דוח מבקר המדינה

הגנה על המידע הממוחשב במשרד ראש הממשלה

תמוז התשפ"ד | יולי 2024

הגנה על המידע הממוחשב במשרד ראש הממשלה

מבוא

משרד ראש הממשלה אמון על מימוש התפיסה המדינית, הכלכלית, החברתית והניהולית של ראש הממשלה, ועוסק הלכה למעשה בהתוויה, תכנון, קידום ויישום של מדיניות הממשלה וראש הממשלה בנושאים המרכזיים שעל סדר יומה של הממשלה. תפקיד מטה המשרד הוא לסייע לראש הממשלה בקביעת מדיניות ובתכלול מדיניות הממשלה, לאפשר את תפקודו היעיל של ראש הממשלה ולהבטיח את שגרת עבודתו התקינה. המטה לביטחון לאומי (להלן - המל"ל) הוא יחידת סמך של משרד רה"ם. המל"ל משמש גוף מטה לראש הממשלה ולממשלה בענייני החוץ והביטחון של ישראל, ומרכז בין השאר את עבודת המטה של הממשלה ושל ועדת השרים לענייני ביטחון לאומי בענייני החוץ והביטחון. משרד רה"ם מספק שירותי ניהול מערכות מידע והגנה על המידע שבהן ל-13 מיחידות הסמך שלו וכן למשרדי ממשלה נוספים, כמפורט בהמשך. כל הגופים והיחידות שלהם מספק משרד רה"ם שירותי ניהול מערכות מידע והגנה על המידע שבהן יכונו להלן - משרד רה"ם.

במערכות הממוחשבות במשרד רה"ם אצור מידע רב, לרבות מידע רגיש, מידע שמסווג כחסוי מהבחינה הביטחונית ומידע ברמת סודיות גבוהה ביותר. פגיעה במידע המצוי במערכות של משרד רה"ם, לרבות דליפת המידע, שיבושו או פגיעה בזמינותו, עלולה לגרום לנזק ממושך חמור מאוד לביטחון מדינת ישראל או למערכותיה החיוניות, ועל אחת כמה וכמה בעיתות מלחמה, כשכמות תקיפות הסייבר עולה. על פי קביעת גורמי המקצוע המופקדים על הגנת המידע, ההגנה הנדרשת על המידע המסווג שבידי משרד רה"ם היא ברמה הגבוהה ביותר.

בחודשים ינואר-מאי 2023 חווה משרד רה"ם אירועי סייבר, ובין היתר חסם כ-6 מיליון הודעות דואר אלקטרוני (72% מכלל הודעות הדואר האלקטרוני שנשלחו למשרד באותה תקופה), בין היתר מכיוון שכתובת השולח הייתה חשודה או משום שהדואר האלקטרוני הכיל נוזקה או קישור זדוני. כמו כן, היו באותה תקופה כ-49 מיליון ניסיונות להתקפה על שירות החיבור מרחוק של משרד רה"ם, ובכלל זה כ-44 מיליון ניסיונות לסריקת פרוטוקולי תקשורת להעברת נתונים; כ-809,000 ניסיונות לסריקת פרטי משתמשים; כ-1.2 מיליון ניסיונות למניעת שירות[1]; וכ-9,170 ניסיונות לניצול חולשות ידועות ברכיבי מערכות המידע (קושחה ותוכנה), הנובעות מסיבות שונות, ובהן פיתוח שגוי או לא עקבי של מוצר, שעלולות לחשוף את מערכות המידע לפעילות עוינת מצד תוקף.

משרד רה"ם ציין בתשובתו ממרץ 2024 כי הניסיונות האמורים נבלמו בידי מערכות האבטחה השונות של המשרד ולא גרמו לפגיעה במערכות המשרד או לדלף מידע מהן.

