דוח מבקר המדינה

מערכות מידע ואבטחת מידע וסייבר במשרד החוץ

▪ סיוון התשפ"ו ▪ מאי 2026 ▪

מערכות מידע ואבטחת מידע וסייבר במשרד החוץ

מבוא

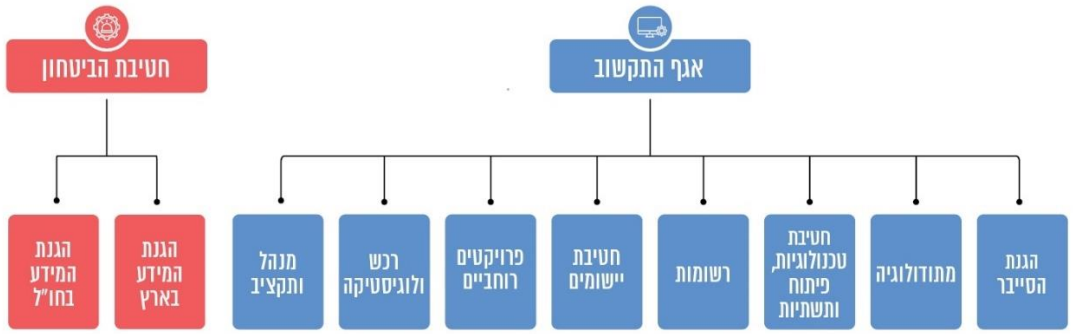
משרד החוץ (להלן גם - המשרד) אחראי לגיבוש מדיניות החוץ של ממשלת ישראל, ביצועה והסברתה. משרד החוץ מופקד, בין היתר, על ייצוג מדינת ישראל בחו"ל ועל ניהול קשרי ממשלת ישראל עם ממשלות זרות ועם ארגונים בין-לאומיים בארץ ובחו"ל. המשרד פועל לחיזוק מעמדה המדיני של ישראל וקשריה עם המדינות השונות, והוא אמון על מתן שירותים קונסולריים לאזרחי ישראל השוהים בחו"ל.

פעולות המשרד מתבצעות באמצעות המשרד הראשי בירושלים (להלן - המטה) ובאמצעות 109 הנציגויות הדיפלומטיות והקונסולריות בחו"ל[1]. פעילות המטה והנציגויות מוכוונת לקידום התמיכה ביעדים המדיניים וקידום האינטרסים של ישראל. המטה מנחה את הנציגויות בחו"ל במכלול נושאי מדיניות החוץ, מקיים עימן קשר שוטף, מקבל את דיווחיהן ומקיים את המגעים עם הנציגויות הזרות בישראל.

משרד החוץ מעסיק אלפי עובדים במגוון צורות העסקה במטה ובנציגויות: עובדים קבועים וזמניים במטה, עובדים ישראלים קבועים הנשלחים לנציגויות לאיוש תפקידי ליבה ותפקידי הניהול הבכירים (להלן - שליחים), וכן אזרחים ישראלים המועסקים בעבודת הנציגויות. (להלן - איתי"ן[2]). כמו כן בנציגויות פועלים עובדים מקומיים זרים הנושאים אזרחות זרה (להלן - עמי"ז).

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 (להלן - בטמ"ח). אגף התקשוב הוא הזרוע הטכנולוגית של המשרד, והוא אחראי לפיתוח מערכות המידע ומתן שירותי תחזוקה, תמיכה, אחסון וטיפול בחומרת מחשוב ותקשורת בכל רשתות המשרד וכן ליישום הגנת הסייבר במערכות המשרד. האגף מונה מאות עובדים. בטמ"ח אחראי לאבטחת המידע בכלל המשרד, לאבטחה הפיזית במטה, בנציגויות ובבתי השגרירים, למתן הנחיות לעובדי המשרד וקביעת כללי התנהגות בנוגע למידע מסווג ומידע רגיש (בלתי מסווג).

תרשים 1: **מבנה ארגוני של מערך התקשוב והגנת המידע במשרד החוץ**



על פי נתוני משרד החוץ, בעיבוד משרד מבקר המדינה.

משרד החוץ נדרש להתמודד עם אתגר מובנה וייחודי, שנגזר מהצורך לנהל מידע מדיני ודיפלומטי רגיש בין המטה לנציגויות: המידע המנוהל במערכות הוא מידע מגוון וכולל בין היתר מידע רגיש

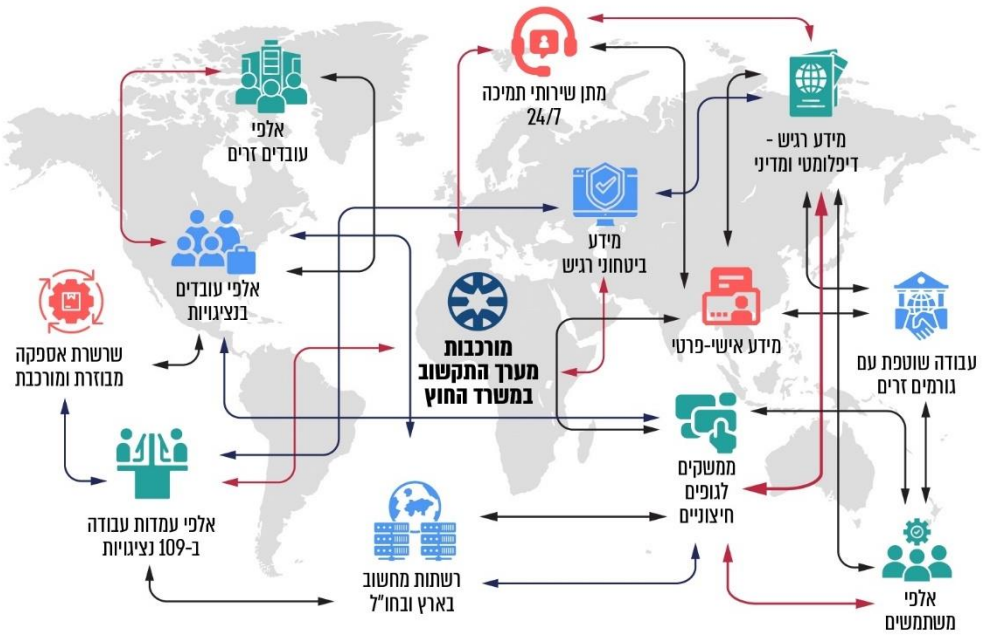
---

[1] נכון למועד הביקורת היו 109 נציגויות דיפלומטיות וקונסולריות בחו"ל, אך ל-7 מהן אין מבנה נציגות משלהן, למשל במקרה של שגריר לא תושב.

[2] איתי"ן - אזרח ישראלי תומך נציגות. עובדים אלה הם אזרחי ישראל המתגוררים במדינת השירות במעמד של תושב ארעי, בני זוג של שליחים או אזרחים ישראלים הגרים בישראל שנשלחים לאיוש משרות בנציגויות.

מהבחינה הדיפלומטית והמדינית וכן מידע פרטי; מערכות התקשוב כוללות רשתות תקשורת ומערכות מידע; פריסה גיאוגרפית נרחבת במטה וב-109 נציגויות ברחבי העולם; אלפי עמדות עבודה ממוחשבות; אלפי משתמשים במערכות המידע, חלקם עמ"זים; צורך במתן שירותי תמיכה בכל העולם לאורך כל שעות היממה; וממשקי עבודה מול גורמי-חוץ רבים בארץ ובעולם. כמו כן, מדובר במשרד שהוא במהותו יעד אסטרטגי להתקפות סייבר - החל מפצחנים (האקרים) יחידים, דרך ארגוני טרור ופשיעה מקוונת וכלה במדינות עוינות - והפריסה הגיאוגרפית הרחבה והעסקת העמ"זים מעצימות את מרחב החשיפה.

תרשים 2: **מערך התקשוב במשרד החוץ - מאפיינים ייחודיים**



על פי נתוני משרד החוץ, בעיבוד משרד מבקר המדינה.

תקציב משרד החוץ לשנת 2024 עמד על כ-1.9 מיליארד ש"ח. התקציב שהוקצה לתחום התקשוב בשנת 2024 עמד על 85.3 מיליון ש"ח, ומתוכו התקציב שהוקצה לתחום הסייבר עמד בשנה זו על כ-13 מיליון ש"ח (כ-15% מתקציב התקשוב).

מערך הדיגיטל הלאומי מנחה מתוקף סמכויותיו[3] את אגף התקשוב במשרד החוץ בכל הנוגע לפעילויות ולתהליכי העבודה העיקריים שלו, ובכלל זה בנוגע להקמה של ועדות היגוי משרדיות לתחום התקשוב ואופן פעילותן; ניהול פרויקטים ופיתוח מערכות מידע; ניהול סיכוני תקשוב; מיקור-חוץ; הכנת תוכניות עבודה; תשתיות, חומרה ותקשורת; מחשוב ענן; ניהול ושיתוף ידע והנגשת מאגרים.

בכל הנוגע להגנה על המידע ברשת הבלמ"ס, משרד החוץ מונחה על ידי יחידת ההגנה בסייבר במערך הדיגיטל הלאומי (להלן - יה"ב), והוא פועל בהתאם להנחיותיה (להלן - הנחיות יה"ב)[4]. בעבר, בשנים 2018 - 2023, הונחה המשרד על ידי מערך הסייבר הלאומי (להלן - מס"ל)[5]; ושירות הביטחון הכללי (להלן - השב"כ)[6] מנחה אותו בכל הנוגע לרשתות מסוימות במשרד (להלן ביחד - הגורמים המנחים).

---

3 החלטת הממשלה 3058 (27.3.11); החלטת הממשלה 2097 (10.10.14); החלטת הממשלה 260 (26.7.20).

4 מכוח החלטת הממשלה 2443 (15.2.15).

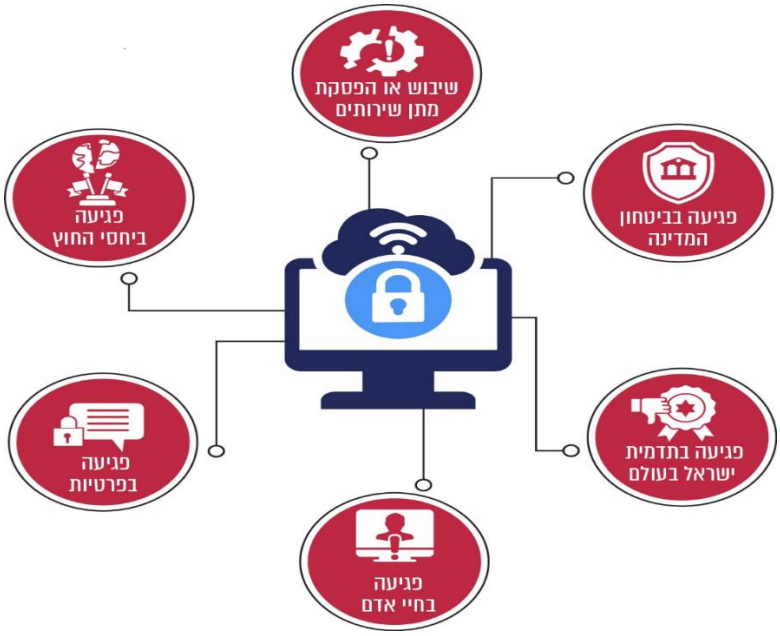
5 מס"ל פרסם מדריך יישומי להגנת הסייבר בארגון, "תורת ההגנה בסייבר 2.0" (להלן - תורת ההגנה).

6 מכוח החוק להסדרת הביטחון בגופים ציבוריים, התשנ"ח-1998.

פגיעה במערכות המידע של משרד החוץ עלולה לגרום לשיבוש מתן השירות ללקוחות המשרד או אף להפסקתו ולפגיעה בתפקוד המשרד בכללותו. מערכות אלו כוללות כאמור מידע רב, לרבות מידע רגיש. פגיעה במידע זה - לרבות דליפת המידע, שיבושו או פגיעה בזמינותו - עלולה לגרום לנזק חמור לביטחון מדינת ישראל ויחסי החוץ שלה, לפגיעה בתדמית ישראל בעולם, כמו גם לפגיעה בפרטיות.

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.

תרשים 3: **נזקים פוטנציאליים של התממשות סיכונים בתחום אבטחת המידע במשרד החוץ**



יצוין כי בשנת 2024 היו ניסיונות דיוג (phishing) כנגד עובדי המשרד; ובשנת 2023 היו תקיפות באמצעות דוא"ל חריג וכן מקרים של חשד לפריצה לדוא"ל או למחשב או לטלפון נייד של עובדי המשרד. במהלך מלחמת "חרבות ברזל" אירעו תקיפות רבות במרחב הסייבר כנגד המשרד ובכלל זה אתרים של המשרד, מערכות טכנולוגיות ועוד, זאת בין היתר כדי להגיע באמצעות מרחב הסייבר לידי תקיפה של עובדי המשרד. כמו כן, במהלך מלחמת "חרבות ברזל" חל גידול של כ-500% באירועי הגנת מידע בנציגויות ישראל בחו"ל ואירעו מאות אירועים בשנת 2023.

<u>פעולות הביקורת</u>

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, התשמ"א-1981 (להלן - חוק הגנת הפרטיות).

כמו כן, במהלך חודש מרץ 2025 בוצע מבדק חוסן הכולל סקר הערכת פגיעויות ומבדק חדירה באחת מרשתות המשרד.

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 חלקים ממנו, לשם שמירה על ביטחון המדינה, בהתאם לסעיף 17 לחוק מבקר המדינה, התשי"ח-1958 [נוסח משולב].

ניהול ופיתוח של מערכות המידע במשרד החוץ

המערכות הממוחשבות במשרד החוץ הן כאמור התשתית התפעולית של המשרד, והן חיוניות לפעולתו התקינה של המשרד ולמימוש יעדיו. המשרד פרוס על פני 109 נציגויות בעולם, ובמטה המשרד ובנציגויות פרוסות רשתות בסיווגים שונים ואליהן מחוברים אלפי עמדות עבודה וציוד היקפי.

בתוכנית העבודה של אגף התקשוב לשנת 2024 הגדיר האגף כמה יעדים מרכזיים לפעילותו, ובהם שדרוג יכולות שליטה ובקרה עולמית למערכות המשרד; אפיון ופיתוח מערכות ליבה חדשות; הנגשת מערכות ויישומים לעבודה מרחוק; הקמת תשתית ניהול תוכן; שדרוג תשתיות התקשוב בארץ ובנציגויות; הנגשת מערכות טכנולוגיות בסביבות מסוימות; מימוש אחריות המשרד להגנה ממתקפות סייבר והיערכות למעבר לעבודה בסביבת הענן.

נכון לשנת 2024, אגף התקשוב מתחזק עשרות מערכות מידע, ובהן מערכת למתן שירותים קונסולריים לאזרחים וזרים בנציגויות, מערכת לניהול ובקרה של שילוח דואר דיפלומטי, מערכת לניהול המידע הארגוני, מערכת לניהול השליחים ומערכות לניהול פיננסי. חלק מהמערכות מיושנות ודורשות שדרוג או החלפה, אחרות מצויות בתהליכי פיתוח או שדרוג (ראו הרחבה להלן).

נוסף על כך, האגף מוביל נכון לשנת 2024 עשרות פרויקטי תקשוב ובהם מערכת לזימון וניהול תורים; איחוד דומיינים; העברת הנציגויות לענן ועוד.

פיתוח ותחזוקה של מערכות המידע מבוצעים ברובם בחטיבת היישומים שבאגף. החטיבה מונה עשרות אנשי פיתוח בתפקידים שונים, ובהם מנהלי פרויקטים, מנתחי מערכות ומתכנתים המאורגנים בצוותים, שנמצאים בכפיפות ישירה לראש חטיבת היישומים.

בהחלטת הממשלה משנת 2014[7] נקבעו תפקידי מערך הדיגיטל הלאומי[8], ובהם קביעת סטנדרטים בתחומי טכנולוגיות מידע, גיבוש מתודולוגיה לניהול מחזור החיים של מערכות מידע ולניהול יעיל של פרויקטים ותהליכים בתחום התקשוב[9]. עוד נקבע בהחלטה כי לשם כך יפרסם מערך הדיגיטל הנחיות מקצועיות מחייבות למשרדי הממשלה[10] (להלן - הנחיות מערך הדיגיטל או ההנחיות). בהנחיות נקבע[11] כי בפעילות שאינה מטופלת על ידי ההנחיות והמתודולוגיה הממשלתית חובה לפעול בהתאם למתודולוגיה מקובלת[12]. עוד נקבע בהנחיות כי על היחידות להגדיר בכתב וליישם נוהלי עבודה, הנחיות והוראות תפעול ותבניות עבור הפעילויות ותהליכי העבודה העיקריים שלהן.

---

7 החלטת ממשלה 2097 "הרחבת תחומי פעילות התקשוב הממשלתי, עידוד חדשנות במגזר הציבורי וקידום המיזם הלאומי "ישראל דיגיטלית"". (10.10.14).

8 החלטת הממשלה 135 (19.7.21).

9 ראו סעיפים 3 (ב) ו-3 (ג) בהחלטת הממשלה 2097.

10 ראו סעיף 5 (א) בהחלטת הממשלה 2097.

11 ראו סעיפים 9.3, 9.4 בהנחיה 1.1.01, "מסגרת מתודולוגיית תקשוב ממשלתית".

12 מתודולוגיה מקובלת - לפי סעיף 5.1 בהנחיה, מתודולוגיה סדורה - מתודולוגיה ממשלתית או מתודולוגיה מוכרת (כגון מפת"ח, CMMI, Scrum, PMI, ITIL, COBIT, TOC), או מתודולוגיה שפותחה על ידי המשרד וכוללת פתרונות להיבטים הניהוליים, הכלכליים והטכנולוגיים, להיבטי הלקוחות של מערכות המידע והטכנולוגיות הדיגיטליות ושל יחידות התקשוב.

נוסף על הנחיות מערך הדיגיטל, הוציא אגף התקשוב במשרד החוץ סט נהלים פנימיים המתייחס לתהליכי ניהול פרויקטים ופיתוח מערכות מידע.

משרד מבקר המדינה בחן כמה היבטים בניהול ופיתוח מערכות המידע במשרד החוץ - ממשל טכנולוגיות המידע במשרד; ניהול פרויקטים ופיתוח מערכות מידע; וקיום תוכנית התאוששות מאסון.

ממשל טכנולוגיות מידע

ממשל טכנולוגיות מידע הוא מסגרת של תהליכים, מדיניות, כלים ובקרות, ומטרתו להבטיח כי טכנולוגיות המידע בארגון תומכות באופן מיטבי באסטרטגיה של הארגון, במטרות העסקיות שלו ובערכים שלו. זהו תחום המשלב ניהול, מדיניות, טכנולוגיה ותפעול כדי למקסם את התועלת מטכנולוגיות מידע תוך כדי ניהול סיכונים וציות לדרישות חוק ורגולציה.

ההכרה בחשיבותם של תהליכי משילות מוסדרים בתחומי התקשוב הלכה וגברה ככל שהניסיון מתהליכי ניהול מערכות מידע, יחידות תקשוב ופרויקטים הלך והעמיק. חשיבות זו גם מקבלת ביטוי בפרקטיקות המקובלות לניהול מערכות מידע ובהן COBIT[13], ISO[14], PMI[15], ITIL[16].

<u>הקמת ועדת היגוי משרדית לתחום התקשוב ופעילותה</u>

בשנת 2014 קיבלה הממשלה החלטה (להלן - החלטת הממשלה 2097)[17], שבמסגרתה הונחו מנכ"לי משרדי הממשלה ויחידות הסמך לבחון הקמת ועדת היגוי משרדית לתחום התקשוב, אשר תפעל לרתימת מערכות המידע וטכנולוגיות מתקדמות לשם השגת יעדי המשרד ושיפור תהליכי הליבה העסקיים בו, תוך דיון בתוכנית העבודה של אגף מערכות המידע ועריכת מעקב שוטף אחר ביצועה. עוד נקבע בהחלטה כי סדרי עבודת הוועדות ייקבעו בהנחיות הממונה על התקשוב הממשלתי.

בהתאם, פרסם מערך הדיגיטל הנחיה שעניינה "ועדות היגוי משרדיות לתקשוב". בהנחיה מפורטים תפקידי הוועדה, ובכלל זה צוין כי ועדת ההיגוי המשרדית תשמש הגורם הניהולי הבכיר ביותר, שתפקידו וסמכותו לאשר סוגיות מרכזיות בנושאי התקשוב ולהכריע בהן, הן בנושאים שיובאו בפניה והן בנושאים שתבחר לדון בהם; הוועדה תקבע את האסטרטגיה של המשרד ומדיניותו בנושאי תקשוב בכפוף למדיניות כלל-ממשלתית; תאשר את יעדי אגף מערכות המידע ותוודא את התאמתן למטרות המשרד ויעדיו; תאשר את תוכניות העבודה והתקציבים הרב-שנתיים והשנתיים של כלל הפעילויות המתקיימות במשרד בתחומים של מערכות מידע ותקשוב; תקבע ותאשרר סדרי עדיפות וחלוקת משאבים; תעקוב אחר ביצוע התוכניות ותוודא מימושן; ותאשר שינויים מהותיים בתקציב ותוכניות העבודה במהלך השנה. לפי ההנחיה, בראש הוועדה יעמוד מנכ"ל המשרד או המשנה למנכ"ל, ובין חבריה יהיו הסמנכ"לים - הצרכנים העיקריים של שירותי התקשוב במשרד, מנהל מערכות המידע של המשרד וממונה הגנת הסייבר במשרד או נציגו.

עוד נקבע בהנחיה כי מומלץ שתדירות מפגשי הוועדה תהיה לא פחות מאחת למחצית ולא יותר מאחת לרבעון, תלוי בהיקף הפעילות ובמנגנוני הבקרה האחרים הפועלים במשרד (ועדות היגוי לפרויקטים עיקריים וכדומה).

---

13 COBIT 2019 היא מסגרת עבודה לממשל (Governance) וניהול של המידע והטכנולוגיה בארגונים, שפותחה ומתוחזקת על ידי ISACA. מסגרת עבודה זו מספקת עקרונות, נהגים, כלים ומודלים מקובלים, שנועדו לסייע לארגונים למקסם את הערך המתקבל מטכנולוגית המידע בארגונים.

14 ISO/IEC 38500:2024 - Information technology - Governance of IT for the organization.

15 PMI - המכון לניהול פרויקטים, PMBOK - מדריך הידע של PMI לניהול פרויקטים.

16 ITIL - Information Technology Infrastructure Library.

17 החלטת הממשלה 2097, "הרחבת תחומי פעילות התקשוב הממשלתי, עידוד חדשנות במגזר הציבורי וקידום המיזם הלאומי 'ישראל דיגיטלית'" (10.10.14). במקור הוענקה הסמכות לרשות התקשוב.

בבקרה שעשה מערך הדיגיטל בשנת 2019 על יישום הנחיותיו באגף התקשוב במשרד החוץ עלה כי ועדת ההיגוי המשרדית לתקשוב במשרד אינה מתכנסת באופן סדיר ופעילותה דעכה. בבקרת מעקב נוספת שביצע המערך בשנת 2020 דיווח המשרד למערך הדיגיטל שהוועדה הוקמה מחדש.

הביקורת העלתה כי ועדת ההיגוי המשרדית לתקשוב, שבהתאם להנחיה היה אמור לעמוד בראשה המנכ"ל או המשנה למנכ"ל, לא התכנסה במשך כשלוש שנים (2021 - 2023). זאת חרף הודעתו של משרד החוץ למערך הדיגיטל בשנת 2020 כי הוועדה הוקמה מחדש. ועדת ההיגוי שבה והתכנסה רק באפריל 2024.

עוד הועלה כי בניגוד להמלצות מערך הדיגיטל, ולפיהן על ועדת ההיגוי להתכנס בתדירות של פעמיים עד ארבע פעמים בשנה, מאז התכנסותה הראשונה של הוועדה באפריל 2024 ועד למועד סיום הביקורת[18] היא לא התכנסה בשנית, והיא אף לא דנה בתוכנית העבודה השנתית של אגף התקשוב לשנת 2025 ולא אישרה אותה. זאת ועוד, מעיון ברשימת חברי הוועדה שנכחו בדיון ועדת ההיגוי האמור עולה כי הוועדה כללה נציגים בכירים של אגפי המנהלה, אך בניגוד להנחיית מערך הדיגיטל בנושא לא כללה סמנכ"לים מקצועיים במטה המשרד כגון: ראש המערך המדיני אסטרטגי, ראש האגף לעניינים קונסולריים וראש האגף לעניינים אסטרטגיים, שהם לקוחות משמעותיים של אגף התקשוב.

פעילות התקשוב במשרד החוץ היא תשתית חיונית התומכת בעשייה המדינית והמנהלית של המשרד, והיא מאופיינת כאמור באתגרים ייחודיים שנגזרים מהצורך לנהל מידע מדיני ודיפלומטי רגיש בין המטה לנציגויות. מתוך כך נודעת חשיבות יתרה לקיומה ולפעילותה של ועדת היגוי משרדית לתקשוב, שתקבע את האסטרטגיה של המשרד ומדיניותו בנושאי תקשוב, שתעקוב אחר יישום תוכנית העבודה של אגף התקשוב, שתכריע בסוגיות מרכזיות, שתפתור חסמים מרכזיים ושתשמש גורם מתווך בין הנהלת המשרד, המטה והאגפים המקצועיים לאגף התקשוב. אי-התכנסותה של הוועדה כנדרש משליך בהכרח על היכולת לבצע בקרה שוטפת על יישום תוכניות העבודה של אגף התקשוב ועל מימוש יעדיו כך שיתמכו בליבת העשייה של המשרד.

משרד החוץ מסר למשרד מבקר המדינה באוקטובר 2025 כי מנכ"ל משרד החוץ מאשר לכל סמנכ"ל את תקציבו השנתי וכי לוועדת ההיגוי המשרדית לתקשוב אין סמכות לאשר תקציב או תוכניות עבודה.

לעניין זה משרד מבקר המדינה מציין כי בהנחיות מערך הדיגיטל נקבע כאמור כי על ועדת ההיגוי להתוות בין היתר את האסטרטגיה של המשרד ומדיניותו בנושאי תקשוב ולאשר את תוכניות העבודה והתקציבים הרב-שנתיים והשנתיים של כלל הפעילויות המתקיימות במשרד בתחומים של מערכות מידע ותקשוב. אף שלפי תשובת משרד החוץ מנכ"ל משרד החוץ מאשר את תקציב אגף התקשוב, אין בכך כדי לייתר את הצורך לקיים דיונים בוועדת ההיגוי על תוכנית העבודה והתקציב של תחום מערכות המידע והתקשוב במשרד ועריכת מעקב שוטף אחר מימושם, והכול בהתאם להנחיות מערך הדיגיטל בנושא.

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 והתקציבים של כלל הפעילויות המתקיימות במשרד בתחומים של מערכות מידע ותקשוב ומעקב אחר יישומם. 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. זאת ועוד, כדי להבטיח כי תוכנית התקשוב תיתן מענה מיטבי לכלל הגורמים העסקיים, מומלץ שהאגף יבצע תהליך מובנה ושיטתי לאיסוף דרישות מהאגפים לטובת שילובן בתוכנית העבודה השנתית של אגף התקשוב.

---

[18] נכון לפברואר 2025.

תוכנית אסטרטגיה דיגיטלית

על פי תקנים מקובלים[19], לכל ארגון צריכה להיות תוכנית אסטרטגיה דיגיטלית, שתוכן בשיתוף עם בעלי העניין הרלוונטיים, כדי להבטיח שהאסטרטגיה אכן תואמת לצרכים העסקיים ומובילה ליצירת ערך. התוכנית מאפשרת לאגף התקשוב להיערך למתן מענה טכנולוגי ודיגיטלי הולם למשרד, הן בתכנון הפרויקטים והתוכניות למיכון והן בהיערכות לתכנון המשאבים הנדרשים כדי לאפשר תוכנית זו. בין המטרות שתוכנית אסטרטגית מסייעת למימושן ניתן למצוא קידום חדשנות; שיפור השירותים הדיגיטליים הניתנים לאזרחים; סיוע בהתמודדות עם אתגרים טכנולוגיים קיימים; והיערכות לשינויים עתידיים, טכנולוגיים ותהליכיים.

במהלך שנת 2023 פנה משרד החוץ לחברה חיצונית לצורך בחינת המבנה הארגוני הקיים של אגף התקשוב והכנת תוכנית אסטרטגית עבורו (להלן - התוכנית האסטרטגית). באפריל 2024 הגישה החברה את התוכנית לאגף התקשוב. התוכנית הציפה פערים משמעותיים בפעילות האגף בתחומי המבנה הארגוני, היקף כוח האדם המוקצה לתחום התקשוב, תהליכי העבודה, התשתיות הטכנולוגיות והתקציב. בין היתר, התוכנית מדגישה את החוב הטכנולוגי הגדול שנוצר בשל בניית פתרונות בטלאים לאורך שנים; עוד היא מציינת שהאגף נמצא במרדף אינסופי "אחרי הזנב של עצמו" ומוגבל ביכולתו להתקדם מהמשימות השוטפות, היות שהוא משקיע את התקציב בפתרונות עבור שימור המצב הקיים ולא במקומות שבהם האגף יכול להתקדם ולפרוץ קדימה; נוסף על כך התוכנית מציפה בעיות הקשורות להיעדר פונקציית OCIO[20] באגף ולהיעדר כלים לניהול ובקרה של פרויקטים. התוכנית כוללת גם שורה של המלצות לשיפור תהליכי משילות מערכות המידע במשרד וכן תיעדוף שלהן, תוך שימת דגש על צעדים שחייבים לנקוט (Must Have) והערכת תקציב ראשונית שנדרשת ליישומם.

משרד מבקר המדינה מציין לחיוב את יוזמת המשרד לגיבוש הצעה לתוכנית אסטרטגית בתחום התקשוב בשנים 2023 - 2024. עם זאת, הביקורת העלתה כי על אף 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, עד פברואר 2025, יותר מתשעה חודשים ממועד הגשתה למשרד, התוכנית לא נדונה על ידי מנכ"ל המשרד או בוועדת ההיגוי המשרדית לתקשוב, ולא נקבעו הצעדים הנדרשים למימושה.

משרד החוץ מסר למשרד מבקר המדינה באוקטובר 2025 כי הפער הטכנולוגי נוצר בעקבות חסר של שנים בתקצוב למשרד החוץ בכלל ולאגף התקשוב בפרט. מנכ"ל משרד החוץ מסר כי האתגרים העומדים בפניו, כפי שעמדו גם בפני קודמיו לתפקיד, ימשיכו להיות אתגרים של משאבים וסדרי עדיפויות, ובכלל זה תקציב מצומצם, כוח אדם שאינו מספק ומערכות שנדרש לשדרגן. עוד מסר המנכ"ל כי הוא הורה לסמנכ"ל תקשוב להציג תכנית עבודה לתיקון הליקויים.

