ניהול סיכוני סייבר לאומי במגזר הפיננסי: צמצום איומים בשרשרת האספקה

גבי סיבוני

זיו סולומון והדס קליין

העבודה בוצעה לטובת המגזר הפיננסי בסיוע בנק הפועלים

בנק הפועלים

INSS
המכון למחקרי ביטחון לאומי
THE INSTITUTE FOR NATIONAL SECURITY STUDIES
אוניברסיטת תל אביב
TEL AVIV UNIVERSITY

ניהול סיכוני סייבר לאומי במגזר הפיננסי
צמצום איומים בשרשרת האספקה

גבי סיבוני
זיו סולומון והדס קליין

המכון למחקרי ביטחון לאומי, המשלב בתוכו את מרכז יפה למחקרים אסטרטגיים, הוקם בשנת 2006.

למכון שתי מטרות מוצהרות: הראשונה היא לערוך מחקרים בסיסיים בנושאי הביטחון הלאומי של ישראל, המזרח התיכון והמערכת הבינלאומית, וזאת על פי אמות המידה האקדמיות הגבוהות ביותר, והשנייה – לתרום לדיון הציבורי ולעבודת הממשל בנושאים שנמצאים, או ראוי שיימצאו, בראש סדר היום הביטחוני של ישראל.

קהל המטרה של המכון הוא דרג מקבלי ההחלטות, מערכת הביטחון, מעצבי דעת הקהל בישראל, הקהילה האקדמית העוסקת בתחומי הביטחון בישראל ובעולם, והציבור המתעניין באשר הוא.

המכון מפרסם מחקרים שהוא מצא כראויים לתשומת הלב הציבורית, תוך שמירה על מדיניות נוקשה של אי משוא פנים. הדעות המובעות בפרסומים הן של המחברים בלבד, ואינן משקפות בהכרח את עמדות המכון, נאמניו או האישים והגופים התומכים בו.

ניהול סיכוני סייבר לאומי במגזר הפיננסי:
צמצום איומים בשרשרת האספקה

גבי סיבוני
זיו סולומון והדס קליין

דצמבר 2018

העבודה בוצעה לטובת המגזר הפיננסי בסיוע בנק הפועלים

בנק הפועלים

INSS
המכון למחקרי ביטחון לאומי
THE INSTITUTE FOR NATIONAL SECURITY STUDIES
TEL AVIV UNIVERSITY אוניברסיטת תל אביב

המכון למחקרי ביטחון לאומי (חברה לתועלת הציבור – חל"ץ)

חיים לבנון 40, ת.ד. 39950
רמת אביב, תל אביב 6997556

דוא"ל: info@inss.org.il
אתר המכון: http://www.inss.org.il/he

עיצוב גרפי: מיכל סמו־קובץ ויעל ביבר, המשרד לעיצוב גרפי, אוניברסיטת תל אביב
עיצוב העטיפה: מיכל סמו קובץ

תמונת השער: Gettyimages

דפוס: אליניר, פתח תקווה

תודות

ראשית אנו מבקשים להודות ליו"ר בנק הפועלים, מר עודד ערן על החלטתו לתמוך בביצוע עבודה זו לטובת המגזר הפיננסי בישראל. כמו כן אנו מבקשים להודות לעמוס ידלין ואורלי הירדני על הקצאת המשאבים שנדרשו למימוש המשימה.

תודות רבות גם לחברי פורום הבנקים במכון למחקרי בטחון לאומי אשר תרמו מזמנם והשתתפו במפגשי החשיבה ובהם: אלי פטל ממערך הסייבר, רחל יעקבי וגיל פולק מבנק ישראל, אליק עציון ושמעון ברדה מבנק הפועלים, שוקי פלג וגיל חתם מהבנק הבינלאומי, לוני יצחק מכ.א.ל, גדי עבאדי, דבש מתוק, שירי גורלי מבנק דיסקונט, אייל היימן ואושרי עמיקם מבנק מרכנתיל, מיכה וייס וענת דיאמנט ממשרד האוצר, אייל אסרף מבנק לאומי, אמיר שרייבר מישראכרט, גדי מרגלית משב"א.

תקציר

עבודה זו עוסקת בסיכוני הסייבר בשרשרת האספקה במגזר הפיננסי ובהצעת דרכי התמודדות עימם. העבודה נכתבה במטרה להציג המלצות מתאימות וישימות בראי המגזר הבנקאי, וגובשה לאחר בחינת הנושא ולמידתו לעומקו, לרבות במסגרת דיונים ומפגשי עבודה עם גורמים רלוונטיים במגזר זה. במסגרת זו גם נערכה סקירה של התקנים הבין־לאומיים המתאימים, ממנה עולה כי קיימת תקינה ענפה העוסקת במגוון רחב של תחומים ובקרות, שנועדו לצמצם את החשיפה לסיכוני סייבר בשרשרת האספקה ולהיערך לקראתם. כן נסקרו תורות הגנה, החלטות ממשלה, הוראות, חוזרים ותקנות רלוונטיים בישראל. סקירתם מצביעה על כך שהרגולציה הישראלית מתייחסת להיבטים שונים של סיכונים בשרשרת האספקה, אך היא אינה מחייבת את כלל הארגונים. זוהי רגולציה הבנויה על בסיס מגזרי, כמו מגזר הביטוח ושוק ההון, או רגולציה נושאית, כמו בנושא הפרטיות.

בנוסף, נבחנו ונותחו במסגרת עבודה זו האיומים הרלוונטיים על שרשרת האספקה. מהניתוח עולה כי האיומים על הארגון, לרבות ארגון פיננסי, כתוצאה מתקיפת שרשרת האספקה יכולים להתממש באמצעות ערוצי תקיפה מגוונים ביותר, כגון חדירה למערכות של ספק בעל רמת הגנה נמוכה יחסית (אך בעל גישה למערכות הארגון), ודרכו חדירה למערכות הארגון; שימוש בעדכוני תוכנה לגיטימיים להפצת נוזקה, וכדומה. אין מדובר באיומים תיאורטיים, אלא בניתוח המסתמך על מספר רב של אירועים שהתרחשו בארץ ובעולם, שמהותם היא פגיעה בארגונים תוך ניצול שרשרת האספקה שלהם. מורכבות האיום, המגוון הרחב של התרחישים האפשריים והתעצמות יכולות התוקפים מחייבים את הארגונים, ובתוכם גם את הארגונים הפיננסיים, לנקוט צעדים הגנתיים משמעותיים כדי להתמודד עם האתגר ולצמצם את הסיכונים הגלומים בו.

בתהליך הבחינה נסקרו מתודולוגיות ומודלים לניהול ספקים בשרשרת האספקה, לרבות בחברות גדולות בעולם. נמצאו מתודולוגיות ומודלים לטיפול ולסיווג ספקים ברמה הארגונית, אך לא נמצאו מתודולוגיות ומודלים לטיפול בספקים ולסיווגם ברמה הלאומית והמגזרית, או לחילופין, לסיווג ספקים בהיבטי סייבר. כן נמצאו במספר תחומים במשק הישראלי גישות בעלות הקשר אפשרי לעבודה זו – קטגוריזציה המבוצעת ברמה הלאומית לספקים מענף משקי אחר (סיווג קבלני בניין) ותהליך

תשתיתי המבוצע/מונחה על ידי גורם מרכזי אחד (היחידה הממלכתית לקביעת התאמה ביטחונית בשירות הביטחון הכללי) עבור מועסקים בגופים רבים.

מערך הסייבר הלאומי של ישראל החל לפעול בהיבט הסייבר לפיתוח מתודה ברמה הלאומית ולהנגשתה בפורטל. למרות שמתודה זו עדיין אינה ממומשת באופן נרחב (נכון למועד כתיבת דוח זה), היא עשויה להפוך בהמשך לפלטפורמה הולמת לשימוש נרחב על ידי גופים רבים. יחידה ייעודית במשרד האוצר, המטפלת בפעילותו של המגזר הפיננסי, נמצאת בשלבי יישום ראשוניים מול ספקי המערכת הפיננסית וגם היא רלוונטית לענייננו.

במסגרת עבודה זו נערך ניתוח כלכלי של שתי חלופות עיקריות לניהול הפעילות הנדרשת מול ספקי המערכת הפיננסית בהיבטים הנוגעים להתמודדות עם סיכוני סייבר בשרשרת האספקה: האחת, ניהול עצמי על ידי כל בנק; השנייה, ניהול מרכזי עבור כל/רוב הבנקים. בנוסף נערך ניתוח רגישות לתוצאות הניתוח הכלכלי. מהניתוחים עולה כי מבחינה כלכלית יש עדיפות מובהקת לניהול הנושא באופן ריכוזי עבור הבנקים המסחריים. לניהול מרכזי יש פוטנציאל לחיסכון של כ־12 סוקרים (אנשי מקצוע מתאימים. טווח ניתוח הרגישות מצביע על פוטנציאל חיסכון של 8–18 סוקרים) בכלל המגזר הבנקאי. זאת ועוד, ניהול מרכזי יחזק את השפעתו ועוצמתו של הגוף הסוקר כלפי הספקים (בהיותו מייצג את כל/רוב הבנקים ולא רק בנק מסוים), יאפשר התמקצעות טובה של הצוות (גוף מתמחה ברמה המגזרית), יקטין תקורות (תקורות ניהול, תקורות פיזיות וכדומה) עבור כל בנק ויגרום גם לחיסכון משמעותי במשאבים אצל הספקים המהותיים עצמם (במקום שיתקיימו כחמישה מבדקים דומים בשנה אצל ספק מהותי, יתקיים מבדק אחד בלבד).

העבודה מציעה שתי חלופות לניהול מרכזי מול ספקי המערכת הפיננסית: בחלופה הראשונה, הניהול המרכזי מבוצע על ידי גוף בבעלות הבנקים המסחריים; בחלופה השנייה הניהול המרכזי מבוצע על ידי גוף חיצוני שאינו בבעלות הבנקים המסחריים (שיכול להיות גוף ממשלתי), שיבצע את בדיקות הספקים בעצמו עבור הבנקים. שתי חלופות אלו נבחנו למול שלושה קריטריונים:

א. **שיפור ביטחון הסייבר במערכת הפיננסית** – הניתוח הראה שחלופה של ניהול מרכזי תשפר משמעותית את רמת ביטחון הסייבר של המערכת הפיננסית בהקשרי שרשרת האספקה.

ב. **כדאיות כלכלית** – ההשוואה בין שתי החלופות נערכה על בסיס משאבי ההקמה והתפעול השוטף; מידת השליטה במשאבים (גמישות, התאמות, קביעת סדר עדיפויות וכדומה); קיומה של אופציה למכירת השירותים לגופים נוספים; השפעת צפויה של פעילות היחידה המרכזית על הספקים; יכולת עמידה בדרישות בנק ישראל.

ג. **מידת הציות לדרישות ההגבלים העיסקיים** – מהניתוח שבוצע עולה שהקמת גוף סוקר מרכזי אינה מהווה פגיעה בדרישות ההגבלים העיסקיים, לאור העובדה שהקמת גוף כזה לא תהווה פגיעה בתחרות בין הבנקים, וכל עניינה הוא שיפור רמת הביטחון והיציבות של המערכת הפיננסית בכללותה.

זאת ועוד, כיום מתמודדים הבנקים עם תהליכים ארוכים הקשורים בהוספת ספקים חדשים למערכת. הפעלה של גוף מרכזי תוכל לאפשר קיצור התהליך ואף ליצור מצב שבו גופים פיננסיים יוכלו לבקש סקירה והסמכה מראש בהקשר להתאמה בהיבטי בטחון הסייבר למערכת הפיננסית.

לאור האמור לעיל, ובהתאם לניתוח הנתונים הקיימים, להלן עיקרי ההמלצות:

א. על הבנקים למפות ולסווג את ספקיהם המהותיים, קרי, את הספקים המהותיים לפעילותם ו/או אלה החושפים אותם לסיכוני סייבר ואבטחת מידע פוטנציאליים גבוהים, שבהתממשותם ניתן יהיה לתקוף את התאגיד הבנקאי או לפגוע בפעילותו.

ב. על הבנקים להגדיר מערכת דרישות עבור הספקים המהותיים בכל הנוגע להתמודדותם עם סיכוני הסייבר בשרשרת האספקה במגזר הפיננסי. על מערכת דרישות זו לעמוד בהלימה עם הוראות בנק ישראל והוראות כל דין ולהתבסס על הנושאים, התחומים והבקרות המכוסים על ידי התקינה הקיימת והניסיון המצטבר.

ג. על הבנקים לוודא כי ספקיהם המהותיים מבצעים את מערכת הדרישות המוגדרת. זאת, באמצעות סוקרים מקצועיים שיפעלו מול הספקים ויבקרו את ביצוען השוטף של הדרישות.

ד. מוצע לבנקים לבחון שימוש (לרבות שימוש משלים) במתודה המפותחת במערך הסייבר הלאומי בנושא הפעילות מול ספקים.

ה. נוכח מסקנות הבדיקה כי יש כדאיות כלכלית מובהקת לנהל פעילות זו באופן מרכזי עבור כלל הבנקים, ולא על ידי כל בנק באופן עצמאי, מומלץ שניהול הפעילות יהיה מרכזי. כך גם תגדל השפעתה של הפעילות מול הספקים, שכן הגוף הסוקר ייצג בפניהם את דרישות כלל הבנקים ולא רק דרישות של בנק אחד. יודגש, עם זאת, כי בנק מסוים יוכל להוסיף לפי הצורך דרישות ספציפיות מסַפָּק מסוים. מוצע שהגוף המרכזי שיוקם יהיה בהעלות הבנקים וכי מנגנון התמחור בין הבנקים לצורך הקמתו ותפעולו יבוצע באופן דיפרנציאלי, שיבטא את היקף הפעילות של כל בנק במיזם.

תוכן העניינים

מבוא

התמודדות מיטבית עם אתגרי הסייבר בשרשרת האספקה מחייבת התייחסות קונקרטית לצרכים של המגזר הבנקאי בכלל ושל המגזר הבנקאי בישראל בפרט. בנקים בישראל כפופים להנחיות הפיקוח על הבנקים והגנתם מחייבת מגוון מרכיבים, בהם: שכבת הגנה טכנולוגית ונהלי עבודה הכוללים ובהם התייחסות לאיומי סייבר בשרשרת האספקה. ככל שתאגיד בנקאי יצליח לזהות את האיומים וינקוט את האמצעים הנדרשים למיגורם בשלב מוקדם, כך תגדל רמת ההגנה הכוללת שלו.

מסמך זה הינו תוצר של עבודת המכון למחקרי ביטחון לאומי לגיבוש מתודולוגיה לניהול לאומי של סיכוני שרשרת האספקה במגזר הפיננסי. הוא כולל את החלקים הבאים:

א. **תקינה** – ניתוח התקינה הרלוונטית.
ב. **רגולציה בישראל** – בחינת הרגולציה הקיימת בישראל בהקשרים רלוונטיים.
ג. **מרחב האיומים הרלוונטיים** – בחינה של מפת האיומים הרלוונטיים לשרשרת האספקה.
ד. **מתודולוגיות קיימות** – מתודולוגיות ומודלים לניהול ספקים בשרשרת האספקה.
ה. **גישות אפשריות** – דוגמאות לגישות קיימות במשק הישראלי, שיש להן קשר אפשרי לנושא עבודה זאת.
ו. **ניתוח חלופות אפשריות** – ניתוח חלופות לניהול לאומי של סיכוני שרשרת האספקה למגזר הפיננסי.
ז. **סיכום והמלצות** – ניתוח והמלצות.

