דוח מבקר המדינה | שבט התשפ"ד | ינואר 2024

נושאים מערכתיים

ניהול סיכוני סייבר מצד שרשרת האספקה בתחום התקשוב

ניהול סיכוני סייבר מצד שרשרת האספקה בתחום התקשוב

רקע

שרשרת אספקה היא מונח המתייחס לכלל המשאבים והתהליכים הקשורים בספקים, בלקוחות ובקבלני ביצוע, אשר דרושים לצורך אספקת מוצר או שירות בארגון. מתקפות סייבר המתבצעות באמצעות שרשרת האספקה מכוונות לפגוע באחד מספקי הארגון, מנצלות את האמון שהארגון נותן בספק שלו כדי לחדור באמצעותו אל הארגון.

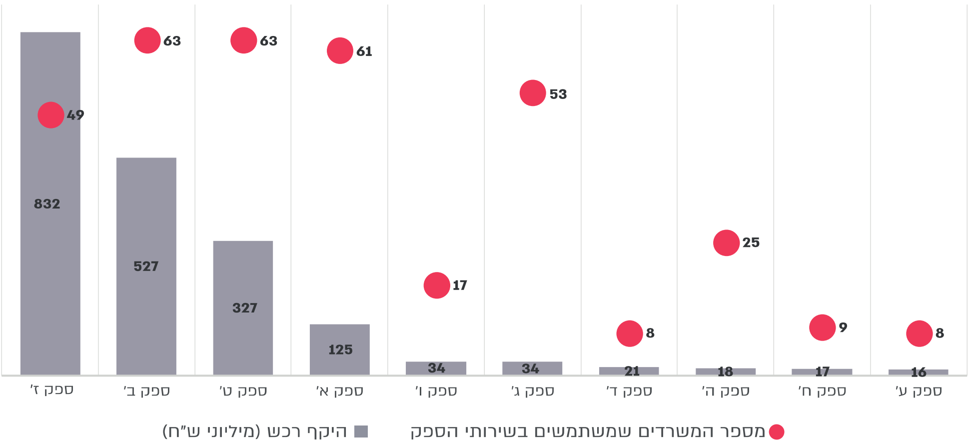
בשנים האחרונות חל גידול ניכר במספר מתקפות הסייבר על ארגונים ועוצמתן גברה, וכיום מתקפות סייבר המתבצעות באמצעות שרשרת האספקה שלהם הן אחד האיומים החמורים ביותר הנשקפים לכלל המשק. כמה דוגמאות למתקפות אלו בשנים 2020-2022: בנובמבר 2020 - דלף מידע רגיש בהיקף של טרה-בייט על לקוחות של חברת ביטוח גדולה ובכלל זה מידע מאלפי תיקים של עובדי מדינה, עקב ניצול חולשה במערכות חברת הביטוח; באוקטובר 2021 - דלף מידע רגיש של מיליון פרופילים באתר היכרויות של הקהילייה הגאה עקב פגיעה בספק שנתן לאתר ההיכרויות ולאתרים אחרים שהתארחו אצלו שירותי אירוח ואחסון של אתרים.

משרדי ממשלה וגופים שהם תשתיות מדינה קריטיות[1] (גופי תמ"ק) נדרשים להתמודד עם הסיכון הנובע משרשרת האספקה באמצעות הכללת דרישות בתחום הגנת הסייבר במסגרת הליכי המכרז וההתקשרות.

הפגיעה בספקים שנותנים שירותים למשרדי ממשלה רבים או לגופי תמ"ק עלולה להיות חמורה במיוחד, זאת משום שפגיעה בהם עלולה לפגוע ברציפות התפקודית של המשק או לגרום לדלף מידע רגיש במיוחד. מהדוח עולה כי למשרדי הממשלה יש 18 ספקים עיקריים בתחום התקשוב והסייבר - מתוכם חמישה ספקים נותנים שירות ליותר מ-49 משרדים ושלושה ספקים נותנים שירות בהיקף כספי שנתי של יותר מ-327 מיליוני ש"ח, ראו תרשים להלן:

1 ארגונים המוגדרים בחוק להסדרת הביטחון לגופים ציבוריים, התשנ"ח-1998, כתשתיות מדינה קריטיות.

ספקים בתחום התקשוב והסייבר אשר מספקים שירות למשרדים רבים (ההיקף הכספי במיליוני ש"ח)



על פי נתוני מערכת הרכש הממשלתית, בעיבוד משרד מבקר המדינה.

מערך הסייבר הלאומי (להלן גם - מערך הסייבר או המערך) זיהה את האיום של תקיפת סייבר באמצעות שרשרת האספקה והשיק בשנת 2018 מתודולוגיה ייעודית למשק בנושא (מתודולוגיית שרשרת האספקה), שמפורסמת באתר של מערך הסייבר[2] כהמלצה למשק. כמו כן מערך הסייבר פרסם לגופי התמ"ק הנחיה ייעודית המבוססת על מתודולוגיה זו. יחידת הסייבר בממשלה (יה"ב), האחראית להכוונה ולהנחיה המקצועית בתחום הגנת הסייבר עבור כלל משרדי הממשלה ויחידות הסמך, פרסמה אף היא בנובמבר 2019 הנחיה ייעודית בנושא שרשרת האספקה, המבוססת על המתודולוגיה של מערך הסייבר. מתודולוגיית שרשרת האספקה עודכנה בדצמבר 2022, וההנחיות לגופי התמ"ק ולמשרדי הממשלה עודכנו בהתאם לכך במהלך שנת 2023.

2 https://www.gov.il/he/departments/guides/supply_chain_guide

שלבי מתודולוגיית שרשרת האספקה של מערך הסייבר

המקור: מערך הסייבר.

נתוני מפתח

נתוני המפתח שלהלן מבוססים על נתונים שנאספו במסגרת מענה של 44 משרדי ממשלה וגופי תמ"ק על שאלון שהפיץ משרד מבקר המדינה.

30%

משרדי הממשלה ומגופי התמ"ק דיווחו שחוו בשנתיים האחרונות אירוע סייבר שמקורו בשרשרת האספקה

86%

ממשרדי הממשלה ומגופי התמ"ק הגדירו שאירוע סייבר באמצעות תקיפת שרשרת האספקה הוא איום ייחוס של הארגון

55%

ממשרדי הממשלה ומגופי התמ"ק אינם עובדים לפי מתודולוגיית שרשרת האספקה של מערך הסייבר

41%

ממשרדי הממשלה ומגופי התמ"ק לא ביצעו ביקורות סייבר על הספקים המהותיים שלהם בשלוש השנים האחרונות (2022 - 2020)

57%

מההתקשרויות של משרדי הממשלה בתחום התקשוב והסייבר בשנת 2021 בוצעו באמצעות מכרזים מרכזיים - שאינם כוללים דרישה ליישום מתודולוגיית שרשרת האספקה

84

אירועי סייבר בחברות אירוח ואחסון של אתרים בשנים 2021 - 2022

43%

ממשרדי הממשלה ומגופי התמ"ק אינם מערבים את ממונה הגנת הסייבר בתהליכי הרכש

אף אחד

מ-13 הספקים המהותיים שנותנים שירותים לכמה גופי תמ"ק לא עבר התעדה[3] על ידי גופי ההסמכה

3 ספקים שסווגו כמהותיים על ידי הארגון (ספקים בדירוג A) - נדרשים לפי מתודולוגיית שרשרת האספקה למלא יחד עם בודק חיצוני שהוסמך על ידי מערך הסייבר שאלון ספקים הבודק את רמת ההגנה שלהם. השאלון מועבר לגוף הסמכה, והוא בודק את הדיווחים שהובאו בשאלון ואת הראיות שצורפו לו. גוף ההסמכה יכול לאשר את הדיווח ולהנפיק לספק תעודת הסמכה שתהיה תקפה לשנתיים או לא לאשר את הדיווח ולבקש ממנו לבצע תיקון ליקויים.

פעולות הביקורת

בחודשים פברואר 2022 עד מאי 2023 בדק משרד מבקר המדינה את נושא ניהול סיכוני הסייבר מצד שרשרת האספקה בתחום התקשוב. הביקורת נעשתה במשרד ראש הממשלה - במערך הסייבר הלאומי ובאגף ביטחון, חירום וסייבר; במערך הדיגיטל הלאומי - ביה"ב וביחידת ממשל זמין; במשרד האוצר - במינהל הרכש ובאגף ביטחון, חירום וסייבר. בדיקות השלמה נעשו בכמה משרדי ממשלה ובגופי תמ"ק. בכלל הארגונים נבדק הנושא בנוגע לרשת הבלתי מסווגת.

במסגרת הביקורת הפיץ משרד מבקר המדינה בקרב 58 משרדי ממשלה וגופי תמ"ק שאלון הבודק כיצד הם מתמודדים עם הסיכון לביצוע מתקפות סייבר על שרשרת האספקה. שאלון זה התבסס, בין היתר, על נושאים ופערים שעלו בפגישות שקיים צוות הביקורת עם משרדים ועם גופי תמ"ק, ומטרתו הייתה להציג תמונת רוחב על אופן הטיפול של משרדי הממשלה ושל גופי התמ"ק בנושא מהותי זה. 44 משרדי ממשלה וגופי תמ"ק ענו על השאלון (31 משרדי ממשלה ו-13 גופי תמ"ק).

רשימת משרדי הממשלה וגופי התמ"ק שהופץ אליהם השאלון (משרדי הממשלה וגופי התמ"ק שענו על השאלון מסומנים בהדגשה): **גוף 1**, **מינהל התכנון**, **גוף 2**, **משרד האנרגייה והתשתיות**, **השירות המטאורולוגי הישראלי**, **גוף 5**, **הרבנות הראשית לישראל**, **משרד הבינוי והשיכון**, המשרד לנושאים אסטרטגיים והסברה, **משרד הרווחה והביטחון החברתי**, **רשות המים**, הנהלת בתי המשפט, **מינהל המחקר החקלאי**, הרשות להגנת הצרכן ולסחר הוגן, **רשות התחרות**, **גוף 11**, **נציבות שירות המדינה**, **גוף 15**, גוף 50, **גוף 16**, גוף 51, **המשרד לשוויון חברתי**, לשכת הפרסום הממשלתית, **משרד החקלאות ופיתוח הכפר**, **משרד התיירות**, גוף 52, **גוף 19**, **גוף 20**, **נתיב (רה"ם)**, **גוף 21**, **משרד ראש הממשלה**, משרד החדשנות המדע והטכנולוגיה, **רשות האכיפה והגבייה**, **המשרד לביטחון לאומי**, **המכון הגיאולוגי**, **משרד הכלכלה והתעשייה**, **הרשות הארצית לכבאות והצלה**, **המשרד לשירותי דת**, **משרד העלייה והקליטה**, משרד התחבורה והבטיחות בדרכים, **משרד התרבות והספורט**, משרד התקשורת, **גוף 38**, **משרד הבריאות**, גוף 53, **גוף 39**, **המינהל לחינוך התיישבותי ועליית הנוער**, **משרד העבודה**, **המשרד להגנת הסביבה**, גוף 54, **הנהלת בתי הדין הרבניים**, רשות מקרקעי ישראל, **משרד הפנים**, **גוף 43**, **גוף 45**, **משרד החוץ**, גוף 55, **משרד המשפטים**.

דוח זה מתמקד בניהול הסיכונים מצד שרשרת האספקה של משרדי ממשלה, ושל גופי תמ"ק המחויבים לעמוד בהנחיות של יה"ב ושל מערך הסייבר בהתאמה, אשר במועד כתיבת הדוח היו מבוססות על גרסה 1.3 של מתודולוגיית שרשרת האספקה. במהלך הביקורת, בדצמבר 2022, עודכנה המתודולוגיה לגרסה 1.4, בין היתר כדי לתת מענה על חלק מהפערים שהוזכרו בדוח זה.

תמונת המצב העולה מן הביקורת

יישום מתודולוגיית שרשרת האספקה של מערך הסייבר בכלל הארגונים - 24 (55%) מתוך 44 משרדי הממשלה וגופי התמ"ק שהשיבו על השאלון אינם עובדים לפי מתודולוגיית שרשרת האספקה של מערך הסייבר. נוכח זאת חלק גדול מהספקים של הארגונים אינם נבדקים בצורה אחודה ובהתאם לבקרות שהגדיר מערך הסייבר. כמו כן כל יחידות הסייבר המגזריות נתקלו בפערים ביישום המתודולוגיה: העלויות הגבוהות של תהליך ההתעדה, פרק הזמן שהיא אורכת, הקושי לפעול מול ספקים בין-לאומיים וכן הקושי להוסיף דרישות בתחום הגנת הסייבר למכרזים קיימים.

הטיפול בפערים במתודולוגיית שרשרת האספקה - מערך הסייבר עדכן את מתודולוגיית שרשרת האספקה (גרסה 1.4) והפיץ אותה לציבור בדצמבר 2022, אולם המתודולוגיה העדכנית לא נתנה מענה על חלק מהפערים המהותיים שהועלו עוד בוועדת ההיגוי של מערך הסייבר בנושא שרשרת האספקה בינואר 2022, ובהם הקושי הגלום בחיוב הספק הנבדק לעמוד במלוא הבקרות הקיימות בשאלון הספקים ללא אפשרות לתת מענה באמצעות בקרות מפצות על חלק מהדרישות או באמצעות הוכחת עמידה בתקנים מקבילים ואי מתן מענה על עבודה מול ספקים בין-לאומיים. לדוגמה, הוצע לבחון את הארכיטקטורה של רכיבים של בקרים תעשייתיים שונים של חברה מסוימת שמסופקים למגזרים שונים במשק הישראלי, ולנוכח תובנות אלו מערך הסייבר כגוף אסדרתי בתחום הסייבר ינהל את השיח לגבי דרישות האבטחה שהחברה צריכה לעמוד בהן.

ניהול הסיכונים מצד שרשרת אספקה במכרזים מרכזיים - אף ש-57% מהרכש הממשלתי בתחום התקשוב והסייבר (בהיקף כספי שנתי של כ-1.4 מיליארד ש"ח) מבוצע באמצעות מכרזים מרכזיים, אין דרישה של מינהל הרכש מהספקים שעימם הוא מתקשר לעמוד במתודולוגית שרשרת האספקה של מערך הסייבר. כמו כן מערך הסייבר ויה"ב, המנחים באופן שוטף את גופי התמ"ק ואת המשרדים, אינם משולבים באופן קבוע בתהליך גיבוש הדרישות של מכרזים אלו.

מיפוי ספקים שיש להם השפעה נרחבת על המשק - מהשאלון שהעביר משרד מבקר המדינה עולה כי יש 18 ספקים עיקריים בתחום התקשוב והסייבר שנותנים שירותים למשרדי ממשלה ולגופי תמ"ק רבים - מתוכם חמישה ספקים נותנים שירות ליותר מ-49 משרדי ממשלה וגופי תמ"ק, ושלושה ספקים נותנים שירות בהיקף כספי שנתי של יותר מ-327 מיליוני ש"ח. נמצא כי מערך הסייבר ויה"ב אינם מנהלים רשימה אחודה של הספקים המהותיים שנותנים שירות למשרדי ממשלה ולגופי תמ"ק, של הספקים שזכו במכרזים מרכזיים ושל הארגונים שמשתמשים בכל התקשרות. כמו כן הם לא אוספים מודיעין באופן יזום לצורך קבלת התרעות על חשש לפגיעה בספקים אלו. נוכח זאת אין ביכולת הגופים האסדרתיים לאמוד את רמת החשיפה של המשרדים ושל גופי התמ"ק לספקים אלו ולבצע פעולות יזומות מול הספקים להעלאת רמת ההגנה שלהם.

ספקי אינטגרציה, IT ואחסון ואירוח של אתרים - למערך הסייבר אין סמכות לאכוף את מתודולוגיית שרשרת האספקה על חברות אחסון ואירוח של אתרים ועל חברות אינטגרציה ו-IT שנותנות שירות לארגונים רבים במשק. כמו כן התגלו בחברות אלו אירועי סייבר חוזרים (84 אירועי סייבר בחברות אחסון בשנים 2021 ו-2022) שמעמידים בסכנה ארגונים רבים במשק.

התעדה של ספקים מהותיים (דירוג A) - שום ספק מ-13 הספקים המהותיים שנותנים שירותים לכמה גופי תמ"ק לא עבר הליך התעדה על ידי גופי ההסמכה אף שלפי הנחיית מערך הסייבר 30% מהספקים המהותיים של גופי התמ"ק היו צריכים להיות מותעדים עד לתום הרבעון הרביעי של שנת 2022. בין הסיבות לשיעור ההתעדה הנמוך: משך תהליך ההתעדה (מעל 9 חודשים) שאינו בהלימה לצרכים העסקיים של הארגון ואי נכונות הגורמים השונים (הספקים, המשרדים, גופי תמ"ק ומערך הסייבר) לשאת בעלויות ההתעדה.

ביצוע ביקורות אצל ספקים מהותיים (דירוג A) - מערך הסייבר, יה"ב ומינהל הרכש אינם עושים ביקורות על ספקים מהותיים הנותנים שירותים למשרדים ולגופי תמ"ק רבים וכן על ספקים שזכו במכרזים מרכזיים (אף ששיעור ההתקשרויות עימם הוא כ-57% מכלל ההתקשרויות של משרדי הממשלה, והיקפן הכספי של התקשרויות עימם הוא כ-1.4 מיליארד ש"ח). כמו כן 14 (41%) מתוך 34 משרדי הממשלה וגופי התמ"ק שענו על השאלון לא ביצעו, מצידם, ביקורת אצל הספקים המהותיים שלהם.

דיווח של ספקים על אירועי סייבר - 13 (30%) מתוך 44 משרדי הממשלה וגופי התמ"ק דיווחו שחוו אירוע סייבר בשנתיים האחרונות (בשנים 2021 - 2022) שמקורו בשרשרת האספקה, ואולם 8 (62%) מתוך 13 משרדי הממשלה וגופי התמ"ק האלו לא קיבלו עדכון על כך מהספק עצמו אלא מגורמים אחרים (כגון מערך הסייבר או אמצעי תקשורת). כמו כן, במכרזים מרכזיים שמפרסם מינהל הרכש לאחר שנת 2021, עם תחילת השימוש בנספח אבטחת מידע, מצוינת חובתו של הספק לדווח ישירות למינהל הרכש על כל אירוע סייבר שהתרחש אצלו, מייד לאחר התרחשותו, אולם לא מצוינת חובתו של הספק לדווח על כך למערך הסייבר. מכיוון שבמינהל הרכש אין מוקד שתפקידו לקבל פניות על חשש לאירועי סייבר ולנתח את המידע המתקבל - כמו המוקד שבמערך הסייבר - הדבר עלול לגרום לחוסר טיפול באירוע או לשיהוי בתגובה ולסכן את המשרדים.

נספח אבטחת מידע - הן בטיוטת נספח ז' של הוראת התכ"ם 7.3.1 שפרסם מינהל הרכש והן בהנחיה 5.19 שפרסמה יה"ב נכללה הנחיה למשרדים להוסיף במכרז ההתקשרות שלהם עם הספק נספח אבטחת מידע. נמצא כי שתי ההנחיות הללו אינן עולות בקנה אחד, וכל הנחיה מפנה לנספח אבטחת מידע ובו סעיפים בנושאים שונים. עקב כך המשרדים יתקשו לדעת איזה נספח עליהם לצרף למכרזים שלהם. הקושי הנובע מקיומם של הנחיות ונספחים שונים מקבל משנה תוקף נוכח העובדה שההנחיות מיועדות לקהלי יעד שונים (הוראת תכ"ם - לבעלי תפקידים ברכש והנחיית יה"ב - לממוני הגנת הסייבר), ובחלק מהארגונים ממוני הגנת הסייבר אינם מעורבים בתהליכי הרכש.

שיתוף גורמי הגנת הסייבר של הארגון בתהליכי הרכש - 19 (43%) מתוך 44 משרדי הממשלה וגופי התמ"ק שהשיבו על השאלון ציינו כי ממונה הגנת הסייבר או הממונה על שרשרת האספקה אינו מעורב בכל תהליכי הרכש בתחום התקשוב והסייבר בארגון. עוד

נמצא כי ב-14 (40%) מתוך 35 משרדי הממשלה וגופי התמ"ק שהשיבו על השאלה הממונה על הגנת הסייבר אינו מעורב בתהליך סיום ההתקשרות עם הספק ואינו מוודא שהספק ממלא את חובותיו בנושא סיום ההתקשרות (מחיקת המידע, החזרת האמצעים, ניתוק גישה מרחוק ועוד). הדבר מעורר חשש כי היבטי אבטחת מידע לא יקבלו ביטוי בהתקשרויות השונות של המשרד בתחום התקשוב והסייבר ויחשפו את משרדי הממשלה ואת גופי התמ"ק לסיכוני אבטחת מידע במהלך תקופת ההתקשרות.

תיאום בין הגופים האסדרתיים הפועלים בתחום שרשרת האספקה - נמצא כי הגופים האסדרתיים (מערך הסייבר, יה"ב, שב"כ, מלמ"ב, הרשות להגנת הפרטיות, יחידות הסייבר המגזריות) ומינהל הרכש קבעו דרישות שונות בנושא שרשרת האספקה ללא תיאום ותכלול של הדרישות. מצב זה אינו עולה בקנה אחד עם החלטת הממשלה 2118 מאוקטובר 2014, שמטרתה להפחית את הנטל הרגולטורי. כמו כן נמצא כי לא נוצרו שיתופי פעולה בין הגופים האסדרתיים כדי לבחון את האפשרות לשיתוף משאבים ביניהם ולבניית מערכים משותפים וכן לשתף מידע וידע בתחום.

משרד מבקר המדינה מציין לחיוב את ששת המשרדים שמיישמים את המתודולוגיה ברמה גבוהה (ציון 74 ומעלה): גוף 31, גוף 22, גוף 18, גוף 28, גוף 8 וגוף 34.

אף כי למערך אין סמכות בנוגע לחברות לאחסון ולאירוח של אתרים, ב-CERT הלאומי נעשים מאמצים, באמצעות מרכז הממשקים, לקביעת סטנדרטים נדרשים לחברות האחסון, שהן "הבטן הרכה" במגזר ה-IT. עד למועד סיום הביקורת במאי 2023 13 חברות הביעו את הסכמתן הוולונטרית למהלך, והמימוש אמור להתחיל בשנת 2023, בכפוף להשלמת התהליך הפנימי במערך.

משרד מבקר המדינה מציין לחיוב את גוף 20, את גוף 44, את גוף 35 (ברשת המסווגת), את גוף 46, ואת גוף 47 על שהשקיעו משאבים ייעודיים בניהול סיכונים הנוגעים לשרשרת האספקה מעבר לנדרש לפי מתודולוגיית שרשרת האספקה.

עיקרי המלצות הביקורת

- מומלץ כי מערך הסייבר ויה"ב, האחראים לגיבוש מתודולוגיית שרשרת האספקה וההנחיות הנובעות ממנה ולפיקוח על יישומם בפועל, יקיימו מעקב שוטף אחר מידת היישום של מתודולוגיה 1.4 ויפעלו מול הגופים למציאת פתרונות לפערים, אם יעלו. עוד מומלץ כי מערך הסייבר יוציא ליחידות הסייבר המגזריות הנחיה רוחבית ליישום גרסה 1.4 של מתודולוגיית שרשרת האספקה בגופים המונחים שלהן ויעקוב אחר יישום המתודולוגיה כדי לוודא שניתן מענה על הפערים שנמצאו ביישום גרסה 1.3 של המתודולוגיה.

- מומלץ כי מינהל הרכש יכלול את דרישות הגופים האסדרתיים בתחום הסייבר במכרזיו ובפרט את הדרישה ליישם את מתודולוגיית שרשרת האספקה גרסה 1.4, ובמקרים בהם

הוא סבור כי יש קושי ליישם דרישות אלו כהווייתן או יש חלופה טובה יותר, מומלץ כי הוא ידון בסוגיה זו עם הגופים האסדרתיים ויקבל את הסכמתם ליישום דרישות חלופיות.

מומלץ כי הגופים האסדרתיים בתחום הסייבר (מערך הסייבר, יה"ב) יפעלו לקבל את מיפוי הספקים המהותיים מהגופים המונחים שלהם ואת מיפוי הספקים שזכו במכרזים מרכזיים בתחום התקשוב והסייבר ממינהל הרכש, וכי הגופים האסדרתיים יהיו אחראים לעדכון רשימות אלו באופן עיתי. כך יוכלו הגופים האסדרתיים לקבל תמונה מקיפה על רמת החשיפה של המשרדים לספקים אלו ולבצע, במקרה הצורך, פעולות יזומות מולם להעלאת רמת ההגנה שלהם. עוד מומלץ שהגופים האסדרתיים בתחום הסייבר יעבירו את רשימת הספקים המהותיים למרכז מודיעין והכוונה במערך הסייבר כדי שהוא יוכל לכסות את הספקים האלו בצי"ח המודיעיני ולהתריע לפני המשרדים אם עולה חשש לפגיעה בהם.

מומלץ כי מערך הסייבר יבחן את סוגיית ההסדרה של גופים כמו חברות IT ואינטגרציה וחברות אירוח אתרים ובכלל זה את היכולת שלהם ליישם את מתודולוגיית שרשרת האספקה, אם בדרך של אסדרה ואם בדרך אחרת. עוד מומלץ כי מערך הסייבר יבחן סוגיה זו בתיאום עם גופים אסדרתיים רלוונטיים בתחום אבטחת המידע והגנת הסייבר כמו מלמ"ב והרשות להגנת הפרטיות.

מומלץ כי הגופים האסדרתיים בתחום הסייבר (מערך הסייבר, יה"ב) יבחנו דרכים להפחתת העלויות שחלות על הגוף שמבקש להוסיף דרישה לעמידה במתודולוגיית שרשרת האספקה לספקים שנותנים שירות לגופי תמ"ק ולמשרדים רבים, למשל באמצעות התעדה משותפת של כמה גופים ובאמצעות סיוע של בודק ספקים מוסמך מטעם הגוף האסדרתי שיבחן את עמידת הספק בבקרות הנדרשות במתודולוגיה.

מומלץ כי מינהל הרכש, מערך הסייבר ויה"ב יגדירו יחד את סוגי המכרזים המרכזיים וסוגי השירותים בתחום התקשוב והסייבר אשר יש תועלת שגוף אסדרתי בתחום הגנת הסייבר יבצע ביקורות עליהם, בדגש על מכרזים מרכזיים שרמת הסיכון והרגישות בהם גבוהה, ויפעלו מול המזמין לשילוב הוראה במכרז המאפשרת להם לבצע ביקורת בנושא. עוד מומלץ כי משרדי ממשלה וגופי תמ"ק שלא ביצעו ביקורות על הספקים המהותיים שלהם יעשו זאת ויעקבו אחר תיקון הליקויים שנמצאו אצל הספקים.

מומלץ כי למכרזים מרכזיים בתחום התקשוב והסייבר וכן לנוסח הסופי של טיוטת נספח ז' בהוראת התכ"ם 7.3.1 תתווסף הנחיה המחייבת את הספק לדווח הן למערך הסייבר והן למזמין על כל חשש לאירוע אבטחת מידע וסייבר שיתרחש אצלו. עוד מומלץ כי הגופים האסדרתיים בתחום הסייבר וגורמים המנחים את עצמם ומשתמשים במכרזים מרכזיים יעבירו למינהל הרכש באופן עיתי סיכום של האירועים שהתרחשו אצל הספקים שזכו בכל מכרז מרכזי ושל אופן הטיפול בהם והמלצות להמשך העבודה עם הספק.

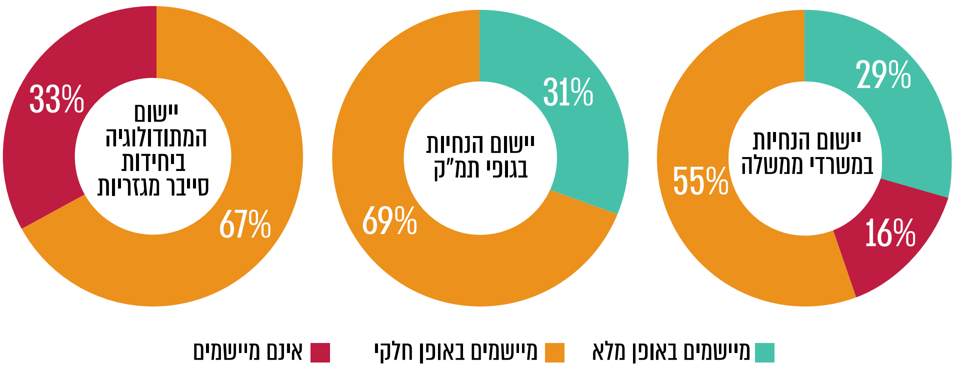
מומלץ כי מינהל הרכש יגבש עם הגופים האסדרתיים בתחום אבטחת המידע והסייבר (שב"כ, מלמ"ב, מערך הסייבר, יה"ב והרשות להגנת הפרטיות) נספח אבטחת מידע שיצורף לכל מסמך התקשרות או שינחה שכל ארגון יצרף נספח אבטחת מידע בהתאם להנחיות הגוף האסדרתי שמנחה אותו בתחום אבטחת מידע והגנת הסייבר.

מומלץ כי אגף החשכ"ל במשרד האוצר יעדכן את הוראות התכ"ם הרלוונטיות באופן שהן יחייבו את המשרדים לערב את ממונה הגנת הסייבר או את ממונה שרשרת האספקה

בתהליכים הנוגעים לרכש בנושא תקשוב וסייבר, ובכלל זה בתהליך סיום ההתקשרות עם הספק, ויקבל מהם דרישות אבטחת מידע לשם מתן מענה כולל והולם על סיכוני סייבר שעלולים להיות כרוכים בתהליך המכרז עצמו.

מומלץ כי מערך הסייבר יפעל לכינוס כל הגופים האסדרתיים המטפלים בתחום שרשרת האספקה (מערך הסייבר, יה"ב, שב"כ, מלמ"ב, הרשות להגנת הפרטיות, יחידות הסייבר המגזריות) ומינהל הרכש כדי לבצע תכלול בין המתודולוגיות השונות, לדון בנושאים משותפים כמו תקינה בין-לאומית, לבדוק את האפשרות להשקעת משאבים משותפת, ליצירת מערכים משותפים ולהקמת פורום מקצועי בנושא שרשרת האספקה.

יישום המתודולוגיה וההנחיות בארגונים שנבדקו



על פי תשובות על השאלון שהעביר משרד מבקר המדינה, בעיבוד משרד מבקר המדינה.

מידת יישום המתודולוגיה בגופי תמ"ק

מהשאלון עולה כי 7 (54%) מתוך 13 גופי התמ"ק שהשיבו על השאלון אינם מיישמים לפחות 25% מהנושאים שנכללים במתודולוגיית שרשרת האספקה.

הנושאים שנבדקו	גוף 38	גוף 39	גוף 16	גוף 5	גוף 45	גוף 15	גוף 20	גוף 43	גוף 1	גוף 21	גוף 11	גוף 2	גוף 19
ביצוע סקר סיכונים שכלל התייחסות לנושא שרשרת האספקה	✗	✗	✓	✗	✗	✓	✗	*	✗	✗	✗	✓	✓
ספקי A שעברו תהליך התעדה בהתאם למערך הסייבר	*	✗	✗	✗	*	✗	✓	*	*	✓	✗	✗	✗
איסוף מודיעין סייבר ומודיעין עסקי על ספקי הארגון	✗	✗	✗	✓	✗	✓	✗	*	✓	✗	✓	✗	✓
מעורבות של הממונה על הגנת הסייבר בתהליך סיום ההתקשרות עם הספק	*	✓	✗	✗	✗	✗	✗	✗	✓	✓	✓	✓	✗
סעיף במכרזי הארגון המחייב עבודה לפי המתודולוגיה של מערך הסייבר	✗	✗	✗	✗	✓	✓	✓	✗	✗	✓	✓	✓	✓
קיום מיפוי של כלל הספקים הכולל את כל פרטי המידע הנדרשים במתודולוגיה	✗	*	✗	*	✗	✓	✓	✗	*	✗	*	✗	*
מינוי בעל תפקיד ייעודי לנושא שרשרת האספקה	✗	✗	✓	✓	✓	✓	✗	✓	✗	✓	✓	✓	✓
סיוע של הגורם המאסדר בתהליך מיפוי הספקים	✗	✗	✗	✓	✓	✓	✗	*	✓	✓	✓	*	✓
ביצוע בקרות אצל הספקים בשלוש השנים האחרונות (2020 - 2022)	✗	✓	✓	!	*	✗	!	*	!	*	✗	✓	!
מתן הנחיה לספקי A לעבור התעדה	*	✓	✗	✗	*	✗	!	*	*	✓	✓	✓	!
מעקב שנתי אחר תיקון הליקויים שנמצאו אצל הספק	✗	✓	✓	✓	✗	✗	✓	*	*	*	✓	✓	✓
סעיף במכרז שמחייב את הספק להודיע לארגון על אירוע סייבר במוצר או בשירות המסופק	✗	✓	✓	✗	✓	✓	✓	✓	✓	✓	✓	✓	✓
הפעלת סנקציה נגד ספקים שלא עמדו ברמת ההגנה הנדרשת בתקופת ההתקשרות	✗	✗	✓	*	*	*	*	*	*	*	✓	✓	✓
עבודה לפי מתודולוגיית שרשרת האספקה של מערך הסייבר	✓	✓	✗	✓	✓	✓	✓	✓	✗	✓	✓	✓	✓
סעיף במכרז שמתיר לארגון לבצע ביקורות סייבר אצל הספק	✗	✓	✓	✗	✓	✓	✓	✓	✓	✓	✓	✓	✓
נושא שרשרת האספקה נדון במסגרת ועדות ההיגוי	✓	✗	✓	✓	✓	✓	✓	✗	✓	✓	✓	✓	✓
קיום ספק מהותי בארגון	✗	✓	✓	✓	*	✓	✓	*	*	✓	✓	✓	✓
ביצוע תרגולים לתקיפת סייבר באמצעות שרשרת האספקה	✓	✗	✓	✓	*	✓	✓	✓	✓	✓	✓	✓	✓
מעורבות ממונה הגנת הסייבר או הממונה על שרשרת האספקה בתהליכי הרכש	✓	!	✓	!	!	!	✓	✓	✓	✓	✓	!	✓
יישום ההנחיות של הגורם המאסדר	!	!	!	!	!	✓	!	!	✓	!	✓	!	✓
שיעור הנושאים שהגופים יישמו באופן מלא או חלקי	**40%**	**55%**	**60%**	**65%**	**75%**	**75%**	**75%**	**80%**	**80%**	**85%**	**85%**	**85%**	**90%**

✓ כן

✗ לא

! באופן חלקי

* לא נמסר מידע/ לא רלוונטי

על פי תשובות על שאלון שהעביר משרד מבקר המדינה, בעיבוד משרד מבקר המדינה.

סיכום

איום הייחוס לתקיפת סייבר באמצעות שרשרת האספקה הוא אחד האיומים המשמעותיים על ארגונים במשק. 86% מ-43 הארגונים שהשיבו על השאלון ציינו כי תקיפה באמצעות שרשרת האספקה היא איום ייחוס שלהם וכ-30% מהארגונים שהשיבו על השאלון דיווחו שחוו אירוע סייבר בשנתיים האחרונות (בשנים 2022-2021) שמקורו בשרשרת האספקה. האתגר בהתמודדות עם איום זה נובע מהעובדה שההגנה הנדרשת על הספק היא לכאורה מחוץ לתחום סמכותו של הארגון.

מדוח זה עולה כי יש ספקים שנותנים שירות לעשרות משרדי ממשלה וגופי תמ"ק ולכן פגיעה בהם עשויה לפגוע פגיעה נרחבת ברציפות התפקודית של הממשלה והמשק.

מערך הסייבר כגוף אסדרתי שאחראי לקדם את רמת הגנת הסייבר במשק גיבש בשנת 2018 מתודולוגיה לניהול האיום הנשקף משרשרת האספקה. ממצאי דוח זה, אשר ביסודו עומדת בחינה של יישום המתודולוגיה של מערך הסייבר במשרדי ממשלה, ביחידות הסמך, בגופי תמ"ק וביחידות הסייבר המגזריות, מעידים על כמה פערים הנוגעים לנושא, כמפורט להלן:

1. כשש שנים לאחר שמערך הסייבר גיבש את המתודולוגיה בנושא שרשרת האספקה היא לא מוטמעת במשק, ויש ארגונים שטוענים שאי אפשר ליישמה. נמצא כי 55% ממשרדי הממשלה וגופי תמ"ק שהשיבו על השאלון אינם עובדים לפי מתודולוגיית שרשרת האספקה, ונוכח זאת חלק גדול מהספקים של הארגונים אינם נבדקים בצורה אחודה ובהתאם לבקרות שהגדיר מערך הסייבר.

2. נמצאו פערים משמעותיים ביישום המתודולוגיה שלא ניתן להם מענה על ידי מערך הסייבר, כמו חוסר יכולת ליישם את הדרישות מול ספקים בין-לאומיים, עלויות גבוהות של התעדה ותהליך התעדה ארוך שאינו בהלימה לצרכים העסקיים של הארגונים.

3. מהדוח עולה כי למשרדי הממשלה יש 18 ספקים עיקריים בתחום התקשוב והסייבר שנותנים שירותים לארגונים רבים - מתוכם חמישה ספקים נותנים שירות ליותר מ-49 משרדים, ושלושה ספקים נותנים שירות בהיקף כספי שנתי של יותר מ-327 מיליוני ש"ח. ספקים אלו אינם מותעדים, ועל חלקם לא מתבצעות בקרות בתחום שרשרת האספקה - דבר שמסכן את הארגונים שהם נותנים להם שירות. כמו כן הגופים האסדרתיים בתחום הסייבר אינם פועלים למיפוי ספקים אלו ולקידום ההתעדה שלהם.

4. מינהל הרכש אינו מונחה על ידי שום גוף אסדרתי בתחום הסייבר. כמו כן, במכרזים המרכזיים אין דרישה של מינהל הרכש מהספקים שעימם הוא מתקשר ליישם את מתודולוגיית שרשרת האספקה ודרישות אבטחה נוספות שגופי האסדרה דורשים מהמשרדים, אף שהיקף הכספי של התקשרויות אלו הוא בממוצע כ-57% מכלל ההתקשרויות של המשרדים בתחום התקשוב והסייבר. נוסף על כך, שום גורם אינו מבצע ביקורות על רמת הגנת הסייבר של הספקים שזכו במכרזים מרכזיים.

5. הממונה על הגנת הסייבר במשרדי הממשלה ובגופי התמ"ק אינו מעורב בתהליכי הרכש בתחום התקשוב והסייבר בארגון ובכלל זה אינו מעורב בתהליך סיום

ההתקשרות עם הספק כדי לוודא שהספק ממלא את חובותיו בנושא סיום ההתקשרות (מחיקת המידע, החזרת האמצעים, ניתוק גישה מרחוק ועוד).

6. משרדים וגופי תמ"ק דיווחו שחוו אירוע סייבר בשנתיים האחרונות (בשנים 2021 - 2022) שמקורו בשרשרת האספקה, ואולם הם לא קיבלו עדכון על כך מהספק עצמו אלא מגורמים אחרים (כגון מערך הסייבר או אמצעי תקשורת). כמו כן, מינהל הרכש אינו מחייב את הספקים שזכו במכרזים מרכזיים לדווח על אירועי סייבר גם למערך הסייבר.

7. הגופים האסדרתיים בתחום הסייבר (מערך הסייבר, יה"ב, שב"כ, מלמ"ב, הרשות להגנת הפרטיות, יחידות הסייבר המגזריות) ומינהל הרכש מתווים מתודולוגיות שונות בתחום שרשרת האספקה ולא מתבצע תכלול של הדרישות, ועקב כך נוצר נטל רגולטורי על הארגונים והספקים.

מכלול הפערים האמורים מחייבים הערכת מצב לגבי המענה המתודולוגי הקיים ודרך מימושו, שכן ממצאיו מלמדים כי נשקף סיכון ממשי לגופי תמ"ק, למשרדי ממשלה ולמגזרים מצד שרשרת האספקה בתחום התקשוב. על מערך הסייבר והגופים האסדרתיים בתחום הסייבר ומינהל הרכש לפעול לקיום הערכת מצב זו. בד בבד על כלל משרדי הממשלה וגופי התמ"ק שנבדקו לפעול, כל אחד על פי תחום אחריותו, לתיקון הליקויים שהועלו בדוח זה על מנת להבטיח שיפור ברמת ההגנה של הספקים ושל המשק כולו.

במהלך הביקורת עדכנו מערך הסייבר הלאומי ויה"ב את הנחיותיהם למשרדים ולגופי התמ"ק, בין היתר כדי לתת מענה על פערים שהוצגו בדוח זה. מוצע אפוא כי מערך הסייבר ויה"ב יעקבו כבר במהלך השנה הקרובה אחר אופן הטמעת המתודולוגיה העדכנית ואחר ישימותה הלכה למעשה.

ניהול סיכוני סייבר מצד שרשרת האספקה בתחום התקשוב

מבוא

בעידן הנוכחי כמעט שלא קיימים חברות וארגונים האחראים לבדם לכל שלבי התכנון, הפיתוח, השיווק והאספקה של המוצרים והשירותים שהם צורכים ומספקים. לחלופין, ארגונים רוכשים את שירותיהן של חברות המתמחות בתחומים שונים ומנהלים תהליך עבודה יעיל וזול יותר. שרשרת אספקה היא מונח המתייחס לכלל המשאבים והתהליכים הקשורים בספקים, בלקוחות ובקבלני ביצוע, אשר דרושים לצורך אספקת מוצר או שירות בארגון.

מתקפות סייבר המתבצעות באמצעות שרשרת האספקה מכוונות לפגוע באחד מספקי הארגון, מנצלות את האמון שהארגון נותן בספק שלו כדי לחדור באמצעותו אל הארגון.

בשנים האחרונות חל גידול ניכר במספר מתקפות הסייבר על ארגונים ועוצמתן גברה, וכיום מתקפות סייבר המתבצעות באמצעות שרשרת האספקה שלהם הן אחד האיומים החמורים ביותר הנשקפים לכלל המשק. על מנת לנהל את סיכון הסייבר שאליו הארגון חשוף מצד נותני השירות והספקים שלו, על הארגון לנתח את סיכוני הסייבר הפוטנציאליים הכרוכים בהתקשרויות עימם ולהיערך אליהם.

