יכולת מגזרית לניהול סיכוני סייבר בשרשרת האספקה

גבי סיבוני, הדס קליין וזיו סולומון

מאמר זה מציג את סיכוני הסייבר שמקורם בשרשרת האספקה ואת אתגרי ההתמודדות עם סיכונים אלה. המאמר בוחן מספר מתודולוגיות ותקינות בעולם לניהול סיכוני הסייבר בשרשרת האספקה ומציע מודל לניהול מגזרי מרוכז של האתגר באופן שייעל את תהליך בדיקת הספקים והסמכתם. המודל המוצע נמצא ככדאי הן מבחינת השקעת המשאבים ואיגומם והן מבחינת העלאת רמת הביטחון הכוללת של המגזרים השונים, וכנגזרת מכך – העלאת רמת המוגנות של הסייבר במשק הישראלי כולו.

מילות מפתח: איום הסייבר, ניהול סיכוני סייבר, שרשרת אספקה, מרחב הסייבר

מבוא

בחודש יולי 2018 זיהה צוות מחקר של חברת "מיקרוסופט" מתקפה[1] על חברת תוכנה, שמטרתה הייתה להטמיע קוד זדוני במוצר תוכנה לגיטימי, ובדרך זו להגיע לאלפי לקוחות אחרים. במקרה זה, תוקפים אנונימיים הצליחו להשתלט על תשתית משותפת של חברת תוכנה המספקת עורך מסמכי PDF ושל חברה המספקת לה את חבילת ההתקנה (Installer), באופן שבו ה־Installer יתקין, בנוסף לעורך ה־PDF, גם קוד זדוני. חקירת המקרה העלתה כי בית התוכנה המספק את עורך ה־PDF כלל לא הותקף; המוצר שלו הוחלף באמצעות התערבות בתהליך

פרופ׳ גבי סיבוני הינו ראש תוכנית ביטחון סייבר במכון למחקרי ביטחון לאומי. הדס קליין היא חוקרת סייבר במכון למחקרי ביטחון לאומי. זיו סולומון הוא יועץ בתחום ביטחון סייבר.

המאמר מתבסס על עבודת מחקר שנכתבה על ידי גבי סיבוני, זיו סולומון והדס קליין, **ניהול סיכוני שרשרת אספקה במגזר הפיננסי: צמצום איומים בשרשרת האספקה**, המכון למחקרי ביטחון לאומי, דצמבר 2018.

1 "Attack Inception: Compromised supply chain within a supply chain poses new risks", *Microsoft Defender Research Team*, July 2018, https://bit.ly/2UcVsGB.

הנמצא בבית התוכנה השני – זה המספק את חבילת ההתקנה. דוגמה זו מהווה הוכחה למשאבים הגדולים אותם משקיעים תוקפים כדי להגיע ליעדם דרך שרשרת האספקה.

"שרשרת אספקה" תוגדר כאן כ"מערכת של גורמים המעורבים באספקה של מוצר או שירות, בכלל אלה: נותני שירותים, ספקי תוכנה ומערכות מידע, ספקי חומרה וכדומה". בעידן הגלובלי הנוכחי, המתאפיין במורכבות טכנולוגית של מוצרים ושירותים, תוך הסתייעות במגוון ספקים רחב לכל מוצר או שירות, קיים צורך להבטיח את הגנת הסייבר אצל ספקים של כל ארגון באשר הוא. הדוגמה שהובאה לעיל הינה אחת מני רבות בהן תוקף ניצל פרצות אבטחה אצל ספקים של ארגון במטרה לחדור לרשת המחשוב הארגונית של הארגון שאותו הוא ביקש לתקוף.

התמודדות מיטבית עם אתגרי הסייבר בשרשרת האספקה מחייבת התייחסות קונקרטית לצורכי הארגון והמגזר אליו הוא משתייך, כמו גם התייחסות לארגונים שמזוהים כישראליים מתוקף היותם חשופים לתקיפות על רקע אנטי ישראלי. ארגונים רבים בישראל כפופים להנחיות של רגולטורים, כגון הפיקוח על הבנקים, הפיקוח על חברות הביטוח, משרד הבריאות בהיותו הרגולטור של ארגוני הבריאות השונים בישראל, ועוד. הגנת ארגונים אלה מחייבת מגוון מרכיבים הגנתיים, בהם שכבת הגנה טכנולוגית ונוהלי עבודה, כולל התייחסות לאיומי הסייבר בשרשרת האספקה. ככל שהארגונים יצליחו לזהות את האיומים ולנקוט את האמצעים הנדרשים למיגורם בשלב מוקדם יותר, כך תגדל רמת ההגנה הכוללת שלהם.

מאמר זה מתאר את אתגר ההתמודדות עם סיכוני הסייבר בשרשרת האספקה ומספק המלצות כלליות להתמודדות, תוך התייחסות לתקינה רלוונטית בעולם, לרגולציה בישראל, לניתוח מפת האיומים הרלוונטיים בהקשרי שרשרת האספקה, למתודולוגיות קיימות, למודלים לניהול ספקים בשרשרת האספקה ולגישות אפשריות. המאמר מביא דוגמאות מהמשק הישראלי, שיש להן קשר אפשרי לנושא.

רקע תיאורטי

בתעשייה ובספרות המקצועית קיימים מספר מודלים ומתודולוגיות לניהול סיכונים בשרשרת האספקה. בספר *Purchasing and Supply Chain Management* מתוארות שלוש קטגוריות של ספקים:[2] ספקים אסטרטגיים בעלי חשיבות גבוהה מאוד לחברה הרוכשת, שיֵש קושי רב במציאת תחליף להם; ספקים מועדפים בעלי חשיבות לחברה הרוכשת, אולם ניתן להחליפם תוך השקעת מאמץ מסוים; ספקים בני החלפה, קרי ספקים שניתן להחליפם בתוך זמן קצר. בנוסף לחלוקה המוצעת

2 W.C. Benton, *Purchasing and Supply Management* (Irwin Professional Publishing, 2nd edition, 2009), Ch. 8.

לסוגי ספקים, תובא להלן סקירה של מספר מודלים של ניהול שרשרת אספקה בגופים רלוונטיים לענייננו.

