פרק רביעי

השלטון המקומי

השלטון המקומי

פעולות הביקורת

בשבע רשויות מקומיות נעשתה ביקורת בנושא אבטחת המידע והגנת הפרטיות. נבדקו בעיקר היחידות הממונות על תחומי המחשוב, הארנונה והחינוך. בדיקות השלמה נעשו במשרד המשפטים, במשרד הרווחה והשירותים החברתיים, במשרד החינוך, במינהל לשלטון מקומי שבמשרד הפנים ובמרכז השלטון המקומי בישראל.

אבטחת מידע והגנת הפרטיות ברשויות מקומיות

תקציר

ברשויות המקומיות מאגרי מידע רבים בתחומים האלה: כספים (גבייה, שכר, תשלומים לספקים ועוד); תכנון ובנייה; חינוך (שירות פסיכולוגי חינוכי, גני ילדים קייטנת ועוד); רווחה; כוח אדם; רישוי עסקים; תחבורה וחניה; תברואה ועוד. מאגרים אלה הם הבסיס לעבודתן של הרשויות. חלקם כוללים גם מידע רגיש כהגדרתו בחוק הגנת הפרטיות, התשמ"א-1981 (להלן - חוק הגנת הפרטיות), למשל אבחונים פסיכולוגיים וחוות דעת של פסיכולוגים ושל עובדים סוציאליים. בשנת 2010 היו ברשויות המקומיות כ-520,000[1] תיקי רווחה פעילים וכ-165,000[2] תיקי שירות פסיכולוגי פעילים.

פעולתם של גופים ציבוריים מושתתת על מערכות מידע הכוללות נתונים רבים על התושבים - מעמד אישי, מצב בריאות, מצב כלכלי, הכשרה מקצועית, דעות ואמונות - שחשיפתם עלולה לפגוע בפרטיותם של התושבים. ככל שגופים עושים שימוש נרחב יותר במאגרי מידע כך גוברת הסכנה שהמידע ייחשף ברבים ויפגע בפרטיותם של תושבים, ולכן מוטלת על בעלי המאגרים החובה להגן על המידע.

כמה חוקים נועדו להבטיח את ההגנה על הפרטיות ואת צנעת הפרט ובכללם - חוק יסוד: כבוד האדם וחירותו, הקובע כי "כל אדם זכאי לפרטיות ולצנעת חייו"; חוק הגנת הפרטיות והתקנות שהותקנו מכוחו.

---

1 על פי הערכה של תחום ארגון ומינהל ברשויות המקומיות שבמשרד הרווחה והשירותים החברתיים.
2 על פי הערכה של אגף השירות הפסיכולוגי במשרד החינוך.

פעולות הביקורת

בחודשים ינואר-יולי 2011 בדק משרד מבקר המדינה, לסירוגין, את אבטחת המידע והגנת הפרטיות בשבע רשויות מקומיות: בחמש עיריות (אשקלון, יהוד-מונוסון, בני ברק, טירה ויקנעם עילית) ובשתי מועצות מקומיות (בני עי"ש ורמת ישי). נבדקו בעיקר היחידות הממונות על תחומי המחשוב, הארנונה, הרווחה והחינוך, ובכלל זה כמה בתי ספר, והשירות הפסיכולוגי החינוכי. בדיקות השלמה נעשו במשרד המשפטים, במשרד הרווחה והשירותים החברתיים, במשרד החינוך, במינהל לשלטון מקומי שבמשרד הפנים (להלן - המינהל לשלטון מקומי), במרכז השלטון המקומי בישראל ובחברה א'.

עיקרי הממצאים

1. במשך שנים לא קבע משרד הפנים מדיניות לאבטחת המידע ולהגנת הפרטיות ברשויות המקומיות; לא הניח את התשתית לטיפול בנושא; ולא פעל לקביעת הנחיות בתחום זה, אף שכבר בשנת 1996 תוקן חוק הגנת הפרטיות ונוספו לו סעיפים הנוגעים להגנה על הפרטיות במאגרי מידע.

2. הרשות למשפט, טכנולוגיה ומידע שבמשרד המשפטים לא קיימה מאז הקמתה פעולות פיקוח ואכיפה על רישום מאגרי מידע. כמו כן היא לא קבעה נהלים והנחיות ולא הטילה קנסות על רשויות מקומיות שלא קיימו את חובתן זו.

3. בכל הרשויות שנבדקו, חוץ מעיריית אשקלון, לא מונה ממונה על אבטחת מידע, והממונה בעיריית אשקלון חסר הכשרה בנושא אבטחת מידע. בעקבות הביקורת מונה גם בעיריית בני ברק ממונה על אבטחת מידע.

4. בחמש משבע הרשויות המקומיות שנבדקו לא נקבעו נוהלי אבטחת מידע. אשר לשתי הרשויות שבהן נקבעו נהלים כאלה - באחת מהן הנהלים מיושמים בחלקם בלבד, ואילו בשנייה הוכנה כבר בשנת 2001 טיוטת "נהלי אבטחת מחשבים ומערכות מידע", אך הנהלת העירייה עדיין לא אישרה אותה, והנהלים אינם מיושמים.

5. שלא לפי הוראות חוק הגנת הפרטיות, שתיים משבע הרשויות שנבדקו לא קיימו מעולם את חובת הרישום של מאגרי המידע שלהן; שלוש רשויות לא שילמו אגרות תקופתיות יותר משלוש שנים, ועקב כך נמחק רישום מאגריהן. רק מאגרי מידע של שתי רשויות היו רשומים ברשות למשפט, טכנולוגיה ומידע, כנדרש בחוק.

6. ברשויות המקומיות שנבדקו לא נקבעו כללים לאבטחת המידע במחשבים מנותקי הרשת ובאמצעים הנתיקים האחרים שנעשה שימוש בהם, למעט בעיריית אשקלון - זו הוציאה נוהל לאבטחת המחשבים הניידים שברשותה.

7. בשש משבע הרשויות שנבדקו אין תכנית שיקום מאסון והמשכיות עסקית. רק בעיריית אשקלון הוכנה תכנית כזו, אך במועד סיום הביקורת טרם הסתיימה הפעלתה.

8. ברשויות המקומיות שנבדקו, פרט לעיריית אשקלון, אין הוראות ונהלים תקפים ומחייבים לאבטחת רשומות מכל הסוגים[3].

9. ברשויות שנבדקו נמצא כי מידע אישי הנוגע לבריאותם של תושבים או למצבם הכלכלי או האישי מוחזק בארונות פתוחים, בכוננויות ובמגירות שאינן ניתנות לנעילה. דבר זה אינו עולה בקנה אחד עם הדרישות הבסיסיות להגנה על מידע רגיש הנוגע לתושבים.

10. באגפי החינוך בשתי רשויות מקומיות שנבדקו לא היו מנעולים בחלק מהארונות ומהמגירות המכילים מידע רגיש; אלה שהיה אפשר לנעול אותם לא היו נעולים; בכוננויות לא נעולות היה דואר ובו מידע רגיש.

11. מפקחי משרד הרווחה והשירותים החברתיים אינם בודקים את מילוי הוראות תקנון העבודה הסוציאלית בנושאי חובת הסודיות וניהול רשומות במחלקות הרווחה ברשויות המקומיות. כמו כן לא בוצעו ביקורות ייעודיות של האגף לביקורת פנימית במשרד לשירותים חברתיים בנושאים אלה.

12. חברה א' מחזיקה במאגרי המידע של כל הרשויות המקומיות שנבדקו. לא נחתמו הסכמים בין הרשויות שנבדקו לחברה א' בדבר מורשי הגישה למאגרי המידע שלהן כפי שנדרש בחוק הגנת הפרטיות. לשלוש רשויות מקומיות אין כלל חוזה למתן שירות עם החברה. במועד הביקורת היו שתי רשויות מקומיות לראשונה בעיצומו של מכרז לאספקת שירותי מחשוב הכולל דרישות לקיום הוראות חוק הגנת הפרטיות ואבטחת מידע. רק בשנת 2010 מילאה לראשונה חברה א' את חובתה כמחזיקה במאגרים של בעלים שונים ומסרה דיווח שנתי לרשות למשפט, טכנולוגיה ומידע.

13. בכל הרשויות שנבדקו לא הוקמו ועדות למסירת מידע. בעיריית אשקלון מונתה ועדה כזאת רק במהלך הביקורת, ביוני 2011.

14. ככלל, הרשויות המקומיות שנבדקו לא קיימו פעולות הדרכה והסברה בתחום אבטחת המידע. רק עיריית אשקלון הכינה תכנית הדרכה שנתית לאבטחת מידע וביצעה פעילות רענון להגברת המודעות לנושא האבטחה, ורק בה פועל ממונה אבטחת מידע המארגן את ההדרכות.

15. נושא אבטחת המידע והגנת הפרטיות אינו נכלל בתכניות הביקורת של רואי החשבון העושים ביקורת ברשויות המקומיות מטעם משרד הפנים. גם מחלקת ביקורת מינהלית באגף לביקורת רשויות מקומיות שבמשרד הפנים מעולם לא קיימה ביקורת בנושא זה.

סיכום והמלצות

מממצאיו של דוח זה מסתמן כי לרשויות המקומיות עדיין חסרה התשתית לטיפול בנושא אבטחת המידע והגנת הפרטיות. ברוב הרשויות שנבדקו אין הנחיות מפורטות לטיפול שוטף בנושא; רובן פועלות ללא ממונה על אבטחת מידע כנדרש בחוק; מאגרי המידע שבהן אינם רשומים כנדרש; היקף פעולותיהן בתחומי ההדרכה והביקורת מצומצם.

---

3 רשומות על גבי אמצעים מגנטיים, אופטיים או על גבי ניירת.

על הרשויות המקומיות: לקיים פעולות בקרה בעניין אבטחת המידע והגנת הפרטיות, כדי לזהות פעולות חריגות או ניסיונות של גורמים בלתי מורשים לעשות פעולות כאלה; למנות לאלתר ממונים על אבטחת מידע כמתחייב מחוק הגנת הפרטיות; לגבש מסמך מדיניות בנושא אבטחת מידע, ולקבוע בו את תדירות ביצועם של סקרי סיכונים ומבחני חדירה; להקפיד לרשום ולנהל את כל מאגרי המידע שברשותן כנדרש בחוק; להקים ועדות להעברת מידע ולהכין נהלים ייעודיים בנושא העברת מידע בין גופים ציבוריים כפי שנקבע בתקנות הגנת הפרטיות; לעשות ביקורות על אבטחת מידע ועל הגנת הפרטיות ברשויות המקומיות באמצעות מבקרי הרשויות.

♦

מבוא

1. ברשויות המקומיות מאגרי מידע רבים בתחומים האלה: כספים (גבייה, שכר, תשלומים לספקים ועוד); תכנון ובנייה; חינוך (שירות פסיכולוגי חינוכי, גני ילדים קייטנות ועוד); רווחה; כוח אדם; רישוי עסקים; תחבורה וחניה; תברואה ועוד. מאגרים אלה הם הבסיס לעבודתן של הרשויות. חלקם כוללים גם מידע רגיש כהגדרתו בחוק הגנת הפרטיות, התשמ"א-1981 (להלן - חוק הגנת הפרטיות), למשל אבחונים פסיכולוגיים, חוות דעת של פסיכולוגים ושל עובדים סוציאליים. בשנת 2010 היו ברשויות המקומיות כ-520,000[4] תיקי רווחה פעילים וכ-165,000[5] תיקי שירות פסיכולוגי פעילים.

פעולתם של גופים ציבוריים מושתתת על מערכות מידע הכוללות נתונים רבים על התושבים - מעמד אישי, מצב בריאות, מצב כלכלי, הכשרה מקצועית, דעות ואמונות - שחשיפתם עלולה לפגוע בפרטיותם של התושבים. ככל שהגופים עושים שימוש נרחב יותר במאגרי המידע כך גוברת הסכנה שהמידע ייחשף ברבים ויפגע בפרטיותם של התושבים, ולכן מוטלת על בעלי המאגרים החובה להגן על המידע.