מפרסום של חברת המחקר גרטנר מאפריל 2022[4], המציג את המגמות המובילות בתחום הגנת הסייבר לשנת 2022, עולה כי עד שנת 2025 יושפעו 45% מהארגונים הגלובליים, בדרך זו או אחרת, ממתקפת סייבר באמצעות שרשרת האספקה, גידול של 300% לעומת שנת 2021.

הגורמים בשרשרת האספקה שהפגיעה בהם עלולה להיות חמורה במיוחד הם הספקים שנותנים שירותים לארגונים רבים או לתשתיות מדינה קריטיות[5] (להלן - גופי תמ"ק), זאת משום שפגיעה בהם עלולה לפגוע ברציפות התפקודית של המשק או לגרום לדלף מידע רגיש במיוחד. דוגמה למתקפת סייבר על שרשרת האספקה שגרמה לפגיעה בתשתית מדינה קריטית היא מתקפת הכופר על חברת הנפט האמריקנית Colonial Pipeline במאי 2021. האירוע גרם לשיבושים בשינוע דלקים במזרח ארצות הברית והביא להכרזה על מצב חירום במדינה.

מערך הסייבר הלאומי (להלן - מערך הסייבר) מעריך[6] כי איום על שרשרת האספקה נוגע לכ-1,700 חברות ישראליות, ובהן חברות המספקות שירותי תוכנה (IT), חברות אירוח ואחסון

4 https://www.gartner.com/en/articles/7-top-trends-in-cybersecurity-for-2022

5 גופים אלו מוגדרים בחוק להסדרת הביטחון בגופים ציבוריים, התשנ"ח-1998 ומכונים גם גופים בעלי מערכות מחשוב חיוניות.

6 מערך הסייבר, **טיפול מערך הסייבר הלאומי בשרשרת האספקה** (25.1.23).

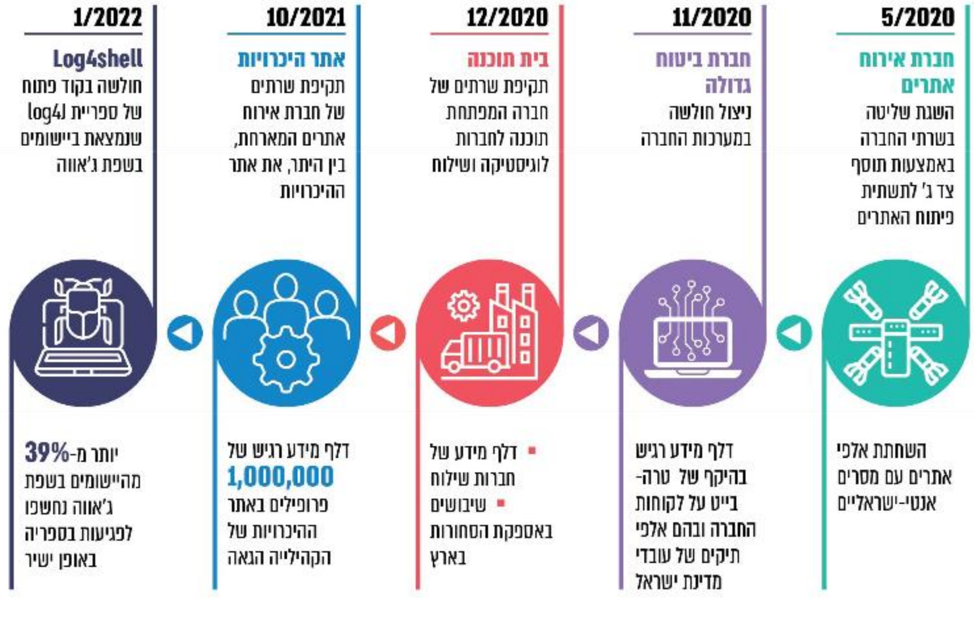
של אתרים (Hosting), ספקים הנותנים שירותי ענן[7] וחברות אינטגרציה. כמו כן איום זה נוגע לכ-1,500 חברות בין-לאומיות המספקות שירותים למשק הישראלי.

להלן דוגמאות לדרכי תקיפה באמצעות שרשרת האספקה:

- השתלטות על עמדת גישה מרחוק של ספק הנותן תמיכה לארגון ושימוש באמצעי הגישה מרחוק (VPN) לשם החדרת נוזקה לארגון.
- השגת גישה למערכות הספק באמצעות שליחת הודעות דואר אלקטרוני כוזבות ("פישינג", "דיוג") כדי לקנות אחיזה בארגון.
- הטמנת פגיעות תוכנה מכוונות כנגד הארגון בסביבת הפיתוח של הספק (לרבות בקוד פתוח), כדי שהארגון יתקין את המוצר "המטופל" בחצרותיו.
- ניצול לרעה של פגיעות תוכנה הקיימות במוצר שהארגון רכש מגורם חיצוני.

להלן דוגמאות מהשנים האחרונות למתקפות סייבר חמורות על שרשרת האספקה של משרדי ממשלה וחברות בישראל ולהיקף הנזק בגינן:

תרשים 1: **מתקפות סייבר על שרשרת האספקה של משרדי ממשלה וחברות בישראל בשנים 2020 - 2022 והיקף הנזק בגינן**



המקור: משרד מבקר המדינה.

7 רשת מחשבים רבת עוצמה שמספקת למשתמשיה, המתחברים אליה מרחוק באמצעות המרשתת (האינטרנט), שירותי מחשוב שונים בהיקף המתאים לצורכיהם, כגון שטח אחסון, עיבוד, אבטחה, שירותי מרשתת ועוד.

הגופים האסדרתיים בתחום הגנת הסייבר המוזכרים בדוח

הגופים האסדרתיים[8] בתחום הגנת הסייבר זיהו את סיכוני הסייבר הנשקפים לשרשרת האספקה כאחד הסיכונים המורכבים ביותר למניעה ולגילוי וגיבשו מתודולוגיות והנחיות ייעודיות לנושא:

1. **מערך הסייבר:** גוף ממלכתי, מבצעי וטכנולוגי האמון על הגנת מרחב הסייבר הלאומי ועל הקידום והביסוס של עוצמתה של ישראל בתחום זה. מערך הסייבר משמש מאסדר בנוגע לגופי התמ"ק המנויים בחוק להסדרת הביטחון בגופים ציבוריים, התשנ"ח-1998 (להלן - החוק להסדרת הביטחון)[9], וכן מנחה את יחידות הסייבר המגזריות בהתאם להחלטת הממשלה 2443[10]. במסגרת תפקידו גיבש מערך הסייבר מתודולוגיה לאומית הקרויה תורת ההגנה בסייבר לארגון (להלן - תורת ההגנה). בשנת 2018 פרסם המערך מתודולוגיה ייעודית למשק בנושא שרשרת האספקה (להלן - מתודולוגיית שרשרת האספקה).

2. **היחידה להגנת הסייבר בממשלה (להלן - יה"ב):** יחידה האחראית להכוונה ולהנחיה המקצועית בתחום הגנת הסייבר עבור כלל משרדי הממשלה ויחידות הסמך (להלן - משרדי הממשלה או המשרדים). היחידה פרסמה בנובמבר 2019 את הנחיה 5.19 בנושא שרשרת האספקה, המבוססת על המתודולוגיה של מערך הסייבר (להלן - הנחיית יה"ב), וכן הנחתה את כל המשרדים במסגרת החלטת ממשלה 2443 לעמוד בתקן ישראלי ISO-27001, שכמה מסעיפיו עוסקים גם בנושא יחסי הגומלין עם ספקים[11].

3. **יחידות הסייבר המגזריות:** יחידות אלו הן חלק ממשרדי הממשלה ותפקידן להנחות את המשק - כל אחת בתחום עיסוק המשרד.

4. **הרשות להגנת הפרטיות:** הרשות להגנת הפרטיות היא המאסדר המופקד על הגנת המידע האישי במאגרי מידע דיגיטליים בהתאם לסמכויות שהוקנו לה בחוק הגנת הפרטיות, התשמ"א-1981, ובתקנות שהותקנו מכוחו ובהן תקנות הגנת הפרטיות (אבטחת מידע) התשע"ז-2017 (להלן - תקנות אבטחת מידע). בידי הרשות סמכויות אכיפה פליליות וסמכויות אכיפה מינהליות ביחס לכל גוף המחזיק או המעבד מידע אישי, אם הוא פרטי ואם הוא ציבורי. תקנה 15 לתקנות אבטחת מידע עוסקת בחובות החלות על בעל מאגר המתקשר עם גורם חיצוני לצורך קבלת שירות הכרוך במתן גישה למאגר מידע (להלן - מיקור חוץ). הרשות פרסמה לאורך השנים הנחיות ומדריכים המתייחסים לאופן ההתנהלות הנדרש מבעלי מאגר מידע בעת שימוש בשירותי מיקור חוץ.

8 ששת הגופים המנויים בפרק זה מכונים לצורך הדוח: "הגופים האסדרתיים", אף שחלקם אינם עונים להגדרת המונח "מאסדר" בהתאם להוראת סעיף 3 לחוק עקרונות האסדרה, התשפ"ב-2021, זאת משום שהם משמשים גורמים מנחים מרכזיים בתחום הגנת המידע והסייבר במדינת ישראל.

9 הגופים המנויים בתוספת החמישית לחוק להסדרת הביטחון והגופים המנויים הן בתוספת השנייה והן בתוספת החמישית לחוק להסדרת הביטחון.

10 החלטת הממשלה 2443, "קידום אסדרה לאומית והובלה ממשלתית בהגנת הסייבר" (15.2.15).

11 סעיף A15 בתקן, "יחסי גומלין עם ספקים" (2013).

5. **שירות הביטחון הכללי (להלן - שב"כ):** מנחה מקצועית בתחום ההגנה על הסוד והגנה על התשתיות הקריטיות במדינת ישראל מתוקף החוק להסדרת הביטחון[12].

6. **הממונה על הביטחון במשרד הביטחון (להלן - מלמ"ב):** אחראי מכוח החוק להסדרת הביטחון[13] להנחיית 26 ארגונים וחברות פרטיות שהוגדרו בצו כמבצעות פרויקטים מסווגים[14]. מלמ"ב גיבש תקינה להגנה על רשתות המכילות מידע רגיש המבוססת על תקן CMMC[15] של משרד ההגנה האמריקאי לצורך ניהול הסיכונים מצד שרשרת האספקה במגזר תעשיית הביטחון.

רכש ממשלתי בתחום תקשוב וסייבר

הרכש הממשלתי נעשה באמצעות התקשרויות עם ספקים. משרדי הממשלה יכולים לחייב ספקים פוטנציאליים לעמוד בדרישות הסף בתחום הגנת הסייבר באמצעות הכללתן כתנאי סף במכרזים. במסגרת פעילותו של כל משרד ממשלתי לניהול הסיכון בעניינו עליו לתת את הדעת על כל מחזור חיי ההתקשרות עם הספק, החל בשלב כתיבת המכרז וחוזה ההתקשרות וכלה בשלב סיום ההתקשרות.

משרדי ממשלה מבצעים רכש על פי הכללים האלו:

1. **חוק חובת המכרזים ותקנותיו:** על פי ההוראות של חוק חובת המכרזים, התשנ"ב-1992, ותקנות חובת מכרזים, התשנ"ג-1993, משרדים מחויבים לבצע מכרז כל אימת שהם מבצעים רכישה מעל סכום מסוים (נכון למועד סיום הביקורת במאי 2023 - 50,000 ש"ח).

2. **תקנון כספים ומשק (להלן - תכ"ם):** הוראות שמפרסם אגף החשב הכללי במשרד האוצר (להלן - החשכ"ל) ומחייבות את המשרדים, ובהן הנחיות מקצועיות ואופרטיביות בנושאים כספיים שונים. למשל: הנחיות בדבר המסמכים שעל המשרדים לצרף לכל מכרז.

משרדי ממשלה יכולים להתקשר עם ספקים בכמה אופנים:

1. מכרזים שהמשרד מפרסם עבור עצמו (להלן - מכרז משרדי).

2. מכרזים מרכזיים שבאמצעותם מינהל הרכש הממשלתי[16] (להלן - מינהל הרכש) מתקשר עם ספק לקבלת טובין או שירות עבור כלל משרדי הממשלה כדי למצות את היתרון לגודל של כלל משרדי הממשלה. כאשר יש מכרז מרכזי מחויבים המשרדים לפי הוראת תכ"מ 7.8.2[17] להזמין את המוצרים או את השירותים רק מהספקים שזכו במכרז המרכזי, והם אינם רשאים לערוך מכרז משרדי ולא להתקשר בכל דרך אחרת, לקבלת הצעות בהתקשרות

---

12 הגופים המונחים על ידי השב"כ הנמנים בתוספת הראשונה, השנייה והרביעית בחוק.

13 החוק להסדרת הביטחון, הגופים המנויים בסעיפים 2 ו-3 לתוספת הראשונה.

14 תפקידי מלמ"ב מעוגנים במסגרת החלטת הממשלה 2444 (15.2.15).

15 Cybersecurity Maturity Model Certification, Version 2.0 (December 2021)

16 יחידת מטה בחטיבת משרדים כלכליים שבאגף החשכ"ל, מתוך אתר מינהל הרכש: https://mr.gov.il/ilgstorefront/he/about

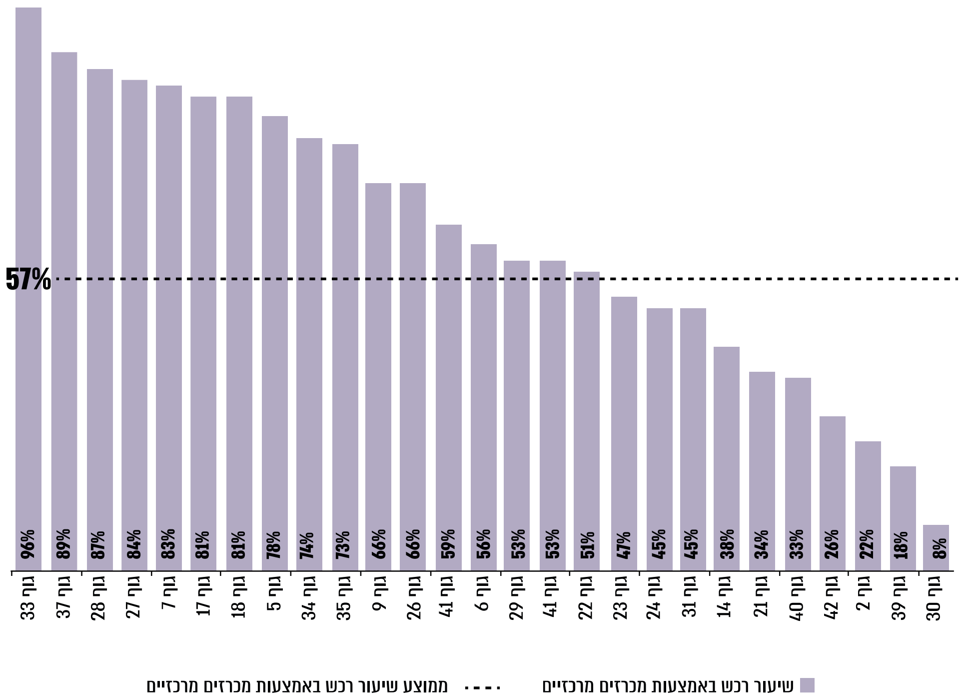
17 הוראת תכ"ם 7.8.2: "מכרז מרכזי והתחייבות ספק לתנאים ומחירים מוסכמים".

באותו נושא, שלא באמצעות המכרז המרכזי אלא אם קיבלו לכך אישור מוועדת הפטור במשרד האוצר. דוגמאות למכרזים מרכזיים בתחום התקשוב והסייבר: מכרז לרכש הטלפונייה VOIP (להלן - מערכת שירלי), מכרז לרכש אנטי-וירוס, מכרז לקבלת שירותי אירוח עבור משרדי הממשלה (DR).

3. התקשרויות בפטור ממכרז בכפוף לתקנות חובת מכרזים, התשנ"ג-1993.

להלן תרשים, המבוסס על נתונים ממערכת הרכש הממשלתית[18], אשר מציג את היקף הרכש הממשלתי בנושאי תקשוב וסייבר של כלל משרדי הממשלה שהשיבו על השאלון שהפיץ משרד מבקר המדינה בנושא שרשרת האספקה (להלן - השאלון) כחלק מתהליך הביקורת. ההיקף הכספי של רכש זה בשנת 2021 היה כ-2.5 מיליארד ש"ח. לצד כל משרד מוצג שיעור הרכש שהוא ביצע באמצעות מכרזים מרכזיים.

תרשים 2: **שיעור הרכש באמצעות מכרזים מרכזיים לשנת 2021 בנושאי תקשוב וסייבר בקרב משרדי הממשלה ויחידות הסמך (להלן - גופים)**



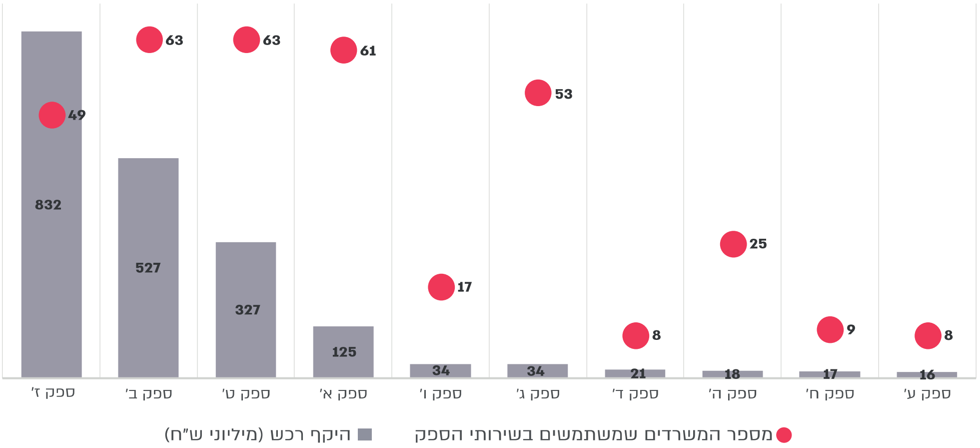
על פי נתוני מערכת הרכש הממשלתית, בעיבוד משרד מבקר המדינה.

18 עיבוד נתונים שהסתמך על נתוני מערכת הרכש הממשלתית הנכונים לשנת 2021. שליפת הנתונים נעשתה לפי המתודולוגיה של סיווג התקשרויות בתחום התקשוב שהוגדרה בדוח מבקר המדינה, 73ג (2023) "התקשרויות בפטור ממכרז בתחום התקשוב".

מהתרשים עולה כי בממוצע כ-57% מההתקשרויות של משרדי הממשלה בתחום התקשוב והסייבר בשנת 2021, שהיו בהיקף כספי של כ-1.4 מיליארד ש"ח, מבוצעות באמצעות מכרזים מרכזיים.

להלן תרשים המבוסס על נתוני הרכש הממשלתי המציג את היקף הרכש בשנת 2021 מספקים שנמצא לפי השאלון שהם נותנים שירותים בתחום התקשוב והסייבר למשרדי ממשלה ולגופי תמ"ק רבים. בנוסף התרשים מציג עבור כל ספק את מספר משרדי הממשלה שהוא נתן להם שירות בשנה זו.

תרשים 3: **ספקים בתחום התקשוב והסייבר אשר מספקים שירות למשרדים רבים (היקף כספי במיליוני ש"ח)**



על פי נתוני מערכת הרכש הממשלתית, בעיבוד משרד מבקר המדינה.

מהתרשימים ומהמענה לשאלון עולה כי יש 18 ספקים עיקריים בתחום התקשוב והסייבר שנותנים שירותים למשרדי ממשלה ולגופי תמ"ק רבים - מתוכם חמישה ספקים נותנים שירות ליותר מ-49 משרדים (ספקים ג', א', ט', ב', ז') ושלושה ספקים (ספקים ט', ב', ז') שנותנים שירות בהיקף כספי שנתי של יותר מ-327 מיליוני ש"ח.

פעולות הביקורת

בחודשים פברואר 2022 עד מאי 2023 בדק משרד מבקר המדינה את נושא ניהול סיכוני הסייבר מצד שרשרת האספקה בתחום התקשוב. הביקורת נעשתה במשרד ראש הממשלה - במערך הסייבר הלאומי ובאגף ביטחון, חירום וסייבר; במערך הדיגיטל הלאומי - ביה"ב וביחידת ממשל

זמין; במשרד האוצר - במינהל הרכש ובאגף ביטחון, חירום וסייבר. בדיקות השלמה נעשו בכמה משרדי ממשלה ובגופי תמ"ק[19]. בכלל הארגונים נבדק הנושא בנוגע לרשת הבלתי מסווגת.

במסגרת הביקורת הפיץ משרד מבקר המדינה בקרב 58 משרדי ממשלה וגופי תמ"ק (להלן - ארגונים או גופים) שאלון הבודק כיצד הם מתמודדים עם הסיכון לביצוע מתקפות סייבר על שרשרת האספקה. שאלון זה התבסס, בין היתר על נושאים ופערים שעלו בפגישות שקיים צוות הביקורת עם משרדים ועם גופי תמ"ק ומטרתו של השאלון הייתה להציג תמונת רוחב על אופן הטיפול של משרדי הממשלה ושל גופי התמ"ק בנושא מהותי זה. 44 משרדי הממשלה וגופי תמ"ק ענו על השאלון (31 משרדי ממשלה ו-13 גופי תמ"ק).

רשימת משרדי הממשלה וגופי התמ"ק שהופץ אליהם השאלון (משרדי הממשלה וגופי התמ"ק שענו על השאלון מסומנים בהדגשה): **גוף 1**, **מינהל התכנון**, **גוף 2**, **משרד האנרגייה והתשתיות**, **השירות המטאורולוגי הישראלי**, **גוף 5**, **הרבנות הראשית לישראל**, **משרד הבינוי והשיכון**, המשרד לנושאים אסטרטגיים והסברה, **משרד הרווחה והביטחון החברתי**, **רשות המים**, הנהלת בתי המשפט, **מינהל המחקר החקלאי**, הרשות להגנת הצרכן ולסחר הוגן, **רשות התחרות**, **גוף 11**, **נציבות שירות המדינה**, **גוף 15**, גוף 50, **גוף 16**, גוף 51, **המשרד לשוויון חברתי**, לשכת הפרסום הממשלתית, **משרד החקלאות ופיתוח הכפר**, **משרד התיירות**, גוף 52, **גוף 19**, **גוף 20**, **נתיב (רה"ם)**, **גוף 21**, **משרד ראש הממשלה**, משרד החדשנות המדע והטכנולוגיה, **רשות האכיפה והגבייה**, **המשרד לביטחון לאומי**, **המכון הגיאולוגי**, **משרד הכלכלה והתעשייה**, **הרשות הארצית לכבאות והצלה**, **המשרד לשירותי דת**, **משרד העלייה והקליטה**, משרד התחבורה והבטיחות בדרכים, **משרד התרבות והספורט**, משרד התקשורת, **גוף 38**, **משרד הבריאות**, גוף 53, **גוף 39**, **המינהל לחינוך התיישבותי ועליית הנוער**, **משרד העבודה**, **המשרד להגנת הסביבה**, גוף 54, **הנהלת בתי הדין הרבניים**, רשות מקרקעי ישראל, **משרד הפנים**, **גוף 43**, **גוף 45**, **משרד החוץ**, גוף 55, **משרד המשפטים**.

דוח זה מתמקד בניהול הסיכונים מצד שרשרת האספקה של משרדי הממשלה ושל גופי תמ"ק המחויבים לעמוד בהנחיות של יה"ב ושל מערך הסייבר בהתאמה, אשר במועד כתיבת הדוח היו מבוססות על גרסה 1.3 של מתודולוגיית שרשרת האספקה של מערך הסייבר. במהלך הביקורת, בדצמבר 2022, עדכן מערך הסייבר את המתודולוגיה לגרסה 1.4, בין היתר, כדי לתת מענה על חלק מהפערים שהוזכרו בדוח זה.

19 ארגונים המוגדרים בחוק להסדרת הביטחון לגופים ציבוריים, התשנ"ח-1998, כתשתיות מדינה קריטיות.

תפיסת ההפעלה של מתודולוגיית שרשרת האספקה ותהליכי גיבושה

רקע

בהחלטת ממשלה 2443 נקבע כי על מערך הסייבר ליזום פעילות רוחבית לשיפור הגנת הסייבר בסקטורים השונים[20] ובשוק הגנת הסייבר[21] ולקדם את ביצועה בפועל של פעילות זו, בכלל זה באמצעות הקמת תשתיות והפעלת מנגנונים. כמו כן נקבע בהחלטה כי על מערך הסייבר לגבש מתווה ועקרונות לרכש של מוצרים ושירותים למגזר הממשלתי[22].

משרדי ממשלה וגופי תמ"ק במשק מתמודדים עם שלושה אתגרים עיקריים בניהול הסיכונים הנשקפים משרשרת האספקה:

1. הגדרת דרישות בתחום אבטחת המידע והגנת הסייבר החלות על הספק: אין מתודולוגיה מוסכמת על כל הגופים האסדרתיים המגדירה את הדרישות מספקי השירות והמוצרים בתחום הסייבר.
2. ביצוע בקרות על ספקים: קשה למשרדי ממשלה ולגופי התמ"ק לנהל את הבקרות ואת תיקון הליקויים מול כל הספקים שלהם.
3. יעילות הבקרה: משרדי ממשלה וגופי תמ"ק רבים בודקים את רמת ההגנה בסייבר של הספקים שלהם באמצעות שאלונים, בחלק מהשאלונים מופיעות בקרות דומות. כפילות שמקורה במענה של הספק על בקרות זהות גורמת להיווצרות תקורות עודפות הן לספק והן לארגון המזמין (להלן - המזמין או הלקוח).

מתודולוגיית שרשרת האספקה של מערך הסייבר נועדה להתמודד עם האתגרים הללו באמצעות קביעת תקן לעניין הדרישות מהספקים, שמשלב בין הדרישות העולות ממשרדי הממשלה ומגופי התמ"ק לבין הדרישות של תקנים ורגולציות מקומיות ובין-לאומיות. מטרה נוספת של המתודולוגיה היא לאפשר בדיקה בעניין פעילותו של הספק לפי פרמטרים מוסכמים מראש, באופן שבו ספק שעומד בהצלחה בבדיקה יוכל לספק שירותים ליתר משרדי הממשלה וגופי התמ"ק, באותם תחומים שנבדק בעניינם, ללא הצורך בחזרה על אותן בדיקות.

המתודולוגיה הושקה בשנת 2018 והיא מפורסמת באתר של מערך הסייבר[23] כהמלצה למשק. מסמכי המתודולוגיה כוללים את שאלון הספקים (ראו פירוט להלן), מסמך דגשים הנוגעים לבודק ומסמך דגשים הנוגעים לארגון. נוסף על המתודולוגיה, יש הנחיות משלימות לגופי תמ"ק ולמגזרים שמבוססות עליה.

---

20 החלטה זו אינה חלה על הגופים המיוחדים, קרי מלמ"ב, הגופים המונחים וספקיהם בהתאם להחלטת הממשלה 3611, "קידום היכולת הלאומית במרחב הקיברנטי" (7.8.11).

21 נספח א' ו-ב' להחלטה לעיל.

22 נספח ז' להחלטה לעיל.

23 https://www.gov.il/he/departments/guides/supply_chain_guide

להלן יוצגו שלושת השלבים העיקריים של המתודולוגיה. בפרקים הבאים בדוח זה יפורטו עבור כל שלב במתודולוגיה דרכי הפעולה המומלצות למשרדי הממשלה ולגופי התמ"ק, כדי להתגונן מהסיכונים הנובעים משרשרת האספקה ואופן היישום של דרכי פעולה אלה.

תרשים 4: **שלבי מתודולוגיית שרשרת האספקה של מערך הסייבר**

המקור: מערך הסייבר.

במערך הסייבר פועלות כמה יחידות שאחראיות לגיבוש המתודולוגיה ולקידום היישום שלה. להלן יפורטו היחידות ותפקידיהן העיקריים בתחום ההגנה על שרשרת האספקה:

תרשים 5: **היחידות במערך הסייבר שמשפיעות על גיבוש מתודולוגיית שרשרת האספקה ועל קידום היישום שלה במשק**

המקור: מערך הסייבר, בעיבוד משרד מבקר המדינה

1. **יחידת התעצמות המשק ומדיניות (להלן - יחידת המדיניות):** היחידה אחראית לגיבוש המתודולוגיה של שרשרת האספקה ולעדכונה. מערך הסייבר הקצה כ-2.5 משרות לשם פעילות היחידה.

2. **עד שנת 2023[24] פעלו במערך הסייבר שני מרכזים האחראים להנחיית המשק:**

   א. היחידה להנחיית גופי תמ"ק: משנת 2016 היחידה אחראית מכוח החוק להסדרת הביטחון להנחיית כ-30 גופי תמ"ק. גופים אלו מספקים למשק שירותים חיוניים, כמו חברת חשמל, רכבת ישראל וחברת מקורות. מערך הסייבר פרסם בקרב גופי התמ"ק הנחיה מחייבת בנושא שרשרת האספקה שמבוססת על המתודולוגיה של המערך.

   ב. היחידה להכוונת גופים מגזריים במערך הסייבר: בהחלטת ממשלה 2443 נקבעה תפיסת אסדרה לאומית שמטרתה העלאה שיטתית ורציפה של רמת ההגנה במרחב הסייבר הכולל במדינה (המרחב האזרחי והמרחב הביטחוני). במסגרת ההחלטה הוקם במערך הסייבר האגף להכוונה מגזרית, שאחראי להנחיה מקצועית ישירה של יחידות הסייבר המגזריות במשרדי הממשלה, ואלו אחראיות להכוונה ולהנחיה של כל הגופים הכפופים לסמכויות האסדרה של אותו המשרד. כך שלמעשה, מערך הסייבר מנחה בעקיפין את כלל הגופים שאינם מוגדרים כתמ"ק וכפופים לסמכויות אסדרה באמצעות אגפי הסייבר המגזריים.

3. **מרכז מודיעין והכוונה:** היחידה אחראית לאיסוף מודיעין על היריבים והתוקפים ועל ניתוח המוטיבציות ודרכי הפעולה שלהם.

4. **אגף ה-CERT:** אגף האחראי לטיפול באירועי סייבר במשק.

5. **אגף ממשקים ב-CERT:** אגף האחראי להכוונה של ארגונים במשק שאינם מונחים על ידי יחידות סייבר מגזריות במשרדי הממשלה, כמו חברות ה-IT, האירוח והאחסון של אתרים וחברות האינטגרציה.

מערכים תומכים של המתודולוגיה

מערך הסייבר יצר במסגרת המתודולוגיה מערכים תומכים שמטרתם לסייע בתהליכי בחינת הספקים ובאישורם בהתאם לכללים מוגדרים. להלן פירוט:

1. **שאלון ספקים:** מערך הסייבר גיבש שאלון העוסק בכ-96 בקרות להערכת מידת ההגנה של הספק מפני מתקפת סייבר בתחום שרשרת האספקה. הבקרות נבדלות זו מזו מבחינת סוג השירות שהספק נותן. להלן סוגי השירותים שהשאלון בוחן אותם: דרישות רוחביות; גישה מרחוק; שירות מבוסס ענן; פיתוח תוכנה; אירוח ואחסון של אתרים. כל ספק צריך להשיב רק על שאלות הנוגעות לבקרות הרלוונטיות לסוג השירות שהוא מספק, למשל: ספק המספק שירותי אחסון של אתרים צריך להשיב רק על שאלות בעניין עמידתו בדרישות רוחביות ועל שאלות בעניין עמידתו בדרישות בתחום אחסון של אתרים. מערך הסייבר מנגיש שני כלים למילוי שאלון הספקים:

[24] בשנת 2023 אוחדו המרכזים בכפוף ליחידת הגנה סקטוריאלית, באופן שבכל מגזר נכללים גופי התמ"ק הרלוונטיים.

א. מערכת המידע יוב"ל (יעדים ובקרות לארגון): מערכת ממוחשבת המאפשרת להפיץ במהירות ובקלות את השאלון, להזין את התשובות על השאלון בממשק משתמש ולצפות בתשובות אלה. כמו כן, אפשר להפיק באמצעות המערכת הצהרות דיווח עצמי על סטטוס העמידה של הספק בדרישות המתודולוגיה.

ב. שאלון ספקים 1.3 בגרסת Excel.

2. **מאגר בודקי ספקים מורשים:** רשימה של בודקי ספקים חיצוניים אשר סיימו בהצלחה תהליך הכשרה שגובש על ידי מערך הסייבר. בודקים אלו ייכללו במאגר בודקי הספקים המורשים שמפרסם מערך הסייבר. כל ספק שרוצה לבצע הליך אישרור יוכל לבחור בודק ספקים מורשה ולפעול בשיתוף עימו למילוי שאלון הספקים, ובכלל זה להגיש אסמכתאות מתאימות. בודק הספקים המורשה ימסור את שאלון הספקים ואת האסמכתאות לגופי ההסמכה. נכון לפברואר 2023 נכללים במאגר כ-80 בודקים.

3. **גופי הכשרה:** מכללות שהוסמכו מטעם מערך הסייבר להכשיר את בודקי הספקים בהתאם למתודולוגיית שרשרת האספקה של המערך.

4. **גופי הסמכה:** ארגונים שהוסמכו מטעם מערך הסייבר לבצע את תהליך אשרור הספקים והנפקת תעודה המאשרת כי הספק עומד בדרישות שנקבעו במתודולוגיית שרשרת האספקה של מערך הסייבר (להלן - התעדה). באתר המערך מתפרסם מאגר הכולל את רשימת הספקים שהותעדו (בכפוף להסכמתם). נכון לינואר 2023 יש שני גופי הסמכה:

א. מכון התקנים הישראלי (מת"י).

ב. המכון לבקרה ואיכות - איי.קיו.סי (IQC).

5. **קריטריונים לדירוג ספקים:** הספקים ידורגו בהתאם לפוטנציאל הנזק שעלול להיגרם לארגון בהתרחש מתקפת סייבר על הספק. מערך הסייבר פרסם קריטריונים שמסייעים לחשב את פוטנציאל הנזק שעלול להיגרם עקב פגיעה בספק בתחום הסייבר:

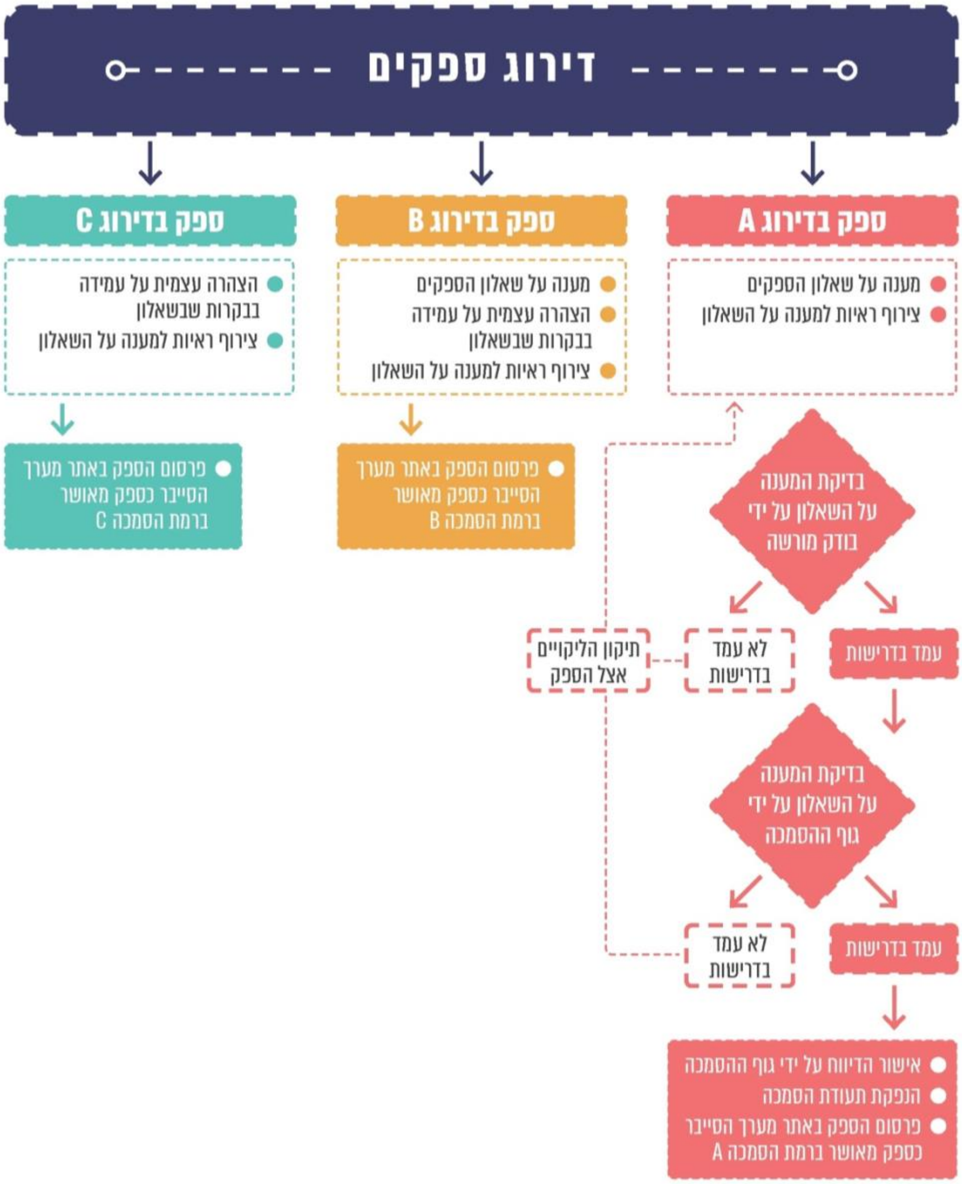
תרשים 6: קריטריונים לדירוג ספקים לפי פוטנציאל הנזק הנשקף מהם

רמת הנזק הצפוי לארגון מהספק (דירוג הספק)	האם מדובר "בספק מהותי" בהתאם להנחיית הגוף האסדרתי	נזק כלכלי לארגון (כולל עלויות כתוצאה מאובדן הכנסה/מוניטין/ אסדרה)	משך זמן ההתאוששות מאירוע אצל הספק	רגישות המידע הנגיש לספק	סבירות להתממשות אירוע כתוצאה מההתקשרות
A גבוה	כן	מעל מיליון ₪	מספר שבועות	מידע רגיש עסקית כגון פטנטים, סודות מסחריים וכו'	ספק בעל תלות גבוהה בסייבר. לדוגמה: ספק אשר מספק שירותי IT, בעל הרשאות גישה מרחוק, מחזיק מידע רגיש
B בינוני	לא	מאות אלפי שקלים	מספר ימים	מידע בעל רגישות בינונית	תלות בינונית בסייבר בהתקשרות עם הספק
C נמוך	לא	עשרות אלפי שקלים	מספר שעות	מידע בעל רמת רגישות נמוכה	תלות נמוכה בסייבר. לדוגמה, ספק של ציוד משרדי, ללא הרשאות ונגישות למערכות הלקוח

המקור: מערך הסייבר

6. **תהליך הערכת ספקים ואישורם:** תהליך ההערכה של הספקים משתנה בהתאם לדירוג שנתן לו הארגון בעניין רמת הסיכון הנשקף בגין פגיעה בו.

תרשים 7: **תהליך הערכת ספקים ואישורם**



על פי נתוני מערך הסייבר, בעיבוד משרד מבקר המדינה.

ספקים אשר הארגון דירג ברמה A: הספקים המהותיים של כל ארגון, אשר פוטנציאל הנזק הנשקף בגין פגיעה בהם הוא הגדול ביותר. ספקים אלו יידרשו להוכיח, באמצעות בודק ספקים חיצוני שהוסמך על ידי מערך הסייבר, את רמת ההגנה שלהם ואת עמידתם בשאלון הספקים.

לאחר בחינת התשובות על שאלון הספקים, גוף ההסמכה יכול לבצע אחת משתי הפעולות האלו: לאשרר את הדיווח ולהנפיק לספק תעודת הסמכה שתהיה תקפה לשנתיים או לא לאשרר את הדיווח ולבקש ממנו לבצע תיקון ליקויים.

ספקים אשר הארגון דירג ברמה B: ספקים אלה ישיבו באופן עצמאי על שאלון הספקים, ויצרפו אליו את הראיות הנדרשות. את הראיות ימסור הספק לארגון בערוץ בטוח שיסוכם בין הצדדים.

ספקים אשר הארגון דירג ברמה C: ספקים אלה ישיבו באופן עצמאי על שאלון הספקים ויחתימו מורשה חתימה מטעמם (לרוב המנכ"ל או הסמנכ"ל של הארגון) על הצהרה בדבר עמידתם בדרישות ההגנה שפורטו בשאלון.

תהליכי גיבוש ועדכון המתודולוגיה

בדיון שהתקיים במאי 2018, בסמוך להשקת המתודולוגיה, הודגשה החשיבות של תהליך הטמעת המתודולוגיה ושל שיתוף הפעולה בין גורמים בתוך המערך ומחוצה לו להצלחת הפרויקט.

ביוני 2022 פרסם מערך הסייבר טיוטה להתייחסות הציבור שעניינה מתודולוגיית שרשרת אספקה הכוללת שאלון ספקים בגרסה 1.4. בדצמבר 2022 אושרה ופורסמה מתודולוגיית שרשרת האספקה באתר של מערך הסייבר בצירוף שאלון 1.4.[25] במסמך עדכון המתודולוגיה שפרסם המערך[26] צוינו בין היתר השינויים שלהלן שבוצעו בשאלון 1.4:

1. נוסף מודול הכולל בקרות עבור בדיקת רכיבי בקרים תעשייתיים "אבטחת OT"[27].

2. מרבית הבקרות שוכתבו על מנת להפחית את חוסר הבהירות שבהן.

3. רמות ההסמכה צומצמו ל-A ול-B בלבד, באופן שספקים מהותיים (רמה A) צריכים לבצע התעדה וספקים ברמה B יכולים להסתפק בהצהרה עצמית של הספק בדבר עמידתו בדרישות המפורטות בשאלון הספקים.

