מבקר המדינה

דוח על הביקורת בשלטון המקומי

אבטחת מידע של מערכות גבייה ברשויות מקומיות

תמוז התשפ"ד | יולי 2024

אבטחת מידע של מערכות גבייה ברשויות מקומיות

מבוא

הרשויות המקומיות עוסקות במגוון רחב של תחומים - איכות הסביבה, בריאות, חינוך, רווחה, תברואה, תחבורה ותרבות, תכנון ובנייה - המשפיעים על ענייני היום-יום של תושביהן ועל רווחתם[1]. פעולות אלה ממומנות מתקציב הרשויות המקומיות הכולל מספר מקורות מימון. נכון לסוף שנת 2021 היו בתחומן של כלל הרשויות המקומיות במדינה כ-9.4 מיליון תושבים, והכנסותיהן העצמיות הסתכמו בכ-44 מיליארדי ש"ח[2]. בשנת 2021 עלות הנזקים מאירועי סייבר[3] בעולם הייתה 6 טריליון דולר[4] ובישראל העלות הכלכלית השנתית של הנזקים מוערכת בלפחות 12 מיליארד ש"ח בשנה[5].

המחוקק הטיל על השלטון המרכזי ככלל, ועל משרד הפנים כמאסדר של השלטון המקומי בפרט, את האחריות לגיבושה וליישומה של מדיניות לאומית בשלטון המקומי. משרד הפנים גם מופקד על הפיקוח על פעולות הרשויות המקומיות, על הכוונתן ועל הסדרת יחסי הגומלין ביניהן[6].

רשויות מקומיות מוסמכות להטיל בתחום שיפוטן תשלומי חובה, כגון ארנונה, אגרות בעד הנפקת רישיונות או הספקת כל שירות אחר, היטלים, דמי השתתפות כדי לאפשר לרשויות ביצוע הדברים שהן נדרשות או מוסמכות לעשותם.

ההתפתחות הטכנולוגית המהירה השפיעה כמעט על כל תחומי החיים של הפרט והמגזרים במשק, לרבות המגזר הציבורי, ובייחוד על הרשויות המקומיות. הרשויות המקומיות משתמשות במערכות דיגיטליות ובאתרים במרשתת (באינטרנט) המאפשרים להן לנהל את ענייניהן ולקיים אינטראקציה עם התושבים באופן מקוון, וחלקן אף מספקות שירותים מקוונים שונים המאפשרים לתושבים, בין היתר, לבצע תשלומים ובפרט לשלם ארנונה ולקבל מידע ושירותים שונים באמצעות המרשתת. חשוב לציין שהרשויות המקומיות נבדלות זו מזו בהרכבי האוכלוסייה שבהן, במשאבים העומדים לרשותן וכן ברמתן הדיגיטלית של מערכותיהן הממוחשבות[7].

לרוב, מערכת הגבייה שבה מבוצע תהליך הגבייה על ידי הרשויות המקומיות מנוהלת ומתופעלת על ידי ספקי שירות חיצוניים המספקים לרשויות את מערכת הגבייה, ולפעמים הרשות המקומית עצמה מנהלת ומתפעלת את המערכת. מערכת הגבייה כוללת מודולים שונים לצורך גבייה של מיסים, אגרות, היטלים ועוד בתחומי הארנונה, החינוך, השילוט וכו'.

במערכות הגבייה של הרשויות המקומיות, הן אלה המנוהלות על ידי ספקי השירות של מערכת הגבייה והן אלה המנוהלות על ידי הרשויות עצמן, מצטבר מידע אישי רב על תושביהן, כמו שם, כתובת, מספר זהות, מספר טלפון, מידע רפואי, מידע על המצב הכלכלי, מידע בתחומי הרווחה ונתונים על אמצעי התשלום המשמשים אותם וכן מידע בלתי מסונן כמו תצלומי לוחיות רישוי,

---

1 מבקר המדינה, **דוחות על הביקורת בשלטון המקומי** (2022), "ניהול מערכות מידע ברשויות המקומיות", עמ' 1255.

2 מתוך אתר הלשכה המרכזית לסטטיסטיקה - "הרשויות המקומיות בישראל - קובצי נתונים לעיבוד 1999 -2022".

3 אירוע סייבר הוא התרחשות אשר מעידה על פגיעה אפשרית בפעילותו התקינה של נכס סייבר, אשר יש יסוד להניח כי היא נובעת מפעילות מכוונת במרחב הסייבר. אירוע סייבר אינו בהכרח מעיד על תקיפת סייבר, אך יש יסוד סביר להניח שכן.

4 על פי נתונים מהפורום הכלכלי העולמי:
https://www.weforum.org/agenda/2023/01/global-rules-crack-down-cybercrime/

5 על פי נתוני מערך הסייבר הלאומי:
https://www.gov.il/he/pages/economic_cost_of_cyber_attacks_8_5_2024

6 מבקר המדינה, **דוח שנתי 63ג** (2012), "היבטים בתפקוד משרד הפנים כמאסדר של השלטון המקומי", עמ' 1223.

7 מערך הסייבר הלאומי, **נייר מדיניות בנושא הגנת הסייבר ברשויות המקומיות** (יולי 2020); מבקר המדינה, **דוחות על הביקורת בשלטון המקומי לשנת 2021** (2021), "שירותים מקוונים של רשויות מקומיות בשגרה ובחירום", עמ' 311 - 414.

תצלומים של תווי פנים, נתוני מיקום ומידע על הרגלי תנועה. הדבר מחייב את הרשויות המקומיות לפעול לשמירה על המידע שנאסף בידיהן ולאבטחתו[8].

מערכות המידע הדיגיטליות של הרשויות המקומיות חשופות למגוון סיכונים, לבעיות חוסן באבטחת המידע ולאיומי סייבר, והפכו למוקד עניין עבור פצחנים (האקרים[9]) ופושעי סייבר. התקפות סייבר ברשויות עלולות לגרום נזקים כגון פגיעה בתשתיות טכנולוגיה (חומרה, תוכנה ויישומים), פגיעה בשלמותו ובמהימנותו של המידע השמור במערכות המידע שבשימוש הרשויות, דליפה של נתונים ומידע ממאגרי המידע[10] שברשותן וחשיפתם לגורמים שאינם מורשים לכך. כמו כן התקפות סייבר ברשויות עלולות לגרום לפגיעה בתשתיות פיזיות, לשיבוש ואף למניעה של אספקת שירותים קריטיים לתושבים כגון שירותים בתחומי האנרגייה, המים, התחבורה והביוב, ובמקרים חמורים הן אף עלולות לגרום לפגיעה ברציפות התפקודית של הרשויות המקומיות[11].

בשנים 2020 - 2023 דווח על כמה אירועי סייבר ברשויות מקומיות[12]. למשל, במאי 2021 דווח על אירוע אבטחת מידע חמור שהתרחש בנובמבר 2020, שעלה כי במסגרתו גורם בלתי מורשה חדר למערכת הממוחשבת של אחת העיריות[13] באמצעות תוכנת השתלטות וכך התחבר למערכות הגבייה והמיסים של העירייה וביצע שינוי בנתוני התושב. מערך הסייבר הלאומי ציין במסמך מדצמבר 2023 כי מראשית מלחמת "חרבות ברזל", מערך הסייבר הלאומי מזהה פעילות הולכת ומתעצמת של תוקפים מסוגים שונים נגד ארגונים במרחב הסייבר הישראלי[14]. על חשיבות הנושא, על התעצמות הסיכון הנשקף בגינו ועל מרכזיותו בעת האחרונה ניתן ללמוד בין היתר מהחוק העדכני שנחקק בנושא: חוק התמודדות עם תקיפות סייבר חמורות במגזר השירותים הדיגיטליים ושירותי האחסון (הוראת שעה - חרבות ברזל), התשפ"ד-2023.

<u>פעולות הביקורת</u>

בחודשים מאי-דצמבר 2023 בדק משרד מבקר המדינה את נושא אבטחת מידע של מערכות גבייה ברשויות המקומיות. הבדיקה כללה את הנושאים שלהלן: הנחיה מקצועית של הרשויות המקומיות בתחום הגנת הסייבר; ניהול מאגרי מידע של מערכות הגבייה; מדיניות ונהלים בתחום אבטחת המידע; תוכנית עבודה להתמודדות עם אירועי סייבר; הסמכה לפי תקן ISO27001[15]; התאוששות מאסון; אבטחה פיזית של מערכות גבייה; ניטור של פעולות במערכת הגבייה והבקרה בנושא; אירועי סייבר; זיהוי ואימות של משתמשים במערכת הגבייה; ניהול הרשאות גישה למערכת הגבייה; עריכת סקרי סיכונים; ביצוע מבדקי חדירה[16]; דיווח ובקרה על ספקי שירות של מערכת גבייה.

הביקורת נעשתה בשש רשויות מקומיות: **בעיריית אור עקיבא**, **בעיריית ראשון לציון**, **בעיריית רהט**, **בעיריית רחובות**, **במועצה המקומית אבן יהודה ובמועצה האזורית עמק חפר (להלן - הרשויות שנבדקו)**, וכן במשרד הפנים. בדיקות השלמה בוצעו ברשות להגנת הפרטיות ובמערך

8 מבקר המדינה, **דוחות על הביקורת בשלטון המקומי לשנת 2022** (2022), "ניהול מערכות מידע ברשויות המקומיות", עמ' 1255.

9 כינוי למומחה בתחום פריצות למחשבים ולרשתות מחשבים - בעיקר במובן השלילי.

10 חוק הגנת הפרטיות, התשמ"א-1981, מגדיר מאגר מידע כך - "אוסף נתוני מידע, המוחזק באמצעי מגנטי או אופטי והמיועד לעיבוד ממוחשב, למעט - (1) אוסף לשימוש אישי שאינו למטרות עסק; או (2) אוסף הכולל רק שם, מען ודרכי התקשרות, שכשלעצמו אינו יוצר אפיון שיש בו פגיעה בפרטיות לגבי בני אדם ששמותיהם כלולים בו, ובלבד שלבעל האוסף או לתאגיד בשליטתו אין אוסף נוסף נוסף".

11 מבקר המדינה, **דוחות על הביקורת בשלטון המקומי לשנת 2022** (2022), "ניהול מערכות מידע ברשויות המקומיות", עמ' 1256.

12 דיווחים שהתפרסמו בתקשורת או הועברו לרשות להגנת הפרטיות במשרד המשפטים או למערך הסייבר הלאומי.

13 מדובר בעיר שבתחומי שיפוטה מתגוררים נכון לשנת 2021 כ-27,000 תושבים; מדד הפריפריאליות שלה - מרכזי; והיא משתייכת לאשכול חברתי-כלכלי בינוני.

14 מערך הסייבר הלאומי, **מלחמת "חרבות ברזל" במימד הסייבר: תובנות ודרכי התמודדות** (דצמבר 2023), עמ' 2.

15 International Organization for Standardization - תקן בין-לאומי לאבטחת מידע.

16 מבדקי חדירה הם מתקפות מתוכננות ומבוקרות על מערכת ממוחשבת שמבצע בודק כדי למצוא חולשות אבטחה ואת פוטנציאל הגישה אל המידע המאוחסן במערכת.

הסייבר הלאומי. השלמות נוספות בוצעו אצל ספקי שירות חיצוניים של מערכות גבייה של רשויות מקומיות שנבדקו. נוכח רגישות הנושאים שנבדקו בביקורת, הרשויות המקומיות יכונו בדוח בשמות חלופיים מקוצרים (למשל רשות מקומית א') שנבחרו באופן אקראי ולא לפי סדר כלשהו.

הרשויות המקומיות שנבדקו - סקירה כללית

להלן יוצגו נתונים כלליים, המעודכנים למועד סיום הביקורת, על הרשויות המקומיות שנבדקו:

לוח 1: **נתונים כלליים של הרשויות המקומיות שנבדקו - נכון למועד סיום הביקורת**[17]

	עיריית אור עקיבא	עיריית ראשון לציון	עיריית רהט	עיריית רחובות	המועצה המקומית אבן יהודה	המועצה האזורית עמק חפר
מספר התושבים	20,874	260,453	79,064	150,748	14,365	43,222
האשכול החברתי-כלכלי	5 (בינוני)	7 (בינוני)	1 (נמוך)	7 (בינוני)	9 (גבוה)	8 (גבוה)
אשכול הפריפריאליות	6 (מרכזי)	9 (מרכזי)	4 (פריפריאלי)	8 (מרכזי)	7 (מרכזי)	6 (מרכזי)
סיווג הרשות המקומית	הבראה	איתנה	ביניים	ביניים	איתנה	יציבה
ביצוע ההכנסות (באלפי ש"ח)	192,907	2,292,394	464,004	1,219,392	91,990	447,688
ביצוע ההוצאות (באלפי ש"ח)	199,383	2,291,099	464,300	1,218,883	91,404	448,684
העודף (או הגירעון) השוטף (באלפי ש"ח)	(6,476)	1,295	(296)	509	586	(996)
העודף (או הגירעון) המצטבר (באלפי ש"ח)	(55,371)	61,983	8,345	(151,087)	7,618	(13,368
שיעור הגירעון המצטבר	30.7%	-	-	13.5%	-	3.1%

על פי נתוני הלשכה המרכזית לסטטיסטיקה (להלן - הלמ"ס) והדוחות הכספיים המבוקרים של הרשויות המקומיות, בעיבוד משרד מבקר המדינה.
מספר התושבים - הנתון לקוח מתוך "הרשויות המקומיות - קובץ נתונים לעיבוד - 2022" שהכינה הלמ"ס.

17 דצמבר 2023.

האשכול החברתי-כלכלי - הלמ"ס מדרגת את הרשויות המקומיות בסולם של עשר דרגות (אשכולות), לפי המצב החברתי-כלכלי של האוכלוסייה המתגוררת בתחום שיפוטן. אשכול 10 מעיד על הרמה החברתית-כלכלית הגבוהה ביותר. מוצג הנתון שהיה מעודכן במועד סיום הביקורת, המתייחס לשנת 2019.
אשכול הפריפריאליות - הלמ"ס מדרגת את הרשויות המקומיות בסולם של עשר דרגות (אשכולות), לפי מקומן הגיאוגרפי ביחס לריכוזי האוכלוסייה, על פי שקלול של שני מרכיבים: נגישות פוטנציאלית לכלל היישובים וקרבה לגבול מחוז תל אביב. אשכול 10 מעיד על היישוב המרכזי ביותר, ואשכול 1 - על היישוב הפריפריאלי ביותר. מוצג הנתון שהיה מעודכן במועד סיום הביקורת המתייחס לשנת 2020.
סיווג הרשות המקומית - משרד הפנים מסווג את הרשויות המקומיות על פי קריטריונים המשקפים את מצבן הכספי ופעולותיהן הכלכליות והמשקיות, כגון שיעור הגירעון השוטף או המצטבר, זכאות למענק איזון, מתן הנחות ומחיקת חובות. על פי הקריטריונים הללו מחולקות הרשויות לשש קבוצות: (1) איתנות (2) יציבות (3) בהמראה (4) בתוכנית הבראה (5) בתוכנית התייעלות (6) במצב ביניים. מוצג הנתון שהיה מעודכן במועד סיום הביקורת.
ביצוע ההכנסות או **ביצוע ההוצאות** - ביצוע ההכנסות או ההוצאות בתקציב הרגיל. הנתון לקוח מתוך הדוחות הכספיים המבוקרים של הרשויות המקומיות המתייחסים לסוף שנת 2022.
העודף (או הגירעון) השוטף או **העודף (או הגירעון) המצטבר** - העודף (ובסוגריים - הגירעון) השוטף או העודף (ובסוגריים - הגירעון) המצטבר בתקציב הרגיל. הנתון לקוח מתוך הדוחות הכספיים המבוקרים של הרשויות המקומיות המתייחסים לסוף שנת 2022.
שיעור הגירעון המצטבר - כהגדרתו בסעיף 140ג לפקודת העיריות [נוסח חדש] ובסעיף 35ג לפקודת המועצות המקומיות [נוסח חדש]). הנתון לקוח מתוך הדוחות הכספיים המבוקרים של הרשויות המקומיות המתייחסים לסוף שנת 2022.

רקע נורמטיבי עיקרי

בחוק הגנת הפרטיות, התשמ"א-1981 (להלן - חוק הגנת הפרטיות או החוק), הוגדר מאגר מידע כלהלן: "אוסף נתוני מידע, המוחזק באמצעי מגנטי או אופטי והמיועד לעיבוד ממוחשב, למעט אוסף לשימוש אישי שאינו למטרות עסק; או אוסף הכולל רק שם, מען ודרכי התקשרות, שכשלעצמו אינו יוצר אפיון שיש בו פגיעה בפרטיות לגבי בני האדם ששמותיהם כלולים בו, ובלבד שלבעל האוסף או לתאגיד שבשליטתו אין אוסף נוסף".

בחוק הגנת הפרטיות, נקבע איסור על פגיעה בפרטיות של הזולת ללא הסכמתו. בחוק נקבע, בין היתר, הצורך ברישום מאגרי המידע בפנקס מאגרי המידע והגורמים האחראים לאבטחת המידע שבמאגר המידע. הפרת החוק גוררת ענישה פלילית ואזרחית.

תקנות הגנת הפרטיות (אבטחת מידע), התשע"ז-2017 (להלן - תקנות הגנת הפרטיות), נכנסו לתוקף במאי 2018. התקנות נועדו לצקת תוכן לעקרונות שנקבעו בחוק הגנת הפרטיות בדבר האחריות לאבטחת מידע במאגר המידע, והן כוללות, בין היתר, מינוי ממונה על אבטחת המידע ואת חובותיו, ובכלל זה החובות לקבוע נוהל אבטחת מידע; לגבש מסמך הגדרות מאגר הכולל מידע על סיכונים עיקריים של פגיעה באבטחת המידע שבמאגר; למפות את מערכות מאגר המידע; החובות הנוגעות לניהול כוח האדם החשוף למאגר; לניהול הרשאות הגישה למאגר המידע; ולתיעוד אירועי אבטחה; וכן את החובות בעניין השימוש בשירותי מיקור חוץ[18]. עוד נקבע בתקנות כי חובות בעל מאגר חלות על מנהל מאגר והמחזיק בו, ובכלל זה חלה עליו החובה לתעד ביצוע פעולות.

"מחזיק" לעניין מאגר מידע הוגדר בחוק הגנת הפרטיות כלהלן: "מי שמצוי ברשותו מאגר מידע דרך קבע והוא רשאי לעשות בו שימוש". "בעל מאגר מידע" הוגדר באתר המרשתת של הרשות להגנת הפרטיות "הגוף שלצרכיו ולמטרות פעילותו נאסף המידע, ובידיו היכולת המשפטית להחליט, בכפוף להוראות החוק, לאילו מטרות ישמש המידע ומה ייעשה בו. לפי החוק, בעל המאגר הוא הנושא העיקרי באחריות לעניין איסוף המידע וניהול המאגר ובחובות כלפי האדם שהמידע נוגע אליו"[19].

---

18 מבקר המדינה, **סייבר ומערכות מידע** (מאי 2023), "הגנת הפרטיות ואבטחת המידע במערכות המרכז לגביית קנסות, אגרות והוצאות ברשות האכיפה והגבייה", עמ' 386.

19 ראו: https://www.gov.il/he/departments/general/reporting.

הרשות המקומית היא בעלת מאגר המידע של מערכת הגבייה, וכאשר המאגר מנוהל על ידי ספק שירות של מערכת גבייה[20] הוא מוגדר כמחזיק המאגר.

בנושאי אבטחת מידע והגנת הסייבר, שאינם מפורטים בתקנות, דוח זה מתייחס לתורת ההגנה בסייבר של מערך הסייבר הלאומי ולהחלטת ממשלה 2443[21], כמייצגים סטנדרטים מקובלים ונורמות מקובלות בתחומים אלה.

גופי אסדרה

את נושא ניהול מערכות מידע ואבטחתם מסדירים ומנחים כמה גופים:

הרשות להגנת הפרטיות: זהו הגוף המסדיר, המפקח והאוכף על פי חוק הגנת הפרטיות וחוק חתימה אלקטרונית, התשס"א-2001. במסגרת תפקידה, מופקדת הרשות להגנת הפרטיות על הגנת המידע האישי במאגרי מידע דיגיטליים מכוח חוק הגנת הפרטיות ועל ביצורה של הזכות לפרטיות. לתכלית זו מפעילה הרשות רגולציה, לרבות אכיפה מינהלית ופלילית, על כלל הגופים בישראל - פרטיים, עסקיים וציבוריים, המחזיקים או המעבדים מידע אישי דיגיטלי. הרשות להגנת הפרטיות היא הגוף המומחה לטיפול בתחום ההגנה על מידע אישי במאגרי מידע דיגיטליים, וייעודה הוא להתוות את מדיניות ההגנה על המידע האישי בישראל[22].

בדוח לשנת 2021 של הרשות להגנת הפרטיות (להלן - דוח שנתי 2021) צוין כי מגזר הרשויות המקומיות הוא אחד מיעדי פיקוח הרוחב המשמעותיים[23]. זאת בשל מאפייניו הייחודיים של מגזר זה, ובהם: ניהול מידע רב ורגיש של הרשות המקומית על תושביה והחזקת מידע זה[24]; שימוש רב בנותני שירותים חיצוניים, שעלול לאפשר חשיפה למידע רגיש המאוחסן במאגרי הרשות; שיתוף פעולה שוטף עם גופים אחרים לשם קבלה ומסירה של מידע אישי על תושבים[25].

לנוכח מאפייניו הייחודיים של מגזר הרשויות המקומיות, נדרשות הרשויות המקומיות במסגרת ניהול מאגרי המידע שלהן להקפיד הקפדה יתרה על העמידה בדרישות החוק והתקנות ולהגן על פרטיות התושבים, לרבות באמצעות קיום חובות אבטחת המידע, קיום חובת השקיפות כלפי התושב שהמידע נוגע לו, התקשרות תקינה עם מעבדי מידע במיקור חוץ[26].

בדוח שנתי 2021 של הרשות להגנת הפרטיות צוין כי הליך פיקוח הרוחב[27] שביצעה הרשות להגנת הפרטיות בכ-70 רשויות מקומיות העלה ממצאים מדאיגים בקרב רשויות גדולות, בינוניות וקטנות, ולפיהם מידת עמידתן בהוראות החוק בתחום ניהול מאגרי מידע, הבקרה הארגונית ואבטחת המידע לוקה בחסר[28].

---

20 ספקי השירות של הרשויות המקומיות הנבדקות בדוח זה הם חברות פרטיות המספקות לרשויות המקומיות שירותי מערכת גבייה שבהן מנוהל מאגר המידע של מערכת הגבייה. השירותים של ספקי השירות כוללים גם את אבטחת המידע של מערכת הגבייה.

21 החלטת הממשלה מס' 2443 מפברואר 2015 בנושא: "קידום אסדרה לאומית והובלה ממשלתית בהגנת הסייבר".

22 מתוך אתר המרשתת של הרשות להגנת הפרטיות:
https://www.gov.il/he/departments/about/about_ppa

23 מערך האכיפה ברשות להגנת הפרטיות מקיים פיקוחי רוחב מגזריים או נושאיים לבחינת יישום חוק הגנת הפרטיות והתקנות מכוחו במגזרים שונים במשק הישראלי.

24 המידע הרגיש שבידי הרשות המקומית כולל, בין היתר, את נתוני מרשם התושבים, נתונים על מצבם של הנכסים ועל בעליהם, על מצב הגבייה ועל תלמידים ועל ספקי העירייה ונתונים כספיים הנוגעים להתקשרות עימם, על זהות התושבים המטופלים על ידי לשכות הרווחה, ואף מידע על ייעוץ פסיכולוגי וסוציאלי.

25 הרשות להגנת הפרטיות, דוח פעילות לשנת 2021 (שנת 2022), עמ' 31.

26 שם, עמ' 31.

27 פיקוח הרוחב התמקד בין היתר באופן ניהול המידע ברשויות בנושאי גבייה, חינוך ומצלמות אבטחה.

28 הרשות להגנת הפרטיות, דוח פעילות לשנת 2021 (שנת 2022), עמ' 31.

מערך הסייבר הלאומי: בשנים 2011 עד 2015 התקבלו שלוש החלטות ממשלה[29] בנושא קידום היכולת הלאומית במרחב הסייבר, האסדרה הלאומית בתחום זה והסדרת האחריות לטיפול בתחום הסייבר. מכוח החלטות אלו הוקמה הרשות הלאומית להגנת הסייבר (הקרויה כיום מערך הסייבר הלאומי)[30].

מערך הסייבר הלאומי הוא גוף ממלכתי, מבצעי וטכנולוגי האמון על הגנת מרחב הסייבר הלאומי ועל הקידום והביסוס של עוצמתה של ישראל בתחום (להלן - מערך הסייבר). מערך הסייבר הלאומי פועל ברמת המדינה לחיזוק תמידי של רמת ההגנה של הארגונים והאזרחים, לטיפול בתקיפות סייבר וסילוקן ולהיערכות לעת חירום בהיבט הסייבר. במסגרת תפקידיו מקדם המערך פתרונות חדשניים וטכנולוגיות צופות פני עתיד, מתווה אסטרטגיה ומדיניות בזירה הלאומית והבין-לאומית ומפתח את ההון האנושי בתחום[31].

מערך הסייבר הלאומי פרסם ביוני 2021 את המסמך "תורת ההגנה - לנהל את הסיכון: המדריך היישומי (השלם) להגנת הסייבר של הארגון" (להלן - תורת ההגנה בסייבר). מטרת תורת ההגנה היא להציג לפני המשק הישראלי שיטה מקצועית סדורה לניהול סיכוני הסייבר בארגון. באמצעות המתודה המובאת במסמך זה הארגון יוכל להכיר את הסיכונים הרלוונטיים לו, לגבש מענה הגנתי בעניינם ולממש בהתאם לכך תוכנית להפחתת הסיכונים[32].

הנחיה מקצועית של הרשויות המקומיות בתחום הגנת סייבר

החלטת הממשלה 2443 עסקה במשרדי הממשלה המחילים את סמכויות הרגולציה שלהם על גופים או פעילויות החשופים לאיומי סייבר. בהחלטה נקבע כי יוטל על המנכ"לים של המשרדים האמורים להסדיר את ההיערכות לאיומי סייבר במסגרת המגזר שבו הם פועלים, וזאת באמצעות הקמת יחידות להכוונה מגזרית. כל יחידה להכוונה מגזרית תהיה כפופה למשרד הממשלתי שהיא שייכת אליו, בהתאם לסמכויות הרגולציה שלו, ותפעל בהנחיה מקצועית של מערך הסייבר.

החלטת הממשלה 2443 מגדירה את תפקידי יחידות הסייבר המגזריות:

1. הכוונה והנחיה בהיבטי הגנת הסייבר, לרבות הגדרה של המדיניות ודרישות האסדרה, ליווי מקצועי שוטף ומענה על פניות מקצועיות בהתאם למאפיינים של הגופים אשר בעניינם מתבצעת הפעילות. בנושאים שחל עליהם החוק להסדרת הביטחון בגופים ציבוריים, התשנ"ח-1998, ובנושאים שחל עליהם חוק הגנת הפרטיות[33] תתבצע ההנחיה בתיאום עם הגורם המוסמך לכך מכוח חוקים אלו, אם הדבר יידרש.

2. בקרת קיום הדרישות המקצועיות בהתאם לאסדרה וברמה המקצועית הנדרשת, לרבות הכרת הפערים והצורך בהתאמות.

3. בנייה והפעלה של תהליכי שיתוף מידע פנימיים וחיצוניים בקרב המגזר, לרבות דיווח על אירועים, איומים, חולשות, פוגענים ונוזקות למרכז הארצי לניהול אירועי סייבר[34] (CERT לאומי) וכן הגדרת הנהלים ושיטות הדיווח בין הגופים במגזר.