כמה חוקים נועדו להבטיח את ההגנה על הפרטיות ואת צנעת הפרט - חוק יסוד: כבוד האדם וחירותו, הקובע כי "כל אדם זכאי לפרטיות ולצנעת חייו"; חוק הגנת הפרטיות, והתקנות שהותקנו מכוחו.

בחודשים ינואר-יולי 2011 בדק משרד מבקר המדינה לסירוגין את אבטחת המידע והגנת הפרטיות בשבע רשויות מקומיות: בחמש עיריות (אשקלון, יהוד-מונוסון, בני ברק, טירה ויקנעם עילית) ובשתי מועצות מקומיות (בני עי"ש ורמת ישי). נבדקו בעיקר היחידות המופקדות על תחומי המחשוב, הארנונה, הרווחה והחינוך, ובכלל זה כמה בתי ספר, והשירות הפסיכולוגי החינוכי. בדיקות השלמה נעשו במשרד המשפטים, במשרד הרווחה והשירותים החברתיים, במשרד החינוך, במינהל לשלטון מקומי שבמשרד הפנים (להלן - מינהל לשלטון מקומי), במרכז השלטון המקומי בישראל ובחברה א'.

---

4 על פי הערכה של תחום ארגון ומנהל ברשויות המקומיות שבמשרד הרווחה והשירותים החברתיים.
5 על פי הערכת אגף השירות הפסיכולוגי במשרד החינוך.

2. מאגר מידע מוגדר בחוק הגנת הפרטיות: "אוסף נתוני מידע, המוחזק באמצעי מגנטי או אופטי והמיועד לעיבוד ממוחשב"[6]. "מידע" מוגדר בחוק הגנת הפרטיות: "נתונים על אישיותו של אדם, מעמדו האישי, צנעת אישיותו, מצב בריאותו, מצבו הכלכלי, הכשרתו המקצועית, דעותיו ואמונתו". "מידע רגיש" מוגדר: "נתונים על אישיותו של אדם, צנעת אישותו, מצב בריאותו, מצבו הכלכלי, דעותיו ואמונתו" וכל מידע ששר המשפטים קבע בצו, באישור ועדת החוקה חוק ומשפט של הכנסת, שהוא מידע רגיש. "מידע מוגבל" מוגדר בתקנות הגנת הפרטיות (תנאי החזקת מידע ושמירתו וסדרי העברת מידע בין גופים ציבוריים), התשמ"ו-1986 (להלן - תקנות הגנת הפרטיות), כאחד מאלה: מידע על מצב בריאותו של אדם או על צנעת אישיותו; מידע השמור במאגרים המנויים בסעיף 13(ה) לחוק; מידע אחר ששר המשפטים קבע בצו כי הוא מוגבל.

היות שמאגרי מידע מכילים פרטים אישיים, ומסירת נתונים על אדם לזולת עלולה לפגוע בפרטיותו, יש לאבטח את המידע. ככל שאדם עלול להיפגע יותר מגילוי המידע עליו ברבים, כך עולה רמת רגישות המידע ועמה רמת האבטחה שיש לנקוט כדי לשמור עליו. כמו כן לדעת משרד מבקר המדינה מן הראוי שגופים המחזיקים מידע יקבעו נהלים ותקנות בעניין שמירה וניהול של רשומות פיזיות המכילות מידע, ובייחוד מידע רגיש, בין שהופקו באמצעות מחשב, בין שנכתבו ביד, כגון דוחות, פלטי מחשב, מזכרים ותיקי נייר.

חוק הגנת הפרטיות קובע כי האחריות לאבטחת מידע מוטלת על בעלי מאגר המידע, על המחזיקים בו או על מנהליו. הגופים המוזכרים בחוק זה, בין היתר הרשויות המקומיות, חייבים למנות ממונה על אבטחת מידע, והוא יופקד על אבטחת המידע במאגרים המוחזקים ברשותן. אבטחת מידע היא "הגנה על שלמות המידע, או הגנה על המידע מפני חשיפה, שימוש או העתקה, והכל ללא רשות כדין".

אבטחת מידע נעשית בכמה שיטות: 1. אבטחת מחשבים פיזית - פעולות בחמרה ובתשתיות שתפקידן למנוע פגיעה פיזית במאגר המידע. 2. אבטחה לוגית - הפעלה של מנגנוני תכנה ייעודיים, לדוגמה שם משתמש וססמה המוזנים כתנאי להפעלת מחשב או לכניסה לבסיס נתונים. שתי השיטות ניתנות לשילוב ב"כרטיס חכם", אמצעי פיזי המזהה את המשתמש אבל גם דורש הזנת ססמה. 3. אבטחת מידע פיזי (רשומות לא ממוחשבות) - כל הפעולות הנדרשות להגנה על פלטי מחשב, על דוחות, על מזכרים ועל מסמכים שונים המכילים מידע, בפרט מידע רגיש.

אבטחה לוגית כוללת, בין השאר, פעולות או אמצעים אלה: בקרת גישה למחשבים; זיהוי משתמשים ומתן הרשאות להם; זיהוי ואימות הזהות של משתמשים באמצעים ביומטריים; בקרה לוגית על משתמשים; הטמעת תכנה או חמרה במערכות מידע ממוחשבות; אבטחת פעילות פיתוח ותחזוקה של מערכות מידע. אבטחה פיזית כוללת, בין השאר: טיפול במסמכי קלט ופלט; ניהול ואבטחה של אמצעי אחסון מגנטיים ואופטיים; העברת מידע והוצאתו; רישום מאגרי מידע; ניהול מלאי חמרה ותכנה; אבטחת רשומות ותעודות רשמיות; שימור רשומות אלקטרוניות; ביעור רשומות; טיפול בסיכוני אש, חשמל ומים בחדר המחשב.

לאבטחת תקשורת ושימושי אינטרנט יש לנקוט את הפעולות או את האמצעים האלה: אבטחת תכנה ברשתות מקומיות; אבטחת אמצעי התקשורת; אבטחת מידע בשימוש באינטרנט; אמצעים נגד תכנות פוגעניות כמו תכנות וירוס במחשב האישי וברשת המקומית[7]; התקנה ואבטחה של תכנות השתלטות מרחוק; הגנה על הפעלת מודמים ועל שימוש בפקס להעברת "מידע רגיש" או מסווג.

---

6 "למעט - (1) אוסף לשימוש אישי שאינו למטרת עסק; או (2) אוסף הכולל רק שם, מען ודרכי התקשרות, שכשלעצמו אינו יוצר אפיון שיש בו פגיעה בפרטיות לגבי בני האדם ששמותיהם כלולים בו, ובלבד שלבעל האוסף או לתאגיד בשליטתו אין אוסף נוסף".

7 תכנה המכילה קוד עוין שמטרתה להסב נזק. התכנה חודרת למחשב ללא ידיעת המשתמש, מופצת למחשבים אחרים וגורמת לשיבושים ולתקלות בהפעלת המחשב ובעבודתו.

כמו כן יש לנקוט אמצעים לגיבוי המידע ולשחזורו, להתאוששות מאסון (DRP[8]) ולהמשכיות עסקית (BCP[9]). נוסף על כך יש לאבטח את המידע במחשבים המנותקים מרשתות הארגון - מחשבים אישיים, ניידים ומחשבי כף יד[10].

3. במשרדי הממשלה ובגופים ציבוריים אחרים נקבעו נהלים שאינם מחייבים את הרשויות המקומיות, ואולם ניתן ללמוד מהם על הדרישות ועל התנאים להבטחת שמירה על מידע בגופים ציבוריים. אחד מהם הוא נוהל מפת"ח - נוהל מסגרת לניהול המחשוב בארגון הן במישור הפרויקט והן במישור הארגון כולו - על פי החלטת ממשלה[11], הוא נוהל מחייב במשרדי הממשלה. נקבע בו כי אבטחת מידע כוללת כמה רכיבים: שמירה על חיסיון המידע (Confidentiality); זמינות מערכות המידע (Availability); שלמות המידע (Integrity). אבטחת המידע מטרתה להגן על ארבע הפעולות הבסיסיות הנעשות בכל מערכת ובסיס נתונים: יצירה והוספה של מידע חדש (Create); קריאה ושליפה של מידע (Read); עדכון ושינוי של מידע (Update); מחיקה וביטול של מידע (Delete). פגיעה במערכות הממוחשבות במגזר הציבורי עלולה לגרום לנזקים כבדים, כמו פגיעה בשירותים הניתנים לאזרח ובצנעת הפרט.

האגף הבכיר לביקורת המדינה במשרד ראש הממשלה פרסם בספטמבר 2005 "נוהל מסגרת לאבטחת מידע" (להלן - נוהל המסגרת). נוהל המסגרת כולל 38 נהלים לאבטחת מידע במשרדי הממשלה, לרבות 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. לפי נוהל המסגרת, על תחום אבטחת מידע בגוף ציבורי יהיה מופקד "הממונה על אבטחת מידע", ובאחריותו לבקר את הפעילויות הממוחשבות כדי לוודא שהמשרד עומד בדרישות אבטחת המידע שמקורן בחוקים, בתקנות ובנהלים. נוהל המסגרת אינו חל על הרשויות המקומיות, ואולם יש בו כדי ללמד על התשתית הדרושה לאבטחת המידע ולשמירה על הפרטיות בגופים ציבוריים.

4. מכון התקנים הישראלי פרסם כמה תקנים (לא רשמיים) 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).

בהיעדר נהלים מפורטים לרשויות המקומיות בחר משרד מבקר המדינה להציג בחלק מפרקי דוח זה את נוהל המסגרת שנועד להנחות את משרדי הממשלה וגופים ציבוריים ואת התקנים הישראליים כאבני בוחן להערכת נקודות התורפה ברשויות המקומיות שנבדקו.

אבטחת המידע והגנת הפרטיות ברשויות המקומיות

אסדרת הטיפול בנושא אבטחת מידע והגנת הפרטיות בכ-250 רשויות מקומיות מחייבת הנחת תשתית של נהלים ושל הדרכה. משרד מבקר המדינה בחן את פעולות משרד הפנים ומשרד המשפטים בנושא זה.

---

8 Disaster Recovery Planning

9 Business Continuity Plan

10 מבוסס על נוהל מסגרת לאבטחת מידע, משרד ראש הממשלה, ספטמבר 2005.

11 החלטת ממשלה (ועדת השרים לענייני כלכלה) כל/103 מאוקטובר 1991.

משרד הפנים

המינהל לשלטון מקומי שבמשרד הפנים (להלן - המינהל לשלטון מקומי) מופקד על השלטון המקומי בארץ. הוא עוסק בתקצוב הרשויות המקומיות; בהקמת רשויות ותאגידים; בבקרה, בביקורת ובמתן אישורים בענייני כוח אדם ושכר; ברישוי עסקים וחופי הרחצה; בהדרכה, בטיפול בנושאים פרטניים ועוד. המינהל לשלטון מקומי מטפל בנושאים אלה בין היתר באמצעות פרסום הוראות וחוזרי מנכ"ל לרשויות המקומיות.

משרד מבקר המדינה העלה כי במשך שנים לא קבע משרד הפנים מדיניות לאבטחת מידע ולהגנת הפרטיות, לא הניח תשתית לביצועה ולא פעל לקביעת הנחיות בתחום זה, אף שכבר בשנת 1996 תוקן חוק הגנת הפרטיות ונוספו לו סעיפים הנוגעים להגנה על הפרטיות במאגרי מידע.

בתשובתו מנובמבר 2011 השיב משרד הפנים כי הוא אינו הגוף המקצועי בעל הידע והמומחיות הנדרשים לצורך קביעת נהלים בנושא אבטחת מידע. נושא זה אמור להיות מוסדר באמצעות הרשות למשפט, טכנולוגיה ומידע שבמשרד המשפטים שבידה הכלים המקצועיים לגיבוש הנחיות בנושא. אם תפנה הרשות למשרד הפנים בעניין זה, הוא ישתף פעולה עמה.

