דוח מבקר המדינה

אבטחת מערכות המידע במשרד הבינוי והשיכון

▪ סיוון התשפ"ו ▪ מאי 2026 ▪

אבטחת מערכות המידע במשרד הבינוי והשיכון

מבוא

משרד הבינוי והשיכון (להלן - משרד הבינוי או המשרד) אמון על הייזום והביצוע של מדיניות הממשלה בתחומי הבנייה והשיכון. המשרד מתמקד בתכנון ובמתן של פתרונות דיור לכלל האוכלוסייה, בפעולות של התחדשות עירונית, בבנייה חדשה וכפרית, בשיקום שכונות, במשכנתאות ובסיוע בדיור לשכבות הראויות לקידום. משרד הבינוי מלווה את מסלול הייזום והבנייה של מבני מגורים ומוסדות ציבור: איתור ותכנון של הקרקע, שיווק הקרקע ופיתוח תשתיות. לצורך ביצוע תפקידיו פועלות במשרד הבינוי יחידות מסוגים שונים: מטות מקצועיים, מטות תומכים ומחוזות.

לצורך ניהול פעילותו משרד הבינוי משתמש בעשרות מערכות מידע שונות. מערכות אלה כוללות כמה מאות תחנות עבודה, שבהן משתמשים כ-780 עובדים (כולל עובדים במיקור-חוץ). כמו כן מפעיל המשרד אתר מרשתת (אינטרנט) לצורך מתן שירות לציבור. בשנת 2025 הסתכם התקציב עבור הוצאות המחשוב של המשרד בכ-74.5 מיליון ש"ח. כ-6.5 מיליון ש"ח (8.7%) מסכום זה יועדו לצורכי אבטחת מידע.

להלן בתרשים כמה מסוגי המידע שמחזיק משרד הבינוי במערכותיו.

תרשים 1: **כמה מסוגי המידע שמחזיק משרד הבינוי במערכותיו**

הוכן בידי משרד מבקר המדינה.

המידע שמשרד הבינוי אוסף, שומר ומנהל במסגרת פעילותו הוא מידע רגיש כהגדרתו בחוק הגנת הפרטיות, התשמ"א-1981 (להלן - חוק הגנת הפרטיות). מדובר במיליוני רשומות ובהן בין היתר מידע אישי על דיירי הדיור הציבורי, מקבלי סיוע לדיור, משתתפים בתוכניות דיור בהנחה וקבלנים רשומים.

בכל הנוגע להגנת הפרטיות ולאבטחת המידע הרב שבידיו, משרד הבינוי נדרש לפעול בהתאם להוראות הדין, ובהן חוק הגנת הפרטיות, והתקנות שהותקנו על פיו. כמו כן נדרש משרד הבינוי לפעול על פי החלטות ממשלה; הנהלים הפנימיים שלו; והנהלים וההנחיות של הגופים האסדרתיים בנושא, ובראשם מערך הדיגיטל הלאומי[1], שבמסגרתו פועלת היחידה להגנת הסייבר בממשלה (להלן - יה"ב), שהיא הגוף המנחה מקצועית את משרדי הממשלה בתחום הגנת הסייבר. בין היתר יה"ב מפעילה מרכז שליטה ובקרה ממשלתי בנושא איומי סייבר (SOC - Security Operation Center), העוסק בגיבוש תמונת מצב ממשלתית שוטפת בהיבטי הגנת סייבר ובמתן מענה לאירועי סייבר.

על פי דוחות סיכום של מערך הדיגיטל הלאומי, בשנת 2023 התקבלו ב-SOC הממשלתי כמה מאות התרעות לגבי משרד הבינוי בגין פעילות החשודה כאיום סייבר, ובשנת 2024, במהלך מלחמת חרבות ברזל, חל גידול של כ-130% במספר ההתרעות לעומת בשנת 2023.

תקנות הגנת הפרטיות (אבטחת מידע), התשע"ז-2017 (להלן - תקנות הגנת הפרטיות או תקנות אבטחת מידע או התקנות), קובעות בין היתר כי על מאגר מידע של גוף ציבורי שבו יש מידע אישי על 100,000 אנשים ומעלה חלה חובת "רמת האבטחה הגבוהה"[2]. "רמת האבטחה הגבוהה" מחייבת את משרד הבינוי לשמור על המידע שברשותו ולוודא שהוא משמש אך ורק למטרות שלשמן הוא נמסר או לצורכי מילוי חובותיו על פי החוק. משרד הבינוי נדרש להגן על סודיות המידע, אמינותו, זמינותו ומהימנותו, ועליו לוודא כי הנתונים לא ישונו או יימחקו, וכי הם ייחשפו רק למי שמורשה לכך מתוקף תפקידו או למי שהמידע נוגע לו. התקנות מפרטות כיצד יש לשמור על רמת האבטחה שנקבעה למאגר.

פעולות הביקורת

בחודשים פברואר עד ספטמבר 2025 בדק משרד מבקר המדינה את נושא אבטחת מערכות המידע וההגנה על פרטיות המידע במשרד הבינוי והשיכון. בין היתר נבדקו הנושאים האלה: ממשל וניהול של אבטחת מידע וסייבר; ניהול הרשאות ומשתמשים; רישום מאגרי המידע; ותוכניות להמשכיות תפקודית ולהתאוששות מאסון.

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. המונח מדיניות וממשל בתחום מערכות המידע 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[3]. 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)[4] וכן בהחלטת הממשלה 2444 משנת 2015[5] בנושא "קידום ההיערכות הלאומית להגנת הסייבר", שבה קבעה הממשלה כי ההגנה על תפקודו התקין והבטוח של מרחב הסייבר היא יעד ביטחוני לאומי חיוני של המדינה. נוסף על כך, תקנות הגנת הפרטיות קובעות כללים מנחים בתחום אבטחת המידע המצוי במאגרי מידע, ובכלל זה בנוגע למיפוי המערכות, לביצוע סקרי סיכונים ומבדקי חדירה, לניהול הרשאות גישה ולאבטחה פיזית.

---

1 מערך הדיגיטל הלאומי משמש גוף המטה הטכנולוגי של משרדי הממשלה והגופים הציבוריים ופועל לשיפור השירות הממשלתי עבור התושבים והעסקים בישראל.

2 התוספת השנייה (תקנה 1) לתקנות הגנת הפרטיות (אבטחת מידע), התשע"ז-2017 - קישור.

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

4 החלטת הממשלה 2443 מ-15.2.15 - קישור.

5 החלטת הממשלה 2444 מ-15.2.15 - קישור.

ועדת היגוי משרדית להגנת הסייבר: בהחלטת הממשלה 2443 נקבע בין היתר כי על מנכ"לי משרדי הממשלה להקים ועדת היגוי משרדית לנושא הגנת הסייבר שתפעל לשיפור רמת הגנת הסייבר של המשרד (להלן - הארגון) ותפקח על הפעילות השוטפת המבוצעת בארגון בנושא זה (להלן - ועדת היגוי סייבר).

על פי 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; אישור תוכנית העבודה בתחום הגנת הסייבר ובקרה על יישומה; התעדכנות בסיכונים ובאיומים הנוגעים לארגון; פיקוח על ניהול סיכוני הסייבר המבוצע בארגון; ניהול התגובה וההתאוששות מאירוע סייבר. לפי ההנחיה, חברי הוועדה הם מנכ"ל הארגון (יו"ר), ממונה הגנת הסייבר בארגון, מנהלי אגפי משאבי אנוש, מערכות מידע וביטחון בארגון, היועץ המשפטי של הארגון, חשב הארגון ונציג יה"ב.

בביקורת נבדקו פעולות משרד הבינוי וועדת ההיגוי להגנת הסייבר הפועלת במסגרתו, לשם יישום החלטת הממשלה 2443, תקנות הגנת הפרטיות והנחיות יה"ב, בכל הנוגע לניהול תחום הגנת הסייבר ולפיקוח ולבקרה על יישומן. להלן הממצאים:

מדיניות אבטחת המידע

מדיניות אבטחת המידע היא רכיב מהותי ובלתי נפרד מהתשתית הניהולית והטכנולוגית של הארגון. המדיניות נועדה להבטיח את שמירת סודיות המידע, שלמותו וזמינותו, הפחתת סיכוני סייבר וציות לאסדרות וליצור מסגרת ברורה להתנהלות כלל העובדים והגורמים החיצוניים. היעדר מדיניות סדורה או יישום חלקי שלה עלולים לחשוף את הארגון לפגיעות טכנולוגיות, פגיעה בשלמותו וזמינותו של המידע, נזק תדמיתי ופגיעה באמון הציבור.

בהנחיית יה"ב 5.2[6] נקבע כי ועדת היגוי סייבר תאשר את מדיניות הגנת הסייבר בארגון, כי מדיניות זו תיושם בהתאם לעקרונות ולתפיסות בנוגע להגנת הסייבר בארגון, וכי על בסיס מדיניות זו תגובש תוכנית העבודה.

עוד קובעת ההנחיה כי מדיניות הגנת הסייבר בארגון תיבדק ותאושרר על ידי ממונה הגנת הסייבר אחת לשנתיים או מוקדם יותר (במקרה של צורך מיוחד, כגון שינויים ניכרים במערך המחשוב או במערך הארגוני של הארגון), וכי בדיקה ועדכון של המדיניות יאושרו על ידי ועדת היגוי סייבר.

