מערכות מידע

# אבטחת מידע של מערכות גבייה ברשויות מקומיות

# אבטחת מידע של מערכות גבייה ברשויות מקומיות

## רקע

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. ברשויות המקומיות מצטבר מידע אישי על תושביהן, כמו שם, כתובת, מספר זהות, מספר טלפון, מידע רפואי, מידע בתחומי הרווחה ונתונים על אמצעי התשלום שהם בוחרים לשלם באמצעותם. דבר זה מחייב את הרשויות המקומיות לנקוט פעולות לשמירה על המידע שנאסף בידיהן ולאבטחתו. תהליך הגבייה מבוצע במערכת הגבייה ברשויות המקומיות, המנוהלת ומתופעלת על ידי הרשויות המקומיות וספקי השירות של מערכת הגבייה, והם בעלי גישה לנתונים במערכת. מערכת הגבייה של הרשות המקומית הינה מערכת מרכזית שבאמצעותה הרשות גובה תשלומים מהתושבים, המאפשרים לה לבצע את פעילותה השוטפת. נכון לסוף שנת 2021 היו בתחומן של כלל הרשויות המקומיות במדינה כ-9.4 מיליון תושבים, והכנסותיהן העצמיות הסתכמו בכ-44 מיליארדי ש"ח. בשנת 2023, 13,040 אירועי סייבר דווחו למערך הסייבר הלאומי. בשנת 2021 עלות נזקי הסייבר[1] בעולם הייתה 6 טריליון דולר[2] ובישראל העלות הכלכלית השנתית מוערכת בלפחות 12 מיליארד ש"ח בשנה[3].

1 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 שכך.

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

3 על פי נתוני מערך הסייבר הלאומי:
https://www.gov.il/he/pages/economic_cost_of_cyber_attacks_8_ 5_2024

**נתוני מפתח**

**13,040**
אירועי סייבר דווחו למערך הסייבר הלאומי (מרכז 119[4]) בשנת 2023

**96**
אירועי סייבר התרחשו ברשויות מקומיות בתקופת מלחמת "חרבות ברזל" עד סוף דצמבר 2023

**164**
אירועי סייבר ברשויות מקומיות דווחו למערך הסייבר הלאומי בחודשים ינואר 2021 עד אוקטובר 2023

**4**
מהרשויות המקומיות שנבדקו: **רשויות מקומיות א', ב', ה'** ו-**ו'** לא הקצו תקציב ייעודי לאבטחת מידע

**2**
מהרשויות המקומיות שנבדקו: **רשויות מקומיות ב'** ו-**ה'** לא רשמו את מאגרי המידע בפנקס מאגרי המידע כנדרש בחוק הגנת הפרטיות, התשמ"א-1981

**1**
מהרשויות המקומיות שנבדקו: ב**רשות מקומית ב'** לא אויש תפקיד המנמ"ר[5]

**5**
מהרשויות המקומיות שנבדקו: **רשויות מקומיות ב', ג', ד', ה'** ו-**ו'**, אינן בעלות ביטוח סייבר

**2**
מספר הרשויות המקומיות שנבדקו שלא בוצע בהן שחזור מידע על ידי ספק שירות מערכת הגבייה שלהן - **רשויות מקומיות א'** ו-**ה'**

## פעולות הביקורת

בחודשים מאי-דצמבר 2023 בדק משרד מבקר המדינה את נושא אבטחת המידע של מערכת הגבייה ברשויות המקומיות. הבדיקה כללה את הנושאים שלהלן: הנחיה מקצועית של הרשויות המקומיות בתחום הגנת הסייבר; ניהול מאגרי מידע של מערכת הגבייה; מדיניות ונהלים בתחום אבטחת המידע; תוכנית עבודה להתמודדות עם אירועי סייבר; הסמכה לפי תקן ISO27001[6]; 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; דיווח ובקרה על ספקי שירות של מערכת הגבייה. הביקורת נעשתה בשש רשויות מקומיות: **בעיריית אור עקיבא**, **בעיריית ראשון לציון**, **בעיריית רהט**, **בעיריית רחובות**, **במועצה המקומית אבן יהודה ובמועצה האזורית עמק חפר**, וכן במשרד הפנים. בדיקות השלמה בוצעו ברשות להגנת הפרטיות ובמערך הסייבר הלאומי. השלמות

4 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. מתוך אתר המרשתת של מערך הסייבר הלאומי.