---

29 החלטת הממשלה 3611, "קידום היכולת הלאומית במרחב הקיברנטי" (7.8.2011); החלטת הממשלה 2444, "קידום ההיערכות הלאומית להגנת הסייבר" (15.2.15); החלטת הממשלה 2443, "קידום אסדרה לאומית והובלה ממשלתית בהגנת הסייבר" (15.2.15).

30 מבקר המדינה, **דוח מבקר המדינה בנושא סייבר ומערכות מידע - דצמבר 2022**, "ניהול מידע ביומטרי בצה"ל והגנת הסייבר עליו".

31 אתר המרשתת של מערך הסייבר הלאומי:
https://www.gov.il/he/departments/israel_national_cyber_directorate/govil-landing-page

32 "**תורת ההגנה - לנהל את הסיכון: המדריך היישומי (השלם) להגנת הסייבר של הארגון**" (יוני 2021), עמ' 8.

33 בחוק הוסמכה רשות להגנת הפרטיות למלא תפקידים בעניין מאגרי המידע.

34 Computer Emergency Response Team הינו הזרוע המבצעית של מערך הסייבר הלאומי. ה-CERT מטפל באירועי סייבר במרחב האזרחי של מדינת ישראל.

4. ייזום ומימוש של פעילות רוחבית, לרבות הקמת תשתיות והפעלת מנגנונים שתכליתם שיפור הגנת הסייבר במגזר[35].

בעקבות קבלת החלטת הממשלה האמורה, הוקם בשנת 2017 אגף הסייבר במשרד הפנים כיחידה מקצועית מגזרית בתחום הגנת הסייבר ואבטחת המידע, הכפוף למינהל לשירותי חירום במשרד הפנים והפועל בהנחיה מקצועית של מערך הסייבר, ובין היתר הוטלה על האגף האחריות להסדרת היערכותן של הרשויות המקומיות לאיומי סייבר[36].

בדוח מבקר המדינה בנושא ניהול מערכות מידע ברשויות המקומיות משנת 2022[37] הומלץ כי משרד הפנים ומערך הסייבר יפעלו במשותף, תוך התחשבות בייחודיות של מגזר השלטון המקומי, לחלוקת הסמכויות ביניהם לשם יישום החלטת הממשלה 2443 בנוגע למגזר זה, באופן שיוסמך רגולטור מוביל להסדרת ההיערכות של הרשויות המקומיות לאיומי סייבר, וכי לאחר הסמכתו יתרמו משרד הפנים ומערך הסייבר כל אחד את חלקו - בהתאם לאופן החלוקה שייקבע - לקביעת נהלים מתאימים שיסדירו את פעילויות הרשויות המקומיות בכל הנוגע לאבטחת מידע ולהגנה עליו מפני איומי סייבר.

בדוח האמור צוינה תשובת משרד הפנים ממאי 2022 ולפיה בתוך חודשיים עד שלושה ממועד מתן התשובה (מאי 2022) הוא יסכם את מתווה המשך הפעילות של היחידה המגזרית, תוך תיאום עם מערך הסייבר. המשך הפעילות יהיה תלוי בין היתר בתקינה ובתקציב שיינתן למשרד הפנים בהקשר זה.

על אף שבתשובת משרד הפנים ממאי 2022 לדוח מבקר המדינה בנושא ניהול מערכות מידע ברשויות המקומיות הוא ציין כי עד שלושה חודשים ממועד מתן התשובה הוא יסכם את מתווה המשך הפעילות של היחידה המגזרית, נמצא כי נכון למועד סיום הביקורת הנוכחית, בסוף שנת 2023, עדיין לא תיאמו ביניהם משרד הפנים ומערך הסייבר הלאומי מתווה המסכם את המשך הפעילות של היחידה המגזרית במשרד הפנים, והיחידה הפסיקה להנחות את מגזר הרשויות המקומיות, זאת לאחר שמשרד הפנים החליט שלא להאריך את חוזי היועצים המקצועיים שפעלו במסגרת המשרד בפיקוח מינהל שירותי חירום, ואלו הסתיימו ב-30.12.23.

מנהל המינהל לשירותי חירום במשרד הפנים מסר לצוות הביקורת באוגוסט 2023 כי מאחר שמשרד הפנים לא הוגדר כרגולטור בתחום הסייבר, הוא לא הפיץ לרשויות המקומיות הוראות בנושא. עוד מסר מנהל המינהל כי מערך הסייבר הלאומי הוא הגורם המנחה, והיחידה המגזרית במשרד הפנים שטיפלה ברשויות המקומיות העבירה לרשויות המקומיות את הנחיות מערך הסייבר הלאומי, בתוספת ההתאמות הנדרשות. על פי החלטת משרד הפנים הופסקה עבודת היחידה המגזרית. לפיכך משרד הפנים אינו מבצע שום פעילות מול הרשויות המקומיות בעניין אבטחת המידע.

מערך הסייבר הלאומי ציין בספטמבר 2023 לפני צוות הביקורת כי הוא מנחה רשויות מקומיות, אך הדבר אינו מוסדר בהוראות חוק אלא הוא פרי יוזמה שגיבש מערך הסייבר הלאומי.

מהאמור עולה כי נכון למועד הביקורת אין גוף המשמש יחידה מגזרית של הרשויות המקומיות כפי שנקבע בהחלטת הממשלה 2443, אשר אחראית להנחות את הרשויות המקומיות במסגרת היערכותן להתמודדות עם אירועי סייבר.

היעדר גורם רשמי אשר אחראי להעביר הנחיות מקצועיות לרשויות המקומיות עשוי לגרום לכך שכל רשות תפעל ללא קווים מנחים ולא יינתן מענה מספק בעניין הסיכונים הקיימים ובעניין

---

35 מבקר המדינה, **דוח מבקר המדינה בנושא סייבר ומערכות מידע - דצמבר 2022** (2022), "הגנת הסייבר במשרד התחבורה", עמ' 55.

36 מבקר המדינה, **דוחות על הביקורת בשלטון המקומי לשנת 2022** (2022), "ניהול מערכות מידע ברשויות המקומיות", עמ' 1265.

37 שם, עמ' 1270.

אופן הפעולה הרצוי בעניינם. כמו כן, בהיעדר גורם כאמור לא יתאפשרו ליווי, הנחיה ובקרה על ההיערכות לקרות אירוע סייבר ועל המוכנות להתמודדות עם אירוע סייבר, במיוחד נוכח העלייה בהתקפות סייבר שהתרחשו כנגד גופים שונים במדינה במהלך מלחמת "חרבות ברזל" ופינוי הרשויות המקומיות בדרום ובצפון הארץ שעלול לחשוף את מערכות המחשוב שלהן לסיכוני אבטחת מידע.

מערך הסייבר הלאומי מסר בתשובתו למשרד מבקר המדינה באפריל 2024 וביוני 2024 כי משרד הפנים טרם הסדיר את פעילות היחידה המגזרית, אשר תפקידה לפי החלטת ממשלה 2443 לרכז את נושא הגנת הסייבר ברשויות המקומיות. עוד מסר כי לא נדרשת הגדרת חלוקת תפקידים בין משרד הפנים למערך הסייבר הלאומי אם זו כבר הוגדרה בהחלטת הממשלה. מערך הסייבר נרתם מעל ומעבר לתפקידיו במצב הדברים הנוצר בהיעדר יחידה מגזרית, כדי לסייע בהגנה הלאומית. על משרד הפנים לקדם בדחיפות את הטיפול בהיערכות לאיומי סייבר מול הרשויות המקומיות ולפעול לקיום החלטת הממשלה 2443. מערך הסייבר הוסיף כי נכון למועד תשובתו, ובעקבות סגירת היחידה המגזרית במשרד הפנים באפריל 2023, מתוך אחריות לאומית והבנת חשיבות מגזר זה והסיכונים הקיימים לו, פועל המערך בהתאם למשאביו ככל הניתן מול רשויות מקומיות מרכזיות בניסיון לסייע בהעלאת החוסן שלהן. במקביל, מאחר ואין בכך מענה מלא, רחב או קבוע, פועל מערך הסייבר מול משרד הפנים לצורך הקמת היחידה המגזרית כנדרש בהחלטת הממשלה. הגם שפועל מול רשויות מקומיות מרכזיות לטובת העלאת חוסן וסיוע בהתמודדות עם אירועי סייבר, המערך פועל מול הרשויות באופן וולונטרי, ללא כלי אכיפה ומבלי שיהיה בכך מענה כולל נדרש, ושלא בהתאם לתפיסה הקבועה בהחלטת הממשלה, הכל מתוך הבנת חשיבות המגזר במיוחד בעת הזו.

משרד הפנים מסר בתשובתו למשרד מבקר המדינה ממאי 2024 כי עמדתו, כפי שהובעה עוד בדיון בינו ובין מערך הסייבר הלאומי בשנת 2018 בעניין הנדון, היא כי אין למשרד הפנים סמכות משפטית ויכולת מעשית לקיים פיקוח ורגולציה על מערכות המחשוב של הרשויות המקומיות ולנהלן. עוד מסר משרד הפנים כי הקביעה ולפיה הוא ישמש גורם מסייע לרשויות המקומיות היא בעייתית, מכמה סיבות. ראשית אין למשרד מלוא הסמכויות הנדרשות בתחום זה. שנית, המשרד אינו בעל מכלול הידע ומומחיות התוכן הנדרשים בתחום מורכב ומקצועי זה, אשר אמונים עליו גורמים ייעודיים אחרים במדינה כמערך הסייבר הלאומי. שלישית, קשה להתוות גבולות ברורים בין פעילות משרד הפנים כנותן "סיוע" בלבד לרשויות בתחום זה לבין פעילותו הנגזרת מהסמכות שאליה מכוונת החלטת הממשלה דלעיל - לשמש הרגולטור האמון על הכוונה ואף הנחיה של רשויות מקומיות. בייחוד של רשויות הכפופות בעת שגרה לרגולציית משרד הפנים. הבעייתיות שבכך מתחדדת לנוכח העובדה כי לא ברור איזה גורם ישמש רגולטור של פעילויות הרשויות בתחום האמור, וכי שום גורם אינו מוכן להכיר באחריותו לכך. עוד המשרד הוסיף כי לאורך התקופה האמורה לא נמשכה בחינת הנושא, והעניין עדיין לא הוכרע.

כפי שכבר העיר משרד מבקר המדינה בדוח הביקורת משנת 2022, על משרד הפנים, שהוא הרגולטור של הרשויות המקומיות, לפעול בשיתוף מערך הסייבר הלאומי לקביעת הגורם אשר ישמש יחידה מגזרית עבור הרשויות המקומיות, ינחה אותן בעניין ההיערכות לאירועי סייבר ויפקח על אופן יישום ההנחיות.

מדיניות ונהלים בתחום אבטחת המידע

מדיניות אבטחת מידע

מדיניות להגנת הסייבר מבוססת על הערכת הסיכונים בתחום אבטחת המידע הנשקפים למערכות המחשוב, למעבדות שמאחסנות את המידע ולרשתות התקשורת, תוך התאמה לצרכים התפעוליים והארגוניים. העקרונות המנחים במדיניות להגנת הסייבר המאושרת על ידי הנהלת הארגון יכולים לשמש בסיס לנוהלי העבודה בתחום הגנת הסייבר. מדיניות להגנת סייבר אפשר שתיקבע בהתאם לחוקים, לתקנות ולתקנים[38].

תקן ISO 27001 הוא תקן בין-לאומי לניהול אבטחת מידע. בתקן צוין כי ההנהלה של ארגון תקבע מדיניות אבטחת מידע, המתאפיינת בין היתר בתכונות אלה: יש הלימה בינה ובין תכלית הארגון; מוצבות בה מטרות בתחום אבטחת המידע ולחלופין היא מספקת את המסגרת להצבת מטרות אלה; המדיניות כוללת מחויבות לעמוד בדרישות הישימות הנוגעות לאבטחת מידע; והיא אף כוללת מחויבות לשיפור מתמיד של המערכת לניהול אבטחת מידע.

בבקרות של תורת ההגנה בסייבר שהכין מערך הסייבר הלאומי הוגדר בין היתר שארגון נדרש לאשר מדיניות הגנת מידע וסייבר.

אף שמערך הסייבר הלאומי העלה את חשיבות הכנתו של מסמך מדיניות הגנת מידע וסייבר, נוסף לנאמר בתקן ISO 27001, נמצא כי לשלוש מהרשויות המקומיות שנבדקו, רשויות מקומיות ב', ג' ו-ה' אין מסמכי מדיניות בנושא אבטחת מידע. רשות מקומית ג' הכינה טיוטה של מסמך כזה, אך הנהלת הרשות המקומית טרם אישרה אותו. יתר הרשויות המקומיות שנבדקו, רשויות מקומיות א', ד' ו-ו', הכינו מסמכי מדיניות.

היעדר מסמך מדיניות שיכלול יעדים ומטרות ברורים עלול לפגוע בהיערכות רשויות מקומיות להתמודדות עם ההיבטים הנוגעים לאבטחת מערכות מידע ולהגנה על פרטיות.

מומלץ לרשויות המקומיות ב' ו-ה' להכין מסמך מדיניות אבטחת מידע, ולהגישו לאישור הנהלת הרשות המקומית, כדי שישמש בסיס לכתיבת נוהלי אבטחת מידע. כמו כן, מומלץ לרשות מקומית ג' להשלים את הכנת מסמך המדיניות בנושא אבטחת מידע ולהגישו לאישורה של הנהלת הרשות המקומית.

רשות מקומית ב' מסרה בתשובתה למשרד מבקר המדינה מיוני 2024 כי היא מקבלת את ממצאי הדוח ותפעל ככל שניתן לאמץ את ההמלצות ולתקן את הליקויים ככל שאפשר.

רשות מקומית ג' מסרה בתשובתה למשרד מבקר המדינה מאפריל 2024 כי היא נמצאת בתהליך התקשרות עם ממונה אבטחת מידע חיצוני, וכי במסגרת תחומי האחריות של הממונה, יבוצע עדכון של הטיוטה ואישורה. היעד להשלמת המסמך הוא הרבעון הרביעי של שנת 2024.

רשות מקומית ה' מסרה בתשובתה למשרד מבקר המדינה מיוני 2024 כי הרשות מתכננת לקלוט למשרה חלקית מנהל אבטחת מידע (CISO) שבין יתר תפקידיו יהיה לכתוב מסמך זה. עוד מסרה הרשות כי כיוון שהיא מצויה בתוכנית הבראה מחד גיסא וחסרה בעלי תפקידים רבים מאידך גיסא, קליטת עובד זה מתעכבת משיקולי תעדוף ועלות, וכי לנוכח ממצאי הביקורת יוצג העניין בפני משרד הפנים בתקווה לקדם את קליטתו.

---

38 ראו: (א) מבקר המדינה, **דוח מבקר המדינה בנושא סייבר ומערכות מידע - דצמבר 2022** (2022), "ניהול מידע ביומטרי בצה"ל והגנת הסייבר עליו", עמ' 133; (ב) הנחיות ראש רשות התקשוב הממשלתי, הנחיות היחידה להגנת הסייבר בממשלה - יה"ב - **מדיניות להגנת הסייבר בממשלה**, סעיפים 5.4,5.5. יצוין כי הנחיות אלה אינן חלות על השלטון המקומי.

נוהל אבטחת מידע

הכנת נוהל אבטחת מידע

בתקנות הגנת הפרטיות נקבע שהממונה על האבטחה בארגון יכין נוהל אבטחת מידע ויביאו לאישור בעל המאגר. לפי התקנות בעל מאגר המידע יקבע נוהל אבטחת מידע בהתאם למסמך הגדרות המאגר והתקנות, הנוהל יחייב כל בעל הרשאה בהתאם לפרטים מהנוהל שאליו הוא חשוף. עוד נקבע בתקנות כי בעל מאגר מידע ישמור את נוהל האבטחה באופן שפרטים ממנו יימסרו לבעלי הרשאה רק בהיקף הנדרש לצורך ביצוע תפקידיהם.

על פי התקנות, נוהל אבטחת מידע יכלול, בין היתר: הוראות בעניין האבטחה הפיזית והסביבתית של אתר המאגר; הרשאות גישה למאגר; תיאור של אמצעים שמטרתם הגנה על מערכות המאגר ושל אופן הפעלתם לצורך כך; הסיכונים שחשוף להם המידע שבמאגר, במסגרת הפעילות השוטפת של בעל המאגר; אופן ההתמודדות עם אירועי אבטחת מידע.

בדוח פיקוח רוחב שהכינה הרשות להגנת הפרטיות בשנת 2021[39], בין יתר הליקויים, עלה כי בחלק גדול מהרשויות המקומיות כלל לא קיים נוהל אבטחת מידע, ובאלה שיש ברשותן נוהל בנושא - הוא כולל פחות מ-50% מהסעיפים המפורטים בהוראות התקנות. גם בקרב הרשויות המקומיות הגדולות, שבהן נמצא השיעור הגדול ביותר של רשויות שברשותן נוהל אבטחת מידע, ב-63% מהן הנוהל אינו כולל את כל שנדרש לכלול בו על פי התקנות.

על אף שבתקנות הגנת הפרטיות נקבע כי בעל המאגר והממונה על האבטחה בארגון יכינו נוהל אבטחת מידע, נמצא כי שתיים מהרשויות המקומיות שנבדקו, רשויות מקומיות ב' ו-ה', לא הכינו נוהל אבטחת מידע כנדרש בתקנות. יתר הרשויות המקומיות שנבדקו, רשויות מקומיות א', ג', ד' ו-ו', הכינו נוהל אבטחת מידע.

נוהל אבטחת מידע אמור לסייע לרשות המקומית לקבוע את תהליכי העבודה לעמידה ביעדי הנוהל. היעדר נוהל עשוי להוביל לקיום תהליכי עבודה שאינם תואמים את הנדרש להשגת היעדים ובכך לתת מענה חלקי על הסיכונים הקיימים.

על רשויות מקומיות ב' ו-ה', וכלל הרשויות המקומיות שלא הכינו נוהל אבטחת מידע או שהנוהל שהכינו היה חלקי, להכין נוהל כאמור ולכלול בו את מלוא ההוראות שנקבעו בתקנות הגנת הפרטיות, וכי הנהלת הרשות המקומית תבחן את יישומו בפועל. מומלץ כי הרשות להגנת הפרטיות תמשיך בפועלה כרגולטור מרכזי כדי לוודא כי רמת האבטחה של מאגרי המידע במשק בכלל, וברשויות מקומיות בפרט, תואמת את דרישות אבטחת המידע המתחייבות על פי החוק והתקנות, לרבות על פי האמור בתקנה 4 בדבר קביעת נוהל אבטחת מידע.

רשות מקומית ה' מסרה בתשובתה כי מנהל אבטחת המידע שייקלט יהיה אמון גם על כתיבת נוהל זה ועל הטמעתו ואכיפתו בקרב עובדי הרשות.

הרשות להגנת הפרטיות מסרה בתשובתה למשרד מבקר המדינה מאפריל 2024 כי היא מברכת על הקביעה הברורה שלפיה על כלל הרשויות המקומיות שלא הכינו נוהל אבטחת מידע (או הכינו נוהל חלקי) להכין נוהל כאמור, וכי על הנהלת הרשות המקומית לבחון את יישומו בפועל.

התאמת נוהל אבטחת מידע ברשויות שנבדקו לנדרש בתקנות הגנת הפרטיות

בתקנות הגנת הפרטיות נקבעו בין השאר נושאים שיש לכלול בנוהל האבטחה: הוראות בעניין האבטחה הפיזית והסביבתית של אתרי המאגר; הרשאות גישה למאגר המידע ולמערכותיו; תיאור של אמצעים שמטרתם הגנה על מערכות המאגר ואופן הפעלתם לצורך כך; הוראות למורשי הגישה

---

39 הרשות להגנת הפרטיות, **דוח פיקוח רוחב - ממצאי הליך פיקוח הרוחב בקרב רשויות מקומיות** (2021), עמ' 24. במסגרת הדוח בוצעה בדיקה בקרב 70 רשויות מקומיות.

למאגר המידע ולמערכות המאגר לצורך הגנה על המידע במאגר; פירוט הסיכונים שחשוף להם המידע שבמאגר במסגרת הפעילות השוטפת של בעל מאגר המידע, לרבות אלה שמקורם במבנה מערכות המאגר, אופן קביעת סיכונים אלה ואופן הטיפול בהם, לרבות על ידי מנגנוני הצפנה מקובלים להגנה על המידע השמור במאגר או במערכות המאגר; אופן ההתמודדות עם אירועי אבטחת מידע, לפי חומרת האירוע ומידת רגישות המידע; הוראות לעניין ניהול של התקנים ניידים ולעניין השימוש בהם.

בלוח שלהלן פירוט לגבי התאמת נוהלי אבטחת מידע לדרישות שבתקנות הגנת הפרטיות ברשויות המקומיות שנבדקו והכינו נוהל כאמור.

לוח 2: **מידת ההתאמה בין נוהל אבטחת מידע של רשויות מקומיות א', ג', ד' ו-ו' לנדרש בתקנות הגנת הפרטיות**

שם הרשות	התייחסות לאבטחת מידע פיזית וסביבתית	התייחסות להרשאות גישה למאגר המידע	תיאור של אמצעי ההגנה על מערכות המאגר	הוראות למורשי הגישה למאגר המידע ולמערכות המאגר	סיכונים שמאגר המידע חשוף להם	אופן ההתמודדות עם אירועי אבטחת מידע	הוראות לעניין התקנים ניידים והשימוש בהם
רשות מקומית א'	✓	✓	✓	✓	✓	✓	✓
רשות מקומית ג'	✓	✓	✓	✓	✓	✓	✓
רשות מקומית ד'	✓ *	✓	✓	✓	×	✓ **	✓
רשות מקומית ו'	✓	✓	✓	✓	✓	✓ ***	✓

הוכן בידי משרד מבקר המדינה.

* נכלל במסמך מדיניות אבטחת מידע של הרשות המקומית.

** נכלל במסגרת "נוהל אירועים חריגים - אבטחת מידע".

*** נכלל במסגרת "נוהל תגובה לאירוע אבטחת מידע".

מהלוח עולה כי הרשויות המקומיות א', ג' ו-ו' מילאו את הנקבע בתקנות הגנת הפרטיות וכללו את המרכיבים הנדרשים בנוהלי אבטחת המידע שלהן. רשות מקומית ד' לא פירטה בנוהלי אבטחת המידע שלה את הסיכונים שאליהם חשוף מאגר המידע שלה. אי הכללת הוראות ופירוט בדבר הסיכונים להם חשוף מאגר המידע של רשות מקומית ד', עלול לפגוע בהיערכותה להתמודדות עם איומים אפשריים.

על רשות מקומית ד' לפרט בנוהלי אבטחת המידע שלה את הסיכונים שמאגר המידע חשוף להם, את אופן קביעת הסיכונים ואת אופן הטיפול בהם, כנקבע בתקנות הגנת הפרטיות. הדבר יאפשר לרשות המקומית לייעל את היערכותה לאיומים הרלוונטיים ואת ההתמודדות איתם.

רשות מקומית ד' מסרה בתשובתה למשרד מבקר המדינה מאפריל 2024 כי היא תבחן את נוהל אבטחת המידע כנדרש בתקנות, לרבות את פירוט הסיכונים שמאגר המידע חשוף אליהם.

ניהול מאגרי מידע של מערכת הגבייה

בחוק הגנת הפרטיות מוגדר מידע כלהלן: הנתונים על אישיותו של אדם, מעמדו האישי, צנעת אישיותו, מצב בריאותו, מצבו הכלכלי, הכשרתו המקצועית, דעותיו ואמונתו.

גילוי דעת שפרסמה הרשות להגנת הפרטיות בדצמבר 2022 מבהיר ומדגים מהו מידע לעניין חוק הגנת הפרטיות וכן מהם סוגי הנתונים שעליהם חלות הוראות חוק זה בהתאם לפרשנותם של בתי המשפט בנוגע לכך. להלן דוגמאות לנתונים הנחשבים/המוגדרים "מידע" לעניין חוק הגנת הפרטיות, אשר נכללו בגילוי הדעת[40]:

1. **אישיותו של אדם:** פרטים אישיים מסוימים על אדם, לרבות מידע שמקורו במבחני התאמה לעבודה, מידע בדבר עברו הפלילי של אדם, ומידע בדבר מוצאו של אדם.

2. **מעמדו האישי:** כגון היותו נשוי, רווק, אלמן או יתום מהוריו.

3. **צנעת אישיותו:** התנהגות אדם ברשות היחיד, נטייה מינית.

4. **מצבו הבריאותי:** מידע גנטי, מידע רפואי או מידע על מצבו הנפשי של אדם, היותו נשא של נגיף מסוים.

5. **מצבו הכלכלי:** נכסיו של אדם, חובותיו והתחייבויותיו הכלכליות, לרבות יכולתו לעמוד בהן ומידת עמידתו בהן בפועל, שינוי במצבו הכלכלי, מקרקעין שברשותו, בעלות על רכב, ירושה, צו עיקול שהוצא נגדו, השקעותיו, מידע על השתכרותו ומידע בנקאי.

6. **דעותיו ואמונתו:** תפיסת עולם, דעה פוליטית או אמונה דתית של אדם.

מערכות הגבייה ברשויות המקומיות כוללות מאגרי מידע על תושבי הרשויות המקומיות וכוללות בין היתר פרטי מידע המפורטים לעיל, כגון פרטים אישיים, נכסים שברשותם, מידע על מצבם הכלכלי.

קביעת רמת האבטחה של מאגרי המידע

תקנות הגנת הפרטיות מפרטות את אופן החלתה של חובת אבטחת המידע המוטלת בחוק הגנת הפרטיות על כל בעל מאגר של מידע אישי, מנהל המאגר והמחזיק בו. התקנות חלות על כלל המשק הישראלי, ונקבעו בהן מנגנונים ארגוניים ודרישות מהותיות, שמטרתם להפוך את אבטחת המידע לחלק משגרת הניהול השוטף של הארגון. עוד נקבעו בתקנות מאפיינים הנוגעים לסוג המידע, להיקפו ולגורם שהמאגר בבעלותו, שבהתאם להם נקבעת רמת האבטחה שחלה על מאגר המידע: בסיסית, בינונית או גבוהה.

לפי תקנות הגנת הפרטיות, על כל רשות מקומית להגדיר מהי רמת האבטחה החלה על כל אחד מן המאגרים שבבעלותה - בינונית או גבוהה. בהתאם להגדרת רמת האבטחה של המאגר תבחן הרשות המקומית אילו תקנות חלות על המאגר. בתקנות נקבע לגבי מאגר שבבעלות גוף ציבורי, כמו רשות מקומית[41], כי חלה עליו לכל הפחות רמת האבטחה הבינונית. עוד נקבע בתקנות כי רמת האבטחה הגבוהה תחול על מאגר שבבעלות גוף ציבורי אם שמור בו מידע על 100,000 אנשים ויותר או אם מספר בעלי ההרשאה לעיון בנתוני המאגר ולביצוע פעולות בו גדול מ-100, אם מדובר במאגר שמטרתו העיקרית היא איסוף מידע לצורך מסירתו לאחר כדרך עיסוק, או במאגר מידע הכולל מידע שהוא אחד מאלה: מידע על צנעת חייו האישיים של אדם, לרבות מידע על התנהגותו ברשות

---

40 הרשות להגנת הפרטיות, "**מהם 'מידע' ו'ידיעה על ענייניו הפרטיים של אדם' בחוק הגנת הפרטיות**".

41 המדריך המלא לתקנות הגנת הפרטיות, עמ' 2.

היחיד; מידע רפואי או מידע על מצבו הנפשי של אדם; מידע על נכסיו של אדם, על מצבו הכלכלי או על הרגלי הצריכה שלו[42].