פרק א׳: תקינה

משפחת תקני ISO

תקן בין־לאומי נפוץ בתחום אבטחת המידע הינו ISO 27001[1] (שם התקן בישראל הוא "ת"י ISO 27001"). תקן זה עוסק במיסוד מערכת לניהול אבטחת מידע ארגונית ובתהליך הכרוך בהקמת המערכת ובשיפורה השיטתי. פרק 15 בתקן עוסק בקשרי ספקים. פירוט הבקרות הרלוונטיות בהקשר זה מופיע בתקן ISO 27001.[2] על פי תקן זה, הארגון נדרש להגדיר מדיניות עבור הספקים, שצריכה להיות מוסכמת על הספק וממוסמכת. בנוסף, המדיניות צריכה להתמקד בתהליכים הרלוונטיים המתרחשים הן באתרי הארגון והן באתרי הספק, ובכלל זה:

א. זיהוי סוגי הספקים שהארגון התיר להם גישה למידע.
ב. הגדרת מחזור חיים לניהול קשרי ספקים.
ג. הגדרת סוגי המידע המותר לְגישה, לפי סוגי הספקים, וכן תהליכי ניטור ובקרה על הגישה למידע.
ד. הגדרת דרישות האבטחה המינימליות לפי סוגי המידע וסוגי הגישה אליו, וזאת כבסיס להסכמים עם כל ספק רלוונטי.
ה. הגדרת אופן הטיפול באירועי אבטחה ובתקלות הקשורות לספק, והגדרת האחריות של כל צד.
ו. העלאת מודעות ותרגול עובדים.

תקן ISO 27002 גם מחייב להגדיר בהסכם כתוב את דרישות האבטחה לכל ספק בעל יכולת גישה לעיבוד, לאחסון וליצור תקשורת, או לאספקת מידע או רכיבי טכנולוגיות מידע לארגון. הדרישות צריכות לכלול, בין היתר:

א. הגדרת המידע המועבר, או המידע אליו מותרת גישה, לרבות השיטה להעברת המידע או לגישה אליו.
ב. הגדרת סיווג המידע בהתאם לשיטת הסיווג הארגונית.
ג. דרישות החוק והרגולטור, לרבות בתחומי הגנה על המידע, קניין רוחני וזכויות יוצרים.

---

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

2 "Code of Practice for Information Security Controls", *ISO/IEC 27002*, 2013.

ד. התחייבות ליישם בקרות של גישה למידע, ניטור, דיווח וחיווי.
ה. דרישות מסַפקי משנה, כולל חובות רגולטוריות ויישום בקרות.
ו. קביעת הזכות של הארגון לבקר את התהליכים והבקרות של הספק, שיש להם קשר להסכם עימו.
ז. חובת הספק לדווח באופן עיתי על אפקטיביות הבקרות שהוא מיישם ועל תיקונים שוטפים שהוא עורך בתחומים הדורשים תיקון.

בנוסף, ההסכמים עם הספק צריכים לכלול דרישות אבטחה הנובעות מסיכונים הנוצרים בשרשרת האספקה של מוצרים או שירותים, ובכלל זה:
א. הגדרת הדרישות הנובעות מאספקת השירות או המוצר, בנוסף לדרישות האבטחה הכלליות הנובעות מעצם קשרי העבודה עם הספק.
ב. דרישה שהספק יממש תהליכי אבטחה הולמים, לרבות כאשר רכיבים מהמוצר או השירות המסופק כוללים מרכיבים המגיעים מספקים אחרים.
ג. מימוש תהליכי ניטור על אספקת המוצרים והשירותים.
ד. הגדרת רכיבים קריטיים והבטחת יכולת המעקב והבקרה על מקורם ומיקומם בשרשרת האספקה.
ה. הגדרת כללים לשיתוף מידע בכל הקשור לשרשרת האספקה.

התקן מדגיש עוד את הצורך לנהל ולנטר שינויים בקשרי ספקים ובשרשרת האספקה.
תקינה עשירה ומקיפה נוספת העוסקת בנושא זה באופן ישיר היא משפחת תקני ISO 28000.[3] תקנים אלה מתייחסים להיבטים הבאים:
א. כתיבת מדיניות אבטחה.
ב. הערכת סיכונים.
ג. הגדרת הדרישות החוקיות והרגולטוריות.
ד. הגדרת יעדים ומטרות של ניהול האבטחה.
ה. הגדרות מבניות ותחומי אחריות.
ו. העלאת מודעות ותרגול.
ז. בקרות תפעוליות.
ח. היערכות ומוכנות לאירועי אבטחה.
ט. מדידה וניטור.
י. בקרות מונעות ומתקנות.
יא. חיווי וסקרי הנהלה.

3 "Specification for Security Management Systems for the Supply Chain", *ISO 28000*; "Security Management Systems for the Supply Chain – Best Practices", *ISO 28001*; "Guidelines for the Implementation of ISO/PAS 28000", *ISO 28004* .

יצוין כי בהחלטת ממשלת ישראל מספר 2443,[4] מצוין בנספח ז' סעיף 2 א' כי גורמים המעבירים מידע ממוחשב, או ספקים של מערכות מחשוב המוטמעות או מקושרות למערכות מחשוב ממשלתיות, המבקשים למכור לממשלה שירותים הקשורים בכך, יחויבו לעמוד בתקן אבטחת מידע ארגוני ממשפחת ת"י ISO 27001.

מכון התקנים האמריקאי

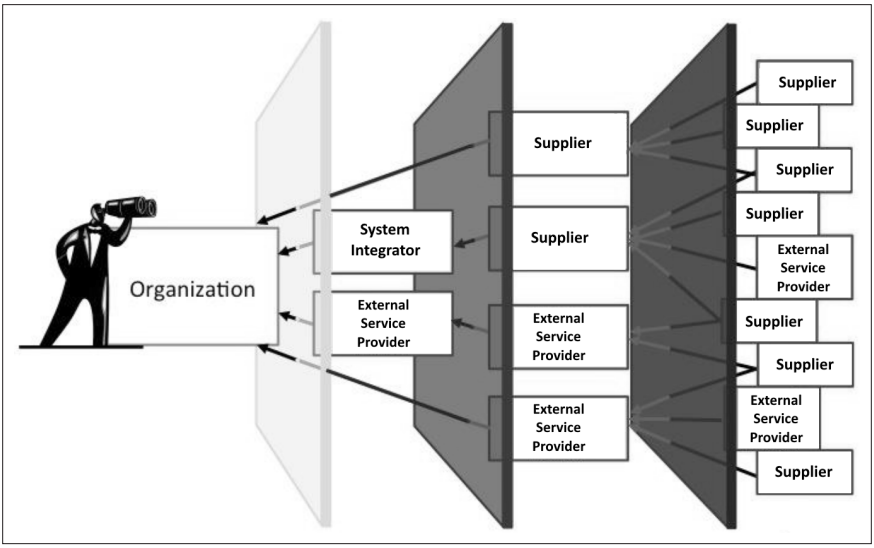
תקן נוסף הרלוונטי לענייננו הוא התקן של מכון התקנים הלאומי של ארצות הברית (National Institute of Standards and Technology – NIST) 800-161 NIST.[5] גם תקן זה מקיף ומפורט ומטרתו היא לספק מדריך לסוכנויות הפדרליות בארצות הברית לזיהוי, הערכה, בחירה והטמעה של תהליכי ניהול סיכונים, וכן בקרות על ניהול סיכונים בשרשרת האספקה של טכנולוגיות המידע. התהליכים והבקרות המפורטים בתקן ניתנים לשינוי או להרחבה בגין דרישות רגולטוריות, מדיניות ארגונית, הנחיות וכדומה.

תקן NIST 800-161 מציין כי על הארגונים לפתח אסטרטגיות להפחתת סיכונים בשרשרת האספקה של טכנולוגיות המידע, שיותאמו ספציפית לאותם סיכונים ויהיו פועל יוצא של המשימות, הצרכים העיסקיים, האיומים והסביבות התפעוליות. התקן מדגיש את מורכבות שרשרת האספקה של טכנולוגיית המידע ואת העובדה שלספקים יש לעיתים ספקים נוספים, דבר היוצר קושי לארגון לראות, להבין ולבקר את שרשרת האספקה, במיוחד כשהספק אינו ספק ישיר שלו. הנושא מומחש בתרשים שלהלן, המופיע בתקן NIST 800-161.

בנוסף, תקן NIST 800-161 מציין כי הטיפול בסיכוני שרשרת האספקה בטכנולוגיית המידע צריך להיות מוטמע בתוך תהליך 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.

4 "קידום אסדרה לאומית והובלה ממשלתית בהגנת הסייבר", *החלטת ממשלה 2443*, פברואר 2015.

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



תרשים 1: קושי בהבנת שרשרת האספקה

מכון התקנים האמריקאי פרסם גם דוח פנימי העוסק בטיפול בסיכונים בשרשרת האספקה – NISTIR-7622.[6] הדוח, שנועד עבור הסוכנויות הפדרליות השונות בארצות הברית, מציג מגוון גישות לטיפול בסיכונים בשרשרת האספקה של טכנולוגיות מידע, ובעיקר בנושאים הבאים:

א. זיהוי הרכיבים, התהליכים והגורמים בשרשרת האספקה.
ב. הגבלת גישה וחשיפה בשרשרת האספקה.
ג. ניהול ותחזוקה של בקרת השינויים בתהליכים, רכיבים, כלים ונתונים.
ד. שיתוף מידע תוך הטלת מגבלות עליו.
ה. ביצוע מהלכי מוכנות ותרגול.
ו. תכנון הגנה למערכות, רכיבים ותהליכים.
ז. ביצוע סְקרי ספקים.
ח. הקשחת מנגנוני העברה.
ט. הבטחת תהליכים ופעילויות.
י. ניהול הפעילויות בסיום מחזור החיים של רכיב או מערכת.

6 "National Supply Chain Risk Management Practices for Federal Information Systems", *NISTIR 7622*, October 2012.

רגולציית ההגנה על המידע

הרגולציה של הגנת המידע (General Data Protection Regulation – GDPR)[7] היא פרי החלטה של הפרלמנט האירופי, מועצת האיחוד האירופי והנציבות האירופית, שנועדה להנחות את מדינות האיחוד האירופי בכל הנוגע לאיסוף, שמירה והעברה של נתונים אישיים של אנשים פרטיים, וקובעת כללים אחידים לשמירה על הפרטיות. הרגולציה התקבלה ב־27 באפריל 2016 ונכנסה לתוקף ב־28 במאי 2018. היא מחליפה את ההנחיה האירופית בנוגע להגנה על נתונים (הנחיה EC/95/46) משנת 1995.

הרגולציה חלה על כל הארגונים המעבדים נתוני מידע שמקורם בטריטוריה של מדינות האיחוד האירופי, גם אם אינם פועלים בשטח האיחוד. הרגולציה מטילה איסורים ומגבלות על העברת מידע אל מחוץ לטריטוריה של האיחוד האירופי, בשל החשש להפרות שעלולות להתרחש באזורים אחרים בעולם, שבהם הפרטיות אינה מוגנת כראוי.

אחד העקרונות של הרגולציה של האיחוד האירופי הוא אחריותיות (Accountability). למשל, ארגונים המשתמשים בספקים כמיקור חוץ לעיבוד נתונים אישיים (כמו הפקת תלושי שכר) חייבים לוודא שנעשה טיפול אבטחתי נאות וכי קיימת תאימות עם הדרישות לאורך כל שרשרת האספקה שלהם, לרבות אצל ספקיהם.

המועצה לבחינת תאגידים פיננסיים פדרליים

המועצה לבחינת תאגידים פיננסיים פדרליים (Federal Financial Institutions Examination Council – FFIEC) הינה גוף רשמי שנועד לגבש שפת ניהול אחידה בין תאגידים פיננסיים בארצות הברית, ובכלל זה עקרונות, תקנים וטופסי דיווח אחידים, וכן מגבש המלצות בעניין אחידות הפיקוח על אותם מוסדות פיננסיים.

החוברת "Information Security"[8] שפרסמה המועצה כוללת פרק המתייחס לעניין שרשרת האספקה (II.C.14, Supply Chain). בפרק מופיעות מספר דוגמאות להתמודדות ארגונית עם איומי שרשרת האספקה, כמפורט להלן:

א. ביצוע רכישות רק מספקים בעלי יכולת שליטה על שרשרת האספקה שלהם.
ב. רכישת חומרה ותוכנה באמצעות צדדים שלישיים כדי להגן על זהות הרוכש.
ג. ביצוע בדיקות אנומליה לחומרה.
ד. ביצוע בדיקות אוטומטיות ובדיקות קוד לתוכנה.

---

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

8 "Information Security", *The Federal Financial Institutions Examination Council (FFIEC)*, September 2016.

ה. בחינה סדירה של אמינות רכיבי תוכנה וחומרה שנרכשו, באמצעות ניטור והערכה על ידי קבוצות משתמשים.

סיכום

מסקירת המקורות השונים עולה כי קיימת תקינה ענפה, הפורסת בפני הארגונים מגוון רחב של נושאים, תחומים ובקרות המאפשרים להם לצמצם את חשיפתם לסיכוני סייבר בשרשרת האספקה ולהיערך לקראתם.

פרק ב': רגולציה בישראל

פרק זה סוקר הנחיות ורגולציות בלתי מסווגות של ממשלת ישראל, שפרטיהן גלויים לציבור הרחב.

מערך הסייבר

תורת ההגנה של מערך הסייבר הלאומי בישראל[9] מתייחסת ספציפית לבקרות הדורשות להגנה על שרשרת האספקה:[10]

א. בקרה 3.2 – הארגון יוודא כתיבת מדיניות הגנה, לרבות מדיניות הגנה על שרשרת האספקה.

ב. בקרה 16.1 – יש להתגונן מפני איומים של שרשרת האספקה על המערכת, כחלק מאסטרטגיה של "הגנה לרוחב" (Defense in Breadth).

ג. בקרה 16.2 – יש להשתמש בכלים חוזיים ומשפטיים בעת רכישת מערכת מידע או שירות מספקים.

ד. בקרה 16.3 – יש לבצע סקר סַפָּק לפני חתימה על חוזה לרכישת שירותים ומוצרים.

ה. בקרה 16.4 – במקרים בהם יש חיבור לרשת הספק, יש ליישם בקרות מונעות שתפקידן הוא למזער נזקים העלולים להגיע מתשתיות הספק.

ו. בקרה 17.8: אבטחת שרשרת אספקה – יש לדרוש מספקי שירותים לציית לדרישות האבטחה הארגוניות, לרגולציות, לתקנים ולהנחיות.

