אבטחת מידע והגנת הפרטיות ברשויות המקומיות

מעקב מורחב

מבקר המדינה, **דוח ביקורת שנתי 62** (2012),
"אבטחת מידע והגנת הפרטיות ברשויות מקומיות"

תקציר

רקע כללי

הזכות לפרטיות וחובת השמירה על צנעת הפרט עוגנו בחקיקה - הזכות לפרטיות היא זכות חוקתית מוגנת על פי סעיף 7 לחוק-יסוד: כבוד האדם וחירותו, הקובע כי "כל אדם זכאי לפרטיות ולצנעת חייו"; חוק הגנת הפרטיות, התשמ"א-1981 (להלן - חוק הגנת הפרטיות או החוק), קובע כי "לא יפגע אדם בפרטיות של זולתו ללא הסכמתו". החוק מגדיר, בין היתר, "מידע" כ"נתונים על אישיותו של אדם, מעמדו האישי, צנעת אישותו, מצב בריאותו, מצבו הכלכלי, הכשרתו המקצועית, דעותיו ואמונתו", ו"מאגר מידע" כ"אוסף נתוני מידע, המוחזק באמצעי מגנטי או אופטי והמיועד לעיבוד ממוחשב". עוד קובע החוק כי "בעל מאגר מידע, מחזיק במאגר מידע או מנהל מאגר מידע, כל אחד מהם אחראי לאבטחת המידע שבמאגר המידע".

ברשויות המקומיות מאגרי מידע רבים המשמשים בסיס לעבודתן בעתות רגיעה וחירום, בין היתר בתחומים האלה: כספים, תכנון ובנייה, חינוך, רווחה, כוח אדם, רישוי עסקים, תחבורה וחניה, תברואה. בשנים האחרונות אף גדל מספר הערים החכמות - ערים המשתמשות בטכנולוגיות מידע ותקשורת לשיפור ניהול נכסיהן ואיכות החיים של תושביהן. מגמה זו מביאה לגידול חד בכמות הנתונים שבידי הרשויות המקומיות ובמספר מאגרי המידע שבבעלותן. פגיעה במערכות הממוחשבות ובמאגרי המידע של הרשויות המקומיות עלולה לגרום לנזקים כבדים, כמו פגיעה בשירותים הניתנים לתושב ובצנעת הפרט, ולכן מוטלת עליהן החובה להגן על המידע.

בדוח בנושא אבטחת מידע והגנת הפרטיות ברשויות המקומיות שפרסם מבקר המדינה במאי 2012[1] (להלן - הביקורת הקודמת) הועלו ליקויים רבים הן במישור המאסדרים בתחום זה - הרשות למשפט, טכנולוגיה ומידע (להלן - רמו"ט), שהוקמה במשרד המשפטים בספטמבר 2006 כרשות להגנת מידע אישי בישראל, והמינהל לשלטון מקומי במשרד הפנים - והן במישור הרשויות המקומיות[2].

1 מבקר המדינה, **דוח ביקורת שנתי 62** (2012), "אבטחת מידע והגנת הפרטיות ברשויות מקומיות", עמ' 1513-1537.

2 הרשויות המקומיות שנבדקו בביקורת הקודמת הן: עיריות אשקלון, בני ברק, טירה, יהוד-מונוסון ויקנעם עילית והמועצות המקומיות בני עי"ש ורמת ישי.

פעולות הביקורת

בחודשים אוקטובר 2016 - ינואר 2017 עשה מבקר המדינה ביקורת בנושא אבטחת המידע והגנת הפרטיות ברשויות המקומיות (להלן - הביקורת הנוכחית). הביקורת הנוכחית כללה גם מעקב אחר אופן תיקון הליקויים שהועלו בביקורת הקודמת בפעולותיהם של עיריות יהוד-מונוסון ויקנעם עילית, רמו"ט ומשרד הפנים בנושא האמור. כמו כן נבדקו פעולותיהן בנושא של חמש רשויות מקומיות נוספות שלא נכללו בביקורת הקודמת - עיריות באר שבע, כרמיאל ונצרת עילית, המועצה המקומית תל מונד והמועצה האזורית הגליל התחתון (להלן - הרשויות המקומיות הנוספות שנבדקו). בדיקות השלמה נעשו ברשות הלאומית להגנת הסייבר במשרד ראש הממשלה.

הליקויים העיקריים

אסדרת הטיפול בנושא אבטחת מידע והגנת הפרטיות

הצוותים לתיקון הליקויים של משרד הפנים ושל משרד המשפטים לא דנו בממצאי הביקורת הקודמת על פעולות המינהל לשלטון מקומי ורמו"ט, בהתאמה, שלא כנדרש בחוק מבקר המדינה, התשי"ח-1958 [נוסח משולב], ולא פעלו לתיקון הליקויים שהועלו בה.

היערכות משרד הפנים לאיומי סייבר[3] נמצאת רק בראשית דרכה, וטרם הוקם גוף שיפקח על היערכותן של הרשויות המקומיות לאיומי סייבר וינחה את הרשויות בתחום זה כמתחייב מהחלטת ממשלה 2443 מפברואר 2015 בה נקבע כי משרדי הממשלה, שבמסגרתם מופעלות סמכויות רגולציה כלפי גופים או פעילויות החשופים לאיומי סייבר, יקדמו את הטיפול בהיערכות לאיומי סייבר במסגרת המגזר שבו הם פועלים.

פעילות הרשויות המקומיות בתחום אבטחת מידע והגנת הפרטיות עדיין אינה מאוסדרת על ידי השלטון המרכזי. המינהל לשלטון מקומי במשרד הפנים ורמו"ט שבמשרד המשפטים ממשיכים להטיל זה על זה את האחריות לאסדרת הנושא. כתוצאה, כל רשות מקומית מתמודדת עם נושא אבטחת המידע והגנת הפרטיות כמיטב הבנתה ולפי התקציב שהקצתה לנושא, ובעקבות כך חלק מהרשויות המקומיות אינן מטפלות כראוי בנושא.

> פעילות הרשויות המקומיות בתחום אבטחת המידע והגנת הפרטיות עדיין אינה מאוסדרת על ידי השלטון המרכזי. משרד הפנים ורמו"ט שבמשרד המשפטים ממשיכים להטיל זה על זה את האחריות לאסדרת הנושא

3 בהחלטת ממשלה 3611 מ-7.8.11 הוגדר מרחב הסייבר כ"המתחם הפיזי והלא פיזי, שנוצר או מורכב מחלק או מכל הגורמים הבאים: מערכות ממוכנות ממוחשבות, רשתות מחשבים ותקשורת, תוכנות, מידע ממוחשב, תוכן שמועבר באופן ממוחשב, נתוני תעבורה ובקרה והמשתמשים של כל אלה".

אבטחת המידע הממוחשב ברשויות המקומיות

רישום מאגרי מידע: עיריית כרמיאל והמועצה המקומית תל מונד לא רשמו את מאגרי המידע שלהן אצל רשם מאגרי המידע ברמו"ט; עיריות יקנעם עילית ונצרת עילית רשמו רק חלק ממאגרי המידע שלהן; וועדים מקומיים[4] במועצה האזורית הגליל התחתון לא רשמו את מאגרי המידע שלהם.

מינוי ממונה על אבטחת מידע: משרד הפנים לא בחן אם יש להחיל על הרשויות המקומיות את הוראות החוק להסדרת הביטחון בגופים ציבוריים, התשנ"ח-1998, ולפיהן ממוני הביטחון מופקדים על הפעולות לאבטחת מידע ומערכות המידע, אף שנדרש לעשות כן בביקורת הקודמת; בקובץ תיאורי התפקיד[5] שפרסם משרד הפנים נקבע, שלא בדומה להמלצות למשרדי הממשלה המפורטות בנוהלי המסגרת לאבטחת מידע[6] (להלן - נוהלי המסגרת), כי מנהל אבטחת המידע ברשות מקומית יהיה כפוף למנהל מערכות המידע הראשי שלה.

נהלים והנחיות לאבטחת מידע: עיריות כרמיאל ונצרת עילית והמועצה המקומית תל מונד לא קבעו נהלים, הנחיות וכללים מחייבים לאבטחת המידע. כל הרשויות המקומיות שנבדקו אינן מנהלות רישום מעודכן של הרשאות הגישה למאגרי המידע שניתנו לכל אחד מעובדיהן.

בקרה ופיקוח לוגיים[7]: כל הרשויות המקומיות שנבדקו אינן מבצעות ניטור יזום של יומני השימוש על מנת לזהות פעולות חריגות אשר גורמים בלתי מורשים ביצעו או ניסו לבצע.

אבטחת חומרה: חדרי המחשב של עיריות יהוד-מונוסון, כרמיאל ונצרת עילית, המועצה המקומית תל מונד והמועצה האזורית הגליל התחתון אינם עומדים בדרישות התקן הישראלי בנושא בטיחות אש של מחשבים וציוד היקפי.

סקרי סיכונים ובדיקות חדירה: עיריות כרמיאל ונצרת עילית, המועצה המקומית תל מונד והמועצה האזורית הגליל התחתון לא ביצעו מעולם סקרי סיכונים ומבחני חדירה כדי להעריך את הסיכונים הנשקפים למאגרי המידע שברשותן ואת הנזק העלול להיגרם למערכות המידע שלהן.

4 הוועדים המקומיים בית קשת, בית רימון, גבעת אבני, הזורעים, מצפה נטופה ושרונה.

5 משרד הפנים, מינהל השלטון המקומי, האגף לכוח אדם ושכר ברשויות המקומיות, **קובץ ניתוח העיסוקים ותיאורי התפקידים ברשויות המקומיות** (ספטמבר 2011).

6 משרד ראש הממשלה, אגף בכיר לביקורת המדינה והביקורת הפנימית, המועצה המייעצת לביקורת ואבטחת מידע, **נוהלי מסגרת לאבטחת מידע**, מהדורה שלישית (ספטמבר 2005).

7 בקרה לוגית - ניטור ממוחשב שוטף של הפעילות במערכת הממוחשבת תוך התמקדות באירועים חריגים או רגישים; פיקוח לוגי - מעקב אחר פעילויות במחשב גם לאחר ביצוע הפעילות.

אירועי אבטחת מידע: אף שבשנים האחרונות גדל היקף התקיפות באמצעות נוזקות (malware)[8] שונות, והפרות החוק ו"פשיעת המידע" הולכות ומתרבות, אין בידי שום גורם תמונת מצב עדכנית על היקף התופעה ברשויות המקומיות, זאת בשל היעדר חובת דיווח על פגיעות מסוג זה. למשל, עיריות יהוד-מונוסון, יקנעם עילית, כרמיאל ונצרת עילית הותקפו לפחות פעם אחת על ידי נוזקה מסוג כופרה (ransomware)[9]. בעיריית נצרת עילית נפגע השרת במחלקת ההנדסה, ולמועד סיום הביקורת, ינואר 2017, הקבצים השמורים בשרת נשארו מוצפנים ולעירייה לא הייתה גישה אליהם.

התקשרויות עם חברות פרטיות המחזיקות במאגרי מידע של הרשות המקומית

רשם מאגרי המידע ברמו"ט אינו אוכף על חברות פרטיות המחזיקות במאגרי מידע של רשויות מקומיות את חובת הדיווח השנתי על מאגרי המידע שהן מחזיקות בהם כנדרש בחוק.

לעיריית כרמיאל אין חוזים למתן שירותים עם כל החברות הפרטיות המחזיקות במאגרי המידע שלה.

הדרכה וביקורת בתחום אבטחת מידע והגנת הפרטיות ברשויות המקומיות

כל הרשויות המקומיות שנבדקו לא קבעו תכנית הדרכה והסברה שנתית לעובדים בתחום אבטחת המידע והגנת הפרטיות.

בשנים 2006-2016 לא בוצעו ביקורות פנימיות בנושא אבטחת מידע והגנת הפרטיות בעיריית כרמיאל, במועצה המקומית תל מונד ובמועצה האזורית גליל תחתון.

האגף לביקורת ברשויות המקומיות של משרד הפנים אינו מבצע ביקורת בנושא אבטחת מידע והגנת הפרטיות במסגרת הביקורת השנתית של רואי החשבון המבקרים.

8 תוכנה שמטרתה לחדור למחשב או להזיק לו ללא ידיעתו של המשתמש בו. הגדרה זו חלה על וירוסים, תולעי מחשבים, רוגלות (תוכנות ריגול), סוסים טרויאניים ותוכנות פרסום.

9 נוזקה המגבילה את הגישה לנתונים השמורים במערכת המחשב ומשמשת לסחוט מהמשתמש תשלום (דמי כופר) על מנת שתוסר מגבלת הגישה למערכת.

ההמלצות העיקריות

על משרד הפנים לפרסם בקרב הרשויות המקומיות קובץ הנחיות מחייב בנושא אבטחת מידע והגנת הפרטיות. על ההנחיות לעסוק בחובת הרישום של מאגרי מידע - ובכלל זה בחובת הרישום החלה על ועדים מקומיים, ובנושאי האבטחה הלוגית והפיזית, בחובת הדיווח על אירועי אבטחת מידע ועל הפעולות שננקטו בעקבותיהם ובחובה לקיים פעולות הדרכה והסברה בתחום אבטחת המידע, בדומה להמלצות המפורטות בנוהלי המסגרת. על המשרד להקים בהקדם גוף מנחה ומפקח בתחום ההיערכות לאיומי סייבר מול הרשויות המקומיות כמתחייב מהחלטת ממשלה 2443 מפברואר 2015.

נוכח מספרם הרב של מאגרי מידע בבעלות רשויות מקומיות שאינם רשומים אצל רשם מאגרי המידע, על רמו"ט לבחון את הפעולות הנדרשות לאסדרת הנושא ולאכוף את הוראות החוק.

על הרשויות המקומיות לרשום את כל מאגרי המידע שלהן; לבצע סקרי סיכונים ובדיקות חדירות; לבצע בקרה ופיקוח לוגיים על הפעולות המתבצעות במאגרי המידע שבבעלותן; לאבטח את חדרי המחשב שלהן ולהתאימם לדרישות התקן הישראלי בנושא בטיחות אש של מחשבים וציוד היקפי; לגבש וליישם תכנית הדרכה והסברה לעובדים; ולכלול בתכניות הביקורת של מבקרי הפנים שלהן ביקורת בנושא אבטחת מידע והגנת הפרטיות.

סיכום

במסגרת פעילותן השוטפת של הרשויות המקומיות נעשה שימוש רב במאגרי מידע הכוללים נתונים אישיים רבים על התושבים. ככל שהן מרבות להשתמש במאגרי מידע גוברת הסכנה שהמידע ייחשף ברבים ותיפגע פרטיותם של התושבים. לכן מוטלת על הרשויות המקומיות החובה להגן על מידע זה ולהגביר את חסינותן הן בפני דליפת מידע והן לצורכי הגנה על רציפות תפקודית לטובת השירות לציבור.

בשנים האחרונות גדל היקף התקיפות של מערכות המחשוב של גופים רבים באמצעות כופרות המגבילות גישה למערכות המחשב, שנועדו לסחוט מהמשתמש תשלום כסף (דמי כופר) על מנת שתוסר מגבלת הגישה או באמצעות נוזקות המאפשרות לאדם שאינו מוסמך לכך להעתיק את הנתונים השמורים בהן. ההיקף הכולל של התופעה ברשויות מקומיות אינו ידוע, בהיעדר חובה לדווח על תקיפות מסוג זה.

ממצאי הביקורת מלמדים כי במועד סיום הביקורת הנוכחית, כחמש שנים לאחר שבוצעה הביקורת הקודמת, משרד הפנים ומשרד המשפטים עדיין

מטילים זה על זה את האחריות לאסדרת הנושא, ולמותר לציין שהם לא פעלו לתיקון הליקויים שהועלו בביקורת הקודמת, והדבר פוגע ברמת אבטחת המידע בשלטון המקומי. עוד מעידים ממצאי הביקורת כי כל רשות מקומית עדיין מתמודדת עם נושא אבטחת המידע והגנת הפרטיות כמיטב הבנתה ולפי התקציב שהקצתה לנושא, ובעקבות כך חלק מהרשויות המקומיות אינן מטפלות כראוי באבטחת המידע שלהן ובהגנה על הפרטיות של תושביהן.

נוכח האמור לעיל, על מנכ"ל משרד הפנים ומנכ"לית משרד המשפטים לגבש מתכונת ברורה של חלוקת תחומי האחריות והסמכויות בין משרדיהם בכל הנוגע לאבטחת המידע והגנת הפרטיות ברשויות המקומיות, ולפעול למימושה של מתכונת זו.

על הרשויות המקומיות לתקן את הליקויים שהועלו בדוח בנוגע לפעולותיהן בתחום אבטחת המידע והגנת הפרטיות, לפעול להעלאת המודעות בקרב עובדיהן לחשיבות הנושא ולהעמיד לרשות העובדים את האמצעים למילוי חובותיהם בתחום זה.

