דוח מבקר המדינה

תשתיות תקשוב לאומיות: היבטים פיזיים, סביבתיים ורציפות תפקודית

▪ תמוז התשפ"ו ▪ יוני 2026

תשתיות תקשוב לאומיות: היבטים פיזיים, סביבתיים ורציפות תפקודית

מבוא

מערכות המידע בארגון הן נכס חיוני, ותפקודן התקין נדרש לצורך ביצוע תהליכי ליבה של הארגון. גופי תשתיות מדינה קריטיות (להלן - גופי תמ"ק[1]) וגופי תשתיות חיוניות (להלן - גופים חיוניים[2]) כוללים משרדי ממשלה, גופים ציבוריים וגופים פרטיים שפגיעה בפעילותם עלולה להביא לפגיעה בחיי אדם, לפגיעה באספקת שירות ציבורי חיוני, לנזק פיזי או לנזק כלכלי ניכר. בגופים אלו נדרשת הגנה מוגברת על מערכות המידע מפני איומים פיזיים וסביבתיים כדי לשמור על פעילותן התקינה של מערכות המידע ולמנוע פגיעה בהן העלולה לגרום להשבתת פעילות הארגון או לפגיעה באבטחת המידע שלו (זמינות, מהימנות וסודיות).

מטרת ההגנה הפיזית על חדרי שרתים ותקשורת היא למנוע מגורמים לא מורשים גישה (כניסה) אליהם. ההגנה כוללת בקרת גישה וכן ניטור הגישה באמצעים טכנולוגיים, תיעוד הגישה ושמירה על הלוגים (תיעוד הפעולות) של מנגנוני בקרה אלו במשך זמן. כן כוללת ההגנה פיקוח על הפעילות בחדרי השרתים והתקשורת, לרבות על הכנסה והוצאה של ציוד ורכיבי מערכת, למשל באמצעות מצלמות.

ההגנה הסביבתית כוללת מנגנונים המאפשרים למערכות המידע לפעול בסביבה מיטבית (כגון, אספקת חשמל יציבה ורציפה, טמפרטורה ולחות תקינות) וכן מאפשרים לזהות נזקים סביבתיים (למשל, נפילת חשמל, נזילת מים או דליקה), להגיב באופן מיידי ולמנוע או לצמצם את הפגיעה במערכות המידע.

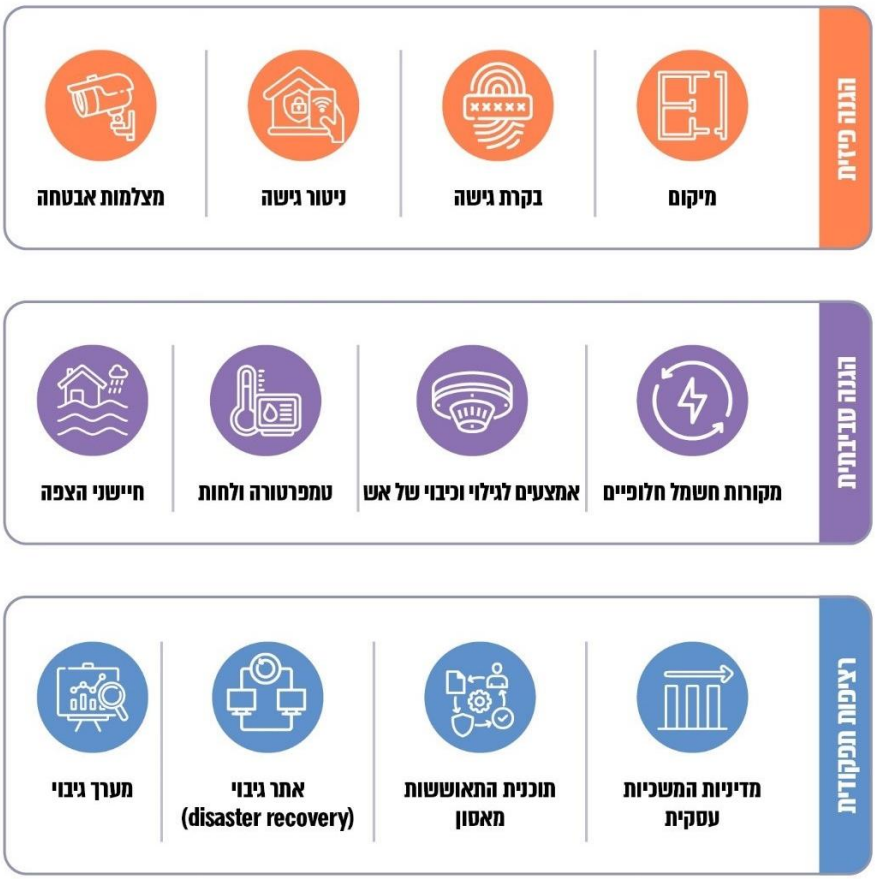
מעטפת ההגנה של הארגון אינה מונעת לחלוטין את קיומם של אירועים חריגים, ולכן חיוני לשמור על הרציפות התפקודית של הגוף, כדי שיוכל להמשיך לספק את השירותים החיוניים בשעת משבר ולמזער את הנזקים שייגרמו לו עקב אירוע חריג. לצורך כך על הארגון להיערך למשבר בעוד מועד, ובכלל זה לגבש מדיניות המשכיות עסקית הכוללת הגדרת יעדים ומטרות של שרידות והתאוששות במצבי חירום. כמו כן, על הארגון לגבש לתקף ולתרגל תוכנית המשכיות עסקית (BCP - Business Continuity Plan). תוכנית זו היא תוכנית פעולה לתהליכים העסקיים הקריטיים בארגון, לצורך התאוששות מלאה או חלקית בפרק זמן מוגדר וברמת שירות מוגדרת, בהתאם למדיניות הארגון. במסגרת תוכנית זו על הארגון לוודא, בין היתר, יכולת שחזור מהירה (העומדת ביעדי הארגון) של תשתיות מערכות המידע ולהיערך מבחינת תשתיות חלופיות באתרים חלופיים (כולל זמינות ויתירות). זאת, באמצעות גיבוש תוכנית התאוששות מאסון (DRP) לחידוש פעילות טכנולוגית ומערכות מידע התומכות בתהליכים הקריטיים בארגון, המהווה מרכיב מרכזי בתוכנית ההמשכיות העסקית (BCP).

---

[1] בחוק להסדרת הבטחון בגופים ציבוריים, התשנ"ח-1998, מוגדרות "מערכות ממוחשבות חיוניות" - "מערכות ממוחשבות שנקבעו כחיוניות על ידי הגוף שהסמיכה לכך הממשלה". בהתאם להחלטת ועדת השרים לענייני בטחון לאומי ב/84 מ-11.12.02, החלטת הממשלה 3611 מ-7.2.11 והחלטת הממשלה 2444 מ-15.2.15, רשימת הגופים המונחים וסיווג המערכות שלהם כמערכות ממוחשבות חיוניות (קרי, גופי תמ"ק) נקבעים על ידי ועדת ההיגוי העליונה להגנה על מערכות ממחושבות בראשות ראש מערך הסייבר הלאומי.

[2] יחידות הסייבר המגזריות - יחידות להכוונה מגזרית בתחום הסייבר לגופים במגזר שבו הן פועלות, מגדירות את הגופים המונחים לפי רמת חשיבות להגנה בסייבר - A, B, C. הגופים המספקים שירותים חיוניים מוגדרים בקטגוריה A.

תרשים 1: **מרכיבים מרכזיים בהיבטים של הגנה פיזית, הגנה סביבתית ורציפות תפקודית**



הוכן בידי משרד מבקר המדינה.

פערים בכל אחד משלושת התחומים האלה - הגנה פיזית, הגנה סביבתית ורציפות תפקודית - עלולים להביא בעת התממשות תרחישי אסון לפגיעה בתפקוד חדרי השרתים וחדרי התקשורת של ארגון, וכפועל יוצא מכך לפגיעה ביכולת של גוף לספק שירותים חיוניים, כמפורט להלן:

1. **הגנה פיזית:** פערים במיקום חדר השרתים (קומה גבוהה, צמידות לקירות חיצוניים או במרחב הפתוח לקהל הרחב) חושפים את מערכות המחשוב שבו (לרבות התשתיות והמידע שבהן) לפגיעה עקב נפילת טיל במקום או כניסת גורמים לא מורשים לחדר במטרה לבצע פעולות זדוניות (התחברות לרשת, פגיעה במערכות המחשוב, גניבת חומרה ועוד); פערים בבקרת הגישה ובניטור הגישה לחדר השרתים פוגעים ביכולת הגוף לזהות ולמנוע גישה של גורמים לא מורשים.

2. **הגנה סביבתית:** היעדר מקורות חלופיים לאספקת חשמל (למשל, גנרטור, UPS) ימנע המשך פעילות סדירה בעת נפילת מקור אספקת חשמל ראשי, וכן לא יאפשר לבצע כיבוי מסודר של המערכות לצורך שמירה על תקינותן; היעדר אמצעים לגילוי וכיבוי של אש, חיישני הצפה ואמצעי ניטור של טמפרטורה ולחות יפגע ביכולת הגוף לזהות בהקדם נזקים סביבתיים (פגיעה בתשתיות חשמל ומים, שריפה או הצפה) ולמנוע פגיעה ניכרת במערכות שנמצאות בחדרי השרתים.

3. **רציפות תפקודית:** תרחישי אסון שונים, כגון סייבר, שריפה, הצפה, נפילת טיל והשבתה ממושכת של תשתיות חשמל ומים, עלולים לפגוע בתפקוד חדר השרתים הראשי. פערים באתר הגיבוי, במערך הגיבוי, במדיניות ההמשכיות העסקית ובתוכנית ההתאוששות מאסון יפגעו ביכולת לשחזור מהיר של תשתיות מערכות המידע ומעבר לתשתיות באתר החלופי, ועקב כך תיפגע יכולת הגוף לספק שירותים חיוניים בעת משבר.

פעולות הביקורת

בחודשים אפריל 2024 עד אפריל 2025 בדק משרד מבקר המדינה את ההגנה הפיזית והסביבתית על חדרי שרתים ותקשורת בגופי תמ"ק ובגופים חיוניים והיבטים ברציפות התפקודית של גופים אלה. בדיקות השלמה בוצעו בחלק מהגופים בנושאים מסוימים עד אוגוסט 2025. בכלל זה נבדקו הנושאים האלה: הנורמות המקובלות והאסדרה המחייבת בתחומים אלה; ההנחיה והפיקוח של הגופים האסדרתיים המדינתיים והמגזריים בתחומים אלה; רמת ההגנה הפיזית וההגנה הסביבתית בפועל על חדרי שרתים וחדרי תקשורת של 12 גופי תמ"ק וגופים חיוניים; הטיפול בנושא הרציפות התפקודית בגופים אלה; היבטים ברציפות התפקודית של משרדי ממשלה ויחידות סמך בעקבות פגיעה בחדרי שרתים; ונושא ממונה הביטחון בגופים ציבוריים.

הביקורת נעשתה בגופים אסדרתיים מדינתיים בתחום הסייבר בהיבטי הנחיה ופיקוח: משרד ראש הממשלה - במערך הסייבר הלאומי (להלן - מערך הסייבר), במטה לביטחון לאומי (להלן - המל"ל) ובשירות הביטחון הכללי (להלן - השב"כ); במשרד המשפטים - ברשות להגנת הפרטיות; במשרד הכלכלה והתעשייה - במערך הדיגיטל הלאומי (להלן - מערך הדיגיטל), לרבות ביחידה להגנת הסייבר בממשלה (להלן - יה"ב); במשרד הביטחון - ברשות החירום הלאומית (להלן - רח"ל); במשרד האוצר - במינהל הרכש הממשלתי ובמינהל הדיור הממשלתי; במשטרת ישראל וביחידות סייבר מגזריות.

במסגרת הביקורת נבדקו פעולות האסדרה והפיקוח של הגופים האסדרתיים המדינתיים בנוגע לרציפות התפקודית ולהגנה הפיזית והסביבתית על חדרי שרתים ותקשורת בגופי תמ"ק וגופים חיוניים; הבדיקה נעשתה על בסיס נורמות שנקבעו לגבי חדרי שרתים המכילים חומר בלתי מסווג ביטחונית (להלן - בלמ"ס). רמת ההגנה על חדרי שרתים וחדרי תקשורת נבדקה ב-12 גופי תמ"ק וגופים חיוניים באמצעות פגישות בשטח ותצפית הכוללת את בחינת עמידתם של הגופים בבקרות שהוגדרו מראש[3] (להלן - התצפית). בסך הכול נבדקו 26 חדרי שרתים וחדרי תקשורת. הבדיקה לא כללה את כל חדרי השרתים וחדרי התקשורת בכל גוף, והיא אינה מדגם מייצג לגבי כלל החדרים בגופים שנבדקו.

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

אסדרה ופיקוח בהיבטי הגנה פיזית, הגנה סביבתית ורציפות תפקודית

גופים אסדרתיים מדינתיים בתחום אבטחת המידע והגנת הסייבר

התחומים של אבטחת המידע, הגנת הסייבר והגנת הפרטיות בישראל מאוסדרים, בין היתר, בחוק להסדרת הבטחון בגופים ציבוריים, התשנ"ח-1998 (להלן - החוק להסדרת הביטחון), בחוק הגנת הפרטיות, התשמ"א-1981 (להלן - חוק הגנת הפרטיות), ובתקנות הגנת הפרטיות שהותקנו מכוחו. לצד זה, הממשלה קיבלה כמה החלטות העוסקות בתחום אבטחת המידע והגנת הסייבר. בהתאם לכך, האסדרה וההנחיה בתחום אבטחת המידע והגנת הסייבר מוטלת על כמה גורמים. בתרשים 2 שלהלן מוצג מבנה האסדרה בתחום אבטחת המידע, הגנת הסייבר והגנת הפרטיות בנוגע לגופי תמ"ק וגופים חיוניים.

מערך הסייבר: מערך הסייבר הוא גוף ממשלתי שאמון על הגנת הסייבר הלאומי. הוא פועל ברמת המדינה לחיזוק תמידי של רמת ההגנה של הגופים במשק והאזרחים, לטיפול בתקיפות סייבר וסילוקן ולהיערכות לשעת חירום. בהתאם לחוק להסדרת הביטחון, מערך הסייבר אחראי להנחיית מרבית גופי התמ"ק ולבקרה עליהם בנושא "פעולות לאבטחת מערכות ממוחשבות

[3] תצפית הכוללת בקרות בנושאי הביקורת על פי תקנים מקובלים בתחום אבטחת המידע - תורת ההגנה 2.0, תקן ISO27001 ו-NIST 800-53.

חיוניות" המוגדרות כפעולות הדרושות לשם שמירה על מערכות ממוחשבות ועל המידע האגור במערכות אלה ומנחה גופים אלה באמצעות מתודולוגיה ייעודית לגופי תמ"ק (להלן - תו"ל ייעודי) ובאמצעות הנחיות משלימות. כמו כן, בהתאם להחלטת הממשלה 2443 מפברואר 2015[4], מערך הסייבר אחראי גם להנחיה מקצועית של יחידות הסייבר המגזריות ושל יה"ב, ומשכך נדרש לבצע בקרה על יישום הנחיותיו ליחידות אלה. זאת ועוד, מערך הסייבר מפרסם הנחיות שונות למשק שהן בגדר המלצות, לדוגמה: תורת ההגנה 2.0 (להלן - תורת ההגנה) - מדריך יישומי להגנת הסייבר בארגון.

הרשות להגנת הפרטיות: הרשות להגנת הפרטיות היא רגולטור רוחבי כלל משקי ומופקדת על הגנת הזכות לפרטיות, ובכלל זה על אבטחת המידע בכלל מאגרי המידע בישראל שבהם מצוי מידע אישי, מכוח הוראות חוק הגנת הפרטיות והתקנות שהותקנו מכוחו. אבטחת מידע מכוח החוק להגנת הפרטיות מוגדרת כהגנה על שלמות המידע האישי והגנה על המידע מפני חשיפה, שימוש או העתקה ללא רשות. לשם כך הרשות להגנת הפרטיות מוסמכת לבצע אכיפה מינהלית ואכיפה פלילית על כלל המחזיקים במאגרי מידע (גופים פרטיים וגופים ציבוריים כאחד), בהתאם להוראות חוק הגנת הפרטיות ותקנותיו. לצורך הפקת תמונת מצב מגזרית בנוגע לעמידה בהוראות החוק והתקנות ולצורך איתור כשלים הטעונים אסדרה קיים בידי הרשות מנעד של כלים, ובהם פיקוח רוחב, הנעשה בעיקר במגזרים שיש בהם סיכון מוגבר לפגיעה בפרטיות. פעילות הרשות להגנת הפרטיות מבוצעת בהיבטים הנוגעים למידע אישי ולגבי מאגרי מידע ממוחשבים, בהתאם לסמכויותיה מכוח חוק הגנת הפרטיות ותקנות הגנת הפרטיות (אבטחת מידע), התשע"ז-2017 (להלן - תקנות אבטחת מידע).