במאגרים שעליהם חלה רמת האבטחה הגבוהה חלות כל תקנות הגנת הפרטיות. ההבדל העיקרי בין רמות האבטחה הוא שברמת האבטחה הגבוהה נדרש לבצע סקר סיכונים או מבדקי חדירה אחת ל-18 חודשים, ואילו במאגרים שרמת האבטחה בהם בינונית הדבר לא נדרש. עם זאת, נדרש כי גורם בעל הכשרה מתאימה לביקורת בנושא אבטחת מידע, שאינו ממונה האבטחה של המאגר, יבצע במאגרים שרמת האבטחה בהם בינונית או גבוהה ביקורת פנימית או חיצונית אחת ל-24 חודשים.

יצוין כי מאגר הכולל 100,000 אנשים ויותר אינו בהכרח תלוי במספר תושבי אותה רשות, שכן המאגר עשוי לכלול רשומות של אזרחים תושבי רשויות מקומיות אחרות ששילמו תשלומים לאותה רשות מקומית (עבור השתתפות בחוגים, בלימודים ובהכשרות שמקיימת הרשות, דמי מנוי לבריכת שחייה של הרשות, תשלומים עבור חנייה וכדומה). ומכאן שמוטלת על כל רשות האחריות לבחון ביוזמתה את מאגרי המידע שלה באופן שוטף נוכח השינויים התכופים שעשויים להתחולל בו.

על כל רשות מקומית להגדיר מהי רמת האבטחה החלה על כל אחד מן המאגרים שבבעלותה - בינונית או גבוהה בהתאם לתקנות הגנת הפרטיות. נמצא כי רשויות מקומיות א' ו-ג' הגדירו את רמת האבטחה הנדרשת למאגרי המידע של מערכת הגבייה שלהן כגבוהה, בכפוף להיקף מאגריהן ובהתאם לתקנות הגנת הפרטיות. רשות מקומית ו' הגדירה את רמת האבטחה הנדרשת כבינונית. עם זאת נמצא כי רשויות מקומיות ב', ד' ו-ה' לא הגדירו את רמת האבטחה הנדרשת למאגריהן בכפוף להיקפם, ומשום כך לא היה ידוע להן אם חלה על מאגריהן רמת אבטחה גבוהה, דבר שמטיל עליהן חובות אבטחה מיוחדות (לעומת רמת אבטחה בינונית). נציין כי רשות מקומית ד' רשמה את נתוני מאגר מערכת הגבייה ברשם מאגרי המידע, ועם זאת לא ידעה להגדיר את רמת האבטחה בהתאם לתקנות הגנת הפרטיות.

אם רשות אינה יודעת מהי רמת האבטחה הנדרשת ממנה ייתכן שלא יהיה באפשרותה לעמוד בדרישות אבטחת המידע בהתאם לתקנות, ובהן הדרישה לבצע סקרי סיכונים ולקיים מבדקי חדירה.

על רשויות מקומיות ב', ד' ו-ה' לקיים בדיקה בדבר היקפם של מאגרי המידע שלהן, על מנת שיוכלו לקבוע את רמת האבטחה הנדרשת של מאגריהן. אם יתברר לרשויות המקומיות כי הן מחויבות ברמת אבטחה גבוהה, עליהן לפעול בהתאם לדרישות האבטחה שנקבעו בתקנות לעניין רמת אבטחה זו.

רשות מקומית ד' מסרה בתשובתה כי היא תבצע בדיקה בדבר היקפם של מאגרי המידע ותקבע את רמת האבטחה הנדרשת של המאגרים. כמו כן, היא תפעל לקיום דרישות האבטחה שנקבעו בתקנות לעניין רמת האבטחה.

רשות מקומית ה' מסרה בתשובתה כי הרשות החלה בתהליך רישום מאגרי המידע שלה אצל רשם מאגרי המידע אך התהליך לא הושלם בעקבות מחסור בכח אדם וביעוץ מקצועי לגבי היקף וסוג המידע שיש לכלול בכל מאגר. עוד מסרה העירייה כי לאחר השלמת תהליך רישום מאגרי המידע תוגדר רמת האבטחה החלה על כל מאגר.

---

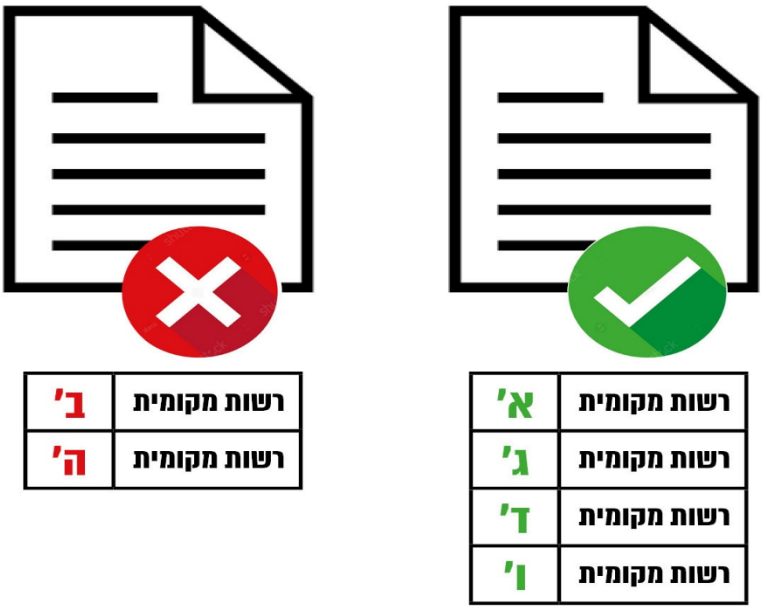
42 סעיף 1 לתוספת הראשונה לתקנות הגנת הפרטיות; סעיפים (1), (2) לתוספת השנייה לתקנות הגנת הפרטיות. ראו גם מבקר המדינה, דוחות על הביקורת בשלטון המקומי (2022), "**ניהול מערכות מידע ברשויות המקומיות**", עמ' 1287.

רישום מאגרי המידע של מערכת הגבייה אצל רשם מאגרי המידע

בחוק הגנת הפרטיות נקבע כי אדם המנהל מאגר מידע או המחזיק בו מחויב לבצע רישום שלו בפנקס של רשם[43] מאגרי המידע. עוד נקבע בחוק כי בבקשה לרישום יפורטו, בין היתר, זהותם של בעל מאגר המידע, המחזיק במאגר ומנהל המאגר[44] ומעניהם בישראל; מטרות הקמת מאגר המידע והמטרות שלהן נועד המידע. בחוק גם נקבעו סמכויות הרשם, שלפיהן, בין היתר, הוא יפקח על מילוי הוראות חוק זה והתקנות לפיו. על בעל המאגר לרושמו אם בעל המאגר הוא, בין היתר, רשות מקומית, בהיותה גוף ציבורי כהגדרתו בחוק הגנת הפרטיות.

מטרת רישום המאגר היא להבטיח הגנה על הפרטיות של מאגרי המידע ולתת כלים, הן בידי רשם מאגרי המידע והן בידי הציבור שהמידע עליו מנוהל במאגרי המידע, שמאפשרים לאכוף את החובות המוטלות בחוק הגנת הפרטיות על בעלי המאגרים ולממש את זכויותיהם[45].

תרשים 1: **רישום מאגרי המידע של מערכת הגבייה של הרשויות המקומיות שנבדקו בפנקס מאגרי המידע, נכון ל-24.12.23**[46]



הוכן בידי משרד מבקר המדינה.

על אף שבחוק הגנת הפרטיות נקבע כי אדם המנהל מאגר מידע או המחזיק בו מחויב לבצע רישום שלו בפנקס של רשם מאגרי המידע, נמצא כי שתיים מהרשויות המקומיות שנבדקו - רשויות מקומיות ב' ו-ה' לא רשמו את מאגרי המידע של מערכת הגבייה בפנקס מאגרי המידע. יתר הרשויות שנבדקו - רשויות מקומיות א', ג', ד' ו-ו' רשמו את מאגרי המידע של מערכת הגבייה בפנקס.

43 בסעיף 7 לחוק הגנת הפרטיות הוגדר רשם: "מי שמתקיימים בו תנאי הכשירות למינוי שופט של בית משפט השלום, והממשלה מינתה אותו, בהודעה ברשומות, לנהל את פנקס מאגרי מידע _להלן - הפנקס) כאמור בסעיף 12"; בסעיף 12(א) לחוק צוין כי הרשם ינהל פנקס מאגרי מידע אשר יהיה פתוח לעיונו של הציבור.

44 בסעיף 7 לחוק הגנת הפרטיות הוגדר מנהל מאגר: "מנהל פעיל של גוף שבבעלותו או בהחזקתו מאגר מידע או מי שמנהל כאמור הסמיכו לכך".

45 אתר המרשתת של הרשות להגנת הפרטיות:
www.gov.il/he/Departments/Guides/registration_fqa?chapterIndex=1

46 על פי הנתונים באתר המרשתת של הרשות להגנת הפרטיות.
https://data.gov.il/dataset/pinkas/resource/fd56bf5b-7918-4906-99e4-b0e5102ae268

על רשויות מקומיות ב׳ ו-ה׳ לרשום את מאגרי המידע של מערכת הגבייה שלהן בפנקס מאגרי המידע בהתאם להוראות חוק הגנת הפרטיות.

מסמך הגדרות המאגר

ריכוז נתונים עדכניים בדבר תוכנו של כל מאגר מידע ומטרותיו יכול לאפשר לרשות המקומית לנהל ביעילות את מאגר המידע ובד בבד לבצע בקרה שוטפת על דבר נחיצותם של כל מרכיבי המאגר.

קיומו של "מסמך הגדרות מאגר" ברשויות שנבדקו

בתקנות הגנת הפרטיות נקבע כי על בעל מאגר מידע להכין "מסמך הגדרות מאגר" שיעסוק, בין היתר, בנושאים אלה: תיאור כללי של פעולות איסוף המידע והשימוש בו; תיאור מטרות השימוש במידע; סוגי המידע השונים הכלולים במאגר המידע; פעולות עיבוד מידע המתבצעות באמצעות המחזיק במאגר המידע; הסיכונים העיקריים של פגיעה באבטחת המידע ואופן ההתמודדות עימם; שמו של מנהל מאגר המידע, של המחזיק במאגר ושל הממונה על אבטחת מידע בו, אם מונה בעל תפקיד כזה. יצוין כי קיומו או אי-קיומו של מסמך הגדרות מאגר אינו מעיד בהכרח על רישום המאגר בפנקס מאגרי מידע.

על אף שבתקנות הגנת הפרטיות נקבע כי על בעל מאגר מידע להכין "מסמך הגדרות מאגר", נמצא כי אין בידי רשויות מקומיות ב׳, ג׳ ו-ה׳ מסמך הגדרות מאגר מידע הכולל את הפרטים הנדרשים על פי תקנות הגנת הפרטיות. רשויות מקומיות א׳, ד׳ ו-ו׳ הכינו "מסמך הגדרות מאגר". נמצא כי מסמך הגדרות המאגר של רשות מקומית א׳ לא כלל את פעולות עיבוד המידע המתבצעות באמצעות המחזיק במאגר המידע; הסיכונים העיקריים של פגיעה באבטחת המידע ואופן ההתמודדות עימם; שמו של מנהל מאגר המידע ושל הממונה על אבטחת המידע בו. כמו כן, אין מסמך המתעד את בחינת עדכניות מסמך הגדרות המאגר ואת הבחינה שנועדה לוודא כי לא נשמר מידע רב מן הנדרש.

קיומו של מסמך הגדרות מאגר הכולל את הנדרש בתקנות הגנת הפרטיות יסייע לרשות מקומית לנהל את מאגרי המידע, ובכלל זה להשמטת הנתונים שנמצא כי אינם חיוניים, כדי להפחית את הסיכון שבניהול המאגר.

על רשויות מקומיות ב׳, ג׳ ו-ה׳ להכין עבור מערכת הגבייה מסמך הגדרות מאגר מידע שיכלול את כלל המידע הנדרש בהתאם לתקנות הגנת הפרטיות. על רשות מקומית א׳ לכלול במסמך הגדרות המאגר את כל המידע הנדרש בתקנות הגנת הפרטיות. כמו כן עליה לבצע בחינה שנתית בנושא עדכניות מסמך הגדרות המאגר עבור מערכת הגבייה ובחינה שנתית שנועדה לוודא כי לא נשמר במערכת מידע רב מן הנדרש, ועליה לתעד את מועד ביצוע הבדיקה במסמך הגדרות המאגר שלה.

עדכניות מסמך הגדרות המאגר

בתקנות הגנת הפרטיות נקבע כי בעל מאגר מידע יעדכן את מסמך הגדרות המאגר בכל עת שנעשה שינוי משמעותי בנושאים המפורטים בו, וכי הוא יבחן את הצורך בעדכון כאמור, בשל שינויים טכנולוגיים ארגוניים או אירועי אבטחה, בכל שנה עד 31 בדצמבר. עוד נקבע בתקנות כי בעל מאגר מידע יבחן, אחת לשנה, אם אין המידע שהוא שומר במאגר רב מן הנדרש למטרות המאגר.

בתקנות הגנת הפרטיות נקבע שבעל מאגר יבצע בחינה של עדכניות מסמך הגדרות המאגר ובחינה אם המאגר כולל מידע רב מן הנדרש. נמצא כי רשות מקומית ו׳ בחנה את מידת העדכניות של מסמך הגדרות המאגר של מערכת הגבייה בנובמבר 2023. כמו כן היא בחנה אם שמור במערכת הגבייה שלה מידע רב מן הנדרש בחודשים נובמבר-דצמבר 2023. נמצא כי רשות מקומית ד׳ בחנה את עדכניות מסמך הגדרות המאגר של מערכת הגבייה שלה במרץ 2021, כלומר, חלפו כשנתיים

וחצי ממועד עריכתה את בדיקתה האחרונה[47]. עוד נמצא כי בחודשים יוני-יולי 2023 בדקה הרשות המקומית אם במאגר המידע שלה שמור מידע רב מן הנדרש למטרות מאגר מערכת הגבייה שלה.

אם מרווח הזמן שבין בדיקות העדכניות של מסמך הגדרות המאגר גדול משנה, עלולים להיכלל במאגר רשומות מיותרות או לא עדכניות. כמו כן, ייתכן כי מידע יימצא אצל רשם מאגרי המידע, שהוא לא רלוונטי בדבר מטרות המאגר, שינויים שבוצעו בו וכו'.

על רשות מקומית ד' לבצע בחינה שנתית בנושא עדכניות מסמך הגדרות המאגר עבור מערכת הגבייה ולתעד את מועד ביצוע הבדיקה במסמך הגדרות המאגר שלה.

רשות מקומית ד' מסרה בתשובתה כי היא תבצע בחינה בנושא עדכניות מסמך הגדרות המאגר עבור מערכת הגבייה ותתעד את מועד ביצוע הבחינה. כמו כן, היא תקבע בקרה על מידת עדכניות הבדיקות.

<u>מינוי בעלי תפקידים</u>

מנהל מאגר מידע וממונה אבטחת מידע

על פי חוק הגנת הפרטיות בעל מאגר מידע, המחזיק במאגר או מנהל מאגר מידע, כל אחד מהם אחראי לאבטחת המידע שבמאגר המידע.

כמו כן, על פי חוק הגנת הפרטיות רשות מקומית נדרשת למנות ממונה על אבטחת המידע[48]. הממונה נדרש להכין תכנית לבקרה שוטפת על מידת העמידה בדרישות התקנות, לבצע אותה ולדווח לבעל מאגר המידע ולמנהל המאגר על ממצאיו. הממונה על האבטחה לא ימלא תפקיד נוסף שעלול להעמידו בחשש לניגוד עניינים במילוי תפקידו לפי תקנות אלה. זאת ועוד, בהתאם לעמדת הרשות להגנת הפרטיות, מניעת החשש לניגוד עניינים תביא לשימור של עצמאות שיקול דעתו וחוסר התלות של ממונה האבטחה. לא ניתן להשיג מטרה זו אם ממונה האבטחה יכהן בעצמו גם כמנמ"ר[49] של הארגון[50].

בלוח שלהלן מובאים ממצאים שהועלו בביקורת הנוגעים למינוי של מנהל מאגר מידע וממונה אבטחת מידע ברשויות המקומיות שנבדקו.

לוח 3: **מינוי מנהל מאגר וממונה אבטחת מידע**

שם הרשות	מנהל מאגר מידע		ממונה אבטחת מידע	
	האם מונה ותפקידו ברשות	האם יש כתב מינוי	האם מונה ותפקידו ברשות	האם יש כתב מינוי
רשות מקומית א'	✓ מנהל אגף גבייה	×	✓ **מנמ"ר הרשות המקומית**	✓
רשות מקומית ב'	✓ גזבר הרשות המקומית	×	✓ יועץ חיצוני לאבטחת מידע	×
רשות מקומית ג'	✓ גזברית הרשות המקומית	✓	✓ יועץ חיצוני לאבטחת מידע	×

47 נכון לספטמבר 2023.

48 לפי סעיף 23 לחוק זה ההגדרה "גוף ציבורי", חלה, בין היתר, על רשות מקומית.

49 מנהל יחידת טכנולוגיות דיגיטליות ומידע ראשי.

50 שאלה 2 באתר המרשתת של הרשות להגנת הפרטיות:
https://www.gov.il/he/departments/guides/data_security_fqa?chapterIndex=2

שם הרשות	מנהל מאגר מידע		ממונה אבטחת מידע	
	האם מונה ותפקידו ברשות	האם יש כתב מינוי	האם מונה ותפקידו ברשות	האם יש כתב מינוי
רשות מקומית ד'	✓ גזבר הרשות המקומית	✓	✓ קב"ט הרשות המקומית	✓
רשות מקומית ה'	✓ מנכ"ל הרשות המקומית	×	✓ **מנמ"ר הרשות המקומית**	×
רשות מקומית ו'	✓ גזברית הרשות המקומית	✓	✓ יועץ חיצוני לאבטחת מידע	✓

על פי נתוני הרשויות המקומיות שנבדקו, בעיבוד משרד מבקר המדינה.

נמצא כי כל הרשויות המקומיות שנבדקו מינו מנהל מאגר מידע כנדרש בחוק הגנת הפרטיות. עם זאת, ברשויות מקומיות א', ב' ו-ה' לא קיים תיעוד לכתב מינוי של מנהל מאגר המידע.

מומלץ כי רשויות מקומיות א', ב' ו-ה' יתעדו בכתב את מינוי מנהל מאגר המידע.

רשות מקומית א' מסרה בתשובתה למשרד מבקר המדינה מאפריל 2024 כי כתב מינוי מנהל מאגר המידע יועבר לרשות להגנת הפרטיות במהלך אפריל 2024.

רשות מקומית ה' מסרה בתשובתה כי יוכן כתב מינוי.

עוד נמצא כי כל הרשויות המקומיות שנבדקו מינו ממונה אבטחת מידע כנדרש בחוק הגנת הפרטיות. עם זאת, ברשויות מקומיות ב', ג' ו-ה', לא מתועדים כתבי המינוי של ממונה אבטחת מידע, וברשויות מקומיות א' ו-ה' ממונה אבטחת המידע משמש גם בתפקיד מנמ"ר הרשות המקומית, ועל פי עמדת הרשות להגנת הפרטיות הדבר עלול להעמיד בעלי תפקידים אלה בחשש לניגוד עניינים מבני.

רשות מקומית א' מסרה בתשובתה כי את שני התפקידים ממלא המנמ"ר, עקב העובדה שאין בעלי תפקיד מתאימים בעלי הבנה מקצועית בהיררכיה הארגונית. האופציה החלופית היחידה היא מינוי יועץ חיצוני, דבר הכרוך בהוצאה ניכרת לרשות, ונוסף על כך ההיכרות שלו עם הארגון תהיה מוגבלת, ולכן פתרון זה יהיה פחות יעיל.

על רשויות מקומיות א' ו-ה' לפעול לכך שאת תפקיד ממונה אבטחת מידע ואת תפקיד מנמ"ר הרשות ימלאו נושאי משרה שונים. כמו כן, מומלץ לרשות מקומית א' לפעול להכשרת גורם מתוך הרשות שאינו המנמ"ר, אשר יכול לשמש בתפקיד ממונה אבטחת מידע ולהבטיח כי לא ייווצר מצב שיעמיד את שני בעלי התפקידים בחשש לניגוד עניינים. מומלץ כי רשויות מקומיות ב', ג' ו-ה' יתעדו בכתב את מינוי ממונה אבטחת המידע.

רשות מקומית ג' מסרה בתשובתה כי ההערה מקובלת עליה, כי היא בתהליך התקשרות עם ממונה אבטחת מידע חיצוני, וכי המינוי יתועד לאחר השלמת הפעלת השירות.

רשות מקומית ה' מסרה בתשובתה כי המלצת הביקורת מקובלת עליה, וזו גם אחת הסיבות שבעטיין הרשות כאמור מתכננת לקלוט מנהל אבטחת מידע.

מינוי מנהל יחידת טכנולוגיות דיגיטליות ומידע ראשי - מנמ"ר

באוגדן תיאורי התפקידים של משרד הפנים צוין כי המנמ"ר משמש הסמכות הבכירה ברשות המקומית בנושאי טכנולוגיות, מידע ודיגיטל, ונכלל בו גם פירוט תפקידיו[51]: ניהול מכלול שירותי

51 מעודכן לתאריך 8.8.23.

הטכנולוגיות, המידע והמחשוב של הרשות וניהול כלל המשאבים בהתאם להנחיות המנכ"ל ובהתאם למסגרת הכוללת של תוכנית העבודה השנתית והרב-שנתית, התקציב והנהלים הקיימים ברשות; ניהול ותפעול תחום אבטחת המידע והסייבר ולתחזוקתו וליישום בפועל את מדיניות אבטחת המידע, לרבות הגנה מפני התקפות סייבר ודליפת מידע ואבטחת תשתיות מידע קריטיות; לנהל ולתפעל את הבקרה והאיכות של ספקי מיקור החוץ הפועלים בתחומי האחריות הכלולים בתפקיד; לגבש את נוהלי העבודה ולהסדיר את תהליכי העבודה בנושאים המקצועיים שבתחומי אחריות הכלולים בתפקיד.

בלוח להלן יוצג מידע על איוש תפקיד המנמ"ר ברשויות המקומיות שנבדקו והיקף משרתם.

לוח 4: **איוש תפקיד מנמ"ר ברשויות המקומיות שנבדקו, נכון לחודש יולי 2023**

שם הרשות	האם אויש תפקיד מנמ"ר?	היקף משרת מנמ"ר
רשות מקומית א'	✓	100%
רשות מקומית ב'	✗	-
רשות מקומית ג'	✓	100%
רשות מקומית ד'	✓	ספק חיצוני בהיקף של 100% משרה.
רשות מקומית ה'	✓	100%
רשות מקומית ו'	✓	ספק חיצוני - עד כ-20 שעות בחודש.

על פי נתוני הרשויות המקומיות שנבדקו, בעיבוד משרד מבקר המדינה.

על פי אוגדן התפקידים של משרד הפנים, אחד התפקידים ברשות מקומית הוא של מנמ"ר. נמצא כי בכל הרשויות המקומיות שנבדקו, למעט רשות מקומית ב', אויש תפקיד המנמ"ר.

אי-מינוי מנמ"ר עלול לגרום לפגיעה בניהול מכלול שירותי הטכנולוגיות, המידע והמחשוב וליישום חלקי או יישום לקוי של מגוון המשימות שהוגדרו במסגרת תפקיד זה באוגדן התפקידים שקבע משרד הפנים.

מומלץ כי רשות מקומית ב' תפעל לאייש את תפקיד מנמ"ר הרשות המקומית.

תוכנית עבודה להתמודדות עם אירועי סייבר

בתורת ההגנה בסייבר נקבע, בין היתר, כי הארגון אחראי להכנת תוכנית עבודה רב-שנתית לעניין התמודדותו עם אירועי סייבר. במסגרת תוכנית העבודה נדרש כל ארגון למפות את הסיכונים הרלוונטיים לו, לגבש מענה הגנתי ובהתאם לכך להכין וליישם תוכנית להפחתת הסיכונים בתחום זה. לפי תורת ההגנה, על מנת לגבש תוכנית עבודה לשיפור ההיערכות לעניין ההגנה מפני אירועי סייבר, על הארגון להגדיר תחילה על מה הוא נדרש להגן, מהי רמת ההגנה הנדרשת בו, ובאילו תחומים עליו להשתפר כדי להגיע לרמה זו[52].

תוכניות עבודה המקושרות לתקציב מאפשרות ניהול שוטף ויעיל יותר של משימות בהתאם לתקציב; מידת שליטה רבה יותר על ההוצאות וההכנסות של הרשות בכל רמות הניהול; יצירת תשתית לקבלת החלטות על בסיס נתונים מפורטים; תכנון תהליכים בתחום משאבי האנוש והמחשוב בהתאם לתקציב; הגברת יכולת ההנהלה לתעדף את פעולותיה בכל אחד מהאגפים על סמך החלטות מבוססות נתונים[53].

בלוח שלהלן יצוין אם ברשויות המקומיות שנבדקו יש תוכנית עבודה להתמודדות עם אירועי סייבר והאם הנושאים שבה מקושרים לתקציב.

---

52 מבקר המדינה, **דוחות על הביקורת בשלטון המקומי** (2022), "ניהול מערכות מידע ברשויות המקומיות", עמ' 1270.

53 מבקר המדינה, **דוחות על הביקורת בשלטון המקומי** (2022), "ניהול התקציב ברשויות המקומיות", עמ' 772. מתוך אגף בכיר תכנון ופיתוח ההון האנושי ברשויות המקומיות, משרד הפנים ומפעם, מדריך התכנון ברשויות המקומיות, (ינואר 2020), עמ' 31 ו-37.

לוח 5: **קיומה או היעדרה של תוכנית עבודה להתמודדות עם אירועי סייבר ברשויות שנבדקו והאם היא מקושרת תקציב**

שם הרשות	האם יש בידי הרשות תוכנית עבודה שנתית או רב-שנתית	האם תוכנית העבודה מקושרת תקציב
רשות מקומית א'	✓	×
רשות מקומית ב'	×	-
רשות מקומית ג'	×	-
רשות מקומית ד'	✓	✓
רשות מקומית ה'	×	-
רשות מקומית ו'	✓	×

על פי נתוני הרשויות המקומיות שנבדקו, בעיבוד משרד מבקר המדינה.

על אף שבתורת ההגנה בסייבר של מערך הסייבר הלאומי צוין הצורך בהכנת תוכנית עבודה להתמודדות עם אירועי סייבר, נמצא כי לרשויות מקומיות ב', ג' ו-ה' אין תוכנית עבודה שנתית להתמודדות עם אירועי סייבר.

הועלה כי לרשויות מקומיות א' ו-ו' יש תוכנית עבודה כאמור. על אף היתרונות שבתוכנית עבודה מקושרת תקציב, עלה כי תוכניות העבודה של רשויות אלה אינן מקושרות תקציב.

אם אין לרשות מקומית תוכנית עבודה להתמודדות עם אירועי סייבר, הכוללת בין היתר את מיפוי הסיכונים הרלוונטיים ברשות ואת המענה ההגנתי הנדרש בעניינם, הרי שבהתרחש אירועי סייבר עלולה להיפגע יכולתה של הרשות להתמודד איתם. תוכנית מקושרת תקציב תבטיח את המקור התקציבי להתמודדות עם הסיכונים.

מומלץ כי רשויות מקומיות א', ב', ג', ה' ו-ו' יכינו תוכנית עבודה שנתית מקושרת תקציב להתמודדות עם אירועי סייבר.

רשות מקומית א' מסרה בתשובתה כי הכינה תוכנית עבודה לשנת 2024, וכי היא מקושרת תקציב.