על תשובת משרד הפנים מעיר משרד מבקר המדינה כי אם, כאמור בתשובתו, אין הוא בעל הידע והמומחיות הנדרשים לצורך קביעת נהלים בנושא אבטחת מידע, מן הראוי שיפנה לרשות למשפט טכנולוגיה ומידע בבקשה שתסייע לו בנושא.

על כל ארגון לגבש נהלים אשר יסדירו את פעולותיו בתחומים השונים. כאמור, חוק הגנת הפרטיות חל על הרשויות המקומיות, ולצורך יישומו יש מקום לקבוע נוהלי עבודה בתחום אבטחת המידע והגנת הפרטיות.

בחמש משבע הרשויות המקומיות שנבדקו לא נקבעו נוהלי אבטחת מידע. בעיריית אשקלון, אחת מן השתיים שנקבעו בהן נוהלי אבטחת מידע, הנהלים מיושמים באופן חלקי בלבד. לדוגמה, בנוהל נקבע כי הממונה על אבטחת מידע יקבע את המדיניות, אך במועד סיום הביקורת עדיין לא הוכן מסמך מדיניות. באוקטובר 2001 הכין יועץ חיצוני עבור עיריית בני ברק טיוטה ובה 40 נהלים בתחום אבטחת מחשבים ומערכות מידע, אך הנהלת העירייה מעולם לא אישרה טיוטה זו, ונהליה אינם מיושמים.

לדעת משרד מבקר המדינה, על משרד הפנים להוציא קובץ הנחיות מחייב לרשויות המקומיות בנושא אבטחת מידע והגנת הפרטיות ולוודא את הטמעתו ואת יישומו. עד שיפורסמו הנחיות אלו על עיריות אשקלון ובני ברק ליישם את נוהלי אבטחת המידע שהכינו במלואם.

משרד המשפטים

בספטמבר 2006 הוקמה במשרד המשפטים הרשות למשפט, טכנולוגיה ומידע[12] כרשות להגנת מידע אישי בישראל. תחומי אחריותה כוללים פיקוח על בעלי מאגרי מידע ועל בעלי רישיונות

---

12 בעקבות החלטה ממשלה 4460 (חכ/195) מ-19.1.06.

(ולצורך זה מוקנות לה סמכויות חיפוש ותפיסה); טיפול בתלונות; חקירת עבֵרות פליליות; הטלת קנסות מינהליים; רישום מאגרי מידע ומתן רישיונות לשירותי נתוני אשראי, שירותי מידע על עוסקים ולגורמים מאשרים; קביעת הנחיות לבעלי מאגרי מידע ולבעלי רישיונות; העלאת מודעות הציבור לזכות לפרטיות של מידע.

משרד מבקר המדינה העלה כי מאז הוקמה הרשות למשפט, טכנולוגיה ומידע היא לא קבעה נהלים והנחיות לרשויות המקומיות המחזיקות במאגרי מידע; לא קיימה פעולות פיקוח ואכיפה על רישום מאגרי מידע ברשויות המקומיות; ולא הטילה קנסות על רשויות מקומיות שלא קיימו את חובתן (בעניין זה ראו להלן).

בתשובתה למשרד מבקר המדינה מספטמבר 2011 מסרה הרשות למשפט, טכנולוגיה ומידע כי היא מקדמת זה כמה שנים יזמת חקיקה לביטול חובת הרישום של מאגרי המידע, ובד בבד עם זאת היא משקיעה את משאביה באכיפה של חובות מהותיים בגופים שהיא מפקחת עליהם (כגון חובות בתחום אבטחת מידע ומתן זכות עיון ושימוש במידע למטרה שלשמה הוא התקבל).

בפברואר 2010 שלחה הרשות למשפט, טכנולוגיה ומידע לכמה גופים ציבוריים, ובכללם שמונה רשויות מקומיות, שאלון שמטרתו לבחון אם הם מקיימים את הוראות חוק הגנת הפרטיות, ובכלל זה את ההוראות בנושאים האלה: מינוי ממונה על אבטחת מידע בארגון; הקמת ועדה להעברת מידע וקביעת סדרי עבודתה; פרסום רשימת הגופים שאליהם מועבר מידע דרך קבע. במועד תום הביקורת, יולי 2011, טרם עובדו התשובות שהתקבלו לכלל דוח סופי.

הרשות למשפט, טכנולוגיה ומידע השיבה למשרד מבקר המדינה כי עיבוד ממצאי הבדיקה נמצא בשלביו האחרונים, וכי הדוח הסופי יופץ עד סוף שנת 2011.

לדעת משרד מבקר המדינה, ראוי שהרשות למשפט, טכנולוגיה ומידע תגבש תכנית למימוש אחריותה בתחום אבטחת המידע והגנת הפרטיות בשלטון המקומי.

לפעילותן של כ-250 רשויות מקומיות בתחום אבטחת מידע והגנת הפרטיות חסרה אסדרה ברמה הממשלתית שתאפשר להניח את התשתית הנוהלית והמקצועית לטיפול בנושא. משרד הפנים ומשרד המשפטים לא נקטו פעולות של ממש לקידום פעולתן של הרשויות המקומיות בתחום זה. המינהל לשלטון מקומי במשרד הפנים והרשות למשפט, טכנולוגיה ומידע במשרד המשפטים נדרשים לקדם פעילות משותפת לצורך קביעת נהלים והנחיות לפעולתן של הרשויות המקומיות. במסגרת זו יש לקבוע את סדרי הטיפול, את הגופים הממונים, את פעולות הפיקוח ועוד.

הבסיס הארגוני והנוהלי לטיפול באבטחת מידע ברשויות המקומיות

1. בחוק הגנת הפרטיות נקבע כי גוף ציבורי חייב למנות אדם בעל הכשרה מתאימה לתפקיד הממונה על אבטחת מידע שבמאגרים שלו (להלן - הממונה). הוראה זו חלה גם על רשויות מקומיות, שכן הן רשויות ציבוריות על פי הגדרות החוק.

בבדיקת משרד מבקר מדינה התברר כי רק אחת משבע הרשויות שנבדקו - עיריית אשקלון - מינתה ממונה על אבטחת מידע, במאי 2011[13], ועובד זה חסר הכשרה בנושא אבטחת מידע. בעקבות הביקורת, בספטמבר 2011, מונה בעיריית בני ברק ממונה על אבטחת מידע.

לדעת משרד מבקר המדינה, על הרשויות המקומיות שנבדקו למנות לאלתר ממונים על אבטחת מידע כמתחייב מחוק הגנת הפרטיות. כמו כן על משרד הפנים ועל הרשות למשפט, טכנולוגיה ומידע לקדם בדיקה בנושא בכלל הרשויות המקומיות ופעולות אשר יבטיחו את מילוי הוראות הדין המחייבות.

2. בחוזר מיוחד של מנכ"ל משרד הפנים מספטמבר 2001 העוסק ב"ממונה על שירותי חירום ובטחון ברשויות מקומיות" תוארה המשרה והוגדרו תפקידיו: ריכוז ועדות הביטחון של הרשות המקומית וועדת משק לשעת חירום (מל"ח) המקומית; ייצוג הרשות המקומית בנושאי חירום וביטחון כלפי משרדי הממשלה, צה"ל, משטרת ישראל וגופים אחרים העוסקים בנושאי חירום וביטחון; קישור ותיאום בין הגופים העוסקים בביטחון ובין שירותי חירום ברשות המקומית; טיפול בכל הקשור בתרגול עובדי הרשות המקומית ובאימונם בנושאי חירום וביטחון; טיפול בהתנדבות לשעת חירום ועוד.

יש לציין כי בגופים ציבוריים כהגדרתם בחוק הגנת הפרטיות, נקבעה חובה למנות אחראי לאבטחת מערכות ממוחשבות חיוניות ולפיקוח עליהן. החוק להסדרת הביטחון בגופים ציבוריים, התשנ"ח-1998, הגם שאינו חל על רשויות מקומיות, מטיל על גוף ציבורי 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.

על משרד הפנים לבחון אם יש מקום להנהיג את ההסדר האמור שנקבע לגבי גופים ציבוריים בחוק להסדרת הביטחון, שלפיו קציני הביטחון מופקדים על פעולות לאבטחת מידע ומערכות מידע, גם ברשויות המקומיות.

מתשובת עיריית אשקלון למשרד מבקר המדינה מספטמבר 2011 עולה כי "באשקלון ממונה אבטחת מידע, אחראי לאבטחת מערכות המידע ובכלל זה בקרת גישה פיזית". עיריית יהוד-מונוסון מסרה בתשובתה מאוקטובר 2011, כי פעולות האבטחה של מערכות מידע ממוחשבות וחיוניות הן בתחום אחריותו של מנהל המחשוב בעירייה.

אבטחת המידע ברשויות המקומיות הלכה למעשה

1. **אבטחה לוגית**: מטרתה העיקרית של האבטחה הלוגית היא לאפשר גישה מבוקרת למערכות המידע וכן לאפשר בקרה על פעילות המשתמשים. האבטחה הלוגית מיושמת - באמצעות מגוון שיטות - במערכות הפעלה, במסדי נתונים, ביישומים, במערכות ייעודיות וכו'. בסוג אבטחה זה נכללות כל פעולות אבטחת המידע המבוססות על תכנה לגילוי ולמניעה של חדירת תכנות זדוניות ומשתמשים בלתי מורשים למידע במחשבי הארגון באמצעות שימוש בשם משתמש ובסיסמה, מידור על ידי מתן הרשאות, תכנת אנטי וירוס, תכנת חומת אש וכו'. בקרה לוגית היא ניטור ממוחשב שוטף של פעילות המערכות הממוחשבות תוך התמקדות באירועים חריגים או

13 הממונה הקודם בעיריית אשקלון מונה בפברואר 2009.

רגישים. פיקוח לוגי הוא מעקב אחר פעילויות שנעשו במחשב. מנהל יחידת המחשב יוודא כי יומן השימוש[14] (log) פועל כתקנו. הממונה על אבטחת המידע יטפל באירועים חריגים באמצעות מערכת ה"לוגים"[15].

בחוק הגנת הפרטיות נקבע כי "לא יפגע אדם בפרטיות של זולתו ללא הסכמתו". עוד נקבע בחוק כי "לא יגלה אדם מידע שהגיע אליו בתוקף תפקידו כעובד, כמנהל, או כמחזיק של מאגר מידע אלא לצורך ביצוע עבודתו... המפר הוראות סעיף זה, דינו מאסר - 5 שנים". על פי חוק הגנת הפרטיות, האחריות לאבטחת מידע חלה על בעליו של מאגר המידע, על הגוף המחזיק במאגר או על מנהלו.

ברשויות המקומיות שנבדקו לא נעשה ניטור יזום של יומן השימוש של המחשבים, אף שבאמצעותו ניתן ללמוד על פריצות למאגר המידע, על חריגות או על שימוש במידע בידי גורמים בלתי מורשים. ברשויות אלה לא ידוע על מקרים כאמור, ואולם בהיעדר ניטור יזום ושיטתי לא ניתן למנוע פעולות כאלה.

לדעת משרד מבקר המדינה, על הרשויות המקומיות לקיים פעולות בקרה בתחום אבטחת המידע והגנת הפרטיות ולנטרן, כדי לזהות מקרים שבהם גורמים בלתי מורשים מבצעים פעולות חריגות או מנסים לבצען.

תקן ישראלי 1495 של מכון התקנים הישראלי בנושא "אבטחת מערכות מידע ממוחשבות - שימוש בסמאות" קובע, בין השאר, את הדרישות לסמה שיש להזין בהתאם לרמת האבטחה. דרישת המינימום היא ארבעה תווים לפחות. בנוהל נדרש כי הסמה תכיל אותיות ומספרים ולא תכיל תווים עוקבים.

על פי נוהל המסגרת, שכאמור לא הוחל על הרשויות המקומיות, הממונה על אבטחת מידע נדרש לקבוע את הדרישות לניהול מערכת הסמאות, לפרסם דרישות אלה בקרב כלל המשתמשים, לפקח על אופן יישומן ולאכוף את חובת היישום. יש לקבוע לכל משתמש שם משתמש וסמה אישית, ואין לשתף בסמאות. הסמה תוחלף בכל שלושה חודשים ותכלול שישה תווים לכל הפחות, ובהם אותיות, ספרות וסימנים. 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.