לנוכח האתגרים הייחודיים שעימם מתמודד כאמור אגף התקשוב במשרד החוץ, ולנוכח הצורך הדחוף בקידום הפעילות התקשובית במשרד וטיפול בפערים ובחסמים שהועלו במסגרת התוכנית האסטרטגית, 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.

יש לתת את הדעת שאם לא יתקבלו החלטות ולא יינקטו בהקדם צעדים להתמודדות עם הפערים שהועלו בתוכנית האסטרטגית, הפערים שהוצפו עלולים לגדול ולפגוע ביכולת אגף התקשוב לתת מענה ראוי ואיכותי לצורכי המשרד כמו גם לשירות לציבור.

---

19 COBIT - תהליך APO02 - ניהול אסטרטגיית מידע וטכנולוגיה; ISO 38500 - Principle 2: Strategy.

20 Office of the CIO - פונקציית מטה של ראש האגף לריכוז הפעילות מול החטיבות באגף.

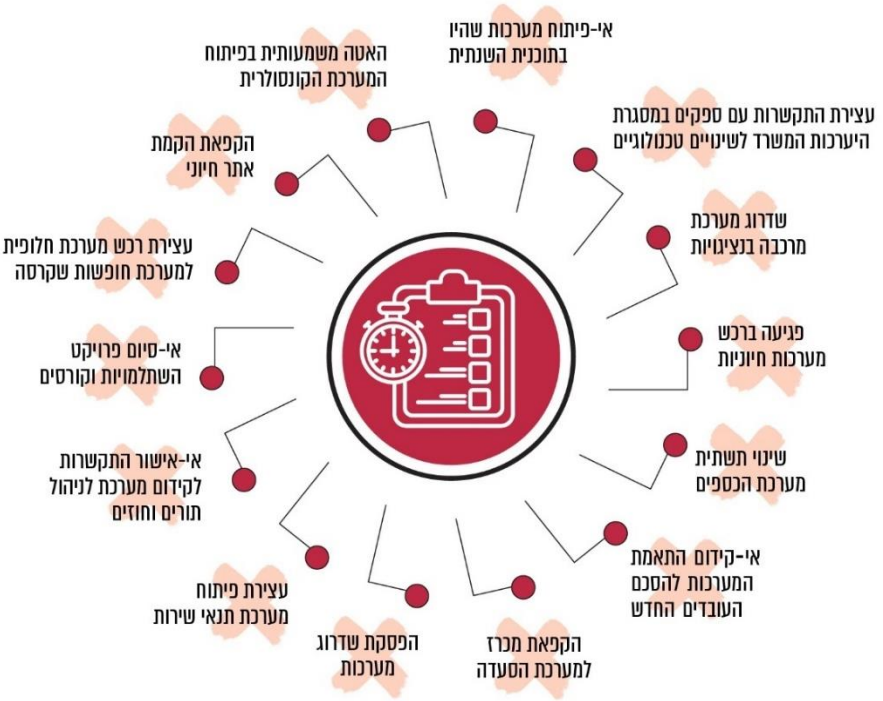
תקציב אגף התקשוב

תקציב אגף התקשוב הוא הבסיס לניהול אפקטיבי של המשאבים הטכנולוגיים, תוך שמירה על איזון בין קיום התהליכים העסקיים השוטפים, מענה לדרישות עסקיות חדשות, שימוש בטכנולוגיות חדשות והשגת יעילות כלכלית.

במאי 2024 שלח מנהל אגף התקשוב למנכ"ל משרד החוץ דאז מסמך שעניינו "משבר תקצוב לשנת 2024". מהמסמך עולה כי תקציב ההוצאות הקשיחות של האגף עומד על סך של כ-103 מיליון ש"ח, ואילו בפועל תקציב האגף לשנת 2024 הועמד על כ-85.3 מיליון ש"ח. כלומר, מהמסמך עולה כי האגף מתוקצב בתקציב חסר של כ-18 מיליון ש"ח, תקציב שאינו מכסה לדבריו את ההוצאות הקשיחות של האגף, ואף אינו מאפשר שדרוג ותחזוקה של מערכות, התמודדות עם אתגרים בתחום הסייבר, מעבר לענן ושימוש בכלי בינה מלאכותית לפעילות דיפלומטית. עוד צוין במסמך כי לקראת דיוני תקציב 2024 העביר האגף בקשה לקבלת תקציב של כ-132.5 מיליון ש"ח, וכי לצורך עמידה בהוצאות הקשיחות, בתוכנית העבודה וביעדי המשרד יש צורך בתקצוב נוסף של לפחות 20 מיליון ש"ח (מעבר לתקציב שהועמד כאמור לרשות האגף).

המסמך כולל פירוט של 14 פרויקטים שפיתוחם יוקפא או יתעכב בהיעדר תקציב בתוכנית העבודה לשנת 2024, ובכלל זאת: שדרוג מערכת מרכב"ה חדשה בנציגויות; האטה בפיתוח המערכת החדשה לניהול הפעילות הקונסולרית, (להרחבה בעניין מערכת זו ראו בהמשך); עצירת פיתוח מערכת חדשה (מערכת תנאי שירות); עלייה לענן - אי-פיתוח מערכות שהיו בתוכנית השנתית ועצירת התקשרות עם ספקים וחברות בתחום.

תרשים 4: **פרויקטים שפיתוחם יוקפא או יתעכב בהיעדר תקציב בתוכנית העבודה לשנת 2024**



על פי מסמכי משרד החוץ, בעיבוד משרד מבקר המדינה.

תיאור התקציב החסר בא לידי ביטוי גם בכמה פניות שהוציא מנהל אגף התקשוב במסגרת ההיערכות לשנת 2025 לכמה מנהלי יחידות, ובמסגרתן ריכז את העלויות הנדרשות לטובת פיתוח, תחזוקה ותמיכה במערכות שנמצאות בשימוש על ידן. עוד ציין כי קידום הפרויקטים מותנה בהקצאת תקציב ייעודי על ידם, ושללא תקצוב זה לא יהיה ניתן להתקדם לשדרוג ופיתוח של מערכות חדשות.

היעדר תקצוב מספק עלה גם במסגרת התוכנית האסטרטגית. בתוכנית הוצג שהאגף נמצא ב"חוב טכנולוגי עצום שמשתק את יכולתו לנוע קדימה". בניתוח שמוצג במסמך עלה כי בהתייחס לשיעור הוצאות תקשוב שוטפות (OPEX) אל מול השקעות (CAPEX), שיעור הוצאות תקשוב השוטפות עומד במשרד החוץ על כ-98% מתוך סך תקציב התקשוב, ואילו ממוצע הוצאות התקשוב השוטפות במשרדי הממשלה בישראל עומד על כ-44%. עוד עולה מהמסמך ששיעור עובדי התקשוב מתוך כלל עובדי המשרד במשרד החוץ הוא 4.1%, ואילו הממוצע במשרדי הממשלה הוא 9.8%. פערי כוח אדם ניכרים בתחומי התשתיות והתמיכה ובטכנאים הוצגו גם בסקר הסיכונים, שבו צוין כי היחס של כמות הטכנאים למספר המשתמשים יוצר עומסים רבים ודחייה במענה לקריאות.

ממסמכי אגף התקשוב עולה שנכון לשנת 2024 התקציב שהוקצה לתפעול שוטף של תחום התקשוב 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 כאמור - 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. זאת ועוד, מהמסמכים עולה כי הדבר השליך גם על היכולת להשקיע ברכש מערכות מסוימות.

גם בשורה של פגישות שקיים משרד מבקר המדינה עם נציגי אגף התקשוב עלה כי לדבריהם התקציב החסר משפיע באופן ניכר על פעולות ליבתיות של יחידות המשרד. כך למשל עלה כי בשל שיקולים תקציביים קיים איוש חלקי של טכנאים אזוריים בכל העולם וקיים קושי לשלוח טכנאים מהארץ לחו"ל, דבר שמשליך על יכולת האגף לתת מענה סביר לתקלות מחשוב ותקשורת בחו"ל.

משרד החוץ ציין בתשובתו למשרד מבקר המדינה מאוקטובר 2025 שעם כניסת המנכ"ל הנוכחי תוגבר תקציב התקשוב בסוף שנת 2024 בתוספת של כ-12 מיליון ש"ח, וזאת לשם התחלת טיפול בבעיות שהועלו על ידי מנהל אגף התקשוב. עוד מסר המשרד כי בשנת 2025 עמד תקציב תקשוב על כ-105.5 מיליון ש"ח, בתוספת עודפים בסך של כ-8.5 מיליון ש"ח שהתקבלו לקראת סוף שנת העבודה. משרד החוץ הוסיף כי חלק מהמערכות שהוזכרו בדוח טופלו והוחלפו, אך חלק עדיין לא טופל, הואיל ונדרש לכך תקציב ייעודי.

תקציב מאפשר הוא תנאי הכרחי למימוש אפקטיבי של ממשל טכנולוגיות מידע, שכן ללא תקצוב מספק, הארגון חשוף לסיכוני תפעול ואבטחה רבים. לאור 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 הערכות עתידית לעבודה בענן).

ניהול סיכונים

בהתאם להנחיות מערך הדיגיטל[21], משרדי הממשלה נדרשים לנהל את סיכוני התקשוב במשרד[22]. מטרות התהליך הן זיהוי ומיפוי של חשיפות ואיומים על נכסי המידע המשרדיים, תיעדוף והקצאה יעילה של משאבים ומתן מענה לשינויים בסביבת הפעילות של המשרד. כמו כן התהליך נועד לסייע בגיבוש תוכניות טיפול מותאמות ואפקטיביות לסיכונים שזוהו, כולל לסיכונים ייעודיים בתחומי ניהול פרויקטי תקשוב ותחזוקת מערכות ותשתיות. בהתאם להנחיות אלה יש לדווח להנהלת המשרד על ממצאי סקרי הסיכונים, הסיכונים המהותיים והתקדמות ביצוע תוכניות הטיפול

---

21 הנחיה 1.3.01 בנושא "עקרונות לניהול סיכוני תקשוב במשרדי הממשלה" מ-14.11.23 והנחיה 1.3.02 בנושא "ביצוע סקר סיכוני תקשוב במשרדי ממשלה" מ-1.11.23.

22 "סיכון תקשוב" הוגדר בהחלטת הממשלה 2097 (מיום 10.10.14) כחשיפת תשתיות התקשוב, תהליכי התקשוב ופרויקטי התקשוב לאירוע כשל אשר עלול לגרום לפגיעה ביעדי הארגון, לפגיעה במידע, לפגיעה ברמת השירות או לאי-עמידה בתקנים מחייבים.

בסיכונים שעלו. עוד נקבע כי הסיכונים שמופו יידונו בפני ועדת ההיגוי המשרדית או הפרויקטלית לפי העניין, אשר תאשר את רשימת סיכוני המפתח ותחליט על נחיצות תוכנית טיפול עבורם.

במהלך השנים 2022 - 2024 בוצע על ידי חברה חיצונית סקר סיכוני תקשוב משרדי. הסקר הוצג להנהלת אגף התקשוב בחודש מאי 2024 (להלן - סקר הסיכונים). הסקר העלה ממצאים מהותיים ביחס למשילות בתחום התקשוב, ובכלל זה אובדן ידע ומידע, חשיפה לסיכוני רגולציה וציות, במיוחד בתחומי הגנת הפרטיות, סיכונים לעמידה בתוכנית העבודה לנוכח היעדר סנכרון בין החטיבות, היעדר תמונת מצב רוחבית על ניהול הפרויקטים, היעדר פגישות עבודה קבועות בין מנהל מערכות המידע הראשי (המנמ"ר) לראשי החטיבות, מבנה ארגוני לקוי, מיומנויות חסרות והיעדר הכשרות מספקות, ועיכובים באספקת מערכות המידע.

קיומו של סקר סיכוני תקשוב משרדי הוא צעד חשוב והכרחי לניהול סדור ושיטתי של סיכוני התקשוב. משרד מבקר המדינה מציין לחיוב את קיום סקר סיכוני התקשוב על ידי משרד החוץ במאי 2024. עם זאת נמצא כי על אף הסיכונים המהותיים שהועלו בסקר, ובניגוד להנחיות מערך הדיגיטל, נכון לינואר 2025, מעל חצי שנה ממועד הגשתו למשרד, ועדת ההיגוי המשרדית עדיין לא דנה בתוצאות הסקר והשלכותיו, ולא אושרה על ידה תוכנית לטיפול בסיכונים שהועלו. התנהלות זו עלולה לפגוע ביכולתו של משרד החוץ להתמודד עם הסיכונים שהועלו.

משרד החוץ מסר למשרד מבקר המדינה באוקטובר 2025 כי סקר הסיכונים שבוצע לא אושר על ידי המשרד ויש בו פערים שהחברה נדרשה להשלים.

על משרד החוץ לפעול להשלים בהקדם את סקר הסיכונים שכן ככל שחולף הזמן מביצוע הסקר, תמונת הסיכונים הולכת ומשתנה, וההשלכות של התממשות הסיכונים על המשרד עלולות להיות רחבות יותר. לאחר השלמת הסקר על מנכ"ל המשרד וועדת ההיגוי המשרדית לדון בממצאי סקר הסיכונים ובתוכנית לטיפול בסיכונים ולאשרה, ולעקוב אחר תהליך ההתמודדות עם סיכונים אלו לשם הפחתתם.

ניהול הסיכונים הלקוי בתחום מערכות המידע בא לידי ביטוי גם בתמונת המערכות שבאחריות אגף התקשוב המשקפת כי ישנן מערכות מיושנות, הנמצאות בפער טכנולוגי או פונקציונלי שמחייב שדרוג או החלפה.

ניתוח נתוני משרד החוץ העלה כי נכון לשנת 2024 קיימות מערכות מסוימות שהוגדרו כ-EOL (End Of Life), או ככאלו הדורשות שדרוג או החלפה.

שימוש במערכות מידע מיושנות בכלל וכאלה שהגיעו לסוף חיי התמיכה שלהן (EOL) בפרט טומן בחובו סיכונים משמעותיים: בהיעדר תמיכה טכנית, המערכות חשופות יותר לתקלות בלתי צפויות, לאי-התאמה לדרישות רגולציה עדכניות, לקשיים בביצוע שינויים ושיפורים במערכות בהתאם לשינויים בתהליכי העבודה ואף לחוסר יכולת לבצעם; התחזוקה השוטפת של מערכות אלו הופכת ליקרה ומורכבת יותר, ועלולה לפגוע ביעילות ובזמינות השירותים לארגון ולציבור, כפי שגם קרה בפועל במערכת אימותים (בעניין זה ראו בהרחבה בדוח מבקר המדינה בנושא אימות מסמכים ציבוריים במשרד החוץ - אפוסטיל); קיומן של מערכות מיושנות אלו עלול גם לפגוע בתאימות וביכולת האינטגרציה עם מערכות חדשות.

זאת ועוד, המשך השימוש במערכות המיושנות עלול להוביל לפגיעה בעבודת האגפים המקצועיים במשרד החוץ; בשירותים הקונסולריים של מדינת ישראל; וביכולתו של המשרד לשמור על רציפות תפקודית.

במרץ 2025 העביר משרד החוץ למשרד מבקר המדינה התייחסות בנוגע לשדרוג של כמה מערכות שהוגדרו כ-EOL, ששדרוגן אמור להסתיים במהלך שנת 2025. אשר ליתר המערכות, צוין כי הפעולות הנדרשות בעניינן יבוצעו במסגרת תוכנית עבודה רב-שנתית, הכוללת גם הגירה לענן של חלק מהמערכות. עיון בתוכנית העלה כי המעבר לענן מתוכנן להתבצע בכמה גלי הגירה על בסיס

ערך עסקי ואומדן עלויות, בעלות כוללת של 126 מיליון ש"ח. גל ההגירה האחרון מיועד להסתיים בשנת 2029[23].

משרד החוץ מסר למשרד מבקר המדינה באוקטובר 2025 כי הפער הטכנולוגי נוצר בעקבות חסר של שנים בתקצוב למשרד החוץ בכלל ולאגף התקשוב בפרט. עוד צוין על ידו כי כל מערכת שנמצאת בסטטוס EOL או מתקדמת לכיוון זה, מועמדת להגירה לענן ונבחנת מול חלופות אחרות.

מהאמור עולה כי משרד החוץ גיבש תוכנית רב-שנתית לטיפול במערכות המידע של המשרד, לרבות באמצעות הגירה לענן, שבמסגרתה ישודרגו או יוחלפו מערכות ישנות. עם זאת, כדי לוודא כי ניתן מענה במסגרת מעבר לענן או בתצורה אחרת לכלל המערכות הישנות, ולנוכח החשש כי חלקן עלול לקרוס עוד לפני שיסתיימו גלי ההגירה לענן בשנת 2029, או שהתקציב שיוקצה לנושא יהיה בחסר, על ועדת ההיגוי לעקוב ולפקח באופן הדוק אחר מימוש התוכנית.

נהלים וסטנדרטים

על פי הנחיות מערך הדיגיטל[24] בכדי לפעול באפקטיביות וביעילות, על היחידות המונחות על ידי רשות התקשוב להגדיר וליישם הוראות ונוהלי עבודה עבור הפעילויות ותהליכי העבודה העיקריים שלהן. בהנחיות צוין כי מסמכי מתודולוגיה עדכניים, כתובים וזמינים הכרחיים כדי לשמר ידע, לוודא הבנה ועמידה בדרישות ולהשיג שפה אחידה, עקבית, ברורה ומובנת. כמו כן, מסמכים כתובים יאפשרו לוודא אי-תלות בזמינות אנשים שמכירים וזוכרים את המתודולוגיה, יקלו על הנחלתה לאנשים חדשים בארגון, וימנעו תקלות שעלולות להתרחש בעת עבודה שאינה תואמת למתודולוגיה ומסתמכת על "התורה שבעל-פה". מצד אחד, הוראות העבודה צריכות להיות בהלימה עם המדיניות, התקנים והקווים המנחים שמוגדרים על ידי מערך הדיגיטל הלאומי, ומצד שני עם סביבת העבודה המקומית במשרד. הצורך בעבודה על פי נהלים וסטנדרטים מסודרים ומעודכנים ביחידות התקשוב הארגוניות מודגש גם בפרקטיקה המקובלת.

בבקרה שביצע מערך הדיגיטל במשרד החוץ בשנת 2019 על יישום הנחיותיו, העיר המערך למשרד החוץ על פערים ניכרים בקיום נהלים ומתודולוגיה לעבודה סדורה באגף התקשוב. בין היתר צוין כי חסרים נהלים העוסקים בפעילויות רוחביות, כגון ניהול סיכונים וניהול לקחים, וכי בנוהל המתודולוגיה המרכזי יש הפניה לתבניות ונהלים רבים שלא קיימים, או כבר לא רלוונטיים, או לא מעודכנים, "נהלים רבים עודכנו לאחרונה לפני 10-20 שנים, מה שמעלה בספק את תקפותם". בבקרה צוין כי נדרש לעדכן את הנהלים ולוודא את עדכניותם לפחות אחת לשנה. בבקרת מעקב נוספת שביצע המערך על יישום הנחיותיו בסוף שנת 2020 עלה כי הושלמו כמה נהלים בשנת 2020, ובתוכנית העבודה של שנת 2021 תוכננה הכנה והטמעה של נהלים נוספים וכן שחזור או עדכון של נהלים קיימים.

בסקר הסיכונים שבוצע בשנת 2024 צוין כי חסרים נהלים ובהם נוהל קליטת עובד חדש באגף, נוהל תיעוד פיתוח, שינויים ותחזוקה במערכות מידע (תיק תחזוקה) כפי שמופיע בנוהל פיתוח מערכות של מערך הדיגיטל, נוהל הערכת עובד ברמה מקצועית, נוהל ביצוע רכש באגף, נוהל לביצוע מעקב אחר תוכנית עבודה והרכש, נוהל לבנייה של תוכנית עבודה ונוהל לבקרת תוכנית עבודה. כאמור, הסקר טרם אושר על ידי המשרד עקב השלמות שנדרשו מהחברה החיצונית שביצעה אותו.

בחינה שביצע משרד מבקר המדינה בנוגע לסט נוהלי התקשוב שהועבר אליו ממשרד החוץ במאי 2024 העלתה כי סט הנהלים הקיים נותר חסר. כך למשל חלק מהנהלים החסרים שזוהו בסקר הסיכונים, משנת 2019 לא הוכנסו ואושרו. במועד סיום הביקורת חסרים נהלים בתחומי פעילות משמעותיים, כגון נוהל לביצוע תהליכי תחקיר והפקת לקחים לפרויקטים; נוהל מסודר לביצוע

---

23 משרד החוץ מסר למשרד מבקר המדינה במאי 2025 כי מערכות לשדרוג בתחום חטיבת יישומים, שנמצאות בתוכנית ההגירה לענן לשנת 2025, נכנסו לתוכנית העבודה לביצוע השדרוג בשנה זו (2025) ויש עבורן תקציב.

24 הנחיית מערך הדיגיטל מספר 1.1.01 מתאריך 17.1.24 בנושא "מסגרת מתודולוגיית תקשוב ממשלתית"; הנחיית מערך הדיגיטל מספר 1.4.01 מתאריך 11.12.22 בנושא "מחזור חיי מערכת תקשוב".

בדיקות על סוגיהן השונים בתהליך הפיתוח (למעט בדיקות הנדרשות בעת ביצוע שינויים); נוהל מנחה לעבודה במתודולוגיית הפיתוח הזריז (מתודולוגיית אג'ייל)[25].

עבודה לפי נהלים וסטנדרטים היא אבן יסוד בממשל מערכות מידע. הנהלים יוצרים אחידות בתהליכי העבודה, מפחיתים טעויות אנוש, ממזערים סיכונים תפעוליים, תורמים לשימור הידע הארגוני ומסייעים בשמירה על איכות העבודה ובעמידה בדרישות רגולציה ותקינה.

לנוכח חשיבות הנושא, מנהל אגף התקשוב נדרש ליזום תהליך מסודר לעדכון וכתיבה של נוהלי העבודה החסרים באגף מערכות מידע, תוך עדכון החוסרים הקיימים על סמך זיהוי פערים והתאמה לדרישות רגולציה, אבטחת מידע ושינויים טכנולוגיים. כמו כן עליו ליישם מנגנון לבקרה ועדכון תקופתי של הנהלים כדי להבטיח תפקוד יעיל של האגף.

מוצע כי השלמת הנהלים החסרים תתבצע בשיתוף ובליווי של מערך הדיגיטל. כמו כן, לנוכח הפערים בנושא ולנוכח הבקרות שבוצעו בעבר על ידי מערך הדיגיטל, מומלץ כי המערך ימשיך לעקוב אחר הנושא.

ניהול פרויקטים ופיתוח מערכות מידע

ניהול פרויקטים מחייב תכנון ויישום שיטתיים תוך ייעול השימוש במשאבים, הגברת שיתוף הפעולה והתיאום בין כל בעלי העניין במטרה להבטיח עמידה ביעדי הפרויקט ולוחות הזמנים, שמירה על התקציב ודרישות האיכות והגדלת סיכויי הצלחת הפרויקט והגשמת יעדיו[26]. חשיבות זו מקבלת ביטוי גם במתודולוגיות לניהול ופיתוח של מערכות מידע המוכרות והמקובלות בארץ ובעולם ובהן נוהל מפת"ח[27], COBIT, PMBOK[28], ITIL (להלן - המתודולוגיות המקובלות).

מתוך הבנה כי נדרש להגדיל במידה ניכרת את אחוזי ההצלחה של פרויקטי תקשוב ואת היעילות של מערכות המידע ונכסי התקשוב בממשלה, מערך הדיגיטל הלאומי פרסם הנחיות הנוגעות לניהול פרויקטים, תוך הבחנה בין השלבים השונים במחזור החיים של מערכת תקשוב[29]: הייזום, התכנון, הביצוע, העלייה לאוויר, הייצוב, התחזוקה השוטפת - ולבסוף הורדת המערכת. בהנחיות שפורסמו בעניין זה צוין כי הן בגדר תקן ממשלתי מחייב. תכלית ההנחיות היא לספק שיטות וכלים שיסייעו לוודא ש"הפעילויות מנוהלות ולא מתנהלות", בדגש על התאמה לצרכים, איכות, עלויות, עמידה בלוחות זמנים, ניהול סיכונים וקיום תהליך של הפקת לקחים.

משרד החוץ מנהל בו-זמנית עשרות פרויקטים בתחום התקשוב לשימוש בארץ ובעולם בתחומים שונים של פעילות המשרד. משרד מבקר המדינה בחן כמה היבטים הנוגעים לפיתוח פרויקטים ומערכות אלו. במסגרת זו בחן שישה פרויקטי פיתוח בשלבים שונים מהשנים האחרונות. כמו כן בוצעה בחינה ספציפית בנוגע לפיתוח אחת ממערכות המשרד. להלן הפרטים.

---

25 מתודולוגיית אג'ייל היא שיטה לניהול פרויקטים המתמקדת בפיתוח הדרגתי וגמיש של מוצרים, תוך שיתוף פעולה רציף עם הלקוח והתאמה מהירה לשינויים.

26 ראו למשל במחקר:
Belassi, W., & Tukel, O. I., "A new framework for determining critical success/failure factors in projects". **International Journal of Project Management**, 14(3) (1996), 141-151

27 נוהל מפת"ח (מתודולוגיית פיתוח ותחזוקה) - מתודולוגיה לניהול פרויקטי תוכנה, הנדסת תוכנה, ניתוח מערכות וניהול איכות תוכנה, שפותחה בישראל על ידי משרד האוצר וחברת מתודה בע"מ. חייבה בעבר את משרדי הממשלה. כיום מתודולוגיה מוכרת שמשלימה במידת הצורך את המתודולוגיה הממשלתית. ראו בקישור methoda.cloud.

28 PMI (Project Management Institute) - המכון לניהול פרויקטים, (Project Management Body of Knowledge) PMBOK - מדריך הידע של המכון לניהול פרויקטים. מתודולוגיה מוכרת שעשויה להשלים את המתודולוגיה הממשלתית. ראו: www.pmi.org.

29 ראו הנחיה 1.4.01, "מחזור חיי מערכת תקשוב".

ועדות היגוי לפרויקטים

ועדת היגוי לפרויקט מערכות מידע היא נדבך הכרחי לניהול הפרויקט, שכן תפקידה לפקח על התקדמותו, לוודא עמידה ביעדים, בתקציב ובלוחות הזמנים, לקבל החלטות קריטיות אם אכן נדרשות, לזהות חסמים ולסייע בפתיחתם, לסייע בפתרון בעיות ובתיאום בין כל הגורמים המעורבים.

הנחיות מערך הדיגיטל הלאומי[30] מחייבות מינוי ועדת היגוי בפרויקטים של מערכות מידע לכל פרויקט שאינו קטן[31] ולפרויקטים מורכבים[32]. תפקיד הוועדה בהתאם להנחיות הוא ללוות את הפרויקט לכל אורכו, והיא מופקדת על פיקוח, הנחיה, אישור אבני דרך, דיון באתגרים ובסיכונים והבטחת עמידה ביעדי הפרויקט[33]. לראש הוועדה יש למנות נציג בכיר של הנהלת המשרד או מנהל של היחידה העסקית, ועם חבריה נמנים נציג בכיר של יחידת התקשוב, נציג היחידה העסקית, חברי מינהלת הפרויקט ונציגי המשתמשים העיקריים[34]. חובת מינוי ועדת היגוי נקבעה גם בנוהל משרד החוץ שעניינו "ניהול פרויקט פיתוח מערכת מידע"[35].

משרד החוץ מסר לביקורת בפברואר 2025 כי הצורך בקיום ועדת היגוי הוא תלוי פרויקט - כאשר נדרשת מעורבות גדולה או כשהפרויקט מהותי לארגון. עוד מסר שבפועל לרוב הפרויקטים המנוהלים במשרד בשנים האחרונות לא הוקמו ועדות היגוי.

בביקורת עלה כי בניגוד להנחיות מערך הדיגיטל לפיהן יש להקים ועדות היגוי לכל פרויקט פיתוח מערכת מידע המוגדר מורכב או שבגודל בינוני ומעלה ולנוהלי המשרד, משרד החוץ לא מינה ועדות היגוי לארבעה מתוך שישה פרויקטים משמעותיים שנבדקו.

באוקטובר 2025 מסר משרד החוץ בתשובתו כי הפרויקטים, לרבות הוספת תכולות, מבוצעים יחד עם הלקוחות העסקיים ותוך קיום ישיבות סטטוס.

משרד מבקר המדינה מעיר כי ביצוע הפרויקט בשיתוף היחידה העסקית וקיום פגישות סטטוס אינם מייתרים את הצורך בדבר קיום ועדת היגוי לפרויקטים מורכבים ומשמעותיים, שתפקידה לפקח על קיומן של אבני הדרך ולאשרן, לדון באתגרים ובסיכונים ולהבטיח את עמידת הפרויקט ביעדיו.

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. יתרה מזו, היעדר ועדת היגוי לפרויקט משליך על מעורבות ההנהלה והגורמים העסקיים ועל היכולת לקבל החלטות מרכזיות לשם קידום הפרויקט, ועלול להגדיל את הסיכון לפגיעה בעמידה ביעדי הפרויקט, להתארכות לוחות הזמנים, לחריגה תקציבית ולפגיעה באיכות התוצרים.

יצוין כי גם בתוכנית האסטרטגית הועלה כי חסרה ועדת היגוי שמתכנסת אחת לכמה שבועות כדי לדון בהתקדמות הפרויקט, וזאת כאחד ממקורות בעיות האגף וחלק מממדי השינוי המרכזיים

---

30 ראו סעיף 3.23.6 בהנחיה 1.4.01 "מחזור חיי מערכת תקשוב".

31 פרויקט קטן לפי סעיף 3.15 בהנחיה 1.4.01, "מחזור חיי מערכת תקשוב" הוא פרויקט שעלותו עד מיליון ש"ח, ושהמאמץ הכרוך בו אינו עולה על שלוש שנות אדם.

32 לפי סעיף 3.16.2 בהנחיה 1.4.01, "מחזור חיי מערכת תקשוב", פרויקט מורכב מאופיין באחד מאלה: גדול מאוד; בין-משרדי; ממשלתי רוחבי; בעל מורכבות ארגונית גבוהה; מרובה ממשקים חיצוניים; בשימוש טכנולוגיה שהיא חדשה במשרד הממשלתי.

33 ראו סעיף 3.23.6 בהנחיה 1.4.01, "מחזור חיי מערכת תקשוב".