ז. בקרה 17.17 – יש לממש שיטות למניעת הכנסה של רכיבי מערכת מזויפים, בדגש על הכנסה של רכיבי חומרה או תוכנה מזויפים לארגון. זאת, בין אם במתכוון ובין אם באמצעות הטעיה של גורם בשרשרת האספקה.

הוראות בנק ישראל

הוראת בנק ישראל – הפיקוח על הבנקים בנושא סיכוני סייבר[11] דורשת מהתאגיד הבנקאי לקבוע את הפעולות הנחוצות כדי לוודא שהגורמים החיצוניים נוקטים את האמצעים הדרושים להפחתת החשיפה של התאגיד הבנקאי לסיכוני סייבר. בתוך כך, ההוראה עוסקת באחריות התאגיד הבנקאי לקיום תצורת עבודה מאובטחת מול

9 "תורת ההגנה בסייבר לארגון", *מערך הסייבר הלאומי*, 18 באפריל 2018.

10 נכון למועד כתיבת דוח זה, התורה אינה מחייבת את הארגונים בישראל.

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

הספקים החיצוניים ובחובתו לנהל בצורה הולמת סיכוני סייבר הקשורים בפעילותם של ספקים אלה "בחצרי התאגיד הבנקאי ובממשקים שלהם עם התאגיד".

ההוראה של הפיקוח על הבנקים גם מתייחסת לצורך במיפוי וזיהוי "ספקים מהותיים",[12] במתן אפשרות לתאגיד הבנקאי לדרוש מהספק לעמוד בהנחיות האבטחה, ובשמירת יכולת אכיפה ובקרה של התאגיד הבנקאי מול הספק.

משרד האוצר – אגף שוק ההון, ביטוח וחיסכון

אגף שוק ההון, ביטוח וחיסכון במשרד האוצר פרסם נוהל[13] החל על גופים המנהלים כספי ציבור, כגון כספי פנסיה וקרנות נאמנות, לרבות חברות ביטוח ובתי השקעות. סעיף ה' בנוהל מתייחס למיקור חוץ ומפרט את דרישות הגנת הסייבר בהסכמי מיקור חוץ, כלהלן:

א. הגוף יגדיר נוהל לדרישות הגנת סייבר ביחס לסיכוני מיקור חוץ וביחס לאבטחת שרשרת האספקה. נוהל זה יישום בעת התקשרות עם גורם מיקור חוץ חדש.

ב. במסגרת הסכם ההתקשרות לקבלת שירותי מיקור חוץ:

- ייאסר על נותן השירות להעביר לצד שלישי מידע שקיבל במסגרת ההתקשרות, או להשתמש במידע שאליו נחשף אגב ביצוע ההתקשרות, לכל מטרה אחרת שאינה קשורה לאותה התקשרות.
- כשקיים צורך בהעברת נתונים, יבוצע תהליך של גישה מבוקרת לנתונים פרטניים לצורך מתן השירות. לא יבוצע שכפול של כלל בסיס הנתונים.
- תיבחן דרישה לעמידה בתקן ת"י ISO 27001 של מכון התקנים הישראלי.

הנוהל של אגף שוק ההון, ביטוח וחיסכון קובע עוד כי אספקה של שירותי תחזוקה מרחוק (מידע, תוכנה או ציוד תקשורת) על ידי גורמי מיקור חוץ תתבצע בתנאים הבאים:

א. נותן שירות מיקור החוץ יקבל אישור להתחברות לפני תחילת עבודתו. מנהל הגנת סייבר יקבע מיהו בעל הסמכות לאשר התחברות מסוג זה.

ב. גישה מרחוק תתאפשר באמצעות משתמש ייעודי לכל נותן שירות מיקור חוץ, בתיאום מראש עם הגוף באחראי לאופן ההתקשרות ותדירותה.

---

12 ההוראה מגדירה את "הספקים המהותיים" כגורמי חוץ הנכללים בשרשרת האספקה של התאגיד הבנקאי (לדוגמה, חברות התומכות במתן שירותי מסחר בשוק ההון), שהינם 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.

13 "ניהול סיכוני סייבר בגופים מוסדיים", *משרד האוצר – אגף שוק ההון, ביטוח וחיסכון*, אוגוסט 2016.

ג. גישה מרחוק תתאפשר לזמן מוגבל, על פי סוג הפעילות אותה יבצע נותן שירות מיקור החוץ.
ד. הגוף יישם הזדהות חזקה בכל גישה מרחוק של נותן שירות מיקור חוץ.
ה. הגוף יישם הצפנה מקצה לקצה לכל אורך נתיב ההתקשרות מרחוק.
ו. הגוף ינטר כל פעילות מהותית שבוצעה בגישה מרחוק.
ז. חשיפת נותן שירות מיקור החוץ למידע על לקוחות תצומצם עד למינימום הכרחי, ובמידת האפשר תחסם במלואה.

הרשות להגנת הפרטיות

תקנות הגנת הפרטיות (אבטחת מידע) של הרשות להגנת הפרטיות (לשעבר רמו"ט) נכנסו לתוקף במאי 2018.[14] הן מבוססות על ההנחה כי מתן גישה לגורם חיצוני יוצרת סיכונים מיוחדים, ולכן מצריכה בחינה של סיכוני אבטחת המידע האפשריים הנובעים מהתקשרות עם אותו גורם חיצוני. על רקע זה, ההנחיה של הרשות להגנת הפרטיות מפרטת את הדרישות הבאות:

א. בחינה, לפני ביצוע ההתקשרות, של סיכוני אבטחת המידע הכרוכים באותה התקשרות, ואם הם גבוהים מדי בהתחשב ברגישות המידע, הימנעות לחלוטין ממיקור החוץ.
ב. בשים לב לסיכוני אבטחת המידע, קביעה מפורשת ובהסכם של הסעיפים הבאים: מהו המידע שהגורם החיצוני רשאי לעבד ולאלו מטרות? לאלו מערכות הוא רשאי לגשת? מהו סוג העיבוד שאותו הוא רשאי לבצע? מהו משך ההתקשרות ומה יהיה אופן השבת המידע לידי הבעלים בסיום ההתקשרות? אופן יישום הוראות התקנות לאבטחת מידע וחובת הגורם החיצוני להחתים את בעלי ההרשאות שלו על התחייבות לשמור על סודיות המידע.

בנוסף, תקנה 15 – מיקור חוץ מציינת את חובת הדיווח ואת הצורך לנקוט אמצעי בקרה ופיקוח על עמידתו של הגורם החיצוני בהוראות ההסכם ובהוראות התקנות, בהיקף הנדרש ובשים לב לסיכוני אבטחת המידע הכרוכים בהתקשרות.

יצוין כי תקנה 15 של הרשות להגנת הפרטיות דומה להנחייה של רשם מאגרי המידע, העוסקת בשימוש בשירותי מיקור חוץ.[15]

---

14 "תקנות הגנת הפרטיות (אבטחת מידע) – תקנה 15 – מיקור חוץ", *כנסת ישראל*, מאי 2017.
15 "הנחיית רשם מאגרי מידע מס' 2011/2 – שימוש בשירותי מיקור חוץ לעיבוד מידע אישי", *הרשות להגנת הפרטיות*, 10 ביוני 2012.

סיכום

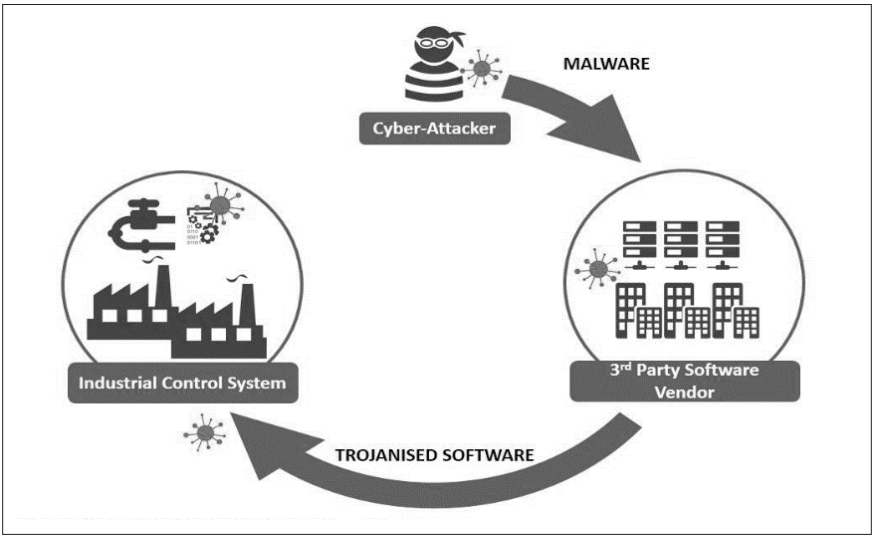
הרגולציה הישראלית כוללת התייחסות גם להיבטים הכרוכים בסיכוני שרשרת האספקה. עם זאת, אין כיום רגולציה ישראלית מחייבת עבור כלל הארגונים במשק, והרגולציה הקיימת היא מגזרית (כמו במגזר הביטוח ושוק ההון) או נושאית (לדוגמה, בנושא הפרטיות).

פרק ג': מרחב האיומים הרלוונטיים

ניתוח האיומים

פרק זה מתאר את מרחב האיומים הרלוונטיים לתקיפה דרך שרשרת אספקה.

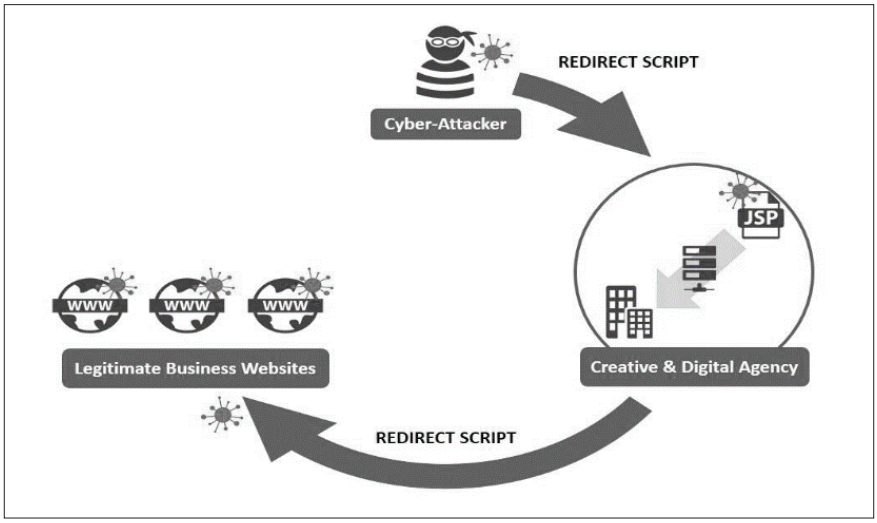
מסמך של CERT UK מציג ארבעה איומים על שרשרת האספקה, המבוססים על אירועי אמת:[16] האיום הראשון הוא תקיפת המערכת דרך ספק צד שלישי. באירוע הספציפי המפורט במקרה זה, התוקף תקף תוכנת מערכת בקרה תעשייתית (Industrial Control System – ICS) המותקנת בארגון, ועשה זאת באמצעות ספק צד שלישי של תוכנה. להלן תרשים הלקוח מהמסמך של CERT UK, הממחיש את האיום:



תרשים 2: המחשת איום ספק צד שלישי

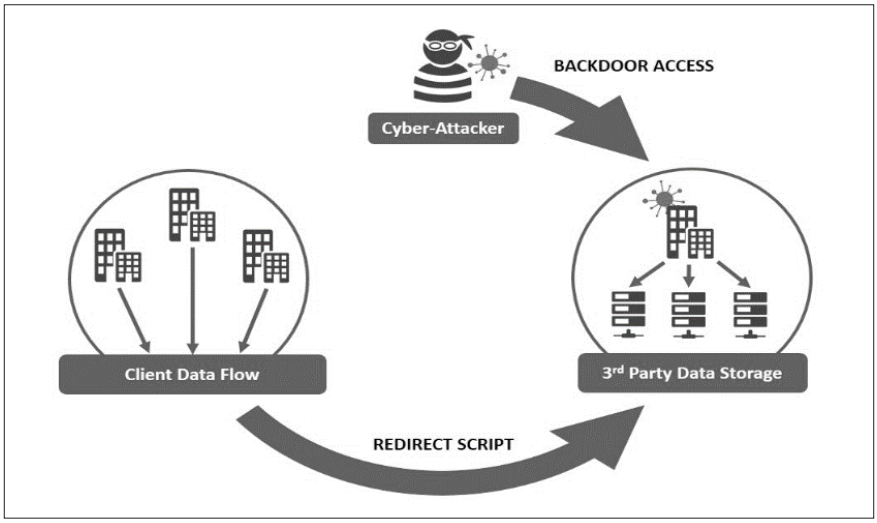
האיום השני המפורט במסמך הינו תקיפת אתרי אינטרנט עיסקיים באמצעות עיצוב ובניית אתרים. במקרה הספציפי המתואר במסמך, התוקף תקף אתרי אינטרנט פיננסיים באמצעות סקריפטים שהועברו מחברות דיגיטציה ועיצוב. להלן תרשים הלקוח מהמסמך, הממחיש את האיום:

16 "Cyber-Security Risks in the Supply Chain", *CERT UK* , 2015.



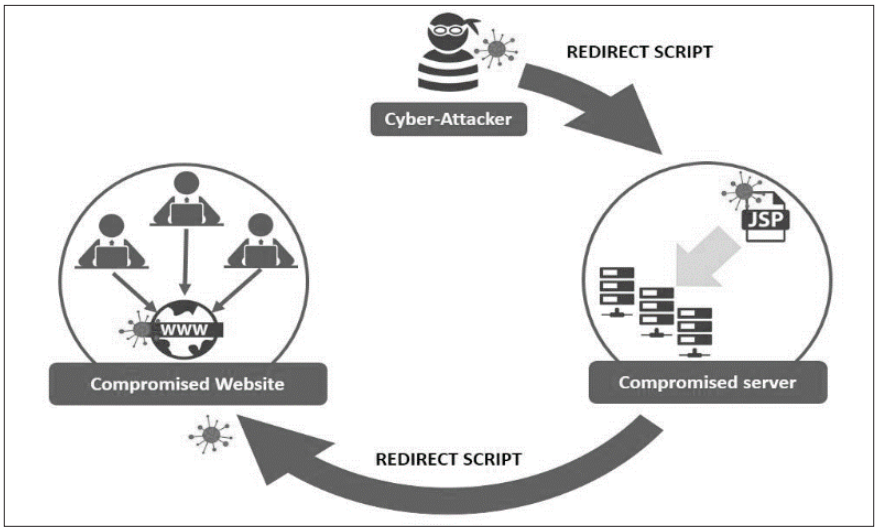
תרשים 3: המחשת איום תקיפת אתר אינטרנט

האיום השלישי הינו התקפה על חברות צד שלישי העוסקות באחסון נתוני חברות. הכוונה היא למצב בו חברות רבות מאחסנות את המידע שלהן, לעיתים אף מידע רגיש, אצל חברות צד שלישי, המהוות גם הן יעד לתקיפה ישירה. להלן תרשים הלקוח מהמסמך, הממחיש את האיום:



תרשים 4: המחשת איום תקיפת אחסון מידע בחברות צד שלישי

האיום הרביעי הינו תקיפת Watering hole. הכוונה במקרה זה היא לשתילת קוד עוין באתרים הנמצאים בשימוש נרחב על ידי מושאי התקיפה, כך שהגישה אליהם תגרום לתקיפת המערכות אצל המשתמשים שהם מושאי התקיפה. להלן תרשים הלקוח מהמסמך של CERT UK, הממחיש את האיום:



תרשים 5: המחשת איום תקיפת Watering hole

דוגמאות נוספות לאיומים בהקשר האמור מופיעות בתקן ISO 27036-1[17] כמפורט להלן:

א. גישה פיזית של ספק לאתרי הלקוח.
ב. גישה למידע או למערכות מידע של הלקוח על ידי עובדי הספק באתרי הלקוח.
ג. גישה מרחוק של הספק למידע או למערכות מידע של הלקוח.
ד. עיבוד מידע של הלקוח על ידי הספק מחוץ לאתרי הלקוח.
ה. הפעלת יישומים של הלקוח על תשתיות הספק.
ו. אירוח (Hosting) של ציוד הלקוח באתרי הספק.
ז. אחסון נתוני הלקוח (לרבות גיבוי) אצל הספק.