משרד מבקר המדינה העלה כי בחמש משבע הרשויות שנבדקו (רמת ישי, בני עי"ש, טירה, בני ברק ויהוד-מונוסון) לא נקבעו כללים מחייבים לאבטחה לוגית של המידע. לדוגמה, נמצא כי הפסיכולוגים והמזכירה העובדים בשירות הפסיכולוגי בעיריית יהוד-מונוסון משתמשים בשם משתמש ובסמה זהים, וכך לא ניתן לדעת מי השתמש במחשב, מתי ובאילו קבצים טיפל. בעיריית יקנעם עילית נמצא כי קצינת ביקור סדיר במחלקת החינוך מקלידה רק שלושה תווים בכניסתה למחשב. רק בעיריית אשקלון נקבעו הנחיות לגבי הרשאות גישה למחשבים, ונקבע שיש צורך בהחלפת סמאות, אך במחשב באגף הגבייה שמחובר לרשת המחשבים של העירייה נמצא כי סמת הכניסה מורכבת מרצף של מספרים עוקבים וללא שילוב אותיות (בעניין זה ראו להלן).

בתשובתה מספטמבר 2011 מסרה עיריית אשקלון כי מחשב זה הוסר. עיריית יהוד-מונוסון השיבה כי "מתבצעת אבטחה לוגית במגוון שיטות... ברשת המחשבים מופעלת בקרת אבטחה ע"י

---

14 "יומן" המנוהל אוטומטית על ידי המחשב, ובו נרשמות הפעולות הנעשות במחשב.

15 ראו לעיל הערה מס' 10.

[תכנה]... המנטרת את מצב הרשת וההתקנות בה... כל משתמש קיבל שם משתמש וסיסמא וכאשר יוחלט על מדיניות בנושא, תוגדר במערכת נוהל שינוי סיסמאות אוטו׳ כל תקופת זמן שתקבע... מופעלת מערכת הרשאות המאפשרת לעובד לצפות רק בתיקיות המותאמות למחלקתו בלבד... לכשתקבע מדיניות אבטחה יבוצעו הפעולות הנדרשות״.

לדעת משרד מבקר המדינה, ראוי שעיריית יהוד-מונוסון תקבע בהקדם מדיניות אבטחת מידע שתכלול הפקת ״לוגים״ מהמערכת, וראוי שתמנה אחראי לבדיקתם ולניתוחם.

הביקורת העלתה כי בשום רשות מן הרשויות שנבדקו לא מתבצעת בקרה לוגית של פעילות המערכות הממוחשבות, ולכן אי-אפשר לברר אם אירעו אירועים חריגים; וכאמור, אין בהן ממונה על אבטחת מידע בעל הכשרה מתאימה שאמור לטפל באירועים חריגים המנוטרים באמצעות מערכת ה״לוגים״.

לדעת משרד מבקר המדינה, בנוהל שיגובש יש לכלול את ההוראות בדבר הסדרת האבטחה הלוגית והבקרה הלוגית. על בסיס נוהל כולל זה יכינו הממונים על אבטחת מידע ברשויות המקומיות כללים מפורטים לניהול מערכת הסמאות, ואלה יחייבו את כלל המשתמשים. כמו כן ראוי שייקבעו וייושמו כללי בקרה לוגית, יוגדרו האירועים החריגים וינוטרו הלוגים. מן הראוי שכללים אלה יפורסמו ויתבצע פיקוח על יישומם.

2. **סקרי סיכונים ומבחני חדירה**[16]: כדי להעריך את הסיכונים למידע ואת הנזקים שהם עלולים לגרום למערכי המידע והמחשוב וכדי להיערך לקראתם, יש לקיים הליך לניהול הסיכונים. הליך זה כולל סקר שמטרתו לאתר את הסיכונים הנשקפים לארגון, להעריך את חומרתם ולאפשר קבלת החלטה מבוססת בעניין הטיפול בהם.

במחזור חיים של פרויקט יש לכלול סקר של סיכונים הנשקפים למערכות המידע בארגון והגדרה או עדכון של מדיניות אבטחת המידע בארגון כבר בשלב אפיון המערכת. נושאים חשובים אחרים באפיון הם היבטי חוק ומינהל בתחום אבטחת המידע; סקירה ומיפוי של אמצעי האבטחה הקיימים בארגון; סקירת כלים לאבטחת מידע הנמצאים בשוק ואפיון פעולות הבקרה הארגוניות והטכניות הנדרשות[17].

משרד מבקר המדינה העלה כי הרשויות המקומיות שנבדקו לא ביצעו מעולם סקרי סיכונים ומבחני חדירה.

לדעת משרד מבקר המדינה, על כל רשות מקומית לקבוע במסמך מדיניות אבטחת המידע שלה הוראות אשר יבטיחו כי יתבצע ניהול סיכונים על כל מרכיביו.

3. **אבטחת חמרה**: את המחשבים ואת כל הציוד ההיקפי של הרשות המקומית יש לאבטח אבטחה פיזית. תקן ישראלי 1243 של מכון התקנים הישראלי ״בטיחות אש של מחשבים וציוד היקפי״ קובע בין השאר את העקרונות האלה: רצפת חדר המחשב[18] תנוקז גם כשהציוד מוצב

---

16 מבחני חדירה (Penetration Tests) בוחנים את פוטנציאל הנזק העלול להיגרם לאתרי האינטרנט ולמערכות המידע ברשת הפנימית.

17 מבוסס על נוהל מפת״ח.

18 חדר מחשב הוא מבנה המכיל ציוד שיש לשמרו בתנאים ייחודיים שאינם קיימים בסביבת עבודה משרדית (נוהל מפת״ח).

במישרין על הרצפה; בכניסה לחדר המחשב תותקן דלת אש תקנית[19] בעלת עמידות אש של 30 דקות לפחות; קירות חדר המחשב יהיו בנויים ללא פתחים; לא יאוחסנו בחדר המחשב חומרים דליקים, כגון קרטון.

משרד מבקר המדינה העלה כי רק אחת הרשויות המקומיות שנבדקו - עיריית יקנעם עילית - עומדת בדרישות התקן. בכל שאר הרשויות שנבדקו אין ניקוז לרצפה או "רצפה צפה"[20] או לא מותקנת דלת אש תקנית בכניסה לחדר המחשב. בעיריית אשקלון נמצא כי חדר המחשב משמש גם מחסן - הוא מכיל ארגזי קרטון רבים, ויש בו חלון גדול. גם ברשויות בני עי"ש ויהוד-מונוסון יש בחדר המחשב חלון חיצוני. ברשויות טירה ורמת ישי אין חדר מחשב.

לדעת משרד מבקר המדינה, ראוי שמשרד הפנים יכלול בהנחיות שיגבש עם הרשות למשפט, טכנולוגיה ומידע שבמשרד המשפטים גם הנחיות בנושא סיכוני האש והמים בחדרי המחשבים, בהתאם להוראות התקן שקבע מכון התקנים הישראלי, ויאכוף אותן. כמו כן, ראוי שהרשויות המקומיות שנבדקו יתקנו את המצב ויעמדו בדרישות התקן בכל הנוגע לחדרי מחשב.

4. **רישום מאגרי מידע אצל רשם מאגרי המידע**: חוק הגנת הפרטיות קובע שכל מאגר מידע המקיים את אחד מתנאי חוק זה חייב ברישום אצל רשם מאגרי המידע ברשות למשפט, טכנולוגיה ומידע[21]. כמו כן נקבעה בחוק זה חובת תשלום אגרה תקופתית בגין מאגר מידע הרשום בפנקס. עקב אי-תשלום אגרה, הרשם רשאי להתלות את תוקפו של הרישום לתקופה שיקבע או לבטל את רישומו של מאגר המידע בפנקס, בכפוף למתן זכות טיעון. מאגרי המידע של רשויות מקומיות שנדרש לרשמם כוללים, בין השאר, מאגרי מידע בתחומי השירות הפסיכולוגי החינוכי, הרווחה והארנונה.

משרד מבקר המדינה העלה כי הרשויות המקומיות בני עי"ש ורמת ישי לא רשמו מעולם את מאגרי המידע שלהן. הרשויות המקומיות יהוד-מונוסון, טירה ויקנעם עילית לא שילמו אגרות תקופתיות יותר משלוש שנים, ועקב כך נמחק רישום מאגריהן. רק מאגרי המידע של עיריות אשקלון ובני ברק היו רשומים ברשות למשפט, טכנולוגיה ומידע, כנדרש בחוק.

על הרשויות המקומיות בני עי"ש, רמת ישי, טירה, יקנעם עילית ויהוד-מונוסון להקפיד לרשום ולנהל את כל מאגרי המידע שברשותן כנדרש בחוק.

5. **אבטחת מידע במחשבים מנותקי רשת**: נוסף על המחשבים המחוברים לרשת, מחזיקות הרשויות המקומיות במחשבים אישיים, במחשבים ניידים, במחשבי כף יד, בטלפונים סלולריים חכמים וכו' (להלן - מחשבים מנותקי רשת); במקצתם נעשה שימוש בהתקני אחסון ניידים לסוגיהם.

מחשבי כף יד, טלפונים סלולריים ודומיהם מאפשרים סנכרון של יומן, ספר כתובות, רשימות ומחשבונים במכשיר קטן ונישא, לעומת יישומי מחשב כמו Outlook. ניתן לחבר מכשירים אלה למחשבים אחרים כמודם ולגלוש באמצעותם באינטרנט. בנוהל המסגרת נכתב כי לנוכח גודלו הפיזי של מחשב כף היד ולנוכח יכולתו "להתממשק" עם כל מחשב אישי ולהעביר קבצים ונתונים

---

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

20 רצפה מוגבהת המשמשת למעבר של כבלים, מערכות תקשורת, אוויר ממוזג, אספקת חשמל וצנרת כיבוי אש.

21 סעיף 8(ג) לחוק הגנת הפרטיות.

באופן דו-כיווני, נשקף סיכון ממשי לגנבת מידע ולהעברתו לידי גורמים בלתי מורשים. לכן חובה לאבטח את השימוש במחשבים אלה: יש להתקין בהם תכנה ייעודית שתדרוש סמה בכל פעם שמפעילים אותם.

עוד עולה מנוהל המסגרת כי התקן אחסון נייד (disk-on-key) מכל סוג שיאבד או ייגנב, יש סבירות גבוהה שייחשפו הנתונים המוזנים בו. לנוכח האמור לעיל, יש לנהוג בהתקן אחסון נייד כבכל דיסק קבוע אחר: יש לנהל רישום מסודר של מלאי ההתקנים הניידים, ובעת מסירתם לתיקון, למחיקה או להשמדה יש לוודא כי הספק הוא "ספק מורשה" אשר חתום על הסכם שמירת הסודיות. לגבי מחשבים מנותקי רשת, דיסקים נתיקים לסוגיהם והתקנים אחרים, יש לקבוע כללי אבטחה ומתכונת לגיבויָם.

ברשויות המקומיות שנבדקו לא נקבעו כללים לאבטחת המידע במחשבים מנותקי הרשת ובאמצעים הנתיקים האחרים שנעשה שימוש בהם, למעט בעיריית אשקלון - זו הוציאה נוהל לאבטחת המחשבים הניידים שבבעלותה. יצוין כי בינואר 2011 נגנב מאחד הפסיכולוגים בעיריית בני ברק מחשב נייד פרטי ובו מידע רגיש על מטופליו.

לדעת משרד מבקר המדינה, על הרשויות המקומיות לקבוע נהלים לאבטחת המידע ולהגנת הפרטיות למחשבים מנותקי רשת; לרבות מחשבי כף יד וכוננים נתיקים, ובכלל זה יש לקבוע את דרכי ההגנה על המידע הנאגר במחשבים אלה, כדי לצמצם את הסיכון שבגנבת הציוד - חשיפת המידע השמור בו ונגישות לרשת המשרד.