מדיניות הגנת הסייבר של משרד הבינוי אושרה בוועדת היגוי סייבר בשנת 2020. מסמך המדיניות קובע כי עקרונות מדיניות אבטחת המידע יתבססו על מערכת ניהול סיכונים. כמו כן, פורטו בו הגורמים שבאחריותם ליישם את מדיניות האבטחה, ובהם ועדת היגוי סייבר, ממונה אבטחת המידע ונאמני אבטחת מידע במחלקות, וכן נקבעו בו כללים לטיפול בנושאים כגון בקרת גישה, שילוב מנגנוני הצפנה, אבטחת אמצעי מחשוב ניידים ועבודה מרחוק.

על אף שינויים ניכרים שהתרחשו בשנים האחרונות בתחום המחשוב (כגון מעבר לשימוש בשירותי ענן ושימוש בכלי בינה מלאכותית במגזר הציבורי) וכן התפתחויות טכנולוגיות בעולם והתקדמות ביכולות התקיפה של תוקפים פוטנציאליים, הביקורת העלתה כי בניגוד להנחיית יה"ב, מאז אישור מדיניות הגנת הסייבר בשנת 2020 בוועדת היגוי סייבר של משרד הבינוי היא לא עודכנה, לא נדונה ולא נבחנה על ידי הממונה על הגנת הסייבר במשרד הבינוי אחת לשנתיים, וממילא גם לא עודכנה בוועדת היגוי סייבר. עקב כך עולה החשש שבעת התממשות של סיכונים ההגנה מפניהם לא תהיה עדכנית.

על משרד הבינוי לעדכן את מדיניות הגנת הסייבר על כלל היבטיה בהתאם למציאות המשתנה ובאופן עיתי ולהביאה לאישור ועדת היגוי סייבר.

---

[6] סעיף 6.1.4.2.

בתשובתו למשרד מבקר המדינה מדצמבר 2025 (להלן - תשובת משרד הבינוי) מסר משרד הבינוי כי יעדכן את מסמך מדיניות אבטחת המידע ויביאו לאישור ועדת ההיגוי עד סוף שנת 2026.

מיפוי וסיווג של נכסי המידע

1. אחד השלבים הראשונים וההכרחיים בקביעת מדיניות הגנת סייבר של ארגון ויישומה הוא מיפוי וסיווג של נכסי המידע של הארגון. זאת בין היתר כדי שתוכנית העבודה לניהול הגנת הסייבר של הארגון תהיה מותאמת לרמת הסיכון של כל מערכת.

בהנחיית יה"ב 5.2 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 בהן 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.

בביקורת עלה כי מאז התכנסה ועדת היגוי סייבר של משרד הבינוי לראשונה בשנת 2020, היא לא פעלה לאישור, מיפוי וסיווג של נכסי המידע של המשרד, כנדרש בהנחיית יה"ב. בסיכומי ועדת ההיגוי מהשנים 2021 - 2025 אומנם צוין כי במסגרת הליך ההסמכה של משרד הבינוי לתקן ISO 270001 (אבטחת מידע מטעם מכון התקנים) בוצע מיפוי נכסים, וכי מיפוי נכסים הוצג באופן שוטף לחברי הוועדה, אולם הוועדה עצמה לא דנה במיפוי, לא בחנה אותו וממילא לא אישרה אותו, כנדרש בהנחיית יה"ב.

בהיעדר דיון ובחינה לגבי מיפוי נכסי המידע של משרד הבינוי נפגעת יכולתה של הנהלת המשרד לבצע בקרה מיטבית על היעילות והאפקטיביות של יישום מדיניות הגנת הסייבר במשרד ועל מידת התאמתה של תוכנית העבודה לניהול הגנת הסייבר של המשרד לרמת הסיכון של כל מערכת.

על משרד הבינוי להביא את המיפוי והסיווג של נכסי המידע של המשרד לדיון ואישור של ועדת היגוי סייבר.

משרד הבינוי מסר בתשובתו כי הוא ימפה את קובץ הנכסים הדיגיטליים שלו עד סוף שנת 2026, וכי סיווג נכסי המידע יובא לדיון ואישור של ועדת ההיגוי כנדרש.

2. **גיל מערכות המידע:** על פי הנחיות של **ISACA**[7] (APO12 - Managed Risk ו-BAI09 - Managed Assets) וכן לפי תקן **ISO/IEC 27001**[8], ניהול מחזור חיי מערכות המידע הוא נדבך מרכזי באבטחת המידע, ומערכות ותיקות שאינן נתמכות עוד על ידי היצרן ואינן מקבלות עדכוני אבטחה נחשבות לנכס עתיר סיכון העלול לחשוף את הארגון לפגיעות.
מנתוני משרד הבינוי עלה כי יש בו כמה מערכות מידע שהוקמו לפני שנים רבות.

כאמור, נמצא כי ועדת ההיגוי לא דנה ולא אישרה את מיפוי מערכות המשרד, וממילא לא דנה בהשפעת גיל המערכות שבהן מנוהלים נכסי המידע על רמת הסיכון שהן חשופות אליו.

משרד הבינוי מסר בתשובתו כי במסגרת תוכנית העבודה הרב-שנתית שלו ובהתאם לאסטרטגיית המחשוב שתיקבע יבוצע שדרוג של המערכות שהטכנולוגיה בהן היא ישנה, ובאופן הדרגתי הן ישודרגו למערכות עדכניות ומופחתות סיכונים.

---

7 ISACA הוא הגוף הבין-לאומי המוביל בתחומי הבקרה, ניהול הסיכונים ואבטחת המידע. כמו כן, גוף זה הוא שמפתח, מנהל ומסמיך את CISA (Certified Information Systems Auditor).

8 סעיף A.8.1.3 מתייחס לניהול נכסים לאורך חיי מערכת המידע, לרבות זיהוי, תיוג, והערכה של סיכונים. מערכות ותיקות שאינן נתמכות על ידי יצרן (end of support) חייבות להיבחן מחדש, שכן הן חשופות לפרצות אבטחה שאינן מטופלות באמצעות עדכוני אבטחה (patches).

מומלץ כי בדיון במיפוי נכסי המידע, סיווגו ואישורו תתייחס ועדת היגוי סייבר גם למידת השפעת גיל המערכות שבהן מנוהלים נכסי המידע על רמת הסיכון שהן חשופות אליו ולמענה לסיכון.

סקרי סיכונים ומבדקי חדירה

סקרי סיכונים

לפי תקנה 5(ג) לתקנות אבטחת מידע, בעליו של מאגר מידע שחלה עליו רמת אבטחה גבוהה אחראי לביצוע סקר לאיתור סיכוני אבטחת מידע. לאחר שיקבל בעל מאגר המידע את ממצאי הסקר עליו לדון בהם, ואם התגלו ליקויים בתחום האבטחה - לפעול לתיקונם. יש לבצע סקר סיכונים אחת ל-18 חודשים לפחות.

סקר סיכונים הוא הליך שיטתי שנועד לזהות, להעריך ולנתח את רמות הסיכון הנשקפות לארגון, ובפרט למערכות המידע ולתהליכים הקריטיים שבו ; לעמוד על האיומים הפוטנציאליים ; להעריך את סבירות התממשותם ואת חומרת השפעתם ; ולבחון את מידת החשיפה של הארגון לאיומים אל מול בקרות קיימות[9].

בהנחיית יה"ב 5.3 נקבע כי על ארגוני הממשלה לבצע תהליך ניהול סיכוני סייבר. תהליך זה מורכב מארבעה שלבים עיקריים : זיהוי הסיכונים ; הערכתם ; קביעת אופן הטיפול בהם ; והטמעת תוכנית עבודה להפחתתם.

עוד קובעת הנחיית יה"ב 5.3 כי 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 ומשאבים נדרשים.

בשנים 2022 - 2024 ביצע משרד הבינוי שמונה סקרי סיכונים.

בביקורת עלה כי על אף החובה לפי תקנה 5(ג) לתקנות אבטחת מידע לדון בממצאי הסקרים, לגבש תוכנית עבודה מתועדפת להתמודדות עם הסיכונים ולהפחתתם ולהגישה לוועדת היגוי סייבר לקבלת אישורה, בפועל קיימה ועדת ההיגוי דיונים רק לגבי ממצאי שניים משמונת הסקרים שבוצעו. יתר הסקרים לא נדונו, וממילא הוועדה לא קבעה תוכנית להפחתת הסיכונים שעלו בהם. על כן לא מוצתה התכלית של סקרי הסיכונים - זיהוי של הסיכונים וקבלת החלטות על פעולות שיש לנקוט כדי להיערך כראוי לקראתם, למנוע את התממשותם או למזער את הנזק שייגרם אם הם יתממשו.

על משרד הבינוי לדון בתוצאות הסקרים ולגבש תוכנית עבודה להתמודדות עם הסיכונים שהתגלו ולהפחתתם ; יש להביא תוכנית זו לדיון ואישור בוועדת היגוי סייבר.

משרד הבינוי מסר בתשובתו כי בעקבות הביקורת הוסמכה ועדת משנה לנושא. הסיכונים יוצגו לפני ועדה זו בפירוט הנדרש, ובאחריותה יהיה לעקוב אחר הפחתתם ולדווח על כך לוועדת ההיגוי.

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

[9] החשיפה מתארת עד כמה הארגון פגיע בפני איום מסוים למול בקרות קיימות בארגון.

במערכות הממוחשבות, אך תוך סיכון גדול יותר לפגיעה במערכות אלה. ניתן לבצע סוגים שונים של מבדקי חדירה, ובהם מבדק חדירה אפליקטיבי[10] ומבדק חדירה תשתיתי[11].