השב"כ: בהתאם לחוק להסדרת הביטחון, השב"כ אחראי להנחיית גופי תמ"ק בתחום התקשורת בנושא "פעולות לאבטחת מערכות ממוחשבות חיוניות" המוגדרות כפעולות הדרושות לשם שמירה על מערכות ממוחשבות ועל המידע האגור במערכות אלה ומנחה גופים אלה באמצעות תו"ל ייעודי ובאמצעות הוראות שעה. נוסף על כך, השב"כ הוא המאסדר המדינתי בנושאי אבטחת מידע ביטחוני מסווג זאת בהתאם לחוק להסדרת הביטחון.

רח"ל: רח"ל הוקמה מכוח החלטת ועדת שרים לענייני ביטחון לאומי ב/43 מדצמבר 2007[5] (להלן - החלטה ב/43) כגוף מטה שכפוף לשר הביטחון. ייעודה של רח"ל הוא לסייע למימוש אחריות-העל לטיפול בעורף בכל מצבי החירום, ובכלל זה טרור סייבר (שיבוש מערכות מידע הגורם לסכנת נפשות או לנזק לתשתיות). תפקידי רח"ל הם, בין השאר, לרכז בזמן שגרה את עבודת המטה בנושא ההיערכות של הארגונים ומשרדי הממשלה בעורף במצבי החירום השונים, את המענה הנדרש מהם בנושא ואת יעדי כשירות וכוננות וכן להכין עבור הממשלה דוח מצב שנתי בנושא מוכנות העורף בתחומים השונים ובהתייחס לתרחישים השונים. עוד בהתאם להחלטה, אם אין גורם אחראי לפעולה מסוימת או שקיים בתחום הקשור לאותה פעולה חוסר תיאום בין גורמים או ריבוי גורמים העוסקים בכך, בלי שיהיה גורם מוסמך בחקיקה או בהחלטות הממשלה לביצוע הפעולה - על רח"ל להמליץ לשר הביטחון לבצע הסדרה[6].

המל"ל: המל"ל הוא "גוף המטה לראש הממשלה ולממשלה בענייני החוץ והביטחון" ופועל בהתאם לסמכויות המוקנות לו בחוק המטה לביטחון לאומי, התשס"ח-2008. היות שממד הסייבר הוא בעל השפעה ישירה על הביטחון הלאומי של מדינת ישראל ועל יחסי החוץ שלה, פועל המל"ל במסגרת סמכויותיו לקידום נושא הסייבר, בשיתוף פעולה עם משרדי הממשלה הרלוונטיים על פי הסמכויות שהוקנו להם בדין ומכוח החלטות הממשלה הרלוונטיות. למל"ל אין סמכויות אסדרתיות פורמליות בתחום הסייבר, אך הוא מתכלל נושאים מסוימים שבהם מעורבים גופים אסדרתיים מדינתיים שונים בתחום הסייבר ואף מסייע לגופים אלה בנושאים הקשורים לביטחון הלאומי.

---

4 החלטת הממשלה 2443 בנושא "קידום אסדרה לאומית והובלה ממשלתית בהגנת הסייבר" (15.2.15).

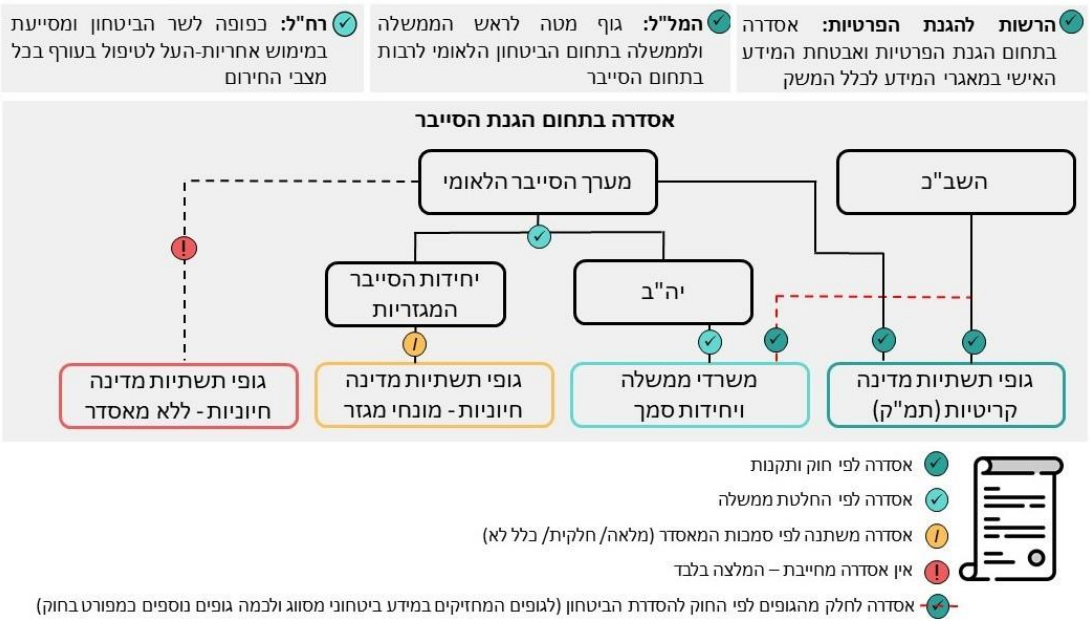
5 החלטה ב/43 של ועדת השרים לענייני ביטחון לאומי (19.12.07).

6 "הסדרה" הוגדרה בהחלטה זו כפעולה שתכליתה לקבוע בידי מי האחריות לנושא מסוים, מה היא תכולתה, אילו פעילויות יבוצעו, ומה הם קשרי הגומלין בין הגורמים השונים הקשורים לאותו נושא.

יה"ב: היחידה הוקמה על פי החלטת הממשלה 2443[7] ואחראית להכוונה והנחיה מקצועית של משרדי הממשלה ויחידות הסמך (להלן - משרדי הממשלה)[8] בתחום הגנת הסייבר. היחידה כפופה ארגונית למערך הדיגיטל (בעבר רשות התקשוב הממשלתי) ופועלת בהנחיה מקצועית של מערך הסייבר.

יחידות הסייבר המגזריות: היחידות המגזריות הוקמו בהתאם להחלטת הממשלה 2443 מפברואר 2015 שהטילה על המנכ"לים של משרדי הממשלה לקדם את הטיפול בהיערכות לאיומי סייבר במסגרת המגזר שבו הם פועלים, על ידי הקמת יחידות להכוונה מגזרית והכנת עבודת מטה לבחינת התיקונים והשינויים המשפטיים הנדרשים כדי שתהיה להן הסמכות הנדרשת להנחות בתחום הסייבר את הגופים במגזר. היחידות כפופות מהבחינה הארגונית למשרד הממשלתי שאליו הן שייכות ופועלות בהנחיה מקצועית של מערך הסייבר.

תרשים 2: **מבנה האסדרה בתחום אבטחת המידע, הגנת הסייבר והגנת הפרטיות לגבי גופי תמ"ק וגופים חיוניים**



הוכן בידי משרד מבקר המדינה.

הנורמות המקובלות והאסדרה המחייבת בהיבטי הגנה פיזית, הגנה סביבתית ורציפות תפקודית

ביקורת זו מתבססת על נורמות מקובלות בתחום הגנת הסייבר ואבטחת המידע, כמפורט להלן:

1. **תקן ISO 27001:** תקן בין-לאומי לניהול אבטחת מידע של ארגון התקינה הבין-לאומי (International Organization for Standardization) שהוכר ואומץ בישראל על ידי מכון התקנים הישראלי (ת"י ISO 27001). בפברואר 2015 התקבלה החלטת הממשלה 2443, ולפיה משרדי הממשלה מחויבים לבצע הטמעה, התעדה והסמכה לגבי תקן זה. התקן מגדיר עקרונות שיטתיים להקמה, לניהול ולתחזוקה של מערכות לניהול אבטחת מידע בארגון.

2. **תורת ההגנה 2.0:** מערך הסייבר הלאומי פרסם לכלל המשק הישראלי מדריך יישומי שמהווה בסיס לתוכנית הגנת הסייבר של ארגונים. תורת ההגנה היא המלצה לכלל הארגונים

---

7 החלטת הממשלה 2443 בנושא "קידום אסדרה לאומית והובלה ממשלתית בהגנת הסייבר" (15.2.15).

8 למעט "הגופים המיוחדים" שפורטו בהחלטה 3611 ופעולות גופים אלה באמצעות משרדי הממשלה במסגרת תפקידם.

במשק וכלי עבודה יישומי לגורמי הסייבר בארגון. תורת ההגנה ממליצה בין השאר על יישום תקן TIA-942[9] - תקן תכנון למרכזי נתונים הכולל דרישות פיזיות (גישה, מיזוג, חשמל) - כתקן מקובל לחדרי שרתים.

3. **תקני NIST:** המכון הלאומי לתקנים וטכנולוגיה של ארצות הברית (National Institute of Standards and Technology), מפרסם מסגרות עבודה ותקנים בתחום הגנת המידע (בכלל זה: NIST 800-53[10] העוסק בבקרות אבטחה ופרטיות עבור מערכות מידע וארגונים). מערך הסייבר הלאומי מכיר בתקני NIST כתקנים מומלצים ואף הסתמך על אחד מתקנים אלה כבסיס מחייב בחקיקה שקידם[11].

כל אחת מנורמות מקובלות אלה כוללת הנחיות מפורטות בכל היבטי ההגנה הפיזית, ההגנה הסביבתית והרציפות התפקודית בקשר לחדרי שרתים וחדרי תקשורת. בהתאם לכך, הנושאים בביקורת זו נבחנו לעומת הנחיות אלה, כמפורט להלן:

1. הגנה פיזית

א. **מיקום פיזי:** מיקום חדרי השרתים וחדרי התקשורת (יעדי ההגנה) בהתאם לפרופיל הסיכון. המיקום יהיה מוגן ככל האפשר (למשל לא בצמוד למקורות מים).

ב. **בקרת גישה:** יישום בקרות גישה פיזיות בכניסה לחדרי השרתים וחדרי התקשורת, במטרה לוודא אפשרות כניסה רק למי שהארגון הגדיר כמורשה לכך[12].

ג. **ניטור גישה:** ניטור כל הגישות הפיזיות לאזורים רגישים (חדרי שרתים, ארונות תקשורת וכו') באמצעות רישום של הנכנסים והיוצאים, לצורך זיהוי ניסיון גישה או גישה בפועל לאזורים כאמור (על ידי אנשים לא מורשים או אנשים מורשים שלא בימים ובשעות של העבודה), ושימוש באמצעי התרעה, למשל מערכת אזעקה בעת ניסיון גישה לא מאושר.

ד. **מצלמות אבטחה:** התקנת מצלמות אבטחה לניטור שוטף ורצוף של כלל הכניסות והפתחים המאפשרים גישה לחדר השרתים ולחדר התקשורת, לרבות לצורך פיקוח על הכנסה והוצאה של פריטים ממתחם העבודה.

2. הגנה סביבתית

א. **מקורות חלופיים של חשמל:** מקור חלופי לאספקת חשמל לטווח קצר (מערכת UPS) נועד לאפשר כיבוי מסודר של המערכות בעת נפילת מקור אספקת חשמל ראשי או בעת העברה למקור חלופי של אספקת חשמל ולמנוע את הפגיעה בהן. מקור חלופי לאספקת חשמל לטווח ארוך (למשל, גנרטור) נועד לאפשר המשך פעילות עסקית סדירה גם בעת נפילת מקור אספקת חשמל ראשי.

---

9 TIA-942 Data Center Standards Overview ADC.

10 NIST 800-53 Security and Privacy Controls for Information Systems and Organizations.

11 חוק התמודדות עם תקיפות סייבר חמורות במגזר השירותים הדיגיטליים ושירותי האחסון (הוראה שעה - חרבות ברזל), התשפ"ד-2023.

12 נדרש לוודא כי לא ניתן לעקוף את אמצעי ההגנה על בקרת הגישה. למשל, למנוע, באמצעות מנגנון דלת מוטרדת, השארת דלת פתוחה במשך זמן.

ב. **אמצעי גילוי וכיבוי של אש** בחדרי שרתים ובחדרי תקשורת.

ג. **טמפרטורה ולחות:** מערכת מיזוג לוויסות הטמפרטורה והלחות בחדרי שרתים ובחדרי תקשורת לרמות מקובלות (הנדרשות לפעולה מיטבית של מערכות המידע), לרבות מערכות גיבוי למערכת המיזוג עצמה ולאספקת החשמל למערכת, אמצעי לניטור הטמפרטורה והלחות והתרעה בעת חריגה מהרמות המוגדרות.

ד. **חיישני הצפה** בחדרי שרתים ובחדרי תקשורת שיתריעו מפני נזילות או הצפות.

3. רציפות תפקודית

א. **מדיניות המשכיות עסקית:** גיבוש מדיניות המשכיות עסקית (לרבות קביעת מדד מקובל לכל שירות ויעדי הגנה התומכים בו) ותיקופה לפחות אחת לשנה.

ב. **תוכנית התאוששות מאסון:** גיבוש תוכנית התאוששות מאסון (DRP - Disaster Recovery Plan), תיקופה לפחות אחת לשנה ותרגולה באופן עיתי.

ג. **אתר גיבוי (DR - Disaster Recovery):** קיומו של אתר גיבוי (DR) נגיש לשעת חירום הנותן מענה לצרכים של הארגון כפי שבאים לידי ביטוי במדיניות ההמשכיות העסקית, תרגול מעבר לאתר הגיבוי אחת לשנה (של כלל הצוותים העוסקים בהקמתו ובתפעולו), הפקת לקחים ותיקון ליקויים.

ד. **מערך גיבוי:** מערך גיבוי (נתונים ומערכות מחשוב התומכים ביעדים עסקיים) התואם את צורכי הארגון לגבי המשכיות עסקית, בהתאם למדיניות ההמשכיות העסקית של הגוף ; בדיקת תקינות הגיבוי והיכולת לשחזור תקין.

לוח 1 : **סעיפי הבקרות בתחומי הגנה פיזית, הגנה סביבתית ורציפות תפקודית בנורמות המקובלות**

תחום	הבקרה	תורת ההגנה 2.0	ISO-27001-2020	NIST 800-53
הגנה פיזית	מיקום	בקרה 9.3	A.11.1.1	PE-18
	בקרת גישה	בקרה 9.1 (דגשים - סעיף 17)	A.11.1.2	PE-3
	ניטור גישה	בקרה 9.4 (דגשים - סעיף 3 וסעיף 5)	A11.1	PE-6(1)
	מצלמות אבטחה	בקרה 9.4 (דגשים - סעיף 3, וסעיף 7 + בקרה ברמה בסיסית 1- סעיף 3)	A 11.1.3	PE-6(2)
הגנה סביבתית	מקור חשמל חלופי	בקרה 9.1 (דגשים - סעיף 22 וסעיף 23)	A 11.2.1	PE-11
	אמצעי גילוי וכיבוי אש	בקרה 9.1 (דגשים - סעיף 25)	A 11.1.4	PE-13
	טמפרטורה ולחות	בקרה 9.1 (דגשים - סעיף 26)	A 11.2.1	PE14
	חיישני הצפה	בקרה 9.1 (דגשים - סעיף 27)	A 11.1.4	PE-15
רציפות תפקודית	מדיניות המשכיות עסקית	בקרה 19.1 (דגשים - סעיף 1, סעיף 5, סעיף 6, סעיף 13 וסעיף 14)	A17.1.2	CP-2
	תוכנית התאוששות מאסון	בקרה 19.1 (דגשים - סעיף 5 וסעיף 6)	A 17.1	CP-1
	אתר גיבוי (DR)	בקרה 19.2 (פירוט הבקרה + בקרה ברמה בסיסית-1 סעיף 1) בקרה 19.4 (דגשים - סעיף 4, סעיף 5 וסעיף 7)	A 17.1.2 / 17.1.3	CP-6 CP-4
	מערך גיבוי	בקרה 12.4 (דגשים - סעיף 1, סעיף 2 וסעיף 4) בקרה 19.3 (דגשים - סעיף 10)	A 12.3.1	CP-9

הוכן בידי משרד מבקר המדינה.

