מבקר המדינה | דוח על הביקורת בשלטון המקומי | התשפ"ב-2022

ביקורת מערכות מידע

# ניהול מערכות מידע ברשויות המקומיות

# ניהול מערכות מידע ברשויות המקומיות

## רקע

השימוש במערכות מידע לניהול ענייני הרשויות המקומיות הפך עם השנים לצורך בסיסי ומחויב המציאות. בכלל זה, בין היתר, נעשה שימוש במאגרי מידע הכוללים נתונים אישיים על התושבים ועל הגורמים המקיימים קשר עם הרשויות במגוון תחומים. ברשויות המקומיות מצטבר מידע אישי על תושביהן, כמו שם, כתובת, מספר זהות, מספר טלפון, מידע רפואי, מידע בתחומי רווחה ונתונים על אמצעי התשלום שהם בוחרים לשלם באמצעותם וכן מידע בלתי מסונן כמו לוחיות רישוי, תווי פנים, נתוני מיקום והרגלי תנועה. רשויות מקומיות מתמודדות עם מגוון סיכונים, ובכלל זה עם פרצות במערך אבטחת המידע ועם איומי סייבר, ומערכות המידע שלהן הפכו למוקד של עניין עבור פצחנים (האקרים) ופושעי סייבר. מכאן נובע הצורך לשמור על מערכות המידע למניעת פגיעה ברציפות התפקודית של הרשויות המקומיות במתן שירותים וכן למניעת דליפה של נתונים ומידע ממאגרי המידע שברשותן ולמניעת חשיפתם לגורמים שאינם מורשים לכך.

**נתוני מפתח**

**67%**
שיעור הרשויות המקומיות (87 מ-130) שקיבלו ציון חוסן קיברנטי נמוך מ-60 במבדק שביצע אגף הסייבר במשרד הפנים

**61%**
שיעור הרשויות המקומיות שאין להן תוכנית להתאוששות מאסון בהתרחש אירוע סייבר - BCP/DRP (36 מ-59 הרשויות שהשיבו על השאלה בעניין זה בשאלון)

**108**
מספר הפניות המצטבר שהתקבלו מ-32 רשויות מקומיות בשנים 2019 - 2021 במרכז לניהול אירועי סייבר (של מערך הסייבר הלאומי)

**41%**
שיעור הרשויות המקומיות שחוו אירועי סייבר (בפועל או ניסיונות שלא צלחו) בשנים 2019 - 2021 (24 מ-59 הרשויות שהשיבו על השאלה בשאלון)

**34%**
שיעור הרשויות המקומיות שאין להן ממונה או מנהל אבטחת מידע (21 מ-61 הרשויות שהשיבו על השאלה)

**64%**
שיעור הרשויות המקומיות שאין להן נוהל אבטחת מידע (37 מ-58 הרשויות שהשיבו על השאלה בעניין זה בשאלון)

**18%**
שיעור הרשויות המקומיות שלא מינו מנהל מערכות מידע ראשי (מנמ"ר) (11 מ-61 הרשויות שהשיבו על השאלון)

**49%**
שיעור הרשויות המקומיות שלא ביצעו מבדקי חדירה בשנים 2019 - 2021 (30 מ-61 הרשויות שהשיבו לשאלון)

# פעולות הביקורת

בחודשים יולי-נובמבר 2021 בדק משרד מבקר המדינה את נושא ניהול מערכות המידע ברשויות המקומיות. הבדיקה נעשתה בשמונה רשויות מקומיות שנבחרו, תוך מתן ביטוי למחוזות המינהליים שבהם שוכנות הרשויות; למעמדן המוניציפלי; ולמדד החברתי-כלכלי שאליו הן משויכות; למדד הפריפריאליות שאליו הן משויכות; למגזר שאליו רוב תושביהן משתייכים; ולמספר התושבים המתגוררים בתחום שיפוטן: בחמש עיריות - **חיפה, יוקנעם, נתיבות, ראש העין ושפרעם**; בשתי מועצות מקומיות - **גדרה ועין מאהל**; ובמועצה האזורית **מטה בנימין** (להלן - הרשויות שנבדקו). בדיקות השלמה נעשו במשרד הפנים - במינהל שירותי חירום ובמפעם עמק יזרעאל, במרכז השלטון המקומי ובמערך הסייבר הלאומי שבמשרד ראש הממשלה (להלן - מערך הסייבר). כמו כן במסגרת הבדיקה נשלחו שאלונים ל-63 רשויות מקומיות, ו-61 (97%) מהרשויות שנדגמו השיבו עליהם.

# תמונת המצב העולה מן הביקורת

- **מבדקים שביצע אגף הסייבר במשרד הפנים** - עלה כי אגף הסייבר במשרד הפנים השלים מבדק בסיסי ב-130 מ-257 רשויות, נכון לאוגוסט 2021. עוד עלה כי 87 (כ-67%) מ-130 הרשויות קיבלו ציון הנמוך מ-60, ואילו רק 11 (כ-8%) מהרשויות קיבלו ציון הגבוה מ-80, והציון הממוצע היה 48. עולה אפוא מהנתונים כי רמת אבטחת המידע והמוכנות של מרבית הרשויות המקומיות (67% מהן) לאיומי סייבר היא נמוכה, וכי הרשויות השונות שבחן משרד הפנים נבדלות זו מזו במידה רבה מבחינת מוכנותן לאירועי סייבר.

- **דיווחים למרכז הארצי לניהול אירועי סייבר (של מערך הסייבר)** - מנתוני מערך הסייבר בנוגע לפניות של רשויות מקומיות למרכז לניהול אירועי סייבר עלה כי בשנת 2019 פנו למרכז 14 רשויות ב-32 פניות, בשנת 2020 פנו למרכז 25 רשויות ב-40 פניות, ובשנת 2021 פנו למרכז 19 רשויות ב-36 פניות. בסך הכול בשנים 2019 - 2021 פנו במצטבר 32 רשויות מקומיות (מתוך 257) ב-108 פניות.

- **הגדרת תחומי האחריות בין משרד הפנים למערך הסייבר** - משרד הפנים ומערך הסייבר לא השלימו את הסדרת הסמכויות החסרות בכל הנוגע לרגולציה ולהנחיה מקצועית של הרשויות המקומיות בתחומי אבטחת מידע והגנת הפרטיות. בתוך כך, משרד הפנים לא פעל להכנת נוהל שמטרתו להנחות את הרשויות המקומיות כיצד לפעול בנושא. כפועל יוצא, נכון למועד סיום הביקורת אין לרשויות המקומיות גורם מאסדר בתחום אבטחת המידע והגנה מאיומי סייבר, ומזה שנים הרשויות המקומיות פועלות ללא הנחיות מקצועיות ברורות בנושא וכל רשות מקומית פועלת בעניין לפי ראות עיניה.

- **תוכניות עבודה בנושא מערכות מידע** - הרשויות המקומיות **גדרה**, **יוקנעם**, **מטה בנימין**, **נתיבות**, **עין מאהל ושפרעם** לא הכינו תוכניות עבודה אסטרטגיות רב-שנתיות בנושא מערכות המידע, ולא הכינו תוכניות עבודה שנתיות מקושרות תקציב בהתאם ליעדי הרשות המקומית לטווח הארוך. עוד נמצא כי עיריות **חיפה וראש העין**, אשר גיבשו תוכניות אסטרטגיות בנושא מערכות המידע, לא תקצבו אותן ומשכך התוכניות לא יושמו.

- **מינוי ממונה אבטחת מידע** - 21 (כ-34%) מ-61 הרשויות שענו על שאלה בעניין זה בשאלון אינן מעסיקות ממונה אבטחת מידע כנדרש, ומבין הרשויות שנבדקו למועצות המקומיות **גדרה** ו**עין מאהל** אין ממונה אבטחת מידע.

- **נוהל אבטחת מידע** - מבין הרשויות שנבדקו, רשויות א', ג' ו-ה' לא הכינו נוהל אבטחת מידע כנדרש בתקנות אבטחת המידע. רשויות ד', ו' ו-ח' הכינו רק טיוטה של הנוהל, ובמועד סיום הביקורת היא לא אושרה.

- **נוהל גיבויים ויישומו** - נמצא כי מבין הרשויות שנבדקו, לרשויות א', ג', ד', ה' ו-ז' אין נוהל גיבויים כנדרש. לרשויות ו' ו-ח' יש טיוטות נוהל גיבויים שטרם אושרו. ברשויות ג', ד' ו-ח' לא נמצאו רישומים המתעדים היסטוריית גיבויים תקינה ברשות. **ניהול הרשאות גישה** - לרשויות ג', ד' ו-ה' אין כללים כתובים בנוגע למתן הרשאות גישה או לביטולן. לרשות א'

יש נוהל שנכנס לתוקף ביוני 2021, ולרשויות ו' ו-ח' יש טיוטות נוהל בנושא מיולי 2020 ומיולי 2021 בהתאמה, שלא אושרו במועד סיום הביקורת.

**תוכנית להתאוששות מאסון בהתרחש אירוע סייבר** - 36 (כ-61%) מהרשויות המקומיות שהשיבו על השאלה בנושא קיום תוכנית להתאוששות מאסון ציינו כי אין ברשות מנגנון מוסדר להמשכיות של פעילות המחשוב ברשות בהתרחש אירוע סייבר. הרשויות שנבדקו - א', ב', ג', ד', ה', ז' ו-ח' - לא הכינו כלל תוכנית להתאוששות מאסון. רשות ו' הכינה טיוטת תוכנית כאמור, ובמועד סיום הביקורת היא טרם אושרה.

**סקרי סיכונים ומבדקי חדירה או ביקורות תקופתיות** - רשות ה' ביצעה סקר לאיתור סיכוני אבטחת מידע (להלן - סקר סיכונים) בשנת 2020 ולא ביצעה מבדקי חדירה במערכות המאגר (להלן מבדקי חדירה). רשות ו' ביצעה סקר סיכונים בשנת 2019 ולא ביצעה מבדקי חדירה. רשויות ג',ד' ו-ח', שאינן מחויבות בביצוע מבדקי חדירה, לא ביצעו כלל סקרי סיכונים או ביקורות תקופתיות. עוד הועלה כי רשות א' לא ביצעה בעצמה מבדק חדירה או סקר סיכונים אלא הסתמכה בעניין זה על החברה הפרטית המספקת לרשות שירותי מחשוב.

יש לציין לחיוב את רשויות ב', ו' ו-ז' על שביצעו מבדקי חדירה או סקרי סיכונים למיפוי הסיכונים ברשות בשנים 2019 - 2021.

## עיקרי המלצות הביקורת

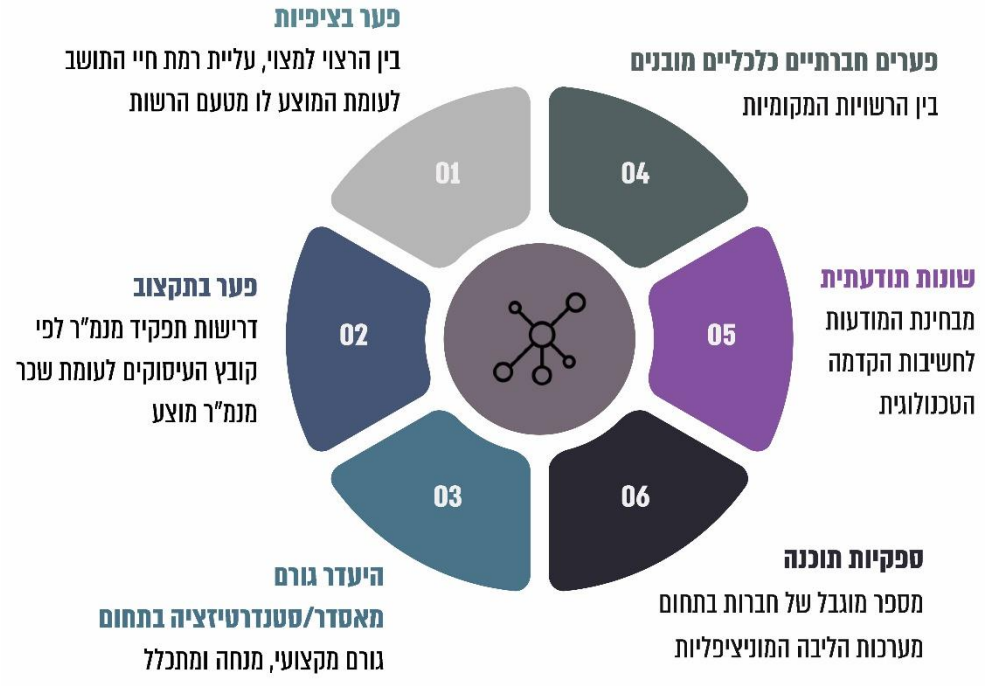
מומלץ כי משרד הפנים ומערך הסייבר יפעלו במשותף, תוך התחשבות בייחודיות של מגזר השלטון המקומי, לחלוקת הסמכויות ביניהם לשם יישום החלטת הממשלה 2443 בנוגע למגזר זה, באופן שיוסמך רגולטור מוביל להסדרת ההיערכות של הרשויות המקומיות לאיומי סייבר ולקביעת נהלים מתאימים שיסדירו את פעילות הרשויות המקומיות בנושא. עוד מומלץ למערך הסייבר לפעול בשיתוף אגף הסייבר במשרד הפנים להעלאת המודעות של הרשויות המקומיות לחשיבות הדיווח למרכז לניהול אירועי סייבר על אירועי סייבר שהן נחשפו להם ולאפשרות ההיוועצות עם מערך הסייבר.

על הרשויות המקומיות **גדרה**, **יוקנעם**, **מטה בנימין**, **נתיבות**, **עין מאהל ושפרעם** להכין תוכנית עבודה אסטרטגית שתשמש בסיס לתוכניות עבודה שנתיות ולהגישה להנהלת הרשות כדי שתדון בה, תבחן אם ניתן ליישמה במסגרת תקציבה ותפעל בהתאם ליישומה.

לאור החובה המוטלת על הרשויות המקומיות לאייש את תפקיד ממונה אבטחת המידע ברשות, על כלל הרשויות המקומיות, שלא מינו ממונה כאמור, וביניהן הרשויות המקומיות **גדרה ועין מאהל**, לפעול לאיוש התפקיד. מומלץ כי משרד הפנים ינחה את הרשויות שלא מינו ממונה לעשות כן, וכן ישלים, בשיתוף מרכז השלטון המקומי, את הגדרת התפקיד של מנהל מערכות המידע הראשי (מנמ"ר) ואת תנאי העסקתו.

- על רשויות א', ג', ו-ה' להכין נוהל אבטחת מידע כנדרש. כמו כן על הרשות המקומית א' לפעול לאישור נוהל אבטחת המידע של חברה ב' ובמידת הצורך להתאימו לצורכי הרשות. על רשויות ד', ו' ו-ח' להשלים את אישור הנוהל ולציין בו את מועד כניסתו לתוקף.
- על רשויות א', ג', ד', ה', ו', ז' ו-ח' לקבוע נוהל גיבויים תקף ולבצע גיבויים על פי הנקבע בו.
- על רשויות ג', ד' ו-ה' לקבוע כללים למתן הרשאות ולביטולן, הן לעובדים הנקלטים ברשות והן לעובדים העוזבים אותה. על רשויות ו' ו-ח' לאשר את טיוטות הנוהל שלהן ולפעול על פיו.
- נוכח החשיבות של הכנת תוכנית להתאוששות מאסון, משרד מבקר המדינה ממליץ לכלל הרשויות המקומיות, ובהן הרשויות שנבדקו (רשויות א', ב', ג', ד', ה', ז' ו-ח'), לפעול להכנת תוכנית להתאוששות מאסון המתאימה לצורכי הרשות, בהתאם להנחיות מערך הסייבר. מומלץ כי רשות ו' תפעל להשלמת הכנתה של התוכנית להתאוששות מאסון.
- על רשויות ג', ד' ו-ח' לבצע ביקורות תקופתיות, רצוי במסגרת סקרי סיכונים, על מנת למפות ולאתר את סיכוני אבטחת המידע ברשות ולהיערך בהתאם לממצאים שיועלו. עוד מומלץ כי הרשויות ג', ד', ו' ו-ח' יבצעו מבדקי חדירה גם מאגרי המידע שלהן כפופים לרמת אבטחה בינונית.

**אתגרים עיקריים בתחום ניהול מערכות המידע ברשויות המקומיות**




התרשים בעיבוד משרד מבקר המדינה.

## סיכום

השימוש במערכות מידע לניהול ענייני הרשויות המקומיות הפך עם השנים לצורך בסיסי ומחויב המציאות, והוא חשוף לאיומי סייבר. נוסף על כך, במאגרי המידע של הרשויות המקומיות שמורים, בין היתר, נתונים אישיים על התושבים ועל הגורמים הבאים בקשר עם הרשויות במגוון תחומים, דבר המחייב נקיטת אמצעים לאבטחת המאגרים, גם לשם הגנה על הפרטיות.

ברשויות המקומיות שנבדקו הועלו ליקויים שונים בתחום הגנת הסייבר ואבטחת המידע, שמקורם, בין היתר, בהיעדר אסטרטגיה והכוונה מצד הגורמים האחראים בתחום. בשל חשיבות הנושא מומלץ כי אגף הסייבר במשרד הפנים בשיתוף מערך הסייבר הלאומי יפעלו להנחיית הרשויות המקומיות באופן שיבהיר מהן החובות החלות עליהן וכיצד ניתן לפעול באופן המיטבי לשיפור אבטחת המידע בהן. עוד מומלץ כי הרשויות המקומיות יפעלו באמצעות הכלים העומדים

לרשותן לקביעת אסטרטגיה רשותית לניהול מערכות המידע שברשותן ולחיזוק אבטחת המידע בהן. על כלל הרשויות המקומיות לנקוט את כל האמצעים העומדים לרשותן לניהול מיטבי של מערכות המידע שלהן ולהגברת מוכנותן להגנה על המידע הרגיש הנמצא בבעלותן ולמניעת פגיעה ברציפות התפקודית שלהן.

# מבוא

השלטון המקומי בישראל מורכב בעיקרו ממערך של 257 רשויות מקומיות. לכל רשות מקומית יש תחום שיפוט, שקבע שר הפנים, ובו היא רשאית להחיל את סמכויותיה. הרשויות המקומיות עוסקות במגוון רחב של תחומים - חינוך, רווחה, בריאות, תברואה, תכנון ובנייה, איכות הסביבה, תחבורה ותרבות - המשפיעים על ענייני היום-יום של תושביהן ועל רווחתם.

לרשויות המקומיות הוקנתה עצמאות לניהול ענייניהן, כמפורט בפקודת העיריות [נוסח חדש] (להלן - פקודת העיריות) ובפקודת המועצות המקומיות [נוסח חדש][1], המונות את הסמכויות הנרחבות שבידיהן. בד בבד הטיל המחוקק על השלטון המרכזי ככלל, ועל משרד הפנים כמאסדר של השלטון המקומי בפרט, את האחריות לגיבושה ולביצועה של מדיניות לאומית בשלטון המקומי. המשרד גם מופקד על ביצוע פיקוח על פעולות הרשויות המקומיות, על הכוונתן ועל הסדרת יחסי הגומלין ביניהן[2].

ההתפתחות הטכנולוגית המהירה בכל הקשור לשימוש במרשתת (להלן - אינטרנט), להיצע המכשירים הניידים, לאפליקציות ולאינטרנט של הדברים (IoT)[3] השפיעה כמעט על כל תחומי החיים של הפרט והמגזרים במשק, לרבות המגזר הציבורי, ובפרט על הרשויות המקומיות. הרשויות המקומיות משתמשות באתרי אינטרנט המאפשרים לתושבים לקיים אינטראקציה עימן באופן מקוון, חלקן אף מספקות שירותים מקוונים שונים המאפשרים לתושבים, בין היתר, לשלם ארנונה, לקבל מידע ושירותים שונים באמצעות האינטרנט. חשוב לציין שהרשויות המקומיות נבדלות זו מזו בהרכבי האוכלוסייה, במשאבים העומדים לרשותן וכן ברמתן הדיגיטלית[4].

עם התרחבות השימוש בטכנולוגיות הדיגיטליות, רשויות מקומיות הופכות לחכמות יותר ומאפשרות חיבור בין מערכות, אנשים ומכשירים. רשויות מקומיות מתחילות להשקיע בטכנולוגיה "חכמה" יותר ויותר. "עיר חכמה" מוגדרת כעיר המצוידת בתשתיות מידע ותקשורת ובכלל זה במכשירים אלקטרוניים האוספים מידע באמצעות האינטרנט ומאפשרים לרשויות המקומיות לשפר את התקשורת שלהן באופן המבוסס על מידע ונתונים.

רשויות מקומיות משתמשות במערכות המחוברות לאינטרנט כגון מערכות מעקב המשמשות לאכיפת החוק, מצלמות תנועה, חיישני תנועה המותקנים על פנסי רחוב ומערכות ניטור לניהול הטיפול בפסולת.

ברשויות המקומיות מצטבר מידע אישי על תושביהן, כמו שם, כתובת, מספר תעודת זהות, מספר טלפון, מידע רפואי, מידע בתחומי רווחה ונתונים על אמצעי התשלום שהם בוחרים לשלם באמצעותם וכן מידע בלתי מסונן כמו לוחיות רישוי, תווי פנים, נתוני מיקום והרגלי תנועה. כמו

1 שמכוחה הוצאו צווים להסדרת פעולותיהן של המועצות המקומיות והמועצות האזוריות - צו המועצות המקומיות (א), התשי"א-1950, וצו המועצות המקומיות (ב), התשי"ג-1953, אשר אוחדו בשנת 2016, וכן צו המועצות המקומיות (מועצות אזוריות), התשי"ח-1958.

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

3 האינטרנט של הדברים (באנגלית: Internet Of Things או בקיצור IoT) - חפצים פיזיים, או "דברים" שיש בהם רכיבי אלקטרוניקה, תוכנה וחיישנים המאפשרים תקשורת מתקדמת ביניהם, בכלל זה איסוף והחלפה של מידע.

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

כן, נאספים ברשויות נתונים על התושבים במסגרת צריכת שירותים כמו אירועי תרבות, פעילות במועדון הספורט העירוני או בהפעלת חוגים לילדים. דבר זה מחייב את הרשויות המקומיות לנקוט פעולות לשמירה על המידע שנאסף בידיהן ולאבטחתו.

רשויות מקומיות מתמודדות עם מגוון סיכונים, בעיות חוסן באבטחת המידע ואיומי סייבר, ומערכות המידע שלהן הפכו למוקד של עניין עבור פצחנים (האקרים[5]) 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[6] שברשותן וחשיפתם לגורמים שאינם מורשים לכך. עוד עלולה להיות פגיעה בתשתיות פיזיות, שיבוש ואף מניעה של אספקת שירותים קריטיים לתושבים כגון תשתיות אנרגייה, מים, תחבורה וביוב, ובמקרים חמורים אף פגיעה ברציפות התפקודית של הרשויות המקומיות. לפי נייר מדיניות של מערך הסייבר הלאומי, בשנים 2016 - 2018 בוצעו התקפות סייבר נגד שתי רשויות מקומיות בישראל, והן כללו דרישה לכופר בתמורה למניעת פגיעה ברשויות שהותקפו. באותן שנים בוצעו לפחות ארבע התקפות סייבר משמעותיות בערים בארה"ב, ובהן הוצפנו קבצים ושובשו שירותים חיוניים כגון תשלומי חשבונות, פיקוח עירוני ושירותי ניקיון ואבטחה[7].

# פעולות הביקורת

בחודשים יולי-נובמבר 2021 בדק משרד מבקר המדינה את נושא ניהול מערכות המידע ברשויות המקומיות. הבדיקה נעשתה בשמונה רשויות מקומיות שנבחרו, תוך מתן ביטוי למחוזות המינהליים שבהם שוכנות הרשויות; למעמדן המוניציפלי; ולמדד החברתי-כלכלי[8] שאליו הן משויכות; למדד הפריפריאליות[9] שאליו הן משויכות; למגזר שאליו רוב תושביהן משתייכים; ולמספר התושבים המתגוררים בתחומן: בחמש עיריות - **חיפה**, **יוקנעם**, **נתיבות**, **ראש העין** **ושפרעם**, בשתי מועצות מקומיות - **גדרה ועין מאהל** ובמועצה האזורית **מטה בנימין** (להלן - הרשויות שנבדקו). בדיקות השלמה נעשו במשרד הפנים - במינהל שירותי חירום ובמפעם עמק

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

6 חוק הגנת הפרטיות, התשמ"א-1981, מגדיר מאגר מידע - "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".

7 ראו נייר המדיניות בנושא הגנת הסייבר בהערת שוליים מס' 4 לעיל.

8 מדד שטווח ערכיו בין 1 ל-10 (10 הוא הגבוה שבהם), שגיבשה הלשכה המרכזית לסטטיסטיקה לאפיון הרשויות המקומיות בישראל לפי הרמה החברתית-כלכלית (סוציו-אקונומית) של האוכלוסייה בהן. המדד נחלק לשישה עשר משתנים שבאמצעותם מסווגות הרשויות המקומיות. המדד משמש להשוואה בין הרשויות.

9 מדד שטווח ערכיו בין 1 ל-10 (10 הוא הגבוה שבהם), שגיבשה הלשכה המרכזית לסטטיסטיקה לאפיון ולדירוג של רשויות מקומיות בישראל לפי מקומן הגיאוגרפי יחסית לריכוזי האוכלוסייה וכן יחסית למרכזי פעילות כלכלית (ככל שהרשות פריפריאלית יותר, הציון במדד יהיה נמוך יותר).

יזרעאל[10], במרכז השלטון המקומי, במערך הסייבר הלאומי שבמשרד ראש הממשלה (להלן - מערך הסייבר) וברשות להגנת הפרטיות במשרד המשפטים.

הבדיקה כללה את הנושאים שלהלן: קביעת אסטרטגיה לניהול מערכות המידע ברשויות המקומיות - אסטרטגיה לאומית בתחום אבטחת המידע, הקשר בין מערך הסייבר הלאומי לאגף הסייבר במשרד הפנים והכנת תוכניות עבודה ונהלים על ידי הרשויות המקומיות; הניהול הטכני של מערכות המידע - בעלי תפקידים בתחום מערכות המידע ומעמדו ותנאי העסקתו של מנהל מערכות המידע הראשי (להלן - המנמ"ר) ברשות המקומית; וכן אבטחת מידע, בעיקר בהקשר של הגנה על הפרטיות.

כמו כן נשלחו במסגרת הבדיקה ביולי 2021 שאלונים ל-63 רשויות מקומיות[11]. עד מועד סיום הביקורת בנובמבר 2021 השיבו 61 (97%) מהרשויות שנדגמו[12]. הממצאים בדוח זה מבוססים על הביקורת שנעשתה ברשויות שנבדקו וכן על המידע שנאסף מהשאלונים ועל ניתוח התשובות.