בדוח של חברת Clearsky, הסוקר תקיפות סייבר משמעותיות שאירעו בשנים 2016-2018 בעולם ובישראל,[18] מצוין כי ארגונים במגזר הפיננסי (בנקים) הם מטרה

17 "Techniques – Information Security for Suppliers Relationship Information Technology – Security", *ISO 27036*.

18 "דו"ח אירועי סייבר 2016-2018, ניצול שרשרת אספקה SWIFT", **חברת Clearsky**, מארס 2018.

מרכזית לתוקפים מיומנים (הן גורמי פשיעה והן תוקפים מדינתיים) וכי מערכות ליבה בנקאיות, כמו Swift ומערכות ATM, הפכו בשנים האחרונות ליעד מועדף של תוקפי סייבר.

הדוח מציין עוד כי חברות וארגונים בנו בעשור האחרון מערכי הגנה קדמיים מול שדרת האינטרנט, אך השקיעו 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 הקלות היחסית לחדור לחברות ולארגונים קטנים יחסית, שיש להם מערך הגנת סייבר מוחלש, כדי לחדור דרכם לארגוני יעד בעלי חשיבות קריטית. תוקפים גם מנצלים את העובדה שלחלק מספקי המשנה של ארגונים קריטיים יש גישה ישירה או קלה יותר אליהם, כדי לחדור באמצעותם לאותם ארגונים. התקיפה באמצעות שרשרת האספקה הופכת למתוחכמת יותר ויותר וכוללת, בין היתר, 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.

הדוח של חברת Clearsky מפרט שלוש תובנות עיקריות הנוגעות להתמודדות הארגונית עם סיכוני סייבר בשרשרת האספקה:

א. **בניית מודל הגנה חדש** – המודל המסורתי, שעיקרו יישום אמצעי אבטחה מוגברים ב"גבולות" הארגון החיצוניים, תוך השארת ליבת הארגון בלתי מוגנת, אינו מתאים יותר. מודל זה הביא בשנים האחרונות לטיפול חסר באבטחת המערכות הפנים־ארגוניות, כאשר ארגונים רבים השקיעו מאמצים בהקשחת מעטפת ההגנה החיצונית שלהם, בעוד שהאבטחה הפנים־ארגונית לא זכתה לתקצוב ולהשקעה מספיקים. חוסר האיזון בהשקעה מביא לכך שכאשר תוקף מצליח לחדור ולהיכנס לתוך הארגון, ביכולתו להתפשט ולפעול בו בקלות רבה.

ב. **הקשחה ועיבוי של מנגנוני ההגנה בין הארגונים ובין ספקי המשנה שלהם** – קיים קושי רב בהגנה על הקשר בין ארגונים וחברות ובין ספקי משנה של שירותים ומידע, קל וחומר כשעוסקים בחברות המספקות שירותי מחשוב מבוססי ענן. חלק מספקי המידע במגזר הבנקאי הם בין־לאומיים (לדוגמה, חברת "בלומברג" וחברת "רויטרס"), והיכולת להשפיע על מערכי הגנת המידע שלהם היא נמוכה יחסית. יכולת ההשפעה והשליטה של בנקים ורגולטורים בישראל על מערך האבטחה של ספקים ישראליים היא גבוהה יותר, אך מחייבת קביעת תקנים ברורים למערכי אבטחת המידע הנדרשים מספקי משנה כאלה, המתחברים באופן ישיר למערכות הליבה הבנקאיות. במקביל, יש לחזק את מערכי ההגנה

במערכות הפנימיות של הבנקים והגופים הפיננסיים ולהקטין ככל האפשר את חשיפתן לספקי משנה.

ג. **פריסת מערך הגנה אחורי הדומה במאפייניו למערך ההגנה הקדמי** – יש לבנות מערך ניטור והגנה מול ספקי המשנה, הזהה במאפייניו למערך ההגנה הקדמי של החברה, כולל הקמת מרחב DMZ,[19] מערך הזדהות חזק הכולל הזדהות כפולה, מערך סינון מידע, מערך "ארגזי חול"[20] לבחינת תוצאות של התקנות עדכוני תוכנה, ומערך ניטור הכולל שמירת הנתונים לפרק זמן ארוך וניטור רציף של הקשר מול ספקי המשנה. מערך הגנה זה אמור להיפרס גם מול החברות הבנות של החברה האם. העבודה מול החברות הבנות, שלהן מערכי הגנה נפרדים ומערכות תוכנה נפרדות, מסכנת את החברה האם בדיוק כמו עבודה מול ספק משנה.

מסמך של מערך הסייבר הלאומי בנושא "סיכונים במיקור חוץ ושרשרת אספקה"[21] מפרט את הסיכונים הייחודיים לשרשרת האספקה:

א. הכנסה של תוכנה או חומרה הנגועה בנוזקה.
ב. ביצוע פעולה זדונית על ידי גורם תחזוקה.
ג. ביצוע פעולה זדונית באמצעות ערוץ התחזוקה מרחוק.

המסמך מציע אמצעים למזעור הסיכון הכרוך במיקור חוץ בשרשרת האספקה:

א. שילוב הסיכון בניהול הסיכונים הארגוני.
ב. פיקוח על גורמי התחזוקה, למשל באמצעות ניטור פעולתם ברשת, ליווי צמוד שלהם בעת שהותם בארגון, הצמדת תג זיהוי לגורם הנכנס, וכדומה.
ג. ניטור ערוץ התחזוקה מרחוק וניתוקו בזמנים שאין בו צורך.
ד. הסתרת יעד הקצה הספציפי במסגרת רכש עבור ארגונים גדולים. לדוגמה, כאשר רוכשים עבור ארגון גדול מאוד, שחלקים ממנו הם רגישים, ניתן לא לציין בהזמנה למי בדיוק באותו ארגון מיועד הרכש.

מסמך של SANS Institute מתייחס להיערכות הנדרשת בארגון נוכח סיכוני הסייבר הנוצרים משרשרת האספקה.[22] התרשים שלהלן, הלקוח מהמסמך, מתאר את סביבת שרשרת האספקה האופיינית לארגון:

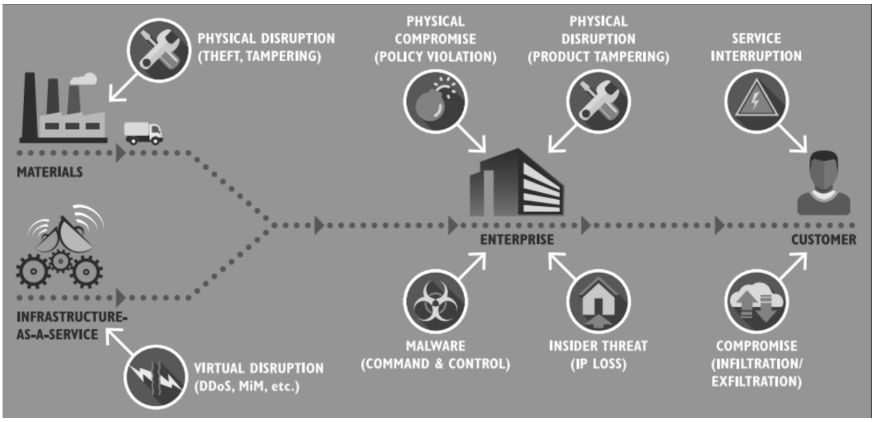
---

19 אזור המשמש כהגנה על רשת ה־LAN הארגונית, ונמצא בין ה־LAN לבין היציאה ל־WAN או אינטרנט.

20 סביבה שבה מאפשרים למשתמשים לפעול מבלי לחשוש לנזקים העלולים להיגרם למערכת ההפעלה.

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

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



תרשים 6: סביבת שרשרת האספקה האופיינית לארגון

המסמך מציע לארגונים לבנות תוכנית לניהול ספקים, המבוססת על ארבעה מרכיבים:

א. זיהוי והגדרת הספקים החשובים.
ב. הגדרה מדויקת של ההסכמים עבור כל ספק.
ג. יישום של ההנחיות והבקרות.
ד. אינטגרציה ארגונית.

התרשים שלהלן מציג את המרכיבים של התוכנית לניהול ספקים:

תרשים 7: מרכיבי תוכנית ניהול ספקים

המסמך של SANS Institute גם מציע לארגונים לפעול על פי מיטב הניסיון שנרכש (בהיבטי כוח אדם, תהליכים וטכנולוגיה) במטרה להקטין את חשיפתם לסיכוני שרשרת האספקה. להלן תרשים הלקוח מהמסמך המפרט הצעה זו:

תרשים 8: ניהול אנשים, תהליכים וטכנולוגיה

לבסוף, המסמך מסכם את המרכיבים העיקריים של התוכנית לאבטחת שרשרת האספקה, על פי חלוקה למרכיבים בסיסיים ולמרכיבים מקיפים בשלושת התחומים – כוח אדם, תהליכים וטכנולוגיה – כמפורט להלן:

המרכיב	בסיסי	מקיף
כוח אדם	בדיקות רקע	דרישות אבטחה המופיעות בחוזים
תהליכים	סקרים בסיסיים וסקרי בקרות וסיכונים אצל הספקים	יישום תוכנית מלאה לניהול ספקים
טכנולוגיה	סגמנטציה (הפרדה) של רשתות וניטורן	Code Review ובדיקת פגיעויות אצל גורמי צד שלישי, ניטור מעמיק, ניתוח איומי אבטחה והתבססות על מודיעין

סיכום

האיומים על הארגון באמצעות תקיפת שרשרת האספקה שלו יכולים להתבצע באמצעות ערוצי תקיפה מגוונים, כגון חדירה למערכות של ספק בעל רמת הגנה נמוכה יחסית (אך בעל גישה למערכות הארגון), וביצוע חדירה דרכו למערכות אלו, וכן שימוש בעדכוני תוכנה לגיטימיים להפצת נוזקה, וכדומה. אין מדובר באיומים תיאורטיים, אלא באיומים המתבססים על מספר רב של אירועים שהתרחשו בפועל בארץ ובעולם, שמהותם הייתה פגיעה בארגונים תוך ניצול שרשרת האספקה שלהם.

מורכבות האיומים, המגוון הרחב של התרחישים האפשריים והתעצמות התוקפים מחייבים את הארגונים לנקוט צעדים הגנתיים משמעותיים כדי להתמודד עם האתגר ולצמצם את הסיכונים שהוא מציב.

פרק ד': מתודולוגיות ומודלים לניהול שרשרת אספקה

נבחנו מספר מודלים ומתודולוגיות לניהול סיכונים בשרשרת האספקה כמפורט בהמשך. כך, למשל, הספר *Purchasing and Supply Chain Management* מתאר שלוש קטגוריות של ספקים:[23]

א. ספקים אסטרטגיים – ספקים בעלי חשיבות גבוהה מאוד לחברה הרוכשת, שיש קושי רב במציאת תחליף להם.

ב. ספקים מועדפים – ספקים בעלי חשיבות לחברה הרוכשת, אולם כאלה שניתן להחליפם תוך השקעת מאמץ מסוים.

ג. ספקים בני החלפה – ספקים שניתן להחליפם תוך זמן קצר.

בנוסף לחלוקה המוצעת של סוגי ספקים, להלן סקירה של מספר מודלים של ניהול שרשרת אספקה בגופים רלוונטיים לענייננו.

Deutsche Telekom

המתודולוגיה בה משתמשת חברת Deutsche Telekom לניהול שרשרת האספקה של יותר מ־30,000 הספקים שלה בלמעלה משמונים מדינות, היא מתודולוגיה בת ארבעה שלבים.[24] 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 מדיניותם בנושאים כגון זכויות אדם, שחיתות, הגנת הסביבה ובריאות תעסוקתית. כל הספקים מחויבים לעבור בחינה חוזרת לאחר שלוש שנים. ככל שהיחסים העיסקיים נמשכים, החברה מבקשת מהספקים הרלוונטיים, שהם בעלי חשיבות אסטרטגית ו/או נמצאים בסיכון גבוה, להעביר אליה מידע נרחב על שיטות העבודה שלהם באמצעות מערכות המידע.

בשלב השני מתבצעת הערכה של הצהרות הספקים על בסיס מידע רקע נוסף ומחקר ממוקד. ספקים בעלי סיכון גבוה יותר נדרשים לספק מידע נוסף, וכן נערכות ביקורות באתרים שלהם. יעילות הביקורת היא גבוהה, שכן היא מונעת ביקורות

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

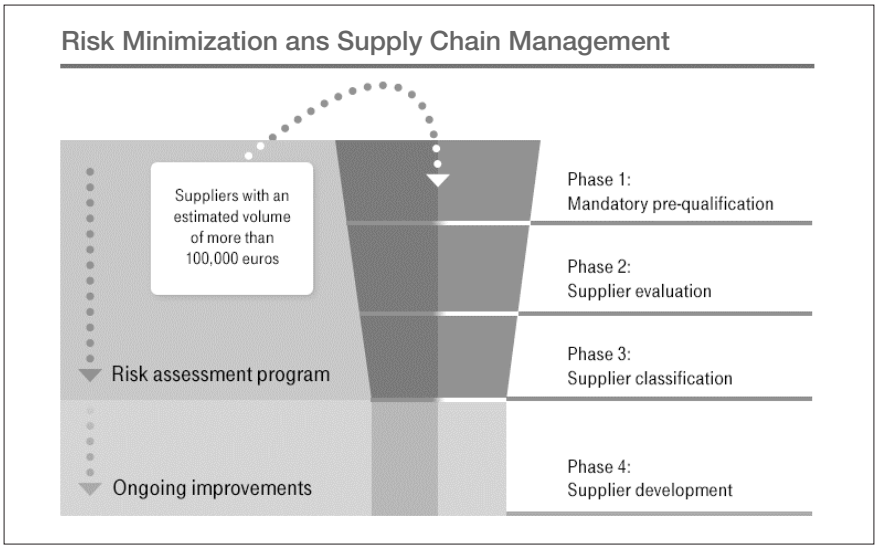
24 "Corporate Responsibility Report", *Deutsche Telekom*, 2017.