4. הוגדרו שלוש רמות סיכון חדשות, כחלופה להגדרות של ספק מהותי או לא-מהותי מהשאלון הקודם: (1) רמה בסיסית, (2) רמה בעלת סיכון משמעותי ללקוח, (3) רמת סיכון קריטית ללקוח. לכל אחת מרמות הסיכון אפשר לבחור ברמת הסמכה A או B. כמו כן הספק נדרש לעמוד במספר בקרות שונה בהתאם לרמת הסיכון שניתנה לו (ככל שהסיכון גבוה יותר, הספק נדרש לעמוד במספר גדול יותר של בקרות).

25 https://www.gov.il/he/departments/guides/supply_chain_guide?chapterIndex=10
26 שרשרת אספקה בהיבט סייבר - תיאור המתודולוגיה של מערך הסייבר הלאומי.
27 טכנולוגיה תפעולית (Operational Technology) - מערכות מחשוב המשמשות לניהול משימות תעשייתיות.

הטיפול בפערים במתודולוגיית שרשרת האספקה

במערך הסייבר פועלת ועדת היגוי בנושא שרשרת האספקה. תפקיד הוועדה הוא ליצור שיתוף פעולה פנים-ארגוני במערך הסייבר לצורך שיתוף בתהליכים, קבלת חוות דעת והתייחסויות מגורמים במערך ומחוצה לו בעניין יישום המתודולוגיה. בראש הוועדה עומד ראש יחידת המדיניות, והמשתתפים הקבועים בוועדה הם נציגיהם של האגפים המשתתפים בשרשרת האספקה: חטיבת ההגנה (שכוללת את מנחי גופי התמ"ק ומנחי יחידות הסייבר המגזריות), החטיבה הטכנולוגית[28] וגורמים משפטיים. הוועדה החלה את פעילותה באפריל 2021 והתכנסה שש פעמים עד ינואר 2022 ופעם נוספת בנובמבר 2022.

בישיבתה של ועדת ההיגוי שהתקיימה בינואר 2022 הוצגו קשיים מהותיים ביישום מתודולוגיית שרשרת האספקה, ובהם הקשיים האלה:

1. חוסר בהירות בעניין הבקרות שבהן עסק שאלון הספקים.
2. שאלון הספקים מכביד ואינו מידתי בכל הנוגע לעסקים קטנים ובינוניים.
3. הספקים מחויבים להטמיע את כל הבקרות בשאלון הספקים כדי לקבל תעודה, והדבר מרתיע ארגונים וספקים.
4. חלק מהבקרות אינן מתאימות לשוק וליכולת של הספקים, למשל: בקרות מסוימות אינן ניתנות ליישום אצל ספקים קטנים, יש דרישה להצגת ראיות לקיום מערכות ומנגנונים כמו מערכת למניעת דלף מידע (DLP) והצפנות של מאגרי מידע, אך המתודולוגיה אינה מאפשרת בקרות מפצות בהיעדר מנגנונים אלו.
5. המקצועיות של בודקי הספקים המורשים מוטלת בספק.
6. העבודה מול ספקים בין-לאומיים, שיש להם חלק חשוב בפרויקטים, היא מאתגרת.

עוד בישיבתה המליצה ועדת ההיגוי לחדד את הניסוחים ולפשט את הבקרות בגרסה 1.4 של שאלון הספקים, לאפשר התעדה חלקית זמנית שתוקפה חצי שנה ולפעול בשיתוף משרד הביטחון לתאימות מול תקן CMMC.

המתודולוגיה עודכנה בדצמבר 2022 לגרסה 1.4 כדי לתת מענה לפערים האלו: הנגשת המתודולוגיה; רידוד ומיקוד של הסעיפים המורכבים; הגדרת המינימום הנדרש של בקרות בתחום הגנת הסייבר לפי עיסוק הספק ורמת הסיכון הנשקף בגינו לארגון והאפשרות להעלאת רמת ההגנה של הספק באופן מדורג.

28 תפקיד החטיבה ליזום, להוביל, לבחון ולפתח שירותים ופלטפורמות מותאמות עבור הלקוחות השונים החל בשלב הייזום, עבור דרך שלבי התכנון, המיפוי וניתוח הצרכים, האפיון והפיתוח וכלה בשלב מבצוע הפתרון הטכנולוגי המתאים ביותר.

נמצא כי מערך הסייבר עדכן את מתודולוגיית שרשרת האספקה (גרסה 1.4) והפיץ אותה לציבור בדצמבר 2022, אולם המתודולוגיה העדכנית לא נתנה מענה על חלק מהפערים המהותיים שהועלו עוד בוועדת ההיגוי בינואר 2022, ובהם הקושי הגלום בחיוב הספק הנבדק לעמוד במלוא הבקרות הקיימות בשאלון הספקים ללא אפשרות לתת מענה חלופי באמצעות בקרות מפצות על חלק מהדרישות או באמצעות הוכחת עמידה בתקנים מקבילים ואי-מתן מענה על עבודה מול ספקים בין-לאומיים.

מומלץ כי מערך הסייבר יוודא כי הפערים המהותיים שנמצאו במתודולוגיה, כמו הקושי הגלום בחיוב הספק הנבדק לעמוד במלוא הבקרות הקיימות בשאלון הספקים ואי מתן מענה לעבודה מול ספקים בין-לאומיים, נבחנים על ידי יחידת המדיניות ומקבלים מענה במתודולוגיה.

בתשובת מערך הסייבר מיולי 2023 נמסר כי יש כוונה לדרוש מהספקיות הבין-לאומיות הצהרה עצמית על עמידה בבקרות שבשאלון הספקים כאשר שאלון הספקים יהיה מתורגם.

עוד מומלץ כי מערך הסייבר יבחן במהלך השנה הקרובה אם המתודולוגיה העדכנית (גרסה 1.4) נותנת מענה על כל הפערים המהותיים שהיו קיימים במתודולוגיה 1.3 ויעדכן את הדרישות המופיעות במתודולוגיה אם הדבר יידרש.

כמו כן נמצא כי ממועד גיבוש המתודולוגיה של שרשרת האספקה בשנת 2018 ועד אפריל 2021 ועדת ההיגוי של מערך הסייבר בנושא שרשרת האספקה, אשר תפקידה לבחון את תהליך ההטמעה של המתודולוגיה, לא התכנסה. כמו כן, אף שבדיון שקיימה הוועדה בינואר 2022 הוצגו פערים מהותיים במידת היישום של המתודולוגיה, הוועדה לא התכנסה במשך כעשרה חודשים - מינואר 2022 ועד נובמבר 2022, זאת אף שבפרק זמן זה עודכנה המתודולוגיה ונעשו בה שינויים ניכרים. נוכח זאת ועדת ההיגוי לא וידאה כי הפערים שהעלתה בישיבתה מינואר 2022 צומצמו במסגרת המתודולוגיה העדכנית.

מומלץ כי ועדת ההיגוי במערך הסייבר תתכנס באופן עיתי כדי לבחון את מידת היישום של המתודולוגיה ולדון במתן מענה לפערים שהועלו בה. כינוס הוועדה חשוב במיוחד לפני ביצוע עדכונים במתודולוגיה ולאחריהם.

בפגישה שקיים צוות הביקורת עם יחידת המדיניות במערך הסייבר נאמר כי מערך הסייבר אינו בוחן באופן עיתי את המתודולוגיה לנוכח אירועי מתקפה על שרשרת האספקה כדי להטמיע במתודולוגיה שינויים ושיפורים כמו הוספה או הפחתה של בקרות שבהם יצטרכו לעמוד הספקים. כמו כן יש פער בין מועד התרחשות האירועים למועדי עדכון המתודולוגיה. לדוגמה: בעקבות תקיפת ספקי שירותי אירוח ואחסון של אתרים בשנת 2020[29] עדכן מערך הסייבר בשיתוף עם חברות האחסון הגדולות, את שאלון 1.4 כדי לקדם את ההגנה על ספקים אלו. שאלון 1.4 פורסם כאמור בסוף שנת 2022.

אגף הביטחון במערך הסייבר פועל לניהול הסיכונים הנוגעים לשרשרת האספקה שלו על פי מתודולוגיה ייעודית הדומה לאלו הנהוגות בארגוני ביטחון, אשר כוללת תחומים נוספים על אלה הנכללים במתודולוגיית שרשרת האספקה של מערך הסייבר המיועדת לכלל המשק, כמו: סיווג

29 מערך הסייבר, **סקירת פעילות מערך הסייבר הלאומי לאור תקיפת ספקי שירותי האירוח** (31.5.20).

ציוד רגיש, הנמקה למניעת פרסום פומבי של התקשרות, מענה בהיבט האיום הפנימי מתוך הספק, בחינת הנגישות הפיזית של נכסים הארגוניים של המערך הנמצאים אצל הספק לגורמים בלתי מורשים, בחינת איומים מצד המוצר עצמו (הטמנה[30], האם המוצר מכיל מרכיבי OT). מנהל אגף הביטחון במערך הסייבר שגיבש את המתודולוגיה הייעודית אינו חבר בוועדת ההיגוי של שרשרת האספקה. כמו כן אגף הביטחון במערך עורך קורסים לממוני ביטחון בגופי תמ"ק שם מציגים בפניהם את המתודולוגיה הייעודית של המערך בנושא שרשרת אספקה וכן הוא עורך הדרכות לקציני ביטחון של משרדי ממשלה.

בתשובת השב"כ מיולי 2023 נמסר כי יש תחומים נוספים שיש לתת מענה עליהם בנושא האיומים על שרשרת האספקה.

נמצא כי מערך הסייבר אינו בוחן באופן עיתי את המתודולוגיה של שרשרת האספקה לנוכח אירועי מתקפה על שרשרת האספקה כדי להטמיע במתודולוגיה שינויים כמו הוספה או הפחתה של בקרות שבהם יצטרכו לעמוד הספקים. למשל: עדכון המתודולוגיה בבקרות הקשורות לאירוח ולאחסון של אתרים בוצע ביוני 2022 בעוד תקיפות משמעותיות אירעו בשנת 2020. עוד נמצא כי על אף שאגף הביטחון במערך הסייבר גיבש מתודולוגיה ייעודית אשר כוללת תחומים נוספים על אלה הנכללים במתודולוגיית שרשרת האספקה של המערך ואף מדריך לפיה את ממוני הביטחון בגופי תמ"ק, הוא אינו חבר בוועדת ההיגוי לנושא שרשרת האספקה.

מומלץ כי מערך הסייבר יעדכן את המתודולוגיה באופן עיתי, גם בהתאם לתובנות שעלו מאירועי סייבר שמקורם בשרשרת האספקה. עוד מומלץ כי נציגי אגף הביטחון ישתתפו בדיוני ועדת ההיגוי ויבחנו אם נדרש להוסיף למתודולוגיית שרשרת האספקה נושאים נוספים שנכללים במתודולוגיה הייעודית של מערך הסייבר.

בתשובת מערך הסייבר מיוני 2023 נמסר כי בישיבת ועדת ההיגוי שהתקיימה בנובמבר 2022 השתתף נציג אגף הביטחון, וכי מנהל אגף הביטחון ישתתף בעצמו בישיבות הוועדה הבאות.

שיתוף ארגונים בעדכון המתודולוגיה

פרויקט שרשרת האספקה מערב ארגונים רבים במערך הסייבר ומחוצה לו. בסיכום מפגש סקירת דרישות פרויקט שרשרת האספקה בשנת 2018 נאמר כי חשוב לוודא קיומו של גורם אשר אמון על שמירת הקשר עם המשק ובכלל זה אוסף מידע על צורכי המשק, תומך בתהליך ההטמעה ומבצע סקר שביעות רצון. כמו כן, במפגש האמור הוגדרו כמה ארגונים אשר ישמשו Early adopters[31]. משתמשים אלו ישלחו אל הספקים שלהם בהדרגה את ההפניה למערכת יוב"ל, כדי לקדם בהדרגה תהליך למידה של המערך ושל כל שותפי הפרויקט.

בישיבתה של ועדת ההיגוי שהתקיימה בינואר 2022 עלה הצורך בשיתוף פעולה עם גופים אסדרתיים נוספים בתחום הגנת הסייבר, ובייחוד עם אלו שהם בעלי פוטנציאל מינוף גבוה כמו

30 הטמנה של מרכיבי חומרה ש"טופלו" על ידי התוקף המאפשרת את ערוץ התקיפה בתווך.

31 גורמים הנוטים לאמץ חידושים בקצב משתנה.

מלמ"ב והגופים האסדרתיים של מגזרי התחבורה, הגנת הסביבה והאנרגייה, כדי להרחיב את היקף האימוץ של המתודולוגיה.

הליך ההתייעצות, ריכוז ההערות של הארגונים המונחים והטמעת התובנות שעולות בתהליך המתודולוגיה הוא תהליך יסודי וחיוני בבואו של מערך הסייבר לפרסם מתודולוגיה עדכנית.

בפגישה שקיים צוות הביקורת עם נציגי יחידת מדיניות נאמר כי מערך הסייבר מסר את הטיוטה של שאלון 1.4, לצורך התייחסות הציבור לטיוטה זו, לארגונים שונים מחוץ למערך, ובהם קבוצת בודקים של שרשרת האספקה, חשכ"ל ומלמ"ב, אך אין בידי מערך הסייבר מסמך ובו מתועדת ההתייחסות של ארגונים אלה לשאלון, אם אכן התקבלה התייחסותם בעניין. כמו כן, יחידת המדיניות מסרה לצוות הביקורת כי היא קיימה פגישות עם גופים שונים ובהם גוף 41, אולם אין בידיה תיעוד הנוגע לגופים עמם נפגשה או לתובנות שעלו מפגישות אלו.

עוד נמסר בפגישה כי נציג מטעם המנחים של גופי התמ"ק מלווה מקצועית את יחידת המדיניות בנושא שרשרת האספקה אולם יחידת המדיניות לא נפגשת באופן עיתי עם המנחים של גופי התמ"ק, עם גופי התמ"ק עצמם ועם המנחים של יחידות הסייבר המגזריות כדי שאלה ישתפו אותה בקשיים שעולים ביישום המתודולוגיה וכדי לבחון דרכים לטיפול בהם.

נמצא כי יחידת המדיניות במערך הסייבר אינה מקיימת פגישות באופן עיתי עם גופים מונחים כמו גופי תמ"ק ויחידות הסייבר המגזריות על מנת לשמוע את התייחסותם למידת היישום של המתודולוגיה. כמו כן, יחידת המדיניות לא תיעדה באופן שיטתי את ההתייחסויות לטיוטת המתודולוגיה ששלחה ביוני 2022 לגופים שונים, ככל והתקבלו. נוכח זאת, אי אפשר להתחקות אחר מידת הטמעת ההתייחסויות במתודולוגיה העדכנית.

מומלץ כי מערך הסייבר יוודא כי יתקיימו פגישות עיתיות של יחידת המדיניות עם גופים מונחים ובכלל זה נציגי גופי התמ"ק ויחידות הסייבר המגזריות וכי פגישות אלו יתועדו באופן שיאפשר לבחון את מידת יישום המתודולוגיה, וזאת בייחוד לפני עדכון המתודולוגיה ואחרי עדכונה.

עקרון "אפס האמון" (Zero Trust)

אחד העדכונים העיקריים של המתודולוגיה לגרסה 1.4 היה הגדרת שלוש רמות סיכון חדשות לכל ספק, כחלופה לסיווגו כספק מהותי או לא-מהותי: (1) רמה בסיסית, (2) רמה בעלת סיכון משמעותי ללקוח, (3) רמת סיכון קריטית ללקוח. הובהר כי לפי השיטה החדשה, בכל רמות הסיכון של הספק (1, 2 ,3) הארגון יכול להחליט שהוא מסתפק בהצהרה עצמית של הספק בדבר עמידתו בדרישות המפורטות בשאלון הספקים.

עוד הובהר כי רמת ההסמכה B (הצהרה עצמית) יכולה לשמש מדרגה זמנית לצורך עמידה בתנאי סף של מכרז או לשמש מדרגה התחלתית על מנת להרגיל ספקים ליישום המתודולוגיה ולהקל על עסקים קטנים ובינוניים ליישם את המתודולוגיה. במסמך העדכון של המתודולוגיה ממליץ מערך הסייבר כי יש לבצע בדיקה גם בעניין ספקים שרמת הסמכתם B, כדי לוודא כי הם עומדים בדרישות המפורטות בשאלון.

אחד מעקרונות היסוד בתחום הגנת הסייבר הוא "אפס האמון". כלומר, בכל הנוגע למידת עמידתו של הספק בדרישות אבטחת המידע והגנת הסייבר - אין לתת מראש אמון בלתי מעורער בספק אלא יש לוודא באופן עיתי ובלתי תלוי כי הוא עומד בדרישות סף.

נמצא כי השינוי שביצע מערך הסייבר במתודולוגיה של שרשרת האספקה בגרסה 1.4, המאפשר גם לספקים שסווגו על ידי משרדי הממשלה וגופי התמ"ק כספקים שרמת הסיכון הנשקף עקב פגיעה בהם היא קריטית להסתפק בהצהרה עצמית, אינו עולה בקנה אחד עם עקרון "אפס האמון" שהוא עקרון יסוד בתחום הגנת הסייבר ומשמעותו שאין לתת מראש אמון בלתי מעורער בספק אלא יש לוודא באופן עיתי ובלתי תלוי כי הוא עומד בדרישות סף. הדבר מקבל משנה תוקף לנוכח העובדה שלא מתבצעות בקרות וסנקציות הבוחנות את נכונות הצהרות הספק.

מומלץ כי מערך הסייבר ינחה את משרדי הממשלה ואת גופי התמ"ק לבדוק באמצעות בודק ספקים מורשה כי ספקים אשר סווגו על ידם כספקים בעלי רמת סיכון קריטית, עומדים בבקרות שהגדיר מערך הסייבר בעניין שרשרת האספקה.

מערכת יוב"ל

מתודולוגיית שרשרת האספקה מונגשת לספק באמצעות מערכת מקוונת הכוללת את שאלון הבקרות לספקים, כדי לאפשר לספק בחינה עצמית של רמת האבטחה שלו. מערך הסייבר מדגיש כי ספקים אינם חייבים להשתמש במערכת יוב"ל, ואין שום מניעה כי הם יגישו באופן ידני תיק ספק באמצעות שאלון האקסל.

במהלך הרבעון הראשון של שנת 2018 השיק המערך את פרויקט מערכת יוב"ל והוגדרו יעדיו, כמפורט להלן:

1. להנגיש לארגונים במשק את הידע המתקדם והרלוונטי כדי להגביר את החוסן שלהם.
2. להקנות למערכת יכולת למדוד את רמת יישום תורת ההגנה במשק.
3. להגיע לפלחי שוק שעדיין אינם נגישים (ספקי B/C).
4. להנגיש סטטיסטיקה ותובנות רוחביות למערך על מצב ההגנה במשק.
5. להקנות למערך הסייבר יכולת להטמיע שינויים במתודולוגיה בזמן קצר, על בסיס מודיעין ונתונים על אירועים שהתרחשו.

בישיבתה של ועדת ההיגוי בינואר 2022 עלה כי למערכת יוב"ל אין ערך מוסף על פני חלופות קיימות כמו שאלון הספקים שמונגש באמצעות אקסל. בין השאר נטען כי המערכת איננה נוחה לשימוש, כי היא אינה מספקת לארגונים ממשלתיים תמונת מצב ויזואלית בנוגע למצב הספקים שלהם, וכי נבצר מארגון המבצע בדיקה בעניין הספקים לקבל תמונת מצב מלאה ומקיפה על כל הספקים במקום אחד. המסקנה שהוסקה בישיבת הוועדה הייתה שיש לשמור על כשירות המערכת ולאפשר עבודה במערכות מקבילות.

בפגישה שקיים צוות הביקורת עם נציגי יחידת המדיניות במערך הסייבר נאמר כי למערך הסייבר אין יכולת להפיק מידע סטטיסטי ותובנות רוחב ממערכת יוב"ל בשל הסיבות האלו:

1. שום ספק אינו מחויב לעבוד במערכת יוב"ל, אפשר להשתמש במקומה בשאלון המונגש באמצעות אקסל.
2. המערכת אינה כוללת כלים שמאפשרים להפיק תובנות רוחב.
3. המערכת איטית ויש בה בעיות טכניות.
4. שום ספק אינו מחויב להזין את פרטיו האישיים במערכת יוב"ל (לא ניתן לוודא שהספק מילא פרטים מהימנים).
5. המידע במערכת כולל גם ניסיונות של ספקים להתאמן על המערכת, נוכח זאת אי-אפשר להבחין בין מידע מהימן שכתב הספק לבין מידע שהוזן בשלב הניסויים.

בפגישה שקיים צוות הביקורת עם נציגי יחידת המדיניות במערך הסייבר בפברואר 2023 נמסר כי מערכת יוב"ל מיועדת לשימוש הספקים כדי שימלאו בה את שאלון הספקים. המערכת אינה מיועדת לארגונים שהספק נותן להם שירות כדי שינהלו את רמת ההגנה של הספקים שלהם. מבחינת מערך הסייבר כל ספק יכול לבחור באיזו מערכת מידע להשתמש כדי לענות על שאלון הספקים ולא מחויב לעבוד במערכת יוב"ל, ובלבד שבסוף התהליך הוא מגיש למכוני ההסמכה את השאלון מלא. ההתקשרות עם החברה שנותנת שירותי פיתוח ותמיכה למערכת יוב"ל נעשית על בסיס הארכת חוזה שהסתיים. בימים אלו המערך בוחן את הצורך בפיתוח היכולות במערכת יוב"ל ואת התקציב הדרוש לכך.

משרד מבקר המדינה קיים פגישות עם כמה גופי תמ"ק שמשתמשים במערכות ממוחשבות לניהול הסיכונים הנשקפים לשרשרת האספקה (שאינן מערכת יוב"ל). להלן כמה דוגמאות:

גוף 15: החברה ציינה במענה על השאלון כי היא משתמשת במערכת ייעודית לניהול ספקים, למעקב אחריהם ולבדיקה ובקרה בעניינם. לדברי החברה, למערכת יש יכולת לבצע בדיקה בעניינו של הספק על פי רמת האיום הנשקף בגין מתקפת סייבר עליו, בהתאם לשאלון 1.3 שמוטמע במערכת. מעבר ליכולות הניהול והתשאול מדובר במערכת פרו-אקטיבית שאוספת מודיעין ויכולה לזהות סיכונים הנשקפים לספקים.

גוף 20: הספקים של גוף 20 מתבקשים למלא באופן עצמאי שאלון בנושא שרשרת האספקה, וזאת במערכת מידע שמבוססת על שאלון 1.3. המערכת מציגה את מידת עמידתם של כל הספקים של גוף 20 בבקרות על שרשרת האספקה.

נמצא כי המערכת המקוונת שמנגיש מערך הסייבר לבחינת יישום הבקרות על ספקים (מערכת יוב"ל) אינה עומדת ביעדים שהוגדרו לה בהקמתה: המערכת אינה מאפשרת למערך הסייבר לבצע חישובים סטטיסטיים ולהפיק תובנות רוחביות, המערכת אינה מיועדת לארגונים ואינה מספקת להם תמונת מצב בעניין הספקים שלהם וכן אי אפשר להטמיע במערכת שינויים על בסיס מודיעין ואירועי סייבר. נוכח זאת חלק מהארגונים משתמשים במערכות חלופיות לצורך ניהול המעקב בעניין מידת עמידתם של הספקים בדרישות האבטחה לעניין שרשרת האספקה, תוך שימוש בגרסה של שאלון הספקים שאיננה מתעדכנת באופן שוטף.

מומלץ כי מערך הסייבר יתקף את היעדים של מערכת יוב"ל לאור הפערים שעלו בה, יגבש מתווה פעולה ויבחן אם יש צורך בהנגשת כלים ממוחשבים ליישום מתודולוגיית שרשרת האספקה במשק.

בתשובת מערך הסייבר מיוני 2023 נמסר כי בכוונתו לבדוק את הצורך בעדכון המערכת במסגרת השנה הקרובה.

מידת יישום המתודולוגיה של מערך הסייבר

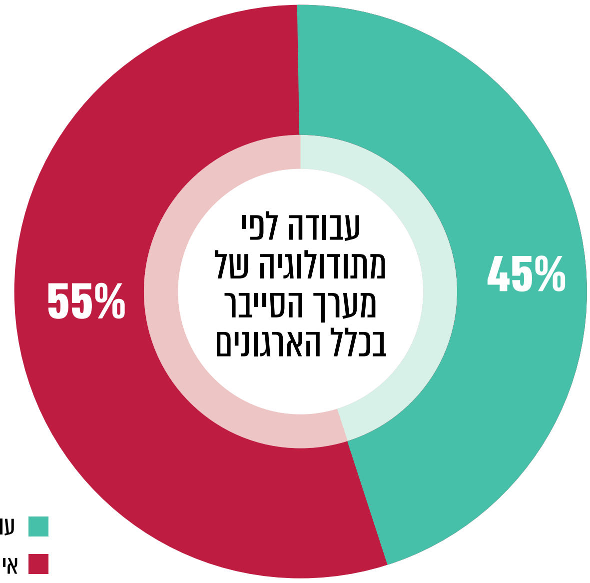
יישום המתודולוגיה בכלל הארגונים

כאמור, אחד מיעדיה המרכזיים של מתודולוגיית שרשרת האספקה הוא להטמיע מתודולוגיה אחידה במשק שתיצור שפה משותפת בין הארגונים לבין הספקים.

משרד מבקר המדינה בדק באמצעות השאלון שהפיץ למשרדי ממשלה ולגופי תמ"ק את מידת היישום של המתודולוגיה גרסה 1.3[32] בארגונים אלו, להלן יוצגו הממצאים שעלו מתשובותיהם:

32 ההנחיות המחייבות במועד הפצת השאלון היו מבוססות על גרסה 1.3 של המתודולוגיה.

תרשים 8: **שיעור הארגונים שעובדים לפי המתודולוגיה של מערך הסייבר**



על פי תשובות על השאלון שהעביר משרד מבקר המדינה, בעיבוד משרד מבקר המדינה.

נמצא כי 24 (55%) מתוך 44 משרדי הממשלה וגופי התמ"ק שהשיבו על שאלה זו בשאלון אינם עובדים לפי מתודולוגיית שרשרת האספקה של מערך הסייבר. נוכח זאת חלק גדול מהספקים של משרדי הממשלה וגופי התמ"ק אינם נבדקים בצורה אחודה ובהתאם לבקרות שהגדיר מערך הסייבר.

בתשובת מערך הסייבר מיוני 2023 נמסר כי ההבנה של רמת היישום הנמוכה וההיכרות עימה הובילו את מערך הסייבר לעדכון מתודולוגיית שרשרת האספקה לגרסה 1.4 שהופצה בדצמבר 2022, וכעת נדרש לקדם את הנושא במסגרת קידום הטמעת המתודולוגיה בקרב כלל הגופים הרלוונטיים, ובראשם הגופים הקריטיים, באמצעות מערך הסייבר, וכן במסגרת קידום הטמעת המתודולוגיה במשרדי הממשלה על ידי יה"ב, בליווי ותמיכה של מערך הסייבר.

בתשובת גוף 9 מיוני 2023 נמסר כי עד לפניית משרד מבקר המדינה הגוף לא היה מודע להנחיה המדוברת. לאחר הגשת השאלון המלא החל הגוף לעבוד מול מערך הסייבר ויה"ב ליישום ההנחיות ובשיתוף פעולה מלא מול מנחה המשרד.

בתשובת גוף 26 מיוני 2023 נמסר כי עם המענה על השאלון החל הגוף ללמוד את שרשרת האספקה, ועיקרי הנושא הובאו לידיעת הגורמים הרלוונטיים ביחידות הטכנולוגיות. הגוף פועל ללא לאות, במסגרת האפשרויות הנתונות לסמכותו, על מנת לבצע את ההתאמות הנדרשות לצורך עמידה במתודולוגיה שהוצגה בדוח.

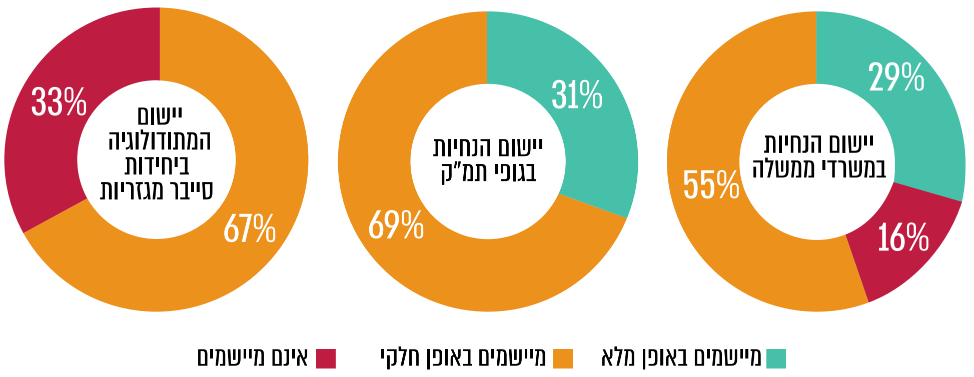
בתשובת גוף 23 מיוני 2023 נמסר כי המתודולוגיה תפורסם בהודעה מסודרת לכלל מנהלי הגוף לצורך יישום מלא.

בתשובת גוף 1 מיוני 2023 נמסר כי המענה שניתן בגוף אפקטיבי וממוקד יותר, ולכן גם משיג רמת אבטחה גבוהה בהרבה, קרי צמצום הסיכון מצד ספקים. תפיסת אבטחת שרשרת אספקה זו תואמה עם מערך הסייבר שמודע לאופן הטיפול ומקבל אותו.

אשר לתשובת גוף 1, מערך הסייבר מסר בתשובתו מיולי 2023 כי הוא לא אישר לגוף 1 לוותר על יישום מתודולוגית שרשרת האספקה.

מערך הסייבר מנחה את הגופים האסדרתיים המגזריים בתחום הגנת הסייבר ואת גופי התמ"ק. יה"ב מנחה את משרדי הממשלה. להלן נתונים המבוססים על המענה לשאלון המלמדים על מידת היישום הנמוכה של המתודולוגיה במשרדי הממשלה, ביחידות הסייבר המגזריות ובגופי התמ"ק. מערך הסייבר ציין בתשובתו כי מערך הסייבר ויה"ב אמונים על הפיקוח והיישום של המתודולוגיה, אך האחריות הבסיסית להבטחת רמת ההגנה או ביצוע הדרישות מוטלת על הגופים.

תרשים 9: **יישום המתודולוגיה במשרדי הממשלה, בגופי התמ"ק וביחידות הסייבר המגזריות**



על פי תשובות על השאלון שהעביר משרד מבקר המדינה, בעיבוד משרד מבקר המדינה.

מומלץ כי מערך הסייבר ויה"ב, האחראים לגיבוש מתודולוגיית שרשרת האספקה וההנחיות הנובעות ממנה ולפיקוח על יישומם בפועל, יקיימו מעקב שוטף אחר מידת היישום של מתודולוגיה 1.4 ויפעלו מול הגופים למציאת פתרונות לפערים, אם יעלו.

בתשובת גוף 22 מיוני 2023 נמסר כי נכון יהיה לקיים את הבחינה לגבי יישום המתודולוגיה במשותף עם משרדי הממשלה ויה"ב כדי לייצר פלטפורמה התואמת יותר למציאות.

בתתי-הפרקים הבאים יוצג פירוט של מידת יישום מתודולוגיית שרשרת האספקה גרסה 1.3 בארגונים השונים.

יישום המתודולוגיה בגופי התמ"ק

גופי התמ"ק מונחים על בסיס תורת לחימה (להלן - תו"ל) ייעודי למערכות ממוחשבות, אך בכל הנוגע לשרשרת האספקה פרסם מערך הסייבר בפברואר 2021 הנחיה המחייבת את גופי התמ"ק ליישם את המתודולוגיה של שרשרת האספקה. בהתאם להנחיה, על גוף התמ"ק המונחה להתחיל ליישם את מתודולוגיית שרשרת האספקה של מערך הסייבר הלאומי ולבחון אם הספק עומד בדרישות שנקבעו במתודולוגיה, תוך שימת דגש מיוחד כאשר הספק מוגדר כספק מהותי או רגיש.

על פי ההנחיה, לטובת מזעור הסכנות מצד שרשרת האספקה יש לנקוט בפעולות הגנה רבות לרבות ביצוע ביקורות מטעם הלקוח אצל הספק. עוד קובעת ההנחיה כי תהליך יישום המתודולוגיה יתבצע בליווי ובהנחיה של מנחה גוף התמ"ק ובהתאם ללוחות זמנים מוגדרים. המנחה של גופי התמ"ק מלווה את גופי התמ"ק בתהליך מיפוי הספקים, מפנה את הספק לבודק ספקים מאושר ובשיתוף עם גוף תמ"ק המונחה קובע אם לאשר כי הספק עומד בתבחיני הבדיקה. לאחר השלמת המיפוי, טבלת הספקים, המכילה את נתוניהם של כלל הספקים של גופי התמ"ק, תועבר למנחה התמ"ק.

במאי 2022 עדכן מערך הסייבר את לוחות הזמנים בהנחיה לגופי תמ"ק. לפי ההנחיה המיפוי היה צריך להסתיים ברבעון השלישי של שנת 2022. כמו כן, לפי היעד שנקבע במסמך ההנחיה המעודכן יש לאשר את מידת עמידתם של 30% מהספקים הקריטיים של הארגון בתבחיני הבדיקה עד לתום הרבעון הרביעי של שנת 2022.

לוח 1: **מידת יישום הנחיות מערך הסייבר בגופי תמ"ק**

השאלה	שיעור גופי התמ"ק
האם הנחיות הגורם המאסדר בנושא שרשרת האספקה מיושמות בארגון? (כן/באופן חלקי/לא)	**69% מהגופים יישמו באופן חלקי את ההנחיות**
האם המנחה מטעם המאסדר סייע לך בתהליך מיפוי הספקים?	**36% מהגופים לא נעזרו במערך הסייבר בתהליך מיפוי הספקים**

נמצא כי 9 (69%) מתוך 13 גופי התמ"ק שהשיבו על השאלה מסרו כי יישמו באופן חלקי בלבד את ההנחיות של מערך הסייבר בנושא שרשרת האספקה, אף שהנחיות אלו הן מחייבות ואף שגופי תמ"ק הם ארגונים שפגיעה בהם עשויה להיות קריטית למשק.

עוד נמצא כי 4 (36%) מתוך 11 גופי התמ"ק שהשיבו על השאלה ציינו כי לא נעזרו במערך הסייבר בתהליך מיפוי הספקים כנדרש בהנחיה.

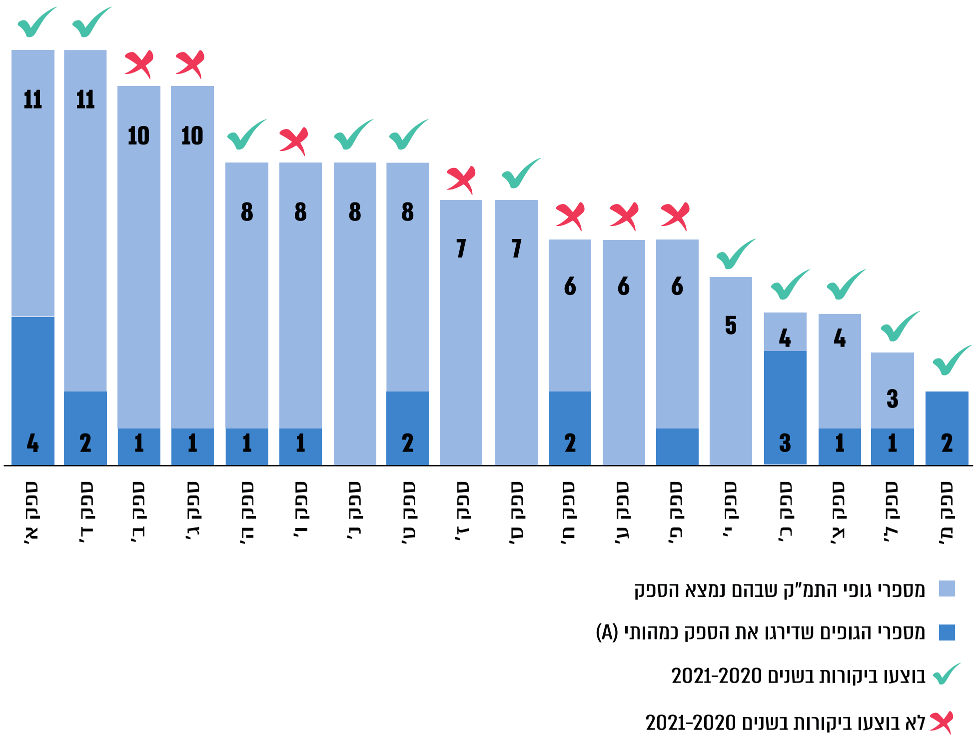
מומלץ כי מערך הסייבר יוודא שגופי התמ"ק, שהם ארגונים עם נכסים רגישים יותר למשק, שלא השלימו את יישום ההנחיות של מערך הסייבר בנושא שרשרת האספקה יעשו זאת בהתאם ללוחות זמנים מעודכנים שיגדיר המערך. עוד מומלץ כי המערך ילווה את תהליכי מיפוי הספקים שמבצעים גופי התמ"ק ויוודא שהגופים ממפים את הספקים שלהם ובפרט את הספקים המהותיים ומנהלים את הסיכון הנשקף מהם.

בפגישה שקיים צוות הביקורת עם המנחים של גופי תמ"ק בנובמבר 2022 נאמר כי בידי המערך אין כיום תמונת רוחב של הספקים של גופי תמ"ק הכוללת, בין היתר מידע על שם הספק, על סיווגו, על גופי התמ"ק הקשורים אליו, על סוג השירות שהוא מספק, על מידת הקריטיות של השירות שלו ועל הסיכונים העיקריים הנשקפים לספק בתחום הסייבר, האם נעשתה בקרה על פעילותו או נבדקה מידת עמידתו בדרישות שנקבעו במתודולוגיית שרשרת האספקה בשנה האחרונה (באמצעות ביקורת, התעדה, שאלון, בדיקה של הארגון), מהם הפערים העיקריים שנמצאו בעניינו, האם יישם תוכנית לתיקון ליקויים. לדברי המנחים בשנת 2014 הוכנה מפת חום של הספקים[33], אך מאז היא לא עודכנה.

משרד מבקר המדינה ריכז את הנתונים מהמענה של 13 גופי התמ"ק על השאלון. מהמענה עולה כי 18 ספקים נותנים שירותים לכמה גופי תמ"ק, 13 מהם הוגדרו על ידי גופי התמ"ק כספק מהותי. כמו כן לגבי כל ספק יש אינדיקציה אם בוצעו עליו ביקורות בתחום שרשרת האספקה בשנתיים האחרונות (2020- 2021). יצוין כי כלל הספקים בתרשים למעט ספק מ' זכו במכרזים מרכזיים ולכן בפועל הם מספקים שירותים למשרדים נוספים על אלו המוצגים בתרשים.

33 דירוג הספקים על פי מידת הסיכון הגלומה בהתקשרות עימם ובהתאם לרמת ההגנה שלהם.

תרשים 10: **ספקים בתחום התקשוב והסייבר שנותנים שירותים לגופי תמ"ק רבים**



על פי ניתוח שאלה 9 בשאלון שהעביר משרד מבקר המדינה.

מהתרשים עולים הממצאים האלה:

1. נכון למרץ[34] 2023 שום ספק מ-13 הספקים המהותיים שנותנים שירותים לכמה גופי תמ"ק לא עבר התעדה על ידי גופי ההסמכה (צורת הסמכה של ספק בסיווג A), אף שלפי הנחיית המערך 30% מהספקים המהותיים של גופי התמ"ק היו צריכים להיות מותעדים עד לתום הרבעון הרביעי של שנת 2022.

2. רק שניים (ספק א' וספק ז') מתוך 18 הספקים של גופי התמ"ק שבתרשים קיבלו אישור ספקים על בסיס הצהרתם (צורת ההסמכה של ספק בסיווג B). יתר הספקים (89%) לא בחנו את מידת עמידתם בבקרות הנדרשות בהתאם למתודולוגיה של שרשרת האספקה המנחה את הגופים לסווג את רמת הסיכון מהספק ולבצע עליו בקרות בהתאם לסיווג שלו.

34 מבדיקה שביצע משרד מבקר המדינה במרץ 2023 באתר המרשתת של מערך הסייבר

3. בשבעה ספקים (ספקים ב', ג', ו', ז', ח', ע, פ') שנותנים שירות גם לגופי התמ"ק וגם למשרדי ממשלה במסגרת מכרז מרכזי לא בוצעה ביקורת בשנתיים האחרונות (2020 - 2021) וזאת שלא בהתאם להנחיית מערך הסייבר המחייבת לערוך ביקורות על הספק.

בישיבתה של ועדת ההיגוי שהתכנסה ביוני 2021 והתמקדה בגופי תמ"ק הוצע לקדם פיילוט להתעדה של עשרה ספקים מהותיים של גופי תמ"ק, שכולל בשלב א' ליווי והכנה להתעדה בידי עובדים מוסמכים מטעם מערך הסייבר ובשלב ב' טיפול בפערים שהתגלו בבדיקות, בין השאר באמצעות סבסוד עלות ההתעדה והשקת תוכנית תמריצים.

