

היערכות גופים חיוניים להגנת הסייבר

תקציר

רקע כללי

על המערך הוטל
לבנות ולחזק את
חוסנו של כלל
המשק להתמודדות
עם התקפות סייבר

המרחב הקיברנטי, הנקרא מרחב הסייבר, מאפשר זרימה חופשית של מידע, הון ושירותים במערכות תקשורת, מחשוב ובקרה, ברשתות ועוד. פעילויות רבות, ובהן סחר קמעונאי, שירותים פיננסיים ותהליכי ייצור, מתבצעות כיום במרחב הסייבר. בד בבד עם התפתחות מרחב הסייבר ניכרת עלייה של ממש בשכיחותם של איומי סייבר ובחומרתם.

משרד מבקר המדינה נדרש בעבר לנושא מרחב הסייבר על היבטיו השונים, ופרסם כמה דוחות ביקורת¹ בנושאים הללו: מעקב אחר אבטחת מידע והגנת הפרטיות, המשכיות עסקית של המערכת הפיננסית, אבטחת תשתיות אינטרנט ומחשוב, היערכות המדינה להגנת המרחב הקריטי, והתמודדות משטרת ישראל עם פשיעת סייבר.

בשנת 2002 קיבלה ועדת השרים לענייני ביטחון לאומי החלטה בנושא "אחריות להגנה על מערכות ממוחשבות במדינת ישראל" (להלן - החלטה 84/ב), שבה הוסדר הטיפול בהגנה על מערכות ממוחשבות חיוניות מפני תקיפות סייבר. כמו כן, הוקמה ועדת היגוי עליונה להגנה על מערכות ממוחשבות במדינת ישראל (להלן - ועדה 84/ב), שעיקר תפקידה הוא להתוות מדיניות כוללת להגנה על מערכות ממוחשבות בישראל. האחריות להנחיית גופים אשר להם מערכות ממוחשבות חיוניות (להלן - גופי תמ"ק²) הוטלה על שירות הביטחון הכללי (להלן - השב"כ), בהתאם לחוק להסדרת הביטחון בגופים ציבוריים, התשנ"ח-1998 (להלן - חוק הסדרת הביטחון או החוק).

בשנת 2011 קיבלה הממשלה החלטה³ על הקמת המטה הקיברנטי הלאומי במשרד ראש הממשלה כחלק מקידום היכולת הלאומית במרחב הסייבר.

- 1 **דוח שנתי 62** (2012), "אבטחת מידע והגנת הפרטיות ברשויות המקומיות, מעקב מורחב", עמ' 301; **דוח שנתי 64 א** (2014), "בניית תכניות להמשכיות עסקית של המערכת הפיננסית באירועי חירום", עמ' 51; מבקר המדינה, **דוח שנתי 64 ג** (2014), "אבטחה פיזית ושרידות של תשתיות אינטרנט ומחשוב עבור משרדי ממשלה", עמ' 1585; **דוח שנתי 67 א** (2016), "היבטים בהיערכות המדינה להגנת המרחב הקיברנטי", עמ' 5; **דוח שנתי 67 ב** (2017), "התמודדות משטרת ישראל עם פשיעת סייבר מתוחכמת", עמ' 1,581.
- 2 תמ"ק - תשתיות מחשוב קריטיות. בחוק המונח הוא מערכות ממוחשבות חיוניות, ואילו בתורת הלחימה למערכות ממוחשבות המונח הוא "תשתיות מחשוב קריטיות". ב"גופי תמ"ק" הכוונה לגופים שנכללו בתוספת השנייה או החמישית לחוק.
- 3 החלטת ממשלה 3611 מ-7.8.11.



תמונת המצב
שהייתה קיימת בידי
המערך לא שיקפה
את רמת מוכנות
הגופים להתמודד
עם התקפות סייבר

בשנת 2015 החליטה הממשלה⁴ על הקמת מערך הסייבר הלאומי (להלן - המערך)⁵. על המערך הוטל, בין היתר, לבנות ולחזק את חוסנו של כלל המשק להתמודדות עם התקפות סייבר. עוד נקבע בהחלטה כי המערך יקבל את האחריות להנחיית גופי תמ"ק.