34 ראו סעיף 3.23.6 בהנחיה 1.4.01, "מחזור חיי מערכת תקשוב".

35 ראו סעיף 2.4.2.1 בנוהל 01-02-05, "ניהול פרויקט פיתוח מערכת מידע".

הנדרשים בו. כמו כן, גם בסקר הסיכונים שבוצע עבור המשרד[36] עלה כי לא קיימת ועדת היגוי בחלק מהפרויקטים והומלץ להגדיר ועדת היגוי לכל אחד מהפרויקטים באגף התקשוב.

בהתאם להנחיות מערך הדיגיטל הלאומי, משרד החוץ נדרש להקים ועדות היגוי לכל פרויקט פיתוח מערכת מידע המוגדר מורכב או שבגודל בינוני ומעלה. על ועדות ההיגוי לכלול נציגים בכירים מהנהלת המשרד, נציגי משתמשים ונציגים כמפורט בהנחיות, ולהתכנס בתדירות שתאפשר בקרה מיטבית על ביצוע הפרויקט וקבלת החלטות במידת הצורך. כמו כן מומלץ להטמיע מערכת לדיווח ומעקב שוטף, שתאפשר בקרה מיטבית על התקדמות הפרויקטים ותסייע במימוש יעדיהם.

ניהול סיכונים בפרויקטים

פרויקטים של מערכות מידע הם בעלי מורכבות גבוהה מטבעם, וכוללים תכנון וביצוע של משימות רבות השלובות זו בזו, עם מעורבות של אנשי מקצוע בעלי התמחויות שונות, תקציב מוגבל, לוח זמנים קצוב וצורך בתיאום הדוק מול הלקוחות. משכך, פרויקטים אלו מצויים בחשיפה גבוהה לסיכונים שעלולים לפגוע ביכולת העמידה בלוחות הזמנים הקצובים, בתכולה הנדרשת, במשאבים שהוקצו להם וביעדיהם. לשם הגדלת סיכויי ההצלחה של הפרויקט, חיוני לבצע זיהוי והערכה של הסיכונים האפשריים ולטפל בהפחתתם לכל אורך מחזור החיים של הפרויקט.

לפי הנחיות מערך הדיגיטל הלאומי, ניהול סיכונים הוא מרכיב הכרחי בניהול הפרויקט בשלביו השונים[37]. החל מהגדרת מטרת פרויקט: "להביא ללקוח ערך מקסימלי, תוך אופטימיזציה של משאבים (כוח אדם וכסף) וסיכונים"[38], המשך בשלב הייזום, בהכנת רשימת סיכונים[39] ובעריכת ניתוח סיכונים ראשוני לפרויקט[40], עבור בהצגת ניהול סיכונים מעודכן לחברי ועדת ההיגוי בכל שלבי הפרויקט[41], ועד חובת ביצוע תוכנית הפחתת סיכוני תפעול ותחזוקת המערכת טרם עלייה לאוויר[42].

בהתאם, גם בנוהל משרד החוץ שעניינו "ניהול פרויקט פיתוח מערכת מידע" נקבעה חובה לבצע ניתוח סיכונים בפרויקט ולגבש תוכנית הפחתה מפורטת להתמודדות עם הסיכונים[43]. בנוהל נוסף העוסק ב"עלייה לאוויר מערכת מידע" של המשרד נקבעה חובת תיעוד ביצוע "בקרת סגירת או צמצום סיכונים" כתנאי להתקנה של מערכת[44].

בפברואר 2025 מסר משרד החוץ כי עד כה לא היה - ועדיין אין - ניהול סיכונים בפרויקטים. עוד מסר המשרד כי לאחרונה מונה באגף מנהל סיכוני תקשוב, וכי הכוונה היא להתחיל ליישם בשנה זו תהליך של ניהול סיכונים בפרויקטים שיוגדרו בתיעדוף גבוה, ובהמשך להרחיב את ניהול הסיכונים לפרויקטים נוספים.

הביקורת העלתה כי בניגוד לנדרש בהנחיות מערך הדיגיטל ובנהלי המשרד לפיהן 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. יצוין כי

---

36 הסקר נערך בין החודשים אוגוסט 2022 לנובמבר 2023 לצורך איתור סיכוני טכנולוגיות מידע באגף התקשוב של משרד חוץ וניתוחם. נבחנו בו מערכות המידע המרכזיות והבקרות הקיימות בתהליכים. מטרתו המרכזית הייתה לספק להנהלה תמונת מצב עדכנית בנוגע לסיכונים העלולים לפגוע באגף התקשוב להשיג את יעדיו או למנוע ממנו לעשות כן. תוצרי הסקר הוגשו להנהלת אגף התקשוב במאי 2024.

37 ראו סעיף 5.3 בהנחיה 1.1.01, "מסגרת מתודולוגיית תקשוב ממשלתית".

38 ראו סעיף 4 בהנחיה 1.4.9, "אמידה ובקרת עלויות במחזור חיי מערכת תקשוב".

39 ראו סעיף 6.3 בהנחיה 1.4.02, "שלב הייזום ושער הכניסה לפרויקט תקשוב".

40 ראו סעיף 6.11 בהנחיה 1.4.02, "שלב הייזום ושער הכניסה לפרויקט תקשוב".

41 ראו סעיף 3.23.6 בהנחיה 1.4.01, "מחזור חיי מערכת תקשוב".

42 ראו סעיף 4.1.5 וסעיף 7 בהנחיה 1.4.07, "שער עלייה לאוויר בפרויקט תקשוב".

43 ראו סעיף 5 בנוהל 01-02-05, "ניהול פרויקט פיתוח מערכת מידע".

44 ראו סעיף 14 בנספח א' בנוהל 01-05-00, "עלייה לאוויר מערכת מידע".

גם בסקר הסיכונים שביצע המשרד עלה כי לא בכל הפרויקטים מבוצעת הערכת סיכונים בתחילת הפרויקט, וכן לא מיושמת מתודולוגיה לניהול סיכוני פרויקט. 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.

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.

תחקירים והפקת לקחים בפרויקטים

תהליכי תחקור והפקת לקחים בפרויקטים של מערכות מידע חיוניים להפקת תובנות וללמידה מטעויות והימנעות מחזרה עליהן, לזיהוי סיכונים פוטנציאליים, להגברת היעילות בפרויקטים עתידיים ולשיפור מתמיד בעבודת הארגון.

הנחיות מערך הדיגיטל הלאומי דורשות ביצוע תהליכי תחקור, הפקת לקחים והטמעתם[45] כלמידה מבוססת נתונים, וזאת לשם שיפור רציף ומתמיד ולצורך שחזור הצלחות ומניעת כישלונות. נקבע כי יש לקיים תחקירים כחלק משגרת העבודה בכל פרויקט המוגדר כגדול[46]; שנרשמה בו חריגה של 25% ומעלה במדד עיקרי (לוח זמנים, תקציב או תכולה); או שהתממש בו סיכון משמעותי. עוד נקבע כי יש לבצע תחקירים (שלא תוכננו מראש) במקרה של תקלה המשפיעה על רמת השירות או על נורמות האיכות. כמו כן, לשם השגת מטרות התחקור ניתן ומומלץ לבצע תחקירים גם במקרים נוספים כמצוין בהנחיות[47].

בשנת 2019 ערך מערך הדיגיטל הלאומי בקרה בנוגע ליישום הנחיות רשות התקשוב במשרד החוץ, שמטרותיה היו לבחון אם קיימת מתודולוגיה אגפית סדורה, אם היא תואמת להנחיות מערך הדיגיטל ואם היא מוטמעת בפרויקטים ובאגף. בבקרה עלה בין היתר כי חסרים נהלים העוסקים בפעילויות רוחביות, ובהם כאלה הנוגעים לניהול לקחים, שבהיעדרם לא מתקיימת הטמעת הידע והלקחים בארגון; לא מבוצעים תחקירים בפרויקטים משמעותיים; ואף כשבוצע תחקיר הוא לא התבצע לפי המתודולוגיה הממשלתית. כך למשל לא צוין מי האחראי להטמעת הלקחים ולא הוסברה הסיבה לכשל. בבקרה נוספת שביצע מערך הדיגיטל בשנת 2020 על יישום הנחיותיו, מובאת התייחסות משרד החוץ, וממנה עולה כי גיבוש נוהל תחקור והפקת לקחים נמצא בתוכנית העבודה של אגף התקשוב.

בביקורת הועלה כי בניגוד להנחיות מערך הדיגיטל לפיהן יש לבצע תהליכי תחקור והפקת לקחים לשם שיפור רציף ומתמיד ולצורך שחזור הצלחות ומניעת כישלונות, במשרד החוץ לא מתקיימים תהליכי תחקור והפקת לקחים לפרויקטים של פיתוח מערכות מידע באופן שגרתי, שיטתי וסדור. כך למשל, אף כשפרויקט משמעותי שמטרתו ניהול העבודה הדיפלומטית, שתוכנן כמערכת מרכזית לתמיכה בתהליכי שגרה וחירום נכשל, והתקבלה ההחלטה להפסיקו אחרי השקעה של יותר ממיליון ש"ח (לא כולל עלויות כוח אדם), לא בוצע תחקיר שבחן את סיבות השורש שהביאו לכישלון ושעמד על הלקחים הנדרשים כדי שכישלון כזה לא יישנה.

עוד הועלה כי נכון למרץ 2025, לא גיבש המשרד נוהל לביצוע תהליכי תחקיר והפקת לקחים לפרויקטים. זאת אף שכבר בשנת 2019 ציין כאמור מערך הדיגיטל במסגרת בקרה שביצע כי נוהל זה חסר. היעדר מנגנון תחקיר והפקת לקחים יוצר פער של ממש ביכולת משרד החוץ לזהות את

---

45 ראו במסמך ההנחיה 1.5.15, "ניהול לקחים - תחקור, הפקה והטמעת לקחים".

46 פרויקט גדול לפי סעיף 3.15 בהנחיה 1.4.01, "מחזור חיי מערכת תקשוב" הוא פרויקט שעלותו 2.5 מיליון ש"ח לפחות, או שהמאמץ הכרוך בו הוא שמונה שנות אדם לפחות.

47 ראו סעיף 5.1 (ב) בהנחיה 1.5.15, "ניהול לקחים - תחקור, הפקה והטמעת לקחים".

סיבות השורש לתקלות ולכשלים, ללמוד מטעויות ומהצלחות ולהטמיע שיפורים נדרשים בתהליכי ניהול הפרויקטים.

על משרד החוץ לקבוע נוהל סדור לביצוע תחקירים והפקת לקחים בהתבסס על הנחיות מערך הדיגיטל הלאומי ומתודולוגיות מקובלות, ולוודא את יישומו. כמו כן מומלץ למנות גורם ייעודי שתפקידו להוביל תהליכי תחקיר ולהבטיח את יישום הלקחים ברמה האגפית וברמת הפרויקט. נקיטת צעדים אלו תסייע להבטיח כי תהליכי התחקיר והפקת הלקחים יישמו בתהליכי העבודה.

סקרים ובקרה על פרויקטים

סקר מוגדר כפעילות לאורך חיי הפרויקט[48] לשם אימות אבן דרך או תוצר ביניים מבחינת שלמותו ואיכותו. ביצוע סקרים ובקרות איכות תקופתיות בפרויקט מאפשר לזהות בעיות או פגמים במערכת בשלב מוקדם, תוך הפחתת העלויות והזמן הנדרשים לתיקון; משפר את תהליכי הפיתוח כך שיהיו מועילים ויעילים יותר; מסייע לוודא שהמערכת עונה לדרישות הלקוח; מסייע בהבנת הסיכונים הקיימים בפרויקט ובהתמודדות עם בעיות אפשריות לפני שהן מתפתחות; ומספק שקיפות בתהליך הפיתוח, דבר המקנה למנהלים ולצוותים הבנה טובה יותר על מצבו הנוכחי של הפרויקט.

הנחיות מערך הדיגיטל הלאומי מחייבות כל משרד ממשלתי לבצע בקרות איכות תקופתיות בפרויקטים לפיתוח מערכות מידע[49] ולהגדיר במסגרת נוהלי העבודה היכן במחזור חיי המערכת יש לשלב שערי איכות[50] נוספים[51] וסקרים בפרויקט[52]. לפי ההנחיות[53], בכל שער איכות ובכל מפגש ועדת היגוי לפרויקט יש לתקף את תועלות הפרויקט וסיכוניו[54] ולהחליט לגבי המשך הפרויקט. עוד נקבע כי בשלב הייזום חובה להגדיר מדדי תפוקה ומדדים להצלחת הפרויקט[55].

בנוהל שגיבש משרד החוץ[56] נקבעו הפעולות והתוצרים הנדרשים כדי לבצע בקרה מועילה על אופן ניהול הפרויקט בהתאמה למתודולוגיית המשרד. בכלל זה נקבע כי בשערי זמן עקרוניים בפרויקט ייערכו סקרי ניהול ובקרה, ובהם לפחות סקרים של ייזום, אפיון-על, ניהול פרויקט, אפיון מפורט (לכל יחידת מסירה), עלייה לאוויר, העברה לתחזוקה והורדת מערכת, וסקרים נוספים בהתאם לצורך. גם בנהלים נוספים של המשרד הנוגעים ל"ייזום מערכת מידע"[57] ו"עלייה לאוויר מערכת מידע"[58] נקבע כי יבוצעו סקרי ייזום ועלייה לאוויר; בנהלים שעניינם "ייזום מערכת מידע"[59] ו-"ניהול פרויקט פיתוח מערכת מידע"[60] נקבע כי יוגדרו בפרויקט מדדי תפוקות ומדדי הצלחה למערכת.

---

48 סקרים נפוצים הם סקרי דרישות, סקרי תכנון, סקרי אפיון ועיצוב, סקרי מוכנות לבדיקות, סקרי סיכום בדיקות וסקרי מוכנות לעלייה לאוויר. ראו סעיף 6.3 בהנחיה 1.4.01, "מחזור חיי מערכת תקשוב".

49 ראו סעיף 5.13, 6.1 בהנחיה 1.4.01, "מחזור חיי מערכת תקשוב".

50 שער איכות בפרויקט - נקודת בקרה לאורך מחזור חיי המערכת, שבה נבדקת שלמות השלבים שהושלמו ומתקבלת החלטה לגבי המשך הפעילות (או עצירתה), או לגבי שינוי משמעותי באופי הפעילות. ראו סעיף 3.21 בהנחיה 1.4.01, "מחזור חיי מערכת תקשוב".

51 מעבר לאלה המוגדרים בהנחיה 1.4.01, "מחזור חיי מערכת תקשוב".

52 ראו סעיף 6.1 בהנחיה 1.4.01, "מחזור חיי מערכת תקשוב".

53 ראו סעיף 8.3 בהנחיה 1.4.9, "אמידה ובקרת עלויות במחזור חיי מערכת תקשוב".

54 יחד עם אומדן העלות.

55 בכל פרויקט רגיל שאינו הרחבת מערכת ובכל פרויקט מורכב. ראו סעיף 10 בהנחיה 1.4.02, "שלב הייזום ושער הכניסה לפרויקט תקשוב".

56 ראו נוהל 00-01-00, "בקרת מתודולוגיה פרויקט פיתוח".

57 ראו סעיף 3.3 בנוהל 00-01-01, "ייזום מערכת מידע".

58 ראו סעיף 3.3.1 בנוהל 00-05-01, "עלייה לאוויר מערכת מידע".

59 ראו סעיף 1.4 בנוהל 00-01-01, "ייזום מערכת מידע".

60 ראו סעיף 1.4.1 בנוהל 05-02-01, "ניהול פרויקט פיתוח מערכת מידע".

בביקורת נמצא כי בניגוד להנחיות מערך הדיגיטל ונוהלי המשרד לפיהן יש לבצע בקרות איכות תקופתיות בפרויקטים לפיתוח מערכות מידע, משרד החוץ אינו מבצע סקרים או שימוש במדדים כבקרה בפרויקטים של מערכות המידע. כמו כן לא נמצא תיעוד לקיום בקרות נוספות ברמה מספקת[61], כגון הערכת איכות התהליך ושלביו, בדיקות עמידה באמות מידה מקצועיות או בקרת שינויים. עוד עלה בביקורת כי אין גורם ייעודי שהוגדר כאחראי לבדיקות איכות תהליכי הפיתוח, כגון מנהל הבטחת איכות ו-PMO[62], למרות ההכרה בצורך זה. היעדר בקרה מספקת על תהליכי הפיתוח ואיכותם עלול לסכן את הצלחת הפרויקט ולגרום לתקלות תפקודיות, לחוויית משתמש ירודה, לחריגות בתקציב ובלוחות הזמנים ולפגיעה בתפקוד השוטף של יחידות המשרד ובשירות לאזרח.

יצוין כי פערים אלו עלו גם במסמך התוכנית האסטרטגית. צוין בו כי חסר יישום של מתודולוגיה וכלים לניהול ומעקב אחר מחזור חיי הפרויקט ואבני הדרך בשלבים השונים, וחסרים גאנטים[63] ובקרות וכן במסמך סקר הסיכונים שם אף צוין כי קיים סיכון לאיכות תוצרי פרויקטים גם בשל היעדר מעקב ביצוע.

לנוכח חשיבות ביצוע בקרות איכות תקופתיות להצלחה של פרויקטים לפיתוח מערכות מידע, על משרד החוץ לוודא שמתקיימים תהליכים של בקרה ובדיקות תקופתיות באופן שיטתי ויעיל על תהליכי פיתוח המערכות, לרבות קביעת מדדים וביצוע סקרים. כמו כן מומלץ למנות גורם ייעודי שיהיה אחראי לניהול בקרת האיכות. ביצוע בקרות כאמור יסייע להבטיח שהמוצר הסופי יהיה באיכות גבוהה, יעמוד בדרישות ויהיה בעל ערך ללקוחות.

ביצוע בדיקות בפיתוח מערכות מידע

בדיקות פיתוח במערכות מידע הן שלב קריטי בתהליך הפיתוח, שכן הן מסייעות לאתר בעיות או תקלות בתפקוד המערכת, מאפשרות לוודא שהמערכת תתפקד כראוי עוד לפני הפצתה למשתמשים ותענה על דרישות המשתמשים ומסייעות להבטיח שהיא מוגנת בהיבטי אבטחת מידע.

הנחיות מערך הדיגיטל הלאומי קובעות כי כתנאי לעלייה לאוויר בכל פרויקט, יאושר על ידי הגורמים המקצועיים גמר ביצוע הבדיקות[64], כולל בדיקות שפיות ושלמות[65], בדיקות מסירה[66] ובדיקות קבלה[67]. עוד נקבע בהנחיות כי חובה לבצע בדיקות טרם התקנת מערכת המידע וגם אחרי

---

61 מלבד ביצוע (בחלק מהמקרים) של הבדיקות הפונקציונליות (QC - Quality Check), שתפקידן לבדוק את הפעולות והלוגיקה של התוכנה ולוודא שההתנהגות בהתאם לדרישות העסקיות. בדיקות אלה מבוצעות על ידי מחלקת QA שבאגף התקשוב.

62 תפקידו לפי מילון המונחים של מערך הדיגיטל הלאומי: אחראי לתכנון, לבקרה ולמתודולוגיות של פונקציית ניהול הפרויקטים בארגון או ביחידה עסקית. עוסק בפיתוח ויישום פתרונות וכלים בתחום תכנון ובקרת פרויקטים, פיתוח, הטמעה ושיפור של תהליכי ניהול פרויקטים, התאמה והטמעה של כלים לניהול פרויקטים ובקרתם, ליווי מנהלי הפרויקטים, בניית תוכניות עבודה ובחינת תכנון מול ביצוע. ראו בקישור: www.gov.il/he/departments/dynamiccollectors/glossary-of-terms-government-ict-authority

63 תרשימים המשמשים בפרויקטים לתיאור פעילויות עם הקשרים ביניהן וציון הזמן של כל אחת מהפעילויות.

64 ראו סעיף 4.1 וסעיף 7 בהנחיה 1.4.07, "שער עלייה לאוויר בפרויקט תקשוב".

65 הגדרה בנוהל מפת"ח: בחינת מוכנות גרסה לתחילת סבב בדיקות חדש, תקינות בסיסית של מערכת לאחר התקנתה (בסביבת הבדיקות או באתר הייצור), בדיקת מוכנות סביבת הבדיקות עצמה.

66 הגדרה בנוהל מפת"ח: בדיקות מסירה של מערכת המפותחת על ידי גורם חיצוני - Factory Acceptance Test. זוהי הבדיקה הסופית והאחרונה לפני בדיקות הקבלה אשר מבוצעות על ידי הלקוח.

67 הגדרה בנוהל מפת"ח: בדיקות קבלה מבוצעות על ידי הלקוח ונציגיו (משתמשי קצה) לאחר סיום מוצלח של בדיקות המערכת. מטרתן לוודא התאמת המערכת לצרכים (Validation) ולדרישות שהוגדרו במשימת הפרויקט.

התקנתה[68], וכן נקבע כי היחידה העסקית[69] והוועדה העסקית[70] נדרשות להיות מעורבות בבדיקות ובבדיקות הקבלה[71]. בהנחיות אף נקבע[72] כי "תיעוד, איכות ובקרת תוצרים ונתונים" בהיבט הטכנולוגי הם נושאי חובה במתודולוגיה סדורה, שעל כל משרד ממשלתי לעבוד לפיה[73].

במשרד החוץ הוטמע נוהל שבו נקבע כי לקראת המעבר לסביבת הייצור יש לוודא כי בוצעו כל הפעולות והבדיקות כדי לאפשר פעולה תקינה של המערכת[74], וכן נדרש אישור על סיום הבדיקות לקראת עלייה לאוויר[75] ואישורי בדיקות קבלה, גמר בדיקות ובדיקת שפיות ושלמות.

בביקורת הועלה כי משרד החוץ לא ביצע את כלל הבדיקות הנדרשות בתהליך הפיתוח. זאת על אף הנחיות מערך הדיגיטל ונוהל משרד החוץ בנושא לפיהן יש חובה לבצע בדיקות טרם התקנת מערכת מידע. עוד עלה שלא מבוצעות בדיקות לא פונקציונליות[76] - כגון בדיקות מאמץ, עומס, ביצועים, תאימות והתאוששות - לפני העלאת מערכת או רכיב חדש לאוויר, כפי שמקובל בכל מתודולוגיה מקובלת בתחום[77]. הפערים בביצוע הבדיקות חושפים את משרד החוץ לסיכונים ניכרים, ובהם אי-איתור בעיות קריטיות בתהליך הפיתוח, ריבוי תקלות בתפקוד המערכות, פגיעה בזמינות השירותים, עיכובים בהעלאת המערכות, הוצאות כספיות חריגות לשם תיקונים מאוחרים וחשש לקריסת מערכות בשל עומסים.

משרד החוץ מסר בתשובתו מאוקטובר 2025 כי מחסור במשאבי בדיקות אינו מאפשר כיסוי לכלל הפרויקטים, וכי בכל הקשור לעלות-תועלת, נכון לתעל את משאבי הבדיקות לבדיקות הפונקציונליות.

על משרד החוץ להבטיח את ביצוען של כל הבדיקות הנדרשות לפי הנחיות מערך הדיגיטל ונוהלי משרד החוץ בשלבים הנדרשים וטרם העברת המערכת למשתמשים, תוך הקפדה על תיעוד נאות של תוצאות הבדיקות. ביצוע הבדיקות כאמור חיוני להבטחת איכות המערכת ושמירה על תפקוד נכון ויעיל שלה, תוך מניעת בעיות עתידיות ועמידה בדרישות הלקוח.

פיתוח מערכת מידע מסוימת

במסגרת בחינת פיתוח וניהול הפרויקטים במשרד החוץ, ביצע משרד מבקר המדינה בחינה ספציפית בנוגע לפיתוח אחת ממערכות המידע במשרד החוץ - להלן הפרטים.

מערכת המידע הקונסולרית של משרד החוץ פותחה בשנת 2002 לצורך מתן שירותים קונסולריים במטה בישראל ובנציגויות ישראל ברחבי העולם. בין השירותים הניתנים באמצעות המערכת: הנפקת מסמכי נסיעה ואשרות, סיוע לאזרחים במצוקה, שירותים נוטריוניים, רישומי מעמד אישי, טיפול בעצורים ואסירים ישראלים בחו"ל ועוד.

---

68 ראו סעיף 6.2 בהנחיה 1.4.07, "שער עלייה לאוויר בפרויקט תקשוב".

69 ראו סעיף 3.23.10 בהנחיה 1.4.01, "מחזור חיי מערכת תקשוב" - היחידה המשרדית הנושאת באחריות הכוללת לפרויקט בשיתוף עם יחידת התקשוב, אמונה על ריכוז דרישות משתמשי המערכת, על בדיקות הקבלה ועל שלב ההטמעה.

70 ראו סעיף 3.23.1 בהנחיה 1.4.01, "מחזור חיי מערכת תקשוב" - הגוף המייצג של לקוחות המערכת, ולה הסמכות לקבל החלטות הנוגעות לדרישות פונקציונליות במערכת.

71 ראו סעיף 3.23.1 וסעיף 3.23.10 בהנחיה 1.4.01, "מחזור חיי מערכת תקשוב".

72 ראו סעיף 5.3 בהנחיה 1.1.01, "מסגרת מתודולוגיית תקשוב ממשלתית".

73 ראו סעיף 9.4 בהנחיה 1.1.01, "מסגרת מתודולוגיית תקשוב ממשלתית".

74 ראו סעיף 2 בנוהל 00-05-01 "עלייה לאוויר מערכת מידע".

75 ראו סעיף 3.3.3 בנוהל 00-05-01 "עלייה לאוויר מערכת מידע".

76 NFT (Non-Functional Tests) - בדיקות שלא עוסקות בפונקציונליות הישירה של המערכת, לעומת בדיקות פונקציונליות שבודקות את הפעולות והלוגיקה של התוכנה כדי לוודא שהיא מתנהגת בהתאם לדרישות העסקיות.

77 ראו למשל סוגי הבדיקות בנוהל מפת"ח בקישור: www.methoda.cloud/?section=254. יצוין כי גם במסמך התוכנית האסטרטגית עלה כי לא כל הפיתוחים עוברים בדיקות "בצורה מקיפה".

בשנת 2015 עלה הצורך להחליף את מערכת המידע. באותה העת, ממוצע השימוש במערכת היה כ-1,000 פעמים מדי יממה, במעל 100 נציגויות ישראל ברחבי העולם, עם מאות משתמשים פעילים בנציגויות ועשרות משתמשים פעילים באגף הקונסולרי במטה המשרד בארץ.

מטרת החלפת המערכת הייתה מעבר לתשתית וטכנולוגיה מתקדמות, עיצוב מודרני, שיפור ושדרוג השיטה, הוספת תהליכים שלא קיימים, שיפור השירות הקונסולרי ושיפור יכולות הפיקוח והבקרה. לשם כך הוחלט על הקמת מערכת חדשה, שתפעל בטכנולוגיה מתקדמת ותכלול את כל הפונקציונליות הקיימת ומודולים[78] נוספים בנושאים שלעיל. הפיתוח פוצל למודולים שונים בהתאם לתחומי הפעילות של המערכת, ותוכנן כך שכל מודול יועלה בנפרד לאחר סיום פיתוחו, כאשר הפונקציונליות תהיה מפוצלת בין שתי המערכות בהתאם להתקדמות, ושתי המערכות יתקיימו במקביל עד לתום פיתוח המערכת החדשה.

פיתוח המערכת, שנועדה להחליף מערכת מסוימת למתן השירותים הקונסולריים בישראל ובנציגויות המשרד ברחבי העולם, לניהול הקשר עם אזרחי ישראל השוהים בחו"ל ולשיפור השירות הקונסולרי נתקל בקשיים ניכרים, כפי שיפורט להלן.

1. **חריגה בלוחות הזמנים:** במסמכי הפרויקט משנת 2015 צוין כי פיתוח כל המערכת מתוכנן להסתיים ברבעון הראשון של שנת 2018. במסמך בנושא משנת 2021, צוין שהפרויקט היה אמור להסתיים בשנת 2019, ושבדיעבד עולה "שהערכת הזמנים וההשקעה בעת תכנון הפרויקט לקתה בחסר", ומוערך כי ידרשו עוד שש שנות פיתוח כדי לסיים את הפרויקט, כאשר ההערכה הראשונית של משך פיתוח השלב הראשון היא כשלוש שנים וחצי.

ביולי 2024 התכנסה לראשונה ועדת היגוי קונסולרית. במסמך סיכום ועדת ההיגוי צוין כי נכון לכוח האדם הקיים, הצפי לסיום העברת התכולה למערכת הוא שנת 2034, קרי חריגה של כ-15 שנה מהמועד שתוכנן לכתחילה, והוצגו שתי חלופות לקידום הפרויקט: האחת - פיתוח חיצוני על ידי מכרז פומבי לשם סיום הפרויקט, השנייה - עיבוי הצוות הקיים תוך ביצוע פיתוחים ייעודיים חיצוניים. בסיכום הדיון הוחלט לבחון את החלופות לשם סיום הפיתוח עד סוף 2027.

בדיון נוסף שהתקיים בוועדת ההיגוי בסוף יולי 2024 הוחלט כי החלופה העדיפה היא ביצוע פיתוח חיצוני על ידי מכרז פומבי. צוין כי פתרון זה נבחר בשל עלויות נמוכות יותר ולוחות זמנים קצרים יותר ליישום.

בבירור שקיים משרד מבקר המדינה בפברואר 2025 עם מנהלת חטיבת היישומים באגף התקשוב עלה כי בשל הקושי להכניס גוף חיצוני להליכי הפיתוח, לרבות בהיבטי קבלת האחריות לפיתוח והמודולים שפותחו עד כה, נכון למועד זה מסתמן שלא יצאו למכרז חיצוני אלא יגייסו כוח אדם ייעודי לטובת הנושא. זאת בשאיפה שגמר הפיתוח יהיה כשלוש שנים לאחר ביצוע חפיפה (2028 - 2029). באוגוסט 2025 נמסר בהקשר זה כי גיוס כל כוח האדם הייעודי לפרויקט צפוי להמשך לפחות עד לסוף שנת 2025 וכי אין שינוי בהערכת המועד הצפוי לגמר הפיתוח.

עולה אפוא כי התכנון העדכני של פרויקט זה (המגלם אף הוא סיכוני יישום) משקף פיגור של כעשר שנים למול התכנון המקורי. כמו כן, לאור העיכוב, שתי המערכות, ימשיכו להתקיים במקביל עד לסיום פיתוח המערכת החדשה.

---

78 מוֹדוּל - חלק של תוכנית שפותח כך שיהיה נבדל או בר זיהוי בכל הקשור לפעולות כגון הידור, כריכה או ביצוע ושעשוי להדד עם תוכניות אחרות או עם חלקים אחרים של אותה תוכנית. ראו במילון שפות תכנות [טכנולוגיית המידע] (התשע"ה) באתר האקדמיה ללשון העברית.