המתודולוגיה הנהוגה בחברת Deutsche Telekom לניהול שרשרת האספקה עבור יותר מ־30,000 הספקים שלה ביותר משמונים מדינות היא מתודולוגיה בת ארבעה שלבים.[3] מטרתה היא למזער את הסיכונים ולעודד את ספקי החברה לשפר את שיטות העבודה שלהם. בשלב הראשון נשאלים כל הספקים הפוטנציאליים עם נפח הזמנה שנתי של יותר מ־100,000 אירו על נושאים כגון זכויות אדם, שחיתות, הגנת הסביבה ובריאות תעסוקתית. כל הספקים מחויבים בבחינה חוזרת לאחר שלוש שנים. ככל שהיחסים העיסקיים נמשכים, החברה מבקשת מהספקים הרלוונטיים מבחינה אסטרטגית ו/או אלה הנמצאים בסיכון גבוה להעביר מידע נרחב על שיטות העבודה שלהם באמצעות מערכות המידע.

בשלב השני מתבצעת הערכה של ההצהרות הללו על בסיס מידע רקע נוסף ומחקר ממוקד. עבור ספקים בעלי סיכון גבוה יותר נדרש מידע נוסף, וכן נערכות ביקורות באתרים שלהם. יעילות הביקורת גוברת, ונמנעת יתירות ביקורות, על ידי שיתוף פעולה עם 13 חברות נוספות, המבצעות את התהליך ב־Joint Audit Cooperation (JAC).

בשלב השלישי מסווגים הספקים ומוערכים בהתבסס על המידע המתקבל מהם ועל תוצאות הביקורת. לפי Deutsche Telekom, החברה מקיימת שיתוף פעולה הדוק עם הספקים שלה כדי לטפל בבעיות חריפות שזוהו.

בשלב הרביעי מבוצעת תוכנית פיתוח ונערכות סדנאות לספקים. במקרים של התעלמות משמעותית של ספק מדרישות החברה, מתחיל תהליך הסלמה – תהליך שבמסגרתו מערבים גורמים גבוהים יותר בקרב הספק ולעיתים ננקטות סנקציות חריפות יותר, וזאת בכדי לזרז את הטיפול ואת תהליך סגירת הפערים בהתאם לנוהלי Deutsche Telekom.

מסמך של Information Technology Infrastructure Library (ITIL) מציג מודל דו־ממדי לסיווג ספקים[4] – Risk and Impact מול Value and Importance. ככל שהערך של הממדים בקרב ספק מסוים הינו גבוה יותר, כך הספק משמעותי יותר. מודל זה מסווג את הספקים לארבעה סוגים:

- ספקי סחורה רגילה: ספקים המספקים מוצרים ושירותים בעלי ערך נמוך ו / או זמינים (למשל ספקי מחסניות נייר או מדפסת).
- ספקים תפעוליים: ספקים של מוצרים או שירותים תפעוליים. קשרים אלה ינוהלו בדרך כלל על ידי ניהול תפעולי זוטר והם יהיו כרוכים בביקורות בתדירות נמוכה

3 "Corporate Responsibility Report", *Deutsche Telekom*, 2017.

4 "ITIL Service Management", Version 3, Ch. 4.7.5.2, https://www.hci-itil.com/ITIL_v3/books/2_service_design/service_design_ch1.html.

אך קבועה של אנשי קשר (למשל, ספק שירותי אירוח אינטרנטי, המספק שטח אירוח לאתר אינטרנט בעל השפעה נמוכה).

- ספקים טקטיים: ספקים שיש עימם פעילות מסחרית משמעותית ואינטראקציה עיסקית. קשרים אלה ינוהלו בדרך כלל על ידי הנהלת הביניים והם יהיו כרוכים בביקורות וסקירות ביצועים קבועות ובתוכניות שיפור מתמשכות (למשל, ספק תחזוקת חומרה המספק פתרון של כשלי חומרת שרתים).
- ספקים אסטרטגיים: ספקים איתם משותף מידע אסטרטגי סודי. קשרים אלה יהיו בדרך כלל באחריות הרמה הניהולית הבכירה וכרוכים בביקורות שוטפות ותכופות (למשל, ספק שירות רשת, המספק שירות רשתות עולמי ותמיכה בהם).

מתודולוגיה המציגה מודל פירמידלי פשוט יותר לסיווג ספקים נמצאת בשימוש על ידי חברת United Utilities[5] – חברה לאספקת מים בצפון־מערב אנגליה, המספקת כ־1,700 מיליון ליטר מים מדי יום. מודל זה מחלק את הספקים לארבעה סוגים: שותף, אסטרטגי, מועדף ומאושר. ככל שהתלות של החברה בספק מורכבת יותר ועלות ערך הסחורה/השירותים גבוהים יותר, כך הספק מוגדר כמשמעותי יותר. המודל מאפשר להגדיר את דרישות החברה מהספק כנגד מדדי ביצוע של לקוחות, רגולציה/משפט, קיימות, יעילות, בטיחות וכדומה.

מתודולוגיה נוספת לסיווג ספקים מופיעה במודל של Amway – Europe Supplier Information Portal.[6] על פי מתודולוגיה זו, סוג היחסים שמתפתח בין ספק ללקוח תלוי בחשיבות האסטרטגית של המוצרים או השירותים המסופקים, ובכישורים, ביכולות ובביצועים של הספק. כל ספק נמדד על פי קריטריונים ומסווג בהתאם, על פי המודל. הדבר מבטיח שכל ספק יקיים פעילויות ממוקדות שתוכננו במיוחד כדי לפתח, לשפר או לייעל ביצועים תפעוליים. הקריטריונים שעל פיהם נמדד כל ספק כוללים מדדי ביצוע (הזמנה, מלאי, אספקה, שירות ובקרת איכות), מוצר/שירות (חדשנות, פיתוח, יתרון שיווקי, ערך כלכלי) ופיננסים (תלות, חלופות, סיכונים פיננסיים ותמחור). הערכת הקריטריונים הללו והתוצאות הנובעות ממנה מובילות לגיבוש תוכניות ספציפיות עם הספק כדי להשיג את רמות הביצועים התפעוליים הנדרשים לצרכים העיסקיים.