להלן לוח שמציג את הפערים שעלו ביישום המתודולוגיה בגופי התמ"ק שענו של השאלון:

לוח 2: **מידת יישום המתודולוגיה בגופי תמ"ק**

הנושאים שנבדקו	גוף 38	גוף 39	גוף 16	גוף 5	גוף 45	גוף 15	גוף 20	גוף 43	גוף 1	גוף 21	גוף 11	גוף 2	גוף 19
ביצוע סקר סיכונים שכלל התייחסות לנושא שרשרת האספקה	✗	✗	✓	✗	✗	✓	✗	*	✗	✗	✗	✓	✓
ספקי A שעברו תהליך התעדה בהתאם למערך הסייבר	*	✗	✗	✗	*	✗	✓	*	*	✓	✗	✗	✗
איסוף מודיעין סייבר ומודיעין עסקי על ספקי הארגון	✗	✗	✗	✓	✗	✓	✗	*	✓	✗	✓	✗	✓
מעורבות של הממונה על הגנת הסייבר בתהליך סיום ההתקשרות עם הספק	*	✓	✗	✗	✗	✗	✗	✗	✓	✓	✓	✓	✗
סעיף במכרזי הארגון המחייב עבודה לפי המתודולוגיה של מערך הסייבר	✗	✗	✗	✗	✓	✓	✓	✗	✗	✓	✓	✓	✓
קיום מיפוי של כלל הספקים הכולל את כל פרטי המידע הנדרשים במתודולוגיה	✗	*	✗	*	✗	✓	✓	✗	*	✗	*	✗	*
מינוי בעל תפקיד ייעודי לנושא שרשרת האספקה	✗	✗	✓	✓	✓	✓	✗	✓	✗	✓	✓	✓	✓
סיוע של הגורם המאסדר בתהליך מיפוי הספקים	✗	✗	✗	✓	✓	✓	✗	*	✓	✓	✓	*	✓
ביצוע בקרות אצל הספקים בשלוש השנים האחרונות (2020 - 2022)	✗	✓	✓	!	*	✗	!	*	!	*	✗	✓	!
מתן הנחיה לספקי A לעבור התעדה	*	✓	✗	✗	*	✗	!	*	*	✓	✓	✓	!
מעקב שנתי אחר תיקון הליקויים שנמצאו אצל הספק	✗	✓	✓	✓	✗	✗	✓	*	*	*	✓	✓	✓
סעיף במכרז שמחייב את הספק להודיע לארגון על אירוע סייבר במוצר או בשירות המסופק	✗	✓	✓	✗	✓	✓	✓	✓	✓	✓	✓	✓	✓
הפעלת סנקציה נגד ספקים שלא עמדו ברמת ההגנה הנדרשת בתקופת ההתקשרות	✗	✗	✓	*	*	*	*	*	*	*	✓	✓	✓
עבודה לפי מתודולוגיית שרשרת האספקה של מערך הסייבר	✓	✓	✗	✓	✓	✓	✓	✓	✗	✓	✓	✓	✓
סעיף במכרז שמתיר לארגון לבצע ביקורות סייבר אצל הספק	✗	✓	✓	✗	✓	✓	✓	✓	✓	✓	✓	✓	✓
נושא שרשרת האספקה נדון במסגרת ועדות ההיגוי	✓	✗	✓	✓	✓	✓	✓	✗	✓	✓	✓	✓	✓
קיום ספק מהותי בארגון	✗	✓	✓	✓	*	✓	✓	*	*	✓	✓	✓	✓
ביצוע תרגולים לתקיפת סייבר באמצעות שרשרת האספקה	✓	✗	✓	✓	*	✓	✓	✓	✓	✓	✓	✓	✓
מעורבות ממונה הגנת הסייבר או הממונה על שרשרת האספקה בתהליכי הרכש	✓	!	✓	!	!	!	✓	✓	✓	✓	✓	!	✓
יישום ההנחיות של הגורם המאסדר	!	!	!	!	!	✓	!	!	✓	!	✓	!	✓
שיעור הנושאים שהגופים יישמו באופן מלא או חלקי	**40%**	**55%**	**60%**	**65%**	**75%**	**75%**	**75%**	**80%**	**80%**	**85%**	**85%**	**85%**	**90%**

✓ כן
✗ לא
! באופן חלקי
* לא נמסר מידע/ לא רלוונטי

על פי תשובות על שאלון שהעביר משרד מבקר המדינה.

מהלוח עולה כי 7 (54%) מתוך 13 גופי התמ"ק שהשיבו על השאלון אינם מיישמים לפחות 25% מהנושאים שנכללים במתודולוגיית שרשרת האספקה.

מומלץ כי מערך הסייבר יפעל לקידום ההתעדה של הספקים המהותיים של גופי תמ"ק וליישום המתודולוגיה בגופי התמ"ק בהתאם להמלצות שהוא העלה בוועדת ההיגוי שלו, תוך ליווי והכנה להתעדה בידי עובדים מוסמכים מטעם מערך הסייבר, טיפול בפערים שהתגלו בבדיקות, סבסוד עלות ההתעדה והשקת תוכנית תמריצים.

יישום המתודולוגיה ביחידות הסייבר המגזריות

כאמור, האגף להכוונה מגזרית במערך הסייבר אחראי להנחיה מקצועית ישירה של יחידות הסייבר המגזריות במשרדי הממשלה, ואלו אחראיות להכוונה ולהנחיה של כל הגופים הכפופים לסמכויות האסדרה של אותו המשרד. כך שלמעשה, מערך הסייבר מנחה בעקיפין את כלל הגופים שאינם מוגדרים כתמ"ק וכפופים לסמכויות אסדרה באמצעות אגפי הסייבר המגזריים.

בהחלטת ממשלה 2443 הוגדרו תפקידי יחידות הסייבר המגזריות כמפורט להלן:

1. הכוונה והנחיה בהיבטי הגנת הסייבר, לרבות הגדרת המדיניות ודרישות האסדרה, ליווי מקצועי שוטף ומענה על פניות מקצועיות בהתאם למאפיינים של הגופים אשר בעניינם מתבצעת הפעילות.

2. בקרה על ביצוע הדרישות המקצועיות בהתאם לאסדרה וברמה המקצועית הנדרשת, לרבות הכרת הפערים וההתאמות הנדרשות.

3. גיבוש והפעלה של תהליכי שיתוף מידע פנימיים וחיצוניים בתוך המגזר, לרבות דיווח למרכז הארצי לניהול אירועי סייבר (CERT לאומי) על אירועים, איומים, חולשות, פוגענים ונוזקות וכן הגדרת הנהלים ושיטות הדיווח בין הגופים במגזר.

4. ייזום ומימוש של פעילות רוחבית, לרבות הקמת תשתיות והפעלת מנגנונים שתכליתם שיפור הגנת הסייבר במגזר.

בישיבת ועדת ההיגוי שהתקיימה בינואר 2021 הועלה נושא שיתוף הפעולה עם הגופים האסדרתיים השונים לקידום המתודולוגיה. הוועדה הגדירה את הגופים האסדרתיים כגופים המשמעותיים ביותר להטמעה של המתודולוגיה. בנוסף, בפגישה של צוות הביקורת עם נציגי יחידת המדיניות במערך הסייבר שהתקיימה בספטמבר 2022 נמסר כי אחד מיעדי היחידה הוא לקדם אימוץ של מתודולוגיית שרשרת האספקה על ידי הגופים האסדרתיים השונים.

נכון למועד סיום הביקורת במאי 2023, מערך הסייבר לא הוציא ליחידות הסייבר המגזריות הנחיה רוחבית ליישום המתודולוגיה בנושא שרשרת האספקה בגופים הכפופים להנחייתן.

ההנחיה של גופים הנעשית על ידי היחידות המגזריות במשרדי הממשלה מחייבת, בהתאם למקור הסמכות של המאסדר, ולכן מידת יישום המתודולוגיה איננה אחידה בקרב המגזרים השונים. צוות הביקורת נפגש עם כמה יחידות מגזריות בתחום הסייבר כדי לבדוק את מידת יישום המתודולוגיה במגזר שעליו הם אמונים. להלן סיכום מצב בעניין מידת יישום המתודולוגיה במגזרים אלו:

1. **משרד התחבורה:** אגף הסייבר במשרד התחבורה פרסם בינואר 2021 את מדיניותו המחייבת את הארגונים במגזר אשר אגף הסייבר הגדיר שרמת הסיכון הנשקפת מהם היא גבוהה (A או B). סעיף 8.9 במדיניות של אגף הסייבר עסק במחויבות הארגונים למפות את הספקים שלהם וכן בחובה לדרוש מספקים מהותיים להציג תעודת "ספק מאושר" מטעם גוף התעדה מורשה. ממסמך שסוקר את הטמעת המדיניות במגזר עולה כי הדרישה לעמידה בהוראות שנקבעו במתודולוגיה של מערך הסייבר נוספה למכרזים החדשים מול

הארגונים, אבל בחוזים קיימים, שלרובם תקופת תחולה ממושכת, לא הצליח אגף הסייבר במשרד בהרבה מהמקרים להכניס את הסעיפים הרלוונטיים.

2. **משרד האנרגייה והתשתיות:** יחידת הסייבר המגזרית במשרד האנרגייה והתשתיות מנחה את יצרני האנרגייה הפרטיים שאינם מחויבים לפעול לפי המתודולוגיה של מערך הסייבר הלאומי. בפגישה שקיים צוות הביקורת עם יחידת הסייבר במגזר האנרגייה בפברואר 2023 נאמר כי המגזר קיים "פגישת התנעה" עם המנחה המגזרי בנושא אנרגיות מתחדשות אך לא התקיימו פגישות נוספות בנושא יישום מתודולוגיית שרשרת האספקה של המערך במגזר האנרגייה. בפועל משרד האנרגייה והתשתיות לא כלל בנוהל של מסמך המדיניות המגזרית שלו, בפרק העוסק בשרשרת האספקה, הנחיה בדבר ביצוע מיפוי ספקים או ביצוע התעדה לפי המתודולוגיה של מערך הסייבר. הוכנה טיוטה של הנוהל שמנחה את היזמים לבצע מיפוי ספקים, למלא את שאלון הספקים ולהגישו ליחידה המגזרית, אך טרם הושלמו הדיונים הפנימיים בנושא, היות שנמצא כי יש קושי בהתעדת הספקים: מרביתם ספקים בין-לאומיים ולכן משרד האנרגייה והתשתיות אינו מוסמך לכפות עליהם לבצע התעדה. כמו כן נאמר בפגישה כי תהליך ההתעדה הוא ארוך ולפיכך עלול לגרום ליזם עיכוב של כמה חודשים בתהליך הקמת מתקן אנרגייה וכן הוא עלול לחייב את היזם להשקיע בהתעדה משאבים רבים, ולכן ייתכן שהתהליך אינו ישים.

3. **משרד הבריאות:** המשרד פרסם ביולי 2020 מסמך מדיניות ניהול סיכוני סייבר בשרשרת האספקה. מסמך המדיניות כולל דרישה מהגופים המונחים במגזר, למשל בתי החולים, לעמוד בדרישות מתודולוגיית שרשרת האספקה של מערך הסייבר בהתאם ללוחות הזמנים המפורטים במסמך המדיניות. במסמך המדיניות נקבע כי באחריות יחידת הסייבר המגזרית, בין השאר, לאסוף ולנתח מידע רוחבי על ספקים מרכזיים של המגזר ולבצע תהליכים לאכיפת מתודולוגיית שרשרת האספקה על הספקים הקיימים ולתמוך בתהליכי ההתעדה שלהם. בתגובות של הגופים המונחים במגזר על מסמך המדיניות הועלו קשיים ביישום המדיניות ובייחוד ביכולתם לאכוף את החובה ליישם את המתודולוגיה על ספקים וביכולתם להוסיף דרישות חדשות לחוזים קיימים עם הספקים.

בפגישה שקיים צוות הביקורת עם נציגי משרד הבריאות בפברואר 2023 נאמר כי למשרד הבריאות אין תמונה מלאה על מצב הספקים במגזר. לבתי החולים יש רשימה של הספקים שהם עובדים עימם, והם מתכוונים לבצע - בעצמם או באופן מרוכז באמצעות היחידה המגזרית - בקרות על הספקים תוך שימוש בשאלון הספקים של מערך הסייבר.

4. **מרכז הסייבר הפיננסי במשרד האוצר:** היחידה המגזרית הפיננסית נבדלת משאר היחידות המגזריות, בכך שהיא אינה גוף אסדרתי: למשרד האוצר אין אחריות וסמכות לגבי הארגונים במגזר הפיננסי. בפגישה שקיים צוות הביקורת עם מנהל מרכז הסייבר הפיננסי בנובמבר 2022 נאמר כי הספקים אינם מחויבים לעמוד במתודולוגיה של מערך הסייבר והם אינם מוכנים ליישם את המתודולוגיה בגלל העלויות הגבוהות הכרוכות ביישומה. למרכז הסייבר הפיננסי יש רשימה של ספקים מהותיים שמשפיעים על תהליכים קריטיים.

נמצא כי אחת (33%) מתוך שלוש יחידות הסייבר המגזריות שנבדקו (משרד האנרגייה והתשתיות) לא הכווינה את הגופים המונחים שלה ליישם את מתודולוגיית שרשרת האספקה של מערך הסייבר. כמו כן, נמצא כי כל יחידות הסייבר המגזריות נתקלו בפערים ביישום המתודולוגיה: העלויות הגבוהות של תהליך ההתעדה, פרק הזמן שהיא אורכת, הקושי לפעול מול ספקים בין-לאומיים וכן הקושי להוסיף דרישות בתחום הגנת הסייבר למכרזים קיימים.

עוד נמצא כי מערך הסייבר לא בחן את הסיבות לשיעור היישום הנמוך של המתודולוגיה במגזרים השונים. במצב הקיים מגזרים שלמים במשק חשופים לסיכונים מצד שרשרת האספקה.

בתשובת משרד האנרגייה והתשתיות מיוני 2023 נמסר כי הנחיית יחידת הסייבר המגזרית מחייבת את הגופים המונחים למפות את הספקים שעימם הם עובדים, את פרטי הציוד ואת דגמיהם כנדרש במתודולוגיה ולנהל את הסיכונים מולם.

אשר לתשובת משרד האנרגייה והתשתיות, יצוין כי יישום שלב מיפוי הספקים הוא השלב הראשון ביישום של המתודולוגיה, ונדרש כי בחינת כל ספק תבוצע בהתאם לשאלון הספקים הכלול במתודולוגיה. אם משרד האנרגייה והתשתיות סבור כי שאלון הספקים אינו מתאים למגזר, עליו לדון בכך עם מערך הסייבר ולבקש את אישורו.

מומלץ כי מערך הסייבר יוציא ליחידות הסייבר המגזריות הנחיה רוחבית ליישום גרסה 1.4 של מתודולוגיית שרשרת האספקה בגופים הכפופים להנחייתן ויעקוב אחר יישום המתודולוגיה כדי לוודא שניתן מענה על הפערים שנמצאו ביישום גרסה 1.3 של המתודולוגיה.

יישום המתודולוגיה במשרדי הממשלה

הנחיות יה"ב

בהחלטת ממשלה 2443 נקבע ייעודה של יה"ב: הכוונה והנחיה מקצועית בתחום הגנת הסייבר עבור כלל משרדי הממשלה. בהתאם להחלטה זו פרסמה יה"ב בנובמבר 2019 את הנחיה 5.19 - הנחיה מחייבת בנושא שרשרת האספקה, שמטרתה להנחות את משרדי הממשלה בדבר ניהול יעיל של מערך אבטחת המידע ומזעור איומי סייבר אשר מקורם בשרשרת האספקה, לצורך הגברת החוסן של המשרד בפני תקיפות סייבר. ההנחיה הותאמה לשאלון הספקים 1.3.

בהנחיית יה"ב 5.19[35] נכללים בין היתר הסעיפים האלו:

35 הנחיית יה"ב 5.19, סעיף 7.1.

1. בהתאם להחלטת הממשלה 2443, ועל פי האמור בהנחיה[36], על המשרדים לדרוש מכל הספקים המדורגים שלהם (A, B ו-C), לעמוד בתקן אבטחת מידע ISO-27001.

2. יש להכין נוהל עבודה שיתבסס על ההנחיה, יאושר ויתוקף על ידי הנהלת המשרד.

הנחיית יה"ב 5.3 בנושא ניהול סיכוני סייבר מחייבת את המשרדים לבצע סקר סיכונים לפחות אחת ל-36 חודשים ולתקף אותו מדי 18 חודשים. במסגרת תהליך סקר הסיכונים נדרשים המשרדים לבצע מבדק אחיד בתחום אבטחת המידע והגנת הסייבר, ושמו מדד יה"ב, אשר כולל בקרות שגיבש יה"ב, חלקן בנושא שרשרת האספקה.

נמצא כי הבקרות במדד יה"ב בנושא שרשרת האספקה אינן מתייחסות לשלבים מהותיים ביישום הנחיה 5.19 - ההנחיה הייעודית של יה"ב בנושא זה, כמו הדרישה מהמשרדים לבצע מיפוי ספקים ולדרגם.

מומלץ כי יה"ב תעדכן את הבקרות במדד יה"ב באופן שהן יעלו בקנה אחד עם הבקרות הקיימות בהנחיה 5.19 ותבדוק שמדד יה"ב כולל שלבים מהותיים בהנחיה כמו הצורך בביצוע מיפוי ספקים ובדירוגם.

בתשובת יה"ב מיולי 2023 נמסר כי ההמלצה לעדכן את הבקרות בנושא שרשרת האספקה במדד יה"ב לפי הנושאים המהותיים הנכללים במתודולוגיית שרשרת האספקה מקובלת על יה"ב ותטופל.

לוח 3: **מידת יישום הנחיות יה"ב במשרדי הממשלה**

השאלה	שיעור המשרדים
האם הנחיות הגורם המאסדר בנושא שרשרת האספקה מיושמות בארגון? (כן/באופן חלקי/לא).	**71% מהמשרדים לא יישמו את ההנחיות או יישמו אותן חלקית**
האם במכרזים של הארגון יש סעיף שמחייב את הספק לעמוד בתקנים מקובלים בתחום אבטחת המידע או שרשרת האספקה כמו ISO-27001 ?	**43% מהמשרדים אינם מחייבים במכרזיהם לעמוד בתקנים מקובלים בתחום אבטחת מידע**

36 בינואר 2021 התווספה דרישה זו לעמידה בתקן אבטחת מידע לאחר שתמה תקופת ההיערכות ליישום שרשרת האספקה שבמהלכה לא הותעדו ספקים מהותיים.

השאלה	שיעור המשרדים
האם יש בארגון נוהל בנושא שרשרת האספקה?	**19% מהמשרדים לא גיבשו נוהל בנושא שרשרת האספקה**

נמצא כי 22 (71%) מתוך 31 המשרדים שהשיבו על השאלה אינם מיישמים את הנחיית יה"ב 5.19 בנושא שרשרת האספקה או מיישמים אותה באופן חלקי.

בתשובת גוף 32 מיוני 2023 נמסר כי הטענה על אי-היכולת לעמידה בכללי יה"ב ומערך הסייבר בנושא שרשרת האספקה הועלתה על ידי הגוף וגופים נוספים במסגרת דיון שהתקיים עם מערך הסייבר.

כמו כן נמצאו הפערים האלו ביישום חלק מהנושאים שכלולים בהנחיית יה"ב 5.19: במכרזיהם של 10 (43%) מתוך 23 המשרדים שהשיבו על השאלה אין סעיף שמחייב את הספק לעמוד בתקנים מקובלים בתחום אבטחת המידע או שרשרת האספקה כמו-ISO-27001 שנדרש גם בהחלטת ממשלה 2443.

בתשובת גוף 7 מיוני 2023 נמסר כי בתיאום עם אגף חוזים והתקשרויות תתווסף למסמך הנחיות אבטחת מידע לספקים הדרישה לעמוד בתקן ISO-27001. עוד נמסר כי במכרז מיקור חוץ החדש הוגדרה דרישה שהספק יעמוד בתקן ניהול אבטחת מידע ISO-27001.

בתשובת גוף 22 מיוני 2023 נמסר כי הגוף מתקשר עם ספקים קטנים אשר נחשפים לנכסים בעלי סיווג גבוה. חלק מהספקים לעיל אינם מוסמכים לפי תקן ISO-27001, אך תהליך האבטחה מולם מספק. דרישה לעמוד בתקן ISO-27001 הייתה מצמצמת את התחרות. עוד נמסר כי הפער ביישום ההנחיה הוצג ליה"ב לצד המנגנונים המפצים שיושמו בתהליך.

אשר לתשובת גוף 22, יצוין כי על משרדי הממשלה לחייב את הספקים שלהם לעמוד בתקן ISO-27001 בהתאם להחלטת הממשלה 2443, ובמקרים חריגים שבהם יש חשש שתהיה פגיעה בתחרות, על המשרדים להציג לגוף האסדרתי שלהם בתחום הסייבר את הבקרות המפצות שניתנו לצורך כך ולקבל את אישורו.

זאת ועוד ב-6 (19%) מתוך 31 המשרדים שהשיבו על השאלה אין נוהל בנושא שרשרת האספקה.

מומלץ כי המשרדים שאינם מיישמים את הנחיות יה"ב או מיישמים אותן באופן חלקי יפעלו ליישום מלא של ההנחיות.

בתשובות גוף 36 וגוף 9 מיוני 2023 נמסר כי יתווסף למכרזים הבאים סעיף המחייב עמידה בתקן ISO-27001.

בתשובות גוף 9, גוף 10 וגוף 26 מיוני 2023 נמסר כי המשרדים יפעלו לגיבוש נוהל בנושא שרשרת האספקה.

בתשובת גוף 35 מיולי 2023 נמסר כי באפריל 2023 התקיים בגוף יום עיון של יה"ב בנושא שרשרת האספקה ברשת הבלתי מסווגת, על מנת לחדד לעובדים את נוהלי הטיפול במערך זה ואת הדגשים וההמלצות שעולים מטיוטת הדוח.

ליווי ופיקוח של יה"ב על ההנחיה בנושא שרשרת האספקה

כאמור, הנחיית יה"ב 5.19 פורסמה לראשונה בנובמבר 2019. לאחר כשנה של היערכות שבמהלכה לא הותעדו ספקים כמצופה ולאחר שיח עם מערך הסייבר, עדכן יה"ב בינואר 2021 את ההנחיה כך שהדרישה שונתה לעמידה בתקן אבטחת מידע ISO27001 לכלל הספקים, ונוסף על כך ספקי A לא חויבו לבצע התעדה מלאה אלא רק למלא שאלון ספקים באמצעות בודק מוסמך חיצוני. באפריל 2023 עודכנה ההנחיה בהתאם לגרסה 1.4 של מתודולוגיית שרשרת האספקה, המאפשרת לארגון להגדיר אילו ספקים מהותיים שלו יבצעו התעדה מלאה ואילו מהם יעבירו רק הצהרה שמולאה בידי בודק חיצוני מוסמך.

בפגישה שקיים צוות הביקורת עם ראש תחום בקרה ביה"ב בספטמבר 2022 נאמר כי בשל מחסור בכוח אדם, יה"ב מבצעת בקרה על מידת היישום של הנחיות מסוימות בהתאם להערכת סיכונים פנימית, אולם היא אינה מבצעת בקרה בעניין יישומה של הנחיה 5.19 בנושא שרשרת האספקה. כאלטרנטיבה יה"ב שמה דגש על ביצוע בקרות מפצות לעניין סיכוני שרשרת האספקה, ובכלל זה היחידה פרסמה הנחיות בנושאים ייעודיים כמו חיבור מרחוק של ספקים ופיתוח מאובטח.

לוח 4: **קיום דיונים בין המשרדים למאסדר**

השאלה	שיעור המשרדים
האם התקיימו דיונים בין הארגון ובין המאסדר הממשלתי בתחום הסייבר בנוגע ליישום הנחיות המאסדר בנושא שרשרת האספקה?	**42% מהמשרדים לא קיימו דיונים עם יה"ב בנוגע ליישום ההנחיות**

נמצא כי יה"ב פרסמה את הנחיה 5.19 בנושא שרשרת האספקה בנובמבר 2019 ואף עדכנה אותה כמה פעמים מאז, ואולם לאורך כל התקופה היא לא ביצעה ביקורות מעקב אחר מידת יישום ההנחיה, בין היתר בשל מחסור בכוח אדם. כמו כן, נמצא כי 13 (42%) מתוך 31 המשרדים שהשיבו על השאלה לא קיימו דיונים עם יה"ב בנוגע ליישום ההנחיות.

בתשובת יה"ב מיוני 2023 נמסר כי יחידת ההנחיה שלה קיימה מפגשים ושולחנות עגולים עם חלק מהמשרדים כדי לקדם את ההנחיה.

בתשובותיהם של גוף 9, גוף 14, גוף 27 וגוף 29 מיוני 2023 נמסר כי הם הבינו כי הדרישה מהם מבחינת יה"ב בנושא שרשרת האספקה היא שהם יעמדו כמשרד בתקן ISO-27001 בכל מה שנוגע לעבודה מול ספקים.

בתשובת גוף 10 מיוני 2023 נמסר כי עד לפרסום השאלון לא עודכן הגוף בדבר קיום הנחיה 5.19 ואף לא נבדק על מידת יישום ההנחיה. עם הגעת הדרישה ממשרד מבקר המדינה למילוי השאלון, המשרד החל לנקוט יוזמות ופעולות ליישום, כדוגמת מיפוי הספקים וסיווגם, כתיבת נוהל עבודה משרדי והנחיית הלשכה המשפטית בדבר הוספת נספחים בנושא סייבר למכרזים עתידיים והסכמים.

מהמענה של המשרדים בדוח זה עולה כי דרישות הנחיה 5.19 אינן ברורות דיין, וכי חלק ממשרדי הממשלה אינם ממלאים את כל הנדרש מהם בהנחיה. נוכח זאת מומלץ כי יה"ב תקיים ימי הדרכה בנושא ההנחיה העדכנית שמתייחסת לגרסה 1.4 של מתודולוגית שרשרת האספקה, וכי לאחר תקופת הטמעה תקיים בקרה על מימוש ההנחיה במשרדי הממשלה. עוד מומלץ כי משרדי הממשלה יקיימו דיונים עם יה"ב בנוגע ליישום ההנחיות וישתפו אותה בפערים שעולים ביישומה.

בתשובת יה"ב מיולי 2023 נמסר כי הבקרה תבוצע באמצעות עדכון מדד יה"ב בהתאם להנחיה 5.19. כמו כן, בתוכנית העבודה של יה"ב קיימת משימה לביצוע סקר סיכונים מקיף בנושא שרשרת האספקה.

בתשובת גוף 24 מיוני 2023 נמסר כי הגוף יפעל לקיום דיון עם יה"ב בנוגע ליישום ההנחיות.

להלן תרשימים שמציגים את הפערים שעלו ביישום המתודולוגיה במשרדים שענו של השאלון לפי רמות היישום (ראו פירוט על הפערים בפרקים הבאים):

לוח 5: **משרדים שמיישמים את המתודולוגיה ברמת יישום נמוכה (ציון נמוך מ-48)**

הנושאים שנבדקו	גוף 37	גוף 26	גוף 32	גוף 9	גוף 13	גוף 42	גוף 25
איסוף מודיעין סייבר ומודיעין עסקי על ספקי הארגון	✗	✗	✗	✗	✗	✗	✗
ביצוע תרגולים לתקיפת סייבר באמצעות שרשרת האספקה	✗	✗	✗	✗	✗	✗	✗
קיום סעיף במכרזי הארגון המחייב עבודה לפי המתודולוגיה של מערך הסייבר	✗	✗	✗	✗	✗	✗	✗
עבודה לפי מתודולוגיית שרשרת האספקה של מערך הסייבר	✗	✗	✗	✗	✗	✗	✗
מינוי בעל תפקיד ייעודי לנושא שרשרת האספקה	✗	✗	✗	✗	✗	✗	✓
ביצוע סקר סיכונים שכלל התייחסות לנושא שרשרת האספקה	✗	✗	✗	✗	✗	✗	✗
מיפוי הספקים כלל את כל פרטי המידע הנדרשים במתודולוגי	*	*	✗	*	*	✓	✗
נושא שרשרת האספקה נדון במסגרת ועדות ההיגוי	✗	✗	✗	✗	✓	✗	✓
דיונים בין הארגון לבין המאסדר בתחום הסייבר הנוגע לנושא שרשרת האספקה	✗	✗	✓	✗	✗	✗	✓
ביצוע ביקורות סייבר אצל הספקים בשלוש השנים האחרונות (2022-2020)	✗	*	✗	✗	!	*	✗
קיום ספק מהותי בארגון	✓	✗	✗	✓	✓	✗	*
קיום סעיף במכרזים המחייב את הספק לעמוד בתקנים מקובלים	✗	✗	✗	✗	✓	*	✓
מעורבות של הממונה על הגנת הסייבר בתהליך סיום ההתקשרות עם הספק	*	*	✗	*	✗	*	✗
קיום סעיף במכרז שמותיר לארגון לבצע ביקורות סייבר אצל הספק	✗	✓	✗	✗	✗	✗	✗
ביצוע התממת מידע רגיש במכרזי הארגון	✗	✓	✓	✓	✗	✗	✓
קיום נוהל שרשרת האספקה בארגון	✓	✗	✗	✗	✓	✓	✗
ביצוע מעקב שנתי אחר תיקון ליקויים שנמצאו אצל הספק	✗	*	*	✗	✓	*	✗
שרשרת האספקה היא איום ייחוס של הארגון	✗	✗	✗	✓	✓	✓	✓
קיום נספח אבטחת מידע במכרזי הארגון	✗	✗	✓	✗	✓	✗	✓
קיום סעיף במכרז שמחייב את הספק להודיע לארגון על אירוע סייבר במוצר או בשירות המסופק	✗	✗	✓	✓	✗	✗	✓
הפעלת סנקציה נגד ספקים שלא עמדו ברמת ההגנה הנדרשת בתקופת ההתקשרות	*	*	*	*	✗	*	✗
יישום ההנחיות של גורם המאסדר	!	✗	!	✓	✗	!	!
מעורבות ממונה הגנת הסייבר או הממונה על שרשרת האספקה בתהליכי הרכש	!	✗	✓	✓	!	✓	✓
שיעור הנושאים שהגופים יישמו באופן מלא או חלקי	**30%**	**30%**	**35%**	**39%**	**43%**	**43%**	**48%**

✓ כן

✗ לא

! באופן חלקי

* לא נמסר מידע/ לא רלוונטי

על פי תשובות על שאלון שהעביר משרד מבקר המדינה.

נמצא כי 7 (23%) מתוך 31 משרדים מיישמים את המתודולוגיה של מערך הסייבר בנושא שרשרת האספקה ברמה נמוכה (ציון נמוך מ-48).

לוח 6: **משרדים שמיישמים את המתודולוגיה ברמת יישום בינונית (ציון בין 52 - 70)**

הנושאים שנבדקו	גוף 33	גוף 12	גוף 10	גוף 23	גוף 14	גוף 30	גוף 4	גוף 3	גוף 17	גוף 36	גוף 41	גוף 35	גוף 29	גוף 24	גוף 7	גוף 40	גוף 6	גוף 27
איסוף מודיעין סייבר ומודיעין עסקי על ספקי הארגון	✗	✗	✗	✗	✗	✗	✗	✗	✓	✗	✗	✓	✓	✓	✗	✗	✗	✗
ביצוע תרגולים לתקיפת סייבר באמצעות שרשרת האספקה	✗	✗	*	✓	✗	✗	✗	✗	✓	✗	✗	✗	✗	✓	✗	✓	✗	✓
קיום סעיף במכרזי הארגון המחייב עבודה לפי המתודולוגיה של מערך הסייבר	✗	✗	✓	✗	✓	✗	✗	✗	✗	✗	✗	✗	✗	✗	*	✗	✓	✗
עבודה לפי מתודולוגיית שרשרת האספקה של מערך הסייבר	✓	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✓	✓	✓	✗	✗
מינוי בעל תפקיד ייעודי לנושא שרשרת האספקה	✗	✓	✗	✗	✗	✗	✗	✗	✗	✓	✓	✓	✗	✗	✗	✗	✗	✗
ביצוע סקר סיכונים שכלל התייחסות לנושא שרשרת האספקה	✗	✓	✗	✗	✓	✗	✓	✗	✓	✗	✗	✗	✓	✓	✗	✓	✗	✗
מיפוי הספקים כלל את כל פרטי המידע הנדרשים במתודולוגיה	✗	✗	*	✗	✗	✓	✓	✓	✗	✗	✗	✗	✗	✗	*	✗	✗	*
נושא שרשרת האספקה נדון במסגרת ועדות ההיגוי	✗	✗	✗	✓	✓	✗	✓	✗	✓	✓	✗	✗	✓	✗	✗	✗	✓	✓
דיונים בין הארגון לבין המאסדר בתחום הסייבר הנוגע לנושא שרשרת האספקה	✗	✓	✗	✓	✗	✗	✓	✓	✓	✓	✓	✓	✗	✗	✓	✓	✓	✗
ביצוע ביקורות סייבר אצל הספקים בשלוש השנים האחרונות (2022-2020)	!	*	✗	✗	!	✗	*	✗	✗	!	!	✗	*	!	*	✓	*	!
קיום ספק מהותי בארגון	✗	✗	✗	✓	✓	✓	✗	✓	✓	✓	✗	✓	✗	✓	✓	✓	*	*
קיום סעיף במכרזים המחייב את הספק לעמוד בתקנים מקובלים	✓	*	*	*	✓	✓	✗	*	✗	✗	✓	✓	*	✓	✗	✓	✗	*
מעורבות של הממונה על הגנת הסייבר בתהליך סיום ההתקשרות עם הספק	✗	*	*	✗	✓	✓	*	✓	*	✓	✓	✗	✓	✓	✓	✗	✓	✓
קיום סעיף במכרז שמותיר לארגון לבצע ביקורות סייבר אצל הספק	✓	✗	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
ביצוע התממת מידע רגיש במכרזי הארגון	✗	✗	✓	✓	✓	✓	✗	!	✓	✗	✓	✓	✗	!	✓	!	✓	✓
קיום נוהל שרשרת האספקה בארגון	✓	✓	✗	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
ביצוע מעקב שנתי אחר תיקון ליקויים שנמצאו אצל הספק	✓	*	✗	✗	✗	*	*	✓	✗	✓	✓	✓	*	✓	✓	✓	*	✓
שרשרת האספקה היא איום ייחוס של הארגון	✓	✗	*	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✗	✓	✗	✓	✓
קיום נספח אבטחת מידע במכרזי הארגון	✓	✓	✓	✓	✓	✓	✗	✓	✓	✓	!	✓	!	✓	✓	✓	✓	✓
קיום סעיף במכרז שמחייב את הספק להודיע לארגון על אירוע סייבר במוצר או בשירות המסופק	✓	*	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✗	✓	✓	✓
הפעלת סנקציה נגד ספקים שלא עמדו ברמת ההגנה הנדרשת בתקופת ההתקשרות	✓	*	*	*	✗	✓	*	✓	✗	*	*	*	*	✗	*	✓	*	*
יישום ההנחיות של גורם המאסדר	✓	✗	✓	✓	✗	!	!	!	!	!	!	✓	✓	!	!	✓	!	✗
מעורבות ממונה הגנת הסייבר או הממונה על שרשרת האספקה בתהליכי הרכש	!	✓	✓	✓	!	!	!	!	!	✓	✓	✓	!	✓	✓	!	!	✓
שיעור הנושאים שהגופים יישמו באופן מלא או חלקי	**52%**	**52%**	**57%**	**61%**	**61%**	**61%**	**61%**	**65%**	**65%**	**65%**	**65%**	**65%**	**65%**	**70%**	**70%**	**70%**	**70%**	**70%**

✓ כן
✗ לא
! באופן חלקי
* לא נמסר מידע/ לא רלוונטי

על פי תשובות על שאלון שהעביר משרד מבקר המדינה.

נמצא כי 18 משרדים (58%) מתוך 31 משרדים מיישמים את המתודולוגיה של מערך הסייבר ברמה בינונית (ציון בין 52- 70).

לוח 7: **משרדים שמיישמים את המתודולוגיה ברמת יישום גבוהה (ציון 74 ומעלה)**

הנושאים שנבדקו	גוף 31	גוף 22	גוף 18	גוף 28	גוף 34	גוף 8
איסוף מודיעין סייבר ומודיעין עסקי על ספקי הארגון	✗	✗	✗	✗	✓	✗
ביצוע תרגולים לתקיפת סייבר באמצעות שרשרת האספקה	✗	✗	✓	✓	✗	✗
קיום סעיף במכרזי הארגון המחייב עבודה לפי המתודולוגיה של מערך הסייבר	✓	✗	✓	✓	✓	✓
עבודה לפי מתודולוגיית שרשרת האספקה של מערך הסייבר	✓	✗	✓	✓	✓	✓
מינוי בעל תפקיד ייעודי לנושא שרשרת האספקה	✗	✓	✗	✓	✓	✓
ביצוע סקר סיכונים שכלל התייחסות לנושא שרשרת האספקה	✗	✓	✓	✗	✓	✓
מיפוי הספקים כלל את כל פרטי המידע הנדרשים במתודולוגיה	✗	*	✗	✗	✗	✗
נושא שרשרת האספקה נדון במסגרת ועדות ההיגוי	✓	✓	✓	✓	✓	✓
דיונים בין הארגון לבין המאסדר בתחום הסייבר הנוגע לנושא שרשרת האספקה	✓	✓	✗	✓	✓	✓
ביצוע ביקורות סייבר אצל הספקים בשלוש השנים האחרונות (2022-2020)	!	!	!	✓	✗	✓
קיום ספק מהותי בארגון	✓	✓	✗	*	✓	✓
קיום סעיף במכרזים המחייב את הספק לעמוד בתקנים מקובלים	✓	✗	✓	*	✓	✓
מעורבות של הממונה על הגנת הסייבר בתהליך סיום ההתקשרות עם הספק	✓	✓	✓	✗	✓	✓
קיום סעיף במכרז שמותיר לארגון לבצע ביקורות סייבר אצל הספק	✓	✓	✓	✓	✓	✓
ביצוע התממת מידע רגיש במכרזי הארגון	✓	✓	✓	!	✓	✓
קיום נוהל שרשרת האספקה בארגון	✓	✓	✓	✓	✗	✓
ביצוע מעקב שנתי אחר תיקון ליקויים שנמצאו אצל הספק	✓	✓	✓	✓	*	✓
שרשרת האספקה היא איום ייחוס של הארגון	✓	✓	✓	✓	✓	✓
קיום נספח אבטחת מידע במכרזי הארגון	✓	✓	✓	✓	!	✓
קיום סעיף במכרז שמחייב את הספק להודיע לארגון על אירוע סייבר במוצר או בשירות המסופק	✓	✓	✓	✓	✓	✓
הפעלת סנקציה נגד ספקים שלא עמדו ברמת ההגנה הנדרשת בתקופת ההתקשרות	✗	*	✓	*	✓	✓
יישום ההנחיות של גורם המאסדר	!	✓	✓	!	!	✓
מעורבות ממונה הגנת הסייבר או הממונה על שרשרת האספקה בתהליכי הרכש	!	✓	✓	✓	✓	✓
שיעור הנושאים שהגופים יישמו באופן מלא או חלקי	74%	78%	78%	83%	83%	87%

✓ כן
✗ לא
! באופן חלקי
* לא נמסר מידע/ לא רלוונטי

על פי תשובות על שאלון שהעביר משרד מבקר המדינה.

משרד מבקר המדינה מציין לחיוב את ששת המשרדים שמיישמים את המתודולוגיה ברמה גבוהה (ציון 74 ומעלה): גוף 31, גוף 22, גוף 18, גוף 28, גוף 34 וגוף 8.

מומלץ כי המשרדים שמיישמים את המתודולוגיה של מערך הסייבר באופן בינוני ונמוך (ציונים שנכללים בטווח 30 - 70) יפעלו בשיתוף יה"ב ומערך הסייבר להעלאת רמת היישום שלהם ויבחנו יחד פתרונות לטיפול בפערים שעלו מהמענה שלהם על השאלון ששלח משרד מבקר המדינה.

בתשובת גוף 6 מיוני 2023 נמסר כי הגוף מקבל את הערות משרד מבקר המדינה ויפעל לצמצום הפערים העולים מן הדוח. נושא "שיפור ההגנה של המשרד וגופיו מפני מתקפות סייבר" אף נכלל כאחד מיעדי השר לשנים 2023 ו- 2024**.**

בתשובת גוף 10 מיוני 2023 נמסר כי לאחר הגשת השאלון החל הגוף לעבוד מול מערך הסייבר ליישום המתודולוגיה ובשיתוף מלא מול מנחה גוף 9.

בתשובת גוף 40 מיוני 2023 נמסר כי לאחר גיוס ממונה שרשרת אספקה, הגוף יפעל לבחינת הפערים שעלו בדוח ולמציאת פתרונות לטיפול בפערים.

ספקים שיש להם השפעה נרחבת על המשק

מערך הסייבר הגדיר בשנת 2022 איום ייחוס לאומי למשק ותרחישי ייחוס. אחד מהתרחישים התייחס למקרים של אפידמיה או "רכזת" - לפי תרחיש זה מתבצעת תקיפת סייבר על ארגון שמקושר לארגונים רבים ולפיכך היקף הנזק הוא נרחב ומתפשט בקרב גופים רבים במהירות בדומה להתפשטות מחלה אפידמית.

לצורך זיהוי ארגונים שמהווים "רכזת" וניהול הסיכון שעלול להיגרם מפגיעה בהם, נדרש כי הגופים האסדרתיים בתחום הסייבר ינהלו מיפוי עדכני של כלל הספקים שנותנים שירות למשרדים השונים ולגופי התמ"ק ובפרט לספקים המהותיים שלהם. כאמור, אין בידי מערך הסייבר מיפוי של הספקים בגופי תמ"ק ומפגישה שקיים צוות הביקורת עם יה"ב עלה כי היא לא ביקשה מהמשרדים לספק לה את מיפוי הספקים שהם ביצעו במסגרת ההנחיה שנתנה להם.

מלמ"ב שהוא גוף אסדרתי בתחום הגנת הסייבר עבור משרד הביטחון והתעשיות הביטחוניות מנהל רשימה של הספקים המהותיים בגופים אלו ומעביר את הרשימה למרכז מודיעין והכוונה במערך הסייבר כדי לקבל התרעות ככל שעולה חשש לפגיעה בהם. גם מערך הסייבר מעביר את רשימת הספקים שלו למרכז מודיעין והכוונה.

מינהל הרכש אינו מנהל רשימה אחודה של הספקים שזכו במכרזים מרכזיים ושל המשרדים וגופי התמ"ק שעושים בהם שימוש בכל התקשרות. מידע זה נדרש כדי לאתר ספקים שמשמשים "רכזת", ובפרט הוא חיוני בקרות אירוע סייבר שמתרחש אצל אחד מהספקים כדי להתריע על כך לפני יתר הגורמים המשתמשים בהתקשרות. מידע זה גם יכול להיות מועבר למרכז מודיעין והכוונה במערך הסייבר כדי לקבל ממנו התרעות. כמו כן, מינהל הרכש אינו מנהל מודיעין על אודות ספקים שמתמודדים במכרזים מרכזיים ועל ספקים שזכו במכרזים מרכזיים.

