דוח מבקר המדינה

אבטחת המידע והגנת הסייבר ברשות מקרקעי ישראל

אייר התשפ"ד | מאי 2024

אבטחת המידע והגנת הסייבר ברשות מקרקעי ישראל

מבוא

רשות מקרקעי ישראל (להלן - רמ"י) מופקדת על ניהול מקרקעי ישראל על פי חוק רשות מקרקעי ישראל, התש"ך-1960, כמשאב, לשם פיתוחה של מדינת ישראל ולטובת הציבור, הסביבה והדורות הבאים. פעילויותיה של רמ"י בתחום ניהול מקרקעי ישראל הן בין היתר תכנון, שיווק, ופיתוח של המקרקעין; שמירה ופיקוח על המקרקעין; קידום הרישום של הזכויות במקרקעין ומתן שירותים לבעלי הזכויות ככל הנדרש, לצורך ניהול זכויותיהם או מימושן.

לצורך ניהול פעילויותיה רמ"י משתמשת בעשרות מערכות מידע שונות, הכוללות מאות עד אלפי תחנות עבודה נייחות ניידות, שבהן משתמשים אלפי עובדים (כולל עובדים במיקור חוץ). כמו כן, רמ"י מפעילה אתר מרשתת (אינטרנט), ובאמצעותו היא נותנת שירות לציבור. מאות אלפי כניסות לאתר נעשות בכל חודש, ויותר עשרות אלפי רבות של הורדות של קבצים נעשות בכל שנה. מערכות המידע של רמ"י כוללות מאות שרתים, שבהם מאוחסנים מיליוני תיקים סרוקים. התיקים הסרוקים כוללים מיליוני תיקי מסמכים, הנוגעים בעיקרם לענייני הזכויות על מקרקעי ישראל, ובהם חוזי חכירה, אישורי תשלומים, דוחות פיקוח וכיו"ב.

משנת 2020 מטמיעה רמ"י במרחבים הגיאוגרפיים שלה מערכת מידע מרכזית חדשה - רמיטק, המערכת תומכת בכל תהליכי העבודה ברמ"י, ורמ"י מבצעת באמצעותה את כלל פעולותיה. רמיטק כוללת כמה מערכות משנה: מערכות ליבה, כגון מערכות לניהול ספר הנכסים, לניהול עסקות מקרקעין ולניהול הכספים; ערוצי שירות דיגיטליים, כגון אתר המרשתת והאזור האישי; ומערכת ניהול מסדי נתונים ובינה עסקית (BI[1]).

בכל הנוגע להגנת הפרטיות ולאבטחת המידע הרב שבידיה, רמ"י נדרשת לפעול בהתאם להוראות הדין, ובהן חוק הגנת הפרטיות, התשמ"א-1981 (להלן - חוק הגנת הפרטיות), והתקנות שהותקנו על פיו. כמו כן נדרשת רמ"י לפעול על פי החלטות ממשלה; הנהלים הפנימיים של רמ"י; והנהלים וההנחיות של הגופים האסדרתיים בנושא, ובהם היחידה להגנת הסייבר בממשלה (להלן - יה"ב), שהיא הגוף המנחה מקצועית את משרדי הממשלה ויחידות הסמך (ובהן רמ"י) בתחום הגנת הסייבר[2].

בשנת 2022, תקציב אבטחת מידע וסייבר של רמ"י מתוך התקציב עבור הוצאות מחשוב עמד על כ-12%.

רוב המידע שרמ"י אוספת, שומרת ומנהלת הוא מידע רגיש על נכסי מקרקעין, הכולל נתונים אישיים ועיסקיים והוא כולל מיליוני רשומות. תקנות הגנת הפרטיות (אבטחת מידע), התשע"ז-2017 (להלן - תקנות הגנת הפרטיות או התקנות), קובעות לגבי מאגר מידע גדול כי על מאגר מידע הכולל מידע על אודות 100,000 אנשים ומעלה חלה חובת "רמת האבטחה הגבוהה"[3]. לפי חובת "רמת האבטחה הגבוהה", על רמ"י חלה החובה לשמור על המידע שברשותה ולוודא שהוא משמש אך ורק למטרות שלשמן הוא נמסר או לצורכי מילוי חובותיה על פי החוק. בנוגע לנכסי המקרקעין, רמ"י נדרשת להגן על סודיות המידע, אמינותו, זמינותו ומהימנותו, ועליה לוודא כי הנתונים לא ישונו או יימחקו, וכי הם ייחשפו רק למי שמורשה לגשת אליהם מתוקף תפקידו או מתוקף היותו הגורם שהמידע נוגע לו.

---

1 Business Intelligence - BI - הוא תחום בטכנולוגיית המידע העוסק בבניית מערכות העוזרות לארגון להפיק מידע חשוב מבחינה עסקית מתוך מכלול הנתונים שהוא אוסף. מערכות הבינה העסקית מספקות מידע היסטורי, מידע עכשווי ותחזיות בנוגע לפעילות העסקית, ובעזרתן ניתן לאתר דפוסים חיוניים לניהול של ארגון וליצור דוחות והתראות לצורך קבלת החלטות ניהוליות.

2 היחידה פועלת במסגרת מערך הדיגיטל הלאומי, שמשמש גוף המטה הטכנולוגי של משרדי הממשלה והגופים הציבוריים ופועל לשיפור הממשק והשירות הממשלתי עבור התושבים והעסקים בישראל.

3 התוספת השנייה (תקנה 1) לתקנות הגנת הפרטיות (אבטחת מידע), תשע"ז-2017.

מערך הדיגיטל הלאומי, שבמסגרתו פועלת גם יה"ב, מפעיל מרכז שליטה ובקרה ממשלתי בנושא איומי סייבר - SOC ממשלתי (SOC - Security Operation Center) - העוסק בגיבוש תמונת מצב ממשלתית שוטפת בהיבטי הגנת סייבר ובמתן מענה לאירועי סייבר.

פעולות הביקורת

בחודשים פברואר עד אוקטובר 2023 בדק משרד מבקר המדינה היבטים בתחום אבטחת המידע וההגנה על הפרטיות במערכות המידע ברמ"י. הבדיקה בוצעה ברמ"י, ובין היתר נבדקו הנושאים האלה: ממשל וניהול של אבטחת מידע וסייבר; רישום מאגרי המידע; ותוכניות להמשכיות תפקודית ולהתאוששות מאסון. ועדת המשנה של הוועדה לענייני ביקורת המדינה של הכנסת החליטה שלא להניח דוח זה במלואו על שולחן הכנסת אלא לפרסם רק חלקים ממנו, לשם שמירה על ביטחון המדינה, בהתאם לסעיף 17 לחוק מבקר המדינה, התשי"ח-1958 [נוסח משולב].

ממשל וניהול של אבטחת המידע

אחד העקרונות המרכזיים בתחום אבטחת המידע בארגונים הוא מדיניות וממשל בתחום מערכות המידע בכלל (IT Governance) ובתחום אבטחת המידע בפרט. מונח זה נוגע לתהליך התאגידי שבאמצעותו הנהלת הארגון מוודאת כי מערכות המידע תומכות ביעדים המקצועיים והעסקיים של הארגון, ובה בעת שהסיכונים הרבים הכרוכים בשימוש במערכות מנוהלים כראוי[4]. ביטוי לתהליך נדרש זה בכל הנוגע לגופי הממשלה ניתן בין היתר בהחלטת הממשלה 2443 משנת 2015 בנושא "קידום אסדרה לאומית והובלה ממשלתית בהגנת הסייבר" (להלן - החלטת הממשלה 2443)[5], בהחלטת ממשלה 2444 משנת 2015[6] בנושא "קידום ההערכות הלאומית להגנת הסייבר", בה קבעה הממשלה כי ההגנה על תפקודו התקין והבטוח של מרחב הסייבר מהווה יעד בטחוני לאומי חיוני של המדינה, ובהנחיות של יה"ב, כמפורט להלן.

ועדת היגוי לנושאי הגנת הסייבר

בהחלטת הממשלה 2443 נקבע בין היתר כי על משרדי הממשלה ויחידות הסמך, ובהן רמ"י, להקים ועדת היגוי משרדית לנושא הגנת הסייבר שתפעל לשיפור רמת הסייבר של המשרד או היחידה (להלן - הארגון) ותפקח על הפעילות השוטפת המבוצעת בארגון בנושא זה (להלן - ועדת היגוי סייבר). להלן בתרשים מבנה ועדת ההיגוי של רמ"י.

---

4 ראו מבקר המדינה, **דוח מבקר המדינה - מאי 2022**, "הגנת סייבר על מכשירים רפואיים ואבטחת המידע הנאגר בהם", עמ' 1168.

5 החלטת הממשלה 2443 מ-15.2.15.

6 החלטת הממשלה 2444 מ-15.2.15.

תרשים 1: **מבנה ועדת היגוי סייבר של רמ"י**

המקור: הנחיית יה"ב 5.2.

על פי הנחיית יה"ב 5.2 "הנחיית מסגרת להגנת הסייבר בממשלה[7]" (להלן - הנחיית יה"ב 5.2), תפקידי ועדת היגוי סייבר הם בין היתר אלה: אישור או אשרור של מדיניות הגנת הסייבר בארגון; אישור, מיפוי וסיווג של נכסי המידע של הארגון; בחינה, תיקוף ואישור של מפת הסיכונים הארגונית, כפי שהיא עולה מסקר הסיכונים הארגוני, כנדרש על פי תורת ההגנה בסייבר[8] לגבי ארגון של מערך הסייבר הלאומי[9] (להלן - תורת ההגנה בסייבר); אישור תוכנית העבודה בתחום הגנת הסייבר ובקרה על יישומה; התעדכנות בסיכונים ובאיומים הנוגעים לארגון; פיקוח על ניהול סיכוני הסייבר המבוצע בארגון; ניהול התגובה וההתאוששות. כמו כן[10], על הוועדה לגבש מדדים כמותיים בנושאי הגנת הסייבר ולהגדיר יעדים כמותיים אשר באמצעותם ניתן יהיה למדוד ולבחון את רמת האפקטיביות של הגנת הסייבר, וכן לבחון את מידת העמידה ביעדים פעם בחצי שנה, במסגרת סקר ההנהלה.