כל רשות מקומית מתמודדת עם נושא אבטחת המידע כמיטב הבנתה ולפי התקציב שהקצתה לנושא, ובעקבות כך חלק מהרשויות המקומיות אינן מטפלות כראוי באבטחת המידע שלהן ובהגנה על הפרטיות של תושביהן

מבוא

הזכות לפרטיות וחובת השמירה על צנעת הפרט עוגנו בחקיקה - הזכות לפרטיות היא זכות חוקתית מוגנת על פי סעיף 7 לחוק-יסוד: כבוד האדם וחירותו, הקובע כי "כל אדם זכאי לפרטיות ולצנעת חייו"; חוק הגנת הפרטיות, התשמ"א-1981 (להלן - חוק הגנת הפרטיות או החוק), קובע כי "לא יפגע אדם בפרטיות של זולתו ללא הסכמתו".

בחוק הגנת הפרטיות הוגדרו: "מאגר מידע" - "אוסף נתוני מידע, המוחזק באמצעי מגנטי או אופטי והמיועד לעיבוד ממוחשב"[10]; "מידע" - "נתונים על אישיותו של אדם, מעמדו האישי, צנעת אישותו, מצב בריאותו, מצבו הכלכלי, הכשרתו המקצועית, דעותיו ואמונתו".

היות שמאגרי המידע מכילים פרטים אישיים, ומסירת נתונים על אדם לזולת עלולה לפגוע בפרטיותו, יש לאבטח את המידע. ככל שאדם עלול להיפגע יותר מגילוי המידע עליו ברבים, עולה רמת רגישות המידע ועמה רמת האבטחה שיש לנקוט כדי לשמור עליו. חוק הגנת הפרטיות מגדיר "אבטחת מידע" - כ"הגנה על שלמות המידע, או הגנה על המידע מפני חשיפה, שימוש או העתקה, והכל ללא רשות כדין". החוק קובע כי "בעל מאגר מידע, מחזיק במאגר מידע או מנהל מאגר מידע, כל אחד מהם אחראי לאבטחת המידע שבמאגר המידע".

היקף מאגרי המידע שבהם מנוהל מידע אישי בישראל גדל מדי שנה, ואף היקף הפרות החוק בנושא ו"פשיעת המידע" הולך וגדל. האמצעים שנוקטים מפרי החוק משתנים תדיר, ועקב כך גוברים הסיכונים הכרוכים בהפרת החוק ובנזק הפוטנציאלי הנשקף עקב כך. המציאות מלמדת שדליפת מידע רגיש, גישה לא מורשית למאגרים ושימוש במידע מהמאגרים למטרות זרות הופכים שכיחים יותר ויותר[11].

אבטחת מידע מתבצעת בכמה תחומים: אבטחה פיזית של מידע ממוחשב - ביצוע פעולות בחומרה ובתשתיות כדי למנוע פגיעה פיזית במאגר המידע; אבטחה לוגית של מידע ממוחשב - הפעלה של מנגנוני תוכנה ייעודיים, לדוגמה הזנת שם משתמש וסיסמה כתנאי להפעלת מחשב או לכניסה לבסיס נתונים; אבטחה פיזית של מידע לא ממוחשב - כל הפעולות הנדרשות להגנה על פלטי מחשב, על דוחות, על מזכרים ועל מסמכים שונים המכילים מידע כהגדרתו בחוק.

ברשויות המקומיות מאגרי מידע רבים המשמשים בסיס לעבודתן בעתות רגיעה וחירום, בין היתר בתחומים האלה: כספים, תכנון ובנייה, חינוך, רווחה, כוח

10 למעט, כפי שנקבע בחוק, "אוסף לשימוש אישי שאינו למטרות עסק" או "אוסף הכולל רק שם מען ודרכי התקשרות, אשר כשלעצמו אינו יוצר אפיון שיש בו כדי לפגוע בפרטיות של בני האדם ששמותיהם כלולים בו, ובלבד שלבעל האוסף או לתאגיד בשליטתו אין אוסף נוסף".

11 משרד המשפטים, הרשות למשפט, טכנולוגיה ומידע, רשם מאגרי המידע, **דוח לשנת 2014** (פורסם בשנת 2015).

אדם, רישוי עסקים, תחבורה וחניה, תברואה. בשנים האחרונות אף גדל מספר הערים החכמות - ערים המשתמשות בטכנולוגיות מידע ותקשורת לשיפור ניהול נכסיהן ואיכות החיים של תושביהן. מגמה זו מביאה לגידול חד בכמות הנתונים שבידי הרשויות המקומיות ובמספר מאגרי המידע שבבעלותן. פגיעה במערכות הממוחשבות ובמאגרי המידע של הרשויות המקומיות עלולה לגרום לנזקים כבדים, ובכלל זה לפגיעה בשירותים הניתנים לתושבים ובצנעת הפרט, ולכן מוטלת עליהן החובה להגן על המידע.

בדוח בנושא אבטחת מידע והגנת הפרטיות ברשויות המקומיות שפרסם משרד מבקר המדינה במאי 2012[12] (להלן - הביקורת הקודמת) הועלו ליקויים הן במישור השלטון המרכזי - הרשות למשפט, טכנולוגיה ומידע במשרד המשפטים (להלן - רמו"ט) והמינהל לשלטון מקומי במשרד הפנים (להלן - המינהל לשלטון מקומי), והן במישור הרשויות המקומיות שנבדקו[13].

> פגיעה במערכות הממוחשבות ובמאגרי המידע של הרשויות המקומיות עלולה לגרום לנזקים כבדים, ובכלל זה לפגיעה בשירותים הניתנים לתושבים ובצנעת הפרט

פעולות הביקורת

בחודשים אוקטובר 2016 - ינואר 2017 עשה מבקר המדינה ביקורת בנושא אבטחת המידע והגנת הפרטיות ברשויות המקומיות (להלן - הביקורת הנוכחית). הביקורת הנוכחית כללה גם מעקב אחר אופן תיקון הליקויים שהועלו בביקורת הקודמת בפעולותיהם של עיריות יהוד-מונוסון ויקנעם עילית, רמו"ט והמינהל לשלטון מקומי בנושא האמור. עוד נבדקו פעולותיהן בנושא של חמש רשויות מקומיות נוספות, שלא נכללו בביקורת הקודמת - עיריות באר שבע, כרמיאל ונצרת עילית; המועצה המקומית תל מונד והמועצה האזורית הגליל התחתון (להלן - הרשויות המקומיות הנוספות שנבדקו). בדיקות השלמה נעשו ברשות הלאומית להגנת הסייבר במשרד ראש הממשלה.

12 מבקר המדינה, **דוח ביקורת שנתי 62** (2012), "אבטחת מידע והגנת הפרטיות ברשויות מקומיות", עמ' 1513-1537.

13 הרשויות המקומיות שנבדקו בביקורת הקודמת הן: עיריות אשקלון, בני ברק, טירה, יהוד-מונוסון ויקנעם עילית והמועצות המקומיות בני עי"ש ורמת ישי.

פעולות השלטון המרכזי לאסדרת אבטחת המידע והגנת הפרטיות

לשם אסדרת אבטחת המידע והגנת הפרטיות ברשויות המקומיות נדרשות הכוונה, הנחיה והנחת תשתית של נהלים ופיקוח של השלטון המרכזי. הגופים העיקריים האחראים לכך הם משרד הפנים - שהוא מאסדר השלטון המקומי, ורמו"ט - שהיא הגורם המוסמך לפי חוק הגנת הפרטיות על מילוי הוראות החוק והתקנות שהותקנו לפיו.

משרד הפנים

המינהל לשלטון מקומי הוא הגורם המקצועי במשרד הפנים המופקד על אופיו ופעולתו של השלטון המקומי. המינהל עוסק, בין היתר, בתקצוב הרשויות המקומיות; בבקרה וביקורת; במתן אישורים בנושאי כוח אדם ושכר; ובהדרכה וטיפול בנושאים פרטניים. הטיפול בנושאים אלה מתבצע, בין היתר, באמצעות פרסום הוראות וחוזרי מנכ"ל לרשויות המקומיות.

להלן יפורטו ממצאי הביקורת העיקריים שעלו בנושא פעילותם של משרד הפנים ושל המינהל לשלטון מקומי בנושא אבטחת המידע ברשויות המקומיות:

1. בביקורת הקודמת הועלה כי פעילותן של 257 הרשויות המקומיות בתחום אבטחת מידע והגנת הפרטיות התבצעה ללא אסדרה בדרג הממשלתי שתאפשר להניח את התשתית הנוהלית והמקצועית לטיפול בנושא. עוד הועלה כי משרד הפנים לא נקט פעולות של ממש לקידום פעילותן של הרשויות המקומיות בתחום זה. המינהל לשלטון מקומי לא קבע מדיניות לאבטחת מידע ולהגנת הפרטיות ברשויות המקומיות, לא הניח תשתית לביצועה ולא פעל לקביעת הנחיות בתחום זה. משרד מבקר המדינה העיר למשרד הפנים בביקורת הקודמת כי עליו להוציא לרשויות המקומיות קובץ הנחיות מחייב בנושא אבטחת מידע והגנת הפרטיות ולוודא כי הוא מוטמע ומיושם, וכי אם אין הוא בעל הידע והמומחיות הנדרשים לצורך קביעת נהלים בנושא אבטחת מידע, ראוי שיפנה לרמו"ט בבקשה שתסייע לו בנושא.

   סעיף 21א לחוק מבקר המדינה, התשי"ח-1958 [נוסח משולב] (להלן - חוק מבקר המדינה), קובע כי ראש כל גוף מבוקר ימנה צוות לתיקון ליקויים, שידון בליקויים שהעלתה הביקורת בפעולתו של אותו גוף, יקבל החלטות בדבר תיקונם וידווח לראש הגוף המבוקר על הדיונים שקיים ועל ההחלטות

שקיבל במסגרתם בתוך 60 יום ממועד הנחת הדוח על שולחן הכנסת. סעיף 21ב לחוק קובע כי ראש הגוף המבוקר ידווח למבקר המדינה על ההחלטות שהתקבלו בתוך שלושים ימים מיום שהן דווחו לו, ובין השאר על הדרכים לתיקון הליקויים ועל המועד שנקבע לתיקונם, וכן עליו לדווח על הליקויים שהוחלט לדחות את תיקונם ולפרט את הנימוקים לכך. סעיף 21ג לחוק קובע כי אם עובד גוף מבוקר לא קיים את שהוטל עליו מכוח סעיף 21א או 21ב, בלא הצדקה סבירה, יהיה הדבר בגדר עבירת משמעת לפי הדין המשמעתי החל באותו גוף מבוקר.

משרד הפנים לא דן בליקויים בפעולות המינהל לשלטון מקומי שהועלו בביקורת הקודמת ובהמלצות משרד מבקר המדינה לתיקונם, כנדרש בחוק

הביקורת הנוכחית העלתה כי צוות תיקון הליקויים של משרד הפנים[14] לא דן בליקויים בפעולות המינהל לשלטון מקומי שהועלו בביקורת הקודמת ובהמלצות משרד מבקר המדינה לתיקונם. עוד העלתה הביקורת הנוכחית כי משרד הפנים לא פרסם קובץ הנחיות מחייב לרשויות המקומיות בנושא אבטחת מידע והגנת הפרטיות ואף לא פנה לרמו"ט בבקשה שתסייע לו בגיבוש קובץ הנחיות כאמור.

משרד מבקר המדינה מעיר למשרד הפנים כי היה עליו לקיים דיון סדור בממצאי הביקורת הקודמת כנדרש בחוק ולתעד את הנימוקים להחלטותיו בדבר תיקון הליקויים. על משרד הפנים להקפיד לפעול בהתאם להוראות חוק מבקר המדינה המחייבות דיון וקבלת החלטות בנושא תיקון ליקויים שהועלו בדוחות ביקורת המדינה - הוראות שאי-עמידה בהן בלא הצדקה סבירה עלולה להיות בגדר עבירת משמעת.

משרד מבקר המדינה מעיר למשרד הפנים על שלמרות חשיבות הנושא ולמרות פרק הזמן הארוך - כחמש שנים - שעבר מאז הסתיימה הביקורת הקודמת הוא לא פעל לפרסום קובץ הנחיות מחייב בנושא אבטחת מידע והגנת הפרטיות ברשויות המקומיות.

בתשובתו למשרד מבקר המדינה ממאי 2017 חזר משרד הפנים על הטענה שהעלה כבר בביקורת הקודמת ולא הייתה מקובלת על משרד מבקר המדינה, כי הוא אינו הגוף המקצועי המוסמך לקבוע נהלים בנושא אבטחת מידע ואין לו הידע והמומחיות הנדרשים לצורך כך ואף לא סמכות טיפול, וכי הנושא אמור להיות מוסדר באמצעות רמו"ט אשר בידיה הכלים המקצועיים לגיבוש הנחיות בנושא.

14 בראש הצוות לתיקון ליקויים עומד מנכ"ל משרד הפנים, והחברים בו הם היועץ המשפטי ומנהלת האגף לביקורת פנימית של המשרד.

משרד מבקר המדינה מעיר למשרד הפנים כי תשובתו אינה מתיישבת עם העיקרון שעליו מתבססת החלטת ממשלה 2443, ולפיו על משרדי ממשלה בעלי סמכויות רגולטוריות להגדיר את המדיניות ודרישות האסדרה עבור המגזר שבו הם פועלים. משרד מבקר המדינה שב ומעיר למשרד הפנים, כמו בביקורת הקודמת, כי עליו להוציא לרשויות המקומיות קובץ הנחיות מחייב בנושא אבטחת מידע והגנת הפרטיות ולוודא כי הוא מוטמע ומיושם. בהיעדר קובץ הנחיות מחייב כל רשות מקומית מתמודדת עם נושא אבטחת המידע והגנת הפרטיות כמיטב הבנתה ולפי התקציב שהקצתה לנושא, ובעקבות כך חלק מהרשויות המקומיות אינן מטפלות כראוי באבטחת המידע שלהן ובהגנה על הפרטיות של תושביהן (בנושא זה ראו בהמשך).

2. בשנים האחרונות קיבלה ממשלת ישראל כמה החלטות בתחום מרחב הסייבר[15] וההגנה עליו:

א. החלטה 3611 מאוגוסט 2011 בדבר הקמת מטה הסייבר הלאומי (להלן - מטה הסייבר), שבין תפקידיו לתת לראש הממשלה ולממשלה המלצות הנוגעות למדיניות הסייבר הלאומית ולהנחות את הגורמים הרלוונטיים בעניין המדיניות שהוחלט לאמץ וליישמה;

ב. החלטה 2443 מפברואר 2015 ובה נקבע כי המנכ"לים של משרדי הממשלה, שבמסגרתם מופעלות סמכויות רגולציה כלפי גופים או פעילויות החשופים לאיומי סייבר, יקדמו את הטיפול בהיערכות לאיומי סייבר במסגרת המגזר שבו הם פועלים, וזאת בין היתר על ידי הגדרת המדיניות ודרישות האסדרה ליישום החלטה זו במסגרת המגזר שהם אחראים לו.

ג. החלטה 2444 מפברואר 2015 בדבר הקמת הרשות הלאומית להגנת הסייבר (להלן - רשות הסייבר) שבין תפקידיה לנהל, להפעיל ולבצע את כלל פעילויות ההגנה האופרטיביות במרחב הסייבר במישור הלאומי; עוד הוחלט על הקמת מערך הסייבר הלאומי הכולל את מטה הסייבר ואת רשות הסייבר כשתי יחידות סמך עצמאיות למשרד ראש הממשלה (להלן - מערך הסייבר).

בביקורת הנוכחית הועלה כי בהתאם להחלטה 2443 מינתה מנכ"לית משרד הפנים (דאז) בשנת 2015 את מנהל המינהל לשירותי חירום במשרד הפנים (להלן - מינהל החירום) להקים גוף שינחה את הרשויות המקומיות כיצד להיערך לאיומי סייבר ויפקח על אופן היערכותן לכך.

15 בהחלטת ממשלה 3611 מ-7.8.11 הוגדר מרחב הסייבר כ"המתחם הפיזי והלא פיזי, שנוצר או מורכב מחלק או מכל הגורמים הבאים: מערכות ממוכנות ממוחשבות, רשתות מחשבים ותקשורת, תוכנות, מידע ממוחשב, תוכן שמועבר באופן ממוחשב, נתוני תעבורה ובקרה והמשתמשים של כל אלה".