כאמור, האסדרה לגבי גופי תמ"ק וגופים חיוניים והנחייתם מוטלת על כמה גופים, ובהם מערך הסייבר, הרשות להגנת הפרטיות, יה"ב, השב"כ ויחידות הסייבר המגזריות. בביקורת זו בדק משרד מבקר המדינה אם קיימות הנחיות ייעודיות של הגופים האסדרתיים המדינתיים לגופי תמ"ק ולגופים חיוניים בהתאם לנורמות המקובלות. בלוח 2 ובלוח 3 שלהלן מוצגים הפערים באסדרה הקיימת (המדינתית והמגזרית בהתאמה) לגבי כל נושא.

לוח 2 : **האסדרה המדינתית בהיבטי רציפות תפקודית ובהיבטי הגנה פיזית וסביבתית על חדרי שרתים וחדרי תקשורת**

מאסדרים	מערך הסייבר הלאומי		שב"כ	הרשות להגנת הפרטיות
	יחידות מגזריות	גופי תמ"ק	גופי תמ"ק	מאגרי מידע ברמת אבטחה בינונית / גבוהה
תחום	המלצה - תורת ההגנה	חובה - תו"ל ייעודי והנחיות משלימות	חובה - תו"ל ייעודי	חובה
הגנה פיזית	יש	חלקית	חלקית	חלקית
הגנה סביבתית	יש	אין	אין	אין
רציפות תפקודית	יש	חלקית	חלקית	אין

הוכן בידי משרד מבקר המדינה.

לוח 3 : **האסדרה במגזרים שנבדקו (לא כולל גופי תמ"ק) בהיבטי רציפות תפקודית ובהיבטי הגנה פיזית וסביבתית על חדרי שרתים וחדרי תקשורת**

תחום	הבקרה	מגזר 1	מגזר 2	מגזר 3	מגזר 4	מגזר 5	מגזר 6
הגנה פיזית	מיקום	אין	אין	אין	אין	יש	חלקית(1)
	בקרת גישה	אין	יש	אין	יש	יש	יש
	ניטור גישה	אין	אין	אין	יש	יש	יש
	מצלמות אבטחה	אין	אין	אין	יש	יש	יש
הגנה סביבתית	מקורות חלופיים לאספקת חשמל	אין	יש	אין	אין	אין	יש
	אמצעים לגילוי וכיבוי של אש	אין	יש	אין	אין	אין	אין
	טמפרטורה ולחות	אין	יש	אין	אין	אין	אין
	חיישני הצפה	אין	אין	אין	אין	אין	אין
רציפות תפקודית	מדיניות המשכיות עסקית	אין	יש	יש	חלקית(2)	יש	יש
	תוכנית התאוששות מאסון	אין	יש	יש	חלקית(2)	יש	יש
	אתר גיבוי (DR)	אין	אין	יש	חלקית(3)	יש	יש
	מערך גיבוי	אין	יש	יש	יש	יש	יש

הוכן בידי משרד מבקר המדינה.

נורמות מקובלות מסדירות את הנושאים הגנה פיזית, הגנה סביבתית ורציפות תפקודית אולם מהלוחות עולה כלהלן:

1. **בתחום ההגנה הסביבתית - אין אסדרה מחייבת, לא ברמה המדינתית ולא ברמה המגזרית. זאת למעט הנחיה בהיבט אחד מתוך ארבעה (מקור חשמל חלופי) בשניים (33.3%) משישה מגזרים שנבדקו, והנחיות בשני היבטים נוספים (אמצעים לגילוי וכיבוי של אש וטמפרטורה ולחות) באחד (16.6%) משישה מגזרים שנבדקו בלבד.**

2. **בתחום הרציפות התפקודית - האסדרה של גופי תמ"ק שמונחים על ידי שב"כ ומערך הסייבר היא חלקית, זאת בשונה מהאסדרה המקיפה יותר שקיימת במגזרים שנבדקו.**

3. **בתחום ההגנה הפיזית - האסדרה המחייבת חסרה הן ברמה המדינתית והן ברמה המגזרית, למעט באחד (16.6%) משש המגזרים שנבדקו.**

4. **כמו כן, יש שונות בין המגזרים בנושאים המוסדרים בהיבטי ההגנה הפיזית, ההגנה הסביבתית והרציפות התפקודית, אף שההמלצה ברמה המדינתית (תורת ההגנה) מתייחסת לכלל ההיבטים בכל שלושת התחומים. פערים אלו יפורטו בהרחבה בהמשך.**

הנחיית גופי תמ"ק בתחומי הגנה פיזית, הגנה סביבתית ורציפות תפקודית על ידי מערך הסייבר והשב"כ

בהתאם להוראות החוק להסדרת הביטחון, מערך הסייבר אחראי להנחיית מרבית גופי התמ"ק והשב"כ אחראי להנחיית גופי תמ"ק בתחום התקשורת, בנושא "פעולות לאבטחת מערכות ממוחשבות חיוניות", המוגדרות כפעולות הדרושות לשם שמירה על מערכות ממוחשבות ועל המידע האגור בהן. מערך הסייבר והשב"כ מנחים את גופי התמ"ק באמצעות התו"ל הייעודי. נוסף על התו"ל הייעודי, מערך הסייבר מפרסם הנחיות משלימות והשב"כ מפרסם הוראות שעה בנושאים שונים שחלים על הגופים שהוא מנחה. השב"כ מעדכן בעת הזו את התו"ל הייעודי. בחינת עמידת הגוף המונחה בדרישות התו"ל הייעודי נעשית על ידי מערך הסייבר והשב"כ באמצעות בקרות ועל פי מדדים שנקבעו. יצוין כי בהחלטת הממשלה 2443 נקבע כי האסדרה בתחום הגנת הסייבר תישען על נורמות מקובלות בעולם.

בספטמבר 2024 הוציא מערך הסייבר הנחייה להיערכות לחירום בנושא רציפות תפקודית לגופי התמ"ק. מלבד הנחיה זו, אין עוד הנחיות משלימות של מערך הסייבר והוראות שעה של השב"כ בנושאים שנבדקו בביקורת בהיבטי רציפות תפקודית ובהיבטי הגנה פיזית והגנה סביבתית על חדרי שרתים וחדרי תקשורת.

ממידע שהתקבל ממערך הסייבר עולה כי ההנחיה המשלימה האמורה טרם הוצאה לחלק מגופי התמ"ק שנבדקו בביקורת. כמו כן הבדיקה בגופים אלו העלתה כי טרם בוצעו פעולות הנחייה בעניינה, אף לא מול גופים בהם קיים פער בנושא רציפות תפקודית. יצוין כי בגופים בהם קיימים פערים בנושא רציפות תפקודית התממשו נזקים סביבתיים ופיזיים שהיו עשויים להשבית את פעילות הגוף.

בלוח 2 שלעיל הוצגו הנחיות התו"ל הייעודי המשמש את השב"כ ואת מערך הסייבר בהנחייתם את גופי התמ"ק וההנחיה המשלימה של מערך הסייבר בנושאי הביקורת. כפי שעולה מהנתונים באותו לוח, ההנחיות בנוגע לחדרי שרתים וחדרי תקשורת כוללות היבטים חלקיים של הגנה פיזית ושל הרציפות התפקודית. נוסף על כך, התו"ל אינו כולל כלל דרישות בהיבטי הגנה סביבתית, שמטרתן לייצר סביבה מיטבית לפעילותן של מערכות המידע, ולהביא לזיהוי נזקים סביבתיים ולמזער את הפגיעה במערכות.

נמצא כי מערך הסייבר והשב"כ, אשר אחראים להנחיה של גופי תמ"ק, הוציאו הנחיות חלקיות לגופי התמ"ק בנושאי הביקורת, כמפורט להלן:

1. **הגנה סביבתית: מערך הסייבר והשב"כ לא הוציאו הנחיות לגופי התמ"ק בהיבטי הגנה סביבתית על חדרי שרתים ותקשורת.**

2. **הגנה פיזית: מערך הסייבר והשב"כ הוציאו הנחיות חלקיות בנושא.**

3. **רציפות תפקודית**

   א. **השב"כ ומערך הסייבר הוציאו הנחיות חלקיות לגופי התמ"ק בהיבטי רציפות תפקודית הרלוונטיים למערכות מידע ולפגיעה בחדרי שרתים וחדרי תקשורת.**

   ב. **נמצאו פערים מסוימים באופן הפצת ההנחיה של מערך הסייבר שעסקה בנושא רציפות תפקודית ובפעולות מערך הסייבר לבדיקת אופן יישומה.**

בתשובת מערך הסייבר למשרד מבקר המדינה נמסר כי המערך אחראי להנחות את גופי התמ"ק בכל הנוגע להגנה על המערכות הממוחשבות החיוניות הפועלות בגוף מפני תקיפת סייבר בלבד. האחריות להיבטים של הגנה סביבתית והיבטים מסוימים ברציפות תפקודית, אשר הטיפול בהם חורג מתחומי ההנחיה של המערך, מצוי באחריות הגופים המונחים, בפיקוח המאסדרים הרלוונטיים, כל אחד בתחומו, בהתאם לדין (למשל, רח"ל בהיבטי רציפות תפקודית). כמו כן, המערך יקיים עבודת מטה סדורה בנושאי רציפות תפקודית והגנה סביבתית, ובמסגרת עבודת המטה יבחן את ההמלצות בדוח הביקורת ובהתאם לכך יגבש המלצות להמשך.

בהתייחס לתשובת מערך הסייבר משרד מבקר המדינה מציין כי בהתאם להוראות החוק להסדרת הביטחון, מערך הסייבר אחראי להנחיית גופי התמ"ק באשר לשמירה על מערכות ממוחשבות ועל המידע האגור בהן. לפיכך סמכות ההנחיה של מערך הסייבר חלה על הגנה פיזית והגנה סביבתית על חדרי שרתים ותקשורת ורציפות תפקודית, הכלולים בנורמות מקובלות בתחום הגנת הסייבר ואבטחת מידע (תקן ISO27001 ; תורת ההגנה 2.0 ; ותקן NIST 800-53) אשר נבדקו בביקורת זו באמצעות 12 בקרות בסיסיות. מעורבותו המקצועית והרגולטורית של מערך הסייבר נחוצה גם בראי הממצאים שעלו בגופים בהם נמצאו פערים בנושא רציפות תפקודית ונכללו בביקורת זאת, ואשר בהם התממשו נזקים סביבתיים ופיזיים שהיו עלולים להשבית את פעילות הגוף.

בתשובת השב"כ נמסר כי בנושא של רציפות תפקודית קיימת התייחסות לנושא זה בתו"ל הייעודי ובימים אלה פועלים גורמי המקצוע לכתיבתו של תו"ל חדש בו יתוקפו כלל הנושאים לרבות מול נורמות מקובלות בעולם. בנושא של הגנה סביבתית אין לשב"כ אחריות, סמכויות ועיסוק בתחום ההגנה הסביבתית (היינו רעידות אדמה ופגעי מזג אוויר), עם זאת ולאור הערת הביקורת תבוצע בחינה וחשיבה מחודשת בנושא זה.

בהתייחס לתשובת השב"כ בעניין אחריותו בנושא של הגנה סביבתית, משרד מבקר המדינה מציין כי החוק להסדרת הביטחון בגופים ציבוריים מטיל אחריות על השב"כ לפעולות אבטחת מערכות ממוחשבות המוגדרות כפעולות הדרושות לשם שמירה על מערכות ממוחשבות ועל המידע האגור בהן. נורמות מקובלות בתחום אבטחת המידע והגנת הסייבר כוללות בקרות בתחום הגנה סביבתית היות והיעדר בקרות אלו יפגע ביכולת הגוף לזהות נזקים סביבתיים ולמנוע פגיעה ניכרת במערכות שנמצאות בחדר השרתים ובמערכות המידע המנוהלות בו ובמידע האגור בהן.

צוות הביקורת ביקר בחדרי שרתים וחדרי תקשורת, חלקם גופי תמ"ק המונחים על ידי מערך הסייבר. הביקורת בוצעה בחלק מחדרי השרתים וחדרי התקשורת של גופים אלו - חלקם מצויים במטה הגוף וחלקם מצויים במתקנים משניים - ונמצאו פערים בחלק מגופי התמ"ק שנבדקו, בהיבטים שבהם קיימים פערים בהנחיות לגופי התמ"ק.

נמצא כי בחלק מגופי התמ"ק שנבדקו בביקורת קיימים פערים בהיבטים של רציפות תפקודית ושל הגנה פיזית וסביבתית על חדרי שרתים וחדרי תקשורת בגופי תמ"ק.

נוכח הפערים שהתגלו בגופי התמ"ק הפועלים בהנחיית מערך הסייבר, ומאחר שהשב"כ פועל במועד הביקורת לעדכון התו"ל הייעודי של גופי התמ"ק, שנמצאו פערים בתיקופו - על מערך הסייבר והשב"כ לקדם אסדרה בהיבטי הגנה סביבתית ולהשלים את האסדרה החסרה בהיבטי הרציפות התפקודית וההגנה הפיזית על חדרי שרתים וחדרי תקשורת. זאת, באמצעות עדכון הנחיות התו"ל הייעודי או פרסום הנחיות מחייבות ייעודיות בנושאים אלה, לרבות באמצעות שילוב ההנחיות בבקרות שהמאסדרים מבצעים בגופי התמ"ק ובמדדים שגופים אלה נמדדים על פיהם. לעניין זה מומלץ כי בבואם של מערך הסייבר והשב"כ לקבוע הנחיות בנושא מומלץ כי הן ישענו על הנורמות המקובלות בעולם, כפי שאף מנחה הממשלה בהחלטתה (החלטה 2443), הכוללות 12 בקרות בסיסיות בהיבטי ההגנה הפיזית וההגנה הסביבתית על חדרי שרתים ותקשורת והרציפות התפקודית. נוסף על כך, מומלץ כי מערך הסייבר והשב"כ יפעלו לתיקון הפערים שנמצאו בתיקוף התו"ל הייעודי.

מערך הסייבר מסר בתשובתו כי הצורך בעדכון ובתיקוף של התו"ל הייעודי ייבדק במסגרת תוכנית העבודה לשנת 2026. כמו כן, כאמור, המערך יקיים עבודת מטה בנושאי רציפות תפקודית והגנה סביבתית, ובמסגרת עבודת המטה יבחן את ההמלצות בדוח הביקורת ובהתאם לכך יגבש המלצות להמשך. כמו כן, כאמור השב"כ מסר בתשובתו כי בימים אלה פועלים גורמי המקצוע לכתיבתו של תו"ל חדש בו יתוקפו כלל הנושאים לרבות מול נורמות מקובלות בעולם.

פעולות הפיקוח בגופי תמ"ק בנושא ההגנה הפיזית של מערך הסייבר

בהתאם לסעיף 15 לחוק להסדרת הביטחון, מערך הסייבר הוא בעל סמכויות פיקוח על הגוף המונחה ורשאי להיכנס בכל עת לגוף המונחה ולבדוק את עמידתו בהנחיותיו.

מערך הסייבר מפקח על גופי תמ"ק באמצעות מנחה מטעמו. המנחה בוחן את עמידת הגוף המונחה בדרישות התו"ל הייעודי באמצעות בקרות ועל פי מדדים שנקבעו.

מערך הסייבר מנהל את ממצאי הבדיקה של העמידה בתו"ל הייעודי באמצעות גיליונות אקסל (להלן - "קובצי הבקרה") ללא מבנה קבוע, ללא ציון מועד הבדיקה האחרונה, עורך הבדיקה, האתרים שנבדקו ותוצאות הבדיקה שלפניה. כמו כן, מערך הסייבר מדווח פעם בשנה לוועדת היגוי עליונה להגנה על מערכות ממוחשבות במדינת ישראל[13] על רמת עמידתו של הגוף בתו"ל הייעודי, כאשר בפועל המערך מבצע פעם בשנתיים הערכה מחדש בעניין עמידת הגוף בנושא.

נוסף על כך, בכל שנה המנחה מטעם מערך הסייבר מגבש, בשיתוף גורמי המקצוע בגוף המונחה, תוכנית עבודה בנושאים הקשורים לשיפור אבטחת המידע והסייבר, ונדרש לאשרה בוועדת היגוי הסייבר של הגוף המונחה. בסוף השנה המנחה נדרש לבדוק את מידת העמידה ביעדים שנקבעו בתוכנית העבודה.