1. לפי תקנה 5(ד) לתקנות אבטחת מידע, בעליו של מאגר מידע שחלה עליו רמת אבטחה גבוהה, ובכלל זה כאמור משרד הבינוי, אחראי לביצוע מבדקי חדירה למערכות המאגר אחת ל-18 חודשים לפחות, לשם בחינת עמידותן בפני סיכונים פנימיים וחיצוניים.

בביקורת נמצא כי על אף חובתו של בעל מאגר מידע לבצע מבדקי חדירה למערכות המאגרים אחת ל-18 חודשים לפחות בהתאם לתקנה 5(ד) לתקנות אבטחת מידע, בשנים 2021 - 2024 ביצע משרד הבינוי שני מבדקי חדירה אפליקטיביים לשתי מערכות מידע ומבדק חדירה תשתיתי אחד בלבד (בשנים 2021, 2022, 2023), על אף חובתו לבצע מבדקי חדירה בכלל מערכות המאגרים שחלה עליהם רמת אבטחה גבוהה.

על משרד הבינוי לבצע מבדקי חדירה בהיקף נרחב יותר, כמתחייב מתקנות אבטחת המידע.

משרד הבינוי מסר בתשובתו כי בשנת 2025 בוצעו עוד כמה סקרים ומבדקי חדירה. כמו כן, בתוכנית העבודה של שנת 2026 נכללים עוד מבדקי חדירה וסקרי סיכונים תשתיתיים ואפליקטיביים.

2. תקנות אבטחת מידע קובעות כי על בעל המאגר לדון בתוצאות מבדקי החדירה ולפעול לתיקון ליקויים שהתגלו. בהנחיות יה"ב נקבע כי אחד מתפקידי ועדת היגוי סייבר הוא התעדכנות בסיכונים ובאיומים הנוגעים לארגון.

בביקורת עלה כי על אף חובתו של בעל מאגר מידע לדון בתוצאות מבדקי החדירה בהתאם לתקנה 5(ד) לתקנות אבטחת מידע ולפעול לתיקון ליקויים שהתגלו, ממצאי המבדקים שביצע משרד הבינוי, לא הובאו בפני ועדת היגוי סייבר כמתחייב. יתרה מכך, לא נמצאו מסמכים המעידים על טיפול כלשהו של המשרד בסיכונים שהתגלו במבדקים, ובכלל זה פעולות לתיקון הליקויים ומבדקים חוזרים במטרה לוודא שהליקויים תוקנו ואינם חוזרים על עצמם.

על משרד הבינוי לדון בתוצאות מבדקי החדירה, לעדכן את ועדת היגוי סייבר בסיכונים ובאיומים העולים מהם ולנקוט פעולות לתיקון הליקויים שעלו בהם, בהתאם לדרישות תקנות אבטחת מידע. על ועדת ההיגוי לעקוב אחר תיקון הליקויים.

משרד הבינוי מסר בתשובתו כי בעקבות הביקורת הוסמכה ועדת משנה לנושא. הסיכונים יוצגו לפני ועדה זו, ובאחריותה לעקוב אחר הפחתתם ולדווח על כך לוועדת ההיגוי.

אי-עמידה על ביצוע מלא של סקרי סיכונים ומבדקי חדירה שנקבעו בהסכם התקשרות עם ספק

משנת 2018 משרד הבינוי מקבל שירותי מיקור-חוץ מחברה האחראית לתפעול ותחזוקה של תשתיות מחשוב מרכזיות וציוד קצה. בתנאי המכרז נקבע, בין היתר, כי החברה הזוכה במכרז מחויבת להתקשר עם ספק משנה בלתי תלוי שיבצע באופן שוטף סקר סיכונים מלא לפחות פעם ב-18 חודשים לכל מערכות המשרד וכן לבצע מבדקי חדירה מהרשת הפנימית.

הביקורת העלתה כי משרד הבינוי לא עמד על כך שהחברה האחראית לתפעול ותחזוקה של תשתיות מחשוב מרכזיות תיישם את מלוא הדרישות שהוגדרו בהסכם ההתקשרות עימה - ביצוע

---

10 מבדק אפליקטיבי מאתר את החולשות ביישומים (אפליקציות) מבוססי דפדפן, למשל אתר מרשתת. המבדק מזהה פרצות במערך האבטחה שיכולות לאפשר גישה לבסיסי נתונים, לגרום לדליפתם או לשיבושם ולהביא לשיבוש מהלך העבודה התקין.

11 מבדק תשתיתי 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.

סקרי סיכונים לפחות אחת ל-18 חודשים ומבדקי חדירה. בפועל החברה ביצעה באופן חלקי בלבד מבדקי חדירה וסקרי סיכונים שנדרשו ממנה.

על משרד הבינוי לוודא עמידה של ספקי השירות בהתחייבויותיהם לביצוע סקרי סיכונים ומבדקי חדירה בהתאם להסכמי ההתקשרות עימם. נוסף על כך, מומלץ כי משרד הבינוי יקיים תהליך של הפקת לקחים בעניין אי-ביצוע מלוא הסקרים והמבדקים כנדרש ויחיל מנגנוני פיקוח ובקרה שיבטיחו עמידה של ספקים בתנאי ההתקשרות עימם, לרבות בכל הנוגע לביצוע סקרי סיכונים ומבדקי חדירה.

משרד הבינוי מסר בתשובתו כי אגף טכנולוגיות דיגיטליות ומידע במשרד (להלן - אגף טד"ם) החל לוודא את עמידתם של ספקי השירותים בהתחייבויותיהם החוזיות בנושא אבטחת מידע ויוודא את הביצוע על פי תוכנית העבודה בשנים הבאות.

החברה מסרה בתשובתה למשרד מבקר המדינה מדצמבר 2025 כי משנת 2021 בוצעו שני מבדקי חדירה וסקר סיכונים, ובשנת 2023 הוטמעה מערכת המבצעת הדמיות (סימולציות) של מבדקי חדירה באופן יום-יומי. החברה הוסיפה כי תחל בתהליך לביצוע סקר סיכונים עבור עשר מערכות מידע בהתאם להוראות ההסכם ולהנחיות משרד הבינוי.

קביעת מדדים ובחינתם בנושא הגנת סייבר

הנחיית יה"ב 5.2[12] קובעת כי על ועדת היגוי סייבר לגבש מדדים כמותיים בנושאי הגנת הסייבר ולהגדיר יעדים כמותיים אשר באמצעותם ניתן יהיה למדוד ולבחון את רמת האפקטיביות של הגנת הסייבר, על ועדת היגוי סייבר גם לבחון את מידת העמידה ביעדים אחת לחצי שנה, במסגרת סקר הנהלה.

בדצמבר 2021 אישרה ועדת היגוי סייבר במשרד הבינוי שבעה מדדי אב בנושאי הגנת סייבר, ולכל נושא נקבעו מדדים כמותיים. לדוגמה, הוועדה קבעה בנושא סקרי בקרת גישה כי יבוצעו בשנה שני סקרי בקרת גישה לפחות. מדד נוסף שנקבע הוא כי יבוצעו סקרים אפליקטיביים על שלוש מערכות מידע שונות לפחות.

בביקורת עלה כי משנת 2022 ועד למועד סיום הביקורת, ספטמבר 2025, תקופה של שלוש וחצי שנים, ועדת היגוי סייבר בחנה את מידת היישום של המדדים באופן חלקי בלבד, ולא בכל חצי שנה, כנדרש בהנחיית יה"ב. עקב כך נפגעה יכולתה לבחון את רמת האפקטיביות של תשתית הגנת הסייבר ולבצע שינויים כאשר הדבר נדרש.

בביקורת עלה כי בדיוני ועדת היגוי סייבר שהתקיימו בפברואר 2023, בינואר 2024 ובינואר 2025 הוצגו לוועדה רק חלק ממדדי האב שאושרו בדצמבר 2021. בפברואר 2023 הוצגו לוועדה שלושה משבעת המדדים שאושרו (כ-43%), בינואר 2024 - חמישה משבעת המדדים שאושרו (כ-71%), ובינואר 2025 - ארבעה משבעת המדדים שאושרו (כ-57%). הביקורת העלתה כי גם במקרים שהמדדים הוצגו לוועדה, לא צוינה מידת העמידה בהם. עוד עלה כי הוועדה לא דנה בעניין אי-הצגתם של יתר המדדים שאושרו.

נמצא אפוא כי אף שהנחיית יה"ב קובעת כי באמצעות גיבוש מדדים כמותיים ועדת היגוי סייבר תוכל לבחון את רמת האפקטיביות של הגנת הסייבר, בפועל מיעוט הדיונים של ועדת ההיגוי, ובכלל זה במידת העמידה במדדים, ואי-ההעמקה הנדרשת בהם הקשו עליה לבחון את רמת האפקטיביות של הגנת הסייבר, דבר המקשה על משרד הבינוי לבחון את מידת היישום של הגנת הסייבר במשרד.

על הוועדה לבצע בחינה סדורה של עמידה ביעדים אחת לחצי שנה, תוך הפקת לקחים, המלצות לשיפור ועדכון של המדדים במידת הצורך.

---

[12] סעיף 5.5 - הנחיית מסגרת להגנת הסייבר בממשלה.

משרד הבינוי מסר בתשובתו כי מנהל יישום הגנת הסייבר יקבע מדדים ויאשרר אותם מול ועדת ההיגוי, וכי ועדת ההיגוי תבצע מעקב על כך.