הבדיקה העלתה כי הפעילות בתחום זה נמצאת רק בראשית דרכה. בנובמבר 2015 התקיימה במינהל החירום פגישה בנושא "הקמת אגף סייבר במשרד הפנים" בהשתתפות נציגי משרד הפנים ומטה הסייבר. בפגישה סוכם כי לצורך הקמת האגף יוקצו למשרד הפנים חמישה תקנים - שלושה תקנים לשנים 2015 ו-2016 ושניים נוספים לשנת 2017 - וכי התקנים לשנים 2015 ו-2016 ימומנו ממקורות מטה הסייבר. הבדיקה העלתה כי רשות הסייבר אישרה הקצאה של ארבעה עובדים לאיוש התקנים להקמת אגף הסייבר במשרד הפנים, וכי בתחילת שנת 2017 החל לעבוד העובד הראשון ושלושת העובדים האחרים טרם החלו בעבודתם. עוד הועלה כי רשות הסייבר הגדירה מתודולוגיה למיפוי מצב מוכנות הסייבר בכלל הארגונים, בהם גם הרשויות המקומיות, ועם השלמת המיפוי תוכן תכנית עבודה להשלמת החוסרים על פי סדרי עדיפויות שיקבעו.

משרד הפנים מסר בתשובתו כי הקמת אגף לסיוע לרשויות המקומיות בתחום הסייבר נמצאת בעיצומה, בין היתר משום שהגורמים המוסמכים לכך במשרד הפנים טרם השלימו את תהליכי אישור המועמדים, כי אין תקן למנהל האגף, וטרם הוסדרה סוגיית המשרדים שבהם ישכון הגוף שיוקם.

משרד מבקר המדינה מעיר למשרד הפנים כי נוכח הסיכונים ההולכים וגוברים אשר נשקפים למידע השמור במערכות המחשב של הרשויות המקומיות, ובייחוד מערכות המידע הנדרשות לפעול בזמן חירום, עליו לפעול בהקדם לאסדרת הנושא בשלטון המקומי ולקידום הוצאת הנחיות מחייבות לרשויות המקומיות בתחום זה - כפי שהוטל עליו בהחלטת הממשלה בהיותו מאסדר השלטון המקומי.

הרשות למשפט, טכנולוגיה ומידע במשרד המשפטים - רמו"ט

בספטמבר 2006 הוקמה במשרד המשפטים רמו"ט כרשות להגנת מידע אישי בישראל. במסגרת תפקידה זה כוללת רמו"ט שלוש יחידות רגולטוריות שפעלו קודם לכן, ובהן רשם מאגרי מידע - אשר אחראי לפי חוק הגנת הפרטיות לפיקוח על מילוי הוראות החוק והתקנות לפיו ולאכיפתן.

תחומי האחריות של רמו"ט חלים הן על המגזר הציבורי - ובכלל זה הרשויות המקומיות - והן על המגזר הפרטי, וכוללים, בין היתר, רישום מאגרי מידע; פיקוח על בעלי מאגרי מידע; טיפול בתלונות; חקירת עבירות פליליות; הטלת קנסות מינהליים; קביעת הנחיות שוק שיספקו לבעלי מאגרי מידע סטנדרט

פעולה מקובל; העלאת המודעות לזכות לשמירה על פרטיות המידע, הן בקרב בעלי מאגרי המידע והן בקרב נושאי המידע[16].

להלן יפורטו ממצאי הביקורת העיקריים בנושא פעילותם של משרד המשפטים ושל רמו"ט בנושא אבטחת המידע ברשויות המקומיות:

1. הביקורת הקודמת העלתה כי מאז הוקמה רמו"ט היא לא פיקחה על הרשויות המקומיות כדי לוודא שהן מקיימות את חובת הרישום של מאגרי המידע שברשותן, לא ביצעה פעולות אכיפה בנושא ולא הטילה קנסות על רשויות מקומיות שלא קיימו את חובתן זו. משרד מבקר המדינה העיר לרמו"ט בביקורת הקודמת כי ראוי שתגבש תכנית למימוש אחריותה בתחום אבטחת המידע והגנת הפרטיות ברשויות המקומיות.

   הביקורת הנוכחית העלתה כי צוות תיקון הליקויים של משרד המשפטים לא דן בליקויים בפעולות רמו"ט שהועלו בביקורת הקודמת ובהמלצות משרד מבקר המדינה לתיקונם.

   משרד המשפטים מסר בתשובתו למשרד מבקר המדינה ממאי 2017 כי מבדיקה שעשה עלה כי במקרה הנדון, באופן חריג, הצוות לתיקון ליקויים אכן לא קיים דיונים בנושא.

   > משרד מבקר המדינה מעיר למשרד המשפטים כי עליו להקפיד לפעול בהתאם להוראות חוק מבקר המדינה המחייבות דיון וקבלת החלטות בנושא תיקון ליקויים שהועלו בדוחות ביקורת המדינה - הוראות שאי-עמידה בהן עלולה להיות בגדר עבירת משמעת.

2. בביקורת הנוכחית נמצא כי רמו"ט עדיין לא גיבשה תכנית למימוש אחריותה בתחום אבטחת המידע והגנת הפרטיות ברשויות המקומיות.

   > משרד מבקר המדינה מעיר לרמו"ט כי על אף הנחיצות שבהסדרת הנושא ברשויות המקומיות ועל אף פרק הזמן הארוך - כחמש שנים - שעבר מאז סיומה של הביקורת הקודמת, היא לא פעלה לגיבוש תכנית למימוש אחריותה לפיקוח ולאכיפה בתחום אבטחת המידע והגנת הפרטיות ברשויות המקומיות.

   רמו"ט מסרה בתשובתה למשרד מבקר המדינה ממאי 2017 (להלן - תשובת רמו"ט) כי היא משקיעה את משאביה בעיקר באסדרת נושאים שהם בעלי השפעה רוחבית על כלל מפוקחיה, ואינה מתמקדת במגזר מסוים. זאת בייחוד כאשר פועל רגולטור מגזרי משיק - משרד הפנים -

16 מתוך אתר רמו"ט בכתובת: http://www.justice.gov.il/Units/ilita/Odot/Pages/Odot.aspx

המסדיר את פעילות הרשויות המקומיות, מפקח עליהן ונמצא בקשר יום-יומי עמן. בתשובה נוספת מיוני 2017 מסרה רמו"ט למשרד מבקר המדינה כי כוח האדם העומד לרשותה מצומצם, והדבר מקשה עליה לבצע פעולות פיקוח יזומות. רמו"ט הוסיפה בתשובתה כי בשנת 2016 החלה תהליך של שינוי אסטרטגי משמעותי ורחב היקף, הבא לידי ביטוי הן בשינוי המבנה הארגוני שלה, והן בשינוי הנושאים שבמוקד פעילותה, וכי היא מתעתדת כבר בשנת 2017 להפעיל מערך פיקוח חדש, תוך הסתייעות של ממש בשירותיהם של ספקים חיצוניים. עובדי מחלקת האכיפה של רמו"ט ינהלו ויכוונו פעילות זו וכן יבצעו בקרה עליה.

המרכז הלאומי להתמודדות עם איומי סייבר מספק התרעות שוטפות על נוזקות חדשות ומדווח על תקיפות סייבר כנגד אתרים וארגונים בישראל רק ל-20 (כ-8%) מכלל הרשויות המקומיות בישראל

המרכז הלאומי להתמודדות עם איומי סייבר

בהחלטת ממשלה 2444 מפברואר 2015 נקבע כי אחד מתפקידיה של רשות הסייבר הוא להפעיל מרכז לסיוע בהתמודדות עם איומי סייבר עבור כלל המשק, ובכלל זה לסייע בטיפול באיומי סייבר ואירועי סייבר וכן לרכז ולשתף מידע רלוונטי עם כלל הגורמים במשק.

בהתאם לכך הוקם ברשות הלאומית להגנת הסייבר המרכז הלאומי להתמודדות עם איומי סייבר[17]. המרכז, שהחל לפעול בשנת 2016, נועד לשרת את כלל הארגונים במדינת ישראל. יכולת הפעולה האפקטיבית שלו מתבססת על שיתוף המידע שהוא מקיים עם גורמים רבים מקהל היעד ועם שותפים נוספים שעמם הוא מקיים קשר לגבי איומי סייבר. זהו קשר הדדי המתבצע באופן אמין, דיסקרטי ומקצועי, על מנת לאפשר שיתוף מידע רלוונטי בסביבה בטוחה, אשר יסייע בהגברת החוסן של המשק הישראלי בתחום הסייבר. המרכז הלאומי מציע אוסף נרחב של שירותים לגופים השונים של קהל היעד, ללא תמורה ובהתאם לחומרת האיום או האירוע[18]. שירותים אלו כוללים, בין היתר, התראות ואזהרות, סיוע בטיפול באירועים ומחקר טכנולוגי לזיהוי ולניתוח של נוזקות (malware)[19], הסברה בתחום הסייבר, הדרכה ותרגול.

בביקורת הנוכחית נמצא כי המרכז הלאומי להתמודדות עם איומי סייבר נותן שירות רק ל-20 (כ-8%) מכלל הרשויות המקומיות בישראל. מדובר ברשויות שפנו אליו ונרשמו לקבלת שירותיו, והן מקבלות ממנו באופן שוטף התרעות על

17 מרכזים אלו מוכרים בעולם בכינוי National CSIRTs - Computer Security Incident Response Team, ולחלופין CERTs – Cyber Event Readiness Teams.

18 מתוך אתר המרכז הלאומי להתמודדות עם איומי סייבר בכתובת:
https://cert.gov.il/About2/Pages/Service-Portfolio.aspx

19 תוכנה שמטרתה לחדור למחשב או להזיק לו ללא ידיעתו של המשתמש בו. הגדרה זו חלה על וירוסים, תולעי מחשבים, רוגלות (תוכנות ריגול), סוסים טרויאניים, תוכנות פרסום ועוד.

נוזקות חדשות וכן דוחות על תקיפות סייבר כנגד אתרים וארגונים בישראל. עוד נמצא כי המרכז לא פנה ביוזמתו ובאופן מסודר לכל הרשויות המקומיות בהצעה למתן השירותים האמורים, וכי גם משרד הפנים, כמאסדר השלטון המקומי, לא פעל למיסוד הקשר ושיתוף הפעולה בין הרשויות המקומיות ובין המרכז ולהעלאת המודעות לשירותים שהוא מספק בקרב הרשויות המקומיות.

מערך הסייבר הלאומי מסר בתשובתו למשרד מבקר המדינה ממאי 2017 כי הוא סבור שחשוב מאוד להגביר את החוסן של הרשויות המקומיות הן בפני דליפת מידע והן לצורכי הגנה על רציפות תפקודית לטובת שירות חיוני לאזרח, וכי במהלך השנה תחל רשות הסייבר בביצוע פעולות הסברה על מנת להרחיב את רשימת מקבלי שירותיו.

עדיין אין בידי הרשויות המקומיות קובץ נהלים שינחה אותן כיצד לפעול לאבטחת המידע שבידן ולהגנה על פרטיות תושביהן

על מנת לשפר את רמת אבטחת המידע ברשויות המקומיות, על משרד הפנים, בשיתוף מרכז השלטון המקומי בישראל ומערך הסייבר הלאומי, להביא בהקדם לידיעת כלל הרשויות המקומיות - עוד לפני שתושלם הקמת אגף הסייבר במשרד הפנים - את דבר קיומם של השירותים שנותן המרכז הלאומי להתמודדות עם איומי סייבר ולצרפן לשירותים אלו. הדבר יסייע לרשויות המקומיות לשפר את היערכותן להתמודדות עם איומי סייבר בעתות שגרה וחירום ואת אבטחת המידע שהן מחזיקות.

☆

במועד סיום הביקורת הנוכחית, כחמש שנים לאחר פרסומה של הביקורת הקודמת, המינהל לשלטון מקומי במשרד הפנים ורמו"ט שבמשרד המשפטים עדיין לא תיקנו את הליקויים שהועלו בה. בין היתר, לא נקבעו נהלים והנחיות בנוגע לפעולתן של הרשויות המקומיות בתחום אבטחת מידע והגנת הפרטיות, לא נקבעו סדרי הטיפול ופעולות הפיקוח ולא ננקטו פעולות של ממש לקידום פעולתן של הרשויות המקומיות בתחום זה. משרד הפנים אף לא פעל להעלאת המודעות לשירותים אשר המרכז הלאומי להתמודדות עם איומי סייבר יכול לספק לרשויות המקומיות כדי לסייע להן להתמודד עם איומי סייבר.

ממצאי הביקורת הנוכחית מעידים כי פעילות הרשויות המקומיות בתחום אבטחת מידע והגנת הפרטיות עדיין אינה מאוסדרת על ידי השלטון המרכזי. המינהל לשלטון מקומי במשרד הפנים ורמו"ט שבמשרד המשפטים ממשיכים להטיל זה על זה את האחריות להסדרת הנושא, ובעקבות כך עדיין אין בידי הרשויות קובץ נהלים מחייב בתחום זה, שינחה אותן כיצד לפעול לאבטחת המידע שבידן ולהגן על פרטיות תושביהן, וכל רשות מקומית פועלת לפי מיטב הבנתה ויכולתה.

על מנכ"ל משרד הפנים ומנכ"לית משרד המשפטים לגבש מתכונת ברורה של חלוקת תחומי האחריות והסמכויות בין משרדיהם בכל הנוגע לאבטחת המידע והגנת הפרטיות ברשויות המקומיות, ולפעול למימושה של מתכונת זו.

אבטחת המידע הממוחשב ברשויות המקומיות

רישום מאגרי מידע, פיקוח ואכיפה

חוק הגנת הפרטיות קובע שכל בעל מאגר מידע המקיים את אחד מתנאי החוק - ובהם רשות מקומית - חייב לרושמו אצל רשם מאגרי המידע ברמו"ט. כמו כן נקבע בחוק כי שר המשפטים רשאי לקבוע חובת תשלום אגרה תקופתית בגין מאגר מידע הרשום בפנקס, וכי עקב אי-תשלום אגרה הרשם רשאי להתלות את תוקפו של רישום המאגר או לבטל את רישומו של המאגר, ובלבד שקודם להתליה או לביטול ניתנה לבעל המאגר הזדמנות להשמיע את טענותיו בנושא. בתקנות הגנת הפרטיות (אגרות), התשס"א-2000 (להלן - תקנות הגנת הפרטיות - אגרות), נקבעו סכומי האגרות וכן עיצומים בגין אי-תשלום האגרות במועד.

ברשויות המקומיות יש מאגרי מידע רבים החייבים רישום, בין השאר מאגרי מידע בתחומי משאבי אנוש, רווחה, חינוך, רישוי עסקים, ארנונה וגבייה. להלן יפורטו ממצאי הביקורת העיקריים בנושא רישום מאגרי המידע ברשויות המקומיות שנבדקו:

1. **עיריות יהוד-מונוסון ויקנעם עילית:** הביקורת הקודמת העלתה, בין היתר, כי עיריות יהוד-מונוסון ויקנעם עילית לא שילמו אגרות תקופתיות במשך יותר משלוש שנים, ועקב כך נמחק רישום מאגריהן. מבקר המדינה העיר בביקורת הקודמת לעיריות האמורות כי עליהן להקפיד לרשום ולנהל את כל מאגרי המידע שברשותן כנדרש בחוק.

> משרד מבקר המדינה מציין לחיוב כי עיריית יהוד-מונוסון תיקנה את הליקוי. העירייה רשמה בדצמבר 2012 את ששת מאגרי המידע שברשותה אצל רשם מאגרי המידע.

עוד נמצא בביקורת הנוכחית כי עיריית יקנעם עילית עדיין לא רשמה את כל מאגרי המידע שברשותה אצל רשם מאגרי המידע ברמו"ט. מבדיקה ברמו"ט הועלה כי רק אחד מחמשת מאגרי המידע שבבעלות העירייה רשום אצלה, אך האגרות התקופתיות בגין המאגר האמור לא שולמו ולפיכך רישומו הותלה. יצוין כי בעיריית יקנעם עילית לא התקבלה הודעה מרשם מאגרי המידע בדבר התליית רישום המאגר, וזאת שלא כנדרש בתקנות הגנת הפרטיות - אגרות.

> ברשויות המקומיות יש מאגרי מידע רבים, בין השאר בתחומי משאבי אנוש, רווחה, חינוך, רישוי עסקים, ארנונה וגבייה, שלא נרשמו אצל רשם מאגרי המידע

עיריית יקנעם עילית מסרה בתשובתה למשרד מבקר המדינה ממאי 2017 כי היא תשלים בתקופה הקרובה את תהליך רישום מאגרי המידע שלה אצל רשם מאגרי המידע.

משרד מבקר המדינה מעיר לעיריית יקנעם עילית על שבמועד סיום הביקורת - זמן רב לאחר הביקורת הקודמת - היא עדיין לא רשמה אצל רשם מאגרי המידע את כל מאגרי המידע שברשותה כנדרש ממנה בחוק, ועליה לעשות כן לאלתר.