מערך הסייבר ציין כי במסגרת הבדיקה שלו לגבי עמידת הגוף המונחה בדרישות התו"ל הייעודי בעניין ההגנה הפיזית על חדרי השרתים וחדרי התקשורת, המנחים מטעמו מבצעים סיורי שטח, יחד עם ממונה הביטחון בגוף המונחה, הן בחדר השרתים באתר המרכזי והן במספר אתרי לוויין מרוחקים וכן מנחים לפעול על פי דרישות התו"ל הייעודי גם ביתר החדרים. אולם מערך הסייבר לא תיעד את הסיורים או ההנחיות שניתנו בנושא ביחס ליתר החדרים. כמו כן, מערך הסייבר שמשתתף בוועדות היגוי סייבר, שמטרתן להעלות לפני גורמי ההנהלה את סיכוני הסייבר המשמעותיים בגוף ולטפל בהם, לא דיווח להנהלה בגוף המונחה על ליקויים בנושא הגנה פיזית. נוסף על כך הוא לא קבע לוחות זמנים לתיקונם או למתן מענים מפצים עד לתיקון מלא שלהם, שכרוך לעיתים בהקצאת משאבים והחלטות הנהלה.

צוות הביקורת מצא בחלק מגופי תמ"ק שמנחה מערך הסייבר פערים בנוגע לפעולות ההנחיה והפיקוח שהתקיימו בשלוש השנים שקדמו למועד הביקורת בנושאי הגנה פיזית שבהם קיימות הנחיות בתו"ל הייעודי.

פערים שנצפו בביקורת בפועל בהגנה הפיזית: הועלה כי בחלק מגופי התמ"ק נצפו פערים בהיבטי ההגנה הפיזית על חדרי השרתים וחדרי התקשורת לעומת ההנחיות הקיימות, וכי פערים אלה לא הופיעו בקובצי הבקרה של מערך הסייבר.

נמצא כי הפיקוח שמקיים מערך הסייבר על עמידת הגוף המונחה בבקרות התו"ל הייעודי הקיימות בנושא הגנה פיזית של חדרי השרתים וחדרי התקשורת, טעון שיפור בכמה היבטים:

[13] בהחלטת הממשלה ב/84 משנת 2002 נקבע כי יש להקים ועדת היגוי עליונה להגנה על מערכות ממוחשבות במדינת ישראל, שתפקידה לבחון אילו גופים יוגדרו "חיוניים" ולכן זקוקים להגנה קיברנטית. האחריות להגנה זו הוטלה על השב"כ ובשנת 2017 עברה למערך הסייבר במסגרת תיקון לחוק להסדרת הביטחון.

1. **בשלוש השנים שקדמו למועד הביקורת (התקופה שנבדקה בביקורת), נמצאו פערים בפעולות ההנחיה והפיקוח שקיים מערך הסייבר בנושא הגנה פיזית על חדרי שרתים ותקשורת בגופי התמ"ק שנבדקו.**

2. **מערך הסייבר מנהל את הבקרות לגבי עמידת הגוף המונחה בדרישות התו"ל הייעודי באמצעות טבלאות אקסל (קובצי הבקרה). הטבלאות אינן במבנה קבוע, והן חסרות מידע בנוגע לפעולות הבקרה שנעשו: למשל, בחלק מהטבלאות לא מצוין עורך הבדיקה, סטטוס הבדיקה שלפניה, מועד הבדיקה האחרון של סעיף הבקרה או האתרים שנכללו בבדיקה.**

3. **מערך הסייבר לא כלל בקובצי הבקרה פערים מסוימים שמצא משרד מבקר המדינה בהיבטי הגנה פיזית בחלק מגופי תמ"ק שנבדקו ושמונחים על ידי מערך הסייבר, אף שהמשמעות של פערים אלה היא אי-עמידת הגופים בהנחיות התו"ל הייעודי.**

4. **מערך הסייבר שמנחה מקצועית את גופי התמ"ק ומשתתף בוועדות היגוי סייבר שמטרתן להעלות לפני גורמי ההנהלה את סיכוני הסייבר המשמעותיים בגוף ולטפל בהם, לא דיווח להנהלה בגוף המונחה הרלוונטי על ליקויים בנושא הגנה פיזית. כמו כן, הוא לא קבע לוחות זמנים לתיקונם או למתן מענים מפצים עד לתיקון מלא שלהם, שכרוך לעיתים בהקצאת משאבים והחלטות הנהלה.**

יצוין כי בעקבות הביקורת מערך הסייבר החל לכלול בדיווח להנהלת הגוף המונחה את המצב בפועל של ההגנה הפיזית.

על מערך הסייבר לבדוק את חדרי השרתים וחדרי התקשורת של הגופים שהוא מנחה בהיבטי ההגנה פיזית עליהם, בין בעצמו ובין באמצעות הנחיית הגוף המונחה לביצוע בדיקה משלימה לגבי החדרים שלא נבדקו (לרבות בעניין אופן הבדיקה), קבלת הממצאים, מעקב ובקרה על תיקון הפערים. כמו כן, מומלץ כי מערך הסייבר ינהל קובצי בקרה הכוללים את כלל הפערים בכל מתקני הגוף המונחה ופירוט הכרחי של פעולות הבקרה שנעשו (למשל, עורך הבדיקה, מועד הבדיקה, האתר מושא הבדיקה, המצב הקודם, המצב הקיים, פעולות לתיקון ולוחות זמנים לביצוע). זאת כדי שמערך הסייבר יחזיק בתמונה כוללת המשקפת את מצב הגופים המונחים לאשורו ויוכל להניע את הגופים לצמצום הפערים ולשיפור רמת ההגנה שלהם. עוד מומלץ כי מערך הסייבר ימשיך לדווח לגורמי ההנהלה בגופים המונחים על ליקויים בנושא ההגנה הפיזית ויגדיר לוחות זמנים לתיקונם או מתן מענים מפצים עד לתיקון מלא של הליקויים.

על גופי התמ"ק שנבדקו בביקורת לפעול לתיקון הליקויים שנמצאו בה, לשם שמירה על רציפות תפקודית וההגנה הפיזית והסביבתית על חדרי שרתים ותקשורת.

הרשות להגנת הפרטיות - הנחיה ופעולות פיקוח על מאגרי מידע בתחומי ההגנה פיזית, ההגנה סביבתית והרציפות התפקודית

הנחיות הרשות להגנת הפרטיות

נורמות מקובלות בנושא אבטחת מידע (תקן ISO 27001; תורת ההגנה 2.0; ותקן NIST 800-53) כוללות 12 בקרות בסיסיות באבטחת מידע בהיבטי ההגנה הפיזית וההגנה הסביבתית על חדרי שרתים ותקשורת והרציפות התפקודית.

הרשות להגנת הפרטיות היא כאמור רגולטור כלל משקי ומופקדת על הגנת הזכות לפרטיות, ובכלל זה על אבטחת המידע בכלל מאגרי המידע המנוהלים בתשתיות ממוחשבות הכוללים מידע אישי בישראל. אבטחת מידע מוגדרת בחוק הגנת הפרטיות כ"הגנה על שלמות המידע האישי או הגנה על המידע האישי מפני עיבוד, ללא רשות כדין". "שלמות המידע" מוגדרת כ"זהות הנתונים במאגר מידע למקור שממנו נשאבו, בלא ששונו, נמסרו או הושמדו ללא רשות כדין"; ו"עיבוד" מוגדר

כ"כל פעולה שמבוצעת על מידע אישי, לרבות קבלתו, איסופו, אחסונו, העתקתו, עיון בו, גילויו, חשיפתו, העברתו, מסירתו או מתן גישה אליו". כלומר, אבטחת מידע כוללת, בין היתר, שמירה על סודיות המידע, מהימנות המידע וזמינות המידע (במובן של אי השמדתו) וכן הגנה גם בהקשר של פעולות הנוגעות לאחסונו של המידע. מעבר להוראות חוק הגנת הפרטיות והתקנות שהותקנו מכוחו, הרשות מפרסמת בהתאם לצורך ולשיקול דעתה המקצועי מסמכי מדיניות שונים, לרבות הנחיות או המלצות ומדריכים.

בהתאם לתקנות אבטחת מידע, מאגרי המידע מסווגים לפי שלוש רמות אבטחת מידע - בסיסית, בינונית וגבוהה ובהתאם לקביעת דרישות האבטחה, כדלהלן:

1. **רמת אבטחה בינונית:** לדוגמה מאגרי מידע של גופים ציבוריים או מאגרי מידע המכילים למשל מידע רפואי או דעות פוליטיות או מידע על עבר פלילי בהתאם לאמור על פי חוק.

2. **רמת אבטחה גבוהה:** מאגרי מידע בעלי רמת אבטחה בינונית המכילים מידע על אודות 100,000 אנשים ויותר או שמספר בעלי ההרשאה בהם גדול מ-100.

3. **רמת אבטחה בסיסית:** מאגרי מידע שלא חלה עליהם רמת אבטחה בינונית או גבוהה ואינם מאגרים המנוהלים על ידי יחיד[14].

יש גופי תמ"ק וגופים חיוניים בעלי שליטה במאגרי מידע המסווגים ברמת אבטחה גבוהה, ובהם מאגרי מידע הכוללים מידע אישי בעל רגישות מיוחדת על כלל תושבי המדינה, מהלידה ועד הפטירה.

תקנה 6 בתקנות אבטחת מידע, שכותרתה "אבטחה פיזית וסביבתית", כוללת הוראות בנושא הגנה פיזית על חדרי שרתים ותקשורת. בעניין רציפות תפקודית אין תקנות. כמו כן, בנושאים אלה אין הנחיות או המלצות של הרשות להגנת הפרטיות.

1. תקנה 6(א) לתקנות אבטחת מידע חלה על תשתיות ומערכות חומרה, סוגי רכיבי תקשורת ואבטחת מידע המשרתות מאגרי מידע בכל רמות האבטחה - בסיסית, בינונית וגבוהה - וקובעת כי מערכות המאגר האלה יישמרו במיקום מוגן המונע חדירה וכניסה אליו בלא הרשאה והתואם את אופי פעילות המאגר ורגישות המידע שבו.

2. תקנה 6(ב) לתקנות אלה חלה על תשתיות ומערכות חומרה, סוגי רכיבי תקשורת ואבטחת מידע המשרתים מאגרי מידע ברמות אבטחה בינונית וגבוהה. התקנה קובעת כי יש לנקוט אמצעים לבקרה ולתיעוד של הכניסה לאתרים שבהם נמצאים בין היתר תשתיות ומערכות חומרה וסוגי רכיבי תקשורת ואבטחת מידע, היציאה מהם, הכנסה של ציוד אל מערכות המאגר והוצאת ציוד מהן.

3. למרות כותרת התקנה - "אבטחה פיזית וסביבתית" - אין בה התייחסות להיבטי הגנה סביבתית. כמו כן, התקנה אינה עוסקת בהיבטי רציפות תפקודית.

לשם ההדגמה, הרשות להגנת הפרטיות משמשת כמאסדרת בתחום אחר - חתימה אלקטרונית, זאת מכוח חוק חתימה אלקטרונית, התשס"א-2001 (להלן - חוק חתימה אלקטרונית). בין יתר תחומי ההסדרה בהם עסקה הרשות בהקשר זה במסגרת סמכויותיה לגבי הגורמים המאשרים - הגופים המנפיקים תעודות אלקטרוניות (להלן - הגורמים המאשרים) - ראש הרשות להגנת הפרטיות, בתפקידו כרשם הגורמים המאשרים, פרסם מסמך דרישות לגבי "הגורם המאשר".

[14] בהתאם לתקנות אבטחת המידע, מאגר מידע שמנהל יחיד או תאגיד בבעלות יחיד ורק היחיד ולכל היותר שני בעלי הרשאות נוספים רשאים להשתמש בו וכאמור במגבלות הקבועות שם.

במסמך הוא התייחס ל-12 הבקרות הנכללות בשלושת הנושאים שנבדקו בביקורת זו (הגנה פיזית, הגנה סביבתית ורציפות תפקודית), נוסף על חובה לעמוד בהוראות תקן ISO27001. ההתייחסות נשענת על תקנים בין-לאומיים הנוגעים לחדרים מסווגים המשמשים לחתימה אלקטרונית. מטרת המסמך לסייע לגורמים שמבקשים מראש הרשות אישור לשמש גורם מאשר בהתאם לסעיף 10 לחוק חתימה אלקטרונית, התשס"א-2001, לעמוד בדרישות החוק ובהנחיות רשם הגורמים המאשרים[15], הרשאי להנפיק תעודה אלקטרונית מאושרת (להלן - מסמך דרישות לגורם מאשר).

נמצא כי בהיעדר תקנות בהיבטי הגנה סביבתית ורציפות תפקודית, הרשות להגנת הפרטיות המאסדרת בתחום אבטחת המידע בכלל מאגרי המידע המנוהלים בתשתיות ממוחשבות וכוללים מידע אישי בישראל, לא פרסמה לכלל המשק הנחיות או המלצות לאבטחת מאגרי המידע בהיבטים אלה לצורך הגנה על שלמות המידע וסודיותו, זאת אף עבור מאגרי מידע ברמת אבטחה גבוהה. כמו כן, בנוגע להיבטי הגנה פיזית, למעט ההוראה החלקית הקבועה בתקנה 6 לתקנות אבטחת מידע, הרשות לא פרסמה הנחיות בנושאים הכלולים בנורמות מקובלות. יצוין לשם ההדגמה כי בתחום אחר, חתימה אלקטרונית, הרשות להגנת הפרטיות נתנה מענה על שלושת הנושאים - הגנה פיזית, הגנה סביבתית ורציפות תפקודית - ופרסמה הנחיות מפורטות לאבטחת מערכות המידע מפני סיכונים של חדירה, שיבוש, הפרעה או גרימת נזק למערכת המידע או למידע השמור בה.

בתשובת הרשות להגנת הפרטיות למשרד מבקר המדינה מאוקטובר 2025 נמסר כי במסגרת קבלת ההחלטה בנוגע לפרסום הנחיה או כל מסמך רגולטורי אחר בנושא מסוים מובאת בחשבון, בין השאר, השאלה אם ההוראות הרלוונטיות בחוק ובתקנות ברורות ובהירות או שנדרשת לגביהן פרשנות משפטית, מהן המגמות וההתפתחויות בתחום, האם קיים בסיס משפטי המאפשר לרשות לגבש מסמך מדיניות בנושא מסוים, האם קיימים פערים וככל שכן - מהן ההשלכות של פערים אלה. כמו כן, פרסום הנחיות וקיום פעולות אכיפה מתבצעים בשים לב לסדרי העדיפויות של הרשות הנקבעים באופן שוטף, לנושאי מיקוד של הרשות, לחלוקת משאבים ולשיקולים מקצועיים נוספים.

בתשובה נוספת ממרץ 2026 נמסר כי ההשוואה בין חוק חתימה אלקטרונית לבין החוק להגנת הפרטיות והתקנות מכוחו שגויה מיסודה, אינה מתיישבת עם לשון הדין ותכליתו, היות ומדובר בשני הסדרים נורמטיביים שונים בתכליתם, במבנה הסמכויות, במודל הפיקוח ובהיקף ההתערבות הרגולטורית. העובדה ששני החוקים מצויים תחת אחריותה של אותה רשות מינהלית אינה יוצרת אחידות נורמטיבית ביניהם ואינה מרחיבה את היקף החובות שבחוק הגנת הפרטיות מעבר ללשונו ותכליתו.

לעמדת הרשות להגנת הפרטיות, תכלית החוק להגנת הפרטיות והתקנות מכוחו, אשר מגדיר "אבטחת מידע" כ"הגנה על שלמות המידע האישי או הגנה על המידע האישי מפני עיבוד, ללא רשות כדין", ממוקדת בשני רכיבים בלבד: שלמות המידע ומניעת עיבוד בלתי מורשה. לפיכך, החוק להגנת הפרטיות והתקנות מכוחו אינם כוללים רכיב של זמינות מערכות או דרישה לרציפות תפקודית. לעומת זאת בחוק חתימה אלקטרונית הזמינות והרציפות התפקודית מצויות בליבת האסדרה, שכן מדובר בתשתית אמון ציבורית שמטרתה לאפשר החלפת חתימה פיזית בחתימה אלקטרונית מאושרת. מסמך דרישות לגורם מאשר מכוח חתימה אלקטרונית נועד לשרת את דרישות אותו חוק בלבד ואינו משמש אמת מידה פרשנית או מקור נורמטיבי ליישום תקנות הגנת הפרטיות.

משרד מבקר המדינה מציין כי הביקורת בחנה את האסדרה הקיימת של הרשות להגנת הפרטיות בתחום אבטחת מאגרי מידע הכוללים מידע אישי מכוח חוק הגנת הפרטיות ותקנותיו אל מול נורמות מקובלות בנושא אבטחת מידע (תקן ISO 27001; תורת ההגנה 2.0; ותקן NIST 800-53), שכוללות 12 בקרות בסיסיות באבטחת מידע בהיבטי ההגנה הפיזית וההגנה הסביבתית על חדרי שרתים ותקשורת והרציפות התפקודית.

