ביקורת מערכות מידע

ניהול מערכות מידע ברשויות המקומיות

ניהול מערכות מידע ברשויות המקומיות

רקע

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

נתוני מפתח

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

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

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

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

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

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

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

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

פעולות הביקורת

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

תמונת המצב העולה מן הביקורת

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

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

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

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

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

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

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

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

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

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

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

עיקרי המלצות הביקורת

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

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

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

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

התרשים בעיבוד משרד מבקר המדינה.

סיכום

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

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

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