5 מנהל יחידת טכנולוגיות דיגיטליות ומידע ראשי.

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

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.

## תמונת המצב העולה מן הביקורת

- **הנחיה מקצועית של הרשויות המקומיות בתחום הגנת סייבר** - בדוח מבקר המדינה משנת 2022[7] צוין כי משרד הפנים מסר כי הוא יסכם את מתווה המשך הפעילות של היחידה המגזרית שהקים בעקבות החלטת ממשלה משנת 2015[8] להנחיית הרשויות המקומיות בתחום הגנת הסייבר, תוך תיאום עם מערך הסייבר הלאומי. נכון למועד הביקורת הנוכחית, בסוף שנת 2023, עדיין לא סוכם על מתווה בין משרד הפנים לבין מערך הסייבר הלאומי לגבי המשך הפעילות של היחידה המגזרית במשרד הפנים, והיחידה הפסיקה להנחות את מגזר הרשויות המקומיות. אי לכך אין גוף המשמש יחידה מגזרית של הרשויות המקומיות, אשר אחראי להנחות את הרשויות המקומיות במסגרת היערכותן להתמודדות עם אירועי סייבר. בהיעדר גורם רשמי לא יתאפשרו ליווי, הנחיה ובקרה בעניין ההיערכות לקרות אירוע סייבר ובעניין 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.

- **מדיניות ונהלים בתחום אבטחת המידע** - אף שמערך הסייבר הלאומי העלה ביוני 2021[9] את חשיבות הכנתו של מסמך מדיניות הגנת מידע וסייבר, כפי שנקבע גם בתקן ISO27001, 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. שתיים מהרשויות המקומיות שנבדקו, **רשויות מקומיות ב'** ו-**ה'**, לא הכינו נוהל אבטחת מידע כנדרש בתקנות הגנת הפרטיות. יתר הרשויות המקומיות שנבדקו, **רשויות מקומיות א', ג', ד'** ו-**ו'**, הכינו נוהל אבטחת מידע. היעדר מסמך מדיניות שיכלול יעדים ומטרות ברורים עלול לפגוע בהיערכות רשויות מקומיות להתמודדות עם ההיבטים הנוגעים לאבטחת מערכות מידע ולהגנה על פרטיות.

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

8 החלטת הממשלה 2443, שעסקה 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.

9 מסמך "תורת ההגנה - לנהל את הסיכון: המדריך היישומי (השלם) להגנת הסייבר של הארגון".

- **קביעת רמת האבטחה של מאגרי המידע** - לפי תקנות הגנת הפרטיות, על כל רשות מקומית להגדיר מהי רמת האבטחה החלה על כל אחד מן המאגרים שבבעלותה - בינונית או גבוהה. 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.

- **ניהול מאגרי מידע של מערכת הגבייה** - על אף שבחוק הגנת הפרטיות, התשמ"א-1981 (חוק 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. על אף שבתקנות הגנת הפרטיות (אבטחת מידע), התשע"ז-2017 (תקנות הגנת הפרטיות), נקבע כי על בעל מאגר מידע להכין "מסמך הגדרות מאגר", אין בידי **הרשויות המקומיות 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 כל הפרטים הנדרשים.

- **מינוי בעלי תפקידים** - ב**רשויות 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. ב**רשות מקומית ב'** לא אויש תפקיד המנמ"ר.

- **תוכניות עבודה להתמודדות עם אירועי סייבר** - על אף שבתורת ההגנה בסייבר של מערך הסייבר הלאומי צוין הצורך בהכנת תוכנית עבודה להתמודדות עם אירועי סייבר, ל**רשויות מקומיות ב', ג'** ו-**ה'** אין תוכנית עבודה שנתית להתמודדות עם אירועי סייבר. על אף היתרונות שבתוכנית עבודה מקושרת תקציב, עלה כי תוכניות העבודה של **רשויות מקומיות א'** ו-**ו'** להתמודדות עם אירועי סייבר, אינן מקושרות תקציב. **לרשויות מקומיות א', ב', ה'** ו-**ו'** אין תקציב ייעודי לאבטחת מידע. 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.