רשות מקומית ג' מסרה בתשובתה כי היא בתהליך התקשרות עם ממונה אבטחת מידע חיצוני. כחלק מתחומי האחריות של הממונה, תגובש תוכנית להתמודדות עם אירועי סייבר ברבעון הרביעי של שנת 2024.

רשות מקומית ה' מסרה בתשובתה כי למרות שאין עדיין תכנית עבודה כתובה בנושא ניהול אבטחת המידע (כשייקלט מנהל אבטחת מידע חדש, הוא יכין תוכנית עבודה), תחום אבטחת המידע מנוהל ע"י אחראי מערכות המידע ברשות (הגם כאמור שהדבר טעון תיקון), מרמת הרשת ועד לרמת עמדת משתמש הקצה.

רשות מקומית ו' מסרה בתשובתה למשרד מבקר המדינה מאפריל 2024 כי המלצת משרד מבקר המדינה מקובלת עליה, וכי היא תפעל ליישמה.

משרד מבקר המדינה מציין את רשות מקומית ד' על שהכינה תוכנית עבודה שנתית מקושרת תקציב.

<u>תקציבים ייעודיים לאבטחת מידע</u>

בהחלטת ממשלה 2443 בנושא הקצאת תקציב ייעודי להגנת הסייבר במסגרת התקציב הקיים של משרדי הממשלה נקבע כדלקמן: "א. המנכ"לים של משרדי הממשלה ומנהלי יחידות הסמך, במסגרת סמכותם ואחריותם הקיימת, יסדירו את מבנה התקציב השנתי של משרדם כך שלכל הפחות 8% מתקציב תחום טכנולוגיית המידע יופנה להגנת הסייבר. ב. מנכ"ל משרד ממשלתי או מנהל יחידת הסמך, לפי העניין, יוכל בנסיבות מיוחדות לאשר הפחתה מהאמור בהחלטה מפורטת ומנומקת שתדווח לוועדת ההיגוי הממשלתית כמפורט בנספח ח' להחלטה זו, ובלבד שלפחות 6%

מתקציב תחום טכנולוגיית המידע יופנה להגנת הסייבר"[54]. יצוין כי החלטה זו אינה חלה על הרשויות המקומיות, וכי לא נקבעה החלטה דומה בנוגע לתקציבי הרשויות המקומיות.

בלוח להלן מובאים נתונים בדבר התקציב הייעודי לאבטחת המידע ברשויות המקומיות שנבדקו ובדבר שיעורו מתוך התקציב הכולל למערכות המידע ברשות.

לוח 6: **הרשויות הנבדקות שיש ברשותן תקציב ייעודי לאבטחת מערכות המידע ושיעורו מכלל התקציב למערכות מידע ברשות, 2022 (בש"ח)**

שם הרשות	התקציב הייעודי של הרשויות לאבטחת מערכות מידע לשנת 2022	שיעור תקציב אבטחת המידע מכלל תקציב מערכות המידע
רשות מקומית א'	אין לרשות המקומית סעיף תקציב ייעודי לנושא זה	-
רשות מקומית ב'	אין לרשות המקומית סעיף תקציב ייעודי לנושא זה	-
רשות מקומית ג'	1.55 מיליון ש"ח מתוך תקציב מערכות מידע בסך כ-49.34 מיליון ש"ח	כ-3.1%
רשות מקומית ד'	339,871 ש"ח מתוך תקציב מערכות מידע בסך כ-2.58 מיליון ש"ח	כ-13.2%
רשות מקומית ה'	אין לרשות המקומית סעיף תקציב ייעודי לנושא זה	-
רשות מקומית ו'	אין לרשות המקומית סעיף תקציב ייעודי לנושא זה	-

על פי נתוני הרשויות המקומיות שנבדקו, בעיבוד משרד מבקר המדינה.

על פי הלוח לעיל עולה כי לרשויות מקומיות א', ב', ה' ו-ו' אין תקציב ייעודי לאבטחת מידע. עוד עולה כי רשות מקומית ג' קבעה תקציב אבטחת מידע ששיעורו כ-3.1% בלבד מתקציב מערכות המידע שלה, וכי רשות מקומית ד' קבעה תקציב אבטחת מידע ששיעורו כ-13.2% מתקציב מערכות המידע.

אף שהחלטת הממשלה 2443 אינה חלה על השלטון המקומי, מומלץ לרשויות מקומיות א', ב', ה' ו-ו' לייחד סעיף תקציב ייעודי לנושא אבטחת מידע. כמו כן, מומלץ לרשות מקומית ג' לבחון אם תקציב אבטחת המידע שלה, ששיעורו כ-3.1% מתוך סך הוצאותיה על טכנולוגיות המידע, עונה על צרכיה; זאת נוכח החלטת הממשלה ולפיה השיעור הנדרש של תקציב זה יהיה 8% לפחות.

רשות מקומית א' מסרה בתשובתה כי לא היה סעיף תקציבי ייעודי אך ורק לאבטחת מידע. לתקציב של שנת העבודה 2024 אשר יאושר ביולי מבוקש סעיף תקציבי ייעודי אך ורק לאבטחת מידע.

רשות מקומית ג' מסרה בתשובתה מיוני 2024 כי קיים הצורך להגדיל את התקציב עד ללפחות 8% מסך תקציב התקשוב העירוני והגדלה זו תוטמע בתוכנית העבודה ובתקציב בשנת תקציב 2025.

רשות מקומית ה' מסרה בתשובתה כי לנוכח היות הרשות מצויה בתכנית הבראה, התקציב השוטף העומד לרשותה למטרה זו מצומצם ביותר ולא מאפשר פיתוח אלא רק חידוש רשיונות שנתיים. הרשות תנסה לאתר מקורות תקציביים ובמידה הדבר יעלה בידה תביאו לאישור משרד הפנים.

רשות מקומית ו' מסרה בתשובתה כי המלצת משרד מבקר המדינה מקובלת עליה, וכי היא תפעל ליישמה.

לאור החלטת הממשלה בה נקבע השיעור המינימלי הנדרש לתקציב אבטחת מידע במשרדי ממשלה, מומלץ כי משרד הפנים ייתן דעתו לצורך בקביעת שיעור התקציב המתאים לרשויות

[54] שם, סעיף 4.

המקומיות לעניין אבטחת מידע בהתחשב במאפיינים הייחודיים להן. בנוסף, מומלץ למשרד הפנים להנחות את הרשויות המקומיות כי במסגרת הכנת תקציבן יבחנו את שיעור התקציב הייעודי הרצוי לאבטחת מידע שבאפשרותו לתת מענה מספק לסיכוני סייבר אתם הן מתמודדות.

הסמכה לפי תקן ISO27001

1. מערכת לניהול אבטחת מידע נועדה לשמור על החיסיון, השלמות והזמינות של המידע באמצעות יישום של תהליך ניהול סיכונים, והיא מעניקה למחזיקי העניין את הביטחון שהסיכונים מנוהלים כראוי. חשוב כי המערכת לניהול אבטחת מידע תשולב בתהליכי הארגון ובמבנה הניהול הכללי שלו ותהיה חלק מהם, ושאבטחת המידע תובא בחשבון בעת התכנון של תהליכים, של מערכות מידע ושל בקרות. מצופה כי יישום מערכת לניהול אבטחת מידע יהיה לפי קנה מידה שיותאם לצורכי הארגון.

   ISO27001 הוא תקן בין-לאומי לניהול אבטחת מידע. התקן פורסם במקור על ידי ארגון התקינה הבין-לאומי (ISO) והנציבות הבין-לאומית לאלקטרו-טכניקה (IEC)[55] בשנת 2005 ומאז עודכן מפעם לפעם. בתקן מפורטות דרישות להקמה, ליישום, לתחזוקה ולשיפור מתמיד של מערכת לניהול אבטחת מידע.

2. אגף איכות והסמכה שבמכון התקנים הישראלי הוא גוף ההתעדה שבידיו הסמכה (בדרך כלל מארגוני הסמכה מדינתיים או מארגונים בין-לאומיים) לבצע בחינה, ביקורת, בדיקות, מדידות וכיולים נאותים בהתאם לתקנים, למפרטים או למסמכי ייחוס אחרים. גוף ההתעדה מוסמך ורשאי להנפיק ללקוחותיו תעודה (תעודת איכות), המעידה שהארגון פועל לפי התקנים החלים עליו[56] (להלן - הסמכה), לרבות הסמכה לפי תקן ISO27001.

3. הרשויות המקומיות אינן מחויבות לפעול בהתאם להנחיות תקן ISO27001. עם זאת, ההחלטה אם לאמץ מערכת לניהול אבטחת מידע היא החלטה אסטרטגית עבור ארגון. ההקמה והיישום של מערכת לניהול אבטחת מידע בארגון מושפעים מצרכיו, ממטרותיו, מדרישות האבטחה שלו, מהתהליכים הארגוניים המתבצעים בו, מגודלו וממבנהו. כל הגורמים האלה צפויים להשתנות במשך הזמן.

   נוסף על כך, גורמים בתוך הארגון ומחוצה לו יכולים להתבסס על תקן זה כדי להעריך אם הארגון יכול לעמוד בדרישות אבטחת המידע שלו.

על אף שאין חובה ליישם תקן ISO27001, הוא יכול לסייע לרשויות המקומיות להעריך את עמידתן בדרישות אבטחת המידע שלו, עולה כי הרשויות המקומיות שנבדקו, רשויות מקומיות א', ב', ג', ד', ה', ו-ו', אינן מוסמכות לפי תקן ISO27001.

רשות מקומית ה' מסרה בתשובתה כי, לרשות לא ידוע על דרישה מחייבת של רגולטור כלשהו לעמוד בתקן זה; במידה והייתה דרישה מחייבת שכזו, הרשות הייתה פועלת לעמוד בו. עוד מסרה הרשות כי עמידה בתקן עשויה להצריך שינויים בתקציב ובכוח אדם ולכן פעולה וולונטרית בנושא זה בשעה שהרשות מצויה בתכנית הבראה כאמור, בעייתית ביותר עבורה.

רשות מקומית ו' מסרה בתשובתה כי היא אינה מחויבת לפעול בהתאם להנחיות תקן ISO27001. לטענת הרשות מרבית ההנחיות המופיעות בתקן זה מופיעות בתקנות הגנת הפרטיות שלאורן המועצה פועלת. העלויות והמשאבים הנדרשים להסמכה לפי תקן זה אינם מצדיקים זאת לנוכח הגודל והמבנה של מערכות המידע הקיימות נכון להיום במועצה. אם דרישות האבטחה או הצרכים של המועצה ישתנו, הרשות תבחן את יישום תקן זה בהתאם לכך.

---

55 International Electrotechnical Commission

56 מבקר המדינה, **דוח שנתי 67א** (2016), "מכון התקנים", עמ' 876.

על אף שאין חובה רגולטורית ועל אף הצורך במשאבים הנדרשים ליישום התקן, מומלץ כי הרשויות המקומיות יפעלו לקבלת הסמכה לפי תקן ISO27001, וזאת בשל חשיבות נושא אבטחת המידע ברשות המקומית.

רשות מקומית א' מסרה בתשובתה כי כהכנה לתוכנית העבודה שלה לשנת 2025 היא תשקול לבצע תהליך שיאפשר לה לעמוד בתקן ISO27001.

רשות מקומית ג' מסרה בתשובתה כי במחצית השנייה של שנת 2024 היא תתחיל את תהליך התכנון לעמידה בתקן. על פי תוכניות העבודה התהליך יושלם בשנת 2025.

רשות מקומית ד' מסרה בתשובתה כי כאמור בדוח הביקורת, הרשויות המקומיות אינן מחויבות לפעול בהתאם להנחיות ISO27001. עם זאת, לאור חשיבות הנושא, גם ברמה האסטרטגית, הרשות תבצע בדיקה מקצועית של הסוגיות לצורך קבלת החלטות.

הסמכת ספקי השירות של מערכות הגבייה ברשויות המקומיות הנבדקות בתקן ISO27001

בלוח שלהלן מצוין אילו מספקי השירות של מערכת הגבייה של הרשויות המקומיות שנבדקו הוסמכו לפי תקן ISO27001 ואם במכרז או בהסכם ההתקשרות[57] בין הרשות המקומית לבין ספק השירות של מערכת הגבייה נכללה דרישה להסמכה.

לוח 7: **הסמכת ספקי השירות של מערכת הגבייה לפי תקן ISO27001 ודרישת הרשויות הנבדקות להסמכת הספק**

שם ספק השירות של מערכת הגבייה	שם הרשות	האם במכרז או בהסכם יש דרישה לעמידה בתקן ISO27001	האם הספק הוסמך לפי תקן ISO27001
ספק שירות א'	רשות מקומית א'	✗	✓
	רשות מקומית ג'	✓	
	רשות מקומית ה'	✓	
ספק שירות ב'	רשות מקומית ב'	✗	✓
ספק שירות ג'	רשות מקומית ו'	✓	✓

הוכן בידי משרד מבקר המדינה.

נמצא כי במכרז של רשויות מקומיות ג', ה', ו-ו' נכללה דרישה שהספק יהיה מוסמך ISO27001. עם זאת נמצא כי, בהסכמים של רשויות מקומיות א' ו-ב' לא נכללה דרישה כי הספק יהיה בעל הסמכה לפי תקן ISO27001.

עוד עולה כי לספקי השירות של מערכת הגבייה של הרשויות המקומיות שנבדקו, המקבלות שירותים מספקים, יש תקן ISO27001.

אם בהסכמיהן של הרשויות המקומיות עם ספקי שירות של מערכות גבייה ובמכרזים להעסקתם תיכלל הדרישה שהספקים יוסמכו לפי תקן ISO27001, הדבר עשוי לסייע לרשויות המקומיות בכך שגורם חיצוני מבצע בקרה על תהליכי העבודה שמבצעים ספקי השירות ועל תקינותם.

מומלץ כי רשויות מקומיות א' ו-ב' יכללו במכרזים ובהסכמים בינן ובין ספקי שירות של מערכות גבייה את הדרישה שהספקים יוסמכו לפי תקן ISO27001.

---

57 יצוין כי בכל חוזי ההתקשרות בין הרשויות המקומיות שנבדקו לבין ספקי השירות של מערכת הגבייה לניהול ולתחזוקה של מערכות המידע נכלל סעיף ולפיו המכרז, מסמכיו ונספחיו הם חלק בלתי נפרד מן החוזה החתום.

רשות מקומית א' מסרה בתשובתה כי היא תוודא שבמכרזיה תידרש מספקי השירות השונים עמידה בתקן ISO27001.

התאוששות מאסון

המשכיות עסקית (BCP - Business Continuity Program) היא דוקטרינת ניהול של הפעולות שארגון נדרש לבצע כדי להבטיח שהפונקציות העסקיות החיוניות שלו יהיו זמינות בעת חירום ללקוחות, לספקים, לגופי האסדרה ולגופים אחרים בעלי עניין בארגון. תוכנית המשכיות עסקית אינה נוגעת לפעולות ההצלה הראשוניות המתבצעות בהתרחש אירוע חירום, אלא בהתכוננות ובהתארגנות להשבת יכולת התפקוד של הארגון ולהתאוששות מהירה לאחר האירוע[58].

על פי תורת ההגנה בסייבר של מערך הסייבר הלאומי, באירועי סייבר רבים התוקפים אינם מתחשבים בגודל הארגון או בנזק הפוטנציאלי לארגון. גם עסקים קטנים רבים חוו מתקפות כופרה[59], דֶּלֶף של מאגר לקוחות, גניבת מידע של לקוחות ועוד. כדי להפחית את הסיכוי להיפגע באירועים מסוג זה, וכדי להגביר את יכולת השרידות וההמשכיות של העסק בהתרחש תקיפה, מומלץ לכל ארגון לאמץ דרישות הגנה רוחביות. כמו כן נקבע בתורת ההגנה בסייבר שיש לוודא כי יש לארגון יכולת התאוששות בעקבות נפילת אתר, מחיקת מידע או נעילת קבצים, וכי בפרט יש לוודא שיש לארגון גיבוי אפקטיבי. עוד צוין כי יש לבצע שחזור יזום בתדירות קבועה ולהגדיר את תדירות הגיבוי ואת סוג הגיבוי הנדרש[60].

<u>הנחיות לגיבוי נתוני מערכת גבייה ולביצוע תרגולים לשחזורם</u>

1. בתקנות הגנת הפרטיות נקבע כי אם חלה על מאגר מידע רמת האבטחה הבינונית או הגבוהה, בעל המאגר יגבה את הנתונים שנשמרו באופן שיבטיח שיהיה ניתן, בכל עת, לשחזר את הנתונים האמורים למצבם המקורי.

2. בתקנות הגנת הפרטיות נקבע כי חובות בעל מאגר (דהיינו הרשות המקומית) לגיבוי הנתונים שנשמרו, לרבות החובה לתעד ביצוע פעולות, חלות על מנהל מאגר ועל המחזיק בו.

   אי לכך, אם מאגר הנתונים של הרשות המקומית נמצא בידי מחזיק חיצוני, חלה עליו החובה לבצע גיבויים ושחזורים ולתעד את פעולותיו. מאחר שמאגר המידע שבבעלותן של רשויות המקומיות מוחזק ומנוהל בידי ספקי השירות, עליהן לוודא כי ספק השירות מבצע בפועל גיבוי נאות של המידע לרבות שחזור מידע ותיעוד של פעולותיו. על הרשויות המקומיות לכלול בהסכמי ההתקשרות שלהן עם ספקי השירות שלהן דרישה כי הם ידווחו להן על פעולותיהם האמורות.

3. במסמך שילוב עקרונות הגנת הסייבר בתהליכי גיבוי ושחזור[61] של מערך הסייבר הלאומי, נקבע כי ארגונים אשר משתמשים בשיטות גיבוי מסורתיות, דוגמת אחסון מידע בקלטות, נחשפים לאתגרים דוגמת גיבוי נפחי מידע הגדלים מיום ליום והצורך לגבות מידע באתרים מרוחקים ובשירותי ענן, וזאת לצד דרישות עסקיות לביצוע תהליכי התאוששות בתוך זמן קצר. נספח 5 של המסמך עוסק במודלים מקובלים לבחינת זמינות אחסון הגיבוי. אחד המודלים הוא שמירת המידע מחוץ לאתר (גיבוי באתר מרוחק), שבמסגרתו מדיית האחסון מאוחסנת פיזית מחוץ למתחם שבו מאוחסן נכס הסייבר.

---

58 מבקר המדינה, **דוח מבקר המדינה בנושא סייבר ומערכות מידע - דצמבר 2022**, "המשכיות עסקית והתאוששות מאסון", עמ' 29.

59 כופרה היא תוכנה מזיקה הנועלת את המחשב ומונעת מהמשתמשים גישה לקבצים או לתוכנות, בדרך כלל באמצעות הצפנת מידע, ודורשות תשלום כופר בתמורה להשבת הגישה.

60 תורת ההגנה בסייבר, עמ' 22 - 23.

61 מסמך שילוב עקרונות הגנת הסייבר בתהליכי גיבוי ושחזור משנת 2021, עמ' 3.

4. בבקרות של תורת ההגנה בסייבר[62] נאמר שהארגון יוודא כי הוא ביצע שחזור תקופתי של המידע שגובה, וזאת לשם בחינת שלמותו ומהימנותו של המידע (Integrity).

נוהל עבודה בנושא גיבויים ושחזורים

בתקנות הגנת הפרטיות נקבע לגבי מאגר מידע שחלה עליו רמת האבטחה הבינונית או הגבוהה כי בעליו של מאגר זה יקבע נהלים לביצוע גיבוי באופן תקופתי שגרתי (להלן - נוהל גיבוי). כמו כן, על בעל המאגר לקבוע נהלים בנוגע לשחזורים שיבוצעו באישור מנהל המאגר. בלוח להלן יוצג מידע על נוהלי גיבויים ושחזורים ברשויות המקומיות שנבדקו.

לוח 8: **קיומם של נוהל גיבויים ושחזורים כנדרש בתקנות הגנת הפרטיות**

שם הרשות	האם קיים נוהל גיבויים	האם נוהל הגיבוי עסק בביצוע גיבויים ושחזורים
רשות מקומית א'*	×	-
רשות מקומית ב'	×	-
רשות מקומית ג'	×	-
רשות מקומית ד'	✓	✓ (נוהל הגיבויים עסק בכך)
רשות מקומית ה'	×	-
רשות מקומית ו'	✓	✓ (נוהל הגיבויים עסק בכך)

הוכן בידי משרד מבקר המדינה.

* משרד מבקר המדינה קיבל **מרשות מקומית א'** רק רשימה של הנהלים שבהם צוין כי יש ברשותה נוהל בנושא גיבויים, אך הוא לא קיבל מסמך המתעד את הנוהל הכתוב.

על אף שבתקנות הגנת הפרטיות נקבע כי בעליו של מאגר מידע יקבע נהלים לביצוע גיבוי, נמצא כי ברשויות מקומיות א', ב', ג' ו-ה' לא נמצא נוהל עבודה בנושא גיבויים ושחזורים. רשויות מקומיות ד' ו-ו', הכינו נוהל גיבויים ושחזורים.

קיומם של נוהלי עבודה סדורים בנושא גיבויים ושחזורים, המסדירים בין היתר את התדירות של ביצוע גיבויים ושחזורים, שמירה של הגיבויים וכו' וניהול תקין של הליכים אלה עשויים לסייע לרשות להתאושש במהירות מאירוע סייבר.

על רשויות מקומיות א', ב', ג' ו-ה' להתקין נהלים בנושא גיבויים ושחזורים בהתאם לתקנות הגנת הפרטיות.

רשות מקומית א' מסרה בתשובתה כי תפעל להקמתו ולהחלתו של נוהל עבודה סדור בנושא גיבויים ושחזורים, בהתאם לתקנות הגנת הפרטיות עד תחילת יולי 2024.

גיבוי נתוני מערכת גבייה

בבדיקה של גיבוי נתונים[63] של מערכות הגבייה של **רשויות מקומיות א', ב', ג' ו-ה'** הועלה כי ספקי השירות של מערכת הגבייה ביצעו בשנת 2023 גיבויים יומיים של נתוני מערכת הגבייה, וכי הנתונים שגובו נשמרים באתר מרוחק פיזית מהשרת שבו מנוהלים הנתונים של מערכת הגבייה. ספק השירות של **רשות מקומית ו'** ביצע גיבויים בשנת 2024, והנתונים שגובו נשמרו באתר מרוחק פיזית מהשרת שבו מנוהלים הנתונים של מערכת הגבייה.

רשות מקומית ד' מנהלת באופן עצמאי את מערכת הגבייה שלה, ונתוני מאגר המידע נשמרים בשרתים הנמצאים בחדר השרתים ברשות המקומית. הועלה כי הרשות המקומית גיבתה את נתוני

62 בקרה 12.4 בבקרות תורת ההגנה בסייבר 2.0 גרסה 1.3.

63 ביצוע גיבויים יומיים וגיבוי נתוני מאגר הגבייה לאתר מרוחק.

מערכת הגבייה, וכי הנתונים שגובו שמורים באתר מרוחק פיזית מהשרת שבו מנוהלים הנתונים של מערכת הגבייה.

משרד מבקר המדינה מציין את העובדה כי בוצעו גיבויים של נתוני מערכות הגבייה של רשויות מקומיות א', ב', ג', ד', ה' ו-ו'.

ביצוע תרגולי שחזור של נתוני מערכת גבייה

בבקרות של תורת ההגנה בסייבר[64] צוין שהארגון יוודא כי הוא ביצע שחזור תקופתי של המידע שגובה, וזאת לשם בחינת שלמותו ומהימנותו של המידע (Integrity).

בנספח 7 במסמך שילוב עקרונות הגנת הסייבר בתהליכי גיבוי ושחזור של מערך הסייבר הלאומי[65] צוין כי מומלץ לבצע שחזור מידע אחת לשנה.

צוות הביקורת בדק אם ספקי השירות של מערכות הגבייה ביצעו תרגול שחזור תקופתי לנתונים ממערכת הגבייה בעבור הרשויות המקומיות, ואם **רשות מקומית ד'**, המנהלת באופן עצמאי את מערכת הגבייה, ביצעה תרגול כאמור, ולהלן יפורטו ממצאי הבדיקה:

לוח 9: **מועדי הביצוע של תרגול תקופתי לשחזור מידע על ידי ספקי השירות בעבור הרשויות המקומיות הנבדקות ועל ידי רשות מקומית ו', נכון ליולי 2023**

שם הרשות	האם בוצע תרגול תקופתי לשחזור מידע (המועד האחרון)
רשות מקומית א'	✗
רשות מקומית ב'	✓ בוצע ביוני 2023
רשות מקומית ג'	✓ בוצע באוגוסט 2022
רשות מקומית ד'	✓ בוצע באפריל 2022
רשות מקומית ה'	✗
רשות מקומית ו'	✓ בוצע בינואר 2024

על פי נתוני הרשויות המקומיות שנבדקו, בעיבוד משרד מבקר המדינה.

בבקרות של תורת ההגנה בסייבר צוין כי הארגון יוודא כי הוא ביצע שחזור תקופתי. נמצא כי ברשויות מקומיות ב', ג', ד' ו-ו' בוצע תרגול תקופתי של שחזור מידע ממערכת הגבייה. עם זאת, נמצא כי ברשויות מקומיות א' ו-ה' לא בוצע תרגול של שחזור נתונים ממערכת הגבייה. עוד עולה כי רשות מקומית ד' ביצעה תרגול של שחזור נתונים ממערכת הגבייה באפריל 2022, כלומר כשנה ושלושה חודשים לפני מועד ביצוע הביקורת.

חשוב לבצע תרגולי שחזור המאפשרים לוודא כי תוצרי הגיבוי תקינים, וכי יש לרשות יכולת התאוששות בהתרחש אסון.

מומלץ כי רשויות מקומיות א' ו-ה' יוודאו כי ספק השירות של מערכת הגבייה יבצע תרגולי שחזור לפחות אחת לשנה בהתאם להמלצות של מערך הסייבר הלאומי ויקבלו דיווח על כך. כמו כן, מומלץ כי רשות מקומית ד' תבצע תרגול של שחזור נתוני מערכת הגבייה לפחות אחת לשנה.

רשות מקומית א' מסרה בתשובתה כי יבוצע תרגול שחזור מול ספקית מערכת הגבייה במהלך הרבעון השני של שנת 2024, וכי הדבר ידווח למערך הסייבר הלאומי.

64 בקרה 12.4 בבקרות תורת ההגנה בסייבר 2.0, גרסה 1.3.

65 מסמך שילוב עקרונות הגנת הסייבר בתהליכי גיבוי ושחזור (2021), עמ' 46.

רשות מקומית ד' מסרה בתשובתה כי כחלק משגרת קיום הבקרות תיבחן ההמלצה לשחזור נתוני גבייה.

רשות מקומית ה' מסרה בתשובתה כי הרשות תפנה לספק השירות של מערכת הגבייה ותוודא כי הוא מבצע תרגול שחזור לפחות אחת לשנה ותבקש לקבל דיווח על כך.

דיווח של ספקי השירות לרשויות המקומיות בנושא גיבויים ותרגולי שחזורים

בלוח להלן יובא מידע על חובת הדיווח של ספקי השירות של מערכת הגבייה לרשויות המקומיות בהסכמים איתם בדבר ביצוע גיבויים ושחזורים, וכן מידע אם הרשויות המקומיות קיבלו מספקי השירות של מערכת הגבייה דיווחים כאמור.

לוח 10: **דיווח של ספק השירות של מערכת הגבייה לרשויות המקומיות הנבדקות בדבר תוצאות של גיבויים ותרגולי שחזורים**

שם הרשות המקומית	האם בהסכם נכללה חובת הספק לדווח לרשות המקומית על ביצוע גיבויים	האם בהסכם נכללה חובת הספק לדווח לרשות המקומית על ביצוע תרגולי שחזורים	האם התקבלו מספקי השירות של מערכת הגבייה דיווחים על ביצוע גיבויים ותרגולי שחזורים
רשות מקומית א'	X	X	X
רשות מקומית ב'	X	X	X
רשות מקומית ג'	V	V	X
רשות מקומית ה'	X	V	X
רשות מקומית ו'	X	X	X

על פי נתוני הרשויות המקומיות שנבדקו, בעיבוד משרד מבקר המדינה.