פעולות ממונה הגנת הסייבר

ממונה הגנת הסייבר הוא דמות מרכזית בעניין התכנון, הניהול, הטיפול והבקרה בנוגע למכלול היבטי הגנת הסייבר בארגון, ולכן תפקידו נקבע בהחלטת ממשלה, נוכח מרכזיותו והצורך באי-תלותו של ממונה הגנת הסייבר. בהחלטת הממשלה 2443 נקבע כי יש להטיל על המנכ"לים של גופי הממשלה לפעול לשיפור רמת הגנת הסייבר, ולשם כך למנות ממונה הגנת סייבר שיהיה כפוף ישירות למנכ"ל או למי מטעמו.

הנחיות יה"ב[13] קובעות כי ממונה הגנת הסייבר אחראי להבטיח את התכנון, הניהול, הטיפול והבקרה בנוגע למכלול 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 היישום והניהול של הגנת הסייבר בהיבט הארגוני הרחב ובהתאם למדיניות; ייזום וניהול של סקרי הנהלה; גיבוש ואישור של נוהלי הגנת הסייבר בארגון; תיאום פעילויות ההגנה בין הגורמים הרלוונטיים בארגון; הגברת המודעות של עובדי הארגון לנושאי הגנת הסייבר; ביצוע סקרים לבחינת הרשאות הגישה למשתמשים במערכות המידע; וניהול ויישום של תוכנית מבדקים פנימיים, אשר יבוצעו על ידו או על ידי מי מטעמו.

במשרד הבינוי מונה ממונה הגנת סייבר בפברואר 2021. בבדיקה עלה כי הממונה מילא חלק מהתפקידים שלו כפי שנקבעו בהנחיית יה"ב - הוא היה שותף לדיוני ועדת היגוי סייבר כחבר בוועדת ההיגוי, עסק בגיבוש ואישור של נוהלי הגנת הסייבר במשרד, קיים פגישות עיתיות עם צוותי אבטחת המידע ועם נציגי יה"ב ופעל להגברת המודעות של עובדי המשרד לנושאי הגנת הסייבר. כמו כן, הוא היה שותף לביצוע סקרי סיכונים תהליכיים באגפים שונים במשרד הבינוי. ואולם הוא לא היה שותף בביצוע סקרים לבחינת הרשאות הגישה למשתמשים במערכות המידע ולא היה מעורב בסקרי סיכונים ובמבדקי חדירה אשר בוצעו על ידי אגף טד"ם והתמקדו בהיבטים טכנולוגיים-מחשוביים. עקב כך תמונת המצב שהייתה בידו ובידה של ועדת היגוי סייבר לא הייתה מלאה[14].

משרד הבינוי מסר בתשובתו כי על פי החלטת מנכ"ל המשרד, מיוני 2025 הועברו הסמכויות בנושא הגנת הסייבר לאגף טד"ם. משרד הבינוי ציין כי הוא מבצע סקרים לבחינת תקפות ההרשאות, וכי בשנת 2025 הסתיים יישומה של תוכנית מקיפה להפחתה ניכרת של ההרשאות שאינן נצרכות, לעומת העבר.

ממונה הגנת הסייבר הוא דמות מרכזית בעניין התכנון, הניהול, הטיפול והבקרה בנוגע למכלול היבטי הגנת הסייבר בארגון, ולכן תפקידו נקבע בהחלטת ממשלה. אשר למשרד הבינוי, על ממונה הגנת הסייבר להשתתף באופן פעיל בתכנון, בניהול, בטיפול ובבקרה בנוגע למכלול היבטי הגנת הסייבר במשרד, בהתאם לנדרש בהנחיות יה"ב, ובכלל זה בניהול וביישום של התוכנית לביצוע סקרי סיכונים ומבדקים.

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 ולהתייחס לכלל הנושאים המהותיים, לרבות טיפול בסיכוני סייבר.

---

13 הנחיית יה"ב 5.2, סעיף 6.3 והנחיית יה"ב 5.12 בנושא "ניהול ותפעול הרשאות".

14 יצוין כי במהלך הביקורת (יוני 2025) סיים ממונה הגנת הסייבר את כהונתו בתפקיד, והאחריות לנושא הועברה למנהלת מערכות המידע במשרד.

בביקורת עלה כי תוכניות העבודה השנתיות בשנים 2022 - 2023 לא גובשו בהתאם למתווה שבהנחיית יה"ב, אלא הן גובשו כמקבץ של החלטות של ועדת ההיגוי בנושאים הנוגעים לסיכונים רוחביים לארגון והגורמים האחראים ליישומן, ולא נכללו בהן משימות שחובה על המשרד לבצען לפי תקנות הגנת הפרטיות והנחיות יה"ב, כגון מבדקי חדירה ומשימות להפחתת סיכונים שעלו במבדקים ובסקרים. בשנת 2024 הביא אגף טד"ם לאישור ועדת ההיגוי תוכנית עבודה שנתית בנושא אבטחת מידע, אך בתוכנית זו לא פורטו הגורמים האחראים ליישום, אומדן כוח האדם והתקציב הנדרשים וכן סדרי עדיפויות לביצוע, וגם בה לא נכללו משימות שחובה על המשרד לבצען לפי תקנות הגנת הפרטיות והנחיות יה"ב, כגון מבדקי חדירה. יצוין כי גם תוכניות העבודה הכלליות של אגף מערכות המידע לשנים 2022 - 2024 לא כללו משימות ייעודיות בתחום אבטחת המידע, למעט משימה כללית של ביצוע פעולות "לשיפור אבטחת המידע" בשנת 2022.

עוד עלה כי ועדת היגוי סייבר לא קיימה מעקב ובקרה שיטתיים לגבי יישומה של תוכנית העבודה שאישרה בשנת 2024, כנדרש בהנחיית יה"ב.

נוסף על כך עלה כי גם במקרים שבהם קיבלה ועדת היגוי סייבר החלטות בדבר פעולות לביצוע, היא לא תמיד עקבה אחר אופן ביצוען. לדוגמה, בישיבה שהתקיימה ב-30.1.23 הנחתה הוועדה לבצע לפחות פעמיים בשנה סקרי הרשאות גישה למערכות המידע של כלל המשתמשים, ובפרט משתמשי-העל (משתמשים עם הרשאות עודפות). עם זאת, משימות אלה לא בוצעו בפועל, והוועדה לא בדקה אם בוצעו.

אי-גיבושן של תוכניות עבודה שנתיות באופן הנדרש בהנחיית יה"ב וכן היעדר בקרה ומעקב מלאים ושיטתיים לגבי היישום שלהן ושל החלטות נוספות של ועדת ההיגוי עלולים לפגוע ביכולת הארגון לטפל בסיכוני סייבר באופן מתוכנן, סדור ויעיל ולהותיר ליקויים מהותיים ללא מתן מענה בזמן.

על אגף טד"ם להביא לאישור ועדת ההיגוי את תוכניות העבודה השנתיות בנושא אבטחת מידע מלאות ומפורטות שייגזרו מסקרי הסיכונים בהתאם להנחיית יה"ב, לרבות פירוט לוחות זמנים, אומדן עלויות, כוח האדם הנדרש, הגדרת הגורמים האחראים וסדרי עדיפויות, על ועדת היגוי סייבר לפעול לאישור של תוכניות עבודה שנתיות אלו ולקיים בקרה ומעקב שוטפים לגבי יישום התוכניות וביצוע החלטותיה.

משרד הבינוי מסר בתשובתו כי ממונה יישום הגנת הסייבר יציג בוועדת ההיגוי את תוכנית העבודה ויאשרר אותה.

תקציב שנתי להגנת הסייבר

לפי החלטת הממשלה 2443[15], המנכ"לים של משרדי הממשלה ומנהלי יחידות הסמך יסדירו במסגרת סמכותם ואחריותם את מבנה התקציב השנתי של המשרדים והיחידות, כך שלפחות 8% מהתקציב שיוקצה לתחום טכנולוגיית המידע יופנה להגנת הסייבר[16].

בדיון ועדת היגוי סייבר שהתקיים במרץ 2021 עלה קיומו של פער תקציבי ניכר בתחום אבטחת המידע. בעקבות זאת הוחלט לבחון הקצאת תקציב ייעודי לנושא זה אשר יהיה נפרד מתקציב אגף טד"ם, וזאת לשם עמידה בדרישות החלטת הממשלה.

בישיבת ועדת ההיגוי שהתקיימה בפברואר 2023 דווח כי הוקצה תקציב ייעודי לאבטחת מידע, אך לא צוין מה הוא שיעור התקציב שהוקצה בפועל, ולא נבדק אם הוא עומד בדרישות החלטת הממשלה.

---

15 נספח ו', סעיף 4א.

16 בהחלטת הממשלה נקבע כי מנכ"ל משרד ממשלתי, יוכל בנסיבות מיוחדות לאשר הפחתה מהאמור בהחלטה מפורטת ומנומקת שתדווח לוועדת ההיגוי הממשלתית, ובלבד שלפחות 6% מתקציב תחום טכנולוגיית המידע יופנה להגנת הסייבר.

בדיון של ועדת ההיגוי שהתקיים בינואר 2025 עלה כי אין בידי הוועדה מידע אם אכן הופנו לפחות 8% מהתקציב לתחום טכנולוגיית המידע לנושאי הגנת סייבר, כנדרש בהחלטת הממשלה 2443. בעקבות כך התבקש אגף טד"ם למסור לוועדה דוח לגבי ניצול התקציב של הגנת סייבר בשנת 2024 וכן דוח תכנון תקציבי עבור שנת 2025, אך במועד סיום הביקורת דוחות אלו טרם נמסרו לוועדה.