- **הסמכה לפי תקן ISO27001** - על אף שאין חובה ליישום תקן ISO27001, הוא יכול לסייע לרשויות המקומיות להעריך את עמידתן בדרישות אבטחת המידע שלו. **רשויות מקומיות א', ב', ג', ד', ה'** ו-**ו'** אינן מוסמכות לפי תקן ISO27001. עוד נמצא כי בהסכמים של **רשויות מקומיות א'** ו-**ב'** עם ספקי שירותי מערכת הגבייה לא נכללה דרישה ולפיה הספק יהיה

בעל הסמכה לפי תקן ISO27001. במכרזים של **רשויות מקומיות ג', ה'** ו-**ו'** נכללה דרישה שהספק יהיה מוסמך ISO27001.

- **התאוששות מאסון** - בתורת ההגנה בסייבר נקבע 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. **רשות מקומית ג'** כללה בהסכם ההתקשרות עם ספק השירות של מערכת הגבייה את חובת הדיווח על ביצוע גיבויים. עם זאת, **רשויות מקומיות א', ב', ה'** ו-**ו'** לא כללו חובה זו. **רשויות מקומיות ג'** ו-**ה'** כללו בהסכם ההתקשרות את חובת הדיווח על ביצוע תרגולי שחזורים; **רשויות מקומיות א', ב'** ו-**ו'** לא כללו בהסכם ההתקשרות חובת דיווח על תרגול שחזורים. **רשויות מקומיות א', ב', ג', ה'** ו-**ו'** לא קיבלו מספקי השירות של מערכת הגבייה דיווחים על ביצוע גיבויים ושחזורים, אף שבחלק מהרשויות, **רשויות מקומיות ג'** ו-**ה'**, נקבעה חובת דיווח של ספק השירות. בבקרות של תורת ההגנה בסייבר צוין כי הארגון יוודא כי הוא ביצע שחזור תקופתי. ב**רשויות מקומיות ב', ג', ד'** ו-**ו'** בוצע תרגול תקופתי של שחזור מידע ממערכת הגבייה. עם זאת, ב**רשויות מקומיות א'** ו-**ה'** לא בוצע תרגול כזה.

- **אבטחה פיזית של מערכת גבייה** - בתקנות הגנת הפרטיות נקבע בין היתר כי בעל מאגר מידע יכלול בנוהל אבטחת מידע את ההוראות בעניין האבטחה הפיזית והסביבתית של אתרי המאגר. ל**רשויות מקומיות ב'** ו-**ה'** אין כלל נהלים לתחום אבטחת מידע, ובכללם נהלים לאבטחה פיזית. עם זאת, ל**רשויות מקומיות א', ג', ד'** ו-**ו'** יש נהלים העוסקים בנושא האבטחה הפיזית של אתרי המאגר כנקבע בתקנות הגנת הפרטיות. **רשויות מקומיות א', ג'** ו-**ה'** לא ביצעו מאז תחילת ההתקשרות עם ספק השירות של מערכת הגבייה בדיקות אבטחה פיזית אצל הספק, על מנת לוודא כי משרדיו, שבהם מאוחסן המידע שלהם, עומדים בדרישות האבטחה הפיזית. בבדיקת חדר השרתים של **רשות מקומית ד'** נמצא כי הרשות המקומית לא נקטה אמצעים לבקרה על כניסה לאתר שבו נמצאת מערכת המידע ועל יציאה ממנו, וכי היא אף אינה מתעדת את הכניסה והיציאה; עוד נמצא כי חדר השרתים לא כלל מערכת לניטור הטמפרטורה ולהתראה על עלייתה; חלון הזכוכית שמעל דלת הכניסה לחדר השרתים מאפשר כניסה לחדר השרתים או חבלה בו; כמו כן נמצא כי בחדר השרתים אוחסנו חפצים דליקים.

- **ניטור של פעולות במערכת הגבייה והבקרה בנושא** - בתקנות הגנת הפרטיות נקבע כי בעל מאגר מידע אחראי לתיעוד כל אירוע המעורר חשש לפגיעה בשלמות המידע, לשימוש בו בלא הרשאה או לחריגה מהרשאה; במידת האפשר יבוסס התיעוד האמור על רישום אוטומטי. **רשויות מקומיות א', ג', ה'** ו-**ו'** אינן מבצעות בקרה על הפעולות שמשתמשי המערכת ביצעו במערכת הגבייה ומתועדות במנגנון הבקרה על מנת לאתר פעולות חריגות או בלתי מורשות.