6. **תקצוב אבטחת מידע**: כל פעולה תקציבית ברשות המקומית משויכת לתקציב ייעודי. על פי נוהל המסגרת שיעורו של תקציב פעילות האבטחה של מערכי מידע קיימים צריך להיות לפחות 5% מהתקציב השנתי לרכישת חמרה, תכנה ותשתיות, להעסקת יועצים ולביצוע סקרים.

הביקורת העלתה כי ברשויות המקומיות שנבדקו לא נקבעו תקציבים ייעודיים לאבטחת מידע, למעט בעיריית אשקלון. עירייה זו קבעה לאבטחת המידע תקציב נפרד מתקציב מערכות המידע.

לדעת משרד מבקר המדינה, ראוי כי הרשויות המקומיות יתקצבו את אבטחת המידע בסעיף תקציב ייעודי בגלל הסיכונים לדליפת מידע או לשאיבת מידע על ידי גורמים שאינם מורשים לכך.

7. **תכנית שיקום מאסון ותכנית המשכיות עסקית**: תכנית שיקום מאסון (DRP) ותכנית המשכיות עסקית (BCP) הן תכניות פעולה לשעת חירום (אסון) שמכין ארגון כדי שבְּקרות אסון שיביא לקריסת המערכות יפעלו מערכות המידע הקריטיות שלו במהירות וביעילות ופעילותו תימשך. רשויות מקומיות שיש בהן מערכות מחשוב להפעלת רמזורים, לניהול מכוני מים וביוב או לשליטה בתאורת הרחובות נדרשות לספק שירותים אלה גם בשעת חירום.

ברשויות המקומיות שנבדקו אין תכניות שיקום מאסון ותכניות להמשכיות עסקית, פרט לעיריית אשקלון. עירייה זו הכינה תכנית שיקום מאסון והמשכיות עסקית, אולם במועד סיום הביקורת טרם סיימה את הפעלתה. לדעת משרד מבקר המדינה, ראוי כי הרשויות המקומיות ייערכו למצבי חירום בעזרת תכניות כאלה.

הטיפול ברשומות "מידע רגיש" ברשויות המקומיות

1. **פרסום נהלים והנחיות**: על הרשויות המקומיות לאבטח את המידע שלהן המאוחסן ברשומות מכל הסוגים. בתקנות הגנת הפרטיות[22] נקבע כי לכל מאגר המכיל מידע מוגבל יהיה קובץ נהלים, ובו יפורטו האמצעים לאבטחתו ולבקרת הטיפול הפיזי באמצעי האחסון שלו.

על פי נוהל המסגרת, הממונה על אבטחת המידע יקיים פעילויות בקרה וביקורת שנתיות כדי לבחון את אבטחת הרשומות ויעביר את ממצאיו לידיעת הממונה הישיר. כל עובד בארגון נושא באחריות אישית לאבטחת הרשומות שברשותו; אחריות כוללת לאבטחת רשומות רגישות מוטלת על המנהל הכללי. רשומות רגישות יישמרו בארון נעול בחדר שדלתו נעולה כאשר אין בו עובד; חלונותיו יהיו נעולים בכל עת שבה אין פעילות במשרד; יש לשמור על המסמכים או התיקים בגובה של 30 ס"מ לפחות מעל הרצפה; הוצאת רשומה מחוץ לכותלי הגוף הציבורי שלא למטרת תפוצה ומשלוח טעונה אישור מראש של הממונים.

הביקורת העלתה כי ברשויות המקומיות שנבדקו, פרט לעיריית אשקלון, אין הוראות ונהלים תקפים ומחייבים לאבטחת מידע פיזי: רשומות מכל הסוגים[23].

לדעת משרד מבקר המדינה, ראוי כי משרד הפנים יקבע עם הרשות למשפט, טכנולוגיה ומידע הנחיות לאבטחת מידע פיזי (רשומות) ויעגנן בנוהל מחייב, וכי הרשויות המקומיות יכינו נהלים פרטניים בהתאם לכך.

2. **מחלקות הגבייה**: מחלקות הגבייה ברשויות המקומיות עוסקות בגביית כספים - ארנונה, אגרות מים, אגרות שילוט, היטלי פיתוח ועוד. הרשויות המקומיות רשאיות להעניק הנחות בארנונה לעומדים בתנאים שנקבעו בתקנות ההסדרים במשק המדינה (הנחה מארנונה) התשנ"ג-1993, למשל לבעלי צרכים מיוחדים. כדי לקבל הנחה זו על מבקשה להציג לרשות המקומית מסמכים מהמוסד לביטוח לאומי המעידים על נכותו. מסמכים אלה מכילים מידע רגיש לפי חוק הגנת הפרטיות.

משרד מבקר המדינה בדק את אופן אבטחת המידע והגנת הפרטיות ביחידות הגבייה בשש רשויות מקומיות (טירה, אשקלון, בני ברק, יקנעם עילית, בני עי"ש ורמת ישי), ובבדיקתו הועלו ליקויים בנושאים אלה. להלן דוגמאות: תיקים עם מידע על תשלומי התושבים ועל חובותיהם לרשות המקומית וכן בקשות ואישורים למיניהם נמצאו מאוחסנים בכוננויות פתוחות במשרדי המחלקה; ארגזי קרטון ובהם מידע כזה נמצאו ללא השגחה במסדרון שבו עוברים מי שאינם מורשי גישה אליו; בחדרי העובדים שבהם מתקיימת קבלת קהל נמצאו ארונות שאי-אפשר לנעול אותם ובהם תיקים עם פרטים אישיים; נמצאו ארונות ללא מנעולים, והמידע המאוחסן בהם נגיש לכל מי שנמצא בחדר; תיקים של מחזיקים בנכסים, הכוללים דוחות מהביטוח הלאומי על מצב בריאותם, על הוראות קבע ועל בקשות להנחות - נשמרים בכוננויות ללא דלתות וללא מנעולים; בעיריית אשקלון נמצאה עמדת מחשב המחוברת לרשת העירייה שהייתה נגישה לכול, בייחוד משום שהיה אפשר להפעיל את המחשב ולעיין בכל מאגרי המידע המוזנים בו בהקשה של סמה פשוטה (רצף מספרים עולה) שאינה עומדת בדרישות התקן.

---

22 סעיפים 8-11.

23 רשומות על גבי אמצעים מגנטיים, אופטיים או על גבי ניירת.

משרד מבקר המדינה העיר לרשויות המקומיות שנבדקו כי אחסון מידע אישי הנוגע לבריאותם של התושבים או למצבם הכלכלי או האישי בארונות פתוחים, בכוננויות ובמגירות שאינן ניתנות לנעילה - אחסון כזה אינו עומד בדרישות הבסיסיות להגנה על מידע רגיש הנוגע לתושבים. הצבת מחשב המחובר לרשת העירייה בכניסה לאגף ההכנסות בעיריית אשקלון ללא השגחה יכולה לאפשר למי שאינם מורשים לכך להשתמש במחשבי העירייה, לשאוב מהם מידע, לגרום נזק למידע האגור בהם ולפגוע בפרטיות התושבים.

בתשובתה מספטמבר 2011 מסרה עיריית אשקלון כי מחשב זה הוסר.

לדעת משרד מבקר המדינה, ראוי שהרשויות המקומיות שנבדקו ינקטו לאלתר צעדים לאבטחת הרשומות האישיות ומערכות המידע המכילות מידע אישי.

3. **השירות הפסיכולוגי החינוכי**: בקוד האתיקה המקצועית של הפסיכולוגים בישראל משנת 2004 נקבע כי ה"פסיכולוגים ישמרו על סודיות ראויה בכתיבה, באחסון, בגישה, בהעברה ובשימוש ברישומים שבאחריותם, בין אם הם כתובים, בין אם הם מוקלטים ובין אם הם נמצאים בכל צורה אחרת".

משרד מבקר המדינה בדק את השירות הפסיכולוגי בשבע הרשויות המקומיות ומצא ליקויים בשש מהן; רק בשירות הפסיכולוגי בעיריית אשקלון לא נמצאו ליקויים. אלה הליקויים שהועלו ביתר הרשויות המקומיות שנבדקו: נמצאו חלונות ללא סורגים; תיקים אישיים המכילים מידע רגיש, לרבות אבחונים ודוחות על מצבם הרגשי של מטופלים נמצאו בכוננית פתוחה ובארונית נטולת מנעול; נמצא מחשב פועל ללא השגחה ובו קבצים הכוללים מידע רגיש על המטופלים; פסיכולוגים מקלידים דוחות על מטופליהם במחשבים שבבתיהם; כאמור בינואר 2011 נגנב מחשב נייד פרטי של פסיכולוג ובו מידע רגיש על מטופליו.

עוד נמצא ביחידות של השירות הפסיכולוגי ברשויות שנבדקו: מחשב המכיל חומר רגיש אינו מוגן בשם משתמש ובסיסמה, ולכן גם גורמים בלתי מורשים יכולים להגיע בקלות אל הדוחות הרגישים. המחשב מחובר לאינטרנט ללא אמצעי הגנה כך שהוא נתון לסכנת פריצה מרחוק ושליפת המידע המאוחסן בו; נמצא פתק שהוצמד לאחד המחשבים, ועליו נכתבו שם משתמש וסיסמה לתיבת הדואר האלקטרוני, דבר שיכול לאפשר לגורמים בלתי מורשים גישה למחשב ושאיבת מידע רגיש ממנו; במזכירות נמצא אלפון פתוח ובו פרטים אישיים של מטופלים: שמות ההורים, מספרי תעודות הזהות, דרכי התקשרות וכו'; למזכירת השירות הפסיכולוגי ידועים שם המשתמש והסיסמה של מנהלת השירות; בשירות פסיכולוגי מסוים באחת הרשויות כל ששת הפסיכולוגים משתמשים בשם משתמש ובסיסמה זהים.

משרד מבקר המדינה מעיר כי בגין השימוש של כל ששת הפסיכולוגים בשם משתמש ובסיסמה אחידים אי-אפשר כלל לעקוב אחר המשתמש האמִתי במחשב, ואבטחת המידע של הארגון נפגעת.

עוד מעיר משרד מבקר המדינה, כי מאחר שהפעלתן של יחידות השירות הפסיכולוגי החינוכי נמצאת באחריות הרשויות המקומיות, על הרשויות להנחות אותן בכל הנוגע לאבטחת מידע ולהגנת הפרטיות. כמו כן על הרשויות לפעול להטמעת הנהלים וההנחיות האמורים בקרב כל מאות העובדים בשירותים הפסיכולוגיים החינוכיים ולקיים בקרה שוטפת אשר תבטיח את יישומם של הנהלים וההנחיות.

עיריית יהוד-מונוסון מסרה בתגובתה על ממצאי הביקורת מאוקטובר 2011 כי "כיום, השירות הפסיכולוגי עבר לבניין מאובטח, חומרים אישיים הועברו לארכיב נעול ולכל פסיכולוג כיום קיים מחשב עם שם משתמש וסיסמא משלו".

אגפי החינוך ובתי הספר

1. משרד מבקר המדינה בדק את סוגיית אבטחת המידע והגנת הפרטיות באגפי החינוך בשתי רשויות מקומיות ובתשעה בתי ספר בשלוש רשויות ומצא את הליקויים האלה:

באגף החינוך של עיריית יקנעם עילית נמצא כי בחלק מהארונות ומהמגירות המכילים מידע רגיש אין מנעולים, ואלה שאפשר לנעול אותם - אינם נעולים; בחדר הדואר של המחלקה נמצאה כוננית דואר פתוחה שאינה ניתנת לנעילה, ובה בין השאר דוח על נפגעי תאונת דרכים. גם כוננית הדואר של מזכירות המחלקה - המכילה בין השאר מידע על תלמידים ואת פרטיהם האישים - פתוחה לכל באי החדר, ואי-אפשר לנעול אותה. המחלקה נמצאת בקומת הקרקע של מבנה העירייה, וכל חלונותיה אינם מסורגים.

