דוח מבקר המדינה

אבטחת המידע והגנת הסייבר ברשות מקרקעי ישראל - תוצאות מבדק חוסן

▪ אייר התשפ"ה ▪ מאי 2025 ▪

אבטחת המידע והגנת הסייבר ברשות מקרקעי ישראל - תוצאות מבדק חוסן

מבוא

בעשור האחרון גברו תקיפות הסייבר על ארגונים ועל אנשים פרטיים ברחבי העולם. בשנת 2023 דווח למערך הסייבר הלאומי[1] על 13,040 אירועי סייבר[2]. בשנת 2021 עלות נזקי הסייבר בעולם הייתה 6 טריליון דולר, ובישראל העלות הכלכלית מוערכת בלפחות 12 מיליארד ש"ח בשנה[3]. אחת ממטרותיהן של תקיפות הסייבר היא לפגוע בחוסנה של מדינת ישראל באמצעות פגיעה בכלכלה ובתפקודו התקין של המשק[4].

רשות מקרקעי ישראל (להלן - רמ"י) מופקדת על פי חוק רשות מקרקעי ישראל, התש"ך-1960, על ניהול מקרקעי ישראל כמשאב, 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 נמסר או לצורך מילוי חובותיה על פי החוק. רמ"י נדרשת להגן על סודיות המידע, אמינותו וזמינותו, ועליה לוודא כי הנתונים לא ישונו ולא יימחקו, וכי הם ייחשפו רק למי שמורשה לגשת אליהם מתוקף תפקידו או כיוון שהמידע נוגע לו[5].

בכל הנוגע להגנת הפרטיות ולאבטחת המידע הרב שבידיה, רמ"י נדרשת לפעול בהתאם להוראות הדין, ובכלל זה חוק הגנת הפרטיות, התשמ"א-1981, 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[6].

על פי דוח של מערך הסייבר הלאומי[7], במחצית הראשונה של שנת 2023 התקבלו ב-SOC הממשלתי[8] התרעות רבות לגבי רמ"י בגין פעילות החשודה כאיום סייבר, אך לפי הדוח לא התרחשו בנוגע להתרעות אלה אירועים חריגים[9].

על הגנת המידע ברמ"י אמון אגף מערכות מידע ומחשוב. האגף אחראי בין היתר לפיתוח מערכות מידע, למתן שירותי תחזוקה, תמיכה, אחסון וטיפול בנוגע לתוכנה ולחומרת המחשוב והתקשורת בכל רשתות הארגון ולהגנה עליהן.

אחד מתפקידיה של רמ"י הוא להקצות קרקע למטרות כגון מגורים, מסחר ותעשייה, והיא עושה זאת בין היתר בדרך של פרסום מכרזי מקרקעין ליזמים ולציבור. על פי נתוני רמ"י בשנת 2022

---

1 המערך הוא גוף ממלכתי, מבצעי וטכנולוגי האמון על הגנת מרחב הסייבר הלאומי ועל הקידום והביסוס של עוצמתה של ישראל בתחום. המערך פועל ברמת המדינה לחיזוק תמידי של רמת ההגנה של הארגונים והאזרחים, לטיפול בתקיפות סייבר ולסילוקן ולהיערכות לחירום.

2 אירוע סייבר הוא התרחשות המעידה על פגיעה אפשרית בפעילותו התקינה של נכס סייבר, אשר יש יסוד להניח כי היא נובעת מפעילות מכוונת במרחב הסייבר.

3 מבקר המדינה, דוחות על הביקורת בשלטון המקומי (2024), "אבטחת מידע של מערכות גבייה ברשויות מקומיות".

4 דוגמה על הנזקים האפשריים של תקיפות הסייבר ראו במבקר המדינה, דוחות על הביקורת בשלטון המקומי (2024), "אבטחת מידע של מערכות גבייה ברשויות מקומיות".

5 מבקר המדינה, דוח מבקר המדינה - מאי 2024, "אבטחת המידע והגנת הסייבר ברשות מקרקעי ישראל".

6 שם.

7 דוח חציוני לשנת 2023 מ-4.6.23.

8 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.