נמצא כי רשות מקומית ג' כללה בהסכם ההתקשרות עם ספק השירות של מערכת הגבייה את חובת הדיווח על ביצוע גיבויים. רשויות מקומיות א', ב', ה' ו-ו' לא כללו חובה זו.

עוד נמצא כי רשויות מקומיות ג' ו-ה' כללו בהסכם ההתקשרות את חובת הדיווח על ביצוע תרגולי שחזורים. רשויות מקומיות א', ב' ו-ו' לא כללו חובה זו.

בנוסף, נמצא כי רשויות מקומיות א', ב', ג', ה' ו-ו' לא קיבלו דיווחים על ביצוע גיבויים ותרגולי שחזורים מאת ספקי השירות של מערכת הגבייה, אף שבחלק מהרשויות, רשויות מקומיות ג' ו-ה', ספק השירות של מערכת הגבייה מחויב לדווח לעיריות בנושאים אלה.

בהיעדר דיווחים של ספקי השירות של מערכת הגבייה על ביצוע גיבויים ותרגולי שחזורים, יש סיכון שהרשות המקומית לא תוכל לבצע פיקוח ובקרה בדבר תקינות התהליכים שמבצעים ספקי השירות של מערכת הגבייה.

מומלץ כי רשויות מקומיות א', ב', ג', ה' ו-ו' יפעלו לקבלת דיווחים תקופתיים על ביצוע גיבויים ותרגולי שחזורים. עוד מומלץ לציין במפורש בהסכמי ההתקשרות של הרשויות המקומיות עם ספקי השירות של מערכת הגבייה כי הספקים מחויבים לדווח על ביצוע גיבויים ותרגולי שחזורים.

רשות מקומית א' מסרה בתשובתה כי תפעל לבצע תרגולים ובדיקות של הגיבויים של ספק השירות של מערכת הגבייה בכל חציון.

רשות מקומית ג' מסרה בתשובתה כי התקבל מספק השירות של מערכת הגבייה מסמך המתעד את הנהלים, וכי ספק השירות של מערכת הגבייה מסר לה שבוצעו פעולות שחזור על פי הנהלים ושהרשות אמורה לקבל אסמכתאות לכך.

רשות מקומית ה' מסרה בתשובתה כי ספק השירות של מערכת הגביה מקיים גיבוי של הנתונים. הרשות תבקש מהספק לדווח על כך ועל תרגילי שחזורים שהוא מבצע. הספק זכה במכרז שהרשות פרסמה בשנת 2018, בטרם נכנסו תקנות הגנת הפרטיות (אבטחת מידע) לתוקפן ולכן אין ביטוי לחובות אלו בהסכם ההתקשרות עימו. בכל מקרה, הרשות מתכוונת לפרסם בשנת 2025 מכרז חדש בו יידרש הזוכה לקיים גיבויים ותרגולי שחזורים.

רשות מקומית ו' מסרה בתשובתה כי המלצת משרד מבקר המדינה מקובלת עליה, וכי היא תפעל ליישמה.

אבטחה פיזית של מערכות גבייה

בחוק הגנת הפרטיות מוגדרת אבטחת מידע כלהלן: "הגנה על שלמות המידע, או הגנה על המידע מפני חשיפה, שימוש או העתקה, והכל ללא רשות כדין".

בתקנות הגנת הפרטיות נקבע כי נדרש להבטיח כי תשתיות ומערכות החומרה, וכן רכיבי התקשורת ואבטחת המידע, יישמרו במקום מוגן המונע חדירה וכניסה אליו בלא הרשאה. עוד נקבע בתקנות כי בעליו של מאגר שחלה עליו רמת אבטחה בינונית או גבוהה חייב לנקוט אמצעים הן לצורכי בקרה על כניסה לאתרים שבהם נמצאות מערכות אלו ועל יציאה מאתרים אלה והן לצורכי תיעוד של כניסה ויציאה כאמור.

בבקרות של תורת ההגנה בסייבר[66] צוין כי יש לבצע שמירה וניטור במתקן שבו נמצא הנכס כדי לוודא כי הטמפרטורה והלחות בו הן ברמות המקובלות.

בבניין שנמצא בו חדר המחשב (להלן - חדר השרתים או חדר המחשב) יש להתקין אמצעי הגנה אלה: קירות בנויים בלא פתחים[67]. התקן אוסר את אחסנתם של מרכיבים אלה בחדר מחשב: כל פריט שאינו קשור ישירות למערכת המחשב; חומרים דליקים, כגון נייר ומוצריו, תיבות קרטון, כרטיסים ודיו בכמות גדולה מהנדרש לתפעול יומי; מכשירים או ציוד מקולקלים; וחומרים או ציוד דליקים שאפשר להוציאם מהחדר[68].

נוהל אבטחה פיזית של מערכות מידע

בתקנות הגנת הפרטיות נקבע כי בעל מאגר מידע יכלול בנוהל אבטחת מידע את ההוראות בעניין האבטחה הפיזית והסביבתית של אתרי המאגר. נוהל אבטחה פיזית של מערכות מידע נועד להסדיר את השמירה על המידע החל משלב הכניסה לאתר שבו מאוחסן המידע (לדוגמה, באמצעות הנחיות לרישום אורחים) ואת אבטחת חדר השרתים.

נמצא כי לרשויות מקומיות ב' ו-ה' אין כלל נהלים לתחום אבטחת מידע, ובכללם נהלים לאבטחה פיזית. עם זאת, נמצא כי לרשויות המקומיות א', ג', ד' ו-ו' יש נהלים העוסקים בנושא האבטחה הפיזית של אתרי המאגר כנקבע בתקנות הגנת הפרטיות.

היעדר נוהל בנושא אבטחה פיזית של מערכות מידע עלול לגרום לביצוע לקוי של הבקרות או לחוסר מודעות של הגורמים הרלוונטיים ברשות המקומית בדבר האמצעים הדרושים לאבטחה.

---

66 בקרה 9.1 בבקרות תורת ההגנה בסייבר 2.0 גרסה 1.3.

67 תקן ישראלי 1243 "בטיחות אש של מחשבים וציודם ההיקפי". כמו כן ראו, מבקר המדינה, **דוח שנתי 64ג** (2013), "אבטחה פיזית ושרידות של תשתיות אינטרנט ומחשוב עבור משרדי ממשלה", עמ' 1593.

68 שם עמ' 1595.

רשות מקומית ה' מסרה בתשובתה כי ברשות אין נהלים כתובים לאבטחה פיסית, אך כל תחנת עבודה מוגנת. בנוסף, מערכת הגביה עובדת ברשת פנימית בלבד ואין יכולת להתחבר ללא שיוך של כתובת IP לרשת הפנימית. חיבור מרחוק (דרך VPN) ניתן למורשים בלבד עם מנגנון אבטחה כפול.

נהלים כתובים מסייעים להסדיר את תהליכי העבודה הנדרשים ולבצע בקרה אחר יישום הנחיות הנהלת הרשות. על רשויות מקומית ב' ו-ה' להכין נהלים בנושא אבטחת מידע פיזית בהתאם לתקנות הגנת הפרטיות.

אבטחה פיזית של חדר השרתים שבו מותקנת מערכת הגבייה

רשויות מקומית א', ג', ה'

רשויות מקומיות א', ג' ו-ה' מקבלות את שירותי מערכת הגבייה מספק א'. בסיס הנתונים של רשויות אלה נמצא בשרתים במשרדים של הספק.

נמצא כי מאז תחילת ההתקשרות של רשויות מקומיות א', ג' ו-ה' עם ספק השירות של מערכת הגבייה הן לא ביצעו בדיקות אבטחה פיזית במשרדי הספק שבו מאוחסן המידע שלהן על מנת לוודא כי הספק עומד בדרישות האבטחה הפיזית של המידע.

בתחילת יוני 2023 קיים צוות הביקורת סיור בחדר השרתים של ספק א' על מנת לבחון את נאותות אבטחת המידע הפיזית של חדר השרתים בהתאם לדרישות האמורות לעיל. בסיור לא אותרו ליקויי אבטחה פיזית.

על רשויות מקומיות א', ג' ו-ה', כבעליהם של מאגרי המידע שבמערכת הגבייה, להבטיח את העמידה בדרישות האבטחה הפיזית של מאגר המידע גם כאשר זה מנוהל במשרדי הספק, כנקבע בחוק הגנת הפרטיות ובתקנות הגנת הפרטיות, ולשם כך עליהן לבחון את הבקרות הפיזיות אצל ספק השירות של מערכת הגבייה על מנת לוודא כי הוא עומד בדרישות אבטחת המידע.

רשות מקומית א' מסרה בתשובתה כי בדיקת אבטחה פיזית תבוצע כחלק מבדיקה ב"חצר ספקים"[69], במסגרת מבדק חדירה כמחויב בתקנות הגנת הפרטיות, פעם בשנה וחצי.

רשות מקומית ג' מסרה בתשובתה כי יתואם סיור במתקני חוות השרתים של ספק השירות של מערכת הגבייה כדי לבחון אם המתקנים עומדים בדרישות האבטחה הפיזית.

רשות מקומית ה' מסרה בתשובתה כי הרשות תבצע בדיקת אבטחה פיזית במשרדי הספק על מנת לוודא כי הוא עומד בדרישות האבטחה הפיזית ותקבע בנוהל חובת בדיקת אבטחה פיזית במשרדי הספק אחת לתקופה.

רשות מקומית ד'

רשות מקומית ד' מנהלת את מערכת הגבייה באופן עצמאי, ובסיס הנתונים של מערכת הגבייה נמצא בשרתים השוכנים במשרדי הרשות המקומית. בסוף יוני 2023 בדק צוות הביקורת את האבטחה הפיזית של חדר השרתים של הרשות המקומית.

בבדיקה נמצא כי רשות מקומית ד' אינה מבצעת בקרה על הכניסה לאתר שבו נמצאת מערכת המידע ועל היציאה ממנו, ואף אינה מתעדת את הכניסה והיציאה; עוד נמצא כי חדר השרתים של רשות מקומית ד' לא כלל מערכת לניטור טמפרטורה ולהתראה על עלייתה, והדבר עלול לפגוע ביעילות השרתים בחדר ובביצועיהם; קירות חדר השרתים כוללים פתח בניגוד לדרישות - חלון

[69] משרדי ספק השירות של מערכת הגבייה.

הזכוכית שמעל דלת הכניסה מאפשר כניסה לחדר השרתים והוא מועד לחבלה; כמו כן, נמצא כי בחדר השרתים אוחסנו חפצים דליקים[70].

על רשות מקומית ד' לבחון את אבטחת האתר שבו מאוחסנים שרתי מערכת הגבייה שלה ולהפעיל בקרה על הנכנסים והיוצאים, וכמו כן עליה להתקין בחדר השרתים מערכת להתראה על עליית טמפרטורה, לחסום את הפתח בקיר חדר השרתים ולפנות ממנו חומרים דליקים.

רשות מקומית ד' מסרה בתשובתה כי נושא האבטחה הפיזית של מערכות הגבייה נמצא בטיפול, וכי היא תנקוט את הצעדים האלה הנוגעים לאתר שבו נמצאת מערכת הגבייה: תיעוד של כניסה ויציאה, התקנת מנטר טמפרטורה, אטימת חלון הזכוכית מעל הדלת, הוצאת חפצים דליקים.

ניטור של פעולות במערכת הגבייה והבקרה בנושא

בתקנות הגנת הפרטיות נקבע כי במערכות של מאגר מידע אשר חלה עליו רמת האבטחה הבינונית או הגבוהה ינוהל מנגנון תיעוד אוטומטי שיאפשר ביקורת על הגישה למערכות המאגר (בתקנה זו - מנגנון הבקרה), ובכלל זה נתונים אלה: זהות המשתמש, התאריך והשעה של ניסיון הגישה, רכיב המערכת שאליו בוצע ניסיון הגישה, סוג הגישה, היקפה, ואם הגישה אושרה או נדחתה.

עוד נקבע בתקנות הגנת הפרטיות כי בעל מאגר מידע יקבע נוהל בדיקה שגרתי של ממצאי התיעוד של מנגנון הבקרה.

בתקנות הגנת הפרטיות נקבע כי בעל מאגר מידע אחראי לתיעוד כל אירוע המעורר חשש לפגיעה בשלמות המידע, לשימוש בו בלא הרשאה או לחריגה מהרשאה (להלן - אירועי אבטחה); במידת האפשר יבוסס התיעוד האמור על רישום אוטומטי.

בפרק על בקרות בתורת ההגנה בסייבר[71] צוין בין היתר שארגון יפעיל מנגנון המייצר רשומות בקרה בנושא אירועים שהתרחשו במערכות הארגון. יש לתעד ברשומות, לכל הפחות, אירועים שהתרחשו במערכות המכילות מידע רגיש או חסוי על לקוחות, במערכות קריטיות לתפקוד הארגון ובמערכות ליבה (שרתים, רכיבי תקשורת, אפליקציות, מסדי נתונים וכו'). כל ארגון יגדיר מידע נוסף המתקבל מהמערכות הארגוניות אשר חיוני לתעדו באמצעות רישום בלוג[72], לרבות מזהה ייחודי של הפעולה, פקודות ושאילתות שבוצעו. מנגנוני הרישום יכללו, לכל הפחות, מידע על אופי הפעולה שבוצעה, חתימת זמן, מקור ויעד הפעולה, מזהה משתמש, מזהה תהליך, כישלון או הצלחה של הפעולה שבוצעה, שם קובץ ותהליך מערכת מעורב.

ניטור פעולות תפעוליות במערכת הגבייה

בין הפעולות המבוצעות במערכת הגבייה: החלפת בעלים בנכס, שינוי כתובת נכס, ביטול חיוב, שינוי סכום ההנחה בארנונה בכפוף לתבחינים שנקבעו, שינוי גודל נכס (המשפיע על סכום החיוב בארנונה), שינוי תעריף למשלם (למשל לפי מטר מרובע, לפי המצב החברתי-כלכלי), שינוי למפרע של חיובים (וזיכוי חשבון החייב), פתיחת חשבון משלם חדש וכו'.

מאחר שמערכת הגבייה פותחה על ידי ספקי השירות, הם בעלי הרשאת גישה לנתוני המערכת. עם זאת, ספק השירות של מערכת הגבייה הוא גורם חיצוני שיש לבצע בקרה על הפעולות והשינויים שהוא מבצע במערכת הגבייה. לכן חשוב לבצע בקרה על הפעולות המתועדות במנגנון התיעוד האוטומטי.
בלוח להלן יסוכמו ממצאי בדיקה שביצע צוות הביקורת בדבר קיומו של מנגנון אוטומטי לתיעוד פעולות שבוצעו במערכת הגבייה, כמפורט בבקרות תורת ההגנה בסייבר. עוד נבדק דבר קיומה של בקרה מטעם גורם ברשות המקומית על ממצאי התיעוד של מנגנון הבקרה.

70 קלסרים וארגזי קרטון.
71 בקרה 16.2 בבקרות תורת ההגנה בסייבר 2.0 גרסה 1.3.
72 מנגנון תיעוד פעולות המבוצעות במערכת.

לוח 11 : **קיומו של מנגנון אוטומטי לתיעוד פעולות שבוצעו במערכת הגבייה, וקיומה של בקרה על ממצאי התיעוד, ברשויות שנבדקו**

שם הרשות	האם יש מנגנון תיעוד אוטומטי	התיעוד הנכלל במנגנון הבקרה האוטומטי בהתאם לבקרות תורת ההגנה בסייבר							האם מתבצעת בקרה על ממצאי התיעוד
		מזהה משתמש	חתימת זמן	שם הקובץ ותהליך מערכת מעורב	אופי הפעולה שבוצעה	מקור הפעולה ויעדה	מזהה תהליך	כישלון/ הצלחה	
רשות מקומית א'	✓	✓	✓	✓	✓	✓	✓	✗	✗
רשות מקומית ב'	✓	✓	✓	✓	✓	✓	✓	✓	✓
רשות מקומית ג'	✓	✓	✓	✓	✓	✓	✓	✗	✗
רשות מקומית ד'	✓	✓	✓	✓	✓	✓	✓	✗	✓
רשות מקומית ה'	✓	✓	✓	✓	✓	✓	✓	✗	✗
רשות מקומית ו'	✓	✓	✓	✓	✓	✓	✓	✗	✗

על פי נתוני הרשויות המקומיות שנבדקו, בעיבוד משרד מבקר המדינה.

נמצא כי בכלל הרשויות המקומיות שנבדקו קיים מנגנון תיעוד אוטומטי שמאפשר ביקורת על הגישה למערכות המאגר כנקבע בתקנות הגנת הפרטיות.

תורת ההגנה בסייבר של מערך הסייבר הלאומי מפרטת את הפרטים שיש לכלול במנגנון התיעוד. נמצא כי מנגנון התיעוד האוטומטי של רשויות מקומיות א', ג', ד', ה', ו-ו' לא כלל סטטוס של הצלחה או כישלון של הפעולה שבוצעה במערכת הגבייה. קיומו של מרכיב זה חשוב לצורך איתור מהיר של פעולות שביצע המשתמש אשר גרמו נזק למידע במערכת.

מומלץ כי מנגנון התיעוד האוטומטי שבמערכת הגבייה של רשויות מקומיות א', ג', ד', ה', ו-ו' יכלול סטטוס של הצלחה או כישלון של הפעולה שבוצעה.

רשות מקומית א' מסרה בתשובתה כי תיבדק האפשרות שיתווסף לנתונים המתועדים שנכללו במנגנון הבקרה האוטומטי סטטוס של כישלון-הצלחה. הרשות הוסיפה כי תדאג לבקש מספק מערכת הגבייה דוח בקרה על שינויים והתאמות וכן על ניסיונות כניסה כושלים.

רשות מקומית ד' מסרה בתשובתה כי היא עתידה לצאת למכרז לקבלת שרות של מערכת גבייה חדשה. כחלק ממנגנון התיעוד האוטומטי, תהיה דרישה לכלול במערכת הגבייה סטטוס של כישלון או הצלחה של פעולה שבוצעה.

רשות מקומית ה' מסרה בתשובתה כי במכרז הבא שהרשות תפרסם, יידרשו המציעים לקיים מנגנון תיעוד בהתאם לדרישות של מערך הסייבר.

רשות מקומית ו' מסרה בתשובתה כי המלצת משרד מבקר המדינה מקובלת עליה, וכי היא תפעל ליישמה.

ברשויות מקומיות ב' ו-ד' מופעל מנגנון בקרה בדבר פעולות שבוצעו במערכת המידע. למשל, למנהלי מחלקות הגבייה ברשויות הללו נשלחו אוטומטית מכתבים אלקטרוניים המדווחים על פעולות שבוצעו במערכת שלגביהן הוגדרה התרעה כגון הפחתת שטח הנכס של תושב.

נמצא כי רשויות מקומיות ב' ו-ד' מבצעות בקרה על הפעולות שבוצעו במערכת הגבייה ומתועדות במנגנון הבקרה. עם זאת נמצא כי רשויות מקומיות א', ג', ה' ו-ו' לא מבצעות בקרה על הפעולות שביצעו המשתמשים במערכת הגבייה ומתועדות במנגנון הבקרה, על מנת לאתר פעולות חריגות או בלתי מורשות.

חוסר במידע במנגנון הבקרה מקשה על הרשות המקומית להתחקות אחר הפעולות הלא מורשות שבוצעו במערכת הגבייה, לנטרן בזמן אמת ולנקוט אמצעים מיידיים לטיפול בהן. היעדר בקרה על הפעולות במנגנון הבקרה עשוי להוביל לכך שגורמי הבקרה לא יוכלו לאתר פעולות לא מורשות שבוצעו במערכת.

מומלץ כי רשויות מקומיות א', ג', ה' ו-ו' יבצעו בקרה שוטפת על הפעולות המבוצעות במערכות הגבייה שלהן, בין היתר לאיתור פעולות המבוצעות ללא הרשאה מתאימה על ידי משתמשי המערכת, על מנת לאתר פעולות חריגות או בלתי מורשות.

רשות מקומית ג' מסרה בתשובתה כי יש בה מחלקת בקרה ופיקוח אשר אמונה על הנושא, וכחלק משילוב ממונה אבטחת מידע בארגון יוכן נוהל לבקרה על הפעולות, לאיתור חריגות ולהצגתן בדוחות מפורטים.

רשות מקומית ו' מסרה בתשובתה כי המלצת משרד מבקר המדינה מקובלת עליה, וכי היא תפעל ליישמה.

ביקורת מטעם מבקרי הרשויות המקומיות

מבקר הרשות המקומית אמון על בדיקת פעילותה של הרשות ועל הגשת דין וחשבון על הביקורת שעשה בכל שנה. את איכות הביקורת ניתן למדוד בין היתר על פי נושאי הביקורת ועל פי רמת הסיכונים הכלולים בתוכנית הביקורת וכן על פי היקף הביקורת, איכות ממצאיה ואיכות המלצותיה[73]. על פי העקרונות לעבודת המבקרים שפרסם איגוד מבקרי הרשויות המקומיות, על עבודת המבקר להתבסס, בין היתר, על תוכנית עבודה המבטאת תהליך תיעדוף מובנה וסדור של נושאים לביקורת בהתחשב בנושאי ליבה, ובהם הביקורת על מערכות המידע ברשות[74].

נוכח הסיכונים הנוגעים להגנת הפרטיות הכרוכים בניהול מערכות מידע שלא בהתאם לדרישות החוק והתקנות, נוסף על הסכנה הגלומה באיומי מתקפות סייבר, חשוב לבצע ביקורת בנושא אבטחת המידע ברשויות המקומיות, ובכלל זה בנושא אבטחת מערכות הגבייה ברשויות.

בלוח להלן מובא פירוט בדבר התייחסות מבקרי הרשויות המקומיות שנבדקו בביקורות שערכו בשנים 2021 - 2023 לנושא אבטחת המידע של מערכות הגבייה.

---

73 ראו: European Commission "Quality Assurance for Internal Audit" Public Internal Control Systems in the European Union Discussion Paper No. 3 Ref. 2014-3.

74 איגוד מבקרי הרשויות המקומיות **סימני דרך** (2020), עמ' 6 - 9. ראו מבקר המדינה, **דוח על הביקורת בשלטון המקומי לשנת 2023** (2023), "המבקר ברשות המקומית - תפקידו והתנהלותו - ביקורת מעקב", עמ' 1566.

לוח 12 : **הרשויות המקומיות שנבדקו שמבקריהן התייחסו בביקורות שערכו לנושא אבטחת המידע של מערכת הגבייה, בשנים 2021 - 2023**

שם הרשות	האם מבקרי הרשויות המקומיות שנבדקו התייחסו לנושא אבטחת המידע שבמערכות הגבייה
רשות מקומית א'	כן (בשנת 2023 החל מבקר הרשות בביצוע ביקורת בנושא)
רשות מקומית ב'	לא
רשות מקומית ג'	כן
רשות מקומית ד'	לא
רשות מקומית ה'	לא
רשות מקומית ו'	כן (בדוח של מבקרת הרשות בשנת 2022)

על פי נתוני הרשויות המקומיות שנבדקו, בעיבוד משרד מבקר המדינה.

על אף החשיבות שבקיום ביקורת בנושא אבטחת מידע של מערכת הגבייה ועל אף הסיכונים הכרוכים בניהול מערכות אלה, בביקורת עלה כי רשויות מקומיות ב', ד' ו-ה' לא קיימו ביקורת כזאת בשנים 2021 - 2023. מבקרי הרשויות המקומיות של רשויות מקומיות א', ג' ו-ו' קיימו ביקורת בנושא אבטחת מידע של מערכת הגבייה כאמור בשנים אלה.

מומלץ כי לאחר שמבקרי הרשויות המקומיות של רשויות מקומיות ב', ד' ו-ה' יבצעו תיעדוף של נושאים לביקורת, בהתחשב בנושאי ליבה ובהם הביקורת על מערכות המידע ברשות, הם יכללו בתוכנית העבודה שלהם ביקורת בנושא אבטחת המידע של מערכות הגבייה.

רשות מקומית ד' מסרה בתשובתה כי עבודת הביקורת ברשות מתבצעת בהתאם לסקר סיכונים. בשנים 2022-2023 נערכה ביקורת מקיפה בנושא אבטחת המידע ברשות בכללותו. המסקנות וההמלצות שהועלו רלוונטיים גם בנושא אבטחת מידע במערכת הגבייה.

רשות מקומית ה' מסרה בתשובתה כי בשנת 2022 ביצע מבקר הרשות ביקורת בנושא תקנות הגנת הפרטיות, אבטחת מידע וסייבר. דוח הביקורת בנושא הכולל ממצאי הביקורת וכן המלצות לתיקונם נכלל במסגרת דוח הביקורת לשנת 2022 אשר הוגש לראש הרשות במרץ 2023. בכוונת מבקר הרשות לבחון את תיקון הליקויים שעלו בדוח הביקורת שנערך על-ידו וכן את הליקויים שהועלו במסגרת דוח מבקר המדינה. מבקר הרשות מקבל את המלצת מבקר המדינה לתעדף במסגרת הביקורת שתערך בנושא את נושא אבטחת המידע של מערכות הגבייה.

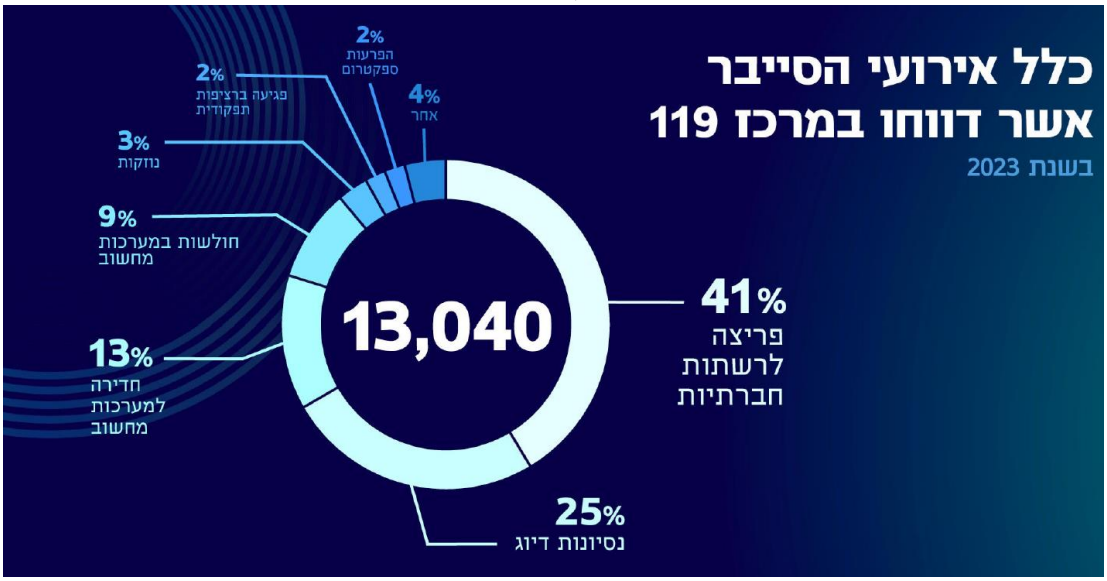
אירועי סייבר

אירוע סייבר הוא התרחשות אשר מעידה על פגיעה אפשרית בפעילותו התקינה של נכס סייבר, אשר יש יסוד להניח כי היא נובעת מפעילות מכוונת במרחב הסייבר. אירוע סייבר אינו בהכרח מעיד על תקיפת סייבר, אך יש יסוד סביר להניח שכן[75].