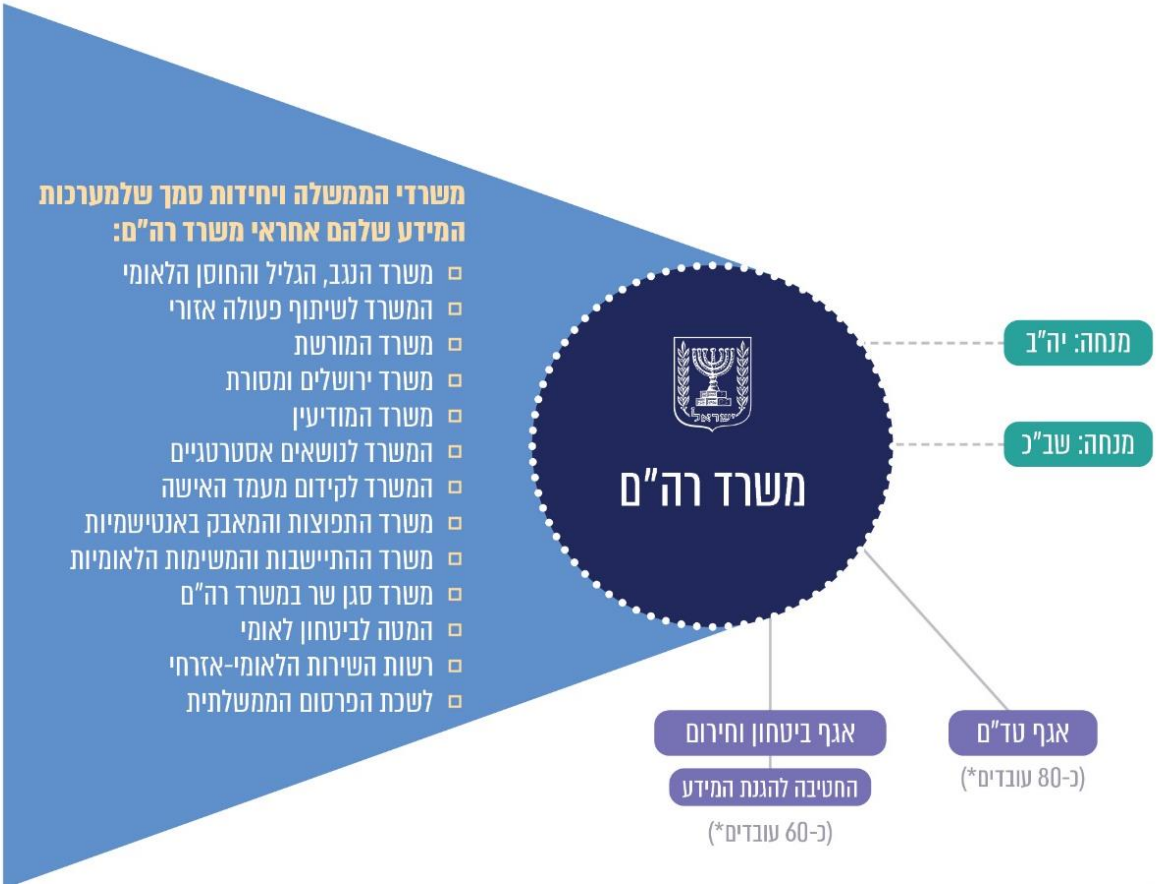
משרד רה"ם מונחה בכל הנוגע להגנה על המידע על ידי יחידת ההגנה בסייבר במערך הדיגיטל הלאומי (להלן - יה"ב) ועל ידי שירות הביטחון הכללי (להלן - שב"כ). משרדי הממשלה נדרשים לעמוד בהנחיות הגופים האלה (להלן - הנחיות הגופים המאסדרים), בכל הנוגע לאבטחת המידע ברשתות המשרד.

גורמי המקצוע במשרד רה"ם האמונים על הגנת המידע במשרד הם אגף בכיר טכנולוגיות דיגיטליות ומידע (להלן - אגף טד"ם) וחטיבת הגנת המידע באגף ביטחון וחירום במשרד (להלן - חטיבת הגנת המידע). אגף טד"ם אחראי להגנת המידע ברשת הבלמ"ס של המשרד וכן לפיתוח מערכות מידע ולמתן שירותי תחזוקה, תמיכה, אחסון וטיפול בחומרת מחשוב ותקשורת בכל רשתות המשרד. חטיבת הגנת המידע אחראית בין השאר להגנת המידע ברשתות המסווגות. בראש שני האגפים האלה עומדים מנהלים בדרג סמנכ"ל, הכפופים ישירות למנכ"ל משרד רה"ם.

[1] מתקפה למניעת שירות נועדה להשבית מערכת מחשב על ידי יצירת עומס חריג על משאביה.