9 מרבית ההתרעות נסגרו על ידי מערך הסייבר הלאומי, לאחר שטופלו ישירות על ידו או לאחר קבלת הבהרה מרמ"י.

היא פרסמה כ-350 מכרזים להקצאת קרקע, ושווקו באמצעות מכרזים כ-83,000 יח״ד למגורים[10], בשווי כולל של מיליארדי ש״ח.

מבדקי חוסן לצורך היערכות לאיומי סייבר

אחת הדרכים להיערכות לאיומי סייבר היא ביצוע מבדקי חוסן, ובהם מבדק חדירה. מבדקים אלו נועדו לבחון את רמת ההגנה של הארגון, לאתר פרצות אבטחה וסיכונים אפשריים בו ולטפל בהם.

מבדק חדירה (Penetration Test) הוא הליך שבו מתבצעת תקיפה מבוקרת ומתוכננת של המערכות הממוחשבות של הארגון, כדי לאתר בה חולשות. המבדק יכול להתבצע בכמה סביבות עבודה של המערכות הממוחשבות, ובהן ״סביבת בדיקות וירטואלית״ (Testing), שבה הסיכון לגרימת נזק למערכות המידע הוא קטן ; ולחלופין במערכות הממוחשבות עצמן (סביבת הייצור - Production)[11]. במבדק בסביבת הייצור אפשר לבחון באופן מדויק יותר את החולשות, אך הסיכון לפגיעה במערכות אלה גדול יותר. ניתן לבצע סוגים שונים של מבדקי חוסן, ובהם מבדק חוסן יישומי - אפליקטיבי ומבדק חוסן תשתיתי.

מבדק חוסן יישומי (אפליקטיבי): המבדק היישומי נועד לאתר את החולשות ביישומים (אפליקציות) מבוססי דפדפן, כמו אתר מרשתת. מטרת המבדק לזהות פרצות במערך האבטחה שיכולות לאפשר גישה לבסיסי נתונים, למשל למידע אישי של לקוחות, ולגרום לדליפתו או לשיבושו, וכן ביצוע של מתקפות למניעת מתן שירות ולשיבוש מהלך העבודה התקין.

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

<u>פעולות הביקורת</u>

בהמשך לדוח הביקורת על אבטחת המידע והגנת הסייבר ברשות מקרקעי ישראל[12] ביצע משרד מבקר המדינה במרץ 2024 מבדק חוסן יישומי (אפליקטיבי) לאחת ממערכות המידע של רמ״י. הביקורת נערכה באגף מערכות מידע ומחשוב ברמ״י. בדיקת החוסן נערכה בסיוע ובליווי של חברת ייעוץ חיצונית והתבצעה בסביבת בדיקות וירטואלית כדי שלא לפגוע במידע הקיים במערכת[13].

ועדת המשנה של הוועדה לענייני ביקורת המדינה של הכנסת החליטה שלא להניח על שולחן הכנסת ולא לפרסם חלקים מפרק זה לשם שמירה על ביטחון המדינה, בהתאם לסעיף 17 (א) לחוק מבקר המדינה, התשי״ח-1958 (נוסח משולב).

---

10 דין וחשבון על פעולות רשות מקרקעי ישראל לשנת התקציב 2022.

11 סביבת הייצור - סביבת העבודה המשרתת את משתמשי הקצה וכוללת מערכות תוכנה ומוצרים טכנולוגיים אחרים.

12 מבקר המדינה, דוח מבקר המדינה - מאי 2024, ״אבטחת המידע והגנת הסייבר ברשות מקרקעי ישראל״.

