משרד מבקר המדינה
ונציב תלונות הציבור

דוח מבקר המדינה

סייבר ומערכות מידע

סיון התשפ"ו | מאי 2026

דוח מבקר המדינה

סייבר ומערכות מידע

תקצירים

76ג, 77א חלק ראשון

סיון התשפ"ו | מאי 2026

ירושלים

מס' קטלוגי 2026-A-003
ISSN 0334-9713

ניתן להוריד גרסה אלקטרונית של דוח זה
מאתר האינטרנט של משרד מבקר המדינה
www.mevaker.gov.il

תוכן העניינים

פתח דבר

דוח הביקורת השנתי של מבקר המדינה המוקדש לנושא סייבר ומערכות מידע מונח על שולחן הכנסת על פי חוק מבקר המדינה, התשי"ח-1958 [נוסח משולב]. דוח זה עוסק בהיבטים מרכזיים של הגנת הסייבר, אבטחת המידע והשירותים הדיגיטליים במגזר הציבורי.

המרחב הדיגיטלי הפך בשנים האחרונות לתשתית יסוד בפעילותה של מדינת ישראל. מערכות מידע, שירותים מקוונים ותהליכי עבודה דיגיטליים משמשים כיום בסיס לפעולתם של משרדי הממשלה, גופי החירום, הרשויות הציבוריות ומערכי השירות לאזרח. לצד היתרונות הרבים שמביאה עימה הטרנספורמציה הדיגיטלית - ובהם ייעול השירות הציבורי, שיפור הנגישות, חיסכון במשאבים וחיזוק הרציפות התפקודית - מתעצמים גם הסיכונים הנובעים מאיומי סייבר, מדליפות מידע ומפערים בהגנת מערכות המידע. מציאות זו מחייבת את כלל הגופים הציבוריים להבטיח כי מערכותיהם יהיו מאובטחות, אמינות, זמינות ועמידות גם בשגרה וגם בשעת חירום.

הגנת הסייבר ואבטחת מערכות המידע הן כיום מאבני היסוד של תפקודה התקין של המדינה המודרנית. מערכות דיגיטליות מרכזות מידע אישי, כלכלי וביטחוני בהיקפים עצומים ומשמשות תשתית לפעילותם של משרדי הממשלה, גופי החירום והשירותים הציבוריים החיוניים. בעידן שבו איומי הסייבר הולכים ומתעצמים, ובייחוד בתקופות חירום ומשבר, נדרשת מהמדינה היערכות מתקדמת שתבטיח את חסינות המערכות, את ההגנה על פרטיות האזרחים ואת המשך אספקת השירותים לציבור באופן רציף, בטוח ואמין. חיזוק תחום זה אינו רק צורך טכנולוגי, אלא נדבך מרכזי בביטחון הלאומי, באמון הציבור במוסדות המדינה וביכולתה של הממשלה להעניק שירות ציבורי יעיל, מתקדם ונגיש לכלל האזרחים.

החשיבות שבחיזוק ההגנה על מערכות מידע ותשתיות דיגיטליות מתחדדת במיוחד על רקע המציאות הביטחונית המורכבת שבה נתונה מדינת ישראל בשנים האחרונות. בתקופות אלה גוברים ניסיונות התקיפה במרחב הסייבר שמבצעים גורמים עוינים, לצד הצורך של גופי המדינה להבטיח רציפות תפקודית ומתן שירותים חיוניים לציבור גם בתנאי חירום. אירועים מסוג זה המחישו כי מערכות המידע, השירותים הדיגיטליים ותשתיות העבודה מרחוק אינם רק כלי ניהולי וטכנולוגי, אלא מרכיב מרכזי בחוסנה הלאומי של המדינה וביכולתה להמשיך לתפקד באופן רציף, יעיל ובטוח.

ארבעת פרקי דוח זה עוסקים בהיבטים שונים ומשלימים של תחום הסייבר ומערכות המידע במגזר הציבורי:

- **מערכות מידע ואבטחת מידע וסייבר במשרד החוץ**
- **הגנת הסייבר בעבודה מרחוק בעיתות שגרה וחירום**
- **אבטחת מערכות המידע במשרד הבינוי והשיכון**
- **שירותים מקוונים לציבור: ההזדהות הלאומית והאזור האישי הממשלתי**

שלושת הפרקים הראשונים עברו הליך חיסיון בוועדת המשנה של הוועדה לענייני ביקורת המדינה בכנסת, והיא החליטה שלא להניחם במלואם על שולחן הכנסת אלא לפרסם רק חלקים מהם, לשם שמירה על ביטחון המדינה.

ממצאי הביקורת מצביעים על פערים בהיערכות, בניהול הסיכונים, בפיקוח וביישום המדיניות הממשלתית בתחום, לצד התקדמות חלקית בלבד בהנגשת שירותים דיגיטליים ובהטמעת מנגנוני הגנה ובקרה מתקדמים. אף שכל אחד מהדוחות עוסק בתחום ייחודי, מכלולם ממחיש כי חיזוק ההגנה על מערכות מידע, הבטחת רציפות תפקודית והעמקת הטרנספורמציה הדיגיטלית של השירות הציבורי הם אתגרים לאומיים המחייבים טיפול מערכתי, מתואם ומתמשך.

הביקורת בנושא **מערכות מידע ואבטחת מידע וסייבר במשרד החוץ** בוצעה במהלך מלחמת חרבות ברזל והעלתה פערים בתחום הניהול והפיתוח של מערכות המידע במשרד ובתחום אבטחת המידע והגנת הסייבר. נוכח תפקידו, משרד החוץ הוא יעד מרכזי לתקיפות סייבר של מגוון יריבים, החל מפצחנים (האקרים) וכלה בגורמים מדינתיים. ממצאי הביקורת מדגישים את הצורך בחיזוק מנגנוני הפיקוח והבקרה של הנהלת משרד החוץ בכל הנוגע למערכות המידע ואבטחת המידע במשרד, במטרה להבטיח פעילות תקינה של מערך התקשוב שלו ולשפר את רמת ההגנה על המשרד ונכסיו.

אחד מפרקי הדוח עוסק ב**יישום המדיניות הממשלתית לקידום שירותים ציבוריים דיגיטליים באמצעות מערכת ההזדהות הלאומית והאזור האישי הממשלתי**. הביקורת העלתה כי אף שמאז שנת 2014 התקבלו החלטות ממשלה רבות בדבר קידום שירותים מקוונים, וחרף העובדה שכ-4.6 מיליון אזרחים כבר רשומים למערכת ההזדהות הלאומית, יישום המדיניות עדיין חלקי ואיטי. רק 16% מהשירותים שמופו מחוברים למערכת ההזדהות, רק כ־23% מהטפסים המקוונים המזוהים מנוהלים באמצעותה, ורק 233 מתוך אלפי השירותים הממשלתיים הונגשו באזור האישי. עוד נמצא כי רק 15 מתוך 258 הרשויות המקומיות התחברו למערכת ההזדהות הלאומית, והיקף החיבור של משרדי הממשלה וגופים ציבוריים נוספים למערכות אלה מצומצם, באופן הפוגע ביכולת הציבור לקבל שירות ממשלתי דיגיטלי מלא, פשוט ונגיש.

פרק נוסף עוסק ב**אבטחת מערכות המידע של משרד הבינוי והשיכון**, המחזיק במיליוני רשומות ובהן מידע אישי ורגיש על אזרחים, זכאים לדיור וקבלנים. לצורך פעילותו משתמש המשרד בעשרות מערכות מידע, ובשנת 2025 עמד תקציב אבטחת המידע והסייבר שלו על כ-6.5 מיליון ש"ח - כ־9% מתקציב המחשוב הכולל של המשרד. הביקורת העלתה ליקויים מהותיים בניהול אבטחת המידע והסייבר במשרד, ובהם פערים בבקרת הרשאות גישה, אי-מיצוי תהליכי ניהול סיכונים, היעדר מנגנוני התרעה מספקים ואי-השלמת רישום של מאגרי מידע כנדרש בדין. ממצאים אלה בולטים במיוחד נוכח העלייה הניכרת (כ-130%) בהיקף התרעות הסייבר שהתקבלו בעניינו של המשרד בשנת 2024, וממחישים את החשיבות שבהבטחת הגנה אפקטיבית על נכסי המידע של המדינה.

הדוח עוסק גם ב**הגנת הסייבר בעבודה מרחוק**, אשר הפכה בשנים האחרונות לחלק בלתי נפרד מפעילותם של גופים ציבוריים וביטחוניים, וביתר שאת בתקופת מגפת הקורונה ובמהלך מלחמת חרבות ברזל. במסגרת הביקורת נבחנו מוכנותם של גופים חיוניים, ובהם משטרת ישראל והרשות הארצית לכבאות והצלה, להתמודד עם איומי הסייבר הנלווים לעבודה מרחוק. הביקורת העלתה פערים מסוימים במידת ההתאמה של מנגנוני ההגנה והבקרה לסיכונים הקיימים, והועלו ליקויים גם במבדק חדירה שביצע משרד מבקר המדינה במערכת העבודה מרחוק של כב"ה.

ממצאים אלה מדגישים את הצורך בהשלמת ההכנה של תוכניות עבודה ובחיזוק ההיערכות להגנת סייבר בגופים החיוניים במדינה.

מכלול ממצאי הדוח מצביע על כך שהתקדמותה של מדינת ישראל לעבר ממשל דיגיטלי מתקדם מחייבת השקעה מתמשכת בתשתיות סייבר, בניהול סיכונים, בפיקוח ובאכיפה, לצד שיתוף פעולה הדוק בין כלל הגופים הציבוריים. הגנה נאותה על מערכות מידע ושירותים דיגיטליים אינה רק צורך טכנולוגי - אלא תנאי הכרחי לשמירה על אמון הציבור, להגנה על פרטיות האזרחים ולהבטחת תפקודו התקין והרציף של השירות הציבורי.

על הגופים המבוקרים מוטלת החובה לפעול בדרך מהירה ויעילה לתיקון הליקויים שצוינו בדוח זה.

תודתי נתונה לעובדי משרד מבקר המדינה, אשר עסקו בהכנת דוח זה במקצועיות, ביסודיות ובמסירות ומתוך תחושת שליחות. אני תקווה כי ממצאי הדוח והמלצותיו יסייעו לחיזוק מערכי הסייבר ואבטחת המידע במגזר הציבורי ויתרמו לשיפור השירות הניתן לאזרחי ישראל.

נייחל ונתפלל להחלמתם המהירה של הפצועים, לשיקום החטופים ששבו אלינו ובני משפחותיהם, לחזרת כל המפונים לבתיהם, לשלום חיילינו ולהצלחת כוחות הביטחון בהגנה על ארצנו.

מתניהו אנגלמן
מבקר המדינה
ונציב תלונות הציבור

ירושלים,
סיון התשפ"ו,
מאי 2026

المقدمة

تقرير الرقابة السنوي لمراقب الدولة المخصص لموضوع السيبرانية وأنظمة المعلومات مطروح على طاولة الكنيست وفقًا لقانون مراقب الدولة، سنة 1958-5718 م. [نص مدمج]. يتناول هذا التقرير جوانب مركزية من الحماية السيبرانية، وأمن المعلومات، والخدمات الرقمية في القطاع العام.

أصبح الفضاء الرقمي في السنوات الأخيرة بنية تحتية أساسية في نشاط دولة إسرائيل. تُستخدم أنظمة المعلومات، والخدمات المحوسبة، ومسارات العمل الرقمية اليوم كأساس لعمل الوزارات الحكومية، وهيئات الطوارئ، والسلطات العامة، ومنظومات الخدمة للمواطن. إلى جانب المزايا العديدة التي تجلبها معها التحولات الرقمية - ومنها نجاعة الخدمة العامة، تحسين إمكانية الوصول، توفير الموارد، وتعزيز الاستمرارية الوظيفية - تتعاظم أيضًا المخاطر الناجمة عن التهديدات السيبرانية، تسرب المعلومات والفجوات في حماية أنظمة المعلومات. يفرض هذا الواقع على جميع الهيئات العامة أن تضمن أن تكون أنظمتها مؤمنة، موثوقة، متاحة، وقادرة على الصمود سواء في الأوقات الاعتيادية الروتينة أو في أوقات الطوارئ.

تُعتبر الحماية السيبرانية وأمن أنظمة المعلومات اليوم من ركائز الأداء السليم للدولة الحديثة. تركز الأنظمة الرقمية معلومات شخصية واقتصادية وأمنية بأحجام هائلة، وتُستخدم كبنية تحتية لعمل الوزارات الحكومية وهيئات الطوارئ والخدمات العامة الحيوية. في عصر تتعاظم فيه التهديدات السيبرانية باستمرار، وخاصة في فترات الطوارئ والأزمات، يُطلب من الدولة توفير جاهزية متقدمة تضمن حصانة الأنظمة وحماية خصوصية المواطنين واستمرار تقديم الخدمات للجمهور بصورة متواصلة وآمنة وموثوقة. إن تعزيز هذا المجال ليس مجرد حاجة تكنولوجية، بل هو ركيزة مركزية للأمن القومي، لثقة الجمهور بمؤسسات الدولة ولقدرة الحكومة على تقديم خدمة عامة ناجعة، متقدمة، ومتاحة لجميع المواطنين.

تبرز أهمية تعزيز حماية أنظمة المعلومات والبنى التحتية الرقمية بشكل خاص على خلفية الواقع الأمني المعقد الذي تعيشه دولة إسرائيل في السنوات الأخيرة. في هذه الفترات تتزايد محاولات الهجوم في الفضاء السيبراني التي تنفذها جهات معادية، إلى جانب حاجة هيئات الدولة إلى ضمان الاستمرارية الوظيفية وتقديم الخدمات الحيوية للجمهور حتى خلال ظروف الطوارئ. لقد أوضحت أحداث من هذا النوع أن أنظمة المعلومات والخدمات الرقمية وبنى العمل عن بُعد ليست مجرد أدوات إدارية وتكنولوجية، بل أنها تعتبر مكونًا مركزيًا في حصانة الدولة الوطنية وفي قدرتها على الاستمرار في العمل بصورة متواصلة وناجعة وآمنة.

تتناول الفصول الأربعة في هذا التقرير جوانب مختلفة ومتكاملة من المجال السيبراني وأنظمة المعلومات في القطاع العام:

- **أنظمة المعلومات وأمن المعلومات و السيبرانية في وزارة الخارجية**
- **الحماية السيبرانية في العمل عن بُعد في الأوقات الروتينيّة وفي حالات الطوارئ**
- **أمن وحماية منظومات المعلومات في وزارة البناء والإسكان**
- **الخدمات الرقمية للجمهور: منظومة التعريف الوطنية والمنطقة الشخصية الحكوميّة**

خضعت الفصول الثلاثة الأولى لإجراء السرية في اللجنة الفرعية التابعة للجنة شؤون مراقبة الدولة في الكنيست، وقد قررت اللجنة عدم عرضها كاملة على طاولة الكنيست، وإنما نشر أجزاء منها فقط، حفاظًا على أمن الدولة.

تشير نتائج الرقابة إلى وجود فجوات في الجاهزية، في إدارة المخاطر، في الإشراف وفي تطبيق السياسة الحكومية في هذا المجال، إلى جانب

حصول تقدم جزئي فقط في إتاحة وتوفير الخدمات الرقمية وفي دمج آليات حماية ورقابة متقدمة. على الرغم من أن كل واحد من التقارير يتناول مجالًا فريدًا من نوعه، فإن مجملها يوضح أن تعزيز حماية أنظمة المعلومات وضمان الاستمرارية الوظيفية وتعميق التحول الرقمي للخدمة العامة هي تحديات وطنية تستوجب معالجة جهازية ومنسقة ومستمرة.