בביקורת נבדק אם הפעילות של ועדת היגוי סייבר ברמ"י היא בהתאם לנדרש ממנה בהחלטת הממשלה 2443 ובהנחיות יה"ב. להלן הממצאים:

מיפוי וסיווג של נכסי המידע

לפי תורת ההגנה בסייבר, על ארגון שיש לו פוטנציאל גבוה להיפגע בעקבות אירוע סייבר למפות את נכסיו (ובהם יישומונים ארגוניים, תשתיות ממוחשבות ורשת הארגון), את ייעודם ואת הממשקים של כל נכס. בסוף שלב זה ידע הארגון להגדיר לאילו מנכסיו יש חשיבות רבה מבחינת תפקודו, ואילו מנכסיו הם נכסים משניים, והדבר יסייע לארגון להגן על הנכסים בהתאם לנזקים האפשריים. על פי הנחיית יה"ב 5.2, אחד השלבים הראשונים וההכרחיים בקביעת מדיניות הגנת סייבר ויישומה הוא מיפוי וסיווג של נכסי המידע של הארגון. זאת בין היתר כדי שתוכנית העבודה לניהול הגנת הסייבר של הארגון (ראו להלן) תהיה מותאמת לרמת הסיכון של כל מערכת. בהנחיה נקבע כי באחריות ועדת היגוי סייבר לאשר, למפות ולסווג את נכסי המידע של הארגון, ובכללם את נכסי התוכנה, את מערכות המידע והיישומים ונכסי המידע האגורים בהם ואת נכסי המידע הפיזיים. רשימת המצאי של הנכסים צריכה לכלול בין היתר את פרטי הנכס, בעליו ורמת הקריטיות שלו. זאת בהתאם לרגישות המידע וחיוניותו ולפי מידת הנזק שייגרם לארגון ולמדינה עקב חשיפת המידע של הארגון, מאגריו או מערכותיו, חבלה בהם, מחיקתם או שיבושם, בין במזיד ובין בשוגג.

במהלך הביקורת העבירה רמ"י לבקשת משרד מבקר המדינה רשימה, ובה מפורטות מערכות המידע שלה (עשרות מערכות מידע הכוללות עשרות תתי-מערכות). לגבי כל מערכת מפורט ברשימה כדלהלן: תיאור המערכת; האחראים למערכת ברמ"י, ובכלל זה הרפרנט באגף מערכות מידע ומחשוב (להלן - אגף מערכות מידע) האחראי למערכת; השייכות של מערכת המידע למאגר המידע הקיים ברמ"י. ברשימה ניתן ציון לרמת הסיכון הכללית של המערכת (גבוהה, בינונית או נמוכה), המבוסס על שקלול רמות הסיכון בנושאי סודיות, זמינות ואמינות של המערכת.

7 סעיף 6.1.4.4

8 תורת ההגנה בסייבר היא מדריך יישומי להגנת הסייבר של ארגון שנכתב על ידי מערך הסייבר הלאומי (עדכון אחרון של המדריך פורסם ביוני 2021).

9 המערך הוא גוף ממלכתי, מבצעי וטכנולוגי האמון על הגנת מרחב הסייבר הלאומי ועל קידום העוצמה של ישראל בתחום וביסוסה. המערך פועל מתוקף החלטות הממשלה ומתוקף החוק להסדרת הבטחון בגופים ציבוריים, התשמ"ח-1998.

10 סעיף 5.5

בביקורת עלה כי מאז התכנסה ועדת היגוי סייבר לראשונה בשנת 2017, היא לא פעלה לאישור, מיפוי וסיווג של נכסי המידע של רמ"י. מסקירת דיוני הוועדה שהתקיימו בשנים 2017 - 2022 עלה כי אגף מערכות מידע הציג לפני הוועדה נתונים כלליים על המידע ברמ"י ועל רמות הסיווג הפוטנציאליות, אך לא הובא לאישורה מיפוי של כלל נכסי המידע של רמ"י (דוגמת הרשימה שהועברה למשרד מבקר המדינה), כנדרש בהנחיית יה"ב, והוועדה מצידה לא דרשה זאת.

עקב כך נפגעת יכולתה של הנהלת רמ"י לבצע בקרה מיטבית על היעילות והאפקטיביות של יישום הגנת הסייבר ברמ"י ועל מידת התאמתה של תוכנית העבודה לניהול הגנת הסייבר של רמ"י לרמת הסיכון של כל מערכת.

על רמ"י להביא לאישור ועדת היגוי סייבר את המיפוי והסיווג של נכסי המידע של רמ"י.

בתשובתה מינואר 2024 (להלן - תשובת רמ"י) מסרה רמ"י כי המיפוי והסיווג של נכסי המידע שלה יובאו לאישור ועדת ההיגוי בישיבתה הבאה.

גיבוש מפת הסיכונים הארגונית ואישורה

על פי הנחיית יה"ב 5.2, על ועדת היגוי סייבר לבחון, לתקף ולאשר את מפת הסיכונים הארגונית כפי שהיא עולה מסקר הסיכונים הארגוני, כנדרש בתורת ההגנה בסייבר.

על פי תורת ההגנה בסייבר, על רמ"י לבצע תהליך הערכה וניהול של סיכונים, ובאמצעותו להגדיר את מפת הסיכונים הארגונית ואת הבקרות הנדרשות להפחתת סיכונים אלו, לרבות סדרי העדיפויות בנדון. בקרות אלו יהוו בסיס לבניית תוכנית העבודה, להקצאת המשאבים ולהיערכות הארגונית בהתאם.

בישיבת ועדת היגוי סייבר של רמ"י שהתקיימה בשנת 2017 סוכם כי רמ"י תבצע סקר סיכונים על בסיס מתאר האיומים הקיימים ותקדם טיפול בליקויים שיעלו. ועדת ההיגוי קבעה כי תוצאות סקרי הסיכונים והטיפול בליקויים יוצגו לוועדת ההיגוי במחצית השנייה של שנת 2017.

עלה כי לפני רמ"י עומדים איומים פנימיים, למשל מצד ספקים שיש לה איתם קשר, ואיומים חיצוניים, דוגמת פצחנים (האקרים) ולקוחות.

תהליך ניהול סיכוני סייבר ברמ"י

בהנחיית יה"ב 5.3 בנושא "ניהול סיכוני סייבר במשרדי ממשלה"[11] (להלן - הנחיית יה"ב 5.3) נקבע כי על ארגוני הממשלה, ובהם רמ"י, לבצע תהליך ניהול סיכוני סייבר. תהליך זה מורכב מארבעה שלבים עיקריים: זיהוי הסיכונים; הערכתם; קביעת אופן הטיפול בהם; והטמעת תוכנית עבודה להפחתתם.

עוד נקבע בהנחיית יה"ב 5.3 כי סקר הערכת סיכונים יכלול את השלבים העיקריים האלה: תוכנית לביצוע סקר, כולל משאבים לביצועה; מיפוי וקטלוג של תהליכים ונכסי מידע; הגדרת רמת הערך לארגון של התהליכים והנכסים; מיפוי מערכות הגנה ובקרות קיימות וקביעת רמת עדכניותן ונחיצותן; מיפוי וניתוח של פגיעויות ואיומים; קביעת רמת ההגנה הנדרשת; התאמת האמצעים לטיפול בסיכונים - הכנת תוכנית למזעור נזקים; והפצת דוח מסכם שיוגש לאישורו של ממונה הגנת הסייבר[12].

על פי הנחיית יה"ב 5.3, דוח הערכת הסיכונים שיוגש ישמש המלצה מקצועית לארגון ויהיה בסיס לתוכנית עבודה מתועדפת להתמודדות עם הסיכונים שהתגלו. התוכנית תוגש לוועדת היגוי סייבר לקבלת אישורה ותכלול לכל הפחות תוכנית הפחתת סיכונים - תכולה, לוחות זמנים לביצוע, אחריות

11 מ-10.7.17, תאריך עדכון 16.9.18, גרסה 2.0.

12 ממונה הגנת הסייבר אחראי להבטחת התכנון, הניהול, הטיפול והבקרה במכלול היבטי הגנת הסייבר בארגון.

ומשאבים נדרשים. עוד נקבע בהנחיה כי יש לבצע את סקר הסיכונים פעם בשלוש שנים ולתקפו לפחות אחת לשנה וחצי. במקרים מיוחדים, למשל מקרים שבהם התרחש שינוי ניכר בסביבה הטכנולוגית או התהליכית, יש לבצע סקר נוסף.

בשנים 2017 - 2022 ביצעה רמ"י עשרות סקרי סיכונים ומבדקי חדירה למערכות המידע שלה.

הביקורת העלתה כי אף שבוצעו סקרי סיכונים רבים, דבר שיש לראותו בחיוב, לא התקיימו דיונים בוועדת היגוי סייבר לגבי הסיכונים שנמצאו, והדרכים להפחתתם, ובכלל זה תכולות עבודה להתמודדות עם הסיכונים, לוחות זמנים לביצוע, אחריות ומשאבים נדרשים. על כן לא מוצתה התכלית של סקרי הסיכונים - זיהוי של מפת הסיכונים הארגונית וקבלת החלטות על פעולות שיש לנקוט כדי להיערך כראוי לקראתם, למנוע את התרחשותם או למזער את הנזק שייגרם אם הסיכונים יתרחשו.

רמ"י מסרה בתשובתה כי מיפוי הסיכונים הוצג למנהל רמ"י ויוצג לוועדת ההיגוי בישיבתה הבאה.

סקר סיכונים למערכות הליבה החדשות: בישיבה שהתקיימה במאי 2019 אישרה ועדת היגוי סייבר ברמ"י לבצע סקר סיכונים לגבי מערכות הליבה החדשות של רמ"י.