- **דיווחים של רשויות מקומיות למערך הסייבר בדבר אירועי סייבר שהתרחשו אצלן** - 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. **ברשות מקומית א'** התרחשו שני ניסיונות לדרישת כופר, אולם הרשות לא דיווחה עליהן למערך הסייבר הלאומי, ולטענתה היא התמודדה עם האירועים באופן עצמאי.

- **ביטוח סייבר -** ביטוח סייבר כולל כיסוי של הוצאות בעקבות אירוע סייבר, ומכאן חשיבותו להתמודדות בקרות אירוע. מלבד **רשות מקומית א'** שיש לה ביטוח סייבר בהיקף של 2 מיליון דולר, **לרשויות מקומיות ב', ג', ד', ה'** ו-**ו'** אין ביטוח סייבר, כך שהן עלולות להידרש לשאת בכלל ההוצאות הכרוכות בהתמודדות עם אירוע הסייבר וההתאוששות ממנו, כגון הקמה מחדש של כל תשתיות המחשוב.

- **זיהוי ואימות של משתמשים במערכת הגבייה -** בתקנות הגנת הפרטיות נקבע כי הזיהוי יתבסס, במידת האפשר, על אמצעי פיזי הנתון לשליטתו הבלעדית של המורשה. **ברשות מקומית ו'** הגישה למערכת הגבייה מבוצעת באמצעות סיסמה וקוד אימות מהטלפון הנייד בהתאם לנדרש בתקנות הגנת הפרטיות. **ברשויות מקומיות א', ג'** ו-**ה'** לא מתבצע אימות דו-שלבי הכולל סיסמה ואמצעי פיזי כנדרש הן בהסכם ההתקשרות עם ספק השירות והן בתקנות הגנת הפרטיות. **ברשויות מקומיות ב'** ו-**ד'** לא מתבצע אימות דו-שלבי הכולל סיסמה ואמצעי פיזי כנדרש בתקנות הגנת הפרטיות, והדרישה לכך לא נכללה בהסכם. מדיניות הסיסמאות של **רשויות מקומיות א', ג', ה'** ו-**ו'** כוללת שמונה תווים, ושל **רשות מקומית ב'** - שבעה תווים, פחות ממספר התווים המזערי שהוגדר (10 תווים) בבקרות שקבע מערך הסייבר הלאומי. ברשויות אלה מדיניות הסיסמאות של מערכת הגבייה כוללת דרישה לקביעת סיסמה מורכבת. עם זאת, במערכת הגבייה של **רשות מקומית ד'** אורך הסיסמה הוא ארבעה תווים, ומדיניות הסיסמאות של מערכת הגבייה לא כוללת דרישה לקביעת סיסמה מורכבת.

- **ניהול הרשאות גישה למערכת הגבייה -** 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. בסקירת המשתמשים במערכות הגבייה של **רשויות מקומיות ב'** ו-**ה'** לא אותר שימוש בשמות משתמש שלא על פי שם העובד. בסקירת המשתמשים של **רשויות מקומיות א', ג', ד'** ו-**ו'** אותרו שמות משתמשים כלליים במערכת הגבייה (כגון שם המחלקה) שאינם מאפשרים לזהות את משתמשי מערכת הגבייה ומקשים את האפשרות להתחקות אחר הגורם שביצע את הפעולה בפועל; על אף שבתורת ההגנה בסייבר של מערך הסייבר הלאומי צוין שיש לבצע סקירה אחת לשנה של המשתמשים ותפקידם והצורך בקיומם, **ברשויות מקומיות א', ד'** ו-**ה'** לא בוצעה סקירה עיתית של הרשאות גישה של משתמשי מערכת הגבייה, על מנת לאתר עובדים או משתמשים שעזבו או שינו תפקיד וגישתם לא נחסמה. **ברשויות מקומיות ב', ג'** ו-**ו'** בוצעה סקירה כזו.