רמו"ט מסרה בתשובתה כי מערכת רישום המאגרים שלה שולחת באופן אוטומטי הודעות בנוגע להתליית מאגרי מידע בעקבות חוב, וכי אינה שומרת העתקים מההודעות שנשלחו.

משרד מבקר המדינה מעיר לרמו"ט כי עליה למסור לבעל מאגר מידע הודעה בדבר התליית רישומו בהתאם לתקנות הגנת הפרטיות - אגרות, וכי עליה לשמור אסמכתאות המתעדות פעולות אלו.

עיריות נצרת עילית וכרמיאל והמועצה המקומית תל מונד: נמצא כי למועד סיום הביקורת הנוכחית עסקה עיריית נצרת עילית בהסדרת רישומם של 23 מאגרי המידע שלה. לדברי העירייה יש צורך במחיקת כמה מאגרי מידע ישנים וברישום כמה מאגרי מידע חדשים. הועלה כי ברמו"ט רשומים רק עשרה מאגרי מידע של עיריית נצרת עילית, וכי עשרה מאגרי המידע של עיריית כרמיאל וחמישה מאגרי המידע של המועצה המקומית תל מונד לא נרשמו כלל אצל רשם מאגרי המידע.

משרד מבקר המדינה מעיר לעיריות כרמיאל ונצרת עילית ולמועצה המקומית תל מונד כי עליהן להסדיר לאלתר את רישום מאגרי המידע שלהן אצל רשם מאגרי המידע, כנדרש בחוק.

עיריות כרמיאל ונצרת עילית והמועצה המקומית תל מונד מסרו בתשובותיהן למשרד מבקר המדינה ממאי 2017 כי הן החלו בהסדרת רישום מאגרי המידע שלהן אצל רשם מאגרי המידע.

2. לשלטון המקומי במרחב הכפרי שני רבדים. הרובד העליון - מועצה שנבחרה או מונתה לניהול ענייניה של מועצה אזורית[20] שבתחום שיפוטה כמה יישובים; הרובד התחתון - ועדים מקומיים שנבחרו או התמנו ביישובי

20 על פי צו המועצות המקומיות (מועצות אזוריות), התשי"ח-1958, מועצה אזורית היא "כל אחת מן המועצות המקומיות אשר שמה נקוב בתוספת הראשונה".

המועצה. בישראל 54 מועצות אזוריות, בתחום שיפוטן כ-970 יישובים, ובכל אחד מהם מכהן ועד מקומי.

בדוח מבקר המדינה בנושא פעילותם של ועדים מקומיים במועצות אזוריות[21] הועלה כי כ-61% מהם הטילו ארנונה כללית לצורך מימוש הסמכויות שהמועצה אצלה להם (להלן - ארנונת ועד מקומי). לצורך גביית הארנונה על הוועד המקומי להחזיק ולנהל מאגר מידע. בהיות הוועד המקומי גוף ציבורי, חלה עליו החובה לרשום את המאגר אצל רשם מאגרי המידע. נמצא כי אצל רשם מאגרי המידע רשומים מאגרי מידע של 68 (כ-7%) מהוועדים המקומיים בלבד.

המועצה האזורית הגליל התחתון: בביקורת הנוכחית הועלה כי 14 מהוועדים המקומיים בתחום שיפוטה של המועצה האזורית הגליל התחתון (להלן - המועצה האזורית) הטילו על המחזיקים בנכסים שבתחום שיפוטם ארנונת ועד מקומי. עלה כי המועצה האזורית מנהלת את החיוב והגבייה של ארנונת הוועד המקומי עבור שמונה מהם, ואילו ששת היישובים האחרים[22] מחייבים וגובים בעצמם את ארנונת הוועד המקומי.

נמצא כי מאגרי המידע של ששת הוועדים המקומיים האמורים לא רשומים אצל רשם מאגרי המידע ברמו"ט.

משרד מבקר המדינה מעיר למועצה האזורית הגליל התחתון כי משאישרה לוועדים מקומיים בתחום שיפוטה להטיל ולגבות ארנונת ועד מקומי, ראוי היה כי תביא לידיעתם שמחובתם לבצע רישום של מאגרי המידע שלהם בהתאם לחוק הגנת הפרטיות.

המועצה האזורית הגליל התחתון מסרה בתשובתה למשרד מבקר המדינה מאפריל 2017 כי העבירה לוועדים המקומיים את הערת המבקר כי עליהם לפעול לרישום מאגרי המידע שברשותם.

הוועדים המקומיים הזורעים ומצפה נטופה מסרו בתשובותיהם למשרד מבקר המדינה מאפריל וממאי 2017, בהתאמה, כי המועצה האזורית הגליל התחתון פועלת לעדכון נוהלי אבטחת המידע לכל גורמי המועצה ובכללם לוועדים המקומיים, וכי עם קבלת הנהלים החדשים הם יפעלו לביצועם.

21 מבקר המדינה, **דוחות על הביקורת בשלטון המקומי לשנת 2009** (2010), "התנהלות ועדים מקומיים במועצות אזוריות", עמ' 291-343.

22 בית קשת, בית רימון, גבעת אבני, הזורעים, מצפה נטופה ושרונה.

משרד מבקר המדינה מעיר לוועדים המקומיים של היישובים בית קשת, בית רימון, גבעת אבני, הזורעים, מצפה נטופה ושרונה כי עליהם לרשום את מאגרי המידע שלהם אצל רשם מאגרי המידע, כנדרש בחוק.

3. חוק הגנת הפרטיות קובע כי רשם מאגרי המידע יפקח על אופן המילוי של הוראות החוק והתקנות שנקבעו לפיו. עוד נקבע בחוק כי הרשם יעמוד בראש יחידת פיקוח והוא ימנה מפקחים לצורך ביצוע הפיקוח, וכי הם רשאים לדרוש מכל אדם הנוגע בדבר למסור ידיעות ומסמכים הנוגעים למאגר מידע, והוקנו להם סמכויות פעולה לשם הבטחת ביצוע החוק ולמניעת עבירה על הוראותיו.

בדוח לשנת 2015[23] שפרסם רשם מאגרי המידע נאמר כי משימתו המרכזית היא לפקח על מילוי הוראות חוק הגנת הפרטיות, לנהל את פנקס מאגרי המידע ולהעמידו לעיון הציבור. בדוח הודגש כי באמצעות ההליך הפורמלי של רישום מאגרי המידע משיגה רמו"ט יעדים נוספים ובהם: הטמעת הליך ניהול תקין של מידע על ידי בעל המאגר; הנעת בעלי מאגרים לציית לחוק ולחדול מפעילות המנוגדת לו; והגברת המודעות של גופים שונים לחשיבות הגנת המידע האישי במאגרי מידע.

הביקורת הקודמת העלתה כי רמו"ט לא קיימה פעולות לפיקוח על רישום מאגרי המידע של הרשויות המקומיות ולאכיפה בנושא ולא הטילה קנסות על רשויות מקומיות שלא קיימו את חובתן זו.

הביקורת הנוכחית העלתה כי הליקוי עדיין לא תוקן. נמצא כי בקובץ מאגרי המידע הרשומים בבעלות רשויות מקומיות שהעבירה רמו"ט לצוות הביקורת רשומים מאגרי מידע[24] של 153 (כ-60% בלבד) מכלל הרשויות המקומיות.

עוד עלה כי אף שברור כי לצורך פעילותן השוטפת משתמשות כל 257 הרשויות המקומיות במאגרי מידע, רמו"ט לא פעלה להסדרת רישום מאגרי המידע של כל הרשויות המקומיות, לא ריכזה את נתוני הרשויות המקומיות שלא רשמו אצלה מאגרי מידע, לא התריעה לפניהן על אי-קיום הוראות החוק ולא ביצעה בהן פעולות פיקוח.

רמו"ט מסרה בתשובתה כי חובת הרישום על פי חוק הגנת הפרטיות חלה על בעל המאגר. כבעלות מאגרים הרשויות המקומיות אחראיות לרשום את מאגרי המידע שלהן ולקיים את הוראות החוק. רמו"ט הוסיפה בתשובתה כי

23 משרד המשפטים, הרשות למשפט, טכנולוגיה ומידע, רשם מאגרי המידע, **דוח לשנת 2015** (פורסם בשנת 2016).

24 לדצמבר 2016 רשומים בקובץ 1,274 מאגרי מידע של רשויות מקומיות.

אין בידיה משאבים שיאפשרו לה לוודא כי בוצע רישום של כלל מאגרי המידע בישראל וכל שכן לאכוף את חובת הרישום של מאגרים אלה.

משרד מבקר המדינה מעיר לרמו"ט, האחראית לפיקוח על מילוי הוראות חוק הגנת הפרטיות, כי עליה ליזום - אם בעצמה ואם באמצעות משרד הפנים, מאסדר השלטון המקומי - פנייה לרשויות המקומיות, ובכלל זה לוועדים המקומיים במועצות האזוריות, לרישום מאגרי המידע ולתשלום האגרות, כקבוע בחוק ובתקנות.

פעולות לאבטחת המידע הממוחשב

נהלים והנחיות לאבטחת מידע

לצורך יישומו של חוק הגנת הפרטיות ולשם אסדרת הטיפול בנושא אבטחת מידע והגנת הפרטיות ברשויות המקומיות, יש מקום לקבוע נוהלי עבודה בתחום אבטחת המידע. על נהלים אלה להסדיר את הפעולות שיש לנקוט מול המערכות השונות של הרשויות המקומיות ולקבוע את שיטות העבודה המיטביות לאבטחת המידע.

בהיעדר נהלים מפורטים המנחים את הרשויות המקומיות בנושאים הנוגעים לאבטחת מידע ולהגנת הפרטיות, מחשיב משרד מבקר המדינה את התקנים הישראליים ואת נוהלי המסגרת שנועדו להנחות את משרדי הממשלה - המפורטים להלן - לאמות מידה להערכת נקודות התורפה ברשויות המקומיות שנבדקו, שכן תקנים ונהלים אלו יש בהם כדי ללמד על המצב הרצוי גם ברשויות המקומיות.

מכון התקנים הישראלי פרסם כמה תקנים (לא רשמיים[25]) בעניין אבטחת מידע, ובכללם: תקן 1495 בנושא אבטחת מערכות מידע; תקן ישראלי 1243 בנושא בטיחות אש של מחשבים וציוד היקפי; תקן 1972 בנושא אבטחת מידע בתקשורת בין מחשבים; תקן 17799 בנושא ניהול אבטחת מידע; ותקן 27001, שנועד לשמש מודל להקמה, להפעלה, לניטור, לסקירה, לתחזוקה ולשיפור של מערכת לניהול אבטחת מידע. מכלול התקנים האלה משמש נורמה מקיפה לאבטחת מידע בארגונים (להלן - התקנים הישראליים).

25 תקן לא רשמי הוא תקן שאינו מחייב ויישומו וולונטרי.

האגף הבכיר לביקורת המדינה במשרד ראש הממשלה פרסם בספטמבר 2005 נוהלי מסגרת לאבטחת מידע[26] (להלן - נוהלי המסגרת). מדובר ב-38 נהלים לאבטחת מידע במשרדי הממשלה העוסקים בין היתר בנושאים אלה: קביעת מדיניות ומיפוי מידע; הגורם האנושי ואבטחת המידע; אבטחה לוגית; אבטחה פיזית; גיבוי, שחזור והתאוששות; אבטחת תקשורת ושימושי אינטרנט; אבטחת מידע במחשבים המנותקים מרשתות המשרד. נוהלי המסגרת לא נקבעו לנוהל מחייב במשרדי הממשלה, אך ניתן ללמוד מהם על התשתית הנדרשת לאבטחת המידע ולהגנת הפרטיות בגופים ציבוריים.

מינוי ממונה על אבטחת מידע

חוק הגנת הפרטיות קובע כי גוף ציבורי, ובכלל זה רשות מקומית, חייב למנות אדם בעל הכשרה מתאימה לממונה על אבטחת מידע (להלן - ממונה אבטחת מידע).

בקובץ תיאורי תפקיד שפרסם משרד הפנים[27] (להלן - קובץ תיאורי התפקיד או הקובץ), נכלל תיאור תפקידו של מנהל אבטחת מידע ברשות המקומית. על פי הקובץ מנהל אבטחת מידע ברשות המקומית אחראי לאלה: תכנון מדיניות אבטחת המידע ובקרה על יישומה; תכנון וביצוע של סקרי אבטחת מידע; ניהול ההרשאות ודרכי הגישה למשתמשים; תכנון ויישום של תכנית התאוששות מאסון[28]; וניהול ההגנה על מערכות המידע והתקשורת.

להלן יפורטו ממצאי הביקורת הנוגעים למינוי ממוני אבטחת מידע ברשויות מקומיות:

1. החוק להסדרת הביטחון בגופים ציבוריים, התשנ"ח-1998 (להלן - החוק להסדרת הביטחון), הגם שאינו חל על רשויות מקומיות, מטיל על גופים ציבוריים המנויים בתוספת לחוק את החובה למנות ממונה ביטחון, שיופקד על "פעולות אבטחה פיזית", לרבות שמירה על רכוש; על "פעולות לאבטחת מערכות ממוחשבות חיוניות"; ועל "פעולות לאבטחת מידע" לשם שמירה על מידע מסווג ומניעת פגיעה בו.

26 משרד ראש הממשלה, אגף בכיר לביקורת המדינה והביקורת הפנימית, המועצה המייעצת לביקורת ואבטחת מידע, **נוהלי מסגרת לאבטחת מידע**, מהדורה שלישית (ספטמבר 2005).

27 משרד הפנים, מינהל השלטון המקומי, האגף לכוח אדם ושכר ברשויות המקומיות, **קובץ ניתוח העיסוקים ותיאורי התפקידים ברשויות המקומיות**, (ספטמבר 2011).

28 תכנית התאוששות מאסון (Disaster Recovery Plan) עוסקת בתהליכים, במדיניות ובנהלים המשמשים להתאוששות מאסון המשבית לזמן לא קצר את התשתית הטכנולוגית החיונית לפעילותו של ארגון. בתכנית ההתאוששות מאסון יש לכלול תכנון לחידוש של יישומים, נתונים, חומרה, תקשורת (כגון רשת) ואלמנטים אחרים של טכנולוגיית המידע.

משרד מבקר המדינה העיר בביקורת הקודמת למשרד הפנים כי עליו לבחון אם יש מקום להנהיג גם ברשויות המקומיות את ההסדר שנקבע לגבי הגופים הציבוריים המנויים בחוק להסדרת הביטחון, ולפיו ממוני הביטחון מופקדים על פעולות לאבטחת מידע ומערכות מידע.

הביקורת הנוכחית העלתה כי משרד הפנים לא בחן את הנושא.

משרד מבקר המדינה שב ומעיר למשרד הפנים כי עליו לבחון אם יש להחיל על הרשויות המקומיות את הוראות החוק להסדרת הביטחון בדבר מינוי ממונה ביטחון ותפקידיו.

2. נמצא כי בנוהל "קביעת מדיניות אבטחת 'מידע רגיש' ומערכי מידע בממשלה ומוסדותיה", הנכלל בנוהלי המסגרת נקבע, כי ממונה אבטחת המידע משמש במשרדו כגורם מנחה מקצועי-אבטחתי, הפועל על פי מדיניות משרדו ונוהלי המסגרת. בין תפקידיו: פיתוח נוהלי אבטחה פנימיים לשם אסדרת פעילויות אבטחת המידע במשרד. עוד נקבע בנוהל כי הממונה לא יהיה "כפוף מינהלית (או בדרך אחרת) למנהל מערכות המידע **בשל ניגוד עניינים בין שני התפקידים"** (ההדגשה במקור).

> בקובץ תיאורי התפקיד שפרסם משרד הפנים נקבע כי מנהל אבטחת המידע יהיה כפוף למנהל מערכות המידע הראשי של הרשות המקומית, זאת שלא בהתאם לנוהלי המסגרת, הקובעים כי יש ניגוד עניינים בין שני התפקידים

הבדיקה העלתה כי בקובץ תיאורי התפקיד שפרסם משרד הפנים נקבע, שלא בהתאם להנחיות נוהלי המסגרת, כי מנהל אבטחת המידע יהיה כפוף למנהל מערכות המידע הראשי של הרשות המקומית (להלן - מנמ"ר) בלי שנמצא נימוק לכך.

משרד מבקר המדינה מעיר למשרד הפנים כי עליו לבחון את הגדרת הכפיפות של מנהל אבטחת מידע ברשות המקומית בהיבט של ניגוד עניינים בין שני התפקידים ולהתאימה להמלצות שנקבעו בנוהלי המסגרת שפרסם משרד ראש הממשלה.

משרד הפנים מסר בתשובתו כי אגף בכיר לניהול ההון האנושי ברשויות המקומיות יבחן מול הגורמים הרלוונטיים אם נכון לבצע תיקון בתיאור התפקיד ובכפיפותו.