בישראל מתקיימות מספר פעילויות לשיפור ההתמודדות עם סיכוני סייבר בשרשרת האספקה. אחת מהן היא פעילות מערך הסייבר הלאומי לפיתוח מתודה להגנה על שרשרת האספקה. מתודה זו כוללת שאלון לספקים, שיטת ביקורת ובקרה והנגשתה באמצעות פורטל. הכוונה היא שהשימוש במתודה ובפורטל יתפתח

5 "Suppliers", *United Utilities,* https://www.unitedutilities.com/corporate/about-us/governance/suppliers.

6 "Supplier Segmentation", *Europe Supplier Information Portal*, http://supplier.amway.com/europeanportal/suppliersegmentation/SitePages/Home.aspx.

באמצעות כוחות השוק ולא יוטל כחובה על הספקים. לצד זאת מתקיימת פעילות במשרד האוצר – על ידי היחידה להסדרת סייבר ורציפות בשרשרת האספקה הפיננסית,[7] שייעודה הוא להבטיח את חוסן המערכת הפיננסית בפני סיכוני סייבר ורציפות בשרשרת האספקה, לשמור על יציבות המערכת ולעמוד ביעדי השירות לציבור ולממשלה. נכון למועד כתיבת המאמר, פעילות היחידה מול הספקים של המערכת הפיננסית הינה וולונטרית וללא עלות. הפעילות מול הספקים כוללת סקירת פעילותם, מיפוי והערכת סיכונים, מיפוי בקרות קיימות, הערכת הבקרות וגיבוש תוכנית להפחתת הסיכון. יצוין כי פעילות זו מול ספקי המערכת הפיננסית הינה חדשה יחסית, ונמצאת בשלבים מוקדמים שלה.

בנוסף לכך קיימות במספר תחומים במשק הישראלי גישות בעלות קשר אפשרי לנושא של מאמר זה, כמו קטגוריזציה המבוצעת ברמה הלאומית לספקים מענף משקי אחר (סיווג קבלני בניין) ותהליך תשתיתי המבוצע/מונחה ממקום אחד (היחידה הממלכתית לקביעת התאמה ביטחונית בשירות הביטחון הכללי) עבור מועסקים בגופים רבים. זאת ועוד, מערך הסייבר במשרד ראש הממשלה הקים בשלהי 2018 מערכת מידע לאומית,[8] שבאמצעותה יוכל כל ארגון במשק לבדוק את רמת ההגנה שלו בסייבר ואת כשירותו בתחומי אבטחת מידע והגנת הסייבר, ולפי הנתונים שיאסוף – לקבל המלצות כיצד להיערך, לשנות ולשפר. המודול הראשון במערכת, ששמה יוב"ל (יעדים ובקרות לארגון), נועד לטיפול בשרשרת האספקה למשק. המערכת מבוססת על תורת ההגנה לארגונים במשק הישראלי, אותה פרסם מערך הסייבר הלאומי. האתגר שעמד לנגד אנשי המערך בבואם לאפיין את המערכת היה הצורך לגבש מתודולוגיה להגנה על שרשרת האספקה במשק. מטרת היוזמה הייתה העלאת רמת האבטחה במשק הישראלי, לצד התייעלות כלכלית. בעזרת המערכת נבנה מערך אחיד ומסודר של שאלות ובקרות, כאשר המטרה היא ליצור אמון בין ארגונים ובין ספקים במשק.

תקן בין־לאומי נפוץ בתחום אבטחת המידע הינו ISO 27001[9] (שם התקן הישראלי שאומץ הינו "ת"י ISO 27001"). תקן זה עוסק במיסוד מערכת לניהול אבטחת מידע ארגונית ובתהליך השוטף הכרוך בהקמת המערכת ובשיפורה השיטתי. פרק 15 בתקן עוסק בקשרי ספקים. הבקרות בהקשר זה מפורטות בתקן ISO 27002.[10] על פי תקן זה, הארגון נדרש להגדיר מדיניות עבור הספקים,

---

7 "היחידה להסדרת סייבר ורציפות בשרשרת האספקה הפיננסית", *משרד האוצר*, http://mof.gov.il/Units/CyberEmergenciesSafetyDraft/Pages/CyberSeriesUnit.aspx.

8 "מערך הסייבר הקים מערכת להגנה על שרשרת האספקה במשק", **אנשים ומחשבים**, ינואר 2019, https://www.pc.co.il/news/282242 /.

9 "Information Technology – Security Techniques – Information Security, Management Systems – Requirements", *ISO/IEC 27001*, 2013.

10 "Code of practice for information security controls", *ISO/IEC 27002*, 2013.

שתהיה מוסכמת עליהם וממוסמכת. בנוסף, המדיניות צריכה להתמקד בתהליכים הרלוונטיים המתרחשים הן באתרי הארגון והן באתרי הספק, ובכלל זה: זיהוי סוגי הספקים שהארגון התיר להם גישה למידע; הגדרת מחזור חיים לניהול קשרי ספקים; הגדרת סוגי המידע המותר לגישה לפי סוגי הספקים; תהליכי ניטור ובקרה על הגישה; הגדרת דרישות האבטחה המינימליות לפי סוגי המידע וסוגי הגישה למידע כדי שיהוו בסיס להסכמים המבוצעים מול כל ספק רלוונטי; הגדרת אופן הטיפול באירועי אבטחה ובתקלות הקשורות לספק; הגדרת האחריות של כל צד; העלאת מודעות ותרגול עובדים. כמו כן, נדרש להגדיר בהסכם כתוב את דרישות האבטחה לכל ספק שיש לו יכולת לגשת/לעבד/לאחסן/ליצור תקשורת, או לספק מידע או רכיבי טכנולוגיות מידע עבור הארגון. בנוסף, ההסכמים עם הספק צריכים לכלול דרישות אבטחה הנובעות מסיכונים הנוצרים משרשרת האספקה של מוצרים או שירותים. התקן גם מדגיש את הצורך לנהל, לנטר ולהכניס שינויים בכל הקשור לקשרי ספקים ולשרשרת האספקה.