---

[15] רשם הגורמים המאשרים - רושם ומנהל המרשם של הגורמים המאשרים ומפקח על הגורמים המאשרים, הכול לפי הוראות חוק חתימה אלקטרונית, התשס"א-2001.

המקור הנורמטיבי ליישום תקנות הגנת הפרטיות הוא חוק הגנת הפרטיות עצמו, בו מוגדרת "אבטחת מידע" כ"הגנה על שלמות המידע האישי או הגנה על המידע האישי מפני עיבוד ללא רשות כדין", כאשר "שלמות המידע" מוגדרת כ"זהות הנתונים במאגר מידע למקור שממנו נשאבו, בלא ששונו, נמסרו או הושמדו ללא רשות כדין" ו"עיבוד" מוגדר ככל פעולה שמבוצעת על מידע אישי, לרבות אחסונו. כלומר, אבטחת מידע כוללת שמירה על זמינות המידע במובן של אי השמדתו וכן הגנה בהקשר של פעולות הנוגעות לאחסונו של המידע ולפיכך מתייחס גם להיבטי הגנה סביבתית ורציפות תפקודית. נוסף לכך, ההתייחסות בביקורת זו לתחום החתימה האלקטרונית הובאה לשם ההדגמה בלבד כי בתחום אחר הרשות להגנת הפרטיות הגדירה דרישות בשלושת היבטים אלה (ביחס לכל 12 הבקרות).

על הרשות להגנת הפרטיות לבחון את הפערים באסדרה הקיימת בתחום אבטחת מאגרי המידע אל מול נורמות מקובלות בתחום אבטחת המידע, הכוללות 12 בקרות בסיסיות באבטחת מידע בהיבטי ההגנה הפיזית וההגנה הסביבתית על חדרי שרתים ותקשורת והרציפות התפקודית. ובכלל זה מומלץ שתקדם אסדרה בהיבטי הגנה סביבתית ורציפות תפקודית ותשלים את האסדרה בהיבטי הגנה פיזית (נוסף על הקבוע בתקנה 6 לתקנות אבטחת מידע) לגבי כלל מאגרי המידע המנוהלים בתשתיות ממוחשבות, ובפרט לגבי המאגרים שרמת אבטחתם גבוהה (בין באמצעות בחינה אם לקדם את הרחבת התקנות ובין באמצעות פרסום הנחיות או המלצות במסגרת מדריכים מטעמה). זאת באופן שיבטיח את ההגנה הנדרשת על שלמות המידע וסודיותו במאגרים רגישים המכילים מידע בהיקף נרחב, בהתאם לחוק הגנת הפרטיות והתקנות מכוחו, כלומר הגנה על זהות הנתונים למקור שממנו נשאבו "בלא ששונו, נמסרו או הושמדו ללא רשות כדין" ובהיבטי אחסון המידע.

פעולות הפיקוח של הרשות להגנת הפרטיות

לרשות להגנת הפרטיות מוקנות סמכויות לבצע אכיפה ולבחון את מידת עמידתם של גופים בכל הוראות החוק להגנת הפרטיות ותקנותיו, לרבות תקנות הגנת אבטחת מידע. בידי הרשות להגנת הפרטיות קיים מנעד רחב של כלי פיקוח ואכיפה, ובהם - אכיפה פלילית, פיקוח רוחב ופיקוח מינהלי. זאת, לצורך איתור ליקויים, הפקת תמונת מצב מגזרית בנוגע לעמידה בהוראות חוק הגנת הפרטיות ובתקנות ואיתור כשלים הטעונים אסדרה.

משנת 2018 מפעילה הרשות להגנת הפרטיות מערך פיקוח רוחבי (Audit). בעקבות תיקון 13 לחוק הגנת הפרטיות ועיגונו של פיקוח הרוחב בחקיקה ראשית, אופיין ההליך מחדש וחוזק מעמדו ככלי אכיפה מרכזי של הרשות להגנת הפרטיות. מדובר בהליך אשר נועד בעיקרו להגביר את המודעות והציות לחוק ולתקנות בקרב הגופים המפוקחים; להסיק מסקנות בדבר דגשים נדרשים לצמצום הפערים הקיימים, הן ברמת הגופים המפוקחים והן ברמת המגזר; להציג תמונת מצב לציבור בנוגע לדרישות הציות מהמגזר הנבחר לגבי הגנת הפרטיות ואבטחת המידע; לאתר פערי ציות מערכתיים ומגזריים; וכן להניח תשתית לנקיטת צעדי אכיפה מנהליים, ככל שיידרש. לצד תכליתו ההסברתית וההכוונתית, מהווה ההליך כלי לאיתור הפרות ולהפעלת סמכויות האכיפה המוקנות לרשות, לרבות הטלת עיצומים כספיים בהתאם להוראות החוק.

מחלקת האכיפה ברשות להגנת הפרטיות מבצעת בכל שנה פיקוח רוחב על שישה מגזרים שנבחרים על בסיס סקר סיכונים שנתי שמבצעת הרשות. כל פיקוח רוחב נעשה בכ-20 עד 80 גופים מדגמיים מכל מגזר שנבחר (בהתאם לגודל המגזר), ובסיומו נשלחות לגוף המפוקח המלצות לשיפור (על פי עמידת הגוף המפוקח בקריטריונים המשקפים מודעות וציות לתקנות אבטחת מידע בהתאם למענה שמסר הגוף המפוקח). במקרים המתאימים, ככל שמתגלים ממצאים המעידים על הפרות מהותיות, רשאית הרשות לשקול נקיטת הליכים מנהליים, לרבות פתיחה בהליך בירור והטלת עיצומים כספיים בהתאם לסמכויותיה על פי דין. נוסף על כך, מפרסמת הרשות להגנת הפרטיות דוחות מסכמים ברמה המגזרית, במטרה לשקף לציבור את תמונת המצב, להבהיר את דרישות הציות המצופות מהמגזר הנבחן, ולתרום לשיפור מתמשך ברמת ההגנה על מידע אישי במשק.

פיקוח רוחב: בחמש השנים האחרונות, עד אפריל 2025, ביצעה הרשות להגנת הפרטיות פיקוח רוחב שכלל חלק מגופי התמ"ק שנבדקו בביקורת זו. אשר למשרדי הממשלה, הרשות לא ביצעה

באותה תקופה פיקוח רוחב בהם, אלא התמקדה בפיקוח רוחבי בענפים שונים במגזר הפרטי ובגופים ציבוריים שאינם משרדי ממשלה (ובהם בתי חולים, רשויות מקומיות, תאגידי מים וגז).

פיקוח מינהלי: במהלך תקופה זו הרשות קיימה הליכי פיקוח מינהלי בכמה משרדי ממשלה ובחלק מגופי התמ"ק שנבדקו בביקורת זו (הליכים אלה התקיימו בעקבות הליך יזום של הרשות, בעקבות דיווח על אירועי אבטחת מידע, בעקבות ידיעה על אירוע ללא דיווח או בעקבות הגשת תלונה). הליכי הפיקוח המינהלי התמקדו בהיבטים לוגיים, ולא בוצעה בעניינם בדיקה בנושאי הביקורת (הגנה פיזית) מכוח תקנה 6 לתקנות אבטחת מידע.

בנוגע לגורמים מאשרים, הרשות להגנת הפרטיות מחייבת ביצוע סקר אבטחה מלא על ידי גורם חיצוני ובלתי תלוי אחת לשנה, הכולל את הבקרות הנדרשות בנושא הגנה פיזית, הגנה סביבתית ורציפות תפקודית, וכן העברת ממצאי הסקר לרשות.

נמצא כי במהלך חמש שנים, עד אפריל 2025, הרשות להגנת הפרטיות לא ביצעה כלל פעילות פיקוח רוחב בכל משרדי הממשלה (100%) ובחלק מגופי התמ"ק שנבדקו בביקורת זו, לשם בחינת ההגנה הקיימת על השלמות והסודיות של המידע המצוי במאגרי המידע המנוהלים בתשתיות ממוחשבות. זאת אף שחלק ממאגרי המידע הם מאגרי מידע גדולים ומשמעותיים של גופים ציבוריים ובהם מצוי מידע אישי בעל רגישות מיוחדת על כלל תושבי המדינה, מהלידה ועד הפטירה. כמו כן, במסגרת הליכי הפיקוח המינהלי שהרשות ביצעה בתקופה זו היא לא כללה היבטים בנושאי הביקורת (הגנה פיזית) בהתאם לתקנה 6 לתקנות אבטחת מידע.

בתשובת הרשות להגנת הפרטיות מאוקטובר 2025 נמסר כי לנוכח המשאבים המוגבלים שברשותה, היא משקיעה את משאביה בנושאים בעלי השפעה רוחבית שנשקפת בגינם סכנה ניכרת לפרטיות. הרשות תבחן באופן עצמאי ובהתאם לשיקול דעתה את הצורך לבצע פעילויות פיקוח שיכללו היבטי הגנה פיזית והגנה סביבתית על חדרי שרתים ותקשורת. כמו כן, בתשובתה מפברואר 2026 נמסר כי היא לא כללה היבטים בנושאי הביקורת (הגנה פיזית) בהליכי הפיקוח המינהלי היות והסוגיות שנבחנו במסגרת הליכי הפיקוח לא העלו צורך לבחון את תקנה 6 לתקנות אבטחת מידע.

לנוכח העובדה כי מאגרי המידע שבידי משרדי ממשלה וגופי תמ"ק מכילים מידע אישי רב בעל רגישות מיוחדת על כלל האוכלוסייה בישראל, מומלץ כי הרשות להגנת הפרטיות תבצע בגופים אלו פעילויות פיקוח ובקרה שיכללו, בין השאר, היבטים משמעותיים בנושא הגנה פיזית על חדרי שרתים ותקשורת הכוללים מאגרי מידע המנוהלים בתשתיות ממוחשבות. זאת, כדי שבידי הרשות להגנת הפרטיות תהיה תמונת מצב בנוגע לעמידה בהוראות החוק והתקנות וכן יכולת לאיתור פערים הטעונים אסדרה לגבי מאגרי המידע.

האסדרה בכל מגזר בהיבטי הגנה פיזית, הגנה סביבתית ורציפות תפקודית

הנחיית יחידות הסייבר המגזריות על ידי מערך הסייבר בתחומי הגנה פיזית, הגנה סביבתית ורציפות תפקודית

כאמור, בהתאם להחלטת הממשלה 2443, מערך הסייבר אחראי להנחיה מקצועית של יחידות הסייבר המגזריות, לרבות יה"ב, ולפיכך נדרש לבצע בקרה על יישום הנחיותיו ליחידות.

מערך הסייבר פרסם המלצה ליחידות הסייבר המגזריות ליישם את תורת ההגנה (מדריך יישומי להגנת הסייבר בארגון, שפרסם מערך הסייבר בשנת 2021 לכלל המשק), הכוללת הנחיות בנושאים של הגנה פיזית, הגנה סביבתית ורציפות תפקודית. בפועל, כל יחידה מגזרית כתבה הנחיות לגופים המונחים שלה באופן עצמאי בהתאם ליכולותיה ולמשאביה ובהתאם לייחודיות של כל מגזר ושילבה בהן חלקים מהנחיות מערך הסייבר כפי שמצאה לנכון. כעולה מלוח 3 שלעיל, יש שונות בנושאים הכלולים בהנחיות של כל יחידה מגזרית, והן אינן כוללות התייחסות לכל הנושאים שכלולים בתורת ההגנה.

נוסף על כך, אחת לשנה כאמור מערך הסייבר מפרסם מסמכי עוגנים שנתיים בנושאים עיקריים שיחידות הסייבר המגזריות יקדמו בתוכניות העבודה. בעניין הרציפות התפקודית, הייתה דרישה כללית לשנת 2025 מיחידות הסייבר המגזריות לגבש רשימה של המערכות והתהליכים התפעוליים המזעריים הנדרשים לרציפות תפקודית ובניית מענה לשרידותם.

נמצא כי אף שבהחלטת הממשלה 2443 נקבע כי מערך הסייבר הוא המנחה המקצועי של יחידות הסייבר המגזריות, מערך הסייבר הסתפק בהנחיה לא מחייבת (המלצה) ליחידות הסייבר המגזריות ליישם את תורת ההגנה הכוללת הנחיות לגבי הגנה פיזית והגנה סביבתית על חדרי שרתים ותקשורת ולגבי רציפות תפקודית. בדומה לכך, ייתכן שההנחיות שמספקות היחידות המגזריות לגופים שלהן לא יכללו נדבכים יסודיים הקיימים בנורמות מקובלות, ואין ביכולתו של מערך הסייבר לפקח על כך שנדבכים אלו מטופלים.

בתשובת מערך הסייבר נמסר כי בהתאם להחלטת הממשלה יש חלוקה ברורה ולפיה היחידה המגזרית נדרשת לפעול מול המגזר המונחה ולקבוע מתודולוגיית הגנה ולבקר אחר יישומה. כמו כן, לאור השונות בין המגזרים והגופים הנכללים בהם, הנחייה מקצועית מנוסחת בצורה רכה יותר ומאפשרת נקיטה בפתרונות חלופיים או בקרות מפצות, אולם לדעת מערך הסייבר אין בכך כדי להפחית מתוקף ההנחיה או ממעמדו של המנחה.

מומלץ כי מערך הסייבר יקבע הנחיות בסיסיות מחייבות ליחידות הסייבר המגזריות בנדבכים עיקריים הנוגעים להגנה פיזית ולהגנה סביבתית על חדרי שרתים ותקשורת וכן בהיבטי רציפות תפקודית, ואלו יהוו בסיס לפיקוח שיבוצע ביחידות הסייבר המגזריות. לגבי יחידות הסייבר המגזריות, הן ינחו את הגופים המונחים בהתאם להנחיות הבסיסיות ויוכלו להרחיב הנחיות אלה בהתאם לסמכויותיהן, למאפייני המגזר ולסיכוניו.

ההנחיות של יחידות הסייבר המגזריות בתחומי הגנה פיזית, הגנה סביבתית ורציפות תפקודית

במסגרת ביקורת זו נבחנה האסדרה הקיימת בשישה מגזרים.

כאמור, יחידות הסייבר המגזריות מונחות על ידי מערך הסייבר. המערך פרסם המלצה ליחידות הסייבר המגזריות ליישם את תורת ההגנה וכן פרסם ליחידות מפעם לפעם הנחיות מחייבות בנושאים שונים, אך הן לא כללו הנחיות פרטניות בנושא חדרי שרתים וחדרי תקשורת. מאחר שתורת ההגנה היא בגדר המלצה, כל יחידה מגזרית כתבה הנחיות לגופים המונחים שלה באופן עצמאי בהתאם ליכולותיה ולמשאביה ובהתאם לייחודיות של כל מגזר ושילבה בהן חלקים מהנחיות מערך הסייבר כפי שמצאה לנכון, כמפורט בלוח 3 שלעיל.

יצוין כי נוסף על הנחיות כמפורט בלוח 3 שלעיל, הגופים המונחים על ידי שתי יחידות סייבר מגזריות מחויבים לקבל הסמכה לגבי עמידה בתקן ISO27001, שכולל כאמור את כלל הבקרות בנושאי הביקורת. הבדיקה לצורך ההסמכה לתקן זה מבוצעת על ידי גוף מוסמך חיצוני (מכון התקנים הישראלי וגופים אחרים). עם זאת, ההסמכה אינה מחייבת עמידה של הגוף בכל הדרישות של התקן ויכולה לכלול דרישות לתיקון ליקויים בפרק זמן מוגדר.