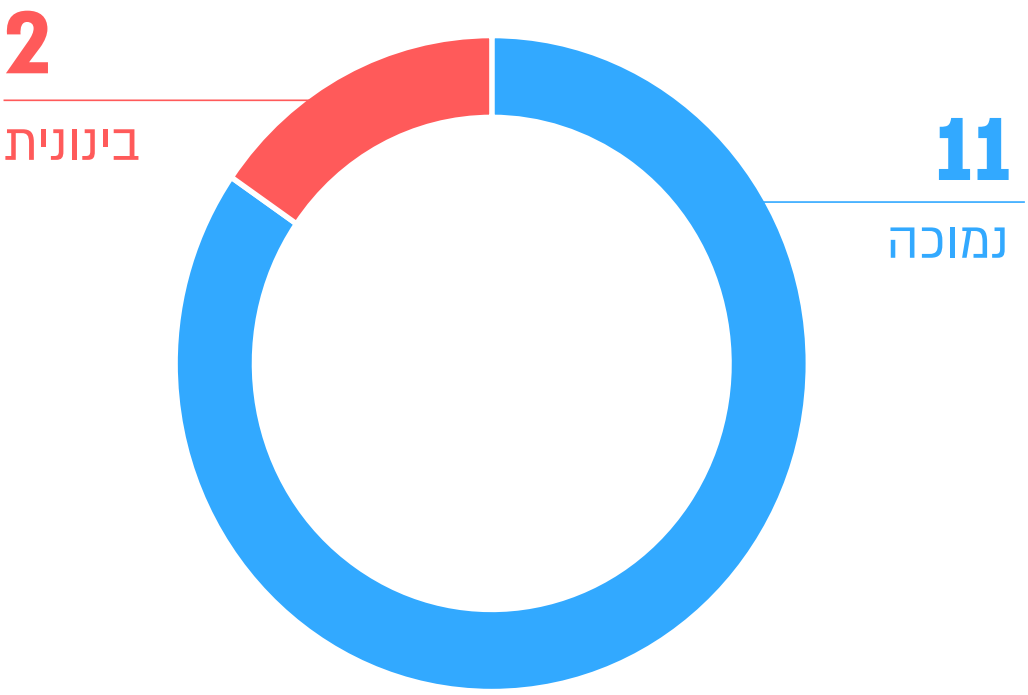
13 סביבת בדיקות וירטואלית היא מערכת המדמה את סביבת הייצור ומאפשרת לבצע בה בדיקות תוכנה בלא לפגוע במידע ובתהליכים בסביבת הייצור.

ליקויים שעלו במבדק החוסן שביצע משרד מבקר המדינה ורמת הסיכון הכרוכה בהם

התכנון והביצוע של מבדק החוסן היישומי (אפליקטיבי) לאחת ממערכות המידע של רמ"י בוצע בשיתוף הנהלת רמ"י. יצוין לטובה שיתוף הפעולה של רמ"י בביצוע מבדק החוסן.

בתרשים שלהלן מוצגים נתונים על ליקויים שעלו בבדיקת החוסן, בחלוקה לפי רמת הסיכון הנשקפת מהם לפעילות הארגון (גבוהה, בינונית או נמוכה). רמת הסיכון נקבעה על פי שקלול של שני אלה: חומרת הנזק הפוטנציאלי של הליקוי והסבירות שהוא אכן יתרחש.

תרשים 2: **ליקויים שנמצאו בבדיקת החוסן שנעשתה למערכת המכרזים במרץ 2024, בחלוקה לפי רמות סיכון**



מהתרשים עולה כי בדיקת החוסן שנעשתה העלתה 13 ליקויים: שני ליקויים ברמת סיכון בינונית ו-11 ליקויים ברמת סיכון נמוכה[14].

[14] יש ליקויים שניתן לייחסם לכמה תרחישים. במקרה כזה רמת החומרה של הליקוי נקבעה על פי רמת החומרה של התרחיש החמור ביותר.

סיכום

רמ"י מקצה קרקעות למגורים, מסחר ותעשייה על ידי פרסום מאות מכרזי מקרקעין מדי שנה בשווי כולל של מיליארדי ש"ח. המידע והמסמכים הנאספים במערכות המידע של רמ"י הם רגישים, ופגיעה בסודיות, בשלמות או בזמינות של המידע שבמערכת עלולה לגרום נזק כלכלי למדינת ישראל.

משרד מבקר המדינה ביצע בדיקת חוסן באחת ממערכות המידע של רמ"י. הבדיקה העלתה בין היתר ליקויים בשירותי הגישה למערכת ובאחת האפליקציות.

על רמ"י לפעול לתיקון הליקויים שעלו בביקורת, כמפורט בדוח זה.

רמ"י מסרה בתשובתה לטיוטת הדוח כי היא פועלת לתיקון הליקויים וליישום מרבית ההמלצות.