תקן רלוונטי נוסף הינו NIST 800-161[11] – גם הוא תקן מקיף ומפורט, שמטרתו היא לספק מדריך לסוכנויות הפדרליות בארצות הברית בהיבטי זיהוי, הערכה, בחירה והטמעה של תהליכי ניהול סיכונים ובקרות על ניהול סיכוני שרשרת האספקה של טכנולוגיות המידע. התהליכים והבקרות המפורסמים בתקן זה ניתנים לשינוי או להרחבה בגין דרישות רגולטוריות, מדיניות ארגונית, הנחיות וכדומה. התקן מציין כי על הארגונים לפתח אסטרטגיות להפחתת סיכוני שרשרת האספקה של טכנולוגיות המידע, המותאמות ספציפית אליהם והמושפעות ממשימות/צרכים עיסקיים, איומים וסביבות תפעוליות. התקן מדגיש את מורכבות שרשרת האספקה של טכנולוגיית המידע ואת העובדה שלספקים יש ספקים נוספים, ולכן יש קושי לארגון לראות, להבין ולבקר את המצב, קושי שגובר ככל שהספק אינו ספק ישיר שלו. התקן גם מציין כי הטיפול בסיכוני שרשרת האספקה בטכנולוגיית המידע צריך להיות מוטמע בתוך תהליכי ניהול הסיכונים הכלל־ארגוני הרחב. הבקרות המפורטות בתקן מתייחסות לנושאים הבאים: בקרת גישה; מוכנות ותרגול; חיווי ואחריות; הרשאות; ניהול תצורה; המשכיות; זיהוי ואימות; תגובה לאירועים; תחזוקה; הגנה על המדיה; אבטחה פיזית; תכנון; ניהול יישומים; מהימנות עובדים; בקרת שינויים; הערכת סיכונים; רכישת מערכות ושירותים; הגנה על מערכות ותקשורת; שלמות מערכות ומידע.

תקן General Data Protection Regulation (GDPR),[12] שנקבע על ידי הפרלמנט האירופי, מועצת האיחוד האירופי והנציבות האירופית, חל על מדינות האיחוד

11 "Supply Chain Risk Management Practices for Federal Information Systems and Organizations", *NIST Special Publication 800-161*, April 2015.

12 "GDPR – General Data Protection Regulation", *The European Parliament*, 2016.

האירופי בכל הנוגע לאיסוף, שמירה והעברה של נתונים אישיים של אנשים פרטיים, וקובע כללים אחידים לשמירה על הפרטיות. התקן התקבל ב־27 באפריל 2016 והוא בר אכיפה החל מ־28 במאי 2018. הוא מחליף את הדירקטיבה האירופית בנוגע להגנה על נתונים (הנחיה EC/95/46) שנקבעה בשנת 1995. התקן חל על כל הארגונים המעבדים נתונים של נושאי מידע בטריטוריה של האיחוד האירופי, גם אם אינם פועלים בטריטוריה של האיחוד. התקן מטיל איסורים ומגבלות על העברת מידע אל מחוץ לשטח האיחוד האירופי בשל החשש להפרות שעלולות להתרחש באזורים בעולם שבהם הפרטיות אינה מוגנת כראוי. אחד העקרונות של התקן הוא אחריותיות (Accountability). במקרים של ארגונים המשתמשים בספקים כמיקור חוץ לעיבוד נתונים אישיים (לדוגמה, הפקת תלושי שכר), עליהם לוודא כי נעשו טיפול אבטחתי נאות והבטחת תאימות לדרישות לאורך כל שרשרת האספקה שלהם, לרבות אצל ספקיהם.

הוראת בנק ישראל־הפיקוח על הבנקים[13] דורשת מהתאגיד הבנקאי לקבוע את הפעולות הנחוצות כדי לוודא שהגורמים החיצוניים נוקטים את האמצעים הנדרשים להפחתת חשיפתו של התאגיד הבנקאי לסיכוני סייבר. ההוראה גם עוסקת באחריות התאגיד הבנקאי לקיום תצורת עבודה מאובטחת מול הספקים החיצוניים, ואת חובותיו לניהול סיכוני סייבר הולמים בפעילותם של ספקים אלה "בחצרותיהם, בחצרי התאגיד הבנקאי" ובממשקים שלהם עם התאגיד. ההוראה מתייחסת לצורך במיפוי וזיהוי "ספקים מהותיים",[14] במתן אפשרות בידי התאגיד הבנקאי לדרוש מהספק לעמוד בהנחיות האבטחה ובשמירת יכולת אכיפה ובקרה של התאגיד הבנקאי מול הספק.

משרד האוצר־אגף שוק ההון, ביטוח וחיסכון פרסם חוזר[15] החל על גופים המנהלים כספים של הציבור, כגון כספי פנסיה וקרנות נאמנות, לרבות חברות ביטוח ובתי השקעות. סעיף ה' בחוזר מתייחס לנושא מיקור חוץ, מפרט את דרישות הגנת הסייבר בהסכמי מיקור חוץ ודורש שהגוף יגדיר נוהל שיפרט את דרישות הגנת הסייבר מול סיכוני מיקור חוץ וביחס לאבטחת שרשרת האספקה. בנוסף לכך, נדרש שייאסר על נותן השירות להעביר לצד שלישי מידע שקיבל במסגרת ההתקשרות, או להשתמש במידע שאליו הוא נחשף אגב ביצוע ההתקשרות לכל מטרה אחרת שלא קשורה לביצוע ההתקשרות. עוד נקבע בחוזר שכאשר קיים

13 "ניהול סיכוני סייבר בשרשרת האספקה", *בנק ישראל*, 2018.

14 ההוראה מגדירה את "הספקים המהותיים" כגורמי חוץ הנכללים בשרשרת האספקה של התאגיד הבנקאי (דוגמת חברות התומכות במתן שירותי מסחר בשוק ההון), שהם מהותיים לפעילותו ו/או חושפים אותו לסיכוני סייבר ואבטחת מידע פוטנציאליים גבוהים, שבהתממשותם ניתן לתקוף את התאגיד הבנקאי או לפגוע בפעילותו. הכוונה היא לגורמי חוץ הנותנים שירותים לתאגיד בתחומים הקשורים לטכנולוגיית המידע בלבד.

15 "ניהול סיכוני סייבר בגופים מוסדיים", *משרד האוצר*, אוגוסט 2016.

צורך בהעברת נתונים, יבוצע תהליך של גישה מבוקרת לנתונים פרטניים ולא שכפול של כלל בסיס הנתונים.