أُجريت الرقابة بشأن **أنظمة المعلومات وأمن المعلومات و السيبرانية في وزارة الخارجية** خلال حرب السيوف الحديدية، وقد كشفت عن وجود فجوات في مجال إدارة وتطوير أنظمة المعلومات في الوزارة، وكذلك في مجال أمن المعلومات والحماية السيبرانية. ونظرًا إلى دورها، تُعد وزارة الخارجية هدفًا رئيسيًا لهجمات السايبر من قبل جهات معادية متنوعة، بدءًا من القراصنة (الهاكرز) ووصولًا إلى جهات دولية. تؤكد نتائج الرقابة الحاجة إلى تعزيز آليات الإشراف والرقابة لدى إدارة وزارة الخارجية في كل ما يتعلق بأنظمة المعلومات وأمن المعلومات في الوزارة، بهدف ضمان التشغيل السليم لمنظومة الحوسبة والاتصالات التابعة لها، وتحسين مستوى حماية الوزارة وممتلكاتها.

يتناول أحد فصول التقرير **تطبيق السياسة الحكومية لتعزيز الخدمات العامة الرقمية بواسطة منظومة التعريف الوطنية والمنطقة الشخصية الحكومية**. أظهرت الرقابة أنه رغم اتخاذ العديد من القرارات الحكومية منذ سنة ٢٠١٤ بشأن تعزيز الخدمات المحوسبة، وعلى الرغم من أن نحو ٤,٦ مليون مواطن مسجلون بالفعل في منظومة التعريف الوطنية، فإن تطبيق هذه السياسة لا يزال جزئيًا وبطيئًا. ١٦٪ فقط من الخدمات التي تم حصرها موصولة بمنظومة التعريف، نحو ٢٣٪ فقط من النماذج المحوسبة المعرّفة تُدار بواسطتها، من بين آلاف الخدمات الحكومية أتيح الوصول الى وفقط ٢٣٣ نموذج فقط في المنطقة الشخصية. كما تبيّن أن ١٥ سلطة فقط من أصل ٢٥٨ سلطة محلية اتصلت بمنظومة التعريف الوطنية، وأن نطاق اتصال الوزارات الحكومية والهيئات العامة الإضافية بهذه المنظومات محدود، بصورة تمس بقدرة الجمهور على تلقي خدمة حكومية رقمية كاملة، بسيطة، ومتاحة.

يتناول فصل إضافي **أمن وحماية أنظمة المعلومات في وزارة البناء والإسكان**، التي تحتفظ بملايين السجلات التي تتضمن معلومات شخصية وحساسة عن المواطنين والمستحقين للسكن والمقاولين. تستخدم الوزارة لغرض نشاطها عشرات الأنظمة من المعلومات، وفي سنة ٢٠٢٥ بلغت ميزانية أمن وحماية المعلومات السيبرانية الخاصة بها نحو ٦,٥ مليون شيكل - أي حوالي ٩٪ من ميزانية الحوسبة الإجمالية للوزارة. أظهرت الرقابة وجود إخفاقات جوهرية في إدارة أمن المعلومات والسيبرانية في الوزارة، ومنها فجوات في مراقبة صلاحيات إمكانيات الوصول، عدم استنفاد عمليات إدارة المخاطر، غياب آليات إنذار كافية وعدم استكمال تسجيل قواعد المعلومات كما يقتضيه القانون. تبرز هذه النتائج بشكل خاص في ظل الارتفاع الملحوظ (نحو ١٣٠٪) في نطاق الإنذارات السيبرانية التي وردت بشأن الوزارة في سنة ٢٠٢٤، وتوضح أهمية ضمان توفير حماية فعالة لأصول المعلومات التابعة للدولة.

يتناول التقرير أيضًا **الحماية السيبرانية في العمل عن بُعد**، الذي أصبح في السنوات الأخيرة جزءًا لا يتجزأ من نشاط الهيئات العامة والأمنية، وبشكل أكبر خلال فترة جائحة الكورونا وخلال حرب السيوف الحديدية. في إطار الرقابة تم فحص جاهزية الهيئات الحيوية، ومنها شرطة إسرائيل والسلطة القطرية للإطفاء والإنقاذ، للتعامل مع التهديدات السيبرانية المرافقة للعمل عن بُعد. أظهرت الرقابة وجود فجوات معينة في مدى ملاءمة آليات الحماية والرقابة للمخاطر القائمة، كما تم أيضًا الكشف عن وجود نواقص وإخفاقات من خلال فحص اختراق أجراه مكتب مراقب الدولة لمنظومة العمل عن بُعد التابعة لسلطة الإطفاء والإنقاذ. تؤكد هذه النتائج الحاجة إلى استكمال إعداد خطط العمل وتعزيز الجاهزية للأمن السيبراني في الهيئات الحيوية في الدولة.

يشير مجمل نتائج التقرير إلى أن تقدم دولة إسرائيل

نحو الحوكمة الرقمية المتقدمة يستوجب استثمارًا متواصلًا في البنى السيبرانية التحتية، في إدارة المخاطر، في الرقابة وفي الإنفاذ، إلى جانب وجوب تعاون وثيق بين جميع الهيئات العامة. إن الحماية الملائمة لأنظمة المعلومات والخدمات الرقمية ليست مجرد حاجة تكنولوجية - بل إنها شرط ضروري للحفاظ على ثقة الجمهور وحماية خصوصية المواطنين وضمان الأداء السليم والمتواصل للخدمة العامة.

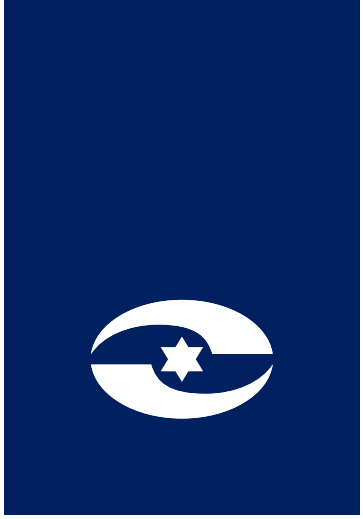
يقع على كاهل الهيئات الخاضعة للرقابة واجب العمل بصورة سريعة وناجعة لتصحيح الإخفاقات والنواقص التي ذُكرت في هذا التقرير.

أتوجه بالشكر الجزيل إلى المستخدمين في مكتب مراقب الدولة، الذين عملوا على إعداد هذا التقرير بمهنية وبدقة وإخلاص، ومن منطلق الشعور بالرسالة. آمل أن تساعد نتائج التقرير وتوصياته في تعزيز المنظومات السيبرانية وأمن المعلومات في القطاع العام، وأن تسهم في تحسين الخدمة المقدمة لمواطني دولة إسرائيل.

نبتهل وندعو بالشفاء العاجل للجرحى، واعادة تأهيل المختطفين الذين عادوا إلينا وأبناء عائلاتهم، وبعودة جميع المُخْلين إلى بيوتهم، وسلامة جنودنا، ونجاح قوات الأمن في الدفاع عن بلادنا.

متنياهو أنـجلمان
مراقب الدولة
ومفوَّض شكاوى الجمهور

القدس،
أيّار **2026**



דוח מבקר המדינה

שירותים מקוונים לציבור: ההזדהות הלאומית והאזור האישי הממשלתי - דוח מיוחד

▪ סיוון התשפ"ו ▪ מאי 2026 ▪

שירותים מקוונים לציבור: ההזדהות הלאומית והאזור האישי הממשלתי - דוח מיוחד

תקציר

רקע

מערכת ההזדהות הלאומית והאזור האישי הממשלתי הם נדבך מרכזי באסטרטגיה הדיגיטלית של ממשלת ישראל, ומטרתם לאפשר גישה טכנולוגית, מאובטחת, אחודה, רציפה ונגישה לשירותים ממשלתיים מקוונים עבור אזרחים ועסקים (גישה המותנית בזיהוי פרטני של מקבל השירות). מערכת ההזדהות מאפשרת למשתמש גישה גם לאזור האישי הממשלתי שנועד לאפשר לאזרחים ולעסקים להתעדכן במידע אישי שקיים במשרדי הממשלה; לבצע פעולות בעצמם; לקבל התראות ותזכורות על פעולות לביצוע, טפסים להגשה או רישיונות לחידוש; ולהתעדכן בסטטוס הפעולות שביצעו מול משרדי הממשלה.

במהלך השנים 2014 עד 2025 התקבלו בממשלה כמה החלטות בעניין קידום השירותים הדיגיטליים לציבור. מכלול החלטות אלה יצר מדיניות ממשלתית רציפה, אשר נועדה לבסס את מערכת ההזדהות בכלל ואת האזור האישי בפרט כמרכיבים מרכזיים במתן שירותים מקוונים לאזרחים ולעסקים. מערכת ההזדהות הלאומית והאזור האישי עלו לאוויר בשנת 2019.

נתוני מפתח

4.6 מיליון
אזרחים היו רשומים למערכת ההזדהות הלאומית בסוף שנת 2024

רק 16%
מהשירותים הממשלתיים שמופו עד כה מחוברים למערכת ההזדהות הלאומית

מאות
טפסים ממשלתיים המיועדים לשימוש הציבור לקבלת שירותים אינם מקוונים, והם מוצעים להדפסה ולמילוי ידני בלבד

23% בלבד
מהטפסים הממשלתיים המקוונים המזוהים (רק כ-400 מתוך כ-1,800) מנוהלים במערכת ההזדהות הלאומית

רק 233 מתוך אלפי
שירותים המוצעים לציבור על ידי הממשלה הונגשו באזור האישי והעסקי הממשלתי

רק 1
רק בית חולים ממשלתי כללי אחד מתוך 11 מחובר למערכת ההזדהות

רק 6%
מהרשויות המקומיות (15 מתוך 258) ניצלו את אפשרות החיבור למערכת ההזדהות הלאומית

3.2 מיליון
רישיונות רכב הופקו בשנת 2024 באמצעות האזור האישי הממשלתי

פעולות הביקורת

בחודשים ינואר עד יולי 2025 בדק משרד מבקר המדינה את יישום המדיניות הממשלתית בדבר הענקת שירותים ציבוריים מקוונים לתושבי המדינה. בביקורת זו נבחן היישום של החלטות הממשלה בנוגע למערכת ההזדהות הלאומית ובנוגע לאזור האישי הממשלתי. הביקורת התמקדה בתהליכי ההזדהות ובהיקף היישומים והשירותים המוצעים לאזרחים ולעסקים וכלולים במערכת ההזדהות ובאזור האישי וכן בחוויית המשתמש בעת תהליכי ההרשמה וההזדהות במערכת ההזדהות ובשימוש באזור האישי. בביקורת נבדקו פעילות מערך הדיגיטל ליישום החלטות הממשלה ושיתוף הפעולה של משרדי ממשלה וגופים נוספים כדי לאפשר לציבור להתחבר למערכת ההזדהות ולקבל שירותים באזור האישי. בדיקות השלמה נעשו ביחידה להזדהות וליישומים ביומטריים במערך הסייבר הלאומי, ברשות המיסים בישראל, במוסד לביטוח לאומי ובשירות התעסוקה.

תמונת המצב העולה מן הביקורת

מערכת ההזדהות הלאומית

חיבור משרדי הממשלה ויחידות הסמך למערכת ההזדהות הלאומית

- יותר מעשור לאחר ההחלטה על הקמת מערכת ההזדהות והחלטות נוספות שקיבלה הממשלה בהמשך, וחרף ההנחיה של היחידה להזדהות וליישומים ביומטריים בדבר חיבור משרדי הממשלה ויחידות הסמך למערכת ההזדהות הלאומית, נמצאו פערים ניכרים בהתחברות שלהם למערכת - 8 משרדי ממשלה מתוך 31 (26%) אינם מחוברים למערכת ההזדהות, ובהם משרד החוץ ומשרד הביטחון המנהל מערכות הזדהות עצמאיות למתן שירותים לאזרחים. מבין 23 המשרדים המחוברים למערכת ההזדהות הלאומית, שלושה משרדים - משרד הבינוי והשיכון, משרד החקלאות ומשרד החדשנות המדע והטכנולוגיה - מאפשרים לקבל באמצעותה רק חלק מהשירותים שהם מספקים, ואילו שירותים אחרים מוצעים לציבור באמצעות מערכת הזדהות עצמאית, כדוגמת מערכת לטובת פרויקט הגרלות דירה בהנחה במשרד הבינוי והשיכון, מערכת יעלה לתהליכי שירות מקוונים בתחום הרישוי והפיקוח במשרד החקלאות ומערכת קדמת המדע במשרד החדשנות המדע והטכנולוגיה.

- רק 11 יחידות סמך ממשלתיות (30%) מתוך כ-36 היחידות מחוברות למערכת ההזדהות הלאומית. נמצא כי המוסד לביטוח לאומי ושירות התעסוקה, הפועלים כתאגידים סטטוטוריים, ורשות המיסים, שהיא יחידת סמך - אינם מחוברים למערכת ההזדהות הלאומית ומנהלים מערכות הזדהות עצמאיות, אף ששלושתם נותנים שירות משמעותי לציבור ואף שנדרשו על פי החלטות הממשלה להתחבר למערכת. כן נמצא כי רק בית החולים רמב"ם, אחד מ-11 בתי החולים הממשלתיים הכלליים, שהם יחידות סמך של משרד הבריאות, מחובר למערכת ההזדהות הלאומית.

- ישנם משרדים ויחידות ממשלתיות שלא התחברו למערכת ההזדהות הלאומית והם מנהלים מערכות הזדהות עצמאיות. הניהול והתחזוקה של מערכת הזדהות עצמאית לצד מערכת ההזדהות הלאומית מביאים לחוסר יעילות, לחשיפה לליקויי אבטחת מידע ולהערמת קשיים על האזרחים והעסקים החפצים לקבל שירותים מגופים אלו.

- **התחברות מצומצמת של רשויות מקומיות למערכת ההזדהות הלאומית לשם מתן שירות לתושב** - הגם שהחלטת הממשלה לא חייבה את הרשויות המקומיות להתחבר למערכת, היא הניעה את המהלכים לחיבור השלטון המקומי למערכת ההזדהות הלאומית. התברר כי כחמש שנים לאחר שהתקבלה ההחלטה רק כ-6% מהרשויות המקומיות (15 מתוך 258) התחברו למערכת כחלופה להזדהות באתר הרשות המקומית. היעדר חיבור של רשויות מקומיות למערכת ההזדהות הלאומית, פוגע בשירות לאזרח שכן הוא מונע את האפשרות להזדהות אחודה לשם קבלת כלל השירותים הממשלתיים והמוניציפליים ומאלץ את האזרחים להתנהל בנפרד מול כל גוף. נוסף על כך, השימוש במערכת הזדהות מקומית, מלבד עלות ניהולה והחזקתה, עלול להחליש את אבטחתו והגנתו של המידע האישי של האזרח ואף לחשוף אותו למתקפות סייבר, לשימוש לא מורשה ולאפשרות של דלף מידע.

- **דיווח של משרדים ויחידות סמך ליחידה להזדהות וליישומים ביומטריים** - יש משרדים ויחידות סמך בעלי מערכת הזדהות עצמאית שאינם מדווחים ליחידה על אופן ביצוע הזיהוי ביישומים שהם מפעילים עבור הציבור, ובהם רשות המיסים, משרד הביטחון ורשות החברות הממשלתיות. בהיעדר דיווח כנדרש על פי החלטת הממשלה, היחידה להזדהות מוגבלת ביכולתה להנחות ולבקר את המשרדים ויחידות הסמך ולוודא כי השירותים שהם מספקים עומדים ברמת הסמך להבטחת הזהות בהרשמה ובאימות הנדרשת על פי מדיניות ההזדהות הלאומית הבטוחה לשמירה על הפרטיות, אבטחת המידע והגנה מפני התחזות או גניבת זהות.

