דוח מבקר המדינה | אייר התשפ"ד | מאי 2024

רשות מקרקעי ישראל

אבטחת המידע והגנת הסייבר ברשות מקרקעי ישראל

אבטחת המידע והגנת הסייבר ברשות מקרקעי ישראל

רקע

רשות מקרקעי ישראל (רמ"י) מופקדת על ניהול מקרקעי ישראל כמשאב, על פי חוק רשות מקרקעי ישראל, התש"ך-1960, לשם פיתוחה של מדינת ישראל ולטובת הציבור, הסביבה והדורות הבאים.

רוב המידע שרמ"י אוספת, שומרת ומנהלת הוא מידע רגיש על נכסי מקרקעין, הכולל נתונים אישיים ועסקיים. כמו כן, רמ"י מפעילה אתר מרשתת (אינטרנט), ובאמצעותו היא נותנת שירות לציבור. 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, לא יימחקו וייחשפו רק למי שמורשה לגשת אליהם מתוקף תפקידו או מכיוון שהמידע נוגע לו.

בכל הנוגע להגנת הפרטיות ולאבטחת המידע הרב שבידיה, רמ"י נדרשת לפעול בהתאם להוראות הדין, ובכלל זה חוק הגנת הפרטיות, התשמ"א-1981 (חוק הגנת הפרטיות), והתקנות שהותקנו על פיו. על פי מיפוי של רמ"י, האיומים עליה כוללים איומים פנימיים, למשל מצד ספקים שיש לה איתם קשר, ואיומים חיצוניים, למשל מצד פצחנים (האקרים) ולקוחות.

נתוני מפתח

עשרות

מערכות מידע שרמ"י משתמשת בהן לצורך ניהול פעילותה

מיליוני

תיקים סרוקים מאוחסנים בשרתים של רמ"י. התיקים הסרוקים כוללים עשרות מיליון מסמכים, הנוגעים בעיקרם לענייני הזכויות על מקרקעי ישראל, ובכלל זה חוזי חכירה, אישורי תשלומים ודוחות פיקוח

2019

השנה האחרונה שבה נדונה ואושרה בוועדת היגוי סייבר ברמ"י מדיניות אבטחת המידע, על אף שינויים ניכרים שהתרחשו מאז אושרה המדיניות

12%

מתוך התקציב עבור הוצאות מחשוב ברמ"י בשנת 2022 הוא לאבטחת מידע וסייבר

מאות אלפי

כניסות לאתר רמ"י נעשות בכל חודש

5 בלבד

מספר מדדי אב בנושא הגנת סייבר שמידת העמידה בהם נבחנה ונדונה בוועדת היגוי סייבר בשנת 2022, מתוך עשרה מדדי אב שהוועדה הייתה אמורה לדון בהם (50%)

5

מאגרי מידע של רמ"י, שאמורים להירשם בפנקס מאגרי המידע כדי להבטיח את ההגנה על פרטיות המידע בהם, לא נרשמו

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].

תמונת המצב העולה מן הביקורת

- **ועדת היגוי לנושאי הגנת הסייבר** - מאז התכנסה ועדת היגוי סייבר ברמ"י לראשונה בשנת 2017, היא לא פעלה לאישור, מיפוי וסיווג של נכסי המידע של רמ"י. נוסף על כך, אף שבוצעו סקרי סיכונים רבים, לא התקיימו דיונים בוועדת היגוי סייבר לגבי התוכניות להפחתת הסיכונים שעלו בהם ואופן ההתמודדות עימם, ובכלל זה תכולות, לוחות זמנים לביצוע, אחריות ומשאבים נדרשים. כמו כן, ועדת ההיגוי לא יזמה ולא גיבשה סקרי הנהלה כנדרש, ולא התכנסה בתדירות הנדרשת לפי החלטת הממשלה בנושא זה. עקב כך נפגעת יכולתה של הנהלת רמ"י לבצע בקרה מיטבית על היעילות והאפקטיביות ביישום הגנת הסייבר ברמ"י ועל מידת התאמתה של תוכנית העבודה לניהול הגנת הסייבר של רמ"י לרמת הסיכון של כל מערכת.