הביקורת העלתה כי אגף מערכות מידע ביצע בשנת 2019 סקר סיכונים ואולם ועדת היגוי סייבר לא דנה בסיכוני אבטחת המידע ובליקויים שהועלו בסקר זה. מדובר בסיכונים שוועדת ההיגוי לא נתנה את דעתה עליהם ולא פיקחה על גיבוש ויישום של התוכנית למזערם.

עוד עלה כי רמ"י לא ביצעה סקרי סיכונים למערכת מסוימת, למעט סקר סיכוני הקמה משנת 2019 שצוין לעיל.

באפריל 2023 מסרה רמ"י למשרד מבקר המדינה כי תבצע סקרי סיכונים למערכות הליבה החדשות שלה בשנת 2023. במועד סיום הביקורת, אוקטובר 2023, לא התקבלו התוצאות של סקרי סיכונים כאמור.

בתשובתה מינואר 2024 ציינה רמ"י כי סקרי הסיכונים יוצגו לוועדת ההיגוי בישיבתה הבאה. בתשובה מפברואר 2024 הוסיפה רמ"י כי בוצע סקר סיכונים בנוגע למערכות הליבה, וטיוטת דוח בעניינו נבחנת על ידי הצוותים המקצועיים.

סקרי הנהלה

בהנחיית יה"ב 5.2[13] נקבע כי על ועדת היגוי סייבר ליזום ביצוע של סקרי הנהלה, כדי לבדוק את מידת הישימות והביצוע של הפעולות המוגדרות למערכת ניהול הגנת הסייבר בארגון, לבחון את ממצאי הסקרים ולשקול הטמעה של ההמלצות וביצוע שינויים רלוונטיים. עוד נקבע כי על הוועדה לגבש מדדים כמותיים ולהגדיר יעדים כמותיים בנושאי הגנת הסייבר אשר באמצעותם ניתן יהיה לבחון ולמדוד את רמת האפקטיביות של תשתית הגנת הסייבר, וכן לבחון את מידת העמידה ביעדים פעם בחצי שנה במסגרת סקר ההנהלה.

בביקורת עלה כי ועדת היגוי סייבר ברמ"י לא יזמה ולא גיבשה סקרי הנהלה כנדרש, ומשכך אלה לא בוצעו. עקב כך נפגעת היכולת לבדוק את מידת הישימות והביצוע של הפעולות המוגדרות למערכות האמונות על הגנת הסייבר ברמ"י.

על ועדת היגוי סייבר ליזום ולגבש סקרי הנהלה כנדרש.

קביעת מדדים בנושא הגנת סייבר

[13] סעיף 6.3.1.

בישיבתה במאי 2019 אישרה ועדת היגוי סייבר ברמ"י עשרה מדדי אב בנושאי הגנת סייבר, ולכל נושא נקבעו מדדים כמותיים. לדוגמה, מדד שנקבע לנושא מודעות אבטחת מידע הוא כי על 80% מהעובדים להשתתף בהדרכות אבטחת מידע. מדד שנקבע בנושא התקנת תוכנת אנטי-וירוס הוא כי התוכנה תותקן ב-100% מעמדות הקצה, מהמחשבים הניידים ומהשרתים. עוד נקבע כי מידת עמידת רמ"י במדדים שאושרו תוצג בישיבתה הבאה.

בביקורת עלה כי משנת 2019 ועד למועד סיום הביקורת, אוקטובר 2023, תקופה של יותר מארבע שנים, הוועדה בחנה את מידת היישום של המדדים פעמיים בלבד (בדצמבר 2019 ובדצמבר 2022), ולא בכל חצי שנה כנדרש. עקב כך נפגעה יכולתה לבחון את רמת האפקטיביות של תשתית הגנת הסייבר, ובהתאם לכך לבצע שינויים רלוונטיים בתכיפות רבה יותר כנדרש.

עלה כי בדיוני ועדת היגוי סייבר שהתקיימו בדצמבר 2019 ובדצמבר 2022 הוצגו לוועדה רק חלק ממדדי האב שאושרו במאי 2019. בדצמבר 2019 הוצגו לוועדה שישה מעשרת המדדים שאושרו (כ-60%), ובדצמבר 2022 - חמישה בלבד (כ-50%). יצוין כי לפי המוצג לוועדה, מידת העמידה במדדים שכן נבדקו הייתה מלאה. עוד עלה כי הוועדה לא דנה בעניין אי-הצגתם של יתר המדדים שאושרו. יוצא אפוא כי בחינת רמת האפקטיביות של תשתית הגנת הסייבר באמצעות המדדים הייתה חסרה ביותר, דבר המקשה על רמ"י לבחון את מידת היישום של הגנת הסייבר בארגון.

מדיניות אבטחת מידע

בהנחיית יה"ב 5.2[14] נקבע כי ועדת היגוי סייבר תאשר את מדיניות הגנת הסייבר בארגון, כי מדיניות זו תיושם בהתאם לתהליך ניהול סיכונים בארגון, וכי על בסיס מדיניות זו תגובש תוכנית העבודה.

עוד נקבע כי מדיניות הגנת הסייבר בארגון תיבדק ותאושרר על ידי ממונה הגנת הסייבר אחת לשנתיים או מוקדם יותר, במקרה של צורך מיוחד (שינויים ניכרים במערך המחשוב או במערך הארגוני של הארגון). במקרה הצורך תעודכן המדיניות על ידי ממונה הגנת הסייבר. הבדיקה והעדכון של המדיניות יאושרו על ידי ועדת היגוי סייבר.

הביקורת העלתה כי מדיניות הגנת הסייבר של רמ"י אושרה בוועדת היגוי סייבר בשנת 2019 ומאז לא נבדקה, לא עודכנה ולא נדונה בוועדה, זאת על אף שינויים ניכרים שהתרחשו משנת 2019 במערך המחשוב של רמ"י, ובכלל זה התפתחויות טכנולוגיות בעולם והתקדמות ביכולות התקיפה של תוקף פוטנציאלי. עקב כך עולה החשש שבעת התממשות של סיכונים תורת ההגנה מפניהם לא תהיה עדכנית.

רמ"י מסרה בתשובתה כי המדיניות בנושאי הענן הממשלתי עודכנה בספטמבר 2023, והעדכון יובא לאישור ועדת ההיגוי בישיבתה הבאה.

על רמ"י לבחון את הצורך בעדכון מדיניות הגנת הסייבר על כלל היבטיה ולהביאה לאישור ועדת היגוי סייבר.

תוכנית עבודה שנתית להגנת הסייבר

כדי להבטיח טיפול יעיל וסדור בסיכוני סייבר נקבע בהנחיית יה"ב 5.3 כי על הארגון להכין תוכנית עבודה שנתית לטיפול בנושא אבטחת המידע, ועל ועדת היגוי סייבר לאשרה ולבצע במשך השנה בקרה על יישומה. תוכנית העבודה תכלול אומדן עלויות, אומדן כוח האדם הנדרש ולוחות זמנים מומלצים לביצוע. התוכנית אמורה להיגזר מסקר הסיכונים ולכלול התייחסות לכלל הנושאים המהותיים, לרבות הכנת תוכנית לטיפול בסיכוני סייבר.

---

[14] סעיף 6.1.4.2.

בתשובתה ציינה רמ"י כי אגף מערכות מידע וממונה הגנת הסייבר מתכננים בכל שנה את תוכנית העבודה ומציגים אותה וכן את סטטוס הביצוע של התוכנית שקדמה לה לפני ועדת ההיגוי.

מעיון בפרוטוקולים של דיוני ועדת היגוי סייבר ברמ"י עלה כי תוכנית העבודה שהוצגה לוועדה כללה רק את פירוט הנושאים המתוכננים לביצוע, ולא כללה לוחות זמנים, פירוט של הגורמים האחראים ליישום, התקציב הנדרש וסדרי העדיפויות. כמו כן, אין מסמכים המעידים על ביצוע מעקב של הוועדה עצמה אחר יישום התוכנית, ובכלל זה אחר תיקון הליקויים שעלו בסקרי הסיכונים ובמבדקי החדירה שבוצעו.

עוד עלה כי גם במקרים שוועדת היגוי סייבר הנחתה לבצע משימות, היא לא עקבה אחר ביצוען. לדוגמה, בישיבתה באוקטובר 2021 הנחתה הוועדה לבצע מבדק חדירה במפתיע עד סוף השנה וכן לכנס את ועדת ההרשאות לצורך הקמת פרופילי הרשאות. ואולם עלה כי משימות אלה לא בוצעו, וכי הוועדה לא בדקה אם בוצעו.

כינוס ועדת היגוי סייבר

בהחלטת הממשלה 2443 נקבע כי על ועדת היגוי סייבר להתכנס לכל הפחות פעם בחצי שנה.

בביקורת עלה כי ועדת היגוי סייבר של רמ"י התכנסה לראשונה בינואר 2017, אך מאז לא התכנסה בהתאם לנדרש בהחלטת הממשלה: בשנים 2017[15], 2018[16], 2021[17] ו-2022[18] הוועדה התכנסה פעם אחת בשנה בלבד, בשנת 2020 היא לא התכנסה כלל, ורק בשנת 2019[19] היא התכנסה פעמיים בשנה כנדרש. אשר לשנת 2023, נכון למועד סיום הביקורת (אוקטובר 2023) הוועדה טרם התכנסה.

בהיעדר התכנסויות של הוועדה כנדרש היא אינה יכולה לעקוב באופן אפקטיבי אחר ביצוע תוכניות העבודה ותיקון הליקויים שהועלו ולפקח על כך.

☆

ועדת היגוי סייבר ברמ"י היא מסגרת ארגונית ניהולית המופקדת על קבלת החלטות אסטרטגיות בתחום הגנת הסייבר וביצוע בקרה ניהולית על יישום הגנת הסייבר. בביקורת הועלו ליקויים בדרך פעולתה של הוועדה: בין היתר, הוועדה לא בחנה ולא אישרה את המיפוי והסיווג של נכסי המידע של רמ"י; לא ניהלה את תהליך ניהול סיכוני הסייבר בכל הנוגע לביצוע סקרי סיכונים; לא גיבשה סקרי הנהלה; לא עקבה אחר מידת הביצוע של תוכניות העבודה, ולא בדקה אם הביצוע הוא בהתאם לנדרש; ולא התכנסה בתדירות שנקבעה בהחלטת הממשלה. בכך נפגעת היכולת של הוועדה לבצע בצורה מיטבית בקרה ניהולית על יישום הגנת הסייבר ברמ"י, להתוות אסטרטגיות לפעילות הגנת הסייבר, לפקח באופן מספק על יישום תוכניות העבודה, להעריך את הנזקים בעקבות תקלות ולגבש המלצות לטיפול.