ביולי 2025 מסר משרד הבינוי למשרד מבקר המדינה כי בשנת 2024 התקציב לאבטחת מידע והגנת הסייבר לא היה "צבוע" בצורה מסודרת כחלק מתקציב אגף טכנולוגיות דיגיטליות ומידע, וכי התקציב עבור אבטחת מידע והגנת הסייבר לשנת 2025 הוא 6.5 מיליון ש"ח[17], שהם כ-9% מסך תקציב האגף - 74.5 מיליון ש"ח.

יוצא אפוא כי בשנים שנבדקו בביקורת לא היה לוועדת ההיגוי מידע בדבר שיעור התקציב המיועד לאבטחת מידע מכלל התקציב המיועד לטכנולוגיות המידע, כדי לוודא כי משרד הבינוי עומד בנקבע בהחלטת הממשלה ומקצה לפחות 8% מהתקציב בתחום טכנולוגיות המידע להתמודדות עם סיכוני האבטחה הנשקפים לו.

משרד הבינוי מסר בתשובתו כי התקציב השנתי להגנת הסייבר הוצג למנכ"ל המשרד בישיבה מיוחדת לנושא הסייבר שהתקיימה בנובמבר 2025 (לאחר מועד סיום הביקורת), וכי בישיבת וועדת היגוי סייבר, שתתקיים בסוף שנת 2025, יוצג התקציב לשנת 2026.

על משרד הבינוי לוודא כי הוא עומד בהוראות החלטת הממשלה 2443 ומקצה לפחות 8% מתקציב תחום טכנולוגיית המידע לנושאי הגנת הסייבר. לשם כך עליו לבצע מיפוי תקציבי מלא של כלל ההקצאות בתחום אבטחת המידע והגנת הסייבר באופן שישקף את המשאבים שהושקעו בנושא, ולהביא מיפוי תקציבי זה לפני ועדת היגוי סייבר.

כינוס ועדת היגוי סייבר

בהחלטת הממשלה 2443[18] נקבע כי על ועדת היגוי סייבר להתכנס לכל הפחות פעם בחצי שנה.

בביקורת עלה כי ועדת היגוי סייבר של משרד הבינוי לא התכנסה באופן סדיר בהתאם לנדרש בהחלטת הממשלה - להתכנס לכל הפחות פעם בחצי שנה, מאז התכנסה לראשונה בפברואר 2020: בשנים 2020, 2023 ו-2024 הוועדה התכנסה פעם אחת בשנה בלבד, בשנת 2022 היא לא התכנסה כלל, ורק בשנת 2021 היא התכנסה פעמיים בשנה כנדרש. אשר לשנת 2025, הוועדה התכנסה בפברואר 2025.

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

על ועדת היגוי סייבר להקפיד להתכנס לכל הפחות פעם בחצי שנה בהתאם לנדרש בהחלטת הממשלה.

משרד הבינוי מסר בתשובתו כי מנכ"ל המשרד הנחה לכנס את ועדת ההיגוי לפחות פעם ברבעון.

☆

ממצאיו של פרק זה משקפים פערים ניכרים בנוגע לדרך פעולתה של ועדת היגוי סייבר במשרד הבינוי, בעיקר בתחום ניהול סיכוני אבטחת המידע ובתחום הבקרה הניהולית על יישום המדיניות, ובכלל זה אי-אישור מדיניות עדכנית, אי-בחינה ואישור של המיפוי והסיווג של נכסי המידע, מיעוט דיונים בממצאי סקרי סיכונים ובממצאי מבדקי חדירה והיעדר מעקב אחר תיקון

---

17 1.5 מיליון ש"ח עבור רכש שירותי אבטחת מידע, 2.4 מיליון ש"ח עבור רכש מוצרי אבטחת מידע ו-2.6 מיליון ש"ח עבור כוח אדם המתמחה באבטחת מידע.

18 נספח ו' להחלטה, סעיף 3.ג.

הליקויים העולים ואחר הכנה וביצוע של תוכניות העבודה. הוועדה גם לא התכנסה בתדירות שנקבעה בהחלטת הממשלה. בכך נפגעת היכולת של הוועדה לבצע בצורה מיטבית בקרה ניהולית על יישום הגנת הסייבר במשרד הבינוי, להתוות אסטרטגיות לפעילות הגנת הסייבר, להעריך את הנזקים בעקבות תקלות ולגבש המלצות לטיפול.

על ועדת היגוי סייבר לפעול לתיקון ליקויים אלה, לשם חיזוק האפקטיביות של הגנת הסייבר במשרד הבינוי.

רישום מאגרי המידע וניהולם

על פי סעיף 17 לחוק הגנת הפרטיות, בעל שליטה במאגר מידע ומחזיק במאגר מידע אחראים לאבטחת המידע שבמאגר המידע. על פי החוק, גוף ציבורי מחויב ככלל ברישום מאגר המידע במרשם (פנקס) מאגרי המידע[19], והאחריות להגשת הבקשה לרישום המאגר מוטלת עליו. מטרת הרישום היא להבטיח את ההגנה על פרטיות המידע שבמאגר המידע ולתת כלים, הן בידי רשם מאגרי המידע והן בידי מי שמידע עליו מנוהל במאגר המידע, לאכוף את החובות המצוינות בחוק הגנת הפרטיות על בעל המאגר.

לפי מרשם מאגרי המידע, משרד הבינוי רשום כבעלים של 13 מאגרי מידע שנרשמו בשנת 2005. לצד זאת, ישנם במשרד הבינוי מאגרי מידע שאינם רשומים.

לפי תקנות הגנת הפרטיות[20], על בעל מאגר מידע לנהל מסמך הגדרות מאגר[21] 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. התקנות גם קובעות כי על בעל מאגר מידע להכין מסמך מעודכן של מבנה המאגר וכן רשימת מצאי מעודכנת של מערכות המאגר, שתכלול בין השאר תוכנות וממשקים המשמשים לתקשורת עם מערכות המאגר, וכן להגדיר מנהל מאגר שיוודא כי המאגר מנוהל בהתאם לחוק ולתקנות. הוראות אלה נכנסו לתוקפן באפריל 2018.

בביקורת עלה כי אף שתקנות הגנת הפרטיות קובעות כי על בעל מאגר מידע לנהל מסמך הגדרות מאגר ולהכין מסמך מעודכן של מבנה המאגר, משנת 2018 ועד מועד סיום הביקורת, ספטמבר 2025, משרד הבינוי לא השלים את רישומם של מאגרי המידע בפנקס מאגרי המידע באופן הנדרש בתקנות.

הביקורת העלתה כי בינואר 2024 משרד הבינוי החליט לאחד כמה ממאגרי המידע אשר נרשמו בשנת 2005 ולרשום שני מאגרים חדשים הנמצאים ברשותו, כך שמספר המאגרים שעליו יהיה לרשום בהתאם לנדרש בתקנות מ-2018 הסתכם בתשעה. עם זאת, נכון למועד סיום הביקורת משרד הבינוי הכין מסמך הגדרת מאגר ומסמך מבנה מאגר לשני מאגרי מידע בלבד מתוך התשעה. לגבי יתר שבעת המאגרים, הוא אף לא הכין את המסמכים הנדרשים לצורך קידום רישומם באופן הנדרש בתקנות. יוצא אפוא כי משרד הבינוי לא הסדיר את רישום כל מאגרי המידע שברשותו באופן הנדרש בתקנות, אף שעברו כשמונה שנים מאז נכנסו התקנות לתוקפן.

עוד עלה בביקורת כי רק בשנים 2024 - 2025 מינה משרד הבינוי מנהלים למאגרי המידע שברשותו, אף שהיה עליו לעשות כן בשנת 2018.

על משרד הבינוי להסדיר את רישומם של מאגרי המידע שברשותו באופן הנדרש בתקנות, ועל ועדת ההיגוי לעקוב אחר יישום הרישום והשלמתו כנדרש.

---

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

20 סעיף 2.

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

משרד הבינוי מסר בתשובתו כי לקראת שנת 2026 הוא ישים דגש בהסדרת המאגרים, וכי התוצאות בנושא זה יוצגו לפני ועדת ההיגוי.

ניהול הרשאות גישה

ניהול הרשאות גישה למערכות מידע נועד להגביל את הגישה למידע ולאפשר אותה רק למי שהמידע נדרש לו, ובכך להגן על פרטיות המידע האישי שבמערכות המידע ולהפחית את הסיכון לדליפות מידע רגיש ולשימוש לרעה במידע כזה.

בתקנות הגנת הפרטיות נקבע[22] כי בעל מאגר מידע יקבע את הרשאות הגישה של בעלי ההרשאות למאגר המידע ולמערכות המאגר, בהתאם להגדרות התפקיד ובמידה הנדרשת לביצוע התפקיד בלבד. עוד נקבע כי בעל מאגר מידע ינהל רישום מעודכן של תפקידים, הרשאות הגישה שניתנו לגביהם ובעלי ההרשאות הממלאים תפקידים אלה.

סקר הרשאות למשתמשים

כדי לוודא שיש התאמה בין המשתמשים ותפקידם להרשאות הקיימות נדרש לבצע סקר הרשאות. בהנחיית יה"ב 5.12 בנושא "ניהול ותפעול הרשאות" נקבע כי אחת לשנה מנהל הגנת הסייבר יפיק דוח הרשאות של כל המשתמשים במערכות, על פי המחלקות. דוח זה יועבר למנהלי המחלקות לבדיקה ולאישור ההרשאות הקיימות לכל עובד.