- **מדיניות אבטחת מידע ותוכנית עבודה שנתית להגנת הסייבר** - מדיניות הגנת הסייבר של רמ"י אושרה בוועדת היגוי סייבר בשנת 2019, ומאז לא נבדקה, לא עודכנה ולא נדונה בוועדה ההיגוי, וזאת על אף שינויים ניכרים שהתרחשו משנת 2019 במערך המחשוב של רמ"י, ובכלל זה התפתחויות טכנולוגיות בעולם. עוד עלה כי תוכנית העבודה שהוצגה לוועדת היגוי סייבר כללה רק את פירוט הנושאים המתוכננים לביצוע, ולא כללה לוחות זמנים, גורמים האחראים ליישום, תקציב וסדרי עדיפויות. כמו כן, אין מסמכים המעידים על ביצוע מעקב של הוועדה אחר יישום התוכנית, ובכלל זה אחר תיקון הליקויים שעלו בסקרי הסיכונים ובמבדקי החדירה שבוצעו.

- **קביעת מדדים בנושא הגנת סייבר ועמידה בהם** - בישיבתה במאי 2019 אישרה ועדת היגוי סייבר ברמ"י עשרה מדדי אב שנקבעו בנושאים שונים הנוגעים להגנת סייבר. לדוגמה, מדד שנקבע לנושא מודעות אבטחת מידע הוא כי על 80% מהעובדים להשתתף בהדרכות אבטחת מידע. 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. עוד 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 מדדי האב שאושרו (כ-60%), ובדצמבר 2022 - חמישה בלבד (כ-50%).

- **רישום מאגרי המידע בפנקס מאגרי המידע** - בשנת 2019 אישרה ועדת היגוי סייבר את מינוים של חמישה מנהלים למאגרי מידע עדכניים, ולמאגרים אלה הוכנו מסמכי הגדרות מאגר ומסמכי מבנה מאגר. ואולם בפועל רמ"י לא רשמה מאגרים אלו, כנדרש בחוק, אף

שעברו כחמש שנים מאז הכירה בצורך בכך, ונכון למועד סיום הביקורת חמשת המאגרים טרם נרשמו. עוד עלה כי ועדת ההיגוי לא דנה בסיבות לאי-רישום המאגרים.

- **ניהול הרשאות גישה למאגרי המידע ובקרה על הגישה -** ועדת הרשאות שהוקמה לפי החלטת ועדת היגוי סייבר לא התכנסה, ובפועל מטריצת ההרשאות לגישה נקבעה על ידי אגף מערכות מידע ברמ"י, ללא אישור של ועדת ההרשאות וגם ללא מעורבות של מנהלי המאגרים שעליהם חלה חובת קביעת ההרשאות. 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.

- **תוכניות המשכיות תפקודית (BCP) והתאוששות מאסון (DRP) -** 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. נוסף על כך, ההתקדמות בהכנת התוכנית לא הוצגה לוועדה בסיכומי הפעילות השנתית.

- **אתר חלופי לאסון (DR) -** מערכות המידע של רמ"י נמצאות במספר אתרים. בסיכום סקר סיכוני תשתיות מערכות מידע שביצעה רמ"י במרץ 2019 צוינו סיכונים שונים לגבי אתר מסוים.

ביצוע מבדקי חדירה - בשנים 2017 - 2022 ביצעה רמ"י עשרות סקרי סיכונים ומבדקי חדירה למערכות המידע שלה. עם זאת, הסיכונים שעלו במבדקי החדירה לא הובאו לפני ועדת ההיגוי.

רמת הגנה על פי מבדק יה"ב - לפי דוח מבדק מדד יה"ב[1] משנת 2022, רמ"י מצויה בחמישון העליון מבחינת רמת הגנת הסייבר. עם זאת, נמצאו פערים בחמש בקרות, כולן מרובד "אחריות הנהלה ותאימות".

1 מדד בדיקה אחיד לארגוני הממשלה בתחום אבטחת המידע והגנת הסייבר שגיבשה היחידה להגנת הסייבר בממשלה.

עיקרי המלצות הביקורת

- על רמ"י להביא לאישור ועדת היגוי סייבר את המיפוי והסיווג של נכסי המידע ואת מדיניות הגנת הסייבר שלה ולהשלים את סקרי הסיכונים למערכותיה. על ועדת היגוי סייבר, בהובלת היו"ר (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.
- על רמ"י לפעול לרישום מאגרי המידע העדכניים כנדרש בחוק, ועל ועדת היגוי סייבר לעקוב אחר הרישום כאמור.
- 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.
- על רמ"י להכין תוכנית להמשכיות תפקודית, הכוללת תוכנית להתאוששות מאסון, על בסיס העקרונות שאושרו על ידי ועדת היגוי סייבר.
- כדי לתת מענה מלא באירועי חירום, ובכלל זה להבטיח את היכולת לחזור בהקדם האפשרי לפעילות תקינה וסבירה, על רמ"י לפעול לתיקון הליקוים שעלו בנושא.

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 והפחתתם.

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 בכל הנוגע 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 ולבצע פיקוח 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 להמשכיות 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.