- **מיפוי היישומים והשירותים שניתן לחבר למערכת ההזדהות הלאומית** - למערך הדיגיטל אין יכולת להעריך את פוטנציאל החיבור של מערכת ההזדהות הלאומית לכלל השירותים הדיגיטליים בממשלה ובגופים ציבוריים נוספים מאחר שהוא עדיין לא השלים את מיפוי השירותים הללו. מערך הדיגיטל מיפה עד למועד הביקורת כ-4,000 שירותים שהממשלה נותנת לציבור, כך שניתן להעריך ש-650 השירותים שמוצעים לציבור במסגרת מערכת ההזדהות הלאומית הם כ-16% מהשירותים שמופו עד למועד זה. מלבד השירותים שכבר מופו, יש עוד מאות או אלפי שירותים שטרם מופו ותוקפו (פעולת התיקוף כוללת בין היתר תיעוד האסמכתאות הנדרשות והגופים המעורבים), ובהם שירותים מקוונים לאזרחים ולעסקים הניתנים על ידי גופים סטטוטוריים, רשויות מקומיות, בתי חולים ממשלתיים וגופים ציבוריים נוספים. היעדר תמונה ברורה של היישומים והשירותים הדיגיטליים שנותנים גופי הממשלה והגופים הציבוריים פוגע במימוש הפוטנציאל והיכולות של מערכת ההזדהות הלאומית. כמו כן בהעדר מיפוי אין ליחידה להזדהות אפשרות להבטיח שכלל היישומים המזוהים עומדים בדרישות המדיניות הלאומית להזדהות בטוחה. בנוסף הדבר פוגע ביכולת לממש כראוי את מדיניות "פעם אחת", המבוססת על מתן שירותים לאזרח תוך זיהויו האחיד בכלל המערכות הממשלתיות.

- **היקף השימוש בטפסים מקוונים מזוהים** - פחות מ-25% (כ-400 בלבד) מהטפסים שמנהלים משרדי הממשלה באמצעות מערך הדיגיטל הם טפסים מקוונים מזוהים, שמייתרים את הצורך בהזנת נתונים אישיים על ידי האזרח. מערך הדיגיטל לא קבע מדיניות בנוגע לטפסים המקוונים בכלל ולטפסים המזוהים בפרט כדי לקדם באופן פעיל את מימוש הרציונל שנקבע בהחלטת הממשלה לשימוש בתשתיות ממשל זמין ובטפסים מקוונים מזוהים לצורך מימוש מדיניות "פעם אחת".

- **טפסים למילוי ידני** - קיימים שירותים רבים לציבור שניתן לצרוך רק באופן לא מקוון באמצעות טפסים להדפסה ולמילוי ידני בלבד, ובהם השירותים הקונסולריים של משרד החוץ - 16 מתוך 18 טפסים (89%); בתי הדין הרבניים - 31 מתוך 39 טפסים (79%); ורשות האוכלוסין וההגירה - 71 מתוך כ-140 טפסים (51%). המצב הקיים מקשה על הציבור ודורש ריבוי פעולות ידניות לשם צריכת השירותים, אינו מאפשר לעמוד בהחלטות הממשלה הנוגעות לצמצום הנטל הבירוקרטי על אזרח ולייעל את השירות הניתן לו ואף משקף חוסר יעילות שכן הוא מחייב טיפול ידני בטפסים אלו בגופים נותני השירותים.

האזור האישי הממשלתי

הנגשה מצומצמת של שירותים באזור האישי הממשלתי - בחלוף כחמש שנים מקבלת החלטת הממשלה על האצת פיתוח האזור האישי הממשלתי באופן שיאפשר לציבור לבצע את כלל הפעולות הנדרשות מול משרדי ממשלה וגופים ציבוריים באמצעותו, רק 34 מתוך יותר מ-67 משרדי ממשלה ויחידות סמך הציעו שירותים במסגרת האזור האישי והעסקי, ואף זאת באופן חלקי - 233 שירותים מתוך אלפי שירותים פוטנציאליים. כמו כן, מאות רשויות מקומיות ועשרות גופים ציבוריים נוספים המציעים שירותים מקוונים לאזרחים ולעסקים בתחומי חיים רבים ומגוונים, ובהם חינוך, תעסוקה, בריאות, נכויות ומוגבלויות, שירותים לשוהים בחוץ לארץ והגנת הצרכן, אינם מנגישים אותם באזור האישי הממשלתי. לפיכך האזור האישי אינו מממש את ייעודו כתשתית מרכזית דיגיטלית לקשר עם האזרח ולביצוע פעולות על ידו למול הממשלה והגופים הציבוריים.

גופים ציבוריים המפעילים אזור אישי עצמאי הנפרד מהאזור האישי הממשלתי - מאות שירותים מוצעים לאזרחים ולעסקים באזורים אישיים עצמאיים של גופים ציבוריים שונים שאינם מחוברים לאזור האישי הממשלתי, ובהם משרד הביטחון, משרד החקלאות, משרד הבינוי והשיכון, שירות התעסוקה, צה"ל, הרשויות המקומיות, רשות המיסים, המוסד לביטוח לאומי ומשרד החינוך. קבלת השירותים מהאזורים האישיים הללו שלא באמצעות האזור האישי הממשלתי מחייבת תהליכי הזדהות נוספים לשם כניסה לכל אתר בנפרד, ואינה מאפשרת שמירה על אחידות המעניקה חוויה אמינה ומוכרת למשתמש עם שירות שלם ואחוד; מענה מלא בכתובת אחת; שירות פשוט, נוח וברור, ללא בזבוז זמן ומשאבים.

הנגשת שירותים בקשר לאירועים מרכזיים בחיי האדם (אירועי חיים) - יותר מארבע שנים אחרי המועד שנקבע למימוש החלטת הממשלה שמטרתה להקל על האזרח בביצוע פעולות מול גופים ממשלתיים ובייחוד בעת אירועי חיים משמעותיים (כגון לידה, מעבר דירה ומעבר בין עבודות), 42% מהשירותים הניתנים בעת אירועים אלו (18 מתוך 43), שנקבע בהחלטת הממשלה כי יועלו לאזור האישי, עדיין אינם פועלים בו. עקב כך, האזרח עדיין נדרש לבצע את רוב הפעולות הבירוקרטיות הנוגעות לאירועי חיים באמצעות ניווט עצמאי ונפרד באתרים השונים של נותני השירותים. לדוגמה, בעת מעבר בין עבודות שלושה גופים שונים מטפלים בתהליכי חיפוש עבודה, באבחון תעסוקתי, בבקשות להחזר מס ולהבטחת הכנסה ובתיאום מס.

היקף השירותים הניתן באזור העסקי באתר הממשלתי - בסוף שנת 2024 הוצעו באזור העסקי רק 46 מתוך מאות השירותים שנותנת הממשלה לעסקים; מדובר בשירותים שנותנים עשרה גופים בלבד מתוך כ-67 משרדי הממשלה ויחידות הסמך ועשרות הגופים הציבוריים הנותנים שירותים לעסקים. גופים מרובי שירותים לעסקים, ובהם רשות המיסים, המוסד לביטוח לאומי, משרד הבריאות, משרד האנרגיה והמשרד להגנת הסביבה, מציעים, אם בכלל, שירותים מעטים בלבד באזור העסקי. היקף השירותים הדל המוצע באזור העסקי אינו נותן מענה של ממש לצורך בשירותים דיגיטליים מתקדמים לעסקים המרוכזים במקום אחד ומשקף אי יישום של החלטת הממשלה בנושא.

חוויית המשתמש בתהליך ההזדהות ובאזור האישי הממשלתי

חוויית המשתמש במערכת ההזדהות ובאזור האישי - תהליך ההרשמה הקיים ומאגרי האימות הקיימים אינם מאפשרים לאזרחים שאין להם כרטיס אשראי ודרכון בתוקף להירשם באופן קל ונוח למערכת. כמו כן, בתהליך ההזדהות המשתמש מועבר ככלל למנגנון שלילת היותו בוט באמצעות תהליך זיהוי אלמנטים מתוך תמונה שחוזר על עצמו שוב ושוב פעמים רבות. תהליך מייגע זה פוגע בחוויית המשתמש; הוא עלול להפחית את הנכונות להשתמש באתר ולהגדיל את שיעורי הנטישה של תהליך ההזדהות בכלל ושל השימוש באזור האישי בפרט. יצוין כי גם מסקר שביצע מערך הדיגיטל בשנת 2024 בקרב משתמשי האזור האישי, עלה כי 65% מהם חוו קשיים בתהליך ההזדהות והכניסה לאזור האישי.

התמצאות באזור האישי ובתוכן המצוי בו - המסך הראשי שמוצג לאזרח לאחר התחברותו לאזור האישי ואשר אמור להיות שער כניסה לשימוש יעיל באזור זה אינו ממומש תכלית זו: המסך הראשי אינו מציג למשתמש מידע משמעותי, כדוגמת לוח מחוונים (דשבורד) ובו נתונים על אודותיו; השירות המוצע במסך זה מצומצם בהתחשב באלפי השירותים שהממשלה מציעה לאזרחיה; הוא אינו מבליט את השירותים המרכזיים הנדרשים לאזרח בתחומי החיים השונים; הוא אינו כולל קטלוג של השירותים המקוונים המוצעים באתר - הן ישירות והן כקישור לאתרים אחרים; ותוכנו מוצג בעברית ובערבית בלבד, ואינו מונגש לדוברי שפות אחרות כגון רוסית או אנגלית.

פעילות מערך הדיגיטל - תצוין לחיוב פעילות מערך הדיגיטל לקידום הטרנספורמציה הדיגיטלית במגזר הציבורי, ובכלל זה הקמת התשתיות הרלוונטיות, פעילות למיפוי השירותים, הקמת תשתיות המאפשרות הן הוספה של טפסים מקוונים מזוהים והן הוספת שירותים לאזור האישי באופן עצמאי על ידי המשרדים וקידום תהליך הדיגיטציה ברשויות המקומיות.

בתקופת הביקורת ובעקבותיה יישם מערך הדיגיטל כמה שינויים בתהליכי ההזדהות המשפיעים לטובה על חוויית המשתמש; בין היתר הוא יישם בתהליך ההזדהות מנגנון חדש לשלילת הזדהות של בוטים, המבוסס על רכיב חדש שפועל בצורה שונה ומשפר את חוויית המשתמש.

עיקרי המלצות הביקורת

על משרדי הממשלה ויחידות הסמך - לרבות בתי החולים הממשלתיים - להתחבר למערכת ההזדהות הלאומית ולהציע לציבור באמצעותה את שירותיהם המזוהים. בכלל זה, על משרד החוץ, משרד הבינוי והשיכון, משרד החקלאות ומשרד הביטחון להשלים את חיבור כלל השירותים המזוהים שהם מציעים לציבור למערכת ההזדהות הלאומית ולאפשר לכלל המשתמשים לקבל את כל השירותים המזוהים באמצעות מערכת הזדהות אחת. כמו כן, על רשות המיסים, המוסד לביטוח לאומי ושירות התעסוקה בשיתוף מערך הדיגיטל לבצע את ההתאמות הנדרשות והסרת חסמים טכנולוגיים אם קיימים לצורך חיבורם למערכת ההזדהות הלאומית בהקדם.

על היחידה להזדהות למפות את כלל משרדי הממשלה ויחידות הסמך הנתונים לסמכותה בהתאם להחלטת הממשלה ולוודא כי גופים אלו ידווחו לה על כלל השירותים המזוהים הניתנים על ידם ועל אופן ביצוע הזיהוי בהם. על היחידה להזדהות לקבוע מנגנוני הנחיה ובקרה יזומים כגון דגימות כדי להבטיח שהשירותים המזוהים הניתנים על ידי גופים אלו אכן עומדים ברמת הסמך להזדהות הנדרשת על פי המדיניות, בהתאם להחלטה 2960.

לאור היתרונות שבשימוש במערכת ההזדהות הלאומית, ובהם החיסכון בצורך בניהול ובתחזוקה של מערכת הזדהות עצמאית, הסתמכות על התשתית הממשלתית המאובטחת ושיפור השירות הציבורי לאזרחים ולעסקים, מומלץ כי מערך הדיגיטל בשיתוף היחידה להזדהות, לאחר שישקלו ויבחנו את הנושא, יפעלו לאסדרה מתאימה כך שגופים ציבוריים המספקים שירותים הדורשים הזדהות יחויבו להתחבר למערכת ההזדהות הלאומית. מומלץ כי הגופים הסטטוטוריים וכן הרשויות המקומיות שטרם התחברו למערכת ההזדהות הלאומית, בשיתוף מערך הדיגיטל ומשרד הפנים, יקדמו את תהליכי החיבור למערכת ההזדהות כדי לשפר את השירות לאזרח, תוך חיסכון בעלויות של הפעלת מערכות מקבילות, וכדי שכלל הגופים הציבוריים יפעלו על בסיס פרוטוקול הזדהות ממלכתי אחיד ומאובטח.

- מומלץ שמערך הדיגיטל יקבע מדיניות בעניין הטפסים המקוונים ויכין תוכנית מערכתית לקידום ההמרה של טפסים לא מקוונים ושל טפסים מקוונים לא מזוהים לטפסים מקוונים מזוהים. בהמשך לכך, מומלץ שהמערך יקדם מול משרדי הממשלה הרלוונטיים את מימוש התוכנית כך שהיקף הטפסים המקוונים המזוהים יגדל באופן ניכר. עוד מומלץ כי מערך הדיגיטל, בשיתוף הגופים הציבורים הרלוונטיים, יוסיף לאזור האישי הממשלתי את המידע בנוגע לסטטוס הטיפול בבקשות שהוגשו באמצעות טפסים אלו.

- על משרדי הממשלה ויחידות הסמך, ובפרט על בתי הדין הרבניים, משרד החוץ ורשות האוכלוסין, להמשיך ולקדם בסיוע מערך הדיגיטל את הנגשת הטפסים הרלוונטיים באתריהם גם כטפסים מקוונים ומזוהים.

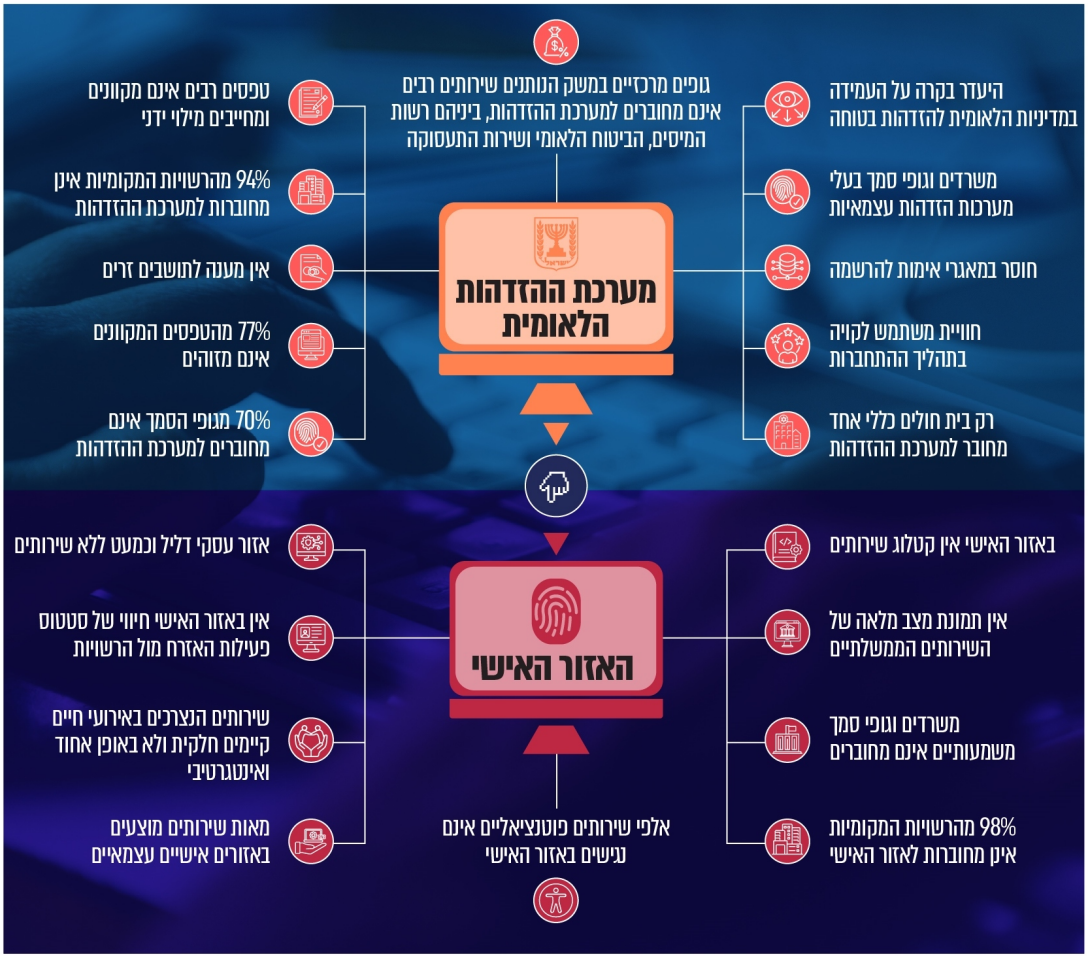
- לשם שיפור השירות לאזרח וצמצום הנטל הבירוקרטי המוטל עליו, וכנדרש בהחלטות הממשלה, על כל משרדי הממשלה, יחידות הסמך והרשויות המקומיות, ובפרט הגופים הכלולים בהחלטות הממשלה - משרד הביטחון, משרד החקלאות, משרד הבינוי והשיכון, שירות התעסוקה, צה"ל, הרשויות המקומיות, רשות המיסים, המוסד לביטוח לאומי, משרד החינוך, רשות האוכלוסין וחברת החשמל - האמונים על מאות שירותים המיועדים לאזרחים ולעסקים, להמשיך ולקדם את הנגשת השירותים המוצעים על ידם גם באמצעות האזור האישי הממשלתי, ובכלל זה לשקף מידע חשוב ועדכני לאזרח - כדוגמת חובות, זיכויים, התראות על הצורך בביצוע פעולות, הודעות חשובות ודוחות שנדרש להגישם.