פעולות הביקורת

בחודשים יולי 2017 עד יולי 2018 (להלן - מועד סיום הביקורת) בדק משרד מבקר המדינה את היערכותם של גופי תמ"ק, משרדי ממשלה, יחידות סמך ויחידות הכוונה מגזריות במשרדי ממשלה לאירועי סייבר. בנוסף נבדקו פעולות המערך והיחידה להגנת סייבר בממשלה (להלן - יה"ב). בדיקות השלמה נעשו בשב"כ.

ועדת המשנה של הוועדה לענייני ביקורת המדינה של הכנסת החליטה שלא להניח על שולחן הכנסת ולא לפרסם חלקים מפרק ביקורת זה לשם שמירה על ביטחון המדינה, בהתאם לסעיף 17 לחוק מבקר המדינה, התשי"ח-1958 [נוסח משולב].

הליקויים העיקריים

היערכות גופי תמ"ק - מערך הסייבר הלאומי

שירות הביטחון הכללי כתב את תורת הלחימה (להלן - תו"ל) למערכות הממוחשבות. שירות הביטחון הכללי הנחה את גופי התמ"ק עד להעברת האחריות על הגופים למערך במרץ וביוני 2017.

במערך עוסקים בהנחיה שוטפת של גופי התמ"ק ובמיפוי מכלול האיומים על מערכותיהם. הנחיית גופי תמ"ק כוללת בניית תוכנית לסגירת הפערים והטמעת המענה האבטחתי.

עד מועד סיום הביקורת הסמיך המערך רק חלק מגופי תמ"ק כעומדים בהנחיות הנדרשות בהתאם לתו"ל, ותמונת המצב שהייתה בידי המערך לא שיקפה את רמת מוכנות הגופים להתמודד עם התקפות סייבר. לאחר מועד סיום הביקורת הציג המערך בפני משרד מבקר המדינה תמונת מצב מקיפה ועדכנית.

4 החלטת ממשלה 2444 "קידום היערכות לאומית להגנת הסייבר" והחלטה 2443 "קידום אסדרה לאומית והובלה ממשלתית בהגנת הסייבר" מ-15.2.15.

5 בהחלטה זו הוקמו שני גופים: רשות הסייבר הלאומית והמטה הקיברנטי הלאומי היוזם את מערך הסייבר הלאומי. בדצמבר 2017 אוחדו שני הגופים לגוף אחד - מערך הסייבר הלאומי.

היערכות גופי תמ"ק - גוף תמ"ק א'

אף שגוף תמ"ק א' הוא גוף מונחה מזה שנים, המצב עדיין אינו משביע רצון. טיוטת מיפוי שהכין גוף תמ"ק א' ב-2015 לא כללה רכיבים הנדרשים בתו"ל. המיפוי שנעשה לא היה עדכני ולא שיקף את תמונת המערכות בצורה מהימנה.

לפי תו"ל נדרש גוף מונחה לכתוב נהלים בכמה נושאים. נמצאו פערים בין הנהלים הקיימים ובין דרישות ההנחיה. חלק מפקודות המבצע לא עודכנו כנדרש בתו"ל.

בביקורת נמצאו פערים, בין היתר, בדיווחים למערך על אירועים ובנושאים נוספים. בשנת 2016 נעשתה ביקורת מקיפה של שירות הביטחון הכללי בגוף תמ"ק א'. עד מועד סיום הביקורת לא השלים הגוף את תיקון חלק מהליקויים.

היערכות גופי תמ"ק - גוף תמ"ק ב'

בניגוד להנחיות תו"ל, מסמך המדיניות ופק"ם חירום לא תוקפו כנדרש. עד מועד סיום הביקורת לא הוטמע רכיב הגנה מסוים.

היערכות גופי תמ"ק - גוף תמ"ק ג'

חלק מהנהלים הנדרשים בתו"ל אינם קיימים בגוף תמ"ק ג'. פק"ם החירום בגוף תמ"ק ג' לא תוקף, על פי המועדים הנדרשים בתו"ל. עוד נמצא כי אין בגוף תמ"ק ג' פק"ם התאוששות.