# רקע נורמטיבי

יש בישראל כמה חוקים, החלטות ממשלה ותקנות הרלוונטיים לנושא ניהול מערכות המידע ברשות המקומית. כמו כן, בין היתר כדי לצמצם את פוטנציאל הפגיעה בפרטיות הגלום במאגרי מידע, נחקק חוק הגנת הפרטיות, התשמ"א-1981 (להלן - חוק הגנת הפרטיות), שכלל הסדר ספציפי העוסק במאגרי מידע ממוחשבים. בשנת 1996 תוקן החוק במסגרת חוק הגנת הפרטיות (תיקון מס' 4) (מאגרי מידע), התשנ"ו-1996, כדי להבטיח יתר הגנה על הפרטיות במאגרי מידע. החוק מגדיר מהו "מאגר מידע" וכן כולל הגדרות של "מידע" ו"מידע רגיש". החוק קובע חובות החלות על בעלים ומנהלים[13] של מאגרי מידע ועל המחזיקים בהם[14].

10 מפעם הוא מרכז הדרכה לרשויות מקומיות, מטעם משרד הפנים, העוסק בניהול ובארגון של פעולות הדרכה לעובדי הרשויות המקומיות, בפיתוח ארגוני ובמתן ייעוץ אסטרטגי לרשויות המקומיות.

11 השאלון נשלח **לעיריות**: אום אל-פחם, אשדוד, אשקלון, בית שמש, ביתר עילית, בני ברק, בת ים, גבעתיים, הוד השרון, הרצלייה, חדרה, חולון, חיפה, טייבה, טירה, יוקנעם, כפר סבא, לוד, מודיעין מכבים רעות, מודיעין עילית, נהרייה, נס ציונה, נתיבות, נתניה, סח'נין, עכו, עפולה, פתח תקווה, צפת, קלנסוואה, קריית אתא, קריית גת, קריית ים, קריית מוצקין, קריית מלאכי, ראש העין, רהט, רחובות, רמלה, רמת גן, רעננה, שדרות, שפרעם, תל אביב-יפו; **למועצות המקומיות**: אבו סנאן, אבן יהודה, בית אל, גדרה, הר אדר, כפר יאסיף, כפר כנא, מבשרת ציון, עין מאהל, פוריידיס, ריינה; **ולמועצות האזוריות**: אל בטוף, גזר, חוף הכרמל, מטה בנימין, מטה יהודה, מנשה, מעלה יוסף, עמק חפר.

12 הרשויות שלא השיבו על השאלון: כפר כנא, פוריידיס.

13 סעיף 7 לחוק הגנת הפרטיות מגדיר מנהל מאגר כ"מנהל פעיל של גוף שבבעלותו או בהחזקתו מאגר מידע או מי שמנהל כאמור הסמיכו לעניין זה".

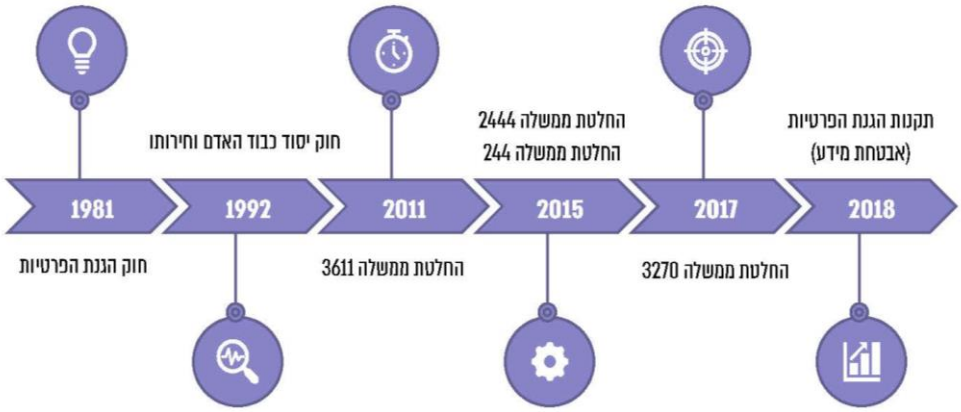
14 ובהן חובת רישומם של מאגרי המידע בפנקס המנוהל בידי רשם מאגרי המידע, אחריות לאבטחת המידע השמור במאגר המידע, ושמירת סודיותו של המידע והימנעות משימוש בו שלא למטרה שלשמה נמסר. סעיף 3 לחוק הגנת הפרטיות מגדיר מחזיק, לעניין מאגר מידע – "מי שמצוי ברשותו מאגר מידע דרך קבע והוא רשאי לעשות בו שימוש".

בשנת 1992 חוקק חוק יסוד: כבוד האדם וחירותו. בחוק היסוד נקבע כי כל אדם זכאי לפרטיות ולשמירה על צנעת חייו[15].

במאי 2018 נכנסו לתוקף תקנות הגנת הפרטיות (אבטחת מידע), התשע"ז-2017 (להלן - תקנות אבטחת המידע או התקנות), המפרטות את אופן יישומה של חובת אבטחת המידע המוטלת בחוק הגנת הפרטיות על כל בעל מאגר של מידע אישי, על מנהל המאגר ועל המחזיק בו. התקנות כוללות מיון של מאגרי מידע לפי מאפיינים שונים (סוגי המידע הכלולים במאגר, מספר האנשים שמידע עליהם כלול במאגר ומספר בעלי ההרשאה) וקובעות לפי המאפיינים את רמת האבטחה שחלה על מאגר המידע.

החלטות הממשלה 3611[16], 2443[17], 2444[18] ו-3270[19] עוסקות, בהתאמה, בהקמת מטה הסייבר הלאומי במשרד ראש הממשלה, בקידום אסדרה לאומית והובלה ממשלתית בתחום הגנת הסייבר, בקידום ההיערכות הלאומית בתחום הגנת הסייבר, בין היתר באמצעות הקמת רשות לאומית להגנת הסייבר במשרד ראש הממשלה ואיחוד מטה הסייבר הלאומי והרשות הלאומית להגנת הסייבר ליחידת סמך אחת, היא "מערך הסייבר הלאומי".

תרשים 1: **חקיקה רלוונטית על ציר הזמן בתחום מערכות מידע, 1981 - 2018**




התרשים בעיבוד משרד מבקר המדינה.

15 סעיף 7 לחוק יסוד: כבוד האדם וחירותו.

16 החלטת הממשלה 3611 "קידום היכולת הלאומית במרחב הקיברנטי" (7.8.11).

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

18 החלטת הממשלה 2444 "קידום ההיערכות הלאומית להגנת הסייבר" (15.2.15).

19 החלטת הממשלה 3270 "(1) איחוד יחידות מערך הסייבר הלאומי; (2) מתן פטור ממכרז למשרת ראש מערך הסייבר הלאומי; (3) הוספת משרת ראש מערך הסייבר הלאומי לתוספת לפי סעיף 23 לחוק שירות המדינה (מינויים); (4) קביעת שכר ותנאי שירות של ראש מערך הסייבר הלאומי" (17.12.17).

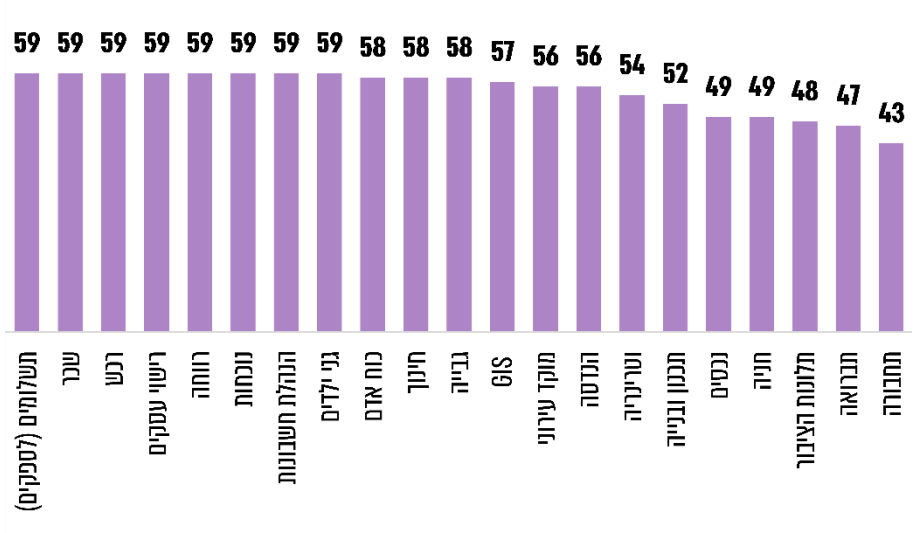
# מיפוי התוכנות הייעודיות ברשויות המקומיות

הרשות המקומית משתמשת במערכות מידע ובתוכנות ייעודיות לצורכי ניהול שוטף של מחלקותיה השונות ושל תחומי הליבה של פעילותיה, כגון כספים, גבייה, שכר, רכש, חינוך, רווחה, מוקד עירוני, מערכת מידע גיאוגרפי (GIS), תכנון ובנייה ורישוי עסקים.

כיום שירותי התוכנה ברשויות המקומיות מסופקים על ידי מספר מצומצם של ספקיות פרטיות, שהמרכזיות בהן: חברה א', חברה ב' וחברה ג'.

במסגרת השאלון התבקשו הרשויות המקומיות לציין אם הן משתמשות בתוכנות מחשב בתחומי הליבה השונים ומיהן החברות המספקות את התוכנות הללו. להלן הנתונים שעלו מהשאלונים:

תרשים 2: **מספר הרשויות המקומיות המשתמשות בתוכנות בנושאים שונים**[20]



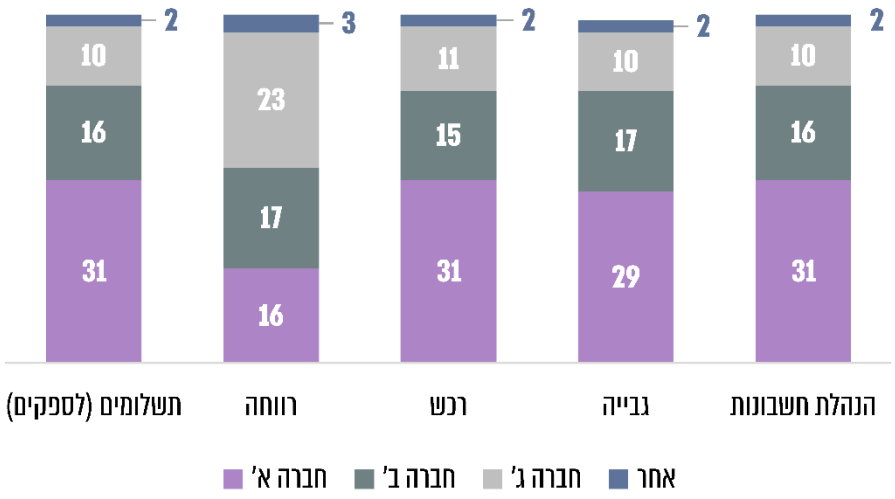

על פי הנתונים שנאספו בשאלון, בעיבוד משרד מבקר המדינה.

מהתרשים עולה כי ככלל, הרשויות המקומיות משתמשות בתוכנות מחשב בתחומים מגוונים, ולמעשה אין כיום תחום בניהול הרשות שבו לא נעשה שימוש במערכות מידע.

מכלל התשובות עולה כי יש כמה חברות המספקות שירותי תוכנה בכל התחומים שפורטו בתרשים, וכי חברות שונות נותנות שירותי תוכנה בתחומים מסוימים, כמפורט בתרשימים שלהלן:

20 59 רשויות מקומיות ענו על שאלה זו (מתוך 61 רשויות שענו על השאלון).

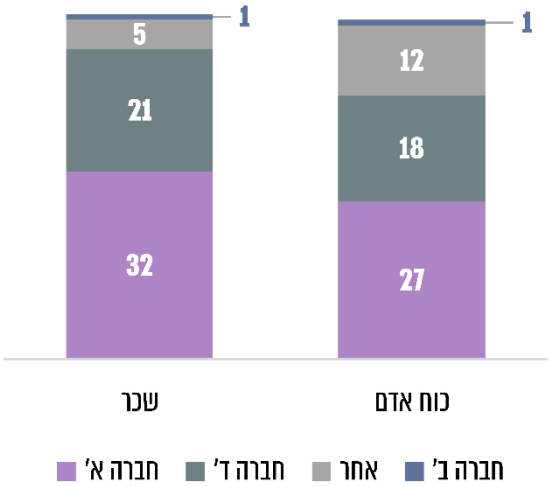
תרשים 3: **החברות שנותנות שירותים לרשויות המקומיות בתחומי הנהלת חשבונות, גבייה, רכש, רווחה ותשלומים (לספקים)**




על פי הנתונים שנאספו בשאלון, בעיבוד משרד מבקר המדינה.

מהתרשים עולה כי ב-96% משוק התוכנות בנושאי גבייה, הנהלת חשבונות, רווחה, רכש ותשלומים (לספקים) שולטות שלוש חברות עיקריות.

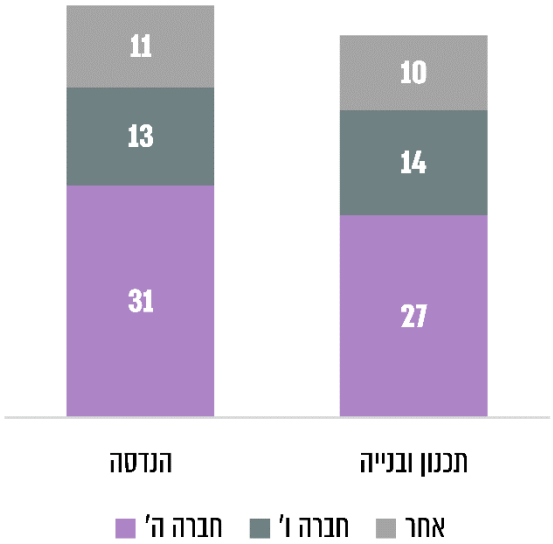
תרשים 4: **החברות שנותנות שירותים לרשויות המקומיות בתחומי שכר וכוח אדם**




על פי הנתונים שנאספו בשאלון, בעיבוד משרד מבקר המדינה.

מהתרשים עולה כי שתי חברות עיקריות עוסקות בנושא שכר וכוח אדם - חברה א' וחברה ד' - הנותנות שירותי תוכנה לכ-90% בתחום השכר, וכן נותנות שירותים בתחום כוח האדם לכ-78% מהרשויות (53 מ-59 רשויות, ו-45 מ-58 רשויות, בהתאמה).

תרשים 5: **החברות שנותנות שירותים לרשויות בתחומי הנדסה ותכנון ובנייה**




על פי הנתונים שנאספו בשאלון, בעיבוד משרד מבקר המדינה.

מהתרשים עולה כי שתי חברות עיקריות נותנות שירותי תוכנה לרשויות המקומיות בתחומי ההנדסה והתכנון והבנייה - חברה ה' וחברה ו' - השולטות בכ-80% בשני התחומים (44 מ-55, ו-41 מ-51, בהתאמה).

בטבלה שלהלן מפורטות החברות שבשירותיהן משתמשות הרשויות שנבדקו בתחומים אלה: הנהלת חשבונות, גבייה, רכש, תשלומים לספקים, רווחה, שכר, כוח אדם, נכסים, הנדסה ותכנון ובנייה:

לוח 1: **פירוט החברות שבשירותיהן משתמשות הרשויות שנבדקו**

| | הנהלת חשבונות | גבייה | רכש | תשלומים לספקים | רווחה | שכר | כוח אדם | נכסים | הנדסה | תכנון ובנייה |
|---|---|---|---|---|---|---|---|---|---|---|
| **גדרה** | חברה ב' | חברה ב' | חברה ב' | חברה ב' | חברה ב' | חברה ד' | חברה ד' | חברה ו' | חברה ו' | חברה ו' |
| **חיפה** | חברה א' | חברה א' | חברה א' | חברה א' | חברה א' | חברה א' | חברה א' | חברה א' | חברה ה' | חברה ה' |
| **יוקנעם** | חברה א' | חברה א' | חברה א' | חברה א' | חברה ג' | חברה א' | חברה א' | חברה א' | חברה ה' | חברה ה' |
| **מטה בנימין** | חברה ג' | חברה ג' | חברה ג' | חברה ג' | חברה ג' | חברה א' | חברה א' | חברה ה | חברה ה' | חברה ה' |
| **נתיבות** | חברה ב' | חברה ב' | חברה ב' | חברה ב' | חברה ב' | חברה א' | חברה א' | חברה ב' | חברה ו' | חברה ו' |
| **עין מאהל** | חברה א' | חברה א' | חברה א' | חברה א' | חברה א' | חברה א' | חברה א' | חברה א' | חברה א' | אין |
| **ראש העין** | חברה ב' | חברה ב' | חברה ב' | חברה ב' | חברה ב' | חברה ד' | אחר | חברה ב' | חברה ו' | חברה ו' |
| **שפרעם** | חברה ב' | חברה ב' | חברה ב' | חברה ב' | אחר | חברה א' | חברה א' | אין | אין | אין |

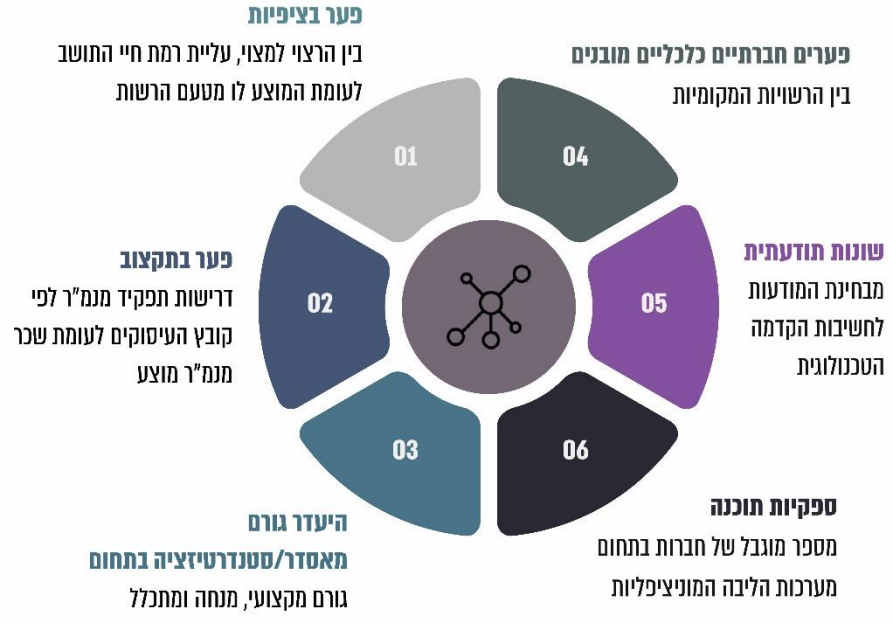
על פי נתונים שנאספו בשאלון, בעיבוד משרד מבקר המדינה.

מנתוני הטבלה עולה כי חברה א' מספקת לכל הרשויות שנבדקו, מלבד ראש העין וגדרה, שירותי תוכנה בתחומים שונים. חברה ב' מספקת שירותי תוכנה לארבע משמונה הרשויות, וחברה ג' מספקת שירותים לשתי רשויות. בתחומי שכר וכוח אדם, חברה א' מספקת שירותי תוכנה לשש משמונה רשויות, ואילו חברה ד' מספקת שירותים אלו לשתי רשויות. בתחומי הנכסים, הנדסה ותכנון ובנייה, עיקר השירותים ניתנים על ידי שתי חברות - ה' ו-ו'.

הרשויות המקומיות מתמודדות עם אתגרים בתחום מערכות המידע, וקיימת ביניהן שונות הן מבחינת משאביהן והן ברמתן הדיגיטלית. השונות ברמתן הדיגיטלית באה לידי ביטוי במקצועיות של בעלי התפקידים הרלוונטיים ברשות, לרבות המנמ"ר ומנהלי אבטחת מידע. בתרשים להלן יוצגו עיקרי האתגרים החיצוניים והפנימיים שהרשויות מתמודדות עימן בתחום מערכות המידע[21].

21 בעניין זה ראו מבקר המדינה, **דוח שנתי 70ב** (2020), "ההיערכות הממשלתית ליישום טכנולוגיות מתקדמות ברשויות המקומיות - מיזם ערים חכמות", עמ' 400.

תרשים 6: **אתגרים עיקריים בתחום ניהול מערכות המידע ברשויות המקומיות**




התרשים בעיבוד משרד מבקר המדינה.

# קביעת אסטרטגיה לניהול מערכות המידע ברשויות המקומיות

השימוש במערכות מידע לניהול ענייני הרשויות המקומיות הפך עם השנים למחויב המציאות, באופן שאין כיום רשויות מקומיות הפועלות ללא מערכות מידע. נוסף על כך, חלק ניכר מהנתונים במאגרי המידע הוא אישי, ומכאן נובע גם הצורך לשמרם באופן בטוח שימנע מגורמים חיצוניים ומבלתי מורשים לעיין בהם או להשתמש בהם באופן בלתי חוקי. ככל שהפגיעה מחשיפת המידע עשויה להיות גדולה יותר, כך עולה רמת רגישות המידע ועימה רמת האבטחה שיש לנקוט כדי לשמור עליו.

ניהול מערכות המידע נחלק לשני חלקים עיקריים: החלק הראשון הוא הניהול הכולל של מערכות המידע בנושאים של רכש ותחזוקה של ציוד מחשוב, פיתוח תחזוקה ושדרוג של תשתיות קיימות והתקשרויות עם גורמי מיקור חוץ במידת הנדרש; החלק השני נוגע לניהול הגנת סייבר ואבטחת המידע ברשות המקומית, בין היתר בהתאם לחוק הגנת הפרטיות ולתקנות אבטחת המידע.

כדי שהרשות תוכל לנהל את מערכות המידע ולהשתמש בהן באופן המיטבי, היא נדרשת לקבוע לעצמה אסטרטגיה ארוכת טווח ולהקצות תקציבים מתאימים לכך במסגרת תוכנית עבודה שנתית שבה ייקבעו, בין היתר, סדרי עדיפויות ליישום האסטרטגיה שלה. במסגרת האסטרטגיה האמורה יש להביא בחשבון הן את הדרישות בחוק הגנת הפרטיות ובדין הכללי המוטלות על הרשות המקומית בהיבטים של אבטחת מידע ומזעור סיכונים והן את הניהול הכולל של מערכות המידע.

# אסטרטגיה לאומית בתחום אבטחת המידע

בהתאם להחלטת הממשלה 2444 הוקם בשנת 2015 מערך הסייבר הלאומי. המערך נועד להגן על מרחב הסייבר של מדינת ישראל, שתפקידו, בין היתר, לפתח את החוסן של כלל המשק בתחום הסייבר, ובכלל זה לשפר את הכשירות וההכוונה של מגזרים וגופים במשק, לרבות של הרשויות המקומיות, שעל פי החלטה 2443 תיעשה באמצעות יחידות מגזריות.

מערך הסייבר הוא גוף ממלכתי, ביטחוני וטכנולוגי שייעודו להגן על מרחב הסייבר הלאומי של המדינה מפני איומי סייבר ולפעול לקידום ולביסוס של מעמדה ועוצמתה בתחום.

לפי החלטת הממשלה 3611, כלל מערך הסייבר עם הקמתו שתי יחידות סמך: הראשונה - מטה הסייבר הלאומי שהוקם בינואר 2012 כגוף מטה של הממשלה, אשר הוטלה עליו בין היתר משימת פיתוח מדיניות ואסטרטגיית סייבר במישור הארצי ופיתוח הכוח הלאומי בתחום זה, לרבות קידום תהליכי הגנה לאומיים והסדרתם, וכן פיתוח היכולות הלאומיות בתחום הסייבר, קידום שיתופי פעולה בין-לאומיים וביסוס מעמדה של מדינת ישראל כמדינה מובילה בתחום; ואילו השנייה - הרשות הלאומית להגנת הסייבר, אשר הוקמה במסגרת אותה החלטת ממשלה כגוף אופרטיבי מרכזי להגנת הסייבר בישראל. ההחלטה לפעול במסגרת שתי יחידות נבעה בזמנו מהצורך לפתח ולחזק את שתי הזרועות של המערך.

במסגרת החלטת הממשלה 3270 נקבע כי שתי יחידות הסמך שמהן מורכב מערך הסייבר יאוחדו ליחידת סמך אחת במשרד ראש הממשלה. בהחלטה נקבע כי יעדי המערך, תפקידיו וסמכויותיו יהיו אלה של המטה והרשות הקבועים בחוק, וכן בהחלטות הממשלה הנוגעות לנושא. עוד נקבע בהחלטה כי על ראש המערך לשמר ולחזק את היכולת המבצעית של המערך ולהמשיך את תהליך הפיתוח וההעצמה של יכולת זו, כפי שהרשות כבר החלה לבצעו, זאת לצד בניין הכוח הטכנולוגי.

כחלק מהזרוע המבצעית של מערך הסייבר פועל **המרכז הארצי לניהול אירועי סייבר** CERT (Computer Emergency Response Team) (להלן - המרכז לניהול אירועי סייבר), אשר מטפל באירועי סייבר במרחב האזרחי של המדינה. המרכז מקבל מדי יום מגורמים שונים, לרבות מרשויות מקומיות, מאות דיווחים וידיעות על ניסיונות למתקפות סייבר מהארץ ומהעולם או על חשדות למתקפות כאמור, והוא בודק חשדות אלה ומטפל בהם.

במרכז לניהול אירועי סייבר פועלים שישה תתי-מרכזים ייעודיים לענפים ולקהלי יעד שונים, שנותנים מענה ייחודי. תת-המרכז הראשון והמרכזי הוא המרכז המבצעי לדיווח על אירועי סייבר, שאמורים להיות מוזרמים אליו באופן שוטף דיווחים על מתקפות סייבר. המרכז בודק ומתחקר

אירועים ונותן סיוע ראשוני והמלצות לטיפול ולהגנה. חמישה תתי-מרכזים נוספים הם מרכזי שליטה ייעודיים שהקים מערך הסייבר, בשיתוף משרדי הממשלה הרלוונטיים, והם משמשים להתמודדות עם איומי סייבר ייחודיים למגזרים מסוימים, ובהם המגזר הממשלתי.

## הקשר בין מערך הסייבר הלאומי לאגף הסייבר במשרד הפנים

משרד הפנים מופקד על תכנונה ויישומה של המדיניות הלאומית בנושאי השלטון המקומי. פעילות המשרד כמאסדר מתבצעת בשני מישורים: במישור הארצי - מתן הנחיות וקביעת מדיניות, ובמישור המחוזי - קיום קשר עם הרשויות באמצעות הדרג הביצועי. המשרד מפקח מטעם הממשלה על הרשויות המקומיות ואחראי להכוונת פעולותיהן בהתאם לחוק ולמדיניות הממשלה[22].