1. **בביקורת עלה כי לגבי יותר ממחצית המערכות לא נסקרו הרשאות המשתמשים אחת לשנה כנדרש בהנחיות יה"ב.**

   על משרד הבינוי לבצע סקירת הרשאות בכלל מערכותיו כנדרש בהנחיות יה"ב ולוודא שקיימות הרשאות פעילות למשתמשים מורשים בלבד.

   משרד הבינוי מסר בתשובתו כי סקר ההרשאות בוצע למערכות הליבה העיקריות שבהן מתנהלת רוב הפעילות העסקית של משרד הבינוי, וכי בשנת 2026 יבוצע סקר גם ליתר המערכות.

2. משרד הבינוי מנהל את המשתמשים במערכותיו באמצעות מערכת Active Directory (AD) שבה ניתן לזהות את כלל המשתמשים במערכות. לבקשת משרד מבקר המדינה הפיק משרד הבינוי קובץ ADUser (להלן - קובץ המשתמשים) שבו יש מידע על פרטי החשבונות של המשתמשים ברשת המחשבים שלו נכון למרץ 2025.

   לפי נתוני סקר ההרשאות, נכללו בו 767 משתמשים. משרד מבקר המדינה השווה בין המשתמשים שנכללו בסקר ההרשאות לבין רשימת העובדים הפעילים של משרד הבינוי[23] ורשימת נותני השירות החיצוניים (הרשומים בקובץ המשתמשים).

   בהתאם להנחיית יה"ב, על מנהל הגנת הסייבר להפיק דוח הרשאות של כל המשתמשים שיועבר למנהלי המחלקות לבדיקה ואישור ההרשאות הקיימות.

   עובדים פעילים של משרד הבינוי: בקובץ העובדים הפעילים של משרד הבינוי נכללים 528 עובדים.

   בבדיקה נמצא כי לא כל העובדים הפעילים נכללו בסקר ההרשאות. כלומר, חלק מהעובדים הפעילים של משרד הבינוי לא עברו סקירה תקופתית כנדרש בהנחיית יה"ב, וממונה הגנת

---

[22] סעיף 8.

[23] על בסיס קובץ מאגף הון אנושי במשרד הבינוי שכולל עובדים המועסקים במשרד הבינוי (אופן ההעסקה: מינוי בפועל, מילוי מקום, קבוע, תקופת ניסיון, חל"ת/חל"ד).

הסייבר לא בדק אם ההרשאות שלהם תואמות את תפקידם. הדבר עשוי ליצור סיכון אבטחה למשרד.

נותני שירות חיצוניים: נוסף על העובדים הפעילים במשרד, קיימים נותני שירות חיצוניים[24]. בקובץ המשתמשים נכללו 229 עובדים במיקור-חוץ שהם משתמשים פעילים, 115 מהם באגף טכנולוגיות דיגיטליות ומידע.

ואולם בבדיקה נמצא כי לא כל נותני השירות החיצוניים שהם משתמשים פעילים (158 נותני שירות) נכללו בסקר ההרשאות. כלומר חלק מנותני השירות החיצוניים לא עברו סקירה תקופתית על ידי ממונה הגנת הסייבר כנדרש בהנחיות יה"ב.

משתמשים לא פעילים שנמצאו בסקר ההרשאות: המשמעות של אי-שימוש בחשבונות במשך תקופה ארוכה היא שייתכן שהגישה למידע במערכת אינה נחוצה. לפי נוהל מדיניות הרשאות ובקרת גישה של משרד הבינוי, חשבונות משתמשים אשר לא הייתה כניסה אליהם יותר מ-60 יום יוקפאו אוטומטית, ויש לבחון את המשך נחיצותם.

בביקורת נמצא כי שלא בהתאם לנוהל מדיניות הרשאות ובקרת גישה של משרד הבינוי, ההרשאה של חלק מהמשתמשים שהוגדרו לא פעילים בקובץ המשתמשים נמצאה תקפה בסקר ההרשאות ולא הוקפאה כנדרש בנוהל. עוד נמצא כי לגבי חלק מהם נרשמה הכניסה האחרונה לרשת בשנים 2020 - 2023.

משרד הבינוי מסר בתשובתו כי לעובדים הפעילים ולנותני השירותים החיצוניים שצוין שלא עברו סקירה תקופתית אין הרשאות למערכות הליבה שנסקרו. משרד הבינוי הוסיף כי הוא מבצע בקרה שוטפת לגבי משתמשים שאינם פעילים ומוחק אותם בתהליך שוטף. עוד מסר משרד הבינוי כי הפער שקיים לגבי הרשאות של יועצים נמצא בטיפול.

על משרד הבינוי לאתר את כלל העובדים שמוגדרים משתמשים לא פעילים ויש להם הרשאות במערכות השונות, לצורך בדיקת נחיצותן, וכן לפעול לשיפור מנגנון הבקרה על הרשאות המשתמשים, נוכח הימצאותן של הרשאות למשתמשים לא פעילים.

3. **סקר הרשאות למשתמשים פריווילגיים (משתמשי-על):** במערכות מידע יש סוגים שונים של הרשאות משתמש, ובהם הרשאות ברמה גבוהה יותר המאפשרות לבעל ההרשאה לבצע שינויים רבים יותר, לנהל את רשימת המשתמשים וההרשאות ואף לבצע שינויי מבנה בתשתית. בהנחיית יה"ב 5.12 בנושא "ניהול ותפעול הרשאות", בפרק "בקרת הרשאות וסקירה תקופתית", נקבע כי יש לבצע אחת לחצי שנה בחינת הרשאות של משתמשי-על[25], לשם הסרת הרשאות עודפות.

בביקורת נמצא כי משרד הבינוי לא ביצע בשלוש השנים האחרונות סקירה תקופתית חצי-שנתית של הרשאות משתמשי-על, כנדרש בהנחיית יה"ב.

היעדר בחינה שיטתית זו מגביר את הסיכון להימצאות הרשאות עודפות שאינן נדרשות לצורך ביצוע התפקיד בפועל ועלול לחשוף את מערכות המידע לאיומי אבטחה, לגישה גורפת למידע רגיש ולפעולות בלתי מורשות.

על משרד הבינוי לבצע סקירה תקופתית חצי-שנתית של הרשאות משתמשי העל, כנדרש בהנחיית יה"ב.

---

24 חלקם אותרו באמצעות השדה Title בקובץ המשתמשים, שבו מצוין תיאור תפקידם, וחלקם זוהו באמצעות השדה Department בקובץ המשתמשים, שבו צוין שיוכם לאגף טד"מ.

25 על פי ההגדרה בהנחיה – משתמש-על (פריווילג) הוא עובד מוסמך באגף מערכות מידע בעל הרשאות ניהול מערכת.

משרד הבינוי מסר בתשובתו כי בתוכנית העבודה של שנת 2026 מתוכנן סקר הרשאות למשתמשי-על.

ניהול חשבונות משתמשים

במערכת Active Directory (AD) של משרד הבינוי ניתן לזהות את כלל המשתמשים במערכות המידע של המשרד. במסגרת הביקורת ביצע משרד מבקר המדינה בדיקה של קובץ חשבונות המשתמשים, לרבות סוגי המשתמשים הקיימים ברשת. להלן הממצאים שעלו בנושא חשבונות עובדי מיקור-חוץ וחשבונות שירות:

חשבונות עובדי מיקור-חוץ: המשרד נעזר בשירותי מיקור-חוץ ומעסיק ספקי שירות חיצוניים במגוון תחומים. על פי נוהל הוספה וגריעה של משתמש (כולל חיבור מרחוק) של משרד הבינוי, יש להגדיר את מועד תפוגת חשבון המשתמש של עובד מיקור-חוץ בהתאם למועד סיום העסקתו.

מבדיקת קובץ המשתמשים עלה כי שלא בהתאם לנוהל הוספה וגריעה של משתמש, משרד הבינוי לא הגדיר לעובדי מיקור-החוץ מועד לתפוגת החשבון כנדרש. עוד עלה כי למשרד אין רשימה עדכנית של עובדי מיקור-החוץ שבאמצעותה ניתן לוודא באופן שוטף אם עובדים שכבר אינם מועסקים עדיין מוגדרים כמשתמשים במערכת.

על משרד הבינוי להגדיר מועד לתפוגת חשבונות המשתמשים של עובדי מיקור-החוץ בהתאם לתקופת העסקתם ולקיים בקרה שוטפת בנדון.

משרד הבינוי מסר בתשובתו כי יעודכנו נוהלי העבודה בנושא.

חשבונות שירות או חשבונות מערכת (Service Accounts): חשבונות שירות או חשבונות מערכת הם חשבונות שנוצרים עבור שירותים, יישומים או תהליכים אוטומטיים, ולא עבור משתמשים אנושיים. הם משמשים למשל להפעלת שירותי מערכת, לגיבויים ולגישה למסדי נתונים. לחשבונות אלה ניתנות לעיתים הרשאות רחבות, ולכן נדרש לעקוב אחר פעילותם כחלק ממדיניות אבטחת המידע הארגונית.

כאמור, לפי נוהל מדיניות הרשאות ובקרת גישה של משרד הבינוי, חשבונות משתמשים אשר לא ביצעו התחברות לרשת במשך יותר מ-60 יום יוקפאו אוטומטית, ויש לבחון את המשך נחיצותם.