בהיעדר מיפוי ספקים שנמצא בידי הגופים האסדרתיים, משרד מבקר המדינה ביצע מיפוי של ספקים שנותנים שירותים למשרדים ולגופי תמ"ק רבים בהתבסס על המענה של משרדי הממשלה על השאלון. לפי מיפוי זה יש 18 ספקים עיקריים בתחום התקשוב והסייבר שנותנים שירותים למשרדים ולגופי תמ"ק רבים - מתוכם חמישה ספקים נותנים שירות ליותר מ-49 משרדים וגופי תמ"ק ושלושה ספקים שנותנים שירות בהיקף כספי שנתי של יותר מ-327 מיליוני ש"ח (ראו תרשים 4 בדוח).

מנתוני תחקיר של אירוע סייבר שאירע בנובמבר 2022 עולה כי ממספר תיבות מיילים של ספק ט' (שנותן שירותים ל-63 משרדים) נשלחו מאות מיילים למשרדים ממשלתיים שהכילו קובץ זדוני. האירוע ממחיש את הסיכון הרב ופוטנציאל הנזק שעשוי להיגרם מפגיעה בספקי "רכזת" אלו.

נמצא כי מערך הסייבר ויה"ב אינם מנהלים רשימה אחודה של הספקים המהותיים שנותנים שירות למשרדי ממשלה ולגופי תמ"ק, של הספקים שזכו במכרזים מרכזיים ושל הארגונים שמשתמשים בכל התקשרות. כמו כן הם לא אוספים מודיעין באופן יזום לצורך קבלת התרעות על חשש לפגיעה בספקים אלו. נוכח זאת אין ביכולת הגופים האסדרתיים לאמוד את רמת החשיפה של המשרדים ושל גופי התמ"ק לספקים אלו ולבצע פעולות יזומות מול הספקים להעלאת רמת ההגנה שלהם.

מומלץ כי הגופים האסדרתיים בתחום הסייבר (מערך הסייבר, יה"ב) יפעלו לקבל את מיפוי הספקים המהותיים מהגופים המונחים שלהם ואת מיפוי הספקים שזכו במכרזים מרכזיים בתחום התקשוב והסייבר ממינהל הרכש, וכי הגופים האסדרתיים יהיו אחראים לעדכון רשימות אלו באופן עיתי. כך יוכלו הגופים האסדרתיים לקבל תמונה מקיפה על רמת החשיפה של המשרדים לספקים אלו ולבצע, במקרה הצורך, פעולות יזומות מולם להעלאת רמת ההגנה שלהם.

בתשובת השב"כ מיולי 2023 נמסר כי זיהוי ארגונים וגופי שרשרת אספקה המשמשים ציר כניסה לתוך גופים מונחים ותשתיות קריטיות הוא חלק מההנחיות הניתנות לגופים המונחים. עוד נמסר כי רשימת הספקים של תשתיות הליבה בגופי תמ"ק על פי רוב ידועה, ומקבלת מענה בכלים הקיימים.

עוד מומלץ שהגופים האסדרתיים בתחום הסייבר יעבירו את רשימת הספקים המהותיים למרכז מודיעין והכוונה במערך הסייבר כדי שהוא יוכל לכסות את הספקים האלו בצי"ח המודיעיני ולהתריע לפני המשרדים אם עולה חשש לפגיעה בהם.

בתשובת מערך הסייבר מיוני 2023 נמסר כי לאור החשיבות שמערך הסייבר רואה בהחזקת תמונה כוללת של מצב הספקים המהותיים, יש יתרון בקבלת תמונת המצב המלאה מהגופים שאותם הם מנחים.

בתשובת יה"ב מיולי 2023 נמסר כי זו דרישה סבירה ממערך הדיגיטל הלאומי לנהל תמונה של הספקים המהותיים המספקים שירות למשרדי הממשלה. עוד נמסר כי איסוף מודיעין מתבצע על ידי יה"ב בנושא מתחמים המזוהים עם המגזר הממשלתי בלבד, וכי אם קיימת רשימת ספקים כזו ניתן לבקש לכסות את הספקים הללו בציר המודיעיני בהתאם להמלצת הדוח.

ספקי אינטגרציה, IT ואחסון ואירוח של אתרים

שירותי אחסון ואירוח של אתרים הם יעד מועדף לתקיפות סייבר, בין היתר בשל הרצון של גורמים עוינים לקבל גישה למקום שבו מוחזק מידע על לקוחות רבים או נתונים רגישים. מנתונים שהתקבלו מה- CERT עולה כי בשנתיים האחרונות (2022-2021) דווח על 84 אירועי סייבר בחברות אחסון.

חברות האחסון הוכרו על ידי הרשות להגנת הפרטיות כמחזיק מאגר מידע כהגדרתו בחוק הגנת הפרטיות, התשמ"א-1981. אי לכך, במקרים רבים כפופות חברות האחסון לחובות שחלות על מחזיק מאגר מידע לפי תקנות הגנת הפרטיות (אבטחת המידע), התשע"ז-2017, והאחראית לאכיפת חובות אלה ולהטלת סנקציות על המפרים היא הרשות להגנת הפרטיות.

הרשות ערכה הליך פיקוח רוחב במגזר חברות האחסון והעיבוד של מאגרי מידע בישראל ופרסמה בשנת 2020 דוח פיקוח רוחב הכולל אמירה חשובה ולפיה עמדת הרשות היא שחברה המספקת לאחר שירותי אחסון או גיבוי של מידע, לרבות בדרך של העמדת שרתים, נחשבת כ"מחזיקה" של המידע ולכן חלות עליה כלל החובות לפי חוק הגנת הפרטיות ותקנות הגנת הפרטיות החלות על מחזיק במאגר מידע.

בפגישה שקיים צוות הביקורת עם נציגי אגף ה-CERT בספטמבר 2022 נאמר כי אף שאירועים רבים מתגלים בחברות אחסון ואירוח של אתרים, חברות אלה אינן ממלאות את כל ההנחיות שהמערך נותן להן, ולכן אותם כשלים שהתגלו בהן ממשיכים להתגלות באירועים הבאים.

בשנת 2022 הקים מערך הסייבר את אגף מרכז ממשקים באגף ה-CERT שאחראי לפעול מול ספקים מהמגזר הפרטי שמשפיעים על גופים רבים ולהעלות את רמת ההגנה שלהם. יצוין כי למערך הסייבר אין מקור סמכות חוקי על ספקים אלו ולכן הטיפול בהם נעשה בשיתוף פעולה, באמצעות פעילויות הדרכה והעלאת המודעות שלהם לסיכונים ולנזק שעשוי להיגרם להם מתקיפת סייבר. כמו כן, במסגרת עבודת מטה לגיבוש חוק הסייבר נבחנת הגדרת גוף אסדרתי לחברות המספקות שירותים דיגיטליים.

להלן דוגמאות לאירועים שהתרחשו בחברות לאחסון ולאירוח אתרים בשנים 2020-2021:

1. באוקטובר 2021 פרצה קבוצת האקרים לחברת אחסון של אתרים והדליפה מידע אישי ורגיש על 1,000,000 משתמשים באתר היכרויות של הקהילייה הגאה וכן מידע על משתמשים באתרים אחרים שאוחסן בשרתים של אותו ספק.

2. בשנת 2020 הושחתו אתרי מרשתת בישראל בעקבות תקיפות סייבר על שירותי אירוח ואחסון של אתרים (Web Hosting). במסמך שפרסם המערך[37] מתוארת פעילות ההסברה הנרחבת של המערך בעקבות האירוע כדי לעורר במשק מודעות לסכנה הנשקפת מצד חברות אלו. פעילות זו היא דוגמה ליכולת של המערך ליזום פעולות במישור הלאומי כדי להעלות את רמת המוגנות של ארגונים רבים במשק שמשתמשים בשירותים של חברות למתן שירותי אחסון ואירוח של אתרים.

37 סקירת פעילות מערך הסייבר הלאומי ב-31.5.20 בנושא תקיפת ספקי שירותי האירוח.

נמצא כי למערך הסייבר אין סמכות לאכוף את מתודולוגיית שרשרת האספקה על חברות אחסון ואירוח של אתרים ועל חברות אינטגרציה ו-IT שנותנות שירות לארגונים רבים במשק. כמו כן התגלו בחברות אלו אירועי סייבר חוזרים (84 אירועי סייבר בחברות אחסון בשנים 2022-2021) שמעמידים בסכנה ארגונים רבים במשק.

בתשובת מערך הסייבר מיוני 2023 נמסר כי אף שלמערך אין סמכות בנוגע לחברות לאחסון ולאירוח של אתרים, ב-CERT הלאומי נעשים מאמצים רבים נושאי פרי, באמצעות מרכז הממשקים, לקביעת סטנדרטים נדרשים לחברות האחסון, שהן "הבטן הרכה" במגזר ה-IT. עד כה 13 חברות הביעו את הסכמתן הוולונטרית למהלך, והמימוש אמור להתחיל בשנת 2023, בכפוף להשלמת התהליך הפנימי במערך.

מומלץ כי מערך הסייבר יבחן את סוגיית ההסדרה של גופים כמו חברות IT ואינטגרציה וחברות אירוח אתרים ובכלל זה את היכולת שלהם ליישם את מתודולוגיית שרשרת האספקה, אם בדרך של אסדרה ואם בדרך אחרת. עוד מומלץ כי מערך הסייבר יבחן סוגיה זו בתיאום עם גופים אסדרתיים רלוונטיים בתחום אבטחת המידע והגנת הסייבר כמו מלמ"ב והרשות להגנת הפרטיות.

ספקים בין-לאומיים

כאמור לכל מגזר יש ספקים מהותיים שמספקים מוצרים או שירותים לארגונים במגזר. בהסתכלות לאומית אפשר למצוא ספקים שמשותפים למגזרים שונים. לעיתים לארגון או אפילו למגזר מסוים אין יכולת לאכוף על ספקים את החובה למלא את הדרישות הנוגעות לשרשרת האספקה, בייחוד כשמדובר בספקים בין-לאומיים גדולים.

בפגישה שקיים צוות הביקורת עם נציגי יחידת המדיניות במערך הסייבר בפברואר 2023 נאמר כי המתודולוגיה המעודכנת עדיין אינה נותנת מענה לספקים בין-לאומיים. כשלב ביניים, המערך הנחה את גופי התמ"ק לפעול לכך שהספקים הבין-לאומיים יגישו הצהרה עצמית בדבר עמידתם במתודולוגיה של המערך. מערך הסייבר החל בתרגום שאלון 1.4, אך נכון למועד סיום הביקורת במאי 2023 הוא לא הושלם.

מהמענה לשאלון של משרד מבקר המדינה עולה כי מתוך כ-60 ספקים שהמשרדים וגופי התמ"ק סיווגו כספקים מהותיים כמחציתם ספקים בין-לאומיים. נכון למרץ 2023 אין אף ספק בין-לאומי מותעד.

בפגישה שקיים צוות הביקורת עם ראש היחידה המגזרית במשרד האנרגייה והתשתיות בפברואר 2023 עלה הצורך לפתח תפיסה לאומית בעניינם של ספקים בין-לאומיים המעניקים שירות לכמה מגזרים. לדוגמה, הוצע לבחון את הארכיטקטורה של רכיבים של בקרים תעשייתיים שונים של חברה מסוימת שמסופקים למגזרים שונים במשק הישראלי, ולנוכח תובנות אלו מערך הסייבר כגוף אסדרתי בתחום הסייבר ינהל את השיח לגבי דרישות האבטחה שהחברה צריכה לעמוד בהן. עוד עלה בפגישה כי משרד האנרגייה והתשתיות ניסה להחיל תקינה בין-לאומית בסייבר על מוצרי יצרני מערכות בקרה אשר מוטמעים במתקני הייצור בישראל כפי שדורשות

כמה חברות בעולם, והוא פנה בעניין זה למערך הסייבר באפריל 2022 אך הנושא לא התקדם נכון למועד הפגישה.

נמצא כי למתודולוגיית שרשרת האספקה של מערך הסייבר אין מענה לספקים בין-לאומיים אף שהם נמצאים במגזרים רבים ובארגונים רבים ובהם גופי תמ"ק. עוד נמצא כי מערך הסייבר לא קידם את הסדרת השימוש בתקינה בין-לאומית בסייבר בתחומים כמו הבקרים התעשייתיים. נוכח זאת ספקים אלו אינם מותעדים ולא מתבצעות עליהם בקרות. כמו כן לא הושלם תרגום של שאלון 1.4 לאנגלית.

מומלץ כי מערך הסייבר יבחן בשיתוף יחידות הסייבר המגזריות כיצד ניתן לבצע בקרות על ספקים בין-לאומיים, בין השאר, באמצעות שאלון מותאם ושימוש בתקינה בין-לאומית כתחליף לבקרות שבשאלון הספקים. כמו כן מומלץ כי מערך הסייבר יאתר ספקים בין-לאומיים שנותנים שירותים למספר מגזרים או להרבה משרדים וגופי תמ"ק ויפעל להפחתת הסיכון הנשקף בגינם. עוד מומלץ כי מערך הסייבר ישלים תרגום לאנגלית של שאלון 1.4 וינגישו לכלל הגופים.

בתשובת השב"כ מיולי 2023 נמסר כי קיימים כמה תהליכים המאפשרים לצמצם את האיום מצד ספקים בין-לאומיים.

☆

מערך הסייבר כגוף אסדרתי בתחום הגנת הסייבר אחראי לקדם את רמת ההגנה במשק. המערך זיהה עוד בשנת 2018 את איום הייחוס של תקיפה באמצעות שרשרת האספקה של ארגונים כסיכון גבוה וגיבש מתודולוגיה בנושא. עם זאת, עולה כי מרבית המשרדים הממשלתיים (71%), וגופי התמ"ק (69%) וכל שלוש יחידות הסייבר המגזריות שנבדקו מיישמים באופן חלקי את המתודולוגיה או לא מיישמים אותה כלל. נוכח זאת, נוצר מצב שיש ספקים שנותנים שירותים למשרדים ולגופי תמ"ק רבים שהם אינם מותעדים ואף אין גורם שמבצע עליהם בקרות כדי לוודא את רמת ההגנה בסייבר שלהם. עוד עולה כי בידי הגופים האסדרתיים בתחום הסייבר ובהם מערך הסייבר ויה"ב, אין תמונת רוחב של הספקים המהותיים שנותנים שירותים למשרדים ולגופי תמ"ק רבים. גיבוש תמונת מצב זו נדרשת לגופים האסדרתיים לצורך נקיטה בפעולות שיביאו להעלאת רמת ההגנה מול ספקים אלו שהסיכון שלהם כלפי המשק הוא גדול יותר.

מומלץ כי מערך הסייבר יפעל בשיתוף כלל הארגונים (המשרדים, גופי התמ"ק ויחידות הסייבר המגזריות) כדי לגשר על החסמים הקיימים ביישום המתודולוגיה וכדי להביא ליישומה המלא.

מכרזים מרכזיים - ניהול הסיכונים של שרשרת האספקה

הכוונה והנחיה של מינהל הרכש על ידי גוף אסדרתי בתחום הסייבר

כאמור בשנת 2021 כ-57% מהיקף הרכש של המשרדים בתחום התקשוב והסייבר שהיה בהיקף כספי של כ-1.4 מיליארד ש"ח, התבצע באמצעות מכרז מרכזי. ספק שזוכה במכרז מרכזי מבצע התקשרויות עם משרדים רבים, חברות ממשלתיות וגופי תמ"ק. לפיכך, גם אם מדובר בספק שמדורג כבעל סיכון נמוך בכל משרד בנפרד ייתכן שנשקף בגינו סיכון גבוה כאשר בוחנים את היקף ההתקשרויות שלו עם כלל לקוחותיו ואת המידע שאליו הוא נחשף במסגרת התקשרויותיו הרבות.

כל התקשרות שבמסגרתה ניתנת לספק גישה למאגר מידע חייבת לעמוד בהוראות תקנה 15 לתקנות אבטחת מידע.

בהחלטת ממשלה 2097 נקבע כי לצורך מימוש תפקידיו של התקשוב הממשלתי יש לתת לו סמכויות, כלים ומשאבים, בין היתר "להנחות את החשבת הכללית והממונה על התקשוב הממשלתי להסדיר את מעורבות הממונה על התקשוב הממשלתי או נציגו בתהליכי הרכש, לרבות בוועדת המכרזים המרכזיים למחשוב וטכנולוגיה ובוועדת המשנה לנושאי שירותי מחשוב".

בתשובת מערך הדיגיטל הלאומי מיוני 2023 נמסר כי בהתאם להחלטה זו יש למערך הדיגיטל הלאומי נציגות בוועדת המכרזים המרכזיים וכמו כן מוטלת על הועדה החובה להיוועץ בראש המערך כשמדובר בנושאים פרויקטליים מורכבים עם סיכון גבוה. הייצוג הזה נעשה עד היום על ידי חטיבת המשילות במערך התקשוב, וכיום על ידי יחידת ה-CIO במערך הדיגיטל הלאומי. הכוונה היא שבדרך זו יובאו לידי ביטוי גם הצרכים הנוגעים להנחיות יה"ב.

בנספח ז' בהחלטת ממשלה 2443 בנושא "הובלה ממשלתית בהגנת הסייבר – רכש" נקבע כי מערך הסייבר (נקרא המטה בזמנו) יקים תת-ועדה בהשתתפות נציגים מהחשב הכללי, יה"ב, שירות הביטחון הכללי ומשרד הכלכלה, שתגבש מתווה ועקרונות בנוגע לאופן רכישת שירותים ומוצרים תוך שימוש בתקינת אבטחת מידע במערכות הממשלתיות, בתוך 180 יום מיום קבלת ההחלטה. לפי ההחלטה מינהל הרכש הממשלתי והמנכ"לים של משרדי הממשלה אחראים לכך שרכש שירותים ומוצרים בתחום הגנת הסייבר יבוצע בהתאם למתווה ולעקרונות שיגובשו על ידי תת-הוועדה.

מפגישות שערך משרד מבקר המדינה עם יחידת המדיניות בפברואר 2023 נאמר כי התקיימו דיונים עם מינהל הרכש ויה"ב בהתאם לנספח ז' בהחלטת ממשלה 2443 בשנים הראשונות לאחר ההחלטה (שנת 2015), אולם אין סיכומים של הפגישות ומכל מקום היחסים בין המערך למינהל הרכש אינם יחסים של מנחה-מונחה אלא יחסים המתאפיינים בשיח בין שותפים ומתן המלצות.

בפועל מערך הסייבר איננו מנחה של מינהל הרכש בתחום הגנת הסייבר. בפגישה שקיים צוות הביקורת עם מערך הסייבר ביוני 2022 נאמר כי כיום אין תהליך סדור שמגדיר את מעורבות מערך הסייבר במכרזים מרכזיים שמבצע מינהל הרכש והמערך מלווה את מינהל הרכש רק במכרזים אחדים לפי בקשת מינהל הרכש. למשל: במכרז נימבוס לאספקת שירותי ענן על גבי פלטפורמה ציבורית עבור משרדי הממשלה.

האגף לביטחון, חירום וסייבר במשרד האוצר (להלן - אגף בטחון וסייבר באוצר) אחראי להנחות מהבחינה המקצועית את כל יחידות משרד האוצר, למעט בנושא הליכי הרכש המרכזי המבוצעים על ידי מינהל הרכש. אגף ביטחון וסייבר באוצר שותף להגדרת דרישות בנושאי אבטחת המידע והגנת הפרטיות במכרזים מרכזיים של יחידות במשרד האוצר (למעט במכרזים שמגבש מינהל הרכש). להלן דוגמאות למכרזים מרכזיים שהאגף היה שותף להם והוסיף דרישות ליישום מתודולוגיית שרשרת האספקה: מכרז ביטוח רכב פרטי לעובדי מדינה 2022, מכרז 6568-2021 לניהול ולהנפקה של אמצעי תשלום מתקדמים.

בפגישה שקיים צוות הביקורת עם ראש מינהל הרכש ביוני 2022 נאמר כי אף שהמינהל אינו גוף מנחה בתחום הסייבר, מתוך הסתכלותו הרחבה וההוליסטית על המכרז ומאפייניו, וכדי לתת למשרדי הממשלה את המענה המיטבי שהוא השגת התמורה הגבוהה ביותר למחיר, באופן המניב לגוף המזמין את מרב היתרונות מהליך הרכש, מינהל הרכש הוא בעל הסמכות הבלעדית לקבוע את דרישות המכרזים ואת תנאיהם בהתייחס לכלל ההיבטים הרלוונטיים, לרבות בנושאי אבטחת המידע וההגנה בסייבר.

מינהל הרכש מסתייע בשירותיהם של יועצים חיצוניים בתחום אבטחת המידע והגנת הסייבר ומקבל מהם חוות דעת בנושא גיבוש מכרזים בתחום התקשוב והסייבר. עורך המכרז, שהוא עובד מינהל הרכש, מקבל את ההחלטה הסופית בעניינם של הנושאים שייכללו במכרז. היועצים החיצוניים של מינהל הרכש עובדים בחברות שמספקות שירותים לממשלה, ולכן הדרישות בנספחי אבטחת המידע חלות גם עליהם.

לדברי מינהל הרכש, הוא החל לצרף למכרזים שהוא מבצע נספח אבטחת מידע רוחבי שמשולב במכרזים המרכזיים המתפרסמים מאז הרבעון השני של שנת 2021.

נמצא כי הנספח שמצרף מינהל הרכש למכרזים מרכזיים לא כולל דרישות בהתאם למתודולוגיה של שרשרת האספקה של מערך הסייבר ואינו מחייב לעבוד לפיה. כמו כן נספח זה אינו כולל דרישות אחרות של הגופים האסדרתיים בתחום הסייבר, כמו העמידה בתקנה 15 א' של הרשות להגנת הפרטיות וחובת עמידת הספק בתקן ISO-27001 בהתאם לנדרש בהחלטת הממשלה 2443.

בנובמבר 2022 פרסם מינהל הרכש את טיוטת נספח ז' להוראת התכ"ם 7.3.1[38] (להלן - טיוטת נספח ז'), העוסקת באחריותם של ספקי הממשלה בתחום אבטחת המידע והסייבר, שתצורף כנספח למכרזים מרכזיים ולמכרזים משרדיים. יובהר כי מדובר בטיוטה הכפופה לשינויים, אשר הופצה לקבלת הערות הציבור וכן לקבלת הערות של ספקי הממשלה וגורמים רלוונטיים אחרים,

38 הוראת תכ"ם 7.3.1 עודכנה לאחרונה ב-14.3.23, ועדכון זה טרם כלל את טיוטת נספח ז'.

ובמסגרת זו ביקש מערך הסייבר לכלול התייחסות למתודולוגיית שרשרת האספקה (ראו פרק בנושא נספח אבטחת מידע במכרזים משרדיים).

מינהל הרכש מסר בתשובתו מיוני 2023 כי לגבי "תקן שרשרת האספקה" הנושא לא נוסף בשנת 2022 לנספח אבטחת מידע בתיאום עם גורמים ממערך הסייבר, בשל הבשלות הנמוכה של התקן ומספר המוסמכים המזערי המשויך לו.

בתשובת מערך הסייבר מיולי 2023 נמסר כי ככלל דרישות אבטחת מידע וסייבר במכרזים מרכזיים צריכות להיות בהלימה להנחיות הגופים האסדרתיים בתחום הסייבר (למשל: עמידה במתודולוגיית שרשרת האספקה). במקרים שבהם מסתמן קושי ליישם דרישות אלו כהווייתן או יש חלופה טובה יותר (למשל: תקינה בין-לאומית ייעודית לנושא), על מינהל הרכש לפנות לגופים האסדרתיים בתחום ולבקש את הסכמתם לדרישות החלופיות. לגבי תגובת מינהל הרכש, במועד כתיבת הביקורת נדרשת עמידה במתודולוגיית שרשרת האספקה כפי שבאה לידי ביטוי בשיח המתמשך שנסב על טיוטת נספח ז', אשר במסגרתו הודגשה החשיבות שמערך הסייבר רואה בהוספת הפניה והתייחסות למתודולוגית שרשרת האספקה.

בתשובת יה"ב מיולי 2023 נמסר כי דרישות אבטחת מידע וההגנה בסייבר צריכות להיכתב בהתאם להנחיות הגופים האסדרתיים בתחום הסייבר במשק. המצב המתואר בדוח איננו תקין להבנתם, ויש להסדיר אותו באופן חד-משמעי.

להלן דוגמאות למכרזים מרכזיים בהם גופים אסדרתיים בתחום הסייבר ביצעו ביקורות על הספקים הזוכים והממצאים שהעלו הביאו להוספת דרישות אבטחה אצל הספק ששיפרו את רמת ההגנה שלו:

מכרז מרכזי לרכש מערכת הטלפונייה "שירלי": לאחר הזכייה של הספק לאספקת שירותי הטלפונייה "שירלי" ביקש מינהל הרכש מיה"ב, באופן חריג, לעשות בקרת אבטחת מידע על המערכת, ובעקבות כך הוציאה יה"ב למשרדי הממשלה הנחיות ודרישות לגבי אופן יישום החיבור למערכת זו שהעלו את רמת ההגנה של המערכת במשרדים השונים.

מכרז בתחום התקשוב - א': בעקבות ביקורת שעשה גוף 21 על הספק שזכה במכרז ונוכח היעדרן של דרישות אבטחה פיזית מספקות בנושא, החליט גוף 21 שלא להתקשר עם הספק הזוכה באמצעות מכרז זה. לאחר שגוף 21 הוסיפו דרישות אבטחת מידע ואבטחה פיזית נוספות והספק יישם אותן, גוף 21 החל להשתמש במכרז.

להלן דוגמא למכרז מרכזי בתחום התקשוב ואבטחת המידע שהיו בו דרישות אבטחה חסרות ביחס לדרישות גופים אסדרתיים בתחום הגנת הסייבר:

במכרז בתחום התקשוב - א' היו חסרות דרישות הנוגעות לנושאים כמו חובת הדיווח למזמין או למי שיקבע על ידו על אירועי סייבר אצל הספק ולסמכות של המזמין או למנחה מטעמו לבצע ביקורות על הספק בעקבות אירועי סייבר. דרישות אלו לא התווספו להתקשרות למרות שתקופת ההתקשרות הוארכה פעמיים ולאחרונה ביולי 2022.

בתשובת מינהל הרכש מיוני 2023 נמסר כי לא הועלה בפניהם הצורך לכלול דרישה לביקורות על הספק מאף גורם מנחה.

אשר לתשובת מינהל הרכש יצוין כי דרישה לביקורות היא דרישה שנכללת בתקנות אבטחת מידע, במתודולוגיית שרשרת האספקה וכן בהנחיית יה"ב, וכי שילוב דרישה זו במסגרת חידוש ההתקשרות עם הספק יאפשר לוודא כי הספק עומד בדרישות אבטחת מידע הכרחיות במכרזים.

נמצא כי אף שכ-57% מהרכש הממשלתי בתחום התקשוב והסייבר (בהיקף כספי שנתי של כ-1.4 מיליארד ש"ח) מבוצע באמצעות מכרזים מרכזיים, אין דרישה של מינהל הרכש מהספקים שעימם הוא מתקשר לעמוד במתודולוגית שרשרת האספקה של מערך הסייבר. כמו כן מערך הסייבר ויה"ב, המנחים באופן שוטף את גופי התמ"ק ואת המשרדים, אינם משולבים באופן קבוע בתהליך גיבוש הדרישות של מכרזים מרכזיים בתחום התקשוב והסייבר שמבצע מינהל הרכש, בעוד שמינהל הרכש מסתייע ביועצים חיצוניים לגיבוש המכרז.

מומלץ כי מינהל הרכש יכלול את דרישות הגופים האסדרתיים בתחום הסייבר במכרזיו ובפרט את הדרישה ליישם את מתודולוגיית שרשרת האספקה גרסה 1.4, ובמקרים בהם הוא סבור כי יש קושי ליישם דרישות אלו כהווייתן או יש חלופה טובה יותר, מומלץ כי הוא ידון בסוגיה זו עם הגופים האסדרתיים ויקבל את הסכמתם ליישום דרישות חלופיות.

בתשובת יה"ב מיולי 2023 נמסר כי מדיניות בנושא סייבר צריכה להיקבע על ידי גורמים מוסמכים בתחום זה, וכי יש להסדיר נושא זה תוך התחשבות באחריות הכוללת של מינהל הרכש למכרז תוך התחשבות באחריות המטריציונית של מערך הסייבר ושל יה"ב בתחום הסייבר בממשלה, וזאת גם לפי החלטות ממשלה 2443 ו-2097.

עוד מומלץ שבמכרזים המרכזיים שיוגדר עבורם שהגופים האסדרתיים בתחום הסייבר מלווים אותם בשלב גיבוש המכרז הם יבצעו, בין היתר את הפעולות האלו: ניתוח סיכונים לאומי לגבי השירות או המוצר שבהם עוסק המכרז, הגדרת דרישות אבטחה הולמות בהתאם לניתוח הסיכונים, מעורבות בשלב בדיקת ההצעות של הספקים, פרסום הנחיות לגבי אופן השימוש המאובטח במוצר או בשירות וכן מתן חוות דעת לעורך המכרז לגבי התחלת השימוש במוצר או בשירות.

ביצוע ביקורות על מכרזים מרכזיים בתחום התקשוב והסייבר

מתודולוגיית שרשרת האספקה מגדירה סדרה של בקרות ליישום במהלך ההתקשרות, למשל: יש לתקף לפחות אחת לשנה את מידת עמידתם של ספקים מהותיים בהתחייבויותיהם שבחוזה ההתקשרות (ראו פרק על בקרות).

אחת ממטרות המתודולוגיה היא לשפר את היעילות ולמנוע מצב שבו ארגונים שונים יבצעו בקרות דומות עבור אותם שירותים של הספק. כשמדובר בספקים מהותיים הנותנים שירותים לארגונים רבים או בספקים המשתתפים במכרזים מרכזיים מתבקש כי ניהול ביקורת אלה ירוכז בידי גורם אחד המומחה בביצוע בקרות בתחום אבטחת המידע.

במערך הסייבר פועלות היחידות האלו: יחידה האחראית לביצוע מבדקי חוסן בגופי תמ"ק ויחידה האחראית למתן סיוע לארגונים בהתעורר חשש לביצוע אירוע סייבר. כמו כן, במערך מועסקים עובדים שהוכשרו כבודקי ספקים מאושרים. גם יחידת יה"ב מבצעת מבדקי חוסן וביקורות כדי לבחון את מצב הגנת הסייבר במשרדי הממשלה. יחידה זו אף ביצעה ביקורת על הספק שזכה במכרז המרכזי לרכש מערכת הטלפונייה "שירלי" היות שמשרדים רבים משתמשים במערכת זו.

במכרזים מרכזיים שפרסם החשכ"ל ואשר כללו פרק הנוגע לבקרה על אבטחת מידע[39], צוין כי "הספק יאפשר לתחום סייבר במשרד האוצר[40] או למזמין (המשרד שמשתמש במכרז) או למי שימונה מטעמו לפקח על אספקת השירותים המבוקשים, טיבם ואיכותם, ולהיכנס לצורך זה לכל מקום, על מנת לבדוק ולפקח על אופן מילוי התחייבויותיו".

לפי טיוטת נספח ז' להוראת התכ"ם 7.3.1, הגורם המנחה ומינהל הרכש יהיו רשאים לקבל לידיהם את כל הסמכויות הנתונות למזמין, ובכלל זה הסמכות לבצע ביקורות תקופתיות וכן הסמכות לבצע ביקורות בהתעורר חשש לתקיפת סייבר.

בפגישות שקיים צוות הביקורת עם נציגי מערך הסייבר ויה"ב נמצא כי הגופים האסדרתיים בתחום הסייבר אינם עושים ביקורות על ספקים מהותיים הנותנים שירותים לארגונים רבים או על ספקים שזכו במכרזים מרכזיים, זאת כיוון שלטענתם לא ניתנה להם סמכות לבצע את הביקורות על ספקים של משרדי ממשלה וגופי תמ"ק וכשביקורת כזו נערכה הדבר היה לבקשת מינהל הרכש.

בפגישות שקיים צוות הביקורת עם ראש מינהל הרכש נאמר כי למינהל הרכש אין גוף שמבצע ביקורות וכי הוא אינו מבצע ביקורות על ספקים במהלך ההתקשרויות עימם. במסגרת המכרז מוקנות מגוון של סמכויות למזמינים. בהודעות המכרזים המתפרסמות בקרב המשרדים מפורטים הדרישות והתנאים הרלוונטיים ומוקנית למשרדים מידה רבה של חופש בניהול תהליכי העבודה מול הספקים, ובכלל זה בביצוע הבקרה הנדרשת עליהם. עוד צוין כי היו מקרים חריגים שבהם נערכו ביקורות על ספקים של מכרזים מרכזיים באמצעות הגופים האסדרתיים בתחום הסייבר, למשל במכרז שירלי שבו יה"ב ביצעה ביקורת.

בפגישות שקיים צוות הביקורת עם משרדי ממשלה נאמר כי המשרדים אינם עורכים ביקורות על ספקים שזכו במכרזים מרכזיים היות והם סומכים על כך שמינהל הרכש כעורך המכרז מבצע זאת עבורם. למשל, בתשובת גוף 32 מיוני 2023 נמסר כי המשרד אינו מוצא טעם לבצע בדיקות של שרשרת אספקה עבור ספקים שנבחרו ונבדקו על ידי מינהל הרכש אשר מספקים ציוד או שירות למשרדי הממשלה.

---

39 לדוגמה, מכרז 6568-2021 לניהול ולהנפקה של אמצעי תשלום מתקדמים, בפרק "בקרה ופיקוח אבטחת מידע".

40 תחום במערך סייבר, חירום וביטחון.

נמצא כי מערך הסייבר, יה"ב ומינהל הרכש אינם עושים ביקורות על ספקים מהותיים הנותנים שירותים למשרדים ולגופי תמ"ק רבים וכן על ספקים שזכו במכרזים מרכזיים, אף ששיעור המכרזים מרכזיים היה בשנת 2021 כ-57% מכלל ההתקשרויות של משרדי הממשלה והיקפם הכספי היה כ-1.4 מיליארד ש"ח. כמו כן המשרדים, שסומכים על כך שהגופים האסדרתיים או מינהל הרכש עושים זאת, אינם מבצעים ביקורות בעצמם, ולפיכך בפועל לא מתבצעת שום בקרה על ספקים אלו כמתחייב ממתודולוגיית שרשרת האספקה ואף שנשקף מספקים אלו סיכון לרציפות התפקודית של משרדי הממשלה ושל גופי התמ"ק.

בתשובות מערך הסייבר ויה"ב מיוני 2023 נמסר כי כיום אין להם מקור סמכות לבצע ביקורות על ספקים של משרדי ממשלה וגופי תמ"ק וכשביקורת כזו נערכה זה היה לבקשת מינהל הרכש. יה"ב הוסיפה כי היא איננה מוסמכת לבצע ביקורות בחצרות ספקים מהמגזר הפרטי והאחריות לביקורות ספקים מוטלת על המזמין. עוד נמסר כי ישנה תועלת מהותית בביצוע בקרות כאשר הן ממוקדות במערכת רוחבית, כגון מערכת "שירלי", ולא במענה גורף לכל מערכת באשר היא.

בתשובת מינהל הרכש מיוני 2023 נמסר כי אין בסמכותו לעשות בקרה זו שכן אין לבדיקה שכזו מעמד בפני המשרדים וכי גם בדיקה של יחידת יה"ב לא תהווה אסמכתא לגופים אסדרתיים נוספים. עוד נמסר כי יינתן מענה לנושא עריכת הביקורות במסגרת עדכון הוראת תכ"ם 7.3.1.

בתשובת גוף 22 מיוני 2023 נמסר כי הוא ממליץ כי במכרזים מרכזיים תתבצע בדיקה של הספק ודירוגו על ידי יחידה ייעודית בממשלה עבור כלל משרדי הממשלה. ניתן לראות דוגמה מוצלחת להמלצה זו בניהול אבטחת פרויקט "שירלי" על ידי יה"ב.

בתשובת גוף 25 מיוני 2023 נמסר כי הגוף מבקש לבחון, לאור ההתבססות המרבית על רכש במסגרת מכרזי חשכ"ל, שהאכיפה והביצוע יחד עם המעקב אחר תיקון הליקויים שנמצאו אצל הספקים יתבצעו במלואם על ידי הגופים האסדרתיים.

מומלץ כי מינהל הרכש, מערך הסייבר ויה"ב יגדירו יחד את סוגי המכרזים המרכזיים וסוגי השירותים בתחום התקשוב והסייבר אשר יש תועלת שגוף אסדרתי בתחום הגנת הסייבר יבצע ביקורות עליהם, בדגש על מכרזים מרכזיים שרמת הסיכון והרגישות בהם גבוהה, ויפעלו מול המזמין לשילוב הוראה במכרז המאפשרת להם לבצע ביקורת בנושא. עוד מומלץ כי ביתר המכרזים המרכזיים יובהר למשרדים ולגופי התמ"ק המשתמשים במכרז שהם אחראים לבצע ביקורות, וכן מומלץ כי המאסדר יבצע מעקב אחר ביצוע הביקורות ותיקון הליקויים שעולים בביקורות.

בתשובת מינהל הרכש מיוני 2023 נמסר כי כל עוד הביקורת תיעשה בהתאם לדרישות האבטחה במכרז כלשונן, ולא בהתאם לדרישות שאינן מחייבות את הספק, אין למינהל התנגדות לכך.

דיווח של ספקים במכרזים מרכזיים על אירועי סייבר

מערך הסייבר הוא הגורם המדינתי המטפל באירועי סייבר, ובכפוף למערך פועל ה-CERT הלאומי. המערך מפעיל גם מרכז מבצעי לדיווח על אירועי סייבר (להלן - מוקד 119), המאפשר לכל אזרח וארגון ליצור קשר עם מערך הסייבר לשם דיווח על אירוע סייבר, על ניסיון לביצועו או על חשד לביצועו. מוקד 119 מאויש 24 שעות ביממה באנליסטים שתפקידם לזהות את סוג האיום, לאמוד את היקף הנזק הנשקף בגינו, ולספק מענה מותאם כדי להפחיתו (הכוונה, כלים לטיפול באירוע ומתן הנחיות להעלאת רמת ההגנה על הנכסים הדיגיטליים)[41]. כאשר מתקבל מידע במוקד, מתבצע מיון ראשוני שבמסגרתו, בין היתר נבדקת מידת הערכיות של הארגון שיש חשש כי התבצע בו אירוע סייבר, למשל האם מדובר בארגון תמ"ק. יש תהליך המגדיר את אופן הטיפול בכל פנייה לפי מאפייניה. כאשר מתגלה אירוע סייבר, האגף מגבש את תמונת המצב לגבי האירוע, ואם נדרשת התערבות וסיוע לארגון שיש חשש כי התרחש בו אירוע סייבר, הרי שצוות הכפוף ל-CERT מבצע אותה.

בפגישה שקיים צוות הביקורת עם ראש מינהל הרכש ביוני 2022 נאמר כי ספקים שזכו במכרזים מרכזיים מחויבים לדווח רק למינהל עצמו על אירוע סייבר שמתרחש אצלם, וכי לא חלה עליהם חובת דיווח למוקד 119 של מערך הסייבר.

בטיוטת נספח ז' להוראת תכ"ם 7.3.1 התווספה דרישה מהספק ולפיה עליו להודיע למזמין בהקדם האפשרי, במהלך כל שעות היממה, על כל אירוע אבטחה אשר נשקף בגינו סיכון למידע או למערכות של המזמין או עלול להשפיע על יכולתו לעמוד בהתחייבויותיו שבהן עוסק ההסכם. בנוסף נקבע כי ניתן יהיה לאצול את סמכויותיו של המזמין גם לגורם המנחה ולמינהל הרכש.

נמצא כי במכרזים מרכזיים שמפרסם מינהל הרכש לאחר שנת 2021, עם תחילת השימוש בנספח אבטחת מידע, מצוינת חובתו של הספק לדווח ישירות למינהל הרכש על כל אירוע סייבר שהתרחש אצלו, מיד לאחר התרחשותו, אולם לא מצוינת חובתו של הספק לדווח על כך למערך הסייבר. כמו כן, בטיוטת נספח ז' להוראת התכ"ם 7.3.1 נקבע כי ניתן יהיה לדווח על האירוע לגורם המנחה או למינהל הרכש במקום למזמין. מכיוון שבמינהל הרכש אין מוקד שתפקידו לקבל פניות על חשש לאירועי סייבר ולנתח את המידע המתקבל - כמו המוקד שבמערך הסייבר - הדבר עלול לגרום לחוסר טיפול באירוע או לשיהוי בתגובה ולסכן את המשרדים.

מומלץ כי למכרזים מרכזיים בתחום התקשוב והסייבר וכן לנוסח הסופי של נספח ז' בהוראת התכ"ם 7.3.1 תתווסף הנחיה המחייבת את הספק לדווח הן למערך הסייבר והן למזמין על כל חשש לאירוע אבטחת מידע וסייבר שיתרחש אצלו, היות ולמערך הסייבר יש מוקד ייעודי הפועל 24 שעות ביממה ומערכות, ידע ומומחיות לטיפול באירועים אלו.

41 מתוך אתר המרשתת של מוקד 119: https://www.gov.il/he/departments/general/contact.

בתשובת מערך הסייבר מיוני 2023 נמסר כי הנושא נמצא בשיח בין מערך הסייבר למינהל הרכש, אשר בוחן את הבקשה לקדם הנחיה המחייבת את הספק לדווח הן למערך הסייבר והן למזמין על כל חשש לאירוע אבטחת מידע וסייבר אצלו.

בתשובת מינהל הרכש נמסר כי חלק גדול מלקוחות המכרזים המרכזיים אינם מונחים על ידי מערך הסייבר. למשל, יש גופים אשר מונחים על ידי השב"כ והוא אוסר לדווח על אירועים לגורמים מנחים אחרים. מכאן כי מינהל הרכש אינו יכול לדרוש מספקי המכרזים המרכזיים חובת דיווח לגורם מנחה כזה או אחר.