**אגף הסייבר במשרד הפנים:** 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.

בעקבות קבלתה של החלטת הממשלה האמורה, הוקם בשנת 2017 **אגף הסייבר במשרד הפנים** כיחידה מקצועית מגזרית בתחום הגנת הסייבר ואבטחת המידע הכפוף למינהל לשירותי חירום במשרד הפנים ובהנחיה מקצועית של מערך הסייבר, ובין היתר הוטלה על האגף האחריות להסדרת היערכותן של הרשויות המקומיות לאיומי סייבר. באגף מועסקים ארבעה יועצים חיצוניים המומחים לאבטחת מידע, אשר נותנים שירות לרשויות המקומיות. תפקיד היועצים הוא ללוות את הרשויות המקומיות בתחום אבטחת המידע והגנת הסייבר, לייעץ להן באופן שוטף ולסייע בקביעת מדיניות ותוכניות עבודה ולהציב יעדים להגברת החוסן הקיברנטי[23] של הרשויות המקומיות.

במסגרת פעילותו, ביצע אגף הסייבר במשרד הפנים מסוף שנת 2018 עד אוגוסט 2021 מבדק בסיסי של רמת החוסן הקיברנטי ב-130 רשויות מקומיות, בהתבסס על מסמך "תורת ההגנה בסייבר" של מערך הסייבר[24] (להלן - מסמך תורת ההגנה). אגף הסייבר מסר למשרד מבקר המדינה כי בכוונתו לבצע מבדקים בנוגע לכ-30 רשויות מקומיות נוספות בשנת 2022.

ההליך כלל בדיקה של מצב הרשויות המקומיות בתחומי אבטחת המידע ושל מידת מוכנותן לאירועי סייבר, וזאת על בסיס שאלון מפורט. לאחר שהרשויות מילאו את השאלון ניתן לכל אחת מהן ציון בטווח שבין 0 ל-100 נקודות, המעיד על מידת היערכותן לאירועי סייבר. הרשות

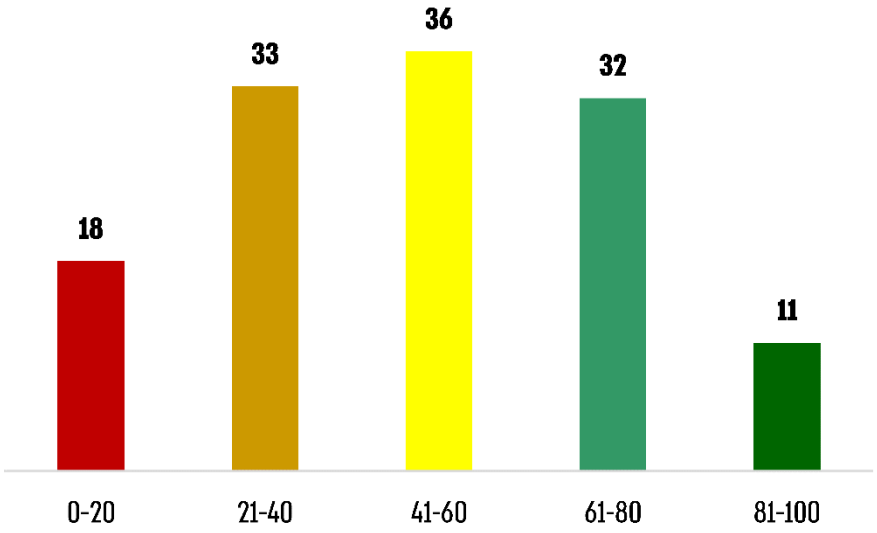
22 ראו הערת שוליים מס' 21 לעיל שם בעמ' 412 - 413.

23 המרחב הקיברנטי הוא מרחב מטפורי של מערכות ורשתות מחשב, ובו נשמרים נתונים אלקטרוניים ומתבצעת תקשורת מקוונת ואינטראקטיבית ללא תלות במקום הימצאם הגיאוגרפי של המשתמשים בו (ויקיפדיה).

24 ביוני 2017 פרסם מערך הסייבר את מסמך "תורת ההגנה בסייבר לארגון" (גרסה 1.0), שמטרתו לשפר את החוסן הארגוני ואת העמידות הארגונית בפני מתקפות סייבר. באפריל 2018 פורסמה מהדורה שנייה של גרסה זו וביוני 2021 פורסמה גרסה נוספת (2.0).

בעלת הציון הגבוה ביותר מבין הרשויות שמילאו את השאלון קיבלה 95 נקודות, והרשות בעלת הציון הנמוך ביותר קיבלה 5 נקודות. המבדק אמור לסייע לרשויות המקומיות בהכנת תוכניות עבודה לשיפור היערכותן לאירועי סייבר. להלן התפלגות הציונים שקיבלו הרשויות במבדק משרד הפנים:

תרשים 7: **התפלגות ציוני החוסן הקיברנטי של הרשויות המקומיות**




על פי נתוני אגף הסייבר במשרד הפנים, בעיבוד משרד מבקר המדינה.

עלה כי אגף הסייבר במשרד הפנים השלים מבדק בסיסי ב-130 רשויות מתוך 257 רשויות, נכון לאוגוסט 2021. עוד עלה כי 87 (כ-67%) מ-130 הרשויות קיבלו ציון הנמוך מ-60, ואילו רק 11 (כ-8%) רשויות קיבלו ציון הגבוה מ-80 והציון הממוצע היה 48. עולה אפוא מהנתונים כי רמת אבטחת המידע והמוכנות של מרבית הרשויות המקומיות (67% מהן) לאיומי סייבר היא נמוכה, וכי הרשויות השונות שבחן משרד הפנים נבדלות זו מזו במידה רבה מבחינת מוכנותן לאירועי סייבר.

בבדיקה שעשה משרד מבקר המדינה בנוגע לקשר בין ציוני החוסן של הרשויות שבדק משרד הפנים לבין המדד החברתי-כלכלי שלהן, המדד הפריפריאלי שלהן וסוג הרשות (עירייה, מועצה מקומית או מועצה אזורית), לא נמצא קשר לאחד מהמשתנים האמורים.

נוכח הציונים הנמוכים מ-60 שקיבלו 67% מהרשויות המקומיות במבדק הבסיסי, המעידים כי רמת אבטחת המידע שלהן ומוכנותן לאיומי סייבר נמוכות, על אגף הסייבר במשרד הפנים בשיתוף מערך הסייבר לתת את דעתם על הנתונים האמורים ולהנחות את הרשויות המקומיות להיערך בהתאם לכך. עוד מומלץ כי אגף הסייבר במשרד הפנים ישלים עריכת מבדקים בכלל הרשויות ויפעל לתיקופם על בסיס תוכנית עבודה רב-שנתית.

בתשובת משרד הפנים למשרד מבקר המדינה ממאי 2022 (להלן - תשובת משרד הפנים ממאי 2022) נמסר כי "אל מול ממצאי המבדקים הועברו לרשויות המקומיות המלצות מקצועיות כיצד לפעול וזאת כחלק מחבילת הסיוע והליווי שמספק משרד הפנים".

מבקר המדינה עמד בדוחות קודמים שלו[25] על החולשות הקיימות בתחום הגנת הפרטיות ואבטחת המידע ברשויות המקומיות. למשל, בדוח שפורסם בנובמבר 2017 צוין כי השלטון המרכזי אינו מסדיר את פעילות הרשויות המקומיות בתחום אבטחת המידע והגנת הפרטיות, וכי כל רשות מתמודדת עם נושא אבטחת המידע כמיטב הבנתה, בין היתר נוכח עמדתו של המשרד כי הוא אינו מוסמך לטפל בנושא[26].

מבקר המדינה קבע, בין היתר בדוח משנת 2017, כי עמדתו של משרד הפנים באותה עת ולפיה הוא אינו מוסמך לטפל בתחום אבטחת המידע, אינה מתיישבת עם העיקרון שעליו מתבססת החלטת הממשלה 2443, ולפיו על משרדי ממשלה בעלי סמכויות רגולטוריות להגדיר את המדיניות ודרישות האסדרה עבור המגזר שבו הם פועלים. המבקר המליץ כי משרד הפנים יוציא לרשויות המקומיות קובץ הנחיות מחייב בנושא אבטחת מידע והגנת הפרטיות ויוודא כי הוא מוטמע ומיושם.

יצוין כי גם במסגרת הביקורת הנוכחית חזר משרד הפנים על עמדתו ולפיה הוא אינו משמש רגולטור עבור הרשויות המקומיות בנושא אבטחת המידע והגנת הסייבר. משרד מבקר המדינה בחן בביקורת זו את הניסיון להסדיר את תחומי האחריות של משרד הפנים ומערך הסייבר בכל הנוגע לרגולציה ולהנחיה מקצועית של הרשויות המקומיות בתחומי אבטחת מידע והגנת הסייבר, להלן פירוט:

1. ביולי 2018 התקיימה ישיבה בין נציגים ממשרד הפנים וממערך הסייבר, ובה נכחו, בין היתר, מנכ"ל משרד הפנים וראש מערך הסייבר. במהלכה ציינו נציגי משרד הפנים כי למשרד אחריות חלקית בתחום הסייבר כלפי הרשויות המקומיות, מאחר שאין לו סמכות משפטית ויכולת מעשית לפיקוח על מערכות המחשוב של הרשויות המקומיות, לביצוע רגולציה בהן ולניהולן, בין היתר משום שמדובר בגופים עצמאיים על פי חוק, ובגלל ההבדל בין מעמדם, למעמדם של גורמי הממשלה האחרים שהם חלק מהממשלה וכל אחד מהם כפוף מהבחינה החוקית והמינהלית למשרד ממשלתי זה או אחר.

   באותה ישיבה הדגיש מנכ"ל משרד הפנים כי המשרד "לא מעוניין להיות במקום בו הרשויות חשופות לאיומי אבטחת מידע, אך המשרד לא יכול לקחת לידיו את כל הסמכויות בשעה שאין לו את הכלים המתאימים". בתום אותה ישיבה סיכמו שני הצדדים כי ימשיכו בדיונים על מנת לקבוע את תחומי האחריות והסמכות של כל צד, וכי מערך הסייבר אחראי להכנת מודל המציג את תחומי אחריותו של משרד הפנים כגורם המסייע לרשויות המקומיות בתחום הסייבר.

2. במאי 2019 הוציא מערך הסייבר "נוהל אב להגדרת מסגרת אחריות משרדי הממשלה ויחידות הסייבר המגזריות למול אגף הכוונת ואסדרת המשק במערך הסייבר הלאומי

25 בהקשר זה ראו: מבקר המדינה, **דוח שנתי 62** (2012), "אבטחת מידע והגנת הפרטיות ברשויות המקומיות", עמ' 1513 - 1537; **דוחות על הביקורת בשלטון המקומי** (2017), "אבטחת מידע והגנת הפרטיות ברשויות המקומיות - מעקב מורחב", עמ' 201 - 245.

26 שם, בעמ' 210.

בהיבטי הגנת מגזרי המשק למול איומי סייבר" (להלן - הנוהל). מטרת הנוהל היא להגדיר כללי מסגרת למימוש האחריות של משרדי הממשלה להגנה בתחום הסייבר כלפי מגזרי המשק, וכן להגדיר נוהג עבודה מוסדר בין היחידות המגזריות במשרדי הממשלה לבין מערך הסייבר, בהתאם לתפיסת אסדרה לאומית מבוזרת שאישרה הממשלה ולפיה מערך הסייבר משמש גורם הכוונה ממלכתי אשר ממלא את תפקידו באמצעות יחידות הסייבר המגזריות הפועלות במשרדי הממשלה.

3. במכתב ששלח ביוני 2019 מנכ"ל משרד הפנים דאז לראש מערך הסייבר הוא ציין כי מערך הסייבר לא הכין, בהתאם לסיכום מיולי 2018, מודל המציג את אחריותו של משרד הפנים כגורם מסייע לרשויות המקומיות בתחום הסייבר. עוד ציין כי מערך הסייבר הפיץ את הנוהל האמור באופן חד-צדדי ובלא שקוימה חובת התייעצות עם המשרד בעניין הנוהל.

מנכ"ל משרד הפנים ציין במכתבו, כי לפי הנוהל מוטלות על משרד הפנים מטלות כבדות משקל ואחריות רבה בהתאם לתפיסה של אסדרה לאומית מבוזרת באמצעות יחידות האסדרה המגזריות, זאת אף שסביר כי יחידות אלה אינן מתאימות לתפקיד האמור ואינן יכולות למלאו בהתחשב באחריות המשרד בתחום הגנת הסייבר ברשויות. מנכ"ל משרד הפנים חזר וביקש במכתבו, לקבל ממערך הסייבר מודל המציג את אחריות משרד הפנים כגורם מסייע לרשויות המקומיות בתחום הסייבר, והדגיש כי "לא ניתן לראות את כלל הגופים המגזריים כמקשה אחת ויש להתייחס למשרד הפנים ולתפקידו ביחס לרשויות המקומיות בעניין זה, בנפרד ובמתואם".

4. ראש מערך הסייבר ציין בתשובתו מיוני 2019 למנכ"ל משרד הפנים כי מערך הסייבר הפיץ לאחרונה "נוהל אב" המגדיר מסגרת למימוש האחריות של משרדי הממשלה להגנת הסייבר במשרדים השונים, וכי הנוהל עוסק בין היתר במיסוד של נוהלי העבודה בין היחידות המגזריות לבין מערך הסייבר ובהסדרת הנהלים.

אשר לבקשת המנכ"ל לקבל ממערך הסייבר מודל המציג את אחריות משרד הפנים כגורם מסייע לרשויות המקומיות בתחום הסייבר, ראש מערך הסייבר השיב כי הוא ממליץ למשרד הפנים לאמץ את הנוהל בתור בסיס, ולבצע בו את ההתאמות והשינויים הדרושים לו, והם יובאו לאישור הגורמים הרלוונטיים במערך הסייבר. בנוגע לשאלת הסמכות המשפטית, ראש מערך הסייבר ציין כי זהו נושא המחייב עבודה מקצועית נוספת, ולכן הוא הנחה את היועץ המשפטי של מערך הסייבר לקדם את העניין מול היועץ המשפטי של משרד הפנים, אולם במועד סיום הביקורת העניין לא קודם.

5. במכתב ששלח ראש מערך הסייבר ביולי 2021 לשרת הפנים הוא הציג את מצב הדברים ולפיו בשנים האחרונות נמנע משרד הפנים מלהכיר בעצמו כגורם מאסדר ואחראי בנושא הגנת הסייבר, בין היתר בטענה כי חסרות לו הסמכויות, המשאבים והידע המקצועי הנדרשים. הוא הבהיר כי "היעדר גורם מאסדר ומתכלל גורם לרמת הגנה ירודה בקרב רשויות רבות ועלייה ברמת הסיכון במגזר הרשויות". ראש מערך הסייבר הוסיף כי לעמדתם, משרד הפנים הוא הגורם הטבעי האחראי להובלה ולאסדרה של הנושא במגזר הרשויות המקומיות שהן תחת אחריותו, כפי שקיים בשאר מגזרי המשק, ועמד על הצורך לפעול יחד להסדרה רוחבית של הנושא.

נמצא כי נכון למועד סיום הביקורת, בנובמבר 2021, משרד הפנים ומערך הסייבר לא השלימו את הסדרת הסמכויות החסרות בכל הנוגע לרגולציה ולהנחיה מקצועית של הרשויות המקומיות בתחומי אבטחת מידע והגנת הפרטיות. בתוך כך, משרד הפנים לא פעל להכנת נוהל שמטרתו להנחות את הרשויות המקומיות כיצד לפעול בכל הקשור לאבטחתם של מערכות המידע ומאגרי המידע שברשותן. כפועל יוצא, אין לרשויות המקומיות גורם מאסדר בתחום אבטחת המידע והגנה מאיומי סייבר, ומזה שנים הרשויות המקומיות פועלות ללא הנחיות מקצועיות ברורות בנושא וכל רשות מקומית פועלת בעניין לפי ראות עיניה.

מערך הסייבר הלאומי ציין בתשובתו למשרד מבקר המדינה ממרץ 2022 (להלן - תשובת מערך הסייבר) כי היחידה המגזרית כפופה למינהל לשירותי חירום במשרד הפנים ואין לה סמכות כלפי הרשויות המקומיות. כמו כן מקום הפעילות של המשרד בתחום הגנת הסייבר, תשומות התקציב והיקפי כוח האדם מעידים כי הפעילות אינה עומדת בראש סדר העדיפויות של הנהלת משרד הפנים, וזאת בלשון המעטה. הדברים עולים במפורש מפנייתו של ראש מערך הסייבר אל שרת הפנים, ובו ביקש כי תיתן את דעתה על הנושא ותפעל לכך שהוא יטופל בדרג הבכיר ביותר. התקציב של היחידה המגזרית במשרד הפנים והיקף כוח האדם המועסק בה אין די בהם כדי לאפשר את מילוי תכליתה של היחידה המגזרית. עוד ציין מערך הסייבר הלאומי כי משרד הפנים לא פעל להגדרת דרישות האסדרה ליישום החלטת הממשלה 2443 ואף לא פעל לקידום תיקוני חקיקה אפקטיביים.

מערך הסייבר ציין עוד כי בדצמבר 2020 התקיימה שיחה טלפונית בין נציגי הלשכות המשפטיות של משרד הפנים ומערך הסייבר בנושא סמכויות משרד הפנים להנעת רשויות מקומיות לקידום היערכותן לאירועי סייבר. נציגי מערך הסייבר הציעו לנציגי משרד הפנים, סעיפי חוק אפשריים בפקודת העיריות שניתן לממש לצורך העלאת רמת הגנת הסייבר ברשויות המקומיות, אך נכון למועד מתן התשובה משרד הפנים עדיין לא יזם מהלך לקידום הנושא. נוסף על כך, ביולי 2021 התקיימה פגישה בין נציגי מחלקת ייעוץ וחקיקה במשרד המשפטים, נציגת הלשכה המשפטית במשרד הפנים ונציג הלשכה המשפטית במערך הסייבר. במהלך הדיון ציינה רפרנטית שלטון מקומי בייעוץ וחקיקה כי היא אינה סבורה שאפשר לקבוע שמשרד הפנים אינו "רגולטור" כלל, שכן יש למשרד הפנים סמכויות שונות שהוא יכול להפעיל כלפי הרשויות המקומיות. כמו כן הוצע למשרד הפנים לבחון נקיטת פעולות שונות לטובת קידום רמת הגנת הסייבר במגזר השלטון המקומי, ובכלל זה חיוב הרשות להקצות תקציב ייעודי להגנת הסייבר, לפעול מול ספקי ה-IT המרכזיים במגזר, לפרסם מדיניות סייבר רצויה בקרב הרשויות המקומיות, להפיץ הנחיות לא מחייבות והמלצות מלשכת מנכ"ל המשרד לכלל הרשויות, ולפנות יחד למנהל הרכש כדי לאפשר לרשויות מקומיות להשתתף במכרזים ממשלתיים לרכש מוצרי הגנת סייבר. נכון למועד מתן התשובה משרד הפנים לא הגיב לשום הצעה מההצעות האמורות.

מערך הסייבר הוסיף בתשובתו, כי הוא הציע לאפשר לרשויות המקומיות להשתתף במכרז של משרדי הממשלה לקבלת שירותי הענן "נימבוס" וכי בעת שבוצעו תיקוני חקיקה רוחביים הממוקדים בדיגיטציה הצביע מערך הסייבר הלאומי על פערי הסמכות הלכאוריים, ועל הצורך להסדיר נושא זה ולהבהירו.

משרד הפנים ציין בתשובתו למשרד מבקר המדינה ממרץ 2022 (להלן - תשובת משרד הפנים) כי מינהל החירום במשרד הפנים הוא גוף מסייע לרשויות המקומיות ואינו גוף המנחה אותן, וכי ההנחיות בנושא אמורות להינתן על ידי מערך הסייבר.

הן משרד הפנים והן מערך הסייבר ציינו בתשובותיהם כי התקיימה ביניהם פגישה נוספת במרץ 2022, אבל לא נחתם סיכום דיון.

בתשובת משרד הפנים ממאי 2022 הוא ציין כי תוך 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.

מומלץ 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 בהמשך לכך יתרמו משרד הפנים ומערך הסייבר כל אחד את חלקו - בהתאם לחלוקה שתיקבע - לקביעת נהלים מתאימים שיסדירו את פעילויות הרשויות המקומיות בכל הנוגע לאבטחת מידע ולהגנה עליו מפני איומי סייבר.

## הכנת תוכניות עבודה ונהלים על ידי הרשויות המקומיות

מסמך תורת ההגנה מגדיר, בין היתר, את אחריות הארגון להכנת תוכנית עבודה רב-שנתית להתגוננות של הארגון מפני 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 המסמך, ועל 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.

השימוש במערכות מידע לניהול ענייני הרשויות המקומיות, לרבות מתן שירותים באמצעים דיגיטליים, מחייב את הרשויות להקים ולתחזק תשתית של מערכות טכנולוגיות מתאימות ולהעסיק עובדים ומומחים שתפקידם לקדם תחום זה.

במתווה להקמה ולהפעלה של יחידות לניהול מערכות מידע ברשויות המקומיות שהכין משרד הפנים בינואר 2019 (להלן - המתווה) נקבע כי על הרשות המקומית להכין תוכנית עבודה אסטרטגית רב-שנתית, ובהתאם לה לקבוע תוכנית עבודה שנתית, שלפיה תפעל יחידת מערכות המידע לביצוע רכש של ציוד, לפיתוח ולשדרוג של תשתיות קיימות ולהתקשרות עם גורמים במיקור חוץ להשגת יעדי התוכנית.

עוד נקבע במתווה כי את תוכנית העבודה האסטרטגית יש ליישם לאחר שימופה המצב הקיים ברשות בכל תחומי האחריות של היחידה לניהול מערכות מידע, כמו תשתיות תקשורת, שרתים, רשתות, מערכות מידע וכלים דיגיטליים, וכן השירותים הדיגיטליים, אבטחת המידע, ניהול מאגרי המידע וההגנה על הפרטיות. כמו כן, יש לבצע איתור של צורכיהן הטכנולוגיים של היחידות

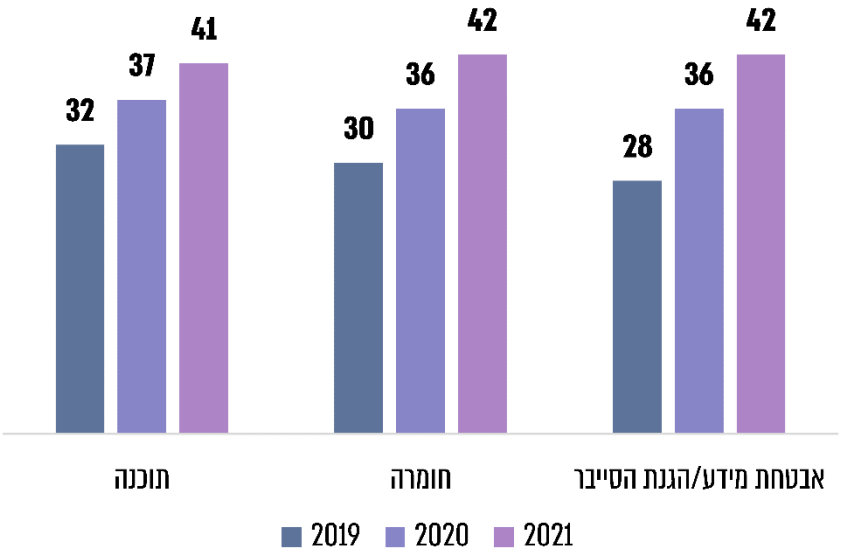
השונות ברשות כדי לברר מה נדרש להן, מהבחינה הטכנולוגית, על מנת שיוכלו ליישם את תוכניות העבודה שלהן ולממש את החזון המקצועי שלהן.

במסגרת ניהול מערכות המידע נדרשת כל אחת מהרשויות המקומיות להגדיר תחילה את חזונה בתחום הטכנולוגיה והדיגיטציה ואת תפיסתה בתחום מערכות המידע וכן את סדר העדיפויות שלה למימושו במסגרת תוכנית עבודה אסטרטגית רב-שנתית, שכן יחידת מערכות המידע ברשות נדרשת לתת מענה לצרכים קיימים וגם לקדם תהליכי חדשנות והתפתחות עתידיים.

קיימת חשיבות רבה להכנת תוכניות עבודה אסטרטגיות רב-שנתיות ותוכניות עבודה שנתיות בנושא ניהול מערכות המידע. זאת כדי למפות את הצרכים של הרשות המקומית וכדי לקבוע דרכי פעולה וסדרי עדיפויות במתן מענה בכל תחומי העשייה של הרשות המקומית הקשורים בהיבט זה.

בשאלון שנשלח לרשויות המקומיות הן התבקשו לציין, בין היתר, אם יש להן תוכניות עבודה שנתיות או רב-שנתיות בתחום ניהול מערכות מידע. בתרשים שלהלן יצוינו הנתונים שמסרו הרשויות במענה על שאלה זו[27].

תרשים 8: **מספר הרשויות שהכינו תוכניות עבודה בתחום ניהול מערכות מידע, 2019 - 2021**




על פי הנתונים שנאספו בשאלון, בעיבוד משרד מבקר המדינה.

27 59 רשויות מקומיות השיבו על שאלות בנוגע להכנת תוכניות עבודה בנושאי תוכנה, חומרה, אבטחת מידע והגנת סייבר.

מתשובותיהן של הרשויות המקומיות שהשיבו על השאלון עולה כי בשנים 2019 - 2021 מסתמנת מגמת גידול במספרן של הרשויות שהכינו תוכניות עבודה בנושא ניהול מערכות מידע: מספר תוכניות עבודה בנושא התוכנה גדל ב-28%, מספר תוכניות העבודה בנושא החומרה גדל ב-40%, ומספר תוכניות העבודה בנושא אבטחת מידע והגנת הסייבר גדל בכ-50%. עם זאת, נכון למועד סיום הביקורת לכ-70% מהרשויות לא היו תוכניות עבודה בתחום ניהול מערכות המידע.

בפגישה שהתקיימה עם מפעם עמק יזרעאל במרץ 2021, נמסר למשרד מבקר המדינה כי בשלב זה מדובר במתווה ראשוני שאינו מחייב, ולכן בהיעדר הנחיה מחייבת כל רשות פועלת כרצונה, לפי תפיסתה ולפי סדרי העדיפויות שלה, אשר אינם בהכרח עונים על צרכיה של הרשות המקומית וגורמים להיווצרות פערים בין הרשויות המקומיות בכל הקשור להקמה ולהפעלה של מערכות המידע ברשויות, לרבות מבחינת הכנת תוכניות העבודה האסטרטגיות ותוכניות העבודה השנתיות. עוד נמסר כי חלק ניכר מהרשויות מתקשות בצמצום הפערים בתחום זה בהיעדר כוח אדם מקצועי ותקציבים וכן בהיעדר מודעות מצד הדרג הניהולי לחשיבות נושא ניהול מערכות המידע.