3. הביקורת הקודמת העלתה כי עיריות יהוד-מונוסון ויקנעם עילית לא מינו ממונה אבטחת מידע. משרד מבקר המדינה העיר להן כי עליהן לעשות כן כמתחייב מחוק הגנת הפרטיות.

בביקורת הנוכחית נמצא כי הליקוי תוקן, ועיריות יהוד-מונוסון ויקנעם עילית מינו ממונים על אבטחת מידע כנדרש. עוד נמצא כי כל הרשויות המקומיות הנוספות שנבדקו - עיריות באר שבע, כרמיאל ונצרת עילית, המועצה המקומית תל מונד והמועצה האזורית הגליל התחתון - מינו ממונים על אבטחת מידע.

נהלים לאבטחה לוגית

מטרתה העיקרית של האבטחה הלוגית היא לאפשר גישה מבוקרת למערכות המידע וכן לאפשר בקרה על פעילות המשתמשים. במסגרת האבטחה הלוגית נכללים שימוש בשם משתמש ובסמה ומידור על ידי מתן הרשאות. בספטמבר 2014 פרסם מכון התקנים הישראלי את פרק 3 בתקן הישראלי ת"י 1495 הנקרא "טכנולוגיית המידע - טכניקות אבטחה: מסגרת להבטחת אימות ישות"[29]. פרק זה מאמץ כלשונו את התקן הבין-לאומי ISO/IEC 29115 מאפריל 2013 וקובע, בין השאר, את הדרישות לסמה שיש להזין בעת התחברות למערכת בהתאם לרמת האבטחה הנדרשת. אורכה המינימלי של הסמה הנדרשת הוא ארבעה תווים.

בנוהלי המסגרת, שכאמור לא הוחלו על הרשויות המקומיות, נקבעו הנחיות ברורות בנושא אבטחה לוגית. בין היתר נקבע כי הממונה על אבטחת מידע נדרש לקבוע את הדרישות לניהול מערכת הסמאות, לפרסם דרישות אלה בקרב כלל המשתמשים, לפקח על אופן יישומן ולאכוף עליהם את חובת היישום. יש לקבוע לכל משתמש שם משתמש וסמה אישית של שישה תווים לכל הפחות - ובהם אותיות, ספרות וסימנים - ולעדכנה מדי שלושה חודשים, ואין לשתף בסמאות. עוד נקבע בנוהלי המסגרת כי לכל אחד מהמשתמשים ייקבעו - עבור כל יישום - הרשאות ביצוע: עדכון, אחזור, תוספת או מחיקה. אם עובד עוזב את תפקידו, מכל סיבה, מנהל היישום יקבל דיווח על כך ויבטל את הרשאותיו.

על פי קובץ תיאורי התפקיד שפרסם משרד הפנים, מנהל אבטחת מידע ברשות המקומית אחראי, בין היתר, להגדרה ולאשרור של מדיניות אבטחת המידע ברשות, בשיתוף המנמ"ר והנהלת הרשות המקומית. להלן יפורטו ממצאי הביקורת בנוגע לאבטחה לוגית ברשויות שנבדקו:

1. **עיריות יקנעם עילית ויהוד-מונוסון:** בביקורת הקודמת נמצא כי שתי העיריות לא קבעו כללים מחייבים לאבטחה לוגית של המידע.

29 תקן זה החליף את התקן הישראלי ת"י 1495 חלק 3 מיוני 2008.

משרד מבקר המדינה מציין לחיוב כי בביקורת הנוכחית נמצא שעיריית יקנעם עילית תיקנה את הליקוי.

עוד נמצא בביקורת הנוכחית כי בעיריית יהוד-מונוסון מנהל אבטחת המידע הכין, רק באוקטובר 2016, טיוטת "מדיניות אבטחת מידע ונהלים" הכוללת, בין היתר, הנחיות וכללים לאבטחה לוגית של המידע. למועד סיום הביקורת העירייה עדיין לא אימצה אותם.

עיריית יהוד-מונוסון מסרה בתשובתה כי הנהלת הרשות תבחן בשנה הקרובה את אימוץ מדיניות אבטחת המידע.

משרד מבקר המדינה מעיר לעיריית יהוד-מונוסון כי עליה לקדם את פעולותיה לאישור נהלים, הנחיות וכללים מחייבים לאבטחת מידע. ביצוע פעולות אלו ישפר את האבטחה הלוגית של מערכות המחשב שלה.

2. **עיריות כרמיאל ונצרת עילית והמועצה המקומית תל מונד:** בביקורת הנוכחית נמצא כי שלוש הרשויות המקומיות האמורות לא קבעו נהלים, הנחיות וכללים מחייבים לאבטחה לוגית של מידע.

משרד מבקר המדינה מעיר לעיריות כרמיאל ונצרת עילית ולמועצה המקומית תל מונד כי עליהן להגדיר מדיניות אבטחת מידע ברשות המקומית, ובכלל זה מדיניות אבטחה לוגית, לעגנה במסמך כתוב ולאשררה כנדרש.

עיריית כרמיאל מסרה בתשובתה כי מנהל אבטחת המידע שלה החל בכתיבת נהלים והנחיות לאבטחת מידע, וכי בימים הקרובים יופצו הנהלים החדשים בקרב כל עובדי הרשות; עיריית נצרת עילית מסרה בתשובתה כי היא החלה בהכנה, בכתיבה וביישום של נוהלי עבודה ומדיניות בנושא אבטחת מידע; המועצה המקומית תל מונד מסרה בתשובתה כי במהלך שדרוג מערך המחשוב שלה, שבוצע לאחרונה, נוצרה מדיניות הרשאות סדורה, הן בנוגע לגישה למחשבים והן בנוגע לגישה למאגרי המידע.

3. נמצא כי כל הרשויות המקומיות שנבדקו אינן מנהלות רישום מעודכן לכל אחד מעובדיהן ובו ריכוז של כל הרשאות הגישה למאגרי המידע שניתנו לאותו עובד. רישום כזה נועד להבטיח כי אם עובד עוזב את תפקידו יבוטלו כל ההרשאות שניתנו לו.

עיריית באר שבע מסרה בתשובתה למשרד מבקר המדינה ממאי 2017 כי לכל גורם המחזיק באחד ממאגרי המידע שלה רישום עדכני של העובדים להם ניתנו הרשאות גישה למאגר. העירייה הדגישה בתשובתה כי נוהלי

> הרשויות המקומיות שנבדקו אינן מנהלות רישום מעודכן לגבי כל אחד מעובדיהן, הכולל את כל הרשאות הגישה למאגרי המידע שניתנו לאותו עובד

המסגרת אינם חלים על הרשויות המקומיות; עיריית יקנעם עילית מסרה בתשובתה כי בהתאם להמלצת מבקר המדינה מנהל אבטחת המידע שלה ינהל ויעדכן באופן שוטף רישום של הרשאות הגישה למאגרי המידע שלה שנתנו לעובדיה; עיריית כרמיאל מסרה בתשובתה כי תמפה את כל ההרשאות שיש לכל עובד, ולאחר השלמת המיפוי ייבדקו ההרשאות מחדש, ואם יימצאו אי-התאמות, הן יתוקנו לאלתר; עיריית נצרת עילית מסרה בתשובתה כי במאגרים שמתפעלים ספקים חיצוניים ניהול ההרשאות מעודכן באופן שוטף, וכי במאגרי מידע שאותם גורמים בעירייה מתפעלים בלעדית יטופל הנושא במסגרת תהליך הטמעת נוהלי אבטחת המידע החדשים.

לשם שיפור האבטחה הלוגית של מערכות המחשוב שלהן, על עיריות באר שבע, יהוד-מונוסון, יקנעם עילית, כרמיאל ונצרת עילית, המועצה המקומית תל מונד והמועצה האזורית הגליל התחתון, לנהל רישום מרוכז של הרשאות הגישה למאגרי המידע שנתנו לכל עובד, ואל להן להסתפק ברישום נפרד אצל המחזיק בכל אחד ממאגרי המידע שלהן.

בקרה ופיקוח לוגיים

נוהל "בקרה ופיקוח לוגי", הנכלל בנוהלי המסגרת, מגדיר "בקרה לוגית" כ"ניטור שוטף ממוחשב אחר הפעילות במערכת הממוחשבת, תוך התמקדות באירועים חריגים או רגישים" (להלן - יומן השימוש) וקובע כי על מנמ"ר לוודא כי פעילותו תקינה, וכן מגדיר "פיקוח לוגי" כ"מעקב אחר פעילויות במחשב גם לאחר ביצוע הפעילות ובהשהיית זמן כלשהו". בנוהל נקבע כי הממונה על אבטחת המידע אחראי להגדיר פעולות חריגות או רגישות - כגון ניסיונות סרק להזנת ססמה, שימוש בשמות משתמש לא פעילים או פעולות שבוצעו מחוץ לשעות העבודה, כניסות רבות של כל עובד למערכת - שינוטרו באמצעות יומן השימוש (Log). עוד נקבע בנוהל כי אחת לשבוע יבדוק הממונה על אבטחת המידע את יומן השימוש, וכי בעת הבדיקה עליו לבחון בין היתר פעילות הקשורה לעובדים שנעדרו מהעבודה, אך שם המשתמש שלהם היה בשימוש. ממצאים המעידים על פעילויות חריגות שבוצעו בכוונה תחילה יועברו לטיפול גורמי ההנהלה הרלוונטיים.

במאי 2015 פרסם מכון התקנים תקן ישראלי ת"י 1495 חלק 4 - "מדריך לניהול יומן אבטחת מחשב"[30]. התקן מספק הדרכה מעשית עבור הפיתוח, היישום והתחזוקה של נוהגי ניהול יומן אפקטיביים בארגון. במהדורה הנוכחית של התקן

30 תקן זה החליף את התקן הישראלי ת"י 1495 חלק 4 ממרץ 2006.

נידונו כמה נושאים, לרבות הקמת תשתית לניהול יומן, וכן פיתוח וביצוע של תהליכי ניהול יומן אפקטיביים בארגון. התקן מציג טכנולוגיות ניהול יומן ממבט-על, אבל אינו מדריך צעד אחר צעד כיצד ליישם טכנולוגיות ניהול יומן או להשתמש בהן.

משרד מבקר המדינה העיר בביקורת הקודמת למשרד הפנים כי ראוי שיכלול בקובץ ההנחיות המחייב שיגבש עבור הרשויות המקומיות בנושא אבטחת מידע והגנת הפרטיות גם הוראות בדבר הסדרת האבטחה הלוגית והבקרה הלוגית.

כאמור, בביקורת הנוכחית הועלה כי משרד הפנים טרם פרסם קובץ הנחיות המחייב את הרשויות המקומיות בנושא אבטחת מידע.

עיריות יהוד-מונוסון ויקנעם עילית: הביקורת הקודמת העלתה כי ברשויות המקומיות שנבדקו, ובהן עיריות יקנעם עילית ויהוד-מונוסון, לא מתבצעת בקרה לוגית על פעולות המערכות הממוחשבות, ולא מתבצע ניטור יזום של יומני השימוש במחשבים. משרד מבקר המדינה העיר לרשויות האמורות בביקורת הקודמת כי עליהן לקיים פעולות בקרה בתחום אבטחת המידע והגנת הפרטיות ולנטרן, כדי לזהות פעילות חריגה של גורמים בלתי מורשים או ניסיונות לביצוע פעילות כאמור.

הביקורת הנוכחית העלתה כי העיריות האמורות לא תיקנו את הליקויים.

עיריות באר שבע, כרמיאל ונצרת עילית; המועצה המקומית תל מונד והמועצה האזורית הגליל התחתון: בביקורת הנוכחית נמצא כי לכל אחד ממאגרי המידע שבבעלות הרשויות המקומיות שנבדקו יש יומן שימוש. עוד נמצא כי הממונים על אבטחת המידע ברשויות המקומיות שנבדקו אינם מבצעים ניטור יזום של יומן השימוש על מנת לזהות פעולות חריגות שמבצעים גורמים בלתי מורשים או ניסיונות לביצוע פעולות אלה.

עיריית באר שבע מסרה בתשובתה כי בפברואר 2017, לאחר מועד סיום הביקורת, היא חתמה על הסכם עם המרכז הלאומי להתמודדות עם איומי סייבר שבמשרד ראש הממשלה, ובמסגרתו היא מקבלת מהמרכז דוחות על אירועים חריגים ברשת המחשבים של העירייה; עיריית יהוד-מונוסון מסרה בתשובתה כי היא בוחנת דרכי התמודדות עם הנושא המותאמים למסגרת התקציבית שלה; עיריית כרמיאל מסרה בתשובתה כי פנתה בבקשה לקבלת הצעות מחיר לרכישת תוכנה שתאפשר למלא את הדרישות ותותקן על רשת המחשבים שלה; עיריית נצרת עילית מסרה בתשובתה כי תבדוק את האפשרות להפקת דוחות שיתריעו על ביצוע פעולות חריגות במאגרי המידע שלה או על ניסיונות לבצען; המועצה המקומית תל מונד מסרה בתשובתה כי בעקבות הביקורת היא החלה לקיים בקרה ופיקוח לוגיים על מערכות המחשוב שלה.

> הממונים על אבטחת המידע ברשויות המקומיות שנבדקו אינם מבצעים ניטור יזום של יומן השימוש, על מנת לזהות פעולות חריגות שמבצעים גורמים בלתי מורשים או ניסיונות לביצוע פעולות כאלה

משרד מבקר המדינה מעיר לעיריות באר שבע, יהוד-מונוסון, יקנעם עילית, כרמיאל ונצרת עילית; למועצה המקומית תל מונד ולמועצה האזורית הגליל התחתון, כי עליהן לבצע ניטור יזום של יומן השימוש של המחשבים שבהם נשמרים מאגרי המידע שלהן, על מנת ללמוד על פריצות למאגר המידע, על חריגות או על שימוש במידע בידי גורמים בלתי מורשים. משרד מבקר המדינה מציין כי השירות שנותן המרכז הלאומי להתמודדות עם איומי סייבר מנטר תקשורת בין רשת התקשורת של הרשות המקומית לבין שרתי תקיפה מוכרים ברשת האינטרנט הכללית, ואינו מייתר את הצורך בניטור יזום של יומן השימוש של המחשבים שבהם נשמרים מאגרי המידע שלה.

אבטחת חומרה

נוהל "בקרת גישה למחשב המרכזי ולמחשבים האישיים", הנכלל בנוהלי המסגרת, קובע כי יש לאבטח אבטחה פיזית את התשתיות ומערכות החומרה המשמשות את מאגרי המידע ואת כל סוגי רכיבי התקשורת ואבטחת המידע, וכי יש לשמור אותם במקום מוגן (להלן - חדר מחשב[31]), המונע חדירה וכניסה אליו בלא הרשאה, ואת בהתאם לאופי פעילותו של מאגר המידע ולרגישות המידע השמור בו. להלן יפורטו ממצאי הביקורת הנוגעים למידת השמירה של הרשויות על האבטחה והבטיחות של חדרי המחשב שלהן:

1. בביקורת הנוכחית נמצא כי לכל הרשויות המקומיות שנבדקו יש חדר מחשב. בעיריות באר שבע, כרמיאל ונצרת עילית הכניסה לחדר המחשב מבוצעת באמצעות כרטיס חכם או קודן; בעיריות יהוד-מונוסון ויקנעם עילית, במועצה המקומית תל-מונד ובמועצה האזורית הגליל התחתון הכניסה לחדר המחשב מבוצעת באמצעות מפתח רגיל. אולם בשום רשות מהרשויות המקומיות שנבדקו אין מערכת ממוחשבת הרושמת את שם העובד שנכנס לחדר המחשב, ואת היום והשעה שבהם נכנס.

ראוי שהרשויות המקומיות יתקינו על דלתות הכניסה לחדרי המחשב שלהן אמצעי נעילה שיאפשרו לבצע מעקב אחר הכניסות לחדר המחשב ולוודא כי רק העובדים המורשים לכך ייכנסו אליו.

עיריית יקנעם עילית מסרה בתשובתה כי היא תתקין אמצעי נעילה אלקטרוני שיאפשר מעקב אחר הכניסות לחדר המחשב שלה; עיריית נצרת עילית מסרה בתשובתה כי תבחן את האפשרות לשדרוג מנגנון הכניסה הנוכחי למנגנון המזהה ומתעד באופן אישי את הכניסות לחדר המחשב.

31 מבנה המכיל ציוד שיש לשומרו בתנאים ייחודיים שאינם מתקיימים בסביבת עבודה משרדית.

2. במאי 1995 פרסם מכון התקנים תקן ישראלי ת"י 1243 - "בטיחות אש של מחשבים וציוד היקפי"[32]. התקן קובע בין השאר את העקרונות האלה: רצפת חדר המחשב תנוקז גם אם הציוד מוצב במישרין על הרצפה; בכניסה לחדר המחשב תותקן דלת אש תקנית[33] בעלת עמידות לאש של 30 דקות לפחות; קירות חדר המחשב יהיו בנויים ללא פתחים; לא יאוחסנו בחדר המחשב חומרים דליקים, כגון קרטון.