אשר לתשובת מינהל הרכש, יצוין כי מערך הסייבר הוא הגוף שמנחה את מרבית הגופים במשק וכן יש לו מנגנון לטיפול באירועי סייבר ולהפצת מידע עליהם ליתר הגופים האסדרתיים בתחום הסייבר ולגופים המונחים על ידו, ולכן מינהל הרכש צריך לדווח על האירוע למערך הסייבר.

עוד מומלץ כי הגופים האסדרתיים בתחום הסייבר וגורמים המנחים את עצמם ומשתמשים במכרזים מרכזיים יעבירו למינהל הרכש באופן עיתי סיכום של האירועים שהתרחשו אצל הספקים שזכו בכל מכרז מרכזי ושל אופן הטיפול בהם והמלצות להמשך העבודה עם הספק.

בתשובת מערך הסייבר מיוני 2023 נמסר כי ההמלצה מקובלת עליו, ובתנאי שמדובר באירועים שבהם יש רלוונטיות למינהל הרכש ושאין מניעה מבצעית או אחרת להעביר מידע על הגוף המותקף או האירוע.

זוכה יחיד במכרזים מרכזיים

מכרז מסגרת הוא מכרז פומבי שבו נבחר יותר מספק אחד, אשר על פי תנאי המכרז ייכרתו בעקבותיו הסכמי מסגרת עם כל ספק שנבחר במכרז המסגרת. זהות הספק ממנו תבוצע בפועל כל הזמנה של טובין, עבודה או שירותים תיקבע מפעם לפעם במהלך תקופת הסכם המסגרת, לפי תנאי מכרז המסגרת.

במכרז מרכזי בתחום התקשוב ב' - תיחור מס' 10 נכתב כי בתיחור זה יבחר זוכה יחיד. עוד נכתב כי המציע שדורג ראשון בתיחור ייבחר כזוכה אשר יהיה ראשי לספק את כל קו המוצרים והשירותים הכלולים בתיחור זה.

במכרזים מרכזיים בתחום התקשוב והסייבר שבהם יש ספק אחד שזוכה במכרז, יש סיכון כי פגיעה באותו ספק תחשוף משרדים רבים לאותה פגיעות ובכך הסיכון יהיה רב יותר ואף עלול לסכן את מרבית משרדי הממשלה מבלי שיהיה לכל המשרדים תחליף (one point of failure).

במכרז בתחום התקשוב - א' זכו שני ספקים, ובמסגרת ההתקשרות נקבעה רשימה של משרדים ויחידות סמך שתעבוד עם כל ספק, וכך הופחת הסיכון.

מומלץ כי מינהל הרכש יקדם ביצוע מכרז מרכזי מסוג מכרז מסגרת בתחום מוצרי האבטחה, באופן שתתאפשר זכייה של כמה ספקים שונים, בהתאם לשיקול דעת ועדת המכרזים ומסמכי המכרז, כך שלא כל משרדי הממשלה ירכשו את אותו המוצר ויהיו חשופים לאותם הסיכונים שהספק חשוף אליהם, אם הוא אכן חשוף לסיכונים. עוד מומלץ כי במידה ונבחר זוכה יחיד יש להקפיד יותר על הרחבת הבקרות בתחום הגנת הסייבר בתנאי ההתקשרות ועל ביצוע ביקורות במהלך תקופת ההתקשרות כדי לוודא שהספק עומד בדרישות אלו.

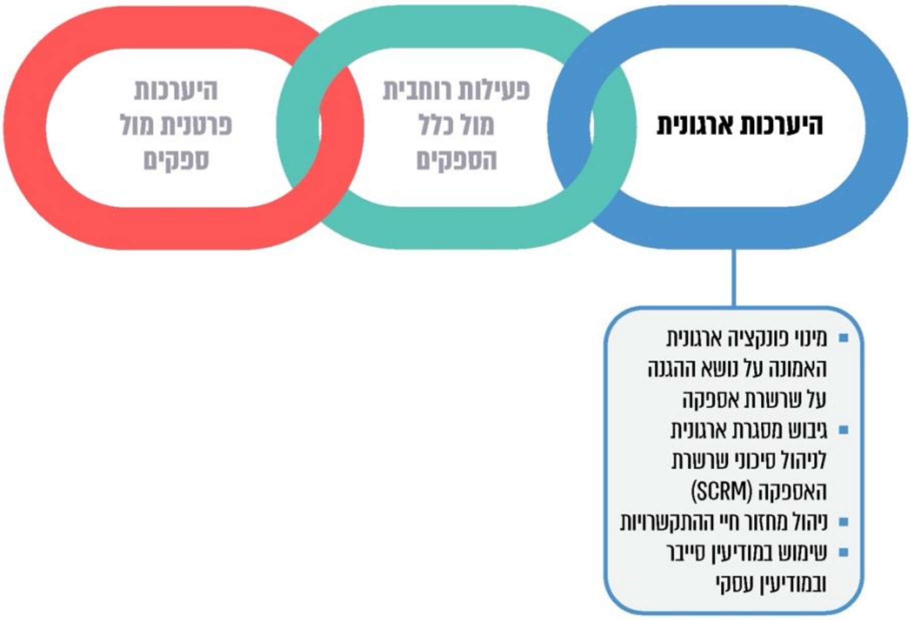
בתשובת מינהל הרכש מיוני 2023 נמסר כי בתחומים שבהם קיים יתרון ברור לבחירה של כמה זוכים, מינהל הרכש מעצב את הליכי הרכש כך שייבחרו כמה ספקים רלוונטיים כמו בתיחורים 1 ו-2 של מכרז בתחום התקשוב - ב'. כמו כן, במסגרת פרויקט נימבוס, מינהל הרכש הטמיע מתודולוגיית רכש שבאופן מכוון מיועדת להכנסת ספקים רבים לממשלה. יתרה מכך, במקרים מסוימים היו אלה דווקא הגופים המנחים שהתעקשו על בחירה של מוצר יחיד כדי לייצר אחידות, להקל על בקרה והטמעה ולהימנע מהכנסת מוצרים שהם רואים כלא איכותיים.

אשר לתגובת מינהל הרכש, יצוין כי במכרזים מרכזיים בתחום אבטחת המידע והגנת הסייבר יש יתרון לשילוב כמה ספקים בכל מכרז שייתנו פתרונות הגנה שונים, לכן מומלץ כי מינהל הרכש יבחן יחד עם מערך הסייבר ויה"ב שילוב של אפשרות כזו כשהדבר מתאפשר ובהתאם לכך תינתן לגופים הנחיה לעבוד עם כמה ספקים.

שלב א' במתודולוגיית שרשרת האספקה - היערכות ארגונית

כאמור המתודולוגיה של מערך הסייבר כוללת שלושה שלבים: היערכות ארגונית, פעילות רוחבית מול הספקים והיערכות פרטנית מול ספקים. להלן נפרט על הפערים שעלו בשלב א':

תרשים 11: **הפעילויות הכלולות בשלב ההיערכות הארגונית**



המקור: מערך הסייבר.

ייעודה העיקרי של תורת ההגנה הוא הגנה מפני האיומים הרלוונטיים, והעקרון המונח ביסודה הוא כי רציפות התפקוד של הארגון וההגנה על נכסיהם ויעדיהם מפני האיומים הרלוונטיים נדרשת להתבסס על הבנת איום הייחוס, המודיעין והמגמות המשתנות בתחום הרלוונטי.

ההבנה של איום הייחוס מצד שרשרת האספקה משמש בסיס להיערכות הארגונית להפחתת האיום. לפי הגדרת אגף הביטחון במערך הסייבר כל איום לתקיפת שרשרת האספקה לשם חשיפה או סיכול של פעילות המערך הוא איום ייחוס על הארגון. המערך הכין רשימה של תרחישים לאיום ייחוס וכן סדרת מענים על כל תרחיש בהתאם לרמת האיום.

לוח 8: **התייחסות הארגונים לתקיפת שרשרת האספקה כאיום ייחוס**

השאלה	שיעור הארגונים
האם אירוע סייבר באמצעות תקיפת שרשרת האספקה הוא איום ייחוס של הארגון?	**86% מהארגונים הגדירו שתקיפת סייבר באמצעות שרשרת האספקה היא איום ייחוס של הארגון**

מהמענה לשאלון עולה כי 37 (86%) מתוך 43 מהמשרדים ומגופי התמ"ק שהשיבו על השאלה הגדירו כי אירוע סייבר באמצעות תקיפת שרשרת האספקה הוא איום ייחוס של הארגון.

לפי המתודולוגיה שלב ההיערכות הארגונית כולל את הפעילויות האלה:

1. **מינוי פונקציה ארגונית האמונה על נושא ההגנה על שרשרת האספקה:** תפקיד המחייב הבנה מקצועית מתאימה בתחום ניהול הסיכונים, הגנת המידע והסייבר, המכרזים וההתקשרויות.

2. **גיבוש מסגרת ארגונית לניהול סיכוני שרשרת האספקה:** מדובר במסגרת ארגונית שתעסוק, בין היתר בהכנת נוהל עבודה ובתיקופו מדי שנה, בבקרות מפצות[42] במסגרת התקשרויות שבהן לא ניתן להעניק את רמת ההגנה הנדרשת על פעילותו של הספק, בכלי ניהול הבקרה על התהליך, בהקצאת המשאבים הנדרשים לשם ביצוע ביקורות על הספקים, בשילוב ממונה הביטחון אם יתבצעו מכרזים והתקשרויות שאין לחשוף אותם ברבים או כאשר הספק ייחשף במסגרת פעילותו למידע מסווג.

3. **ניהול מחזור החיים של ההתקשרויות:** הגדרת היבטי הגנת המידע והסייבר החוזיים מול הספק, עירוב ממונה הגנת מידע וסייבר בתהליכי הוספת הספק במערכת, חידוש התקשרות קיימת עם הספק וסיום ההתקשרות עם הספק.

4. **שימוש במודיעין סייבר ובמודיעין עסקי:** בחינת המודיעין הקיים על הספק בנוגע לסיכוני אבטחת המידע שלו, לפני ההתקשרות ובמהלכה.

מינוי פונקציה ארגונית וגיבוש מסגרת ארגונית

בתורת ההגנה 2.0 של מערך הסייבר וכן במדיניות להגנת הסייבר בממשלה של יה"ב[43] הוגדרו המסגרות הארגוניות אשר יישמו את מדיניות הגנת הסייבר במשרד ויבקרו את אופן יישומה, ובכלל זה את אופן הטיפול בסיכונים הנשקפים מצד שרשרת האספקה. להלן יפורטו המסגרות הארגוניות האמורות:

1. **ועדת היגוי לנושאי הגנת סייבר:** מסגרת אירגונית ניהולית לקבלת החלטות אסטרטגיות בתחום הגנת הסייבר ולביצוע בקרה ניהולית על יישום הגנת הסייבר במשרד.

2. **ממונה הגנת הסייבר:** אחראי להבטיח כי התכנון והניהול של מכלול היבטי הגנת הסייבר במשרד, הטיפול במכלול היבטים אלה והבקרה בנושא יתבצעו כנדרש.

---

42 פעולות להפחתת הסיכון כאשר לא ניתן למנוע את הסיכון.

43 יה"ב, **הנחיה 5.1 בנושא מדיניות להגנת הסייבר בממשלה**, סעיף 4.2.1

3. **ממונה שרשרת אספקה:** במתודולוגיית שרשרת האספקה[44] וכן בהנחיית יה"ב 5.19[45] נקבע כי על הארגון למנות פונקצייה ארגונית האמונה על נושא ההגנה על שרשרת אספקה.

לפי מתודולוגיית שרשרת האספקה[46], על הארגון להיות ערוך לתפעל אירוע אבטחת מידע מהבחינה החוזית, התהליכית והטכנולוגית. כמו כן, לפי המתודולוגיה[47] יש לפעול לכך שהארגון יוכל לנתק באופן מיידי את הקישור מהספק כאשר מזוהה אירוע חריג. דוגמה לצורך בניתוק מספק עלה בפגישה שקיים צוות הביקורת עם גוף 35 בינואר 2023: בשנת 2022 גילה הגוף כי בוצעה מתקפת DDOS על קווי תקשורת של גוף 47 ומיד התנתק מהספק ועבר לעבוד באמצעות ספק אחר.

במכרז א' - התווספה הדרישה שהמזמין יתרגל בסיוע הספק תרחיש של נפילת מערכות באתר המזמין, על כל המשתמע מכך, לרבות הקצאת עמדות עבודה למשתמשים ועמדות תמיכה והעברת נתונים מהשרתים הנמצאים באתר הספק לאתרי קצה של המזמין. הספק ייטול חלק בתרגיל ויעמיד לרשות המזמין את צוות האתר והטכנאים המטפלים במתחם מזמין. המכרז קובע כי תרגיל מהסוג האמור יתבצע פעמיים בשנה וכל תרגול יתבצע במסגרת זמן של יומיים.

משרד מבקר המדינה מציין לחיוב את גוף 20, את גוף 44, את גוף 35 (ברשת המסווגת), את גוף 46 ואת גוף 47 על שהשקיעו משאבים ייעודיים בניהול סיכונים הנוגעים לשרשרת האספקה מעבר לנדרש לפי מתודולוגיית שרשרת האספקה: לדוגמה, גוף 20 הקים בשנת 2021 מינהלה בראשות סמנכ"ל החברה, מינהלת סיכונים ואחראי רכש וטובין, אשר אחראית לאבטחת המידע בנוגע לשרשרת האספקה. כמה ארגונים, ובהם גוף 44 וגוף 47, הכשירו את ממונה שרשרת האספקה לתפקיד בודק ספקים. גוף 47 שהוא ספק תשתיות של משרדי הממשלה הותעד כספק מהותי. אגף הביטחון במערך הסייבר מקיים קורסים לממוני ביטחון בגופי תמ"ק ולקב"טים של משרדי ממשלה שבהם מוצגת להם המתודולוגיה הביטחונית הייעודית של המערך בנושא שרשרת אספקה. גוף 46 של גוף 15 גייס לאחרונה ראש תחום שרשרת אספקה שתפקידו ללוות את הספקים שהוגדרו כמהותיים למגזר הפיננסי כדי לשפר ולבסס את חוסנה של שרשרת האספקה הפיננסית.

---

44 מערך הסייבר, **הרחבה מקצועית בנושא שרשרת אספקה - דגשים עבור צד לקוח**, סעיף 7.1

45 יה"ב, **הנחיה 5.19**, סעיף 7.1.

46 הרחבה מקצועית בנושא שרשרת אספקה- דגשים עבור צד הלקוח, סעיף 9.3.2.4

47 שם, סעיף 9.3.2.7.

לוח 9: **פעילות הארגונים לניהול הסיכון מצד שרשרת האספקה**

השאלה	שיעור הארגונים
האם הארגון ערך בשנתיים האחרונות (2021 - 2022) סקר סיכונים העוסק במפורש בסיכון של שרשרת אספקה?	**65% מהארגונים לא ביצעו סקר סיכונים שכלל התייחסות לנושא שרשרת האספקה**
האם בשנתיים האחרונות (2021 - 2022) נדון נושא שרשרת האספקה בוועדת ההיגוי בנושא הסייבר בארגון?	**39% מהארגונים לא דנו בנושא שרשרת האספקה בוועדת ההיגוי**
האם מונה בעל תפקיד ייעודי לנושא שרשרת אספקה?	**59% מהארגונים לא מינו בעל תפקיד ייעודי לנושא שרשרת האספקה**
האם כשהארגון מבצע תרגולים של המשכיות עסקית או של התמודדות עם אירוע סייבר נכללים גם תרחישים של תקיפת סייבר באמצעות שרשרת האספקה?	**60% מהארגונים אינם מבצעים תרגולים לתקיפת סייבר באמצעות שרשרת האספקה**

נמצא כי 86% מהמשרדים וגופי התמ"ק שהשיבו על השאלה הגדירו כי אירוע סייבר באמצעות תקיפת שרשרת האספקה הוא איום ייחוס של הארגון, למרות זאת הם לא פעלו באופן מספק כדי לנהל ולהפחית סיכונים אלו:

1. 28 (65%) מתוך 43 מהמשרדים וגופי התמ"ק שהשיבו על השאלה לא ביצעו בשנתיים האחרונות (2021 - 2022) סקר סיכונים העוסק במפורש בסיכון של שרשרת אספקה.

2. 17 (39%) מתוך 44 המשרדים וגופי התמ"ק שהשיבו על השאלה לא דנו בוועדת היגוי בתחום הסייבר על נושא שרשרת האספקה בשנתיים האחרונות (2021 - 2022).

בתשובת גוף 32 מיוני 2023 נמסר כי נושא שרשרת האספקה אכן עלה בדיון בוועדת ההיגוי האחרונה בהקשר של ניהול המידע ומאגרי מידע שנמצא ומנוהל אצל מפעילי מסגרות ונותני שירותים בתחום העיסוק של הגוף. הנושא של בדיקת שרשרת האספקה אצל ספקים המספקים שירותי מחשוב למשרד לא עלה בוועדת ההיגוי משום שאין להם גישה לרשת המשרדית.

אשר לתשובת גוף 32, יצוין כי גם אם אין ספקים עם גישה לרשת המשרדית עדיין יש לדון בספקים שנותנים לגוף שירות ומציבים לפניו סיכון, למשל כאלו שמספקים תוכנה לגוף.

3. 26 (59%) מתוך 44 המשרדים וגופי התמ"ק שהשיבו על השאלה לא מינו בעל תפקיד ייעודי לנושא שרשרת אספקה שיהיה אחראי על ניהול הסיכונים מצד שרשרת האספקה כנדרש במתודולוגיה של שרשרת האספקה ובהנחיה 5.19 של יה"ב. עקב כך בארגונים אלו אין פונקציה ארגונית מוסדרת שתוודא כי הסיכונים מצד שרשרת האספקה בארגון מנוהלים ומטופלים כראוי.

מומלץ כי המשרדים וגופי התמ"ק שלא דנו בוועדות ההיגוי בתחום הסייבר על נושא שרשרת האספקה יקיימו דיון על ניהול הסיכונים מצד שרשרת האספקה. עוד מומלץ כי משרדים וגופי תמ"ק שלא מינו בעל תפקיד ייעודי האחראי לאבטחת שרשרת האספקה ימנו בעל תפקיד ויכשירו אותו לתפקיד, למשל באמצעות קורס בודק ספקים שגובש על ידי מערך הסייבר.

בתשובות גוף 7, גוף 30, גוף 10 וגוף 40 מיוני 2023 נמסר כי סקר סיכונים העוסק במפורש בסיכון שרשרת אספקה מתוכנן לביצוע בשנת 2023.

בתשובות גוף 3, גוף 18, גוף 7, גוף 23, גוף 39 וגוף 40 מיוני 2023 נמסר כי ימונה בעל תפקיד ייעודי לנושא שרשרת האספקה אשר יוכשר לתפקיד.

בתשובות גוף 43, גוף 24, גוף 7, גוף 30, גוף 23 וגוף 40 מיוני 2023 נמסר כי נושא שרשרת האספקה יועלה בוועדות ההיגוי הבאות.

בתשובת גוף 35 מיולי 2023 נמסר כי בסוף החודש צפויה להתכנס ועדת היגוי אבטחת מידע לצורך אסדרת תחומי האחריות בנושא שרשרת האספקה בין אגף טכנולוגיות מידע לבין אגף ביטחון וחירום.

עוד נמצא כי 26 (60%) מתוך 43 המשרדים וגופי התמ"ק שהשיבו על השאלה אינם מבצעים תרגול של תרחישי תקיפת סייבר באמצעות שרשרת האספקה כמו בחינת הרציפות התפקודית בתרחיש של פגיעה בספק מהותי כמתחייב במתודולוגיית שרשרת האספקה. עקב כך נשקף סיכון כי משרדים וגופי תמ"ק רבים לא ידעו כיצד להתמודד בזמן אמת עם מתקפות סייבר על שרשרת האספקה אשר עלולות לפגוע ברציפות התפקודית שלהם.

מומלץ כי משרדים וגופי תמ"ק שאינם מבצעים תרגולים של תרחישי מתקפות על שרשרת האספקה יתרגלו תרחישים כמו פגיעה בספק מהותי במסגרת תרגולי הסייבר וימפו את התהליכים העסקיים שכל ספק משפיע עליהם.

בתשובות גוף 22, גוף 14, גוף 7 וגוף 8 מיוני 2023 נמסר כי הגופים יפעלו בשנת 2023 לביצוע תרגול אשר יכלול תרחישי מתקפות על שרשרת האספקה.

עוד מומלץ כי מערך הסייבר בשיתוף יה"ב יגבש מתווה לתרגיל תקיפה באמצעות שרשרת האספקה עבור כלל המשרדים וגופי התמ"ק, וינחה אותם כיצד לתרגל את התרחישים השונים של מתקפות סייבר על שרשרת האספקה ויבצע מעקב אחר ביצוע תרגילים באופן עיתי.

ניהול מחזור חיי ההתקשרות

שלב זה כולל את הפעילויות האלה: צירוף נספח אבטחת מידע במכרזים בנושא תקשוב וסייבר, עירוב ממונה הגנת מידע וסייבר בתהליכי הרכש, חידוש התקשרות קיימת עם הספק וסיום ההתקשרות עם הספק.

נספח אבטחת מידע במכרזים משרדיים

לפי תקנה 15(א)(1) לתקנות אבטחת מידע, על בעל מאגר מידע לבחון לפני ביצוע התקשרות עם הספק, הכרוכה במתן גישה למאגר מידע, את סיכוני אבטחת המידע הכרוכים בהתקשרות. כמו כן, לפי תקנה 15(א)(2) על בעל מאגר המידע לקבוע במפורש בהסכם עם הספק, בשים לב לסיכונים שהוגדרו, התניות כמו המידע שהספק רשאי לעבד ומטרות השימוש המותרות בו לצורכי ההתקשרות, מערכות המאגר שהגורם החיצוני רשאי לגשת אליהן, סוג העיבוד או הפעולה שהגורם החיצוני רשאי לעשות וכן חובתו של הגורם החיצוני להחתים את בעלי ההרשאות שלו על התחייבות לשמור על סודיות המידע, להשתמש במידע רק לפי האמור בהסכם וליישם את אמצעי האבטחה הקבועים בהסכם.

לפי ההנחיה שבמתודולוגיית שרשרת האספקה[48] יש להגדיר את היבטי הגנת המידע והסייבר החוזיים מול הספק, כמו הסמכות לבצע ביקורות סייבר בחצרות הספק, החלת דרישות הגנת מידע וסייבר על ספקי המשנה, חובת הספק לעדכן מייד את הארגון על התרחשותו של אירוע סייבר אשר עשוי להשפיע על הארגון או על לקוחותיו. לפי ההמלצה שבמתודולוגיה יש לוודא כי בכל הסכם התקשרות ובכל מכרז של הארגון ייכלל סעיף אשר מגדיר את דרישות הגנת המידע והסייבר במסגרת ההתקשרות.

הנחיית יה"ב 5.19 בנושא שרשרת האספקה מיועדת לקהל היעד הבא במשרדים: ממוני הגנת הסייבר, מנהלי מערכות מידע ומנהלי אבטחת מידע. ההנחיה מחייבת את המשרדים לצרף לכל

48 מערך הסייבר, **הרחבה מקצועית בנושא שרשרת אספקה צד לקוח**, סעיף 7.3.3.

מכרז ממשלתי נספח אבטחת מידע[49], ומצורף לה גם נספח לדוגמה[50]. נספח אבטחת מידע הוא מסמך המפרט את אחריות הספק בנושאים שונים הנוגעים לאבטחת מידע במסגרת ההתקשרות. במכרזים טכנולוגיים ובמכרזים הקשורים לאספקת שירותים הנוגעים לנכסי מידע של הארגון נספח זה הוא חיוני היות שבהיעדרו ייתכן שהמוצר או השירות לא יאובטחו במידה מספקת.

בהוראת תכ"ם 7.3.1[51] המיועדת לבעלי תפקידים בתחום הרכש הוגדר אילו מסמכים חייבים המשרדים לכלול בכל הליך של מכרז המתבצע בממשלה. לפי ההוראה, משרד רשאי להוסיף דרישה להוספת מסמכים נוספים. נכון למועד סיום הביקורת במאי 2023 בהוראת תכ"ם 7.3.1 אין חובה לצרף לכל מכרז ממשלתי נספח אבטחת מידע.

כאמור, בנובמבר 2022 פרסם מינהל הרכש את טיוטת נספח ז' להוראת התכ"ם 7.3.1, העוסקת באחריותם של ספקי הממשלה בתחום אבטחת המידע והסייבר, שתצורף כנספח למכרזים. טיוטת נספח ז' עוסקת, ביו היתר, בנושאים האלו:

1. **ניתוח הסיכונים הכרוכים בהתקשרות:** הוגדר כי לצורך קביעת דרישות בנושא הגנת מידע ואבטחת סייבר על המזמין לבצע ניתוח של סיכונים הנוגעים למהות ולכמות של המידע על המשרד המועבר אל הספק, למידע הנוצר אצל הספק במסגרת ההתקשרות או למידע שהוא נחשף אליו, וכן הגנות סייבר הנדרשות למערכות המופעלות על ידי הספק הרלוונטיות לאותה התקשרות. לצורך כך יש לפעול עם הגורמים הרלוונטיים במשרד בהתאם להנחיות הרלוונטיות כגון הוראה 5.19 של יה"ב בנושא שרשרת האספקה.

2. **סיווג רגישות ההתקשרות והוספת נספח אבטחת מידע שמתאים לסיווג שנבחר:** הוגדר כי כל מזמין נדרש לסווג את מידת רגישותה של ההתקשרות עם הספק כנמוכה, רגילה, גבוהה או גבוהה מאוד בהתאם לקריטריונים שצוינו בנספח, ובהם ההיקף הכספי של ההתקשרות, האם ההתקשרות היא עם ספק המקושר למערכות המידע של המזמין או למערכות אחרות המחזיקות מידע ממשלתי רגיש. בהתאם למידת רגישות ההתקשרות שאותה סיווג המזמין, עליו לצרף למסמכי המכרז אחד משלושה נספחי אבטחת מידע שפרסם מינהל הרכש (השונה מהנספח לדוגמה שפרסמה יה"ב). נוסף על נספח אבטחת המידע של מינהל הרכש, רשאי המזמין להוסיף דרישות ייעודיות בנושא אבטחת מידע הרלוונטיות למשרד שלו.

בדצמבר 2022 העביר מינהל הרכש למערך הסייבר, ליה"ב ולמשרדי הממשלה את הטיוטה של הוראת תכ"ם 7.3.1 ואת נספחי אבטחת המידע הנלווים אליה, לקבלת התייחסותם בנושא. בהתייחסות של מערך הסייבר ביקש המערך ממינהל הרכש לתקן את הסעיף בהוראת התכ"ם שמפנה להנחיית יה"ב 5.19 ובמקומה לחייב את המשרדים לעבוד לפי המתודולוגיה עצמה, זאת לטובת ארגונים שאינם כפופים ליה"ב ולטובת יצירת בהירות ואחידות מול הספקים שאינם חשופים להנחיות יה"ב. בתגובה לבקשת מערך הסייבר, מינהל הרכש עדכן את טיוטת נספח ז' והוסיף בהערת שוליים הפנייה למתודולוגיה של שרשרת האספקה, ראו תרשים להלן:

---

49 יה"ב, **הנחיה 5.19 - שרשרת האספקה**, גרסה 1.1 מ-3.11.19 (עודכנה ב-11.1.21), סעיף 7.1.

50 "נספח אבטחת מידע לצורך התקשרות עם ספק חיצוני", הדוגמה מצורפת להנחיה 5.19.

51 הוראת תכ"ם 7.3.1: "מסמכי מכרז", סעיף 1.3.1.

תמונה 1: **הערת שוליים בטיוטת נספח ז'**

[1] הנחיית יה"ב 5.19, מתייחסת באופן ישיר למתודת שרשרת האספקה של מערך הסייבר הלאומי, ניתן למצוא בקישור הבא את שאלון הבקרות העדכני בנוסף למסמכי הסבר נוספים.

דוגמה נוספת לדרישה של גוף אסדרתי בתחום הסייבר שאינה כלולה בטיוטת נספח ז' היא ההנחיה למשרדים לחייב את הספקים שלהם לעמוד בתקן ISO-27001 בהתאם להנחיה 5.19 ולהחלטת ממשלה 2443.

לוח 10: **יישום ההנחיות בעניין נספח אבטחת מידע במכרזים**

השאלה	שיעור הארגונים
האם המכרזים של הארגון בתחום התקשוב והסייבר כוללים נספח אבטחת מידע?	**14% מהארגונים לא כללו במכרזים נספח אבטחת מידע**
האם במכרזים של הארגון יש סעיף שמחייב עבודה לפי המתודולוגיה של מערך הסייבר בנושא שרשרת האספקה?	**67% מהארגונים לא כללו במכרזים סעיף שמחייב עבודה לפי המתודולוגיה של מערך הסייבר**

נמצא כי במסמכים של מכרזי התקשוב והסייבר של 6 (14%) מתוך 44 המשרדים וגופי התמ"ק שהשיבו על השאלה אין נספח אבטחת מידע כנדרש בהנחיית יה"ב 5.19. נוכח זאת יש משרדים וגופי תמ"ק שלא הגדירו עבור הספקים שלהם דרישות בנושא הגנת הסייבר ואבטחת המידע ואין ביכולתם להחיל על הספק דרישות בנושא זה, לפקח על רמת ההגנה הקיימת ולבקש שינקוט צעדים לצורך שיפור המצב.

עוד נמצא כי במכרזים של 29 (67%) מתוך 43 המשרדים וגופי התמ"ק שהשיבו על השאלה אין סעיף שמחייב עבודה לפי המתודולוגיה של מערך הסייבר בנושא שרשרת האספקה.

מומלץ כי המשרדים וגופי התמ"ק שהמכרזים שלהם לא כוללים נספח אבטחת מידע יפעלו כדי להוסיף נספח כזה בכל מכרז. עוד מומלץ כי מערך הסייבר ויה"ב, כגופים אסדרתיים בתחום הסייבר, בשיתוף מינהל הרכש, ינקטו פעולות שיבטיחו כי בכל מכרז הנוגע לתקשוב וסייבר או הכולל העברת מידע רגיש של ארגון לספק נכלל נספח אבטחת מידע, וכי נספח זה יחייב עבודה לפי מתודולוגיית שרשרת האספקה של מערך הסייבר.

בתשובת גוף 38, גוף 40, גוף 5 וגוף 35 מיוני 2023 נמסר כי נספח אבטחת מידע יצורף למכרזים של הגופים בתחום התקשוב והסייבר.

בתשובת גוף 38 וגוף 9 נמסר כי ההמלצה להוסיף למכרזים סעיף שמחייב עבודה לפי המתודולוגיה של מערך הסייבר מקובלת ותיושם החל מהמכרזים הבאים.

בתשובת גוף 22 מיוני 2023 נמסר כי לנוכח אי-התאמת מתודולוגיית מערך הסייבר בנושא שרשרת אספקה לצרכים העסקיים של הגוף, לא ניתן כרגע לחייב עבודה על פי המתודולוגיה עד ביצוע חשיבה משותפת להתאמתה כנדרש.

בתשובת גוף 35 מיולי 2023 נמסר כי הנושא אמור להיות בטיפול רוחבי במינהל הרכש וביה"ב.

הן בטיוטת נספח ז' של הוראת התכ"ם 7.3.1 שפרסם מינהל הרכש, והן בהנחיה 5.19 שפרסמה יה"ב נכללה הנחיה למשרדים להוסיף במכרז ההתקשרות שלהם עם הספק נספח אבטחת מידע. נמצא כי שתי ההנחיות הללו אינן עולות בקנה אחד, וכל הנחיה מפנה לנספח ובו סעיפים בנושאים שונים. עקב כך המשרדים יתקשו לדעת איזה נספח עליהם לצרף למכרזים שלהם. הקושי הנובע מקיומם של הנחיות ונספחים שונים מקבל משנה תוקף נוכח העובדה שההנחיות מיועדות לקהלי יעד שונים (הוראת תכ"ם - לבעלי תפקידים ברכש והנחיית יה"ב - לממוני הגנת הסייבר), ובחלק מהארגונים ממוני הגנת הסייבר אינם מעורבים בתהליכי הרכש.

מומלץ כי מינהל הרכש יגבש עם הגופים האסדרתיים בתחום אבטחת המידע והסייבר (שב"כ, מלמ"ב, מערך הסייבר, יה"ב והרשות להגנת הפרטיות) נספח אבטחת מידע שיצורף לכל מסמך התקשרות או שינחה שכל ארגון יצרף נספח אבטחת מידע בהתאם להנחיות הגוף האסדרתי שמנחה אותו בתחום אבטחת מידע והגנת הסייבר. באופן זה תהיה הלימה בין הדרישות של הגוף האסדרתי מהארגון (כמו עמידה בתקנה 15 לתקנות אבטחת מידע, במתודולוגיית שרשרת האספקה ובתקן ISO27001) ובין הדרישות בהוראת תכ"ם המחייבות גם הן את המשרדים.

בתשובת מינהל הרכש מיוני 2023 נמסר כי מגובש כעת נספח אבטחת שרשרת אספקה עם הגופים האסדרתיים, אך עדיין מדובר במדיניות בגיבוש. עוד נמסר כי מינהל הרכש לא היה מעורב בגיבוש נספח אבטחת מידע הכלול בהנחיית יה"ב.

בתשובת יה"ב מיולי 2023 נמסר כי נספח אבטחת מידע לדוגמה שקיים כחלק מהנחיית יה"ב 5.19 נותן מענה על מרבית הנושאים הרלוונטיים הנוגעים להתקשרות עם ספק. הן מינהל הרכש והן המשרדים יכולים להיעזר במסמך זה בכתיבת נספח אבטחת מידע למכרזים או התקשרויות משרדיות המותאם לצרכים הספציפיים של מכרז מסוים. עוד נמסר כי טיוטת הוראת תכ"ם טרם יצאה כהוראה בתוקף ויש לוודא כי אין סתירה בינה לבין הנספח לדוגמה שגיבשה יה"ב.

בתשובת מערך הסייבר מיולי 2023 נמסר כי ככלל דרישות אבטחת מידע וסייבר במכרזים המרכזיים צריכות להיות בהתאם להנחיות הגופים האסדרתיים בתחום הסייבר (למשל: עמידה במתודולוגיית שרשרת האספקה). במקרים שבהם מסתמן קושי ליישם דרישות אלו כהווייתן או שיש חלופה טובה יותר (למשל: תקינה בין-לאומית ייעודית לנושא) יש לפנות לגופים האסדרתיים ולבקש את הסכמתם ליישום דרישות חלופיות.

אשר לתשובות הגופים האסדרתיים, מומלץ כי גופים אלו יגבשו במשותף עם מינהל הרכש נספח אבטחת מידע שיהיה מקובל על כלל הגופים, היות שהוא יחייב את המשרדים ואת גופי התמ"ק וכן תהיה לו השפעה ישירה על הרכש הממשלתי. יצוין כי טיוטת נספח ז', כפי שקיימת במועד כתיבת דוח הביקורת, לא יכולה לשמש נספח אבטחת מידע היות שחסרות בה דרישות אבטחת מידע שקיימות בנספחים אחרים שגיבשו הגופים האסדרתיים.

דרישות הגנת סייבר בהתקשרויות הפטורות ממכרז

בתקנות חובת המכרזים מפורטות העילות לביצוע התקשרות בפטור ממכרז. נכון לפברואר 2023 צוינו בתקנות כ-25 עילות אפשריות לביצוע התקשרויות בפטור ממכרז, והנפוצות שבהן הן: התקשרות עם ספק יחיד[52], התקשרות ששוויה אינו עולה על 50,000 ש"ח והתקשרות המשך[53].

מדוח של משרד מבקר המדינה משנת 2023[54] עלה כי היקף הרכש הממשלתי התקשובי הפטור ממכרז בשנים 2021-2019 היה בין 497 מיליון ש"ח ל-691 מיליון ש"ח, ושיעורו הממוצע היה כ-14.2% מסך הרכש בתחום התקשוב.

נמצא כי מינהל הרכש מנגיש למשרדים מערכת ממוחשבת שבאמצעותה הם יכולים לבצע גם רכישות בתחום התקשוב והסייבר בהיקף כספי של עד 50,000 ש"ח, וכל התהליך מבוצע על ידי הגורם המשרדי שמבקש לרכוש את המוצר או השירות ואינו מועבר לטיפולם של גורמים כמו ממונה הגנת הסייבר או ממונה שרשרת האספקה באותו המשרד כדי שיבחנו אם ההתקשרות לאספקת השירות או המוצר המוצע נותנת מענה הולם מבחינת היבטי אבטחת מידע.

בתשובת מינהל הרכש מיוני 2023 נמסר כי לא קיימת כלל חובה ולפיה בהתקשרויות בהליך מקוצר יש לפנות לאותם גורמים שנדרשים במכרז, ואם תתקיים חובה שכזו, הדבר יביא לעיכוב בהליך רכש זה אשר קיימת חשיבות רבה שהוא יהיה כשמו - מקוצר. אם הגורם הרוכש רוצה להתייעץ עם ממונה הסייבר אין מניעה לכך.

מומלץ כי בהתקשרויות בתחום תקשוב וסייבר תיכלל במערכת הממוחשבת הודעה שמנחה את הגורם הרוכש להביא לידיעת ממונה הגנת הסייבר המשרדי את מהות ההתקשרות וזהות הספק, ואם הוא ימצא לנכון לבחון את ההתקשרות או להעיר בעניינה הוא יעשה כן בלי לעכב את השלמת הליך ההתקשרות.

52 התקשרות עם ספק שבהתאם לזכויות מכוח הדין או בהתאם למצב הדברים בפועל הוא היחיד המסוגל לעמוד בתנאי ההתקשרות.

53 התקשרות המתבצעת לצורך הרחבה או הארכת התקופה של התקשרות ראשונה, שלא מכוח זכות ברירה הכלולה בהתקשרות הראשונה.

54 מבקר המדינה, **דוח שנתי 73ג** (2023): "התקשרויות בפטור ממכרז בתחום התקשוב".

עוד נמצא כי בכל הנוגע להתקשרויות הפטורות ממכרז, אין הוראות תכ"ם המחייבת להתייחס לנושאי אבטחת מידע והגנת הסייבר בכלל, ולנושא שרשרת האספקה והגנת הסייבר של הספקים בפרט, זאת אף שמדובר בכ-14.2% מסך הרכש בתחום התקשוב. יצוין כי רבות מההתקשרויות האלו מתבצעות עם ספקים קטנים, אשר מטבע הדברים רמת האבטחה שלהן בתחום הסייבר נמוכה יותר, ולכן הם פגיעים יותר למתקפות על שרשרת האספקה ונשקף למשרדים סיכון גדול יותר בגינם.

בתשובת מערך הדיגיטל הלאומי מיולי 2023 נמסר כי גם אם ההתקשרות עם ספקים היא בהיקף קטן נדרשת התייחסות להיבטי אבטחת המידע והסייבר, וכי יש צורך בפיתוח סולם הערכת סיכון שמאפשר לסמן סוגי פעילויות שבהן האיום על שרשרת האספקה הוא מהותי ולבצע בדיקה של פעילויות אלה ומעקב של הספק בעניינן.

מומלץ כי אגף החשכ"ל במשרד האוצר יפרסם הוראת תכ"ם המחייבת להתייחס לנושאי אבטחת מידע והגנת הסייבר בהתקשרויות הפטורות ממכרז שהן בסיכון גבוה למתקפות על שרשרת האספקה. עוד מומלץ כי אגף החשכ"ל יגדיר יחד עם מערך הסייבר ויה"ב על אילו התקשרויות יש לבצע מעקב אחר יישום דרישות אבטחת המידע והסייבר.

בתשובת מינהל הרכש מיוני 2023 נמסר כי בהמשך לגיבוש המדיניות במסגרת העבודה על עדכון הוראת תכ"ם 7.3.1 היא תורחב גם להתקשרויות בפטור ממכרז.

שיתוף גורמי הגנת הסייבר של הארגון בתהליכי הרכש

לפי מתודולוגיית שרשרת האספקה, לפני יציאה למכרז או התקשרות חדשה או חידוש התקשרות קיימת יש להביא זאת לידיעת ממונה הגנת מידע וסייבר[55]. כמו כן, לפי המתודולוגיה מדיניות הערכת סיכונים בשרשרת האספקה צריכה לכלול התייחסות לתהליכים כמו שילוב ממונה הביטחון במקרה של מכרזים והתקשרויות שאין לחשוף אותם לנחלת הכלל או במקרה שבו הספק ייחשף במסגרת פעילותו למידע מסווג[56].

ממונה הגנת הסייבר או ממונה שרשרת אספקה אמון על הגנת הסייבר של הארגון ועל הגנת המידע שלו מפני האיומים הנשקפים לשרשרת האספקה של הארגון. שילוב גורמים אלו באופן סדור בתהליכי הרכש של הארגון בתחום התקשוב והסייבר מאפשר לבחון אם במסגרת ההתקשרות נכללות דרישות אבטחת מידע מספקות הנותנות מענה הולם על הסיכונים הנשקפים לארגון; וכמו כן שילובם מאפשר לבצע בדיקת חוסן של הספק; לוודא כי המידע הנכלל בהתקשרות ומיועד להתפרסם לציבור אינו רגיש וכי חשיפתו אינה עשויה לפגוע בארגון, ואם יש צורך בכך הוא פועל להתמים[57] את המידע הרגיש.

לפי הוראת תכ"ם 7.1.1[58], ועדת המכרזים המשרדית היא ההרכב שאחראי לכל ההתקשרויות שבהן מעורב המשרד. ועדת מכרזים חייבת לכלול את בעלי התפקידים האלה: מנכ"ל או נציגו

55 הרחבה מקצועית בנושא שרשרת אספקה - דגשים עבור צד לקוח, סעיף 7.3.1.

56 הרחבה מקצועית בנושא שרשרת אספקה - דגשים עבור צד לקוח, סעיף 7.2.5.

57 הליך שנועד להגנה על פרטיות ובמסגרתו מושמט מידע מזהה ממאגר נתונים בטרם יימסר לשימוש של גורם חיצוני.

58 הוראת תכ"ם 7.1.1, מהדורה 9: "ועדת המכרזים".