הבדיקה העלתה כי משרד הפנים לא סיים הכנת מתווה מחייב ולא הנחה את הרשויות המקומיות בעניין הכנת תוכניות עבודה אסטרטגיות ותוכניות עבודה שנתיות בנושא מערכות המידע וכן המשרד אינו מבצע מעקב ובקרה בנושא.

נוכח ההתפתחות הטכנולוגית המהירה שמשפיעה על כל הארגונים עולה הצורך בגיבוש מתווה שיסדיר את פעילות הרשויות המקומיות בתחום ניהול מערכות המידע שברשותן. לפיכך מומלץ כי משרד הפנים ישלים את גיבושו של המתווה, יבצע בו התאמות במידת הצורך, ינחה את הרשויות המקומיות בהתאם לכך ויעקוב אחר הטמעתו.

משרד הפנים חזר בתשובתו על עמדתו לעיל כי נכון למועד מתן תשובתו נושא ניהול מערכות המידע ברשויות המקומיות אינו בתחום אחריותו על פי דין והוא אינו גוף מתכלל של הרשויות המקומיות בנושא. משרד הפנים ציין כי פעולותיו בתחום זה נעשות כחלק מפעולות ממשלתיות לקידום ממשקים דיגיטליים ברשויות המקומיות, כדוגמת הקמת צוות בין-משרדי, לפני כחצי שנה, בשיתוף משרד הפנים ומערך הדיגיטל הלאומי שבוחן כיצד ניתן לבצע טרנספורמציה דיגיטלית ברשויות המקומיות, וכן גיבוש אסטרטגיה להתערבות ממשלתית בתחום הדיגיטל בשלטון המקומי, בדגש על השירותים של הרשויות המקומיות לתושבים והתייעלות באמצעות מערכות מידע ושימוש בידע. עוד ציין המשרד כי הוא קיים בשנה האחרונה פגישות עבודה שוטפות עם איגוד המנמ"רים של הרשויות המקומיות ועם מנמ"ר מרכז השלטון המקומי לקידום התחום ולפתרון סוגיית החסמים הרבים שבו. בתשובת משרד הפנים ממאי 2022 ציין המשרד כי הוא הכין תבנית של תוכנית אסטרטגית דיגיטלית רשותית, בהתאם ליכולת הדיגיטלית של כל רשות, על מנת לקבוע לפיה תוכנית עבודה.

נמצא כי הרשויות המקומיות גדרה, יוקנעם, מטה בנימין, נתיבות, עין מאהל ושפרעם לא הכינו תוכניות עבודה אסטרטגיות רב-שנתיות בנושא מערכות המידע ולא הכינו תוכניות עבודה שנתיות מקושרות תקציב בהתאם ליעדי הרשות המקומית לטווח הארוך. עוד נמצא כי עיריות חיפה וראש העין, אשר גיבשו תוכניות אסטרטגיות בנושא מערכות המידע, לא תקצבו אותן ומשכך התוכניות לא יושמו.

מנמ"רית עיריית **חיפה** הכינה בנובמבר 2020, סמוך לכניסתה לתפקיד, תוכנית עבודה אסטרטגית לשנת 2021, ובה מופו צורכי מינהל המחשוב לרבות צרכיו בנושא אבטחת מידע (לשנים 2021 ו-2022). המנמ"רית מסרה כי אומנם העירייה הכינה תוכנית עבודה שנתית לשנת 2021, אך היא בגדר תוכנית ראשונית. עוד הבהירה כי תוכנית העבודה לא תוקצבה במסגרת תקציב העירייה לשנת 2021, שכן התקציב הוכן עוד לפני הכנת התוכנית.

מנמ"ר עיריית **ראש העין** הכין בשנת 2020 תוכנית אסטרטגית לשלוש שנים בנושא ניהול מערכות המידע, שבמסגרתה מופו הקשיים, החסמים והצרכים של העירייה בהיבט של מערכות המידע וכן הוערך התקציב הנדרש ליישום התוכנית. הועלה כי במועד סיום הביקורת לא התקיים בעירייה דיון בנושא התוכנית האסטרטגית, ובפועל היא לא יושמה נכון למועד סיום הביקורת.

מומלץ כי הנהלות עיריות חיפה וראש העין ידונו בהיבטים השונים של תוכנית העבודה האסטרטגית שהכינו המנמ"רים, לרבות בהתחשב במגבלות התקציב, ויפעלו למימושה בהתאם לכך.

עיריית **חיפה** ציינה בתשובתה למשרד מבקר המדינה ממרץ 2022 (להלן - תשובת עיריית חיפה) כי היא תקצבה כ-1.7 מיליון ש"ח עבור אבטחת המידע במסגרת תקציבה לשנת 2022, זאת בעקבות סקר סיכונים ומבדק חדירה[28] שביצעה העירייה.

עיריית **ראש העין** ציינה בתשובתה למשרד מבקר המדינה ממרץ 2022 (להלן - תשובת עיריית ראש העין) כי היא תפעל לשפר את תקצוב נושא מערכות המידע.

בתשובת עיריית **שפרעם** למשרד מבקר המדינה ממרץ 2022 (להלן - תשובת עיריית שפרעם) צוין כי אין לעירייה תוכניות עבודה רב-שנתיות בתחום מערכות המידע, שכן בהיעדר משאבים אין באפשרותה להתפתח בתחום, והיא הסתפקה ברכישת מערכות מידע בסיסיות בלבד. עוד ציינה העירייה כי לבקשתה היא נכללה בפיילוט של רשויות מקומיות בתחום הדיגיטציה, בהובלת "ישראל דיגיטלית", והחלה בהליך איתור וגיוס מתאם דיגיטציה, אפיון כלל מערכות המידע בעירייה והכנת תוכנית עבודה אסטרטגית רב-שנתית בנושא המחשוב.

28 לעניין זה ראו בפרק בנושא "הגנת סייבר ואבטחת מידע", בתת הפרק "ביצוע מבדקי החדירה וסקרי הסיכונים ברשויות שנבדקו".

על הרשויות המקומיות גדרה, יוקנעם, מטה בנימין, נתיבות, עין מאהל ושפרעם להכין תוכנית עבודה אסטרטגית שתשמש בסיס לתוכניות עבודה שנתיות ולהגישה להנהלת הרשות כדי שתדון בה, תבחן אם ניתן ליישמה במסגרת תקציבה ותפעל בהתאם ליישומה.

המועצה המקומית **גדרה**, עיריית **יוקנעם** והמועצה האזורית **מטה בנימין** ציינו בתשובותיהן למשרד מבקר המדינה ממרץ 2022 (להלן - תשובת המועצה המקומית גדרה, תשובת עיריית יוקנעם ותשובת המועצה האזורית מטה בנימין, בהתאמה) כי הן יפעלו להכנת תוכניות עבודה אסטרטגיות רב-שנתיות מקושרות תקציב.

עיריית **נתיבות** ציינה בתשובתה למשרד מבקר המדינה ממרץ 2022 (להלן - תשובת עיריית נתיבות) כי היא הכינה תוכנית עבודה רב-שנתית לשנים 2021 - 2022.

# הניהול הטכני של מערכות המידע ברשויות המקומיות

## בעלי התפקידים בתחום מערכות המידע

באוגדן תיאורי תפקידים האחרון שפרסם משרד הפנים בדצמבר 2020 (להלן - אוגדן תיאורי התפקידים או האוגדן) נכללו תיאורי תפקידים של שישה בעלי תפקיד בתחום המחשוב ומערכות המידע, כמפורט להלן:

**מנהל אבטחת מידע:** סעיף 17ב לחוק הגנת הפרטיות קובע כי גוף ציבורי, ובכלל זה רשות מקומית, חייב למנות אדם בעל הכשרה מתאימה לממונה על אבטחת מידע (להלן - מנהל או ממונה אבטחת מידע). על פי האוגדן, מנהל אבטחת מידע ברשות המקומית אחראי לתחומים אלה: תכנון מדיניות אבטחת המידע ובקרה על יישומה; תכנון סקרי אבטחת מידע וביצועם; ניהול ההרשאות ודרכי הגישה למשתמשים; תכנון ויישום של תוכנית להתאוששות מאסון (DRP); וניהול ההגנה על מערכות המידע והתקשורת. באוגדן נקבע כי מנהל אבטחת המידע יהיה כפוף למנמ"ר הרשות.

**מנהל מערכות מידע ראשי (המנמ"ר):** לפי האוגדן, מנמ"ר הרשות המקומית אחראי לאלה: אספקת מערכות מחשוב ושירותי מחשוב לרשות; גיבוש ויישום של מדיניות מערכות מידע ברשות בהלימה לאסטרטגיה ולתהליכי העבודה של הרשות; תכנון תוכניות עבודה וניהול התקציב בתחום מערכות המידע; ניהול עובדים וספקים של מערכות המידע; וניהול התקשרויות ורכש בתחום מערכות המידע. באוגדן נקבע כי המנמ"ר יהיה כפוף למנכ"ל הרשות. יצוין כי לא נקבעה באוגדן החובה למנות מנמ"ר לרשות המקומית.

**מנהל שירותים דיגיטליים:** לפי האוגדן, מנהל השירותים הדיגיטליים ברשות אחראי לאלה: ניהול תחום הדיגיטל ברשות; הזנת תכנים ועדכונם השוטף בפלטפורמות הדיגיטליות השונות;

ניהול מערכת התוכן של הכלים הדיגיטליים; עידוד השימוש בכלים דיגיטליים למתן שירותים לתושב ולהנגשתם לציבור; הכנת הפלטפורמות הדיגיטליות לשעת חירום במסגרת מתן השירות הדיגיטלי לתושב.

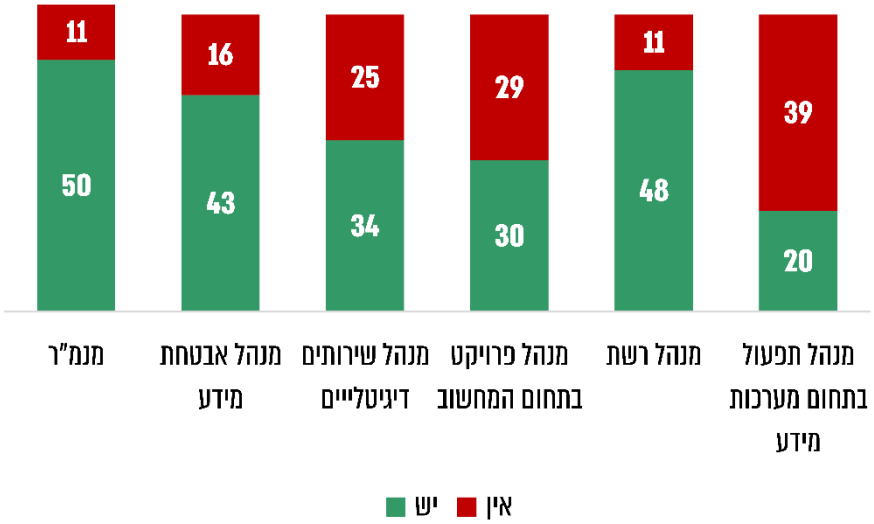
**מנהל פרויקט (בתחום המחשוב):** לפי האוגדן, תחומי האחריות של מנהל פרויקט בתחום המחשוב הם אלה: הגדרת צורכי הרשות בעניין פרויקטים הנוגעים למערכות המידע; הובלת פרויקטים הקשורים למערכות המידע של הרשות; והטמעה ויישום של כלים מתקדמים ופתרונות מידע ותקשורת בקרב משתמשי הרשות.

**מנהל רשת:** לפי האוגדן, תחומי האחריות של מנהל הרשת הם: ניהול ותפעול של רשת המשתמשים (שרתים, עמדות קצה, ציוד תקשורת וציוד היקפי) של הרשות וניהול יישומי תוכנה.

**מנהל תפעול (בתחום מערכות מידע):** לפי האוגדן, תחומי האחריות של מנהל התפעול בתחום המחשוב הם: תמיכה במשתמשי מערכות המידע והתקשורת ברשות; תפעול ותחזוקה של מערכות המידע והתקשורת.

במסגרת השאלון התבקשו הרשויות המקומיות לציין אילו תפקידים מאיישת הרשות בתחום המחשוב ומערכות המידע. להלן הנתונים שנמסרו:

תרשים 9: **איוש התפקידים בתחום מערכות המידע ברשויות המקומיות**




על פי הנתונים שנאספו בשאלון, בעיבוד משרד מבקר המדינה.

מהנתונים עולה כי כ-82% מ-61 הרשויות שענו לשאלה בשאלון מעסיקות מנמ"ר, כ-81% מהן מעסיקות מנהל רשת, כ-73% מהן מעסיקות מנהל אבטחת מידע, כ-58% מהן מעסיקות מנהל שירותים דיגיטליים, כ-51% מעסיקות מנהל פרויקטים בתחום המחשוב, וכ-34% מעסיקות מנהל תפעול בתחום מערכות מידע.

בלוח שלהלן מפורט אילו תפקידים אוישו ברשויות שנבדקו:

לוח 2: **התפקידים שאוישו ברשויות שנבדקו**

| | מנמ"ר | מנהל אבטחת מידע | מנהל שירותים דיגיטליים | מנהל פרויקט בתחום המחשוב | מנהל רשת | מנהל תפעול בתחום מערכות מידע |
|---|---|---|---|---|---|---|
| **גדרה*** | ✗ | ✗ | ✗ | ✗ | ✓ | ✓ |
| **חיפה** | ✓ | ✓ | ✓ | ✓ | ✓ | ✗ |
| **יוקנעם** | ✓ | ✓ | ✗ | ✗ | ✓ | ✗ |
| **מטה בנימין** | ✓ | ✓ | ✗ | ✗ | ✓ | ✗ |
| **נתיבות** | ✓ | ✓ | ✗ | ✗ | ✗ | ✗ |
| **עין מאהל** | ✓ | ✗ | ✗ | ✗ | ✓ | ✗ |
| **ראש העין** | ✓ | ✓ | ✗ | ✗ | ✓ | ✗ |
| **שפרעם** | ✓ | ✓ | ✗ | ✗ | ✗ | ✗ |

על פי מידע שנאסף בביקורת, בעיבוד משרד מבקר המדינה.

* שירותי המחשוב של המועצה ניתנים לה במיקור חוץ על ידי חברה ב'. במסגרת זו מקבלת המועצה חלק מהשירותים שבאחריות בעלי התפקידים שאינם מאוישים ברשות.

מהלוח שלעיל עולה כי כל הרשויות המקומיות שנבדקו, להוציא המועצה המקומית גדרה, מעסיקות מנמ"ר; כי לגדרה ולעין מאהל אין מנהל אבטחת מידע; וכי כל הרשויות שנבדקו, למעט נתיבות ושפרעם, מאיישות את התפקיד של מנהל רשת. עוד עולה מהלוח כי למעט עיריית חיפה, כל הרשויות שנבדקו אינן מעסיקות מנהל שירותים דיגיטליים ומנהל פרויקט בתחום המחשוב.

עוד נמצא כי מבין כל הרשויות שנבדקו, המועצה המקומית גדרה מקבלת את כל שירותי המחשוב שלה באמצעות חברה ב', במסגרת הסכם שנחתם בין הצדדים ביולי 2015. יצוין כי המועצה מעסיקה מנהל תפעול בתחום המחשוב, המשמש בין היתר איש הקשר בינה ובין החברה.

בתשובת המועצה המקומית **גדרה** צוין כי המועצה מקבלת את כל שירותי המחשוב שלה באמצעות חברה ב', וכי התפקידים הבאים מאוישים על ידי החברה מתוקף ההסכם עימה: מנהל מערכות מידע, מנהל אבטחת מידע, מנהל פרויקט בתחום המחשוב עוד ציינה המועצה כי היא תבחן שימוש "בשירותי מנמ"ר אשכול שורק דרומי לצורכי המועצה בתחום מערכות המידע האפליקטיביות", וכן לצורכי איוש תפקיד מנהל השירותים הדיגיטליים.

יוצא אפוא כי ברשויות שאינן מאיישות חלק מהתפקידים המפורטים לעיל בתחום המחשוב אמור המנמ"ר למלא תפקידים אלה על פי הצורך, והדבר עלול להגדיל את עומס העבודה המוטל עליו, לפגוע בתפקודו התקין וביכולתו לבצע את משימותיו.

בתשובת המועצה האזורית **מטה בנימין** צוין כי איוש כוח האדם במועצה מבוצע בהתאם לצורכי המועצה ובהתאם לשיקולים תקציביים וארגוניים. עוד ציינה המועצה כי צרכי כוח האדם בתחום המחשוב ומערכות המידע ייבחנו על ידי מנמ"ר המועצה וכי לאחר מועד סיום הביקורת, המועצה איישה את תפקיד רכזת תחום שירותים דיגיטליים.

בתשובת עיריית **נתיבות** צוין, כי היא ערה לחשיבות התפקידים ולצורך באיושם ולכן היא עתידה לאייש משרה נוספת בתחום המחשוב במהלך שנת 2022, וכי יש קושי תקציבי לאייש את כל המשרות בתחום.

עיריית **ראש העין** ציינה בתשובתה כי היא תבחן את הוספת התפקידים הלא מאוישים בהתאם לצרכיה ולתקציבה.

עיריית **שפרעם** מסרה בתשובתה כי בשנת 2019 היא איישה את תפקיד מנהל השירותים הדיגיטליים ואת תפקיד מנהל הרשת במשרה חלקית, אולם הדבר לא צלח והתפקידים כיום אינם מאוישים. העירייה הוסיפה כי תפעל לגיוס כוח אדם בהתאם לצרכיה.

על הרשויות המקומיות ובכללן המועצה המקומית גדרה לפעול לאייש את תפקיד מנהל אבטחת המידע, גם אם במיקור חוץ, וכן להסדיר את מינויו באמצעות כתב מינוי. כמו כן, מומלץ שהרשויות שנבדקו יבחנו את הצורך באיוש התפקידים הפנויים בתחומי המחשוב, כל אחת בהתאם לצרכיה ולתקציבה.

## מינוי מנהל מערכות מידע ראשי (מנמ"ר)

כאמור, במסגרת תפקידו, המנמ"ר אחראי על הניהול הכולל והתפעול השוטף של תחום מערכות המידע, לרבות אספקת מערכות מחשוב ושירותי מחשוב לרשות, גיבוש ויישום של מדיניות מערכות מידע ברשות, תכנון תוכניות עבודה וניהול התקציב בתחום מערכות המידע.

הבדיקה העלתה כי עיריות **חיפה**, **נתיבות**, **ראש העין** ו**שפרעם** מעסיקות מנמ"ר שהוא עובד הרשות אשר נבחר בהליך מכרזי ומועסק על ידי הרשות בחוזה מיוחד; במועצה האזורית **מטה בנימין** מועסק כמנמ"ר - במסגרת חוזה מיוחד - עובד הרשות שנבחר למנהל מחשוב בשנת 2007 ואינו עומד בתנאי המכרז הנוכחיים לתפקיד זה; במועצה המקומית **עין מאהל** ממלא את

תפקיד המנמ"ר עובד הרשות שלא השתתף בהליך מכרז; בעיריית **גדרה** אין מנמ"ר, ובעיריית **יוקנעם** תפקיד המנמ"ר מאויש במסגרת מיקור חוץ.

במהלך הביקורת, באוקטובר 2021, מסרה המועצה המקומית **עין מאהל** למשרד מבקר המדינה כי היא עתידה לפרסם בקרוב מכרז לאיוש תפקיד המנמ"ר בה, ונכון למועד סיום הביקורת המכרז לא פורסם. המועצה האזורית **מטה בנימין** פרסמה ארבעה מכרזים חיצוניים לאיוש תקן מנמ"ר ביוני ובדצמבר 2020 ובאפריל ובאוגוסט 2021. מכרז נוסף פורסם לאחר מועד סיום הביקורת, וועדת המכרזים עתידה להתכנס בינואר 2022.

נוכח החשיבות של תפקיד המנמ"ר ברשות המקומית, בהיותו אחראי לניהול כל מערכות המידע בה, לרבות הניהול האסטרטגי והתקציבי, מומלץ למועצות המקומיות גדרה ועין מאהל לבצע מכרזים לאיוש תפקיד המנמ"ר ברשות. כמו כן, מומלץ כי עיריית יוקנעם תשקול לאייש את תפקיד המנמ"ר בעובד מן המניין. מומלץ למועצה האזורית מטה בנימין לפעול להשלמת הליכי המכרז לאיוש תפקיד המנמ"ר.

בתשובת המועצה האזורית **מטה בנימין** צוין כי הליך מכרז מנמ"ר המועצה הסתיים בהצלחה, והתפקיד אויש לאחר מועד סיום הביקורת.

## כפיפות המנמ"ר ברשות המקומית

כפי שנקבע באוגדן, המנמ"ר יהיה כפוף למנכ"ל הרשות שבה הוא מועסק. הדבר נועד להקנות למנמ"ר עצמאות וחופש פעולה במילוי תפקידו ובקידום התהליכים שבתחום אחריותו וכן נועד לאפשר לו לקבל את הסיוע הדרוש לו בקידום תהליכים רוחביים כגון דיגיטציה ברשות, פיתוח תוכנות ואפליקציות ושדרוג תשתיות הרשות. הכפפתו של המנמ"ר למנכ"ל הרשות המקומית מעידה כי הוא ממלא תפקיד מרכזי בהליך קבלת ההחלטות בנושא ניהול מערכות המידע ברשות.

נמצא כי הכפיפות של המנמ"ר ברשויות המקומיות חיפה, מטה בנימין, נתיבות, עין מאהל ושפרעם היא למנכ"ל; ביוקנעם המנמ"ר כפוף למנהל הרכש; בראש העין המנמ"ר כפוף למנכ"ל מהבחינה המקצועית ולמנהל האגף הכללי בעירייה בעניינים המינהלתיים. יצוין כי בעירייה לא נקבעה כפיפות כאמור במסמך מחייב, ובפועל לא ברורה חלוקת האחריות והסמכויות בין המנכ"ל למנהל האגף הכללי.

על עיריות יוקנעם וראש העין למלא את הדרישות שנקבעו באוגדן תיאורי התפקידים, ולהכפיף את המנמ"ר שלהן למנכ"ל העירייה.

בתשובת עיריית **ראש העין** צוין כי מנכ"ל העירייה יפרסם הבהרה בכתב בדבר הכפפת מנמ"ר העירייה למנכ"ל באופן מלא.

## תכולת עבודתו של המנמ"ר

כפי שמתואר באוגדן, המנמ"ר אחראי לספק לרשות מערכות מחשוב ושירותי מחשוב, לגבש וליישם את מדיניות מערכות המידע בה בהלימה לאסטרטגיה ולתהליכי העבודה שלה, לתכנן תוכניות עבודה ולנהל את התקציב, הרכש וההתקשרויות בתחום מערכות המידע ברשות המקומית.

נמצא כי המנמ"רים בעיריות יוקנעם, נתיבות ושפרעם, במועצה המקומית עין מאהל ובמועצה האזורית מטה בנימין עוסקים בניהול השוטף של מערכות המחשוב ברשות ובקידום פרויקטים נקודתיים, בין היתר במסגרת קולות קוראים - כגון שדרוג מערכות המחשוב ברשות - ואינם יוזמים הכנה של תוכניות עבודה אסטרטגיות ותוכניות עבודה מקושרות תקציב. בעיריות חיפה וראש העין המנמ"רים עוסקים, נוסף על הניהול השוטף של מערכות המחשוב ברשות, גם במיפוי ובתכנון אסטרטגי ובהכנת תוכניות עבודה.

**עיריית שפרעם**: המנמ"ר של העירייה נבחר לתפקיד מנהל אגף מערכות מידע בשנת 1993. נוסף על המנמ"ר מועסק באגף עובד תחזוקה שאמור לטפל בקריאות עובדי העירייה הקשורות לנושא המחשוב. נוסף על תפקידו, באפריל 2016 התקבל המנמ"ר לתפקיד מנהל אגף משאבי אנוש לאחר שזכה במכרז שפרסמה העירייה למילוי תפקיד זה. מאז ועד למועד סיום הביקורת, בנובמבר 2021, המנמ"ר ממלא את שני התפקידים בו זמנית. באגף משאבי אנוש מועסק מלבד המנמ"ר עובד בתפקיד חשב שכר. בפגישה שנערכה עם המנמ"ר במהלך הביקורת ציין כי הוא משקיע את רוב זמן עבודתו באגף משאבי אנוש, ואת הזמן הנותר במילוי תפקידו כמנמ"ר. כמו כן ציין המנמ"ר כי הוא מתקשה למלא את שני התפקידים בו זמנית ללא סיוע, וכי נדרש לתת מענה שוטף בעניינים הקשורים לשני התפקידים, וציין כי הדבר פוגע בתפקודו ובאיכות השירותים שהוא אמור לספק.

מילוי שני התפקידים בו זמנית על ידי המנמ"ר, ללא תוספת כוח אדם, מעמיס עליו מעבר למקובל ואף עלול לפגוע בתפקודו התקין. מומלץ שעיריית שפרעם תבחן את הנושא ותפעל למציאת פתרון לסוגיה זו.

עיריית **שפרעם** ציינה בתשובתה כי היא נמצאת בהליך מכרזי לאיוש משרת מנהל משאבי אנוש, וכי הדבר יביא לשחרור המנמ"ר מתפקידו הנוסף כמנהל משאבי אנוש ויאפשר לו לעסוק באופן בלעדי בתפקידו.

## מעמדו ותנאי העסקתו של המנמ"ר ברשות המקומית

במהלך הביקורת הציג המנמ"ר של מרכז השלטון המקומי את עמדת מרכז השלטון המקומי בעניין תפקיד המנמ"ר ברשות המקומית, וזאת בעיקר בשני היבטים: האחד - בנוגע לכפיפות של המנמ"ר ולביסוס מעמדו, והשני בנוגע לשכרו. המנמ"ר ציין כי מרכז השלטון המקומי קיים כמה שיחות ומפגשים עם נציגי משרד הפנים כדי לקדם את סוגיית מעמדו ושכרו של המנמ"ר ברשות המקומית. לדוגמה, בנובמבר 2020 התקיימה שיחה עם נציגי משרד הפנים, בראשות סמנכ"ל

בכיר למינהל והון אנושי בפועל, בנושא היוועצות בעניין ניהול IT[29] בשלטון המקומי. בשיחה זו "הבהרנו את עמדתנו ודעתנו כי בעידן הדיגיטלי העסקי המנמ"ר חייב להיות חבר בהנהלה הבכירה ביותר של הרשות (כפיפות ודיווח ישירות למנכ"ל) וכפועל יוצא מזה העלאת שכרו ושכרם של כל אנשי הטכנולוגיה ברשות".

מנמ"ר מרכז השלטון המקומי ציין עוד כי למשרד הפנים הוצג הקושי הרב של הרשויות לגייס כוח אדם איכותי לשורותיהן. מדובר בקושי בגיוס עובדים בכל תחומי הטכנולוגיה (טכנאים, מנהלי רשתות, עובדים בתחום התשתיות ובתחום הדיגיטציה וכו'), והקושי מחריף בתחום אבטחת המידע. דרגות השכר של המנמ"רים ואנשי הטכנולוגיה ברשויות המקומיות נמוכות מדרגות השכר של בעלי אותם תפקידים במגזר הממשלתי ומכאן ששכרם נמוך מהשכר במגזר הממשלתי.

