקיים, לסמן בבירור את אבני הנגף העיקריות ולקבוע המלצות לטיפול בהן.