דוח מבקר המדינה

אבטחת מערכות המידע במשרד הבינוי והשיכון

▪ סיוון התשפ"ו ▪ מאי 2026 ▪

אבטחת מערכות המידע במשרד הבינוי והשיכון

תקציר

רקע

משרד הבינוי והשיכון (משרד הבינוי) אמון על הייזום והביצוע של מדיניות הממשלה בתחומי הבנייה והשיכון. משרד הבינוי 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. המידע שמשרד הבינוי אוסף, שומר ומנהל במסגרת פעילותו הוא מידע רגיש כהגדרתו בחוק הגנת הפרטיות, התשמ"א-1981. מדובר במיליוני רשומות ובהן בין היתר מידע אישי על דיירי הדיור הציבורי, מקבלי סיוע לדיור, משתתפים בתוכניות דיור בהנחה וקבלנים רשומים. משרד הבינוי נדרש להגן על סודיות המידע, אמינותו, זמינותו ומהימנותו, ועליו לוודא כי הנתונים לא ישונו, לא יימחקו וייחשפו רק למי שמורשה לכך מתוקף תפקידו או למי שהמידע נוגע לו.

נתוני מפתח

עשרות
מערכות מידע שמשרד הבינוי משתמש בהן לצורך ניהול פעילותו

שיעור מסוים
ממערכות המידע במשרד הבינוי הוקם לפני שנים רבות

6.5 מיליון ש"ח
תקציב משרד הבינוי לאבטחת מידע וסייבר. מדובר בכ-9% מתוך 74.5 מיליון ש"ח שהוקצו עבור הוצאות מחשוב בשנת 2025

9
מאגרי מידע שברשות משרד הבינוי שרישומם נדרש במרשם מאגרי המידע, אך המשרד לא השלים את רישומם באופן הנדרש בתקנות הגנת הפרטיות

130%
שיעור הגידול בהתרעות שהתקבלו ב-SOC הממשלתי לגבי משרד הבינוי בגין פעילות החשודה כאיום סייבר בשנת 2024 (בעת מלחמת חרבות ברזל), לעומת ההתרעות שהתקבלו בשנת 2023

43%
שלושה משבעה מדדים בנושא הגנת סייבר שהיו אמורים להידון בוועדת היגוי סייבר במשרד הבינוי בשנת 2025 לא נדונו ונבחנו כנדרש

חלק
מנותני השירות החיצוניים המשתמשים במערכות המידע במשרד הבינוי לא עברו סקירה תקופתית לשם בדיקת התאמה בין תפקידם להרשאות הקיימות

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: הממשל והניהול של אבטחת המידע והסייבר; ניהול הרשאות ומשתמשים; רישום מאגרי המידע; ותוכניות להמשכיות תפקודית ולהתאוששות מאסון.

תמונת המצב העולה מן הביקורת

- **המדיניות והתקציב בנושא אבטחת המידע** - 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, הועלה כי בניגוד להנחיית היחידה להגנת הסייבר בממשלה (יה"ב), מאז אושרה 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. כמו כן, בשנים שנבדקו לא היה לוועדת ההיגוי סייבר מידע בדבר שיעור התקציב המיועד לאבטחת מידע מכלל התקציב המיועד לטכנולוגיות המידע, כדי לוודא שמשרד הבינוי עומד בהוראות החלטת הממשלה ומקצה די משאבים להתמודדות עם סיכוני האבטחה הנשקפים לו.

- **מיפוי וסיווג של נכסי המידע** - 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 היגוי סייבר מהשנים 2021 - 2025 אומנם צוין כי במסגרת הליך ההסמכה של משרד הבינוי לתקן ISO270001 (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.

- **סקרי סיכונים** - בשנים 2022 - 2024 ביצע משרד הבינוי שמונה סקרי סיכונים. ואולם על אף החובה לפי תקנה 5(ג) לתקנות הגנת הפרטיות (אבטחת מידע), התשע"ז-2017 (תקנות הגנת הפרטיות או תקנות 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 מהסקרים שבוצעו. יתר הסקרים לא נדונו, וממילא הוועדה לא קבעה תוכנית להפחתת הסיכונים שעלו בהם.

- **מבדקי חדירה** - על אף חובתו של בעל מאגר מידע לביצוע מבדקי חדירה למערכות המאגר 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. כמו כן, ממצאי המבדקים שביצע משרד הבינוי לא הובאו לפני ועדת היגוי סייבר כמתחייב. יתרה מכך, לא נמצאו מסמכים המעידים על טיפול כלשהו של משרד הבינוי בסיכונים שהתגלו במבדקים, ובכלל זה פעולות לתיקון הליקויים ומבדקים חוזרים במטרה לוודא שהליקויים תוקנו ואינם חוזרים על עצמם.

אי-עמידה על ביצוע מלא של סקרי סיכונים ומבדקי חדירה שנקבעו בהסכם התקשרות עם ספק - אף שבהסכם התקשרות של משרד הבינוי עם חברה חיצונית לתפעול ותחזוקה של מערכות מחשוב נקבע שעליה לבצע סקרי סיכונים למערכות לפחות אחת ל-18 חודשים ומבדקי חדירה, משרד הבינוי לא עמד על ביצועו המלא של ההסכם. בפועל החברה ביצעה באופן חלקי בלבד סקרי סיכונים מבדקי חדירה שנדרשו בהסכם.