- על כלל הגופים הנותנים שירותים לעסקים, ובפרט רשות המיסים, המוסד לביטוח לאומי, משרד הבריאות, משרד האנרגייה והמשרד להגנת הסביבה, להנגיש בהקדם את שירותיהם לעסקים גם במסגרת האזור העסקי, באופן ישיר או באמצעות קישור מתוך האזור העסקי הממשלתי אל האתר האישי של כל אחד מהגופים.

- על מערך הדיגיטל להרחיב ולטייב את פעילות האזור האישי והעסקי בהתאם להחלטת הממשלה, כך שיעמוד לרשות אזרחי המדינה אזור אישי ועסקי מתקדם, משמעותי, שימושי ואינטראקטיבי, המאפשר גישה פשוטה ונוחה לכלל השירותים המקוונים הממשלתיים.

- חוויית משתמש טובה תורמת ליעילות השירות, לשוויון בגישה, לשקיפות ולשיפור היחסים שבין המדינה לאזרח. על מערך הדיגיטל לשפר באופן ניכר את חוויית המשתמשים בתהליכי ההרשמה וההזדהות למערכת ההזדהות והשימוש באזור האישי. מומלץ להוסיף לוח מחוונים מרוכז מותאם אישית המציג את המידע הרלוונטי לאזרח באותו המועד, כדוגמת חובות לתשלום וזיכויים, ולהרחיב את ההתראות על פעולות שיש לבצע, הודעות חשובות ודוחות שנדרש להגישם - תזכורות אשר יהיה בהן כדי לשפר את חוויית המשתמש ולהגביר את התועלת שהציבור יכול להפיק מהאזור האישי. כמו כן מומלץ להוסיף מפת אתר וקטלוג של השירותים המוצעים במסגרת האזור האישי, להנגישו לדוברי שפות נוספות ולבחון שילוב מנגנוני אבטחה שלא יפגעו בחוויית השימוש באתר. זאת, לצד הרחבה ניכרת של סל השירותים המוצעים באזור האישי לשם שיפור חוויית המשתמש, כפי שנקבע בהחלטות הממשלה שתכליתן להנגיש את כלל שירותי הממשלה באזור האישי.

עיקרי הליקויים בדוח



סיכום

בשנים האחרונות חלה ברחבי העולם האצה ניכרת בפיתוח ובהנגשה של שירותים דיגיטליים מזוהים, ומדינות רבות מציעות כיום שירותים אלו בהיקף רחב. לצורך מתן שירותים מזוהים באופן מרוכז ובהיקף הראוי נדרש להקים ולהפעיל תשתית ממשלתית מרכזית, אשר תאפשר מנגנון הזדהות אחוד מול מגוון רחב של אתרים ושירותים ממשלתיים וכן אזור אישי ממוקד אשר ירכז את כלל השירותים הממשלתיים המיועדים לאזרחים ולעסקים. משנת 2014 קיבלה ממשלת ישראל כמה החלטות שתכליתן להעניק לאזרחים את מרב השירותים הציבוריים באופן מקוון. יישומה של מדיניות ממשלתית זו מחייבת מימוש של החלטות הממשלה בקשר להקמת מערכת הזדהות לאומית דיגיטלית ואזור אישי ממשלתי שירכז את כלל השירותים הציבוריים לאזרח באתר אחד. יישום המדיניות הממשלתית והחלטות הממשלה בנושא נוגע למאות גופים ממשלתיים וציבוריים, ובהם משרדי ממשלה, תאגידים סטטוטוריים, רשויות מקומיות, חברות ממשלתיות ועוד, המספקים אלפי שירותים שניתנים כיום לציבור ללא מיצוי האפשרויות המקוונות שיש בהן כדי לטייב ולייעל את השירות באופן דרמטי.

ממצאיו של דוח ביקורת זה מצביעים על כך שיותר מעשור אחרי החלטת הממשלה הראשונה על הקמת תשתית ההזדהות הממשלתית, ועל אף שורה של החלטות ממשלה נוספות שהתקבלו במהלך עשור זה בעניין מערכת ההזדהות והאזור האישי, המדיניות הממשלתית וההחלטות שנועדו לקדמה מיושמות באופן איטי וחלקי, ואזרחי המדינה עדיין אינם יכולים ליהנות מקבלת מרבית השירותים הציבוריים באופן מקוון, מרוכז וידידותי. בביקורת נמצאו פערים בפעולות מערך הדיגיטל ליישום החלטות הממשלה בנוגע למערכת ההזדהות הלאומית והאזור האישי, בפעולות מערך הסייבר ליישום המדיניות הלאומית להזדהות בטוחה ובפעולתם של משרדי ממשלה וגופים ציבורים

נוספים לצורך התחברות למערכת ההזדהות ולאזור האישי. פערים אלה נמצאו בארבעה תחומים מרכזיים: היעדר תמונת מצב בדבר פוטנציאל השירותים לחיבור למערכת ההזדהות ממשלתית; חיבור חלקי בלבד של גופים ציבוריים למערכת ההזדהות הלאומית; חיבור חלקי בלבד של גופים ציבוריים ומיעוט שירותים ממשלתיים המונגשים לאזרח באזור האישי הממשלתי; ופערים בחוויית המשתמש בתהליך ההזדהות ובאזור האישי הממשלתי.

ייעודו של האזור האישי כתשתית מרכזית דיגיטלית לקשר עם האזרח ולביצוע פעולות על ידיו למול הממשלה והגופים הציבוריים, מחייב את כלל הגופים הציבוריים להתחבר למערכת ההזדהות הלאומית ולהציע פרו-אקטיבית באמצעות האזור האישי והעסקי שירותים נגישים ומותאמים אישית, מקצה לקצה, וזאת באופן ידידותי, פשוט, נוח וברור. כדי להשיג יעילות וחיסכון, צמיחה כלכלית ופישוט של תהליכים בירוקרטיים באמצעות טרנספורמציה דיגיטלית לאומית, על מערך הדיגיטל להכין תוכנית עבודה מפורטת להרחבת היקף היישומים המחוברים למערכת ההזדהות הלאומית והשירותים המוצעים במסגרת האזור האישי והעסקי, ובכלל זה לוחות הזמנים והבקרות הנדרשות להבטחת מימושה, וככל הנדרש לקדם החלטות ממשלה לאכיפת שיתוף הפעולה של משרדי הממשלה והגופים הציבוריים לשם קידום הטרנספורמציה הדיגיטלית של שירותיהם במערכת ההזדהות הלאומית ובאזור האישי הממשלתי.

דוח מבקר המדינה

הגנת הסייבר בעבודה מרחוק בעיתות שגרה וחירום

▪ סיוון התשפ"ו ▪ מאי 2026 ▪

הגנת הסייבר בעבודה מרחוק בעיתות שגרה וחירום

תקציר

רקע

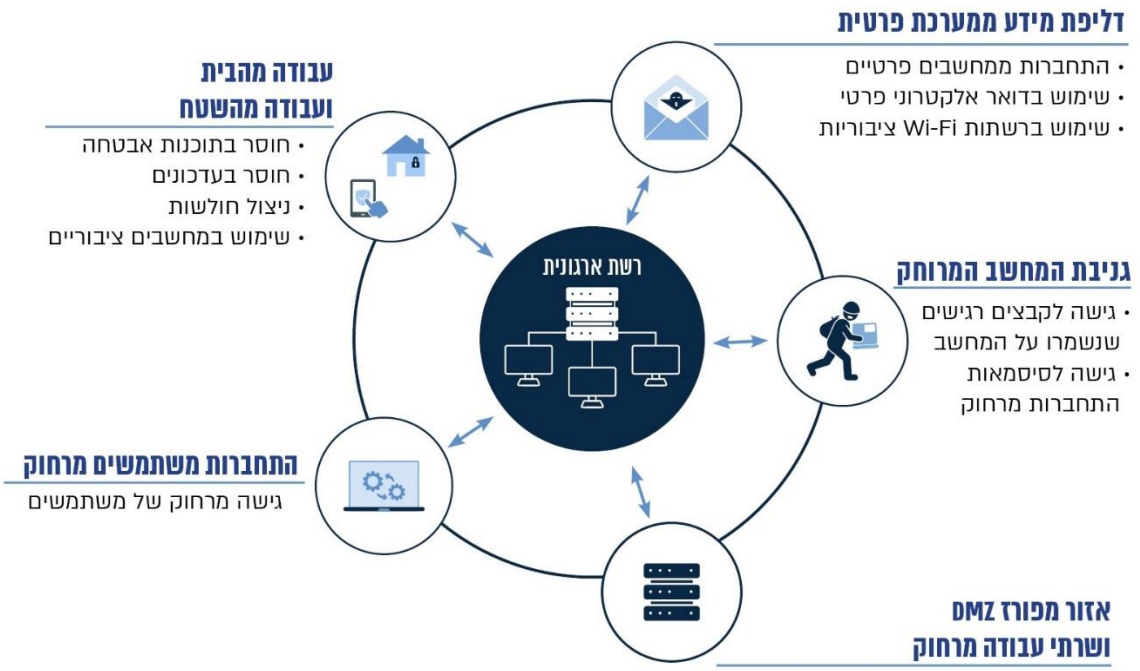
"עבודה מרחוק" מתבצעת בכמה מתווים: עבודה המתבצעת בדרך כלל מבית המגורים של העובד או ממקום אחר תוך שימוש בטכנולוגיית מידע ותקשורת ולא מהאתר של המעסיק (מקום העבודה); התחברות של עובדי שטח למערכות הארגון. בעידן הטכנולוגי עבודה מרחוק הפכה לחלק בלתי נפרד מתפקוד המשק. עבודה מרחוק מאפשרת גמישות תפעולית (כגון לעובדים הנדרשים לעבוד במקומות גיאוגרפיים שונים), וכן היא מקנה גמישות לעובדים המבקשים לאזן בין העבודה לבית ומאפשרת שמירה על רציפות תפקודית במצבי משבר (כמו מלחמות או מגפות) שבהם עובדים אינם יכולים להגיע למקום עבודתם. למשל, הצורך של ארגונים בכל העולם ביכולת עבודה מרחוק התעצם במיוחד בעת מגפת הקורונה, ובישראל הוא התעצם גם בתקופת מלחמת חרבות ברזל.

נציבות שירות המדינה מאפשרת כיום לכל עובד מדינה לעבוד מרחוק יום בשבוע, ומרבית הגופים בשירות המדינה עובדים כך. מדובר במאות אלפי עובדים במגזר הציבורי ובהם משרדי הממשלה, מערכת החינוך הממשלתית, מערכת הבריאות הממשלתית, גופי הביטחון, חברות ממשלתיות, שלטון מקומי ותאגידים.

שני הגופים העיקריים שנבדקו בביקורת הם משטרת ישראל (המשטרה) והרשות הארצית לכבאות והצלה (כב"ה), והם גופי החירום המרכזיים במדינת ישראל, הפועלים באופן שוטף למתן מענה מהיר ויעיל על אירועים מבצעיים, פליליים וביטחוניים - הן בעיתות שגרה והן בעיתות חירום.

מערכות העבודה מרחוק הן כיום רכיב קריטי בתפקודו של מערך הביטחון הלאומי.

עבודה מרחוק - מתארי תקיפה ואיומים אפשריים



הוכן בידי משרד מבקר המדינה.

נתוני מפתח

מאות אלפי

עובדי המגזר הציבורי רשאים לעבוד יום בשבוע מהבית, והם מבצעים זאת באמצעות התחברות מרחוק לרשת המשרדית

עשרה חודשים

לאחר שהנחה מערך הסייבר הלאומי את מערך הדיגיטל להפסיק את השימוש בתשתית העבודה מרחוק שלו משום שנמצאו בה חולשות קריטיות אשר נוצלו לרעה, נמצא כי מערך הדיגיטל ו-65% ממשרדי הממשלה עדיין השתמשו בתשתית זו. השימוש בתשתית הופסק בינואר 2025

0

מבדקי חדירה בוצעו במערכת העבודה מרחוק ברשות לכבאות והצלה (עד לביצוע המבדק על ידי משרד מבקר המדינה במהלך הביקורת)

אלפי

מחשבים ניידים וטאבלטים של המשטרה משמשים לעבודה מרחוק

במאות

כבאיות יש ללוחמי האש גישה לעבודה מרחוק מהשטח

פעולות הביקורת

בחודשים יולי 2024 עד אוגוסט 2025 בדק משרד מבקר המדינה את נושא הגנת הסייבר בעבודה מרחוק בעיתות שגרה וחירום. במסגרת ביקורת זו נבדקו הרשתות הארגוניות של כמה גופים, ובהם גופים במגזר הביטחון הלאומי, המרבים להשתמש במתאר העבודה של עבודה מרחוק במסגרת פעילותם השוטפת, לרבות במסגרת פעילות מבצעית. בביקורת נבדקו בין היתר הנושאים האלו: אסדרה של אבטחת המידע בעבודה מרחוק, אבטחה של מכשירים ניידים ותהליכי העבודה מרחוק, אבטחת המשאבים הארגוניים בגישה מרחוק, מדיניות ונהלים לגבי עבודה מרחוק ועבודה בשעת חירום. הביקורת נעשתה ברשות הארצית לכבאות והצלה, במשטרת ישראל, בהנהלת בתי המשפט, במשרד הכלכלה והתעשייה - במערך הדיגיטל הלאומי (מערך הדיגיטל), לרבות ביחידה להגנת הסייבר בממשלה (יה"ב), במשרד ראש הממשלה - במערך הסייבר הלאומי (מס"ל) ובמשרד המשפטים - ברשות להגנת הפרטיות.

יצוין כי חלק מהממצאים בדוח מסומנים עם סיווג חומרה גבוה (לרוב מדובר בממצאים רוחביים הנוגעים לגופים רבים או לממצאים שרמת הנזק שלהם עשויה להיות גבוהה או שההסתברות להתרחשותם גבוהה).

משרד מבקר המדינה ביצע בכב"ה מבדק חדירה. מטרת המבדק הייתה לזהות חולשות העשויות לסכן את הזמינות, המהימנות והסודיות של התשתיות הנגישות לעובדים מרחוק, זאת באמצעות תרחישי תקיפה שונים שבמסגרתם מנוצלות חולשות אבטחה. מאחר שהבדיקה בוצעה בסביבת הייצור ננקטו כמה פעולות להפחתת הסיכונים הכרוכים בביצועה, והדבר השפיע על תכנון המבדק. למשל, כלים אוטומטיים הופעלו באמצעות סריקה מדורגת כדי שלא להכביד את העומסים על השרתים, ולא נוצלו חולשות שנמצאו במבדק אלא רק הוכחה היכולת לנצלן.