בתרשימים להלן יוצגו נתונים על כלל אירועי הסייבר שדווחו ותועדו בישראל בשנים 2021 - 2023.

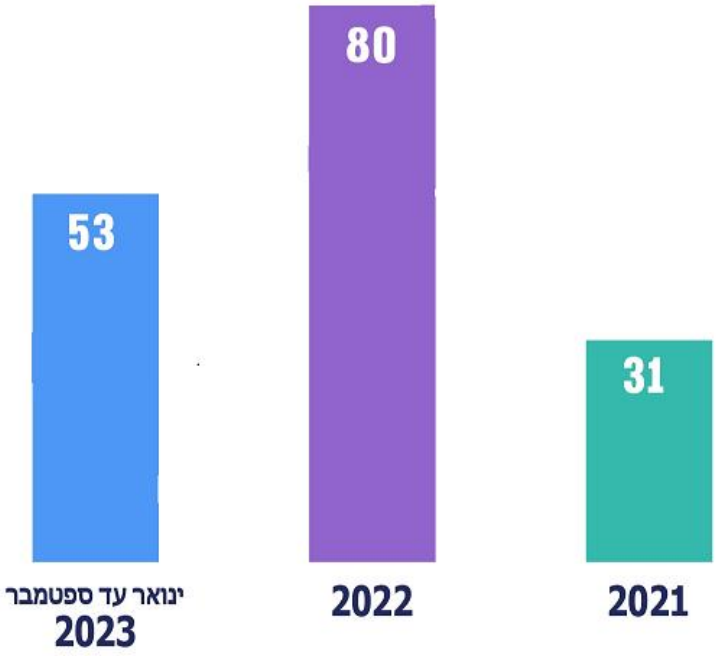
[75] מונחון סייבר באתר המרשתת של מערך הסייבר הלאומי:
https://www.gov.il/he/departments/general/terms

תרשים 2: **כלל אירועי הסייבר אשר דווחו במרכז 119[76] בשנת 2023 על פי דוח סיכום לשנת 2023 של מערך הסייבר הלאומי**



תצלום מסך, מתוך דוח סיכום שנת 2023 של מערך הסייבר הלאומי.

תרשים 3: **מספר אירועי הסייבר שהתרחשו בכלל הרשויות המקומיות ותועדו במערך הסייבר הלאומי, ינואר 2021 - ספטמבר 2023[77]**

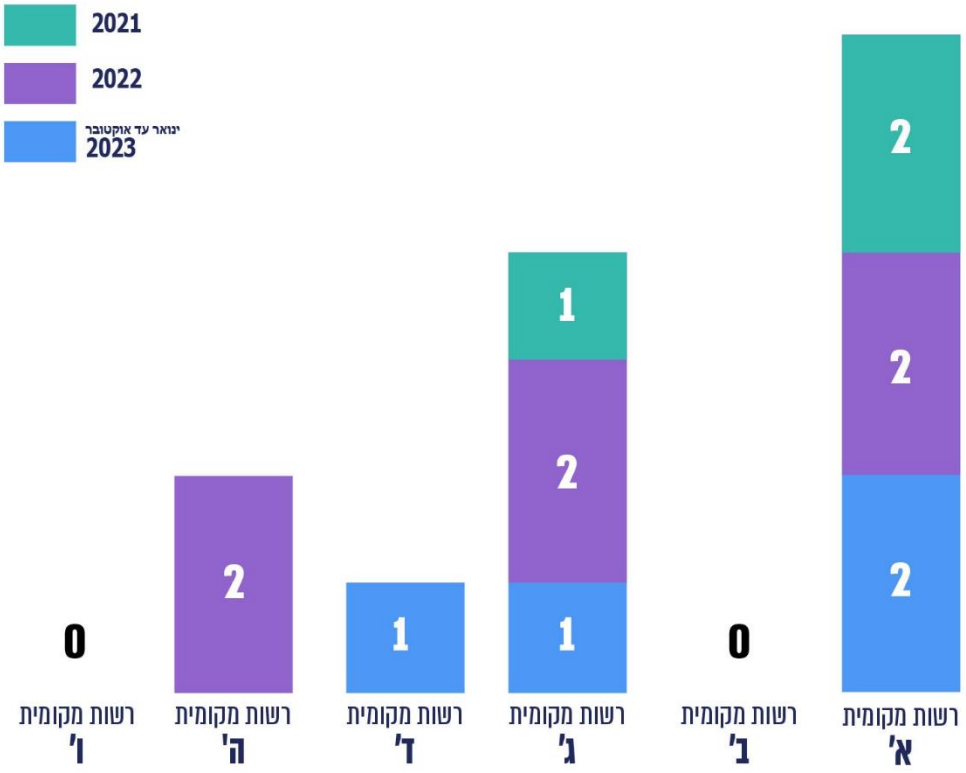


על פי נתונים ממערך הסייבר הלאומי, בעיבוד משרד מבקר המדינה.

76 על פי אתר המרשתת של מערך הסייבר הלאומי, מרכז 119 הוא מרכז של מערך הסייבר הלאומי לדיווח על אירועי סייבר, המאויש 24 שעות ביממה באנליסטים ובאנליסטיות שתפקידם לזהות את סוג האיום, לאמוד את היקף הנזק הנשקף ממנו, ולספק את המענה המותאם לאזרח ולארגון.

77 5.9.23.

תרשים 4: **מספר אירועי הסייבר שהתרחשו בכל אחת מהרשויות המקומיות הנבדקות ותועדו במערך הסייבר הלאומי, ינואר 2021 - אוקטובר 2023**



על פי נתונים ממערך הסייבר הלאומי, בעיבוד משרד מבקר המדינה.

אירועי סייבר הקשורים למערכת הגבייה ברשויות המקומיות הנבדקות

בתקנות הגנת הפרטיות נקבע כי אירע אירוע אבטחה חמור - יודיע על כך בעל המאגר לרשם מאגרי המידע באופן מיידי, וכן ידווח לרשם על הצעדים שנקט בעקבות האירוע. מהנתונים שהתקבלו מהרשות להגנת הפרטיות עולה כי הרשות לא קיבלה דיווח על אירועי סייבר הקשורים למערכת הגבייה שהתרחשו ברשויות המקומיות הנבדקות.

חשד לאירועי סייבר אצל ספקי השירות של מערכות הגבייה

חשד לאירועים שתועדו במרכז הארצי לניהול אירועי סייבר (CERT[78]) לגבי ספקי השירות של מערכת הגבייה או שטופלו על ידי הרשות להגנת הפרטיות

לוח 13: **פירוט של חשד לאירועים שתועדו במרכז הארצי לניהול אירועי סייבר**

שם ספק השירות של מערכת הגבייה	תיאור החשד לאירוע
ספק א'	בשנת 2022 הועברו לספק דיווחים על כמה תקשורות חשודות וחולשות אבטחה.
ספק ב'	הספק עלה ב-CERT פעמיים במסגרת "צמצום חשיפות" של כתובות החשופות לפגיעויות.
ספק ג'	דווח לספק על אינדיקציה לכך שתוקף גילה עניין במערכותיו וכי אותרה תקשורת חשודה (נסגר ללא ממצאים).

על פי נתוני ה-CERT, בעיבוד משרד מבקר המדינה.

<u>דיווחים של רשויות מקומיות למערך הסייבר בדבר אירועי סייבר שהתרחשו אצלן</u>

בביקורת עלה כי רשויות מקומיות א', ב', ד', ה' ו-ו' לא קיבלו ממערך הסייבר הלאומי בקשה לדווח לו על אירועי סייבר שהתרחשו אצלן. רשות מקומית ג' ציינה כי קיבלה בקשה כזאת.

רשויות מקומיות ב', ג', ד', ה' ו-ו' מסרו לצוות הביקורת כי לא התרחשו אצלן אירועי סייבר, ולפיכך מבחינתן לא היה צורך שהן ידווחו על אירועים אלה למערך הסייבר הלאומי.

ברשות מקומית א' התרחשו שני ניסיונות לדרישת כופר, אולם הרשות לא דיווחה עליהן למערך הסייבר הלאומי, ולדבריה היא התמודדה עם האירועים באופן עצמאי.

משרד הפנים מסר בתשובתו ממאי 2024 כי הוא שותף לחשיבות הדיווח של הרשויות המקומיות למערך הסייבר על התרחשות אירועי סייבר אצלן, ואולם, באשר לחלקו של משרד הפנים בעניין הנחיית הרשויות בעניין זה, הרשויות המקומיות - בשונה ממשרדי הממשלה השונים והיחידות שבתחום אחריותם - אינם חלק מגופי הממשלה הכפופים להחלטותיה, אלא גופים עצמאיים בעלי מעמד על פי דין אשר לצורך הנחייתם והטלת חובות עליהם, יש צורך בעיגון הסמכות והכללים בחקיקה או בהתאם לחקיקה.

מערך הסייבר הלאומי מסר בתשובתו מיוני 2024 כי להבדיל מסמכות ההנחיה של המערך מול גופים המהווים תשתית מדינה קריטית, בהתאם להחלטת הממשלה הפעילות מול הרשויות המקומיות צריכה להתבצע על ידי היחידה המגזרית במשרד הפנים, לרבות בכל הנוגע להסדרת דיווח על אירוע.

עד להקמתה של יחידה מגזרית עבור הרשויות המקומיות שתהווה גורם רשמי אשר אחראי להעביר הנחיות מקצועיות לרשויות המקומיות, מומלץ כי מערך הסייבר הלאומי, במסגרת הפעילות שהוא מקיים מול הרשויות המקומיות, בשיתוף משרד הפנים ינחו את הרשויות המקומיות לדווח למערך הסייבר על התרחשות אירועי סייבר, ובסמוך ככל האפשר למועד התרחשותם. כמו כן, מומלץ כי כלל הרשויות המקומיות לרבות רשות מקומית א' ידווחו למערך הסייבר הלאומי על התרחשות אירוע סייבר אצלם, בין לצורך קבלת סיוע ובין לצורך העברת מידע על האירוע. הנחיית הרשויות המקומיות בדבר הצורך בדיווח על אירועי סייבר שהתרחשו אצלן

78 Computer Emergency Response Team - הוא הזרוע המבצעית של מערך הסייבר הלאומי. ה-CERT מטפל באירועי סייבר במרחב האזרחי של מדינת ישראל.

יכולה למנוע מצבים כדוגמת אי-דיווחה של רשות מקומית א' על שני אירועים שבהם היא נדרשה לשלם כופר.

רשות מקומית ג' מסרה בתשובתה כי היא בקשר שוטף עם מערך הסייבר הלאומי ובמידה ויתקיים ברשות אירוע סייבר, היא תדווח למערך הסייבר לצורך סיוע וקבלת מידע.

רשות מקומית ה' מסרה בתשובתה כי המלצת הביקורת מקובלת עליה.

מערך הסייבר הלאומי מסר בתשובתו מיוני 2024 כי בהתאם לתפיסה המקצועית ולהחלטת הממשלה, הגורם הנדרש והאחראי לריכוז נתונים בכל מגזר הוא היחידה המגזרית במגזר עצמו, ולעניינו במשרד הפנים. עוד מסר מערך הסייבר כי על משרד הפנים לרכז את המידע מכל הרשויות במגזר ולהעבירו למערך הסייבר הלאומי, לצורך יצירת תמונה לאומית וכדי להפיק תובנות והמלצות לכלל המשק.

עד להקמתה של יחידה מגזרית עבור הרשויות המקומיות שתהווה גורם רשמי אשר אחראי להעביר הנחיות מקצועיות לרשויות המקומיות, מומלץ שמערך הסייבר הלאומי ירכז את המידע שיתקבל מהרשויות המקומיות, בין אם המידע יתקבל באופן ישיר או באמצעות גורם אחר, בדבר אירועי סייבר שהתרחשו אצלן. מידע זה יאפשר למערך הסייבר לנתח את מאפייני האירועים ומידת הנזק הפוטנציאלי שלהם ובהתאם להוציא המלצות לרשויות, והדבר יסייע לו בשיפור ההיערכות ברמה הלאומית להתמודדות עם מתקפות סייבר.

<u>אירועי סייבר בעקבות מלחמת חרבות ברזל</u>

במסמך של מערך הסייבר הלאומי מדצמבר 2023[79] צוין כי מראשית מלחמת "חרבות ברזל" מזהה מערך הסייבר הלאומי פעילות הולכת ומתעצמת של תוקפים מסוגים שונים כנגד ארגונים במרחב הסייבר הישראלי. התוקפים פועלים במנעד רחב של שיטות וטכניקות, החל במתקפות פשוטות, לא מתוחכמות, כגון השחתת אתרים או מתקפות מניעת שירות, וכלה בתקיפות ממוקדות של ארגונים המשמשים חוליה בשרשרת האספקה לארגונים רבים במשק, וזאת כדי להגדיל את היקף הפגיעה.

עוד צוין במסמך כי במהלך המלחמה ניכר שדרוג משמעותי בפעילות התקיפה, וזאת בהדרגה ולאורך זמן. נכון לדצמבר 2023, בשלב זה של המלחמה מטרתן של מרבית המתקפות היא גרימת נזק, בניגוד למגמה שהסתמנה לפני הלחימה ובתחילתה והתאפיינה בעיקר במתקפות למטרות ריגול וגניבת מידע[80].

על פי המסמך, במהלך הלחימה זוהו כ-15 קבוצות תקיפה עיקריות הפועלות במרחב הסייבר הישראלי. מרביתן משתפות ביניהן מידע מודיעיני, שיטות וכלים, לצורכי מימוש מגוון סוגי תקיפות הנכסים בישראל שהן פועלות מולם[81].

עוד הובהר במסמך כי פעילות התוקפים זוהתה מול נכסים נפוצים רבים המשמשים את המשק: מערכות אבטחה פיזית המשרתות ארגונים שונים במשק, דוגמת מצלמות אבטחה; ממשקי ניהול חשופים, דוגמת ממשק בקר המנוהל מרחוק; ציוד תקשורת החושף ממשקי ניהול למרשתת, כגון: Cisco, Juniper; מערכות ניטור ושליטה מרחוק, החשופות ישירות למרשתת; ממשקי גישה מרחוק, כגון Fortinet, Citrix[82].

---

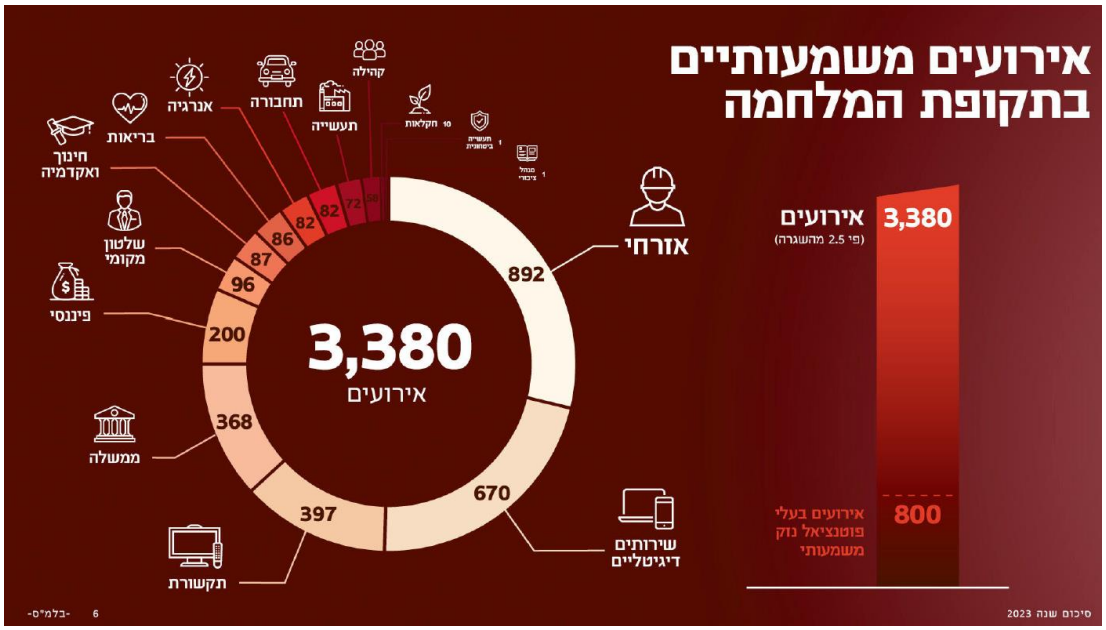
79 מערך הסייבר הלאומי, **מלחמת "חרבות ברזל" במימד הסייבר: תובנות ודרכי התמודדות** (דצמבר 2023, עמ' 2.

80 שם, עמ' 3.

81 שם, עמ' 3.

82 שם, עמ' 5.

תרשים 5: **אירועי סייבר משמעותיים בתקופת המלחמה על פי דוח סיכום לשנת 2023 של מערך הסייבר הלאומי**



תצלום מסך, מתוך דוח סיכום שנת 2023 של מערך הסייבר הלאומי

מתרשימים 3 ו-5 עולה כי בתקופה ינואר עד ספטמבר 2023 התרחשו 53 אירועי סייבר ברשויות מקומיות, וכי בתקופת מלחמת חרבות ברזל, בחודשים אוקטובר עד סוף דצמבר 2023, התרחשו 96 אירועי סייבר ברשויות המקומיות. כלומר, כ-65% מאירועי הסייבר בשנת 2023 (96 מתוך 149 אירועים) ברשויות מקומיות התרחשו בתקופת מלחמת חרבות ברזל, תקופה של שלושה חודשים.

ביטוח סייבר

בעשור האחרון גובר הביקוש לכיסוי ביטוחי בפני תקיפות סייבר. הכיסוי הביטוחי בתחום הסייבר כולל למשל כיסוי של הוצאות אלה: הוצאות שבוצעו בעקבות אירוע סייבר; הוצאות רגולטוריות משפטיות; הוצאות הקשורות לרכיבי אבטחת מידע; הוצאות על ביצוע מחקר בנוגע לזהות התוקף; פגיעה בפרטיות; נזקי פגיעה בפעילות העסקית של הארגון; נזקי פגיעה במערכות הארגון; והחזר כספי בהתרחש מתקפת כופר. עם זאת, מסקר שביצע מערך הסייבר הלאומי בשנת 2019 עולה כי רק ל-13% מהחברות במשק היה ביטוח סייבר. לפי הערכת מערך הסייבר הלאומי, המורכבות שבקידום הנושא נובעת, בין היתר, מכך שמדובר בתחום ביטוחי חדש שלחלק מחברות הביטוח אין ידע מספק בענייננו, ומהיעדר ביקוש בשל חוסר מודעות של ארגונים לסיכון[83].

ביטוח סייבר כולל כיסוי של הוצאות בעקבות אירוע סייבר, ומכאן חשיבותו להתמודדות בקרות אירוע סייבר. נמצא כי מלבד רשות מקומית א' שיש לה ביטוח סייבר בהיקף של 2 מיליון דולר, ליתר הרשויות המקומיות שנבדקו, רשויות מקומיות ב', ג', ד', ה', ו-ו', אין ביטוח סייבר.

רשויות מקומיות שאינן מבוטחות בפני אירועי סייבר עלולות להידרש לשאת בכלל ההוצאות הכרוכות בהתמודדות עם אירוע הסייבר ובהתאוששות ממנו, כגון הקמה מחדש של כל תשתיות המחשוב.

מומלץ כי רשויות מקומיות ב', ג', ד', ה', ו-ו', שאין בידיהן ביטוח סייבר, ינהלו את הסיכון ויבחנו אם עליהן לרכוש ביטוח סייבר כמענה לסיכון.

---

83 מבקר המדינה, **דוח מבקר המדינה**, מאי 2022 (2022), "הגנת סייבר על מכשירים רפואיים ואבטחת המידע הנאגר בהם" עמ' 1185.

עוד מומלץ כי מערך הסייבר כמנחה מקצועי של המשק בתחום הסייבר יגבש מדיניות בנושא ביטוח סייבר.

מערך הסיבר הלאומי מסר בתשובתו מיוני 2024 כי העמדה המקצועית של מערך הסייבר הלאומי היא כי ביטוח סייבר מביא לעליה ברמת ההגנה, וכמובן תורם בניהול הסיכונים בעת אירוע התקיפה. מצד שני, קיימת מורכבות בנושא, בכלל האמור העובדה כי דמי הפוליסה הנוגעים לביטוחי סייבר הם יחסית יקרים. עוד נמסר כי להבנת מערך הסייבר הלאומי, בשל מורכבות התחום, אין מדיניות קונקרטית לנושא הזה באף אחת ממדינות המערב. במקביל מערך הסייבר מעורב בנושא מורכב זה, עוקב אחרי שוק ביטוח הסייבר בישראל, נמצא בקשר עם השותפים הבינלאומיים שלו בנושא ואף עם מבטחי המשנה העולמיים של חברות הביטוח בארץ. בכלל האמור, בהיבט העשייה הבינלאומית, המערך שותף, יחד עם למעלה מ 60 מדינות מובילות, במיזם CRI (Counter Ransomware Initiative) אשר עוסק בהתמודדות עם תקיפות כופרה. אחת מקבוצות העבודה במיזם עוסקת בבחינה מדיניות לתחום ביטוח הסייבר. ברם כאמור, העמדה המקצועית בנושא במדינות מערביות טרם גובשה.

רשות מקומית ג' מסרה בתשובתה כי היא בוחנת כמה הצעות לביטוח סייבר. היעד לרכישת הפוליסה הוא עד סוף 2024.

רשות מקומית ד' מסרה בתשובתה כי היא תפעל ככל הניתן להסדרת ביטוח סייבר.

רשות מקומית ה' מסרה בתשובתה כי הרשות תפנה לסוכן הביטוח שלה כדי לבטח עצמה בביטוח זה.

רשות מקומית ו' מסרה בתשובתה כי על פי ההסכם עם ספק השירות של מערכת הגבייה, הוא נדרש לרכוש ביטוח סייבר. ביטוח זה נועד לכסות את הנזק העתידי מכל אירוע סייבר שיתרחש בשרתי הספק ושיש לו השפעה על הרשות. הרשות הוסיפה כי הסיכון השיורי הנוגע לפוטנציאל הנזק שאינו מבוטח בביטוח לעיל מוערך על ידי המועצה כנמוך וככזה שאינו מצדיק עלות גבוהה של ביטוח סייבר. על כן, הרשות מתעדפת את התקציב לטובת השקעה בניטור מערכות המידע ובהגנה שוטפת עליהן. עם זאת הרשות מבצעת הערכת סיכונים באופן תקופתי, ואם עוצמת הנזק הצפוי מאירועי סייבר תעלה על עלות הביטוח תפעל להסדיר ביטוח שכזה.

זיהוי ואימות של משתמשים במערכת הגבייה

<u>זיהוי על בסיס אמצעי פיזי</u>

בתקנות הגנת הפרטיות נקבע כי בעל מאגר מידע ינקוט אמצעים מקובלים בנסיבות העניין, בהתאם לאופי המאגר ולטיבו, כדי לוודא כי הגישה למאגר ולמערכות המאגר ניתנת לבעל הרשאה המורשה לכך בלבד, לפי רשימת ההרשאות התקפות. עוד נקבע כי במאגר מידע שחלה עליו רמת האבטחה הבינונית או הגבוהה הזיהוי יתבסס, במידת האפשר, על אמצעי פיזי הנתון לשליטתו הבלעדית של המורשה. אמצעי זיהוי פיזי כוללים, בין היתר, זיהוי באמצעות אימות קוד טלפוני, טביעת אצבע, כרטיס חכם.

בבקרות של תורת ההגנה בסייבר[84] בנושא מדיניות סיסמאות צוין כי "השימוש בפקטור יחיד (דוגמת סיסמה) יוצר סיכון משמעותי לארגון, ולפיכך יש להעדיף שימוש ב - MFA[85]".

השימוש בשם משתמש וסיסמה כשלב אימות יחיד (בודד) נחשב לנטילת סיכון, וזאת לנוכח העובדה כי "תוקף" עלול להשיג את הסיסמה באמצעים טכנולוגיים ואחרים. להלן דוגמאות:

84 בקרה 3.9 לבקרות תורת ההגנה בסייבר 2.0 גרסה 1.3.

85 Multi Factor Authentication - אימות רב-שלבי, לדוגמה אימות הן באמצעות סיסמת כניסה והן באמצעות קוד טלפוני.

באמצעות שימוש בהנדסה חברתית (Social Engineering)[86] ומתקפת דיוג (Phishing) התוקף עשוי לשכנע את המשתמש למסור לו את סיסמת ההתחברות לממשק המחייב אימות מקדים; "הצצה מעבר לכתף" (Surfing Shoulder) עשויה לאפשר לתוקף לזהות את סיסמת הגישה באמצעות צפייה במשתמש הנמצא במרחב הציבורי והמתחבר למשאבי הארגון; ניתן להפעיל נוזקה (Malware) במחשב המשתמש אשר תשדר לתוקף את סיסמת הגישה, ובכך תאפשר לו לקבל גישה מלאה וממושכת למשאבי הארגון. לנוכח זאת, פותחה מתודולוגיה הנקראת "הזדהות חזקה" (Strong Authentication) אשר מאפשרת הגדרה של תהליך אימות רב-שלבי (או רב-גורמי), אשר בכל שלב משלביה המשתמש נדרש להציג מזהה ייחודי אחד או יותר[87].

בדוח פיקוח רוחב שנערך על ידי הרשות להגנת הפרטיות בשנת 2021[88] צוין כי בחלק מהרשויות המקומיות הקטנות והגדולות נמצא כי הכניסה של עובד הארגון למאגר מתבצעת ללא שימוש באמצעי פיזי הנתון לשליטתו המלאה של המורשה.

ברשויות המקומיות שנבדקו רמת האבטחה היא בינונית או גבוהה. אי לכך, לצורך זיהויו וכניסתו למערכת הגבייה עליו לבצע אימות דו-שלבי הכולל אמצעי פיזי נוסף על הסיסמה.

מסקירת מסמכי המכרזים והחוזים של **רשויות מקומיות א', ג', ה' ו-ו'** עולה כי יש דרישה שמערכת הגבייה שיציעו המציעים תאפשר גישה למאגרי המידע באמצעות אמצעי פיזי. במסמכי המכרז והחוזה של **רשות מקומית ב'** עם ספק השירות של מערכת הגבייה אין התייחסות לנושא.

ברשות מקומית ו' הגישה למערכת הגבייה מבוצעת באמצעות סיסמה וקוד אימות מהטלפון הנייד בהתאם לנדרש בתקנות הגנת הפרטיות.

בתקנות הגנת הפרטיות נקבע כי הזיהוי יתבסס, במידת האפשר, על אמצעי פיזי הנתון לשליטתו הבלעדית של המורשה. נמצא כי ברשויות מקומיות א', ג' ו-ה' לא מתבצע אימות דו-שלבי הכולל שימוש בסיסמה ובאמצעי פיזי כנדרש בהסכם ההתקשרות עם ספק השירות ובתקנות הגנת הפרטיות. ברשויות מקומיות ב' ו-ד' לא מתבצע אימות דו-שלבי הכולל סיסמה ואמצעי פיזי כנדרש בתקנות הגנת הפרטיות.

מבדיקת צוות הביקורת עם ספקי השירות של מערכת הגבייה של רשויות מקומיות א', ב', ג' ו-ה' עולה כי המנגנון קיים במערכת, אולם רשויות אלה לא פעלו ליישם אותו במערכות שלהם.

רשות מקומית א' מסרה בתשובתה כי תיבדק האפשרות של אימות דו-שלבי, וכי נוכח דפוס העבודה של פקידי הגבייה ברשות, הדבר מצריך שינוי תפיסתי.

רשות מקומית ג' מסרה בתשובתה כי אין ברשותה אפשרות לאימות דו-שלבי של משתמשים במערכת הגבייה. הוחלט עם ספק השירות של מערכת הגבייה שיקיימו יחד דיון לצורך קבלת החלטות בנושא.

