

דוח מבקר המדינה | שבט התשפ"ד | ינואר 2024



נושאים מערכתיים

# ניהול סיכונים 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 במערכת חברת הביטוח; באוקטובר 2021 - דלף מידע רגיש של מיליון פרופילים באתר היכריות של הקהילייה הגאה עקב פגיעה בספק שנתן לאתר ההיכריות ולאתרים אחרים שהתארחו אצלו שירותי אירוח ואחסון של אתרים.

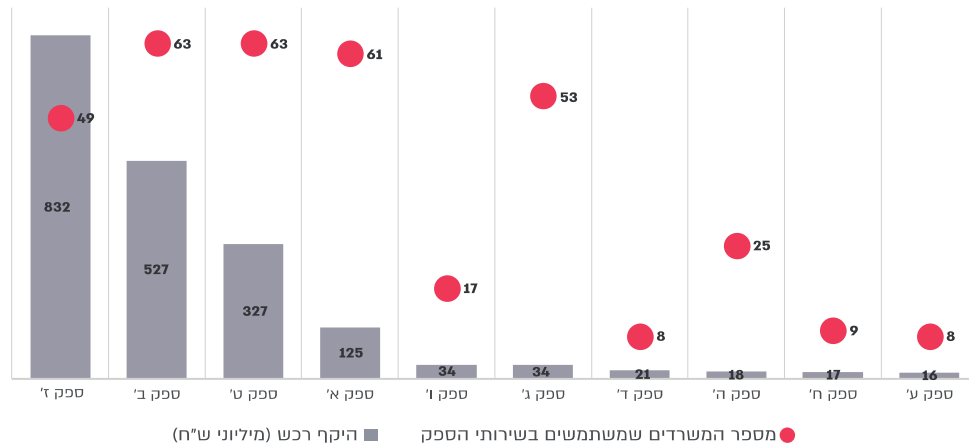
משרדי ממשלה וגופים שהם תשתיות מדינה קריטיות<sup>1</sup> (גופי תמ"ק) נדרשים להתמודד עם הסיכון הנובע משרשרת האספקה באמצעות הכללת דרישות בתחום הגנת הסייבר במסגרת הליכי המכרז וההתקשרות.

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 מיליון 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<sup>2</sup> 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.



## שלבי מתודולוגיית שרשרת האספקה של מערך הסייבר

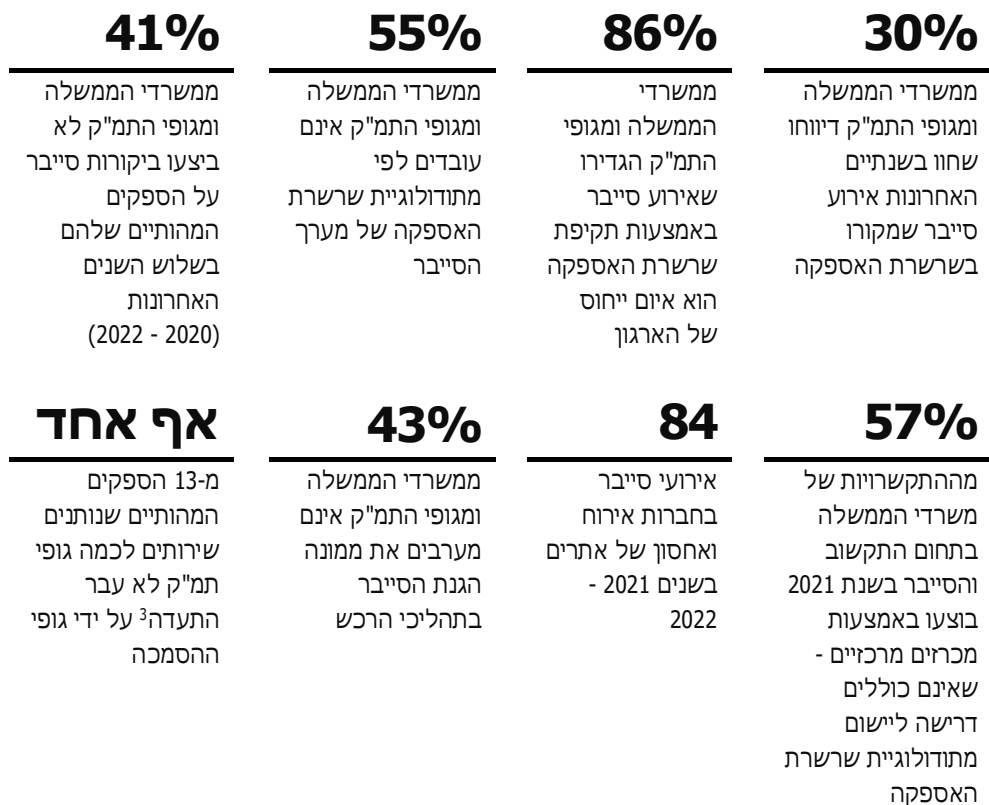


המקור: מערך הסייבר.



**נתוני מפתח**

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



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 לאשרר את הדיווח ולהנפיק לספק תעודת הסמכה שתהיה תקפה לשנתיים או לא לאשרר את הדיווח ולבקש ממנו לבצע תיקון ליקויים.