- **סקרי סיכונים -** מטרתו של סקר סיכונים למערכת הגבייה היא זיהוי הסיכונים שהרשות המקומית חשופה להם ולקבוע תוכנית למניעתם או הפחתתם של הסיכונים. אף שבתקנות הגנת הפרטיות נקבע שיש לבצע סקר סיכונים ומבדק חדירה, **רשות מקומית ד'**, אשר מנהלת באופן עצמאי את מערכת הגבייה שלה, לא ביצעה סקר סיכונים למערכת הגבייה. 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. הסכם ההתקשרות של **רשות מקומית ג'** כלל דרישה כזו. ספקי השירות של מערכת הגבייה של **רשויות מקומיות א', ב', ג', ה'** ו-**ו'** ביצעו סקר סיכונים, אך תוצאות הסקר לא דווחו לרשויות המקומיות שנבדקו.

**מבדקי חדירה** - 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. בהנחיות מערך הסייבר נאמר כי על בעל מאגר (בכלל זה רשות מקומית) להגדיר מול הספק בהסכם ההתקשרות את היבטי הגנת המידע והסייבר, כמו הסמכות לבצע ביקורות סייבר באתר הספק. **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 הספק שעימו התקשרו. **רשויות מקומיות א', ב', ה'** ו-**ו'** לא צוינה חובתו של ספק השירות של מערכת הגבייה לדווח על ביצוע מבדק חדירה ועל תוצאותיו. עוד עולה כי אומנם ספקי השירות של מערכת הגבייה של **רשויות מקומיות א', ב', ג', ה'** ו-**ו'** ביצעו מבדק חדירה, אך תוצאות מבדק החדירה לא דווחו לרשויות המקומיות.

**בקרה ובדיקות של הרשויות שנבדקו על רמת אבטחת המידע אצל ספקי השירות** - בדוח פיקוח רוחב שהכינה הרשות להגנת הפרטיות בשנת 2021 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. **רשויות מקומיות א', ב', ג', ה'** ו-**ו'**, המקבלות שירותי מערכת גבייה מספקי שירות, לא ביצעו בקרה על רמת אבטחת המידע אצל ספק השירות של מערכת הגבייה.

**תוכניות עבודה להתמודדות עם אירועי סייבר - רשות מקומית ד'** הכינה תוכנית עבודה מקושרת תקציב.

**ביטוח סייבר - לרשות מקומית א'** יש ביטוח סייבר.

## עיקרי המלצות הביקורת

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 יישום ההנחיות, כפי שהתחייב בדוח הביקורת משנת 2022.

מומלץ ל**רשויות מקומיות ב'** ו-**ה'** להכין מסמך מדיניות אבטחת מידע ולהגישו לאישור הנהלת הרשות המקומית, כדי שישמש בסיס לכתיבת נוהלי אבטחת מידע. כמו כן, מומלץ ל**רשות מקומית ג'** להשלים את הכנת מסמך המדיניות בנושא אבטחת מידע ולהגישו לאישור הנהלת הרשות המקומית. 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. עוד 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 האמור בתקנה 4 בדבר קביעת נוהל אבטחת מידע.

- 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.

- על **רשויות מקומיות ב'** ו-**ה'** לרשום את מאגרי המידע של מערכת הגבייה שלהן בפנקס מאגרי המידע בהתאם להוראות חוק הגנת הפרטיות. על **רשויות מקומיות ב', ג'** ו-**ה'** להכין מסמך הגדרות מאגר מידע עבור מערכת הגבייה, שיכלול את כלל המידע הנדרש בהתאם לתקנות הגנת הפרטיות. על **רשות מקומית א'** לכלול במסמך הגדרות המאגר את כל המידע הנדרש בתקנות הגנת הפרטיות.

- על **רשויות מקומיות א'** ו-**ה'** לפעול לכך שאת תפקיד ממונה אבטחת מידע ואת תפקיד מנמ"ר הרשות ימלאו נושאי משרה שונים, וזאת על מנת לקיים את ההוראות בתקנות הגנת הפרטיות. כמו כן, מומלץ כי **רשות מקומית ב'** תפעל לאייש את תפקיד המנמ"ר.