על רמ"י להביא לאישור ועדת היגוי סייבר את המיפוי והסיווג של נכסי המידע ואת מדיניות הגנת הסייבר שלה ולהשלים את סקרי הסיכונים למערכות הליבה. על ועדת היגוי סייבר, בהובלת יו"ר הוועדה (מנהל רמ"י), לגבש סקרי הנהלה, לעקוב אחרי ביצוע תוכניות העבודה בתחום הגנת הסייבר, לבחון את מידת האפקטיביות של הגנת הסייבר ברמ"י על פי המדדים שנקבעו ולהקפיד להתכנס בהתאם לנדרש בהחלטת הממשלה.

---

15 הוועדה התכנסה ב-1.2.17.
16 הוועדה התכנסה ב-8.7.18.
17 הוועדה התכנסה ב-18.10.21.
18 הוועדה התכנסה ב-11.12.22.
19 הוועדה התכנסה ב-12.5.19 וב-18.12.19.

פעולות ממונה הגנת הסייבר

בהחלטת הממשלה 2443 נקבע כי יש להטיל על המנכ"לים של גופי הממשלה, ובהם רמ"י, לפעול לשיפור רמת הגנת הסייבר, ולשם כך למנות ממונה הגנת סייבר שיהיה כפוף ישירות למנכ"ל או למי מטעמו.

בהנחיית יה"ב 5.2[20] נקבע כי ממונה הגנת הסייבר אחראי להבטיח את התכנון, הניהול, הטיפול והבקרה במכלול היבטי הגנת הסייבר בארגון. תפקידיו הם בין היתר אלה: גיבוש מדיניות הגנת הסייבר בארגון, בהתאם לתהליך ניהול סיכונים בארגון; בניית מתווה לתוכנית עבודה להגנת הסייבר על פי המדיניות שגובשה; גיבוש תוכנית בקרה על יישום וניהול של הגנת הסייבר בהיבט הארגוני הרחב ובהתאם למדיניות; ייזום וניהול של סקרי הנהלה; גיבוש ואישור של נוהלי הגנת הסייבר בארגון; וניהול ויישום של תוכנית מבדקים פנימיים, אשר יבוצעו על ידו או על ידי מי מטעמו.

בבדיקה עלה כי ממונה הגנת הסייבר ברמ"י מילא חלק מהתפקידים שנקבעו לו בהנחיית יה"ב - הוא היה שותף לדיוני ועדת היגוי סייבר כחבר ועדת היגוי לסייבר, וקיים פגישות עיתיות עם צוותי אבטחת המידע ברמ"י ועם נציגי יה"ב, לצורך התעדכנות בהנחיות יה"ב; בפעילויות אבטחת המידע המתוכננות ברמ"י, כגון מבדקי חוסן; ובכלי אבטחת המידע החדשים שרמ"י רוכשת. ואולם הוא לא עסק בגיבוש ואישור של נוהלי הגנת סייבר של רמ"י ולא יזם סקרי הנהלה.

ממונה הגנת סייבר הוא דמות מרכזית בעניין התכנון, הניהול, הטיפול והבקרה במכלול היבטי הגנת הסייבר בארגון, ולכן תפקידו נקבע בהחלטת ממשלה. נוכח מרכזיותו והצורך באי-תלותו של ממונה הגנת סייבר אף נקבע שהוא יהיה כפוף ישירות למנכ"ל הארגון. על ממונה הגנת הסייבר להשתתף באופן פעיל יותר בתכנון, בניהול, בטיפול ובבקרה במכלול היבטי הגנת הסייבר ברמ"י, בהתאם לנדרש ממנו בהנחיות יה"ב, ובכלל זה להשתתף בגיבוש ואישור של נוהלי הגנת הסייבר, בייזום סקרי הנהלה ובמעקב אחר ביצוע תוכנית העבודה.

עמידה בחוק ובתקנות הגנת הפרטיות (אבטחת מידע)

תקנות הגנת הפרטיות קובעות כללים מנחים בתחום אבטחת המידע המצוי במאגרי מידע, ובכלל זה בנוגע למינוי ממונה על אבטחת המידע, קביעת נוהל אבטחה, מיפוי המערכות במאגר המידע, ביצוע סקר סיכונים, אבטחה פיזית וסביבתית וניהול הרשאות גישה.

משרד מבקר המדינה בדק את מידת עמידתה של רמ"י בהוראות ובכללים המרכזיים שנקבעו בחוק הגנת הפרטיות ובתקנות. להלן הממצאים:

רישום מאגרי המידע בפנקס מאגרי המידע

על פי סעיף 17 לחוק הגנת הפרטיות, בעל מאגר מידע, מחזיק במאגר מידע או מנהל מאגר מידע - כל אחד מהם אחראי לאבטחת המידע שבמאגר המידע. על פי החוק, בעל מאגר מידע מחויב ברישום מאגר המידע בפנקס מאגרי המידע[21], והאחריות להגשת הבקשה לרישום המאגר מוטלת עליו. מטרת הרישום היא להבטיח את ההגנה על פרטיות המידע שבמאגרי המידע ולתת כלים, הן בידי רשם מאגרי המידע והן בידי מי שמידע עליו מנוהל במאגרי המידע, לאכוף את החובות המצוינות בחוק הגנת הפרטיות על בעלי המאגרים.

לפי פנקס מאגרי המידע, בינואר 2023 הייתה רמ"י רשומה כבעלים של עשרה מאגרי מידע שנרשמו בשנת 2005 בפנקס מאגרי המידע.

---

20 סעיף 6.3.

21 בהתאם לסעיף 12(א) לחוק הגנת הפרטיות, הרשות להגנת הפרטיות מנהלת את פנקס מאגרי המידע, הפתוח לעיון הציבור.

חובת גיבוש וניהול של מסמכים: לפי תקנות הגנת הפרטיות[22], על בעל מאגר מידע לנהל מסמך הגדרות מאגר[23] ולעדכנו בכל עת שנעשה שינוי ניכר בנושאים שפורטו בתקנות. כמו כן, על בעל מאגר מידע לבחון את הצורך בעדכון מסמך הגדרות מאגר בשל שינויים טכנולוגיים וארגוניים או אירועי אבטחה, עד 31 בדצמבר בכל שנה (להלן - מסמך הגדרות המאגר). הוראות אלה הותקנו בשנת 2017 ונכנסו לתוקפן במאי 2018, לאחר שנה מיום פרסומן.

התקנות גם קובעות כי על בעל מאגר המידע להכין מסמך מעודכן של מבנה מאגר המידע וכן רשימת מצאי מעודכנת של מערכות המאגר, שתכלול בין השאר תוכנות וממשקים המשמשים לתקשורת עם מערכות המאגר.

בעקבות כניסת התקנות לתוקפן פעלה רמ"י לארגון ורישום מחדש של מאגרי המידע שברשותה נוכח הנדרש בתקנות, וזאת לאחר שמצאה כי המאגרים הרשומים מיושנים ואינם תואמים עוד את פעילות הארגון[24]. בהתאם לכך, בתוכניות העבודה שאושרו על ידי ועדת היגוי סייבר בשנים 2019 - 2022 נקבעו משימות בדבר ארגון המאגרים ורישומם מחדש.

בביקורת עלה כי בשנת 2019 אישרה ועדת היגוי סייבר את מינוים של חמישה מנהלים למאגרי מידע עדכניים (שבאחד מהם אוחדו מאגרי המידע שנרשמו בעבר)[25], ולמאגרים אלה הוכנו מסמכי הגדרות מאגר ומסמכי מבנה מאגר. ואולם בפועל רמ"י לא רשמה מאגרים אלה, כנדרש בחוק, אף שעברו כחמש שנים מאז הכירה בצורך בכך. נכון למועד סיום הביקורת חמשת מאגרי המידע טרם נרשמו. עוד עלה כי ועדת ההיגוי לא דנה בסיבות לאי-רישום המאגרים.

על רמ"י לפעול לרישום מאגרי המידע העדכניים כנדרש בחוק, ועל ועדת היגוי סייבר לעקוב אחר הרישום כאמור.

מינוי מנהלי מאגרי מידע

בתקנות הגנת הפרטיות[26] נקבע כי בעל מאגר מידע יגדיר במסמך הגדרות המאגר את מנהל המאגר, שעליו חלות גם החובות המפורטות בתקנות בעניין אבטחת המידע שבמאגר המידע. על פי התנאים להגשת בקשה[27] לרישום מאגר מידע בפנקס מאגרי המידע, על בעל מאגר לצרף לבקשת הרישום כתב מינוי של מנהל המאגר[28] והצהרה חתומה על ידי מנהל המאגר כי ניתנו לו המשאבים והסמכויות לביצוע חובותיו לפי חוק הגנת הפרטיות והתקנות. יצוין כי לפי החוק, מנהל מאגר מידע חב באחריות לאבטחת המידע שבמאגר, יחד עם בעל המאגר או המחזיק בו וגם לחוד.

בביקורת עלה כי שניים מחמישה מנהלי המאגרים שמונו על ידי רמ"י לא חתמו על הצהרת מנהל מאגר, כפי שנדרש בתנאים לרישום מאגר המידע בפנקס מאגרי המידע, וכי אחד מהשלושה שחתמו כבר אינו בתפקיד רלוונטי על מנת לשמש מנהל אותו מאגר[29].

על רמ"י להשלים את תהליך מינוי המנהלים למאגרים שלה, ובכלל זה קיום הצהרות כנדרש, וידוא כי מי שמונה למנהל מאגר ממלא תפקיד רלוונטי כדי לשמש מנהל אותו מאגר, ובמידת הצורך מינוי מנהל מאגר חלופי.