בביקורת עלה כי שלא בהתאם לנוהל מדיניות הרשאות ובקרת גישה של משרד הבינוי, רק אחוז מסוים מחשבונות השירות ביצעו התחברות לרשת בשנה שקדמה למועד הפקת הדוח. נתון זה עשוי להעיד על קיומם של חשבונות שירות שאינם בשימוש שוטף, ויש לבחון את המשך נחיצותם.

משרד הבינוי מסר למשרד מבקר המדינה כי הוא מצוי בעיצומה של הכנת תוכנית עבודה לבחינת הצורך בחשבונות השירות שאינם בשימוש שוטף. בתשובתו הוסיף משרד הבינוי כי מכיוון שמדובר בחשבונות שירות, בדיקת ההתחברות לרשת (log on) אינה מעידה בהכרח על שימוש או חוסר שימוש, וכי לחלק ממשתמשים אלו מוגדר שהם אינם יכולים לבצע log on למחשב.

על משרד הבינוי לבצע בדיקה של נחיצות חשבונות השירות, כדי לצמצם את הסיכון של ריבוי משתמשים בעלי הרשאות מיותרות שלא לצורך.

בקרה על הגישה למאגרי המידע ותיעוד הגישה למאגרים

בקרה על גישה למאגרי המידע ותיעוד הגישה הם רכיבים קריטיים בהגנה על מידע רגיש בארגון. ניהול גישה מבוקר ויעיל מבטיח שהגישה למאגרים תינתן רק למורשים, תוך שמירה על עקרונות

אבטחת המידע וציות לאסדרות. תיעוד כל גישה למאגרים מאפשר זיהוי, מעקב ותגובה על אירועים חריגים, מספק שקיפות ומאפשר לאכוף נהלים.

על פי תקנות הגנת הפרטיות[26], יש לנהל מנגנון תיעוד אוטומטי שיאפשר ביקורת על הגישה למערכות המאגר (מנגנון בקרה). התיעוד יכלול את הנתונים האלה: זהות המשתמש שביצע את ניסיון הגישה, 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. 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.

בהנחיית יה"ב 5.2[27] נקבע כי איתור ניסיונות לבצע פעולות לא מורשות במערכת ייעשה בין היתר באמצעות ניתוח סמוך ככל שניתן לזמן אמת של רשומות תיעוד הפעולות (רשומות הלוג)[28] במערכות.

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 שבהם 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[29].

בביקורת עלה כי בעוד שתקנות הגנת הפרטיות קובעות כי על בעל מאגר המידע נדרש לקבוע נוהל בדיקה שגרתי של הנתונים המתועדים במנגנון הבקרה ולנהל מנגנון תיעוד אוטומטי שיאפשר ביקורת על הגישה למערכות המאגר, נמצא כי במשרד הבינוי מערכות המידע מתעדות את הגישה של המשתמשים אל רוב מאגרי המידע ומאפשרות בקרה על כך, אולם במערכות אלה לא הוגדרו פעולות חריגות, ולא קיימים מנגנונים אוטומטיים להתרעה על פעולות חריגות.

עקב כך ניסיונות לבצע פעולות לא מורשות במערכות המידע אינם מנוטרים באמצעות ניתוח רשומות הלוג סמוך ככל שניתן לזמן אמת, והבקרה על הגישה למערכות המידע אינה מיטבית ואינה תואמת את הדרישות.

על משרד הבינוי להגדיר מה הן פעולות חריגות ולהפעיל מנגנונים אוטומטיים להתרעה מפניהן.

משרד הבינוי מסר בתשובתו כי הנושא ייבדק ותגובש מדיניות בוועדת ההיגוי.

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 בפעילותו הרגילה באופן ובהיקף שתוכננו מראש. מטרותיה העיקריות של תוכנית המשכיות 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 חירום לשם השבת הארגון לפעולה. גופים ציבוריים נדרשים אף להבטיח כי ביכולתם לספק

---

26 סעיף 10.

27 סעיף 11.14.

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

29 מבקר המדינה, **דוח מבקר המדינה - 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.

שירותים חיוניים לציבור בעת אירוע חירום. סיכונים לפגיעה בארגון עלולים לנבוע מסיבות שונות, ובהן השתלטות מרחוק על מערכות מחשוב ומידע ושיבוש מידע האגור במערכות; אסונות טבע או אירועי לוחמה; ופגיעה במערכות מיזוג האוויר[30].

גיבוש תוכנית להמשכיות תפקודית דורש תכנון וכולל בין היתר ניתוח סיכונים, הצבעה על התהליכים 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 (הפיזית והלוגית) שבה הוא ישוחזר. בתוכנית התאוששות 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[31] קובעת כי על ארגון לגבש תוכנית המשכיות תפקודית, וכי על תוכנית כזאת לכלול גם תוכנית התאוששות מאסון.

הנחיית יה"ב 5.30 בנושא "גיבוי ושחזור מידע" קובעת 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 DR, Disaster Recovery).

נוהל משרד הבינוי בנושא "היבטי ניהול המשכיות עסקית" משנת 2019 מפרט את העקרונות ואת התהליכים שיש לבצע בהכנת תוכנית "ניהול המשכיות עסקית" - BCP. הנוהל קובע כי תוכנית ההמשכיות העסקית של המשרד תכלול הגדרה של המערכות והתהליכים החיוניים, בדגש על מערכות אבטחת מידע (כגון מערכות השולטות בתנועת המידע בין הרשתות - Firewall, מערכות ניהול משתמשים ומערכות ניטור), וזיהוי של האסונות והכשלים הפוטנציאליים העלולים לשבש את פעילות המשרד. נוסף על כך, התוכנית תגדיר את התנאים להפעלתה (למשל פגעי מזג אוויר או אירוע טרור); תפרט את תהליכי הערכת המצב, בעלי התפקידים והצוותים הנדרשים בשעת חירום (כגון צוותים לטיפול במשפחות העובדים והתקשורת); ותכלול שלבי תגובה מיידית, זמני התאוששות של המערך החלופי ופרק הזמן עד לשיקום מלא של הפעילות. כמו כן, התוכנית תכלול הדרכה לעובדים על הנהלים לשעת חירום, וכן יוגדר כי בדיקה, עדכון וניסוי שלה יבוצעו אחת לשנה. עוד נקבע כי ועדת היגוי סייבר תאשר אחת לשנה, במסגרת סקר ההנהלה, את תוקפה ועדכניותה של תוכנית ההתאוששות העסקית ואת תוכנית התחזוקה והבדיקה.

בישיבת ועדת היגוי סייבר שהתקיימה בינואר 2025 הוחלט לכלול בתוכנית העבודה השנתית לשנת 2025 את הכנתה של תוכנית התאוששות עסקית מקיפה.

מבדיקת משרד מבקר המדינה עלה כי נכון למועד סיום הביקורת נמצאו פערים בנוגע לטיפול בנושא התוכנית להמשכיות תפקודית הכוללת תוכנית התאוששות מאסון, כנדרש בהנחיות יה"ב, בין השאר לצורך המשך פעילות מערכות המידע של המשרד במקרה אסון.

כדי שמשרד הבינוי יוכל להבטיח את המשך פעילותו גם באירועי חירום העלולים לפגוע במערכות המידע והמחשוב שלו, עליו להכין תוכנית להמשכיות תפקודית, הכוללת תוכנית התאוששות מאסון, על בסיס העקרונות שתאשר ועדת היגוי סייבר.

---

30 ראו מבקר המדינה, **דוח מבקר המדינה - מאי 2024**, "אבטחת המידע והגנת הסייבר ברשות מקרקעי ישראל", עמ' 12.

31 סעיף 13.5.

תרגול לשחזור מידע

מנגנון הגיבוי והשחזור בארגון הוא מנגנון קריטי המאפשר להתמודד עם סוגיות הנוגעות בין היתר לשלמות, לאמינות ולזמינות של המידע. על פי הנחיית יה"ב 5.30[32], יש לבצע בין היתר בדיקה של תקינות שחזור המידע לפחות אחת לחצי שנה. כמו כן, יש לבצע בדיקת שחזור שנתית יזומה של מערכת הייצור במקום חלופי וניסיונות שחזור מדגמיים. כל זאת כדי לוודא את תקינות מערך הגיבוי. נוסף על כך צוין בהנחיה כי יש להצפין את עותק הגיבויים לפני הוצאתו לשמירה מחוץ לאתר הראשי או מחוץ לאתר הגיבויים (DR)[33]. בהנחיה נאמר כי סיכום בדיקת תקינות השחזור יישלח להנהלה הארגון, וכי יתבצע מעקב אחר בדיקות השחזור. 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[34] וקבלת החלטות לגבי ביצוע שינויים בעקרונות הגנת הסייבר.

בביקורת עלה כי שלא בהתאם להנחיות יה"ב, משרד הבינוי לא ביצע תרגול של העלאת השחזורים של הנתונים משרתי מערכות המידע באופן מלא, אלא ביצע בדיקת שחזור מידע לשרתים אחדים בכל פעם.

עוד עלה כי סיכומים של בדיקות תקינות השחזור שבוצעו לא הועברו לוועדת היגוי סייבר, וכי היא אינה מבצעת מעקב בעניינן של בדיקות השחזור.

משרד הבינוי מסר בתשובתו כי הוא מבצע בדיקות מדגמיות אחת לרבעון, וכי לא ניתן לבצע בדיקה מלאה של כל האתר. משרד הבינוי הוסיף כי סיכומי הבדיקות יוצגו לוועדת היגוי סייבר.