נמצא כי חמש (83%) משש יחידות הסייבר המגזריות שנבדקו בביקורת הוציאו הנחיות חלקיות בלבד בנוגע לאבטחת חדרי שרתים וחדרי תקשורת; לגבי מגזר אחד אין הנחיות שלפיהן מחויבים גופים אלה לפעול. להלן פירוט הנדבכים החסרים בהנחיות שהוצאו, כמוצג בלוח 3:

1. **מגזר 6: ההנחיות כוללות התייחסות מלאה לכלל היבטי הרציפות התפקודית הרלוונטיים למערכות מידע לרבות פגיעה בחדרי שרתים וחדרי תקשורת, אך אינן כוללות התייחסות להגנה סביבתית על חדרי שרתים ותקשורת, למעט היבט אחד (מקור חשמל חלופי). לגבי ההגנה הפיזית על חדרי שרתים ותקשורת, חסרה התייחסות למיקום הפיזי של החדרים (ומצוינת דרישה להגדיר את ההגנה של מבנה, ללא פירוט נוסף).**

2. **מגזר 3: ההנחיות כוללות התייחסות להיבט הרציפות התפקודית הרלוונטיים למערכות מידע לרבות פגיעה בחדרי שרתים וחדרי תקשורת בלבד ואינן כוללות כל התייחסות להיבטי ההגנה הפיזית וההגנה הסביבתית על חדרי שרתים ותקשורת. נוסף על כך, ההנחיות חלות רק על 7% מהגופים במגזר, ואינן חלות על יתר הגופים שאינם מחויבים בעמידה בהנחיות להגנת הסייבר שפרסמה היחידה המגזרית.**

3. **מגזר 2: ההנחיות כוללות התייחסות חלקית להיבט ההגנה הפיזית על חדרי שרתים ותקשורת (רכיב אחד מארבעה בלבד - בקרת גישה). אשר להיבטי ההגנה הסביבתית על חדרי שרתים ותקשורת ולהיבטי הרציפות התפקודית הרלוונטיים למערכת מידע לרבות פגיעה בחדרי שרתים וחדרי תקשורת, ההתייחסות בכל תחום היא לשלושה מארבעה רכיבים (אין התייחסות לחיישני הצפה ולאתר גיבוי - DR, בהתאמה).**

4. **מגזר 5: ההנחיות כוללות התייחסות להיבט ההגנה הפיזית על חדרי שרתים ותקשורת ולהיבט הרציפות התפקודית הרלוונטיים למערכת מידע לרבות פגיעה בחדרי שרתים וחדרי תקשורת, אך אינן כוללות כל התייחסות להיבט ההגנה הסביבתית על חדרי שרתים ותקשורת.**

5. **מגזר 4: ההנחיות כוללות התייחסות לנושא ההגנה הפיזית על חדרי שרתים ותקשורת, מלבד נושא המיקום הפיזי. אשר לרציפות התפקודית הרלוונטית למערכת מידע לרבות בעקבות פגיעה בחדרי שרתים וחדרי תקשורת - ההנחיות מחייבות את קיומו של גיבוי, אך אינן כוללות הנחיות לגבי כלל הגופים במגזר בנושאי מדיניות המשכיות עסקית והתאוששות מאסון ובנושא קיום אתר גיבוי. כמו כן, ההנחיות אינן כוללות כל התייחסות להיבטי הגנה סביבתית על חדרי שרתים ותקשורת.**

היחידות המגזריות השיבו בנושא ההנחיה כמפורט להלן: בתשובת מגזר 6 למשרד מבקר המדינה מדצמבר 2025 נמסר כי הוא יקיים עבודת מטה כדי לבחון את ההנחיה בנושא הגנה סביבתית על חדרי שרתים ותקשורת. בתשובת מגזר 5 למשרד מבקר המדינה מאוקטובר 2025 נמסר כי במהלך שנת 2026 ייכנס לתוקף נוהל שבמסגרתו יוטמעו הסוגיות שעלו בביקורת בנושא הגנה סביבתית. בתשובת מגזר 4 למשרד מבקר המדינה מספטמבר 2025 נמסר כי הדרישות החסרות בהיבטי הגנה סביבתית שולבו בקובצי הבקרה ויעודכנו בנוהל סייבר בתחילת שנת 2026. בתשובת מגזר 2 למשרד מבקר המדינה מאוקטובר 2025 נמסר כי הוא פועל בשנה האחרונה לשיפור רמת ההמשכיות העסקית.

פערים שנצפו בפועל

משרד מבקר המדינה ביקר בעת הביקורת בכמה גופים בשלוש משש יחידות סייבר מגזריות שנבדקו, ומצא בשתיים מהן (66%) פערים בהגנה הפיזית ובהגנה הסביבתית על חדרי שרתים ותקשורת באותם היבטים שלא הוסדרו כאמור באמצעות נהלים ייעודיים. בארבעה גופים משני מגזרים, שבהם אין הנחיה באחד מהיבטי רציפות תפקודית, נמצאו פערים בנושא זה.

בפועל, בביקורת נמצאו פערים בהגנה הפיזית ובהגנה הסביבתית על חדרי שרתים וחדרי התקשורת וברציפות התפקודית של גופים שמונחים על ידי יחידות הסייבר המגזריות שנבדקו, בהיבטים שלא קיימת אסדרה בעניינם, כמפורט להלן:

א. **נמצאו פערים בנושא רציפות תפקודית בגופים שמונחים על ידי שתיים (66%) משלוש יחידות סייבר מגזריות שנבדקו.**

ב. **פערים בהגנה הפיזית בגופים שמונחים על ידי אחת (33%) משלוש יחידות סייבר מגזריות שנבדקו.**

ג. **פערים בהגנה הסביבתית בגופים שמונחים על ידי אחת (33%) משלוש יחידות סייבר מגזריות שנבדקו.**

על יחידות הסייבר המגזריות האחראיות להנחיית המגזרים בהתאם להחלטת הממשלה 2443, לעדכן את ההנחיות כך שיהיו מלאות ויתייחסו לנושאים החסרים כיום (הגנה פיזית והגנה סביבתית על חדרי שרתים ותקשורת ורציפות תפקודית). זאת באופן שיחייב את הגופים המונחים לפעול על פיהן ויאפשר ליחידות הסייבר המגזריות לפקח על פעילותם של הגופים בנושאים אלה. לעניין זה מומלץ כי בבואן של יחידות הסייבר המגזריות לקבוע נורמות בנושא נכון יהיה כי ישענו על הנורמות המקובלות בעולם, כפי שאף מנחה הממשלה בהחלטתה.

על הגופים החיוניים שנבדקו בביקורת ונמצאו בהם פערים בהיבטי הגנה פיזית וסביבתית על חדרי שרתים ותקשורת ורציפות תפקודית, לפעול לטיפול בפערים בהקדם.

פעולות הפיקוח של יחידות הסייבר המגזריות

בהתאם להגדרת תפקידי יחידות הסייבר המגזריות בנספח ד' להחלטת הממשלה 2443, יחידות הסייבר המגזריות נדרשות לבצע בקרה על ביצוע הדרישות המקצועיות בהתאם לאסדרה וברמה המקצועית הנדרשת.

להלן תהליך הפיקוח של יחידות הסייבר המגזריות בנושאים שנבדקו בביקורת:

1. **מגזר 6:** אחת לשנה הגופים המונחים נדרשים למסור דיווח בהתאם לטבלת בקרות בנושא אבטחת מידע וסייבר וכן את ההסמכה השנתית בתקן ISO27001. כאמור, ההסמכה אינה מחייבת עמידה של הגוף בכל הדרישות של התקן ויכולה לכלול דרישות לתיקון ליקויים בפרק זמן מוגדר ללא בקרה של היחידה.

2. **מגזר 3:** אחת לשנה הגופים המונחים נדרשים למסור ליחידה דיווח ללא בקרה של תוכן הדיווח על ידי היחידה.

3. **מגזר 2:** אחת לשלוש שנים מבצעת היחידה ביקורת בנושא אבטחת מידע בגופים שהיא מנחה, כחלק מהליך ביקורת רישוי כללי, באמצעות שאלות מובנות שעל הגופים להשיב עליהן ללא בקרה של היחידה.

4. **מגזר 5:** הפיקוח מתבצע בהתאם לשלוש רמות קריטיות שונות - ההנחיה והפיקוח בשתי הרמות הגבוהות מתבצעים באופן רציף, וברמה הנמוכה באופן מדגמי. כמו כן, בכל הגופים מתבצעת בדיקה מלאה בעת הקמה.

5. **מגזר 4:** בהתאם לתוכנית העבודה, אחת לשנתיים מבצעת היחידה ביקורת בגופים המונחים, נוסף על ביצוע תרגילי סייבר ואבטחת מידע.

נמצא כי שלוש (60%) מחמש יחידות הסייבר המגזריות שנבדקו דורשות לקבל דיווחים מהגופים המונחים בנוגע לעמידתם בהנחיות, אך אינן מבצעות בקרה על הדיווח, ולכן ייתכנו פערים בין תמונת המצב שבידי יחידות הסייבר המגזריות לבין המצב בפועל. לדוגמה, במיפוי הנתונים של אחת מיחידות הסייבר המגזריות, על בסיס מענה על שאלון ששלחה בנושא רציפות תפקודית, דווח שאחד הגופים עומד בהיבט מסוים בנושא רציפות תפקודית, אולם בפועל, כפי שעולה מבדיקת משרד מבקר המדינה, הגוף אינו עומד בהיבט זה כלל, בניגוד לתמונת המצב שבידי היחידה המגזרית.

מומלץ כי יחידות הסייבר המגזריות שנבדקו ונמצא בהן פער בנוגע לבקרה שהן עושות על ביצוע הדרישות המקצועיות יבצעו פיקוח אפקטיבי שכולל בקרה על דיווחי הגופים המונחים.

בתשובת מגזר 2 נמסר כי הוא חיזק לאחרונה את יכולותיו בתחום הפיקוח והבקרה, בין היתר באמצעות הוספת משרה ייעודית לתקן, בהיקף מלא, לשם ביצוע בקרות שוטפות ומתודולוגיות בגופים. עוד מסר כי החל משנת 2026 מתוכנן מערך בקרות שיכלול ביקורות יזומות אחת לשנה לכל ארגון. מטרת מהלך זה היא להעלות את רמת הפיקוח, לקצר את פרקי הזמן שבין הבקרות, לחזק את ההגנה על נכסי הסייבר ולקדם את הרציפות התפקודית במגזר.

בתשובת מגזר 6 נמסר כי מרבית הבקרות מתבצעות באמצעות שאלונים ודיווח של הגופים המונחים, וכי הוא יבחן את האפשרות לביצוע בקרות פיזיות באופן מדגמי. כמו כן, לקראת תוכנית העבודה לשנת 2026 הגופים יונחו לדווח אם בוצע "תרגיל חם" של מערך ההתאוששות ולכלול תרגיל מסוג זה בתוכנית העבודה השנתית.

בתשובת מגזר 3 למשרד מבקר המדינה מנובמבר 2025 נמסר כי בשנת 2025 החלה היחידה המגזרית לבצע בקרה ייעודית על תוכן דיווחי הגופים שהוגשו למשרד עבור שנת 2024.

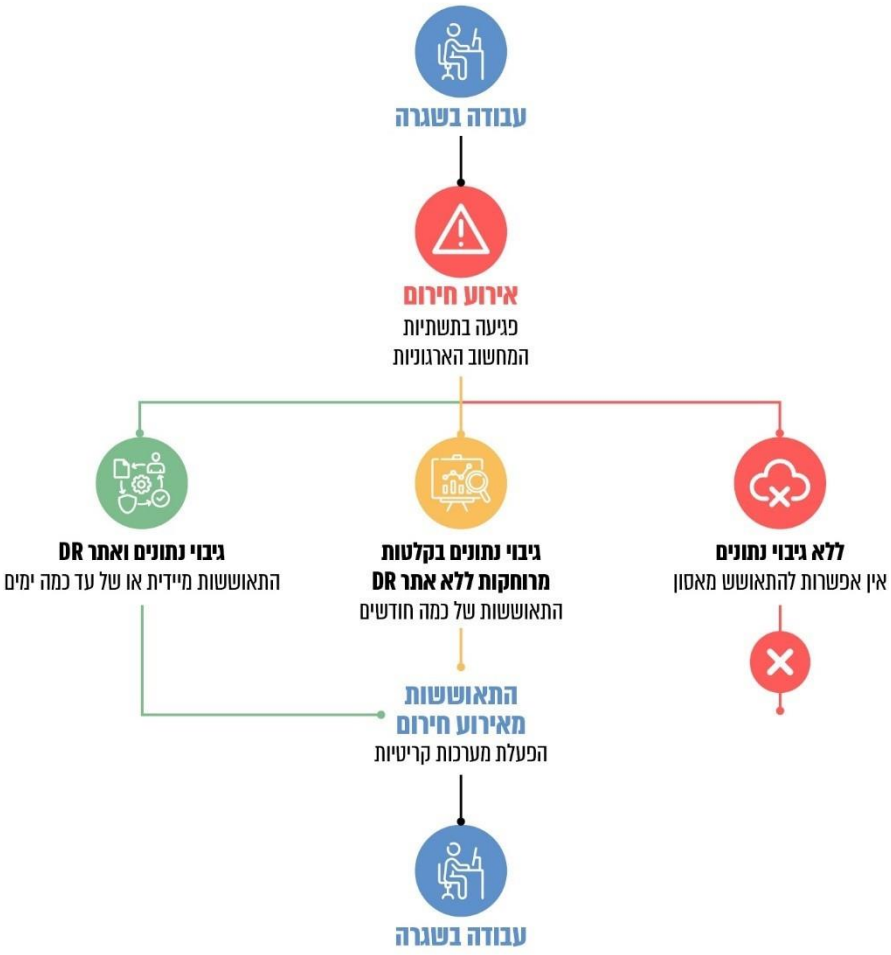
<u>היבטים ברציפות התפקודית של משרדי ממשלה ויחידות סמך בעקבות פגיעה בחדרי שרתים</u>

הרציפות התפקודית של משרדי הממשלה עלולה להיפגע בשל אירועים וגורמים שונים (אירוע סייבר, קריסת מערכות, נפילת תשתיות תקשורת וחשמל, מחסור בעובדים, הגבלות של פיקוד העורף וכיו"ב). ביקורת זו מתמקדת בפגיעה ברציפות התפקודית של משרדי ממשלה שמקורה הוא פגיעה בחדרי השרתים של המשרדים. הסבירות להתממשותה של פגיעה כזאת גדלה במידה ניכרת במלחמת חרבות ברזל, בעקבות אפשרות לפגיעה ישירה של מטח טילים בחדרי השרתים של המשרדים או פגיעה ממושכת בתשתיות חשמל ומים.

כאמור, מעטפת ההגנה של ארגון אינה מונעת לחלוטין את הפגיעה במערכות המידע שלו, ולכן לצד ההגנה המוגברת יש לשמור גם על הרציפות התפקודית של הגוף ועל יכולתו למזער נזקים ולהמשיך לספק את השירותים החיוניים בשעת משבר. לצורך כך על הארגון להיערך למשבר בטרם עת ולגבש תוכנית התאוששות מאסון (DRP) לחידוש פעילות טכנולוגית ומערכות מידע התומכות בתהליכים הקריטיים בארגון. זאת, כחלק מתוכנית ההמשכיות העסקית (BCP) המהווה תוכנית פעולה לתהליכים העסקיים הקריטיים בארגון, לצורך התאוששות מלאה או חלקית בפרק זמן וברמת שירות התואמים את מדיניות הארגון (מדיניות המשכיות עסקית). בכלל זה - על הארגון לוודא יכולת שחזור מהירה של תשתיות מערכות המידע שלו ולהיערך מבחינת תשתיות חלופיות באתרים חלופיים (כולל זמינות ויתירות).

לפי נורמות מקובלות, בהיבטי רציפות תפקודית, כמפורט לעיל, יכולת השחזור של תשתיות מערכות המידע והזמן הנדרש לכך נגזרים משני מרכיבים מרכזיים: (א) גיבוי נתונים (ב) קיומו של אתר גיבוי (DR) המכיל את יכולות התקשוב של הגוף הנדרשות בחירום בהתאם למדיניות (גיבוי של מערכות מחשוב; תקשורת פנים-ארגונית, תקשורת חיצונית ואמצעי אבטחת מידע). כמו כן, הארגון נדרש לתרגל מעבר לאתר הגיבוי (של כלל המערכות והצוותים העוסקים בהקמתו ובתפעולו) אחת לשנה ולבצע בדיקת תקינות של הגיבוי ושל היכולת לשחזור תקין, לזהות פערים ולתקנם.

תרשים 3 : **ההשפעה של מערך הגיבוי ואתר הגיבוי (DR) על זמן ההתאוששות מאירוע חירום**



הוכן בידי משרד מבקר המדינה.

בהתאם להחלטת הממשלה 2097, מערך הדיגיטל הלאומי משמש מנהל סיכוני התקשוב הראשי הממשלתי[16] ואחראי לרכז תמונת מצב ממשלתית בדבר סיכוני התקשוב וליזום פעילות רוחבית להפחתת הסיכונים. במסגרת זו ה-CIO (Chief Information Officer) הממשלתי במערך הדיגיטל הלאומי מנחה את כלל משרדי הממשלה ויחידות הסמך בנושאי תקשוב, ובכלל זה בהיבטים של רציפות תפקודית. נוסף על כך, יה"ב מנחה את משרדי הממשלה ויחידות הסמך (שאינם גופי תמ"ק) בנושאי אבטחת מידע וסייבר. משרדי הממשלה ויחידות הסמך שמוגדרים גופי תמ"ק מונחים על ידי מערך הסייבר בנושאי אבטחת מידע וסייבר, במקביל להנחיית ה-CIO הממשלתי בנושאי תקשוב כאמור.