תקנות הגנת הפרטיות (אבטחת מידע) של הרשות להגנת הפרטיות (לשעבר רמו"ט), שנכנסו לתוקף במאי 2018,[16] מתבססות על ההנחה שמתן גישה לגורם חיצוני יוצר סיכונים מיוחדים, ולכן מצריך בחינת סיכוני אבטחת המידע האפשריים הכרוכים בהתקשרות עימו. התקנות קובעות שיש לבחון, לפני ביצוע ההתקשרות, סיכוני אבטחת מידע הכרוכים בה, ואם הם גבוהים מדי בהתחשב ברגישות המידע – יש להימנע ממיקור החוץ לחלוטין. כמו כן קובעות התקנות שיֵש להגדיר מהו המידע שהגורם החיצוני רשאי לעבד ולאלו מטרות; לאלו מערכות הוא רשאי לגשת; מהו סוג העיבוד שאותו הוא רשאי לבצע; מהו משך ההתקשרות; מה יהיה אופן השבת המידע לידי הבעלים בסיום ההתקשרות; אופן יישום ההוראות של תקנות אבטחת המידע; חובת הגורם החיצוני להחתים את בעלי ההרשאות שלו על התחייבות לשמור על סודיות המידע.

כפי שעולה מהנאמר לעיל, קיים מגוון רחב של תקינות ורגולציות ברחבי העולם המיועדות לניהול סיכונים כלליים בשרשרת האספקה, דבר שמלמד כי קיימת מודעות גלובלית לנושא זה. במסגרת זו קיימת מוּדעוּת גם לאיומי הסייבר שמקורם בשרשרת האספקה. איומים אלה מציבים מספר אתגרים המחייבים התייחסות ייחודית.

איומי סייבר וסיכוני שרשרת האספקה

על פי ה־CERT הבריטי, ניתן להבחין בארבעה סוגי איומים על שרשרת האספקה, המבוססים על אירועי אמת:[17] האיום הראשון הינו תקיפת המערכת דרך ספק צד שלישי. באירוע האמת הספציפי התוקף תקף תוכנת מערכת בקרה תעשייתית (Industrial Control System – ICT) המותקנת בארגון באמצעות ספק תוכנה צד שלישי; האיום השני הינו תקיפת אתרי אינטרנט עיסקיים באמצעות עיצוב ובניית אתרים. באירוע האמת הספציפי התוקף תקף אתרי אינטרנט פיננסיים באמצעות סקריפטים שהועברו מחברות דיגיטציה ועיצוב; האיום השלישי הינו תקיפת חברות צד שלישי העוסקות באחסון נתוני חברות. הכוונה הינה למצב שבו חברות רבות מאחסנות את המידע שלהן, לעיתים אף מידע רגיש, אצל חברות צד שלישי, המהוות גם הן יעד לתקיפה ישירה; האיום הרביעי הינו תקיפת Watering hole. הכוונה היא לשתילת קוד עוין באתרים הנמצאים בשימוש נרחב על ידי מושאי

16 "תקנות הגנת הפרטיות (אבטחת מידע) – תקנה 15 – מיקור חוץ", *כנסת ישראל*, מאי 2017.

17 "Cyber-security Risks in the Supply Chain", *Cert UK*, 2015.

התקיפה, כך שהגישה אל אותם אתרים תגרום לתקיפת מערכות המשתמשים שהם מושאי התקיפה.

דוגמאות לאיומים בהקשר האמור מופיעות גם בתקן ISO 27036-1:[18] גישה פיזית של ספק לאתרי הלקוח; גישה למידע או למערכות מידע של הלקוח על ידי עובדי הספק באתרי הלקוח; גישה מרחוק של הספק למידע או למערכות מידע של הלקוח; עיבוד מידע של הלקוח על ידי הספק מחוץ לאתרי הלקוח; הפעלת יישומים של הלקוח על תשתיות הספק; אירוח (Hosting) של ציוד הלקוח באתרי הספק ואחסון נתוני הלקוח (לרבות גיבוי) אצל הספק.

בדוח של חברת מודיעין סייבר, הסוקר תקיפות סייבר משמעותיות שאירעו בשנים 2016–2018 בעולם ובישראל,[19] מצוין כי ארגונים במגזר הפיננסי (בנקים) הינם מטרה מרכזית לתוקפים מיומנים (הן גורמי פשיעה והן תוקפים מדינתיים), וכי מערכות ליבה בנקאיות, כמו Swift ומערכות ATM, הפכו בשנים האחרונות ליעד מועדף לתוקפי סייבר. כמו כן מצוין בדוח כי בעשור האחרון בנו חברות וארגונים מערכי הגנה קדמיים מול שדרת האינטרנט והשקיעו פחות בהגנה על הקישורים שלהם מול ספקים. כך הפכה תקיפת סייבר שמקורה באחת מהחוליות בשרשרת האספקה לשיטה יעילה להשגת אחיזה וחדירה לארגונים אסטרטגיים: התוקפים מנצלים את היכולת הקלה יחסית לחדור לחברות ולארגונים קטנים בעלי מערך הגנת סייבר מוחלש, כדי לחדור דרכם לארגוני יעד בעלי חשיבות קריטית. תוקפים גם מנצלים את העובדה שלחֵלק מספקי המשנה של ארגונים קריטיים יש גישה ישירה או קלה יותר אל הארגון, כדי לבצע חדירה דרכם. התקיפה באמצעות שרשרת האספקה הופכת למתוחכמת יותר, וכוללת שימוש בעדכוני תוכנה לגיטימיים כדי להפיץ נוזקה. מכיוון שארגונים אינם מסוגלים להתמודד עם בדיקה של עדכוני תוכנה, חלה עלייה משמעותית ברמת הסיכון של פגיעה במערכות הליבה של ארגונים ומדינות.

על פי הדוח של חברת מודיעין הסייבר, ניתן להפיק שלוש תובנות עיקריות מהמצב הקיים בכל הנוגע להיבטי ההתמודדות הארגונית עם האיומים:

- **בניית מודל הגנה חדש** – המודל המסורתי, שעיקרו יישום אמצעי אבטחה מוגברים ב"גבולות" הארגון החיצוניים, תוך השארת ליבת הארגון בלתי מוגנת, אינו מתאים יותר. תפיסה זו הביאה בשנים האחרונות לטיפול חסר באבטחת המערכות הפנים־ארגוניות. המצב הנוכחי הוא שארגונים רבים משקיעים מאמצים רבים בהקשחת מעטפת ההגנה שלהם, אך האבטחה הפנים־ארגונית אינה זוכה

18 "Information Technology – Security Techniques – Information Security for Supplier Relationships", *ISO 27036*.

