טיפול באירוע סייבר

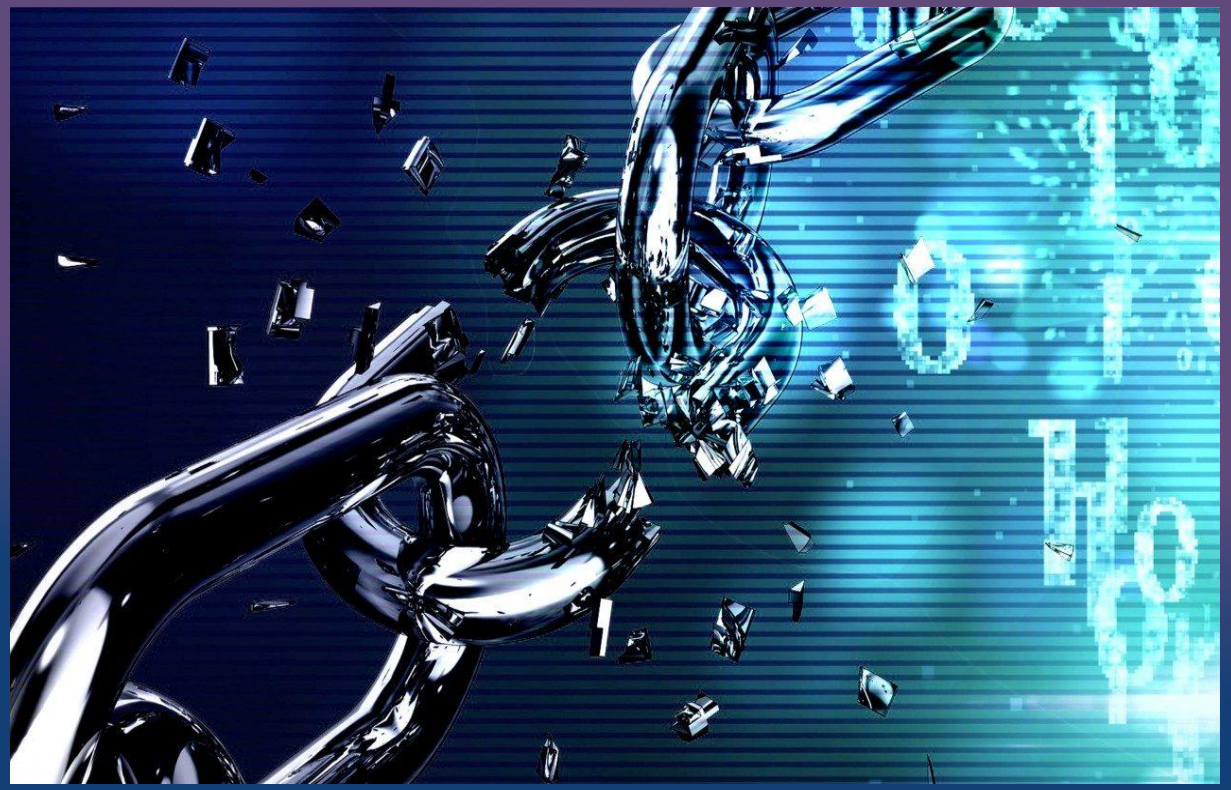
חנן טויזר
שותף, מנהל מח' ייעוץ וביקורת מערכות מידע
פאהן קנה ניהול בקרה בע"מ
Hanan.Twizer@il.gt.com
יוני 2022

Fahn Kanne
Grant Thornton
An instinct for growth™

סיכוני סייבר בשרשרת אספקה

ארגונים רבים נעזרים בגורמי צד ג' לצרכי תמיכה, פיתוח, ניהול ותחזוקה של מערכות מידע ומאגרי נתונים.

מצב זה חושף את הארגונים לסיכונים שונים כגון דליפת מידע ושיבוש נתונים ומאלץ את הארגונים לקיים תהליכים ובקרות לצמצום הסיכונים והחשיפות.



תחקיר אירוע סייבר

מנהל הכספים מקבל הודעה מגורם אנונימי, אשר טוען כי עלה בידו לחדור למערכות הארגון ולשלוף מאגר מידע הכולל פרטים רבים וחסויים.
הגורם מבקש 25 אלף דולר בביטקויין ובמידה ולא יקבל את הסכום בתוך 48 שעות, מאגר המידע יפורסם.

הארגון מפעיל נוהל אירוע סייבר

- מוקם צוות תגובה אשר כולל את מנכ"ל החברה, מנהל אבטחת המידע, מנמ"ר החברה, יעוץ המשפטי של החברה, מנהלת משאבי אנוש ואנשי צוות טכני מחברה ייעודית של לניהול תגובה לארועי סייבר.
- מוכרז אירוע סייבר בארגון

מתחיל תחקור האירוע

במסגרת התחקור, הצוותים הטכניים, בודקים מי התחבר לרשת ולמערכות, מי ניגש למסדי נתונים, מי שלף מידע ואף את תעבורת הרשת בתקופה האחרונה.

במסגרת כל הבדיקות לא נמצאה התחברות לרשת או גישה לבסיסי נתונים שאינה מוכרת, או תעבורת רשת חשודה.

המשך תחקור של האירוע

לאחר בחינה מחודשת של היסטורית הגישה לבסיסי הנתונים ושליפתם, מתברר כי לפני מספר שנים החברה נעזרה בספק חיצוני לצורך פיתוח תוכנה באחת המערכות ובמסגרת הפיתוח ולצורך בדיקת המערכת עם נתוני אמת, העבירה החברה בסיס נתונים לספק.

עם זאת, מבדיקה עם ספק הפיתוח עולה כי הוא אינו מכיר מתקפת סייבר כלל.

המשך תחקור של האירוע

אולם, בהמשך התחקור עולה כי ספק הפיתוח העסיק קבלן (גורם צד ג' נוסף) מיקור חוץ לצורך הפיתוח אשר קיבל לידו את בסיס הנתונים ואצלו מסתבר בוצעה מתקפת הסייבר ודרכו דלף המאגר...

טיפים לדירקטור

- לוודא כי הארגון הגדיר ויישם מדיניות הערכת סיכונים בשרשרת האספקה - SCRM – Supply Chain Risk Management
- ודא כי מיפוי ספקים שנערך כולל את דירוגם על פי רמת רגישות המידע אילו הם נחשפים
- במסגרת הסכם התקשרות, עיגון דרישות לעמידה בתקני אבטחת מידע מחמירים, לרבות ביצוע סקר ספק בטרם ביצוע התקשרות
- ביצוע ביקורות בחצרות הספק
- דרישה מהספק לעבור מבדקי חדירה
- יישום מדיניות סיום התקשרות עם ספק
- קיום תרגילים תגובה לאירועי סייבר
- שילוב הספק בתרגילי תגובה לאירועי סייבר.

תודה על ההקשבה!

חנן טויזר
שותף, מנהל מחלקת מערכות מידע
050-8230209
Hanan.Twizer@il.gt.com

Fahn Kanne
Grant Thornton