- מומלץ כי **רשויות מקומיות א', ב', ג', ה'** ו-**ו'** יכינו תוכנית עבודה שנתית מקושרת תקציב להתמודדות עם אירועי סייבר. בנוסף, מומלץ ל**רשויות מקומיות א', ב', ה'** ו-**ו'** לייחד סעיף תקציב ייעודי לנושא אבטחת מידע. על אף שאין חובה רגולטורית ליישום תקן ISO27001 ועל אף הצורך במשאבים הנדרשים ליישום התקן, מומלץ כי הרשויות המקומיות יפעלו לקבל הסמכה לפי התקן, וזאת בשל חשיבות נושא אבטחת המידע ברשות המקומית. כמו כן, מומלץ כי **רשויות מקומיות א'** ו-**ב'** יכללו דרישת חובה להסמכת ISO27001 במכרזים ובהסכמים שהן עורכות עם ספקי שירות של מערכות גבייה.

- מומלץ לכלול בהסכמי ההתקשרות עם ספקי שירות של מערכות גבייה חובת דיווח של ספק השירות של מערכת הגבייה על ביצוע גיבויים ותרגולי שחזורים. עוד מומלץ כי **רשויות מקומיות א', ב', ג', ה'** ו-**ו'** יפעלו לקבלת דיווחים תקופתיים על ביצוע גיבויים ותרגולי שחזורים. כמו כן, מומלץ כי **רשויות מקומיות א'** ו-**ה'** יוודאו כי ספק השירות של מערכת הגבייה יבצע תרגולי שחזורים לפחות אחת לשנה, בהתאם להמלצות של מערך הסייבר הלאומי, וכי הן מקבלות דיווח על כך. כמו כן, מומלץ כי **רשות מקומית ד'** תבצע תרגול של שחזור נתוני מערכת הגבייה לפחות אחת לשנה.

- על **רשויות מקומיות ב'** ו-**ה'** להכין נהלים בנושא אבטחת מידע פיזית בהתאם לתקנות הגנת הפרטיות. על **רשויות מקומיות א', ג'** ו-**ה'**, כבעלים של מאגרי המידע שבמערכת הגבייה, להבטיח כי מאגר המידע עומד בדרישות האבטחה הפיזית, ולשם כך עליהן לבחון את הבקרות הפיזיות אצל ספק השירות על מנת לוודא כי הוא עומד בדרישות אבטחת המידע. על **רשות מקומית ד'** לבחון את אבטחת האתר שבו מאוחסנים שרתי מערכת הגבייה שלה ולהפעיל בקרה על הנכנסים אליו והיוצאים ממנו, וכמו כן עליה להתקין בחדר השרתים מערכת להתראה על עליית טמפרטורה, לחסום את הפתח בקיר חדר השרתים ולפנות ממנו חפצים דליקים.

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

- 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.

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

- על **רשויות מקומיות א', ב', ג', ד'** ו-**ה'** לאמץ שימוש באמצעי פיזי, נוסף על סיסמה, לצורך זיהוי משתמשים וקבלת גישה למערכת הגבייה. מומלץ כי **רשויות מקומיות א', ב', ג', ד', ה'** ו-**ו'** יקבעו אורך סיסמה מינימלי של עשרה תווים בהתאם לבקרות של מערך הסייבר הלאומי. כמו כן, מומלץ ש**רשות מקומית ד'** תגדיר דרישה לגבי מורכבות הסיסמה.

- 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. כמו כן, על **רשויות מקומיות א', ד'** ו-**ה'** לבצע סקירת הרשאות גישה תקופתית למשתמשים במערכת הגבייה.