19 "דו"ח אירועי סייבר 2016–2018 – ניצול שרשרת אספקה SWIFT", *CLEARSKY*, מארס 2018.

לתקצוב והשקעה מספקים. חוסר האיזון בהשקעה מביא לכך שכאשר תוקף מצליח לחדור לתוך הארגון, ביכולתו להתפשט בתוכו ולפעול בו בקלות רבה.

- **הקשחה ועיבוי מנגנוני ההגנה בין הארגונים ובין ספקי המשנה שלהם** – קיים קושי רב בהגנה על הקשר בין ארגונים וחברות ובין ספקי משנה המספקים להם שירותים ומידע, קל וחומר כשעוסקים בהגנה על מידע מפני חברות המספקות שירותי מחשוב מבוססי ענן. חלק מספקי המידע במגזר הבנקאי הם גופים בין־לאומיים (לדוגמה, חברת "בלומברג" וחברת "רויטרס"). ברי כי היכולת להשפיע על מערכי הגנת המידע שלהם היא פחותה יחסית. יכולת ההשפעה והשליטה של בנקים ורגולטורים על מערך האבטחה של ספקים בישראל היא גבוהה יותר, אך מחייבת קביעת סטנדרטים ומערכי הגנה ברורים למערכי אבטחת המידע הנדרשים מספקי משנה המתחברים באופן ישיר למערכות הליבה הבנקאיות. במקביל, יש לחזק את מערכי ההגנה ולהקטין ככל האפשר חשיפה לספקי משנה במערכות הפנימיות של הבנקים ושל הגופים הפיננסיים.
- **פריסת מערך הגנה אחורי הדומה במאפייניו למערך ההגנה הקדמי** – מומלץ לבנות מערך ניטור והגנה מול ספקי המשנה, הזהה במאפייניו למערך ההגנה הקדמי של החברה, כולל הקמת מרחב DMZ, מערך הזדהות חזק הכולל הזדהות כפולה, מערך סינון מידע, מערך "ארגזי חול" לבחינת תוצאות של התקנת עדכוני תוכנה, ומערך ניטור הכולל שמירת הנתונים לפרק זמן ארוך וניטור רציף של הַקשר מול ספקי המשנה. מערך הגנה זה אמור להיפרס גם מול החברות הבנות של החברה. העבודה מול החברות הבנות, שלהן מערכי הגנה נפרדים ומערכות תוכנה נפרדות, מסכנת את החברה בדיוק כמו עבודה מול ספק משנה.

מסמך של מערך הסייבר הלאומי בנושא "סיכונים במיקור חוץ ושרשרת אספקה"[20] מפרט את הסיכונים הבאים כסיכונים ייחודיים לשרשרת האספקה: הכנסה של תוכנה או חומרה הנגועה בנוזקה; ביצוע פעולה זדונית על ידי גורם תחזוקה; ביצוע פעולה זדונית באמצעות ערוץ התחזוקה מרחוק. המסמך מציע אמצעים למזעור הסיכון, בכללם: שילוב הסיכון בניהול הסיכונים הארגוני; פיקוח על גורמי התחזוקה – למשל, באמצעות ניטור פעולתם ברשת, ליווי צמוד שלהם בעת שהותם בארגון, הצמדת תג זיהוי לגורם הנכנס, ניטור ערוץ התחזוקה מרחוק וניתוקו בזמנים שאין בו צורך; הסתרת יעד הקצה הספציפי במסגרת רכש עבור ארגונים גדולים – למשל, כאשר רוכשים עבור ארגון גדול מאוד, שרק חלקים ממנו הינם רגישים, ניתן לא לציין בהזמנה למי בדיוק בארגון מיועד הרכש.

מסמך של *SANS Institute* מתייחס להיערכות הנדרשת בארגון נוכח סיכוני הסייבר הנוצרים משרשרת האספקה.[21] המסמך מציע לארגונים לבנות תוכנית

20 "סיכונים במיקור חוץ ושרשרת אספקה", *מערך הסייבר הלאומי*, 18 במאי 2017.

21 "Combatting Cyber Risks in the Supply Chain", *SANS*, 2015.

לניהול ספקים, המבוססת על ארבעה מרכיבים: זיהוי והגדרת הספקים החשובים; הגדרה מדויקת של ההסכמים עבור כל ספק; קביעת הנחיות ובקרות ויישומן; אינטגרציה ארגונית. כמו כן מציע המסמך לארגונים לפעול על פי Best Practices (בהיבטי אנשים, תהליכים וטכנולוגיה) כדי להקטין את חשיפתם לסיכוני שרשרת האספקה. לבסוף מסכם המסמך את המרכיבים העיקריים של התוכנית לאבטחת שרשרת האספקה על פי מרכיבים בסיסיים ומקיפים, בחתך של כל אחד משלושת המרכיבים, כמפורט בטבלה הבאה:

המרכיב	בסיסי	מקיף
אנשים	בדיקות רקע	דרישות אבטחה המופיעות בחוזים
תהליכים	סקרים בסיסיים וסקרי בקרות וסיכונים אצל הספקים	יישום תוכנית מלאה לניהול ספקים
טכנולוגיה	סגמנטציה ברשתות וניטור	Code Review ובדיקת פגיעויות אצל גורמי צד שלישי, ניטור מעמיק, ניתוח איומי אבטחה והתבססות על מודיעין

האיומים על הארגון באמצעות תקיפת שרשרת האספקה שלו יכולים להתבצע באמצעות ערוצי תקיפה מגוונים מאוד, כגון: חדירה למערכות של ספק בעל רמת הגנה נמוכה יחסית (אך בעל גישה למערכות הארגון), ודרכו ביצוע חדירה למערכות הארגון, שימוש בעדכוני תוכנה לגיטימיים להפצת נוזקה וכדומה. אין המדובר באיומים תיאורטיים לארגונים, אלא באיומים המתבססים על מספר רב של אירועים שאירעו בפועל בארץ ובעולם, שמהותם פגיעה בארגונים תוך ניצול שרשרת האספקה שלהם. מורכבות האיום, המגוון הרחב של התרחישים האפשריים והתעצמות התוקפים מחייבים את הארגונים לנקוט צעדים הגנתיים משמעותיים כדי להתמודד עם האתגר ולצמצם את הסיכונים.