2. **צמצום בתכולות הפרויקט:** "הגדרת התכולה" היא התהליך שבו מפורטים רכיביו השונים של הפרויקט ושל המוצר. תהליך זה הוא אבן היסוד להצלחת הפרויקט כיוון שעליו יישען רוב תהליך התכנון. תיאור הרכיבים נועד למעשה לבסס הבנה בין כל הצדדים בפרויקט והסכמה לגבי הנדרש לביצוע.

ניהול תכולת הפרויקט הוא טיפול בכל התהליכים הדרושים להבטיח שהפרויקט יקיף את כל העבודה הדרושה, ורק את העבודה הדרושה, כדי לסיים את הפרויקט בהצלחה. זהו אחד הנושאים החשובים בביצוע כל פרויקט. יש לטפל בו לאורך כל מחזור חיי הפרויקט, החל בשלב הייזום, המשך בביצוע וכלה באישור תוצרי הפרויקט[79].

המערכת החדשה יועדה לכלול כאמור גם פיתוחים חדשים, ובהם קשר עם מקבלי השירות ושיפור יכולות הפיקוח והבקרה על הפעילויות במטה ברמה גלובלית ובכל נציגות ברמה מקומית[80]. נוכח העיכובים הרבים בהתקדמות הפיתוח, הוחלט בשנת 2021 לוותר על פיתוח המודולים בעלי הפונקציונליות החדשה שתוכננה ולהתמקד בפיתוח מודולים שיחליפו מודולים הקיימים במערכת הישנה בלבד, ללא פונקציונליות נוספת.

הועלה כי נכון ליולי 2024, כחמש שנים לאחר המועד המתוכנן לסיום הפרויקט, פותחו כמחצית מהמודולים המתוכננים (53% מתוך התכולה שנותרה לאחר קיצוץ התכולה הראשונית) ושיעור התכולה שנותרה לפיתוח היה 47%.

3. **חריגה בתקציב:** אף שהפיתוח תוכנן להסתיים ב-2019, הועלה כאמור כי חלו עיכובים ניכרים בלוחות הזמנים ובתכולות שעוד נותרו לביצוע. כמו כן המשך פיתוח הפרויקט הוערך בסיכומי ועדת ההיגוי הקונסולרית ביולי 2024 בכ-12 - 18 מיליון ש"ח. בירור שעשה משרד מבקר המדינה עם משרד החוץ כדי לאמוד את עלויות הפרויקט עד לאותו מועד העלה כי היות שהצוותים עובדים על כמה פרויקטים במקביל, אין למשרד החוץ דרך לגזור עלויות לפרויקט מסוים.

פיתוח הפרויקט תוכנן מלכתחילה להסתיים בשנת 2019. לנוכח העובדה שבשנים 2019 - 2024 עסקו בפיתוח הפרויקט שניים עד ארבעה עובדים, ניתן להעריך שבפיתוח הפרויקט הושקע בתקופה זו תקציב משמעותי נוסף מעבר לזה שתוכנן. כמו כן, הועלה כי נדרשת תוספת תקציב ניכרת של 12 - 18 מיליון ש"ח לשם הבאת הפרויקט לידי גמר.

מערכת זו נועדה להחליף מערכת מסוימת ולהביא לשיפור השירות הקונסולרי. מכל האמור עולה כי פיתוח המערכת נתקל בקשיים ניכרים, ובכלל זה חריגות גדולות בכל שלושת מדדי הביצוע העיקריים של הפרויקט - חריגה בלוחות הזמנים, חריגה בתקציב וצמצום בתכולות הפרויקט: 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. עלה כי היות שהצוותים עובדים על כמה פרויקטים במקביל, אין למשרד החוץ דרך לגזור עלויות לפרויקט מסוים וכי 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 של 12 - 18 מיליון ש"ח, כדי להביאו לידי גמר; זאת ועוד, נכון ליולי 2024, חמש שנים לאחר המועד המקורי לסיום הפרויקט, בוצעה רק כמחצית התכולה הנדרשת ברמת הפיתוח (53%), ואף זאת לאחר שהוחלט על צמצום התכולות שתוכננו מלכתחילה.

---

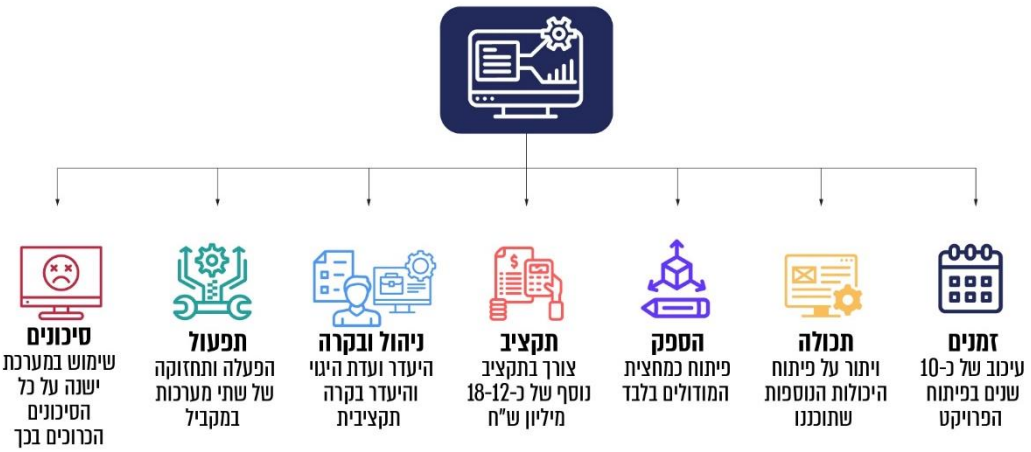
79 שלמה גלוברזון ואבי שטוב, **ניהול פרויקטים - תכנון ביצוע ובקרה** (2006).

80 יכולות אלו כללו גם אפשרות הצגה, מעקב והתרעות בכל הקשור לביצועי המערכת והמשתמשים בה, ניהול מדדי ביצועים מרכזיים, הצגה גרפית, מתן כלים בידי ההנהלה להסקת תובנות עסקיות לשיפור תהליכי העבודה העסקיים של האגף ונוהלי העבודה במערכת. לדוגמה: הוספת נציג דיגיטלי ומוקדי שירות, זימון וניהול תורים, תהליכים מונחים והדרכה מוטמעת, בקרות מול מדדי איכות, מדדי איכות לזמן תגובה ועוד.

הועלה כי לעיכוב בפיתוח המערכת והמשך השימוש במערכת הקונסולרית הישנה השלכות וסיכונים. לנוכח העובדה שפותחו רק כמחצית מהמודולים המתוכננים, אגף התקשוב מפעיל זה כמה שנים את המערכת הקונסולרית הישנה במקביל למערכת החדשה, והוא נדרש לתת שירותי תמיכה ותחזוקה לשתי המערכות.

זאת ועוד, הביקורת העלתה כי על אף הקשיים והעיכובים המהותיים שחלו בקידום הפרויקט ועל אף הסיכונים הממשיים וההשלכות שיש לאי-קידומו, הפרויקט פעל כתשע שנים ללא ועדת היגוי ייעודית - ועדת היגוי לפרויקט הוקמה רק בשנת 2024. ביולי 2024 קיימה ועדת ההיגוי שני דיונים והתקבלו החלטות בעניינו, אולם נכון למרץ 2025, ועדת ההיגוי הקונסולרית לא התכנסה פעם נוספת מאז יולי 2024 כדי לעקוב אחר התקדמות הפרויקט וכדי להבטיח כי הצעדים הנדרשים לשם יישומו אכן ננקטים.

תרשים 5 : **פערים עיקריים בפרויקט מסוים**



על פי נתוני משרד החוץ, בעיבוד משרד מבקר המדינה.

על ועדת ההיגוי הייעודית של הפרויקט 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.

הממצאים האמורים שהועלו בנוגע לפרויקט פיתוח מערכת זו ממחישים את הצורך בהטמעת מתודולוגיות ותהליכים של ניהול סיכונים בפרויקטים המנוהלים במשרד החוץ, לצד חיזוק של כלי הבקרה והפיקוח. כמו כן, מומלץ כי מנכ"ל המשרד יבצע תהליך הפקת לקחים מפרויקט זה לשם למידה מטעויות והימנעות מחזרה עליהן. צעדים אלה נדרשים כדי להבטיח כי ניהול הפרויקטים במשרד ייעשה בצורה מיטבית ומתודולוגית ובאופן שיסייע בהגדלת סיכויי הצלחת הפרויקטים והגשמת יעדיהם.

תוכנית התאוששות מאסון

תוכנית התאוששות מאסון (להלן - תוכנית DRP[81]) היא תוכנית הכוללת מדיניות, נהלים ותהליכים המשמשים להתאוששות מאסון או מאירוע חמור, המשבית לזמן לא קצר את המערכים הטכנולוגיים של הארגון. תוכנית זו היא מרכיב קריטי בהבטחת הרציפות התפקודית בחירום. הדרישה להכנת תוכנית DRP היא פרקטיקה מקובלת, הנכללת בהנחיות מערך הדיגיטל וכן בכל הסטנדרטים הרלוונטיים, ובכללם NIST, COBIT והתקנים ISO 27301 ו-ISO 27031.

חלק מהיישום של תוכנית ההתאוששות מאסון מתייחס לרכש ותחזוקה של תשתיות המיועדות לתמוך ולאפשר את ההתאוששות של הארגון בחירום. אתר גיבוי והתאוששות מאסון (להלן - אתר DR) הוא חוות שרתים משנית, המשמשת לגיבוי ואישוש תכולות האתר הראשי[82] ומספקת שירותים חיוניים בעת חירום או תקלה בחוות השרתים הראשית[83]. היעדר אתר גיבוי עלול לגרום להשלכות חמורות במקרה של כשל או אסון, כגון אובדן מידע קריטי, השבתה ממושכת של מערכות ושירותים ופגיעה באמינות הארגון ובמוניטין שלו.

כלל מערכות המידע של משרד החוץ מופעלות מחוות השרתים הראשית של משרד החוץ. חווה זו פועלת באופן מלא מפברואר 2023. במועד זה השלים המשרד את העברת חוות השרתים הראשית לחוות שרתים מודרנית. נוסף על כך, למשרד אתר DR, שאליו מגובות מערכות המידע הפועלות ברשתות השונות של המשרד.

בשנת 2024 החל משרד החוץ בהיערכות להכנת תוכנית התאוששות מאסון, ושכר לשם כך חברה חיצונית אשר ביצעה תהליך BIA[84] להערכת השפעת התממשות תרחישי הייחוס השונים על התהליכים העסקיים הקריטיים של המשרד. כמו כן שכר המשרד חברה נוספת, שתכין עבורו תוכנית להתאוששות מאסון.

מאחר שפעולות אלה משקפות תכנון עתידי רב שנתי, בחן משרד מבקר המדינה את מצב הדברים כפי שהוא היום ושבהכרח יהיה רלוונטי לשנים הקרובות, עוד טרם יישום תכנון זה. במסגרת זו בחן משרד מבקר המדינה האם במשרד החוץ קיימת תוכנית DRP מעודכנת וכן עמד על איכות המענה הניתן כיום להתאוששות מאסון במשרד החוץ, בהתאם להנחיות מערך הדיגיטל והפרקטיקה המקובלת. להלן ממצאי הבדיקה.

---

81 Disaster Recovery Plan

82 אתר ראשי - אתר (או אתרים) המשמשים ומכילים בעת שגרה את תשתיות המחשוב, מערכות המידע, האחסון ומרכז הבקרה והניהול של האגף.

83 מערך הדיגיטל הלאומי, מילון מונחים בתחום התקשוב.

84 BIA - Business Impact Analysis: ניתוח וחיזוי של השלכות עסקיות ותפקודיות הנוגעות להפסקה או לשיבוש של פעילויות במצב חירום.

לוח 1 : **ממצאים בנוגע לתוכנית ה-DRP במשרד החוץ ולאיכות המענה הקיים באתר ה-DR**

הנושא	ההנחיות	הממצאים
קיום תוכנית DRP ועדכניותה	יש לוודא כי קיימת במשרד תוכנית התאוששות מאסון (DRP) מעודכנת. התוכנית צריכה להיבחן לפחות אחת לשנה וכן בעת שינויים משמעותיים בתרחישי הייחוס, בסיכונים ובתשתיות ובמערכות המידע.	**יישום של תוכנית התאוששות מאסון כולל בין היתר, רכש תשתיות והיערכות מקדימה ונרחבת. נמצא כי במשרד קיימת תוכנית DRP ישנה משנת 2011, שעודכנה לאחרונה ב-2016 (להלן - התוכנית הישנה). לדברי המשרד תוכנית זו לא יושמה בהיעדר תקציב.** במאי 2022, כחלק מההיערכות להכנת תוכנית DRP, הוכן אפיון-על לשרידות שירותי התקשוב (להלן - מסמך האפיון לשרידות). עם זאת, **נכון לספטמבר 2024, לא חלה התקדמות בנושא. נוכח זאת, התוכנית הישנה שעודכנה לאחרונה לפני כעשור, בשנת 2016, עודנה בתוקף, אף כי חלק ניכר מהנתונים שבה אינם עדכניים על כל המשמעויות שיש לדבר.**
איום ייחוס ותרחישי ייחוס	זיהוי ומיפוי תרחישי ייחוס שיכללו, לכל הפחות, התייחסות למשבר תקשובי (כגון אובדן או קריסה של מערכות מידע, קריסת תשתיות, פגיעת סייבר, קריסת תקשורת); למשבר מדינתי או גלובלי (כגון מלחמה, רעידת אדמה ומגפה); למשבר תפעולי ועסקי הפוגע בתחום העיסוק הספציפי של המשרד.	**התוכנית הישנה אינה מתייחסת לתרחיש ייחוס משמעותי. כך גם אין בתוכנית מענה לתרחיש קלאסי כדוגמת רעידת אדמה.**

הנושא	ההנחיות	הממצאים
רשימת מערכות מידע קריטיות בתוכנית ה-DRP	התוכנית תכלול את רשימת מערכות המידע המאפשרות את קיום התהליכים העסקיים הקריטיים.	רשימת המערכות הקריטיות עודכנה במסגרת תהליך ה-BIA, שאגף התקשוב ביצע בשנת 2024.
זיהוי תרחישי סיכון והערכת השפעה על התהליכים העסקיים הקריטיים	כבסיס להכנת תוכנית DRP, יש לקיים תהליך BIA להערכת השפעת התממשות תרחישי הייחוס השונים על התהליכים העסקיים הקריטיים של המשרד.	בשנת 2024 ביצע אגף התקשוב תהליך של מיפוי נכסים וניתוח מובנה של התהליכים העסקיים הקריטיים וההשפעות העסקיות להתממשות תרחישי הייחוס.
קביעת מדדי / יעדי התאוששות	התוכנית תכלול לכל מערכת קריטית הגדרה של RPO[85] ו-RTO[86].	במסגרת הכנת ה-BIA הוכנו מדדי התאוששות למערכות הקריטיות. בספטמבר 2024 דנה בנושא ועדת ההיגוי להגנת הסייבר וקיבלה החלטות בנוגע למדדים האמורים.

[85] RPO - Recovery Point Objective - מתייחסת לחישוב של כמה אובדן נתונים ארגון יכול לחוות, לפני שמתרחש נזק משמעותי, מנקודת האירוע המשבש ועד לגיבוי הנתונים האחרון. RPO עוזרת לקבוע כמה אובדן נתונים הארגון יכול לסבול במהלך אירוע בלתי צפוי.

[86] RTO - Recovery Time Objective - טווח הזמן הנדרש להפעלה מחדש של הפעילות העסקית. מתייחס לפרק הזמן שבו אפליקציה, מערכת ותהליך יכולים להיות מושבתים מבלי לגרום נזק משמעותי לעסק ולזמן המושקע בשחזור האפליקציה והנתונים שלה עד לחידוש הפעילות העסקית הרגילה לאחר אירוע משמעותי.

הנושא	ההנחיות	הממצאים
יכולת המשרד לעמוד ביעדי התאוששות שנקבעו על ידו	אתר ה-DR יכיל תשתיות המאפשרות את מימוש תוכנית ה-DRP, כולל עמידה ביעדי ההתאוששות שנקבעו.	**ה-RTO שאושר כיעד למערכות מסוימות על ידי הנהלת המשרד - עדיין אינו בר השגה.**
רשימת הספקים	בתוכנית יפורטו הספקים הקריטיים ודרכי הקשר עימם.	התוכנית הישנה כוללת פרטים בנוגע לתשעה ספקים וגורמים חיצוניים. **בבדיקה שעשה משרד מבקר המדינה בפברואר 2025 נמצא כי אנשי קשר של חברות וגורמים חשובים נוספים, שייתכן שיידרשו בעת חירום, אינם מפורטים בתוכנית. כמו כן, אנשי הקשר של ארבע מהחברות כבר אינם עובדים בחברה שמצוינת בתוכנית, או שעברו לתחום פעילות אחר בחברה, ולפיכך אינם רלוונטיים. כמו כן, בשתי חברות נוספות המופיעות בתוכנית הישנה אין פירוט של אמצעי הקשר או אנשי הקשר שאיתם ניתן ליצור קשר.** **משכך, בעת אסון, ללא פרטים עדכניים של החברות והגורמים החיצוניים שנדרשים לסייע למשרד ואנשי הקשר שלהם, תהליך איתור הגופים הנדרשים לסיוע ומציאת אנשי הקשר הרלוונטיים בכל גוף יארך זמן יקר, אשר עלול לעכב את תהליך ההתאוששות ולפגוע בו עד כדי אי-עמידה ביעדי ההתאוששות.**
רשימת השרתים המגובים	על מנת לעמוד בהנחיות הנוגעות לאתר ה-DR, התוכנית תכלול את רשימת השרתים המגובים לאתר ה-DR ואת תהליך שחזורם באתר.	**התוכנית הישנה מפרטת את מערכות המידע ברשתות המשרד השונות באתר ה-DR, אך אינה כוללת את כתובות ה-IP של השרתים ואת שמות השרתים באחת הרשתות וכן את תהליך וסדר שחזורם באתר. עוד יצוין כי אין התאמה בין השרתים המפורטים בנוהל לבין השרתים הקיימים כיום בפועל.**

הנושא	ההנחיות	הממצאים
צוותים לשעת חירום	יש להגדיר צוותי עבודה לעת חירום לתמיכה במעבר ל-DR ולתפעול האתר בעת חירום. האגף יתקף את רשימות האיוש אחת לשנה.	**נמצא כי רשימת צוותי העבודה בתוכנית לשעת חירום אינה מעודכנת.** התוכנית הישנה כוללת פירוט של בעלי תפקידים מרכזיים והגדרה של צוותי עבודה בחירום, כולל פירוט התפקידים של כל צוות בחירום. **עם זאת, התוכנית אינה כוללת פירוט של בעלי התפקידים בכל צוות. כמו כן, בבדיקה נקודתית שביצע משרד מבקר המדינה נמצא כי ראש צוות ניהול המשבר המוזכר בתוכנית סיים את תפקידו במשרד לפני כשלוש שנים.**
בדיקות ותרגול תוכנית ה-DR	קיום תרגילי DR תקופתיים (לפחות אחת לשנה עד שנתיים); תיעוד מלא של התוצאות ושיפור נהלים בהתאם.	**נציגי אגף התקשוב מסרו למשרד מבקר המדינה בספטמבר 2024 שהתוכנית הישנה לא תורגלה ולא נבדקה, למעט תרגול נקודתי של מערכת הדוא"ל.**
משילות	אחת לשנה לפחות, או בעת שינוי מהותי, האגף יבחן את תרחישי הייחוס, יעדי השירות בעת חירום, ניהול הסיכונים ואת התוכנית להמשכיות עסקית ותפקודית, ויציג את מסקנותיו לדיון ואישור הנהלת המשרד.	**ב-2016 עודכנה לאחרונה התוכנית הישנה. לא נמצא כי הנושא עלה לדיון בהנהלת המשרד או בוועדת ההיגוי מאז, למעט הדיון שהתקיים בספטמבר 2024 בנוגע למסמך ה-BIA.**

הנושא	ההנחיות	הממצאים
זמינות התוכנית ונוהלי השחזור באתר ה-DR	בהיעדר גישה לאתר המשרד או לחוות השרתים שלו, נדרש לייצר שחזור מאפס באתר החלופי. לפיכך, על מנת בדרישה לעיל, יש לשמור עותק פיזי או דיגיטלי של תוכנית ה-DR ונוהלי השחזור גם באתר ה-DR כדי שהמידע הבסיסי להתחלת תפעול האתר ותהליכי השחזור וההתאוששות יהיה זמין לצוותי החירום.	**בסיור שקיים משרד מבקר המדינה באתר ה-DR בינואר 2025 נמצא כי באתר אין עותק פיזי או דיגיטלי של התוכנית הישנה ואין כל מסמך נוסף היכול לסייע בתהליכי שחזור והתאוששות של המערכות הקריטיות בחירום. כך, במקרה של אי-יכולת הגעה פיזית למשרד הראשי בירושלים, המידע החיוני להתחלת תפעול האתר ולתהליכי השחזור וההתאוששות לא יהיה זמין לצוותי החירום.**

מכל האמור עולה כי נכון לספטמבר 2024 ישנם פערים של ממש ביכולתו של משרד החוץ להתאושש מאסון. בכלל זה הועלה כי:

1. **אין למשרד תוכנית DRP מעודכנת, סדורה ותקפה להתאוששות מאסון.**

2. **תרחיש הייחוס שהוגדר למשרד אינו מתייחס לתרחיש משמעותי וכן למקרה של אירוע חירום כגון רעידת אדמה.**

3. **בהיעדר נוהלי שחזור זמינים באתר ה-DR, לא תהיה למשרד אפשרות לאושש את מערכות המידע שלו. זאת גם אם הגיבויים יבוצעו כיאות ויישמרו בו כראוי.**

4. **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. בהיעדר תרגול ובחינה של יכולת המשרד לאושש את מערכות המידע ותשתיות התקשוב מאסון, אין כל ביטחון שהמשרד יוכל לממש זאת במצב חירום אמיתי.**

באוקטובר 2025 מסר משרד החוץ בתשובתו למשרד מבקר המדינה כי המשרד מבצע העתקה קבועה של כלל הנתונים ברשתות המשרד באופן קבוע וכי כלל המידע נשמר באתר ה-DR על בסיס קבוע באמצעות רפליקציה[87]. המשרד הוסיף כי כדי להביא את האתר ליכולת התאוששות בהתאם למדדים שאושרו בוועדת ההיגוי להגנת הסייבר, נדרשת השקעה משמעותית שעד כה לא התאפשרה. המשרד הוסיף כי הוא נמצא בעיצומו של תהליך בניית מערך DR לרשת נוספת, וכי

[87] תהליך שבו נתונים משוכפלים ומועתקים ממערכת אחת לאחרת, לרוב בזמן אמת או כמעט בזמן אמת.

במסגרת תהליך זה נקבע איום ייחוס של אי-זמינות מלאה של מערכות המחשב במטה ובחדר מחשב. עוד הדגיש כי התוכנית היא להמשיך פריסה בהתאם לתקציב וכוח אדם ובהתאם לתיעדוף המשרד.

כדי להבטיח את הרציפות התפקודית של משרד החוץ, על משרד החוץ להגדיר פעולות שעליו לנקוט כדי להבטיח את התאוששות מערכות המידע הקריטיות באתר ה-DR בהתאם למדדי ההתאוששות שאישרה הנהלת המשרד בספטמבר 2024 - ולייישם. 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 המידע הקריטיות והקמתן באתר זה.

כמו כן, מומלץ כי המשרד ייתן דעתו לכך שתרחיש הייחוס שהוגדר למשרד אינו מתייחס לתרחיש ייחוס משמעותי ורלוונטי, ויבחן אם יש צורך בעדכון תרחיש ייחוס זה.

גיבויים והתאוששות נתונים

תהליכי גיבוי של נתונים ומערכות מידע מיועדים לשחזור המידע או המערכת בהתרחש אסון שבו נפגעת חוות השרתים או אין גישה אליה, או בהתרחש מקרים שבהם המידע כולו או חלקו נמחק או הושחת. לפיכך תהליכי הגיבוי צריכים לכלול גם תהליכי שחזור סדורים, שיבטיחו את יכולת השחזור המלאה של המידע בעת הצורך.

על פי הנחיות מערך הדיגיטל, על האגף לקבוע נהלים לגיבוי נתונים, שיפרטו את תהליכי הגיבוי ותדירות הגיבוי לכל אחת ממערכות המידע ואת אופן הטיפול בגיבויים. בכלל זה נקבע בהנחיות כי כדי להתמודד עם מתקפת כופרה, על המשרד לגבות את נכסי המידע בגיבוי קר (Offline) על גבי קלטות המאוחסנות באתר חיצוני ומרוחק, בכספת חסינת אש, כולל בקרת גישה, או באמצעות פתרונות טכנולוגיים או פתרונות אחרים השומרים על המידע ברמת Read Only.

עוד נקבע בהנחיות מערך הדיגיטל כי בדיקת תקינות שחזור תבוצע לפחות אחת לחצי שנה, וכי סיכום בדיקת התקינות תישלח להנהלה לבקרה. כמו כן נקבע כי כדי לוודא את תקינותו של מערך הגיבוי יש לבצע באופן יזום ניסיונות שחזור מדגמיים. על פי ההנחיה, רשימת הבדיקות הנדרשת בתדירות שנתית היא: (א) בדיקת שחזור יזומה של פריט מידע; (ב) בדיקת שחזור יזומה של שרת; (ג) בדיקת שחזור יזומה של מערכת בסביבת ייצור; (ד) תרגילים שנתיים.

בהנחיות משרד החוץ בעניין זה נקבע כי יש לבצע בדיקות תקופתיות לכל אחד מהנכסים המגובים, וכן לבצע תרגיל שחזור לבדיקה יסודית של כל מאגרי הגיבוי אחת לשנה.

בירור שקיים משרד מבקר המדינה עם אגף התקשוב במשרד החוץ בספטמבר 2024 העלה כי האגף שומר גיבויים למערכות מידע מסוימות באופן מקוון בחוות השרתים הראשית, עותק נוסף נשמר באתר ה-DR באמצעות רפליקציה[88] לשרתי האחסון שבאתר, ועותק נוסף מגובה לקלטות. אשר לביצוע תהליכי שחזור, נציגי האגף מסרו כי תהליכי שחזור נקודתיים בכלל הרשתות מבוצעים אד-הוק על פי הצורך, אך לא באופן מתוכנן, כולל ומתועד, וכי שחזורים נקודתיים שבוצעו הסתיימו בהצלחה.

באוקטובר 2025 מסר משרד החוץ כי המשרד מבצע העתקה של כלל הנתונים ברשתות מסוימות באופן קבוע, וכי מתבצע תהליך נוסף של גיבוי כמחצית מרשת מסוימת לסביבת הענן המשרדית.

הביקורת העלתה כי אף שנוהל הגיבוי והשחזור של משרד החוץ[89] כולל הנחיות לביצוע בדיקות תקופתיות לכל אחד מהנכסים המגובים וכן תרגיל שחזור יזום אחת לשנה, הרי שלמעט שחזורים

---

[88] תהליך שבו נתונים משוכפלים ומועתקים ממערכת אחת לאחרת, לרוב בזמן אמת או כמעט בזמן אמת.

[89] הנחיית ראש אגף התקשוב - נוהל גיבוי ושחזור. הנוהל כולל את מדיניות הגיבויים הנהוגה במשרד.

נקודתיים שבוצעו אד-הוק, לא ביצע המשרד בדיקות תקופתיות ותרגילי שחזור שנתיים. התנהלות זו גם אינה עולה בקנה אחד עם הנחיות מערך הדיגיטל.

בהיעדר ביצוע של תרגילי שחזור סדירים ומקיפים, שבהם בודקים שחזור של מערכות באופן מלא במקרה של תקלה או אסון - קיים סיכון ממשי לזמינות מערכות המידע של משרד החוץ, עד כדי פגיעה ברציפות התפקודית שלו. במצב הדברים הקיים, משרד החוץ אינו יכול להבטיח כי בעת הצורך או במצב חירום יתאפשר לו לבצע שחזור מלא ומוצלח של המידע הקריטי, של מערכות המידע הקריטיות, ובפרט של נכסי המידע המצויים בקלטות.

על משרד החוץ לבצע תרגילי שחזור באופן רחב ועיתי, אחת לשנה לפחות, כפי שנדרש בהנחיותיו, בהנחיות מערך הדיגיטל ובפרקטיקה המקובלת, דבר שיסייע בהבטחת הרציפות התפקודית שלו.

☆

מחקרים שנעשו בעולם[90] ובארץ[91] מצביעים על כך שקיים מתאם חיובי בין ממשל טכנולוגיות מידע לקוי לבין כישלונות של פרויקטים לפיתוח מערכות, תפקוד לקוי של ה-IT הארגוני ופגיעה ביעדים העסקיים. בדומה, מחקרים נוספים מלמדים על מתאם חיובי בין ממשל טכנולוגיות מידע מוצלח לבין עמידה ביעדים העסקיים של הארגון[92].

הביקורת שעשה משרד מבקר המדינה העלתה פערים בניהול ממשל טכנולוגיות המידע במשרד החוץ, בניהול הפרויקטים ובקיומה של תוכנית התאוששות מאסון.

---

90 Asgarkhani, Mehdi; Cater-Steel, Aileen; Toleman, Mark; and Ally, Mustafa, "Failed IT projects: is poor IT governance to blame?", **ACIS 2017 Proceedings**, (2017), 103. aisel.aisnet.org/acis2017/103
Lee, J., Lee, C., & Jeong, K. Y., "Governance Inhibitors in IT Strategy and Management: An Empirical Study of Korean Enterprises", **Global Economic Review**, 37(1) (2008), 1-22. doi.org/10.1080/12265080801911899.

91 Ahituv, N., Zviran, M., & Glezer, C., "Top Management Toolbox for Managing Corporate IT"; **Communications of the ACM**, 42(4) (1999), 93-99. doi.org/10.1145/299157.299177.