היערכות משרדי הממשלה ויחידות הסמך

בהחלטת הממשלה 2443 מפברואר 2015 הוחלט על הקמת יה"ב אשר תפעל לשיפור רמת הגנת הסייבר, תכנון ותנחה את משרדי הממשלה ואת יחידות הסמך. רשימת הגופים המונחים על ידי יה"ב כוללת מספר גופים (להלן - רשימת הגופים): משרדי ממשלה ויחידות סמך; שתי יחידות סמך לא נכללו ברשימת הגופים של יה"ב.

עוד הוחלט כי משרדי הממשלה ויחידות הסמך נדרשים למנות בעל תפקיד האחראי להגנת הסייבר במשרד (להלן - ממונה הגנת הסייבר); להקים ועדת היגוי משרדית שתתכנס פעם בחציון לפחות; למנות מנהל הגנת הסייבר ביחידות מערכות המידע, ולפעול לכך שהן יעמדו בתקני אבטחת מידע


 חלק משרדי
 הממשלה ומיחידות
 הסמך לא השלימו
 את ההיערכות
 הנדרשת לפי
 החלטות הממשלה
 והנחיות יה"ב

ארגוניים⁶. יה"ב פרסמה מספר הנחיות בתחום הגנת הסייבר, בין היתר, בנושא
 המסגרות הארגוניות, ניהול סיכוני סייבר והקשחת מערכות ההפעלה. עוד
 נקבע כי יה"ב בשיתוף המערך יקימו מרכז שליטה ובקרה ממשלתי לאיומי
 סייבר - ה-SOC הממשלתי.

מנתונים שהתקבלו מיה"ב, עולה כי: לא כל היחידות מינו מנהל הגנת סייבר;
 רק חלק משרדי הממשלה הוסמכו לתקן 27001; לחלק משרדי הממשלה
 ויחידות הסמך אין מסמך מדיניות אבטחת מידע וסייבר; חלק משרדי
 הממשלה ויחידות הסמך טרם השלימו את תהליך סקר הסיכונים; חלק
 משרדי הממשלה ויחידות הסמך חוברו ל-SOC הממשלתי.

היערכות משרדי הממשלה להכוונה מגזרית

בהחלטת ממשלה 2444 מפברואר 2015 נקבע לראשונה כי המדינה תאסדר
 את המרחב האזרחי. הוחלט כי משרדי ממשלה יקימו בתוכם יחידות להכוונה
 מגזרית, והן יפעלו לשיפור ההגנה במגזרי המשק השונים. עוד נקבע בהחלטה
 כי על המערך ועל הלשכה המשפטית במשרד ראש הממשלה בשיתוף משרד
 המשפטים להכין תזכיר חוק הגנת הסייבר ולהביאו לאישור ראש הממשלה
 בתוך חצי שנה מיום קבלת ההחלטה.

בהחלטה 2443 מפברואר 2015 הטילה הממשלה על המנכ"לים של משרדי
 הממשלה לקדם את הטיפול בהיערכות לאיומי סייבר במסגרת המגזר⁷ שבו
 הם פועלים, על ידי הקמת יחידות להכוונה מגזרית והכנת עבודת מטה
 לבחינת התיקונים והשינויים המשפטיים הנדרשים. בהחלטה נקבע כי היחידה
 תהיה כפופה למשרד הממשלתי שהיא שייכת אליו, בהתאם לסמכויות
 הרגולציה שלו, ותפעל על פי הנחיה מקצועית של המערך.

פערים בתשתית משפטית לתחום הגנת הסייבר

מערך הסייבר הכין תזכיר של חוק הגנת הסייבר ומערך הסייבר הלאומי,
 התשע"ח-2018 (להלן - התזכיר או תזכיר החוק). התזכיר הופץ להערות
 הציבור ביוני 2018. במועד סיום הביקורת, כשלוש שנים לאחר קבלתה של
 החלטת הממשלה, ועל אף החשיבות הלאומית שבהסדרת ההגנה על
 המרחב האזרחי, טרם הושלמו התהליכים הנדרשים לגיבוש נוסח חוק
 הסייבר.

המערך פועל מכוח החלטות הממשלה 2444 ו-2443, אשר בהן לא הוסדרו
 בחקיקה סמכויות עובדי המערך כלפי יחידות ההכוונה המגזרית במשרדי
 הממשלה והארגונים הכפופים לאחריות המערך, וכן היבטים תפעוליים
 בעבודתם מול גופים אלו. היעדר מקור נורמטיבי לסמכות עובדי המערך עלול

6 תקן ישראלי ISO 27001 (להלן - תקן 27001).