משרד מבקר המדינה מציין לחיוב את שיתוף הפעולה מצד כב"ה ויחידת הסייבר המגזרית של המשרד לביטחון לאומי (היחידה המגזרית) בכל שלבי מבדק החדירה: החל בתכנון המבדק, עבור דרך ביצועו ותהליך הצגת הממצאים וכלה בנקיטת פעולות לשיפור התהליכים הקיימים ובטיפול בחלק מהליקויים שנמצאו עוד לפני פרסום הדוח.

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).

תמונת המצב העולה מן הביקורת

- **מסמך דגשים לעבודה מרחוק של הרשות להגנת הפרטיות** - הרשות להגנת הפרטיות פרסמה בשנת 2020 - בעקבות התפשטות נגיף הקורונה - מסמך דגשים לעבודה מרחוק שלא התעדכן מאז ולכן כולל המלצות על שימוש בפתרונות אבטחת מידע שאינם עדכניים (כמו אנטי-וירוס) או פרוטוקולי הצפנה (כמו WPA2 ל-Wi-Fi).

- **השוואת הנושאים העיקריים בהנחיותיהם של מס"ל ויה"ב בנושא אבטחת העבודה מרחוק** - אין תאימות בין הנחיות מס"ל בנושא עבודה מרחוק לאלו של יה"ב, אף שיה"ב מונחית על ידי מס"ל.

- **פיקוח מס"ל על יישום הנחייתו בנושא עבודה מרחוק במערך הדיגיטל** - מאוקטובר 2023, מועד פרסום ההנחיה לחיבור משתמשים מרחוק לרשת הארגונית בגופי תמ"ק (תשתיות מדינה קריטיות), מס"ל לא פיקח באופן מלא על יישום הבקרות הכלולות בהנחיה במערך הדיגיטל אלא ביצע מבדק חדירה לתשתית העבודה מרחוק ובמסגרתו נבדקו רק חלק מהנושאים.

- **פיקוח יה"ב על יישום הנחייתה בנושא עבודה מרחוק במשרדי הממשלה** - ממרץ 2020, מועד פרסום ההנחיה לגישה מרחוק, יה"ב לא ביצעה בקרה על אופן יישום ההנחיה במשרדי הממשלה המונחים על ידה. כמו כן, מדד יה"ב, שמשמש תבנית אחודה שלפיה מפקחים על עמידתם של משרדי ממשלה בהיבטים שונים של הנחיות אבטחת מידע, כולל רק חמש בקרות על עבודה מרחוק, וזאת בשעה שהנחיית יה"ב בנושא זה כוללת 45 בקרות, ועל כן יש חשש כי פיקוח על פי המדד מספק תמונת מצב חלקית בלבד על מצב אבטחת המידע בהיבטי עבודה מרחוק.

- **פיקוח היחידה המגזרית של המשרד לביטחון לאומי על יישום הנחיית מס"ל בנושא עבודה מרחוק** - מס"ל לא העביר ליחידה המגזרית של המשרד לביטחון לאומי את הנחייתו מאוקטובר 2023 לחיבור משתמשים מרחוק לרשת הארגונית. על כן היחידה המגזרית, האחראית להנחיית כב"ה, לא פיקחה על אופן יישום ההנחיה בכב"ה.

- **השימוש של כ-65% ממשרדי הממשלה במוצר טכנולוגי לעבודה מרחוק שהיו בו חולשות רבות, ובניגוד להנחיית מס"ל** - אף שמס"ל הנחה את מערך הדיגיטל עוד במרץ 2024 שלא להשתמש בכלי י"ג, המשמש לעבודה מרחוק, עקב הפגיעויות הרבות שהיו בו בשנים האחרונות, נכון לאוקטובר 2024 עדיין השתמשו בו מערך הדיגיטל ו-31 (65%) מ-48 משרדי הממשלה, בניגוד להנחיית מס"ל. יצוין כי מערך הדיגיטל נערך להחלפת כלי י"ג באמצעות התקשרות רכש חדשה לאחר קבלת ההנחיה ממס"ל להפסיק את השימוש במוצר, אולם לא הנחה את המשרדים להפסיק את השימוש במוצר זה ולעבור למוצר חליפי שהיה זמין לרכישה באמצעות אחד מן המכרזים המרכזיים הקיימים. רק בינואר 2025 נפסק השימוש במוצר.

הגנת הסייבר בעבודה מרחוק בכב"ה

- **נושאי עבודה מרחוק במדיניות ונוהלי אבטחת מידע** - מסמך מדיניות אבטחת המידע של כב"ה אינו עוסק בנושא העבודה מרחוק, ובנוהלי העבודה מרחוק חסרות בקרות מסוימות שנכללות בהנחיית מס"ל.

- **נושאים טכנולוגיים שנבדקו בנושא עבודה מרחוק** - נבדקו נושאים טכנולוגיים בכב"ה, במשטרה ובהב"ה. מצ"ב פירוט הנושאים שנבדקו: אבטחת גישת מחשבים ומכשירים מרוחקים, אבטחת תווך התקשורת בין המכשירים המרוחקים לארגון, אבטחת המערכות הארגוניות בהיבטי עבודה מרחוק, עדכוני מערכות הפעלה ואבטחה, ניהול משתמשים והרשאות בגישה מרחוק, ניטור אירועי עבודה מרחוק . בחלק מנושאים אלו בחלק מהגופים נמצאו פערים. יצוין כי חלק מן הפערים הללו תוקנו במהלך הביקורת.

- **המשכיות עסקית ורציפות תפקודית** - לכב"ה אין תוכנית המשכיות עסקית (BCP) ועל כן, בין השאר, אין ביכולתה להגדיר את הפערים בציוד וברישיונות הנדרשים לצורך עבודה מרחוק בשעת חירום כדי לשמור על רציפות תפקודית תקינה בעבודה מרחוק, בניגוד לנדרש על פי תורת ההגנה, ולפיה על הארגון לוודא כי הנהלת הארגון הגדירה ואישרה מדיניות ואסטרטגיה בנושא המשכיות עסקית (BCP).

- **תרגילים להתמודדות עם מצבי חירום** - לא בוצעו תרגולים להתמודדות עם אירועי חירום, בניגוד להנחיית מס"ל ולפיה יש לבצע תרגול עיתי של אירועים אלו. עקב כך קיים חשש כי הארגון לא יהיה ערוך לאירוע סייבר ולא ידע לקבל החלטות בזמן אמת וכי העבודה מרחוק תינזק.

- **מבדקי חדירה למערכות עבודה מרחוק** - בכב"ה לא בוצעו מבדקי חדירה למערכת העבודה מרחוק עד אפריל 2025 (המבדק שבוצע במסגרת הביקורת על ידי משרד מבקר המדינה), בניגוד להנחיה של מס"ל, ולפיה נדרש לבצע מבדק חדירה לפתרון הטכנולוגי המשמש לעבודה מרחוק. היעדר ביצוע של מבדקי חדירה גורם לכך שהארגון אינו ער לחולשות שבמערכותיו.

- **מבדק החדירה שבוצע על ידי משרד מבקר המדינה** - משרד מבקר המדינה ביצע סקר הערכות פגיעויות ומבדק חדירה (להלן - "מבדק חוסן") ברשת כב"ה. מטרת מבדק החוסן הייתה לזהות חולשות אבטחת מידע בתשתיות הגישה מרחוק ובתשתיות המחשוב ברשת ארגון כב"ה, אשר גורמים חיצוניים או פנימיים עשויים לנצלן לביצוע תרחישי תקיפה שונים ולהביא בכך לפגיעה בזמינות, במהימנות ובסודיות של המידע והמערכות ברשת.

הגנת הסייבר בעבודה מרחוק במשטרה

- **אימוץ של הנחיות מאסדר מדינתי** - ככלל, החלטה של גוף בדבר אימוץ הנחיות של מאסדר מדינתי, כולן או חלקן, גם אם היא נעשית באופן וולונטרי, הינה מהלך אשר לדעת משרד מבקר המדינה מחייב את הגוף לקיים את ההנחיות שאימץ. על כן על הגוף להגדיר מראש את גבולות התחייבותו ולפרט את הטעמים להחרגת אותן הנחיות שבחר שלא לאמץ. אימוץ וולונטרי של חלקים מההנחיות שאינם מוגדרים, באופן שאינו מוסדר - עלול לרוקן מתוכן את מהלך האימוץ.

- **נושא העבודה מרחוק במדיניות אבטחת מידע** - מסמך מדיניות אבטחת המידע של המשטרה אינו עוסק בנושא העבודה מרחוק.

- **נושאים טכנולוגיים שנבדקו בנושא עבודה מרחוק** - נבדקו נושאים טכנולוגיים בכב"ה, במשטרה ובהב"ה. מצ"ב פירוט הנושאים שנבדקו: אבטחת גישת מחשבים ומכשירים מרוחקים, אבטחת תווך התקשורת בין המכשירים המרוחקים לארגון, אבטחת המערכות הארגוניות בהיבטי עבודה מרחוק, עדכוני מערכות הפעלה ואבטחה, ניהול משתמשים והרשאות בגישה מרחוק, ניטור אירועי עבודה מרחוק. בחלק מנושאים אלו בחלק מהגופים נמצאו פערים. יצוין כי חלק מן הפערים הללו תוקנו במהלך הביקורת.

המשכיות עסקית ורציפות תפקודית - למשטרה אין תוכנית המשכיות עסקית טכנולוגית (BCP) ועל כן, בין השאר, אין ביכולתה להגדיר את הפערים בציוד וברישיונות הנדרשים לצורך עבודה מרחוק בשעת חירום כדי לשמור על רציפות תפקודית תקינה בעבודה מרחוק, בניגוד לנדרש על פי תורת ההגנה, ולפיה על הארגון לוודא כי הנהלת הארגון הגדירה ואישרה מדיניות ואסטרטגיה בנושא המשכיות עסקית (BCP).

תרגולים להתמודדות עם אירועי חירום - לא בוצעו תרגולים להתמודדות עם אירועי חירום, בניגוד להנחיית מס"ל ולפיה יש לבצע תרגול עיתי של אירועים אלו. עקב כך קיים חשש כי הארגון לא יהיה ערוך לאירוע סייבר ולא ידע לקבל החלטות בזמן אמת וכי העבודה מרחוק תינזק.

מבדקי חדירה למערכות עבודה מרחוק - המשטרה ביצעה מבדק חדירה במערכת הטכנולוגית המשמשת לעבודה מרחוק במהלך הביקורת בתחילת שנת 2025, מבדק שבו נמצאו פערים, כשמונה שנים אחרי המבדק הקודם. זאת בניגוד להנחיה של מס"ל, שלפיה נדרש לבצע מבדק חדירה לפתרון הטכנולוגי המשמש לעבודה מרחוק. היעדר ביצוע של מבדקי חדירה גורם לכך שהארגון אינו ער לחולשות שבמערכותיו.

הגנת הסייבר בעבודה מרחוק בהנהלת בתי המשפט

נושאי עבודה מרחוק במדיניות ובנוהלי אבטחת מידע - בנוהלי העבודה מרחוק בהב"ה חסרות בקרות מסוימות שנכללות בהנחיית יה"ב.

נושאים טכנולוגיים שנבדקו בנושא עבודה מרחוק - נבדקו נושאים טכנולוגיים בכב"ה, במשטרה ובהב"ה: אבטחת הגישה למחשבים ולמכשירים מרוחקים, אבטחת תווך התקשורת בין המכשירים המרוחקים לארגון, אבטחת המערכות הארגוניות בהיבטי עבודה מרחוק, עדכוני מערכות הפעלה ואבטחה, ניהול משתמשים והרשאות בגישה מרחוק, ניטור אירועי עבודה מרחוק. בחלק מנושאים אלו בחלק מהגופים נמצאו פערים. יצוין כי חלק מן הפערים הללו תוקנו במהלך הביקורת.

כב"ה - השבתת כלי י"ג לפני מתקפת הסייבר בינואר 2025 - משרד מבקר המדינה מציין לחיוב את כב"ה על ההחלטה להשבית את כלי י"ג הארגוני לעבודה מרחוק בדצמבר 2024 עם היוודע דבר קיומה של חולשת אבטחה קריטית שהתגלתה בה.

המשטרה - ביצוע סקר סיכונים על מערכות ותהליכי העבודה מרחוק - משרד מבקר המדינה מציין לחיוב את המשטרה על שביצעה בשנת 2024 סקר סיכונים לגבי המערכות והתהליכים הקשורים לעבודה מרחוק, שכלל תחומי איום וחשיפות אפשריות וכן פירוט פעולות שבוצעו כדי לצמצם חשיפות אלו.

עיקרי המלצות הביקורת

- מומלץ כי הרשות להגנת הפרטיות תעדכן את מסמך הדגשים לעבודה מרחוק שפרסמה - או תבחן את הצורך בו - באופן שיהיה רלוונטי ובהלימה להנחיות יתר הגופים האסדרתיים המדינתיים.

- על מס"ל ויה"ב (שמונחית על ידי מס"ל) לבחון ולהתאים את ההנחיות שפרסמו בנושא עבודה מרחוק לגופים המונחים שלהם ולוודא שכלל הבקרות הרלוונטיות נמצאות בהן.

- על מס"ל לפקח באופן עיתי על מידת עמידתו של מערך הדיגיטל כגוף תמ"ק, ובפרט כגוף שמספק תשתיות למשרדי הממשלה, בהנחיה לעבודה מרחוק שפרסם. לחלופין על מס"ל לבקש באופן שוטף ממערך הדיגיטל לדווח לו על מידת עמידתו בהנחיה.

- על יה"ב לבצע בקרה על הגופים שהיא מנחה בכל הנוגע לתחום העבודה מרחוק וכן לבקש מהגופים דיווח על מידת עמידתם בהנחיה שקבעה בנושא.

- על מס"ל לוודא שכל הנחיה חדשה שלו מועברת לכל יחידות הסייבר המגזריות ושהנחיות אלו מיושמות.

- על היחידה המגזרית של המשרד לביטחון לאומי האחראית לעבודת כב"ה, לפקח על מידת עמידת כב"ה בהנחיית מס"ל בנושא עבודה מרחוק או לבקש מכב"ה לדווח לה על מידת עמידתם בהנחיה.

- מומלץ כי מינהל הרכש בשיתוף יה"ב ומס"ל יוודאו כי בכל המכרזים המרכזיים המספקים פתרונות לעבודה מרחוק ייכללו דרישות אבטחת מידע, וכי הגופים האסדרתיים המדינתיים בתחום הסייבר מצאו אותם הולמים לשימוש.

- מומלץ כי אם תתגלה חולשה קריטית במוצרי עבודה מרחוק בעתיד והיצרן לא יספק דרכי התמודדות עימה בטווח זמן קצר, יפרסמו מס"ל ויה"ב הנחיה רלוונטית בסמוך לאחר גילויה של החולשה ויוודאו מול מינהל הרכש שיש הלימה בין הנחיה זו למחויבות החוזית שבהסכמי המכרז המרכזי.

- מומלץ כי יה"ב תבחן את יכולות הכלים הטכנולוגיים שמאפשרים עבודה מרחוק ומוצעים במסגרת מכרזים מרכזיים או במסגרת הסכמי מחירים מרכזיים אל מול דרישות אבטחת המידע הטכנולוגיות שלה ותביא לידיעת המשרדים את ממצאי בחינה זו.

הגנת הסייבר בעבודה מרחוק בכב"ה

- על כב"ה לעדכן את מסמכי המדיניות והנהלים שלה באופן שהם יכללו את הבקרות הנדרשות בהנחיית מס"ל. על היחידה המגזרית במשרד לביטחון לאומי לוודא כי מסמכי המדיניות והנהלים לעבודה מרחוק של הגופים הכפופים להנחייתה תואמים להנחיות.

- על כב"ה לטפל בפערים בנושאים הטכנולוגיים שנמצאו בביקורת ולתקנם.

- מומלץ כי כב"ה תגבש ותאשר תוכנית המשכיות עסקית טכנולוגית (BCP) הכוללת התייחסות להתאוששות המערך הטכנולוגי של הארגון ולעבודה מרחוק בעיתות חירום, כנדרש על פי תורת ההגנה.
- על כב"ה לבצע תרגולים עיתיים של ההמשכיות העסקית של התשתיות הטכנולוגיות שמאפשרות חיבור ועבודה מרחוק, בהתאם להנחיית מס"ל.
- על כב"ה לבצע מבדקי חדירה עיתיים וייעודיים במערכות העבודה מרחוק, בהתאם להנחיית מס"ל.