92 De Haes, S., & Van Grembergen, W., "An Exploratory Study into IT Governance Implementations and its Impact on Business/IT Alignment"; **Information Systems Management**, 26(2) (2009), 123-137. doi.org/10.1080/10580530902794786
Joshi, A., Benitez, J., Huygh, T., Ruiz, L., & De Haes, S., "Impact of IT governance process capability on business performance: Theory and empirical evidence", **Decision Support Systems,** 153 (2022). https://www.sciencedirect.com/science/article/pii/S0167923621001780

תרשים 6: **פערים מרכזיים בתהליכי ניהול ופיתוח של מערכות מידע**

יצוין כי במהלך השנים 2022 - 2024 פעל אגף התקשוב בכמה צירים לשם הגברת ממשל טכנולוגיות המידע. במסגרת זו הוכנה תוכנית אסטרטגית, הכוללת התייחסות למבנה הארגוני המומלץ, ובוצע סקר סיכוני תקשוב משרדי. עם זאת, התוכנית האסטרטגית וסקר סיכוני התקשוב טרם הובאו כאמור בפני הנהלת המשרד או ועדת ההיגוי המשרדית לתקשוב, ולא התקבלו החלטות בנוגע לצעדים הנדרשים כדי להתמודד עם הפערים והסיכונים שהועלו ולממש את ההמלצות שניתנו במסגרתם. יודגש כי מעורבות הנהלה ובראשה מנכ"ל המשרד בתהליכי מחשוב ארגוניים חיונית להצלחתם, שכן היא מבטיחה הקצאת משאבים, תיעדוף משימות ויישום מדיניות התואמת את יעדי הארגון.

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.

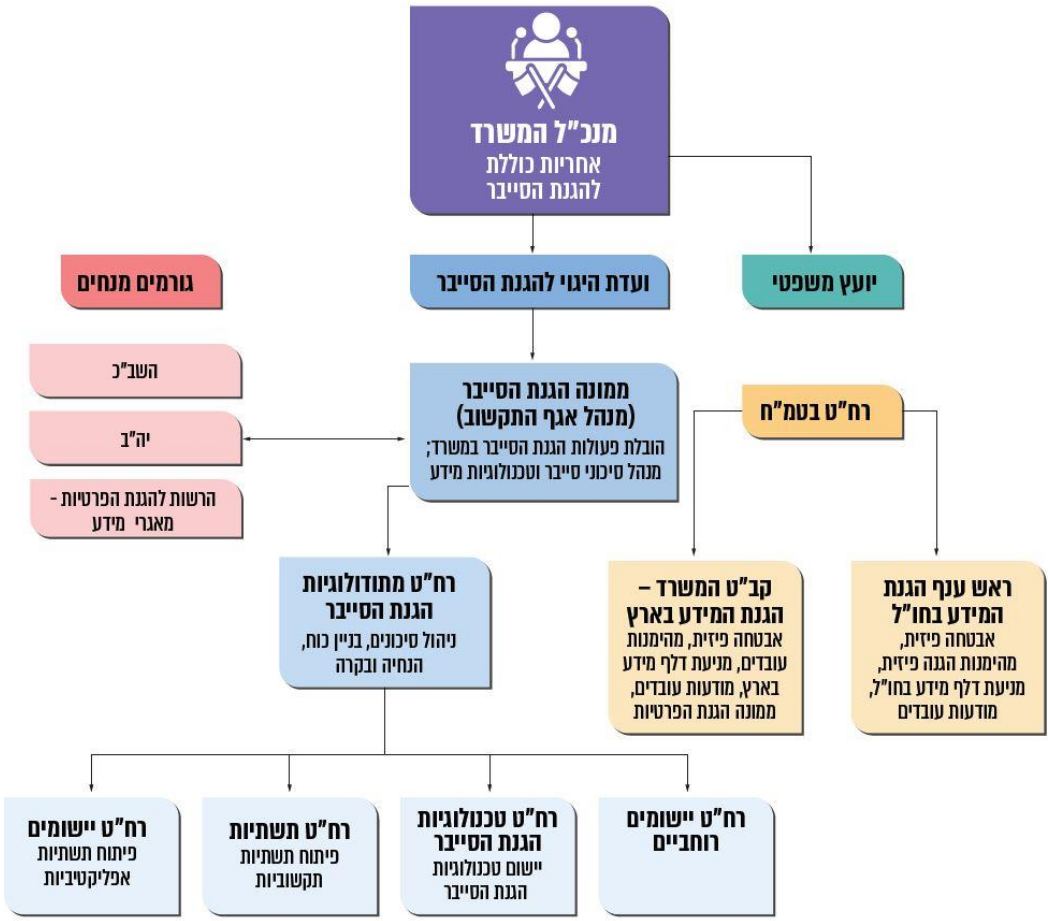
מנכ"ל משרד החוץ מסר למשרד מבקר המדינה באוקטובר 2025 כי האתגרים העומדים בפניו, כפי שעמדו גם בפני קודמיו לתפקיד, ימשיכו להיות אתגרים של משאבים וסדרי עדיפויות, ובכלל זה תקציב מצומצם, כוח אדם שאינו מספק ומערכות שנדרש לשדרגן. עוד מסר המנכ"ל כי הוא הורה לסמנכ"ל תקשוב להציג תכנית עבודה לתיקון הליקויים.

אבטחת המידע והגנת הסייבר במשרד החוץ

הסביבה התקשובית שבה פועל משרד החוץ היא מאתגרת, ייחודית ופריסתה גלובלית. כאמור בין מטה משרד החוץ בירושלים לנציגויות בכל העולם פרוסות כמה רשתות מחשוב.

גורמי המקצוע האחראים לנושא אבטחת המידע והגנת הסייבר במשרד הם אגף התקשוב וחטיבת בטמ"ח. במסגרת יישום החלטת הממשלה העוסקת בין היתר בקידום הגנת הסייבר בממשלה[93] (להלן - החלטה 2443), מונה במשרד החוץ ממונה על הגנת הסייבר במשרד (להלן - ממונה הגנת הסייבר) והוקמה ועדת היגוי משרדית להגנת הסייבר (להלן - ועדת ההיגוי להגנת הסייבר), המשמשת מסגרת ארגונית-ניהולית לקבלת החלטות אסטרטגיות בתחום הגנת הסייבר ולביצוע בקרה ניהולית על יישום הגנת הסייבר במשרד.

תרשים 7: **המבנה הארגוני של המערך להגנת הסייבר במשרד החוץ**



הוכן בידי משרד מבקר המדינה.

יה"ב מנחה את משרד החוץ בכל הנוגע לרשת הבלמ"ס, והשב"כ אחראי להנחיית המשרד בכל הנוגע לרשתות מסוימות במשרד וכן בנוגע לנושאים ספציפיים שקשורים לרשת הבלמ"ס. השב"כ מעביר לגופים המונחים אוסף הנחיות להגנת נכסי מידע מסוימים במרחב הסייבר הארגוני. עמידה בהנחיותיו מאפשרת לארגון להתמודד כנדרש עם אתגרי ההגנה, וכמו כן היא מאפשרת לגורם המנחה למדוד את מידת עמידותו של הארגון בפני איום הייחוס, כדי שהגורם המנחה יוכל להגביר את מידת עמידותו של הארגון, על פי התפתחות האיום.

93 החלטת הממשלה 2443, "קידום אסדרה לאומית והובלה ממשלתית בהגנת הסייבר" (15.2.15).

משרד החוץ מחזיק מידע רגיש מהבחינה המדינית-דיפלומטית ומידע רגיש נוסף. המידע כולל, בין היתר, הערכות מצב מדיניות, אסטרטגיה מדינית, שיתופי פעולה בין-לאומיים ותכתובות עם גורמי ממשל.

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.

לנוכח האתגרים הייחודיים שמתמודד עימם משרד החוץ בהיבטי התקשוב, בחן משרד מבקר המדינה היבטים הנוגעים לאבטחת המידע והגנת הסייבר במשרד החוץ. נוסף על כך ביצע משרד מבקר המדינה מבדק חוסן הכולל סקר הערכת פגיעויות ומבדק חדירה לאחת מרשתות המשרד.

ממשל אבטחת מידע במשרד החוץ

מסגרת ממשל לאבטחת מידע ברורה, מקיפה ויציבה נדרשת כדי להבטיח הגנה אפקטיבית על נכסי המידע של הארגון. מסגרת זו היא התשתית הניהולית והארגונית שבאמצעותה ניתן לקבוע מדיניות, להטיל אחריות ולפקח על תהליכי אבטחה בהתאם ליעדים ולסיכונים של הארגון. הממשל מתבסס על שילוב של נהלים, תקנים ובקרות, הנתמכים על ידי מינוי בעלי תפקיד מרכזיים, כגון ממונה הגנת הסייבר, ממונה הגנה על הפרטיות וועדת ההיגוי וקביעת תחומי אחריות לגבי כל רמות הפעולה. מסגרת זו מדגישה גם את חשיבות אבטחת המידע בארגון כחלק אינטגרלי מהאסטרטגיה העסקית. לצורך כך, על ההנהלה הבכירה להיות מעורבת בתהליך קבלת ההחלטות ולהפגין מחויבות ברורה לנושא. אחד המרכיבים המרכזיים במסגרת זו הוא קיום תהליך מובנה לזיהוי פערים ולהערכת סיכונים, המאפשר התאמה דינמית של המדיניות והבקרות לסיכונים שזוהו לאורך זמן[94].

לנוכח האתגרים שמתמודד עימם משרד החוץ כאמור גוברת החשיבות של ממשל אבטחת מידע יעיל שמזהה סיכונים ופערים, מכין תוכנית עבודה להתמודדות עם הסיכונים ולצמצום הפערים, ובכלל זה מקצה את המשאבים הנדרשים לטיפול בנושא, וכן מבצע בקרה על רמת ההגנה בסייבר במשרד.

<u>מדיניות הגנת הסייבר ועדכונה</u>

בהחלטת הממשלה 2443 נקבע כי ממונה הגנת הסייבר יפעל לגיבוש מדיניות הגנת הסייבר במשרד ממשלתי בהתאם לתהליך של ניהול סיכונים ארגוני וביצוע ניתוח והערכה שוטפים של תוכנית הגנת הסייבר והמדיניות, הנשען על הערכת צרכים, איומים ומענים.

בהנחיות יה"ב נקבע כי על ועדת ההיגוי להגנת הסייבר לאשר ולתקף את מדיניות הגנת הסייבר במשרד, וכי המדיניות תיבדק ותאושרר אחת לשנתיים או מוקדם יותר, בהתאם לצורך מיוחד (לנוכח שינויים ניכרים במערך המחשוב או במערך הארגוני של המשרד). בנוגע למידע מסווג נקבע כי מנכ"ל המשרד הממשלתי, או מי שהוא הסמיך מטעמו לעניין זה, יקבע אם לאשר את המדיניות, והיא תתוקף אחת לשלוש שנים.

כמו כן, בהנחיות יה"ב מפורטת רשימת הנושאים שיש להידרש אליהם במסגרת מסמך מדיניות ההגנה על הסייבר במשרד, כגון הגדרת מסגרות ארגוניות שיישמו את המדיניות ויבקרו את יישומה, הגדרת שכבות הגנה בתחומים הלוגיים, ניהול וסיווג של נכסים, טיפול באירועי סייבר וגיבוש תוכנית עבודה ותקציב בתחומי הגנת הסייבר.

---

94 מס"ל, תורת ההגנה בסייבר 2.0 (יוני 2021).

באפריל 2018 אישרו ועדת ההיגוי להגנת הסייבר ומנכ"ל המשרד את מסמך מדיניות הגנת הסייבר ואבטחת המידע במשרד החוץ (להלן - מסמך מדיניות הגנת הסייבר). במהלך השנים 2018 - 2024 חלו שינויים מהותיים במפת האיומים ובמבנה הארגוני של מערך התקשוב של משרד החוץ.

1. **שינוי איום הייחוס של המשרד**.

2. **שינוי בזהות הגורם המנחה את משרד החוץ**.

3. **שינוי במבנה הארגוני של הגנת הסייבר במשרד**.

4. **שינויים טכנולוגיים:** בשנים 2018 - 2024 אירעו שינויים טכנולוגיים מהותיים כמו שימוש במערכות מבוססות ענן; מעבר לעבודה מרחוק; שימוש העובדים והמשרד ברשתות חברתיות; שימוש העובדים ביישום מסוים במחשבי המשרד; הטמעת יישומים משרדיים מאובטחים; ושימוש באפליקציות של בינה מלאכותית.

5. **הגדרת מידע רגיש שאינו מסווג:** בהנחיות יה"ב ותורת ההגנה בסייבר של מס"ל נקבעו הגדרות מפורטות ועדכניות בנוגע למידע רגיש שאינו מסווג, המתייחסות לכמה סוגי מידע רגיש (מידע רגיש, מידע משפטי או כלכלי, מידע חסוי או מידע שהוא חסוי לפי חוק) וכן למידת הנזק שתיגרם מחשיפת מידע רגיש. מסמך מדיניות הגנת הסייבר של המשרד אינו כולל התייחסות מפורטת מעין זו.

6. **שרשרת אספקה:** בשנים 2018 - 2024 ניתנו הוראות חדשות של מס"ל ויה"ב לגבי ההגנה על הסייבר ואבטחת המידע בשרשרת האספקה.

7. **רשת מסוימת:** במשרד פועלת רשת מסוימת. במסמך המדיניות אין התייחסות מיוחדת לרשת זו, אף שבשנים 2022 - 2024 עסקו במשרד בשדרוגה לנוכח ליקויים בהגנה עליה.

יצוין כי נושא היעדר מדיניות סייבר ברורה הועלה ביוני 2023 לפני מנכ"ל המשרד וסמנכ"לית תיאום, המשמשת יו"ר ועדת ההיגוי להגנת הסייבר במשרד.

משרד החוץ מסר למשרד מבקר המדינה באוקטובר 2024 כי מאז אישורה של מדיניות הגנת הסייבר בשנת 2018 נעשתה פעילות לעדכון המדיניות, אך היא לא הבשילה לכדי הבאתה לאישור מחדש של ההנהלה.

מדיניות הגנת סייבר מעודכנת היא כלי מרכזי בהגנה על נכסי המידע, בניהול סיכונים, בהתמודדות עם איומים משתנים ובהבטחת המשכיות תפקודית. נמצא כי נכון לינואר 2025 ועדת ההיגוי להגנת הסייבר ומנכ"ל משרד החוץ לא עדכנו ולא תיקפו את מסמך מדיניות הגנת הסייבר, אף שחלפו כשבע שנים ממועד אישורו על ידי ועדת ההיגוי להגנת הסייבר ומנכ"ל המשרד באפריל 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", בזהות הגורם המנחה של המשרד ובמבנה הארגוני של הגנת הסייבר של המשרד. בהיעדר מדיניות הגנת סייבר מקיפה ועדכנית גוברת החשיפה של משרד החוץ לתקיפות סייבר ולדליפת מידע רגיש, וכן גובר הסיכון הכרוך בכך.

נוכח החשיבות שיש לעבודה על פי מדיניות סייבר ארגונית מעודכנת, על מנכ"ל משרד החוץ לוודא כי מדיניות הגנת הסייבר במשרד תעודכן ותובא בהקדם לאישור הגורמים האחראים לנושא - מנכ"ל המשרד וועדת ההיגוי להגנת הסייבר - דבר שיסייע להבטיח כי הגנת הסייבר

על המשרד ועל נכסיו האסטרטגיים תהיה מיטבית ואפקטיבית. כמו כן, 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".

אישור תוכנית העבודה בתחום הגנת הסייבר ובקרה על יישומה

הבניית תוכנית עבודה רב-שנתית בתחום הגנת הסייבר וגיבוש תוכניות עבודה שנתיות ליישומה הם צעדים נדרשים להתמודדות עם האיומים המתפתחים. תוכנית כזו מאפשרת תכנון ארוך טווח, הקצאת משאבים מושכלת, קביעת סדרי עדיפויות לטיפול בפערים, שיפור ההיערכות הארגונית והתאמה מתמדת של הגנת הסייבר לטכנולוגיות חדשות. הכנת תוכנית רב-שנתית מסייעת להבטיח כי מרב הפערים בתחום זה יטופלו בשנים הקרובות.

בהחלטת הממשלה 2443 נקבע כי על ממונה הגנת הסייבר לגבש תוכנית עבודה להגנת הסייבר על פי מדיניות המשרד. בהנחיות יה"ב ושב"כ נקבע כי על ועדת ההיגוי לאשר את תוכנית העבודה בתחום הגנת הסייבר ולבצע בקרה על יישומה. בהנחיות שב"כ נקבע גם כי יש להגדיר תוכנית הטמעה רב-שנתית ליישום הנחיות שב"כ, ועליה תתבסס תוכנית האבטחה הנדרשת.

לנוכח קביעת איום ייחוס עדכני על ידי הגופים המנחים גובשה בשנת 2019 תוכנית רב-שנתית להגנת הסייבר במשרד החוץ לשנים 2020 - 2024 בסך כולל של כ-54 מיליון ש"ח כתקציב ייעודי. התוכנית הרב-שנתית כוללת צירים מרכזיים וכן פירוט של התכולות, אבני הדרך והמשאבים הנדרשים לשם מימוש התכולות.

באוגוסט 2019 מנכ"ל המשרד אישר עקרונית את התוכנית, וקבע כי אי-נקיטת פעולה מיידית בתחום הגנת הסייבר היא אופציה בלתי מתקבלת על הדעת מהבחינה הארגונית, ולפיכך יש להשיק את התוכנית בשנת 2020 בהנחה שאכן יתקבלו המשאבים הדרושים.

מדיוני ועדת ההיגוי בשנים 2020 - 2021 עלה כי התוכנית הרב-שנתית לשנים 2020 - 2024 לא תוקצבה באופן ייעודי, וכי אגף התקשוב מימש כמה רכיבים בתוכנית הרב-שנתית במסגרת היכולות והמשאבים שעמדו לרשותו, ללא תוספות חיצוניות, ובהם הקמת מרכז גלובלי לניטור ותגובה לאירועי סייבר (SOC) שמנטר אלפי עמדות קצה ומאות מערכות בסביבות הרשת של המשרד, וכן הקמת חטיבה למתודולוגיות סייבר באגף התקשוב שאמונה על הנחיה ובקרה בתחום הגנת הסייבר. אשר לתוכנית העבודה של שנת 2021, במסגרת דיוני הוועדה צוין על ידי יו"ר ועדת ההיגוי כי התוכנית יועדה לביצוע משימות שניתן לקדם במהלך שנת עבודה בלבד, וכי לנוכח העובדה שמדובר בשנה של תקציב המשכי, קיים קושי ממשי במימוש תוכניות עבודה בשנה זו. בהקשר זה יצוין כי נציג מס"ל ציין בדיון לגבי התוכנית הרב-שנתית שחלפו שנתיים מאז גיבושה ויש לשוב ולתקף אותה, היות שתחום הסייבר הוא דינמי מאוד, ומה שנקבע לפני כשנתיים אינו רלוונטי עוד.

משרד החוץ מסר למשרד מבקר המדינה כי בשנת 2021 הוחלט שאין טעם להמשיך בניסיונות לקדם אישור תקציב ייעודי רב-שנתי לתוכנית שגובשה בשנת 2019, ולכן המשרד התמקד בשנים שלאחר מכן בתוכניות ברמה השנתית, תוך ניסיון לממש חלק מרכיבי התוכנית הרב-שנתית הקודמת במסגרתן.

בדיון ועדת ההיגוי מנובמבר 2022 צוין בנוגע לתוכנית העבודה לשנת 2022 כי היא עודנה בביצוע, ויו"ר הוועדה סיכמה כי תמונת המצב שהוצגה מטרידה ומחייבת התייחסות ניהולית ראויה. כן הדגישה שנדרש להציג תוכנית עבודה רב-שנתית לטיפול בסוגיות שהוצגו, המתכללת את הגופים הרלוונטיים, לרבות את הדרישות מבחינת כוח האדם והתקציב, וכי יש להגדיר לוח זמנים לסיום ביצועה של התוכנית. הוועדה ביקשה כי ממונה הגנת הסייבר ירכז את התוכנית ויציג לה אותה בינואר 2023. עוד עלה כי הוועדה קיבלה דיווח על יישום תוכנית העבודה לשנת 2021.

בדיון הוועדה ממאי 2023 צוין כי מרבית תוכנית העבודה לשנת 2023 מוקפאת לנוכח אי-אישור תקציב המדינה וכי מקודמות משימות בתחום המתודולוגיות. מבירור שביצע משרד מבקר המדינה עם נציג אגף התקשוב באוקטובר 2024 עולה כי לא הוכנה תוכנית רב-שנתית חדשה להגנת הסייבר.

באוקטובר 2025 מסר משרד החוץ למשרד מבקר המדינה כי אין באפשרותו להוציא לפועל תוכנית רב-שנתית.

עולה אפוא כי בשנת 2019 גובשה במשרד החוץ תוכנית רב-שנתית להגנת הסייבר לשנים 2020 - 2024, הכוללת יעדים, פעולות נדרשות, סדרי עדיפויות ומשאבים שנדרשים למימושם בסך כולל של כ-54 מיליון ש"ח, אולם תוכנית זו יושמה באופן חלקי בלבד עקב קשיים בהעמדת משאבים למימושה. נמצא כי המשרד לא הכין תוכנית רב-שנתית חדשה במקומה. עוד עולה כי החל משנת 2021 הציג אגף התקשוב לפני ועדת ההיגוי להגנת הסייבר תוכניות עבודה שנתיות בלבד ואת ממצאי המעקב אחר יישומן.

זאת ועוד, הועלה כי בניגוד להנחיות הגורמים המנחים, ועדת ההיגוי כלל לא אישרה את תוכנית העבודה לשנת 2024, ואף שבספטמבר 2024 התקיים דיון של ועדת ההיגוי, נושא תוכנית העבודה וסטטוס יישומה לא הועלה לפני הוועדה.

תוכניות עבודה שנתיות ורב-שנתיות בתחום הגנת הסייבר נועדו להבטיח פעילות סדורה ושוטפת להתמודדות עם איומים ותקיפות באמצעות הגדרת יעדים, ניתוח סיכונים, הקצאת משאבים ויישום בקרות מתאימות. תמונת המצב המשתקפת מכל האמור מלמדת על חולשה של ועדת ההיגוי להגנת הסייבר במשרד החוץ בכל הנוגע לפעילות סדורה המבוססת על תוכנית רב-שנתית, לפיקוח ובקרה על מימוש תוכניות העבודה וליכולתה לעמוד על הפערים הקיימים בתחום הגנת הסייבר ולקבל החלטות בהתאם לכך.

על ועדת ההיגוי להגנת הסייבר לאשר מדי שנה בשנה תוכנית עבודה הכוללת את כלל המשימות הנוגעות להגנת הסייבר, לרבות משימות שההחלטה לבצען התקבלה בישיבת ועדת ההיגוי, וכן עליה לעקוב אחר יישומה מדי שנה. כמו כן על הוועדה לעמוד על כך שתגובש תוכנית רב-שנתית להגנת הסייבר שתבטיח טיפול בכל הפערים, תוך קביעת סדרי העדיפויות והקצאת המשאבים הנדרשים וכן לעקוב אחר מימושה.

<u>פעילות ועדת ההיגוי להגנת הסייבר</u>

משרד מבקר המדינה בדק את פעילות ועדת ההיגוי להגנת הסייבר במשרד החוץ בשנים 2018 - 2024. הבדיקה התמקדה במעקב שקיימה הוועדה אחר נושאים מהותיים בהגנה על הסייבר שהובאו לפתחה וההחלטות שקיבלה על מדיניות המשרד בנושאים אלו. להלן כמה דוגמאות:

מדיניות הגנת המידע: בוועדת ההיגוי מפברואר 2020 סוכם כי ראש חטיבת בטמ"ח יגבש מדיניות לסיווג מידע רגיש שאינו מסווג מהבחינה הביטחונית ולטיפול במידע זה, לרבות בהיבטי הגנת הפרטיות.

נמצא כי אף שכבר בשנת 2020 ביקשה ועדת ההיגוי שתגובש מדיניות לסיווג מידע רגיש (שאינו מסווג מהבחינה הביטחונית) ולטיפול בו, נכון לאוקטובר 2024 מדיניות זו עודנה בגדר טיוטה והוועדה לא אישרה אותה, ומשכך היא גם לא פורסמה בקרב עובדי המשרד.

מדיניות המשרד בנוגע לשימוש העובדים ביישום מסוים: בדיון של ועדת ההיגוי מנובמבר 2022 הועלה נושא זה לראשונה כאחד הנושאים שיש לקבל החלטה בעניינם, והועלתה הצעה בנוגע לאופן השימוש של העובדים ביישום זה. בסיכום הדיון ציינה יו"ר הוועדה כי המשרד נדרש לגבש מדיניות בנושא, והיא הנחתה לזמן דיון ממוקד בראשותה ולהציג בו את ההחלטות הנדרשות. בישיבת ועדת ההיגוי ממאי 2023 נמסר לחברי הוועדה כי טרם התקבלה החלטה לגבי מדיניות המשרד להנגשת היישום לעובדים ונדרשת החלטה ברורה של ההנהלה בנושא.

נמצא כי אף שכבר בשנת 2022 הועלה נושא השימוש של העובדים ביישום זה, ועדת ההיגוי לא דנה בנושא ונכון ליולי 2025 לא התקבלה החלטה בעניינו ומשכך לא ניתנו הנחיות לעובדים בנושא.

הגנת הפרטיות: במסמך המדיניות להגנה על הסייבר מאפריל 2018 צוין כי הנהלת המשרד מחויבת להגן על מידע על עובדים שהוא בגדר צנעת הפרט בהתאם להוראות הדין, לרבות תקנות הגנת הפרטיות. בישיבת ועדת ההיגוי להגנת הסייבר מפברואר 2020 שדנה בממצאי סקר שבחן את עמידת המאגר הקונסולרי בתקנות הגנת הפרטיות (אבטחת מידע), התשע"ז-2017 צוין כי למשרד פערים לעמידה בתקנות בכלל המאגרים שברשותו ויש לגבש תוכנית לעמידת כלל מאגרי המשרד בתקנות אבטחת המידע עד לסוף שנת 2021 לרבות ביצוע סקרי סיכונים גם למאגרים אלו.

הועלה כי אף שוועדת ההיגוי עסקה בהגנה על מאגרי מידע שבהם מידע פרטי בשנים 2020 - 2023, נכון לאוקטובר 2024 לא בוצעו סקרי הערכת סיכונים (להלן - סקרי סיכונים) לגבי מאגרי מידע שברשות משרד החוץ (מלבד המאגר הקונסולרי), ולא הוכנה תוכנית לעמידה בתקנות הגנת הפרטיות בעניינם.

משרד החוץ ציין בתשובתו מאוקטובר 2025 בנוגע למדיניות המשרד בנושא שימוש העובדים ביישום המסוים, כי בוועדת ההיגוי הקרובה תוצג מדיניות עדכנית לרבות התייחסות חוזרת ליישום זה.

ועדת ההיגוי להגנת הסייבר אמורה לשמש מסגרת ארגונית ניהולית לקבלת החלטות בתחום הגנת הסייבר ולמעקב אחר יישומן. בביקורת עלה כי ועדת ההיגוי במשרד החוץ לא עקבה באופן שיטתי ורציף אחר יישום החלטות שקיבלה בנוגע לנושאים מהותיים. היעדר מעקב אחר יישום החלטות שנועדו לקדם טיפול בסוגיות אבטחת מידע חושף את המשרד לסיכונים ופוגע ביכולת לשפר את רמת ההגנה על המשרד ונכסיו.

על ועדת ההיגוי להגנת הסייבר לעקוב באופן שיטתי ורציף אחר קידום נושאים שנדונו בישיבותיה ולקבל החלטות בנושאים מהותיים שנדרשת הכרעה בהם כדי לשפר את רמת ההגנה על הסייבר במשרד החוץ ולוודא כי המשרד עומד בדרישות הגורמים המנחים.

ביצוע סקרי סיכונים ומבדקי חדירה

על פי הנחיית יה"ב, סקר הערכת סיכונים (להלן - סקר סיכונים) הוא תהליך שיטתי שמטרתו לזהות נכסים, תהליכי מידע ואיומים הנשקפים להם, להעריך את הסיכון הנובע מהם ולזהות את הבקרות הנדרשות לצמצום הסיכונים, תוך התחשבות בסבירות ההתממשות והנזק הפוטנציאלי כתוצאה מכך. בכל הנוגע לעולם הסייבר ומערכות המידע, הסיכון שנדרש להעריך בסקר סיכונים מוגדר כאפשרות לחשיפה לפגיעה או לפגיעה ממשית וגרימת נזק לנכסי המידע[95] כתוצאה מניצול פגיעות או חולשה הקיימות בנכסי המידע. מקובל לאמוד תחילה את הסיכון המובנה הקיים בנכס מידע או בתהליך מידע ללא התחשבות בבקרות כלשהן, וכן את הסיכון השיורי שנותר לאחר התחשבות בבקרות הקיימות. בתרשים מוצגים השלבים הכלולים בסקר הערכת הסיכונים על נכסי המידע, אשר עשויים לגרום נזק לתפקודו התקין של המשרד.

[95] נכסי המידע של המשרד הם המידע, מערכות המחשוב שמעבדות ומאכסנות אותו, התקשורת וכן האמצעים והציוד שעליו הוא מושתת. לפי הנחיית יה"ב 5.1 סעיף 4.5, מידע מוגדר ככל נתון הנוגע ו/או הקשור לפעילותם, תפעולם או תפקודם של המשרדים, לרבות מידע הנוגע לצנעת הפרט ומידע ממשלתי רגיש, הקיים על גבי אמצעי אחסון ממוחשבים, מגנטיים או אלקטרוניים, מצעי מידע פיזיים וכן מידע המועבר בעל פה.

תרשים 8: **שלבי הביצוע של סקר הערכת סיכונים**

על פי הנחיית יה"ב בעיבוד משרד מבקר המדינה.

על פי הנחיית יה"ב, על משרד ממשלתי לבצע סקר סיכונים כולל במערכות המידע שלו, לכל הפחות אחת ל-36 חודשים, ולתקף את ממצאי הסקר לפחות אחת ל-18 חודשים. סקר הסיכונים ישמש עבור המשרד בסיס לבניית תוכנית עבודה רב-שנתית ושנתית. במקרים מיוחדים, כגון שינוי מהותי בסביבה הטכנולוגית או בתהליכי העבודה, על המשרד לבצע סקר סיכונים נוסף.

מהנחיות הגורמים המנחים עולה כי תפקידי ועדת ההיגוי הם בין השאר בחינה, תיקוף ואישור של מפת סיכונים משרדית כפי שהיא עולה מסקר הסיכונים המשרדי, התעדכנות בסיכונים ובאיומים הנוגעים למשרד, פיקוח על ניהול סיכוני סייבר המבוצע במשרד וקבלת החלטות בנוגע לצורך בביצוע שינויים בעקרונות הגנת הסייבר.

משרד מבקר המדינה בחן את סקרי הסיכונים שביצע משרד החוץ בשנים 2017 - 2024 ולהלן הממצאים שהועלו.