דוח של מבקר המדינה מנובמבר 2024 בנושא ניהול סיכונים ממשלתי בתחום התקשוב הצביע על כך שכבר משנת 2019 זיהה מערך הדיגיטל את הסיכון בנוגע להמשכיות עסקית והיערכות לחירום כאחד מסיכוני התקשוב העיקריים והרוחביים במשרדי הממשלה[17].

16 סעיף 6 להחלטת הממשלה 2097 בנושא "הרחבת תחומי פעילות התקשוב הממשלתי, עידוד חדשנות במגזר הציבורי וקידום המיזם הלאומי 'ישראל דיגיטלית'" מ-10.10.14 מטיל על הממונה על התקשוב הממשלתי "למנות מנהל סיכוני תקשוב ראשי במטה התקשוב הממשלתי". בהחלטה צוין ש"תפקידי מנהל סיכוני תקשוב ראשי יהיו כדלקמן: א. הנחייה מקצועית של מנהלי סיכוני התקשוב באגפי מערכות המידע וסיוע בהטמעת המתודולוגיה הממשלתית בתחום... ג. ריכוז תמונת מצב ממשלתית בדבר סיכוני התקשוב וייזום פעילות רוחבית להפחתתה. בכל הנוגע להיבטי הגנה בסייבר מנהל סיכוני התקשוב הראשי יונחה מקצועית על ידי היחידה להגנה בסייבר בממשלה".

17 מבקר המדינה, **דוח שנתי של מבקר המדינה בנושא סייבר ומערכות מידע - נובמבר 2024**, "ניהול סיכונים ממשלתי בתחום התקשוב", עמ' 11.

בהנחיה של מערך הדיגיטל בנושא "היערכות להמשכיות עסקית ותפקודית במצב חירום", המתמקדת במשמעויות הנגזרות מתחומי האחריות של אגף טד"ם (טכנולוגיות דיגיטליות ומידע), נקבעו דרישות בהיבטי רציפות תפקודית של חדרי שרתים ותקשורת: גיבוש מדיניות המשכיות עסקית, תוכנית התאוששות מאסון וכן הקמת מערך גיבוי ואתר גיבוי בהתאם למדיניות הארגון. כמו כן, כאמור, מערך הסייבר הוציא בספטמבר 2024 הנחייה להיערכות לחירום בנושא הקמת אתר גיבוי הכוללת גם הנחיה לגיבוש תוכנית התאוששות מאסון מפורטת הכוללת הגדרת מצבים וזמנים ביחס למשרדי ממשלה שהם גופי תמ"ק.

תמונת המצב לגבי משרדי הממשלה ויחידות הסמך והטיפול בפערים

בתחילת מלחמת חרבות ברזל עסק מערך הדיגיטל בנושא הרציפות התפקודית של משרדי הממשלה ויחידות הסמך. עד אז קיבל מערך הדיגיטל מהגופים, במסגרת גיבוש תוכניות העבודה שלהם, את המידע בדבר קיומו של אתר גיבוי (DR). עם פרוץ המלחמה באוקטובר 2023 בדק מערך הדיגיטל לאילו משרדי ממשלה ויחידות סמך יש גיבוי והיכן הוא ממוקם, אם יש למשרד הממשלתי או ליחידת הסמך אתר גיבוי, ואם המשרד או היחידה מבצעים תרגולים לבדיקת תקינות הגיבויים ולגבי מעבר לאתר הגיבוי. הבדיקה התבססה על דיווחי משרדי הממשלה ויחידות הסמך, בלי שמערך הדיגיטל בדק את הדיווחים. בנובמבר 2023 שלח מערך הדיגיטל מכתבים למנכ"לי המשרדים והיחידות אשר כללו פירוט של הפערים שהתגלו בכל גוף וכן דרישה לטיפול בפערים אלה, כדי להבטיח את הרציפות התפקודית בגוף. מערך הדיגיטל מיפה את הפערים במשרדי הממשלה על בסיס תשובות הגופים לסקר וריכז את הפערים הרוחביים.

מהנתונים שריכז מערך הדיגיטל לגבי 50 משרדי ממשלה ויחידות סמך, בעקבות סקר שערך בתקופת מלחמת חרבות ברזל, בנובמבר 2023, עולה כי קיימים פערים בהיבטי רציפות תפקודית של משרדי ממשלה.

מערך הדיגיטל גיבש דרכי פעולה לצמצום הפערים, במטרה להבטיח רציפות תפקודית של משרדי הממשלה בעת משבר (להלן - תוכנית הפעולה). מערך הדיגיטל העריך את עלות הפרויקט לכלל משרדי הממשלה במשאבים רבים בהם עלויות הקמה ועלות שנתית שוטפת, ולא הוסדר מקור תקציבי.

המיפוי ותוכנית הפעולה הוצגו בדיוני פורום גופי החירום בראשות המל"ל באוקטובר 2023 ופורום מנכ"לים במרץ 2024, והנושא עלה שוב באחד מדיוני פורום מנכ"לים ביוני 2025. ביולי 2025 שלח מערך הדיגיטל מכתבי תזכורת לגופים שבהם התגלו פערים ברציפות תפקודית. מערך הדיגיטל לא קבע לוחות זמנים לטיפול בפערים.

נמצא כי על אף הפערים ברציפות תפקודית של משרדי הממשלה, רק במרץ 2024, בעת מלחמת חרבות ברזל, החל מערך הדיגיטל לקדם תוכנית פעולה לצמצום הפערים. ואולם התוכנית אינה נותנת מענה מלא לפערים ויישומה הוא מורכב: בין השאר נדרשים משאבים רבים ולא הוסדר בעניינם מקור תקציבי. כמו כן מערך הדיגיטל לא קבע לוחות זמנים לטיפול בפערים שמצא ברציפות התפקודית של משרדי הממשלה ויחידות הסמך שנבדקו, ולא קיים דיוני המשך ייעודיים לצורך טיפול מערכתי בפערים בהשתתפות הגופים האסדרתיים המדינתיים, ובהם מערך הסייבר, השב"כ, רח"ל והמל"ל ובפועל הנושא לא תוקצב.

בתשובתו ציין מערך הדיגיטל כי מנכ"לי משרדי הממשלה אחראים להגדיר יעדים ברורים לרציפות תפקודית והתאוששות מאסון במשרדם. בשנת 2024 יה"ב ורח"ל קידמו את ביצועו של תרגיל סייבר לאומי שבמהלכו משרדי הממשלה תרגלו תוכניות רציפות תפקודית במשרדים, הופקו מכך לקחים והוטמעו תיקונים בהתאם לכך. בכלל זה, יה"ב ורח"ל קיימו בשנת 2025 שני מחזורי קורס בנושא תרחישי סייבר וחירום. כמו כן, מערך הדיגיטל, במסגרת חובתו לקדם פתרונות ממשלתיים בתחום, הציע למשרדים פתרון שהבשיל רק בתחילת המלחמה.

מומלץ כי מערך הדיגיטל יגבש, בשיתוף הגופים האסדרתיים המדינתיים (מערך הסייבר, השב"כ ורח"ל) ובשיתוף המל"ל, תוכנית פעולה שתיתן מענה מערכתי לפערים בהיבטי רציפות

תפקודית של משרדי ממשלה. כמו כן מומלץ כי מערך הדיגיטל יפעל באופן מיידי ובהתאם ללוחות זמנים מוגדרים לטיפול בפערים הקיימים במשרדי הממשלה ויחידות הסמך בנושא הרציפות התפקודית ובכלל זה לקדם את ההיבט התקציבי מול כלל הגורמים הרלוונטיים. בכלל זה מומלץ כי מערך הדיגיטל ינחה אותם לפעול לפי הנחיות מקובלות: לתפעל מערך גיבוי ואתר גיבוי (DR) לכלל מערכות המחשוב התומכות בתהליכים קריטיים לתפקוד המשק בחירום (שירותים לאזרח, שירותי חירום ותשתיות), לתרגל מעבר לאתר הגיבוי אחת לשנה, לבצע בדיקה של תקינות הגיבוי ויכולת השחזור ולתקן פערים, אם יתגלו.

תמונת המצב שבידי רח"ל

בהתאם להחלטת הממשלה 1577[18], אחריות-העל לטיפול בעורף בכלל מצבי החירום מוטלת על שר הביטחון. כאמור, תפקידי רח"ל הם, בין השאר, לרכז בזמן שגרה את עבודת המטה בנושא ההיערכות של הארגונים ומשרדי הממשלה בעורף למצבי החירום השונים והמענה הנדרש מהם, ואת יעדי הכשירות והכוננות, וכן להכין דוח מצב שנתי לממשלה על מוכנות העורף בתחומים השונים ובהתייחס לתרחישים השונים (להלן - תמונת המצב).

רציפות התפקוד לפי הגדרת רח"ל היא שמירה על היכולת של הארגון לספק במצב חירום מוצר או שירות שהוגדר חיוני לעורף. רח"ל הגדירה 15 יעדים שהמדינה נדרשת לעמוד בהם בשעת חירום (רפואה, מחסה הולם, מזון ומים ראויים, חינוך, חילוץ והצלה, חופש תנועה ביבשה, באוויר ובים, דת, חופש פולחן ושירותי זיהוי וקבורה, היגיינה וסניטציה, ניהול וקבלת החלטות, מניעת פגיעה חמורה בסביבה, הסברה והנחיה של הציבור, המערכת הכלכלית הלאומית, הגנת יכולות חיוניות במשק וצמצום היקף הנזק, תמיכה במאמץ המלחמתי, שמירת החוק והסדר; להלן - היעדים הלאומיים) וכן ארבעה "מאפשרים" לאומיים (אנרגייה, תקשורת, כוח אדם ותחבורה) שקיומם מאפשר למעשה עמידה ביעדים.

משרדי הממשלה מדווחים לרח"ל באמצעות מערכת השליטה והבקרה של פיקוד העורף על רמת העמידה שלהם בנושא הרציפות התפקודית בהלימה ליעדים הלאומיים (בשגרה דיווח שנתי ובעיתות חירום דיווח יומי). נוסף לכך, משרדי הממשלה מדווחים על שני מדדים כלליים בהיבטי אבטחת מידע והגנת הסייבר[19].

משרדי הממשלה נושאים באחריות לתחומים שבסמכותם גם במצב חירום[20]. משרד ממשלתי אחראי אפוא לשמור על הרציפות התפקודית שלו ולהמשיך לספק גם בעת חירום את השירותים החיוניים שהגדיר. על משרדי הממשלה לכלול במסגרת השירותים החיוניים גם את היעדים הלאומיים שהוגדרו על ידי רח"ל. כאמור, המשרדים נדרשים על פי נורמות מקובלות לגבש תוכנית המשכיות עסקית הכוללת תוכנית התאוששות מאסון, לתמוך ביעדי התוכנית על ידי הקמת אתר גיבוי (DR) והפעלת מערך גיבוי, שיאפשרו להמשיך לתת שירותים חיוניים גם בעת פגיעה במערכות המידע באתר הראשי, באמצעות שחזור הנתונים והפעלת מערכות באתר הגיבוי (DR).

כמו כן מדדי הרציפות התפקודית של משרד ממשלתי אחד אינם משפיעים בהכרח רק על המשרד עצמו ועל יכולתו לספק את השירותים הקריטיים שהוא מופקד עליהם במצב חירום, אלא יכולים להשפיע גם על גופים אחרים ועל יכולת מימוש הרציפות התפקודית שלהם. גופים אלה לאו דווקא מונחים על ידי אותו מאסדר, וכל מאסדר (מערך הסייבר, מערך הדיגיטל ויחידות הסייבר המגזריות) מחזיק מידע לגבי מצב הרציפות התפקודית של הגופים המונחים על ידו.

---

18 החלטת הממשלה 1577, "הטלת האחריות הכוללת לטיפול בעורף במצבי חירום על שר הביטחון" (15.4.07).

19 (1) יכולת זיהוי והתמודדות עם אירועי סייבר משמעותיים (2) יכולת להבטיח אמינות, זמינות, וסודיות של מידע, מערכות, רכיבים שירותים ותהליכים. ביחס לכל שאלה ניתן מענה ל-5 מרכיבים: תורה ותפיסה, הכשרה, כוח אדם, אמצעים ותרגול.

20 החלטת הממשלה 1577, "הטלת האחריות הכוללת לטיפול בעורף במצבי חירום על שר הביטחון" (15.4.07).

נמצא כי תמונת המצב שבידי רח"ל, האמונה (בהתאם להחלטת ממשלה ב/43) על הצגת תמונת מצב לממשלה בנוגע למוכנות העורף בתחומים השונים במצבי משבר וחירום אינה משקפת את הפערים הקיימים בהיבטי רציפות תפקודית במשרדי ממשלה.

עוד נמצא, כי מערך הדיגיטל ומערך הסייבר אינם מנחים את משרדי הממשלה ויחידות הסמך לכלול את היעדים הלאומיים (שרח"ל הגדירה כיעדים שהמדינה נדרשת לעמוד בהם בשעת חירום) במסגרת השירותים החיוניים שמוגדרים בתוכנית ההתאוששות מאסון (DRP) באופן שהתוכנית שמנכ"לי משרדי הממשלה ויחידות הסמך נדרשים לאשר תיתן בהכרח מענה על היעדים הלאומיים ומערכות התקשוב יתמכו ביעדים אלה בעיתות שגרה וחירום.

תחום הרציפות התפקודית בממשלה משלב כמה גורמים ובהם: משרדי הממשלה, מס"ל, מערך הדיגיטל ורח"ל. מומלץ כי מערך הדיגיטל ומערך הסייבר ינחו את משרדי הממשלה ויחידות הסמך להגדיר את היעדים הלאומיים (שרח"ל הגדירה כיעדים שהמדינה נדרשת לעמוד בהם בשעת חירום) כחלק מהשירותים החיוניים שלהם בתוכנית ההתאוששות מאסון שלהם (DRP), ויוודאו שמערכות התקשוב יתמכו ביעדים אלה בעיתות שגרה וחירום, כדי שהמשרדים ויחידות הסמך יעמדו באופן מלא ביעדים הלאומיים. כמו כן, מומלץ כי הם ינחו את משרדי הממשלה ואת יחידות הסמך לפרט בתוכניות ההתאוששות מאסון (DRP) את ההשפעה שיש לאותו ארגון על גופים אחרים ולהפך.

עוד מומלץ כי בשל חשיבות הרציפות התפקודית של משרדי הממשלה ויחידות הסמך למשק האזרחי בחירום, מערך הדיגיטל ומערך הסייבר יוודאו כי תמונת המצב שבידי רח"ל תואמת את המצב בפועל של הגופים המונחים בעת חירום. כמו כן מומלץ כי רח"ל והגופים האסדרתיים המדינתיים יציפו פערים בין גופים ומגזרים שמשפיעים זה על זה ויפעלו לצמצום הפערים.

בתשובת מערך הדיגיטל נמסר כי הוא פעל לקידום המלצה זו בשנתיים האחרונות. בתשובה נוספת מסר מערך הדיגיטל כי הוא מקבל את המלצת הביקורת ופועל לקידום הנחיה אחידה בנושא הרציפות התפקודית במשרדי הממשלה ויחידות סמך לצד חלוקת אחריות בין המאסדרים, וזאת באמצעות בחינת הנושא בשיתוף הגופים האסדרתיים המדינתיים הרלוונטיים ועדכון הנחייתו בנושא הרציפות התפקודית בהתאם לכך. כמו כן, ההנחיה שתגובש תגדיר את חלוקת האחריות בין הגופים האסדרתיים המדינתיים וכן את אחריות המשרדים בתחום זה.

בתשובת רח"ל למשרד מבקר המדינה מאוקטובר 2025 נמסר כי יש לגבש את תוכנית ההמשכיות העסקית של הגופים על בסיס שאלון שפיתחה בשיתוף יה"ב[21]. כמו כן, רח"ל תקיים דיון בנושא תחומי אחריותה מול הגופים האסדרתיים המדינתיים בתחום הגנת הסייבר בכל הקשור לאחריות הנחיית הרציפות התפקודית של הגופים בהיבטים הטכנולוגיים ובתחומי אבטחת המידע באופן שתהיה בהלימה ליעדים הלאומיים שהיא הגדירה ושהגופים מחויבים לעמוד בהם.

<u>ממונה הביטחון בגופים ציבוריים</u>

הכשרה של ממוני בטחון

תפקידי ממונה הביטחון בגופים ציבוריים נקבעו בחוק להסדרת הביטחון בהתאם לסוג הגוף, בהחלטת ממשלה, ובהנחיות יה"ב ונציבות שירות המדינה, והם כוללים בין היתר פעולות לאבטחה פיזית (חיי אדם), לאבטחת מידע מסווג ולאבטחת מערכות ממוחשבות (הגנה פיזית, הגנה סביבתית ורציפות תפקודית), כמפורט להלן:

אבטחה פיזית (חיי אדם): פעולות הדרושות לשם שמירה על ביטחונו של אדם או שמירה על רכוש במבנה או במקום של גוף ציבורי וכן פעולות למניעת פגיעה בכל אחד מאלה.