---

22 סעיף 2 לתקנות הגנת הפרטיות (אבטחת מידע), תשע"ז-2017.

23 על המסמך להכיל פרטים על בעל המאגר (יחיד, תאגיד, עסק, גוף ציבורי); מטרת המאגר; סוגי המידע במאגר; מנהל המאגר; מידע המוחזק אצל גורם חיצוני, אם מוחזק; ופירוט בדבר העברת מידע לצדדים שלישיים.

24 כפי שעלה בסיכום של ועדת היגוי שהתכנסה בשנת 2018.

25 חמשת מאגרי המידע שאושרו הם אלה: חוזים, ספקים ופניות הציבור; מכרזים; משפטי; פיקוח ועובדים.

26 סעיף 2 לתקנות הגנת הפרטיות (אבטחת מידע), תשע"ז-2017.

27 רשימת המסמכים הנדרשים ממגיש הבקשה לרישום מאגר מידע.

28 על מנהל המאגר הממונה להיות עובד בכיר של בעל מאגר המידע, אשר יש ביכולתו לפעול באופן עצמאי, על מנת לקיים את חובותיו כמנהל המאגר.

29 מדובר על מאגר החוזים שלגביו מונה מנהל אגף עסקאות דאז שכבר אינו משמש בתפקידו זה.

נוהל אבטחת מאגרי מידע

בתקנות נקבע[30] כי על בעל המאגר לקבוע במסמך נוהל אבטחה ארגוני, שבו מפורטת מדיניות האבטחה הארגונית לשם התמודדות עם סיכוני האבטחה שלהם חשוף המידע שבמאגר. אחת לשנה יש לבחון את הצורך בעדכון הנוהל.

בביקורת עלה כי ברמ"י גובשה טיוטת נוהל "אבטחת מאגרי מידע" על ידי יועץ חיצוני לאבטחת מידע, ובה צוין כי היא בתוקף מדצמבר 2022. ואולם בפועל הטיוטה לא אושרה על ידי הנהלת רמ"י, כנדרש לגבי נוהלי הארגון, וגם ועדת היגוי סייבר לא דנה בה, וממילא לא אישרה אותה.

על רמ"י לפעול לאישור נוהל אבטחת המידע.

בקרה על עמידה בתקנות

כדי לוודא כי קיימת בקרה על העמידה בתקנות הגנת הפרטיות, נקבע בתקנות[31] כי הממונה על אבטחת המידע בארגון[32] יכין תוכנית לבקרה שוטפת על העמידה בדרישות התקנות (ובכלל זה עריכת סקרים לאיתור סיכוני אבטחת מידע, ביצוע מבדקי חדירה למערכות המאגר ותיקון הליקויים שהתגלו, ניהול הרשאות הגישה, בקרה על הגישה ותיעוד הגישה), יפעל על פי התוכנית שגיבש ויודיע לבעל מאגר המידע ולמנהל המאגר על ממצאיו.

בביקורת עלה כי הממונה על אבטחת המידע ברמ"י קיים בקרה על העמידה בדרישות התקנות, אך לא דן בממצאי הבקרה עם מנהלי המאגרים. עקב כך מנהלי המאגרים אינם מודעים לחולשות במאגרי המידע, ואין באפשרותם להתריע עליהן לפני הנהלת הארגון.

בתשובה מפברואר 2024 ציינה רמ"י כי התקיימו פגישות שוטפות עם מנהלי המאגרים בהן הוצג להם תפקידם ותחומי אחריותם.

על הממונה על אבטחת המידע ברמ"י לקיים דיונים עיתיים עם מנהלי המאגרים גם לגבי ממצאי הבקרה על העמידה בדרישות התקנות.

ניהול הרשאות גישה

1. בתקנות הגנת הפרטיות נקבע[33] כי בעל מאגר מידע יקבע את הרשאות הגישה של בעלי ההרשאות למאגר המידע ולמערכות המאגר, בהתאם להגדרות התפקיד ובמידה הנדרשת לביצוע התפקיד בלבד (להלן - פרופיל המשתמש). יצוין כי החובות בנוגע לניהול הרשאות הגישה למאגר, ובכלל זה קביעת הרשאות הגישה, חלות גם על מנהל המאגר.

   עוד נקבע כי בעל מאגר מידע ינהל רישום מעודכן של תפקידים, הרשאות הגישה שניתנו לגביהם ובעלי ההרשאות הממלאים תפקידים אלה.

   לצורך יצירת פרופיל משתמש לכל העובדים, החליטה ועדת היגוי סייבר באוקטובר 2021 להקים ועדת הרשאות שתהיה אחראית ליצירת פרופיל לכל תפקיד ולאישור ההרשאות הנדרשות לכל תפקיד (להלן - מטריצת ההרשאות).

   בביקורת עלה כי ועדת ההרשאות האמורה שהוקמה על פי החלטת ועדת היגוי סייבר לא התכנסה, ובפועל מטריצת ההרשאות לגישה נקבעה על ידי אגף מערכות מידע ברמ"י, ללא

---

30 סעיף 4 לתקנות הגנת הפרטיות (אבטחת מידע), תשע"ז-2017.

31 סעיף 3 לתקנות הגנת הפרטיות (אבטחת מידע), תשע"ז-2017.

32 על פי סעיף 3 לתקנות גוף ציבורי המחזיק בחמישה מאגרי מידע החייבים ברישום לפי חוק נדרשים למנות ממונה על אבטחת מידע על פי סעיף 17ב לחוק.

33 סעיף 8 לתקנות הגנת הפרטיות (אבטחת מידע), תשע"ז-2017.

אישור של ועדת ההרשאות וגם ללא מעורבות של מנהלי המאגרים שעליהם חלה חובת קביעת ההרשאות.

2. לשם המחשת החשיבות של הסדרת ההרשאות, בדק משרד מבקר המדינה באוגוסט 2023 את אפשרויות הגישה של בעל תפקיד זוטר (רכז שירות לחוכר) במרחב השירות תל אביב-מרכז לתיקי נכסים (חוזים) במרחבים אחרים במערכות הליבה החדשות (רמיטק). יצוין כי בעל תפקיד זה אחראי לתת שירות לציבור במרחב תל אביב-מרכז בלבד, ובכלל זה הפקת אישורים על זכויות בקרקע ומתן התחייבויות לרישום משכנתה.

הבדיקה העלתה כי עלו פערים בין אפשרויות הגישה של רכזי השירות לחוכר לתיקי נכסים לבין דרישות התפקיד שלו.

עוד יצוין לגבי ניהול הרשאות כי בדוח מבקר המדינה בנושא "מניעת מעילות והונאות ברשות מקרקעי ישראל", שהתפרסם במאי 2022[34], נכללו בין היתר ממצאי בדיקת המנגנון של ביטול הרשאות לעובדים שפרשו, והועלה כי לתשעה מ-353 עובדים שהעסקתם ברמ"י הסתיימה בין ינואר 2018 ליוני 2021 נותרו הרשאות גישה למערכות מידע של רמ"י.

רמ"י מסרה בתשובתה כי מטריצת ההרשאות נקבעה על ידי "גורמי המטה הרלבנטיים, בשיתוף ועדת ההרשאות, גורמי השטח ואגף מערכות מידע", וכי יש צורך לכנס את ועדת ההרשאות, לשם המשך עבודתה.

מומלץ כי רמ"י תכנס את ועדת ההרשאות כדי להסדיר את נושא הרשאות הגישה, ובכלל זה לבחון אם ההרשאות לכל ממלא תפקיד הן בהתאם לצורכי התפקיד. עוד מומלץ שרמ"י תשתף את מנהלי המאגרים שמונו על ידי ועדת היגוי סייבר בתהליך קביעת ההרשאות.

בקרה על הגישה למאגרי המידע ותיעוד הגישה למאגרים

על פי תקנות הגנת הפרטיות[35], יש לנהל מנגנון תיעוד אוטומטי שיאפשר ביקורת על הגישה למערכות המאגר (מנגנון בקרה). התיעוד יכלול את הנתונים האלה: זהות המשתמש, התאריך והשעה של ניסיון הגישה, רכיב המערכת שאליו בוצע ניסיון הגישה, סוג הגישה, היקפה, ואם הגישה אושרה או נדחתה. עוד נקבע בתקנות הגנת הפרטיות כי בעל מאגר המידע נדרש לקבוע נוהל בדיקה שגרתי של הנתונים המתועדים במנגנון הבקרה ולערוך דוח של הבעיות שהתגלו והצעדים שננקטו בעקבות כך.

בהנחיית יה"ב 5.2[36] נקבע כי איתור ניסיונות לבצע פעולות לא מורשות במערכת יתבצע בין היתר באמצעות ניתוח בזמן סמוך ככל שניתן לזמן אמת של רשומות תיעוד הפעולות (להלן - רשומות הלוג)[37] במערכות. נוסף על כך, במדריך לתקנות הגנת הפרטיות (אבטחת מידע) שפרסמה הרשות להגנת הפרטיות צוין כי כדי לעמוד בחובתו לאתר אירועי אבטחה בזמן אמת, מומלץ שבעל המאגר יישם מנגנונים אוטומטיים להתרעה.

ביטוי לאמור נמצא גם בטיוטת נוהל אבטחת מידע של רמ"י, ולפיו במאגר המידע של רמ"י יופעל מנגנון תיעוד של רשומות הלוג על פעולות של משתמשים במערכות המאגר; בקרה על פעילויות תבוצע על פי צורך, באמצעות מערכת "בקרת פעילויות"; ואירועי גישת משתמשים חריגים ידווחו לגורמי אבטחת המידע ברמ"י.

על הערך הרב שיש לתיעוד הגישה של משתמשים למאגר מידע של גוף ציבורי ניתן ללמוד מדיון שהתקיים בוועדת המדע והטכנולוגיה של הכנסת בשנת 2017 לגבי מקרים שהתגלו ברשות ציבורית,

---

34 מבקר המדינה, **דוח מבקר המדינה -מאי 2022**, "מניעת מעילות והונאות ברשות מקרקעי ישראל", עמ' 751.