נוספות ומיותרות בשל שיתוף פעולה עם 13 חברות נוספות, במסגרת Joint Audit Cooperation (JAC).

בשלב השלישי הספקים מסווגים ומוערכים בהתבסס על המידע המתקבל מהם ועל תוצאות הביקורות. Deutsche Telekom משתפת פעולה באופן הדוק עם כל הספקים שלה כדי לטפל בבעיות חריפות שזוהו.

בשלב הרביעי מגובשת תוכנית פיתוח מקצועי לספקים ונערכות סדנאות. במקרים של התעלמות משמעותית של הספק מדרישות החברה, מתחיל תהליך שנועד לגבש פתרון מהיר למצב, וזאת בהתאם לנהלים הפנימיים של Deutsche Telekom.

תוצאות הערכות הספק והצעדים שננקטו לפתרון הבעיות שנחשפו נרשמות בחברה ומנוהלות על ידה. להלן תרשים המתאר את המתודולוגיה של Deutsche Telekom לניהול מערכת האספקה:



תרשים 9: הקשנת הסיכון וניהול שרשרת האספקה

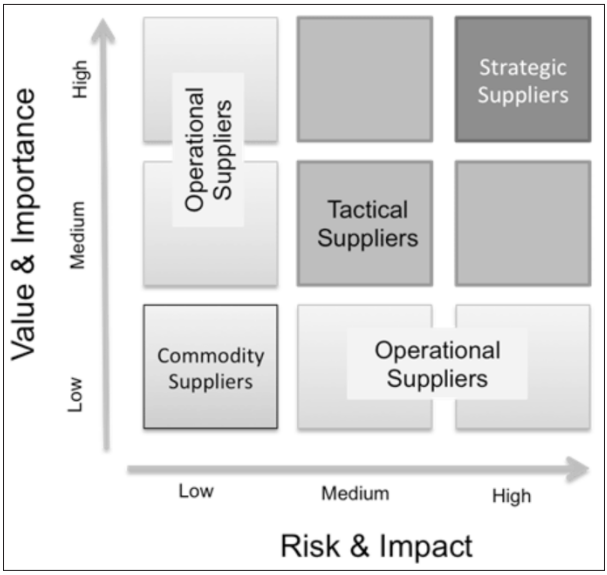
Information Technology Infrastructure Library

מסמך של ארגון Information Technology Infrastructure Library (ITIL) מציג מודל דו־ממדי לסיווג ספקים.[25] ממד אחד הוא הסיכון והשלכותיו (Risk and Impact) והממד השני הוא "ערך וחשיבות" (Value and importance). ככל שערך הממדים של ספק מסוים גבוה יותר, כך הספק הוא משמעותי יותר. המודל מסווג

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

את הספקים לארבעה סוגים של אספקה:,Commodity, Operational, Tactical, Strategic.

להלן תרשים המתאר סיווג זה והלקוח מהמסמך:



תרשים 10: מודל ITIL לסיווג ספקים

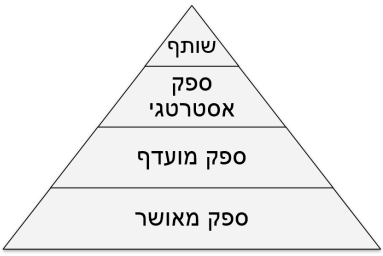
United Utilities

מתודולוגיה המציגה מודל פירמידלי פשוט יותר לסיווג ספקים משמשת את חברת United Utilities – חברה לאספקת מים בצפון־מערב אנגליה, המספקת כ־1,700 מיליון ליטר מים מדי יום.[26]

המודל מחלק את הספקים לארבעה סוגים: שותף, אסטרטגי, מועדף ומאושר. ככל שהתלות בספק, המורכבות של מוצריו ועלותם גבוהות יותר, כך הספק מוגדר כמשמעותי יותר. המודל מאפשר להגדיר את דרישות החברה מהספק כנגד מדדי ביצוע של לקוחות, רגולציה, הפן המשפטי, קיימות, יעילות, בטיחות וכדומה.

להלן תרשים המתאר את המודל:

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

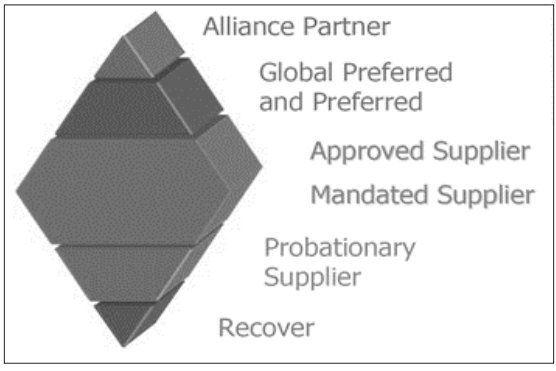


תרשים 11: מודל United Utilities לסיווג ספקים

Amway

מתודולוגיה נוספת לסיווג ספקים מופיעה במודל של הפורטל האירופי לספקים (Amway – Europe Supplier Information Portal).[27] על פי מתודולוגיה זו, סוג היחסים שמתפתח בין ספק ללקוח תלוי בחשיבות האסטרטגית של המוצרים או השירותים המסופקים, וכן בכישורים, ביכולות ובביצועים של הספק.

על פי המודל, כל ספק נמדד על פי קריטריונים ומסווג בהתאם להם. הדבר מבטיח קיומן של פעילויות ממוקדות לכל ספק, שתוכננו במיוחד עבורו כדי לפתח, לשפר או לייעל את ביצועיו התפעוליים. הקריטריונים על 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 קריטריונים אלה אצל הספק והתוצאות שינבעו מהם יסייעו לגבש תוכניות ספציפיות עם אותו ספק כדי שיגיע לרמות הביצוע התפעולי הנדרשות לצרכי העסק. התרשים שלהלן מציג את סיווג הספקים על פי המודל של Amway:



תרשים 12: מודל Amway לסיווג ספקים

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

סיכום

המתודולוגיות והמודלים שפורטו לעיל לטיפול בספקים ולסיווגם עוסקים ברמה הארגונית בלבד. לא אותרו מתודולוגיות ומודלים לסיווג ספקים ברמה הלאומית והמגזרית, או לחילופין לסיווג ספקים בהיבטי סייבר.

פרק ה': דוגמאות לגישות רלוונטיות במשק הישראלי

במסגרת המחקר נסקרו מספר גישות הקיימות במשק הישראלי בהקשרי ניהול וסווג ספקים במטרה לבחון באיזו מידה ניתן ללמוד מהן לגבי פיתוח מתודולוגיה מתאימה.

רישום וסיווג קבלנים

רישום וסיווג קבלני בניין במדינת ישראל הוא דוגמה לקטגוריזציה המבוצעת ברמה הלאומית לספקים מענף הבנייה. רישום קבלנים לעבודות הנדסה בנאיות מבוצע על ידי רשם הקבלנים[28] במשרד הבינוי והשיכון. רשם הקבלנים ממונה על ידי שר הבינוי והשיכון ופועל מכוח חוק.[29] מטרת רישום הקבלנים היא לקבוע כי עבודות הנדסה בנאיות יבוצעו רק על ידי מי שזכאי להירשם בפנקס הקבלנים ועומד בהוראות החוק.

תפקידי רשם הקבלנים הם:

א. ניהול פנקס הקבלנים – רישום קבלנים, ביטול רישום, שינוי או העלאת סיווג של קבלנים.
ב. הנפקת רישיון קבלן דו־שנתי.
ג. ניהול הליכי משמעת נגד קבלנים המפֵרים את הנוהג המקובל ועוברים עבירות שיש עימן כדי לערער את מהימנותם.
ד. טיפול בתלונות על קבלנים – בדיקת תלונות על קבלן רשום והטלת אמצעי משמעת במקרים שבהם עלה כי הקבלן עבר עבירה והפר תקנה מתקנות רישום הקבלנים לעבודות הנדסה בנאיות (ערעור מהימנות והתנהגות בניגוד למקובל).
ה. אכיפה נגד קבלנים העוברים על החוק – איסוף מידע על קבלנים שאינם רשומים בפנקס הקבלנים והפועלים באתרי בנייה בניגוד לחוק, והגשת חומר החקירה לתובע מטעם הרשות המקומית שבה בוצעה העבירה.

---

28 "רשם הקבלנים", *משרד הבינוי והשיכון*, http://www.moch.gov.il/rasham_hakablanim/Pages/rasham_hakablanim.aspx .

29 "חוק רישום קבלנים לעבודות הנדסה בנאיות", *משרד הבינוי והשיכון*, תשכ"ט-1969.

תקנות ייעודיות[30] קובעות את הענפים הראשיים ואת ענפי המשנה של ביצוע עבודות הנדסה בנאיות. לדוגמה, ענף ראשי "כבישים, תשתיות ופיתוח", ובתוכו הענף המשני "עבודות אספלט".

החוק קובע כי עבודות הנדסה בנאיות, החורגות בהיקפן הכספי או במהותן המקצועית מן התחום שנקבע בתקנות, חייבות להתבצע רק בידי קבלן הרשום בפנקס הקבלנים וקיבל רישיון מאת הרשם. לפיכך, קבלן המבצע עבודות בענף ראשי בהיקף כספי מוגדר,[31] או קבלן המבצע עבודות בענף משנה בהיקף כספי מוגדר,[32] חייבים להיות רשומים בפנקס הקבלנים. החוק גם מגדיר את התנאים לרישום בפנקס הקבלנים, בכפוף לקריטריונים כגון השכלה ושנות ניסיון. כמו כן, קובע החוק את התנאים לפסילת רישום או מחיקתו. הן קבלן יחיד והן חברה יכולים להירשם בפנקס הקבלנים.

תקנות אחרות של משרד הבינוי והשיכון[33] קובעות חמש דרגות סיווג לפי ענפים לקבלנים הרשומים בפנקס הקבלנים. כל דרגת סיווג מתייחסת להיקף הכספי של עבודת הקבלן בענף שבו הוא רשום (בבנייה למגורים ההתייחסות היא גם להיקף הבנייה במ"ר). סוג 1 הוא הסיווג הנמוך ביותר וסוג 5 הוא הגבוה ביותר. כמו כן קובעות התקנות את התנאים לשינוי סיווג, את העילות לאי־שינוי הסיווג, את אופן הגשת הבקשה לסיווג, ועוד.

בתום 12 חודשים מתאריך אישור סיווגו של הקבלן, ואם הוכח כי סיים עבודות בהיקף הדרוש, הוא רשאי לפנות לרשם הקבלנים בבקשה להעלות את סיווגו בדרגה אחת. כדי להעלות את הסיווג נדרש הקבלן להוכיח כי בעבודותיו עמד בשמונים אחוזים לפחות מההיקף הכספי המרבי על פי סיווגו, או במקרה של בנייה למגורים – על שמונים אחוזים מן ההיקף במ"ר של תקרת הסיווג שלו הוא מורשה.

רישום ספקי משרד הביטחון

התהליך הנדרש כדי להיות סַפָּק של משרד הביטחון דומה לתהליך שכל ארגון גדול במשק הישראלי אמור לנקוט בטיפולו בספקים. המרכז לשילוב ובקרת ספקים במינהל ההרכשה והייצור של משרד הביטחון מנהל את מאגר הספקים של המשרד ונושא באחריות לבחינת עמידתם בקריטריונים השונים ובדרישות לאבטחת האיכות.

30 "תקנות רישום קבלנים לעבודות הנדסה בנאיות (קביעת ענפים וחלוקת ענפים לענפי משנה)", *משרד הבינוי והשיכון*, תשנ"ג-1993.

31 מעל 83,399 ₪ (נכון למארס 2018).

32 מעל 43,583 ₪ (נכון למארס 2018).

33 "תקנות רישום קבלנים לעבודות הנדסה בנאיות (סיווג קבלנים רשומים)", *משרד הבינוי והשיכון*, תשמ"ח-1988.

המרכז לשילוב ספקים גם אחראי לרישומם של הספקים במערכת ולהשמתם מול הגופים השונים במערכת הביטחון (למעט ספקי אגף הבינוי ואגף הכספים).

כחלק מעבודתו, מנהל המרכז לשילוב ובקרת ספקים את "קובץ הספקים המרכזי", המכיל את רשימת כל ספקי משרד הביטחון. רשימה זו כוללת את כל הספקים שעברו את תהליכי הבדיקה וקיבלו את כל האישורים הנדרשים ורשומים כ"ספק מוכר". בנוסף, מבצע המרכז לשילוב ובקרת ספקים מעקב שוטף אחר ביצועיו של הספק, בהתאם לקריטריונים של עמידה בלוחות זמנים, תוצאות של בדיקות הקבלה ובחינת המוצר הסופי, וכן יחסי הגומלין בין הספק למשרד הביטחון ולצה"ל. על סמך קריטריונים אלה נקבע לספק ציון משוקלל לביצועיו ("הערכת ביצועים") שיכול לשמש כתנאי סף במכרזים.

ספק המבקש לקבל מעמד של "ספק מוכר" של משרד הביטחון צריך לפנות למרכז לשילוב ספקים במנה"ר – היחידה לשילוב ובקרת ספקים[34] בבקשה להיכלל ברשימת הספקים המוכרים. הטיפול בבקשה מתבצע בתהליך הכולל מספר שלבים קבועים, בהתאם לנוהלי המרכז. בסיום התהליך מוגשת הבקשה לוועדה במשרד הביטחון המוסמכת לכך, כדי שתחליט בעניין התאמת הספק, וכל זאת בהתאם להוראות משרד הביטחון.

כדי להבטיח את איכות תהליכי עבודתו, כל ספק של משרד הביטחון נדרש להנהיג במפעלו מערכת אבטחת איכות שאושרה על ידי משרד הביטחון כעונה לדרישותיו בתחום אבטחת האיכות. דרישות אלו מבוססות ברובן על תקן ISO 9000.

בדיקת התאמה ביטחונית

תהליך הבדיקה להתאמה ביטחונית[35] למועסקים במשרות מסווגות הוא דוגמה לתהליך תשתיתי המבוצע/מונחה על ידי גורם מרכזי אחד (היחידה הממלכתית לקביעת התאמה ביטחונית בשירות הביטחון הכללי) עבור מועסקים בגופים רבים.

לפי סעיף 7 (ב) (3) וסעיף 15 לחוק שירות הביטחון הכללי התשס"ב-2002 והתקנות והכללים שמכוחו של חוק זה, שירות הביטחון הכללי הוא הגורם המוסמך במדינת ישראל לקבוע התאמה ביטחונית של אדם לתפקיד או למשרה שסווגו בסיווג ביטחוני. בדיקת ההתאמה הביטחונית מתבצעת לקראת שירות צבאי ובמהלכו (כולל שירות מילואים), לפני קבלה לתפקיד ו/או משרה מסווגים, לפני מעבר לתפקיד ו/

34 "רישום ספק", *משרד הביטחון*, www.mod.gov.il/Service_Business/sapakim/supplierinfo/Pages/registration-.aspx

35 האמור מהווה תוכן בלתי מסווג הלקוח מטופס "בדיקת התאמה ביטחונית – עלון מידע לנבדק", הזמין באינטרנט באתר השב"כ.