רשות מקומית ד' מסרה בתשובתה כי מערכת הכספים היא בניהול הרשות (און-פריים[89]), וכי אין אפשרות לאימות דו-שלבי. עם החלפת המערכת תפעל הרשות ליישם דרישה זו.

רשות מקומית ה' מסרה בתשובתה כי הצורך באימות דו־שלבי במערכות הספק ידוע אך טרם יושם כיוון שמעבר לאימות דו־שלבי יחייב לעשות כן לגבי כלל המערכות הפועלות ברשות ולא רק לגבי מערכת הגבייה. הרשות תבחן את השלכות העברת כלל המערכות לאימות דו-שלבי ותגבש את הדרך הטובה ביותר לביצוע מעבר זה.

---

86 ניצול של תכונות פסיכולוגיות של האדם לצורכי פעולות בתחום הסייבר.

87 מערך הסייבר הלאומי, **שיטות אימות מתקדמות הגברת המוכנות לאיומי סייבר באמצעות הזדהות רב שלבית קווים מנחים** (2020), עמ' 4.

88 **דוח פיקוח רוחב - ממצאי הליך פיקוח הרוחב בקרב רשויות מקומיות** (נובמבר 2021), עמ' 25. במסגרת הדוח בוצעה בדיקה בקרב 70 רשויות מקומיות.

89 שרת מרכזי השוכן פיזית במשרדי הרשות.

על רשויות מקומיות א', ב', ג', ד' ו-ה' לאמץ שימוש באמצעי פיזי, נוסף על סיסמה, לצורך זיהוי המשתמש וקבלת גישה למערכת הגבייה.

אורך סיסמת כניסה למערכת ומורכבותה

באתר המרשתת של הרשות להגנת הפרטיות צוינה החשיבות של קביעת סיסמה "חזקה"[90] ונקבע כי סיסמה ארוכה עדיפה על פני סיסמה קצרה וכי לאורך הסיסמה חשיבות רבה, שכן עם כל תו שנוסף לסיסמה קשה יותר לנחש אותה[91].

בבקרות של תורת ההגנה בסייבר[92] צוין בנושא של בקרות גישה בבקרה ברמה בסיסית[93] שאורך הסיסמה למשתמש אנושי צריכה להיות עשרה תווים לפחות.

בלוח להלן מוצגת הדרישה שנקבעה במדיניות הסיסמאות של מערכת הגבייה מבחינת מספר התווים של הסיסמה ומורכבותה (מספרים, אותיות, סימנים וכו').

לוח 14: **אורך הסיסמה ומורכבותה, כפי שנקבע במדיניות הסיסמאות שבמערכת הגבייה ברשויות שנבדקו**

שם הרשות	מספר התווים של הסיסמה	האם נקבעה דרישה בעניין מורכבות הסיסמה
רשות מקומית א'	שמונה תווים	✓
רשות מקומית ב'	שבעה תווים	✓
רשות מקומית ג'	שמונה תווים	✓
רשות מקומית ד'	ארבעה תווים	✗
רשות מקומית ה'	שמונה תווים	✓
רשות מקומית ו'	שמונה תווים	✓

על פי נתוני הרשויות המקומיות שנבדקו, בעיבוד משרד מבקר המדינה.

בבקרות של תורת ההגנה בסייבר של מערך הסייבר הלאומי צוין כי יש לקבוע סיסמה הכוללת עשרה תווים לפחות. מהלוח עולה כי לפי מדיניות הסיסמאות של רשויות מקומיות א', ג', ה' ו-ו' סיסמת הכניסה למערכת הגבייה של הרשות צריכה לכלול שמונה תווים, ולפי המדיניות של רשות מקומית ב' הסיסמה צריכה לכלול שבעה תווים, פחות ממספר התווים המינימלי שהוגדר בבקרות שקבע מערך הסייבר הלאומי. ברשויות אלה מדיניות הסיסמאות של מערכת הגבייה כוללת דרישה לקביעת סיסמה מורכבת. לעומת זאת, במערכת הגבייה של רשות מקומית ד' אורך הסיסמה הוא ארבעה תווים ומדיניות הסיסמאות של מערכת הגבייה אינה כוללת דרישה לקביעת סיסמה מורכבת, שלא לפי הנחיות מערך הסייבר הלאומי.

---

90 אורך הסיסמה ומורכבותה.

91 באתר המרשתת של הרשות להגנת הפרטיות פורסמה בתאריך 1.6.21 דוגמה לכך: "הסיסמה Sucaria המכילה 7 תווים של אותיות קטנות וגדולות, תדרוש 1,028,071,702,528 ניחושים (52 אותיות אפשריות, גדולות וקטנות, בחזקת 7). בהינתן קצב עיבוד של 2 מיליארד ניחושים בשנייה, הסיסמה הזו תיפרץ בתוך 9 דקות, וככל שהמחשב חזק יותר, סביר שאף הרבה קודם לכן. לעומת זאת, תהליך פריצתה של סיסמה באורך 12 תווים, הכוללת ספרות ותווים מיוחדים כגון Suc@r!@M2uka, באותו קצב חישוב, עשוי לארוך 7.5 מיליון שנים. שכן, ישנם 94 תווים אפשריים (26 אותיות גדולות, 26 אותיות קטנות, 10 ספרות, ו-32 תווים מיוחדים) בחזקת 12. מדובר בלא פחות מ-475,920,314,814,253,376,475,136 אפשרויות שונות. כלומר הוספתו של כל תו נוסף מקשה באופן משמעותי על ניחוש הסיסמה".

92 בקרה 3.9 בבקרות תורת ההגנה בסייבר 2.0, גרסה 1.3.

93 רמת הבקרה הוגדרה כך בתורת ההגנה בסייבר - "לכל המלצת הגנה הוגדרה רמה שנעה על ציר של 1-4, כאשר 1 מייצג בקרה בסיסית ואילו 4 - בקרה שיש ליישם במקום שבו פוטנציאל הנזק משמעותי יותר. סיווג זה נועד לשמש כלי תומך החלטה כאשר שוקלים אם ליישם בקרה ביעד הגנה מסוים, שכן לא כל הבקרות מיושמות בצורה זהה בכל תהליכי ומערכות הארגון. בנוסף, חלוקה זו מסייעת לייצר בידול (דיפרנציאציה) לטובת מידתיות, כך שארגונים יכולים להתחיל עם יישום בקרות בסיסיות, ובהמשך לבחון יישום בקרות מתקדמות ומורכבות יותר".

רשות מקומית ה' מסרה בתשובתה כי הגדלת מספר תווי הסיסמא מקשה על עובדים לזכור אותן. הרשות סבורה כי שימוש בסיסמאות חזקות, הגם שהן מורכבות משמונה תווים בלבד, צריך להיות מספיק.

מומלץ כי רשויות מקומיות א', ב', ג', ד', ה' ו-ו' יקבעו אורך סיסמה מינימלי של עשרה תווים בהתאם לבקרות של מערך הסייבר הלאומי. עוד מומלץ שרשות מקומית ד' תגדיר דרישה לקביעת סיסמה מורכבת.

רשות מקומית א' מסרה בתשובתה כי תועבר לספק השירות של מערכת הגבייה הנחיה להאריך את הסיסמה, באופן שהיא תכלול לפחות עשרה תווים.

רשות מקומית ד' מסרה בתשובתה כי הנושא יטופל.

רשות מקומית ו' מסרה בתשובתה כי המלצת משרד מבקר המדינה מקובלת עליה, וכי היא תפעל ליישמה.

ספק שירות ג', שמספק שירות ל**רשות מקומית ו'**, מסר בתשובתו למשרד מבקר המדינה מאפריל 2024 כי עד לסוף אפריל 2024 - כל המשתמשים יעברו לסיסמה באורך עשרה תווים.

ניתוק אוטומטי מהמערכת לאחר פרק זמן של אי-פעילות

תקנות הגנת הפרטיות קובעות כי נוהל אבטחת מידע צריך לכלול גם הוראה לעניין ניתוק אוטומטי לאחר פרק זמן של אי-פעילות, זאת כדי למנוע מגורם לא מורשה להשתמש במערכת.

בבקרות של תורת ההגנה בסייבר[94] צוין בנושא של בקרות גישה בבקרה ברמה בסיסית ש"הארגון יוודא כי יעד ההגנה מבצע נעילה (Lock) של מסך [המערכת] המשתמש לאחר 15 דקות ללא פעילות".

לוח 15 : **ניתוק אוטומטי מהמערכת לאחר פרק זמן של אי-שימוש**

שם הרשות	האם ההסכם עם ספק השירות של מערכת הגבייה כלל התייחסות לפרק הזמן לניתוק מהמערכת לאחר אי פעילות?	זמן הניתוק האוטומטי שהוגדר בפועל במערכת
רשות מקומית א'	✓ (30 דקות)	60 דקות
רשות מקומית ב'	×	לא הוגדר ניתוק מהמערכת
רשות מקומית ג'	✓ (לא הוגדר פרק זמן)	60 דקות
רשות מקומית ד'	הרשות המקומית מגדירה את פרק הזמן באופן עצמאי	60 דקות
רשות מקומית ה'	×	60 דקות
רשות מקומית ו'	✓ (לא הוגדר פרק זמן)	55 דקות

על פי נתוני הרשויות המקומיות שנבדקו, בעיבוד משרד מבקר המדינה.

תקנות הגנת הפרטיות קובעות כי לאחר פרק זמן של אי-פעילות במערכת היא תנותק אוטומטית ובבקרות של תורת ההגנה בסייבר של מערך הסייבר הלאומי צוין כי הניתוק יבוצע לאחר 15 דקות של אי פעילות במערכת. נמצא כי בהסכם ההתקשרות עם ספק השירות של מערכת הגבייה של רשויות מקומיות ב' ו-ה' לא צוין פרק הזמן הרצוי לניתוק מהמערכת לאחר אי-פעילות. בהסכם ההתקשרות עם ספק השירות של מערכת הגבייה של רשויות מקומיות ג' ו-ו' צוין כי יבוצע ניתוק

94 בקרה 3.3 בבקרות תורת ההגנה בסייבר 2.0 גרסה 1.3.

אוטומטי אך לא הוגדר פרק הזמן של אי-הפעילות במערכת. בהסכם ההתקשרות של רשות מקומית א' הוגדר זמן ניתוק אוטומטי אך בפועל ספק השירות של מערכת הגבייה הגדיר פרק זמן שונה (בהסכם נקבע זמן ניתוק לאחר 30 דקות של אי פעילות, בפועל הוגדר במערכת 60 דקות). עוד עולה כי במערכת הגבייה של רשויות מקומיות א', ג', ד' ו-ה' הוגדר זמן ניתוק אוטומטי לאחר 60 דקות של אי פעילות. ברשות מקומית ו' הוגדר זמן ניתוק אוטומטי לאחר 55 דקות של אי-פעילות, וברשות מקומית ב' לא הוגדר זמן ניתוק מהמערכת.

ההחלטה לבצע ניתוק אוטומטי לאחר 55-60 דקות של אי-פעילות אינה תואמת להנחיות מערך הסייבר הלאומי, מאחר שמדובר בפרק זמן ממושך שבמהלכו עשוי גורם לא מורשה לבצע פעולות במערכת.

על רשויות מקומיות ב' ו-ה' לפעול לכך שלהסכמי ההתקשרות של מערכות מידע יתווספו הוראות הנוגעות לפרק הזמן של אי-פעילות שלאחריו תנותק המערכת. על רשויות מקומיות ג' ו-ו' לכלול בהסכם ההתקשרות של מערכות מידע הוראות הקובעות את פרק הזמן של אי-פעילות שלאחריו תנותק המערכת ולא רק לציין את החובה כי יבוצע ניתוק של המערכת. על רשויות מקומיות א', ג', ד', ה' ו-ו' להפחית את משך אי-הפעילות במערכת הגבייה עד לניתוקה בהתאם לבקרות תורת ההגנה בסייבר של מערך הסייבר הלאומי (15 דקות). כמו כן, על רשות מקומית ב' להגדיר את משך הזמן של אי-פעילות במערכת הגבייה עד לניתוקה.

רשות מקומית א' מסרה בתשובתה כי תעביר לספק השירות של מערכת הגבייה הנחיה לבצע ניתוק אוטומטי לאחר 30 דק' של אי-פעילות.

רשות מקומית ד' מסרה בתשובתה כי בהתאם לתורת ההגנה בסייבר הלאומי כלל המחשבים ברשות[95] ננעלים מייד לאחר 15 דקות של חוסר שימוש במחשב, והדבר משמש שכבת הגנה.

רשות מקומית ה' מסרה בתשובתה כי ניתן לקצר את פרק הזמן לניתוק אוטומטי אך ניתוק שכזה לאחר רבע שעה יכול להיות קצר מידי ולהביא לניתוק עובד בזמן שהוא מכין חומר להזנה במערכת או ממתין לחתימה. הרשות תבדוק מהו משך הזמן האופטימלי ותבקש מהספק לקצר את משך הזמן לניתוק אוטומטי בהתאם.

רשות מקומית ו' מסרה בתשובתה למשרד מבקר המדינה כי המלצת משרד מבקר המדינה מקובלת עליה, וכי היא תפעל ליישמה.

ספק שרות ג' (שמספק שירות לרשות מקומית ו') מסר בתשובתו כי זמן הניתוק האוטומטי ניתן להגדרה על פי דרישות הלקוח. עוד מסר כי אם הרשות תנחה אותם לקצר את זמן הניתוק, הדבר יבוצע על ידם.

על רשות מקומית ד' להפחית את משך אי-הפעילות במערכת הגבייה עד לניתוקה בהתאם לבקרות תורת ההגנה בסייבר של מערך הסייבר הלאומי ל-15 דקות, זאת נוסף על נעילת המסך כפי שנוהגת הרשות, כדי להעלות את רמת אבטחת המידע של מערכת הגבייה.

95 מדובר ברשת הארגונית של הרשות ולא במערכת הגבייה.

ניהול הרשאות גישה למערכת הגבייה

תקנות הגנת הפרטיות קובעות שבעל מאגר מידע יקבע הרשאות גישה של בעלי הרשאות למאגר המידע ולמערכות המאגר, בהתאם להגדרות תפקידם; הרשאת הגישה לכל תפקיד תהיה במידה הנדרשת לביצוע התפקיד בלבד. בעל מאגר מידע ינהל רישום מעודכן של בעלי תפקידים, של הרשאות הגישה שניתנו להם, ושל בעלי ההרשאות הממלאים תפקידים אלה.

הרשאות הגישה למערכת הגבייה כוללות הרשאות כתיבה וקריאה למסכים ספציפיים במערכת כגון הצגת מצב חשבון, דוח יתרות למשלם, תיק נכס, עדכון הנחה, חישוב הנחה.

נוהל עבודה בנושא הרשאות

בתקנות הגנת הפרטיות נקבע כי נוהל האבטחה יכלול הרשאות גישה למאגר המידע ולמערכות המאגר בהתאם לתקנה 8.

על אף שבתקנות הגנת הפרטיות נקבע שנוהל אבטחת מידע יכלול הרשאות גישה למאגר המידע, נמצא כי לשתיים מהרשויות המקומיות שנבדקו, רשויות מקומיות ב' ו-ה', אין נוהל עבודה בנושא הרשאות גישה.

היעדר נוהל הרשאות גישה עלול לגרום למתן הרשאות שלא על פי הגדרת התפקיד של עובדי הרשות המקומית וכן להיעדר בקרה על הרשאות עודפות שניתנו לבעלי התפקיד.

על רשויות מקומיות ב' ו-ה' לקבוע נהלים בנושא הרשאות גישה בהתאם לתקנות הגנת הפרטיות.

תיעוד זהות המשתמשים במערכת הגבייה

בבקרות של תורת ההגנה בסייבר נאמר כי יש לוודא באופן מדגמי כי לא נעשה שימוש בחשבונות של משתמש אנושי או אפליקטיבי (לרבות חשבון מחשב) כלליים או בשמות משתמש המסגירים את התפקיד או שמשולב בהם מידע אישי.

בתקנות הגנת הפרטיות נקבע כי יש לנהל מנגנון תיעוד אוטומטי שיכלול את זהות המשתמש. תיעוד זהות המשתמשים במערכת הגבייה, כגון שימוש בשמו הפרטי של המשתמש, והימנעות מכינויים כלליים (לדוגמה "עובד כללי") יאפשרו קיום בקרה זמינה והתחקות אחר הגורם שביצע את הפעולה בפועל.

בנובמבר 2023 בחן צוות הביקורת אם יש במערכת הגבייה משתמשים שהוגדרו באמצעות שם משתמש כללי שאינו מאפשר לזהותם, כגון שם משתמש על שם מחלקה ברשות (לדוגמה ארנונה), או שם משתמש שהוא שם התפקיד של המשתמש (לדוגמה, גבייה).

בסקירת המשתמשים במערכות הגבייה של **רשויות מקומיות ב' ו-ה'** לא אותר שימוש בשמות משתמש שלא על פי שם העובד.

על אף שבבקרות תורת ההגנה בסייבר של מערך הסייבר הלאומי צוין כי לא יעשה שימוש בשמות משתמש גנריים או המסגירים את התפקיד ובתקנות הגנת הפרטיות נקבע הצורך לזהות את המשתמש, נמצא כי במערכת הגבייה של רשות מקומית ג' קיים משתמש אחד עם שם מחלקה; ברשות מקומית א' קיימים שני משתמשים עם שם מחלקה; ברשות מקומית ו' קיים משתמש "כללי"; וברשות מקומית ד' אותרו משתמשים עם שמות המחלקה שמשתמשת בהם, ושם משתמש עם שם התפקיד שלו ולא שמו הפרטי לדוגמה וטרינרית, מנהל מוקד.

שימוש בשם משתמש שאינו מאפשר לזהות את משתמשי מערכת הגבייה מקשה את האפשרות להתחקות אחר הגורם שביצע את הפעולה בפועל.

על רשויות מקומיות א', ג', ד' ו-ו' להגדיר שם משתמש המאפשר זיהוי של המשתמש שביצע את הפעולות במערכת הגבייה ולהימנע משימוש בשמות גנריים העשויים לחשוף מידע כללי בלבד בנוגע לתפקיד המשתמש.

רשות מקומית ו' מסרה בתשובתה כי ביצעה סקירת הרשאות ובהתאם לממצאי הסקירה הוסרו שמות משתמש גנריים ושמות של עובדים שסיימו את עבודתם.

ספק שירות ג' (שמספק שירותים לרשות מקומית ו') מסר בתשובתו כי ניהול המשתמשים הוא באחריות הרשות. לאחר שיחה עם מנמ"ר הרשות נחסמו הרשאות גישה למשתמש "כללי".

סקירת משתמשים תקופתית

בבקרות של תורת ההגנה בסייבר[96] בנושא בקרות גישה צוין כי על הארגון לוודא כי אחת לשנה, לכל הפחות, תיסקר רשימת המשתמשים האנושיים והתפקידים שהם ממלאים, וכי מתבצע תיקוף של הצורך בקיומם.

סקירת הרשאות תקופתית שביצעו הרשויות שנבדקו

סקירת הרשאות תקופתית במערכת הגבייה נועדה לאתר עובדים או משתמשים שעזבו את תפקידם ולא נחסמה גישתם למערכת, או עובדים שעברו לתפקיד אחר ונדרש לעדכן את הרשאותיהם וכן לאתר משתמשים במערכת הגבייה שהם בעלי הרשאות עודפות, שהם לא היו רשאים לקבל.

על אף שבתורת ההגנה בסייבר של מערך הסייבר הלאומי צוין שיש לבצע סקירה אחת לשנה של המשתמשים ותפקידם והצורך בקיומם, נמצא כי ברשויות מקומיות א'[97], ד' ו-ה' לא בוצעה סקירה עיתית של הרשאות גישה של משתמשי מערכת הגבייה. ברשויות מקומיות ב', ג' ו-ו' בוצעה סקירה כזו.

על רשויות מקומיות א', ד' ו-ה' לבצע סקירת הרשאות גישה תקופתית של משתמשים במערכת הגבייה.

רשות מקומית א' מסרה בתשובתה כי תבצע סקירת הרשאות גישה מלאות ברבעון השני של שנת 2024.

רשות מקומית ד' מסרה בתשובתה כי היא תקפיד לתעד סגירת משתמש במערכת הכספים והסרת הרשאות גישה.

---

96 בקרה 3.1 בבקרות תורת ההגנה בסייבר 2.0 גרסה 1.3.

97 לפי ממצאי תיעוד של סקירת ההרשאות שצוות הביקורת קיבל, שאינם כוללים מידע על משתמשי מערכת הגבייה.

עריכת סקרי סיכונים

בבקרות של תורת ההגנה בסייבר[98] נקבע כי יש לוודא כי הנהלת הארגון אישרה בכתב את ממצאי סקר הסיכונים ואת תוכנית העבודה לצמצום הפערים; כי יש לוודא כי סקרי הסיכונים בארגון מתבססים על מודיעין סייבר ברמות הארגון, סקטור הפעילות והמדינה; וכי יש לתת את הדעת על הסיכונים הנובעים משרשרת האספקה של הארגון.

בתקנות הגנת הפרטיות נקבע לגבי מאגר מידע שחלה עליו רמת האבטחה הגבוהה, כי בעל המאגר לענייננו הרשות המקומית, אחראי לביצוע סקר לאיתור סיכוני אבטחת מידע (להלן - סקר סיכונים); בעל מאגר המידע ידון בתוצאות סקר הסיכונים שיועברו לו, יבחן בהתאם להם את הצורך בעדכון של מסמך הגדרות המאגר או של נוהל האבטחה ויפעל לתיקון הליקויים שהתגלו במסגרת הסקר, אם התגלו; סקר סיכונים כאמור יתבצע אחת ל-18 חודשים לפחות.

מטרתו של סקר סיכונים למערכת הגבייה היא זיהוי הסיכונים שהרשות המקומית חשופה להם ולקבוע תוכנית למניעתם או הפחתתם של הסיכונים.

אם רשויות מקומיות, האחראיות למידע המנוהל במערכת הגבייה ולאבטחתו, אינן מבצעות סקרי סיכונים, יש חשש שסיכוני אבטחת מידע הנשקפים להן לא יזוהו ולא יטופלו.

עריכת סקרי סיכונים למערכות גבייה המנוהלות על ידי רשויות מקומיות

אף שבתקנות הגנת הפרטיות נקבע שיש לבצע סקר סיכונים, נמצא כי רשות מקומית ד' לא ביצעה סקר סיכונים למערכת הגבייה. כאמור, לרשות מקומית ד', אשר מנהלת באופן עצמאי את מערכת הגבייה שלה, לא היה ידוע מהי רמת האבטחה שלה, אף שאילו רמת אבטחה זו הייתה גבוהה, היא הייתה מחוייבת לבצע סקרי סיכונים כפי שנקבע בתקנות הגנת הפרטיות.

על רשות מקומית ד' (שמנהלת בעצמה את מערכת הגבייה) לבדוק אם מוטלת עליה החובה לבצע סקרי סיכונים בהתאם לרמת אבטחת המידע החלה עליה ולהוראות התקנות הרלוונטיות, ואם נמצא שמוטלת עליה חובה זו, עליה לבצע סקרים כאמור. אם רמת האבטחה ברשות מקומית ד' היא בינונית ולא גבוהה, מומלץ כי היא תבצע סקרים לזיהוי הסיכונים הנשקפים לאבטחת המידע של מערכת הגבייה שבניהולה ותקבע תוכנית למניעתם או להפחתתם.

רשות מקומית ד' מסרה בתשובתה כי כחלק מהדרישות ליציאה למכרז של מערכת כספים חדשה, יידרש הספק הזוכה לבצע סקר סיכונים אחת לשנה.

עריכת סקרי סיכונים למערכות גבייה המנוהלות על ידי ספקי שירות

כדי שרשות מקומית, שהיא הבעלים של מאגרי המידע שבמערכת הגבייה, ושמאגריה מנוהלים על ידי ספק שירות של מערכת הגבייה, תוכל לוודא כי בוצעו סקרים לאיתור סיכוני אבטחת מידע במערכת, נדרש שהיא תכלול במסגרת הסכמי ההתקשרות שלה עם ספק השירות של מערכת הגבייה, התחייבות של הספק לביצוע סקרי הסיכונים. במסגרת ההתחייבות יפורטו מתכונתם של הסקרים ואופן העברת הדיווח על תוצאות הסקרים לעיון הרשות המקומית. מידע זה יאפשר לרשות לקיים בקרה על התנהלות הספק נוכח סיכוני סייבר אפשריים.

בלוח להלן מובאים פרטים בדבר הכללה בהסכם של הרשות המקומית עם ספק השירות של מערכת הגבייה את החובה לדווח לה על ביצוע סקר סיכונים שהוא ביצע וקבלת דיווח ממנו על ביצועו בפועל.

---

98 בקרה 1.2 בבקרות תורת ההגנה בסייבר 2.0 גרסה 1.3.

לוח 16 : **הכללה בהסכם של הרשות המקומית עם ספק השירות של מערכת הגבייה את החובה לדווח לה על ביצוע סקר סיכונים וקבלת דיווח על ביצועו בפועל**

שם הרשות	האם ההסכם עם ספק השירות של מערכת הגבייה כלל התייחסות לקבלת דיווח על ביצוע סקר סיכונים ותוצאותיו על ידו?	האם ספק השירות של מערכת הגבייה ביצע סקר סיכונים בשנים 2021 - 2023?	האם הרשות המקומית קיבלה מספק השירות דיווח על ביצוע סקר סיכונים ותוצאותיו?
רשות מקומית א'	✗	✓	✗
רשות מקומית ב'	✗	✓	✗
רשות מקומית ג'	✓	✓	✗
רשות מקומית ה'	✗	✓	✗
רשות מקומית ו'	✗	✓	✗ [1]

על פי נתוני הרשויות המקומיות שנבדקו, בעיבוד משרד מבקר המדינה.
[1] ספק השירות של מערכת הגבייה מסר כי תוצאות סקר הסיכונים לא נמסרים לרשויות המקומיות מכיוון שהסקר כולל פרטים מסווגים על החברה.

מהלוח עולה כי הסכמי ההתקשרות של רשויות מקומיות א', ב', ה' ו-ו' לא כללו דרישה מחייבת לקבלת דיווח על ביצוע סקר סיכונים על ידי ספקי השירות של מערכת הגבייה. הסכם ההתקשרות של רשות מקומית ג' כלל דרישה כזו. עוד עולה כי ספקי השירות של מערכת הגבייה של הרשויות המקומיות הנבדקות ביצעו סקר סיכונים, אך תוצאות הסקר לא דווחו לרשויות המקומיות שנבדקו.

רשות מקומית ו' מסרה בתשובתה בנוגע להמלצה בדבר סקרי סיכונים למערכת הגבייה כי יישום המלצה זו מורכב מהבחינה המשפטית, הטכנית והכלכלית.

בהיות הרשות המקומית אחראית לאבטחת המידע במערכת הגבייה, על רשויות מקומיות א', ב', ה' ו-ו' להבטיח ביצוע סקרי סיכונים למערכות הגבייה המנוהלות על ידי ספקי שירות. במסגרת זו מומלץ כי הן יכללו בהסכמי ההתקשרות שלהן עם ספקי מערכות מידע דרישה בדבר חובה למסירת דיווח על ביצוע סקרי סיכונים ועל תוצאותיהם. עוד מומלץ כי רשויות מקומיות א', ב', ג', ה' ו-ו' יבחנו את תוצאות סקרי הסיכונים המבוצעים על ידי ספק השירות של מערכת הגבייה, לכשיתקבלו, על מנת לאתר חולשות אבטחה החושפות את הרשות המקומית לאירועי סייבר. מומלץ לרשות מקומית ו' למצוא את הפתרונות הנוגעים להיבטים המשפטיים, הטכניים והכלכליים שהעלתה הכרוכים בביצוע סקרי סיכונים מטעמה אצל ספק השירות של מערכת הגבייה כדי שתוכל לעמוד בדרישות המתאימות.