35 סעיף 10 לתקנות הגנת הפרטיות (אבטחת מידע), תשע"ז-2017.

36 סעיף 11.14.

37 לוג (log) הוא מנגנון תיעוד של פעולות המבוצעות במערכות מידע.

שבהם 50 עובדים ביצעו שאילתות במאגר המידע של הרשות שלא לצורך עבודתם. חיפושים אלו של העובדים האמורים לא היו מתגלים, אילו לא היה מתבצע תיעוד לגבי החיפושים במאגר המידע ולגבי המידע שנצפה, ואילו לא הייתה מתבצעת בקרה על כך[38].

גם בדוח מבקר המדינה בנושא "מניעת מעילות והונאות ברשות מקרקעי ישראל" שהתפרסם במאי 2022, צוין כי בשנים 2018 - 2020 התרחשו כמה מקרים ברמ"י שבהם עלה חשד כי בוצעה העברת מידע לגורם לא מורשה. במסגרת הליך הפקת לקחים שקיימה רמ"י לגבי מקרה אחד, התקיים דיון בראשות סמנכ"ל מינהל ומטה של רמ"י דאז, ובו הוא הדגיש כי יש לחסום את האפשרות לבצע במערכות המידע פעולות בניגוד לנהלים וללא קבלת אישור.

בביקורת עלה כי ברמ"י קיים מנגנון בקרה מסוים אך הוא אינו מתריע על פעולות מסוימות. עקב כך, בפועל מנגנון הבקרה אינו מיטבי ואינו תואם את הדרישות, ומומלץ כי רמ"י תפעל לתיקון הדבר.

תוכניות המשכיות תפקודית (BCP - Business Continuity Plan) והתאוששות מאסון (DRP - Disaster Recovery Plan)

יכולת המשכיות תפקודית (עסקית) היא יכולתו של ארגון להתכונן לאירועים המפריעים לפעילותו ולהגיב עליהם, כדי להמשיך בפעילות הרגילה באופן ובהיקף שתוכננו מראש. מטרותיה העיקריות של תוכנית להמשכיות תפקודית הן להבטיח את שרידותו של הארגון, להגן על נכסיו החשובים, לאפשר להנהלתו שליטה על סיכונים וחשיפות, לקדם צעדים המונעים את התממשותם של חלק מאירועי החירום האפשריים, ולאפשר פעולה יעילה ואפקטיבית של הנהלת הארגון בשעת אירוע החירום לשם השבת הארגון לפעולה. גופים ציבוריים נדרשים אף להבטיח כי ביכולתם לספק שירותים חיוניים לציבור בעת אירוע חירום[39]. סיכונים לפגיעה בארגון עלולים לנבוע מסיבות שונות, ובהם השתלטות מרחוק על מערכות מחשוב ומידע ושיבוש מידע האגור במערכות; פגיעות בשל אסונות טבע או אירועי לוחמה; ופגיעות עקב פגיעה במערכות מיזוג האוויר או עקב הצפות.

גיבוש תוכנית להמשכיות תפקודית דורש תכנון, וכולל בין היתר ניתוח סיכונים, הצבעה על ההליכים הקריטיים שיש לשמור על זמינותם בעת אסון והגדרת המשאבים - האנושיים והחומריים - הנדרשים בעת אסון. תוכנית התאוששות מאסון נוגעת לתהליכים במערכות המידע שארגון צריך לבצע כדי להתאושש מאסון ולאפשר המשכיות תפקודית, תוך מתן דגש על אופן גיבוי המידע ועל הסביבה (פיזית ולוגית) שבה הוא ישוחזר. במסגרת תוכנית להתאוששות מאסון הארגון קובע את ה-RPO (Recovery Point Objective) - כמה מידע הוא מוכן לאבד במקרה של אסון, ואת ה-RTO (Recovery Time Objective) - כמה זמן הוא יכול להמתין עד חזרה לפעילות.

הנחיית יה"ב 5.2[40] קובעת כי על הארגון לגבש תוכנית המשכיות תפקודית, וכי על תוכנית כזאת לכלול גם תוכנית התאוששות מאסון. עוד קובעת ההנחיה כי ועדת היגוי סייבר תאשר תחילה את עקרונות ההיערכות שיאפשרו את המשך הפעילות של מערכות התקשוב החיוניות של הארגון בעת חירום, וכי מנהל מערכות המידע בארגון יפעל ליישום עקרונות ההיערכות ויהיה אחראי לתחזוקתה ועדכניותה של התוכנית. נוסף על כך נקבע בהנחיה כי אחת לתקופה שתיקבע בתוכנית, אך לא יותר מחמש שנים, יתבצע ניסוי לבחינת מערך השיקום וההתאוששות של הארגון.

---

38 מבקר המדינה, **דוח שנתי של מבקר המדינה בנושא סייבר ומערכות מידע - מאי 2023**, "הגנת הפרטיות ואבטחת המידע במערכות המרכז לגביית קנסות, אגרות והוצאות ברשות האכיפה והגבייה", עמ' 387; פרוטוקול דיון ועדת המדע והטכנולוגיה של הכנסת שהתקיים ב-18.7.17, עמ' 6.

39 ראו מבקר המדינה, **דוח שנתי 64א** (2013), "בניית תכניות להמשכיות עסקית של המערכת הפיננסית באירועי חירום", עמ' 51; מבקר המדינה, **דוח שנתי 64ג** (2014), "היערכות שירותי הבריאות לעתות חירום - ממצאי מעקב", עמ' 717.

40 סעיף 13.5.

הנחיית יה"ב 5.30 בנושא "גיבוי ושחזור מידע"[41] (להלן - הנחיית יה"ב 5.30) מוסיפה וקובעת כי בתוכנית יש להגדיר מדדים מקובלים לחזרה לפעילות אם יתרחש אירוע סייבר, כגון RTO, ומדגישה את הצורך ביכולת התאוששות במקרים של נפילת אתר, מחיקת מידע ונעילת קבצים, וכן את הצורך בביצוע גיבויים למערכות המידע, בין היתר באתר גיבוי (אתר ה-DR, Disaster Recovery).

בביקורת נבדקו התוכנית להמשכיות תפקודית, הכוללת תוכנית להתאוששות מאסון, וכן האתר החלופי של רמ"י; התוכנית והאתר הם חלק מהמערך שתפקידו לאפשר המשך פעילות של מערכות המידע במקרה של אסון.

בביקורת עלה כי אגף מערכות מידע ברמ"י הכין נוהל בנושא "מדיניות המשכיות עיסקית ותפקודית", ובו פורטו העקרונות והתהליכים שיש לבצע לשם המשכיות כאמור. ואולם הנוהל אינו כולל הנחיות מפורטות בין היתר לגבי תרחישי ייחוס שונים (לדוגמה, משבר מקומי, משבר עולמי, משבר תקשובי), ניתוח סיכונים, בקרות לתרחיש הייחוס, קביעת יעדי שירות למצב חירום ויעדי התאוששות (לרבות רמת התאוששות וזמני התאוששות צפויים). כמו כן, הנוהל אינו כולל התייחסות לנושאים כגון הגדרת כוח אדם חיוני ואתרי עבודה. נוסף על כך, עלה שהנוהל לא הובא לפני ועדת היגוי סייבר, וממילא היא לא אישרה אותו.

עוד עלה כי מאז התכנסה לראשונה ועדת היגוי סייבר בשנת 2017, היה בכל הישיבות שלה על סדר היום נושא הכנת תוכנית להתאוששות מאסון. ואולם בפועל הנושא לא נדון בישיבותיה, ולא התקבלו החלטות אופרטיביות בעניינו. כמו כן, ההתקדמות בהכנת התוכנית לא הוצגה לוועדה בסיכומי הפעילות השנתית.

יצוין כי במסמך המיפוי והסיווג של נכסי המידע שמסרה רמ"י למשרד מבקר המדינה בעת הביקורת, צוינו לצד כל מערכת מידע רמת הסיכון שלה וזמן ההמתנה עד חזרתה לפעילות. ואולם זמני ההמתנה כאמור נקבעו על ידי אגף מערכות מידע, בלי שהועברו לעיונה ולאישורה של ועדת היגוי סייבר, שהיא המוסמכת לאשר את עקרונות ההיערכות שיאפשרו את המשך הפעילות של מערכות התקשוב החיוניות של הארגון בעת חירום.

כדי שרמ"י תוכל להבטיח את שרידותה ותפעולה גם באירועי חירום העלולים לפגוע במערכות המידע והמחשוב שלה, עליה להכין תוכנית להמשכיות תפקודית, הכוללת תוכנית להתאוששות מאסון, על בסיס העקרונות שאושרו על ידי ועדת היגוי סייבר.

רמ"י מסרה בתשובתה כי תוכנית בנדון תוצג לוועדת ההיגוי בישיבתה הבאה.

אתר חלופי לאסון (DR)

כאמור, בתוכנית להמשכיות תפקודית (BCP) נדרש גם לקבוע אתר חלופי זמין לשם המשך פעילות מערכות המידע במקרה של אסון - נזק לאתר המרכזי או השבתתו (להלן - אתר חלופי לאסון). אתר כזה יאפשר במקרה של אסון להחזיר לשימוש באופן מהיר את מערכות המידע. מערכות המידע של רמ"י נמצאות במספר אתרים:

בסיכום סקר סיכונים מסוים שביצעה רמ"י במרץ 2019 עלו פערים תשתיתיים לגבי אתר מסוים.

בביקור שקיים צוות הביקורת באתר מסוים באוגוסט 2023 נמסר לו על ידי האחראים לאתר שאף שהמקור לבעיות בו הוא התשתיות של המבנה, לא נעשו שינויים במבנה מאז בוצעו סקרי הסיכונים בשנת 2019.

41 הנחיית יה"ב 5.30 גרסה 1.0 מ-20.5.21.

רמ"י מסרה בתשובתה מינואר 2024 כי מתחם מסוים עבר שדרוג היא בוחנת פתרון נוסף בתשובה מפברואר 2024 הוסיפה רמ"י כי חלק מהליקויים אמורים להיות מטופלים ע"י הנהלת המבנה ורמ"י תבצע מעקב ובקרה שאכן הם יתוקנו.