(יו"ר), חשב המשרד או נציגו והיועץ המשפטי או נציגו. מלבדם, רשאי המנכ"ל למנות עד שני חברי ועדה נוספים. כמו כן הוועדה רשאית להזמין לישיבותיה גם גורם מקצועי רלוונטי במעמד של משקיף.

בפגישה שקיים צוות הביקורת עם נציגי גוף 22 במאי 2022 נאמר כי המשרד משלב את ממונה הגנת הסייבר בכל תהליכי הרכש בתחום התקשוב, לפי נוהל משרדי פנימי. גם בפגישה שקיים צוות הביקורת עם מערך הסייבר בפברואר 2023 נאמר כי כל רכש של המערך (כולל רכש בסכום של פחות מ-50,000 ש"ח) מחייב את אישור אגף הביטחון. במדיניות הביטחון במערך הסייבר נקבע, בין השאר, כי נציג אגף הביטחון יהיה חבר קבע בוועדת המכרזים ובוועדות הבלאי במערך או משקיף בדיוניהן, וכי הוא יהיה בעל הרשאת צפייה במערכת הרכש הממשלתית לצורך פיקוח ובקרה בהיבטי אבטחת המידע על כלל הנתונים בתחום הרכש השמורים במערכת.

מלמ"ב פרסם תקן בנושא תחומי האחריות והסמכות של ממונה ביטחון, הקובע כי ממונה הביטחון יכול להיות מעורב ברכש בעצמו או להסמיך את איש הרכש לשמש נאמן ביטחון בתחום הרכש ולטפל בנושאי האבטחה.

לפי תקנה 15(2)(ד) לתקנות אבטחת מידע, על בעל המאגר לקבוע בהסכם עם הספק את משך ההתקשרות, את אופן השבת המידע לידי הבעלים בסיום ההתקשרות, את השמדת המידע מרשותו של הספק ואת חובת הדיווח על כך לבעל מאגר המידע.

לפי הנחיית יה"ב[59], בסיום ההתקשרות עם ספק על המשרד לוודא כי בתום ההתקשרות בין הצדדים הספק עמד בכל הדרישות הנוגעות למחיקת הנתונים או להעברתם לידי המשרד, אם הם עדיין נדרשים למשרד. כמו כן על המשרד לוודא כי לספק לא נותרו הרשאות גישה או אמצעי הזדהות או אמצעים שיאפשרו לו גישה פיזית או לוגית למידע שברשות המשרד.

לוח 11: **מעורבות ממונה הגנת הסייבר בתהליכי הרכש**

השאלה	**שיעור הארגונים**
האם הממונה על הגנת הסייבר ו/או הממונה על שרשרת האספקה מעורבים בכל תהליכי הרכש בתחום התקשוב והסייבר בארגון?	**43% מהארגונים** **אינם מערבים את הממונה על הגנת הסייבר בכל תהליכי הרכש**
האם הממונה על הגנת הסייבר בארגון מעורב בתהליך סיום ההתקשרות עם הספק ומוודא שהספק ממלא את חובותיו בנושא סיום ההתקשרות (מחיקת המידע, החזרת האמצעים, ניתוק גישה מרחוק ועוד)?	**40% מהארגונים** **לא מערבים את הממונה על הגנת הסייבר בתהליך סיום ההתקשרות עם הספק**

59 הנחיית יה"ב 5.19 סעיף 7.1.2.

נמצא כי ב-19 (43%) מתוך 44 המשרדים וגופי התמ"ק שהשיבו על השאלה ממונה הגנת הסייבר או הממונה על שרשרת האספקה אינו מעורב בכל תהליכי הרכש בתחום התקשוב והסייבר בארגון. הדבר מעורר חשש כי היבטי אבטחת מידע לא יקבלו ביטוי בהתקשרויות השונות של המשרד בתחום התקשוב והסייבר ויחשפו את המשרדים לסיכוני אבטחת מידע במהלך תקופת ההתקשרות.

כן נמצא כי בהוראת התכ"ם 7.1.1, בפרק "התקשרויות בנושא תקשוב"[60], לא מצוינת החובה לערב את גורמי אבטחת המידע והגנת הסייבר המשרדיים בדיוני ועדת המכרזים המשרדית העוסקים בהתקשרויות בתחומי התקשוב והסייבר ולקבל מהם דרישות אבטחת מידע.

עוד נמצא כי ב-14 (40%) מתוך 35 משרדי הממשלה וגופי התמ"ק שענו על השאלה הממונה על הגנת הסייבר אינו מעורב בתהליך סיום ההתקשרות עם הספק ואינו מוודא שהספק ממלא את חובותיו בנושא סיום ההתקשרות (מחיקת המידע, החזרת האמצעים, ניתוק גישה מרחוק ועוד). הדבר חושף את הארגון לסיכון של גישה לא מורשית של הספק למידע או לנכסי הארגון לאחר סיום ההתקשרות.

מומלץ כי משרדי הממשלה וגופי התמ"ק יעדכנו את נוהל הרכש באופן שממונה הגנת סייבר יהיה מעורב בתהליכי הרכש בתחום התקשוב והסייבר בארגון ובכלל זה בתהליך סיום ההתקשרות עם הספק. עוד מומלץ כי אגף החשכ"ל במשרד האוצר יעדכן את הוראות התכ"ם הרלוונטיות באופן שהן יחייבו את המשרדים לערב את ממונה הגנת הסייבר או ממונה שרשרת האספקה בתהליכים הנוגעים לרכש בנושא תקשוב וסייבר ויקבל מהם דרישות אבטחת מידע לשם מתן מענה כולל והולם על סיכוני סייבר שעלולים להיות כרוכים בתהליך המכרז עצמו.

בתשובת גוף 15, גוף 5 וגוף 40 מיוני 2023 נמסר כי נוהל העבודה בנושא הרכש יעודכן ובכלל זה הסעיף שמתייחס לסיום ההתקשרות עם הספק.

בתשובת גוף 39 וגוף 40 מיוני 2023 נמסר כי הגופים יבחנו את נושא מעורבותו של ממונה הגנת הסייבר בתהליכי הרכש.

פעולות לחיסוי ולהתממה של מידע רגיש במכרז

בחוק חופש המידע, התשנ"ח-1998 (להלן - חוק חופש המידע), נקבע בין היתר כי רשות ציבורית אינה חייבת למסור מידע אשר גילויו עלול לגרום לנזק בתפקוד התקין של הרשות הציבורית וביכולתה לבצע את תפקידיה. נוסף על כך החוק קובע כי גם אם הרשות הציבורית רשאית או חייבת שלא למסור מידע כאמור, אם הרשות יכולה לגלות את המידע ללא הקצאה בלתי סבירה של משאבים או ללא הכבדה ניכרת על פעולתה של הרשות, תמסור הרשות את המידע בהשמטות פרטים, בשינויים או בתנאים המחויבים לעניין דרך קבלת המידע והשימוש בו.

60 הוראת תכ"ם 7.1.1, סעיף 2.6.8.

בנוהל ההתקשרויות[61] נקבע כי לא יפורסמו התקשרויות שיסווגו כרגישות. הסמכות לסווג התקשרות כרגישה נקבעה בנוהל ההתקשרויות. אם נמצא כי פריט מידע בעניין ההתקשרות מסומן במערכת הרכש הממשלתית כאסור בפרסום עקב רגישותו, יש לבחון אם אפשר להתמים אותו.

לפי מתודולוגיית שרשרת האספקה[62], במסגרת מדיניות הארגון יש לקבוע כי ממונה הביטחון (להלן - מנב"ט) יהיה מעורב בטיפול בעניינם של מכרזים והתקשרויות שאין לחשוף אותם ברבים או בעניינן של התקשרויות שבהן הספק ייחשף במסגרת פעילותו למידע מסווג.

פרסום מידע רגיש במסמכי המכרז עלול להעמיד לרשותו של תוקף פוטנציאלי כלים לתקיפת הארגון. לרוב מידע זה כולל פרטים על הטכנולוגיה והמוצרים שבהם משתמש הארגון, תיאור הרשתות ושרטוטי ארכיטקטורה. יצוין כי יש ארגונים שאינם מפרסמים בחלק מההתקשרויות מידע רגיש זה לציבור אלא מבצעים מכרז הנחלק לכמה שלבים, ובשלבים האחרונים במכרז מעבירים את המידע רק לידיעתם של מציעים שעומדים בתנאי אבטחת המידע.

מערך הסייבר הגדיר בנוהל הרכש שלו כמה קטגוריות של מוצרים רגישים או מסווגים שההתקשרויות לרכישתם לא יפורסמו לציבור ולא יופיעו במערכת הרכש הממשלתית מידע לגביהם. קטגוריות אלו כוללות מערכות תקשוב, מחשוב וחומרה, החזקה ותחזוקה של מערכות אבטחה, ביטחון ומיגון והתקשרויות עם ארגונים ממשלתיים. ההזמנות חולקו להזמנות רגילות (העולות לפורטל הספקים וניתנות לפרסום פומבי), הזמנות רגישות (העולות לפורטל הספקים, ללא פרסום פומבי, המסומנות כרגישות במערכת הרכש הממשלתית), הזמנות מסווגות (המתפרסמות ברשת המסווגת, שאינן עולות לפורטל הספקים). אגף הביטחון במערך הסייבר ממציא לוועדת הפטור במשרד האוצר הנמקה לגבי מניעת פרסום פומבי של התקשרות במסגרת כל מכרז שמסווג כרגיש.

להלן דוגמה למכרז מרכזי שפורסם ובו מידע רגיש: מכרז בתחום התקשוב ב' - בסעיף 1.8 במכרז זה נכתב כי המציע והיצרן לא יהיו רשאים לפרסם את עובדת זכייתם בתיחור זה, אולם מינהל הרכש פרסם באתר שלו את שמות הספקים הזוכים.

בתשובת מינהל הרכש מיוני 2023 נמסר כי לא כל מידע מחייב התממה. עוד נמסר כי במכרזים המרכזיים אין באמת תיאור תשתית אמיתית של גוף זה או אחר. במכרזים המרכזיים קיים רק תיאור דרישות סינתטי שמאגד תכונות של משרדים רבים, ומכאן שהוא למעשה "מותמם" מטבעו.

אשר לתשובת מינהל הרכש, יצוין כי הגורמים שאמונים על התממת מידע בתחום הסייבר הם הגופים האסדרתיים בתחום הסייבר או ממונה שרשרת האספקה, ולכן יש לערבם בתהליך ולקבל את אישורם לפרסום המידע.

61 משרד המשפטים, נוהלי חופש המידע - פרסום התקשרויות הממשלה, הקדמה.

62 מערך הסייבר, הרחבה מקצועית בנושא שרשרת אספקה צד לקוח, סעיף 7.2.5.

לוח 12: **יישום הדרישה להתממת מידע רגיש במכרזים**

השאלה	שיעור הארגונים
האם בפרסום מכרזים של הארגון בתחום התקשוב והסייבר אתם מתמימים מידע שקשור למבנה הרשתות ולסוגי הטכנולוגיות הרצויות?	**17% מהארגונים** **אינם מתממים מידע רגיש**

נמצא כי 8 (18%) מתוך 44 משרדי הממשלה וגופי התמ"ק שהשיבו על השאלה, אינם מתמימים במסגרת פרסום מכרזים של הארגון מידע רגיש כמו מידע שקשור למבנה הרשתות ולסוגי הטכנולוגיות הרצויות. עוד נמצא כי יש מכרזים מרכזיים שההתקשרויות שלהם מפורסמות במסגרת חוק חופש המידע ומכילות מידע רגיש למשל מכרז בתחום התקשוב ב'. עקב כך מידע רגיש אודות הטכנולוגיה, מבנה הרשתות והמוצרים שקיימים במשרדים ובגופי תמ"ק מפורסם לציבור ועשוי לשמש תוקף פוטנציאלי.

מומלץ כי משרדי הממשלה וגופי התמ"ק יוסיפו לנוהל שרשרת אספקה את ההנחיה להתמים מידע רגיש במסמכי המכרז ובהתקשרויות שמפורסמות במסגרת חוק חופש המידע, וכי תתבצע בקרה על ידי ממונה הגנת הסייבר או ממונה שרשרת האספקה על ביצוע ההנחיה כדי לוודא שמידע רגיש איננו מפורסם לציבור.

מודיעין סייבר ועסקי

לפי מתודולוגיית שרשרת האספקה, על הארגון לשקול להשתמש במודיעין סייבר ועסקי לשם בחינת מצב הספק לפני ההתקשרות עימו ובמהלכה.

למערך הסייבר יש יחידת מודיעין שאוספת מידע ברמה הלאומית, מקבלת מידע מגורמי קשרי חוץ ורוכשת מאגרי מודיעין. מידע זה כולל מידע על ספקים, אך מידע זה אינו מועבר באופן יזום ונקודתי לארגונים שמשתמשים בשירותים של ספקים אלו. כמו כן, המערך עצמו מבצע בדיקה בעניין הספקים שלו לפני ההתקשרות עימם ובמהלכה. בבדיקות אלו נבחן, בין היתר אם הספק מפרסם את העובדה שהוא נותן שירות לארגון. סט הכלים שבהם משתמש המערך להגדרת הסיכון הכרוך בהתקשרות עם הספק כולל מודיעין גלוי (OSINT) ומקורות נוספים.

יש משרדים שאוספים בעצמם מודיעין, למשל גוף 35 וגוף 24.

לוח 13: **קיום תהליך איסוף מודיעין סייבר במשרדים ובגופי תמ"ק**

השאלה	**שיעור הארגונים**
האם קיים תהליך של איסוף מודיעין סייבר ומודיעין עסקי על ספקי הארגון?	 **77% מהארגונים** **אינם אוספים מודיעין סייבר על ספקי הארגון**

נמצא כי ב-33 (77%) מתוך 43 משרדי הממשלה וגופי התמ"ק שהשיבו על השאלה לא מתבצע תהליך של איסוף מודיעין סייבר ומודיעין עסקי על ספקי הארגון, שלא לפי המלצות המתודולוגיה.

בתשובת גוף 18 מיוני 2023 נמסר כי נושא איסוף מודיעין סייבר עסקי על ספקי הארגון הוא בגדר המלצה ובשלב זה אינו מתועדף לטיפול בשנים 2023 ו-2024. בהתאם להמלצת מבקר המדינה הצורך באיסוף מודיעין ייבחן יחד עם מערך הסייבר ויה"ב.

בתשובת גוף 31 מיוני 2023 נמסר כי הגוף אינו מוצא לנכון לבצע איסוף סייבר ומודיעין עסקי על ספקי הארגון, ולפיכך גם אינו מקצה לכך משאבים. לטענת הגוף פעולות אלו אמורות להתבצע באמצעות גורם בעל רקע ויכולות בתחום ולהיות מונחות על ידי מערך הסייבר הלאומי. עוד נמסר כי הגוף יבחן את הנושא מול יה"ב.

בתשובת גוף 22 מיוני 2023 נמסר כי קיים מענה חלקי בנושא לגופים המחוברים למרכז הבקרה והשליטה הממשלתי (SOC) המספק מידע רב על אודות פגיעויות מפורסמות, ובתהליך זה משתתף גם ה-CERT הממשלתי.

בתשובת גוף 38, גוף 39 וגוף 40 מיוני 2023 נמסר כי הגופים מקבלים מידע מודיעיני ממערך הסייבר או מיה"ב באופן שוטף. עוד נמסר בתשובת גוף 38 כי בהתאם לצרכים ספציפיים שהתעוררו בשנת 2023, הגוף רכש גם מודיעין פומבי על שני ספקים בין-לאומיים מחברה חיצונית.

בתשובת גוף 7 מיוני 2023 נמסר כי תהליך של איסוף מודיעין סייבר ומודיעין עסקי על ספקי הארגון פחות מתאים לגוף 7 בשל מספרם הקטן יחסית של ספקים שיש להם גישה לרשת ולמערכות הגוף.

מומלץ כי משרדי הממשלה וגופי התמ"ק שהשיבו כי הם אינם מבצעים תהליך של איסוף מודיעין סייבר ועסקי על ספקי הארגון שלהם יבחנו יחד עם מערך הסייבר ויה"ב אם קיים במקרים מסוימים צורך באיסוף מודיעין וכן יבחנו את האפשרות לקבל מידע מודיעיני קיים על הספקים המהותיים שלהם. באופן זה יוכל המשרד לנהל את הסיכון מול הספק גם לפני ההתקשרות מולו ולתת את הדעת על סיכונים מקיפים יותר בשרשרת האספקה מעבר לפגיעויות ידועות במוצר זה או אחר.

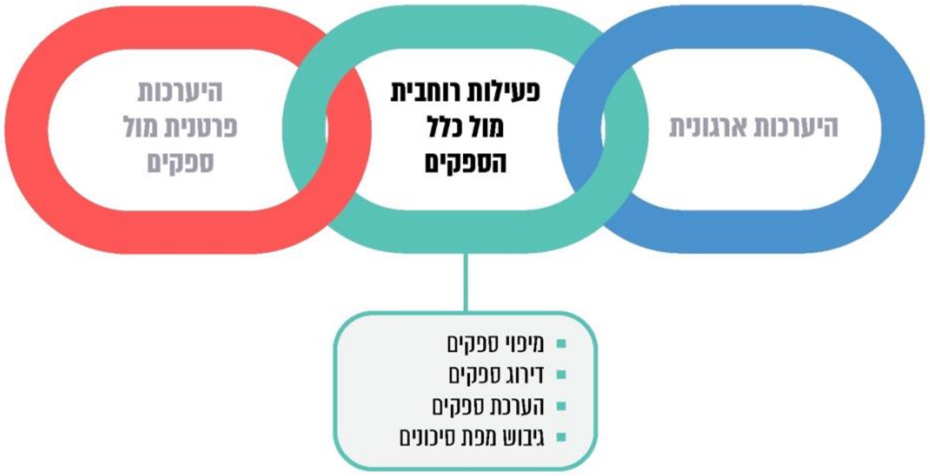
בתשובת גוף 7 וגוף 10 מיוני 2023 נמסר כי הגופים יבחנו ביחד עם מערך הסייבר הלאומי ויה"ב את האפשרות לקבל מודיעין זה ממערך הסייבר.

שלב ב' במתודולוגיית שרשרת האספקה - פעילות רוחבית מול כלל הספקים

כאמור המתודולוגיה של מערך הסייבר כוללת שלושה שלבים: היערכות ארגונית, פעילות רוחבית מול הספקים והיערכות פרטנית מול ספקים. להלן נפרט על הפערים שעלו בשלב ב':

שלב זה נחלק על פי המתודולוגיה לכמה תתי-שלבים: מיפוי הספקים שעימם התקשר הגוף, דירוג ספקים, מילוי שאלון על ידי הספקים, הפניה של השאלון לגורם בדיקה מוסמך, בחינת השאלון המלא והאסמכתאות. להלן פירוט בעניינו של כל תת-שלב:

תרשים 12: **פעילויות רוחביות של הארגון מול כלל הספקים שלו**



המקור: מערך הסייבר.

מיפוי ודירוג של ספקים

לפי ההנחיה שבמתודולוגיית שרשרת האספקה, בשלב הראשון של הפעילות הרוחבית מול הספקים על כל ארגון לבצע מיפוי של כלל ספקי המחשוב והסייבר שלו. במסגרת המיפוי יובא בחשבון סוג השירות שמספק הספק, המוגדר בהתאם לחמש הקטגוריות האלו:

1. **דרישות רוחביות:** כל ספק נדרש לעמוד ברמת הגנת סייבר בסיסית בתחומים השונים, כמעט ללא תלות בסוג השירות שהוא מספק. דרישות אלו מייצגות את המינימום המצופה מכל ספק שהארגון מתקשר איתו, בהתאם לרמת הסיכון הנשקפת לנוכח ההתקשרות עימו.

2. **גישה מרחוק:** האם הספקים נדרשים, במסגרת חוזה ההתקשרות עימם, להתחבר למשאבי הארגון לצורך אספקת המוצר או השירות.

3. **שירות מבוסס ענן:** האם הספקים מספקים ללקוח, במסגרת ההתקשרות עימו, שירות או מוצר מבוסס ענן.

4. **פיתוח תוכנה:** האם הספקים מפתחים תוכנה שתותקן אצל הלקוח.

5. **אירוח ואחסון של אתרים:** האם הספקים מפתחים או מאחסנים אתרי מרשתת (אינטרנט) עבור לקוחותיהם.

במסגרת מיפוי הספקים יש לפרט מידע זה: (**א**) **שם הספק**; (**ב**) **מאפייני התקשרות** עם הספק; (**ג**) **איש קשר** מהצד העסקי בארגון הפועל מול הספק; (**ד**) **פרטי ההתקשרות עם נציג הספק**; (**ה**) **קטגוריית השירות הניתן** (שירות מבוסס ענן, שירות פיתוח תוכנה, שירותי גישה מרחוק, שירות אחסון של אתרים או שירות שכולל חשיפת מידע של הלקוח); (**ו**) **רמת הסיכון** של הספק (האם מדובר בספק מהותי או לא-מהותי): ספק מהותי הוגדר במתודולוגיה כספק של שירותי תמיכה או של שירותי תחזוקת מערכות מידע, כספק שירותי אחסון נתונים רגישים מחוץ לחצרות המשרד הממשלתי, כספק שירותי מיקור חוץ טכנולוגיים או כספק שהפגיעה בו עלולה לגרום נזק מהותי למשרד הממשלתי. ההחלטה אם להגדיר ספק כמהותי נתונה לשיקול דעתו של הארגון או המאסדר.

לוח 14: **יישום מיפוי ספקים במשרדים ובגופי תמ"ק**

השאלה	**שיעור הארגונים**
האם יש לארגון מיפוי של כלל הספקים שלו בתחום התקשוב והסייבר ושל ספקים שיש להם גישה למידע רגיש?	**23% מהארגונים לא ביצעו כלל מיפוי של ספקים או ביצעו מיפוי של חלק מהספקים**
כמות הארגונים שהשיבו שאין להם אף ספק מהותי בתחום התקשוב והסייבר או שאין להם אף ספק שיש לו גישה למידע רגיש	**37% מהארגונים לא סיווגו שום ספק שלהם כספק מהותי**

נמצא כי 10 (23%) מתוך 43 המשרדים וגופי התמ"ק שענו על השאלה לא ביצעו כלל מיפוי של ספקים או ביצעו מיפוי של חלק מהספקים.

עוד נמצא כי המיפוי של 24 (83%) מתוך 29 המשרדים וגופי התמ"ק שהעבירו למשרד מבקר המדינה את ממצאי מיפוי הספקים שלהם, לא כלל את כל פרטי המידע הנדרשים לפי המתודולוגיה של מערך הסייבר. מיפוי חסר שלא כולל את כל הספקים או אינו כולל מידע מהותי על הספק כמו סיווג הספקים מעלה חשש שהארגון לא יוכל לפעול לניהול הסיכונים מול הספקים המהותיים שלו.

כמו כן נמצא כי 14 (37%) מתוך 38 המשרדים וגופי התמ"ק שענו על השאלה לא סיווגו שום ספק שלהם כספק מהותי או כספק שיש לו גישה למידע רגיש, אף שבהכרח יש להם ספקים שעומדים בתבחינים של ספק מהותי על פי המתודולוגיה של שרשרת האספקה כדוגמת ספק של שירותי תמיכה או של שירותי תחזוקת מערכות מידע או ספק שירותי מיקור חוץ טכנולוגיים שהפגיעה בהם עלולה לגרום נזק מהותי למשרד הממשלתי.

מומלץ שמשרדים וגופי תמ"ק שלא ביצעו מיפוי מלא של הספקים שלהם ישלימו את המיפוי ויעבירו אותו לגוף שמנחה אותם בתחום הסייבר לבחינה. עוד מומלץ כי משרדים וגופי תמ"ק שלא סיווגו שום ספק שלהם כספק מהותי או כספק שיש לו גישה למידע רגיש יבחנו שוב את רשימת הספקים ויוודאו שאכן שום ספק ברשימתם לא עומד בתבחין של ספק מהותי לפי מתודולוגיית שרשרת האספקה, שפגיעה בו תגרום לנזק מהותי בארגון.

בתשובות גוף 38, גוף 15, גוף 24, גוף 9, גוף 10 וגוף 40 מיוני 2023 נמסר כי ההמלצות מקובלות עליהם והגופים יפעלו למיפוי מלא של כל הספקים בהתאם לנדרש במתודולוגיה.

בתשובת גוף 15 מיוני 2023 נמסר כי לאחר קבלת המתווה החדש של מתודולוגיית שרשרת האספקה גרסה 1.4 נקבעה פגישה עם המאסדר לבחינה של הספקים המהותיים ולטיוב הרשימה.

בתשובת גוף 15 וגוף 10 מיוני 2023 נמסר כי הגופים יבחנו מחדש את הספקים שלהם ויבדקו אם קיימים ביניהם ספקים שהפגיעה בהם עלולה לגרום נזק מהותי לגופים.

הערכת ספקים

לפי מתודולוגיית שרשרת האספקה, יש להעריך את הספקים בהתאם לשאלון ספקים שמפרסם מערך הסייבר. בשאלון הספקים נכללות משפחות של בקרות בתחומים שונים, ומערך הסייבר מעדכן אותו במרשתת ובמערכת יוב"ל באופן עיתי בהתאם לאיומים בתחום שרשרת האספקה.

לוח 15: **שימוש של משרדים וגופי תמ"ק בשאלון ייעודי להערכת ספקים**

השאלה	שיעור הארגונים
האם הארגון בודק את נושא שרשרת אספקה אצל הספק באמצעות שאלון ייעודי שפיתח לנושא (שונה משאלון הספקים של מערך הסייבר הלאומי) .	**26% מהארגונים משתמשים בשאלונים ייעודיים**

נמצא כי 9 (26%) מתוך 35 המשרדים וגופי התמ"ק שענו על השאלה אינם משתמשים בשאלון הספקים שגיבש מערך הסייבר אלא משתמשים בשאלונים חלופיים שפיתחו הארגונים, וזאת בלא שמערך הסייבר בחן האם השאלונים החלופיים כוללים את כלל הבקרות העדכניות שהגדיר מערך הסייבר כרלוונטיות לנושא שרשרת האספקה. כמו כן, בשיטה זו ארגונים שונים נבדלים זה מזה מבחינת האופן שבו הם בודקים את מידת עמידתו של הספק בדרישות שנקבעו במתודולוגיה.

בתשובת גוף 35 מיולי 2023 נמסר כי הגוף משתמש בשאלון רחב יותר הכולל סעיפים של שאלונים של מערך הסייבר.

בתשובת גוף 22 מיוני 2023 נמסר כי איסוף המידע וסקר הסיכונים להערכת הספק נעשה על בסיס שאלון הספקים שגיבש מערך הסייבר, וכי בחלק מהשאלון לא נעשה שימוש בשל חוסר רלוונטיות בהתקשרות או בשל האופן שההתקשרות מתנהלת מול המשרד.

מומלץ כי משרדים וגופי תמ"ק שמשתמשים בשאלונים חלופיים שפיתחו יעברו להשתמש בשאלון הספקים של מערך הסייבר, ואם נדרש לבצע התאמות בשאלון הם יעלו את צורכיהם מול מערך הסייבר. עוד מומלץ כי מערך הסייבר יוודא מול המשרדים וגופי התמ"ק שהם משתמשים בשאלון העדכני הכולל את הבקרות שהגדיר המערך. זאת כדי להבטיח שבדיקת הספקים תהיה אחידה באופן שתוצאותיה יוכלו לשמש ארגונים נוספים.

בתשובת גוף 36 מיוני 2023 נמסר כי בכוונת הגוף לבחון את השאלון שפיתח מול יה"ב על מנת לקבוע אחידות או לחלופין להשתמש בשאלון של מערך הסייבר.

בתשובת גוף 7 מיוני 2023 נמסר כי עבור ספקים בסיווג בינוני ומטה קיים שאלון ייעודי של הגוף. הגוף יבחן שימוש בשאלונים של מערך הסייבר גם עבור ספקים בסיווג זה.

קצב ההתעדה ומשכה

בפגישה שקיים צוות הביקורת עם יחידת המדיניות במערך הסייבר בספטמבר 2022 נאמר כי הצפי המקורי של המערך היה שבשנת 2019, תוך שנה מהשקת המתודולוגיה אלפי ספקים יעברו התעדה.

נכון למרץ 2023, כחמש שנים לאחר התנעת המתודולוגיה, היו רק שמונה ספקים מאושרים שעברו התעדה, ראו תצלום מסך מאתר מערך הסייבר.

תמונה 2: **רשימת ספקים מאושרים - רמה A**

מאגר ספקים מאושרים- רמה A

ספקים אשר דורגו ברמה A (פלטינה)- נדרשו לענות על השאלון בעזרת בודק ספקים מורשה, אשר בודק כי הספק עומד בדרישות ההגנה שבשאלון לרבות צירוף הראיות הנדרשות בשאלון, (את הראיות העביר הספק ללקוח בערוץ בטוח שסוכם בין הצדדים).
בנוסף- לביקורת צד ג' שמתבצעת על ידי מכון בדיקת תאימות מורשה מטעם מערך הסייבר.

תיגבור מאגר כ"א אדם מקצועי זמני בע"מ

אפסילון אחזקה והשקעות בע"מ

שימקוטק בע"מ

מעוף משאבי אנוש

חילן בע"מ

אי.פי.גרופ בע"מ (אי.פי סק)

ווי-אייטי בע"מ

מערך הדיגיטל הלאומי

- **שם הספק:** מערך הדיגיטל הלאומי
- **טלפון:** 02-6664649
- **ח.פ.:** 500100037
- **דוא"ל:**
- **כתובת:** נתנאל לורך 1, ירושלים
- **איש קשר**

- **סוגי התקשרויות:** דרישות רוחביות
- **התהליך המותעד:** פיתוח, הקמה, הפעלה, תחזוקה, אבטחת המידע והגנה בסייבר של אתרי רשת, מערכות ושירותים דיגיטליים בחוות האירוח המקומית ובענן.
- **מספר אישור:** I25754
- **תוקף האישור:** עד ה- 19/9/2023
- **גוף מסמיך:** מכון לבקרה ואיכות איי.קיו.סי. בע"מ
- **איש/אשת הקשר בגוף המסמיך:**

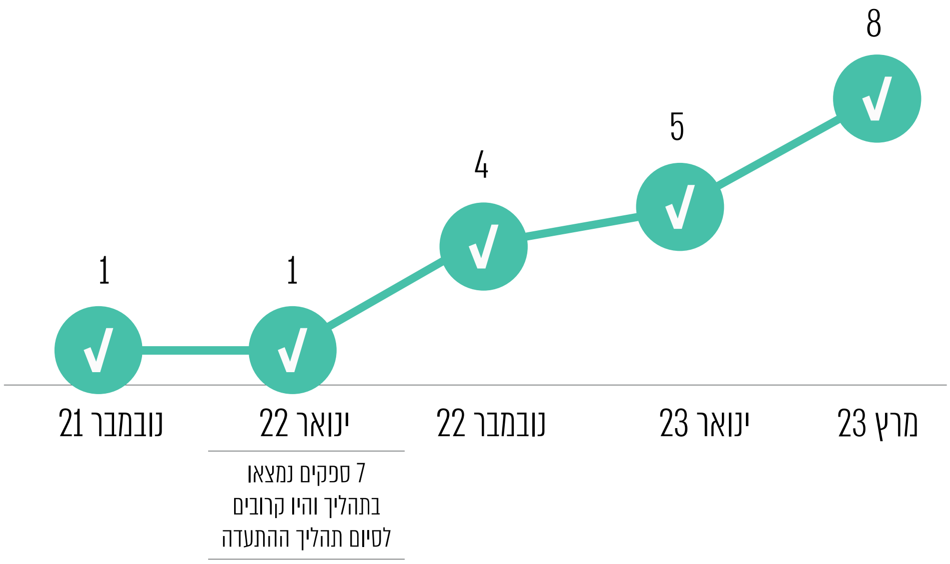
המקור: אתר מערך הסייבר, צולם במרץ 2023.

מתשובות המשרדים וגופי התמ"ק לשאלון ששלח משרד מבקר המדינה עולה כי ארגונים אלו סיווגו 59 ספקים כמהותיים (רמה A). מתוך 59 ספקים אלו רק שלושה ספקים עברו הסמכה ומופיעים באתר מערך הסייבר (ספק ק', ספק ר' וספק ש').

בפגישה שקיים צוות הביקורת עם אגף ביטחון וסייבר בגוף 21 נאמר כי תהליך ההתעדה שקידם המשרד מול ספק ק' בתחום הפיננסי ארך כ-9 חודשים. בפגישה שקיים צוות הביקורת עם גוף 2 נאמר כי משך תהליך ההתעדה, שאורכו כשנה קלנדרית, אינו עונה על הצורך העסקי של הארגון ועשוי לפגוע ביעדיו ובעמידתו בלוחות הזמנים של פרויקטים שקצובים בזמן.

במענה של גוף 28 על השאלון צוין כי אומנם קיימת הנחיה ולפיה ספקים מהותיים יעברו תהליך התעדה, אולם הגוף לא היה עומד בתוכנית העבודה ובמתן השירות לו היה דורש מספקים אלו לבצע התעדה, ולכן הגוף מבצע ביקורות על ספקים בתחום שרשרת האספקה ללא דרישה לבצע תהליך ההתעדה.

תרשים 13: **מספר הספקים שהותעדו או שנמצאו בתהליך התעדה בשנים 2021 - 2023**



המקור: סיכומי הישיבות של ועדות ההיגוי שעסקו בנושא שרשרת האספקה ונתונים שהוצגו באתר מערך הסייבר במרץ 2023.

נמצא כי קצב ההתעדה של ספקים מהותיים איטי יותר מכפי שהעריך מערך הסייבר: עד מרץ 2023 הותעדו רק שמונה ספקים וכן התקבלו 28 הצהרות עצמאיות של ספקים מתוך כ-1,700 ספקים רלוונטיים שנדרשים בהתעדה או בהצהרה עצמית לפי הערכת מערך הסייבר. עוד נמצא כי משך תהליך ההתעדה (מעל 9 חודשים) אינו בהלימה לצרכים העסקיים של הארגונים.

לוח 16: **יישום ההתעדה של ספקים שסווגו ברמה A**

השאלה	**שיעור גופי התמ"ק**
לכמה מהספקים שהארגון סיווג ברמה A לא נתת הנחיה לעבור התעדה?	**30% מהארגונים לא הנחו את הספקים שדורגו כמהותיים (A) לעבור תהליך התעדה**

עוד נמצא כי 3 (30%) מתוך 10 גופי תמ"ק לא הנחו את הספקים שהם סיווגו כספקים מהותיים ברמת סיווג A לעבור תהליך התעדה.

בתשובת מערך הסייבר מיוני 2023 נמסר כי במסגרת גרסה 1.4, שגובשה במהלך הביקורת, עודכנו דרישות שאמורות לסייע בהעלאת שיעור הספקים שיעברו הליך התעדה באמצעות בודק ספקים והצהרה עצמית, ולא רק באמצעות מכון התעדה.

בתשובת גוף 5 מיוני 2023 נמסר כי במערך הסייבר נבדקת פנייה רשמית לספקיות מרכזיות כמו ספק א' וספק ד' לבצע התעדה מסודרת, נושא שיספק מענה לגופים רבים.

בתשובת גוף 7 מיוני 2023 נמסר כי במכרז מיקור חוץ החדש הוגדרה דרישה שהספק יעבור בתוך שנה תהליך התעדה ברמת ספק מהותי A על פי הנחיית מערך הסייבר.

מומלץ כי גופי התמ"ק שעובדים עם ספקים שסווגו ברמה A ולא עברו תהליך התעדה ידרשו מהספקים לעבור את התהליך בהתאם להנחיה. כמו כן מומלץ כי מערך הסייבר יבחן מדוע טרם הותעדו מרבית הספקים המהותיים של גופי התמ"ק ומדוע ארגונים אלו לא הנחו את אותם הספקים לעבור תהליך התעדה. עוד מומלץ כי מערך הסייבר יבחן מדוע תהליך ההתעדה מתמשך זמן כה רב, יגבש תכנית לקיצור לוחות הזמנים ויפעל לפיה.

בתשובת מערך הסייבר מיוני 2023 נמסר כי ההמלצות לבירור ולקידום של התעדת המערך על ספקים קריטיים של גופי התמ"ק, וכן גיבוש תוכנית לקיצור זמנים של תהליך ההתעדה, יועברו לבחינה.

בתשובת גוף 15 מיוני 2023 נמסר כי הגוף ישלח מכתבים לכלל הספקים המהותיים שלו, ובו יסביר על חשיבות תהליך ההתעדה ויפנה לאיש קשר במערך הסייבר המטפל בנושא.

עלות ההתעדה

בישיבתה של ועדת ההיגוי במערך הסייבר בנושא שרשרת האספקה ממאי 2021 עלה כי אחד החסמים בביצוע ההתעדה הוא העלויות הגבוהות של התהליך, וכי העלויות העיקריות מקורן בתהליך שבו יועץ מורשה בוחן אם הספק עומד בהצלחה בבקרות ומכין אותו לתהליך ההתעדה

בנוסף לעלויות אלו יש את עלות גוף ההסמכה שמוערכת בכ-10,000 ש"ח. בפגישה שקיים צוות הביקורת עם מנחים של גופי תמ"ק בנובמבר 2022 נאמר כי רוב העלויות הגבוהות של ההתעדה מקורן בעיקר בהוצאות על תיקון הליקויים אצל הספקים כדי לעמוד בכל הבקרות שנכללות בשאלון הספקים, וכי הספקים משיתים עלויות אלה על גופי התמ"ק באמצעות דרישתם לתוספת תשלום במסגרת ההתקשרויות. נוכח זאת, ובהיעדר תקציב מדינתי לכיסוי העלויות, לעיתים גופי התמ"ק אינם דורשים מהספקים במסגרת ההתקשרויות שלהם לעמוד בדרישות שנקבעו במתודולוגיה של שרשרת האספקה.

להלן דוגמאות לניסיונות של ארגונים להתעיד ספקים שלא בוצעו עקב העלויות הגבוהות שכרוכות בתהליך:

1. **גוף 2:** הגוף ביקש לעבוד עם ספק של מערכת ממוחשבת לניהול תחזוקת מבנים שנמצאת במשרדי ממשלה נוספים ומחזיקה מידע רגיש שלהם, ספק זה לא קיבל הסמכה של ספק מאושר. הגוף, שהוא כאמור גוף תמ"ק שנדרש לעמוד בהנחיות שרשרת האספקה של מערך הסייבר, ביקש מהספק לעבור הליך התעדה בשל היותו ספק מהותי. הספק דרש מהגוף לשלם עבור תהליך ההתעדה סכום של 30,000 ש"ח. הגוף הסכים לשלם זאת מתקציבו, אף שספק זה נותן שירותים למשרדים נוספים והתעדת הספק יכולה לשמש גם אותם. התהליך נמשך כשנה, ובסופו סירב הספק לעבור את הליך ההתעדה בשל חוסר כדאיות עבורו.

2. **גוף 24:** הגוף ניסה להעביר את הספקים המהותיים שלו תהליך התעדה, זאת ללא הצלחה מאחר שהספקים לא יכלו לעמוד בעלויות הניכרות הכרוכות בתהליך.

כאמור, בישיבת ועדת ההיגוי שהתקיימה ביוני 2021 והתמקדה בגופי תמ"ק הוצע שמערך הסייבר יקדם פיילוט להתעדה של עשרה ספקי ליבה של גופי תמ"ק, ועובדיו ילוו את גופי התמ"ק בתהליך ההתעדה במקום שישכרו יועצים חיצוניים. פיילוט זה לא יצא לפועל בסופו של דבר.

בפגישה שקיים צוות הביקורת עם יחידת המדיניות במערך הסייבר בפברואר 2023 נאמר כי מערך הסייבר אינו מתכנן להשקיע משאבים בתהליך ההתעדה של ספקים, אף אם הם נותנים שירותים לארגונים רבים. כמו כן נאמר כי הם מזהים תהליך חדש לפיו ארגונים שמקבלים שירותים מאותו הספק חוברים יחד ביוזמתם כדי לממן את הליך ההתעדה.

נמצא כי גופי תמ"ק אינם מוכנים לממן מתקציבם את עלויות ההתעדה ואף הספקים אינם מוכנים לשאת מצידם בעלויות אלו, עקב כך גופי התמ"ק אינם דורשים מהספקים במסגרת ההתקשרויות עימם לעמוד בדרישות שנקבעו במתודולוגיה של שרשרת האספקה. לדוגמה: גוף 2 לא הצליח להתעיד ספק של מערכת ממוחשבת לניהול תחזוקת מבנים שנמצאת במשרדי ממשלה נוספים ומחזיקה מידע רגיש שלהם. גם מערך הסייבר אינו מתכנן להשקיע משאבים בתהליך ההתעדה של ספקים אלו, נוכח זאת אין מי שישא בעלויות ההתעדה של ספקים מהותיים שנותנים שירותים לגופי תמ"ק.

מומלץ כי הגופים האסדרתיים בתחום הסייבר (מערך הסייבר, יה"ב) יבחנו דרכים להפחתת העלויות שחלות על הגוף שמבקש להוסיף דרישה לעמידה במתודולוגיית שרשרת האספקה לספקים שנותנים שירות לגופי תמ"ק ולמשרדים רבים, למשל באמצעות התעדה משותפת של כמה גופים ובאמצעות סיוע של בודק ספקים מוסמך מטעם הגוף האסדרתי שיבחן את עמידת הספק בבקרות הנדרשות במתודולוגיה.

חשיפת מידע רגיש

חשיפת עצם ההתקשרות עם הספק

בפגישה שקיים צוות הביקורת עם אגף הביטחון של מערך הסייבר נאמר כי המערך בודק את מידת עמידתם של הספקים שלו בדרישות שרשרת האספקה בהתאם לשאלון הספקים וכן בהתאם לבקרות נוספות המותאמות לאיום הייחוס שלו. את הבדיקה מבצע עובד מערך הסייבר, שהוא בודק ספקים מאושר. עוד נאמר בפגישה כי ממצאי הבדיקה אינם מועברים למכון ההתעדה, כיוון שהמערך אינו מעוניין לפרסם לציבור או לארגונים אחרים את שמות הספקים שנותנים לו שירות ושלדעתו מדובר במידע רגיש. יצוין כי במסגרת המידע על הספק שהותעד, אשר מתפרסם באתר מערך הסייבר במרשתת, לא מפורט מיהו הארגון שביצע את ההתעדה ולא מצוינים שמות הארגונים שהוא מספק להם שירות.