1. **ביצוע סקר סיכוני סייבר כולל: נמצא כי בשנים 2017 - 2024 ערך המשרד כמה סקרי סיכונים כוללים שהוצגו לוועדת ההיגוי, אולם סקרים אלו היו חלקיים בלבד ולא כללו את כל רשתות המחשוב במשרד או שחסרו בהם חלק מהרכיבים הנדרשים לביצוע סקר סיכונים. כך למשל: בשנים 2017 ו-2019 ביצע המשרד סקרי סיכונים רק על חלק מרשתות המשרד, הסקרים בוצעו בחלק מיחידות המשרד; הסקר משנת 2017 העריך רק את הסיכון המובנה ולא את הסיכון השיורי, ובסקר משנת 2019 הוערכו סיכונים רוחביים במשרד ולא סיכונים לכל נכס מידע[96]; בשנת 2021 ערך אגף התקשוב סקר סיכונים שכלל 41 סיכונים רוחביים והוכנה תוכנית להפחתתם, עם זאת הסקר לא עסק בנכסי מידע ספציפיים. בשנת**

[96] בשנת 2019 בוצע גם סקר סיכונים בנושא הגנת הפרטיות על המאגר הקונסולרי.

2024 נערך מיפוי נכסים בכל רשתות המשרד, שבדק את מידת הקריטיות של כל נכס או תהליך לפעילות המשרד, אולם המיפוי לא כלל הערכה של הסיכון המובנה והסיכון השיורי בכל נכס מידע שנכלל במיפוי.

עוד נמצא כי מאז שנת 2021 ועדת ההיגוי לא דנה בתוכנית להפחתת הסיכונים, במפת הסיכונים ובסיכונים השיוריים ולא אישרה אותם. עלה כי מתוך חמש ישיבות שערכה ועדת ההיגוי בשנים 2019 - 2024, רק בשתי ישיבות, בשנים 2020 ו-2021, הוצגה לוועדה תוכנית עבודה להפחתת הסיכונים, וגם בישיבות אלו לא אישרה הוועדה תוכנית להפחתת הסיכונים.

2. ביצוע סקרי סיכונים ומבדקי חדירה ייעודיים בנכסי מידע ברשתות מסוימות במשרד: לפי הנחיות הגורמים המנחים, על הארגון לבצע סקר סיכונים או מבדק חדירה פרטני לכל נכס מידע קריטי אחת לשלוש שנים (בין שבמסגרת סקר הסיכונים הכולל ובין שבמסגרת סקר סיכונים ייעודי). בשנים 2020 - 2024 ביצע המשרד 17 סקרי סיכונים ומבדקי חדירה ייעודיים לתהליכים ונכסי מידע. נמצא כי, נכון ליולי 2024 בוצעו סקרי סיכונים או מבדקי חדירה רק לחלק ממערכות מידע.

ביצוע סקרי סיכונים ומבדקי חדירה הם כלים מהותיים בניהול וחיזוק של אבטחת המידע בארגון. הסקר מאפשר לזהות את האיומים והפגיעויות, לנתחם ולהעריכם ולמקד את המשאבים והמאמצים בהתאם לרמת הסיכון. עולה כי משרד החוץ פעל במהלך השנים 2018 - 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.

משרד החוץ מסר למשרד מבקר המדינה באוקטובר 2025 כי סקרי הסיכונים מתבצעים בהתאם ליכולת אגף התקשוב בהיבטי כוח אדם ותקציב. המשרד הוסיף כי חלק מתשתיות המחשוב מיושנות, ולכן להבנתו מבדק חדירה אינו כלי אפקטיבי מול תשתיות ויישומים בסטטוס EOL, שכן לא ניתן ליישם תיקוני אבטחה בעקבות הממצאים הצפויים. לפיכך במקום מבדקי חדירה ננקטו צעדים ובקרות מפצות לצמצום הסיכונים, ובהם הקמת ה-SOC.

בהתייחס לתשובת משרד החוץ יוער כי מבדקי חדירה נדרשים להיעשות גם מול תשתיות מחשוב ישנות, שכן הם בודקים גם את ההרשאות שניתנות במערכות המידע למשתמשים. כמו כן, גם אם מדובר במערכת מידע שמעולם לא נעשה לה מבדק חדירה או סקר, נכון לעשות לה לפחות סקר כדי לעמוד על הסיכונים הקיימים לגביה.

על משרד החוץ, בשיתוף הגורמים המנחים יה"ב והשב"כ, לבצע סקר סיכונים הכולל את כלל נכסי המידע והתהליכים הקריטיים, לחשב עבור כל נכס מידע את הסיכון השיורי בהתחשב בבקרות הקיימות, 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. עוד על המשרד לגבש תוכנית עבודה שתבטיח ביצוע מבדקי חדירה לכל נכסי המידע שיש לבצע לגביהם בדיקה זו.

הצגת רמת הגנת הסייבר במשרד החוץ לפני ועדת ההיגוי

לפי החלטת הממשלה מפברואר 2015 (החלטה 2443), אחד מתפקידיו של ממונה הגנת הסייבר במשרד הוא ביצוע בקרה על יישום הגנת הסייבר וניהולה בהיבט הארגוני הרחב ובהתאם למדיניות, ועל ועדת ההיגוי להגנת הסייבר לפעול לשיפור רמת ההגנה בסייבר של המשרד ולפקח על הפעילות השוטפת המבוצעת במשרד בנושא זה.

בהנחיות יה"ב נקבע כי ועדת ההיגוי תיזום סקרי הנהלה שיבדקו את הישימות והביצוע של כלל הפעילויות להגנת הסייבר במשרד, לרבות ישימותם של מסמך המדיניות ונוהלי הגנת הסייבר.

תוצאות הסקרים יועברו לוועדה, אשר תשקול הטמעת ההמלצות וביצוע שינויים רלוונטיים כנדרש. עוד נקבע בהנחיות כי כחלק מסקר ההנהלה, תגבש הוועדה מדדים כמותיים בנושאי הגנת הסייבר, שבאמצעותם יהיה ניתן לבחון ולמדוד את רמת האפקטיביות של יישום תשתית הגנת הסייבר בתום כל חציון. גם בהנחיות השב"כ נקבע כי אחד מהנושאים שנדרשים במסמך המדיניות הוא פיקוח ובקרה של יישום הנחיות השב"כ באמצעות הגדרת עקרונות הנוגעים לפיקוח ובקרה שוטפים אחר הנחיותיו ולאופן הצגת הפערים להנהלה.

1. **הנחיות יה"ב מחייבות כי ועדת ההיגוי תיזום סקרי הנהלה שיבדקו ביצוע כלל הפעילויות להגנת הסייבר במשרד. הוועדה נדרשת על פי הנחיות יה"ב לשקול ביצוע שינויים לאור המלצות הסקרים. נמצא כי בשנים 2021 - 2024 לא הובא לפני חברי הוועדה מידע על פערי אבטחה שצפו כגון אמצעי הגנה מסוימים שנדרשו להיות מותקנים לא הותקנו כנדרש.**

2. **עוד נמצא כי ועדת ההיגוי להגנת הסייבר לא קבעה מדדים כמותיים בנושאי הגנת הסייבר, אשר באמצעותם יהיה ניתן לבחון ולמדוד את רמת האפקטיביות של יישום תשתית הגנת הסייבר כנדרש בהנחיות יה"ב.**

3. **לפי החלטת הממשלה תפקידה של ועדת ההיגוי לשפר את רמת ההגנה בסייבר במשרד. תפקיד זה מחייב כי הוועדה תקבל מידע על רמת ההגנה בסייבר הקיימת במשרד ובכלל זה על אפקטיביות תשתית הגנת הסייבר. נמצא כי מאז 2021 לא הוצגה לחברי הוועדה הערכה בדבר אפקטיביות תשתית הגנת הסייבר[97] וכן לא הוצג מדד כללי שהמחיש לחברי הוועדה באופן כמותי את הפער שבין רמת ההגנה בסייבר במשרד לבין זו הרצויה לפי תתי-תחומים של הגנת הסייבר (הגנת הסייבר ברובד הלוגי, הגנת הסייבר ברובד הפיזי, הגנת הסייבר ברובד האנושי, אחריות הנהלה ותאימות, אבטחת מיקור-חוץ ושרשרת האספקה).**

4. אחת מהדרכים לבדוק את הישימות והביצוע של כלל הפעילויות להגנת הסייבר במשרד היא ביצוע סקרי סיכונים או מבדקי חדירה למערכות מידע בגוף, שמעלים בין היתר פערים בפעילותם של אמצעים להגנת הסייבר. בהנחיות השב"כ נקבע כי עיקר הממצאים החריגים שיעלו בביצוע בקרות פנימיות בגוף המונחה יוצגו במעמד ועדת ההיגוי בגוף.

כאמור, בשנים 2020 - 2024 ערך משרד החוץ 17 סקרי סיכונים או מבדקי חדירה למערכות המחשוב במשרד. נמצא כי אף שבשישה מהם הועלו ממצאים שנדרש היה להביאם בפני ועדת ההיגוי, הם לא הוצגו לפני חברי ועדת ההיגוי.

חברי ועדת ההיגוי להגנת הסייבר אחראים לפעול לשיפור רמת הגנת הסייבר של המשרד, ועליהם לפקח על הפעילות השוטפת המבוצעת בתחום זה, לאשר את מפת הסיכונים המשרדית ולאשר את תוכנית העבודה בתחום הגנת הסייבר ולבקר את יישומה. לשם כך עליהם לקבל את מלוא המידע על סקרים ומבדקים שנערכו במשרד, המשקפים את יישום הגנת הסייבר במשרד. מידע זה יכול להשפיע על התייחסות חברי הוועדה למפת הסיכונים המשרדית ולתוכנית העבודה בתחום הגנת הסייבר שהם נדרשים לאשר.

מומלץ כי ממונה הגנת הסייבר יעדכן את חברי ועדת ההיגוי בתחילת כל שנת עבודה בנוגע לסקרים ומבדקי חדירה שעתידים להתבצע, יביא בפניהם את ממצאי הסקרים והמבדקים לאחר ביצועם וכן ידווח לוועדה על הפעולות שננקטו לשם התמודדות עם הפערים ומידת תיקון הליקויים הקריטיים שעלו בהם.

---

97 בישיבת ועדת ההיגוי באפריל 2021 הוצגו 41 סיכונים בתחום הסייבר במשרד וכן מגמות השינוי בהם. כמו כן הוצגה תמונת מצב של רמת ההגנה בסייבר בשקף הממחיש את רמת ההגנה בסייבר במשרד לפי תתי-תחומים בהשוואה לרמת ההגנה הנדרשת בכל אחד מהם.

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 2018-2024 לא הועברו לוועדת ההיגוי כל הדיווחים על אירועי הסייבר המשמעותיים שאירעו במשרד כמתחייב על פי הנחיות יה"ב.

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.

יידוע חברי ועדת ההיגוי בדבר אירועי סייבר חריגים נועד כדי שחברי הוועדה יכירו את רמת ההגנה בסייבר הקיימת במשרד וכן לצורך ביצוע הערכת נזקים בעקבות האירועים וגיבוש המלצות לטיפולם. העברת מידע על חלק מאירועי הסייבר, ובאיחור ניכר לאחר מועד התרחשותם, אינה מאפשרת לחברי הוועדה להעריך במועד את הנזק שנגרם לרמת הגנת הסייבר המשרד ולגבש המלצות לצורך תיקון הפערים שהועלו.

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.

מינוי חברי ועדת ההיגוי להגנת הסייבר ותדירות התכנסותה

לפי החלטת הממשלה מפברואר 2015[98] והנחיית יה"ב, בראש ועדת ההיגוי יעמוד מנכ"ל המשרד ויתר חבריה יהיו בעלי התפקידים הבאים במשרד: ממונה הגנת הסייבר, מנהל משאבי אנוש, מנהל מערכות מידע, מנהל ביטחון (הגנה פיזית), יועץ משפטי, חשב וכן נציג יה"ב. עוד נקבע כי הוועדה תתכנס לכל הפחות פעם בחציון. בהנחיות השב"כ נקבעו הוראות דומות בנוגע לוועדת ההיגוי שתפעל על פי הנחיותיו[99].

ועדת ההיגוי להגנת הסייבר במשרד החוץ החלה לפעול בינואר 2016 והתכנסה עד לשנת 2018 בתדירות הנדרשת. בספטמבר 2019 הוקמה ועדה נוספת, הוועדה התקשובית להגנת הסייבר, בראשות ממונה הגנת הסייבר במשרד ובהשתתפות מנהלים מאגף התקשוב במשרד, ותפקידיה היו יישום החלטות ועדת ההיגוי העליונה; מעקב אחר מימוש תוכנית העבודה של המשרד בתחום הגנת הסייבר; גיבוש נושאים לדיון בוועדת ההיגוי העליונה והמלצה לממונה הגנת הסייבר על תיעדוף משימות בהתאם לרמות הסיכון.

נמצא כי בניגוד להחלטת הממשלה ולהנחיות יה"ב שלפיהן על ועדת ההיגוי להתכנס לכל הפחות פעם בחציון, ועדת ההיגוי במשרד החוץ לא התכנסה כלל בשנת 2019, ובשנים 2020 - 2024 התכנסה פעם אחת בלבד בכל שנה[100]. זאת אף שבדיון של ועדת ההיגוי באפריל 2021 ציין נציג מס"ל כי "לאור הסיכונים המהותיים שהוצגו, מס"ל מבקשים כי הנהלת המשרד תקיים ועדת היגוי אחת לרבעון ברשות מנכ"ל המשרד; ועדת היגוי אמורה להתקיים לפחות פעמיים בשנה. על ההנהלה להבין כי היא אחראית על הגנת הסייבר של המשרד"[101].

---

98 החלטת הממשלה 2443 (15.2.15).

99 חברי הוועדה ימונו על ידי המנכ"ל או על ידי מי שהמנכ"ל הסמיכו; הוועדה תכלול גורמים בדרג הנהלה בכיר ובעלי זיקה לנושא ההגנה בסייבר, וחברי הוועדה יקבלו מינוי רשמי בכתב שישקף את תפקידם ואחריותם.

100 הוועדה התכנסה ב-25.2.20, 5.4.21, 23.11.22, 14.5.23, 30.9.24.

101 יצוין כי הוועדה התקשובית להגנת הסייבר התכנסה שלוש פעמים בפרק הזמן שמספטמבר 2019 ועד פברואר 2020.

עוד נמצא כי אף שהחלטת הממשלה מחייבת שמנכ"ל המשרד יעמוד בראש ועדת ההיגוי להגנת הסייבר, במהלך כל שנות פעילותה של הוועדה במשרד החוץ עמד בראשה סמנכ"ל תיאום ותכנון מדיני.

משרד החוץ השיב כי בשנת 2015 הוחלט שבראש ועדת ההיגוי תעמוד סמנכ"ל תיאום ולא המנכ"ל. המשרד הוסיף כי בפברואר 2025 העביר אגף התקשוב ללשכת מנכ"ל המשרד רשימה מוצעת של חברי וועדה לצורך פרסום כתבי מינוי עדכניים.

ממצאי דוח זה, כפי שיפורטו גם להלן, מצביעים כי נכון לסוף שנת 2024 משרד החוץ מתמודד עם סיכונים מהותיים בהגנה על הסייבר במטה המשרד ובנציגויות בחו"ל. לנוכח זאת, ובהתאם להחלטת הממשלה והנחיות יה"ב, על מנכ"ל משרד החוץ לעמוד בראש ועדת ההיגוי להגנת הסייבר ולהקפיד לכנס אותה לפחות פעמיים בשנה כדי לעקוב אחר החלטות הוועדה ולקדם ביעילות את נושא הגנת הסייבר במשרד.

עמידה ברמת ההגנה הנדרשת ברשתות מסוימות

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

באוקטובר 2025 ציין אחד הגורמים המנחים בתשובתו כי לאחרונה אישרה נציבות שירות המדינה למשרד החוץ שלוש משרות נוספות בתחום הגנת הסייבר[102], ואיוש משרות אלה יאפשר לקדם משמעותית את רמת ההגנה על רשתות המשרד.

משרד החוץ הוא יעד המצוי באיום תמידי. תמונת המצב המתוארת לעיל משקפת כי על אף פעולות שביצע משרד החוץ במטרה לקדם את רמת ההגנה על מערכותיו, עדיין קיים פער בין רמת האיום לבין רמת ההגנה שנקבעה ושעל המשרד לעמוד בה בשלב זה. הותרת הרשתות שבידי המשרד ברמת הגנה נמוכה מהנדרש עלולה להביא לפגיעה במדינת ישראל בהיבטים המדיניים, הביטחוניים, הכלכליים והתדמיתיים.

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

---

[102] מנב"ט סייבר, מנהל SOC ומתודולוג חו"ל.

הגנה על המידע ברשתות המחשוב במשרד החוץ

משרד החוץ מחזיק מידע רגיש, ובכלל זאת מידע רגיש מהבחינה המדינית-דיפלומטית.

סיווג נכסי המידע במשרד החוץ

הנחיות הגורמים המנחים מחייבות כל ארגון לסווג את נכסי המידע שברשותו[103] כדי להבטיח כי כל נכסי המידע של המשרד מפוקחים ומאובטחים כנדרש וכי קיים גורם הנושא באחריות לגבי כל אחד מהנכסים. בהנחיות יה"ב נקבע כי יש לקבוע עקרונות לגבי סיווג המידע ומערכות המחשוב המעבדות ומאחסנות אותו, וכי קביעת העקרונות והקריטריונים להגדרת סיווג רגישות המידע תיעשה לפי מידת הנזק שייגרם למשרד, למדינת ישראל או לגורמים אחרים בשל חשיפה של המידע, חבלה בו, מחיקה או שיבוש שלו, של מאגריו או מערכותיו, בין שבמזיד ובין שבשוגג[104]. עוד נקבע כי המידע יסומן בתווית לפי סיווגו, וייקבעו הנחיות לגבי מקום אחסונו, העברתו במשרד והרשאות הגישה אליו. בהתאם, צוין כי ממונה הגנת הסייבר בארגון יקבע את רמת ההגנה המחייבת לכל נכס מידע (כגון - רמת ההזדהות, רמת המידור, רמת הבקרה, צורך בהצפנה וכיו"ב).

במסמך מדיניות הגנת הסייבר של משרד החוץ משנת 2018 נקבע כי נכסי המידע של המשרד יסווגו על ידי הממונה על הביטחון[105] וכי סיווגו של נכס מידע ייקבע, בין היתר, על פי רגישותו בהיבטים השונים (המדיניים, הביטחוניים, המשפטיים, הכלכליים וכדומה) ובפוטנציאל הנזק למשרד במקרה של דלף, פגיעה או שיבוש המידע. במסמך הוגדרו מספר רמות לסיווג המידע במשרד.

בשנת 2022 הוצגה ואושרה בוועדת ההיגוי העליונה להגנת הסייבר במשרד החוץ הגדרה חדשה לרמת הסיווג "בלמ"ס רגיש" - מידע אשר חשיפתו לגורם בלתי מורשה, שינויו ללא סמכות, מחיקתו או מניעת גישה אליו יסייעו לגרום נזק כלכלי או תפעולי, או יפגעו בצנעת הפרט או ביכולת המשרד לקיים דרישות כל דין.

במסמך מדיניות הגנת הסייבר של משרד החוץ נקבעו כאמור רמות סיווג שונות למידע, בהתאם לרגישותו ולפוטנציאל הנזק שלו. עם זאת הועלה כי במשרד החוץ לא קיים נוהל לסיווג מידע הכולל הנחיות מפורטות המגדירות את הקריטריונים והתבחינים שלפיהם תיקבע מידת רגישות המידע וסיווגו וכן את רמת ההגנה הנדרשת בכל אחת מהרמות. במצב דברים זה, בידי עובדי המשרד אין כללים ברורים לקביעת סיווגו ורגישותו של כל נכס מידע, ומכאן שקיים קושי לקבוע את רמת ההגנה המחייבת לגבי כל אחד מנכסי המידע לרבות זהות המורשים לגשת אליו והיקף הרשאותיהם. ללא סיווג נכון של נכסי המידע, נכסי מידע רגישים עלולים להיות חשופים לסיכונים כמו גישה לא מורשית, דליפת מידע והפרה של הוראות הדין הנוגעות להגנה על מידע, כגון הוראות הנוגעות להגנה על הפרטיות.

במהלך השנים גורמים שונים הצביעו לפני משרד החוץ על היעדרו של נוהל הנוגע לסיווג המידע ועל השלכות היעדרו של נוהל כזה.

1. סקר סיכוני סייבר שבוצע במשרד החוץ בשנת 2019 הצביע על סיכוני-העל במשרד ובהם סיכון הנוגע לסיווג המידע. בעניין זה צוין כי במשרד קיימת רשת מסוימת שמכילה מידע רגיש, אולם אין נהלים והנחיות המגדירים את אופן ההגנה על המידע הקיים בהתאם לסיווגו. עוד צוין כי המערכות התומכות בשמירה על המידע אינן עונות על הצרכים הנדרשים בהתאם לסוג המידע.

---

103 לפי הנחיית יה"ב, נכסי מידע הם "המידע, מערכות המחשוב המעבדות ומאכסנות אותו והתקשורת, האמצעים והציוד עליו הוא מושתת".

104 אשר לרמות סיווג המידע, בהנחיות יה"ב נקבע כי המידע במשרד ימופה לפי סוגי המידע הבאים: מידע ביטחוני; מידע אישי מוגן על פי חוק הגנת הפרטיות; כל מידע במאגר המוגן על פי תקנות הגנת הפרטיות (אבטחת מידע); מידע כלכלי ו/או מסחרי; מידע הנוגע לשלום הציבור ו/או לשלום היחיד. עוד נקבע בהנחיית יה"ב כי בנוהלי המשרד ייקבעו רמות התייחסות למידע שאינו ביטחוני אך רגיש בהתאם לרמות הבאות: פנימי; חסוי או חסוי אישי; חסוי ביותר.

105 ראש חטיבת בטמ"ח.

2. בנובמבר 2022 בוצעה על ידי השב"כ בדיקה ייעודית לצמצום ומניעה של דלף מידע במשרד החוץ שבה עלו ממצאים הדורשים התייחסות.

3. ביולי 2023 הוגש למשרד החוץ סקר סיכונים שהוזמן על ידו בנושא דלף מידע. אחד מהסיכונים שהוצפו בסקר נגע להיעדר נוהל סיווג מידע המגדיר מהם הפרמטרים של מידע מסווג וכיצד פרמטרים אלו מיושמים בפועל בתהליך העברת המידע.

במאי 2023 הכין אגף התקשוב במשרד טיוטה של הנחיה בנושא אסדרת התבחינים והתהליכים למניעת דלף מידע מסביבות רשת של משרד החוץ, שכללה הגדרות עדכניות לסוגי המידע במשרד, רשימת סיכונים ותבחיני נזק וכן קביעת הנחיות להגנה על המידע בהתאם לסיווגו. נכון לינואר 2025 טרם אושרה טיוטה זו על ידי ראש חטיבת בטמ"ח ועל ידי מנהל אגף התקשוב במשרד.

עולה אפוא כי אף שגורמים שונים הצביעו כבר משנת 2019 על הסיכון הקיים של דלף מידע, בהיעדרו של נוהל המסדיר את סיווג נכסי המידע ואת מעטפת ההגנה הנדרשת בהתאם לסיווגם - עד ינואר 2025 טרם הוסדר נושא זה בהנחיות משרד החוץ ולא הופץ לעובדים.

לנוכח הסיכונים הטמונים באי-סיווג המידע או בסיווג לא נכון שלו, על משרד החוץ להשלים את גיבוש ההנחיה בנושא סיווג מידע והגנה עליו, להטמיע אותה במשרד באמצעות הדרכות ולוודא שהעובדים אכן יודעים כיצד לנהוג בנכסי המידע השונים בהתאם לרמת רגישותם.

ניהול הרשאות הגישה ברשתות המשרד

עובדים בארגון הם אחד מהסיכונים המהותיים ביותר לאבטחת המידע בארגון. בין היתר מדובר בעובדים או משתמשים המשוטים על ידי אחרים ללא מודעות לכך ; סקרנים ; עובדים ממורמרים או בעלי כוונת זדון ; ועובדים בעלי מודעות נמוכה להגנת הסייבר והמידע עצמו.

עקרון יסוד בהגנה על מידע הוא מתן הרשאות על בסיס תפקידו של העובד. לפי עיקרון זה, רמת החשיפה של העובד למידע ארגוני תיקבע לפי הצורך לדעת (need to know), והיקף וסוג ההרשאות ייקבעו לפי מינימום הפעולות שנדרשות לו לצורך ביצוע עבודתו (least privileges). הגבלת הגישה של עובדים למידע האגור במערכות המשרד נועדה לצמצם את החשיפה של המידע לגורמים שאינם מורשים ואת אפשרויות הפגיעה במידע על ידי העובדים עצמם או על ידי גורמים חיצוניים, שישיגו גישה בלתי מורשית למערכות. לשם כך, נקבע בהנחיות הגורמים המנחים כי יש לבצע מידור של המידע ושל המשתמשים בו, וכי ההרשאות יינתנו על בסיס פרופיל הרשאות, כך שלכל תפקיד במשרד יוגדר פרופיל הרשאות מתאים, ויוענקו לו הרשאות גישה לפרטי מידע הדרושים לו לביצוע עבודתו בלבד, כפי שיוגדר על ידי בעלי המידע ובשיתוף ממונה הגנת הסייבר במשרד[106].

משרד החוץ מנהל את המידע ברשתות המשרד בין היתר באמצעות ספריות, שלהן ניתנת הרשאה לעובד מסוים או קבוצה מוגדרת של עובדים. באפשרות מנהלי הרשתות לקבוע על פי בקשת בעלי המידע בספריות את זהות המשתמשים או קבוצת המשתמשים שלהם תינתן הרשאה לכל ספרייה (לכל משתמשי הרשת, רק למשתמשים המוגדרים כמשתמשי-על וכיו"ב) וכן את הפעולות שעבורן תינתן הרשאה (הרשאה כוללת לרבות הרשאת כתיבה, הרשאה לקרוא ולהפעיל את הקובץ, הרשאת קריאה בלבד וכיו"ב). באפשרות מנהל הרשת, על פי בקשת בעלי המידע בספריות, גם להחליט אילו ספריות יהיו גלויות לכל המשתמשים ואילו יהיו גלויות רק למשתמשים מסוימים או לקבוצת משתמשים מסוימת.

106 יצוין כי חובת ניהול הרשאות הגישה קבועה גם בסעיף 8 בתקנות הגנת הפרטיות (אבטחת מידע), התשע"ז-2017.

משרד מבקר המדינה ניתח את ההרשאות שניתנו לספריות רשת משותפות ברשתות משרד החוץ נכון לספטמבר 2024. בניתוח נמצאו ספריות בחלק מרשתות המשרד שהיו פתוחות לכלל משתמשי הרשת.

עולה אפוא כי בניגוד להנחיות שלפיהן יש להגביל את הרשאות הגישה של העובדים למינימום ההרשאות הנדרשות לצורך ביצוע עבודתם ושלא על פי העיקרון היסודי של הצורך לדעת, הרי שבמשרד החוץ ניתנה גישה לחלק מספריות המשרד לכלל משתמשי הרשת. דבר זה מעלה את החשש לדלף מידע, לפגיעה במידע או לשימוש לא ראוי בו.

באוקטובר 2025 ציין משרד החוץ בתשובתו למשרד מבקר המדינה כי עם קבלת המידע ממבקר המדינה צומצמו מיידית הרשאות למשתמשים בספריות הציבוריות בצורה מבוקרת, וכי במקביל לתהליך הידני התבצעה התקשרות עם חברה המתמחה בתהליך ניתוח הרשאות וצמצומן. עוד ציין המשרד כי ההרשאות המיותרות נבחנו וצומצמו, וכי המשך התהליך ברשתות מסוימות מתבצע בשיתוף צוותי פיתוח וכלי AI, שכן צמצום בצורה דרסטית עלול לפגוע בסביבת הייצור.
על משרד החוץ להשלים את הבקרה על ההרשאות שניתנו בכל הספריות ברשתות של המשרד ולהגביל את הגישה בהתאם לעקרון הצורך לדעת והצורך לבצע את מינימום הפעולות לפי תפקידו של כל עובד.

<u>הגנה על מידע רגיש ברשת מסוימת</u>

בהתאם לחוק הגנת הפרטיות ותקנותיו ועל פי הנחיות הגורמים המנחים[107], כל בעל נכס מידע נדרש לקבוע את סיווג המידע שבנכס, וכן עליו לקבוע למי יינתנו הרשאות אליו בהתאם לעקרון הצורך לדעת. הדבר נכון גם לגבי כונני הרשת, ועל בעל הכונן לקבוע אילו קבצים יהיה אפשר לאחסן בכונן זה. אם בעל הכונן החליט כי הכונן יהיה כונן ציבורי, עליו לקבוע כללים לניהול המידע בכונן זה, למשל בנוגע לסוג המידע שיהיה ניתן לשמור בכונן, הזמן המרבי שהמידע יישמר בכונן לפני שיימחק, ואם יש מקום לאפשר גישה אליו לכלל המשתמשים.

משרד מבקר המדינה בדק את המידע המצוי ברשת מסוימת. הבדיקה העלתה כי נכון לספטמבר 2024 פעל ברשת זו כונן (להלן - כונן X) שהכיל עשרות אלפי מסמכים[108], חלקם כוללים מידע רגיש, כגון מידע אישי-פרטי והוא היה פתוח לכלל משתמשי הרשת. יצוין כי מאות קבצים בנושאים שונים נשמרו ישירות בכונן זה ולא אוחסנו בספרייה ייעודית. להלן דוגמאות לקבצים שנמצאו שלהם הייתה נגישות לכלל משתמשי הרשת:

הנגישות למסמכים הכוללים מידע פרטי של עובדי המשרד ושל אזרחים ישראלים וזרים:

הזכות לפרטיות מעוגנת בחוק-יסוד: כבוד האדם וחירותו, ובמסגרתו נקבע כי "כל אדם זכאי לפרטיות ולצנעת חייו"[109]. חוק הגנת הפרטיות, התשמ"א-1981, קובע כי פגיעה בפרטיות היא בין היתר הפרה של חובת סודיות שנקבעה בדין לגבי ענייניו הפרטיים של אדם, או הפרה של חובת סודיות לגבי ענייניו הפרטיים של אדם, שנקבעה בהסכם מפורש או משתמע. החוק גם קובע כי בעל מאגר מידע אחראי לאבטחת המידע שבמאגר המידע[110]. תקנות הגנת הפרטיות (אבטחת מידע), התשע"ז-2017 (להלן - תקנות הגנת הפרטיות), קובעות כי בעל מאגר מידע יקבע הרשאות גישה של בעלי הרשאות למאגר המידע ולמערכות המאגר בהתאם להגדרות תפקיד; הרשאת הגישה לכל תפקיד תהיה במידה הנדרשת לביצוע התפקיד בלבד[111]. עוד נקבע בתקנות כי בעל מאגר מידע ינקוט

---

107 בעניין זה ראו גם תקנות הגנת הפרטיות (אבטחת מידע), התשע"ז-2017.