המבנה הארגוני הכללי של תחומי טכנולוגיות דיגיטליות והגנת המידע במשרד רה"ם, כלל המשרדים ויחידות הסמך שלמערכות המידע שלהם אחראי משרד רה"ם וכן הגורמים המנחים את המשרד, מוצגים בתרשים שלהלן:

תרשים 1: **המבנה הארגוני הכללי של תחומי טכנולוגיות דיגיטליות והגנת המידע במשרד רה"ם, המשרדים ויחידות הסמך שלמערכות המידע שלהם אחראי משרד רה"ם והגורמים המנחים את המשרד**



המקור: משרד רה"ם, אגף טד"ם, מצגת עבודה 2022; אגף טד"ם, מצגת ועדת היגוי להגנת סייבר, 2.5.23; החוק להסדרת הבטחון בגופים ציבוריים, התשנ"ח-1998; החלטת הממשלה מס' 2443 (15.2.15).

* עובדים במשרות בתקן משרד רה"ם וכן עובדים שהמשרד שכר את שירותיהם (מיקור חוץ). על פי נתוני אגף ביטחון וחירום במשרד רה"ם, כ-10 מ-60 העובדים בחטיבת הגנת המידע שבאגף עסקו בהגנת הסייבר.

מהתרשים עולה כי משרד רה"ם אחראי לניהול טכנולוגיות המידע ולהגנת המידע גם בעשרה משרדי ממשלה אחרים ובשלוש יחידות סמך.

במשרד רה"ם פועלות מספר רשתות, בהן רשתות מסווגות.

<u>פעולות הביקורת</u>

בחודשים מרץ עד אוגוסט 2023 ביצע משרד מבקר המדינה ביקורת בנושא ההגנה על המידע הממוחשב המצוי בעיקר ברשתות מחשוב של משרד רה"ם, בהן רשתות מסווגות. בביקורת נבחנו בין היתר הנושאים האלה: ניהול-העל של הגנת המידע במשרד רה"ם, לרבות היבטי תקציב הכרוכים בניהול; מערך הזדהות המשתמשים וניהול ההרשאות; ניטור המערכות ברשת מסויימת שנבחנה; עדכניות הגרסאות של מערכות ההפעלה והתוכנה; ואבטחת המידע המסווג ביטחונית.

הביקורת נערכה בעיקרה במשרד רה"ם ובמל"ל. בדיקות השלמה נעשו ביה"ב, בשב"כ ובנציבות שירות המדינה.

ועדת המשנה של הוועדה לענייני ביקורת המדינה של הכנסת החליטה שלא להניח על שולחן הכנסת ולא לפרסם נתונים מפרק זה לשם שמירה על ביטחון המדינה, בהתאם לסעיף 17 לחוק מבקר המדינה, התשי"ח-1958 [נוסח משולב]. חסיון נתונים אלה אינו מונע את הבנת מהות הביקורת.

ניהול-העל של הגנת המידע

בשנת 2015 החליטה הממשלה (להלן - החלטה 2443) להטיל על כל אחד מהמנהלים של משרדי הממשלה ויחידות הסמך לפעול לשיפור רמת ההגנה במרחב הסייבר[2]. בין היתר, הוחלט למנות בכל אחד ממשרדי הממשלה ממונה על הגנת הסייבר ולהקים ועדת היגוי משרדית להגנת הסייבר, שתפעל לשיפור רמת הגנת הסייבר של המשרד הממשלתי ותפקח על הפעילות השוטפת המבוצעת בתחום זה. תפקידיה של ועדת ההיגוי בנוגע למידע בלתי מסווג מפורטים בהנחיות הגופים המאסדרים, מהן עולה כי תפקידי ועדת ההיגוי הם בין השאר להתוות עקרונות ותפיסות בהיבטי הגנת הסייבר במשרד הממשלתי; לאשר, למפות ולסווג את נכסי המידע של המשרד; לאשר מפת סיכונים משרדית; לאשר את תוכנית העבודה בתחום הגנת הסייבר ולבקר את יישומה; ולהקצות משאבים ליישום דרישות תשתית הגנת הסייבר. על פי הנחיות הגופים המאסדרים, תפקיד ועדת ההיגוי הוא גם לאשר את מדיניות הגנת הסייבר. אישור המדיניות הוא בסמכות מנכ"ל המשרד הממשלתי, העומד בראשה. יצוין כי החלטה 2443, שחייבה להקים את ועדת ההיגוי להגנת הסייבר במשרד ממשלתי, לא הבחינה בין הגנה על מידע מסווג לבין הגנה על מידע בלמ"ס.

ועדת היגוי להגנת הסייבר

במשרד רה"ם פועלות שתי ועדות היגוי: ועדת היגוי משרדית להגנת הסייבר, אשר עוסקת במערכות מידע בלמ"ס (להלן - הוועדה למידע בלמ"ס); וועדת היגוי לאבטחת המידע המסווג של המשרד (להלן - הוועדה למידע מסווג).