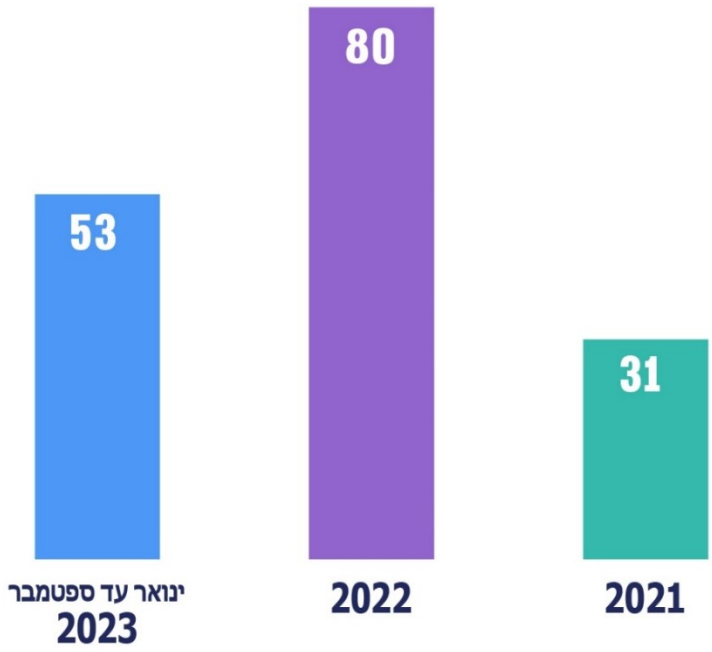
- על **רשות מקומית ד'** (שמנהלת בעצמה את מערכת הגבייה) לבדוק אם מוטלת עליה החובה לבצע סקרי סיכונים ומבדקי חדירה בהתאם לרמת אבטחת המידע החלה עליה ולהוראות התקנות הרלוונטיות, ואם נמצא שמוטלת עליה חובה זו, עליה לבצע סקרים ומבדקים כאמור. אם רמת האבטחה ב**רשות מקומית ד'** היא בינונית ולא גבוהה, מומלץ כי היא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

- 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. 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 ועל תוצאותיו. עוד מומלץ כי **רשויות מקומיות**

**א', ב', ג', ה'** ו-**ו'** יבחנו את תוצאות מבדקי החדירה שמבצע 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 הם מקיימים רמת אבטחת מידע שתמנע מגורמים שאינם מורשים לכך גישה למערכת.

**אירועי סייבר ברשויות המקומיות, ינואר 2021 - ספטמבר 2023**




על פי נתוני מערך הסייבר הלאומי, בעיבוד משרד מבקר המדינה.

# סיכום

ברשויות המקומיות מצטבר מידע אישי רב על תושביהן, ודבר זה מחייב אותן לנקוט פעולות לשמירה על המידע שנאסף בידיהן ולאבטחתו. רשויות מקומיות מתמודדות עם מגוון סיכונים, עם בעיות חוסן באבטחת המידע ועם איומי סייבר. התקפות סייבר ברשויות המקומיות עלולות לגרום נזקים להן ולכלל הציבור. יודגש כי בעקבות מלחמת "חרבות ברזל" התגברו הסיכונים להתרחשות אירועי סייבר בכלל הגופים במדינה לרבות ברשויות המקומיות.

ממצאי דוח הביקורת מעלים ליקויים ביישום הדרישות שחלקן מופיע בחוק הגנת הפרטיות, בתקנות על פיו ובהנחיות מערך הסייבר הלאומי, וליקויים אלה עלולים לחשוף את הרשויות המקומיות לאירועי סייבר, ובהם: היעדר גוף המשמש יחידה מגזרית של הרשויות המקומיות המנחה אותן מהבחינה המקצועית בהיבטי הגנת הסייבר; ליקויים בניהול מאגר המידע של מערכת הגבייה על ידי הרשויות המקומיות. כמו כן נמצא כי הרשויות המקומיות לא ביצעו סקרי סיכונים ומבדקי חדירה למערכת הגבייה ואינן מבצעות בקרה שוטפת על ספקי השירות המחזיקים במאגרי המידע שלהן וכן לא קיבלו מספקי השירות דיווחים תקופתיים על מידת עמידתם בחובותיהם לפי תקנות הגנת הפרטיות.

על מנת להפחית את החשיפה של הרשויות המקומיות לאירועי סייבר ולהבטיח שימוש יעיל באמצעי אבטחת מידע נאותים במערכות הגבייה שלהן ושמירה על המידע שבהם, על משרד הפנים ומערך הסייבר הלאומי לפעול לקביעת הגורם אשר ישמש יחידה מגזרית עבור הרשויות המקומיות. נוסף על כך על הרשויות המקומיות לפעול לתיקון הליקויים שהועלו בדוח על מנת לשפר את יכולות השלטון המקומי להתמודד עם איום התקפות סייבר והשפעותיו, ובמסגרת זו לבצע ביקורת אבטחת מידע אצל ספקי השירות החיצוניים כדי לבחון את נאותות אמצעי אבטחת המידע שהם צריכים לנקוט.