לסיכום, הסקירה שהובאה לעיל מלמדת כי קיימת התייחסות רבה לנושא איומי הסייבר בשרשרת האספקה. אולם התייחסות זו אינה יעילה, שכן כל גוף נדרש לקיים את ההנחיות וההמלצות בעצמו ובאופן מבוזר, ובנוסף לכך, כל ספק נדרש לענות על דרישות לקוחותיו בנפרד ולהשקיע משאבים רבים ביישום הדרישות השונות, שמִטָבע הדברים אינן אחידות.

המודל המוצע

אחד המרכיבים הקריטיים בניהול סיכוני שרשרת האספקה הוא היכולת לסקור את סיכוני הסייבר בקֶרב הספקים ולבנות תוכנית עבודה שתאפשר לסגור פערים באמצעות בקרות מתאימות. ככלל, מאמר זה מבקש להתמקד בגיבוש תהליך רוחבי מגזרי שיאפשר לספקים לקבל הסמכה מגוף בוחן מרכזי. המאמר מתבסס על ההנחה שארגונים המשתייכים לאותו מגזר עיסקי חולקים חלק ניכר מספקיהם (ספקים

משותפים). כך, לדוגמה, מרבית הבנקים בישראל נעזרים באותו ספק הדפסות, אלא שהמצב כיום הוא שכל בנק מבצע סקר עבור אותו ספק הדפסות בנפרד.

המודל המוצע הוא שתהליכי ההסמכה ימומנו על ידי כלל הארגונים הנעזרים בספק, ובכך יתאפשר איגום משאבים והשקעת משאבים גדולים יותר באופן יחסי בכל תהליך ההסמכה. ההסמכה תבוצע על פי מדרגים שונים ועל פי מאפייני הספק ודרישות הארגונים החברים במגזר. באופן זה, הארגונים יישענו על עבודת הגוף הבוחן, ולספקים ייחסכו ביקורות חוזרות ונשנות בכל פעם על ידי גוף אחר. המודל המוצע יכול להוות בסיס בלבד; במידת הצורך, הארגונים השונים יוכלו להעמיק את הדרישות מספקיהם המהותיים בשרשרת האספקה, לדוגמה: הצבת דרישות מחמירות ואף דרישות להתקנה של מערכות ניטור נוספות אצל הספק.

את פעילות סקירת הסיכונים, הנדרשת לביצוע מול הספקים בהיבטי ההתמודדות עם סיכוני הסייבר בשרשרת האספקה, ניתן לבצע באמצעות שתי חלופות תפעוליות עיקריות:

- **ניהול עצמי על ידי כל ארגון במגזר**. זהו למעשה המצב הנוהג כיום, בו כל ארגון פועל באופן עצמאי מול ספקים בשרשרת האספקה שלו. כל ארגון גם קובע את מערכת הדרישות שלו מכל ספק או קבוצת ספקים.
- **ניהול מגזרי מרכזי (עבור כלל/רוב הארגונים במגזר)**. לשם מימוש הדבר, יהיה צורך לבחון הקמת גוף מגזרי מרכזי שיהיה בבעלות משותפת של הגופים הפעילים במגזר. מטרתו של גוף זה תהיה, רובה ככולה, טיפול וניהול סקרי סייבר ומעקב ביצוע בקרב ספקי המגזר. גוף זה יהיה אחראי לנהל את הסוקרים (בין אם בביצוע סקרים באופן ישיר על ידי סוקרים העובדים בגוף ובין אם באמצעות סוקרים חיצוניים), להכתיב את מערכת הדרישות מהסקרים, לנטר ולעקוב אחר יישום תוכניות לתיקון הפערים שיעלו מהסקרים, ולעדכן את מתודולוגיות הבדיקה ואת הכלים שבשימוש על פי צורכי השעה והתפתחות התחום. בנוסף לכך יצטרך הגוף לדון בשאלת הבקרה על ספקים מחו"ל – כיצד ליישם את הבדיקות ואת תהליכי הבקרה גם עליהם. דוגמה לגוף כזה ניתן לראות בחברת מס"ב/שב"א, שהוקמה על ידי הבנקים הגדולים בישראל ומספקת שירותים לכלל המגזר הבנקאי.

מערכת הדרישות תוכל להתבסס על תקינה מקובלת או על הצעת מערך הסייבר הלאומי בישראל לסיווג ספקים. בחינת שתי החלופות נוגעת למספר היבטים עיקריים נוספים:

- **שיפור ביטחון הסייבר המגזרי** – ההיבט הראשון בניתוח נוגע לשאלה: איזו חלופה תגדיל את רמת ביטחון הסייבר והיציבות של המגזר הספציפי? לאור הניתוח שערכנו, התשובה לשאלה זו ברורה. לניהול מרכזי של סקירת ספקים יש יתרונות במגוון היבטים: הקמת גוף מקצועי מתמחה תאפשר לו לפַתח ידע באופן שיטתי ולשפר ולשכלל את יכולותיו עבור כלל המגזר; סקירת ספקים

אחודה תאפשר קביעה של ספי ביטחון סייבר נדרש עבור כלל המגזר, תוך נרמול הדרישות מספקים בשרשרת האספקה, ובכך תסייע משמעותית ליציבות המגזר בהקשר של שרשרת האספקה; הגדלת עוצמת הדרישות של הארגונים במגזר מהספקים תיצור יכולת טובה יותר לכפות מימוש בקרות משופרות, מאחר ודרישות אלו יהיו תוצר של גוף מרכזי; הקטנה משמעותית של העומס על הספקים, המתמודדים כיום עם סקירה ודרישות נפרדות של ארגונים שונים במגזר; ולבסוף, יכולת איגום המשאבים תאפשר הגדלה משמעותית באיכות ובעומק הסקירה, וכתוצאה מכך – ברמת ניהול סיכוני הספקים.