נמצא כי מערך הסייבר אינו מבצע התעדה של הספקים שנותנים לו שירות כדי שלא לחשוף לציבור או לארגונים אחרים את שמות הספקים שנותנים לו שירות מחשש לפגיעה בהם כשרשרת האספקה של הארגון, וזאת אף שהוא דורש מגופי התמ"ק לבצע התעדה לספקים שלהם. גישה זו מעלה ספק אם תהליך ההתעדה מתאים לארגונים שמחזיקים בנכסי מידע מסווגים ורגישים.

מומלץ כי מערך הסייבר יבחן את סוגיית ההתעדה ופרסום המידע בנושא הספקים שעברו התעדה עבור ספקי המערך עצמו ועבור גופים אחרים המחזיקים בנכסי מידע מסווגים ורגישים, על מנת למזער את החשש שהוא העלה לגבי האפשרות שהספק יפרסם את שמות הארגונים שביצעו את תהליך התעדתו או את שמות הארגונים שהוא מספק להם שירות.

בתשובת מערך הסייבר מיוני 2023 נמסר כי מערך הסייבר יקיים בחינה של סוגיה זו.

החזקת מידע רגיש בגופי ההסמכה

לפי המתודולוגיה של המערך, בודקים מוסמכים חיצוניים של שרשרת האספקה ממלאים את השאלון עבור הספק ואוספים ממנו את המסמכים המשמשים ראיות לכך שהוא עומד בדרישות הסף. אחרי מילוי השאלון הבודקים מעבירים לגופי ההסכמה באמצעות כספות את השאלון ומסמכי הראיות, לצורך קבלת אישורם. בפגישה שקיים צוות הביקורת עם יחידת המדיניות במערך הסייבר בספטמבר 2022 נאמר כי מערך הסייבר סיווג את גופי ההסמכה כספק ברמה C שנדרש לבצע הערכה עצמית בלבד.

השאלון ומסמכי הראיות מכילים מידע רגיש בתחום הגנת הסייבר על הספקים, שחלקם נותנים שירות ומוצרים לגופי תמ"ק ולכן מידע רגיש זה עשוי להיות יעד לתקיפה.

גוף 20 וגוף 15 הם גופי תמ"ק שהתקשרו עם חברות חיצוניות שיבצעו עבורן את בדיקת הספקים. גופים אלו לא סיווגו את החברות כספקים מהותיים שנדרשים לבצע התעדה, וכמו כן גוף 20 אף לא כלל את חברה זו במיפוי הספקים שלו.

נמצא כי גופי ההסמכה של שרשרת האספקה והספקים שנותנים שירותי בדיקת ספקים, המקבלים מגופים שונים לרבות מגופי תמ"ק את השאלון ואת מסמכי הראיות שמכילים מידע רגיש, לא סווגו כספקים מהותיים הנדרשים להצהיר על עמידתם בדרישות שבשאלון הספקים, אף שלנוכח המידע הרגיש שהם מחזיקים הם עלולים להיות יעד לתקיפה כך לדוגמא גוף 20 לא כלל במיפוי הספקים שלו את החברה החיצונית עימה התקשר לביצוע בדיקת הספקים.

מומלץ כי מערך הסייבר יבחן את האפשרות לסווג מחדש את גופי ההסמכה כספקים מהותיים בהלימה למידת רגישות המידע שמוחזק בידם וידרוש מהם להצהיר על עמידתם בבקרות שבשאלון הספקים לאחר שגורם חיצוני מוסמך, כמו בודק מטעם מערך הסייבר, בדק את המענה שלהם על השאלון לרבות ההצהרה. עוד מומלץ כי כל ארגון שנעזר בספק לקבלת שירותי בדיקת ספקים יסווג ספק זה כספק מהותי וידרוש ממנו להצהיר על עמידתו בבקרות שבשאלון הספקים.

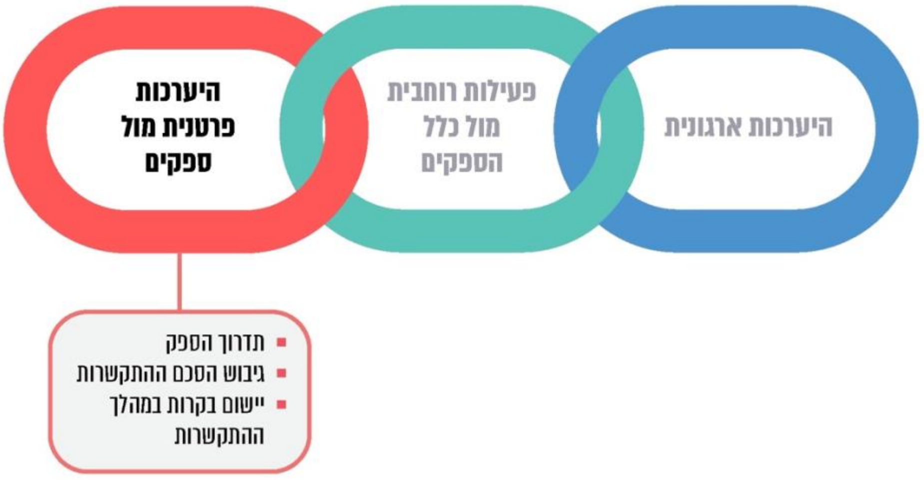
בתשובת גוף 15 מיוני 2023 נמסר כי הוא הוסיף את החברה שנותנת שירותי בדיקת ספקים כספק מהותי במיפוי הספקים שלו.

שלב ג' במתודולוגיית שרשרת האספקה - היערכות פרטנית מול ספקים

כאמור המתודולוגיה של מערך הסייבר כוללת שלושה שלבים: היערכות ארגונית, פעילות רוחבית מול הספקים והיערכות פרטנית מול ספקים. להלן נפרט על הפערים שעלו בשלב ג':

שלב זה כולל חתימה על הסכם התקשרות עם הספק, הכולל נספח אבטחת מידע העוסק בכלל היבטי ניהול סיכוני הסייבר בשרשרת האספקה, בתדרוך הספק ובבקרות שיש לבצע במהלך ההתקשרות. אשר לספקים מהותיים, יש לתקף אחת לשנה לפחות את עמידתם בהתחייבויות שבחוזה ההתקשרות עימם.

תרשים 14: **פירוט הפעילויות להיערכות פרטנית מול ספקים**



המקור: מערך הסייבר.

יישום בקרות במהלך ההתקשרות עם הספקים

לפי תקנה 15(א)(ח) לתקנות אבטחת מידע מחובתו של הספק לדווח, אחת לשנה לפחות, לבעל מאגר מידע על אודות אופן ביצוע חובותיו לפי התקנות. כמו כן, לפי תקנה 15(4) על בעל מאגר המידע לנקוט אמצעי בקרה ופיקוח על עמידתו של הספק בהוראות ההסכם ובהוראות תקנות אבטחת מידע בהיקף הנדרש, בשים לב לסיכונים שהוגדרו.

לפי מתודולוגיית שרשרת האספקה, מדיניות הארגון תכלול בין היתר היבטי ביקורת ובקרה על הספק. אשר לספקים שלא מתבצעת התעדה שלהם, מסיבה זו או אחרת, נקבע במתודולוגיה כי יש לכלול בחוזה ההתקשרות דרישה ולפיה יתאפשר ביצוע ביקורת עליהם[63]. במתודולוגיה מוגדרת סדרה של בקרות ליישום במהלך ההתקשרות, למשל: יש לתקף לפחות אחת לשנה את מידת עמידתם של ספקים מהותיים בהתחייבויותיהם שבחוזה ההתקשרות.

לטיוטת נספח ז' להוראת התכ"ם 7.3.1 התווסף נספח אבטחת מידע אשר באחד מסעיפיו צוין: "המזמין יהיה רשאי לבצע ביקורת תקופתית אודות עמידת הספק בדרישות הגנת המידע, הפרטיות והסייבר במסגרת אספקת השירותים למזמין"[64], וכן נוסף לטיוטה סעיף ולפיו "המזמין יהיה רשאי לבצע ביקורת בעקבות חשש לתקיפת סייבר המשפיעה על אספקת השירותים או המוצרים למזמין".

63 הרחבה מקצועית בנושא שרשרת אספקה -דגשים עבור צד לקוח, סעיף 4.3.1.2

64 ההתקשרויות שרמת רגישותן "רגילה" נבדלות מהתקשרויות שרמת רגישותן "מוגברת" נבדלות זו מזו מבחינת אופן ביצוע הביקורת התקופתית עליהן.

אם תהליך הביקורת על הספק העלה ליקויים בפעילותו, הארגון המזמין נדרש לבצע מעקב אחר תיקון הליקויים. חידוש חוזה עם הספק הוא הזדמנות טובה לדרוש כי יתקן את הליקויים שהועלו בביקורת כתנאי לחידוש החוזה.

בפגישה שקיים צוות הביקורת עם נציגי יה"ב בספטמבר 2022 נאמר כי גופים שונים כמו גוף 27 וגוף 49 מבצעים ביקורות על ספקים, אולם גופים אלה אינם מעבירים את ממצאי הביקורת ליה"ב ואינם מעדכנים אותה אם הספקים תיקנו את הליקויים בפעילותם (אם אכן נמצאו ליקויים בפעילות הספקים).

לוח 17: **ביצוע ביקורות של ארגונים על ספקים**

השאלה	שיעור הארגונים
האם במכרזים של הארגון יש סעיף שנותן לארגון רשות לבצע ביקורות סייבר אצל הספק?	**20% מהארגונים** **לא כללו במכרזים סעיף שמאפשר להם לבצע ביקורות סייבר על הספק**
האם הארגון ביצע ביקורות סייבר אצל ספקים מהותיים (בסיווג A) שלא עברו התעדה בשלוש השנים האחרונות (2020 - 2022)?	**41% מהארגונים** **לא ביצעו ביקורת על ספקים מהותיים בשלוש שנים האחרונות**
האם הארגון מבצע מעקב שנתי אחר תיקון הליקויים שנמצאו אצל הספק?	**31% מהארגונים** **לא ביצעו מעקב שנתי אחר תיקון הליקויים שנמצאו אצל הספק**

נמצא כי במכרזים של 9 (20%) מתוך 44 מהמשרדים וגופי התמ"ק שענו על השאלה אין סעיף במכרז שמאפשר להם לבצע ביקורות סייבר על הספק.

מומלץ כי המשרדים וגופי התמ"ק שלא כללו במכרזים שלהם סעיף המחייב את הספק לפעול בהתאם למתודולוגיית שרשרת האספקה, יוסיפו סעיף כזה, ולכל הפחות יוסיפו סעיף המאפשר לארגון לבצע ביקורות סייבר על הספק.

בתשובת גוף 5 מיוני 2023 נמסר כי סעיף זה יתווסף לחוזים חדשים עבור פרויקטים משמעותיים שמחייבים ביצוע פעולה זו.

בתשובת גוף 9 מיוני 2023 נמסר כי אגף טכנולוגיות, דיגיטל ומידע (טד"ם) הנחה את הלשכה המשפטית בגוף להוסיף סעיפים רלוונטיים לביצוע ביקורות סייבר על הספקים לחוזים עתידיים.

עוד נמצא כי 14 (41%) מתוך 34 מהמשרדים וגופי התמ"ק שענו על השאלה לא ביצעו בשלוש השנים האחרונות (2020 - 2022) ביקורת על הספקים המהותיים שלהם שלא עברו הליך התעדה, וזאת כדי לוודא שהם עומדים בהתחייבויות החוזיות שלהם בנושא אבטחת המידע כנדרש במתודולוגיה.

בתשובת גוף 11 מיוני 2023 נמסר כי הספק המהותי שלו אינו מחויב בביצוע ביקורת בהתאם לחוזה שנחתם מולו בשנת 2014, וכי למרות הסכמתו לביצוע ביקורת היא לא יצאה לפועל בשל אילוצי תקציב וקורונה. הגוף הוסיף כי הוא נמצא בעיצומו של מכרז להחלפת הספק הנוכחי שבמסגרתו יידרש הספק החדש לעמוד בביקורת של הגוף.

בתשובת גוף 3 מיוני 2023 נמסר כי בתחילת השנה אגף טכנולוגיות דיגיטליות ומידע החל בהטמעת נוהל שבמסגרתו תבוצע בקרה שנתית על כל ספק המחזיק במאגרי מידע של הגוף באמצעות חברת אבטחת סייבר המוכרת כספק מורשה של גוף 49. בהתאם לנוהל הספקים, המחזיקים במאגרי מידע של הגוף מחויבים לתקן ליקויים, אם יימצאו כאלה בביקורת, וכן מחויבים לעמוד בכל דרישות אבטחת המידע של הגוף כתנאי להמשך פעילותם.

בתשובת גוף 9 וגוף 10 מיוני 2023 נמסר כי בעקבות הפנייה של משרד מבקר המדינה ולאחר ביצוע מיפוי הספקים יתווסף סעיף בנושא זה בהסכמים עתידיים בשיתוף עם הלשכה המשפטית וכן יתבצעו ביקורות ומעקב אחר תיקון ליקויים.

כמו כן נמצא כי 10 (31%) מתוך 32 המשרדים וגופי התמ"ק שענו על השאלה לא ביצעו מעקב שנתי אחר תיקון הליקויים שנמצאו אצל הספקים שלהם כדי לוודא שליקויים אלו תוקנו. בנוסף, גופים כמו גוף 27 וגוף 49 שערכו ביקורות על ספקים, לא העבירו את ממצאי הביקורת ותיקון הליקויים, ככל והיו, ליה"ב. נוכח זאת, ממצאי ביקורת על ספק מסוים שמשרת משרדים וגופי תמ"ק רבים לא מונגשים לכלל הארגונים הרלוונטיים.

מומלץ כי המשרדים וגופי התמ"ק שלא ביצעו ביקורות על הספקים המהותיים שלהם יעשו זאת ויעקבו אחר תיקון הליקויים שנמצאו אצל הספקים. עוד מומלץ כי מערך הסייבר ויה"ב ינחו את המשרדים וגופי התמ"ק להעביר להם את ממצאי הביקורת שביצעו על ספקים שמשרתים ארגונים רבים כדי שיוכלו להנגיש את הממצאים לכלל הארגונים הרלוונטיים.

בתשובת גוף 27 מיוני 2023 נמסר כי הגוף יישם את ההמלצה להעברת הדוחות ליה"ב.

הפעלת סנקציות נגד ספקים

המתודולוגיה מנחה כי אם הספק חורג מהנחיות האבטחה של הארגון, יש להפעיל שיקול דעת בעניין הצעדים שינקטו כנגדו ובמידת הצורך יש להפסיק את ההתקשרות עימו או לנקוט נגדו סנקציות כספיות.

לרשות להגנת הפרטיות יש סמכות אכיפה מינהלתית ופלילית כנגד בעליהם של מאגרי מידע דיגיטליים המכילים מידע אישי שלא עמדו בתקנות אבטחת מידע וכנגד הגורמים המחזיקים במאגרים אלה. למשל: באמצעות מתן הוראה לניתוק מערכות הארגון, מתן הנחיות לתיקון ליקויים, קביעה כי אותו ספק מפר את החוק, או כלי אכיפה אחרים המוקנים לה מכוח סמכויותיה בחוק (כגון התליית רישום מאגר מידע, שמשמעותה היא כי חל איסור לנהל את המאגר או להחזיק בו). פעילות במתווה זה תאפשר למנוע לפחות חלק מהאירועים ואת התממשות הנזק, שהשפעתם על המשק ועל האזרחים עלולה להיות עצומה.

לוח 18: **פעילות הארגונים נגד ספקים שלא עמדו ברמת ההגנה הנדרשת**

השאלה	שיעור הארגונים
האם הארגון פעל כנגד ספקים שלא עמדו ברמת ההגנה הנדרשת בתקופת ההתקשרות עימם?	**17% מהארגונים** **לא נקטו כלל סנקציה נגד ספקים שלא עמדו ברמת ההגנה הנדרשת**

נמצא כי 6 (17%) מתוך 35 המשרדים וגופי התמ"ק שענו על השאלה לא נקטו כלל סנקציה נגד ספקים מהותיים שלא עמדו ברמת ההגנה הנדרשת בתקופת ההתקשרות עימם. ככלל, הימנעות מנקיטה בסנקציות נגד ספק שחרג מהנחיות האבטחה, עלולה לגרום לכך שהספק ימשיך לא לעמוד בדרישות לגבי רמת ההגנה הנדרשת ולסכן גם ארגונים נוספים במשק המשתמשים בשירותיו.

מומלץ כי המשרדים וגופי התמ"ק שלא נקטו סנקציות נגד ספקים שלא עמדו ברמת ההגנה הנדרשת יעשו זאת בעת הצורך בהתאם לתנאי החוזה מול הספק ובמידה שההפרות נוגעות למידע אישי יעבירו את המידע לרשות להגנת הפרטיות כנדרש בתקנות אבטחת מידע והיא תוכל לפעול מול הספק באמצעים העומדים לרשותה כמו ניתוק מערכות הספק, מתן הנחיות לתיקון ליקויים, קביעה כי אותו ספק מפר את החוק, או כלי אכיפה אחרים המוקנים לה מכוח סמכויותיה בחוק.

בתשובת גוף 38 מיוני 2023 נמסר כי הגוף נמצא בעיצומו של מכרז לבחירת ספק, שבמסגרת תפקידו אמור לפעול גם מול ספקים שלא עמדו ברמת ההגנה הנדרשת בתקופת ההתקשרות איתם.

בתשובת גוף 36 מיוני 2023 נמסר כי בכוונתו להוסיף למכרזים סעיף של קנסות או הפסקת התקשרות אם ספק לא עמד ברמת ההגנה הנדרשת בתקופת ההתקשרות עימו.

דיווח על אירועי סייבר המתרחשים אצל הספקים

לפי תקנה 15(א)(2)(ח) לתקנות אבטחת מידע חלה חובה על הספק לדווח לבעל מאגר מידע בהתרחש אירוע אבטחת מידע.

במתודולוגיית שרשרת האספקה נקבע כי יש להגדיר בחוזה עם הספק כי בהתרחש אירוע סייבר אשר עשוי להשפיע על הארגון או על לקוחותיו, מחובתו לעדכן בכך מיד את הלקוח.

בנוסף לדוגמא שצורף להנחיית יה"ב 5.19 נכתב כי בעת אירוע אבטחת מידע או אירוע חריג אצל הספק, בו קיים חשש לגבי דלף מידע של המשרד, הספק מחויב להודיע באופן מידי לאיש הקשר מטעם המשרד.

לוח 19: **מסירת דיווח לארגונים על אירועי סייבר אצל הספק**

השאלה	שיעור הארגונים
האם במכרזים של הארגון יש סעיף שמחייב את הספק להודיע לארגון על כל אירוע סייבר במוצר או בשירות המסופק?	 **14% מהארגונים** **לא כללו במכרזים סעיף שמחייב את הספק להודיע לארגון על כל אירוע סייבר**
האם בשנתיים האחרונות (2021 - 2022) היו בארגון שלך אירועי סייבר שמקורם בשרשרת האספקה?	 **30% מהארגונים** **דיווחו שחוו אירוע סייבר בשנתיים האחרונות שמקורו בשרשרת האספקה**
מי הגורם שממנו נודע לך על אירוע סייבר? (נוגע לארגונים שדיווחו שחוו אירועי סייבר)	 **73% מהארגונים** **לא קיבלו את הדיווח על אירוע סייבר מהספק**

נמצא כי במכרזיהם של 6 (14%) מתוך 43 הארגונים שענו על השאלה אין סעיף שמחייב את הספק להודיע לארגון על כל אירוע סייבר שיש בו כדי לסכן את המוצר או השירות שנרכש.

מומלץ כי משרדים וגופי התמ"ק שאין במכרזיהם סעיף שמחייב את הספק להודיע לארגון על כל אירוע סייבר במוצר או בשירות שנרכש, יוסיפו למכרזיהם סעיף כזה.

בתשובת גוף 38 מיוני 2023 נמסר כי ההמלצה מקובלת עליו ותיושם כחלק מעדכון נספח אבטחת המידע.

בתשובת גוף 14 מיוני 2023 נמסר כי בהתאם להמלצה יעודכן מחדש נוסח סעיף הסייבר במכרזי הרכש באופן שיחייב את הספק לעדכן באופן מיידי על כל אירוע סייבר שהיה בחברתו ויוציא לגוף בתוך 48 שעות ממועד התקיפה דוח סיכום תקיפה אשר יכלול את פרטי האירוע ואופן הטיפול בו.

בתשובת גוף 5 מיוני 2023 נמסר כי מדובר בהערה חשובה מאוד, וכי הנושא יתווסף לנספח הגנה בסייבר של כל חוזה חדש או מתחדש.

נמצא כי 13 (30%) מתוך 44 משרדים וגופי תמ"ק דיווחו שחוו אירוע סייבר בשנתיים האחרונות (בשנים 2021 - 2022) שמקורו בשרשרת האספקה, ואולם 8 (62%) מתוך 13 הארגונים האלו לא קיבלו עדכון על כך מהספק עצמו אלא מגורמים אחרים (כגון מערך הסייבר או אמצעי תקשורת).

מומלץ כי משרדים וגופי תמ"ק שחוו אירוע סייבר ולא קיבלו עדכון על כך מהספק יוודאו כי קיימת דרישת דיווח בחוזה מול הספק וידרשו ממנו לעמוד במחויבותו החוזית. כמו כן מומלץ כי ארגונים אלו יפנו לספק לקבלת פרטים על האירוע ועל אופן הטיפול שלו באירוע.

בתשובת גוף 3 מיוני 2023 נמסר כי באירוע המדובר הספק הפר כמה סעיפים בחוזה, לרבות את חובת הדיווח החלה עליו בעת אירוע סייבר. הגוף בחן אפשרות לנקוט סנקציות, ולחלופין בחן את האפשרות לוודא שהספק מוסיף למערכות הארגון מנגנונים של אכיפה עצמית בנושא. לאחר שהספק הוכיח שהוסיף למערכות הארגון אמצעי אבטחה להגנה על התקפות סייבר, הוחלט לוותר לו על הסנקציות, וזאת בכפוף לביצוע ביקורות עיתיות גם על ידי הגוף.

דיווח ארגונים על אירוע סייבר אצל הספק

כדי לספק תמונה רוחבית במשק נדרש כי הארגונים שהתרחש אירוע סייבר אצל הספק שלהם ידווחו עליו גם לגוף אסדרתי, שכן מידע זה עשוי לסייע לגופים נוספים במשק להיערך לאירועים דומים ולהתגונן מפניהם.

לפי תקנה 11(ד)(1) לתקנות הגנת הפרטיות, על כל מי שבבעלותו מאגר מידע ברמת אבטחה בינונית או גבוהה לפי התקנות, חלה חובת דיווח לרשות להגנת הפרטיות בנוגע לכל אירוע אבטחת מידע חמור כהגדרתו בתקנות אלו.

לוח 20: **דיווח ארגונים למאסדר על אירוע סייבר אצל הספק**

השאלה	שיעור הארגונים
האם דווח על האירוע למערך הסייבר?	**38% מהארגונים לא דיווחו למערך הסייבר על אירוע סייבר שהתרחש אצל הספק**

נמצא כי 5 (38%) מתוך 13 המשרדים וגופי התמ"ק שענו על השאלה ודיווחו שהתרחש אצל הספק שלהם אירוע סייבר לא דיווחו על כך למערך הסייבר. בהיעדר דיווחים כאמור, מערך הסייבר לא יוכל להתריע על כך לפני ארגונים נוספים שעלולים להיות חשופים לפגיעה בגין אותו אירוע.

מומלץ כי משרדים וגופי תמ"ק שחוו אירוע סייבר ידווחו למערך הסייבר וגם לרשות להגנת הפרטיות על מקרים שבהם האירוע היה חמור כהגדרתו בתקנות אבטחת מידע. עוד מומלץ כי מערך הסייבר, יה"ב, הרשות להגנת הפרטיות ומינהל הרכש יפתחו מנגנון אחוד לקבלת דיווח על אירוע סייבר מהארגונים, וכי במתודולוגיה בנושא שרשרת האספקה תתווסף חובת דיווח באמצעות מנגנון זה, באופן שבו כל גוף אסדרתי יקבל מידע על האירוע ויוכל לטפל בו בהתאם לסמכויות שלו.

בתשובת מערך הסייבר מיוני 2023 נמסר כי ההמלצה מבורכת, וכי גישת ה-CERT היא שיש לדווח להם על כל אירוע.

בתשובת מינהל הרכש מיוני 2023 נמסר כי הוא לא קיבל דיווחים מסודרים לגבי אירועי סייבר הנובעים ממכרזיו, מהגופים המזמינים או מהגופים האסדרתיים. למינהל הרכש כלי אכיפה יעילים נגד ספקים שלו בכל התחומים הקשורים לביצוע ההתקשרות, ואם התקבלה הערה כאמור, תתבצע אכיפה יעילה למנוע את הישנותם של מקרים כאמור.

תיעוד אירועי סייבר אצל הספק

לפי תקנה 11(א) בעל מאגר מידע אחראי לתיעוד כל מקרה שבו התגלה אירוע המעלה חשש לפגיעה בשלמות המידע, לשימוש בו בלא הרשאה או לחריגה מהרשאה.

לפי מדד יה"ב[65] על המשרד לנהל במרוכז הן דיווחים על אירועי סייבר והן מידע על אירועים אלה לצורך קבלת תמונת מצב אחידה ומלאה על אופי האירוע ולצורך הערכת סיכונים. תיעוד

65 בקרת יה"ב 1.18, יש לתעד אירועי אבטחת מידע, את תהליכי הטיפול באירוע לרבות איסוף מידע, פעולות שבוצעו ומסקנות.

אירועי סייבר המתרחשים אצל הספק נדרש לצורך קבלת תמונת המצב המלאה על השפעות האירוע על הארגון עצמו ועל ארגונים נוספים במשק.

לוח 21: **תיעוד אירועי סייבר בארגונים**

השאלה	שיעור הארגונים
האם אתה מתעד את אירועי הסייבר שקרו אצל כל ספק שנותן לך שירות בתחום התקשוב והסייבר ואצל ספקים שיש להם גישה למידע רגיש של הארגון?	**23% מהארגונים אינם מתעדים את אירועי הסייבר שהתרחשו אצל הספקים**

נמצא כי 3 (23%) מתוך 13 המשרדים וגופי התמ"ק שענו על השאלה אינם מתעדים את אירועי הסייבר שהתרחשו אצל כל ספק שנותן להם שירות בתחום התקשוב והסייבר ואצל ספקים שיש להם גישה למידע רגיש של הארגון. בהיעדר תיעוד ובלא שמופקות התובנות הנדרשות, אירוע כזה עלול להישנות.

מומלץ כי המשרדים וגופי התמ"ק יתעדו את אירועי הסייבר שהתרחשו אצל כל ספק שנותן להם שירות בתחום התקשוב והסייבר ואצל ספקים שיש להם גישה למידע רגיש של הארגון ויפיקו ממנו את התובנות הנדרשות כדי למנוע הישנות אירועים מסוג זה.

שיתוף פעולה בין הגופים האסדרתיים בתחום שרשרת האספקה

רשות האסדרה במשרד ראש הממשלה הוקמה מכוח חוק עקרונות האסדרה, התשפ"ב -2021. בין היתר, הרשות אמונה על יישום והטמעה של מדיניות "רגולציה חכמה" במשרדי הממשלה ומנחה את המשרדים השונים בביצוע תוכנית להפחתת הנטל הרגולטורי ולהטמעת מתודולוגיית הערכת השפעות הרגולציה (RIA) בהתאם להחלטת הממשלה 2118[66].

בהחלטת ממשלה 2443[67] נקבע כי על מערך הסייבר להקים תת-ועדה בהשתתפות נציגים מאגף החשב הכללי, מיה"ב, משירות הביטחון הכללי וממשרד הכלכלה, שתגבש מתווה ועקרונות בנוגע לאופן רכישתם של שירותים ומוצרים תוך שימוש בתקינת אבטחת מידע במערכות הממשלתיות, בתוך 180 יום מיום קבלת החלטה זו.

66 החלטת הממשלה 2118, "הפחתת הנטל הרגולטורי" (22.10.14).

67 החלטת ממשלה 2443 , נספח ז' סעיף א1.

יש במשק כמה מתודולוגיות ותקנים בתחום הגנת הסייבר בכלל ובתחום שרשרת האספקה בפרט. מלבד מערך הסייבר קיימים גופים אסדרתיים מדינתיים נוספים כמו שב"כ, מלמ"ב והרשות להגנת הפרטיות שלכל אחד תקן והנחיות משלו הנוגעות לנושא שרשרת האספקה.

מלמ"ב נמצא בתהליך אימוץ של תקן בין-לאומי CMMC בנושא שרשרת האספקה, באופן שבו משרד ההגנה האמריקני יכיר בכל ספק ישראלי העומד בתקן מלמ"ב כספק העומד גם בתקן ה-CMMC. לפי תקן זה, תהליך בדיקת הספקים (תהליך ההתעדה) יבוצע על ידי מעריכים חיצוניים שיוסמכו לכך על ידי גוף שקיבל את אישור מלמ"ב (בדומה למאגר הספקים המורשים שהקים מערך הסייבר ולמכונים שמכשירים את היועצים מטעמו), ואילו מלמ"ב יוכל לאשר את תוצרי התהליך ולבצע בקרה עליהם. זאת לעומת המתודולוגיה של המערך שלפיה גוף ההסמכה מבצע את תהליך האישור עבור מערך הסייבר בלי שהמערך מעורב בכך.

בפגישות שקיים צוות הביקורת עם הגופים האסדרתיים הפועלים בתחום שרשרת האספקה עלה הצורך בהקמת פורום מקצועי בנושא שרשרת האספקה שיביא לשיתוף מידע בתחום ויאפשר לייצר שיתופי פעולה בין הארגונים השונים, למשל לצורך התעדת ספקים משותפים.

בהצגת מתודולוגיית שרשרת האספקה[68] נאמר כי אחד העקרונות העומדים בבסיס המתודולוגיה הוא תיאום בין הגופים האסדרתיים. הוסבר כי המתודולוגיה תתבסס על מדיניות המולטי-רגולציה, ולפיה יבוצע תכלול בין הדרישות שמצופה מהספק לעמוד בהן ובין הדרישות המוגדרות בתקנים וברגולציות מקומיות ובין-לאומיות. לדוגמה: תקן CMMC; דרישות שגופי התמ"ק נדרשים לעמוד בהן; חוזר הפיקוח על הבנקים בנושא שרשרת אספקה; תקן ISO27001; ותקנות הגנת הפרטיות (אבטחת מידע), התשע"ז-2017.

עוד צוין בהצגת המתודולוגיה כי לתכלול בין המתודולוגיה של מערך הסייבר ובין הדרישות של תקנות הגנת הפרטיות יש חשיבות יתרה, מאחר שזהו מכפיל כוח ולפיכך הוא עשוי להקל על ארגונים. כמו כן, הוצגה התפיסה ולפיה גופים אסדרתיים ישתתפו במהלך באופן שהנטל על המשק יפחת. הוסבר כי מתבצעות פעולות מול כמה גופים אסדרתיים (רשות שוק ההון, מחלקת הפיקוח על הבנקים).

בפגישה שקיים צוות הביקורת עם מלמ"ב בפברואר 2023 נאמר כי נכון למועד הפגישה מובילי האסדרה בתחום שרשרת האספקה בכל אחד מהגופים האסדרתיים אינם משתפים ביניהם מידע וידע באופן שוטף, למשל: בנוגע לתובנות על אופן היישום של המתודולוגיה. עקב כך מוכפל העומס הבירוקרטי המוטל על הספק, היות שלעיתים הספק ייתן שירות גם למלמ"ב וגם למשרד ממשלתי ולכן יהיה מחויב לעמוד בדרישות שנקבעו בשתי המתודולוגיות אף שהן כוללות בקרות בתחומים דומים. בפגישה הציעו מלמ"ב, למשל, כי יש לתכלל בין הבקרות שנקבעו במתודולוגיות השונות באופן שספק של אחד הגופים האסדרתיים שכבר ביצע התעדה יידרש לבצע ביקורת רק בתחומים שהמאסדר השני לא ביצע עליהם ביקורת.

עוד הוצע להקים מערכים משותפים לכל הגופים האסדרתיים בתחום זה. למשל, מאגר בודקי ספקים שישתתפו בהכשרות שאושרו בידי שני הארגונים, בתי ספר משותפים לביצוע ההכשרות. באופן כזה ישרור אמון בין הארגונים בנוגע למקצועיות הבודקים שנכללים במאגר והם יוכלו

68 מערך הסייבר, הצגת פרויקטים יובל ומודול שרשרת אספקה, דיון מ-6.5.2018.

לסמוך על בדיקות ובקרות המשותפות לשתי המתודולוגיות. מלמ"ב ומערך הסייבר אף התחילו בתהליך של גיבוש טיוטה בנושא.

נמצא כי הגופים האסדרתיים (מערך הסייבר, יה"ב, שב"כ, מלמ"ב, הרשות להגנת הפרטיות, יחידות הסייבר המגזריות) ומינהל הרכש קבעו דרישות שונות בנושא שרשרת האספקה ללא תיאום ותכלול של הדרישות. מצב זה אינו עולה בקנה אחד עם החלטת הממשלה 2118 מאוקטובר 2014, שמטרתה להפחית את הנטל הרגולטורי. כמו כן נמצא כי לא נוצרו שיתופי פעולה בין הגופים האסדרתיים השונים כדי לבחון את האפשרות לשיתוף משאבים ביניהם ולבניית מערכים משותפים וכן לשתף מידע וידע בתחום.

מומלץ כי מערך הסייבר יפעל לכינוס כל הגופים האסדרתיים המטפלים בתחום שרשרת האספקה (מערך הסייבר, יה"ב, שב"כ, מלמ"ב, הרשות להגנת הפרטיות, יחידות הסייבר המגזריות) ומינהל הרכש כדי לבצע תכלול בין המתודולוגיות השונות, לדון בנושאים משותפים כמו תקינה בין-לאומית, לבדוק את האפשרות להשקעת משאבים משותפת, ליצירת מערכים משותפים ולהקמת פורום מקצועי בנושא שרשרת האספקה.

בתשובת מערך הסייבר מיוני 2023 נמסר כי בימים אלו הוא החל במגעים ליצירת שיח משותף עם כלל הגופים הביטחוניים, בשלב הראשון, לתיאום המתודולוגיות. בין היתר דובר על העברת ידע על התמודדות בתחום והעברת המתודולוגיה של המערך אליהם לצורך בחינת האפשרות שהם יאמצו אותה. כמו כן, בהמשך דובר על קיום מפגשים עם כלל הנציגים הרלוונטיים של הגופים הביטחוניים לצורך גיבוש דרך התמודדות משותפת.

בתשובת השב"כ מיולי 2023 נמסר כי למרות שלפי סעיף 21 להחלטת הממשלה 4398 החלטת הממשלה 2118 לא תחול על הנחיות או הוראות לפי החוק להסדרת הביטחון בגופים ציבוריים, מקובלת עליו ההמלצה לכנס את כלל הגופים האסדרתיים על מנת לייצר מתודולוגיה ושפה אחידה תוך צמצום כפילויות ובירוקרטיה מיותרת.

בתשובת מינהל הרכש מיוני נמסר כי מסגרת מחייבת לרכש צריכה להיכתב על ידי הגורם המקצועי לגבי הרכש הממשלתי. זאת מכיוון שגורם זה מכיר את כלל השיקולים הנוגעים לרכש הממשלתי.

אשר לתשובות הגופים האסדרתיים בתחום הסייבר, יצוין כי גופים אלו צריכים לקבוע את הדרישות בתחום הסייבר בנוגע לשרשרת האספקה, וזאת תוך שיקולים מידתיים ומתוך הבנה שעודף דרישות ישליך על עלות הרכש ועל כמות המתחרים.

סיכום

איום הייחוס לתקיפת סייבר באמצעות שרשרת האספקה הוא אחד האיומים המשמעותיים על ארגונים במשק. 86% מ-43 המשרדים וגופי התמ"ק שהשיבו על השאלון ציינו כי תקיפה באמצעות שרשרת האספקה היא איום ייחוס שלהם, וכ-30% מהמשרדים וגופי התמ"ק שהשיבו על השאלון דיווחו שחוו אירוע סייבר בשנתיים האחרונות (בשנים 2021-2022) שמקורו בשרשרת האספקה. האתגר בהתמודדות עם איום זה נובע מהעובדה שההגנה הנדרשת אצל הספק היא לכאורה מחוץ לתחום סמכותו של הארגון.

מדוח זה עולה כי יש ספקים שנותנים שירות לעשרות משרדי ממשלה וגופי תמ"ק, ולכן פגיעה בהם עשויה לפגוע פגיעה נרחבת ברציפות התפקודית של הממשלה והמשק.

מערך הסייבר כגוף אסדרתי שאחראי לקדם את רמת הגנת הסייבר במשק גיבש בשנת 2018 מתודולוגיה לניהול האיום הנשקף משרשרת האספקה. ממצאי דוח זה, אשר ביסודו עומדת בחינה של יישום המתודולוגיה של מערך הסייבר במשרדי ממשלה, בגופי תמ"ק וביחידות הסייבר המגזריות, מעידים על כמה פערים הנוגעים לנושא, כמפורט להלן:

1. כשש שנים לאחר שמערך הסייבר גיבש את המתודולוגיה בנושא שרשרת האספקה היא לא מוטמעת במשק, ויש ארגונים שטוענים שאי אפשר ליישמה. נמצא כי 55% מהמשרדים וגופי התמ"ק שהשיבו על השאלון אינם עובדים לפי מתודולוגיית שרשרת האספקה, ונוכח זאת חלק גדול מהספקים של הארגונים אינם נבדקים בצורה אחודה ובהתאם לבקרות שהגדיר מערך הסייבר.

2. נמצאו פערים משמעותיים ביישום המתודולוגיה שלא ניתן להם מענה על ידי מערך הסייבר, כמו חוסר יכולת ליישם הדרישות מול ספקים בין-לאומיים, עלויות גבוהות של התעדה ותהליך התעדה ארוך שאינו בהלימה לצרכים העסקיים של הארגון.

3. מהדוח עולה כי למשרדי ממשלה יש 18 ספקים עיקריים בתחום התקשוב והסייבר שנותנים שירותים למשרדים ולגופי תמ"ק רבים - מתוכם חמישה ספקים נותנים שירות ליותר מ-49 משרדי ממשלה וגופי תמ"ק, ושלושה ספקים נותנים שירות בהיקף כספי שנתי של יותר מ-327 מיליוני ש"ח. ספקים אלו אינם מותעדים, ועל חלקם לא מתבצעות בקרות בתחום שרשרת האספקה - דבר שמסכן את הארגונים שהם נותנים להם שירות. כמו כן, הגופים האסדרתיים בתחום הסייבר (מערך הסייבר ויה"ב) אינם פועלים למיפוי ספקים אלו ולקידום ההתעדה שלהם.

4. מינהל הרכש אינו מונחה על ידי שום גוף אסדרתי בתחום הסייבר. כמו כן, במכרזים המרכזיים אין דרישה של מינהל הרכש מהספקים שעימם הוא מתקשר ליישם את מתודולוגיית שרשרת האספקה ודרישות אבטחה נוספות שהגופים האסדרתיים דורשים מהמשרדים, אף שהיקף הכספי של התקשרויות אלו הוא בממוצע כ-57% מכלל ההתקשרויות של המשרדים בתחום התקשוב והסייבר. נוסף על כך שום גורם אינו מבצע ביקורות על רמת הגנת הסייבר של הספקים שזכו במכרזים מרכזיים.

5. הממונה על הגנת הסייבר במשרדי הממשלה ובגופי התמ"ק אינו מעורב בתהליכי הרכש בתחום התקשוב והסייבר בארגון ובכלל זה אינו מעורב בתהליך סיום

ההתקשרות עם הספק כדי לוודא שהספק ממלא את חובותיו בנושא סיום ההתקשרות (מחיקת המידע, החזרת האמצעים, ניתוק גישה מרחוק ועוד).

6. משרדים וגופי תמ"ק דיווחו שחוו אירוע סייבר בשנתיים האחרונות (בשנים 2022-2021) שמקורו בשרשרת האספקה, ואולם הם לא קיבלו עדכון על כך מהספק עצמו אלא מגורמים אחרים (כגון מערך הסייבר או אמצעי תקשורת). כמו כן, מינהל הרכש אינו מחייב את הספקים שזכו במכרזים מרכזיים לדווח על אירועי סייבר גם למערך הסייבר.

7. הגופים האסדרתיים השונים בתחום הסייבר (מערך הסייבר, יה"ב, שב"כ, מלמ"ב, הרשות להגנת הפרטיות, יחידות הסייבר המגזריות) ומינהל הרכש מתווים מתודולוגיות שונות בתחום שרשרת האספקה ולא מתבצע תכלול של הדרישות, ועקב כך נוצר נטל רגולטורי על הארגונים והספקים.

מכלול הפערים האמורים מחייבים הערכת מצב לגבי המענה המתודולוגי הקיים ודרך מימושו, שכן ממצאיו מלמדים כי נשקף סיכון ממשי לגופי תמ"ק, למשרדי ממשלה ולמגזרים מצד שרשרת האספקה בתחום התקשוב. על מערך הסייבר והגופים האסדרתיים בתחום הסייבר ומינהל הרכש לפעול לקיום הערכת מצב זו. בד בבד על כלל הארגונים שנבדקו לפעול, כל אחד על פי תחום אחריותו, לתיקון הליקויים שהועלו בדוח זה על מנת להבטיח שיפור ברמת ההגנה של הספקים ושל המשק כולו.

במהלך הביקורת עדכנו מערך הסייבר הלאומי ויה"ב את הנחיותיהם למשרדים ולגופי התמ"ק, בין היתר כדי לתת מענה על פערים שהוצגו בדוח זה. מוצע אפוא כי מערך הסייבר ויה"ב יעקבו כבר במהלך השנה הקרובה אחר אופן הטמעת המתודולוגיה העדכנית ואחר ישימותה הלכה למעשה.