ניהול ועדת ההיגוי ותדירות דיוניה

על פי החלטה 2443, בראש ועדת ההיגוי להגנת הסייבר יעמוד מנכ"ל המשרד, ועל הוועדה להתכנס לכל הפחות פעם בחצי שנה. על פי ההחלטה, ועדת ההיגוי נדרשת לבצע מדי שנה בשנה פעולות מסוימות, ובהן אישור תוכנית העבודה בתחום הגנת הסייבר ובקרה עליה והקצאת משאבים ליישום דרישות בנוגע לתשתית הגנת הסייבר.

1. בשנים 2018 - 2023 הוועדה למידע בלמ"ס במשרד רה"ם התכנסה חמש פעמים: פעם אחת בכל אחת מהשנים 2018, 2019 ו-2022 ופעמיים בשנת 2023. הוועדה למידע בלמ"ס לא התכנסה בשנים 2020 ו-2021. הוועדה למידע מסווג התכנסה ארבע פעמים בשנים 2020 - 2023.

   על פי כתבי המינוי של חברי הוועדה למידע בלמ"ס וסיכומי הדיונים שלה, בראש הוועדה עמדו בשנים 2018 - 2019 מנכ"לי משרד רה"ם באותן שנים, אך הם לא השתתפו בדיונים שקיימה הוועדה בכל אחת מאותן שנים; בשנת 2020 משרד רה"ם לא מינה יו"ר ועדה; בשנים 2021 -2022 מונה מנהל אגף טד"ם, המשמש גם הממונה על הגנת הסייבר של המשרד, לתפקיד ממלא מקום יו"ר הוועדה. ממרץ 2023, תחילת תקופת הביקורת, עמד מנכ"ל משרד רה"ם בראש הוועדה, והוא השתתף בדיונים שקיימה הוועדה בשנה זו.

2. משרד רה"ם לא מינה בכתב את חברי הוועדה למידע מסווג.

[2] מרחב הסייבר - מרחב וירטואלי ופיזי המורכב מרובד פיזי - כלל רכיבי המחשוב והתקשורת, רובד לוגי - הקוד שמפעיל את רכיבי המחשוב, ורובד אנושי - כלל האנשים המשתמשים ברשת.

בביקורת עלו ליקויים בקשר לעבודתן של שתי הוועדות, אשר נדרשות, על פי החלטת הממשלה, לבצע פעולות מסוימות בכל שנה, ובהן אישור תוכנית העבודה בתחום הגנת הסייבר, בקרתה והקצאת משאבים ליישום דרישות תשתית הגנת הסייבר. להלן פירוט: הוועדה למידע בלמ"ס לא התכנסה בשנים 2018, 2019 ו-2022 בתדירות הנדרשת, ובשנים 2020 ו-2021 לא התכנסה כלל; תפקיד יו"ר הוועדה לא אויש בשנת 2020, ובשנים 2020 - 2022 לא עמד בראש הוועדה מנכ"ל משרד רה"ם, כנדרש בהחלטת הממשלה; בדיונים שקיימה הוועדה בשנים 2018 - 2022 לא השתתף מנכ"ל המשרד, האמור לעמוד בראש הוועדה. אשר לוועדה למידע מסווג, נמצא כי חבריה לא מונו בכתב כנדרש.

על משרד רה"ם לפעול על פי החלטה 2443 בדבר מינוי ועדת היגוי להגנת הסייבר בראשות מנכ"ל המשרד לגבי מידע מסווג ומידע בלמ"ס ובדבר התדירות הנדרשת של הדיונים.

משרד רה"ם ציין בתשובתו כי החל לפעול לתיקון הליקויים, ובכלל זה קבע את הגורם האחראי לביצוע ההמלצה האמורה ולוח זמנים לביצועה.

אישור תוכנית העבודה השנתית על ידי ועדת ההיגוי

בנוגע לגיבוש ואישור של תוכנית עבודה נקבע כדלהלן: בהחלטה 2443 נקבע כי על ממונה הגנת הסייבר במשרד לבנות תוכנית עבודה להגנת הסייבר, על פי מדיניות המשרד להגנת הסייבר. בהנחיות הגופים המאסדרים נקבע כי על ועדת ההיגוי להגנת הסייבר לבחון את תוכנית העבודה בתחום הגנת הסייבר המובאת לפניה, ולהחליט אם לאשר אותה, וכי תפקיד ועדת ההיגוי הוא לאשר תיעדוף ותקצוב של פעילויות הגנה מפני איומי סייבר. תיעדוף פעילויות של משרדי ממשלה נעשה ככלל באמצעות קביעת תוכנית עבודה. יוצא אם כן שוועדת ההיגוי להגנת הסייבר נדרשת לבחון את הצעת תוכנית העבודה להגנת הסייבר ולהחליט אם לאשרה.