- **ההיבט הכלכלי** – רכיב נוסף אותו ראוי לבחון נוגע להיבטים הכלכליים, להם משמעות לכל מגזר בנפרד. בחינת היבט זה מראה שהקמת יכולת סקירה מרוכזת תוכל להוזיל את עלות המאמץ בכל גוף, ולעומת זאת תגדיל את האפקטיביות של הסקירה לאור ההתמקצעות של הגוף הסוקר במגזר האמור.
- **הגבלים עיסקיים** – היבט נוסף המחייב בחינה נוגע לשאלת ההגבלים העיסקיים. בהקשר זה יש לבחון באיזו מידה פעולה משותפת של הארגונים במגזר למול ספקים בשרשרת האספקה תיצור חריגה מתקנות ההגבלים העיסקיים. בניתוח שערכנו התברר שהקמת גוף סוקר מרכזי אינה מהווה פגיעה בתקנות ההגבלים העיסקיים, וזאת לאור ההבנה שתקנות אלו אמורות לחול על היבטים של תחרות עיסקית, ואילו הקמה של גוף סקירה מרכזי אינה נוגעת במרכיב זה וכל עניינה הוא שיפור רמת הביטחון והיציבות של המגזר הספציפי. בנוסף, בתהליך הסקירה ניתן יהיה לוודא שמידע רגיש של הארגונים אינו משותף לגורמים אחרים – דבר המתרחש כבר כיום, למשל במרכז הסייבר הפיננסי בבאר שבע, כמו גם בארגונים של המערכת הפיננסית בעולם, דוגמת FFIEC ואחרים. ברור שבתהליך הקמתו של הגוף המרכזי נדרש יהיה להסדיר את מגוון המגבלות שיחולו על תהליך הסקירה. להבנתנו, ניתן יהיה ליצור הסְדרה באופן שייתן מענה לדרישות הרגולטורים השונים.
- **פתיחה של ספקים חדשים** – כבר כיום מתמודדים ארגונים שונים עם תהליכים ארוכים הכרוכים בפתיחה של ספקים חדשים במערכת. תהליכים אלה נמשכים חודשים ארוכים מאוד. הפעלה של גוף מרכזי תוכל לאפשר קיצור התהליך ואף ליצור מצב שבו גופים יוכלו לבקש סקירה והסמכה מראש.

מכלל הנאמר לעיל ניתן לראות שהקמת גוף מרכזי תשפר מהותית את רמת ביטחון הסייבר המגזרי ותאפשר פיתוח ידע מתמיד. זאת ועוד, ניהול מרכזי יחזק את השפעתו ועוצמתו של הגוף הסוקר כלפי הספקים (שכן הוא ייצג את כל/רוב הגופים במגזר ולא רק ארגון מסוים), יאפשר התמקצעות טובה של הצוות (גוף מתמחה ברמה המגזרית), יקטין תקורות (תקורות ניהול, תקורות פיזיות וכדומה) עבור כל ארגון ויביא לחיסכון משמעותי של המשאבים הנדרשים בסקירת גורמים

בשרשרת האספקה. יודגש כי האחריות למתקפת סייבר כתוצאה מכשל בשרשרת האספקה תיוותר גם אז בידי הגוף המפעיל את הספק, שכן מטרת המודל המוצע הינה אך ורק לייעל ולשפר את התהליך ואת העלויות הנלוות אליו.

סיכום והמלצות

מכיוון שמבחינה כלכלית ישנה כדאיות מובהקת לנהל סקירות מרכזיות של סיכוני סייבר בשרשרת האספקה, מומלץ שניהול הפעילות יהיה מרכזי. כך גם תגדל השפעתה של הפעילות מול הספקים, מכיוון שהגוף הסוקר ייצג עבורם את דרישות כלל הארגונים החברים במגזר ולא רק דרישות של גוף מסוים. יודגש כי ארגון מסוים יוכל להוסיף דרישות ספציפיות מספק מסוים, במידת הצורך. מוצע כי מנגנון התמחור בין הארגונים החברים במגזר, לצורך הקמתו ותפעולו של הגוף המרכזי, יבוצע באופן דיפרנציאלי, שיבטא את היקף הפעילות של כל ארגון במיזם.

המודל המוצע טומן בחובו גם סיכונים, אותם יהיה צורך לבחון באופן מקיף ולנהל בהתאמה. סיכונים אלה כוללים, בין היתר, פגיעה אפשרית בשוק החברות המספקות סקרי סייבר (ייתכן שחברות יחליטו להפסיק לספק שירותים אלה, שכן יידרשו פחות חברות לאחר בחירת "הגוף הבוחן" בכל מגזר), דבר שיפחית את התחרות בענף; כאשר כל תהליך הסקירה מבוצע על ידי גוף אחד, קיים סיכון שלא כל הליקויים יתגלו. זאת, לעומת מצב שבו קיימים סוקרים שונים, המהווים "עין" נוספת ומגלים לעיתים ליקויים שאינם מתגלים על ידי סוקר מרכזי אחד; סיכון נוסף נוגע לאבטחת רמת המוּגנוּת של הגוף המנהל ולחדירה של גורם עוין לגוף הבוחן, חדירה שעלולה במקרה זה לסכן את כל המגזר; לבסוף, קיים סיכון של ניגוד אינטרסים, קרי, במצב שהחברה הבודקת היא גם מתקנת הליקויים. סיכון זה רלוונטי כמובן רק למקרה שבו הגוף המרכזי שיוקם יבחר להפעיל ספקים חיצוניים לביצוע הסקרים מטעמו.

באשר לישראל, מומלץ שמערך הסייבר הלאומי יקיים תהליך עומק של בחינת המודל המוצע. ראוי שראשית התהליך תהיה במיפוי המגזרים הרלוונטיים למודל (קרי, מגזרים שלגביהם מתקיימת ההנחה כי חלק משמעותי מספקיהם הם ספקים משותפים). לאחר מכן כדאי לקיים תהליך של בחינת כדאיות, בדומה למגזר הפיננסי, כפי שהוצג במאמר זה. בשלב הבא אנו ממליצים להגדיר עבור כל מגזר את מערכת הדרישות הרלוונטיות מהספקים השונים ואת תהליכי סקירת הסיכונים.