משרד מבקר המדינה העיר בביקורת הקודמת למשרד הפנים כי ראוי שיכלול בקובץ ההנחיות המחייב שיגבש עבור הרשויות המקומיות בנושא אבטחת מידע והגנת הפרטיות גם הנחיות בנושא סיכוני אש ומים בחדרי המחשבים, בהתאם להוראות התקן שקבע מכון התקנים הישראלי, ויאכוף הנחיות אלה.

כאמור, בביקורת הנוכחית הועלה כי משרד הפנים טרם פרסם קובץ הנחיות מחייב עבור הרשויות המקומיות בנושא אבטחת מידע ובכלל זה אבטחת חומרה.

עיריית יהוד-מונוסון: בביקורת הקודמת נמצא, בין היתר, כי בחדר המחשב של עיריית יהוד-מונוסון אין ניקוז לרצפה או "רצפה צפה"[34], לא מותקנת בכניסה אליו דלת אש תקנית ויש בו חלון חיצוני. משרד מבקר המדינה העיר לעירייה בביקורת הקודמת כי ראוי שתתקן את הליקוי האמור ותעמוד בדרישות התקן בכל הנוגע לחדרי מחשב.

בביקורת הנוכחית נמצא כי הליקוי תוקן באופן חלקי. הותקנו מערכות לניטור חום, מים ואש; הותקנה מערכת כיבוי מותאמת; והותקן סורג פנימי קבוע על החלון החיצוני - אולם חדר המחשב שלה עדיין אינו עומד בדרישות התקן.

עיריית יהוד-מונוסון מסרה בתשובתה כי תבחן את האפשרות להחלפת דלת חדר המחשבים לדלת אש בהתאם להמלצת נציג כיבוי וכן תבחן את האפשרות להתקנת "רצפה צפה".

משרד מבקר המדינה מעיר לעיריית יהוד-מונוסון על שבמועד סיום הביקורת, כחמש שנים לאחר שהסתיימה הביקורת הקודמת, חדר המחשב שלה עדיין אינו עומד בדרישות התקן. על העירייה לפעול לאלתר להתאמת חדר המחשב שלה לדרישות התקן.

32 תקן זה החליף את התקן הישראלי ת"י 1243 משנת 1984.

33 דלת אש כהגדרתה בסעיף 3.1.1.1 לתקנות התכנון והבניה (בקשה להיתר, תנאיו ואגרות), התש"ל-1970.

34 רצפה מוגבהת המשמשת להעברת כבלים, מערכות תקשורת, אוויר ממוזג, אספקת חשמל וצנרת כיבוי אש.

עיריות כרמיאל ונצרת עילית, המועצה המקומית תל מונד והמועצה האזורית הגליל התחתון: בביקורת הנוכחית נמצא כי בחדרי המחשב של עיריות כרמיאל ונצרת עילית יש חלונות גדולים ומאוחסנים בהם ארגזי קרטון רבים; בחדרי המחשבים של המועצה המקומית תל מונד והמועצה האזורית הגליל התחתון לא הותקנו מנגנון ניקוז לרצפה או "רצפה צפה", ובכניסה אליהם לא הותקנה דלת אש תקנית.

משרד מבקר המדינה מעיר לעיריות כרמיאל ונצרת עילית, למועצה המקומית תל מונד ולמועצה האזורית הגליל התחתון על שחדרי המחשב שלהן אינם עומדים בדרישות התקן הישראלי.

עיריית כרמיאל מסרה בתשובתה כי בעקבות הביקורת הוצאו מחדר המחשב כל קרטוני הנייר והוזמנו סורגים לחלונות שבחדר המחשב, וכי בימים הקרובים תפרסם מכרז להתקנת מערכת לגילוי אש ולכיבויה בחדר המחשבים; עיריית נצרת עילית מסרה בתשובתה כי בעקבות הביקורת נוקה חדר השרתים מכל הארגזים והארונות, וכיום יש בו ציוד מחשוב בלבד. העירייה הוסיפה בתשובתה כי תבחן פתרון הנדסי ותקציבי לעניין החלונות שבחדר; המועצה האזורית הגליל התחתון מסרה בתשובתה כי בניין המועצה נמצא בשיפוצים, ובסיומם יותאם חדר המחשבים שלה לדרישות התקן הישראלי.

משרד מבקר המדינה מעיר לרשויות המקומיות האמורות כי עליהן לפעול לאלתר להתאמת חדרי המחשב שלהן לדרישות התקן הישראלי.

סקרי סיכונים ומבחני חדירה

בקובץ תיאורי התפקיד נקבע כי אחד מתפקידיו של הממונה על אבטחת מידע הוא תכנון וביצוע של סקרי אבטחת מידע וייזום מבחני חדירה למערכות המידע והתקשורת לשם הדמיית ניסיונות פריצה על ידי פורצים מתוך הרשות המקומית ומחוצה לה.

מטרתו של "סקר סיכונים" היא לאפיין את פגיעות האבטחה של מערכות המחשוב של הרשות המקומית. הסקר אמור להקיף תחומים רבים ומגוונים ולבחון היבטים שונים הקשורים לאבטחת המידע ברשות המקומית, כדי להעריך את הסיכונים הנשקפים למידע, את חומרתם ואת הנזקים שהם עלולים לגרום

למערכות המחשוב ולמאגרי המידע, ולאפשר קבלת החלטה מבוססת בעניין הטיפול בהם.

"מבחני חדירות תשתיות" - בוחנות את איכות אבטחת תשתיות המחשוב ברשות המקומית. במסגרת בדיקות אלו נעשה ניסיון לחדור למערכות המחשוב השונות של הרשות המקומית, להשיג הרשאות ולהגיע למידע הארגוני; "מבחני חדירות אפליקטיביות" - בוחנות את איכות אבטחת יישומי המחשב ברשות המקומית. במסגרתן נבדקים מנגנון הזיהוי, ממשק המשתמש והממשקים מול מאגרי המידע.

עיריות יקנעם עילית ויהוד-מונוסון: בביקורת הקודמת הועלה כי הרשויות המקומיות שנבדקו - ובהן עיריות יהוד-מונוסון ויקנעם עילית - לא ביצעו מעולם סקרי סיכונים ומבחני חדירה. משרד מבקר המדינה העיר בביקורת הקודמת כי על כל רשות מקומית לקבוע במסמך מדיניות אבטחת המידע שלה הוראות אשר יבטיחו כי יתבצע ניהול סיכונים על כל מרכיביו.

משרד מבקר המדינה מציין לחיוב כי עיריית יקנעם עילית תיקנה את הליקוי. העירייה מבצעת סקרים לבדיקת הסיכונים הנשקפים למערכות המידע שלה ומבחני חדירה למערכות חדשות המוטמעות בה, בהתאם לרמת הסיכון של המערכות השונות, בין היתר בעת ביצוע שדרוג או שינוי ניכר במערכות מחשוב ומידע קיימות, וזאת בהתאם למסמך מדיניות אבטחת מידע שאימצה העירייה.

עוד נמצא כי עיריית יהוד-מונוסון תיקנה את הליקוי באופן חלקי. העירייה טרם קבעה מסמך מדיניות אבטחת מידע. בטיוטת מסמך מדיניות אבטחת מידע שהכין מנמ"ר העירייה רק באוקטובר 2016, ולמועד סיום הביקורת - ינואר 2017 - טרם אומץ על ידי העירייה, נאמר כי מנהל אבטחת המידע ייזום את ביצועם של סקרי אבטחת מידע ומבחני חדירה תקופתיים. עם זאת נמצא כי בספטמבר 2016 אישרה ועדת הרכש של העירייה התקשרות עם חברה חיצונית על מנת שתבצע סקר סיכונים ומבחני חדירה למערכות המחשוב והמידע של העירייה. בפברואר 2017, לאחר מועד סיום הביקורת, קיבלה העירייה טיוטה ראשונית של סקר הסיכונים ואת ממצאיהם של מבחני החדירה.

עיריית יהוד-מונוסון מסרה בתשובתה כי רבות מההמלצות הדחופות שהועלו לנוכח ממצאי הסקר יושמו עוד במהלך ביצועו וחלקן יושמו לאחר הגשתו, וכי יתר ההמלצות ייושמו בשנים 2017 ו-2018 בהתאם לדחיפות ההמלצות ולתקציב שיעמוד לרשותה.

משרד מבקר המדינה מעיר לעיריית יהוד-מונוסון כי עליה להמשיך לפעול לתיקון הליקויים שהועלו בסקר הסיכונים ומבחני החדירה, ולנקוט את הפעולות הנדרשות על מנת לשפר את אבטחת מערכות המחשוב והמידע שלה בהתבסס על ממצאי הסקר והמבחנים.

עיריות כרמיאל ונצרת עילית, המועצה המקומית תל מונד והמועצה האזורית הגליל התחתון: בביקורת הנוכחית נמצא כי רשויות מקומיות אלו לא ביצעו מעולם סקר סיכונים ומבחני חדירה.

עיריית כרמיאל מסרה בתשובתה כי פנתה לקבלת הצעות מחיר לביצוע סקר סיכונים ומבחני חדירה; עיריית נצרת עילית מסרה בתשובתה כי היא תשקול לגייס תקציבים ממקורותיה היא וממשרד הפנים לשם ביצוע סקר סיכונים ומבחני חדירה כמתבקש; המועצה המקומית תל מונד מסרה בתשובתה כי היא נמצאת בסיום תהליך ההטמעה והמעבר לציוד המחשוב החדש ומיד בסיום התהליך יבוצעו סקר סיכונים ומבחני חדירה על ידי חברה חיצונית; המועצה האזורית הגליל התחתון מסרה בתשובתה כי בעקבות הערת מבקר המדינה היא מתכננת שגורם מקצועי חיצוני יבצע סקר סיכונים ומבחני חדירה למערכות המחשב שלה.

משרד מבקר המדינה מעיר לעיריות כרמיאל ונצרת עילית, למועצה המקומית תל מונד ולמועצה האזורית הגליל התחתון כי עליהן לבצע סקר סיכונים ומבחני חדירה במערכות המחשוב והמידע שלהן ולקבוע במסמך מדיניות אבטחת המידע שלהן הוראות אשר יבטיחו את ביצועם של סקר סיכונים ומבחני חדירה כאמור בתדירות קבועה גם בעתיד.

חלק מהרשויות המקומיות שנבדקו לא ביצעו מעולם סקרי סיכונים ומבחני חדירה

אירועי אבטחת מידע

אירוע אבטחת מידע הוא אירוע המעורר חשש לפגיעה מכוונת בשלמות מאגר המידע או אירוע שבמסגרתו נעשה שימוש בנתוני מאגר מידע ללא הרשאה. בשנים האחרונות גדל היקף התקיפות באמצעות נוזקות שונות המאפשרות את העתקת הנתונים השמורים במערכות המחשוב על ידי מי שאינו מוסמך לכך; או באמצעות כופרות (ransomware) המגבילות את הגישה למערכות המחשוב ומשמשות לסחוט מהמשתמש תשלום כסף (דמי כופר) על מנת שתוסר מגבלת הגישה. חלק מהכופרות מבצעות הצפנה לקבצים על הכונן הקשיח, ובכך מקשות את תהליך הסרת ההצפנה בלי לשלם כופר עבור מפתח ההצפנה, ואילו תוכנות כופר אחרות נועלות את המערכת ומציגות הודעת שווא ולפיה לא

מתאפשרת גישה לקבצים, וזאת על מנת לחייב את המשתמש לשלם את הכופר במרמה. תוכנת הכופר חודרת לרוב כסוס טרויאני[35], המוסווה כקובץ תמים.

מפרסומי המרכז הלאומי להתמודדות עם איומי סייבר[36] עולה כי בכל יום מתבצעים בממוצע כ-170 ניסיונות תקיפה באמצעות כופרות בישראל, ועקב כך היא מדורגת במקום ה-29 ברשימת המדינות המותקפות בעולם בנוזקות מסוג זה. מנתוני משטרת ישראל[37] עולה כי בשנת 2015 נפתחו 1,076 תיקי עבירות מחשב[38], עלייה של 22.4% לעומת השנה הקודמת. סעיף האשמה השכיח ביותר בשנה זו (44% מכלל ההאשמות) היה חדירה לחומר מחשב.

> בשנים האחרונות גדל היקף התקיפות באמצעות נוזקות המאפשרות פגיעה בשלמות מאגר המידע או שימוש בנתוני מאגר המידע ללא הרשאה

הביקורת הנוכחית העלתה כי בעיריות יהוד-מונוסון, יקנעם עילית, כרמיאל ונצרת עילית נפגעו בשנת 2016 עמדות מחשב על ידי כופרות בעקבות כך שאחד העובדים פתח קישורים בדואר אלקטרוני ממקור לא ידוע. נמצא כי בעיריות יהוד-מונוסון, יקנעם עילית וכרמיאל הפגיעה הייתה נקודתית בעמדת מחשב יחידה ולא נגרם נזק ממשי.

עיריית נצרת עילית: נמצא כי באוגוסט 2016 פגעה כופרה בשרת המשמש את מחלקת ההנדסה של עיריית נצרת עילית, לאחר שעובדת המחלקה פתחה קובץ שנשלח לכתובת הדואר האלקטרוני שלה. הבדיקה העלתה כי הגיבוי האחרון של המידע בשרת מחלקת ההנדסה בוצע בסוף שנת 2015, וכי לעירייה לא היה גיבוי מלא של כל הקבצים שאוחסנו בשרת באותו מועד, שכן מערכת הגיבוי שלה לא גיבתה את כל סוגי הקבצים שאוחסנו בשרת. בעקבות כך לא ניתן היה לשחזר חלק מהמידע, כגון חלק מקובצי התמונות המאוחסנות בשרת שתיעדו עבירות בנייה. בהיעדר תיעוד נפגעה יכולת העירייה להגיש כתבי אישום נגד עברייני הבנייה.

התוקף דרש מהעירייה לשלם כופר בסך 10,000 ש"ח לשם הסרת מגבלת הגישה לקבצים, והיא בחרה שלא לשלמו. העירייה הגישה למשטרה תלונה בנושא, אך המשטרה סגרה אותה בנימוק שמדובר ב"עבריין לא ידוע". פניות של העירייה לקבלת עזרה מהמחזיק במאגר המידע, ממשרד הפנים ומגופים פרטיים נוספים לא הועילו, ולמועד סיום הביקורת, ינואר 2017, הקבצים שהיו שמורים בשרת נשארו מוצפנים ולעירייה לא הייתה גישה אליהם.

35 סוס טרויאני מופיע בדרך כלל כקובץ המצורף להודעת דואר אלקטרוני או כתוכנה חופשית להורדה, ובעת הפעלתו יבצע פעילות משעשעת או מועילה (למשל, סרטון קצר), כדי לגרום למקבל הווירוס לשלוח אותה הלאה לחברים נוספים. אותה פעילות היא הסוואה לכך שהתוכנה מתקינה את עצמה במחשב ועלולה לגרום נזק.

36 המרכז הלאומי להתמודדות עם איומי סייבר, **נוזקות כופר למתחילים** (פברואר 2017). מתוך אתר המרכז https://cert.gov.il/Resources/best_practices/Pages/best_practices.aspx

37 משטרת ישראל, **השנתון הסטטיסטי לשנת 2015 (**מאי 2016), עמ' 36.

38 עבירות הכלולות בחוק המחשבים, התשנ"ה-1995.

משרד מבקר המדינה מעיר לעיריית נצרת עילית כי מערכת הגיבוי שלה לא הותאמה לגיבוי כל סוגי הקבצים שנשמרו בשרתי המחשב שלה, וכי הגיבויים בוצעו בתדירות נמוכה. על העירייה לוודא שמערכת הגיבוי שלה מסוגלת לגבות את כל סוגי קובצי המחשב המאוחסנים בשרתיה ולבצע את הגיבוי בתדירות התואמת לרגישות החומר המגובה, וזאת על מנת להבטיח שלא תאבד מידע חשוב אם תתבצע תקיפה נוספת או תקלה מכל סוג.

עיריית נצרת עילית מסרה בתגובתה כי תוכנת הגיבויים שבה היא משתמשת שודרגה לגרסה החדשה ביותר, וכי היא בוחנת את האפשרות לביצוע גיבוי נוסף באתר חיצוני. העירייה הוסיפה כי מפעם לפעם נשלחות באופן יזום לכלל עובדיה הודעות ריענון בנושא אבטחת מידע המזהירות מפני פתיחת הודעות דואר אלקטרוני חשודות.

האירוע האמור בעיריית נצרת עילית והשפעותיו צריכים לשמש למשרד הפנים "תמרור אזהרה" המעיד על חשיבות אסדרת נושא אבטחת המידע ברשויות המקומיות.