הגנת הסייבר בעבודה מרחוק במשטרה

- מומלץ כי המשטרה תעדכן את מסמך המדיניות שלה כך שיכלול התייחסות לנושא העבודה מרחוק. כמו כן, הכללת נושא העבודה מרחוק במסמך מדיניות אבטחת המידע של המשטרה עולה בקנה אחד עם הנחיית מס"ל.
- על המשטרה לטפל בפערים בנושאים הטכנולוגיים שנמצאו בביקורת ולתקנם.
- מומלץ כי המשטרה תגבש ותאשר תוכנית המשכיות עסקית טכנולוגית (BCP) הכוללת התייחסות להתאוששות המערך הטכנולוגי של הארגון ולעבודה מרחוק בעיתות חירום, כנדרש על פי תורת ההגנה.
- על המשטרה לבצע תרגולים עיתיים של ההמשכיות העסקית של התשתיות הטכנולוגיות שמאפשרות חיבור ועבודה מרחוק, בהתאם להנחיית מס"ל.
- על המשטרה לבצע מבדקי חדירה עיתיים וייעודיים במערכת העבודה מרחוק, בהתאם להנחיית מס"ל.

הגנת הסייבר בעבודה מרחוק בהנהלת בתי המשפט

- על הב"ה לעדכן את מסמכי המדיניות והנהלים שלה באופן שהם יכללו את הבקרות הנדרשות בהנחיית יה"ב. על יה"ב לוודא כי מסמכי המדיניות והנהלים לעבודה מרחוק של הגופים הכפופים להנחייתה תואמים להנחיות.
- על הב"ה לטפל בפערים הטכנולוגיים שנמצאו בביקורת ולתקנם.

סיכום

עבודה מרחוק הפכה לנפוצה בשנים האחרונות והיא חלק משמעותי במערך העבודה של עובדים וארגונים. היכולת לעבוד מרחוק משמשת עובדי שטח ועובדים שמעוניינים בגמישות, ונוסף על כך בשנים האחרונות, וביתר שאת לאחר משבר הקורונה, היא הפכה לחלק אינטגרלי במערך העבודה של ארגונים, בין היתר כדי להבטיח איזון בין בית לעבודה (כיום נציבות שירות המדינה מאפשרת לעובדי מדינה לעבוד יום בשבוע מהבית, ומרבית הגופים בשירות המדינה עובדים כך).

בארגונים האחראים לטיפול באירועי חירום העבודה מרחוק היא חלק משמעותי מהיכולת לנהל את האירועים ולטפל בהם. כך למשל באירועים כגון שריפות ופעולות טרור עבודה מרחוק חיונית אפוא לשמירה על הרציפות התפקודית של גופי חירום שנדרשים להמשיך לספק שירותים לתושבים, בעיקר בעיתות חירום. צורך זה בא לידי ביטוי באופן בולט במהלך מלחמת חרבות ברזל ובתקופת מגפת הקורונה.

בדוח זה נבחנו ההיערכות של גופים חיוניים והתמודדותם עם האתגרים שמציבה העבודה מרחוק בתחום הגנת הסייבר. מדובר באתגרים שנובעים מכך שתצורת עבודה זו חושפת את הארגון לתקיפות סייבר עקב ריבוי אמצעי גישה מרוחקים.

בביקורת נבדקו מידת מוכנותם ורמת התמודדותם של משטרת ישראל, הרשות הארצית לכבאות והצלה, הנהלת בתי המשפט ומערך הדיגיטל עם סיכונים אלו. כמו כן נבדק כיצד הגופים האסדרתיים המדינתיים - הרשות להגנת הפרטיות, מס"ל, יה"ב והיחידה המגזרית במשרד לביטחון לאומי - מנחים את הגופים וכיצד הם מפקחים עליהם.

ממצאי הדוח מעידים על פערים מסוימים במוכנות של חלק מן הגופים שנבדקו בביקורת להתמודד עם איומי הסייבר הרלוונטיים לעומת ההנחיות של הגופים האסדרתיים המדינתיים בנושא עבודה מרחוק וכן לעומת התצורות ומאפייני העבודה מרחוק הספציפיים של כל גוף. במסגרת הביקורת ביצע משרד מבקר המדינה מבדק חדירה במערכת העבודה מרחוק המרכזית של כב"ה, בשיתוף עימה, מבדק שאיפשר להעריך את מוכנותו של הגוף לעמוד בפני תקיפות סייבר העלולות להתבצע דרך מערכת זו. במבדק נמצאו פערים מסוימים. משרד מבקר המדינה מציין לחיוב את שיתוף הפעולה מצד כב"ה ויחידת הסייבר המגזרית של המשרד לביטחון לאומי בכל שלבי מבדק החדירה.

על משטרת ישראל, הרשות הארצית לכבאות והצלה, הנהלת בתי המשפט ומערך הדיגיטל, בשיתוף מס"ל ויה"ב, לפעול בהקדם להשלמת תוכנית עבודה לטיפול בפערים שצוינו בדוח זה. על מס"ל ויה"ב לוודא שאין פערים כאלה בגופים נוספים שמונחים על ידם.

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.

דוח מבקר המדינה

מערכות מידע ואבטחת מידע וסייבר במשרד החוץ

▪ סיוון התשפ"ו ▪ מאי 2026 ▪

מערכות מידע ואבטחת מידע וסייבר במשרד החוץ

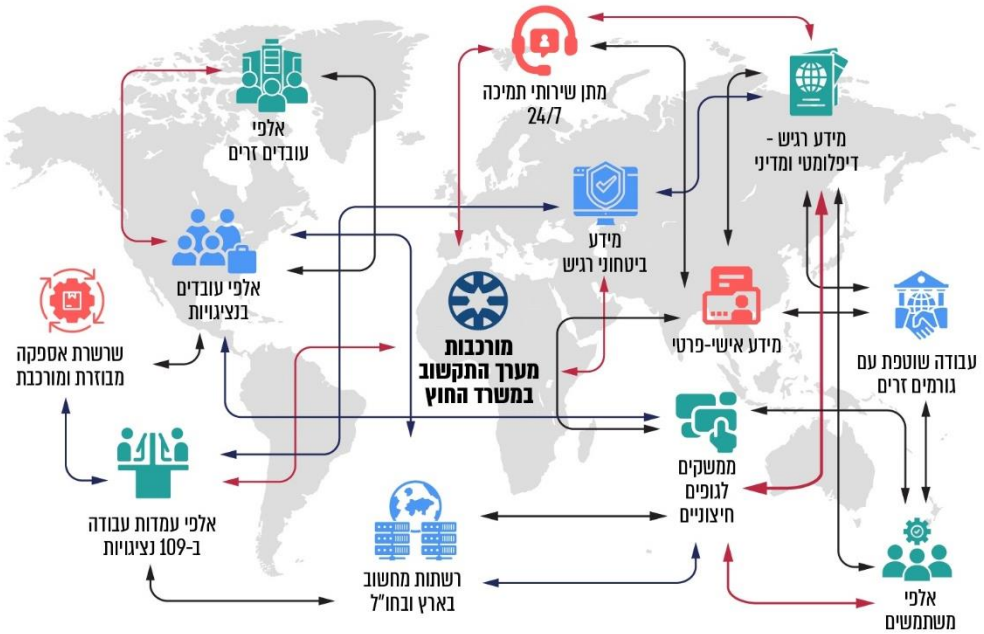
תקציר

רקע

משרד החוץ אחראי לגיבוש מדיניות החוץ של ממשלת ישראל, ביצועה והסברתה. פעולות המשרד מתבצעות באמצעות המשרד הראשי בירושלים ובאמצעות 109 הנציגויות הדיפלומטיות והקונסולריות בחו"ל. המערכות הממוחשבות במשרד החוץ מהוות את התשתית התפעולית של משרד החוץ, והן חיוניות לפעולתו התקינה של המשרד. גורמי המקצוע במשרד החוץ האמונים על מערכות המידע והטכנולוגיה ועל הגנת המידע במשרד הם אגף התקשוב וחטיבת הביטחון במשרד (בטמ"ח).

משרד החוץ נדרש להתמודד עם אתגר מובנה וייחודי, שנגזר מהצורך לנהל מידע מדיני ודיפלומטי רגיש בין המטה לנציגויות.

מערך התקשוב במשרד החוץ - מאפיינים ייחודיים



מערך הדיגיטל הלאומי מנחה מתוקף סמכויותיו את אגף התקשוב במשרד החוץ בכל הנוגע לפעילויות ולתהליכי העבודה העיקריים שלו. באשר להגנה על המידע, יה"ב (יחידת ההגנה בסייבר במערך הדיגיטל הלאומי) מנחה את המשרד לגבי רשת הבלמ"ס, והשב"כ מנחה אותו בכל הנוגע לרשתות מסוימות במשרד.

משרד החוץ הוא יעד מרכזי לתקיפות סייבר של מגוון יריבים, החל בפצחנים בודדים וכלה בגורמים מדינתיים. פעילויות סייבר שזוהו במשך השנים יוחסו לגורמים איראניים, לגורמים מחיזבאללה, מחמאס ואחרים. בשנים 2020 - 2024 אירעו אירועי סייבר חריגים ברשתות המחשוב של משרד החוץ. במהלך מלחמת "חרבות ברזל", חל גידול של כ-500% באירועי הגנת מידע בנציגויות ישראל בחו"ל, ואירעו מאות אירועים בשנת 2023, בהם למשל ניסיון פריצה לדואר אלקטרוני של עובד הנציגות.

נתוני מפתח

85.3 מיליון ש"ח

תקציב תחום התקשוב במשרד החוץ לשנת 2024, המהווה כ-4.5% מסך תקציב המשרד (1.9 מיליארד ש"ח). מתוכו התקציב שהוקצה לתחום הסייבר עמד על כ-13 מיליון ש"ח

EOL

נמצאו מערכות שהוגדרו כפגות תוקף (EOL[1]), או ככאלו הדורשות שדרוג או החלפה

מאות

אירועי הגנת מידע התרחשו בנציגויות ישראל בחו"ל בשנת 2023

הגנה חלקית

רמת ההגנה על המידע ברשתות מסוימות נמוכה מרמת ההגנה הנדרשת ואינה עומדת בדרישות הגורם המנחה

משנת 2018

לא עודכן מסמך מדיניות הגנת הסייבר ואבטחת המידע במשרד החוץ. זאת אף שחלו שינויים מהותיים במפת האיומים ובמבנה הארגוני של מערך התקשוב

ספריות רשת משותפות

נמצאו ספריות בחלק מרשתות המשרד שהיו פתוחות לכלל משתמשי הרשת

תשתיות ומערכות מידע

נמצאו פערים בעדכניות תשתיות ומערכות המידע

15 ממצאים

זוהו במבדק החוסן שביצע משרד מבקר המדינה. הממצאים ברמות סיכון שונות: רמה גבוהה ביותר, רמה גבוהה, רמה בינונית ורמה נמוכה

פעולות הביקורת

בחודשים מרץ 2024 עד אפריל 2025, במהלך מלחמת "חרבות ברזל", ביצע משרד מבקר המדינה ביקורת על מערכות המידע ואבטחת המידע במשרד החוץ. הביקורת בחנה נדבכים הנוגעים לניהול ופיתוח של מערכות המידע במשרד: ממשל טכנולוגיות המידע; ניהול פרויקטים ופיתוח מערכות מידע; תוכנית התאוששות מאסון. כמו כן נבחנו נדבכים הנוגעים לאבטחת המידע והגנת הסייבר במשרד החוץ: ממשל אבטחת מידע; הגנה על המידע ברשתות המחשוב; עדכניות תשתיות ומערכות המידע; הגנה על רשת מסוימת במשרד; הזדהות משתמשים וניהול הרשאות; הגנה על מאגרי מידע לפי חוק הגנת הפרטיות. בנוסף, במהלך חודש מרץ 2025 בוצע מבדק חוסן הכולל סקר הערכת פגיעויות ומבדק חדירה ברשת מסוימת במשרד.

הביקורת נערכה בעיקרה במשרד החוץ. בדיקות השלמה נעשו במערך הדיגיטל הלאומי, לרבות ביה"ב הפועלת בו, במס"ל ובשב"כ.

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].

[1] End of Life.

תמונת המצב העולה מן הביקורת

ניהול ופיתוח של מערכות המידע במשרד החוץ

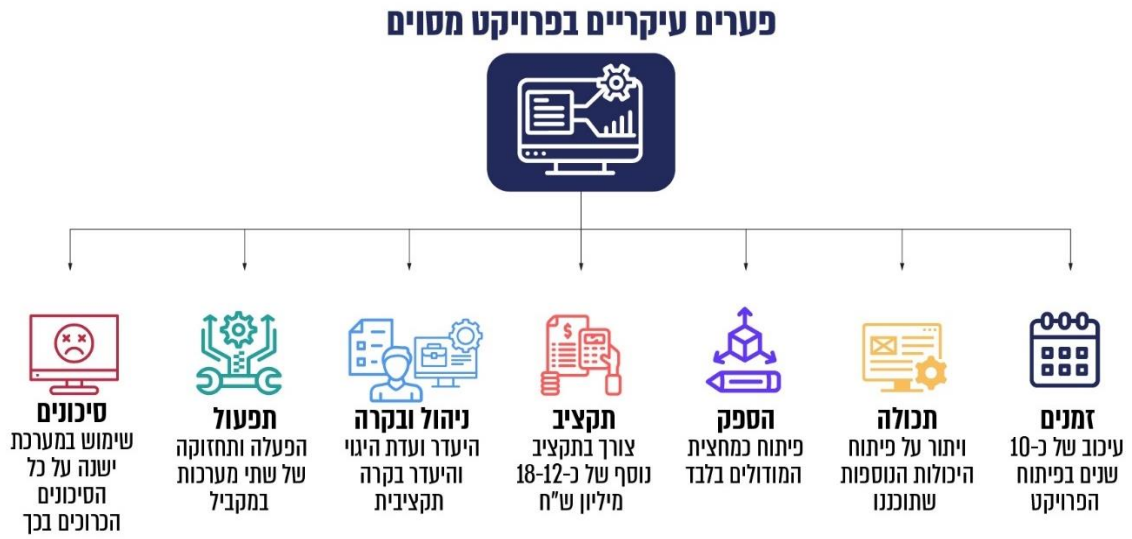
הקמת ועדת היגוי משרדית לתחום התקשוב ופעילותה - בניגוד להנחיות מערך הדיגיטל, ועדת ההיגוי המשרדית לתקשוב שתפקידה בין היתר לקבוע את האסטרטגיה של המשרד ומדיניותו בנושאי תקשוב; לאשר את תוכניות העבודה והתקציבים הרב-שנתיים והשנתיים של כלל הפעילויות המתקיימות במשרד בתחומים של מערכות מידע ותקשוב; לקבוע ולאשרר סדרי עדיפות וחלוקת משאבים; ולעקוב אחר ביצוע התוכניות ולוודא את מימושן, לא התכנסה במשך כשלוש שנים (2021 - 2023). ועדת ההיגוי שבה והתכנסה רק באפריל 2024.

תקציב אגף התקשוב - תקציב משרד החוץ לשנת 2024 עמד על כ-1.9 מיליארד ש"ח. התקציב שהוקצה לתפעול שוטף של תחום התקשוב עמד על 85.3 מיליון ש"ח, המהווה כ-4.5% מסך התקציב. ממסמכי אגף התקשוב עולה שהתקציב שהוקצה לשנת 2024 אינו מספק ואינו תואם את צורכי המשרד בפועל, וכי יש צורך בתקצוב נוסף של לפחות 20 מיליון ש"ח. כתוצאה מכך, נכון לשנת 2024, 14 פרויקטים - ובהם שדרוג מערכת מרכב"ה, המערכת הקונסולרית, ותהליכי מעבר לענן - הוקפאו או עוכבו בשל היעדר תקציב. כמו כן היו פערים בתחזוקת מערכות קיימות ועיכובים בשדרוג תשתיות חיוניות.