או משרה בעלי סיווג ביטחוני גבוה יותר, וכן במסגרת בדיקות ביטחון חוזרות למי שנמצא בתפקיד מסווג.

תכליתה של בדיקת ההתאמה הביטחונית היא להבטיח שבתפקידים ובמשרות שהוגדרו כמסווגים יועסקו אנשים המתאימים מבחינה ביטחונית, וזאת כדי להגן על סודות המדינה ועל אישים ומתקנים מאובטחים. בדיקת ההתאמה הביטחונית מונחית ו/או מבוצעת על ידי שירות הביטחון הכללי, אולם חלקים מסוימים של הבדיקה, כמו התחקור הביטחוני (ראיון) והליכים נוספים מבוצעים לרוב על ידי הגוף אליו מיועד המועמד או מועסק בו. גם פעולות אלו נעשות בכפוף ובהתאם להנחיות שירות הביטחון הכללי.

הליך בדיקת ההתאמה הביטחונית עשוי לכלול מרכיבים שונים, כגון: מילוי שאלונים, תחקור ביטחוני, בדיקה רפואית, אבחון פסיכולוגי, בדיקות מהימנות, בדיקות פוליגרף, עיון במאגרי מידע של גופים ציבוריים ופעולות נוספות, כמו פנייה לאנשים המכירים את המועמד מהעבר ו/או בהווה. מרכיבי בדיקת ההתאמה הביטחונית משתנים מבדיקה לבדיקה, בהתאם לצורך ולשיקול דעתם של בודקי ההתאמה הביטחונית. ייתכן שבמסגרת הליך הבדיקה, בני משפחה מדרגה ראשונה של המועמד יידרשו לעבור גם הם בדיקות שונות, לרבות תחקור ביטחוני ובדיקת פוליגרף, לצורך קביעת ההתאמה הביטחונית של המועמד.

פעולות בתחום הסייבר

שתי פעילויות נוספות המבוצעות בישראל הן בעלות הקשר ישיר לעבודה זו:

א. פעילות המתקיימת במערך הסייבר הלאומי לפיתוח מתודה להגנה על שרשרת האספקה. מתודה זו צפויה לכלול שאלון לספקים, שיטה לביקורת ולבקרה והנגשתם באמצעות פורטל. הכוונה היא שהשימוש במתודה ובפורטל יתפתח באמצעות כוחות השוק ולא כחובה המוטלת על הספקים. נכון לכתיבת דוח זה, הפעילות נמצאת בשלבי פיילוט לקראת יישומה בהיקף נרחב.

ב. פעילות המבוצעת במערך סייבר, חירום וביטחון במשרד האוצר על ידי היחידה להסדרת סייבר ורציפות בשרשרת האספקה הפיננסית.[36] ייעודה של פעילות זאת הוא להבטיח את חוסן המערכת הפיננסית בפני סיכוני סייבר ואת הרציפות בשרשרת האספקה, לשמור על יציבות המערכת ולעמוד ביעדי השירות לציבור ולממשלה. ההסתייעות בפעילות היחידה להסדרת סייבר ורציפות שרשרת האספקה מול הספקים של המערכת הפיננסית היא וולונטרית ואינה כרוכה בעלות. פעילות היחידה מול הספקים כוללת סקירת פעילותם, מיפוי והערכת

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

סיכונים, מיפוי הבקרות הקיימות אצלם והערכתן, וגיבוש תוכנית להפחתת הסיכונים. מדובר בפעילות חדשה יחסית מול ספקי המערכת הפיננסית, הנמצאת בשלביה המוקדמים.

סיכום

במספר תחומים במשק הישראלי קיימות גישות ומתודות שונות לאבטחת שרשרת האספקה, שהן בעלות קשר אפשרי לנושא עבודה זו. המודלים הקיימים עוסקים בסיווגים ברמה הלאומית לספקים מענף מִשקי מסוים (למשל, סיווג קבלני בניין) ובתהליך תשתיתי המבוצע/מונחה על ידי גורם מרכזי אחד (למשל, היחידה הממלכתית לקביעת התאמה ביטחונית בשירות הביטחון הכללי) עבור מועסקים בגופים רבים. גם במרחב הסייבר החלה פעילות ברמה הלאומית לפיתוח מתודה לאבטחת שרשרת האספקה והנגשתה בפורטל, אך פעילות זו נמצאת רק בתחילת תהליך המימוש שלה, ולפיכך מוקדם להתייחס אליה כדוגמה מעשית. גם הפעילות של יחידה ייעודית במשרד האוצר למגזר הפיננסי בישראל נמצאת בשלבי יישום ראשוניים מול ספקיה של המערכת הפיננסית.

פרק ו': ניתוח חלופות

עד כה הציג מסמך זה מגוון של התייחסויות לנושא ניהול איומי סייבר בשרשרת האספקה. זאת, תוך התייחסות למתודולוגיות שפותחו בעולם, לתהליכים רלוונטיים המתקיימים בתאגידי ענק גלובליים ולגופי מחקר, גופי תקינה וגופים רגולטוריים מדינתיים.

הקו המנחה בניסוח המענה הלאומי לאיומי סייבר בשרשרת האספקה במגזר הפיננסי במדינת ישראל הינו הצורך בשיפור הגנת הסייבר הכוללת במגזר זה, הנשען כיום בפעילותו על מגוון ספקים מהותיים. אחד המרכיבים הקריטיים בניהול סיכונים בשרשרת האספקה הוא היכולת לסקור את סיכוני הסייבר אצל מגוון הספקים של המגזר הפיננסי ולבנות תוכנית עבודה שתאפשר לסגור פערים קיימים באמצעות בקרות מתאימות.

ככלל, עבודה זו מבקשת להתמקד בגיבוש תהליך רוחבי, אשר יאפשר לספקים לקבל הסמכה מגוף בוחן מרכזי. ההסמכה תבוצע על פי מדרגים שונים, בהתאם למאפייני הספק ודרישות הבנקים. באופן זה יישענו הגופים הפיננסיים על עבודת הגוף הבוחן מצד אחד, ולספקים ייחסכו ביקורות חוזרות ונשנות, כל פעם על ידי לקוח אחר, מצד שני.

ניתוח סיכוני שרשרת האספקה מצביע על קיומו של אתגר מרכזי הנוגע ליכולתם של גורמי המגזר הפיננסי לסקור לכל הפחות את ספקיהם המהותיים בהתאם למידת החשיבות של פעילותם בארגון. סקירה זו יכולה להוות הבסיס בלבד. ארגונים פיננסיים יוכלו להרחיב את הדרישות מספקים מהותיים בשרשרת האספקה, ובכלל זה דרישות מחמירות ואף דרישה להתקנה של מערכות ניטור נוספות אצל הספק.

חלופות

את הסקירה הנדרשת מול ספקי המערכת הפיננסית[37] בהיבט של התמודדותם עם סיכוני סייבר בשרשרת האספקה, ניתן לבצע באמצעות שתי חלופות תפעוליות עיקריות:

37 פעילות זו כוללת, לכל הפחות, העברת הדרישות לספק וביצוע סקרים שוטפים אצלו כדי לוודא את עמידתו בדרישות. במידת הצורך, ניתן לשקול הוספת אמצעי בקרה, ניטור ודיווח נוספים על הספקים.

א. **ניהול עצמי על ידי כל בנק** – זהו למעשה המצב הנוהג כיום בו כל בנק פועל באופן עצמאי מול ספקים בשרשרת האספקה שלו. כל בנק גם קובע כיום את מערכת הדרישות שלו מכל ספק או קבוצת ספקים.
ב. **ניהול מרכזי (עבור כל/רוב הבנקים)** – ניהול מרכזי של סקירת ספקים, תוך קביעת רשימת דרישות מוסכמת על הבנקים, בהתאם לסיווג הספקים. רשימת הדרישות תוכל להתבסס על תקינה מקובלת או על הצעת מערך הסייבר הלאומי לסיווג ספקים, המקודמת בימים אלה.

בחינת שתי החלופות נוגעת למספר היבטים, ביניהם בולטים: שיפור ביטחון הסייבר; ההיבט הכלכלי; שאלת ההגבלים העיסקיים; צירוף ספקים חדשים.

שיפור ביטחון הסייבר במערכת הפיננסית

ההיבט הראשון בניתוח נוגע לשאלה: איזו חלופה תגדיל את רמת ביטחון הסייבר ואת היציבות של המגזר הפיננסי בישראל? לאור הניתוח שבוצע בעבודה זו, התשובה לשאלה ברורה: לניהול מרכזי של סקירת ספקים יש יתרונות במגוון היבטים:

א. גוף מקצועי מתמחה יוכל לפתח ידע באופן שיטתי ולשפר ולשכלל את יכולותיו עבור כלל המגזר.
ב. סקירת ספקים אחודה תאפשר קביעה של ספי ביטחון סייבר נדרשים עבור כלל המגזר, תוך נרמול הדרישות מספקים בשרשרת האספקה. בכך היא תסייע משמעותית ליציבות המערכת הפיננסית בהקשרים של שרשרת האספקה.
ג. גוף מרכזי יאפשר העמקת הדרישות של הבנקים מהספקים ויכולת טובה יותר לכפות עליהם יישום ומימוש בקרות משופרות.
ד. הדבר יאפשר הקטנה משמעותית של העומס על הספקים, המתמודדים כיום עם סקירה ודרישות נפרדות של לקוחות שונים במגזר הפיננסי.
ה. איגום משאבים יאפשר שיפור משמעותי באיכות סקירת הספקים ובעומקה וכתוצאה מכך גם ברמת ניהול סיכוני הספקים.

ההיבט הכלכלי

רכיב נוסף אותו ראוי לבחון בתהליך גיבושה של שיטה להתמודדות עם סיכוני סייבר בשרשרת האספקה נוגע להיבטים הכלכליים, שיש להם משמעות לכלל המגזר הפיננסי. להלן מספר נתונים והנחות עבודה לצורך ניתוח שתי החלופות דלעיל:

א. בנק גדול נדרש להפעיל באופן שוטף כחמישה סוקרים כדי לבדוק את ספקיו המהותיים. מספר זה מאפשר לבנק לסקור כחמישים אחוזים מהספקים בכל שנה.[38]

38 מבוסס על תחשיב שנעשה באחד הבנקים הגדולים בישראל.

ב. רוב הספקים המהותיים של המגזר הפיננסי נותנים שירות לכל/רוב הבנקים. לצורך החישוב נניח כי שמונים אחוזים מהספקים המהותיים במגזר זה הם ספקים משותפים.[39]

ג. לפי רשימת התאגידים הבנקאיים בישראל,[40] המפורסמת על ידי בנק ישראל, קיימים בישראל 15 בנקים מסחריים (ועוד בנק מסחרי אחד שמונה לו מפרק זמני). מדובר במספר בנקים גדולים ובינוניים ועוד כמה בנקים קטנים יותר.

לאור הנאמר ניתן להניח את ההנחות הבאות:

א. אם כל בנק ינהל את פעילות הסקירה בעצמו, מספר הסוקרים המוערך שהמגזר הבנקאי יצטרך להפעיל יהיה כ־24.[41] מספר סוקרים זה יכסה (סטטיסטית) את מרבית הספקים המהותיים בכל שנה. זאת, בהנחה שכל בנק יבדוק כמחצית מספקיו. אולם, מאחר ואין תיאום בין הבנקים, יש להניח כי במהלך השנה יסוקרו מרבית הספקים של המגזר. לפיכך יידרשו במקרה זה כ־24 סוקרים במגזר הבנקאי כולו לכיסוי הפעילות מול כלל הספקים המהותיים.

ב. אם ניהול הסקירות יהיה מרכזי, מספר הסוקרים שהמגזר הפיננסי יצטרך להפעיל יהיה שישה (חמישה סוקרים לספקים המשותפים ועוד סוקר אחד לספקים ייחודיים לבנק ספציפי או למספר קטן של בנקים). מספר סוקרים זה יכסה כמחצית מהספקים בכל שנה. כדי לכסות את כל הספקים, ידרשו כ־12 סוקרים בכל המגזר הבנקאי לכיסוי הפעילות מול כלל הספקים המהותיים. מדובר בחיסכון פוטנציאלי ישיר של כ־12 סוקרים לעומת המצב הצפוי בחלופה הקודמת. לכך יש להוסיף חיסכון בתקורות תפעול וניהול.[42]

הגבלים עיסקיים

היבט נוסף המחייב בחינה נוגע לשאלת ההגבלים העיסקיים. בהקשר זה יש לבחון באיזו מידה פעולה משותפת של הבנקים למול ספקים בשרשרת האספקה תפגע בהגבלים העיסקיים החלים על הבנקים. מהניתוח שבוצע במסגרת עבודה זו עולה שהקמת גוף סוקר מרכזי אינה מהווה פגיעה בהגבלים העיסקיים, וזאת לאור ההיבטים הבאים:

---

39 מבוסס על הערכה שנעשתה בתיאום עם אחד הבנקים הגדולים בישראל.

40 "רשימת תאגידים בנקאיים בישראל – כתובות וקישורים", *בנק ישראל*, http://www.boi.org.il/he/BankingSupervision/BanksAndBranchLocations/Pages/IsraeliBanks.aspx.

41 אומדן זה בוצע באמצעות התחשיב הבא: חמישה סוקרים לכל בנק גדול × שני בנקים גדולים (סה"כ עשרה סוקרים) ועוד שלושה סוקרים לבנק אחד בינוני־גדול ועוד שני סוקרים לכל בנק בינוני × שני בנקים בינוניים (סה"כ ארבעה סוקרים) ועוד שבעה סוקרים לכל עשרת הבנקים הקטנים יותר (חצי משרה עד משרה לכל בנק). סה"כ 7+4+3+10=24 סוקרים.

42 ראו ניתוח רגישות בנספח.

א. ההגבלים העיסקיים צריכים לחול על היבטים של תחרות עיסקית, ואילו הקמה של גוף סקירה מרכזי אינו נוגע למרכיב זה, וכל עניינו הוא שיפור רמת הביטחון והיציבות של המערכת הפיננסית בכללותה.
ב. בתהליך הסקירה ניתן יהיה לוודא שמידע רגיש של בנקים אינו משותף לגורמים אחרים – דבר המתרחש כבר כיום במרכז הסייבר הפיננסי בבאר שבע, כמו גם בארגונים של המערכת הפיננסית בעולם, דוגמת FFIEC ואחרים.

ברור שבתהליך הקמתו של גוף מרכזי לסקירת ספקים נדרש יהיה להסדיר את מגוון המגבלות שיחולו על תהליך הסקירה עצמו. להבנתנו, ניתן יהיה להגיע להסדרה כזאת באופן שייתן מענה לרגולטורים השונים.