108 בגודל כולל של 5.56 TB.

109 סעיף 7 לחוק.

110 מאגר מידע מוגדר בחוק כאוסף נתוני מידע, המוחזק באמצעי מגנטי או אופטי והמיועד לעיבוד ממוחשב, למעט אוסף לשימוש אישי שאינו למטרות עסק; או אוסף הכולל רק שם, מען ודרכי התקשרות, שכשלעצמו אינו יוצר אפיון שיש בו פגיעה בפרטיות לגבי בני האדם ששמותיהם כלולים בו, ובלבד שלבעל האוסף או לתאגיד בשליטתו אין אוסף נוסף.

111 תקנה 8 (א).

אמצעים מקובלים בנסיבות העניין, ובהתאם לאופי המאגר וטיבו, כדי לוודא כי הגישה למאגר ולמערכות המאגר נעשית בידי בעל הרשאה המורשה לכך בלבד, לפי רשימת ההרשאות התקפות[112]. התקנות קובעות שלוש רמות של מאגרי מידע, שעליהן חלות רמות אבטחה שונות בהתאם לסיכוני האבטחה שמייצרים מאגרי המידע.

במסמך מדיניות הגנת הסייבר של משרד החוץ צוין כי מערכות המידע במשרד מכילות בין היתר מידע על עובדים שהוא בגדר צנעת הפרט, הנדרש במסגרת תהליכי העבודה התקינים, וכי הנהלת המשרד מחויבת להגן על מידע זה בהתאם להוראות הדין, לרבות תקנות הגנת הפרטיות, כדי למזער את הסיכון לפגיעה בזכות העובדים לפרטיות. בהקשר זה יצוין כי בדצמבר 2019 מונה קב"ט המשרד גם כ"ממונה על אבטחת מידע", כהגדרתו בתקנות הגנת הפרטיות.

בבדיקה שעשה משרד מבקר המדינה בכונן X ברשת מסוימת שלכלל משתמשי הרשת הייתה הרשאת גישה אליו נמצאו עשרות מסמכים המכילים מידע פרטי-אישי ובהם ספרייה שלמה, שכוללת מסמכי הערכות של עובדים; חוות דעת תעסוקתיות של מכוני מיון והשמה על עובדים; קובץ שהכיל מידע בנוגע לדרגות השכר של 728 עובדים במשרד; מידע על מימון לימודים לעובדים; בקשה להסגרה של ישראלי השוהה בחו"ל, שבה פורטו העבירות שבהן הוא מואשם ונכלל צו המעצר שהוצא לו בישראל; מסמך המתכלל מידע על 2% מהעובדים שהוערכו כחזקים ביותר ו-2% מהעובדים שהוערכו כחלשים ביותר באחת היחידות במשרד לשנת 2015.

תמונה 1: **2% מהעובדים שהוערכו כחלשים ביותר לשנת 2015 באחת היחידות במשרד**

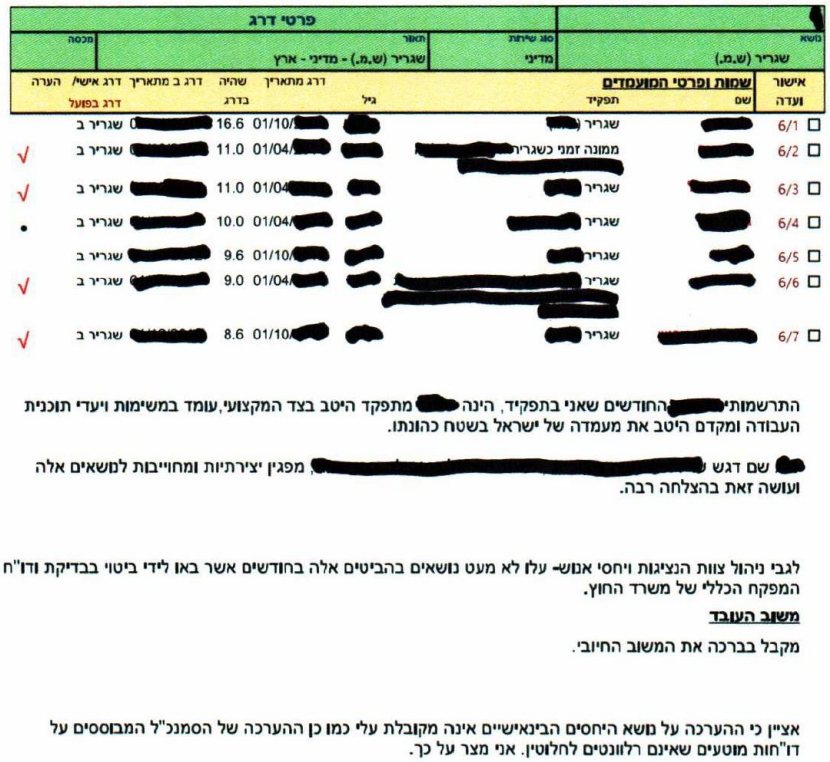
מספר הערכות	ציון מעריך	שם מעריך	הפרש	ממוצע מעריך	ציון סופי	שם פרטי	שם משפחה	מספר זהות	שנת הערכה
1	12	[redacted]	12.05909	0	12.05909	[redacted]	[redacted]	[redacted]	2015
12	12	[redacted]	-2.338812	14.62375	12.28494	[redacted]	[redacted]	[redacted]	2015
14	12	[redacted]	-2.317159	14.63856	12.3214	[redacted]	[redacted]	[redacted]	2015
4	13	[redacted]	-0.78723	13.53906	12.75183	[redacted]	[redacted]	[redacted]	2015
2	12	[redacted]	-0.289353	13.07188	12.78253	[redacted]	[redacted]	[redacted]	2015
1	13	[redacted]	12.98769	0	12.98769	[redacted]	[redacted]	[redacted]	2015

המקור: משרד החוץ.

כמו כן נמצא מסמך (בהיקף של 977 עמודים) של ועדת דרגים של אגף משאבי אנוש והדרכה מאפריל 2022 שנשא סיווג "שמור-אישי" וכלל שמות ופרטים של עשרות מועמדים לכמה משרות שהיו אמורות להידון בוועדת הדרגים, כולל סימונים ליד שמותיהם של עובדים שהצטיינו וליד שמותיהם של עובדים שקיימת לגביהם לפחות הערת משמעת אחת בתוקף. כמו כן, לגבי כל מועמד פורטו עיקרי ההערכות המילוליות של המעריך הישיר והעקיף וכן תוצאות ההערכה של המועמד בכמה ממדי הערכה. ליותר מ-1,000 עובדים של המשרד הייתה הרשאת גישה למסמך זה.

[112] תקנה 9 (א).

תמונה 2 : **דוגמה לדף ריכוז מועמדים שנדונו בוועדת הדרגים, כולל הערכת המנהל העקיף של העובד המוערך**



נושא		סוג שיחות	תאור	פרטי דרג						
שגריר (ש.מ.)		מדיני	שגריר (ש.מ.) - מדיני - ארץ							מכסה
אישור ועדה	שמות ופרטי המועמדים שם	תפקיד	גיל	דרג מתאריך	שהיה בדרג	דרג ב מתאריך	דרג אישי/ דרג בפועל	הערה		
6/1		שגריר		01/10/	16.6		שגריר ב			
6/2		ממונה זמני כשגריר		01/04/	11.0		שגריר ב	√		
6/3		שגריר		01/04	11.0		שגריר ב	√		
6/4		שגריר		01/04/	10.0		שגריר ב	•		
6/5		שגריר		01/10/	9.6		שגריר ב			
6/6		שגריר		01/04/	9.0		שגריר ב	√		
6/7		שגריר		01/10/	8.6		שגריר ב	√		

התרשמותי [redacted] החודשים שאני בתפקיד, הינה [redacted] מתפקד היטב בצד המקצועי,עומד במשימות ויעדי תוכנית העבודה ומקדם היטב את מעמדה של ישראל בשטח כהונתו.

שם דגש [redacted] מפגין יצירתיות ומחוייבות למשאים אלה ועושה זאת בהצלחה רבה.

לגבי ניהול צוות הנציגות ויחסי אנוש- עלו לא מעט נושאים בהביטים אלה בחודשים אשר באו לידי ביטוי בבדיקת ודו"ח המפקח הכללי של משרד החוץ.

משוב העובד

מקבל בברכה את המשוב החיובי.

אציין כי ההערכה על נושא היחסים הבינאישיים אינה מקובלת עלי כמו כן ההערכה של הסמנכ"ל המבוססים על דו"חות מוטעים שאינם רלוונטים לחלוטין. אני מצר על כך.

המקור : משרד החוץ.

ממצאי הביקורת מלמדים כי משרד החוץ לא קיים את הוראות חוק הגנת הפרטיות ותקנותיו, וכי בניגוד למתחייב מהוראות הדין ניתנה לכלל משתמשי הרשת המסוימת גישה לכונן X הכולל מסמכים רגישים רבים עם מידע אישי-פרטי, דבר המעלה חשש לפגיעה בפרטיותם של עובדי המשרד ואזרחים.

בהקשר זה יצוין כי נציג משרד מבקר המדינה התריע בעת ביקור במשרד החוץ לפני נציג המשרד על הימצאותו של מידע פרטי בכונן האמור ללא שהוגבלה הגישה אליו, אולם בדיקה נוספת שנעשתה בחלוף חודש וחצי העלתה כי מידע זה נותר בכונן וטרם הוגבלה הגישה אליו.

נוכח רגישות המסמכים שאותרו בכונן האמור, ובמטרה לצמצם את חשיפתם לגורמים שאינם מורשים, משרד מבקר המדינה עדכן במהלך הביקורת את נציגי אגף התקשוב ונציגי בטמ"ח במשרד החוץ בדבר ממצאיו.

בינואר 2025 עדכן משרד החוץ את משרד מבקר המדינה כי הגישה לכונן זה נחסמה לכלל המשתמשים ברשת וכן מונה עובד לסידור המידע בספריות שהיו בכונן זה.

על משרד החוץ להידרש לנושא בצורה רוחבית ולנקוט צעדים שיבטיחו שהמידע השמור במערכות המשרד יהיה זמין רק לעובדים שנדרשים לו לצורך עבודתם.

ביצוע בקרות

תקנות הגנת הפרטיות (אבטחת מידע), התשע"ז-2017, מחייבות לבצע בקרה על מנגנון הרשאות[113]. בנוהל של אגף התקשוב שאושר באפריל 2022 צוין כי באחריות הגורם המקצועי במשרד לבצע סקירת הרשאות במערכות שבהן הוא המשתמש המוביל או שבהן הוא מוגדר מנהל המאגר, ולוודא כי הרשאות העובדים תואמות את הצרכים העסקיים.

נמצא כי אגף התקשוב במשרד ובטמ"ח לא ערכו ביקורת סקירת הרשאות על הכוננים ברשת שנבדקה.

משרד החוץ השיב כי אי-ביצוע הבקרות נובע מהיעדר כוח אדם לתפעול ובקרה על ההרשאות. יצוין כי המשרד קידם אל מול נציבות שירות המדינה תקנון של משרות נוספות בתחום הגנת הסייבר ואושרו שלוש משרות נוספות חדשות.

<u>מניעת דלף מידע</u>

נמצאו ליקויים בכל הנוגע למניעת דלף מידע מרשתות המחשוב במשרד החוץ.

☆

ממצאי פרק זה שמסכמים את הבדיקה בנושא הגנה על המידע ברשתות המחשוב במשרד החוץ - חמורים. ממצאים אלו חושפים ליקויים מהותיים בכל הנוגע להגנה על המידע. ליקויים אלו אינם עולים בקנה אחד עם הוראות הדין ועם הנחיות הגורמים המנחים.

אחד מהליקויים החמורים שנמצאו נגע לגישה לכונן שהיה פתוח לכלל משתמשי רשת מסוימת במשרד ושהכיל עשרות אלפי מסמכים, חלקם כוללים מידע רגיש כגון מידע אישי-פרטי.

---

113 ראו תקנה 8(א) ותקנה 9(ג) לתקנות.

תרשים 9: **מסמכים הכוללים מידע אישי, שהיו נגישים לכלל משתמשי רשת מסוימת במשרד**

על פי נתוני משרד החוץ, בעיבוד משרד מבקר המדינה.

ממצאי הביקורת משקפים תרבות ארגונית לקויה במשרד החוץ בכל הנוגע לשמירה על מידע ולהגנה על מידע רגיש ופרטי. לנוכח הליקויים האמורים והחשש שייגרם דלף מידע שעשוי לפגוע בפרטיותם של אנשים, על מנכ"ל משרד החוץ לנקוט ללא דיחוי צעדים שיבטיחו את תיקונם. בכלל זה, המשרד נדרש להשלים את גיבוש הנוהל הנוגע לסיווג נכסי המידע; להשלים את בחינתן של הרשאות הגישה שניתנו לספריות שונות, וזאת במטרה להבטיח כי הגישה לכל אחת מהספריות תינתן רק לעובדים שהמידע נדרש להם לצורך עבודתם; לבצע בדיקה מעמיקה בנוגע לכלל המסמכים הנמצאים ברשת שנבדקה, באופן שיאפשר למחוק מסמכים הכוללים מידע רגיש ושאינם נדרשים עוד ולהגביל את הגישה למסמכים אחרים רק לעובדים שהמידע דרוש להם לצורך עבודתם. זאת ועוד, הנהלת המשרד נדרשת לוודא כי בדיקה דומה תיערך גם בנוגע לתיקיות ברשתות נוספות ובכל מקום אחסון אחר של קבצים ומידע ברשתות המשרד.

הליקויים שהועלו עשויים אף ללמד כי לעובדים אין מודעות רבה בכל הקשור לנושא אבטחת מידע והגנת הפרטיות. לפיכך על משרד החוץ לנקוט צעדים להעלאת מודעות העובדים לסיכונים הטמונים בנושא זה, ולהטמיע את הפעולות הנדרשות מהם בנושא זה, בין היתר באמצעות ביצוע הדרכות ובקרות עיתיות.

עדכניות תשתיות מערכות המידע במשרד החוץ

רכיבי מערכות המידע (קושחה ותוכנה) כגון שרתים ומתגים עלולים להיות חשופים לפגיעויות (להלן גם חולשות - Vulnerabilities) מסיבות שונות: פיתוח שגוי או לא עקבי של מוצר, דרישות אבטחה לא מספקות בשלב הפיתוח, גילוי חולשות חדשות במערכות מידע ופרוטוקולי תקשורת וכיוצא באלה[114]. חולשות אלה עלולות לחשוף את מערכות המידע בארגון לפעילות עוינת מצד תוקף (פנימי או חיצוני).

[114] חולשה מוגדרת כפגיעות בעיצוב, הטמעה, תפעול או בקרות פנימיות של מערכת (הנחיית יה"ב 5.15, "מדיניות עדכון מערכות מידע בממשלה" [להלן - הנחיה 5.15], סעיף 4 וסעיף 7.1).

ככלל, עם התגלותה של חולשה חדשה, היצרן פועל לפתח עדכון לתוכנה ("טלאי"), שהתקנתו במערכת אמורה להתמודד עם החולשה שהתגלתה ולאיינה. בד בבד, לאחר פרסום בדבר קיומה של החולשה, נוצר פער שבו תוקפים מנצלים את פרסום החולשה לתקיפת המערכות עד לעדכונן על ידי טלאים שפורסמו או על ידי בקרות מפצות. פרק זמן זה מוגדר קריטי, ועל גורמי אבטחת המידע לפעול במהירות וביעילות לעדכון המערכות או לביצוע בקרות מפצות כדי לוודא שהארגון אינו פגיע עוד לחולשה הרלוונטית.

מרשם הפגיעויות הלאומי האמריקאי NVD (National Vulnerability Database) של המוסד הלאומי לתקינה וטכנולוגיה בארה"ב (National Institute of Standards and Technology - NIST) מרכז מידע על פגיעויות המתגלות ברכיבי מערכות מידע. הפגיעויות המתגלות[115] מתועדות ונרשמות. היות שהשפעתן של הפגיעויות על רכיבי מערכות המידע אינה זהה, ה-NVD מגדיר לכל פגיעות דירוג המתאר את דרגת החומרה האיכותנית של הפגיעות בסולם של 1 - 10 (CVSS - Common Vulnerability Scoring System); דירוג של 7.0 - 8.9 משקף דרגת חומרה גבוהה ודירוג של 9.0 - 10.0 משקף דרגת חומרה קריטית[116]. הימנעות מהתקנת עדכוני האבטחה חושפת את רכיבי מערכות המידע שלא עודכנו לפגיעויות קריטיות, לרבות כאלו שנעשה בהן שימוש מוכח על ידי תוקפי סייבר ברחבי העולם[117].

לפיכך בתקנות הגנת הפרטיות[118], בהנחיות יה"ב[119] ובהנחיות שב"כ נקבעו הוראות בדבר הצורך לשמור על עדכניות מערכות הארגון וכאלה האוסרות שימוש בגרסאות מערכת שהגיעו לסוף תקופת התמיכה שלהם. אשר להתקנת טלאי אבטחה, בהנחיות יה"ב נקבע כי יש ליישם בקרות מפצות ולערוך ניהול סיכונים עד להתקנת הטלאי, ובכל מקרה יש להתקין את הטלאי לפי לוחות הזמנים שנקבעו בהנחיה בהתאם לרמת חומרתו.

סביבות מחשוב כוללות מערכות מסוגים שונים, כגון שרתים, תחנות עבודה, מתגים, חומות אש (FW) ומדפסות.

תשתית מחשוב מסוימת

מחזור החיים של תשתית מחשוב מסוימת, כולל **תקופת תמיכה עיקרית** - תקופה שבה ככלל היצרן מפרסם עדכונים בנוגע למערכת, לרבות עדכוני אבטחה בדרגות חומרה שונות, ומאפשר שינויים והתאמות במוצר על פי הדרוש לארגון; **תקופת תמיכה מוארכת** - תקופה שבה הארגון מקבל מהיצרן עדכוני אבטחת מידע ואפשרות לתמיכה בתשלום; **והתקופה שלאחר סוף התמיכה במוצר** (להלן - סוף התמיכה או סוף מחזור החיים) - תקופה שבה חדל היצרן מלפתח עדכוני אבטחה למוצר, אינו מספק לו עוד תמיכה וממליץ על מעבר למוצר חלופי (או גרסה עדכנית של אותו מוצר). לפיכך, שימוש בגרסה לאחר מועד "סוף התמיכה" הרלוונטי לגביה עלול לחשוף את המערכת לחולשות שיפורסמו ממועד זה ואילך, וכן למצב שבו תתרחש תקלה קריטית במערכת שלא תיתמך עוד על ידי היצרן.

נמצאו פערים בעדכניות תשתיות ומערכות המידע.

---

115 Common Vulnerabilities and Exposures.

116 אתר NIST תחת הכותרת Vulnerability Metrics.

117 לדוגמה, במאי 2019 פרסם יצרן של מוצרי אבטחת מידע עדכון אבטחה לפגיעות קריטית שהתגלתה באחד ממוצריו. כעבור שנתיים, בספטמבר 2021, העלתה הרשות האוסטרלית הממשלתית לאבטחת מידע כי במקרה שבו לא בוצע העדכון, הפגיעות נוצלה במערכת של ישות אוסטרלית Australian Signals Directorate, ASD Cyber Threat Report 2022 - 2023.

118 תקנות הגנת הפרטיות (אבטחת מידע), התשע"ז-2017, סעיף 13: "לא ייעשה שימוש במערכות שהיצרן לא תומך בהיבטי אבטחה שלהן אלא אם כן ניתן מענה אבטחתי מתאים".

119 הנחיית יה"ב 5.15, "מדיניות עדכון מערכות מידע בממשלה".

על משרד החוץ להיערך מבעוד מועד לקראת סוף התמיכה של תשתיות מחשוב במשרד, ובכלל זה להכין תוכנית עבודה סדורה ולוחות זמנים להחלפתן ולעקוב בהמשך אחר הנושא ולבצע החלפות מבעוד מועד.

<u>רכיבי מחשוב נוספים ברשתות משרד החוץ</u>

נמצאו רכיבי מחשוב נוספים שאינם נתמכים על ידי היצרן.

☆

ממצאי פרק זה מלמדים כי קיימים פערים בכל הנוגע לתשתית המחשוב של משרד החוץ. למצב זה של תשתית המחשוב עלולות להיות כמה השלכות ובהן כאלה העשויות לפגוע ברציפות התפקודית של המשרד וביכולתו לספק שירותים חיוניים.

על מנהל אגף התקשוב לשקף להנהלת המשרד ולוועדת ההיגוי להגנת הסייבר את הפער הקיים בין תשתית המחשוב הקיימת לזו הנדרשת 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 שחושף את המשרד למתקפות אפשריות של גורמים עוינים ועל יה"ב והשב"כ לבצע בקרה כדי לוודא כי הפער הקיים בתשתיות המחשוב מטופל כנדרש.

הגנה על רשת מסוימת במשרד החוץ

נמצאו פערים בהגנה על רשת מסוימת במשרד החוץ.

הזדהות משתמשים וניהול הרשאות

ההגנה הלוגית[120] על המידע האגור במערכות המידע והתקשורת של הארגון נועדה בין היתר לקבוע את המגבלות הארגוניות על הנגישות למידע הארגוני ולהגדיר את השימוש המותר לכל אחד מהמשתמשים במערכות של הארגון על בסיס עקרונות "הצורך לדעת" ו"מינימום הרשאות לביצוע התפקיד". כאשר ההגנה הלוגית אינה מוגדרת כהלכה או שאינה מיושמת באופן מלא, תשתיות המחשוב של הארגון והמידע והתהליכים הנסמכים עליהן חשופים לסיכונים, כגון דליפת מידע רגיש או מסווג של הארגון לגורמים שאינם מורשים לקבלו, שיבוש המידע או פגיעה בזמינותו.

קביעת מדיניות לגבי מערך הזדהות[121] אפקטיבי של המשתמשים בעת הכניסה לרשת הארגונית ומימושה בפועל, וכן קביעת מדיניות מערך ההרשאות של הארגון וניהול המערך באופן סדור, הם נדבכים מרכזיים בהגנה הלוגית.

גורמים עוינים עלולים להשתמש במגוון שיטות כדי להשיג גישה לא מורשית לרשתות הארגון. כאשר מדובר במערכות רגישות, דוגמת מערכות המידע במשרד החוץ, עלולה השתלטות גורמים עוינים עליהן לגרום נזק במישור הביטחוני, הכלכלי והתדמיתי של מדינת ישראל.

---

120 הגנה המשתמשת בתוכנות ובנתונים כדי להגן על הזמינות של הנתונים והתהליכים הממוחשבים, שלמותם וסודיותם.

121 הזדהות היא נתון המאפשר לזהות את המשתמש או הרכיב או השירות באופן חד-ערכי.

הזדהות משתמשים במערכות הממוחשבות

מערך ההזדהות בעת הגישה למערכות הארגון נועד לוודא כי הגישה למערכת מידע, לרכיב תקשורת או למידע מוגבלת למורשים בלבד. כמו כן נועד מערך ההזדהות למנוע מתוקף פוטנציאלי להתחזות למשתמש אחר או לנצל את מנגנוני הזיהוי של שירותים ויישומים ולהתחזות אליהם, בין היתר באמצעות כלים לניחוש סיסמאות, או כלים אחרים המשבשים את פעולתם של כלי אבטחת הכניסה.

אמצעי הזדהות לצורך כניסה לרשתות המשרד

הנחיות לקביעת סיסמת משתמש - בהנחיות יה"ב נקבעו הוראות הנוגעות לאורכה המינימלי של הסיסמה ולמורכבותה, כגון צירוף של אותיות, ספרות ותווים מיוחדים, כדי להקשות על תקיפה באמצעות כלים לניחוש סיסמאות[122]; מספר הפעמים שלא ניתן לחזור על סיסמה קיימת; תדירות מינימלית להחלפת סיסמה ומספר ניסיונות כושלים של הקשת סיסמה שלאחריהם יינעל החשבון. בהנחיית יה"ב נקבעו הוראות שונות למשתמשים רגילים ולמשתמשים חזקים או משתמשים אפליקטיביים, זאת בשל הסיכון המוגבר הקיים במצב של השתלטות גורם עוין על הרשאת גישה של משתמשים חזקים. הנחיות השב"כ כוללות אף הן התייחסות לנושא, ובכלל זה לצורך בסיסמאות ארוכות ומורכבות, למספר הפעמים שלא ניתן לחזור על סיסמה קיימת ולתדירות החלפת הסיסמה.

משרד מבקר המדינה בחן אם הנחיות משרד החוץ והמצב בפועל בעניין זה ברשתות המשרד תואמים את הנחיות הגופים המנחים. ממצאי הבחינה העלו פערים.

נמצאו ליקויים בהזדהות משתמשים לרשתות המחשב במשרד החוץ.

☆

מערך ההזדהות המיושם בעת הגישה למערכות הארגון נועד לוודא כי הגישה למערכת מידע, לרכיב תקשורת או למידע מוגבלת למורשים בלבד, וכן מטרתו למנוע מגורמים עוינים להשיג גישה לרשתות הארגון. כאשר מדובר במערכות רגישות, כדוגמת מערכות המידע במשרד החוץ, עלולה השתלטות עוינת או לא מורשית על הגישה לרשת לגרום לנזק במישור הביטחוני, הכלכלי והתדמיתי של מדינת ישראל.

ממצאי הביקורת העלו ליקויים במערך ההזדהות שקבע משרד החוץ ויישם בפועל. ליקויים מן הסוג הזה פוגעים ברמת ההגנה של המערכות, מעמידים בסיכון את שלמות המידע האצור בהן, סודיותו וזמינותו, ומחייבים תיקון.

על משרד החוץ לתקן את הליקויים בתחום זה בהתאם להנחיות הגופים המנחים.

ניהול הרשאות גישה למערכות הממוחשבות

על פי הנחיית יה"ב, יש להגביל את גישתם של עובדי הארגון למידע האגור במערכות הארגון לצורך צמצום אפשרויות הפגיעה במידע על ידי העובדים עצמם, או על ידי גורמים חיצוניים שישיגו גישה בלתי מורשית למערכות הארגון. בבסיס הנחיה זו עומד עקרון האחריות האישית של העובד, אשר נדרש להגן על המידע שאליו הוא נחשף במהלך עבודתו, ולצורך זה מוגדר לו שם משתמש ייחודי. בהנחיה אחרת של יה"ב נקבע כי הרשאת גישה של עובד למערכות המידע תינתן על פי המידע הדרוש לו למילוי תפקידו, על פי העיקרון של הצורך לדעת (need to know) ועל פי העיקרון של

[122] על פי מסמך של חברת מיקרוסופט Security policy settings מ-17.2.23, סיסמה ארוכה העושה שימוש גם בתווים ייחודיים, יוצרת מספר רב של קומבינציות אפשריות ומכאן מקשה על חשיפת הסיסמה.

מתן מספר ההרשאות המזערי הנדרש לצורך ביצוע העבודה (least privilege). עיקרון זה נקבע גם בנוהלי משרד החוץ.

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

☆

הגבלת גישתם של עובדי הארגון למידע האגור במערכות הארגון נועדה לצמצם אפשרויות לפגיעה במידע על ידי העובדים עצמם או על ידי גורמים חיצוניים שישיגו גישה בלתי מורשית למערכות הארגון. ניתוח הנתונים שביצע משרד מבקר המדינה מלמד כי קיימים פערים בכל הנוגע לניהול הרשאות הגישה למערכות המידע במשרד החוץ.

מומלץ כי משרד החוץ ינקוט צעדים להבטחת ניהול תקין של הרשאות הגישה לרשתות המשרד.

משרד החוץ השיב למשרד מבקר המדינה באוקטובר 2025 כי לאחרונה נערך דיון ובו הוצגו הפערים בניהול משתמשים והרשאות במשרד. בדיון זה התקבלה החלטה עקרונית על הקמת יחידה ארגונית אשר תישא באחריות כוללת לניהול משתמשים והרשאות בארץ ובחו"ל. במסגרת ההיערכות להקמת היחידה החל תהליך למיפוי ולניתוח התהליכים התפעוליים הקיימים בהיבטי משאבי אנוש, ומתוכננות התאמות ככל שיידרש.

בקרה על מערך ניהול ההרשאות

בהנחיית יה"ב נקבע כי מפעם לפעם תיערך בקרה על מערך ניהול ההרשאות כדי לוודא את יישום ההנחיות והעקרונות שנקבעו: אחת לחצי שנה ייבחנו ההרשאות של משתמשים חזקים ויבוטלו הרשאות עודפות; אחת לשנה יוודא מנהל הגנת הסייבר עם מנהלי המחלקות במשרד הממשלתי כי ההרשאות שניתנו לעובדי המחלקה עודן נדרשות. הוראות דומות נקבעו בהנחיות השב"כ. גם בנוהלי משרד החוץ נקבע כי כל בעל נכס מידע במשרד ייזום אחת לשנה לפחות סקר הרשאות גישה למאגר עבור כלל המשתמשים; הרשאות שאינן נדרשות יבוטלו; וסקר הרשאות יבוצע גם במסגרת סקרי סיכוני סייבר שייזום ממונה הגנת הסייבר מפעם לפעם.

משרד מבקר המדינה בחן את יישום ההנחיות האמורות. בהתאם להנחיות, משרד החוץ נדרש לבצע בסך הכול שבע בקרות בשנים 2021 - 2024 (עד יולי 2024) לבחינת הרשאות של משתמשים חזקים, וארבע בקרות לבדיקת ההרשאות של משתמשים רגילים.

הביקורת העלתה כי בשנים 2021 - 2024 (עד יולי 2024) בוצעה בדיקה אחת בלבד, בינואר 2023, מתוך שבע בדיקות נדרשות לבחינת הרשאות של משתמשים חזקים. הבדיקה בוצעה בקבוצה אחת של משתמשים חזקים בחלק מרשתות המשרד. עוד נמצא כי אגף התקשוב במשרד ביצע בשנים 2021 - 2024 בקרות לזיהוי משתמשים שלא נכנסו לרשת זה 90 יום או 180 יום, ומשתמשים שלא החליפו סיסמה זמן רב. עם זאת, ההרשאות של כל המשתמשים לא נשלחו למנהלי המחלקות במשרד לצורך בחינה אם הן עדיין נדרשות ובאיזה היקף.

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.