[21] שאלון הערכה בדבר פגיעה צפויה ביכולת הגוף לביצוע משימה (בהתבסס על היעדים הלאומיים).

אבטחת מידע מסווג: פעולות הדרושות לשם שמירה על מידע מסווג של גוף ציבורי או על מידע כאמור המצוי אצלו וכן פעולות למניעת פגיעה בכל אחד מאלה.

אבטחת מערכות ממוחשבות (כולל היבטי הגנה פיזית, הגנה סביבתית ורציפות תפקודית): פעולות הדרושות לשם שמירה על מערכות ממוחשבות, על מידע האגור במערכות אלה ועל מידע מסווג הקשור למערכות אלה וכן פעולות למניעת פגיעה במערכות או במידע כאמור.

בלוח שלהלן מוצגים הגופים המנחים לגבי פעולות האבטחה בגופי תמ"ק ובמשרדי ממשלה ויחידות סמך שאינם גופי תמ"ק:

לוח 4: **הגוף המנחה לגבי פעולות האבטחה בגופי תמ"ק ובמשרדי ממשלה ויחידות סמך שאינם גופי תמ"ק**

	אבטחה פיזית (חיי אדם)	אבטחת מידע מסווג	אבטחת מערכות ממוחשבות (הגנה פיזית, הגנה סביבתית ורציפות תפקודית)
גופי תמ"ק	משטרה	שב"כ/מערך הסייבר	שב"כ/מערך הסייבר
משרדי ממשלה שאינם גופי תמ"ק	משטרה*	שב"כ	יה"ב

הוכן בידי משרד מבקר המדינה.
* למעט הגופים המפורטים בתוספת הראשונה בחוק להסדרת הביטחון.

הכשרות בתחום האבטחה הפיזית (חיי אדם) - ממונה הביטחון נדרש לעבור קורס ממוני ביטחון (להלן - מנב"טים) במכללות פרטיות שהוסמכו לכך על ידי המשטרה, וכן הוא עובר ריענון דו-יומי אחת לשנה לשם שמירה על כשירותו.

הכשרות בתחום אבטחת מידע מסווג - השב"כ מעביר קורסי הכשרה למנב"טים בנושא אבטחת מידע מסווג. גופי תמ"ק שעברו להנחיית מערך הסייבר בתחום זה (על פי כללי השב"כ) עוברים הכשרה בתחום מטעם מערך הסייבר בהתאם לתו"ל הייעודי.

הכשרות והשתלמויות בתחום אבטחת מערכות ממוחשבות

1. **השב"כ:** עד לשנת 2017 השב"כ הנחה את כל גופי התמ"ק והעביר למנב"טים בגופים אלה הכשרות וימי עיון תקופתיים בנושא אבטחת מערכות מידע ממוחשבות (קורס ביטחון למערכות ממוחשבות). לאחר שהנחיית מרבית גופי התמ"ק הועברה למערך הסייבר, השב"כ מקיים הכשרות משלימות למנב"טים בגופי התמ"ק שנשארו מונחים על ידו (גופי תקשורת).

2. **מערך הסייבר:** הנחיית מרבית גופי התמ"ק הועברה למערך הסייבר בשנת 2017. מערך הסייבר קיים שלושה מחזורי השתלמות למנב"טים, ביולי 2021, ביוני 2022 וביוני 2025. ההשתלמות כללה התייחסות לנושא ההגנה הפיזית בהיבט של "מערכות אבטחה טכנולוגיות ומיגון למניעת גישה לנכסי הארגון", ולא הייתה בה כלל התייחסות להיבטים של הגנה סביבתית ורציפות תפקודית. כמו כן, ההשתלמות כללה היבטים מסוימים בתחום אבטחת מידע מסווג. ההשתלמות היא רשות, ומשתתפים בה גם בעלי תפקידים בגופים שאינם גופי תמ"ק. יצוין כי בפגישה של נציגי משרד מבקר המדינה עם ראש אגף סקטוריאלי במערך הסייבר נמסר כי למנחים האחראים להנחיה של גופי תמ"ק ולפיקוח עליהם יש פערים מסוימים בהכשרה בנושא הגנה פיזית.

3. **יה"ב:** מבצעת הכשרות עבור ממוני סייבר ומנב"טים במשרדי הממשלה שאינם גופי תמ"ק.

נמצא כי קיימים פערים בהכשרה שמקיים מערך הסייבר לממוני הביטחון בגופי תמ"ק בנושא אבטחת מערכות ממוחשבות חיוניות בשניים מתוך שלושה היבטים הנוגעים לביקורת - רציפות תפקודית והגנה סביבתית על חדרי שרתים ותקשורת אף שהנושא הוא בתחום אחריותו של ממונה הביטחון. ההכשרה כוללת את נושא ההגנה הפיזית על חדרי שרתים ותקשורת. עוד נמצא כי קיימים פערים בהכשרת המנחים במערך הסייבר שאחראים להנחיית הגופים המונחים בתחומי ההגנה הפיזית על חדרי שרתים.

על מערך הסייבר להשלים את הפערים הקיימים בהכשרות למנחים מטעמו וכן לממונים על הביטחון בגופי תמ"ק בכלל הנושאים הנוגעים לאבטחת מערכות ממוחשבות חיוניות שבתחום אחריותם - ובכלל זה גם בהיבטי רציפות תפקודית והגנה סביבתית על חדרי שרתים ותקשורת. נוסף על כך, יש לבצע הכשרות ריענון תקופתיות בהתאם לשינויים בתחומים אלה.

בתשובת מערך הסייבר נמסר כי ההשתלמות בנושא תואמה בתוכנית העבודה 2025 וכתוצאה מתיעדוף פנימי של הכשרות למנחים היא נדחתה לשנת 2026. כמו כן, במסגרת מינוי מנב"טים חדשים, מוגדרת דרישה כי המנב"טים יעברו הכשרה של מערך הסייבר במהלך שנת עבודתם הראשונה.

ממוני הביטחון בקריות הממשלה

חטיבת הנכסים של החשב הכללי במשרד האוצר אחראית להקמה, שכירה, תפעול, תחזוקה ואבטחה של מבני ממשלה עבור כלל משרדי הממשלה, בין השאר באמצעות מינהל הדיור הממשלתי. החטיבה מובילה תוכנית לריכוז משרדי הממשלה במתחמים משותפים בבעלות המדינה. נכון לאפריל 2025 היו מספר מתחמים משותפים כאמור ועוד מספר פרויקטים בשלבי הקמה.

בכל קריות הממשלה יש חדרי תקשורת, ובשלוש קריות ממשלה ממוקם גם חדר שרתים מרכזי המשרת כמה משרדי ממשלה ויחידות סמך. למשל, צוות הביקורת ביקר בקרית ממשלה אחת שכללה חדר שרתים המארח שרתים של כ-10 משרדי ממשלה ויחידות סמך. כמו כן, בקרית הממשלה האמורה יש חדרי מצב לאומיים לשעת חירום. לאור ריכוז וריבוי משרדי ממשלה ויחידות סמך בקרית ממשלה כאמור מינהל הדיור נדרש כבר בשלב התכנון לתת מענה לאיום ייחוס לאומי, לרבות איום ייחוס לאומי צופה פני עתיד שכן תהליך הבנייה של הדיור הממשלתי נמשך מספר שנים והמבנה משרת את משרדי הממשלה במשך עשרות שנים.

אגף ביטחון מבני ממשלה בחטיבת הנכסים, בראשותו של מנהל האבטחה הארצי, מרכז ומנהל את כלל צורכי הביטחון של משרדי הממשלה המאוכלסים בקריות הממשלה, ובכלל זה את נושא ההגנה על חדרי השרתים וחדרי התקשורת, ומנחה את המנב"טים מטעמו בכל קריות הממשלה. כמו כן, בניית חדרי השרתים וחדרי התקשורת מבוצעת על בסיס מפרט טכני של מינהל הדיור, נוסף להתייעצות בתחומי חירום, הגנת הסייבר ורציפות תפקודית.

פעולות האבטחה של האגף כוללות תכנון וליווי של מינהלת הבינוי הממשלתי ומינהל הדיור הממשלתי ואבטחת פעילות קריות הממשלה ומבני הדיור הממשלתי בתחומי ביטחון, חירום, סייבר ורציפות תפקודית, לרבות הגנת סייבר על מערכות ביטחון והמערכות המתקניות במבנים ובקרת המבנים. כמו כן, האגף אחראי למפעלים חיוניים בקריות הממשלה, לניהול חדרי מצב לאומיים, לניהול Data Center במשרדי הממשלה וכן למערכת לניהול בקרת כניסה במשרדי הממשלה (למשל, בקרת הגישה לקריית הממשלה בה ביקר משרד מבקר המדינה מנוהלת במרוכז עבור כלל המשרדים במתחם זה על ידי מנב"ט הקריה הממשלתית מטעם מינהל הדיור).

כאמור, משרדי הממשלה ויחידות סמך מונחים על ידי יה"ב או מערך הסייבר. מינהל הדיור הממשלתי, שבונה ומתחזק עבור עשרות משרדי ממשלה ויחידות סמך אלה חדרי שרתים, חדרי תקשורת וחדרי מצב לאומיים - אינו מוגדר גוף מונחה ולא מבוקר על ידי גורם אסדרתי מדינתי (למשל, בקרית הממשלה בה ביקר משרד מבקר המדינה לא בוצעה בקרה על מכלול חדר השרתים וחדרי התקשורת על ידי גורם אסדרתי מדינתי).

נמצא כי אין גוף אסדרתי מדינתי בתחום אבטחת המידע והסייבר שתפקידו להנחות את ממונה הביטחון הארצי במינהל הדיור הממשלתי בתחום זה ואף גוף אסדרתי מדינתי אינו מבצע בקרה על פעילותו בתחום. זאת, למרות אחריותו הכוללת של ממונה הביטחון הארצי להקמה ולתחזוקה של פרויקטים משמעותיים בדיור הממשלתי: הקמת קריות ממשלה ובהם חדרי מצב לאומיים, חדרי שרתים וחדרי תקשורת של משרדי ממשלה ויחידות סמך, המשמשים אותם למשך שנים רבות וצריכים לענות על איומים צופי פני עתיד.

יצוין כי החשב הכללי באמצעות חטיבת הנכסים פועל לקידום שינוי חקיקתי בחוק להסדרת הבטחון בגופים ציבוריים, התשנ"ח-1998, במטרה להגדיר את השב"כ כגורם אסדרתי מדינתי שינחה את מינהל הדיור הממשלתי עצמו.

בתשובת מערך הדיגיטל נמסר כי הוא אינו המאסדר הלאומי אשר אחראי, בין היתר, להגדיר את איום הייחוס להגנה על קריות הממשלה, ולנוכח זאת אינו מגדיר את תקני האבטחה שבהם נדרש לעמוד מינהל הדיור הממשלתי. לפיכך, הוא יפעל עם הגופים האסדרתיים המדינתיים בתחום הסייבר להטמעת הנחיות ובקרות בנושא זה, אם אלו יקודמו על ידם.

מומלץ כי חטיבת הנכסים בחשב הכללי תפעל, בשיתוף מערך הסייבר, יה"ב והשב"כ, להשלים שינויי האסדרה הקיימת, כדי שהיא תבטיח ליווי והנחיה בקריות ממשלה בנושאים של אבטחת מידע וסייבר הנתונים לאחריות מנב"ט מינהל הדיור הממשלתי, ובכלל זה בנושאי הגנה פיזית והגנה סביבתית על חדרי שרתים וחדרי תקשורת ושמירה על הרציפות התפקודית.

סיכום

גופי התמ"ק וגופים חיוניים כוללים משרדי ממשלה, גופים ציבוריים וגופים פרטיים שפגיעה בפעילותם עלולה להביא לפגיעה בחיי אדם, לפגיעה באספקת שירות ציבורי חיוני ולנזק פיזי או כלכלי ניכר. מערכות המידע בגופי תמ"ק ובגופים חיוניים הן נכס ראשון במעלה בחשיבותו, ותפקודן התקין נדרש לצורך ביצוע תהליכי ליבה של הגופים בעיתות שגרה ובעיתות חירום. בשל ההשפעות החמורות שיש לפגיעה בתפקודן של מערכות המידע בגופים אלה, נדרשת הגנה מוגברת עליהן מפני איומים פיזיים וסביבתיים, לצד שמירה על הרציפות התפקודית של גופים אלה.

הפערים שנמצאו בנושאים שנבדקו בביקורת זו ב-12 גופי תמ"ק וגופים חיוניים מחייבים נקיטת פעולות מיידיות מצד הגופים האסדרתיים המדינתיים בהיבטים האלה:

1. **אסדרה ופיקוח: האסדרה המחייבת בהיבטי רציפות תפקודית ובהיבטי הגנה פיזית וסביבתית על חדרי שרתים ותקשורת חסרה, הן ברמה המדינתית והן ברמה המגזרית, וגם הפיקוח של הגופים האסדרתיים המדינתיים על עמידת גופי תמ"ק וגופים חיוניים בהנחיות הקיימות בהיבטים אלה טעון שיפור. כמו כן, קיימים בפועל פערים בהיבטי רציפות תפקודית ובהיבטי הגנה פיזית וסביבתית על חדרי שרתים ותקשורת בגופים שנבדקו בביקורת.**

2. **רציפות תפקודית: דוח זה חושף פערים בתחום הרציפות התפקודית במשרדי ממשלה ויחידות סמך. תמונת המצב שבידי רח"ל, האמונה על הצגת תמונת מצב לממשלה בנושא מוכנות העורף בתחומים השונים במצבי משבר וחירום, אינה משקפת את הפער האמור.**

3. **הכשרה: קיימים פערים בהכשרה שמקיים מערך הסייבר לממוני הביטחון בגופי תמ"ק אף שהנושא נמצא בתחום אחריותם. נמצאו פערי הכשרה בנושא אבטחת מערכות מידע ממוחשבות. כמו כן נמצאו פערים בהכשרת המנחים של גופי תמ"ק במערך הסייבר בתחומי ההגנה הפיזית על חדרי שרתים.**

על הגופים האסדרתיים המדינתיים בתחום הגנת הסייבר והגנת הפרטיות (מערך הסייבר הלאומי, השב"כ, הרשות להגנת הפרטיות ויחידות הסייבר המגזריות) להשלים את האסדרה המדינתית והמגזרית בהיבטי רציפות תפקודית והגנה פיזית וסביבתית על חדרי שרתים ותקשורת. מומלץ כי הגופים האסדרתיים המדינתיים יקבעו לגופים שהם מנחים הנחיות ייעודיות מחייבות בנושאים אלה, בהתאם לנורמות המקובלות, ויבחנו ויתקפו אותן באופן עיתי. זאת באופן שיחייב את הגופים המונחים לפעול על פיהן ויאפשר לגופים האסדרתיים המדינתיים לפקח על כך. כמו כן, על הגופים האסדרתיים המדינתיים לפעול להכשרת בעלי התפקידים האחראים לנושאים אלה.

מומלץ כי מערך הדיגיטל, בשיתוף הגופים האסדרתיים המדינתיים (מערך הסייבר, השב"כ ורח"ל) ובשיתוף המל"ל, יגבש תוכנית פעולה שתיתן מענה מערכתי לפערים בהיבטי רציפות תפקודית. עוד מומלץ כי מערך הדיגיטל יפעל באופן מיידי ובהתאם ללוחות זמנים מוגדרים לטיפול בפערים הקיימים במשרדי הממשלה ויחידות הסמך בנושא הרציפות התפקודית, ויקדם את ההיבט התקציבי מול כלל הגורמים הרלוונטיים.

נוסף על כך מומלץ כי בשל חשיבות הרציפות התפקודית של משרדי הממשלה ויחידות הסמך למשק האזרחי בחירום, מערך הדיגיטל ומערך הסייבר יוודאו כי תמונת המצב שבידי רח"ל תואמת את המצב בפועל של הגופים המונחים בעת חירום. כמו כן מומלץ כי רח"ל והגופים האסדרתיים המדינתיים יציפו פערים בין גופים ומגזרים שמשפיעים זה על זה ויפעלו לצמצום הפערים.

ממצאיו של דוח זה אמורים להוות בסיס לתכנית תיקון משמעותית שיובילו ראש מערך הסייבר הלאומי, ראש רח"ל, ראש מערך הדיגיטל, ראש הרשות להגנת הפרטיות ומנכ"לי משרדי הממשלה, גופי התמ"ק והגופים החיוניים - כל אחד על פי תחום תפקידו ואחריותו.