צרוף ספקים חדשים

כבר כיום מתמודדים הבנקים עם תהליכים ארוכים הקשורים בצירוף ספקים חדשים למערכת. תהליכים אלה נמשכים חודשים ארוכים, פוגעים ביכולות הפעולה התקינה של הבנקים ואף ביכולות ההטמעה של ידע חדש במגוון נושאים. הפעלה של גוף מרכזי לסקירת ספקים, ובכללם חדשים, תוכל לאפשר קיצור התהליך ואף ליצור מצב בו גופים יוכלו לבקש סקירה והסמכה מראש של ספקים פוטנציאליים בכל מה שנוגע לביטחון סייבר במערכת הפיננסית.

סיכום

הקמת גוף מרכזי לסקירת ספקים תשפר מהותית את רמת ביטחון הסייבר של המגזר הפיננסי ותאפשר פיתוח ידע מתמיד. הדבר מקנה עדיפות מובהקת לניהול הנושא באופן מרכזי עבור כל הבנקים המסחריים. זאת ועוד, ניהול מרכזי כזה יחזק את השפעתו ועוצמתו של הגוף הסוקר המרכזי כלפי הספקים (בשל היותו מייצג את כל/רוב הבנקים ולא רק בנק מסוים), יאפשר התמקצעות טובה של צוות הסוקרים (גוף מתמחה ברמה המגזרית), יקטין תקורות (תקורות ניהול, תקורות פיזיות וכדומה) עבור כל בנק ויביא לחיסכון משמעותי במשאבים אצל הספקים המהותיים עצמם (לדוגמה, במקום שיתקיימו אצל ספק מהותי כחמישה מבדקים דומים בשנה, יתקיים מבדק אחד בלבד ברמה גבוהה משמעותית).

פרק ז': בחינת חלופות לגוף מרכזי

ניתן לבחון את כדאיותו של גוף מרכזי שינהל את סיכוני שרשרת האספקה למגזר הפיננסי על פי שתי חלופות:

א. **גוף בבעלות הבנקים** – גוף שיוקם, ינוהל וימומן על ידי הבנקים, בדומה לגופים אחרים שהוקמו על ידי הבנקים לצרכים שונים.

ב. **גוף חיצוני שאינו בבעלות הבנקים** – למשל, גוף מדינתי המספק את השירות לבנקים בדומה ל-CERT הפיננסי או ליחידה לניהול סיכוני שרשרת אספקה במשרד האוצר.

חלופה א': גוף בבעלות הבנקים

חלופה זו מתייחסת למצב שבו הניהול המרכזי הוא בידיו של גוף הנמצא בבעלות הבנקים המסחריים. המודל של גוף בבעלות בנקים מסחריים אינו תקדימי ויושם בעבר בכמה מקרים, כגון שב"א (שירותי בנק אוטומטיים)[43] ומס"ב (מרכז סליקה בנקאי).[44]

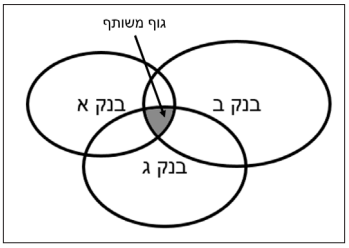
במודל זה כל בנק תורם ממשאביו, והבנקים מנהלים ומתפעלים יחדיו את הפעילות השוטפת. המודל יכול להתבצע במסגרת גוף קיים או במסגרת גוף חדש שיוקם לצורך זה. על הגוף יהיה לגייס את הסוקרים, לוודא את כשירותם המקצועית ולנהל אותם באופן שוטף. על הבנקים יהיה לוודא כי הבדיקה שתבוצע מול הספקים תהיה תואמת את דרישות בנק ישראל והוראות כל דין. הבנקים יוכלו, כאופציה, לשקול מכירת שירות זה גם לגורמים נוספים (דוגמת חברות כרטיסי אשראי, חברות ביטוח וכדומה).

להלן תרשים המתאר חלופה זו (השטח האפור מייצג את הגוף המשותף):

---

43 חברת שירותי בנק אוטומטיים בע"מ היא חברה פרטית שהוקמה בשנת 1979 . החברה משמשת כצומת מרכזי וכתשתית לסליקה בכרטיסי אשראי ועובדת עם כל חברות האשראי הן כסולקות והן כמנפיקות. בנוסף, עובדת החברה מול המפיצים והיצרנים ונותנת שירות גם לבתי עסק. החברה פועלת כחברת שירותים משותפת בבעלות בנק לאומי, בנק הפועלים, בנק דיסקונט והבנק הבינלאומי הראשון.

44 מרכז סליקה בנקאי בע"מ, שהוקם בשנת 1982, הינו חברת שירותים משותפת של בנק הפועלים (25% מהבעלות), בנק לאומי (25% מהבעלות), בנק דיסקונט (25% מהבעלות), בנק המזרחי (12.5% מהבעלות) והבנק הבינלאומי הראשון (12.5% מהבעלות). התמחות החברה הינה במתן שירותים בתחומים הבאים: העברה ממוחשבת של תשלומי משכורות ותשלומים אחרים (תשלומים לספקים וכו') מהמשלם לחשבון הבנק של המוטב; העברה ממוחשבת של הפרשות המעסיק והעובד ישירות מהמעסיק לחשבון העמית בקופות הגמל ובקרנות ההשתלמות; גבייה באמצעות חיובים על פי הרשאה (הוראות קבע); שירות של פירוט החזרות חיובים לגובֶה באופן ממוחשב.



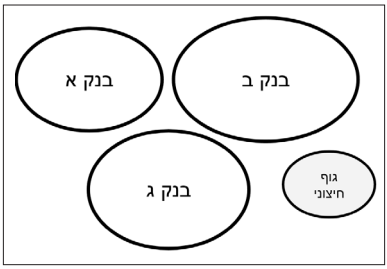
תרשים 13: מודל גוף בבעלות הבנקים

חלופה ב׳: גוף בבעלות חיצונית

חלופה זו מתייחסת למצב שבו הניהול המרכזי מבוצע על ידי גוף חיצוני, שאינו בבעלות הבנקים המסחריים. גוף חיצוני זה אמור לבצע בעצמו את בדיקות הספקים עבור הבנקים. הגוף המדובר יכול להיות גוף ממשלתי.

במודל זה, הבנק מקבל את שירות הבדיקות מהגוף החיצוני, אינו מתַפעל אותו ואינו שולט במשאביו, בסדר העדיפויות שלו ובשיטות עבודתו. הגוף החיצוני, מצידו, צריך לגייס את הסוקרים, לוודא את כשירותם המקצועית ולנהל אותם באופן שוטף, וכן לוודא כי הבדיקה שתבוצע מול הספקים תהיה תואמת את דרישות בנק ישראל בנושא והוראות כל דין. הבנקים לא יוכלו למכור שירות זה לגורמים נוספים (דוגמת חברות כרטיסי אשראי וחברות ביטוח), מכיוון שהגוף הבודק החיצוני לא יהיה בשליטתם ולא כפוף לאחריותם.

להלן תרשים המתאר חלופה זו (השטח האפור מייצג את הגוף החיצוני):



תרשים 14: מודל גוף בבעלות חיצונית

השוואה בין החלופות

הקריטריונים שייבחנו לצורך ההשוואה בין החלופות לניהול מרכזי של סיכוני שרשרת האספקה למגזר הפיננסי (חלופות א׳ ו־ב׳, כמפורט לעיל) הם:

א. משאבי הקמה ותפעול שוטף.

ב. שליטה במשאבים (גמישות, התאמות, קביעת סדר עדיפויות וכדומה).

ג. אופציה למכירת השירותים לגופים נוספים.
ד. השפעה צפויה של פעילות היחידה על הספקים.
ה. יכולת עמידה בדרישות בנק ישראל.

משאבי הקמה ותפעול שוטף

בחלופה א' – כל בנק תורם ממשאביו, והבנקים מנהלים ומתפעלים יחדיו את הפעילות השוטפת. כאמור, נדרש להקים ולתפעל יחידה בת כ־12 סוקרים עבור כלל המגזר הבנקאי.
בחלופה ב' – היחידה מוקמת ומתופעלת על ידי גורם חיצוני, שאינו בבעלות הבנקים המסחריים. לפיכך, אין לבנקים המסחריים עלויות הקמה ותפעול שוטף, בהנחה שהשירותים יינתנו להם בחינם.

השוואה בראי המגזר הבנקאי – בקריטריון זה חלופה ב' עדיפה.

שליטה במשאבים

בחלופה א' – מכיוון שהיחידה הינה בבעלות הבנקים המסחריים, תהיה להם שליטה בפעילותה. הבנקים המסחריים יוכלו להתאים את הפעילות של היחידה בהיבטים של סדרי עדיפויות, הוספת יכולות (למשל, באמצעות גיוס העובדים והכשרתם), התאמת שיטות העבודה וכדומה.
בחלופה ב' – מכיוון שהיחידה אינה בבעלות הבנקים המסחריים, אין להם שליטה במשאביה.

השוואה בראי המגזר הבנקאי – בקריטריון זה חלופה א' עדיפה.

אופציה למכירת השירותים לגופים נוספים

בחלופה א' – היחידה מספקת שירותים היכולים להתאים גם לגופים נוספים (כגון חברות כרטיסי אשראי וחברות ביטוח). מכיוון שהיחידה הינה בבעלות הבנקים המסחריים, הם יוכלו, כאופציה, לשקול מכירת שירות זה גם לגורמים נוספים.
בחלופה ב' – היחידה מספקת שירותים היכולים להתאים גם לגופים נוספים (כגון חברות כרטיסי אשראי וחברות ביטוח). מכיוון שהגוף הבודק אינו בשליטתם או באחריותם של הבנקים המסחריים, הם לא יוכלו למכור שירות זה לגורמים נוספים (כמו חברות כרטיסי אשראי וחברות ביטוח).

השוואה בראי המגזר הבנקאי – בקריטריון זה חלופה א' עדיפה.

השפעת פעילות היחידה על ספקים

בחלופה א' – מכיוון שהיחידה פועלת מול הספקים כגוף אחד המייצג את דרישות כלל הבנקים (ולא כמייצגת בנק אחד בלבד), צפוי שתהיה לה השפעה חזקה על הספקים.

בחלופה ב' – מכיוון שהיחידה פועלת מול הספקים כגוף אחד המייצג את דרישות כלל הבנקים, צפוי גם אז שתהיה לה השפעה חזקה על הספקים.

השוואה בראי המגזר הבנקאי – שתי החלופות טובות. אין עדיפות לאחת מהן.

עמידה בדרישות בנק ישראל

בחלופה א' – מכיוון שדרישות בנק ישראל הוגדרו והופצו לבנקים המסחריים, ובהנחה שיגויסו ליחידה אנשי מקצוע מתאימים, לא צפויה בעיה בפעילות היחידה מול הספקים בהתאם לדרישות בנק ישראל ובדרך תאפשר לבקר את מימושן באופן מיטבי.

בחלופה ב' – מכיוון שדרישות בנק ישראל הוגדרו והופצו לבנקים המסחריים, ובהנחה דומה שיגויסו ליחידה אנשי מקצוע מתאימים, לא צפויה גם במקרה זה בעיה בפעילות היחידה מול הספקים בהתאם לדרישות בנק ישראל ובדרך תאפשר לבקר את מימושן באופן מיטבי.

השוואה בראי המגזר הבנקאי – שתי החלופות טובות. אין עדיפות לאחת מהן.

להלן טבלה המרכזת את ההשוואה בין החלופות:

הקריטריון	חלופה א' (ניהול מרכזי על ידי גוף בבעלות הבנקים)	חלופה ב' (ניהול מרכזי על ידי גוף חיצוני)
משאבי הקמה ותפעול שוטף		✓
שליטה במשאבים	✓	
אופציית שירות לגופים נוספים	✓	
השפעה צפויה על הספקים	✓	✓
עמידה בדרישות בנק ישראל	✓	✓

ניתן לראות כי שתי החלופות טובות ובעלות פוטנציאל לטפל בנושא באופן הולם. לשתי החלופות יש יתרונות וחסרונות, אולם **נראה כי לחלופה א' (ניהול מרכזי על ידי גוף בבעלות הבנקים) ישנם יתרונות רבים יותר בראי המגזר הבנקאי.**

פרק ח': סיכום והמלצות

עבודה זו סקרה, הציגה וניתחה את הנושאים הבאים:

א. **תקינה** – נסקרו תקני ISO, תקני NIST, GDPR ו־FFIEC. מהסקירה עולה כי קיימת תקינה ענפה הפורסת בפני הארגונים מגוון רחב של תחומים ובקרות המאפשרים להיערך להתמודדות עם סיכוני סייבר בשרשרת האספקה ולצמצם את החשיפה אליהם.

ב. **רגולציה בישראל** – נסקרו תורת ההגנה של מערך הסייבר הלאומי, החלטת ממשלה מס׳ 2443, הוראת בנק ישראל בנושא ניהול סיכוני סייבר בשרשרת האספקה, חוזר משרד האוצר – אגף שוק ההון, ביטוח וחיסכון בנושא ניהול סיכוני סייבר בגופים מוסדיים, ותקנות הגנת הפרטיות (אבטחת מידע) של הרשות להגנת הפרטיות. מהסקירה עולה כי קיימת ברגולציה הישראלית התייחסות לסיכונים בשרשרת האספקה. עם זאת, אין בישראל רגולציה מחייבת עבור כלל הארגונים, והרגולציה הקיימת היא מגזרית (לדוגמה, במגזר הביטוח ושוק ההון) או נושאית (לדוגמה, בנושא הפרטיות).

ג. **מרחב האיומים הרלוונטיים** – נותחו האיומים הרלוונטיים מתוך שורה של מסמכים: CERT UK, תקן ISO 27036-1, דוח אירועי סייבר 2016-2018 – ניצול שרשרת אספקה SWIFT של חברת Clearsky, מסמך של מערך הסייבר הלאומי בנושא סיכונים במיקור חוץ ושרשרת האספקה ומסמך של SANS Institute. מהניתוח עולה כי האיומים על ארגון (לרבות ארגון פיננסי) באמצעות תקיפת שרשרת האספקה עשויים להתממש 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 מדובר באיומים תיאורטיים, אלא באיומים הנובעים ממספר רב של אירועים שהתרחשו בישראל ובעולם שנועדו לפגוע 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 הנובעים ממנו.

ד. **מתודולוגיות ומודלים לניהול ספקים בשרשרת האספקה** – הוצגו מתודולוגיות ומודלים של חברת Deutsche Telekom, של ITIL ושל חברת United

Amway – Europe Supplier Information Portal, של Utilities ושל הספר "Purchasing and Supply Chain Management". במסגרת זו נמצאו מתודולוגיות ומודלים לסיווג ספקים ברמה הארגונית. לא נמצאו מתודולוגיות ומודלים לסיווג ספקים ברמה הלאומית ו/או המגזרית, או לחילופין לסיווג ספקים בהיבטי סייבר.