באגף החינוך של עיריית אשקלון נמצאו קלסרים המכילים, בין השאר, מידע על סייעות ודוחות שכר בארונות שאין בהם דלתות כלל; נמצאו תלושי שכר של צוות בית הספר ודוחות על תלמידים בחלק מתאי הדואר של בתי הספר באגף החינוך שאין להם מנעול; נמצא מידע אישי על עובדי המחלקה בארוניות לא נעולות המכילות תיקיות, חלקן בעלות מנעולים אך לא נעולות וחלקן ללא מנעולים כלל; בארגזי קרטון נמצאו דוחות על מצב בריאותם של תלמידים המתגוררים מחוץ לרשות והזקוקים להסעות לבית ספר; במחלקת הנוער נמצא מידע על תלמידים בקלסרים המאוחסנים בארונות ללא מנעול.

משרד מבקר המדינה מעיר כי על הרשויות המקומיות להנחות את מחלקות החינוך בדבר אבטחת רשומות פיזיות ולוודא כי ההנחיות מולאו. יש לראות בחומרה את העובדה שמידע רגיש, כגון דוחות על מצב בריאות, אינו נשמר נעול. ראוי שהרשויות המקומיות יקבעו את הנחיותיהן על בסיס נוהל המסגרת.

2. חוזר מנכ"ל משרד החינוך מנובמבר 2009 "מאגרי מידע בבתי ספר - רישום, דיווח ואבטחת מידע" (להלן - חוזר מנכ"ל משרד החינוך) כולל הנחיות מפורטות ומקיפות בעניין אבטחת מידע, ועל בתי הספר לקיים הנחיות אלה. נקבעו בו הנחיות בדבר אבטחה פיזית של מידע השמור במחשבים ובעותקים מודפסים. באתר האינטרנט של מינהלת יישומי מנב"ס[24] של משרד החינוך פורסמה נורמה מחייבת בנושא אבטחת מידע; נורמה זו כוללת הוראות בדבר אבטחה פיזית וסימון של סוגי מדיה מגנטית וחומר מודפס: "דיסקטים וחומר מודפס המכילים מידע על הפרט יאוחסנו בכספת או בארון מתכת נעול... על כל דיסקט או אמצעי אחר לאחסון מידע, המכיל מידע על הפרט ירשם: 'מידע מוגן לפי חוק הגנת הפרטיות'. תדפיסי מחשב המכילים מידע על הפרט יכילו כתובת בולטת לעין בכל עמוד בנוסח: 'מכיל מידע מוגן לפי חוק הגנת הפרטיות; המוסרו שלא כדין עובר עבירה'".

---

24 מערכת ניהול בית ספר.

הנחיות משרד החינוך לאבטחת מידע נוגעות רק למאגרי מידע ולפלטי מחשב, אך לא לאבטחה פיזית של רשומות נייר, כגון מזכרים, תרשומות ודוחות שנוצרו בכתב יד, גם אם אלה מכילים מידע רגיש.

בתשובתו מאוקטובר 2011 השיב משרד החינוך, כי הוראות חוק הגנת הפרטיות, התשמ"א-1981, אינן חלות על מידע או על מאגרי מידע שאינם ממוחשבים, דוגמת רשומות נייר שנוצרו בכתב יד, ולכן מתוקף הוראות פרק ב' לחוק הגנת הפרטיות פרסם משרד החינוך הנחיות בעניין אבטחת מידע במאגרי מידע ושל פלטי מחשב ממאגרי מידע, אולם לא בכל הנוגע לרשומות שנוצרו בכתב יד.

3. (א) משרד מבקר המדינה בדק את אופן יישומו של חוזר מנכ"ל משרד החינוך בתשעה בתי ספר ברשויות יהוד-מונוסון, יקנעם עילית ואשקלון. מחוזר המנכ"ל עולה, בין השאר, כי על בתי הספר לרשום ברשות למשפט, טכנולוגיה ומידע שבמשרד המשפטים באמצעות משרד החינוך את כל מאגרי המידע שברשותם, לרבות מאגרי מידע מקומיים; מנהל בית הספר נושא באחריות לדווח למשרד החינוך על מאגרי המידע שבבית ספרו; ושימוש במאגר מידע שלא נרשם אסור על פי חוק ועלול להיחשב עברה פלילית.

משרד מבקר המדינה העלה כי משרד החינוך רשם רק חלק ממאגרי המידע של בתי הספר שנבדקו ברשות למשפט, טכנולוגיה ומידע, אף שהיה עליו לרשום את כולם.

לפי חוזר מנכ"ל משרד החינוך, על בית הספר לדווח למשרד החינוך בכל שנה עד נובמבר על מצבת מאגרי המידע של בית הספר.

משרד מבקר המדינה העלה כי תשעת בתי הספר שנבדקו לא מסרו למשרד החינוך דיווח עד המועד שנקבע.

במרץ 2009 החליט רשם מאגרי המידע ברשות למשפט, טכנולוגיה ומידע כי משרד החינוך אחראי למיפוי כל המאגרים בבתי הספר, ועליו להעביר את המידע במרוכז לרשם מאגרי המידע.

במועד סיום הביקורת ביולי 2011 עדיין לא סיים משרד החינוך את תהליך המיפוי של כלל מאגרי המידע של בתי הספר.

בתשובתו מאוקטובר 2011 השיב משרד החינוך, כי התחייב בפני הרשות למשפט, טכנולוגיה ומידע למפות את כלל מאגרי המידע אשר בבעלותו, אך מכיוון שהתבקש להעביר את הדיווחים בפורמט אלקטרוני ולא בדיווחים ידניים, הוא נאלץ לפתח מערכת, ופיתוחה הסתיים לפני כחצי שנה. בשנת הלימודים התשע"א נאסף דיווח מכ-3,200 בתי ספר, ופעולת המיפוי חודשה בשנת הלימודים התשע"ב. עוד הוסיף כי הסתיים פיתוח הממשק לייצוא הנתונים ולהעברתם לרשות למשפט, טכנולוגיה ומידע, ועתה הוא נבדק בדיקות סופיות. עם סיומן ואישור הממשק יחל משרד החינוך בהעברת המידע.

(ב) לפי סעיף 17ב לחוק הגנת הפרטיות, על משרד החינוך למנות בעלי תפקידים שיהיו אחראים להגנת הפרטיות ולאבטחת המידע במאגר המידע של מערכת המנב"ס ובמאגרי המידע המנוהלים בבתי הספר על כל היבטיהם. לנוכח זאת דרשה הרשות למשפט, טכנולוגיה ומידע שבמשרד המשפטים ממשרד החינוך במרץ 2009 למנותם.

משרד החינוך השיב באוקטובר 2011 כי על פי חוזר מנכ"ל שהוציא בנושא הרישום, הדיווח ואבטחת המידע, כל מנהל בית ספר מונה למנהל מאגרי המידע שבבית ספרו ולממונה על אבטחת המידע במאגרים אלה ועל יישום הוראות החוזר. הוא הוסיף כי דיווח בכתב למנהלים כי הם משמשים מנהלי מאגרי המידע לצורך הוראות חוק הגנת הפרטיות, וכי מינהל תקשוב ומערכות מידע במשרד החינוך מפקח על יישום הנוהל ומסייע ביישומו.

בעקבות תשובת משרד החינוך עשה משרד מבקר המדינה בירורים עם חלק ממנהלי בתי הספר שנבדקו. בדיקתו העלתה כי אף שבחוזר מנכ"ל משרד החינוך נקבע כי מנהל בית הספר הוא הממונה על אבטחת המידע במאגרים שבבית ספרו, ואף שחלקם אף חתמו על הצהרה כזו, הם אינם מודעים לתפקיד המוטל עליהם ולא קיבלו הדרכה בנושא. עוד נמצא כי מינהל תקשוב ומערכות מידע במשרד החינוך אינו מפקח על יישום הנוהל בבתי הספר ואינו אוכף אותו.

לדעת משרד מבקר המדינה, מאחר שכל מנהלי בתי הספר ממונים על אבטחת המידע בבתי הספר, ראוי כי יקבלו הדרכה בנושא אבטחת מידע ומאגרי מידע.

(ג) בחוזר מנכ"ל משרד החינוך נדרש כי סמאות הגישה יהיו חסויות, יימסרו רק למורשי גישה למאגר ויוחלפו פעמיים בשנה. אורך הסמה יהיה שישה תווים לפחות, והיא תכלול שילוב של מספרים ואותיות.

משרד מבקר המדינה העלה כי הוראה זו שבחוזר מנכ"ל משרד החינוך אינה מיושמת בכל בתי הספר שנבדקו. בחלק מבתי הספר נמצא כי סמאות למערכת המנב"ס מוחלפות רק פעם בשנה או בשנתיים, ובאחד מבתי הספר היא לא הוחלפה כלל במשך שנים.

(ד) בחוזר מנכ"ל משרד החינוך נקבע כי על מנהל בית הספר לקבוע נהלים בדבר תיוק פלטי מחשב ואחסונם בארון נעול.

משרד מבקר המדינה העלה כי בתשעת בתי הספר שנבדקו לא נקבעו נהלים כתובים בעניין.

(ה) בחוזר מנכ"ל משרד החינוך נקבע כי על מנהל בית הספר להיערך לשעת אסון באמצעות הכנת גיבויים במקום מאובטח ובחינה חד-שנתית של יישום ההיערכות. עוד נקבע כי גיבויים יבוצעו לפחות אחת לשבוע, יישמרו ארבעת הגיבויים האחרונים לפחות, יש לאחסן אותם בכספת המיועדת לכך, ויש לסמן מדיה מגנטית המכילה מידע בכיתוב "מידע מוגן לפי חוק הגנת הפרטיות".

משרד מבקר המדינה העלה כי בבתי הספר שנבדקו אין תכנית היערכות לשעת אסון, וכי המדיות המגנטיות אינן מסומנות בכיתוב הנדרש. אשר לתדירות ביצוע הגיבויים בבתי הספר, בחלק מבתי הספר נמצאו בין השאר הליקויים האלה: האמצעי שעליו מגובה המידע אינו נשמר בכספת, באחד מבתי הספר המזכירה שומרת אמצעי זה בתיקה האישי; חלק מהגיבויים מתבצעים אחת לחודש ואף אחת לחודשיים.

(ו) לפי חוזר מנכ"ל משרד החינוך, יש למפות ולסווג את מאגרי המידע השמורים בבית הספר ולקבוע את רמת החיסיון שלהם (למשל "בלתי מסווג" או "חסוי").

משרד מבקר המדינה העלה כי כל בתי הספר שנבדקו לא מיפו ולא סיווגו את מאגרי המידע שלהם.

(ז) בחוזר מנכ"ל משרד החינוך נקבע כי כל מנהל בית ספר יקבע בעל תפקיד לאחראי לענייני ניהול משתמשים, עדכון והחלפת סיסמאות, בקרה ודיווח על חריגים ויישום הנחיות הנוהל.

משרד מבקר המדינה העלה כי בשלושה בתי ספר לא קבע מנהל בית הספר אחראי לנושאים האמורים.

(ח) בחוזר מנכ"ל משרד החינוך נקבע בין השאר כי יש להתקין מערכות אל פסק (UPS), וכי יש לאבטח את החדר שבו נמצא המחשב נגד פריצה, וזאת על ידי דלת פלדלת, סורגים ואזעקה.

משרד מבקר המדינה העלה כי בארבעה מבתי הספר שנבדקו אין מערכת אל פסק, בחמישה אין דלת פלדלת ובשלושה אין סורגים.

(ט) בחוזר מנכ"ל משרד החינוך נקבע כי יש להתקין במחשבים תכנת אנטי-וירוס שתתעדכן פעם ביום באופן אוטומטי. פעם בחודש תבוצע בעזרת תכנת האנטי-וירוס בדיקה יזומה.

משרד מבקר המדינה העלה כי בבית ספר אחד תכנת האנטי-וירוס מתעדכנת רק פעם אחת בשנה, ובשלושה בתי ספר - באופן לא סדיר. בשום בית ספר שנבדק לא התקיימה בדיקה יזומה של המחשב בעזרת תכנת האנטי-וירוס.

