דוח מבקר המדינה

מערכות מידע ואבטחת מידע וסייבר במשרד החוץ

▪ סיוון התשפ"ו ▪ מאי 2026 ▪

מערכות מידע ואבטחת מידע וסייבר במשרד החוץ

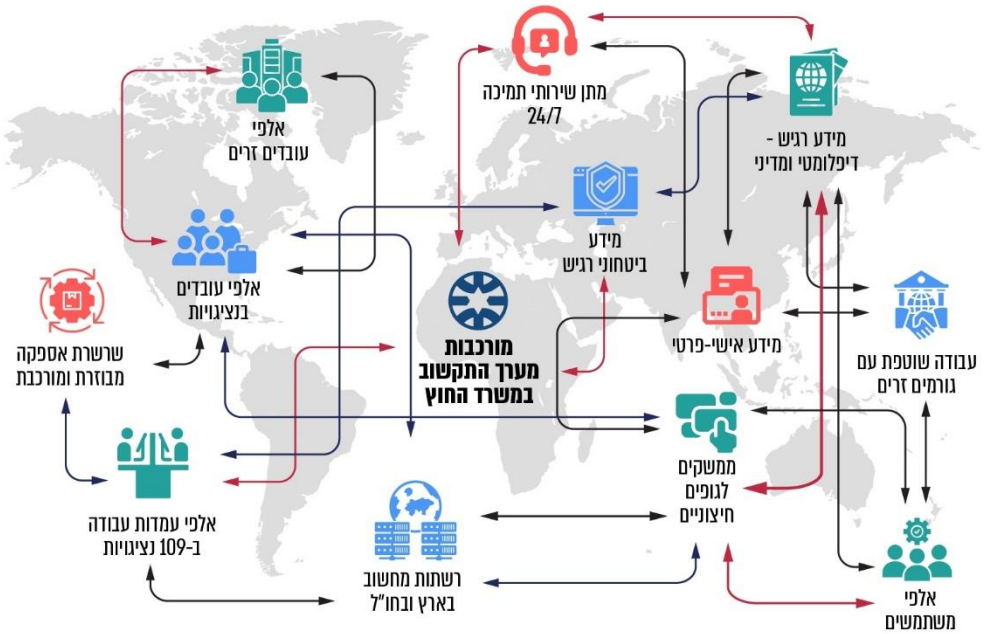
תקציר

רקע

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

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

מערך התקשוב במשרד החוץ - מאפיינים ייחודיים



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

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

נתוני מפתח

85.3 מיליון ש"ח

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

EOL

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

מאות

אירועי הגנת מידע התרחשו בנציגויות ישראל בחו"ל בשנת 2023

הגנה חלקית

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

משנת 2018

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

ספריות רשת משותפות

נמצאו ספריות בחלק מרשתות המשרד שהיו פתוחות לכלל משתמשי הרשת

תשתיות ומערכות מידע

נמצאו פערים בעדכניות תשתיות ומערכות המידע

15 ממצאים

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

פעולות הביקורת

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

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

ועדת המשנה של הוועדה לענייני ביקורת המדינה של הכנסת החליטה שלא להניח דוח זה במלואו על שולחן הכנסת אלא לפרסם רק חלקים ממנו, לשם שמירה על ביטחון המדינה, בהתאם לסעיף 17 לחוק מבקר המדינה, התשי"ח-1958 [נוסח משולב].

[1] End of Life.

תמונת המצב העולה מן הביקורת

ניהול ופיתוח של מערכות המידע במשרד החוץ

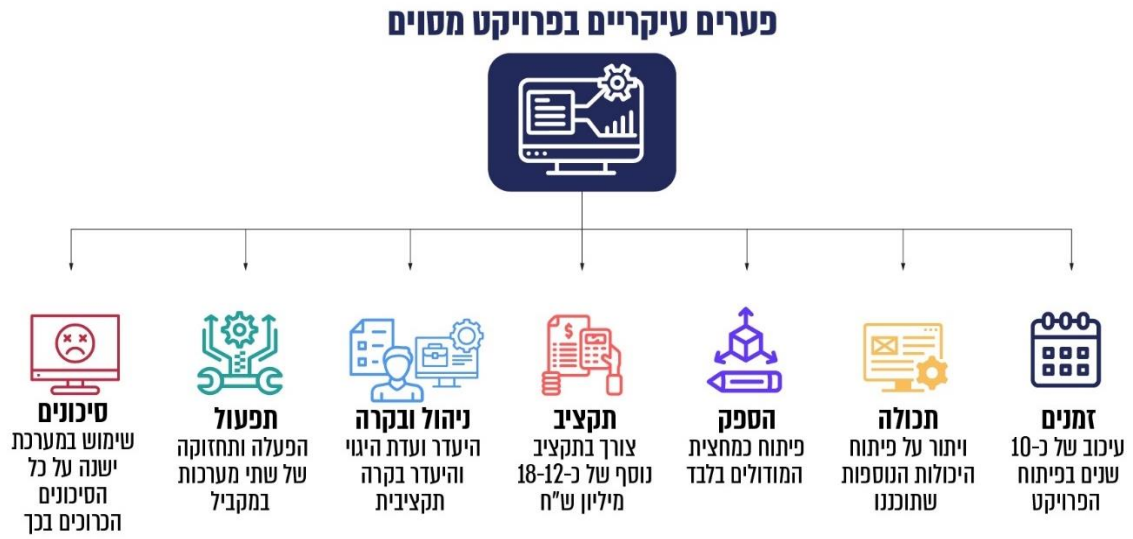
הקמת ועדת היגוי משרדית לתחום התקשוב ופעילותה - בניגוד להנחיות מערך הדיגיטל, ועדת ההיגוי המשרדית לתקשוב שתפקידה בין היתר לקבוע את האסטרטגיה של המשרד ומדיניותו בנושאי תקשוב; לאשר את תוכניות העבודה והתקציבים הרב-שנתיים והשנתיים של כלל הפעילויות המתקיימות במשרד בתחומים של מערכות מידע ותקשוב; לקבוע ולאשרר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

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

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

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

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



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

אבטחת המידע והגנת הסייבר במשרד החוץ

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

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

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

---

[2] Disaster Recovery Plan.

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

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

מסמכים הכוללים מידע אישי שהיו נגישים לכלל משתמשי רשת מסוימת במשרד

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

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

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

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

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

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

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

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

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

עיקרי המלצות הביקורת

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

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

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

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

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

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

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

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

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

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

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

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

הפערים המרכזיים בתהליכי הניהול והפיתוח של מערכות המידע

הפערים המרכזיים באבטחת המידע והגנת הסייבר

סיכום

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

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

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

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

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

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

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

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

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