ה. **דוגמאות לגישות במשק הישראלי בעלות הקשר אפשרי למגזר הפיננסים** – הוצגו תהליכי רישום וסיווג של קבלני בניין במדינת ישראל, וכן תהליך בדיקת ההתאמה הביטחונית למועסקים במשרות מסווגות. בנוסף, צוינו שתי פעילויות המבוצעות בישראל בהקשר ישיר יותר למגזר הפיננסי – פעילות הנערכת במערך הסייבר הלאומי לפיתוח מתודה להגנה על שרשרת האספקה, ופעילות המבוצעת במערך הסייבר, חירום וביטחון במשרד האוצר על ידי היחידה להסדרת סייבר ורציפות בשרשרת האספקה הפיננסית. במספר תחומים נמצאו במשק הישראלי גישות שיש להן קשר אפשרי למגזר הפיננסי: קטגוריזציה המבוצעת ברמה הלאומית לספקים מענף משקי מסוים (סיווג קבלני בניין), ותהליך תשתיתי המבוצע/מונחה על ידי גוף מרכזי אחד (היחידה הממלכתית לקביעת התאמה ביטחונית בשירות הביטחון הכללי) עבור מועסקים בגופים רבים. גם בהיבט הסייבר מתנהלת פעילות ברמה הלאומית: מערך הסייבר הלאומי החל לפתח מתודה להגנה על שרשרת האספקה והנגשתה בפורטל. מתודה זו עדיין אינה מיושמת בהיקף נרחב, אך היא עשויה לאפשר בהמשך הדרך הקמתה של פלטפורמה הולמת לשימוש נרחב על ידי גופים רבים. גם הפעילות להסדרת הרציפות בשרשרת האספקה של היחידה הייעודית במשרד האוצר רלוונטית למגזר הפיננסי. גם פעילות זאת נמצאת בשלבי יישום ראשוניים מול ספקיה של המערכת הפיננסית.

ו. **ניתוח כלכלי עקרוני של ניהול עצמי על ידי כל בנק מול ניהול מרכזי** – נערך ניתוח כלכלי של שתי חלופות עיקריות לניהול הפעילות הנדרשת מול ספקי המערכת הפיננסית בהיבטי ההתמודדות עם סיכוני הסייבר בשרשרת האספקה: ניהול עצמי על ידי כל בנק, וניהול מרכזי (עבור כל/רוב הבנקים). בנוסף, בוצע ניתוח רגישות לתוצאות הניתוח הכלכלי. מהניתוחים עולה כי מבחינה כלכלית יש עדיפות מובהקת לנהל את הנושא באופן מרכזי עבור הבנקים המסחריים. לניהול מרכזי יש פוטנציאל חיסכון של כ־12 סוקרים (טווח ניתוח הרגישות מצביע על פוטנציאל חיסכון של 8–18 סוקרים) בכלל המגזר הבנקאי. ניהול מרכזי גם יחזק את השפעתו ועוצמתו של הגוף הסוקר כלפי הספקים (שכן הוא ייצג את כל/רוב הבנקים ולא רק בנק מסוים), יאפשר התמקצעות טובה של הצוות (גוף מתמחה ברמה המגזרית), יקטין תקורות (תקורות ניהול, תקורות פיזיות

וכדומה) עבור כל בנק ויגרום לחיסכון משמעותי של המשאבים הנדרשים אצל הספקים המהותיים עצמם (במקום שיתקיימו אצל ספק מהותי כחמישה מבדקים דומים בשנה, יתקיים מבדק אחד בלבד).

ז. **הצגת החלופות לניהול מרכזי** – הוצגו שתי חלופות לניהול מרכזי: חלופה ראשונה, בה הניהול המרכזי מבוצע על ידי גוף בבעלות הבנקים המסחריים, וחלופה שנייה, בה הניהול המרכזי מבוצע על ידי גוף חיצוני שאינו בבעלות הבנקים המסחריים, שיבצע את בדיקות הספקים בעצמו עבור הבנקים (גוף כזה יוכל להיות גוף ממשלתי).

ח. **השוואה בין החלופות לניהול מרכזי** – נערכה השוואה בין שתי החלופות לניהול מרכזי, וזאת בהתאם לקריטריונים הבאים: משאבי הקמה ותפעול שוטף; שליטה במשאבים (גמישות, התאמות, קביעת סדר עדיפויות וכדומה); אופציה למכירת השירותים לגופים נוספים; השפעה צפויה של פעילות היחידה על הספקים; יכולת עמידה בדרישות בנק ישראל. מההשוואה עולה כי שתי החלופות הן טובות ובעלות פוטנציאל לטפל בנושא באופן הולם. לשתי החלופות יש גם יתרונות וגם חסרונות, ולאף חלופה אין עדיפות מובהקת על האחרת. אולם, נראה כי **לחלופה של ניהול מרכזי על ידי גוף בבעלות הבנקים יש מעט יותר יתרונות בראי המגזר הבנקאי.**

המלצות

לאור האמור לעיל, ובהתאם לניתוח הנתונים הקיימים, להלן עיקרי ההמלצות:

א. על הבנקים למפות ולסווג את ספקיהם המהותיים, קרי, ספקים המהותיים לפעילותם ו/או כאלה החושפים אותם לסיכוני סייבר ואבטחת מידע פוטנציאליים גבוהים, שבהתממשותם ניתן יהיה לתקוף את התאגיד הבנקאי או לפגוע בפעילותו.

ב. על הבנקים להגדיר מערכת דרישות עבור הספקים המהותיים בכל מה שנוגע להתמודדות עם סיכוני סייבר בשרשרת האספקה שלהם. על מערכת דרישות זאת לעמוד בהלימה עם הוראות בנק ישראל והוראות כל דין, ולהתבסס על הנושאים והבקרות המכוסים בתקינה הקיימת ועל הניסיון המיטבי.

ג. על הבנקים לוודא כי ספקיהם המהותיים מבצעים את מערכת הדרישות שתוגדר. זאת, באמצעות פעילות של אנשי מקצוע מתאימים (סוקרים מקצועיים), שיפעלו מול הספקים כבקרה על ביצוען השוטף של הדרישות.

ד. מוצע לבנקים לבחון שימוש (לרבות שימוש משלים) במתודה המפותחת במערך הסייבר הלאומי בנושא הפעילות מול ספקים.

ה. נוכח תוצאות הבחינה הכלכלית לפיהן ישנה כדאיות מובהקת לנהל פעילות זו באופן מרכזי עבור הבנקים, ולא על ידי כל בנק באופן עצמאי, **מומלץ כי**

ניהול הפעילות יהיה מרכזי. בדרך זו גם תגדל השפעתה של הפעילות המרכזית מול הספקים, שכן הגוף הסוקר ייצג את דרישות כלל הבנקים ולא רק דרישות של בנק מסוים. יודגש, עם זאת, כי כל בנק יוכל להוסיף דרישות ספציפיות מספק מסוים שלו, לפי הצורך. כן מוצע כי מנגנון התמחור בין הבנקים לצורך הקמתו ותפעולו של הגוף המרכזי יבוצע באופן דיפרנציאלי, שיבטא את היקף הפעילות של כל בנק במיזם.

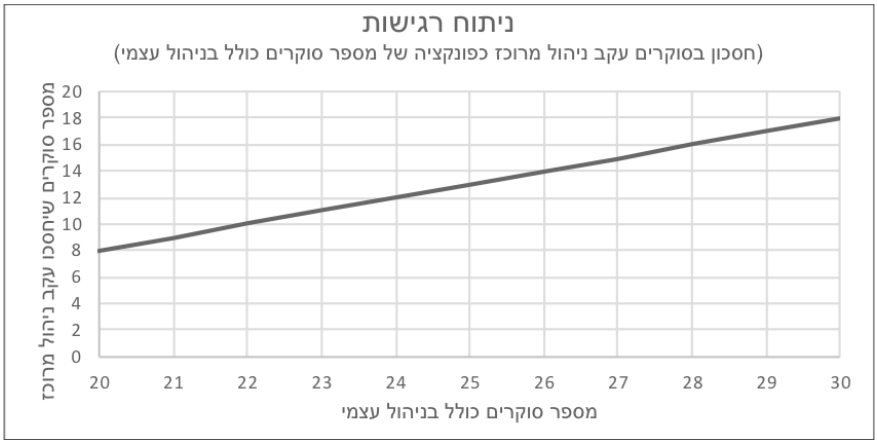
לאור כל זאת, בראי המגזר הבנקאי, מוצע להקים גוף מרכזי בבעלות הבנקים.

נספח: ניתוח רגישות כלכלית

כאמור, אם כל בנק ינהל את הפעילות בעצמו יהיה צורך ב־24 סוקרים בכלל המגזר הבנקאי. ניתוח הרגישות יבדוק את הכדאיות הכלכלית אם חישוב מספר הסוקרים ישתנה (בטווח של עשרים עד שלושים סוקרים). להלן תוצאות ניתוח הרגישות:

מספר סוקרים כולל בניהול עצמי	מספר סוקרים בניהול מרכזי	מספר סוקרים שייחסכו עקב ניהול מרכזי
20	12	8
21	12	9
22	12	10
23	12	11
24	12	12
25	12	13
26	12	14
27	12	15
28	12	16
29	12	17
30	12	18

להלן ניתוח הרגישות באופן גרפי:



על פי ניתוח הרגישות, קיימת כדאיות כלכלית לניהול מרכזי בכל טווח של חישוב מספר הסוקרים הכולל בניהול עצמי (מעשרים עד שלושים סוקרים).

- The banks must define a set of requirements for important suppliers with respect to handling cyber risks in the financial sector supply chain. These requirements must harmonize with the instructions of the Bank of Israel and the provisions of every law, and be based on the matters, areas and controls covered by existing regulation and accumulating experience.
- The banks must ensure that their important suppliers comply with the defined set of requirements, by means of professional reviewers who will check their regular implementation of the requirements.
- The banks should examine the use (including supplementary use) of the method developed by the National Cyber Directorate on activity with suppliers.
- In view of the findings regarding the clear economic feasibility of managing this activity centrally for all banks, rather than by each bank separately, this is the recommended option. This will also increase the effect of the work on suppliers, who will know they are dealing with all the banks and not just one bank. However, it is stressed that a specific bank may add its own specific requirements for a specific supplier, as it deems fit. The central body should be owned by the banks, with a mechanism to split the cost of setup and operations differentially, in order to reflect the scope of activity of each member bank.

the important suppliers themselves (instead of about five similar checks over a year of a large supplier, one check will suffice).

The paper proposes two alternatives for central management of suppliers in the financial system: in the first, central management is performed by a body owned by the commercial banks; in the second alternative, central management is performed by an external body (possibly a government body) that will carry out its own checks for the banks. Both these alternatives were examined in the light of three criteria:

- **Improving cyber security in the financial system**: the analysis showed that central management will significantly improve the level of cyber security in the financial sector in the context of the supply chain.
- **Economic feasibility**: the comparison between the alternatives was based on the resources needed for setup and regular operation; degree of control of resources (flexibility, adaptations, setting priorities etc.); the existence of an option to sell the services to other bodies; the expected effect of the central unit's activity on suppliers; the ability to meet the Bank of Israel's requirements.
- **Compliance with anti-trust requirements**: the analysis shows that setting up a central reviewing body is not contrary to anti-trust requirements, since such a body will not affect competition between banks, and its sole purpose is to improve the security and stability of the financial system as a whole.

Not only that, today the banks should deal with lengthy processes when adding new suppliers to the system. The operation of a central body could shorten these processes and even create a situation in which financial entities could ask for a review and prior approval of new suppliers in the context of suitability in aspects of cyber security.

In view of the foregoing, and based on the analysis of existing data, the main recommendations are as follows:

- The banks must map and classify their important suppliers, that is, those that are important to their activity and/or those that expose them to potentially significant cyber and data security risk that could seriously damage their operation.

The preparatory work also included a review of methodologies and models for managing suppliers in the supply chain, including large global corporations. Methodologies and models were found for handling and classifying suppliers at organizational level, but not at national or sectorial level, or alternatively, for classifying suppliers in cyber terms. The findings in several areas of the Israeli economy suggested possible approaches in the context of this paper – categorization at national level for suppliers from a different industry (such as building contractors), and an infrastructure process carried out/ guided by one central element (the National Unit for Determining Security Suitability in the Israel Security Agency) for the employees of many different entities.

Israel's National Cyber Directorate has begun work on the development of a methodology at national level, accessible through a portal. Although this method has not yet been extensively implemented (as of the time of writing), it could soon become a suitable platform for wide use by large numbers of entities. A special unit in the Ministry of Finance designed to focus on activity in the financial sector is in the preliminary states of implementation with respect to suppliers and is also relevant to the present discussion.

As part of this work, the two main alternatives for managing activity regarding suppliers to the financial system were analyzed with reference to aspects of handling cyber threats: one, independent handling by each bank; and two, central management for all/ most banks. The results of the financial analysis were also put through a sensitivity analysis. All the findings show that, in economic terms, there is a clear preference for central management of this subject for the commercial banks. Central management means the potential saving of some 12 reviewers (suitable professionals; the sensitivity analysis indicates a potential saving of 8-18 reviewers) in the whole banking sector. Not only that, central management will reinforce the effect and power of the reviewer in the eyes of the suppliers (since he represents all/ most of the banks, not just one), facilitate better professionalism in the team (who can specialize at sectorial level), reduce overheads (management, physical costs and so on) for every bank, and lead to significant savings in resources for

Abstract

This paper deals with the cyber risks in the supply chain of the financial sector, and a proposal for ways of dealing with them. The purpose of the paper is to present suitable and practical recommendations for the banking sector, and it was written after a thorough study of the subject, including in the framework of discussions and working meetings with relevant people in this sector. The process also included a review of pertinent international standards, which showed that there are numerous standards covering a variety of areas and controls, designed to limit the exposure to cyber risks in the supply chain, and to prepare for them. Further surveys looked at relevant doctrines of protection, government resolutions, instructions, directives and regulations in Israel. The findings indicate that Israeli regulations refer to several aspects of supply chain risks but are not binding on all organizations. The regulations are aimed at specific sectors, such as the insurance and the capital market sectors, or specific subjects, such as privacy.

The preliminary work included an examination and analysis of the relevant threats to the supply chain, showing that attacks on organizational supply chains, including those of financial organizations, could materialize through a very wide range of channels, such as penetration of the systems of a supplier with relatively low protection levels (but with access to the organization's systems); the use of legitimate software updates to spread malware, and so on. These are not theoretical threats, and the analysis is based on a large number of actual incidents in Israel and worldwide, in which organizations were the victims of cyber attacks that exploited their supply chains. The complexity of the threat, the wide range of possible scenarios, and the increasingly more powerful capabilities of attackers oblige organizations, including financial organizations, to take significant steps to meet the challenge and to minimize the dangers they face.

National Cyber Risk Management for the Financial Sector: Reducing Supply Chain Risks

Gabi Siboni
Ziv Solomon and Hadas Klein

This work has been supported by Bank Hapoalim

National Cyber Risk Management for the Financial Sector: Reducing Supply Chain Risks

Gabi Siboni
Ziv Solomon and Hadas Klein

This work has been supported by Bank Hapoalim
בנק הפועלים

INSS
המכון למחקרי ביטחון לאומי
THE INSTITUTE FOR NATIONAL SECURITY STUDIES
TEL AVIV UNIVERSITY אוניברסיטת תל אביב