משרד החוץ השיב כי באוגוסט 2024 החל בפרויקט סקירת הרשאות שהתמקד בצמצום סיכוני הסייבר על ידי הערכה שיטתית של רמות ההרשאה הקיימות, זיהוי הרשאות עודפות והבטחת הגישה המינימלית ההכרחית לכל תפקיד. כמו כן נערכה סקירת הרשאות למשתמשים במספר מערכות מידע.

משרד מבקר המדינה מציין לחיוב את יישום פרויקט סקירת ההרשאות וממליץ כי הפרויקט יורחב גם לסקירת ההרשאות של המשתמשים בכל יחידה עסקית. על משרד החוץ לגבש גם תוכנית עבודה סדורה לביצוע כל הבקרות הנדרשות בהתאם להנחיות הגורמים המנחים, ליישמה באופן שיטתי ולטפל בפערים שיעלו בבקרות. זאת כדי להקטין את החשיפה לסיכון של גישה לא מורשית למערכות המידע של המשרד.

הגנה על מאגרי מידע לפי חוק הגנת הפרטיות

חוק הגנת הפרטיות, התשמ"א-1981[123], מחייב בעלים של מאגר מידע, מחזיק במאגר מידע[124] ומנהל מאגר מידע להגן על מאגרי מידע שברשותם כהגדרתם בחוק. מאגר מידע מוגדר בחוק כאוסף נתוני מידע, המוחזק באמצעי מגנטי או אופטי ומיועד לעיבוד ממוחשב[125]. החוק מגדיר "מידע" כנתונים על אישיותו של אדם, מעמדו האישי, צנעת אישיותו, מצב בריאותו, מצבו הכלכלי, הכשרתו המקצועית, דעותיו ואמונתו, ו"מידע רגיש" כנתונים על אישיותו של אדם, צנעת אישיותו, מצב בריאותו, מצבו הכלכלי, דעותיו ואמונתו[126].

תקנות הגנת הפרטיות (אבטחת מידע), התשע"ז-2017 (להלן - תקנות הגנת הפרטיות), מפרטות את החובות המוטלות על מי שאחראי לאבטחת המידע של מאגר המידע, כאשר רמת האבטחה הנדרשת נקבעת בהתאם לרגישות המידע שמנוהל או מוחזק במאגר[127], ובהתאם למספר האנשים שיש מידע עליהם במאגר ומספר המורשים לגשת אליו[128]. בחוק נקבע כי גופים מסוימים - ובהם גוף ציבורי כהגדרתו בחוק, הכולל משרדי ממשלה ומוסדות מדינה אחרים - נדרשים למנות ממונה על אבטחת מידע שיהיה אחראי לאבטחת המידע במאגרים שברשות הגוף שבו הוא עובד. כמו כן, על פי התקנות, מאגרי מידע שהם בבעלות משרד ממשלתי נדרשים להיות ברמת אבטחה בינונית לפחות.

במסמך מדיניות הגנת הסייבר ואבטחת המידע במשרד החוץ שאושר באפריל 2018 קבע המשרד כי מידע על עובדים שהוא בגדר צנעת הפרט נשמר במאגרי מידע ארגוניים, והנהלת המשרד מחויבת להגן עליהם בהתאם להוראות הדין, לרבות תקנות הגנת הפרטיות, כדי למזער את הסיכון לפגיעה בזכות העובדים לפרטיות.

במשרד החוץ מנוהלים עשרות מאגרי מידע, חלקם כוללים מידע אישי-פרטי, מידע כלכלי, ומידע רפואי.

<u>יישום חוק הגנת הפרטיות ותקנותיו במשרד החוץ</u>

משרד מבקר המדינה בחן את יישום חוק הגנת הפרטיות ותקנותיו במשרד החוץ. להלן הממצאים.

---

123 ב-14.8.24 פורסם ברשומות תיקון מקיף לחוק הגנת הפרטיות, אך התיקון ייכנס לתוקף רק ב-14.8.25.

124 "מחזיק", לעניין מאגר מידע, הוא מי שמצוי ברשותו מאגר מידע דרך קבע והוא רשאי לעשות בו שימוש.

125 למעט אוסף לשימוש אישי שאינו למטרות עסק; או אוסף הכולל רק שם, מען ודרכי התקשרות, שכשלעצמו אינו יוצר אפיון שיש בו פגיעה בפרטיות לגבי בני האדם ששמותיהם כלולים בו, ובלבד שלבעל האוסף או לתאגיד בשליטתו אין אוסף נוסף.

126 וכן מידע ששר המשפטים קבע בצו, באישור ועדת החוקה, חוק ומשפט של הכנסת, שהוא מידע רגיש. יובהר כי עם כניסת תיקון 13 לתוקף ב-14.8.25 חלו שינויים בהגדרות של מונחים שונים בחוק, כגון "מידע בעל רגישות מיוחדת" (במקום "מידע רגיש"), "בעל שליטה במאגר מידע" (במקום "בעל מאגר") ו"פנקס רשם מאגרי מידע" (במקום "המרשם") וכי דוח זה מתייחס להגדרת המונחים טרם כניסת תיקון 13 לתוקף.

127 למשל, מידע רפואי של אדם ומידע על מצבו הכלכלי של אדם או שינוי בו.

128 התוספת הראשונה לתקנות; רמת אבטחה גבוהה נדרשת במאגר מידע שיש בו אחד מסוגי המידע הרגישים המפורטים בתקנות, ושיש בו מידע על אודות 100,000 אנשים ומעלה, או שמספר בעלי ההרשאה בו עולה על 100.

לוח 2 : **יישום חוק הגנת הפרטיות ותקנותיו במשרד החוץ**

הנושא	ההנחיות המחייבות	הממצאים
מיפוי מאגרי המידע	התקנות[129] מחייבות לערוך מיפוי של כלל מאגרי המידע כדי לקבוע תחילה אם המאגרים עונים על הגדרת מאגר מידע לפי החוק; אם כן, יש לקבוע - בהתאם לסוגי המידע שמנוהלים או מוחזקים במאגר, ובהתאם למספר האנשים שיש מידע עליהם במאגר ולמספר המורשים לגשת אליו - את רמת האבטחה הנדרשת והחובות המוטלים על בעל המאגר.	ביוני 2023 ביצע משרד החוץ מיפוי של נכסי מערכות המידע ברשתות מסוימות של המשרד. במסגרת זו הוכן קובץ שכלל מיפוי של מערכות המידע או מאגרי המידע בכל רשתות המשרד, וכן מידע על ייעוד המערכת או המאגר, זהות המשתמשים בו, סוגי המידע שמנוהלים במאגר (רפואי, אישי, כלכלי...), מספר האנשים שבעניינם קיים מידע במאגר, מספר בעלי ההרשאות לגישה למאגר וסיכונים הצפויים בחשיפת המידע שבמאגר (להלן - קובץ המיפוי). **עיון בקובץ המיפוי העלה כי המידע שנכלל בקובץ המיפוי אינו שלם ועדכני - הקובץ כלל התייחסות גם למערכות שכבר הוחלפו במערכות חדשות יותר; המידע בנוגע לחלק ממאגרי המידע היה חלקי, ולא מולאו בו כלל הנתונים הנדרשים לצורך המיפוי. כך למשל לעיתים לא פורטו סוגי המידע שנכללים במאגר.** **עד אוקטובר 2024 טרם השלים משרד החוץ מיפוי מלא ועדכני של כלל מאגרי המידע שנמצאים ברשותו, ומכאן שאין ביכולתו לדעת איזו רמת אבטחה נדרשת לכל מאגר לפי התקנות, ואם רמת ההגנה הקיימת אכן עונה על הנדרש בתקנות.**
מיפוי מאגרי המידע	התקנות עוסקות במאגר המידע כחלק ממערכת מידע או כמאגר בפני עצמו, אך הן מחייבות להגן גם על מידע שנשמר בקובצי Excel שמופקים מתוך מערכות ומאגרים אלו, וכן על קובצי Excel שנוצרו לראשונה על ידי עובדים.	**במסגרת הביקורת נמצאו קובצי Excel שענו על הגדרת מאגר מידע לפי החוק, חלקם כללו מידע אישי-פרטי, כגון מידע רפואי, מידע כלכלי ועוד. קבצים אלו לא נכללו ברשימה של מאגרי מידע שהוכנה במשרד, ולא נקבעה רמת האבטחה הנדרשת לגביהם בהתאם לתקנות.**

129 סעיפים 4 ו-5 לתקנות.

הנושא	ההנחיות המחייבות	הממצאים
 **רישום מאגרי המידע**	החוק קובע (סעיף 8) כי יש לרשום את מאגר המידע בפנקס מאגרי המידע ולכלול בבקשה לרישום המאגר גם פרטים על אודות זהות בעל מאגר המידע המחזיק במאגר ומנהל המאגר; מטרות הקמת מאגר המידע וסוגי המידע שייכללו במאגר.	**בפנקס מאגרי המידע במשרד המשפטים רשומים רק שלושה מאגרי מידע של משרד החוץ[130], אף שהמשרד מנהל עשרות מאגרים נוספים.**
 **מסמך הגדרות המאגר**	לפי תקנה 2, על בעל מאגר מידע להגדיר במסמך הגדרות מאגר עניינים שונים, כגון תיאור פעולות האיסוף והשימוש במידע, מטרות השימוש במידע וסיכונים עיקריים של פגיעה באבטחת המידע.	**אין בידי משרד החוץ מסמך הגדרות מאגר לכל מאגרי המידע שברשותו, שמפרט את כלל הנושאים הנדרשים לפי התקנות, למעט בנוגע למאגר הקונסולרי.**
 **נוהל אבטחת המידע**	תקנה 4 מחייבת לקבוע במסמך נוהל אבטחת מידע שיכלול התייחסות לכמה נושאים[131]. עוד נקבע כי ארגון שהוא בעל כמה מאגרי מידע רשאי לקבוע נוהל אבטחה כאמור במסמך אחד לעניין כל מאגרי המידע שברשותו, המצויים באותה רמת אבטחה.	**אין בידי משרד החוץ נוהל אבטחה כללי או פרטני למאגרי המידע שברשותו, למעט נוהל אבטחה שנכתב למאגר הקונסולרי.**
 **מסמך מבנה מאגר המידע ורשימת מערכותיו**	לפי תקנה 5, על בעל מאגר מידע להחזיק מסמך מעודכן של מבנה מאגר המידע וכן רשימת מצאי מעודכנת של מערכות המאגר[132]. בתקנות נקבע כי ארגון שהוא בעל כמה מאגרי מידע רשאי לקבוע את רשימת המצאי במסמך אחד לעניין כל מאגרי המידע שברשותו, המצויים באותה רמת אבטחה.	**אין בידי משרד החוץ מסמך מעודכן של מבנה מאגר המידע ורשימת מצאי למאגרי המידע שברשותו, למעט מסמך שנכתב למאגר הקונסולרי.**

130 מאגר connect.il שנרשם במאי 2013 וכלל מידע על ניהול קשרי משלחות מחו"ל בידי נציגי משרד החוץ; המאגר הקונסולרי שנרשם ביולי 2020; ומאגר מתמחים זרים בחקלאות שנרשם ביום 11.12.24.

131 המסמך צריך להתייחס לנושאים הבאים: האבטחה הפיזית והסביבתית של אתרי המאגר; הרשאות גישה למאגר המידע ולמערכות המאגר; אמצעי ההגנה על מערכות המאגר ואופן הפעלתם; הסיכונים שחשוף להם המידע שבמאגר ואופן הטיפול בהם; אופן התמודדות עם אירועי אבטחת מידע; אמצעי הזיהוי והאימות לגישה למאגר ולמערכות המאגר; אופן הבקרה על השימוש במאגר המידע, ובכלל זה תיעוד הגישה למערכות המאגר.

132 ובכלל זה מידע על תשתיות ומערכות חומרה, סוגי רכיבי תקשורת ואבטחת מידע; מערכות התוכנה המשמשות להפעלת מאגר המידע, לניהול המאגר ולתחזוקתו, לתמיכה בפעילותו, לניטור שלו ולאבטחתו; תוכנות וממשקים המשמשים לתקשורת אל מערכות המאגר ומהן; תרשים הרשת שפועל בה המאגר.

הנושא	ההנחיות המחייבות	הממצאים
 **מנגנון תיעוד אוטומטי על הגישה למערכות המאגר**	לפי תקנה 10 במערכות של מאגר מידע אשר חלה עליו רמת אבטחה בינונית או גבוהה, ינוהל מנגנון תיעוד אוטומטי שיאפשר ביקורת על הגישה למערכות המאגר (לוגים), ובכלל זה נתונים אלה: זהות המשתמש, התאריך והשעה של ניסיון הגישה, רכיב המערכת שאליו בוצע ניסיון הגישה, סוג הגישה, היקפה, ואם הגישה אושרה או נדחתה.	**נמצא כי בארבע מערכות מידע שנבדקו ברשת מסוימת, שנשמר בהן מידע אישי ושעל פי התבחינים נדרשת לגביהן רמת אבטחה בינונית או גבוהה - לא קיימים לוגים כנדרש בתקנות.**
 **ביצוע סקר סיכונים ומבדק חדירה**	בתקנה 5 נקבע כי במאגר מידע בעל רמת אבטחה גבוהה יבוצעו סקר לאיתור סיכוני אבטחת מידע וכן מבדק חדירות למערכות המאגר. עוד נקבע כי סקר סיכונים ומבדק החדירה ייערכו אחת ל-18 חודשים לפחות.	**נבדקו כמה מערכות מידע ברשת מסוימת במשרד החוץ, שנדרשת בהן רמת אבטחה גבוהה לפי התקנות, ונמצא כי לא נעשה להן סקר סיכונים או מבדק חדירה.**
 **ביצוע ביקורות תקופתיות**	בתקנה 3 נקבע כי הממונה על האבטחה יכין תוכנית לבקרה שוטפת על העמידה בדרישות תקנות אלה, יבצע אותה, ויודיע לבעל מאגר המידע ולמנהל המאגר על ממצאיו.	**נמצא כי קב"ט המשרד, שלפי מסמכי המשרד נקבע כאחראי על האבטחה בכל הנוגע להגנה על הפרטיות, לא הכין תוכנית לבקרה שוטפת על העמידה בדרישות התקנות, ולא נערכה ביקורת על עמידת מאגרי המידע שברשות המשרד בהוראות התקנות, למעט המאגר הקונסולרי.**
 **הקצאת משאבים לממונה על אבטחת המידע**	בתקנה 3 נקבע כי בעל מאגר המידע יקצה לממונה את המשאבים הדרושים לו לשם מילוי תפקידו.	**ממסמכי בטמ"ח עולה כי נושא ההגנה על הפרטיות שמצוי באחריותם נמנה עם הנושאים בתוכנית העבודה לשנת 2024, ובו עלו פערים מהותיים בין התוכנית לביצועה בפועל. בעבודת מטה שהוכנה בבטמ"ח במחצית הראשונה של 2024 כלל לא צוינו נתונים על שעות העבודה הנדרשות לביצוע המשימות של הגנה על הפרטיות ועל מאגרי המידע, ונרשם כי כלל לא בוצעו שעות עבודה במשימות אלו.**

הנושא	ההנחיות המחייבות	הממצאים
 **קביעת נהלים בתחום הגנת הפרטיות**	במסמך מדיניות הגנת הסייבר נקבע כי ראש חטיבת בטמ"ח, ראש אגף הון אנושי והדרכה וראש אגף תקשוב, כל אחד בתחום אחריותו ובתיאום עם האחרים, על פי הצורך, יפרסמו נהלים מחייבים הנגזרים ממדיניות ההגנה בסייבר. הנהלים יתייחסו, בין היתר, לדרישות אסדרה ולדרישות על פי תקנות הגנת הפרטיות.	**נמצא כי עד דצמבר 2024 לא פרסם משרד החוץ נהלים בכל הנוגע להגנה על מאגרי המידע לפי תקנות הגנת הפרטיות.**

על פי נתוני משרד החוץ, בעיבוד משרד מבקר המדינה.

מהאמור עולה כי משרד החוץ אינו מיישם באופן מלא את דרישות חוק הגנת הפרטיות ותקנותיו, ובכלל זה לא ביצע מיפוי מלא של המאגרים שברשותו; לא רשם את כלל מאגרי המידע שברשותו שחלה חובה לרשמם; לא קבע את רמת האבטחה הנדרשת בעניינם ולא נקט פעולות הנדרשות לפי החוק והתקנות כדי להגן עליהם באופן מספק. המשמעות של ליקויים אלו היא כי ללא מיפוי מקיף של כלל מאגרי המידע שברשותו, המשרד לא יכול לוודא כי הוא מגן על כלל המאגרים כנדרש.

זאת ועוד, היעדר מנגנון תיעוד אוטומטי לגישה לחלק ממאגרי המידע של המשרד לא מאפשר למשרד לאתר חדירה של גורם לא מורשה למערכות המאגר, בזמן אמת או בדיעבד. כמו כן, אי-ביצוע סקרי סיכונים ומבדקי חדירה למאגרים שבהם נדרשת רמת אבטחה גבוהה מונע מהמשרד מידע על פערים ברמת ההגנה המחייבים טיפול. נוסף על כך, ללא ביצוע של ביקורות תקופתיות על מאגרי המידע בכל הנוגע לעמידתם בדרישות התקנות, המשרד לא יכול לדעת מה רמת ההגנה בפועל על מאגרי המידע שברשותו, וייתכן שמאגרי המידע חשופים לסיכונים העלולים לפגוע בפרטיות המידע שנשמר בהם.

יצוין בהקשר זה כי העובדה שמשרד החוץ אינו מיישם באופן מלא את דרישות חוק הגנת הפרטיות ותקנותיו עלתה בביקורת זו גם בהקשרים נוספים. כך למשל הועלו בדוח זה ליקויים חמורים בכל הנוגע להימצאות מידע פרטי רגיש בכונן ברשת מסוימת של המשרד, הפתוח לכל משתמשי הרשת ללא כל מידור של הרשאות כנדרש לפי תקנות הגנת הפרטיות. כמו כן, גם בסקר סיכוני תקשוב שהוגש למשרד במאי 2024 צוין כי קיימים ליקויים בתחום הגנת הפרטיות, וכי הדבר חושף את המשרד לתביעות ציבוריות.

לנוכח חומרת הממצאים שהועלו בפרק זה העוסק בהגנה על מאגרי מידע לפי חוק הגנת הפרטיות, על הממונה על הגנת הפרטיות במשרד החוץ לגבש תוכנית עבודה מקיפה וסדורה, לרבות לוחות זמנים ומשאבים הנדרשים לטיפול בנושא הגנת הפרטיות, שתובא לאישור ועדת ההיגוי להגנת הסייבר ומנכ"ל המשרד. על התוכנית לכלול ביצוע של מיפוי מקיף ויסודי לפי תקנות הגנת הפרטיות של כלל מאגרי המידע הנמצאים ברשות המשרד, לרבות המידע המלא הנדרש כדי לקבל החלטה בנוגע לרמת ההגנה הנדרשת על מאגרי המשרד, וכן על המשרד לפעול ליישום התוכנית. כמו כן, על המשרד לפרסם נהלים שיסדירו את טיפולו בנושא ולקיים ביקורות תקופתיות, שבמסגרתן תיבחן עמידתם של כלל מאגרי המידע בתקנות הגנת הפרטיות, והן ישמשו ליצירת תוכנית עבודה לטיפול בפערים.

טיפול ועדת ההיגוי להגנת הסייבר בנושא הגנת הפרטיות

בהנחיות יה"ב נקבע כי הגנת הסייבר במשרדים תיושם בכפוף לחוקי מדינת ישראל הנוגעים לתחום הגנת המידע וסייבר ולרבות חוק הגנת הפרטיות ותקנותיו; באחריות ממונה הגנת הסייבר, מנהלי המשרד והמחלקה המשפטית לוודא כי כל יחידות המשרד פועלות בהתאם לחוק הישראלי, התקנות והרגולציות הנוגעות להיבטי הגנת הסייבר. כן נקבע כי ועדת ההיגוי תשמש מסגרת ניהולית לקבלת החלטות אסטרטגיות בתחום הגנת הסייבר ולביצוע בקרה ניהולית על יישום הגנת הסייבר במשרד.

משרד מבקר המדינה בחן אם ועדת ההיגוי עסקה בנושא זה במהלך השנים 2020 - 2024 וקיבלה החלטות בעניינו, להלן פרטים:

בישיבת ועדת ההיגוי להגנת הסייבר מפברואר 2020, שדנה בממצאי סקר סיכונים שנעשה למאגר הקונסולרי, צוין כי למשרד פערים בנוגע לעמידה בתקנות בכלל המאגרים שברשותו, ויש לגבש תוכנית לעמידת כלל מאגרי המשרד בתקנות אבטחת המידע עד לסוף שנת 2021, לרבות ביצוע סקרי סיכונים גם למאגרים אלו.

בישיבה נוספת של ועדת ההיגוי מאפריל 2021 אישרה הוועדה את תוכנית הפעולה להשלמת הפערים בכל הנוגע להגנה על המאגר הקונסולרי, ובאותה ישיבה צוין בסיכום הדיון כי אי-עמידה בדרישות החוק בישראל ובחו"ל חושפת את המשרד לסיכונים משפטיים ומדיניים.

בנובמבר 2022 קיבלה הוועדה דיווח כי הבקרה על ביצוע התוכנית לטיפול בפערים של המאגר הקונסולרי ורישום יתר המאגרים בוצעו באופן חלקי, והביצוע של משימות אלו יסתיים רק במרץ 2023. בנוגע לסקר סיכונים כולל בנושא הגנת הפרטיות, צוין שנדרש לבצעו כל 18 חודשים - הוא בוצע ב-2019 ויבוצע פעם נוספת בשנים 2022 - 2023. במצע לדיון שהוכן לקראת הישיבה הודגש כי קיימת אחריות אישית פלילית של מנכ"ל המשרד וראשי האגפים המנהלים את המאגרים לאי-רישום המאגרים ולאי-עמידה בתקנות הגנת הפרטיות. הוועדה עודכנה כי נכון למועד כינוס הוועדה, רק המאגר הקונסולרי רשום כחוק, וקב"ט המשרד, שמונה כממונה על האבטחה לפי החוק, מוביל את רישום יתר המאגרים.

בישיבת הוועדה ממאי 2023 נמסר לוועדה כי המשימה של בקרה ורישום של מאגרים לפי חוק הגנה על הפרטיות טרם הושלמה. בישיבת הוועדה מספטמבר 2024 כלל לא דנו בנושא זה.

אף שנושא העמידה בדרישות תקנות הגנת הפרטיות וביצוע סקרי סיכונים עלה בדיוני ועדת ההיגוי כבר בפברואר 2020, גם כעבור חמש שנים לא בוצעו סקרי סיכונים בהקשר של הגנת הפרטיות למאגרי מידע נוספים שברשות המשרד, וכאמור לא נרשמו מאגרי מידע נוספים בפנקס מאגרי המידע שבמשרד המשפטים. זאת אף שהודגש במסמכי הוועדה כי קיימת אחריות אישית פלילית של מנכ"ל המשרד וראשי האגפים המנהלים את המאגרים לאי-רישום המאגרים ואי-עמידה בתקנות הגנת הפרטיות.

☆

הנהלת משרד החוץ התחייבה להגן על מאגרי מידע הכוללים מידע פרטי בהתאם להוראות הדין, לרבות תקנות הגנת הפרטיות, כדי למזער את הסיכון לפגיעה בזכות לפרטיות. ממצאי פרק זה מלמדים שמשרד החוץ אינו מטפל כנדרש בחובות המוטלות עליו לפי חוק הגנת הפרטיות ותקנותיו. בטמ"ח שמונה כאחראי לאבטחת המאגרים לא מקדיש לכך משאבים כנדרש, וממילא תמונת המצב שהועלתה מעידה שהמשרד אינו עומד לפחות בחלק מהנדרש בתקנות הגנת הפרטיות. אי-עמידה בחוק ובתקנותיו עלולה להביא לפגיעה בפרטיותם של עובדי המשרד ומשפחותיהם ושל אזרחים הנזקקים לשירותי המשרד. נוסף על כך, היא חושפת את המשרד לסיכוני אבטחת מידע, ובהם חשיפת המידע הפרטי ושימוש בו באופן שאינו מורשה, שינוי מידע זה ופגיעה בזמינות של המידע הדרושה לצורך הבטחת הרציפות התפקודית של המשרד.

פער זה מתחדד לנוכח כניסתו לתוקף של תיקון מספר 13 לחוק הגנת הפרטיות באוגוסט 2025 המטיל חובות משמעותיות על ארגונים המחזיקים מאגרי מידע ולנוכח העובדה כי המשרד היה צריך להיערך לנושא זה עוד לפני כניסת העדכון לתוקף.

משרד החוץ ציין בתשובתו כי במשרד קיים פער בתחום ההגנה על הפרטיות וכי אין ולא היה בעבר תקן לממונה על הגנת הפרטיות (DPO). המשרד הוסיף כי לקב"ט המשרד שעליו הוטלה האחריות לתחום זה אין היכולת לעשות כן ללא המשאבים הנדרשים.

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.

מבדק חוסן באחת מרשתות משרד החוץ

אחת הדרכים להיערכות לאיומי סייבר בארגון היא ביצוע מבדקי חוסן, ובכללם מבדק חדירה וסקרי הערכת פגיעויות. מבדקים אלו נועדו לבחון את רמת ההגנה המיושמת בארגון, לאתר חולשות אבטחה וסיכונים אפשריים - ולטפל בהם.

בחודשים מרץ-אפריל 2025 ביצע משרד מבקר המדינה מבדק חדירה בשילוב סקר הערכת פגיעויות (להלן - מבדק החוסן) באחת מהרשתות במשרד החוץ.

להלן תרשים המציג את השלבים בתהליך מבדק החוסן שבוצע:

תרשים 10 : **השלבים של מבדקי החוסן שביצע משרד מבקר המדינה במשרד החוץ**

הוכן בידי משרד מבקר המדינה.

ממצאי מבדקי החוסן דורגו על פי שני תבחינים : (א) **חומרת הנזק** הגלומה בהם, הנקבעת בהתאם לרמת ההשפעה על יכולת משרד החוץ לקיים את התהליכים העסקיים במקרה של התממשות הסיכון ; (ב) **הסבירות להתממשות הסיכון**, הנוגעת לכל ממצא בנפרד, ובקביעתה מובאים בחשבון רמת המורכבות של ניצול הפער שהתגלה במסגרת הממצא ומידת חשיפתו של הפער. לכל תבחין יש ארבע דרגות אפשריות : גבוהה מאוד, גבוהה, בינונית ונמוכה. המכפלה בין שני התבחינים יוצרת את הערך הנקרא **רמת הסיכון**.

לוח 3 : **טבלת דירוג של ניהול הסיכונים**

החומרה / הסבירות	נמוכה	בינונית	גבוהה	גבוהה מאוד
דרגה גבוהה מאוד				סיכון גבוה מאוד
דרגה גבוהה			סיכון גבוה	
דרגה בינונית		סיכון בינוני		
דרגה נמוכה	סיכון נמוך			

במבדק החוסן שערך משרד מבקר המדינה זוהו 15 ממצאים בתחומים שונים, וברמות סיכון שונות: רמה גבוהה ביותר, רמה גבוהה, רמה בינונית ורמה נמוכה. יצוין כי ממצא אחד בעל רמת סיכון גבוהה טופל על-ידי משרד החוץ כבר במהלך ביצוע המבדק. ממצאים אלו מעלים את הסיכון לפגיעה מהותית בסודיות המידע, בזמינותו ובמהימנותו וביכולתו של משרד החוץ לקיים את התהליכים העסקיים ברשת שנבדקה באמצעות ניצול פערי אבטחת המידע שזוהו.

בהתייחס לליקויים שנמצאו במבדק הבהיר המשרד כי נעשתה פעילות בכל הרשתות לתיקון הליקויים שעלו במבדק.

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.

☆

בתשובת משרד החוץ מאוקטובר 2025 צוינו כמה תחומים בהגנת הסייבר אשר קודמו בשנים 2023 - 2025 ונועדו לשפר את יכולות המשרד בהגנה על נכסי המידע: המשרד הוסמך לתקנים מובילים בתחום הגנת הסייבר ובהם תקן לניהול אבטחת המידע בארגון (ISO 27001) ותקן לניהול סיכוני האבטחה בשרשרת האספקה (ISO 28000). המשרד נקט פעולות כדי לקדם את רמת ההגנה על המידע במשרד; המשרד הסדיר את תחומי האחריות בין אגף תקשוב לבין בטמ"ח ומתקיים שיתוף פעולה סינרגטי; הוקם SOC שמנטר אלפי עמדות קצה ומאות מערכות ברשתות של המשרד; המשרד החל בחיזוק תהליכי ההזדהות בכניסה לרשתות המשרד; באגף התקשוב הוקם תחום הנחיה ובקרה המבצע ביקורות וסקרי סיכונים; בוצעו תרגילים בתרחישי סייבר ברמת המשרד ובדרגי התפעול; בוצעה פעילות בתחום ניהול סיכוני הסייבר בשרשרת האספקה, והמשרד נמצא בעיצומו של תהליך לחידוש תשתיות מחשוב ומערכות מידע ישנות.

מנכ"ל משרד החוץ השיב כי בחן את ממצאי הדוח ברצינות הראויה, כי חלק מהליקויים כבר תוקנו, וכי הוא ביקש שתוצג בפניו תוכנית עבודה לתיקון הליקויים. המנכ"ל הוסיף כי האתגרים שעומדים בפניו - כמו אלו שעמדו בפני קודמיו בתפקיד - יוסיפו להיות אתגרים של משאבים וסדרי עדיפויות: התקציב המצומצם, כוח האדם שאינו מספיק לכל המשימות ומערכות שנדרש לשדרגן.

השב"כ השיב כי דוח הביקורת מפרט ממצאים רבים שיש לתקנם. השב"כ הוסיף כי לנוכח פערים קיימים בכוח אדם בתחום הגנת הסייבר במשרד החוץ, קודם אל מול נציבות שירות המדינה תקנון של משרות נוספות בתחום הגנת הסייבר ואושרו שלוש משרות נוספות חדשות. השב"כ ציין כי כדי לאפשר קפיצת מדרגה בתחום ההגנה יש חשיבות גבוהה לאיוש משרות אלה ולהשקעת משאבים ותקציבים ייעודיים לנושא. השב"כ עמד על כך שמשרד החוץ הוא אחד מגופי הדגל שאותם הוא מנחה, וכי הוא רואה חשיבות רבה בהעלאת רמת החוסן שלו בהקדם בשיתוף משרד החוץ ובאמצעות תוכניות עבודה.

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.

תרשים 11 : **פערים מרכזיים בתהליכי הניהול והפיתוח של מערכות המידע**

תרשים 12 : **פערים מרכזיים באבטחת 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 יום 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 יסייע 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.