נמצא כי בעקבות פגישות ושיחות של מרכז השלטון המקומי עם משרד הפנים הושווה באפריל 2019 שכר בעלי התפקידים בתחום המחשוב לשכרם של עובדי המדינה בתחום, אולם הדבר נעשה באמצעות העסקתם בחוזים אישיים ולא על ידי העלאת דירוג תפקידם.

מנמ"ר מרכז השלטון המקומי הבהיר כי השוואת שכר זו איפשרה לקלוט עובדי מחשוב לתפקידים ברמות נמוכות, כגון טכנאים, בשכר סביר, אולם לא פתרה את בעיית השכר של הדרג הניהולי והמקצועי בתחום המחשוב כגון מנמ"רים ומנהלי מחלקות, והרשויות המקומיות עדיין מתקשות להתמודד עם השוק החופשי אשר מציע משכורות ותנאי שכר גבוהים בהרבה מאלה שמציעות להם הרשויות המקומיות. במצב זה רשויות מקומיות מפרסמות מכרזים לקליטת עובדים כמה פעמים, וכאשר הניסיונות לא צולחים הן פונות לחברות חיצוניות לאיוש המשרות.

נמצא כי בכל הרשויות המקומיות שנבדקו שבהן מועסקים מנמ"רים בתור עובדי הרשות הם מועסקים בחוזים מיוחדים שלפיהם שכרם הוא בשיעור של 30% עד 80% משכרו של מנכ"ל הרשות מקומית. דבר זה תלוי בשיקול דעתה של הרשות המקומית, בכפוף לאישור משרד הפנים, ויוצר חוסר אחידות ופערים בין הרשויות השונות מבחינת השכר המשולם לבעלי אותם תפקידים.

עוד ציין מנמ"ר מרכז השלטון המקומי כי בשיחה נוספת עם נציגי משרד הפנים, שהתקיימה ביוני 2021, השתתפו בין היתר סמנכ"ל בכיר למינהל והון אנושי בפועל במשרד הפנים וכן יו"ר איגוד המנמ"רים. בשיחה זו הוצגו שוב סוגיות מצוקת השכר והכפיפות של המנמ"רים ברשויות המקומיות. בשיחה נוספת שהתקיימה בהמשך אותו החודש עם נציגי משרד הפנים סוכם כי משרד הפנים יפעל עם מרכז השלטון המקומי לקידום מעמדו ושכרו של המנמ"ר ברשות המקומית, אולם נמצא כי במועד סיום הביקורת לא נעשו פעולות נוספות לקידום הנושא.

29 טכנולוגיות מידע - Information Technology.

לנוכח הסכנות הגוברות הטמונות בהפעלת מערכות מידע למיניהן ברשויות המקומיות, העלולות לגרום נזקים ניכרים לרשויות ולתושביהן - החל בפגיעה בתשתיות פיזיות, עבור דרך שיבוש באספקת שירותים חיוניים לתושבים וכלה בפגיעה בפרטיותם - יש לשים דגש בסוגיית ההתמודדות עם סכנות אלה באמצעות ניהול מערכות המידע ברשויות המקומיות. כמו כן מתחדד הצורך בהעסקת עובדים מקצועיים ומיומנים ובביסוס מעמדו של המנמ"ר ברשות המקומית - הן מבחינת שכרו והן מבחינת מקומו במדרג הארגוני של הרשות - על מנת שיהיה ניתן לקלוט בשורותיהן של הרשויות המקומיות עובדים בעלי ידע מקצועי ראוי שיאפשרו להן להתמודד עם הקדמה וההתפתחויות הטכנולוגיות ועם האתגרים והאיומים הכרוכים בהן.

מומלץ כי משרד הפנים, בשיתוף מרכז השלטון המקומי, ישלימו את הפעולות הנדרשות לקידום מעמדו ושכרו של המנמ"ר ברשות המקומית.

משרד הפנים ציין בתשובתו כי כחלק מחיזוק מעמדו של המנמ"ר ברשות המקומית, אגף בקרת ההון האנושי במשרד הגדיר את משרת המנמ"ר כ"משרת ליבה חיונית" בכל רשות מקומית, ולכן לא נדרש אישור משרד הפנים לאיוש המשרה הניהולית של המנמ"ר. אשר לסוגיית שכר המנמ"ר ציין המשרד בתשובתו כי אם המשרה מוגדרת במסגרת המבנה הארגוני של הרשות כמחלקה או כאגף, המשרד מאשר חוזה אישי בהתאם לכללים החלים על הרשויות המקומיות. המשרד אף ציין כי הוא פעל בשיתוף עם איגוד המנמ"רים ומרכז השלטון המקומי לעדכון תיאור תפקיד המנמ"ר באוגדן תיאורי התפקידים.

# הגנת סייבר ואבטחת מידע

1. ברשויות המקומיות מצטברת כמות עצומה של מידע אישי על תושבי הרשות, שמקורו במאגרים שונים. פגיעה במערכות הממוחשבות ובמאגרי המידע של הרשויות המקומיות עלולה לגרום לנזקים כבדים, כגון דליפת מידע אישי של תושבי הרשות, פגיעה בצנעת הפרט ופגיעה בשירותים הניתנים לתושבים ואף בתשתיות בתחום הרשויות. לפיכך מחויבות הרשויות המקומיות להגן על המידע הנמצא במאגרים הללו ולנהלם באופן מאובטח, תוך הקפדה על הוראות החוק בנושא זה[30], חובה המוטלת עליהן בהיותן הבעלים והמנהלים של מאגרי המידע הללו[31].

במערכות המידע שני מרכיבים עיקריים - חומרה (Hardware) ותוכנה (Software). חומרה מוגדרת כאוסף של כל הרכיבים הפיזיים במחשב עצמו (כגון לוח אם[32], ספק כוח, כרטיס גרפי וכרטיס קול). למעשה ניתן לומר שכל התקן פיזי המחובר למחשב ומשמש לצורך פעילותו נחשב חומרה. תוכנה מוגדרת כאוסף של הוראות הניתנות לביצוע על ידי מחשב.

30 משרד המשפטים - הרשות להגנת הפרטיות, **מדריך הגנת הפרטיות לעיר החכמה** (ינואר 2020).

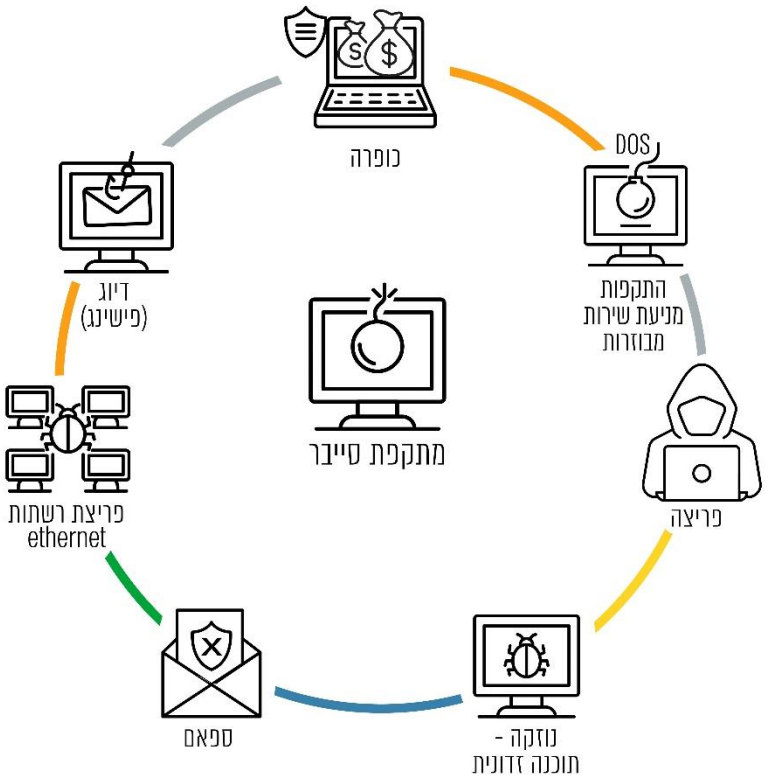
31 סעיף 17 לחוק הגנת הפרטיות קובע כי "בעל מאגר מידע, מחזיק במאגר מידע או מנהל מאגר מידע, כל אחד מהם אחראי לאבטחת המידע שבמאגר המידע".

32 שעליו מורכבים המעבד, הזיכרון הראשי של המחשב ורכיבים נוספים.

נהוג לסווג את התוכנה לשני סוגים; האחד - תוכנת תשתית, המנהלת את התוכניות והנתונים במחשב ונותנת שירותים לסוגי תוכנה אחרים המתבצעים במחשב (כגון מערכת ההפעלה במחשב); והשני - תוכנת יישום, שתפקידה להשיג מטרה מסוימת לשימוש ארגון או עבור משתמש ביתי.

מערכות המחשוב והתשתיות של הרשויות המקומיות חשופות לאיומי סייבר מתוחכמים וחמורים ולמתקפות הרסניות, תדירות ומסוכנות מצד גורמים עוינים שונים, ולכן תחום הגנת הסייבר ואבטחת המידע נעשה קריטי וחיוני להתמודדות עם איומים אלה. בתרשים שלהלן מתוארים סוגים נפוצים של איומי סייבר:

תרשים 10: **סוגים נפוצים של איומי סייבר שאיתם מתמודדות הרשויות המקומיות**



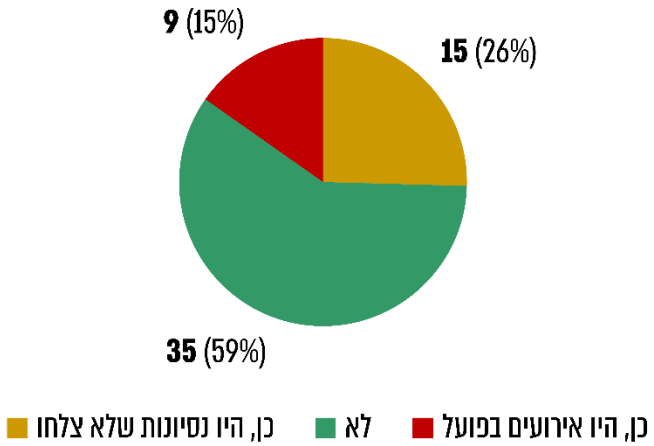

התרשים בעיבוד משרד מבקר המדינה.

ממחקר שבוצע בשנת 2018[33] ניתן ללמוד על פערים בין רשויות רבות בישראל מבחינת מוכנותן להתקפות סייבר. מהמחקר עולה כי יש רשויות שלהן מערכות מידע העומדות בחזית הטכנולוגיה ומסוגלות לספק פתרונות המאפשרים להתמודד עם התקפות סייבר. לעומת זאת, יש רשויות החסינות פחות בפני התקפות סייבר, שכן אין ברשותן המשאבים, כוח האדם והידע הדרוש כדי להתמודד עם התקפות סייבר בעידן הנוכחי.

גם מבקר המדינה עמד בדוחות קודמים על החולשות הקיימות בהיבטי הגנת הפרטיות ואבטחת המידע ברשויות המקומיות. למשל, בדוח שפורסם במאי 2020 צוין כי חלק מהרשויות המקומיות אינן ערוכות להתמודד כראוי עם מתקפות סייבר, כפי שנדרש ומצופה מהן[34].

2. באחת השאלות שבשאלון התבקשו הרשויות לציין אם בשלוש השנים האחרונות (2019 - 2021) התרחשו בהן אירועי אבטחת מידע או שהיו חשופות לאיומי סייבר, ומתשובותיהן של הרשויות על שאלה זו התקבלו הנתונים שלהלן:

תרשים 11: **מספר הרשויות שדיווחו על אירועי אבטחת מידע או על איומי סייבר, 2019 - 2021**




על פי הנתונים שנאספו בשאלון, בעיבוד משרד מבקר המדינה.

מהאמור לעיל עולה כי 24 (כ-41%) מ-59 הרשויות המקומיות שענו על השאלה ציינו שחוו ניסיונות להתקפות סייבר או אירועי סייבר בשנים 2019 - 2021[35].

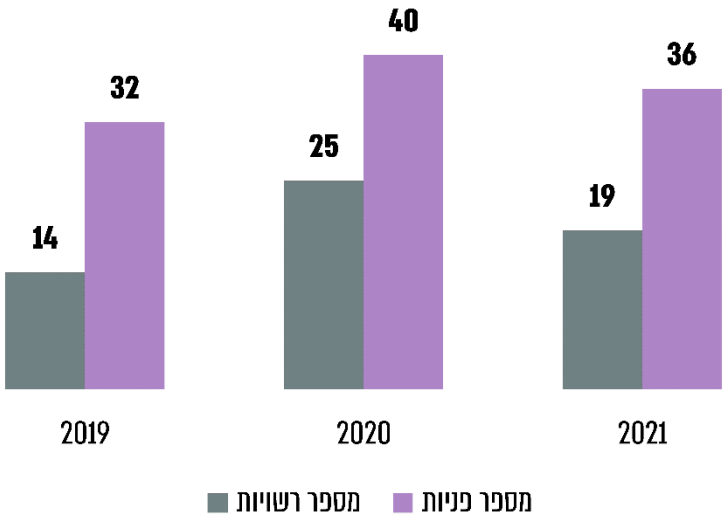
33 טלי חתוקה (עורכת), **העיר בעידן הדיגיטלי: תכנון, טכנולוגיה, פרטיות ואי-שוויון** (2018).

34 ראו הערת שוליים מס' 21.

35 הנתונים נכונים לאוקטובר 2021. יש להניח כי יש רשויות שחוו ניסיונות להתקפות סייבר, שהן כלל אינן ערות להן.

בתרשים שלהלן יוצגו נתונים שהמציא מערך הסייבר, לבקשת משרד מבקר המדינה, בנוגע למספר הפניות של רשויות מקומיות למרכז לניהול אירועי סייבר ולמספר הרשויות שפנו למרכז בשנים 2019 - 2021[36]:

תרשים 12: **מספר הפניות מרשויות מקומיות ומספר הרשויות המקומיות שפנו למרכז לניהול אירועי סייבר, 2019 – 2021**




על פי נתוני מערך הסייבר, בעיבוד משרד מבקר המדינה.

מנתוני מערך הסייבר עולה כי חל גידול של 25% במספר הפניות בין שנת 2019 לשנת 2020, ולעומת זאת מספרן פחת בכ-10% בשנת 2021. עוד עולה מהנתונים ש-14 (כ-5%) מ-257 הרשויות המקומיות פנו למרכז לניהול אירועי סייבר בשנת 2019, לעומת 25 (כ-10%) מהרשויות שפנו למרכז בשנת 2020, ו-19 (כ-7%) מהרשויות שפנו למרכז בשנת 2021.

נוכח שיעורן הגדול של הרשויות שציינו בשאלון שחוו אירועי סייבר (ניסיון או תקיפה של ממש), שהסתכם כאמור בכ-41%, ניתן היה לצפות למספר גדול בהרבה של רשויות מקומיות (כ-100 רשויות מקומיות בשלוש שנים, בהתאם ליחס), שיפנו למרכז לניהול אירועי סייבר בהתרחש אירוע כאמור. בפועל, בתקופה שנבדקה (מינואר 2019 עד דצמבר 2021) התקבלו במצטבר 108 פניות מ-32 רשויות במרכז לניהול אירועי סייבר, והדבר עלול להעיד על פער בין הרשויות מבחינת מודעותן לקיומו של המרכז ולאפשרות לקבל סיוע ממנו בהתרחש אירוע סייבר.

36 יש רשויות שפנו יותר מפעם אחת.

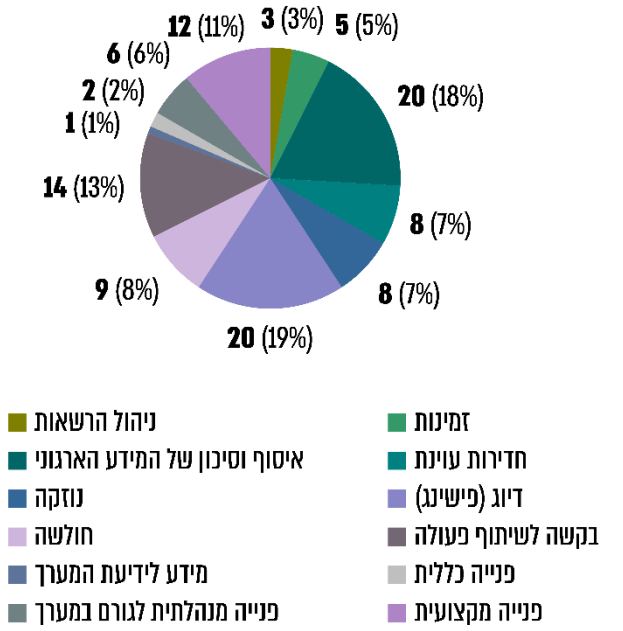
עלה כי שתיים מהרשויות שנבדקו, ז' ו- ה', דיווחו במסגרת השאלון כי הן חוו אירועי אבטחת מידע או איומי סייבר בשנים 2019 - 2021. הבדיקה העלתה כי הן לא פנו למרכז לניהול אירועי סייבר כדי לדווח על האירועים הללו.

הרשות המקומית ז' מסרה כי לא הייתה ערה בזמנו לעובדה כי חוותה תקיפה, אלא ייחסה את אירועי הסייבר האמורים לכשל מערכתי פנימי. הרשות המקומית ה' מסרה כי לא הייתה ערה לכך שחוותה תקיפה עד שקיבלה פנייה יזומה ממערך הסייבר, שזיהה את הפגיעות והמליץ לרשות כיצד להיערך להתמודדות עימן.

בתשובת רשות ה' צוין כי ממצא זה יועבר לטיפולו של מנהל אבטחת המידע החדש עם כניסתו לתפקיד.

בתרשים להלן יובאו נתוני מערך הסייבר בנוגע לסוגי הפניות מהרשויות המקומיות למרכז לניהול אירועי סייבר בשנים 2019 - 2021 (בסך הכול 108 פניות מ-32 רשויות מקומיות):

תרשים 13: **סוגי הפניות של הרשויות המקומיות, 2019 - 2021**




על פי נתוני מערך הסייבר, בעיבוד משרד מבקר המדינה.

מהתרשים עולה כי התקבלו פניות בנוגע לסוגים רבים של מתקפות בתחומים שונים וכי התחומים העיקריים של פגיעות שזוהו בשנים 2019 - 2021 היו פגיעות באמצעות דיוג (פישינג) (19%) וכן איסוף המידע הארגוני ואיום לפגוע בו (18%).

עלה כי כל הפניות שהתקבלו במרכז לניהול אירועי סייבר בשנים 2019 - 2021 היו מעיריות ולא ממועצות מקומיות או מועצות אזוריות.

נוכח נתוני מערך הסייבר והנתונים שנאספו באמצעות השאלון בנוגע לאיומי או לאירועי הסייבר שנחשפו אליהן הרשויות המקומיות, וכן נוכח הצורך בהתמודדות אפקטיבית עם הסכנות הטמונות בכך, משרד מבקר המדינה ממליץ למערך הסייבר לפעול בשיתוף אגף הסייבר במשרד הפנים להעלאת המודעות של הרשויות המקומיות לחשיבות הדיווח למרכז לניהול אירועי סייבר על אירועי סייבר שהן נחשפו להם ולאפשרות ההיוועצות עם מערך הסייבר. בפרט מומלץ למקד את ההסברה בקרב המועצות המקומיות והמועצות האזוריות בפגיעות שעלו מהפניות של הרשויות המקומיות במיוחד בנושאי דיוג (פישינג), איסוף המידע הארגוני ואיום לפגוע בו.

עוד מומלץ כי מערך הסייבר בשיתוף אגף הסייבר במשרד הפנים ישקלו להפיץ לרשויות המקומיות, את המידע בנוגע לפניות המתקבלות במרכז לניהול אירועי סייבר, בצירוף דוגמאות שמהן ניתן ללמוד כיצד לטפל ולהתמודד עם אירועים דומים.

בתשובת מערך הסייבר צוין כי הוא מקבל את ההמלצה לשיתוף וממליץ כי היחידה המגזרית תשמש ציר הקשר עם הרשות המקומית, וכאשר תתקבל פנייה למרכז לאירועי סייבר, הקשר לרשות המקומית ייעשה על ידי היחידה המגזרית באמצעות המנחה. עוד צוין כי מערך הסייבר יעביר לאגף הסייבר במשרד הפנים מידע טכני על המערכות הפגיעות, בלי לחשוף את שם הרשות שהותקפה. המשרד והרשויות המקומיות ייעזרו במידע זה לשם הפקת תובנות וכן לשם היערכות לאירועי סייבר.

בתשובת משרד הפנים צוין כי מערך הסייבר מכתיב את המדיניות בנושא הטיפול באירועי סייבר, ופעילות מינהל החירום במשרד הפנים נעשית בהתאם לתקציב הקיים. בתשובת משרד הפנים ממאי 2022 צוין כי הוא מקיים פעילות נרחבת להעלאת המודעות לאבטחת מידע ובכלל זה הוא מקיים בקרב הרשויות המקומיות הדרכות, בדגש על האיומים והמתקפות העדכניות ביותר, וכן בדגש על חשיבות הדיווח על אירועים אלה גם במסגרת הפעילות השוטפת.

על משרד הפנים לתת את דעתו לסוגיה, ולפעול בשיתוף פעולה עם מערך הסייבר בכל הקשור לפניות המתקבלות מהרשויות המקומיות, להעלאת תובנות, הגברת המודעות והפקת לקחים בקרב הרשויות המקומיות.

3. תקנות אבטחת המידע מפרטות את אופן יישומה 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, והן קובעות מנגנונים ארגוניים ודרישות מהותיות, שמטרתן להפוך את אבטחת המידע לחלק משגרת הניהול השוטף של הארגון. עוד קובעות התקנות

מאפיינים הנוגעים לסוג המידע, להיקפו ולגורם שהמאגר בבעלותו, שבהתאם להם נקבעת רמת האבטחה שחלה על מאגר המידע: בסיסית, בינונית או גבוהה[37].

לפי תקנות אבטחת המידע, 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. התקנות מגדירות שמאגר שבבעלות גוף ציבורי, כמו רשות מקומית, חלה עליו לכל הפחות רמת האבטחה הבינונית. עוד מגדירות התקנות 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 היחיד; מידע רפואי או מידע על מצבו הנפשי של אדם; מידע על נכסיו של אדם, על מצבו הכלכלי או על הרגלי צריכה שלו.

במסגרת הביקורת נבדק אם הרשויות המקומיות שנבדקו עומדות בדרישות תקנות אבטחת המידע בתחומים אלה: **רישום מאגרי מידע; מסמך הגדרות המאגר; מינוי ממונה על אבטחת מידע; נוהל אבטחת מידע; ניהול מצאי, הדרכות בנושא אבטחת מידע במעמד קליטת עובדים; הדרכות עובדים; ניהול הרשאות גישה; התקנים ניידים; בקרת גישה בחיבור מרחוק; אבטחת מחשוב; עדכון המערכות; מדיניות גיבויים ועריכתם; תוכנית להתאוששות מאסון; ביצוע מבדקי חדירה וסקרי סיכונים.** להלן פירוט הממצאים:

# מאגרי מידע

## רישום מאגרי מידע

בשל פוטנציאל הפגיעה בפרטיות הגלום במאגרי מידע ממוחשבים, חוק הגנת הפרטיות קובע, בין היתר, חובות החלות על בעלים, מנהלים ומחזיקים של מאגרי מידע, ובהן חובת רישומם של מאגרי המידע בפנקס המנוהל בידי רשם מאגרי המידע, אחריות לאבטחת המידע הנכלל במאגר המידע, ושמירת סודיותו של המידע והימנעות משימוש בו שלא למטרה שלשמה נמסר.

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 הזכויות והחובות המוטלות בחוק הגנת הפרטיות על בעלי המאגרים[38].

37 במאגרים שעליהם חלה רמת האבטחה הגבוהה, חלות כל תקנות אבטחת המידע. ההבדל העיקרי בין רמות האבטחה הוא שברמת אבטחה בינונית לא נדרש לבצע סקר סיכונים או מבדקי חדירה (אחת ל-18 חודשים). עם זאת נדרש כי גורם בעל הכשרה מתאימה לביקורת בנושא אבטחת מידע, שאינו ממונה האבטחה של המאגר, יבצע ביקורת פנימית או חיצונית על המאגר אחת ל-24 חודשים.

38 אתר המרשתת של הרשות להגנת הפרטיות: www.gov.il/he/Departments/Guides/registration_fqa?chapterIndex=1. במסגרת ביקורת זו לא נבדקו פעולות האכיפה של הרשות להגנת הפרטיות בנוגע לחובת רישום מאגרי המידע (להרחבה בנושא זה ראו מבקר המדינה, **דוח שנתי 69ב** (2019), "היבטים בהגנה על הפרטיות במאגרי מידע").

משרד מבקר המדינה השווה בין מספר מאגרי המידע של הרשויות שנבדקו אשר היו רשומים בפנקס מאגרי המידע במשרד המשפטים ובין מספר המאגרים שבידי הרשות[39]. להלן יפורטו ממצאי השוואתו:

לוח 3: **מספר מאגרי המידע ברשויות שנבדקו**

| שם הרשות | מספר המאגרים ברשות | מספר המאגרים הרשומים | מספר המאגרים הלא רשומים |
|---|---|---|---|
| ב' | 26 | 26 | - |
| ג' | 7 | 0 | 7 |
| ו' | 16 | 8 | 8 |
| ז' | 19 | 19 | - |
| ח' | 7 | 3 | 4 |
| א' | 15 | 8 | 7 |
| ד' | * | 0 | * |
| ה' | 9 | 8 | 1 |

על פי המידע שנאסף בביקורת, בעיבוד משרד מבקר המדינה.
* במועד סיום הביקורת הרשות המקומית ד' לא ציינה כמה מאגרי מידע יש ברשותה.

מהטבלה עולה כי במועד סיום הביקורת הרשות המקומית ד' לא ידעה מהם מאגרי המידע שבבעלותה ולא רשמה אותם. רשות ג' לא רשמה אף מאגר מידע שלה, הרשויות המקומיות ו' ו-ח' רשמו כ-50% וכ-43% ממאגרי המידע שלהן בהתאמה. הרשות המקומית א' ו-ה' רשמו כ-53% וכ-89% ממאגרי המידע שלהן בהתאמה, והרשות המקומית ב' רשמה את כל מאגרי המידע שלה.

על הרשויות המקומיות א', ג', ד', ה', ו', ו-ח' לפעול לרישום כל מאגרי המידע שלהן בפנקס מאגרי המידע במשרד המשפטים. כמו כן, על משרד המשפטים להנחות את הרשויות לפעול בהתאם לנקבע בתקנות אבטחת המידע ולבצע מעקב אחר יישום הוראות החוק.