## פעולות הביקורת

בחודשים פברואר 2022 עד מאי 2023 בדק משרד מבקר המדינה את נושא ניהול סיכונים 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 הבדק 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 תמ"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 תמ"ק שהופץ אליהם השאלון (משרדי הממשלה וגופי תמ"ק שענו על השאלון מסומנים בהדגשה): **גוף 1, מינהל התכנון, גוף 2, משרד האנרגיה 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 לבקורות 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 הבקורות הקיימות בשאלון הספקים ללא אפשרות לתת מענה באמצעות בקורות 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 במתודולוגיית 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 בטיטוט 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 רחבית 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 במכרזים 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 השימות 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 בצ"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 בבקורות 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.

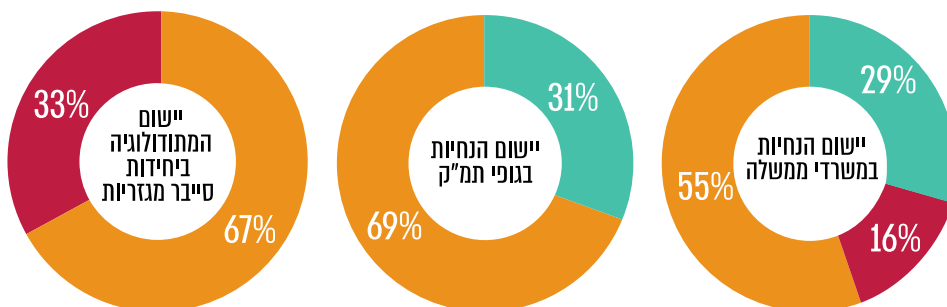
מומלץ כי אגף החשכ"ל במשרד האוצר יעדכן את הוראות התכ"ם הרלוונטיות באופן שהן יחייבו את המשרדים לערב את ממונה הגנת הסייבר או את ממונה שרשרת האספקה



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 המכרה 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



■ מיישמים באופן מלא ■ מיישמים באופן חלקי ■ אינם מיישמים

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.

נושאים שנבדקו	גוף 19	גוף 2	גוף 11	גוף 21	גוף 1	גוף 43	גוף 20	גוף 15	גוף 45	גוף 5	גוף 16	גוף 39	גוף 38
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 הנכלל את כל פרטי המידע הנדרשים במתודולוגיה	✓	✓	✓	✓	✓	✓	✗	✓	✓	✓	✗	✗	✗
מיפוי בעל תפקיד ייעודי לנושא שרשרת האספקה	✓	✓	✓	✓	✓	✓	✗	✓	✓	✓	✗	✗	✗
סיוע של הגורם המאסדר בתהליך מיפוי הספקים	✓	✓	✓	✓	✓	✓	✗	✓	✓	✓	✗	✗	✗
ביצוע בקורת 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 בשיחת המסופק	✓	✓	✓	✓	✓	✓	*	*	*	*	✓	✗	✗
הפעלת סנקציה נגד ספקים שלא עמדו ברמת ההגנה הנדרשת בתקופת ההתקשרות	✓	✓	✓	✓	✓	✓	*	*	*	*	✓	✗	✗
עבודה לפי מתודולוגיית שרשרת האספקה של מערך הסייבר	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✗	✗	✗
סעיף במכרז שמחייב לארגון לבצע ביקורת סייבר אצל הספק	✓	✓	✓	✓	✓	✓	✓	✓	✓	✗	✓	✗	✗
נושא שרשרת האספקה נדון במסגרת ועדות היעוץ	✓	✓	✓	✓	✓	✓	✗	✓	✓	✓	✓	✗	✗
קיום ספק מזהיני בארגון	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✗	✗
ביצוע תרגולים לתקיפת סייבר באמצעות שרשרת האספקה	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✗	✗
מעורבות ממונה הגנת הסייבר או הממונה על שרשרת האספקה בתהליכי הרכש	✓	!	✓	!	✓	!	!	!	!	!	!	!	!
יישום ההנחיות של הגורם המאסדר	✓	!	✓	!	✓	!	!	!	!	!	!	!	!
<b>שיעור הנושאים שהגופים יישמו באופן מלא או חלקי</b>	<b>90%</b>	<b>85%</b>	<b>85%</b>	<b>85%</b>	<b>80%</b>	<b>80%</b>	<b>75%</b>	<b>75%</b>	<b>75%</b>	<b>65%</b>	<b>60%</b>	<b>55%</b>	<b>40%</b>

✓ 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 2021-2022) שמקורו בשרשרת האספקה. האתגר בהתמודדות עם איום זה נובע מהעובדה שההגנה הנדרשת על הספק היא לכאורה מחוץ לתחום שמכותו של הארגון.

מדוח זה עולה כי יש ספקים שנותרו 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, ונכח זאת חלק גדול מהספקים של הארגונים אינם נבדקים בצורה אחודה ובהתאם לבקורות 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 שנותרו שירותים לארגונים רבים - מתוכם חמישה ספקים נותרו ליותר מ-49 משרדים, ושלושה ספקים נותרו שירות בהיקף כספי שנתי של יותר מ-327 מיליוני ש"ח. ספקים אלו אינם מותעדים, ועל חלקם לא מתבצעות בקורות בתחום שרשרת האספקה - דבר שמסכן את הארגונים שהם נותרו 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 תמ"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 מימוש, 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.