כדי לתת מענה מלא באירועי חירום, ובכלל זה להבטיח את היכולת לחזור בהקדם האפשרי לפעילות תקינה וסבירה, על רמ"י לפעול לתיקון הליקויים שעלו בנושא.

גיבויים ושחזור מידע

לצורך שמירת כלל המידע במערכות המידע, לצורך שחזור המידע במקרה של אסון ולצורך שמירה על ההמשכיות התפקודית נדרשות מערכות גיבוי. רמ"י משתמשת בשתי מערכות גיבוי, באמצעות שתי חברות חיצוניות.

תרגול לשחזור מידע ממערך הגיבוי: בהנחיית יה"ב 5.30[42] צוין כי מנגנון הגיבוי והשחזור בארגון הוא מנגנון קריטי המאפשר להתמודד עם סוגיות הנוגעות בין היתר לשלמות, לאמינות ולזמינות של המידע. על פי ההנחיה, יש לבצע בין היתר בדיקה לגבי תקינות שחזור המידע לפחות אחת לחצי שנה. כן יש לבצע בדיקת שחזור שנתית יזומה של מערכת הייצור במקום חלופי וניסיונות שחזור מדגמיים. כל זאת כדי לוודא את תקינות מערך הגיבוי. כמו כן צוין בהנחיה כי יש להצפין את עותק הגיבויים לפני הוצאתו לשמירה מחוץ לאתר הראשי או אתר הגיבויים (DR)[43]. בהנחיה נאמר כי סיכום בדיקת תקינות השחזור יישלח להנהלה, וכי יתבצע מעקב. בהנחיית יה"ב 5.2 נקבע כי תפקידי ועדת היגוי סייבר בהקשר זה הם התעדכנות בסיכונים ובאיומים הנוגעים לארגון, פיקוח על ניהול סיכוני הסייבר המבוצע בארגון, אישור הסיכונים השיוריים[44] וקבלת החלטות לגבי ביצוע שינויים בעקרונות הגנת הסייבר.

בביקורת עלה כי רמ"י לא קיימה תרגול של העלאת השחזורים של מערכות המידע באופן מלא, אלא ביצעה העלאת גיבויים למערכת אחרת בכל פעם. עוד עלה כי סיכומים של בדיקות תקינות השחזור שבוצעו לא הועברו לוועדת היגוי סייבר, וכי היא אינה מבצעת מעקב בעניינן.

רמ"י ציינה בתשובתה כי במשך השנה מתורגלות למעשה כל המערכות, וכי מערך הגיבויים והשחזורים יוצג לוועדה בישיבתה הבאה.

סקר לבדיקת אבטחת מידע למערך הגיבויים: בנובמבר 2022 ביצעה רמ"י סקר אבטחת מידע למערך הגיבויים שלה. הסקר בוצע במטרה לשקף את רמת אבטחת המידע של מערך הגיבויים, לצורך גיבוש תוכנית עבודה לצמצום הפערים הקיימים. הסקר העלה כמה ליקויים.

ממסמך של אגף מערכות מידע מיוני 2023 בנושא תיקון הליקויים שעלו בסקר עלה כי האגף תיקן ליקויים מסוימים.

עלה כי אגף מערכות מידע לא הביא את המסמך לפני ועדת היגוי סייבר, לצורך דיון בליקויים שעלו ובתיקונים שביצע. אשר לוועדה, היא לא דנה בהחלטתו של האגף שלא לתקן ליקויים מסוימים וממילא לא אישרה את ההחלטה.

מומלץ כי אגף מערכות מידע ברמ"י יקפיד לעדכן את ועדת ההיגוי בדבר ממצאי סקרי הסיכונים והצעותיו לטיפול בממצאים, ובפרט במקרים שבהם החליט על אי-ביצוע תיקונים.

---

42 סעיף 6.26

43 בגיבוי קר (offline) על גבי קלטות המאוחסנות באתר חיצוני ומרוחק, בכספת חסינת אש שכוללת בקרת גישה, על הגיבוי להיות מנותק ממערכות הארגון.

44 "סיכון שיורי" - השפעת הסיכוי להתממשות הסיכון בהתחשב בתהליכי הבקרה ובדרכי הפעולה הקיימות בארגון לטיפול בסיכון.

הגנה פיזית

על פי הנחיה 5.2, הגנה פיזית בכל הקשור להגנת סייבר היא הגנה על מכלול הציוד והמידע המצויים באתרי הארגון מפני גישה פיזית של גורמים בלתי מורשים, אשר תוצאותיה עשויות להיות חשיפה, גניבה, שינוי או הרס של מידע. ההנחיה קובעת כי יש לבצע ביקורות מדגמיות ביחידות הארגון לשם בדיקת מידת היישום של נוהלי ההגנה הפיזית, וכי הביקורות יוגדרו בתוכנית העבודה השנתית.

הביקורת העלתה כי תוכניות העבודה של רמ"י בתחום אבטחת המידע לשנים 2020 - 2022 לא כללו ביצוע ביקורת בעניין אבטחה פיזית. לגבי תוכנית העבודה לשנת 2023, נמצא כי קיימת בתוכנית העבודה הקצאה של 400 שעות עבודה לסקרי אבטחה פיזית, אולם במועד סיום הביקורת לא בוצעו סקרים כאלו.

מומלץ כי רמ"י תשלים את ביצוע הביקורות לגבי אבטחה פיזית, כנדרש בהנחיית יה"ב.

רמ"י מסרה בתשובתה כי הנושא יטופל במסגרת תוכנית העבודה לשנת 2024.

התמודדות עם נוזקה מסוג כופרה (Ransomware)

תקיפות סייבר מסוג כופרה מונעות מהמשתמש גישה לקבצים או לציוד שברשותו, בדרך כלל באמצעות הצפנת המידע, והתוקפים דורשים מהמשתמש לשלם כופר תמורת החזרת היכולת להשתמש בקבצים או בציוד.

מערך הסייבר הלאומי פרסם באוגוסט 2019 מסמך הסוקר את נושא הכופרות, ובו רשימה מפורטת של המלצות בדבר דרכי ההתמודדות עם התקפת כופרה. המסמך כולל המלצות כיצד להיערך לאירוע כופרה, ובכלל זה התקנת עדכוני אבטחה שמפרסמים יצרני מערכות ההפעלה ומפתחי היישומים השונים, הסרת תוכנות שאינן בשימוש, גיבוי באופן קבוע ביותר משיטה אחת (כונן חיצוני, גיבוי לענן, גיבוי רשתי וכו'), הגבלת סוגי צרופות שניתן לשלוח למשתמשי הארגון, שימוש במערכות המנהלות את חשבונות המשתמשים בצורה מרוכזת ומחליפות את הסיסמאות באופן אוטומטי מפעם לפעם.

לצורך התגוננות מפני נוזקה מסוג כופרה התקשרה רמ"י בשנת 2023 עם חברה פרטית. החברה הכינה עבור רמ"י מסמך "נוהל נוזקת כופר" (להלן - מסמך הכופרה), שמטרתו להכין את רמ"י לכמה תרחישים אפשריים בעניין זה. במסמך הכופרה פורטו בין היתר רשימת הפעולות המומלצות לביצוע במקרה שזוהתה התקפת כופרה.

ביולי 2023 הגישה החברה הפרטית לרמ"י דוח סיכום של סקר מוכנות כופרה שביצעה, אשר במסגרתו בוצעו הדמיות הצפנה לבחינת מערך הניטור. בדוח פורטו תרחישים אפשריים של תקיפות זדוניות ופעולות הגנה שרמ"י אמורה להפעיל (באמצעות כתיבת חוקי הגנה והטמעתם במערכות המידע).

נמצא כי רמ"י החלה ביישום המלצות דוח הסיכום של סקר מוכנות כופרה שביצעה.

על רמ"י להשלים את היערכותה לאירוע כופרה בהתאם להמלצות הדוח ובכלל זה בדיקה חוזרת והטמעה של מוצרים חדשים לאור שינויים ועדכוני גרסאות שנעשו במערכות המידע.

ביצוע מבדקי חדירה

מבדק חדירה (PT - Penetration Test) הוא הליך שבו מתבצעת תקיפה מבוקרת ומתוכננת של המערכות הממוחשבות של הארגון, כדי לאתר בהן חולשות. המבדק יכול להתבצע בכמה סביבות עבודה של המערכות הממוחשבות, ובהן "סביבה נקייה", שבה אפשר לבצע בדיקות שיש בהן סיכון נמוך לגרימת נזק למערכות המידע (סביבת בדיקה - Testing); או לחלופין במערכות הממוחשבות עצמן (סביבת ייצור - Production) באופן שמאפשר לבחון באופן מדויק יותר את החולשות במערכות

הממוחשבות, אך תוך סיכון גדול יותר לפגיעה במערכות אלה. ניתן לבצע סוגים שונים של מבדקי חדירה, ובהם מבדק חדירה אפליקטיבי ומבדק חדירה תשתיתי.

המבדק האפליקטיבי: המבדק האפליקטיבי מאתר את החולשות ביישומים (אפליקציות) מבוססי דפדפן, למשל אתר מרשתת. המבדק מזהה פרצות במערך האבטחה שיכולות לאפשר גישה לבסיסי נתונים, למשל לפרטים אישיים של לקוחות, ולגרום לדליפתם או לשיבושם; ביצוע מתקפות למניעת שירות; ושיבוש מהלך העבודה התקין.

המבדק התשתיתי: המבדק התשתיתי מזהה את הנקודות החשופות ביותר לפגיעה בתשתיות הרשת הפנימית של הארגון, ובכלל זה במערכות ההפעלה שלו, בשרתים ובציוד תקשורת, ומאפשר לארגון לתקן את החולשות שעלו במבדק, לשם התגוננות מרבית מפני התקפות של גורמים זדוניים על הרשת הארגונית.