39 הרשויות הן שדיווחו על מספר המאגרים שלהן. מספר המאגרים הרשומים נמסר למשרד מבקר המדינה על ידי הרשות להגנת הפרטיות במשרד המשפטים במרץ 2022.

בתשובת הרשות להגנת הפרטיות שבמשרד המשפטים למשרד מבקר המדינה ממרץ 2022 צוין כי הרשות פועלת רבות להעלאת רמת הגנת המידע והפרטיות ברשויות המקומיות, תוך השקעת משאבים רבים, לרבות הסברה, הדרכה הנגשה ואכיפה.

הרשות פירטה לצורך הדוגמה פעולות אלה: (א) כתיבת מדריך הגנת הפרטיות בעיר החכמה; (ב) פעילויות הסברה והדרכה; (ג) ייזום שיתופי פעולה בין הרשויות המקומיות וקידום סוגיות הנוגעות לפרטיות; (ד) אכיפה - הרשות השלימה בשנת 2021 פיקוח רוחבי ב-70 רשויות מקומיות המנהלות מידע אישי על יותר מ-5 מיליון תושבים בנושא הגנת הפרטיות ואבטחת המידע.

בתשובותיהן של הרשויות המקומיות א', ג' ו-ח' וכן בתשובת הרשות המקומית ד' למשרד מבקר המדינה ממרץ 2022 (להלן - תשובת הרשות המקומית ד') נמסר כי הן יפעלו לרישום כל מאגרי המידע שברשותן במשרד המשפטים.

בתשובת רשות ו' צוין כי עד למועד מתן התשובה פעלה הרשות לרישום שני מאגרי מידע נוספים, וכי היא פועלת להשלמת הרישום של שאר מאגרי המידע במשרד המשפטים.

משרד מבקר המדינה מציין לחיוב את הרשויות המקומיות ב' ו-ז' על רישום כל מאגרי המידע שלהן כנדרש.

## מסמך הגדרות מאגרי מידע

תקנות אבטחת המידע קובעות עוד כי על בעל המאגר להכין מסמך הגדרות מאגר, ובו יפורטו מאגרי המידע שברשותו ופרטים נוספים על המאגר לרבות סוגי המידע הכלולים בו, מטרות השימוש בו ושמו של מנהל מאגר המידע ושל המחזיק בו (שלעיתים אינו אותו גורם). עריכת המסמך מסייעת לרשות להגדיר מהי רמת האבטחה החלה עליה, התלויה במספר בעלי ההרשאה למאגרי המידע ברשות, מספר האנשים עליהם שמור מידע במאגרים ואופי המידע השמור.

נמצא כי הרשויות המקומיות שנבדקו ב', ג', ד', ה', ו', ז' ו-ח', לא הכינו מסמך הגדרות מאגרי מידע ולפיכך לא הגדירו את רמת האבטחה החלה על מאגרי המידע שלהן. עוד נמצא כי לרשות א' יש מסמך הגדרות מאגר ובו כל הפרטים כנדרש בתקנות.

על הרשויות המקומיות ב', ג', ד', ה', ו', ז' ו-ח' להכין מסמך הגדרות מאגר כנדרש בתקנות באופן שיוכלו להגדיר את רמת האבטחה החלה על מאגרי המידע שלהן.

רשות ב' צירפה לתשובתה מסמך הגדרות מאגר ובו פרטים על מאגרי המידע השונים שלה.

רשות ג' מסרה בתשובתה כי תפעל להכנת מסמך הגדרות מאגרי מידע כנדרש.

בתשובת הרשות המקומית ה' צוין כי המלצת משרד מבקר המדינה מקובלת עליה, וכי מנמ"ר הרשות הנכנס יידרש להסדיר את הנושא.

בתשובת רשות ו' צוין כי טיוטת נוהל אבטחת המידע הובאה לאישור בעלי התפקידים הרלוונטיים, והיא תובא לאישור מועצת הרשות בישיבתה הקרובה. עוד ציינה הרשות כי היא פועלת עם האשכול להגדיר את רמות האבטחה של מאגרי המידע.

רשות ח' ציינה בתשובתה כי הגדרת רמת אבטחת המידע מטופלת במסגרת הליך רישום מאגרי המידע במשרד המשפטים.

בתשובת רשות ז' צוין כי מנכ"ל הרשות ינחה את מנהלת מאגרי המידע של הרשות להכין את מסמך הגדרות מאגרי המידע וכן להגדיר את רמת האבטחה שלהם.

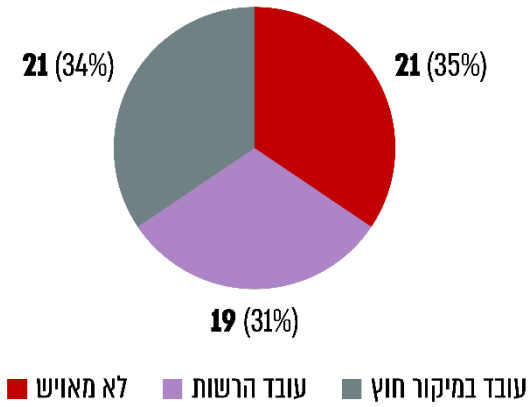
# ניהול אבטחת מידע

## מינוי ממונה או מנהל אבטחת מידע

כאמור, כל הגופים הציבוריים, ובכללם רשויות מקומיות, מחויבים למנות ממונה אבטחת מידע, שתפקידו לנהל את אבטחת המידע ברשות המקומית, בהתאם להוראות הדין, לנוהלי הרשות ולמדיניותה.

אחת השאלות שבשאלון הייתה האם הרשות מינתה ממונה אבטחת מידע, מהו אופן העסקתו ואם הוא עובד הרשות או עובד במיקור חוץ. מתשובותיהן של הרשויות על שאלה זו נאספו הנתונים שלהלן:

תרשים 14: **מספרן ושיעורן של הרשויות המעסיקות ממונה או מנהל אבטחת מידע ואופן העסקתו**




על פי הנתונים שנאספו מהשאלון, בעיבוד משרד מבקר המדינה.

מהנתונים עולה כי 21 (כשליש) מ-61 הרשויות שענו על השאלה בשאלון אינן מעסיקות ממונה אבטחת מידע כנדרש, וכי 21 מהרשויות המעסיקות ממונה אבטחת מידע, מעסיקות עובד במיקור חוץ לתפקיד זה.

מקרב הרשויות שנבדקו נמצא כי לרשויות המקומיות א' ו-ד' אין ממונה אבטחת מידע. רשויות ג', ו' ו-ח' מעסיקות ממונה על אבטחת מידע במיקור חוץ ובמשרה חלקית (הרשויות המקומיות ג' ו-ו' - 25% משרה במיקור חוץ; רשות מקומית ח' - 18 שעות חודשיות במיקור חוץ). רשות ז' מעסיקה מממונה אבטחת מידע במיקור חוץ במשרה מלאה, הרשויות המקומיות ב' ו-ה' מעסיקות מנהל אבטחת מידע כעובד הרשות במשרה מלאה.

לאור החובה המוטלת על הרשויות המקומיות לאייש את תפקיד ממונה אבטחת המידע ברשות, על כלל הרשויות המקומיות שלא מינו ממונה כאמור וביניהן הרשויות המקומיות א' ו-ד', לפעול לאיוש התפקיד. מומלץ כי משרד הפנים ינחה את הרשויות המקומיות לאייש את התפקיד.

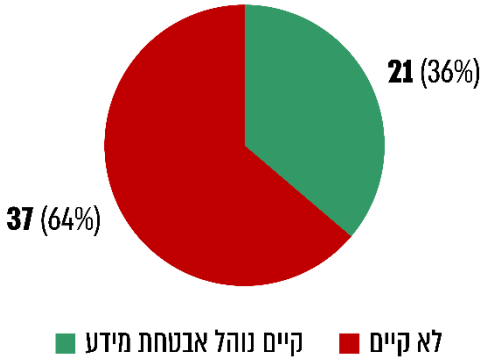
משרד הפנים מסר בתשובתו כי במסגרת עדכון תיאורי התפקידים בתחום המחשוב, אגף בכיר לבקרת ההון האנושי ברשויות המקומיות יסב את תשומת ליבן של הרשויות המקומיות לעצם קיומו של תיאור התפקיד של ממונה אבטחת מידע ולחשיבותו. בתשובת משרד הפנים ממאי 2022 ציין משרד הפנים כי במסגרת הדרכות המודעות שמקיימת היחידה המגזרית, חובת מינוי ממונה אבטחת מידע מצוינת ומודגשת להנהלות הרשויות המקומיות וכן כחלק מתוכניות העבודה שאגף הסייבר (היחידה המגזרית) ממליץ לרשויות המקומיות.

## נוהל אבטחת מידע

תקנה 3 לתקנות אבטחת המידע קובעת, בין היתר, כי על הממונה להכין נוהל אבטחת מידע ולהביאו לאישור בעל המאגר. תקנה 4 לתקנות אבטחת המידע מפרטת את הנושאים שיש לעסוק בהם במסגרת נוהל האבטחה, ובהם האבטחה הפיזית והסביבתית של אתרי המאגר; הרשאות גישה למאגרי המידע ולמערכות המאגר; תיאור האמצעים שמטרתם הגנה על מערכות המאגר; אופן התמודדות עם אירועי אבטחת מידע; ניהול התקנים ניידים והשימוש בהם.

בתשובה לשאלה בשאלון אם יש ברשות נוהל אבטחת מידע, התקבלו הנתונים שלהלן:

תרשים 15: **מספרן ושיעורן של הרשויות שיש להן נוהל אבטחת מידע**




על פי נתונים שנאספו בשאלון, בעיבוד משרד מבקר המדינה.

מהנתונים עולה כי 64% מהרשויות המקומיות - 37 מ-58 הרשויות שענו על השאלה - ציינו כי אין להן נוהל אבטחת מידע כנדרש.

נמצא כי מבין הרשויות שנבדקו הרשויות המקומיות א', ג' ו-ה' לא הכינו נוהל אבטחת מידע כנדרש בתקנות אבטחת המידע. הרשויות המקומיות ו' ו-ח' הכינו טיוטה של הנוהל, ובמועד סיום הביקורת היא לא אושרה, ואילו רשות ד' הכינה נוהל אבטחת מידע במהלך תקופת הביקורת, ללא תאריך תוקף. ברשויות המקומיות ב' ו-ז' יש נוהל אבטחת מידע כנדרש.

על רשויות ג' ו-ה' להכין נוהל אבטחת מידע כנדרש. על רשויות ו' ו-ח' להשלים את אישור הנוהל. על רשות ד' לאשר את הנוהל ולציין בו את מועד כניסתו לתוקף.

בתשובות הרשויות ג' ו-ה' צוין כי הן מקבלות את המלצת משרד מבקר המדינה בעניין הכנת נוהל אבטחת מידע, וכי הן יפעלו ליישומה.

רשות ח' מסרה בתשובתה כי מנכ"ל הרשות אישר את הנהלים לאחר מועד סיום הביקורת, וכי היא נערכת ליישומם.

בתשובת רשות א' מאפריל 2022 צוין כי לחברה ב', המספקת שירותים לרשות, יש נוהל אבטחת מידע ומניעת נזקי סייבר.

על רשות א' להכין נוהל אבטחת מידע אשר יכלול הוראות הנוגעות להרשאות הגישה למערכות המחשוב ברשות, לאמצעי הזיהוי והאימות לגישה למערכות המחשוב, לפירוט הסיכונים הנשקפים למידע במערכות המחשוב במהלך הפעילות השוטפת, וכן הוראות נוספות בכל הנוגע להתנהלות עובדי הרשות בסביבת מערכות המחשוב. כמו כן על הרשות לפעול לאישור נוהל אבטחת המידע של חברה ב', ובמידת הצורך להתאימו לצורכי הרשות.

## רשימת מצאי של מערכות המידע

חובת רישום המצאי העירוני, שרכיבי החומרה הם חלק ממנו, נקבעה בתקנות העיריות (הסדר רכישות, ניהול מחסנים, רישום וניהול טובין), התשנ"ח-1998[40]. ניהול רשימת מצאי חשוב בשל הצורך לשמור על הרכוש הציבורי, למנוע רכישות מיותרות של מיטלטלין, ואם המיטלטלין מבוטחים - לשם הבטחת קבלת פיצוי מחברת הביטוח. עוד קובעות תקנות אבטחת המידע כי על בעל המאגר להכין מסמך הכולל רשימת מצאי מעודכנת של מערכות המאגר, הכוללת בין היתר תשתיות ומערכות חומרה, סוגי רכיבי תקשורת ואבטחת מידע, תוכנות וממשקים המשמשים לתקשורת (להלן - רשימת מצאי של מערכות המידע). המסמך צריך לכלול תאריך עדכון אחרון, ויש לעדכנו מפעם לפעם.

הביקורת בחנה אם יש לרשויות שנבדקו רשימת מצאי של רכיבי החומרה הנמצאים בהן, ולהלן הממצאים:

ברשויות המקומיות א', ג', ד', ה', ו', ז' ו-ח' אין מסמך מעודכן המתעד את רשימת המצאי של החומרה ברשות. ברשות ב' יש מסמך המתעד את רשימת החומרה והתוכנה של כל משתמש קצה, אך לא מתועד במסמך תאריך העדכון האחרון שלו.

בתשובות הרשויות ג', ה' ו-ז' צוין כי הן יפעלו להכנת רשימת מצאי הן של החומרה והן של מערכות המידע כנדרש.

על הרשויות המקומיות א', ג', ד', ה', ו', ז' ו-ח' לנהל רשימת מצאי מעודכנת של מערכות המידע הנמצאות בחזקתן ולציין בה את תאריך העדכון האחרון שלה. על רשות ב' לתעד את תאריך העדכון האחרון ברשימת המצאי שלה.

בתשובת רשות ב' צוין כי רשימת המצאי שהועברה למשרד מבקר המדינה הייתה מעודכנת לתאריך שליחתה, וכי הרשות תקפיד להבא לציין את תאריך העדכון של כל דוח מצאי שתכין בעתיד.

רשות ו' ציינה בתשובתה כי יש לה רשימת מצאי חלקית, וצירפה אותה לתשובתה. מעיון ברשימה עולה כי לא צוין בה תאריך הכנתה או תאריך עדכונה האחרון.

רשות ח' ציינה בתשובתה כי היא מנהלת רשימת מצאי של כלל המחשבים במשרדיה, אולם מבדיקת משרד מבקר המדינה עולה כי רשימה זו אינה כוללת את כל הנתונים הנדרשים כאמור בתקנות אבטחת המידע וכן לא מצוין בה תאריך הכנתה או תאריך עדכונה האחרון.

בתשובת רשות א' צוין כי יש בידי חברה ב' רשימת מצאי של מערכות המידע.

40 מצאי מוגדר בתקנות אלו כ"טובין בני קיימה שאינם מאוחסנים במחסן העירייה". טובין מוגדרים בתקנות כ"מטלטלין שבבעלות העירייה או שנמסרו לה דרך שכירות, שאילה או רשיון, לרבות כאלה שנתרמו או נרכשו מכספי תרומה". החובה להכין רשימת מצאי קבועה בתקנה 30 לתקנות. חובה דומה חלה על מועצות מקומיות ומועצות אזוריות מכוח סעיף 30 לתוספת החמישית לצו המועצות המקומיות, התשי"א-1950, ולגבי מועצות אזוריות מכוח סעיף 30 לתוספת הרביעית לצו המועצות המקומיות (מועצות אזוריות), התשי"ח-1958.

על רשות א' לנהל בעצמה רשימת מצאי מעודכנת של מערכות המידע הנמצאות בחזקתה ולציין בה את תאריך העדכון האחרון שלה. זאת, לצד ביצוע בקרה באופן שוטף על רשימות המצאי שבידי חברה ב'.

# הדרכות בנושא אבטחת מידע

## הדרכות בנושא אבטחת מידע במעמד קליטת עובדים

תקנות אבטחת המידע קובעות כי במהלך קליטת עובדים ושיבוצם לתפקיד, ועוד לפני שתינתן להם גישה למאגר המידע, על בעל המאגר לקיים הדרכות לבעלי ההרשאות בנושא החובות החלות עליהם לפי החוק והתקנות. בפועל נהוג שבמעמד קליטת העובד הוא מקבל הדרכה ראשונית בנושא אבטחת מידע וכן מוחתם על טופס ולפיו הוא קרא והבין את החובות החלות עליו בנוגע לאבטחת מידע (להלן - טופס שימוש במערכות מידע).

נמצא כי שתיים מהרשויות שנבדקו - ב' ו-ז' - ממלאות את הוראות תקנות אבטחת המידע, מקיימות הדרכה ראשונית לעובדים הנקלטים ברשות ומחתימות אותם על טופס שימוש במערכות מידע. ברשויות המקומיות א' ג', ד' ו-ה' לא מתקיים הליך סדור של הדרכה לעובדים הנקלטים לעבודה ברשות בנושא אבטחת מידע, והעובדים לא נדרשים לחתום על טופס שימוש נאות במערכות המידע לפני תחילת העסקתם. עוד נמצא כי לרשות ו' יש טיוטת נוהל בנושא קליטת עובדים ושמירה על אבטחת מידע, אך במועד סיום הביקורת היא לא אושרה והרשות לא מקיימת הדרכה ראשונית לעובדים הנקלטים בנושא אבטחת מידע.

יצוין כי במהלך הביקורת הכינה רשות ח' טופס שימוש במערכות המידע והחתימה את עובדי הרשות עליו בנובמבר 2021.

על רשויות א', ג', ד', ה ו-ו', לדאוג שהעובדים הנקלטים לעבודה ברשות יקבלו הדרכה ראשונית בנושא החובות החלות על עובדיהן בתחום אבטחת המידע, עם קליטתם ומומלץ כי הדבר ייעשה גם באמצעות חתימה על טופס שימוש נאות במערכות מידע. עוד מומלץ כי רשות ו' תאשר את טיוטת הנוהל בנושא קליטת עובדים ואבטחת מידע ותפעל ליישמו.

בתשובת רשות ו' נמסר כי טיוטת נוהל בנושא קליטת עובדים ואבטחת מידע, לרבות הדרישה לחתימת העובד על טופס שימוש נאות במערכות מידע, תובא לאישור מועצת הרשות בישיבתה הקרובה.

רשות ה' ציינה בתשובתה כי המלצת משרד מבקר המדינה מקובלת עליה, וכי אגף מערכות מידע ימסור לאגף משאבי אנוש, האמון על קליטת עובדים, דרישה כי במעמד הקליטה של העובדים הם יעברו הדרכה קצרה בתחום מערכות מידע.

רשות א' ציינה בתשובתה כי היא תבצע הדרכות רבעוניות לעובדים החדשים. כמו כן היא תטמיע בתהליך קבלת העובדים החדשים את חובתם לחתום על טופס סודיות ואבטחת מידע כחלק מתהליך קבלתם לעבודה ברשות, ותחתימם על הטופס במעמד קליטתם לעבודה.

## הדרכות תקופתיות לעובדים בנושא אבטחת מידע

בתקנה 7(ג) לתקנות אבטחת המידע נקבע כי בעניינו של מאגר מידע שחלה עליו רמת אבטחה בינונית או גבוהה, יש לקיים בקרב בעלי הרשאות לשימוש במאגר פעילות הדרכה תקופתית אחת לשנתיים לפחות בנושא נוהל אבטחת המידע והוראות החוק והתקנות החלים בנושא. במסגרת הביקורת נבחן אם בשנים 2019 - 2021 הרשויות שנבדקו קיימו הדרכות לעובדים ואם יש להן תוכנית הדרכה.

הרשות המקומית א' ביצעה ביולי 2021 הדרכה בנושא "מערכות מידע והגנה על הפרטיות", ובה השתתפו 87 מ-164 עובדי הרשות. נמצא כי הרשות לא קיימה הדרכה נוספת לעובדים שלא השתתפו באותה הדרכה. עוד נמצא כי אין ברשות תוכנית הדרכה כתובה, וכי היא לא קבעה מועדים מתוכננים לביצוע הדרכות נוספות בעתיד.

אגף הסייבר במשרד הפנים קיים עשר הדרכות בנושא אבטחת מידע באמצעים מקוונים לעובדי רשות ב' בפברואר ובאפריל 2021. עם זאת, נמצא כי הרשות אינה מבצעת מעקב כדי לבחון מי מבין עובדיה השתתף בהדרכות האמורות, והיא לא תכננה הדרכות נוספות לעובדים שלא השתתפו בהן. יצוין כי הרשות שלחה לעובדיה במסגרת "שבוע הסייבר", שהתקיים בדצמבר 2021, הודעות בדואר האלקטרוני שנועדו להעלות את המודעות בנושא אבטחת מידע, כגון הסבר על תופעת הדיוג (פישינג) ועל הדרכים לזהות אותה, כמתואר בדוגמה שלהלן:

הרשות המקומית ו' קיימה בקרב עובדיה הדרכות בנושא "אבטחת מידע" בנובמבר 2018. הרשות ערכה רישום של העובדים שהשתתפו בפועל בהדרכות אולם לא התקיימה הדרכה נוספת מאז. יצוין כי הרשות הכינה בשנת 2021 תוכנית הדרכה מקוונת לעובדים בנושא אבטחת מידע, הכוללת גם מבחן מקוון, אולם במועד סיום הביקורת היא עדיין לא קיימה את ההדרכה ואת עריכת המבחן המקוון בקרב עובדיה כמתחייב.

מנמ"ר רשות ז' מסר למשרד מבקר המדינה במהלך הביקורת כי בוצעו כמה הדרכות תקופתיות לעובדים בנושא אבטחת מידע בשלוש השנים האחרונות, והאחרונה שבהן בוצעה בדצמבר 2021, אך הרשות לא תיעדה את הביצוע של אותן הדרכות.

נמצא כי רשות מקומית ז' מקיימת באופן שוטף בקרב עובדיה תחקורי מקרים וכן תרגילי "פישינג", שבמסגרתם נשלחת להם בדואר האלקטרוני הודעה לא מוכרת ובה הם מתבקשים ללחוץ על קישור לא מוכר או למסור פרטים אישיים שלהם. העובד שלוחץ על קישור מקבל הודעה כי מדובר בתרגיל, כמוצג בדוגמה שלהלן:

הבדיקה העלתה כי הרשויות המקומיות ג' ו-ח', הרשויות המקומיות ד' ו-ה' לא קיימו הדרכות תקופתיות לעובדים אחת לשנתיים כנדרש. עוד נמצא כי הרשויות המקומיות א', ב', ו' ו-ז', לא ביצעו מעקב שוטף אחר השתתפות כל העובדים בהדרכות שביצעו, ולא קיימו הדרכות נוספות לאותם עובדים שלא נטלו בהן חלק.

על הרשויות המקומיות ג', ד', ה' ו-ח' לקיים הדרכות תקופתיות לעובדיהן בנושא אבטחת מידע כנדרש. על הרשויות המקומיות א' ב' ו-ו' לבצע את ההדרכות במועדן כנדרש ולהשלים את קיום ההדרכות בקרב אותם עובדים שטרם השתתפו בהן.

רשות ב' מסרה בתשובתה כי הנושא טופל, וכי החלה לבצע מעקב אחר השתתפות כל עובדי הרשות בהדרכות, וזאת בעזרת מחלקת ההדרכה ברשות.

רשות א' מסרה בתשובתה כי תפעל לתאם הדרכת השלמה לעובדים שלא נכחו בהדרכת המודעות הקודמת.

בתשובת רשות ה' צוין כי המלצת משרד מבקר המדינה מקובלת עליה, וכי הנושא יוסדר במסגרת תוכנית העבודה של אגף מערכות מידע לשנת 2022.

רשות ו' ציינה בתשובתה כי היא קבעה שני מועדים להדרכות פרונטליות במרץ 2022, שבהן אמורים להשתתף כל עובדי הרשות. מנכ"ל הרשות אף שלח לכלל מנהלי האגפים והמחלקות ברשות מכתב ובו הדגיש את חשיבות ההדרכה ואת חובת נוכחות העובדים באחד המועדים. עוד ציינה הרשות כי מועדי ההדרכות נדחו בשל מגיפת הקורונה, וכי נוסף על האמור לעיל היא הכינה מצגת מידע שבסופה יש קישור לשאלון שאותו אמורים למלא עובדי הרשות.

בתשובת רשות ז' צוין כי מנכ"ל הרשות ינחה את מחלקת ההדרכה באגף משאבי אנוש לתעד את הדרכות אבטחת המידע ואת שמות הנוכחים בהן.

רשות ח' ציינה בתשובתה כי היא שלחה לכלל עובדיה מסמך ובו הסבירה את חשיבות נושא אבטחת המידע ואת הסיכונים והאיומים הכרוכים בנושא, זאת כדי להגביר את ערנותם של העובדים לסיכונים ולאיומים אלה ולעודדם להקפדה על הנהלים לשם מניעת פגיעה במאגרי המידע של הרשות וזליגת מידע החוצה. עוד ציינה הרשות כי היא מתכננת לקיים בקרב העובדים הרצאות והדרכות בנושא בתדירות של כפעמיים בשנה. כמו כן בוצעה פנייה לחברה חיצונית לבחינת העברת ההדרכות כאמור.

על הרשויות המקומיות שנבדקו לקבוע תוכנית הדרכה בנושא אבטחת מידע וההוראות והכללים החלים בנושא ולתעד את קיום ההדרכות באופן שיאפשר מעקב אחר ביצוען ובקרה בנושא.

בתשובת רשות ב' צוין כי השנה מתכנן אגף הסייבר במשרד הפנים לקיים תשע הדרכות לעובדים והדרכה למנהלים, וכי כל עובדי הרשות מחויבים להשתתף בהדרכות הללו.

רשות ג' השיבה כי היא מקבלת את המלצות משרד מבקר המדינה בנושא הדרכות לעובדים, וכי היא תפעל ליישם את ההמלצות בשנים 2022 ו-2023.

בתשובת רשות א' צוין כי היא תפעל לקביעת תוכנית הדרכה ותבצע תיעוד שוטף של ההדרכות ושל המשתתפים בהן.

משרד מבקר המדינה מציין לחיוב את רשות ב' ורשות ז' על ששלחו הודעות בנושא בדואר האלקטרוני ועל שביצעו עבור העובדים תרגילים שוטפים בנושא אבטחת מידע באופן המעלה את מודעותם לנושא ומשפר את אבטחת המידע ברשות.

רשות ב' הוסיפה בתשובתה כי היא מתכננת לבצע ברבעון האחרון של השנה תרגיל סייבר תיאורטי להנהלת הרשות בשיתוף אגף הסייבר של משרד הפנים.

לאור העובדה שאגף הסייבר במשרד הפנים יזם כיום הדרכות בנושא אבטחת מידע לרשויות המקומיות, מומלץ כי האגף יגבש בשיתוף עם מערך הסייבר הלאומי הכשרה מקוונת לכלל עובדי הרשויות המקומיות בנושא אבטחת מידע ויפעל להנחות את כלל הרשויות לבצע את ההדרכות לעובדיהן כנדרש.