מומלץ כי משרד הבינוי יבצע תרגול שחזור נתונים מלא לכל מערכות המידע שלו באופן קבוע. כמו כן, עליו לוודא כי ועדת היגוי סייבר מקבלת ומבקרת את ממצאי הבדיקות באופן שוטף.

<u>הטיפול בהתרעות מה-SOC הממשלתי</u>

שלב חשוב בהתמודדות עם אירועי סייבר הוא זיהוי והגדרה של אירועים חריגים, בהתבסס על איומי ייחוס ידועים. אירועים אלו יתועדו וינוטרו באמצעות מערכות מידע שונות, בין היתר על ידי יצירת לוגים (logs) המתעדים פעולות חריגות ואירועים (events). המידע שנאסף יועבר למערכת SIEM (Security Information and Event Management)[35], שם הוא ינותח ויוערך. לאחר מכן יועבר המידע למערך שליטה ובקרה מרכזי (SOC - Security Operations Center), אשר מנהל את הטיפול באירועים באופן שיטתי ומבוקר[36].

משרד הבינוי מחובר למערך ה-SOC הממשלתי, המשמש מרכז שליטה ובקרה בתחום אבטחת המידע. מערך זה מופעל על ידי מערך הדיגיטל הלאומי ומספק רובד אופרטיבי לניטור רשתות המידע.

ה-SOC הממשלתי הוא שכבת הגנה חיונית, האחראית לזיהוי, ניתוח וניהול של אירועים חריגים בזמן אמת. ה-SOC הממשלתי מגדיר חוקות (rules) ייעודיות לזיהוי חריגות ומבצע הצלבה בין

---

32 סעיף 6.26.

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

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

35 מערכת לניטור, איסוף וניתוח מרכזי של לוגים ואירועי אבטחת מידע מארגונים, המאפשרת גילוי, חקירה ותגובה לגבי איומי סייבר בזמן אמת.

36 החלטת הממשלה 2443 - "קידום אסדרה לאומית והובלה ממשלתית בהגנת הסייבר" (15.2.15); נוהל יידוע משתמשים ברשת המחשוב המשרדית אודות ניטור התעבורה ברשת לצרכי הגנת הסייבר ב-SOC הממשלתי.

אירועים ממקורות שונים, לצורך חשיפת תבניות תקיפה מתקדמות. עם זיהוי פעילות חשודה נוצרת התרעה, אך לא כל התרעה מחייבת פעולה של הגורמים המבצעיים. לאחר תהליך סיווג ראשוני, ה-SOC הממשלתי מחליט אילו מההתרעות מחייבות העברה לגורמים הרלוונטיים במשרד, לרוב לצורך בדיקה טכנית, חקירה או טיפול מיידי. עם קבלת ההתרעה, על הארגון לבצע בירור ולמסור את תגובתו על ההתרעה. אם התגובה שנמסרה מאשרת את הממצאים או נותנת מענה מספק - ההתרעה נסגרת. במקרים שבהם לא מתקבל מענה בפרק זמן של חמישה ימי עבודה, ה-SOC הממשלתי סוגר את ההתרעה באופן עצמאי, תוך תיעוד היעדר ההתייחסות. סגירה כזו היא אינדיקציה להיעדר טיפול בהתרעה. מספר ההתרעות שהועברו למשרד הבינוי על פי דיווחי ה-SOC הממשלתי עמד על כמה מאות מדי שנה בשנים 2022 - 2024.

מהשוואה בין נתוני משרד הבינוי לבין נתוני משרדי ממשלה אחרים שבוצעה ב-SOC הממשלתי לגבי המחצית השנייה של שנת 2024 עלה כי מצבו של משרד הבינוי מעט טוב יותר לעומת משרדי ממשלה אחרים - 90% מההתרעות שנשלחו למשרד הבינוי נסגרו לאחר קבלת מענה לעומת 85% בלבד במשרדים אחרים, ושיעור ההתרעות שנסגרו בלי שניתן להן מענה במשרד הבינוי היה 9.2% לעומת 10.8% במשרדים אחרים.

מומלץ כי משרד הבינוי ימשיך לפעול לשיפור מנגנוני התגובה על התרעות אבטחת מידע.

משרד הבינוי מסר בתשובתו כי יפעל לשיפור מנגנוני התגובה במסגרת תוכנית העבודה.

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. דוח מערך הסייבר הלאומי על פשיעת סייבר בישראל שפורסם בפברואר 2025 מציין כי בשנת 2024 תועדו בישראל יותר מ-300 מתקפות כופרה שמאחוריהן עומדים ככל הנראה פושעי סייבר. כך למשל, בשנת 2021 הודיע המרכז הרפואי הלל יפה לציבור על אירוע סייבר מסוג כופרה ללא התרעה מוקדמת שפגע במערכות המחשוב שלו.

מערך הסייבר הלאומי פרסם מסמך הסוקר את נושא הכופרות, ובו המלצות כיצד להיערך לאירוע כופרה.

מבדיקת משרד מבקר המדינה עלה כי משרד הבינוי טרם השלים את היערכותו לאירוע כופרה.

על משרד הבינוי להשלים את היערכותו לאירוע כופרה.

הגנה פיזית

הגנה פיזית בכל הקשור לסייבר היא הגנה על מכלול הציוד והמידע המצויים באתרי הארגון מפני גישה פיזית של גורמים בלתי מורשים. תוצאותיה של גישה כזאת עשויות להיות חשיפה, גניבה, שינוי או הרס של מידע. הנחיית יה"ב 5.2 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 אגף טד"ם במשרד הבינוי בתחום אבטחת המידע לשנים 2022 - 2024 לא כללו ביצוע ביקורת בעניין אבטחה פיזית.

עוד עלה כי בהסכם ההתקשרות שמשרד הבינוי חתם עם חברה חיצונית להספקת שירותי מיקור-חוץ של תפעול ותחזוקה של תשתיות מחשוב נקבע כי על החברה לבצע מדי שנה בשנה תרגילי חדירה פיזיים למתקן המחשב המרכזי, באמצעות התחזות לגורם שיש לו הרשאות גישה למערכות. ואולם תרגילים אלו לא בוצעו.

על משרד הבינוי לכלול בתוכנית העבודה השנתית ביצוע ביקורות לגבי אבטחה פיזית, כנדרש בהנחיית יה"ב, ולאכוף את ביצוען.

משרד הבינוי מסר בתשובתו כי הוא מתכנן לכלול ביקורת אבטחה פיזית בתוכנית העבודה לשנת 2026.

סיכום

משרד הבינוי אמון על ייזום וביצוע של מדיניות הממשלה בתחומי השיכון והבנייה למגורים. לצורך ניהול פעילותו משתמש המשרד בכמה עשרות מערכות מידע הכוללות במצטבר מיליוני רשומות, ובהן מידע אישי ורגיש בין השאר על דיירי הדיור הציבורי, מקבלי סיוע לדיור, משתתפים בתוכניות דיור בהנחה וקבלנים רשומים. מידע זה נדרש לאבטח ברמת אבטחה גבוהה.

ביקורת זו העלתה ליקויים מהותיים בפעולותיו של משרד הבינוי בנוגע לניהול אבטחת המידע שברשותו וההגנה על מערכותיו. בין היתר נמצא כי ועדת היגוי סייבר של המשרד, שאמורה להתוות מדיניות בתחום אבטחת המידע ולפקח על יישומה, להתעדכן בסיכונים ובאיומים בתחום הסייבר שהמשרד חשוף אליהם ולפקח על ניהול סיכוני הסייבר במשרד, לא בחנה ולא אישרה את המיפוי ואת הסיווג של נכסי המידע של המשרד, לצורך קיום בקרה מיטבית; מיעטה לדון בממצאי סקרים ומבדקים שבוצעו, וממילא לא קבעה תוכנית להפחתת הסיכונים שעלו מהם; וגם לא וידאה ביצוע של תוכניות העבודה, כמתחייב בהנחיות יה"ב. עוד עלה כי משרד הבינוי לא עמד על ביצוע מלא של סקרי סיכונים ומבדקי חדירה שנקבעו בהסכם התקשרות עם ספק חיצוני.

בדיקה לגבי ניהול הרשאות גישה למערכות מידע העלתה שיותר ממחצית המערכות לא נסקרו אחת לשנה כנדרש בהנחיות יה"ב, וכי למשרד הבינוי אין רשימה עדכנית של עובדי מיקור-החוץ שבאמצעותה ניתן לבדוק באופן שוטף אם עובדים שכבר אינם מועסקים בו עדיין מוגדרים כמשתמשים במערכת. משרד הבינוי גם לא הגדיר לגבי גישה למערכות המידע מה הן פעולות חריגות שמצריכות בדיקה ואף לא הסדיר מנגנונים אוטומטיים להתרעה מפניהן, ולפיכך הבקרה שהוא מבצע על הגישה למערכותיו אינה מיטבית.

עוד עלה כי במועד סיום הביקורת עלו פערים בנוגע לנושא תוכנית להמשכיות תפקודית, הכוללת תוכנית התאוששות מאסון, לשם המשך פעילות מערכות המידע של משרד הבינוי במקרה כזה.

על משרד הבינוי לפעול לתיקון הליקויים שצוינו בדוח זה, לצורך שיפור ההגנה על המידע שבידיו והגברת האפקטיביות של פעולותיו בתחום זה.