רשות מקומית א' מסרה בתשובתה כי היא תוודא שבהסכמים העתידיים תתווסף הדרישה שממצאי סקרי הסיכונים יוצגו במועדם. עוד מסרה כי תבחן את סקר הסיכונים הנוכחי של ספק השירות של מערכת הגבייה.

רשות מקומית ג' מסרה בתשובתה כי תתואם פגישה עם ספק השירות בנושא קבלת תוצאות סקרי הסיכונים.

רשות מקומית ה' מסרה בתשובתה כי הספק עורך סקר סיכונים תקופתי על פי התקנות ושולח לה את ממצאיו אם הוא מוצא במסגרתם ליקויי אבטחה. בנוסף, הרשות מתכוונת לפרסם בשנת 2025 מכרז חדש בו יידרש הזוכה לדווח על ביצוע סקרי סיכונים ועל תוצאותיהם.

רשות מקומית ו' מסרה בתשובתה כי נמסר לה על ידי ספק מערכת הגבייה שהוא עומד בתקנים בין-לאומיים ISO27799 ו-ISO27001 אשר מחייבים ביצוע סקרי סיכונים ומבדקי חדירות באופן תקופתי.

ספק שירות ב' מסר למשרד מבקר המדינה באפריל 2024 כי סקרי סיכונים הם פעולות פנימיות אשר הספק מבצע מדי תקופה לצורך למידה ושיפור של מערכות האבטחה. הבדיקות מבוצעות

בכלל שרתי החברה שבהם יש לקוחות רבים ולא לקוח ספציפי. אם לקוח מעוניין לקבל את החומרים הרלוונטיים כדוגמת סקר הסיכונים, הוא יכול לפנות לחברה שתספק את המידע גם אם הנושא לא צוין בהסכם ההתקשרות איתה.

ביצוע מבדקי חדירה

מבדקי חדירה הם מתקפות מתוכננות ומבוקרות על מערכת ממוחשבת שמבצע בודק כדי למצוא חולשות אבטחה ואת פוטנציאל הגישה אל המידע המאוחסן במערכת.

בבקרות של תורת ההגנה בסייבר[99] בנושא מדיניות ונוהלי עבודה לגילוי ולזיהוי של פגיעויות וחולשות ברשת הארגון נאמר שיש לבצע מבדקי חדירה למערכות בתדירות קבועה, וכי יש למנות גורם עצמאי או בלתי תלוי לביצוע המבדקים.

בתקנות הגנת הפרטיות נקבע בעניינו של מאגר מידע שחלה עליו רמת האבטחה הגבוהה, כי בעל המאגר, לעניינו הרשות המקומית, אחראי לביצוע מבדקי חדירות למערכות המאגר לבחינת עמידותן בפני סיכונים פנימיים וחיצוניים, אחת ל-18 חודשים לפחות; וכי בעל המאגר ידון בתוצאות מבדקי החדירה ויפעל לתיקון הליקויים שהתגלו, אם התגלו.

רשויות מקומיות שאינן מבצעות מבדק חדירה נחשפות לסיכונים שמקורם באי-זיהוי של חולשות אבטחת מידע או באי-טיפול בהן, וגורם לא מורשה עשוי לנצל זאת.

ביצוע מבדקי חדירה למערכות גבייה המנוהלות על ידי רשויות מקומיות

על אף שבתקנות הגנת הפרטיות נקבע שיש לבצע מבדק חדירה, נמצא כי רשות מקומית ד', אשר מנהלת באופן עצמאי את מערכת הגבייה שלה, לא ביצעה מבדק חדירה למערכת הגבייה.

על רשות מקומית ד' (שמנהלת בעצמה את מערכת הגבייה) לבדוק אם מוטלת עליה החובה לבצע מבדקי חדירה בהתאם לרמת אבטחת המידע החלה עליה ולהוראות התקנות הרלוונטיות, ואם מצאה שמחובתה לבצע את המבדקים, עליה לבצעם. אם רמת האבטחה ברשות מקומית ד' היא בינונית ולא גבוהה, מומלץ כי היא תבצע מבדקי חדירה לזיהוי חולשות אבטחה ולהערכת פוטנציאל הגישה למידע המאוחסן במערכת הגבייה.

רשות מקומית ד' מסרה בתשובתה כי תבחן אם מוטלת עליה חובה לבצע מבדקי חדירה.

ביצוע מבדקי חדירה למערכות גבייה המנוהלות על ידי ספקי שירות

מערך הסייבר נערך להסדרת הטיפול במצבים בהם מערכת הגבייה אינה מצויה בניהולה של הרשות המקומית כי אם בידי ספק שירות. כך, לפי ההנחיה שבמתודולוגיית שרשרת האספקה[100] שגיבש מערך הסייבר, על בעל מאגר (בכלל זה רשות מקומית) להגדיר מול הספק בהסכם ההתקשרות את היבטי הגנת המידע והסייבר, כמו הסמכות לבצע ביקורות סייבר באתר הספק.

בלוח להלן פרטים בדבר טיפול הרשויות המקומיות בנושא ביצוע מבדקי חדירה: הכללה בהסכם עם ספק השירות של מערכת הגבייה את הסמכת הרשויות לביצוע מבדק חדירה אצל הספק, החובה לדווח על ביצוע מבדק חדירה, ביצועו בפועל וקבלת דיווח על ביצועו.

---

99 בקרה 15.1 בבקרות תורת ההגנה בסייבר 2.0 גרסה 1.3.

100 מערך הסייבר, **הגנת סייבר שרשרת האספקה דגשים עבור צד לקוח - הרחבה מקצועית** (אוגוסט 2020), סעיף 7.2.1.

לוח 17 : **הכללה בהסכם עם ספק השירות של מערכת הגבייה את הסמכת הרשויות המקומיות לביצוע מבדק חדירה אצל הספק; חובת הספק לדווח לרשות על ביצוע מבדק חדירה; ביצועו בפועל וקבלת הדיווח מהספק על ביצועו בפועל**

שם הרשות	האם הסכם ההתקשרות כלל מתן סמכות לרשות המקומית לביצוע מבדק חדירה במערכת הגבייה המנוהלת על ידי ספק השירות?	האם ההסכם עם ספק השירות של מערכת הגבייה כלל התייחסות לקבלת דיווח על ביצוע מבדק חדירה ותוצאותיו?	האם בוצע מבדק חדירה על ידי ספק השירות של מערכת הגבייה?	האם הרשות המקומית קיבלה דיווח על ביצוע מבדק חדירה ותוצאותיו?
רשות מקומית א'	×	×	✓	×
רשות מקומית ב'	×	×	✓	×
רשות מקומית ג'	×	✓	✓	×
רשות מקומית ה'	×	×	✓	×
רשות מקומית ו'	×	×	✓	× [(1)]

על פי נתוני הרשויות המקומיות שנבדקו, בעיבוד משרד מבקר המדינה.

(1) ספק השירות של מערכת הגבייה מסר לצוות הביקורת בחודש יוני 2023 כי תוצאות המבדקים אינם מועברים לרשויות המקומיות מכיוון שהם כוללים מידע מסווג. אם רשות מקומית מבקשת לקבל מידע, יימסר לה מידע חלקי על הליקויים ברמת חומרה נמוכה בלבד על מנת שלא יזלוג החוצה מידע מסווג.

מהלוח עולה כי הרשויות המקומיות שנבדקו - רשויות מקומיות א', ב', ג', ה' ו-ו', אשר מערכת הגבייה שלהן מנוהלת בידי ספק שירות, לא כללו בהסכמי ההתקשרות עימו את הסמכתן לביצוע מבדקי חדירה במערכת הגבייה המנוהלת בידי ספק זה.

עוד עולה מהלוח כי בהסכמי ההתקשרות של רשויות מקומיות א', ב', ה' ו-ו' לא צוינה חובתו של ספק השירות של מערכת הגבייה לדווח על ביצוע מבדק חדירה ותוצאותיו. עוד עולה כי אומנם ספקי השירות של מערכת הגבייה של הרשויות המקומיות הנבדקות ביצעו מבדק חדירה, אך תוצאות מבדק החדירה לא דווחו לרשויות המקומיות.

רשות מקומית ו' מסרה בתשובתה כי נמסר לה על ידי ספק מערכת הגבייה שהוא עומד בתקנים בין-לאומיים ISO27799 ו-ISO27001 אשר מחייבים ביצוע סקרי סיכונים ומבדקי חדירות באופן תקופתי. אשר להמלצה בדבר מבדקי חדירה למערכת הגבייה, קיימת מורכבות משפטית, טכנית וכלכלית ליישם המלצה זו.

על רשויות מקומיות א', ב', ג', ה' ו-ו' לפעול בהתאם להנחיות מערך הסייבר ולכלול בהסכמי ההתקשרות עם ספק השירות של מערכת הגבייה את הסמכתן לביצוע מבדקי חדירה במערכות הגבייה המנוהלות על ידו. יודגש כי אי-הכללת הסמכה זו, לבד מהעובדה שאינה תואמת את הנחיות מערך הסייבר, גם אינה מאפשרת לרשות המקומית כבעלת המאגר לבצע מבדק חדירה בעצמה, וכך היא נתונה לביצוע מבדקים רק על ידי הספק. מומלץ לרשות מקומית ו' למצוא את הפתרונות הנוגעים להיבטים המשפטיים, הטכניים והכלכליים שהעלתה הכרוכים בביצוע מבדקי חדירה מטעמה אצל ספק השירות של מערכת הגבייה כדי לעמוד בדרישות המתאימות.

בהיות הרשות המקומית אחראית לאבטחת המידע במערכת הגבייה, על רשויות מקומיות א', ב', ה' ו-ו' להבטיח ביצוע מבדקי חדירה למערכות הגבייה המנוהלות על ידי ספקי השירות. במסגרת זו מומלץ כי הן יכללו בהסכמי ההתקשרות שלהן עם ספקי השירות של מערכת הגבייה גם התייחסות לדיווח על ביצוע מבדק חדירה ותוצאותיו. עוד מומלץ כי רשויות מקומיות א', ב', ג', ה' ו-ו' יבחנו את תוצאות מבדקי החדירה שמבצע ספק השירות של מערכת הגבייה, לכשיתקבלו, על מנת לאתר חולשות אבטחה החושפות את הרשות המקומית לאירועי סייבר.

רשות מקומית א' מסרה בתשובתה כי בהסכמים הבאים תוודא כי תתווסף דרישה של הצגת מבדקי חדירה במועדם, וכי ייבחן מבדק החדירה הנוכחי של ספק השירות של חברת הגבייה.

רשות מקומית ג' מסרה בתשובתה כי תתואם פגישה עם ספק השירות בנושא תוצאות מבדקי חדירה. כמו כן, תתווסף לנוהל שנתי הדרישה לעבור על תוצאות מבדקי החדירה.

רשות מקומית ה' מסרה בתשובתה כי הספק מבצע מבדקי חדירה אחת לשנה והוא מאפשר לרשות לראות את התוצאות אם הדבר נדרש. עוד מסרה הרשות כי אין לה תקציב לביצוע מבדקי חדירה גם במערכות הספק. בנוסף, הרשות מתכוונת לפרסם בשנת 2025 מכרז חדש בו יידרש הזוכה לדווח על ביצוע מבדקי חדירה ותוצאותיהם.

ספק שירות ב' מסר בתשובתו כי בדיקות חדירה הן פעולות פנימיות אשר הספק מבצע בתדירות קבועה לצורך למידה ושיפור מערכות האבטחה. הבדיקות מבוצעות על כלל שרתי החברה שיש בהם לקוחות רבים ולא לקוח ספציפי. אם לקוח מעוניין לקבל את החומרים הרלוונטיים הוא יכול לפנות לחברה שתספק את המידע גם אם הנושא לא צוין בהסכם ההתקשרות איתה.

דיווח ובקרה על ספקי שירות של מערכת הגבייה

נושאים נדרשים להיכלל בהסכם ההתקשרות עם ספק שירות

בתקנות הגנת הפרטיות נקבע שבעל מאגר מידע המתקשר עם גורם חיצוני לצורך קבלת שירות הכרוך במתן גישה למאגר מידע יקבע בהסכם ביניהם במפורש, בין היתר: אופן יישום החובות בתחום אבטחת המידע המוטלות על המחזיק לפי תקנות אלה, וכן הנחיות נוספות לעניין אמצעי אבטחת מידע שקבע בעל מאגר המידע, אם קבע; חובתו של הגורם החיצוני להחתים את בעלי ההרשאות שלו על התחייבות לשמור על סודיות המידע, להשתמש במידע רק לפי האמור בהסכם וליישם את אמצעי האבטחה הקבועים בהסכם; חובתו של הגורם החיצוני לדווח לבעל מאגר המידע, אחת לשנה לפחות, על אופן ביצוע חובותיו לפי תקנות אלה ולפי ההסכם, ובהתרחש אירוע אבטחה עליו להודיע על כך לבעל המאגר.

לפי ההנחיה שבמתודולוגיית שרשרת האספקה שהכין מערך הסייבר[101] מומלץ לוודא כי בכל הסכם התקשרות ובכל מכרז של הארגון ייכלל סעיף מובנה אשר מגדיר את דרישות הגנת הסייבר במסגרת ההתקשרות.

בלוח שלהלן יפורט לגבי כל אחת מהרשויות הנבדקות אם היא כללה בהסכמי ההתקשרות שלה עם ספקי השירות את הדרישות שנקבעו בתקנות הגנת הפרטיות.

לוח 18: **הדרישות שכללו הרשויות שנבדקו בהסכמי ההתקשרות עם ספקי שירות של מערכת הגבייה**

שם הרשות	אופן יישום החובות בתחום אבטחת מידע שספק השירות של מערכת הגבייה חייב בהן	החתמת בעלי ההרשאה של הספק על סעיף סודיות	דיווח אחת לשנה על אופן ביצוע חובותיו לפי תקנות הגנת הפרטיות	דיווח על אירועי אבטחה	הכללת סעיף שמגדיר את דרישות הגנת הסייבר
רשות מקומית א'	✓	✓	×	✓	✓
רשות מקומית ב'	✓	✓	×	×	✓
רשות מקומית ג'	✓	✓	✓	✓	✓

101 מערך הסייבר, **הרחבה מקצועית בנושא שרשרת אספקה צד לקוח**, סעיף 7.2.1.

שם הרשות	אופן יישום החובות בתחום אבטחת מידע שספק השירות של מערכת הגבייה חייב בהן	החתמת בעלי ההרשאה של הספק על סעיף סודיות	דיווח אחת לשנה על אופן ביצוע חובותיו לפי תקנות הגנת הפרטיות	דיווח על אירועי אבטחה	הכללת סעיף שמגדיר את דרישות הגנת הסייבר
רשות מקומית ה'	✓	✓	×	×	✓
רשות מקומית ו'	✓	✓	✓	✓	✓

הוכן בידי משרד מבקר המדינה.

בתקנות הגנת הפרטיות נקבע המידע שיש לכלול בהסכמי ההתקשרות עם ספקי השירות. נמצא כי רשויות מקומיות ג' ו-ו' כללו את המידע שנבדק על ידי הביקורת בהסכמי ההתקשרות עם ספק השירות של מערכת הגבייה. עוד נמצא כי בהסכמי ההתקשרות של רשויות מקומיות א', ב' ו-ה' עם ספקי השירות של מערכת הגבייה אין התייחסות לחובתו של ספק השירות של מערכת הגבייה לדווח אחת לשנה על אופן ביצוע חובותיו לפי תקנות הגנת הפרטיות. עוד עולה כי בהסכמים של רשויות מקומיות ב' ו-ה' אין התייחסות לדיווח של ספק השירות של מערכת הגבייה על אירועי אבטחה.

על רשויות מקומיות א', ב' ו-ה' לכלול בהסכמי ההתקשרות עם ספק השירות של מערכת הגבייה את הנושאים הנדרשים בהתאם לנקבע בתקנות הגנת הפרטיות.

רשות מקומית א' מסרה בתשובתה כי ייבדקו הדרישות של תקנות הגנת הפרטיות בהסכמי ההתקשרויות עם ספקי השירות השונים.

רשות מקומית ה' מסרה בתשובתה כי הרשות מתכוונת לפרסם בשנת 2025 מכרז חדש בו יידרש הזכיין לדווח על אירועי אבטחה.

<u>בקרה ובדיקות של הרשויות שנבדקו בנושא רמת אבטחת המידע אצל ספקי השירות</u>

תקנות הגנת הפרטיות מפרטות את הפעולות שעל בעל מאגר מידע לבצע בעת התקשרות עם גורם חיצוני הכרוך במתן גישה למאגר מידע. נקבע בין היתר כי בעל מאגר מידע ינקוט אמצעי בקרה ופיקוח בעניין עמידתו של הגורם החיצוני בהוראות ההסכם ובהוראות תקנות הגנת הפרטיות. הרשויות המקומיות, בהיותן הבעלים של מאגרי המידע שבמערכת הגבייה, אחראיות לכך שספק השירות של מערכת הגבייה יקיים רמת אבטחת מידע נאותה וימלא את הוראות תקנות הגנת הפרטיות.

על מנת להבהיר לארגונים ולספקים אילו דרישות יש לקיים כדי לעמוד ברמת הגנה נאותה בסייבר, מערך הסייבר הלאומי הכין שאלון הכולל בקרות על כמה נושאים, ובהם: הגנה על שירותי אחסון בענן, גישה מרחוק ואחסון אתרים. שאלון הספקים נועד לאפשר למקבלי השירות להעריך את הסיכונים ולעמוד על רמת ההגנה של הספק, ובד בבד הוא נועד להבהיר לספקים מה נדרש מהם, ובין היתר אילו בקרות עליהם לבצע, על מנת לעמוד ברמת הגנה נאותה[102].

לפי ההנחיה שבמתודולוגיית שרשרת האספקה[103] יש להגדיר מול הספק את היבטי הגנת המידע והסייבר החוזיים, כמו הסמכות לבצע ביקורות סייבר באתר הספק.

---

102 מתוך אתר המרשתת של מערך הסייבר הלאומי:
https://www.gov.il/he/Departments/Guides/supply_chain_guide?chapterIndex=2

103 מערך הסייבר, **הגנת סייבר שרשרת האספקה דגשים עבור צד לקוח - הרחבה מקצועית** (אוגוסט 2020), סעיף 7.2.1.

בדוח פיקוח רוחב שהכינה הרשות להגנת הפרטיות בשנת 2021[104] נמצא כי רק 21% מהרשויות המקומיות מבצעות בדיקה ממשית כדי לוודא שהספק נוקט את האמצעים הנדרשים בכדי לעמוד בהוראות. 60% מהרשויות שאלו את הספק אם הוא עומד בהוראות ההסכם והתקנות, בלי לנקוט פעולות כדי לוודא את נכונות האמירה, ו-19% מהרשויות לא נקטו פעולות כלל כדי לוודא שהספק עומד בהוראות ההסכם והתקנות.

על פי חוזה ההתקשרות של **רשויות מקומיות א', ג' ו-ו'**, הן רשאיות לבצע בדיקות אבטחה אצל ספקי השירות של מערכת הגבייה.

נמצא כי המכרז והחוזה של רשויות מקומיות ב' ו-ה' לא כללו התייחסות לכך שזכותה של הרשות המקומית לבצע בדיקות ובקרת אבטחה אצל ספק השירות של מערכת הגבייה.

מומלץ כי רשויות מקומיות ב' ו-ה' יקבעו בהסכמים עם ספקים חיצוניים בתחום של מערכות מידע כי זכותה של הרשות המקומית לבצע בקרה ובדיקות אבטחה.

רשות מקומית ה' מסרה בתשובתה כי הרשות מתכוונת לפרסם בשנת 2025 מכרז חדש בו תצויין זכותה של הרשות לבצע בקרה ובדיקות אבטחה.

נמצא כי רשויות מקומיות א', ב', ג', ה' ו-ו', המקבלות שירותי מערכת גבייה מספק שירות של מערכת גבייה, לא ביצעו בדיקות אבטחה על ספק השירות של מערכת הגבייה.

מומלץ כי רשויות מקומיות א', ב', ג', ה' ו-ו' יבצעו בדיקות אבטחת מידע אצל ספקי השירות של מערכת הגבייה על מנת לוודא כי אלה מקיימים רמת אבטחת מידע שתמנע מגורמים בלתי מורשים גישה למערכת.

רשות מקומית א' מסרה בתשובתה כי בדיקת אבטחה ונהלים אצל ספקים חיצוניים כרוכה בהוצאה ניכרת אשר אינה מתוקצבת.

רשות מקומית ג' מסרה בתשובתה בעניין זה כי תקיים סיור במתקני חוות השרתים של ספק השירות של מערכת הגבייה על מנת לבחון עמידה בדרישות האבטחה הפיזית.

רשות מקומית ה' מסרה בתשובתה בעניין בדיקות אבטחת מידע אצל ספקי השירות כי הספק מבצע מבדקי חדירה אחת לשנה והוא מאפשר לרשות לראות את התוצאות אם הדבר נדרש. עוד מסרה הרשות כי אין לה תקציב לביצוע מבדקי חדירה במערכות הספק.

מומלץ לרשויות המקומיות ג' ו-ה' כי הבדיקות אצל ספקי השירות יכללו את העמידה בדרישות אבטחת המידע בכללותן ולא רק בהיבטי האבטחה הפיזית או מבדקי החדירה. כמו כן מומלץ לרשויות המקומיות א' ו-ה' לקבוע את סדרי העדיפויות למציאת מקורות תקציביים למטרה זו, בשים לב לנזקים הפוטנציאליים שייגרמו בגינה אם יהיה כשל.

---

104 דוח פיקוח רוחב - ממצאי הליך פיקוח הרוחב בקרב רשויות מקומיות (2021), עמ' 19. במסגרת הדוח בוצעה בדיקה בקרב 70 רשויות מקומיות.

סיכום

ההתפתחות הטכנולוגית המהירה השפיעה כמעט על כל תחומי החיים של הפרט והמגזרים במשק, לרבות המגזר הציבורי, ובייחוד על הרשויות המקומיות. הרשויות המקומיות משתמשות במערכות דיגיטליות ובאתרים במרשתת המאפשרים להן לנהל את ענייניהן ולקיים אינטראקציה עם התושבים באופן מקוון, וחלקן אף מספקות שירותים מקוונים שונים המאפשרים לתושבים, בין היתר, לבצע תשלומים ובפרט לשלם ארנונה ולקבל מידע ושירותים שונים באמצעות המרשתת. נכון לסוף שנת 2021 היו בתחומן של כלל הרשויות המקומיות במדינה כ-9.4 מיליון תושבים, והכנסותיהן העצמיות הסתכמו בכ-44 מיליארדי ש"ח.

בהתאם לכך במערכות הממוחשבות של הרשויות המקומיות מצטבר מידע אישי רב על תושביהן, כמו שם, כתובת, מספר זהות, מספר טלפון, מידע רפואי, מידע בתחומי רווחה ונתונים על אמצעי התשלום שהם בוחרים לשלם באמצעותם. הדבר מחייב את הרשויות לנקוט פעולות לשמירה על המידע שנאסף בידיהן ולאבטחתו. רשויות מקומיות מתמודדות עם מגוון סיכונים, ובהם בעיות באבטחת המידע ואיומי סייבר, ומערכות המידע שלהן הפכו למוקד עניין עבור פצחנים (האקרים[105]) ופושעי סייבר. התקפות סייבר ברשויות עלולות לגרום נזקים כגון פגיעה בתשתיות טכנולוגיה, פגיעה בשלמותו ובמהימנותו של המידע השמור במערכות המידע שבשימוש הרשויות, דליפה של מידע ממאגרי המידע שברשותן וחשיפתו לגורמים שאינם מורשים לכך. נדגיש כי בעקבות מלחמת "חרבות ברזל" התגברו הסיכונים להתרחשות אירועי סייבר בכלל הגופים במדינה לרבות ברשויות המקומיות.

דוח הביקורת העלה כי אין גוף המשמש יחידה מגזרית של הרשויות המקומיות שיישא באחריות להנחיית הרשויות בעניין התמודדותן עם אירועי סייבר. עוד עלו ליקויים בתחום הגנת הפרטיות ואבטחת המידע במערכות הגבייה של הרשויות המקומיות שנבדקו, שחלקן מנוהלות ומתופעלות על ידי הרשויות וחלקן על ידי ספקי שירות חיצוניים, ובהם: ברשויות מקומיות ב', ג' ו-ה' אין מסמכי מדיניות אבטחת מידע; ברשויות המקומיות ב' ו-ה' אין נוהלי עבודה בתחום אבטחת המידע; רשויות מקומיות ב' ו-ה' לא רשמו את מאגרי מידע של מערכת הגבייה בפנקס מאגרי המידע; ברשויות מקומיות א' ו-ה' לא בוצע תרגול של שחזור נתונים ממערכת הגבייה; רשויות מקומיות א', ב', ג', ה' ו-ו', לא קיבלו דיווח על ביצוע גיבויים ושחזורים מספק השירות של מערכת הגבייה; רשויות מקומיות א', ג', ה' ו-ו' לא ביצעו בקרה על ממצאי התיעוד במנגנון הבקרה האוטומטי (לוג) של מערכת הגבייה; ברשויות מקומיות א', ב', ג', ד' ו-ה' לא מתבצע אימות דו-שלבי הכולל סיסמה ושימוש באמצעי זיהוי פיזי לפני כניסה למערכת הגבייה; ברשויות מקומיות א', ג', ד', ה' ו-ו' הוגדר זמן ניתוק אוטומטי ממערכת הגבייה החורג מהנורמה וברשות מקומית ב' לא הוגדר כלל ניתוק מהמערכת; רשויות מקומיות א', ד' ו-ה' לא ביצעו סקירת הרשאות עיתית של משתמשי מערכת הגבייה; רשות מקומית ד' לא ערכה סקר סיכונים ומבדק חדירה למערכת הגבייה שהיא מנהלת בעצמה; הסכמי ההתקשרות של רשויות מקומיות א', ב', ה' ו-ו' לא כללו דרישה מחייבת לקבלת דיווח על ביצוע סקר סיכונים על ידי ספק השירות של מערכת הגבייה; רשויות מקומיות א', ב', ג', ה' ו-ו' לא כללו בהסכמי ההתקשרות עם ספק השירות את הסמכתן לביצוע מבדקי חדירה במערכת הגבייה המנוהלת בידי הספק; רשויות מקומיות א', ב', ג', ה' ו-ו' לא ביצעו ביקורת אבטחת מידע ובדיקות אבטחה פיזית אצל ספק השירות של מערכת הגבייה.

בביקורת עלה כי רשות מקומית ד' הכינה תוכנית עבודה להתמודדות עם אירועי סייבר מקושרת תקציב וכי לרשות מקומית א' יש ביטוח סייבר.

על מנת לצמצם את החשיפה של הרשויות המקומיות לאירועי סייבר ולהבטיח שהן משתמשות ביעילות באמצעים נאותים לאבטחת המידע שבמערכות הגבייה ולשמירה על מידע זה, על משרד הפנים לפעול בשיתוף מערך הסייבר הלאומי לקביעת הגורם אשר ישמש יחידה מגזרית עבור הרשויות המקומיות. נוסף על כך על הרשויות המקומיות לפעול לתיקון הליקויים שהועלו בדוח על מנת לעמוד בדרישות שחלקן צוינו בחוק הגנת הפרטיות והתקנות שנקבע על פיו, וכן עליהן

105 כינוי למומחה בתחום פריצות מחשבים ופריצות רשתות מחשבים - בעיקר במובן השלילי.

לבצע ביקורת אבטחת מידע אצל ספקי השירות החיצוניים כדי לבחון את נאותות אמצעי אבטחת המידע.

משרד מבקר המדינה
ונציב תלונות הציבור