משרד הפנים ציין בתשובתו כי אם מערך הסייבר הלאומי ייזום הדרכות מקוונות לרשויות המקומיות בנושא אבטחת מידע, משרד הפנים ישתף פעולה עמו. בתשובת משרד הפנים ממאי 2022 מסר המשרד כי הוא אינו מבצע הכשרה מקוונת של כלל עובדי הרשויות המקומיות, היות שהנושא עתיר תקציב.

# ביצוע בקרות על הגישה למערכות המידע

## חדרי השרתים ברשויות המקומיות

שרת (Server) הוא מחשב רב עוצמה שעליו מותקנות תוכנות ויש בו נתונים המספקים שירותים למחשבים אחרים. הארגון עשוי להחזיק בשרת אחד או יותר, בהתאם למערכות המחשוב שבארגון. בשל הצורך לאבטח את הנתונים השמורים בשרתים נהוג להקים חדר שרתים - חדר מאובטח שנועד לאחסון השרתים, ובו חיבור לתשתית חשמל, למתקני קירור (השרתים זקוקים לטמפרטורה מסוימת כדי לפעול) ולכבלי תקשורת ותשתית.

תקנות אבטחת המידע[41] מחייבות שמירה פיזית של תשתיות ושל מערכות החומרה המשמשות את מאגרי המידע, וזאת במקום מוגן שלא ניתן להיכנס אליו ללא הרשאה מתאימה. עוד קובעות התקנות כי על בעל מאגר מידע שחלה עליו רמת האבטחה הבינונית או הגבוהה לנקוט אמצעים לבקרה ולתיעוד של הכניסה והיציאה מאתרים שבהם שמורות מערכות המאגר, למשל להתקין מצלמות באתרים אלה. בהתאם למספר השרתים ולגודלם, יש רשויות מקומיות שחדר השרתים שלהן נמצא בתחומן, ולעומתן יש רשויות שחדרי השרתים שלהן נמצאים בחברות חיצוניות המספקות להן שירותי מחשוב. מכל מקום, הרשויות הן בעלות מאגרי המידע (להבדיל מהחברות המשמשות כמחזיקות) ולכן מוטלת גם עליהן האחריות למלא את הוראות התקנות שלעיל.

במסגרת הביקורת נבדקו חדרי השרתים של הרשויות שנבדקו, בפרמטרים האלה: האם מותקנת בהם מצלמה המתעדת את הנכנסים ואת הנעשה בחדר; האם נדרשות הרשאות כניסה לחדר; האם מותקן בחדר השרתים חיישן טמפרטורה; האם יש בחדר מערכת לכיבוי אש; האם קיימת מערכת לשליחת התראות לגורם המוסמך ברשות בהתרחש אירוע חריג כגון שרפה, תקלה טכנית, נפילת תקשורת או כניסת אנשים בלתי מורשים לחדר השרתים. להלן יוצגו ממצאי הבדיקה:

לוח 4: **חדרי השרתים ברשויות שנבדקו**

| | מצלמה חיצונית ופנימית | הרשאות כניסה לחדר | קיום חיישן טמפרטורה בחדר | קיום מערכת לכיבוי אש | תקשורת במקרה חיווי בעייתי |
|---|---|---|---|---|---|
| א'* | ✓ | ✓ | ✓ | ✓ | ✓ |
| ב' | ✓ | ✓ | ✓ | ✓ | ✓ |
| ג' | ✓ | ✓ | ✗ | ✓ | ✗ |
| ה' | ✓ | ✓ | ✓ | ✓ | ✓ |
| ו'* | ✓ | ✓ | ✓ | ✗ | ✓ |

41 תקנה 6(א) ו-6(ב).

| | מצלמה חיצונית ופנימית | הרשאות כניסה לחדר | קיום חיישן טמפרטורה בחדר | קיום מערכת לכיבוי אש | תקשורת במקרה חיווי בעייתי |
|---|---|---|---|---|---|
| ד'* | ✓ | ✓ | ✓ | ✓ | ✓ |
| ז' | ✓ | ✓ | ✓ | ✓ | ✓ |
| ח' | ✗ | ✗ | ✗ | ✗ | ✗ |

על פי מידע שנאסף בביקורת, בעיבוד משרד מבקר המדינה.

* השרתים נמצאים בחברה פרטית מחוץ לרשות.

מהטבלה עולה כי ברשויות המקומיות א', ב', ה', ד' ו-ז' כל הרכיבים שנבדקו בחדרי השרתים נמצאו תקינים. בחדר השרתים של רשות ג' אין חיישן טמפרטורה ואין תקשורת במקרה של חיווי בעייתי. בחדר בו נמצאים השרתים של רשות ו' לא היה במועד הביקורת מטף כיבוי אש, והמטף הקרוב נמצא בחדר הסמוך. בחדר השרתים של רשות ח' לא נמצאו כל הרכיבים שנבדקו.

על רשות ח' לתעד את הכניסה לחדר השרתים באמצעות מצלמה חיצונית ופנימית, להצטייד במטף כיבוי, להצטייד בחיישן טמפרטורה ולוודא שמתאפשרת התקשרות במצב של חיווי בעייתי.

רשות ח' מסרה בתשובתה כי היא תפעל באופן מידי לקיים את הנדרש.

על רשות ג' להצטייד בחיישן טמפרטורה ולהתקין מערכת לשליחת התראות לגורם המוסמך בה, בעקבות אירוע חריג, כגון: שריפה, תקלה טכנית, נפילת תקשורת או כניסת אנשים בלתי מורשים.

רשות ג' מסרה בתשובתה כי תפעל להתקין בחדר השרתים שלה חיישן טמפרטורה ומערכת לניטור תקשורת.

על רשות ו' לוודא שחדר השרתים שלה יהיה מצויד במטף כיבוי דרך קבע.

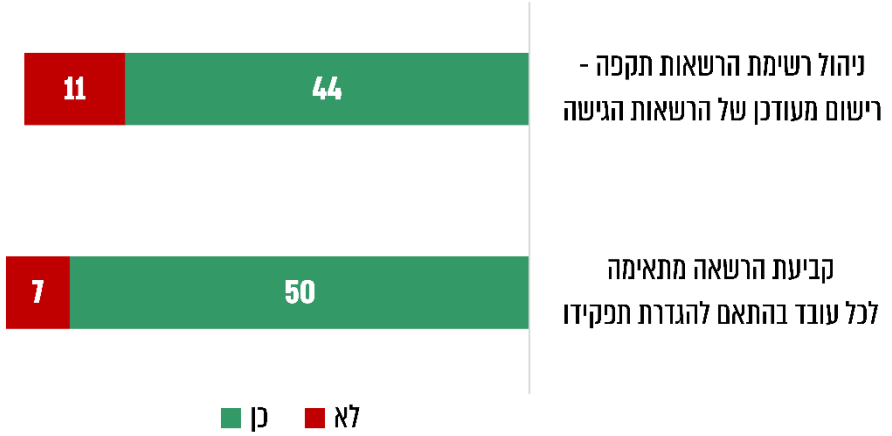
## ניהול הרשאות גישה

בתקנות אבטחת המידע נקבע בין היתר כי יש לקבוע הרשאות גישה למאגר לכל עובד רק במידה הנדרשת לו לצורך ביצוע תפקידו, וכי יש לנהל רשימת הרשאות מעודכנת, הכוללת את התפקידים, את הרשאות הגישה שניתנות להן ואת בעלי ההרשאות הממלאים תפקידים אלו (להלן - רשימת הרשאות תקפות), וכי יש לכלול את רשימת ההרשאות התקפות בנוהל

האבטחה. עוד נקבע בתקנות כי בעל המאגר ידאג לביטול ההרשאות של בעל הרשאה שסיים את תפקידו, מייד עם סיומו.

אחת השאלות שבשאלון הייתה האם הרשות קובעת הרשאות גישה לכל עובד בהתאם להגדרת תפקידו, והאם הרשות מנהלת רשימת הרשאות תקפות. מתשובותיהן של הרשויות על שאלות אלה התקבלו הנתונים שלהלן[42]:

תרשים 16: **מספר הרשויות שקובעות ומנהלות רשימת הרשאות לעובדיהן**




על פי מידע שנאסף בביקורת, בעיבוד משרד מבקר המדינה.

מהאמור לעיל עולה כי מרבית הרשויות (87% מהן) דיווחו כי הן קובעות הרשאות לכל עובד בהתאם להגדרת תפקידו, אולם כ-80% מהן מנהלות רשימת הרשאות תקפה.

בתשובותיהן על השאלון השיבו הרשויות שנבדקו, מלבד רשות ד', כי הן קובעות לכל עובד הרשאה בהתאם לתפקידו ברשות, וכי הן מנהלות רשימת הרשאות תקפה כנדרש.

ברשויות שנבדקו נבדק אם יש הליך סדור למתן הרשאות לעובדי הרשות ולביטולן. להלן יוצגו ממצאי הבדיקה:

לרשויות המקומיות ג', ד' ו-ה', אין כללים כתובים בנוגע למתן הרשאות גישה או לביטולן. לרשות א' יש נוהל שנכנס לתוקף ביוני 2021, ולרשויות המקומיות ו' ו-ח' יש טיוטות נוהל בנושא מיולי 2020 ומיולי 2021 בהתאמה, שלא אושרו במועד סיום הביקורת. לרשויות המקומיות ב' ו-ז' יש נוהל מתן הרשאות כנדרש.

42 57 רשויות מקומיות השיבו על השאלה של קביעת הרשאה מתאימה לכל עובד ו-55 רשויות מקומיות השיבו על השאלה של ניהול רשימת הרשאות תקפה.

על הרשויות המקומיות ג', ד' ו-ה' לקבוע כללים, רצוי בנוהל, למתן הרשאות ולביטולן, הן לעובדים הנקלטים ברשות והן לעובדים העוזבים אותה. על הרשויות המקומיות ו' ו-ח' לאשר את טיוטות הנוהל שלהן ולפעול על פיו.

רשות ה' ציינה בתשובתה כי המלצת משרד מבקר המדינה מקובלת עליה, וכי הנושא יטופל.

רשות ג' ציינה בתשובתה כי תפעל להכנת נוהל בכתב בהתאם להמלצת הביקורת.

רשות ו' ציינה בתשובתה כי טיוטת נוהל העבודה בנושא מתן הרשאות וביטולן הובאה לאישור בעלי התפקידים הרלוונטיים ברשות, וכן תובא לאישור מועצת הרשות בישיבתה הקרובה.

רשות ח' ציינה בתשובתה כי נוהל מתן ההרשאות אושר, וכי היא אמורה להחילו על כלל העובדים, לרבות עובדי קבלן נותני שירות.

## התקנים ניידים

התקן נייד הוא מחשב או התקן אחסון המיועד לשימוש נייד, כגון התקן זיכרון נייד (USB), כונן חיצוני וטלפון סלולרי חכם. בתקנות אבטחת המידע[43] נקבע כי בעל המאגר יגביל או ימנע את האפשרות לחיבור התקנים ניידים למערכות המחשוב. הדבר חשוב שכן יש סיכון כי מידע מהמאגר ידלוף החוצה באופן לא מורשה או כי חיבור ההתקן הנייד יגרום נזק למערכות המאגר.

במסגרת הביקורת נבדק אם בוצעה חסימה או הגבלה אחרת לחיבור התקנים ניידים למערכות המחשוב של הרשויות שנבדקו ואם קיים חיווי לגורם כלשהו ברשות בעת חיבור של התקן נייד למחשבי הרשות, כגון מערכת ניטור.

ברשות ו' נקבעה הגדרה המנטרת חיבור של התקן חיצוני, כך שקופצת התראה ולא ניתן לפתוח את הקבצים המועברים באמצעות ההתקן הנייד.

ברשות ז' מותקנת חסימה באמצעות מערכת EDR[44] של חברה חיצונית, המנטרת חיבור של התקן חיצוני כך שקופצת התראה ולא ניתן לפתוח את הקבצים באמצעות ההתקן. רק למשתמשים נבחרים ניתנת הרשאה לחיבור USB, וההרשאה ניתנת למחשב קבוע באופן שאינו מאפשר להעביר את ההרשאה למחשב אחר. למנמ"ר יש רישומים של העובדים בעלי ההרשאות האמורות.

ברשויות המקומיות ב', ג', ד' ו-ח', אין חסימה של התקנים ניידים ואין מערכת המנטרת חיבור התקנים ניידים. עם זאת, ברשות ב' יש תוכנה החוסמת התקנת קובצי הרצה[45], והדבר מפחית את הסיכון שבחיבור התקן נייד אולם לא מונע אותו כליל (למשל לא מונע העתקת קבצים

43 תקנה 12 לתקנות.

44 מערכת אבטחת סייבר שמבטיחה הגנה כוללת על תחנות הקצה.

45 קובץ הרצה הוא קובץ המפעיל פקודה או תוכנה מסוימת. הסיכון הנשקף מקובץ מסוג זה הוא שניתן להטעות את המשתמש ולגרום לו "להריץ" קובץ נגוע ובכך לסכן את הארגון.

והעברת מידע). במסגרת התוכנית האסטרטגית למחשוב של רשות ב' לשנת 2022 מתוכננת רכישת מערכת לניטור חיבור התקנים ניידים.

ברשות א' יש מערכת המנטרת חיבור התקנים ניידים. עם זאת, נמצא כי עובדים מקבלים הרשאת חיבור התקן נייד לפי דרישה כך שמנהל התפעול פונה בשמם לחברה ב' נותנת השירות כדי שזאת האחרונה תאפשר את החיבור עבור אותו משתמש, אך לא מתבצעים מעקב או בקרה בנושא, כגון רישום של אותם עובדים שקיבלו אישורים לחיבור התקן נייד. כמו כן, עלה כי מרגע שהאישור התקבל הוא אינו מוגבל בזמן.

רשות ה' שקלה את הסוגיה והחליטה לאפשר חיבור התקן נייד לכלל העובדים ברשות. הרשות ציינה במהלך הביקורת שהדבר נעשה שכן תוכנת האנטי-וירוס חוסמת את האפשרות להתקנת קובצי הרצה.

יוצא אפוא כי הרשויות המקומיות ג', ד' ו-ח' לא מגבילות את האפשרות לחיבור התקנים ניידים וגם לא מנטרות את חיבורם. ברשות א' יש מערכת לניטור התקנים ניידים אך הרשות לא מנהלת תיעוד של העובדים שניתנה להם הרשאה לחיבור התקן נייד ולא מגבילה את תקופת ההרשאה. ברשויות המקומיות ב' ו-ה', אין הגבלה פיזית לחיבור התקנים ניידים אולם קיימת חסימה חלקית המפחיתה את הסיכון בחיבור התקנים ניידים. ברשויות המקומיות ו' ו-ז' יש חסימה פיזית לרוב המוחלט של מחשבי הרשות ובנוסף ניטור בעת חיבור התקנים ניידים.

על הרשויות המקודמיות ב', ג', ד', ה' ו-ח' להגביל או לנטר את חיבור ההתקנים החיצוניים. מומלץ כי רשות ב' תפעל בהתאם לתוכנית האסטרטגית שלה ותרכוש תוכנת ניטור כאמור. כאשר הרשויות מאפשרות חיבור התקנים ניידים לחלק מהעובדים, מומלץ לתעד את העובדים המורשים ולבצע בקרה בעניינם.

על רשות א' לנהל תיעוד של העובדים שניתנה להם הרשאה לשימוש בהתקן נייד ובכלל זה להגביל את תקופת ההרשאה.

רשות א' ציינה בתשובתה, בהתייחס למצב הדברים לאחר הביקורת, כי חיבור ההתקנים הניידים חסום באופן גורף לכלל המשתמשים ברשות, למעט שני משתמשים.

רשות ה' ציינה בתשובתה כי תבחן את הנושא.

רשות ב' ציינה בתשובתה כי במסגרת התקציב ליישום התוכנית האסטרטגית שלה היא אמורה לרכוש תוכנה לניטור חיבור התקנים חיצוניים ולהפעילה השנה.

רשות ג' ציינה בתשובתה כי תפעל להגבלת חיבור התקנים ניידים למחשבים כולל ניטור.

רשות ח' ציינה בתשובתה כי ההתקנים החיצוניים חוברו לרשת נפרדת מרשת הרשות, וכי החלה ביישום פתרון אמין יותר.

## אבטחת מחשוב (תוכנת אנטי וירוס)

בתקנות אבטחת המידע נקבע שאין לחבר את מערכות המאגר לאינטרנט או לרשת ציבורית אחרת בלא התקנת אמצעי הגנה מתאימים מפני חדירה לא מורשית או מפני תוכנות העלולות לגרום נזק או שיבוש למחשב. לכן יש להקפיד על התקנת אמצעי הגנה על המחשבים, כגון תוכנת אנטי-וירוס בעלת רישיון[46] ומעודכנת. הקפדה כאמור נדרשת על מנת לסכל את האפשרות שהאקרים יפרצו למערכת המידע של הרשות. חשוב להתקין את עדכוני התוכנה מיד עם פרסומם ובכך לצמצם את זמן החשיפה לסיכונים ואת "חלון הזמן" שבו הם יכולים להיות אפקטיביים[47].

ברשויות המקומיות ב', ג', ה' ו-ז' נמצא כי תוכנת האנטי-וירוס בעלת רישיון ומעודכנת.

מנמ"ר רשות ד' מסר למשרד מבקר המדינה כי לרשות עומדות שלוש עמדות מחשב בלבד ולהן רישיון לתוכנת-אנטי וירוס, וכי על יתר העמדות מותקנת גרסה פרוצה וללא רישיון[48]. כמו כן, אין ברשות מערכת אוטומטית לניהול אנטי-וירוס והעדכונים מתבצעים ידנית, והדבר מקשה על המנמ"ר לוודא כי הרשות מעדכנת בקפידה את מערכת ההפעלה והתוכנות שלה. לדוגמה, בעמדת המחשב הנייח של המנמ"ר מותקנת גרסת אנטי-וירוס לא מעודכנת, והדבר הוא בבחינת פרצת אבטחה ונקודת תורפה לתקיפת סייבר ועלול לסכן את חוסנה של מערכת המחשוב ברשות.

הועלה כי ברשות ו' מותקנת תוכנת אנטי-וירוס במצב תקין בעמדותיהם של 43 (כחמישית) מ-227 משתמשי המחשב ברשות בנקודות הקצה. עוד הועלה כי ברשות א', בשתי נקודות קצה שנדגמו נמצאה גרסת אנטי-וירוס לא מעודכנת.

ברשות ח' אין מערכת אוטומטית לניהול אנטי-וירוס, והעדכונים מתבצעים ידנית. לדוגמה, בעמדת המחשב הנייח של המנמ"ר מותקנת גרסת אנטי-וירוס לא מעודכנת.

הועלה כי ברשויות המקומיות א' ד' ו-ח', תוכנות האנטי-וירוס אינן מעודכנות בכל עמדות הקצה ברשות. עוד הועלה, כי הרשות המקומית ד' עושה שימוש בתוכנת אנטי-וירוס ללא רישיון. ברשויות המקומיות ב', ג', ה' ו-ז' תוכנת האנטי-וירוס בעלת רישיון ומעודכנת.

רשות ו' מסרה בתשובתה כי היא נמצאת בתהליך של השלמת התקנת תוכנת אנטי-וירוס בכל עמדות המחשב ברשות, ובמועד מתן תשובתה כבר הותקנה התוכנה ב-94 עמדות.

רשות א' ציינה בתשובתה כי היא ממתינה לתוצאות הבדיקה והתיעוד שביצעה חברה ב' בעניין תוכנת האנטי-וירוס.

46 בתוכנת אנטי-וירוס בעלת רישיון - להבדיל מתוכנת אנטי-וירוס פרוצה - מדובר בגרסה מלאה של התוכנה, המתעדכנת באופן שוטף ועמידה בפני פרצות אבטחה חדשות. כמו כן, רוכש הרישיון זכאי לתמיכה טכנית אם הדבר נדרש. הרישיון כרוך בתשלום לחברה שיצרה את התוכנה, בייחוד אם מדובר ביותר ממחשב אחד.

47 המלצת מערך הסייבר הלאומי בהקשר של עדכוני תוכנה:
www.gov.il/he/departments/general/update_all_the_time

48 אנטי-וירוס פרוץ - ללא רישיון, קרי בדרך כלל אין מדובר בגרסה המלאה של התוכנה, והאנטי-וירוס אינו מתעדכן באופן שוטף ואין אפשרות לקבל תמיכה.

רשות ח' ציינה בתשובתה כי עמדת המחשב שנדגמה לא הייתה בשימוש תדיר בזמן הביקורת ולכן מערכת האנטי-וירוס בעמדה זו לא הייתה מעודכנת. עוד ציינה הרשות כי כל העמדות המחוברות לרשת האינטרנט מתעדכנות באופן אוטומטי, וכי היא מתכוונת לרכוש בקרוב מערכות ממוחשבות שיסייעו בניהול מערכות המידע שלה באופן אמין ויעיל יותר.

אי-התקנת תוכנות אנטי-וירוס בעלות רישיון בתוקף ברשויות המקומיות עלול לסכן את מערכות המחשוב שלהן ולחשוף אותן לאירועי פריצת מידע והתקפות סייבר. על הרשויות המקומיות א, ד', ו' ו-ח' לוודא כי תוכנת האנטי-וירוס מעודכנת בכלל נקודות הקצה ברשות. על רשות ד' להפסיק את השימוש בתוכנות אנטי-וירוס שאינן מורשות ולפעול להתקנת תוכנה בעלת רישיון.

## עדכון מערכת ההפעלה וביצוע גיבויים

1. תקנות אבטחת המידע קובעות שבעל המאגר נדרש לעדכן באופן שוטף את מערכות המאגר ואת החומרה והתוכנה בהתאם להנחיות היצרן על מנת לנטרל פגיעויות וחולשות המתגלות מפעם לפעם.

נמצא כי בכל הרשויות שנבדקו יש עמדות ובהן מותקנת מערכת הפעלה מסוג Windows 7, שהיא מערכת הפעלה מיושנת, שלא ניתן לעדכנה או לתת תמיכה למשתתפים בה (שכן הוכנסו לשימוש מערכות הפעלה חדשניות יותר)[49]. השימוש במערכת הפעלה שאינה מעודכנת או נתמכת גורמת פגיעה חמורה באבטחת המידע ברשות.

מומלץ שהרשויות המקומיות שנבדקו יפעלו להחלפה או לשדרוג של מערכות ההפעלה ברשות ובכלל זה יבטיחו כי יינתנו שירותי תמיכה מקצועיים למשתמשים במערכות.

רשות ה' ציינה בתשובתה כי נושא זה הוסדר מכבר לאחר הביקורת, וכי כל מערכות ההפעלה שודרגו.

רשות ב' ציינה בתשובתה כי היא תקצבה סך של כחצי מיליון ש"ח לשדרוג המחשבים הישנים, וכי במועד מתן תשובתה כבר שודרגו כ-200 עמדות. עוד ציינה כי לאחר קבלת תקציב נוסף יושלם השדרוג של שאר העמדות, לרבות של מערכות ההפעלה הישנות.

רשויות א' ו-ג' מסרו בתשובותיהן כי הן נמצאות בתהליך החלפת מערכות ההפעלה למערכות חדשות ועדכניות.

49 מערכת כזו מכונה מערכת End Of Life - EOL.

רשות ו' מסרה בתשובתה כי יש בה שמונה עמדות מחשב עם מערכת הפעלה מסוג Windows 7 וכי הרשות פועלת להחליף את המחשבים כחלק מתוכנית העבודה של שנת 2022.

רשות ז' ציינה בתשובתה כי היא תגבש תוכנית מתוקצבת להחלפה הדרגתית של התחנות המיושנות בתחנות עם מערכת הפעלה מתקדמת.

רשות ח' מסרה בתשובתה כי היא ערה לחשיבות התקנת מערכות הפעלה עדכניות ולפיכך היא רכשה עוד קודם לביקורת מערכות הפעלה מעודכנות ובעלות רישיון. עוד מסרה הרשות כי היא השמידה את מלאי המחשבים שלא ניתן היה לשדרג בהם את מערכת ההפעלה בשל מערכת החומרה שלהם.

2. תקנות אבטחת המידע[50] קובעות לגבי מאגרי מידע שחלות עליהם רמת האבטחה הבינונית או הגבוהה שיש לגבות את הנתונים הנצברים בהם באופן שיאפשר בכל עת לשחזר את מצבם המקורי של הנתונים האמורים. עוד נקבע[51] לגבי מאגרי מידע אלה שיש לקבוע במסמך נוהל אפקטיבי לביצוע גיבויים עתיים דרך שגרה, ובכלל זה לשמר את הרישומים המתעדים את היסטוריית הגיבויים ברשות (להלן - נוהל גיבוי או נוהל פנימי לגיבוי).

בשאלון נבדק אם יש לרשות נוהל פנימי לגיבוי מערכות המידע שברשותה.

עולה כי ל-38 (64%) מ-59 הרשויות המקומיות שהשיבו על שאלה זו, יש נוהל פנימי לגיבוי מערכות המידע ברשות וביניהן רשות ב', ול-21 (36%) הרשויות הנותרות אין נוהל גיבוי, וביניהן הרשויות א', ג', ד', ה' ו-ז'.

רשות א' ציינה בתשובתה כי אכן אין בידיה נוהל גיבוי, עם זאת לחברה ב' הנותנת שירותי התוכנה ברשות קיים נוהל גיבוי ובתשובתה הנוספת של הרשות צרפה מכתב בנוגע למדיניות הגיבויים של חברה ב' שהופנה למנהל התפעול ברשות. במכתב צוין שהנוהל חסוי ולכן אם הרשות מעוניינת לעיין בו, עליה לתאם לשם כך פגישה במשרדי החברה.

עלה כי רשות א' לא גיבשה בעצמה נוהל פנימי לגיבוי וכן לא בחנה ואישרה את נוהל הגיבוי של חברה ב', וכי אין בידיה רישומים המתעדים את היסטוריית הגיבויים ברשות עבורה, והיא אינה מבצעת בקרה אודות עמידת חברה ב' בדרישות הגיבוי. עוד עלה כי לרשויות ו' ו-ח' יש טיוטות נוהל גיבוי שטרם אושרו.

50 ראו תקנה 17(ב) וראו גם מערך הסייבר הלאומי, תורת ההגנה לסייבר 2.0, בעמ' 24.

51 תקנה 18(א).

על הרשויות המקומיות ג', ד', ה' ו-ז' לקבוע נוהל גיבויים תקף ולבצע גיבויים על פי הנקבע בו. על רשות א' לגבש נוהל גיבויים או לחלופין לבחון את נוהל הגיבויים של חברה ב' ולקבוע אם לאשרו, להחזיק רישומים המתעדים את היסטוריית הגיבויים ולבצע בקרה באופן עיתי בעניין מידת עמידתה של חברה ב' במחויבותה לביצוע גיבויים כנדרש. על רשויות ו' ו-ח' להשלים את הליך הכנת נוהל הגיבויים ואישורו.