בבירור שקיים משרד מבקר המדינה עם משרד החינוך בנושא יישום חוזר מנכ"ל משרד החינוך השיב משרד החינוך ביולי 2011 כי יישום הנוהל מוטל על מנהל בית הספר, וכי מינהל תקשוב ומערכות מידע במשרד החינוך מפקח על יישום הנוהל ומסייע ביישומו. הוא עושה זאת ישירות מול מנהלי בתי הספר באמצעות מינהלת המנב"ס.

באוקטובר 2011 השיב משרד החינוך למשרד מבקר המדינה, כי "על כל רשות מקומית מוטלת האחריות הבלעדית בכל הנוגע לרכישה, תחזוקה ובדיקה של מבנים וציוד פיזי בבתי הספר, לרבות אבטחתם הפיזית, פרסום הנחיות מקצועיות בנושאים אלה ווידוא כי הנחיות מולאו. משרד החינוך אחראי על אבטחת מידע והגנת הפרטיות במאגרי מידע אשר בבעלותו המצויים בבתי הספר אולם לא על רכישה ותחזוקה של הציוד הפיזי ואבטחתו, להם אחראית כאמור באופן בלעדי הרשות המקומית".

משרד מבקר המדינה מעיר כי על משרד החינוך, משרד הפנים והרשות למשפט, טכנולוגיה ומידע למפות את כלל החובות המוטלות על בתי ספר בתחום אבטחת המידע ולהגדיר באופן ברור את הגופים המופקדים על הפיקוח בתחום זה. תיאום זה נדרש בעיקר במקום שבו גופים שונים אחראים לפיקוח על נושאי טיפול שונים בתחום אבטחת המידע.

משרד הרווחה והשירותים החברתיים ומחלקות הרווחה ברשויות המקומיות

תקנון העבודה הסוציאלית (להלן - תע"ס) של משרד הרווחה והשירותים החברתיים (להלן - משרד הרווחה) הוא אוגדן של הוראות והודעות לעובדים במחלקות לשירותים חברתיים. הוראה בדבר "ניהול רשומות" בתע"ס עוסקת בנושא ניהול הרשומות, ובכלל זה בניהול רשומות שנוצרו באמצעים ממוחשבים במחלקות לשירותים חברתיים. בהוראה נקבע כי לפני שיצא העובד הסוציאלי מחדרו עליו לנעול את כל התיקים במגירת ארון תיקים ולשמור את המפתח במקום חסוי. עוד נקבע בה כי מאחר שדוחות מחשב מכילים מידע רב יש לשמור אותם בהתאם לכללי אבטחת מידע.

הוראה אחרת בתע"ס עוסקת בחובת הסודיות וקובעת כי תיקי הפונים ופלטי מחשב הכוללים נתונים אישיים שאינם בטיפול יישמרו בארונות או במגירות נעולים במשך יום העבודה. בסיום יום העבודה יינעל כל החומר שבטיפול ושאינו בטיפול. תיקי פונים שאינם פעילים יישמרו במגנזה במכלים סגורים מתאימים, ורק לעובדי המחלקה תתאפשר גישה אליהם. המפקחים במחוזות ועובדי האגף לביקורת פנימית במשרד הרווחה יפקחו על ביצוע ההוראות.

משרד מבקר המדינה בדק את אופן יישומן של הוראות תע"ס במחלקות לשירותים חברתיים בשש מתוך שבע הרשויות המקומיות שנבדקו (אשקלון, יהוד-מונוסון, בני ברק, טירה, יקנעם עילית ורמת ישי). בבדיקה הועלו הליקויים האלה: חלק מהמחלקות שוכנות בקומת הקרקע של מבנה העירייה, ולחלקן חלון או קיר זכוכית שקוף, שאינו מסורג הפונה לרחוב; בחדרים פתוחים ובלתי מאוישים של עובדים סוציאליים נמצאו תיקים אישיים על השולחנות ובארונות לא נעולים; במסדרון נמצא שק ובו חומר לגריסה הכולל דוחות ומידע רגיש שהיה נגיש לכל מבקרי המחלקה; בחדרי העובדים נמצאו תיקים ובהם מידע רגיש המאוחסנים בתיקיות ובארונות לא נעולים. עוד נמצא כי מחשבים של עובדים סוציאליים המכילים חומר רגיש נגישים ללא צורך בהקלדת שם משתמש וסיסמה; ארכיון של מחלקת רווחה הנמצא בקומה הראשונה של המבנה נמצא פתוח ונגיש לכל באי המקום; גם במסדרונות המבנה נמצאו ארונות לאחסון שאינם נעולים אף שהם מכילים חומר רגיש. יודגש כי במחלקות לשירותים חברתיים שברשויות המקומיות מתקיימת קבלת קהל באופן שוטף במשך היום.

הביקורת העלתה כי מפקחי משרד הרווחה אינם בודקים את אופן מילוי ההוראות במחלקות הרווחה ברשויות המקומיות. לא בוצעו ביקורות ייעודיות של האגף לביקורת פנימית במשרד לשירותים חברתיים בנושאים אלה. עוד נמצא כי הוראות "ניהול רשומות" אמנם קובעות כי יש לשמור דוחות הכוללים מידע לפי כללי אבטחת מידע, אך הן אינן מפרטות מהם כללים אלה ומה מתחייב מהם.

משרד מבקר המדינה מעיר כי הממצאים שהועלו במחלקות הרווחה בשש הרשויות שנבדקו מלמדים על ליקויים בתחום אבטחת המידע והגנת הפרטיות. הדבר מחייב את משרד הרווחה ואת הרשויות המקומיות להטמיע את הוראות תע"ס בקרב העובדים בשירותים הסוציאליים ולקיים בקרה על יישומם. כמו כן על הרשויות המקומיות לוודא כי יש בידי מחלקות הרווחה הציוד הנדרש להן כדי שיוכלו לעמוד בדרישות המוטלות עליהן, ובכלל זה ארונות עם מנעולים.

עוד מעיר משרד מבקר המדינה למשרד הרווחה כי עליו לקבוע כללים והנחיות מפורטים בנושא אבטחת מידע, וזאת מעבר לדרישות הכלליות המופיעות בהוראת "ניהול רשומות". לעניין זה, משרד הרווחה יכול להיעזר בנוהל המסגרת שהוציא האגף לביקורת המדינה במשרד ראש הממשלה.

משרד הרווחה הודיע בתשובתו מספטמבר 2011 כי האחריות להטמעתן של הוראות אבטחת מידע היא של הרשות המקומית.

משרד מבקר המדינה מפנה את תשומת לבו של משרד הרווחה לכך שבהוראות התע"ס נקבע באופן חד-משמעי כי את הבקרה השוטפת על יישום ההוראות יעשו המפקחים במחוזות ועובדי האגף לביקורת פנימית.

טיפול במידע היוצא מהרשות המקומית

1. **הסכמים בין הרשויות המקומיות לבין חברה א'**: חברה א' משמשת בית תכנה של השלטון המקומי. החברה מפתחת ומיישמת מערכות ממוחשבות ברשויות המקומיות ונותנת להן ייעוץ שוטף בכל הקשור לתכנון, להקמה ולהפעלה של מערכות מידע ביישובים. החברה מפעילה את אחת הרשתות הגדולות במדינה להעברת נתונים. ברשותה כ-80 מחשבים מקומיים המותקנים ברשויות המקומיות, ואלה משרתים כ-15,000 משתמשי קצה. המערכות שהחברה מספקת כוללים, בין השאר: מערכות גבייה ואוכלוסין, מערכות שכר ומערכות ניהול משאבי אנוש.

חברה א' מחזיקה במאגרי מידע של בעלים שונים, ובכללם שבע הרשויות שנבדקו. בחוק הגנת הפרטיות[25] נקבע כי המחזיק במאגרי מידע של בעלים שונים יבטיח כי אפשרות הגישה לכל מאגר תהיה נתונה רק למי שהורשה במפורש לעשות זאת בהסכם בכתב בינו ובין בעליו של אותו מאגר. מחזיק שברשותו לפחות חמישה מאגרי מידע החייבים ברישום ימסור לרשם מדי שנה רשימה של מאגרים אלה ויצרף לרשימה את שמות בעלי המאגרים, תצהיר על כך שנקבעו בעלי זכות הגישה לכל אחד מהמאגרים בהסכם שנקבע בין המחזיקים בו ובין בעליו, וכן שמו של הממונה על האבטחה. רק בשנת 2010 קיימה לראשונה חברה א' את חובתה כמחזיקה במאגרים של בעלים שונים ומסרה דיווח שנתי לרשות למשפט, טכנולוגיה ומידע.

משרד מבקר המדינה העלה כי לרשויות המקומיות רמת ישי, אשקלון ובני ברק אין כלל הסכם למתן שירות מחברה א'. המועצה המקומית בני עי"ש ועיריית טירה נמצאו במועד הביקורת לראשונה בעיצומו של מכרז לאספקת שירותי מחשוב הכולל דרישות לקיום הוראות חוק הגנת הפרטיות ואבטחת מידע. רק לרשויות יהוד-מונוסון ויקנעם עילית היו הסכמים המגדירים את האחריות לנושא אבטחת מידע הנדרשת מחברה א'. עוד העלה משרד מבקר המדינה כי כל שבע הרשויות המקומיות שנבדקו, שכאמור מאגריהן מוחזקים בידי חברה א', לא חתמו עמה על הסכמים לגבי המורשים לקבל גישה למאגרי המידע שלהן כנדרש בחוק הגנת הפרטיות.

2. **טיפול במאגרי מידע המוחזקים בידי גופים פרטיים**: רשויות מקומיות מתקשרות לעתים עם חברות חיצוניות כדי שיבצעו עבורן עבודות שונות. הרשויות מעסיקות חברות כאלה, בין היתר, לצורך הטיפול בגביית מסי עירייה. מחלקות הארנונה של הרשויות המקומיות טירה, יקנעם עילית ובני עי"ש מקיימות את עיקר פעולות הגבייה באמצעות חברה ב'.

---

25 סעיף 17א.

במרץ 2003 הוציא מנכ"ל משרד הפנים[26] נוהל בנושא העסקת חברות גבייה[27], ולפיו רשויות מקומיות רשאיות להעסיק חברות גבייה לצורך שליחת הודעות חיוב במסי עירייה, גבייה שוטפת של מסים אלו וגביית חובות שמקורם בפיגורים בתשלומיהם. חברות אלה צריכות לפעול לפי נוהל עבודה בכתב שיקבע גזבר הרשות, ובו יפורטו כל הפעולות שתבצע החברה והאישורים שיידרשו לכל פעולה. עוד נקבע בנוהל של מנכ"ל משרד הפנים, 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. עוד נקבע כי לפחות אחת לרבעון תגיש חברה ב' דוח מפורט על הפעולות שביצעה עבור הרשות.

משרד מבקר המדינה העלה כי בנוהל שהוציא משרד הפנים להעסקת חברות גבייה אין התייחסות לפעולות הנדרשות מן החברות לצורך אבטחת המידע המועבר אליהן.

בדיקת ההתקשרויות של שלוש הרשויות המקומיות המעסיקות את חברה ב' בתחום הגבייה העלתה כי במכרז בעיריית טירה שבו זכתה החברה לא הוזכר כלל נושא אבטחת המידע, ומכאן שהיא לא הוחתמה במסגרת המכרז על ההתחייבות הנזכרת בנוהל של מנכ"ל משרד הפנים. העירייה לא החתימה את חברה ב' ואת עובדיה על טופס הצהרת סודיות כלפי העירייה, אף שניתנה להם גישה מלאה למידע על התושבים. גם נוהל העבודה שנחתם בין עיריית טירה לחברה ב' אינו מתייחס לנושא אבטחת המידע.