קביעת מדדים בנושא הגנת סייבר ועמידה בהם - בביקורת עלה כי משנת 2022 ועד למועד סיום הביקורת ועדת היגוי סייבר בחנה את מידת היישום של מדדי האב בנושאי הגנת הסייבר באופן חלקי בלבד, ולא בכל חצי שנה, כנדרש בהנחיית יה"ב. למשל, בדיון ועדת היגוי סייבר שהתקיים 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%). עקב כך נפגעה יכולתה של הוועדה לבחון את רמת האפקטיביות של תשתית הגנת הסייבר ולבצע שינויים כאשר הדבר נדרש.

ניהול הרשאות גישה - בביקורת עלה כי לגבי יותר ממחצית המערכות לא נסקרו הרשאות המשתמשים אחת לשנה כנדרש בהנחיות יה"ב. עוד נמצא כי חלק מהעובדים הפעילים וחלק מנותני השירות החיצוניים של משרד הבינוי לא עברו סקירה תקופתית כנדרש בהנחיות יה"ב. עוד עלה כי ההרשאה של חלק מהמשתמשים שהוגדרו "לא פעילים" בקובץ המשתמשים נמצאה תקפה בסקר ההרשאות ולא הוקפאה כנדרש.

ניהול משתמשים "פריווילגיים" (משתמשי-על) - משתמשי-על הם משתמשים בעלי הרשאות ברמה גבוהה יותר ממשתמשים רגילים, המאפשרות לבצע שינויים רבים יותר, לנהל את רשימת המשתמשים ולבצע שינויי מבנה בתשתית. בביקורת נמצא כי משרד הבינוי לא ביצע בשלוש השנים האחרונות סקירה תקופתית חצי-שנתית של הרשאות משתמשי-העל, 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.

בקרה על הגישה למאגרי המידע - נמצא, בין היתר, כי מערכות המידע במשרד הבינוי מתעדות את הגישה של המשתמשים אל רוב מאגרי המידע ומאפשרות בקרה על כך. ואולם 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 תיעוד הפעולות (הלוג) סמוך ככל שניתן לזמן אמת, והבקרה על הגישה למערכות המידע אינה מיטבית ואינה תואמת את הדרישות.

תוכניות המשכיות תפקודית (BCP) והתאוששות מאסון (DRP) - עלה כי במועד סיום הביקורת נמצאו פערים בנוגע לנושא הכנת תוכנית להמשכיות תפקודית הכוללת תוכנית התאוששות מאסון, כנדרש בהנחיות יה"ב, בין השאר לצורך המשך פעילות מערכות המידע של המשרד במקרה אסון.

רישום מאגרי המידע - משרד הבינוי לא הסדיר את רישום כל תשעת מאגרי המידע שעליו לרשום באופן הנדרש בתקנות הגנת הפרטיות, אף שעברו כשמונה שנים מאז נכנסו התקנות לתוקפן. מאגרים אלה כוללים במצטבר מיליוני רשומות, ובהן מידע אישי על דיירי הדיור הציבורי, מקבלי סיוע לדיור, משתתפים בתוכניות דיור בהנחה וקבלנים רשומים.

התמודדות עם נוזקה מסוג כופרה - עלה כי למרות המלצות מערך הסייבר ולמרות תקיפות סייבר מסוג כופרה על מוסדות ממשלתיים, משרד הבינוי טרם השלים את היערכותו לאירוע כופרה.

הטיפול בהתרעות מה-SOC הממשלתי - מצבו של משרד הבינוי טוב יותר לעומת הממוצע במשרדי ממשלה אחרים (90% מההתרעות שנשלחו למשרד הבינוי נסגרו לאחר קבלת מענה, לעומת 85% מההתרעות במשרדים אחרים).

עיקרי המלצות הביקורת

- על משרד הבינוי לדון בתוצאות סקרי הסיכונים ולגבש תוכנית עבודה להתמודדות עם הסיכונים שהתגלו ולהפחתתם. יש להביא תוכנית זו לדיון ולאישור בוועדת היגוי סייבר.

- על משרד הבינוי לבצע מבדקי חדירה בהיקף נרחב יותר, כמתחייב מתקנות אבטחת מידע. נוסף על כך, על משרד הבינוי לדון בתוצאות מבדקי החדירה, לעדכן את ועדת היגוי סייבר בסיכונים ובאיומים העולים מהמבדקים ולנקוט פעולות לתיקון הליקויים שעלו בהם, בהתאם לדרישות תקנות אבטחת מידע. על ועדת היגוי סייבר לעקוב אחר תיקון הליקויים.

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

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

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

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

- 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.

- על משרד הבינוי להסדיר את רישומם של מאגרי המידע שברשותו באופן הנדרש בתקנות, ועל ועדת היגוי סייבר לעקוב אחר ביצוע הרישום והשלמתו כנדרש.

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 נמצאו פערים בנושא 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.