בתקנות הגנת הפרטיות[45] נקבע כי בעל מאגר אחראי לכך שייערכו מבדקי חדירה למערכות המאגר, לשם בחינת עמידותן בפני סיכונים פנימיים וחיצוניים, אחת ל-18 חודשים לפחות.

בבדיקה עלה כי בשנים 2020 - 2022 ביצעה רמ"י 17 מבדקי חדירה: יש לציין לחיוב היקף זה של מבדקי חדירה שיזמה רמ"י.

עוד נקבע בתקנות הגנת הפרטיות כי בעל מאגר ידון בתוצאות מבדקי החדירה ויפעל לתיקון הליקויים שהתגלו בהם. בהנחיות יה"ב נקבע כי אחד מתפקידי ועדת היגוי סייבר הוא התעדכנות בסיכונים ובאיומים הנוגעים לארגון.

הבדיקה העלתה כי הטיפול בתיקון הליקויים ברמ"י, ובכלל זה ההחלטה בדבר אופן תיקונם, סדרי הקדימות בעניין זה ואי-תיקונם של ליקויים מסוימים, מתבצע על ידי אגף מערכות מידע, בהתאם לשיקול דעתו המקצועי, אולם הסיכונים שעולים במבדקי החדירה אינם מובאים לפני ועדת ההיגוי.

מומלץ כי הסיכונים העולים ממבדקי החדירה וכן הליקויים שלגביהם סובר אגף מערכות המידע כי נוכח סדרי עדיפויות ושיקולים מקצועיים אין מקום או דחיפות לתקנם, יוצגו לוועדת ההיגוי במסגרת ישיבותיה.

רמ"י מסרה בתשובתה כי תוצאות המבדקים יוצגו לוועדת ההיגוי.

מדד יה"ב לבקרות בתחום הגנת סייבר

במסגרת ביצוע תפקידה גיבשה יה"ב מדד בדיקה אחיד לארגוני הממשלה בתחום אבטחת המידע והגנת הסייבר, המכונה "מדד יה"ב". המדד כולל כ-180 בקרות המתבססות על תורת ההגנה בסייבר, על הנחיות יה"ב, על תקנות הגנת הפרטיות ועל תקן ISO-27001[46]. הארגון שמבצע את הבקרות ממלא את שיעור הביצוע לגבי כל בקרה (0% - 100%), ובסוף התהליך מתקבל על בסיס התשובות דירוג של רמת הגנת הסייבר של הארגון לפי רבדים על גבי תרשים (ראו להלן), ונציג יה"ב בודק בשיתוף הארגון את ממצאי המבדק.

ציון מדד יה"ב מבוסס על שקלול של חמישה רבדים של הגנה ואבטחה, שמייצגים ביחד את רמת הגנת הסייבר בארגון. טווח ציוני המדד הוא 1 - 5.

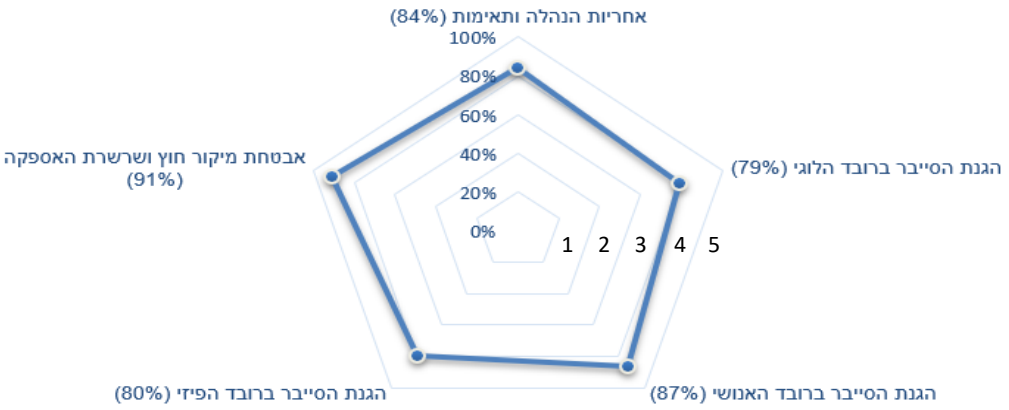
---

45 סעיף 5(ד) לתקנות הגנת הפרטיות (אבטחת מידע), תשע"ז-2017.

46 תקן אבטחת מידע ארגוני ISO 27001 הוא תקן בין-לאומי העוסק במיסוד מערכת ארגונית לניהול אבטחת מידע ובתהליך השוטף של ניהול המערכת ושיפורה. בשנת 2018 הוסמכה רמ"י לראשונה כעומדת בדרישות תקן ISO 27001.

להלן בתרשים רמת ההגנה ברמ"י לפי חמשת רובדי ההגנה של מדד יה"ב, כפי שצוינו בדוח המבדק לשנת 2022 שבוצע על ידי גורמי המקצוע ברמ"י:

תרשים 2: **רמות ההגנה ברמ"י לפי רובד, 2022**



על פי דוחות מדד יה"ב של רמ"י לשנת 2022, בעיבוד משרד מבקר המדינה.

מהתרשים עולה כי על פי דוח מבדק מדד יה"ב משנת 2022 הציון שהתקבל לגבי רמת ההגנה ברמ"י היה 5, כלומר רמ"י מצויה בחמישון העליון מבחינת רמת הגנת הסייבר.

להלן השוואה שעשה משרד מבקר המדינה בין דוח מדד יה"ב של רמ"י לשנת 2022 לבין מצב הדברים כפי שעלה בביקורת לגבי מספר בקרות שבוצעו, כמפורט בלוח שלהלן:

לוח 2: **השוואה בין דוח מדד יה"ב לשנת 2022 לממצאי הביקורת**

הבקרה	שיעור היישום על פי מדד יה"ב לשנת 2022	הממצאים שעלו בביקורת	הערכת הביצוע
כינוס ועדת היגוי סייבר פעמיים בשנה לפחות.	100%	לא התכנסה כנדרש בהחלטת הממשלה.	X
אחת לשנה תוצג המדיניות הארגונית לאבטחת המידע והגנת הסייבר, כנגזרת ממפת סיכוני הסייבר של הארגון. ועדת היגוי סייבר תאשר את מפת הסיכונים ואת המדיניות הנגזרת ממנה, לרבות עמידה בתקנות הגנת הפרטיות.	100%	מדיניות אבטחת המידע הוצגה לאחרונה לוועדת היגוי סייבר בשנת 2019.	X
מסמך המדיניות יכלול פרק "הגנת הפרטיות" אשר ייתן מענה מלא לדרישות שבתקנות.	100%	אין פרק "הגנת הפרטיות" במסמך מדיניות אבטחת המידע של רמ"י.	X
המשימות שעל ועדת היגוי סייבר לבצע הן בין היתר לדון לפחות פעם בשנה במאגרי המידע, ולדון אחת לרבעון לפחות במאגר מידע שחלה עליו רמת האבטחה הגבוהה; לאשר בכל שנה את מדיניות אבטחת המידע והגנת הסייבר; ולהקצות משאבים לצורך מימושה.	100%	משימות אלה אינן מבוצעות בהתאם לנדרש בתקנות.	X
יש ליישם את הנחיית יה"ב 5.30 בנושא גיבוי ושחזור של מידע.	100%	ההנחיה יושמה חלקית, כמפורט בדוח זה.	X

מהלוח עולה כי נמצאו פערים בחמש בקרות, כולן מרובד "אחריות הנהלה ותאימות".

מומלץ כי רמ"י ויה"ב יבחנו את הסיבות לפערים שנמצאו. כמו כן, על רמ"י להמשיך לפעול להעלאת רמות ההגנה במערכותיה, לפעול לתיקון הליקויים שעלו ולקיים בקרה, בשיתוף יה"ב, על תהליך המבדק.

סיכום

רמ"י מופקדת על ניהול אחד המשאבים החשובים ביותר של המדינה - מקרקעי ישראל. רוב המידע שרמ"י אוספת, שומרת ומנהלת הוא מידע רגיש על נכסי מקרקעין, שכולל מיליוני רשומות, ועל כן נדרש לאבטחו ברמת אבטחה גבוהה ביותר. לשם כך מפעילה רמ"י מערכות ומנגנונים להגנה על מאגרי המידע שלה ומערכותיה ונוקטת פעולות לאיתור סיכונים בנושא ולהפחתתם.

בביקורת זו נבדקו היבטים בתחום אבטחת המידע וההגנה על הפרטיות במערכות המידע ברמ"י, ובכלל זה מידת עמידתה של רמ"י בכללים המרכזיים שנקבעו בחוק, בתקנות הגנת הפרטיות ובהנחיות יה"ב. עלה כי רמ"י ביצעה מגוון סקרי סיכונים ומבדקי חדירה למערכותיה, והיא פועלת לתיקון הליקויים בהן, אך פעולותיה בנוגע לפיקוח ובקרה על ניהול תחום הסייבר לקו בחסר: עלה בין היתר שוועדת היגוי סייבר של רמ"י, שאמורה להתוות מדיניות בתחום אבטחת המידע ולפקח על יישומה, להתעדכן בסיכונים ובאיומים הנוגעים לרמ"י ולפקח על ניהול סיכוני הסייבר ברמ"י, לא בחנה ולא אישרה את המיפוי ואת הסיווג של נכסי המידע של רמ"י, לצורך קיום בקרה מיטבית; לא גיבשה סקרי הנהלה, שאמורים לבדוק את טיב ניהול אבטחת המידע והסייבר ברמ"י; ולא עקבה אחר מידת ביצוע תוכניות העבודה בנדון בהתאם לנדרש. כמו כן, לא הוצגו לה הסיכונים שעלו במבדקי החדירה ואופן היישום של התוכניות להפחתתם.

עוד עלו בביקורת פערים בנוגע למנגנון בקרה מסוים ובנוגע לנושא המשכיות תפקודית והתאוששות מאסון.

על רמ"י לפעול לתיקון הליקויים שצוינו בדוח זה, לצורך חיזוק ההגנה על המידע שבידיה והגברת האפקטיביות של הפעולות שהיא נוקטת בתחום זה.

משרד מבקר המדינה
ונציב תלונות הציבור