רשות ה' ציינה בתשובתה כי היא מקבלת את המלצת משרד מבקר המדינה, וכי היא נוהגת לבצע גיבויים על פי הנחיות פנימיות שקיימות היום באגף מערכות מידע ברשות, אולם אופן העבודה של הרשות בנושא טרם הוסדר בנוהל כתוב, והיא תפעל להכנת נוהל גיבוי בכתב.

רשויות ו' ו-ז' ציינו בתשובותיהן כי הוכנו טיוטות נוהל בנושא גיבויים, והן יובאו לאישור הנהלות הרשויות כנדרש.

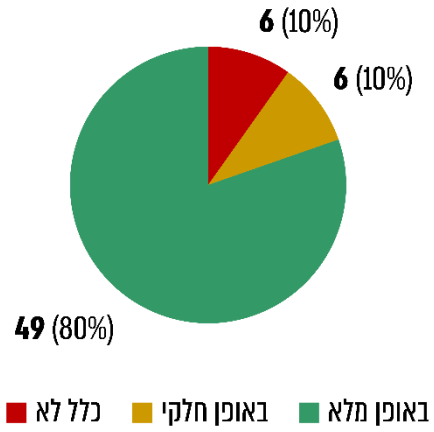
רשות ג' ציינה בתשובתה כי קיים נוהל גיבוי מסודר לשרת וצירפה לתשובתה העתק של הנוהל.

מבדיקת הנוהל של רשות ג' עולה כי הוא אינו כולל ניהול גרסאות, אין בו תאריך תחולה, לא צוינו בו הגדרות או מטרות, לא הוגדרו בו הגורמים האחראים לביצוע, לא תואר בו תהליך הגיבוי או מדיניות הגיבוי והוא לא אושר על ידי גורם מוסמך ברשות.

על רשות ג' לעדכן את נוהל הגיבויים בהתאם לאמור לעיל.

3. בשאלון התבקשו הרשויות המקומיות לציין, בין היתר, אם הן מבצעות בפועל גיבוי שוטף של כל מערכות המידע שברשותן. מתשובותיהן של הרשויות על השאלון התקבלו הנתונים שלהלן:

תרשים 17: **מספרן ושיעורן של הרשויות המקומיות המבצעות גיבוי שוטף של מערכות המידע שלהן**




על פי הנתונים שנאספו בשאלון, בעיבוד משרד מבקר המדינה.

מהתרשים עולה כי 49 (80%) מ-61 הרשויות המקומיות שענו על השאלה בשאלון ציינו שהן מבצעות גיבוי מלא של מערכות המידע שלהן, ואילו שש (10%) מהרשויות ציינו שהן מבצעות גיבוי חלקי בלבד. 6 הרשויות הנותרות (10% מכלל הרשויות שענו על השאלה בשאלון) השיבו כי הן לא מבצעות כלל גיבוי שוטף של מערכות המידע שלהן.

יצוין כי אף שכ-90% מהרשויות מסרו שהן מבצעות גיבוי כלשהו (מלא או חלקי), כאמור ל-36% מהן אין נוהל גיבוי כנדרש.

נמצא כי ברשויות המקומיות ב', ה', ו' ו-ז' מתבצעים גיבויים באופן שוטף. ברשויות ג', ד' ו-ח' לא נמצאו רישומים המתעדים היסטוריית גיבויים תקינה ברשות.

על רשויות ג', ד' ו-ח' לבצע גיבויים שוטפים של מערכות המידע שברשותן, על מנת שניתן יהיה לשחזר את הנתונים בהן בעת הצורך.

# תוכנית להתאוששות מאסון

בתורת ההגנה בסייבר שהכין מערך הסייבר הלאומי נקבע, בין היתר, שארגון (ובכללו רשות מקומית) צריך להיערך למצב של התאוששות מאסון[52] באופן מובנה, כדי לוודא שהארגון יוכל להתמודד כנדרש עם "נפילת" מערכות המחשוב, עם מחיקת מידע או אם נעילת קבצים, ועל מנת שבהתרחש אירוע סייבר הוא יוכל לתפקד באופן סדור ולהתמודד עימו באופן המיטבי.

בשאלון התבקשו הרשויות המקומיות לציין, בין היתר, אם יש להן תוכנית מוסדרת להתאוששות מאירועי סייבר (DRP/BCP)[53].

מתשובותיהן עולה כי ל-23 (כ-39%) מ-59 הרשויות שהשיבו על שאלה זו יש מנגנון מוסדר להמשכיות של פעילות המחשוב ברשות בהתרחש אירוע סייבר, ול-36 (כ-61%) מהרשויות המקומיות שהשיבו על השאלה אין מנגנון כזה.

בבדיקה נמצא כי הרשויות המקומיות א', ב', ג', ד', ה', ו', ז' ו-ח' לא הכינו תוכנית להתאוששות מאסון. עוד נמצא כי רשות ו' הכינה טיוטת תוכנית להתאוששות מאסון, וכי במועד סיום הביקורת היא לא אושרה.

נוכח החשיבות של הכנת תוכנית להתאוששות מאסון, משרד מבקר המדינה ממליץ לכלל הרשויות המקומיות וביניהן הרשויות שנבדקו לפעול להכנת תוכנית להתאוששות מאסון המתאימה לצורכי הרשות, בהתאם להנחיות מערך הסייבר הלאומי. מומלץ כי רשות ו' תפעל להשלמת הכנתה של התוכנית להתאוששות מאסון.

רשות ב' ציינה בתשובתה כי תוכנית להתאוששות מאסון כלולה בתוכניתה האסטרטגית לשנת 2022.

רשות ו' ציינה בתשובתה כי טיוטת תוכנית להתאוששות מאסון הובאה לאישור על ידי בעלי התפקידים הרלוונטיים ברשות ותובא לאישור מועצת הרשות בישיבתה הקרובה.

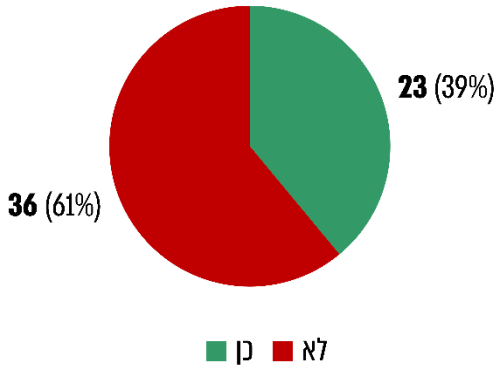
רשות ז' ציינה בתשובתה כי מנמ"ר הרשות יכין תוכנית מקושרת תקציב לנושא התאוששות מאסון, והיא תתוקצב כנדרש.

הרשויות א' ו-ח' ציינו בתשובותיהן כי הן יפעלו להכנת תוכנית להתאוששות מאסון המתאימה לצורכיהן ובהתאם להנחיות מערך הסייבר.

52 דוגמאות לאסון - מתקפת כופרה, דליפת נתונים ממאגר לקוחות וגנבת מידע של לקוחות. עקרונית מדובר באירוע סייבר שמונע מהארגון לתפקד באופן מהותי.

53 BCP - Business Continuity Plan; DRP - Disaster Recovery Plan תוכנית המשכיות עסקית לארגון.

תרשים 18: **מספרן ושיעורן של הרשויות שהכינו תכנית להתאוששות מאסון**



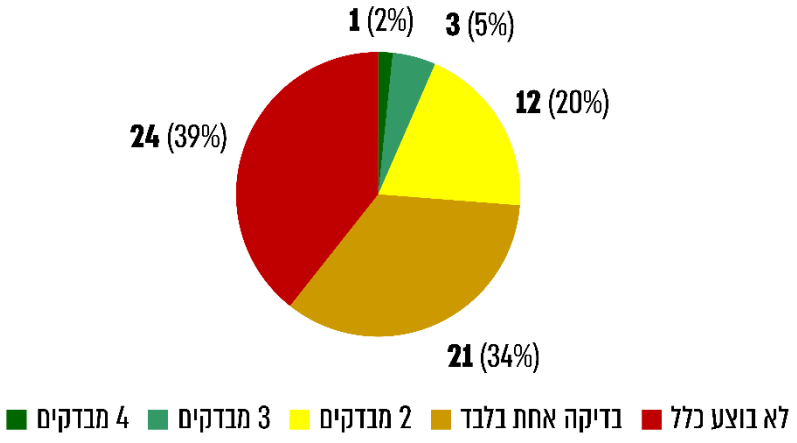

על פי הנתונים שנאספו בשאלון, בעיבוד משרד מבקר המדינה.

## ביצוע של סקרי סיכונים ומבדקי חדירה או ביקורות תקופתיות

בתקנות אבטחת המידע נקבע כי במאגר שחלה עליו רמת אבטחה גבוהה חובה לבצע סקר לאיתור סיכוני אבטחת המידע (להלן - סקר סיכונים), וכן חובה לבצע מבדקי חדירות במערכות המאגר (להלן - מבדקי חדירה) על מנת לבחון את מידת עמידותן בפני סיכונים פנימיים וחיצוניים, וזאת אחת ל-18 חודשים לפחות. עוד נקבע בתקנות כי במאגר מידע שחלה עליו רמת אבטחה גבוהה או בינונית יש לבצע ביקורת תקופתית - פנימית או חיצונית, אחת ל-24 חודשים לפחות, על ידי גורם בעל הכשרה מתאימה לביקורת בנושא אבטחת מידע, שאינו ממונה אבטחת המידע בארגון, כדי לוודא שהמאגר עומד בתנאי תקנות אבטחת המידע (להלן - ביקורת תקופתית). עוד קובעות התקנות כי בעל מאגר מידע שחלה עליו רמת האבטחה הגבוהה רשאי לקיים את הביקורת התקופתית במסגרת ביצוע סקר סיכונים.

אחת השאלות בשאלון הייתה אם הרשויות ביצעו סקרי סיכונים ומבדקי חדירה בשנים 2018 - 2021. מתשובותיהן של הרשויות על השאלון התקבלו הנתונים:

תרשים 19: **מספרן ושיעורן של הרשויות שביצעו סקרי סיכונים, 2018 - 2021**

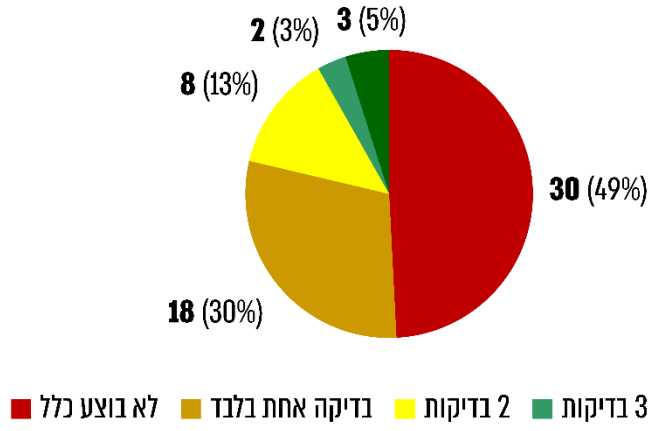



על פי הנתונים שנאספו בשאלון, בעיבוד משרד מבקר המדינה.

מהתרשים עולה כי 39% מהרשויות המקומיות שהשיבו לשאלה זו בשאלון (24 מתוך 61 רשויות), ציינו כי הן כלל לא ביצעו סקרי סיכונים בשנים 2018 - 2021; 34% מהרשויות (21) עשו סקר סיכונים אחד בשנים אלו; 20% מהרשויות (12) עשו שני סקרי סיכונים; 5% מהרשויות (3) עשו שלושה סקרי סיכונים ואילו רשות אחת השיבה כי היא ביצעה ארבעה סקרי סיכונים.

בתשובה לשאלה בשאלון בנוגע לביצוע מבדקי חדירה נתקבלו הנתונים הבאים:

תרשים 20: **מספרן ושיעורן של הרשויות שביצעו מבדקי חדירה, 2018 - 2021**




על פי הנתונים שנאספו בשאלון, בעיבוד משרד מבקר המדינה.

מהתרשים עולה כי 49% מהרשויות המקומיות שהשיבו לשאלה זו בשאלון (30 מתוך 61 רשויות), ציינו כי הן כלל לא ביצעו מבדקי חדירה בשנים 2018 - 2021; 30% מהרשויות (18) עשו מבדק חדירה אחד בשנים אלו; 13% מהרשויות (8) עשו שני מבדקי חדירה; שתי רשויות השיבו כי עשו שלושה מבדקי חדירה ושלוש רשויות השיבו כי עשו ארבעה מבדקי חדירה.

## ביצוע מבדקי החדירה וסקרי הסיכונים ברשויות שנבדקו

בלוח שלהלן יוצגו הממצאים על ביצוע סקרי סיכונים ומבדקי חדירה ברשויות שנבדקו (בשנים 2019 - 2021):

לוח 5: **ביצוע סקר סיכונים ומבדק חדירה על ידי הרשויות שנבדקו**

| שם הרשות | סקר סיכונים | מבדקי חדירה |
|---|---|---|
| א' | X | X |
| ב' | 2021 | 2021 |
| ג' | X | X |
| ד' | X | X |
| ה' | 2020 | X |
| ו' | 2019 | X |
| ז' | 2021 | 2020 |
| ח' | X | X |

על פי נתונים שהועלו בביקורת, בעיבוד משרד מבקר המדינה.

מהלוח עולה כי רשויות ב' ו-ז' ביצעו סקרי סיכונים בשנת 2021 ומבדקי חדירה בשנים 2021 ו-2020 בהתאמה. רשות ה' ביצעה סקר סיכונים בשנת 2020 ולא ביצעה מבדקי חדירה. רשות ו' ביצעה סקר סיכונים בשנת 2019 ולא ביצעה מבדקי חדירה. רשויות ג', ד' ו-ח', לא ביצעו סקרי סיכונים או ביקורות תקופתיות. עוד הועלה כי רשות א' לא ביצעה בעצמה מבדק חדירה או סקר סיכונים אלא הסתמכה בעניין זה על החברה הפרטית המספקת לרשות שירותי מחשוב (חברה ב').

על הרשויות המקומיות ג', ד' ו-ח' לבצע ביקורות תקופתיות, רצוי במסגרת סקרי סיכונים, על מנת למפות ולאתר את סיכוני אבטחת המידע ברשות ולהיערך בהתאם לממצאים שיועלו. עוד מומלץ כי הרשויות המקומיות ג', ד', ה', ו' ו-ח' יבצעו מבדקי חדירה גם אם מאגרי המידע שלהן כפופים לרמת אבטחה בינונית. על רשות א' לדאוג שיהיו בידיה הממצאים הרלוונטיים של סקרי הסיכונים ומבדקי החדירה הנוגעים אליה.

רשות ה' מסרה בתשובתה כי היא מבצעת כיום מבדקי חדירה מעת לעת.

רשות א' ציינה בתשובתה כי היא תסדיר את ביצוע סקרי הסיכונים ומבדקי החדירה מול חברה ב'.

## סיכום ממצאי מבדקי החדירה וסקרי הסיכונים שבוצעו ברשויות שנבדקו

ביצוע סקרי סיכונים ומבדקי חדירה נועד לאתר את החולשות והסיכונים שבמערכות המחשוב בכל הנוגע לחשיפת הרשות לאיומי אירוע סייבר ולסיכונים בדרגות חומרה שונות, על מנת שהרשות תוכל לטפל בהם ולשפר את דרגת אבטחת המידע שלה ואת המוגנות שלה בפני איומים כאלה. התרשים שלהלן מתאר את דרגת הסיכון של ממצאי מבדקי חדירה וסקרי סיכונים בטווח שבין דרגת סיכון נמוכה לדרגת סיכון קריטית:

תרשים 21: **דרגת הסיכון של ממצאי מבדקי חדירה וסקרי סיכונים**

התרשים בעיבוד משרד מבקר המדינה.

להלן סיכום הממצאים שעלו בסקרי הסיכונים ובמבדקי החדירה שביצעו הרשויות שנבדקו[54]:

54 הרשויות הן שמסרו את הנתונים.

לוח 6: **סיכום ממצאי סקרי הסיכונים ומבדקי החדירה ברשויות שנבדקו**

| הרשות | שנת ביצוע המבדק או הסקר | סה"כ ליקויים שנמצאו* | דרגת הסיכון של הליקויים שנמצאו | מצב הטיפול בליקויים** |
|---|---|---|---|---|
| ב' | 2021 | 43 | 12 - גבוהה<br>25 - בינונית<br>6 - נמוכה | 17 - טופלו<br>19 - נמצאים בטיפול<br>(4 - גבוהה, 12 - בינונית, 3 - נמוכה)<br>7 - בתוכנית העבודה 2022<br>(3 - גבוהה, 3 - בינונית, 1 - נמוכה) |
| ז' | 2020 | 9 | 6 - גבוהה<br>3 - בינונית | 8 - טופלו<br>1 -טופל חלקית (בינונית) |
| ו' | 2019 | 44 | 27 - קריטית<br>12 - גבוהה<br>1 - בינונית<br>4- נמוכה | 22 - טופלו<br>17 - טופלו חלקית<br>(12 - קריטית, 3 - גבוהה, 2 - בינונית)<br>5 - טרם טופלו<br>(3 - גבוהה, 2 - בינונית). |
| ה' | 2020 | 25 | 21 - גבוהה<br>3 - בינונית<br>1 - נמוכה | לא התקבלו נתונים |

על פי נתונים שהועלו בבדיקה, בעיבוד משרד מבקר המדינה.

* הנתונים המוצגים על הרשויות המקומיות ב' ו-ז' מקורם בממצאים של מבדקי החדירה, ואילו הנתונים על הרשויות המקומיות ה' ו-ו' מקורם בממצאי סקרי הסיכונים.

** נכון למועד סיום הביקורת.

הרשות המקומית ג' ציינה בתשובתה כי היא מקבלת את המלצות משרד מבקר המדינה בעניין ביצוע סקרי סיכונים ומבדקי חדירה, וכי היא תפעל ליישם את ההמלצות בשנים 2022 ו-2023.

יצוין כי בסקר הסיכונים שבוצע ברשות המקומית ה' הוצגו הליקויים במישור הכללי בלי לפרט המלצות לתיקון. מנמ"ר הרשות מסר לנציגי משרד מבקר המדינה כי חלק מהממצאים מיושם, אך אין בידו פירוט מה נעשה בפועל ומהו סטטוס הטיפול לגבי הליקויים השונים.

הרשות המקומית ו' ציינה בתשובתה כי היא "פועלת בימים אלה ביחד עם האשכול לבצע מבדקי חדירה".

מהלוח עולה כי במבדק החדירה שביצעה הרשות המקומית ב' עלו 43 ליקויים בדרגות סיכון נמוכה עד גבוהה וכי עד למועד סיום הביקורת הרשות טיפלה ב-17 ליקויים מתוכם, 19 ליקויים נמצאים בטיפול ושבעה ליקויים טרם טופלו. במבדק חדירה שערכה הרשות המקומית ז' עלו תשעה ליקויים בדרגות סיכון בינונית וגבוהה והרשות טיפלה בשמונה ליקויים מתוכם ואחד טופל חלקית. בסקר הסיכונים שערכה הרשות המקומית ו' נמצאו 44 ליקויים בדרגות סיכון נמוכה עד קריטית, מתוכם טיפלה הרשות ב-22 ליקויים, 17 ליקויים טופלו באופן חלקי וחמישה ליקויים טרם טופלו. בסקר הסיכונים שביצעה הרשות המקומית ה' עלו 25 ליקויים בדרגות סיכון נמוכה עד גבוהה ואין בידי הרשות פירוט האם תוקנו הליקויים האמורים.

הרשות המקומית ד' ציינה בתשובתה כי היא מתכוונת לפעול בשיתוף אשכול העמקים לתיקון הליקויים שהועלו בדוח, ובכלל זה לביצוע סקר סיכונים כנדרש.

הנתונים האמורים מדגישים את חשיבות ביצועם של סקרי סיכונים ומבדקי חדירה ברשויות המקומיות ואת תרומתם לחיזוק מידת חוסנן הקיברנטי ולהפקת לקחים לשיפור ביצועיהן ולייעול מערכות המידע בתחומן.

הרשות המקומית ח' ציינה בתשובתה כי היא נמצאת בהליך בחירת חברה לביצוע סקרי סיכונים ומבדקי חדירה, וממצאיהם ישמשו בסיס לתוכנית אסטרטגית רב-שנתית.

על הרשות המקומית ה' לפעול ליישום מלא של ממצאי סקר הסיכונים ובמסגרת זו לברר עם החברה שביצעה אותו מהן המלצותיה המפורטות לתיקון הליקויים שעלו ולוודא כי היא פועלת לתיקונם.

יש לציין לחיוב את הרשויות המקומיות ב', ו' ו-ז' על שביצעו מבדקי החדירה או סקרי הסיכונים למיפוי הסיכונים ברשות. עם זאת, עליהן להשלים את הטיפול ביישום ההמלצות, ובפרט באותם ליקויים בעלי רמת סיכון גבוהה.

## לוח 7: סיכום הליקויים ברשויות שנבדקו

| | א' | ב' | ג' | ד' | ה' | ו' | ז' | ח' |
|---|---|---|---|---|---|---|---|---|
| רישום מאגרי מידע | √ | √ | X | X | √ | √ | √ | √ |
| מסמך הגדרות מאגרי מידע | ½ | X | X | X | X | ½ | X | X |
| מינוי ממונה/ מנהל אבטחת מידע | √ | √ | √ | X | √ | √ | √ | √ |
| נוהל אבטחת מידע | X | √ | X | ½ | X | ½ | √ | ½ |
| רשימת מצאי | X | √ | X | X | X | X | X | X |
| הדרכות במעמד קליטת עובד חדש | X | √ | X | X | X | ½ | √ | X |
| הדרכות תקופתיות לעובדים | ½ | √ | X | X | X | ½ | √ | X |
| חדרי שרתים | √ | √ | ½ | √ | √ | ½ | √ | X |
| ניהול הרשאות גישה | √ | √ | X | X | X | √ | √ | √ |
| התקנים ניידים | X | ½ | X | X | ½ | ½ | √ | X |
| אבטחת מיחשוב (אנטי וירוס) | √ | √ | √ | X | √ | √ | √ | X |
| מערכת הפעלה | X | X | X | X | X | X | X | X |
| נוהל גיבויים | X | √ | X | X | X | √ | X | √ |
| ביצוע גיבויים | √ | √ | X | X | √ | √ | √ | X |
| תכנית התאוששות מאסון | X | X | X | X | X | ½ | X | X |
| ביצוע סקר סיכונים | - | √ | - | - | √ | √ | √ | - |
| ביצוע מבדק חדירה | - | √ | - | - | - | - | √ | - |

מקרא:

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| X | לא תקין | ½ | חלקי | √ | תקין | - | אין חובה על פי התקנות |

# סיכום

השימוש במערכות מידע לניהול ענייני הרשויות המקומיות הפך עם השנים לצורך בסיסי ומחויב המציאות. במאגרי המידע של הרשויות המקומיות שמורים, בין היתר, נתונים אישיים על התושבים ועל הגורמים הבאים בקשר עם הרשויות במגוון תחומים ומכאן נובע הצורך לשמור על מאגרי המידע באופן שלא יאפשר לגורמים בלתי מורשים גישה לנתונים השמורים בהם או לעשות בהם שימוש בלתי חוקי ולגרום בכך נזק, בנוסף לצורך של הגנה על מערכות המידע מפני איומי סייבר. בביקורת נבדק האופן שבו מנהלות הרשויות המקומיות את מערכות המידע שלהן, ובכלל זה נבדקו סוגיות מרכזיות ביישום ההוראות החוקיות החלות על אבטחת מאגרי המידע.

הביקורת העלתה כי אין אסטרטגיה כוללת לניהול מערכות המידע ברשויות, ומשרד הפנים ומערך הסייבר הלאומי לא פרסמו הנחיות בנוגע לאופן שבו על הרשויות לנהל את מערכות המידע שלהן ולאבטח אותן, לרבות בפני אירועי סייבר. בהיעדר הנחיה מחייבת כל רשות פועלת בתחום זה כרצונה, לפי תפיסתה ולפי סדרי העדיפויות שלה, אשר אינם בהכרח עונים על צרכיה. עלה כי בשש משמונה הרשויות שנבדקו לא הוכנו תוכניות בתחום הסייבר, לרבות תוכניות עבודה אסטרטגיות ותוכניות עבודה שנתיות מקושרות תקציב וכי בשתי הרשויות שהוכנו תוכניות אסטרטגיות - אלו לא תוקצבו.

כמו כן הועלו ליקויים שונים בתחום אבטחת המידע בחלק מהרשויות המקומיות, ובהם אי-מינוי מנהל אבטחת מידע ובעלי תפקידים אחרים בתחום מערכות המידע; היעדר נוהל אבטחת מידע; אי-רישום מאגרי המידע של הרשות; היעדר רשימת מצאי של רכיבי החומרה והתוכנה ברשות; אי-קיום הדרכות במעמד קליטת העובדים לרשות; אי-קיום הדרכות תקופתיות; שימוש בתוכנת אנטי-וירוס ללא רישיון או שאינה עדכנית; שימוש במערכת הפעלה שאינה עדכנית או שאינה נתמכת; היעדר תוכנית להתאוששות מאסון וכן אי-ביצוע בדיקת חוסן קיברנטי, לרבות אי-ביצועם של סקרי סיכונים ומבדקי חדירה. בארבע מהרשויות שנבדקו בוצעו מבדקי חדירה וסקרי סיכונים, וממצאיהם עולה שהרשויות אינן ערוכות לאירועי סייבר. יש לציין לחיוב את הרשויות המקומיות ב', ו' ו-ז' על שביצעו מבדקי החדירה או סקרי הסיכונים למיפוי הסיכונים ברשות.

ההגנה על תפקודן התקין של מערכות המידע וכן הגנה על המידע הנמצא בשימוש השלטון המקומי חיוניות לשמירה על מרקם החיים בעיתות שגרה וחירום, והן עשויות להשפיע רבות על חייו של הפרט ברשות המקומית. מכאן שקידום הגנת הסייבר בשלטון המקומי הוא יעד לאומי חשוב. לנוכח זאת משרד מבקר המדינה ממליץ למשרד הפנים ולמערך הסייבר הלאומי לפעול במשותף ליישום החלטת הממשלה 2443 בנוגע להסדרת ההיערכות של הרשויות המקומיות לאיומי סייבר, תוך התחשבות בייחודיות של מגזר השלטון המקומי, ולקביעת נהלים והנחיות לרשויות המקומיות בתחום ניהול מערכות המידע, לבדיקת חוסנן ולאבטחתן בפני התקפות סייבר. על כלל הרשויות המקומיות לבחון את הליקויים וההמלצות שהועלו בדוח זה ולנקוט את כל האמצעים העומדים לרשותן לניהול מיטבי של מערכות המידע שלהן ולהגברת מוכנותן להגנה על המידע הרגיש הנמצא בבעלותן ולמניעת פגיעה ברציפות התפקודית שלהן.