7 כלל הגופים הפועלים במסגרת תחום מקצועי של משרד ממשלתי ובכפוף לאחריות הרגולטורית.



חלק משרדי
הממשלה טרם
השלימו את איוש
היחידות המגזריות,
בחלקם כלל לא
מונה ראש יחידה
מגזרית. בשני
משרדים טרם הוקמו
היחידות

להקשות את שיתוף הפעולה עם הגופים ולגרום להימנעותם של עובדי המערך מביצוע פעולות מסוימות (כגון לקיחת מחשבים לצורך בדיקה וביצוע בדיקות פורנזיות) עקב חוסר בהירות בעניין תחומי הסמכות.

פעילות ההנחיה על ידי היחידות מבוססת על סמכויות האסדרה הקיימות בכל משרד ומשרד, אשר מטבען שונות בכל אחד מהמשרדים ומשפיעות גם על אפשרויות הבקרה, הפיקוח והאכיפה של יחידות ההכוונה המגזרית. היעדר תשתית משפטית מספיקה לביסוס הנחיה מגזרית על ידי משרדי הממשלה, מעורר קושי למלא אחר החלטות הממשלה.

היערכות חסרה להכוונה מגזרית

מרכז להכוונת מגזרים: בשנת 2016 הוקם במערך אגף הנחיית המשק, ובו מרכז להכוונת מגזרים (להלן - המרכז). מרכז המגזרים מבחין בין שלוש קבוצות מגזרים, כדי שיוכל לגבש הנחיה ספציפית לכל קבוצה. רק בשנת 2017 החלו משרדי הממשלה את תהליך המיפוי. עד פברואר 2018, רק חלק ממשרדי הממשלה סיימו לעשות כן.

הקמת היחידות המגזריות: בהחלטה 2443 נקבע כי התקציב וכוח האדם לכל יחידה ייקבעו בהתאם להערכת המערך את הנזק הפוטנציאלי כתוצאה מפגיעה במערכות ממוחשבות של הגופים במגזר. עוד נקבע כי יש לאייש את תפקיד מנהל היחידה עד תום המחצית הראשונה של שנת 2015.

מרכז המגזרים החל לפעול ב-15 משרדי ממשלה. במועד סיום הביקורת, חלק מהמשרדים טרם השלימו את איוש היחידות המגזריות; בחלק מהמשרדים מונו מרבית עובדי היחידה רק במהלך שנת 2017; בחלק מהמשרדים גויס ראש היחידה רק משנת 2016 ואילך, ובחלק כלל לא מונה ראש יחידה מגזרית. בשני משרדים טרם הוקמו היחידות.

במגזר מסוים, מיפוי ראשוני שביצעה היחידה המגזרית העלה כי לגופים במגזר נדרשת הכוונה ובקרה של יחידת ההכוונה המגזרית. ביחידה המגזרית חסרים עובדים הדרושים לה לביצוע תפקידה.

במגזר נוסף, המיפוי שעשתה היחידה כלל את כלל הגופים תחת רגולציה מסוימת, וזאת ללא הבחנה בין ארגונים שמושפעים מאיומי סייבר, ועל פי מידת עוצמתה של השפעה זו, ואף לא סיווג אותם על פי הצורך שלהם להתגונן מאיומי סייבר. יתרה מזו, בביקורת נמצא כי גופים רבים ברשימה שייכים למגזרים אחרים, חלקם אף גופי תמ"ק אשר חל עליהם חוק הסדרת הביטחון והמערך מנחה אותם ישירות.

ההמלצות העיקריות

דווקא משרדי
הממשלה ויחידות
הסמך, שלפעולתם
התקינה חשיבות
רבה הן מבחינת
הציבור והן מבחינת
המשק, אינם
מיישמים כראוי את
החלטות הממשלה
ואת הנחיות יה"ב
בתחום הגנת
הסייבר

על המערך בשיתוף משרד המשפטים ומשרד ראש הממשלה לקדם תהליך חקיקה שיאפשר לטפל בבעיות האסדרה הקיימות בנושא: סמכויות עובדי המערך ופער בין סמכויות מאסדרים.