דיווח על אירועי אבטחת מידע

הביקורת הנוכחית העלתה כי האסדרה הַתְקָפָה אינה מחייבת בעלים של מאגר מידע או גורם המחזיק בו לתעד את אירועי אבטחת המידע ואת הפעולות שננקטו בעקבותיהם. עוד העלתה הביקורת הנוכחית כי האסדרה הקיימת אינה מחייבת בעלים של מאגר מידע או גורם המחזיק בו לדווח על אירועי אבטחת מידע לרשם מאגרי המידע או לכל גוף מאסדר אחר ואף לא לאזרחים שמידע עליהם נחשף, ועקב כך הם עלולים להיפגע מהאירוע.

במאי 2017, לאחר סיום הביקורת, פורסמו ברשומות תקנות הגנת הפרטיות (אבטחת מידע), התשע"ז-2017[39], שייכנסו לתוקף במאי 2018. תקנה 11 מחייבת בעל מאגר מידע, בין היתר, לתעד אירועים המעוררים חשש לפגיעה בשלמות המידע, לשימוש בו ללא הרשאה או לחריגה מהרשאה ואת הפעולות שננקטו בעקבותיהם; לקבוע הוראות לעניין ההתמודדות עם אירועי אבטחת מידע, לפי חומרת האירוע ומידת רגישות המידע, לרבות לעניין ביטול הרשאות וצעדים מידיים אחרים שיש צורך בהם. אשר לדיווח על אירועי אבטחת מידע, בתקנה 11(ה-ו) נקבע כי בעל מאגר מידע חייב לדווח לרשם מאגרי המידע על אירוע

39 קובץ התקנות 7809 (מאי 2017).

אבטחת מידע חמור[40] ועל הצעדים שנקט בעקבותיו. במקרה זה רשאי הרשם להורות לבעל המאגר, לאחר שנועץ בראש הרשות הלאומית להגנת הסייבר, להודיע על אירוע האבטחה למי שעלול להיפגע ממנו.

משרד מבקר המדינה מעיר לרמו"ט, האחראית לפי חוק הגנת הפרטיות לתחומי הפיקוח ולאכיפת נהלים והנחיות הנוגעים להגנת מידע אישי, כי עליה להיערך ליישום התקנות החדשות, ובכלל זה להביא לידיעת בעלי מאגרי המידע, ובהם הרשויות המקומיות, את חובת הדיווח לרשם מאגרי המידע על אירועי אבטחת מידע חמורים. על רמו"ט לרכז את הנתונים על אירועי אבטחת מידע אלו. הדבר יאפשר לרשם מאגרי המידע לעקוב אחר היקף תופעת אירועי אבטחת המידע במישור הארצי והמגזרי, לנתח אירועים אלה, ליזום פעולות לצמצום התופעה ולחזק את ההגנה על המידע האישי.

רמו"ט מסרה בתשובתה כי היא נערכת ליישום התקנות הן מבחינת היערכות פנימית והן בהיבטי הסברה והנגשה לציבור ופעילות מול רגולטורים מגזריים ספציפיים אשר פרסמו הנחיות אבטחת מידע למפוקחיהם.

ראוי שמשרד הפנים, כמאסדר של השלטון המקומי, יכלול בקובץ ההנחיות לרשויות המקומיות בנושא אבטחת המידע והגנת הפרטיות את החובה לדווח לו על כל אירוע אבטחת מידע שאירע במאגרי המידע שלהן ועל הפעולות שהן נקטו בעקבות כך. ריכוז הדיווחים יאפשר למשרד לעקוב אחר היקף תופעת אירועי אבטחת המידע ברשויות המקומיות, לנתחם וליזום פעולות לצמצום התופעה. הדבר יחזק את ההגנה על המידע שבידי הרשויות המקומיות, ובכלל זה המידע האישי על התושבים.

> ראוי שמשרד הפנים ינחה את הרשויות המקומיות לדווח לו על כל אירוע אבטחת מידע, דבר שיאפשר לו לעקוב אחר היקף התופעה וליזום פעולות לצמצומה

40 במאגר מידע שחלה עליו רמת אבטחה גבוהה - אירוע שבמהלכו נעשה שימוש במידע מן המאגר בלא הרשאה או בחריגה מהרשאה או נפגעת שלמות המידע; במאגר שחלה עליו רמת אבטחה בינונית - אירוע שבמהלכו נעשה שימוש בחלק מהותי מן המאגר בלא הרשאה או בחריגה מהרשאה או נפגעת שלמות המידע של חלק מהותי מהמאגר.

התקשרויות עם חברות פרטיות המחזיקות במאגרי מידע של הרשות המקומית

בחוק הגנת הפרטיות נקבע כי "מחזיק, לעניין מאגר מידע" הוא "מי שמצוי ברשותו מאגר מידע דרך קבע והוא רשאי לעשות בו שימוש". עוד נקבע בחוק כי "בעל מאגר מידע, מחזיק במאגר מידע או מנהל מאגר מידע, כל אחד מהם אחראי לאבטחת המידע שבמאגר המידע". רשויות מקומיות מתקשרות עם חברות פרטיות לקבלת שירותים שונים, כמו שירותי מחשוב, חיוב וגביית מסים וגביית קנסות. לצורך קבלת שירותים אלו מוקנית לחברות הפרטיות גישה למאגרי המידע של הרשויות המקומיות, ורבים ממאגרי המידע שבבעלות הרשויות המקומיות שמורים בשרתי החברות הפרטיות (להלן - מחזיק במאגר מידע). להלן יפורטו ממצאי הביקורת העיקריים בנושא התקשרות הרשויות המקומיות עם נותני שירותים בעלי גישה למאגרי המידע שלהן:

1. בחוק הגנת הפרטיות נקבע, כאמור, כי אדם לא ינהל ולא יחזיק במאגר שום מידע החייב ברישום, אלא אם כן המאגר נרשם בפנקס מאגרי המידע. עוד נקבע בחוק כי מחזיק שברשותו חמישה מאגרי מידע לפחות החייבים ברישום ימסור לרשם מדי שנה רשימה של מאגרי המידע שהוא מחזיק בהם ובכלל זה יציין, בין היתר, את שמות בעלי המאגרים.

   בביקורת הנוכחית נמצא כי חלק ממאגרי המידע של עיריות יקנעם עילית, כרמיאל ונצרת עילית והמועצה המקומית תל מונד, שכאמור אינם רשומים אצל רשם מאגרי המידע ברמו"ט, שמורים בשרתי חברות פרטיות.

   התברר כי רשם מאגרי המידע ברמו"ט אינו אוכף על חברות פרטיות המחזיקות במאגרי מידע של רשויות מקומיות את חובת הדיווח השנתי על מאגרי המידע שהן מחזיקות כנדרש בחוק.

   משרד מבקר המדינה מעיר לרמו"ט על שהפיקוח הלקוי על הרשויות המקומיות ועל המחזיקים במאגרי המידע שלהן פגע ביכולתה לאכוף את הוראות חוק הגנת הפרטיות.

2. נוהל "קשר עם גורמי חוץ ב-outsourcing (מיקור חוץ)" הנכלל בנוהלי המסגרת, קובע כי התקשרות עם גורם חוץ מותנית באישור מוקדם של הממונה על אבטחת המידע, וכי ייחתם חוזה עם כל גורם חוץ - לרבות ספק ציוד, שירות לחומרה או תוכנה - הבא במגע עם עמדת עבודה או עם המחשב המרכזי, ובו תהיה התייחסות מיוחדת לנושא אבטחת המידע.

החוזה יתייחס לטיפול נאות בציוד; לאיסור לגעת בעמדות העבודה, בחומר השמור באמצעים מגנטיים, בפלטים מודפסים ומסמכי קלט; ולחובה לשמור על סודיות מוחלטת של כל מידע שיתגלה להם. כמו כן קובע הנוהל כי גורם החוץ ועובדיו יחתמו על התחייבות לשמירת סודיות.

במרץ 2003 הוציא מנכ"ל משרד הפנים[41] נוהל בנושא העסקת חברות גבייה[42], ולפיו רשויות מקומיות רשאיות להעסיק חברות גבייה לצורך שליחת הודעות חיוב במסי עירייה, גבייה שוטפת של מסים אלו וגביית חובות שמקורם בפיגורים בתשלומיהם. בנוהל נקבע שהסכם התקשרות עם חברת גבייה חייב לכלול התחייבות של החברה כי כל מידע שיגיע אליה או אל עובדיה הנותנים שירות לרשות מקומית מסוימת ישמש רק לצורך ביצוע השירות, וכי לא ייעשה בו כל שימוש אחר והוא לא יימסר לאדם שאינו מוסמך לקבלו. להלן יפורטו ממצאי הביקורת בנוגע לאבטחת המידע אשר לגורמים המחזיקים במאגרי המידע שלה יש גישה אליו:

א. בביקורת הקודמת העיר משרד מבקר המדינה למשרד הפנים כי בנוהל שהוציא להעסקת חברות גבייה אין התייחסות לפעולות שנדרשות החברות לבצע לצורך אבטחת המידע המועבר אליהן.

הועלה כי משרד הפנים פעל לתיקון הליקוי. ביוני 2014 פורסמה ברשומות הצעת חוק לתיקון פקודת העיריות (מס' 138)(חברות גבייה), התשע"ד-2014[43] (להלן - הצעת החוק). מטרת הצעת החוק, שיזם המשרד, היא הסדרת אופן העסקתן של חברות גבייה על ידי רשויות מקומיות. בין היתר הוצע להוסיף לפקודת העיריות את סעיף 330יא: "קבלת מידע בידי חברת גבייה והטיפול במידע". סעיף זה קובע הוראות בעניין אופן ההעברה של מידע מהעירייה לחברת הגבייה ולעובדיה ומחייב את החברה ועובדיה באבטחת המידע ובחובת סודיות לגבי כל מידע שהגיע לידי חברת הגבייה במסגרת מתן השירות לעירייה. כמו כן מסדיר הסעיף את אופן הטיפול במידע הנמצא בידי חברת הגבייה בעת סיום ההתקשרות עם העירייה, וקובע כי שר הפנים יהיה רשאי לקבוע הוראות לעניין ביעור המידע שנמצא בידי חברת הגבייה.

על הצעת החוק הוחל דין רציפות בהתאם לחוק רציפות הדיון בהצעות חוק, התשנ"ג-1993. כמו כן, במועד סיום הביקורת ועדת הפנים והגנת הסביבה של הכנסת טרם קיבלה החלטה בעניינו.

41 חוזר מנכ"ל 2/2003.

42 בעניין זה ראו גם מבקר המדינה, **דוחות על הביקורת בשלטון המקומי לשנת 2008** (2009), "פעולות הגבייה של הרשויות המקומיות באמצעות חברות פרטיות", עמ' 425-459.

43 הצעות חוק הממשלה 875 (יוני 2014).

ב. **עיריית כרמיאל:** בביקורת הנוכחית נמצא כי העירייה לא חתמה על חוזים למתן שירות עם שניים מהמחזיקים במאגרי המידע שלה ואף לא החתימה אותם על התחייבות לשמירת סודיות.

עיריית כרמיאל מסרה בתשובתה כי תינתן לכל המחלקות הנחיה לצרף לכל מכרז טופס התחייבות לשמירת סודיות שייחתם על ידי נותן השירות ועל ידי כל אחד מעובדיו שיש לו גישה למאגרי המידע שלה. עוד מסרה העירייה כי היא פנתה לכל נותני השירות כיום שיש להם ולעובדיהם גישה למאגרי המידע שלה וביקשה שיחתמו על טופס התחייבות כאמור. העתקים של הטפסים החתומים יועברו לממונה על אבטחת המידע בעירייה לצורכי ביקורת ומעקב.

יצוין כי בפברואר 2017, לאחר סיום הביקורת, החתימה העירייה את שני הספקים האמורים וכן ספק שלישי, שעמו חתמה על חוזה לאספקת שירותים שלא כלל התחייבות לשמירת סודיות, על "הצהרה לאי קיום ניגוד עניינים והתחייבות לשמירת סודיות ושמירת זכויות".

> רשויות מקומיות לא כללו בהסכמים שחתמו עם המחזיקים במאגרי המידע שלהן התייחסות לגבי המורשים לקבל גישה למאגרי מידע אלה

משרד מבקר המדינה מעיר לעיריית כרמיאל כי עליה להתקשר על פי דין ולחתום על הסכמים למתן שירות עם כל המחזיקים במאגרי המידע שלה. על העירייה לכלול בהסכמים סעיף סודיות המגדיר את האחריות של המחזיקים במאגרי המידע ושל עובדיהם לאבטחת המידע של הרשות המקומית ולשמירה על סודיות.

3. בחוק הגנת הפרטיות נקבע כי גורם המחזיק במאגרי מידע של בעלים שונים יבטיח כי הגישה לכל מאגר תתאפשר רק למי שהורשה לכך במפורש בהסכם בכתב בינו לבין בעליו של אותו מאגר.

עיריות יהוד-מונוסון ויקנעם עילית: הביקורת הקודמת העלתה כי שום רשות מהרשויות המקומיות שנבדקו, ובהן עיריות יהוד-מונוסון ויקנעם עילית, לא חתמה עם המחזיקים במאגרי המידע שלהן על הסכמים לגבי המורשים לקבל גישה למאגרי המידע שלהן כנדרש בחוק הגנת הפרטיות.

בביקורת הנוכחית נמצא כי הליקוי לא תוקן, וכי שתי העיריות טרם כללו בהסכמים שחתמו עם המחזיקים במאגרי המידע שלהן התייחסות למורשים לקבל גישה למאגרי המידע שלהן. עוד נמצא כי הממונה על אבטחת המידע בעיריית יקנעם עילית מוסר למחזיקים במאגרי המידע שלה אישור בכתב לגבי כל עובד שהורשה לקבל גישה למאגר מידע שבבעלותה. בעיריית יהוד-מונוסון מאושרות הרשאות הגישה לכל עובד על ידי מנהל האגף שבו הוא מועסק, והן מוגדרות במערכת על ידי החברה החיצונית המנהלת את מאגר המידע הרלוונטי.

עיריות כרמיאל ונצרת עילית, המועצה המקומית תל מונד והמועצה האזורית הגליל התחתון: הביקורת הנוכחית העלתה כי הרשויות המקומיות האמורות לא כללו בהסכמים האמורים התייחסות ללגבי המורשים לקבל גישה למאגרי המידע שלהן. הועלה כי רשויות מקומיות אלו הסתפקו במסירת אישור בכתב לחברות החיצוניות המחזיקות במאגרי המידע שלהן לגבי כל עובד שהורשה לקבל גישה למאגר מידע שבבעלותן. האישור כולל את פרטי העובד, את שם המאגר אשר יש לאפשר לעובד גישה אליו ואת ההרשאות המאושרות לו במאגר.

עיריית נצרת עילית מסרה בתשובתה כי היועצת המשפטית שלה בוחנת נוסח לעיגון ולהטמעה של הנושא בהסכמים עם ספקים חיצוניים, וכי היא החלה להכין טופס ייעודי למתן הרשאות גישה למאגרי המידע שלה הכולל את כל המידע והאישורים הנדרשים.

משרד מבקר המדינה מעיר לעיריות יהוד-מונוסון, יקנעם עילית, כרמיאל ונצרת עילית, למועצה המקומית תל-מונד ולמועצה האזורית הגליל התחתון כי עליהן לעגן בהסכמים שהן חותמות עם חברות חיצוניות המחזיקות במאגרי המידע שלהן את נוסח האישור הנדרש כדי לתת לעובד הרשות המקומית גישה למאגר המידע, וכן עליהן לקבוע בהסכם מיהו בעל התפקיד המוסמך להוציא את האישור. מתן הרשאה המאפשרת לעובד גישה למאגר מידע של הרשות שבו מחזיקה חברה חיצונית, שינוי ההרשאה או ביטולה - כל אלה ראוי שיבוצעו בטופס ייעודי על ידי מנהל אבטחת המידע של הרשות המקומית, באופן שיאפשר לדעת בכל רגע ורגע למי מהעובדים יש הרשאת גישה למאגרי המידע של הרשות.

הדרכה וביקורת

הדרכה והסברה

הדרכת עובדי הרשות המקומית, ובייחוד עובדים חדשים, בנושאי אבטחת מידע נדרשת כדי להבטיח כי העובדים יהיו ערים לקיומם של גורמים העלולים לסכן את מערכות המידע ולחשיבות הפעולות לאבטחת המידע הנהוגות ברשות.