ועדות היגוי לפרויקטים - בניגוד להנחיות מערך הדיגיטל ולפיהן יש להקים ועדות היגוי לכל פרויקט פיתוח מערכת מידע המוגדר מורכב או שבגודל בינוני ומעלה, משרד החוץ לא מינה ועדות היגוי לארבעה מתוך שישה פרויקטים משמעותיים שנבדקו. בהיעדר ועדת היגוי לפרויקט, לא יכול להתבצע הליך סדור ומיטבי של פיקוח והנחיה, אישור אבני דרך, ניתוח וניהול סיכונים, בקרה שוטפת של ביצוע מול תכנון וקביעת דרכי הפעולה להתמודדות עם אתגרים שעולים. זאת ועוד, עלה כי היות שהצוותים עובדים על כמה פרויקטים במקביל, אין למשרד החוץ דרך לגזור עלויות לפרויקט מסוים. בהיעדר תשתית מידע מלאה ומפורטת בנוגע לתקציב הפרויקט ויכולת לגזור את עלויותיו, לא ניתן לפקח על הפרויקט ועל ההחלטות המתקבלות במסגרתו בצורה מיטבית.

ניהול סיכונים בפרויקטים - בניגוד לנדרש בהנחיות מערך הדיגיטל ולפיהן ניהול סיכונים הוא מרכיב הכרחי בניהול הפרויקט בשלביו השונים, משרד החוץ אינו מקיים תהליכים של ניהול סיכונים בפרויקטים לכל אורך מחזור חיי הפרויקט. זאת, אף על פי שמדובר בפרויקטים משמעותיים, שמטבעם בעלי סיכונים טכנולוגיים, פיננסיים ותפעוליים למשרד החוץ. בהיעדר ניהול סיכונים, גדל הסיכון לאי-עמידה בלוחות הזמנים שהוגדרו לפרויקט, לחריגה בתקציב, לפגיעה באיכות תוצרים, לכישלון פרויקטים ולפגיעה במתן שירות לציבור ובתפקוד יחידות שונות במשרד החוץ.

פיתוח מערכת מידע מסוימת - המערכת נועדה להחליף מערכת מסוימת במשרד החוץ ולהביא לשיפור השירות הקונסולרי. עלה כי: אף שהפרויקט תוכנן מלכתחילה להסתיים בשנת 2019, הרי שלפי לוחות הזמנים המעודכנים הפרויקט עתיד להסתיים לכל המוקדם בשנת 2028, כעשר שנים לאחר המועד המקורי שתוכנן; בנוסף, מדובר בפרויקט שניהולו לקה באופן יסודי בהיבטי המעקב והבקרה התקציביים. משרד החוץ לא העריך לאורך השנים את עלויות הפרויקט ולא אמד את עלויותיו עד כה - עלות בפועל מול התכנון ואיתור חריגות תקציביות; נוכח העיכוב הניכר שחל בפיתוח הפרויקט נדרש להקצות כוח אדם נוסף, דהיינו להשקיע תקציב נוסף שהוערך על-ידי ועדת ההיגוי של הפרויקט בכ-12 - 18 מיליוני ש"ח, כדי להביאו לידי גמר; זאת ועוד, נכון ליולי 2024, חמש שנים מהמועד המקורי לסיום הפרויקט, בוצעה רק כמחצית התכולה הנדרשת ברמת הפיתוח (53%), ואף זאת לאחר שהוחלט על צמצום התכולות שתוכננו מלכתחילה.



תוכנית התאוששות מאסון - נכון לספטמבר 2024 ישנם פערים ביכולתו של משרד החוץ להתאושש מאסון. בכלל זה: אין למשרד תוכנית DRP[2] מעודכנת, סדורה ותקפה להתאוששות מאסון; נמצאו ליקויים ביכולת ההתאוששות של אתר ה-DR; המשרד לא תרגל באתר ה-DR תהליך של העלאת מערכות מידע משחזור, ולא בחן את הישימות הטכנית של התהליך, את מוכנות כוח האדם לבצע את התהליך ואת לוחות הזמנים שיידרשו למימושו. יוצא אפוא שבפועל משרד החוץ נעדר את ההיערכות ואת היכולת הנחוצות על מנת להתאושש מאסון.

אבטחת המידע והגנת הסייבר במשרד החוץ

מדיניות הגנת הסייבר ואבטחת המידע במשרד החוץ ועדכונה - נכון לינואר 2025, ועדת ההיגוי להגנת הסייבר ומנכ"ל המשרד לא עדכנו ולא תיקפו את מסמך מדיניות הגנת הסייבר, אף שחלפו כשבע שנים ממועד אישורו על ידם בשנת 2018. זאת בניגוד להנחיות הגורמים המנחים שלפיהן יש לאשרר את המדיניות מדי שנתיים עד שלוש שנים, ואף על פי שבשנים 2018 - 2024 חלו שינויים מהותיים במפת האיומים ובמבנה הארגוני של מערך התקשוב של משרד החוץ, ובכלל זה באיום הייחוס של המשרד ובפרט לאור העלייה באיומי הסייבר במהלך מלחמת "חרבות ברזל". בהיעדר מדיניות הגנת סייבר מקיפה ועדכנית גוברת החשיפה של משרד החוץ לתקיפות סייבר ולדליפת מידע רגיש, וכן גובר הסיכון הכרוך בכך.

פעילות ועדת ההיגוי להגנת הסייבר - ועדת ההיגוי להגנת הסייבר בראשות סמנכ"לי תיאום ותכנון מדיני במשרד החוץ אמורה לשמש מסגרת ארגונית ניהולית לקבלת החלטות בתחום הגנת הסייבר ולמעקב אחר יישומן. עלה כי ועדת ההיגוי במשרד החוץ לא עקבה בשנים 2018 - 2024 באופן שיטתי ורציף אחר יישום החלטות שקיבלה בנוגע לנושאים מהותיים, כגון - מדיניות לסיווג מידע רגיש (שאינו מסווג מהבחינה הביטחונית), שימוש העובדים ביישום מסוים והגנת הפרטיות. היעדר מעקב אחר יישום החלטות שנועדו לקדם טיפול בסוגיות אבטחת מידע חושף את המשרד לסיכונים ופוגע ביכולת לשפר את רמת ההגנה על המשרד ונכסיו.

ביצוע סקרי סיכונים ומבדקי חדירה - נמצא כי משרד החוץ פעל במהלך השנים 2017 - 2024 לביצוע סקרי סיכונים (הן סקרים כוללים והן סקרים ייעודיים) ומבדקי חדירה. עם זאת, סקרי הסיכונים ומבדקי החדירה היו חסרים, או שלא נגעו לכלל נכסי המידע והתהליכים הקריטיים במשרד. כך לדוגמה, בשנים 2017 ו-2019 ביצע המשרד סקרי סיכונים רק על חלק מרשתות המשרד ובחלק מיחידות המשרד.

---

[2] Disaster Recovery Plan.

התעדכנות באירועי סייבר חריגים במשרד - לפי הנחיות יה"ב, אחד מתפקידי ועדת ההיגוי הוא להתעדכן באירועי סייבר חריגים שאירעו במשרד, לקיים הערכת נזקים בעקבות תקלות ולגבש המלצות לטיפול. נמצא כי בשנים 2020 - 2024 אירעו אירועי סייבר חריגים, אולם רק בספטמבר 2024 הובא דיווח תמציתי לוועדת ההיגוי על התרחשותם, ודיווח זה נגע רק לחלק מהאירועים. העברת מידע על חלק מאירועי הסייבר, באיחור ניכר לאחר מועד התרחשותם, אינה מאפשרת לחברי הוועדה להעריך במועד את הנזק שנגרם לרמת הגנת הסייבר המשרד ולגבש המלצות לצורך תיקון הפערים שהועלו.

הגנה על המידע ברשתות המחשוב במשרד החוץ - נמצאו ליקויים חמורים המשקפים תרבות ארגונית לקויה במשרד החוץ בכל הנוגע לשמירה על מידע רגיש ופרטי. ליקויים אלה מעלים את הסיכון לדלף מידע, דבר שיכול אף להביא לחשיפה של זהותם של עובדי המשרד. להלן פירוט הליקויים: היעדר נוהל המסדיר את סיווג נכסי המידע ואת מעטפת ההגנה הנדרשת בהתאם לסיווגם של הנכסים; ניתנה גישה לכונן שהיה פתוח לכלל משתמשי רשת מסוימת ושהכיל עשרות אלפי מסמכים, חלקם כוללים מידע רגיש, כגון מידע אישי-פרטי.

מסמכים הכוללים מידע אישי שהיו נגישים לכלל משתמשי רשת מסוימת במשרד

עמידה ברמת ההגנה הנדרשת ברשתות מסוימות - נמצא כי רמת ההגנה על המידע ברשתות מסוימות נמוכה מרמת ההגנה הנדרשת ואינה עומדת בדרישות הגורם המנחה.

עדכניות תשתיות ומערכות המידע במשרד החוץ - נמצאו פערים בעדכניות תשתיות ומערכות המידע.

הגנה על רשת מסוימת במשרד החוץ - עלו פערים בנוגע להגנה על רשת מסוימת במשרד החוץ.

הזדהות משתמשים - נמצאו ליקויים בהזדהות משתמשים לרשתות המחשב במשרד החוץ.

ניהול הרשאות - נמצאו פערים בכל הנוגע לניהול הרשאות הגישה למערכות המידע במשרד החוץ.

הגנה על מאגרי מידע לפי חוק הגנת הפרטיות - הנהלת משרד החוץ מחויבת להגן על מאגרי מידע הכוללים מידע פרטי בהתאם להוראות הדין, לרבות תקנות הגנת הפרטיות, כדי למזער את הסיכון לפגיעה בזכות לפרטיות. עלה כי משרד החוץ אינו מיישם באופן מלא את דרישות חוק הגנת הפרטיות ותקנותיו, ובכלל זה לא ביצע מיפוי מלא של המאגרים שברשותו; לא קבע את רמת האבטחה הנדרשת בעניינם ולא נקט פעולות הנדרשות לפי החוק והתקנות כדי להגן עליהם באופן מספק; בפנקס מאגרי המידע במשרד המשפטים רשומים רק שלושה מאגרי מידע של משרד החוץ, אף שהמשרד מנהל עשרות מאגרים נוספים. אי-עמידה בחוק ובתקנותיו עלולה להביא לפגיעה בפרטיותם של עובדי המשרד ושל אזרחים המקבלים שירותים ממנו. נוסף על כך, היא חושפת את המשרד לסיכוני אבטחת מידע.

מבדק חוסן שבוצע על ידי משרד מבקר המדינה באחת הרשתות במשרד החוץ - המבדק העלה 15 ממצאים בתחומים שונים וברמות סיכון שונות: רמה גבוהה ביותר, רמה גבוהה, רמה בינונית ורמה נמוכה.

תוכנית אסטרטגיה דיגיטלית - משרד מבקר המדינה מציין לחיוב את יוזמת המשרד לגיבוש הצעה לתוכנית אסטרטגית בתחום התקשוב בשנים 2023 - 2024. לנוכח הפערים הניכרים שהתוכנית הציפה בנוגע לפעילות התקשובית במשרד החוץ ובהם פערים הנוגעים למבנה הארגוני, להיקף כוח האדם המוקצה לתחום התקשוב, לתהליכי העבודה, לתשתיות הטכנולוגיות ולתקציב התקשוב, על מנכ"ל משרד החוץ להידרש לנושא בהקדם, לכנס את ועדת ההיגוי המשרדית לשם דיון בתוכנית האסטרטגית ובהשלכותיה, ולקדם את קבלת ההחלטות הנדרשות לטיפול ולצמצום הפערים שהועלו, כמו גם לקביעת לוחות זמנים ותקציב נדרש לטובת הנושא.

בקרה על ניהול הרשאות - יצוין לחיוב כי בשנת 2024 אגף התקשוב השווה מדי חודש בין מידע שקיבל מאגף הון אנושי במשרד בנוגע לעובדים שסיימו את העסקתם לבין משתמשים פעילים בכל אחד מהדומיינים במשרד. כמו כן האגף ביצע את הבקרות בנוגע למשתמשים שסיסמתם חלשה וניתנת לפיצוח בזמן קצר.

עיקרי המלצות הביקורת

על מנכ"ל משרד החוץ לוודא כי ועדת ההיגוי לתקשוב תתכנס באופן סדיר, בתדירות של פעמיים עד ארבע פעמים בשנה, ותמלא את כל תפקידיה כמוגדר בהנחיות מערך הדיגיטל, ובכלל זה אישור תוכנית העבודה ומעקב אחר יישומה. כמו כן עליו למנות לחברי הוועדה סמנכ"לים מקצועיים במשרד, שכן הם מושפעים בעבודתם השוטפת מתפקוד אגף התקשוב וממערכות המידע של הארגון ומביאים עימם תובנות בנוגע לצורכי היחידות.

תקציב מאפשר הוא תנאי הכרחי למימוש אפקטיבי של ממשל טכנולוגיות מידע, שכן ללא תקצוב מספק, הארגון חשוף לסיכוני תפעול ואבטחה רבים. לנוכח הקשיים המשמעותיים שהוצפו בעניין זה, נדרש כי מנכ"ל משרד החוץ יבצע בחינה מעמיקה בנוגע לתקצוב תחום התקשוב, במטרה להבטיח כי במציאות של מחסור יסודי במשאבים התקציב מנוצל בהלימה לסדרי העדיפויות המשרדיים. כמו כן עליו לוודא כי המחסור בתקציב לא יוצר סיכונים עכשוויים או עתידיים שהמשרד אינו יכול לקבל (למשל בתחום אבטחת מידע, ביצוע משימות ליבה או היערכות עתידית לעבודה בענן).

- על משרד החוץ לפתח מדיניות מקיפה ומפורטת לניהול סיכוני התקשוב בפרויקטים, תוך שימוש במתודולוגיה סדורה ובהלימה עם הנחיות מערך הדיגיטל. במסגרת זו יש להקים מנגנון זיהוי והערכה של סיכונים בכל שלבי הפרויקט, לתעד את הסיכונים ולגבש תוכנית פעולה מותאמת להתמודדות עם כל סיכון. עוד מומלץ להכשיר את מנהלי הפרויקטים בתחום זה ולהקצות משאבים לצורך פיתוח כלים וטכנולוגיות שיסייעו בניהול סיכונים מיטבי.

- על ועדת ההיגוי הייעודית של פרויקט מסוים וועדת ההיגוי המשרדית לתחום התקשוב לבחון לעומקם את הליכי ההערכה והתכנון בפרויקט ולנהל מעקב הדוק אחר התקדמות אבני הדרך שלו בכל שלב ושלב. זאת כדי למנוע עיכובים נוספים ביישומו של הפרויקט וכדי להבטיח כי המשך היישום בשנים הבאות ייעשה בהתאם לתוכניות ולתכולות שאושרו. כמן כן, על הוועדות האמורות לתת את הדעת להיעדר היכולת לאמוד את עלויות הפרויקט. יוער כי בהיעדר תשתית מידע מלאה ומפורטת בנוגע לתקציב הפרויקט ויכולת לגזור את עלויותיו, לא ניתן לפקח על הפרויקט ועל ההחלטות המתקבלות במסגרתו בצורה מיטבית.

- כדי להבטיח את הרציפות התפקודית של משרד החוץ, על משרד החוץ לבחון אילו צעדים עליו לנקוט כדי להבטיח את התאוששות מערכות מידע מסוימות באתר ה-DR בהתאם למדדי ההתאוששות שאישרה הנהלת המשרד בספטמבר 2024 - וליישמם. במקביל, עליו לגבש באופן מיידי תוכנית DRP, שתיתן מענה לכלל רשתות המשרד, ולוודא כי באתר ה-DR קיים עותק מעודכן עם המידע הנדרש לשם שחזור מערכות מידע מסוימות והקמתן באתר זה.