למועצה המקומית בני עי"ש אין נוהל עבודה בכתב עם חברה ב' כנדרש על ידי משרד הפנים, והחברה לא הגישה דוחות אחת לרבעון. עם זאת, עובדי חברה ב' חתומים במסגרת ההסכם עם המועצה על טופס הצהרת סודיות, ונכללת בו התייחסות לחוק הגנת הפרטיות ולתקנותיו. אשר לחברה עצמה, אין בהסכם כל דרישה מפורשת ממנה לאבטחת המידע ולהגנת הפרטיות.

נמצא כי בהסכם בין עיריית יקנעם עילית לחברה ב' אין דרישה מהחברה בנושא אבטחת המידע והגנת הפרטיות. עובדי החברה חתמו על טופס הצהרת סודיות, וכן נחתם נוהל עבודה בין החברה לרשות.

על משרד הפנים לבחון האם יש צורך להוסיף לנוהל בנושא העסקת חברות גבייה הנחיות שיבטיחו שחברות הגבייה ינקטו פעולות ממשיות לאבטחת המידע שבידן וישתמשו בו בהתאם להוראות הדין. כמו כן יש להבהיר את אחריותן של הרשויות המקומיות לכך שהחברות שעמן הן יתקשרו יבצעו את פעולות האבטחה הנדרשות. זאת ועוד, על הרשויות המקומיות הפועלות באמצעות חברות גבייה למלא את הוראות הנוהל שנקבעו בעניין השימוש במידע ובעניין ההקפדה על סודיות.

3. **העברת מידע בין גופים ציבוריים**: לעתים גופים ציבוריים, ובכללם רשויות מקומיות, נדרשים להעביר מידע לגופים ציבוריים אחרים או לקבל מהם מידע לצורך עבודתם.

פרק ד' לחוק הגנת הפרטיות מסדיר מסירת מידע בין גופים ציבוריים וקובע מגבלות לעניין זה. הנושא הוסדר בהרחבה בתקנות הגנת הפרטיות. בתקנות אלו מפורטות ההוראות לניהול מאגר מידע, להעברת מידע בין גופים ציבוריים ולניהול מאגר המכיל מידע מוגבל, וכן מפורטים כללי

---

26 חוזר מנכ"ל 2/2003.

27 בעניין העסקת חברות גבייה ראו מבקר המדינה, **דוחות על הביקורת בשלטון המקומי**, שנת 2008, עמ' 425.

השימוש בו. בתקנות הגנת הפרטיות נקבעה החובה להקים בכל גוף ציבורי ועדה שתפקידה לדון בבקשות למסירת מידע שהגיש גוף ציבורי ולהחליט אם ובאיזו מידה להיעתר להן, וכן לבחון אם לאשר בקשות של אותו גוף ציבורי לקבלת מידע מגוף ציבורי אחר. כמו כן על הוועדה לקבוע הוראות בעניין הרשאות והגבלות הנוגעות לגישה למאגר המידע. בתקנות הגנת הפרטיות נקבע גם כי הגוף המוסר את המידע חייב לנהל רשימה של הגופים שהוא מוסר להם מידע דרך קבע, ובכלל זה סוג המידע הנמסר.

משרד מבקר המדינה העלה כי בשום רשות משבע הרשויות שנבדקו לא הוקמו ועדות למסירת מידע. בעיריית אשקלון מונתה ועדה כזאת רק במהלך הביקורת ביוני 2011.

באוקטובר 2011 השיבה עיריית בני ברק למשרד מבקר המדינה כי בעקבות הביקורת מונתה בעירייה בספטמבר 2011 ועדה למסירת מידע בין גופים ציבוריים. ועדה זו תשמש גם ועדת היגוי לנושא הגנת הפרטיות ואבטחת המידע במאגרי העירייה.

משרד מבקר המדינה מעיר כי על הרשויות המקומיות להקים ועדות ייעודיות לנושא העברת מידע בין גופים ציבוריים וכן לקבוע נהלים ייעודיים בנושא זה, כפי שנקבע בתקנות.

הדרכה וביקורת

1. **הדרכות והכשרות של עובדים בתחום אבטחת מידע:** הדרכת עובדים, ובייחוד עובדים חדשים, בנושאי אבטחת מידע נדרשת כדי להבטיח כי עובדי הארגון יהיו ערים לקיומם של גורמי סיכון בשימוש במערכות המידע ולחשיבות הפעולות לאבטחת המידע בארגון.

בנוהל המסגרת, שכאמור אינו חל על הרשויות המקומיות, נקבע כי הממונה על אבטחת מידע הוא האחראי לייזום פעילויות הדרכה והסברה בקרב כל העובדים בארגון, ובמסגרת הטמעת נושא אבטחת המידע בגופים ציבוריים יודרכו כל משתמשי המחשב לשמור בסוד את סיסמתם ולא להעבירה לאחר. כמו כן יודרכו המשתמשים להודיע לממונה על אבטחת מידע על כל חשד לחשיפת סיסמתם מיד לאחר שהתעורר חשדם. עוד נקבע בנוהל כי יוקצה תקציב הולם לפעילות ההדרכה; כי משתמשים יקבלו הדרכה בנושא נוהלי אבטחה ובנושא השימוש הנכון באפשרות לעיבוד מידע, כדי למזער סיכוני אבטחה אפשריים. נקבע גם כי לפני שיקבלו עובדי המשרד ומשתמשי צד שלישי הרשאת גישה למידע או לשירותים, הם יקבלו הדרכה נאותה ויעודכנו דרך קבע בנוגע לשיטות הפעולה ולנהלים של המשרד.

פעילויות הדרכה לעובדים בנושא אבטחת מידע יתבצעו, על פי נוהל המסגרת, פעם בשנה. את ההדרכה יארגן הממונה על אבטחת המידע בתיאום עם הממונה על ההדרכה. ימי עיון ייעודיים לעובדים חדשים או לעובדים שטרם קיבלו הדרכה בנושא אבטחת מידע יתואמו עם מחלקת ההדרכה. במהלך השנה תתבצע פעילות של רענון להגברת המודעות בנושא האבטחה. מדבקות ופלקטים מעוררי מודעות לנושאי האבטחה יפוזרו בקרבת מוקדים של מערכות ממוחשבות. 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 אירוע כזה בעתיד.

אם יתעורר חשד לעברה משמעתית או פלילית בנוגע לגילוי סודות או למסירת מידע שלא כדין, יש לדווח על כך מיד לסמנכ"ל בכיר למינהל.

ככלל, הרשויות המקומיות שנבדקו לא קיימו פעולות הדרכה והסברה בתחום אבטחת המידע. מקרב הרשויות המקומיות שנבדקו רק עיריית אשקלון הכינה תכנית הדרכה שנתית לאבטחת מידע וביצעה פעילות רענון להגברת המודעות בנושא האבטחה, ורק בה פועל ממונה אבטחת מידע המארגן את ההדרכות.

לדעת משרד מבקר המדינה, מן הראוי שהרשויות המקומיות יקיימו פעולות הדרכה והסברה בתחום אבטחת המידע בדומה לדרישות המפורטות בנוהל המסגרת.

2. **(א) הביקורת בתחום אבטחת המידע והגנת הפרטיות ברשויות המקומיות:** האגף לביקורת רשויות מקומיות במשרד הפנים מקיים ביקורות על הרשויות המקומיות. את הביקורות האלה מבצעות בעיקר שתי מחלקות: (א) מחלקת ביקורת ראיית חשבון בשלטון המקומי, האחראית למינוי רואי חשבון לביצוע ביקורות בשלטון המקומי. משרד הפנים מוציא מדי שנה עבור עובדי המחלקה הנחיות מקצועיות במסגרת "ספר ירוק", הכולל תכנית ביקורת שעל רואה החשבון לבצע ברשות המקומית. כמו כן בכל שנה נבחר נושא נוסף לביקורת של עובדי המחלקה, כגון תקציבים בלתי רגילים, שכר וכוח אדם; (ב) מחלקת ביקורת 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 ובגופים הנלווים לה, כגון חברות עירוניות וכלכליות, איגודי ערים וועדות מקומיות לתכנון ובנייה.

משרד מבקר המדינה העלה כי נושא אבטחת מידע והגנת הפרטיות לא נכלל כלל בתכניות הביקורת שנדרשו מרואי החשבון כנושאים לבדיקה ברשויות המקומיות. עוד הועלה כי מחלקת ביקורת מינהלית מעולם לא קיימה ביקורת בנושא זה.

משרד מבקר המדינה העיר למשרד הפנים כי ראוי שישקול בעתיד לשלב ביקורות הנוגעות לנושא אבטחת מידע והגנת הפרטיות.

משרד הפנים הודיע בתשובתו מנובמבר 2011 כי ישקול בעתיד לשלב גם ביקורות הנוגעות לנושא אבטחת מידע והגנת הפרטיות במסגרת הביקורות שעורך האגף לביקורת ברשויות המקומיות.

(ב) בפקודת העיריות [נוסח חדש] ובצו המועצות המקומיות (א), התשי"א-1950, נקבע כי הרשויות המקומיות ימנו מבקר. תפקידיו יהיו, בין היתר, לבדוק אם פעולות הרשויות נעשו כדין בידי הגוף המוסמך לעשותם, תוך שמירת טוהר המידות ועקרונות היעילות והחיסכון; לבדוק את פעולות עובדי הרשויות; ולבדוק אם הוראות הנוהל הנהוגות ברשויות עולות בקנה אחד עם הוראות כל דין ועם עקרונות טוהר המידות, היעילות והחיסכון.

התברר כי ברוב הרשויות המקומיות שנבדקו לא נעשו ביקורות ייעודיות בנושא אבטחת מידע והגנת הפרטיות. בעיריית יקנעם עילית נעשתה בשנת 2004 "ביקורת מערכות ממוחשבות" שכללה, בין השאר, היבטים שונים של נושא אבטחת מידע. גם בעיריית יהוד-מונוסון נעשתה ביקורת אבטחת מערכות מידע בחודשים דצמבר 2010 עד מרץ 2011, זאת במהלך הביקורת של משרד מבקר המדינה.

מתשובת עיריית אשקלון מספטמבר 2011 עולה כי יועץ חיצוני מטעם הממונה על אבטחת מידע בעירייה עשה ביקורת אבטחת מידע בשירות הפסיכולוגי החינוכי ובאגף הרווחה שלה והגיש המלצות בנושא.

לדעת משרד מבקר המדינה, ראוי כי המבקרים שמונו ברשויות המקומיות ישקלו - תוך התייעצות עם ראשי הרשויות המקומיות - לעשות ביקורות גם בנושא אבטחת מידע. בין השאר יש לשקול קיום ביקורות שבמסגרתן ימופו הסיכונים שמקורם במחשוב בכל תחומי הפעילות של הרשות תוך התייחסות גם לתחום האבטחה הפיזית.

סיכום

מממצאיו של דוח זה מסתמן כי לרשויות המקומיות עדיין חסרה התשתית לטיפול בנושא אבטחת המידע והגנת הפרטיות. ברוב הרשויות שנבדקו אין הנחיות מפורטות לטיפול שוטף בנושא; רובן פועלות ללא ממונה על אבטחת מידע כנדרש בחוק; מאגרי המידע שבהן אינם רשומים כנדרש; היקף פעולותיהן בתחומי ההדרכה והביקורת מצומצם.

על הרשויות המקומיות: לקיים פעולות בקרה בעניין אבטחת המידע והגנת הפרטיות, כדי לזהות פעולות חריגות או ניסיונות של גורמים בלתי מורשים לעשות פעולות כאלה; למנות לאלתר ממונים על אבטחת מידע כמתחייב מחוק הגנת הפרטיות; לגבש מסמך מדיניות בנושא אבטחת מידע, ולקבוע בו את תדירות ביצועם של סקרי סיכונים ומבחני חדירה; להקפיד לרשום ולנהל את כל מאגרי המידע שברשותן כנדרש בחוק; להקים ועדות להעברת מידע ולהכין נהלים ייעודיים בנושא העברת מידע בין גופים ציבוריים כפי שנקבע בתקנות הגנת הפרטיות; לעשות ביקורות על אבטחת מידע ועל הגנת הפרטיות ברשויות המקומיות באמצעות מבקרי הרשויות.