נוהל "מודעות, הדרכה, הטמעה והסברה", הנכלל בנוהלי המסגרת, קובע כי מנהל אבטחת המידע אחראי לכך העובדים ישתתפו פעם בשנה בהדרכה בנושא נוהלי אבטחה והשימוש הנכון באפשרות לעיבוד מידע, כדי למזער סיכוני אבטחה אפשריים, וכי במהלך השנה תתבצע פעילות ריענון להגברת המודעות של העובדים - הן עובדים חדשים והן עובדים שטרם קיבלו הדרכה מתאימה - בנושא אבטחת מידע ויתקיימו ימי עיון ייעודיים בנושא. עוד קובע הנוהל כי לפני שעובדי המשרד ומשתמשי צד שלישי יקבלו הרשאת גישה למידע או לשירותים, הם יקבלו הדרכה נאותה ויעודכנו, דרך קבע, בנוגע לשיטות הפעולה ולנהלים של המשרד. מנהלים ועובדים יתודרכו לדווח על כל חריגה בתחום המערכות הממוחשבות שעלולה להשפיע על אבטחת המידע. כל אירוע חריג בתחום האבטחה ייחקר ויוסקו ממנו מסקנות כדי למנוע את הישנותו. אם יתעורר חשד לביצוע עבירה משמעתית או פלילית בנוגע לגילוי סודות או למסירת מידע שלא כדין, יש לדווח על כך מיד לסמנכ"ל בכיר למינהל.

בתיאור תפקיד הממונה על אבטחת המידע שבקובץ תיאורי התפקיד צוין כי תחומי האחריות שלו הם, בין היתר, הדרכת משתמשים בנושא אבטחת מידע והחתמת עובדים חדשים על הצהרת סודיות וכן על התחייבות ולפיה הם אחראים להיבטי אבטחת מידע.

הביקורת הקודמת העלתה כי הרשויות המקומיות שנבדקו, ובהן עיריות יהוד-מונוסון ויקנעם עילית, לא קיימו פעולות הדרכה והסברה בתחום אבטחת המידע. משרד מבקר המדינה העיר בביקורת הקודמת כי לדעתו ראוי שהרשויות המקומיות יקיימו פעולות הדרכה והסברה בתחום אבטחת המידע בדומה לדרישות המפורטות בנוהל המסגרת.

עיריית יהוד-מונוסון: בביקורת הנוכחית נמצא כי הליקוי עדיין לא תוקן. בטיוטת מסמך "מדיניות אבטחת מידע ונהלים" שהכין מנמ"ר העירייה רק באוקטובר 2016, אשר העירייה טרם אימצה, נאמר כי מנהל אבטחת המידע יתווה תכנית הדרכה להעלאת המודעות של העובדים לנושא אבטחת המידע בעירייה, וכי לעובדים יינתנו הדרכות אבטחת מידע בהתאם לידע הנחוץ לכל בעל תפקיד. נמצא כי עובדים חדשים מקבלים הדרכה אישית בנושא אבטחת המידע ומוחתמים על טופס שמירת סודיות, וכי נשלחים לכלל העובדים בקביעות הודעות ורענונים בנושא השימוש הנכון בדואר האלקטרוני של הארגון,

אך מנהל אבטחת המידע עדיין לא גיבש תכנית הדרכה בנושא כנדרש במסמך המדיניות.

עיריית יהוד-מונוסון מסרה בתגובתה כי בשנת 2017 היא תכין עבור כל עובדיה תכנית הדרכה בנושא אבטחת מידע והגנת הפרטיות.

משרד מבקר המדינה מעיר לעיריית יהוד-מונוסון כי על אף פרק הזמן הארוך שעבר מאז סיום הביקורת הקודמת, היא טרם אימצה מדיניות אבטחת מידע ואף לא הכינה תכנית הדרכה להעלאת מודעות העובדים לנושא זה. על העירייה לאמץ בהקדם מדיניות אבטחת מידע, לגבש תכנית הדרכה בנושא זה עבור עובדיה וליישמה.

עיריית יקנעם עילית: בביקורת הנוכחית נמצא כי הליקוי תוקן באופן חלקי בלבד. בידי העירייה יש תכנית הדרכה שנתית לאבטחת מידע, שמטרתה הגברת המודעות לסוגיות אבטחת מידע, מתן כלים להתמודדות עם האיומים השונים ורתימת העובדים לעמידה במדיניות ובנהלים הנוגעים לאבטחת המידע של העירייה. התכנית מפרטת את אוכלוסיות היעד להדרכה, את נושאי ההדרכה ואת הדרך לבחינת האפקטיביות שלה. נמצא כי עובדים חדשים מקבלים הדרכה אישית בנושא אבטחת המידע ומוחתמים על טופס שמירת סודיות, אך תכנית ההדרכה השנתית שגיבשה העירייה לכלל העובדים אינה מיושמת.

משרד מבקר המדינה מעיר לעיריית יקנעם עילית כי עליה ליישם בהקדם את תכנית ההדרכה השנתית בנושא אבטחת מידע שגיבשה לצורך העלאת מודעות העובדים לנושא זה.

עיריית יקנעם עילית מסרה בתגובתה כי היא תבצע פעילות ריענון בנושא ותפרסם הנחיות מפורטות לגבי אמצעי הזהירות בשימוש ברשת ובקבלת הודעות דואר אלקטרוני וקבצים מצורפים, וכמו כן תיישם תכנית הדרכה שנתית בנושא.

עיריות באר שבע, כרמיאל ונצרת עילית, המועצה המקומית תל מונד והמועצה האזורית הגליל התחתון: נמצא כי הרשויות המקומיות האמורות לא קבעו תכנית הדרכה שנתית ואינן מקיימות בקרב עובדים חדשים הדרכות סדורות בנושא אבטחת מידע והגנת הפרטיות ואף אינן מארגנות פעולות הדרכה והסברה שנתיות עבור כלל עובדיהן. יחד עם זאת יצוין כי עיריית באר שבע מפיצה אחת לרבעון דף הנחיות מעודכן לשימוש ברשת וביצעה בשנת 2016 הדרכות נקודתיות על פי הצורך ורגישות המידע, ללא תכנית הדרכה מפורטת; בעיריית נצרת עילית כל אימת שטכנאי מחשב מתקין עמדת מחשב לעובד חדש הוא מדריך את העובד כיצד להשתמש בסיסמה ולשמור על סודיותה.

על עיריות באר שבע, כרמיאל ונצרת עילית, המועצה המקומית תל מונד והמועצה האזורית הגליל התחתון לקיים מדי שנה פעולות הדרכה והסברה בתחום אבטחת המידע בדומה לדרישות המפורטות בנוהל המסגרת.

עיריית באר שבע מסרה בתשובתה כי בימים אלו היא מכינה תכנית להגברת מודעותם של העובדים לנושא אבטחת מידע, כי התכנית האמורה מוטמעת בתכנית העבודה לשנת 2017 וכי היא החלה לבחון את האפשרויות לביצוע התכנית. עיריית כרמיאל מסרה בתשובתה כי היא תחל בביצוע הדרכה לכלל העובדים בנושא אבטחת מידע בתדירות של אחת לשנה באמצעות חברה המתמחה בתחום זה; עיריית נצרת עילית מסרה בתשובתה כי עם יישום נוהלי האבטחה החדשים יבוצעו הדרכות יזומות בנושא אבטחת מידע לעובדי העירייה, ובמקרה הצורך גם על ידי מומחים חיצוניים; המועצה המקומית תל מונד מסרה בתשובתה כי ביולי 2017, וכן מדי שנה, יקבלו כלל משתמשי המערכת (חדשים וותיקים) הדרכה בנושא נוהלי אבטחה והשימוש הנכון במאגרים לשם עיבוד מידע, וכי כלל העובדים יוחתמו על הצהרת סודיות והתחייבות לשמירה על הסודיות של נתוני המועצה המקומית; המועצה האזורית הגליל התחתון מסרה בתשובתה כי לאחר קבלת סקר הסיכונים ובמסגרת יישום המלצותיו יבוצעו הדרכות לכל העובדים הרלוונטיים.

על משרד הפנים לכלול במסגרת קובץ ההנחיות המחייב לרשויות המקומיות בנושא אבטחת המידע והגנת הפרטיות את החובה לקיים פעולות הדרכה והסברה בנושא זה, בדומה לדרישות המפורטות בנוהלי המסגרת.

> על משרד הפנים להנחות את הרשויות המקומיות לקיים פעולות הדרכה והסברה לעובדיהן בנושא אבטחת המידע והגנת הפרטיות, בדומה לדרישות המפורטות בנוהלי המסגרת

ביקורות בתחום אבטחת מידע והגנת הפרטיות

ביקורת פנימית

בפקודת העיריות [נוסח חדש] ובפקודת המועצות המקומיות [נוסח חדש] נקבעה החובה למינוי מבקר בכל רשות מקומית (להלן - מבקר פנימי), אשר תפקידיו, בין היתר, לבדוק אם פעולות הרשות המקומית בוצעו כדין ואם הדרכים שבהן העירייה מחזיקה את כספיה ואת רכושה ושומרת על רכוש זה מניחות את הדעת.

בביקורת הקודמת הועלה כי המבקרים הפנימיים של רוב הרשויות המקומיות שנבדקו לא ביצעו ביקורות ייעודיות בנושא אבטחת מידע והגנת הפרטיות. בעיריית יקנעם עילית בוצעה בשנת 2004 "ביקורת מערכות ממוחשבות" שכללה, בין השאר, היבטים שונים של נושא אבטחת מידע. בעיריית יהוד-מונוסון נעשתה ביקורת אבטחת מערכות מידע בחודשים דצמבר 2010 - מרץ 2011, זאת במהלך הביקורת הקודמת של משרד מבקר המדינה.

בביקורת הנוכחית הועלה כי בשנים 2016-2006 לא בוצעו ביקורות פנימיות בנושא אבטחת מידע והגנת הפרטיות בעיריית כרמיאל, במועצה המקומית תל מונד ובמועצה האזורית גליל תחתון.

ראוי כי המבקרים הפנימיים של עיריית כרמיאל, המועצה המקומית תל מונד והמועצה האזורית גליל תחתון יכללו ביקורות בנושא אבטחת מידע והגנת הפרטיות בתכנית העבודה שלהם.

ביקורת חיצונית

המחוקק הקנה למשרד הפנים סמכויות פיקוח, בקרה וביקורת על פעילותו של השלטון המקומי[44]. אגף בכיר לביקורת ברשויות המקומיות שבמשרד הפנים פועל, בין היתר, מכוח הסמכויות שהעניק המחוקק לשר הפנים ואלו שהוקנו בחוק לממונה על ביקורת החשבונות ברשויות המקומיות. את הביקורות מבצעות בעיקר שתי מחלקות: (א) המחלקה לביקורת מינהלית - שתפקידה לעשות ביקורות כלליות ואופקיות בשלטון המקומי בהתאם לתכנית עבודה שנתית וכן לעשות ביקורות מיוחדות על פי החלטות של הנהלת משרד הפנים. בביקורות אלה נבדקים מגוון נושאים ותחומי פעילות מרכזיים ברשות המקומית. (ב) המחלקה לביקורת ראיית חשבון - האחראית למינוי רואי חשבון לביצוע ביקורות בשלטון המקומי. ביקורות אלו כוללות ביקורת על הדוחות הכספיים של הרשות המקומית (דוח כספי שנתי מבוקר), וביקורת שנתית על אופן תפקודה של הרשות המקומית (דוח ביקורת מפורט). משרד הפנים מוציא מדי שנה הנחיות מקצועיות במסגרת "ספר ירוק", הכולל תכנית ביקורת שעל רואה החשבון לבצע ברשות המקומית. בכל שנה נבחר נושא נוסף לביקורת של עובדי המחלקה, כגון הקצאת קרקע או מבנים ללא תמורה או בתמורה סמלית ותמיכה במוסדות ציבור.

הביקורת הקודמת העלתה כי המחלקה לביקורת מינהלית מעולם לא עשתה ביקורת בנושא אבטחת מידע והגנת הפרטיות, וכי המחלקה לביקורת ראיית

44 בנושא זה ראו גם: מבקר המדינה, **דוחות על הביקורת בשלטון המקומי לשנת 2015** (2015), "העסקת מערך רואי חשבון על ידי משרד הפנים לביקורת החשבונות ברשויות המקומיות", עמ' 69-105.

חשבון לא כללה נושא זה בתכניות הביקורת שנדרשו להכין רואי החשבון המבקרים. בביקורת הקודמת העיר משרד מבקר המדינה למשרד הפנים כי ראוי שישקול בעתיד לשלב בתכנית העבודה שלו ביקורות הנוגעות לנושא אבטחת מידע והגנת הפרטיות.

בתגובתו על הביקורת הקודמת מסר משרד הפנים כי ישקול בעתיד לשלב גם ביקורות הנוגעות לנושא אבטחת מידע והגנת הפרטיות במסגרת הביקורות שעושה האגף לביקורת ברשויות המקומיות.

בביקורת הנוכחית הועלה כי תחום אבטחת המידע והגנת הפרטיות לא נכלל בתכנית העבודה של המחלקה לביקורת מינהלית ולא נבחר כנושא נוסף בתכניות הביקורת שנדרשו מרואי החשבון המבקרים.

בתגובתו על הביקורת הנוכחית מסר משרד הפנים כי נושא הנחיית הרשויות המקומיות בעניין אבטחת מידע אינו בתחום אחריותו, ולפיכך אגף בכיר לביקורת ברשויות המקומיות לא יבצע ביקורת בנושא.

> ראוי שמשרד הפנים יכלול את נושא אבטחת המידע והגנת הפרטיות בתכנית הביקורת שלו, בייחוד נוכח הליקויים הרבים בפעולותיהן של הרשויות המקומיות בנושא זה

משרד מבקר המדינה מעיר למשרד הפנים כי נוכח העיקרון שעליו מתבססת החלטת ממשלה 2443, ולפיו על משרדי ממשלה בעלי סמכויות רגולטוריות להגדיר את המדיניות ודרישות האסדרה של המגזר שבו הם פועלים, ומתוקף היותו מאסדר השלטון המקומי, ראוי לכלול את נושא אבטחת המידע והגנת הפרטיות בתכנית הביקורת שלו. זאת בייחוד נוכח העובדה שבביקורת הנוכחית נמצאו ליקויים רבים בפעולותיהן של הרשויות המקומיות בנושא זה. באמצעות ריכוז ממצאי הביקורת כאמור יוכל משרד הפנים לקבל תמונת מצב עדכנית ומלאה של הליקויים ואופן טיפולן של הרשויות המקומיות בנושא.

סיכום

במסגרת פעילותן השוטפת של הרשויות המקומיות נעשה שימוש רב במאגרי מידע הכוללים נתונים אישיים רבים על התושבים. ככל שהן מרבות להשתמש במאגרי מידע כך גוברת הסכנה שהמידע ייחשף ברבים ותיפגע פרטיותם של התושבים. לכן מוטלת על הרשויות המקומיות החובה להגן על מידע זה, להגביר את חוסנן בפני דליפת מידע ולהגנה על רציפות תפקודית לטובת השירות לציבור.

בשנים האחרונות גדל היקף התקיפות של מערכות המחשוב של גופים רבים באמצעות כופרות המגבילות גישה למערכות המחשב, שנועדו לסחוט מהמשתמש תשלום כסף (דמי כופר) על מנת שתוסר מגבלת הגישה או באמצעות נוזקות המאפשרות לאדם שאינו מוסמך לכך להעתיק את הנתונים השמורים בהן. ההיקף הכולל של התופעה ברשויות מקומיות אינו ידוע, בהיעדר חובה לדווח על תקיפות מסוג זה.

ממצאי הביקורת מלמדים כי במועד סיום הביקורת הנוכחית, כחמש שנים לאחר שבוצעה הביקורת הקודמת, המינהל לשלטון מקומי במשרד הפנים ורמו"ט שמשרד המשפטים עדיין מטילים את האחריות לאסדרת הנושא האחד על השני ולמותר לציין שהם לא פעלו לתיקון הליקויים שהועלו בביקורת הקודמת, דבר הפוגע ברמת אבטחת המידע בשלטון המקומי. עוד מעידים ממצאי הביקורת כי כל רשות מקומית עדיין מתמודדת עם נושא אבטחת המידע והגנת הפרטיות כמיטב הבנתה ולפי התקציב שהקצתה לנושא, ובעקבות כך חלק מהרשויות המקומיות אינן מטפלות כראוי בנושא אבטחת המידע שלהן וההגנה על הפרטיות של תושביהן.

נוכח האמור לעיל, על מנכ"ל משרד הפנים ומנכ"לית משרד המשפטים לגבש מתכונת ברורה של חלוקת תחומי האחריות והסמכויות בין משרדיהם בכל הנוגע לאבטחת המידע והגנת הפרטיות ברשויות המקומיות.

על הרשויות המקומיות לתקן את הליקויים שהועלו בנוגע לפעולותיהן בתחום אבטחת המידע והגנת הפרטיות, לפעול להעלאת המודעות בקרב עובדיהן לחשיבות הנושא ולהעמיד לרשותם את האמצעים לקיום חובותיהם בתחום זה.