- על מנכ"ל משרד החוץ לקיים בחינה מעמיקה ויסודית, בשיתוף עם ועדת ההיגוי המשרדית לתקשוב, בנוגע לפערים בתהליכי ניהול ופיתוח של מערכות מידע, כמו גם בנוגע לממצאים שהועלו בתוכנית האסטרטגית ובסקר הסיכונים, תוך ניתוח השלכותיהם על פעילות המשרד. בחינה זו תסייע בזיהוי בעיות השורש ותאפשר קבלת החלטות מושכלת תוך תיעדוף משימות, וגיבוש תוכנית פעולה ברורה הכוללת צעדים אופרטיביים, לוחות זמנים וגורמים אחראים לביצוע. זאת ועוד, דבר זה יסייע גם להבטיח כי תחום התקשוב במשרד החוץ יטופל באופן יסודי ומקיף תוך מתן התמיכה הנדרשת ליחידות המשרד בביצוע תפקידיהן ובהשגת יעדיהן בתחומי הפעולה השונים בזירה הבין-לאומית ובתחומים הקונסולריים.

- על מנכ"ל המשרד לוודא כי מדיניות הגנת הסייבר תתוקף כנדרש באופן עתי על ידי ועדת ההיגוי להגנת הסייבר ובכלל זה לנוכח האיומים שנוספו במהלך מלחמת "חרבות ברזל".

- על משרד החוץ, בשיתוף הגורמים המנחים יה"ב והשב"כ, לבצע סקר סיכונים הכולל את כלל נכסי המידע והתהליכים הקריטיים, ובהתאם לכך ליצור מפת סיכונים משרדית שתאושר על ידי ועדת ההיגוי להגנת הסייבר. כמו כן, על המשרד לגבש תוכנית להפחתת הסיכונים שהועלו, שתאושר גם היא על ידי ועדת ההיגוי במשרד.

- על מנכ"ל משרד החוץ לוודא כי גורמי המקצוע במשרד יעבירו דיווח מפורט על אירועי סייבר חריגים לוועדת ההיגוי בכינוס הוועדה בסמוך למועד התרחשותם, כך שלפני חברי הוועדה תוצג תמונת המצב המלאה בנושא, מהלך שיאפשר להם לקדם את רמת ההגנה בסייבר במשרד.

- המשרד נדרש להשלים את גיבוש הנוהל הנוגע לסיווג נכסי המידע ולהגביל את הגישה למסמכים רק לעובדים שהמידע דרוש להם לצורך עבודתם.

- על מנכ"ל משרד החוץ להבטיח כי ייעשו הפעולות הדרושות להשגת רמת ההגנה הנדרשת ברשתות מסוימות בהקדם, כמתחייב מרמת איום הייחוס שהוגדרה ושעל המשרד לעמוד בה. כמו כן, על הגורם המנחה להמשיך ולעקוב אחר יישום הנחיותיו במסגרת בחינת עמידת המשרד ברמת הגנה הנדרשת.

- על מנהל אגף התקשוב לשקף להנהלת המשרד ולוועדת ההיגוי להגנת הסייבר את הפער הקיים בנושא מסוים על פי הנחיות הגורמים המנחים, את הסיכונים הכרוכים בפער זה ולגבש תוכנית סדורה להשלמת הפער תוך גיבוש משאבים תקציביים. על מנכ"ל משרד החוץ לפעול להשלמת פער זה. על הגורמים המנחים לבצע בקרה כדי לוודא כי הפער הקיים בנושא זה מטופל כנדרש.
- על מנכ"ל משרד החוץ, בשיתוף הגורמים הרלוונטיים במשרד ובהם אגף התקשוב, הלשכה המשפטית וחטיבת בטמ"ח, לוודא עמידת המשרד בדרישות חוק הגנת הפרטיות ותקנותיו באופן מקיף, סדור ושיטתי ולהקצות לכך משאבים מתאימים, כך שהמידע הפרטי של העובדים והאזרחים שנשמר במאגרי המידע של המשרד יהיה מוגן כנדרש.
- נוכח היקף הממצאים שעלו במבדק החוסן שבוצע על משרד החוץ לקיים הערכת מצב ולבנות תוכנית אופרטיבית לתיקון הליקויים שפורטו בדוח הטכני המפורט שנמסר למשרד החוץ.

הפערים המרכזיים בתהליכי הניהול והפיתוח של מערכות המידע

הפערים המרכזיים באבטחת המידע והגנת הסייבר

סיכום

משרד החוץ אמון על גיבוש מדיניות החוץ של מדינת ישראל, ביצועה והסברתה, ומתוקף תפקידו הוא מחזיק במידע רגיש. המערכות הממוחשבות של משרד החוץ חיוניות לפעילותו התקינה ולמימוש יעדיו, ופגיעה בהן או במידע המצוי בהן עלולה לגרום לפגיעה בתפקוד המשרד בכללותו ובשירות שהוא נותן לציבור, ולפגיעה ביחסי החוץ של המדינה ותדמיתה בעולם. נוכח תפקידו, משרד החוץ הוא יעד מרכזי לתקיפות סייבר של מגוון יריבים, החל מפצחנים וכלה בגורמים מדינתיים.

ממצאי דוח זה מלמדים על פערים בשני התחומים שנבדקו - הניהול והפיתוח של מערכות המידע במשרד החוץ ואבטחת המידע והגנת הסייבר במשרד.

תמונת המצב העולה מביקורת זו מלמדת על פער טכנולוגי מתמשך במערכות המחשוב של משרד החוץ של שנים רבות ועל תרבות ארגונית שאינה הולמת את איום הייחוס שהוגדר למשרד החוץ.

ממצאי ביקורת זו מדגישים את הצורך בחיזוק מנגנוני הפיקוח והבקרה של הנהלת משרד החוץ וועדת ההיגוי להגנת הסייבר בראשות מנכ"ל משרד החוץ בכל הנוגע למערכות המידע ואבטחת המידע במשרד.

על מנכ"ל משרד החוץ להידרש לממצאי דוח זה ולוודא כי הליקויים והפערים שהועלו בו יטופלו. בכלל זה, יש להכין תוכנית עבודה סדורה ומפורטת, לרבות לוחות זמנים, כדי לתעדף את הטיפול בכלל הפערים שהועלו ולצמצם את הסיכונים הקיימים. כל זאת, במטרה להבטיח פעילות תקינה של מערך התקשוב במשרד החוץ ולשפר את רמת ההגנה על המשרד ונכסיו.

זאת ועוד, על השב"כ ויה"ב להידרש אף הם לממצאי דוח זה ולעקוב אחר הטיפול בפערים שהועלו בו, כדי לשפר את רמת ההגנה על המידע במשרד החוץ ולהבטיח שרמת ההגנה תהיה בהלימה לאיום הייחוס של המשרד.

ואולם בסופו של דבר התובנות והלקחים העולים מדוח זה אינם מסתכמים בפעולת משרד החוץ והפיקוח על פעולתו. משרד מבקר המדינה ביצע בשנים האחרונות שורה של ביקורות בגופים ממשלתיים ובגופים ציבוריים רגישים בתחום התקשוב ובפרט בנושא אבטחת המידע והסייבר. ממצאים שעלו בדוחות אלו - ובאים לידי ביטוי ברור גם בדוח זה - מחייבים בחינה מעמיקה בקרב הרגולטורים המדינתיים - מערך הדיגיטל הלאומי, מערך הסייבר הלאומי, השב"כ והרשות להגנת הפרטיות - בנוגע לכמה סוגיות יסודיות וזאת בקשר לכלל משרדי הממשלה:

1. בחינת הצורך בהטמעה ממשית ועמוקה של הסיכונים הטמונים בתחום הסייבר ופוטנציאל הנזק העלול להיגרם בגינם לארגון ולמדינה בכלל וכי איום הסייבר הוא איום ביטחוני ואסטרטגי לאומי. הטמעה זו נדרשת להיעשות בראש ובראשונה בקרב כלל המנהלים הכלליים של משרדי הממשלה ומכך אף נגזרת הדרישה בנוגע למידת מעורבותם בנושא.
2. כנגזרת של תפיסת האיום, נדרשת בחינה בנוגע לחיזוק מנגנוני הפיקוח והרגולציה של הגורמים המנחים, ובפרט כאשר ישנם כמה גורמים המנחים את אותו הגוף. זאת, על מנת להבטיח את אפקטיביות פעילות הגורמים המנחים למול גופים ממשלתיים ומתן מענה לכלל הסיכונים בצורה הוליסטית.
3. בחינה מעמיקה של הפערים הקיימים במגזר הממשלתי בנוגע לתקצוב תחום התקשוב ובכלל זה תחום אבטחת המידע והגנת הסייבר, במטרה להבטיח כי במציאות של מחסור יסודי במשאבים, היקף התקציב ייתן מענה הן לדרישות המקצועיות ולהתפתחויות הטכנולוגיות והן לאיום הקיים. זאת במטרה להבטיח כי המחסור בתקציב לא יוצר סיכוני תקשוב או סיכוני אבטחת מידע, עכשוויים או עתידיים כמו גם נזקים הנובעים מאי-הטמעת טכנולוגיות חדשות.
4. מתן הדעת על כך שחלק מהפערים, דוגמת אלו הנוגעים להגנה על הפרטיות, נובעים מתרבות ארגונית לקויה וכי ניתן לתת להם מענה באמצעות טיפול וקשב מצד הנהלות הגופים ובאמצעות כלים, לרבות כלים טכנולוגיים, שאינם דורשים בהכרח הקצאת משאבים, כגון הדרכות ונקיטת פעולות להעלאת מודעות העובדים.

ביצוע בחינה מעמיקה כאמור תסייע במיקוד המאמצים וטיוב עבודת משרדי הממשלה בכל הנוגע לתחום התקשוב, אבטחת מידע והגנת הסייבר ובקידום רמת ההגנה באופן שיהלום את רמת האיום והשלכותיו, כמו גם לשיפור יעילות פעילות עבודת הממשלה ושיפור השירות לציבור.

coupled with close collaboration among all public entities. Ensuring adequate protection of information systems and digital services is not merely a technological requirement, but a necessary prerequisite for maintaining public trust, safeguarding citizens' privacy, and securing the proper and continuous functioning of public services.

The audited entities are responsible for acting expeditiously and effectively to rectify the deficiencies identified in this report.

I extend my gratitude to the personnel within the Office of the State Comptroller who prepared this report with professionalism, thoroughness, dedication, and a strong sense of mission. It is my hope that the report's findings and recommendations will contribute to the strengthening of cyber and information security systems within the public sector and enhance the quality of services delivered to the citizens of Israel.

We express our hopes and prayers for the swift recovery of the injured, the rehabilitation of the hostages who have returned to us and to their families, the safe return of all evacuees to their homes, the safety of our soldiers, and the success of the security forces in safeguarding our nation.

Matanyahu Englman
State Comptroller
and Ombudsman

Jerusalem,
May 2026

registration of approximately 4.6 million citizens within the national identification system, policy implementation remains partial and sluggish. Only 16% of mapped services are connected to the identification system; only approximately 23% of the identified online forms are managed through it; and merely 233 out of thousands of government services have been made accessible via the personal area. Furthermore, it was found that only 15 of 258 local authorities have connected to the national identification system, and the integration of government ministries and other public bodies with these systems is limited, thereby hindering the public's ability to receive comprehensive, straightforward, and accessible digital government services.

Another chapter addresses **the security of information systems within the Ministry of Construction and Housing**, which maintains millions of records containing personal and sensitive data about citizens, housing beneficiaries, and contractors. The Ministry utilizes numerous information systems, and in 2025, its information and cyber security budget amounted to approximately NIS 6.5 million, representing roughly 9% of its total computing budget. The audit identified significant shortcomings in the management of information and cyber security within the Ministry, including deficiencies in access authorization controls, inadequate application of risk management processes, absence of sufficient alert mechanisms, and incomplete registration of databases as mandated by law. These findings gain particular significance in light of the substantial increase (approximately 130%) in cyber alerts received by the Ministry in 2024, underscoring the critical importance of effective protection of the state's information assets.

The report further examines **cyber protection in remote work**, which has become integral to the operations of public and security bodies in recent years, particularly during the COVID-19 pandemic and the Swords of Iron War. The audit assessed the readiness of critical agencies, including the Israel Police and the National Fire and Rescue Authority, to manage the cyber threats associated with remote work. Findings exposed certain gaps in the adaptation of protection and control mechanisms with respect to extant risks. Moreover, a penetration test conducted by the Office of the State Comptroller on the Fire and Rescue Authority's remote work system revealed deficiencies. These outcomes highlight the necessity to finalize work plans and to enhance cyber protection preparedness within the nation's critical bodies.

Overall, the report findings indicate that Israel's advancement toward a sophisticated digital government mandates sustained investment in cyber infrastructure, risk management, oversight, and enforcement,

The four chapters of this report address distinct yet complementary dimensions within the domain of cyber and information systems in the public sector:

- **Information Systems and Information and Cyber Security at the Ministry of Foreign Affairs**
- **Cybersecurity in Remote Work during Routine Times and Emergencies**
- **Information System Security at the Ministry of Construction and Housing**
- **Online Public Services: The National Identification System and the Government Personal Area**

The first three chapters underwent a confidentiality process in the Knesset State Audit Committee sub-committee, which decided not to bring them in their entirety before the Knesset, but to publish only parts thereof, to protect the state's security.

The audit findings reveal deficiencies in preparedness, risk management, supervision, and the execution of government policy in this field, alongside only partial progress in enhancing digital service accessibility and in deploying advanced protection and control mechanisms. Although each report examines a specific subject area, their collective results demonstrate that strengthening the protection of information systems, ensuring operational continuity, and advancing the digital transformation of public service constitute national challenges necessitating systemic, coordinated, and sustained intervention.

The audit of **Information Systems and Information and Cyber Security at the Ministry of Foreign Affairs** was conducted during the Swords of Iron War and identified deficiencies in the management and development of the Ministry's information systems, as well as in the domains of information security and cyber protection. Given its role, the Ministry of Foreign Affairs represents a key target for cyber-attacks perpetrated by a range of adversaries, from hackers to state actors. The audit findings underscore the necessity of enhancing the supervisory and control mechanisms governing the Ministry of Foreign Affairs' management of information systems and information security, in order to ensure the proper functioning of its IT infrastructure and to augment the protective measures for the Ministry and its assets.

One chapter of the report addresses **the implementation of government policy for promoting digital public services through the national identification system and the government personal area**. The audit disclosed that despite numerous governmental resolutions since 2014 concerning the enhancement of online services, and notwithstanding the

Foreword

The State Comptroller's annual audit report on Cyber and Information Systems is hereby submitted to the Knesset in accordance with the provisions of the State Comptroller Law, 5718-1958 [Consolidated Version]. This report addresses key aspects of cyber protection, information security, and digital services within the public sector.

In recent years, the digital domain has emerged as a fundamental infrastructure underpinning the activities of the State of Israel. Information systems, online services, and digital work processes currently constitute the operational foundation for government ministries, emergency bodies, public authorities, and citizen service systems. While digital transformation offers numerous advantages – including the streamlining of public services, enhancement of accessibility, resource optimization, and reinforcement of functional continuity – it concomitantly engenders elevated risks associated with cyber threats, information breaches, and vulnerabilities in information system protection. This prevailing reality necessitates that all public entities ensure their systems are secure, reliable, accessible, and resilient in both routine times and during emergencies.

Cyber protection and information system security presently constitute the cornerstones of good governance in the contemporary state. Digital systems aggregate personal, financial, and security-related information on a massive scale and serve as essential infrastructure for government ministries, emergency bodies, and critical public services. In an era marked by escalating cyber threats, and particularly during emergencies and crises, the state must undertake advanced preparations to guarantee system integrity, safeguard citizens' privacy, and maintain uninterrupted, secure, and reliable public service delivery. Strengthening this domain is not only a technological requisite, but also a fundamental pillar of national security, public confidence in state institutions, and governmental capacity to deliver efficient, advanced, and accessible public services to all citizens.

The importance of enhancing the protection of information systems and digital infrastructures is especially pronounced given the complex security environment that the State of Israel has faced in recent years. During this period, hostile entities have increasingly attempted cyberattacks, while state bodies have been required to assure operational continuity and the provision of essential public services even under emergency conditions. These developments have demonstrated that information systems, digital services, and remote work infrastructures function not merely as administrative and technological instruments, but as integral components of national resilience and the state's ability to operate continuously, efficiently, and securely.

State of Israel

Report of the State Comptroller

Cyber and Information Systems

May 2026

Jerusalem