על גופי התמ"ק בשיתוף המערך לבחון את הצורך בהשלמת תהליך המיפוי, כדי שלממשלה תהיה תמונת מצב עדכנית ומדויקת יותר בנושא רמת מוכנותם להתמודדות עם איומי סייבר, ותוכל לתת מענה בהתאם.

על יה"ב לוודא כי רשימת הגופים שהיא מנחה מעודכנת ולדאוג להנחותם בהקדם.

על יה"ב לפעול ביתר שאת לכך שמשרדי הממשלה ויחידות הסמך ישלימו את היערכותם בתחום הגנת הסייבר.

על המרכז להכוונת מגזרים ומשרדי הממשלה להשלים בהקדם את מיפוי מגזרי ההכוונה באופן מלא, ולאייש במלואן את יחידות ההכוונה המגזרית בכלל משרדי הממשלה.

סיכום

מרחב הסייבר הוא גורם משמעותי בשגרת החיים השוטפת של המשק. בשנים האחרונות אנו עדים להתקפות סייבר מסוגים שונים, אירועי כופרה⁸ ונוזקה, הונאות, מעילות וגניבת מידע עסקי. זירת הסייבר אף הפכה לזירת לוחמה בין ארגוני טרור ופשעה למדינות ואף בין מדינות. בשנים הבאות צפוי גידול ניכר בחדירת מרחב הסייבר לשגרת היום-יום, לנוכח התפתחותם של מוצרי IoT⁹, מכוניות אוטונומיות ועוד, ובהתאם צפויה עלייה ניכרת בשכיחותם של איומי סייבר ובמידת חומרתם.

למרות מאמצים שנעשו בשנים האחרונות לקידום הנושא, עדיין קיימים פערים בהגנת הסייבר של גופים מסוימים של הממשלה ואף של המשק. ממצאי הדוח מעידים כי דווקא משרדי הממשלה ויחידות הסמך, אשר נדרשו לתת דוגמה לציבור ולמשק, שלפעולתם התקינה חשיבות רבה הן מבחינת הציבור והן מבחינת המשק, אינם מיישמים כראוי את החלטות הממשלה ואת הנחיות יה"ב בתחום הגנת הסייבר. יחידות ההכוונה המגזרית טרם אוישו במלואן, והן נמצאות בתהליך התחלתי של העבודה מול המגזרים במשק, וזאת שלוש וחצי שנים לאחר קבלתה של החלטת הממשלה.

8 תוכנה זדונית המוחדרת למחשב מצפינה את הקבצים המאוחסנים בו ומונעת גישה של המשתמש אליהם.

9 Internet Of Things - מרשתת הדברים, התפתחות טכנולוגית שמרחיבה את מרשתת האינטרנט לתקשוב של חפצים.



ללא הובלה
ממשלתית ראויה
ייוותר המשק חשוף
להתקפות סייבר

ההתמודדות עם אתגר הגנת הסייבר מורכבת. מדובר בתחום דינמי ומהיר הדורש גמישות, מקצועיות ויעילות. נראה כי משרדי הממשלה מתקשים לעמוד בקצב הנדרש ולקדם מהלכים אפקטיביים להתמודדות. המגזר האזרחי יתקשה לעמוד באתגר הגנת הסייבר ללא הנחיה והכוונה. יש חשש כי ללא הובלה ממשלתית ראויה ייוותר המשק חשוף להתקפות סייבר.

אף על פי שהגופים שבהם קיימות תשתיות קריטיות מונחים באופן שוטף, בחלק מהם נמצאו ליקויים בהיערכות הארגונית, בכתיבת נהלים ובתיקון ליקויי אבטחה שנמצאו בדוחות ביקורת של הגורם המנחה. נוכח האיומים המתגברים בתחום הסייבר והחשש לפגיעה קשה במשק בגינם, אם יתרחש אירוע חמור או יתרחשו אירועים בכמה תשתיות קריטיות, על הממשלה לוודא ביתר שאת כי התשתיות הקריטיות ערוכות ומעדכנות כל העת את מידת עמידתן במתקפות אפשריות, וכי תמונת המצב שלה בדבר התשתיות הקריטיות שבידיה עדכנית ומשקפת באופן מלא את פגיעותן של מערכתיה.