1. על פי סיכומי הדיונים של הוועדה למידע בלמ"ס בשנים 2019 - 2022 ובדיקת המסמכים שהועברו אליה לקראת הדיונים, הצעות אגף טד"ם לתוכנית עבודה שנתית לא הועברו לוועדה לקראת הדיונים, אלא הועברו אליה מצגות שבהן הוצגו חלק מתוכניות העבודה המוצעות, ולא הוצגו לפניה כל רכיבי התוכניות שכללו משימות לביצוע בתחום אבטחת הסייבר. למשל, לא הוצגו לפני הוועדה שהתכנסה בנובמבר 2022 המשימות האלה: ביצוע "סגמנטציה" (כלומר, הפרדה בין משתמשים, מדפסות, סביבות פיתוח, שעוני נוכחות, שרתים ואתרים); הטמעה של מערכת לזיהוי חולשות ברשת הבלמ"ס; מעבר לגלישה במרשתת (אינטרנט) באמצעות יישום של ממשל זמין; והצפנת מחשבים ברשת. על פי סיכומי הדיונים, הוועדה לא אישרה את תוכניות העבודה החלקיות שהוצגו לפניה.

2. על פי המסמכים של הוועדה למידע מסווג לשנים 2020 - 2022, לא הוצגו לפניה במלואן הצעות לתוכנית עבודה להגנת המידע המסווג, אלא רק בחלקן, והוועדה לא אישרה אותן. לשני דיונים אחרים לא נרשמו כאמור סיכומי דיון. עם זאת, משרד רה"ם העביר לשב"כ לפני הדיונים את הצעותיו לתוכניות עבודה, והשב"כ התייחס אליהן.

שתי ועדות ההיגוי הפועלות במשרד רה"ם - הוועדה למידע בלמ"ס והוועדה למידע מסווג - קיימו דיונים בשנים 2019 - 2022 לגבי תוכניות העבודה השנתיות, בלי שהונחו לפניהן ההצעות המלאות והמפורטות לתוכניות עבודה, לצורך אישורן. לוועדות הוצגו מצגות שהיו בהן תוכניות עבודה חלקיות בלבד, ולא היו בהן כלל המשימות וכלל הרכיבים שנכללו בתוכניות העבודה. יוצא אפוא כי בשנים האמורות הוועדות לא מילאו את תפקידן כנדרש בכל הנוגע להליך הבחינה והאישור של תוכניות העבודה השנתיות.

מומלץ שהוועדה למידע בלמ"ס והוועדה למידע מסווג של משרד רה"ם ידונו בתוכניות העבודה בתחום אבטחת המידע במשרד מדי שנה בשנה, לרבות בכל המשימות הנכללות בתוכניות האלה ועל בסיס מלוא המידע הרלוונטי להן, יקבלו החלטות אם לאשרן ויתעדו את ההחלטות בסיכומי הדיונים.

משרד רה"ם ציין בתשובתו כי החל לפעול לתיקון הליקויים, ובכלל זה קבע את הגורם האחראי לביצוע ההמלצה האמורה ולוח זמנים לביצועה. משרד רה"ם הוסיף כי ידאג להעביר את תוכניות העבודה השנתיות לחברי ועדת ההיגוי לפני שהיא תתכנס, כדי שחברי הוועדה יוכלו לבחון אותן ולקבל החלטות בהתאם להן.

גיבוש מדיניות הגנת הסייבר

בהחלטה 2443 קבעה הממשלה כי הממונה על הגנת הסייבר במשרד הממשלתי יגבש מדיניות להגנת הסייבר של המשרד. אחד מתפקידי ועדת ההיגוי המשרדית הוא אישור מדיניות הגנת הסייבר במשרד, על רכיביה, ובהם המסגרות הארגוניות שיישמו את המדיניות; ההגנה הפיזית על מכלול הציוד והמידע מפני גורמים בלתי מורשים; הגדרת הטיפול ברשומות במטרה לצמצם את סיכוני הפגיעה במידע האגור בהן; הגדרת שכבות ההגנה על המידע בתחומי המחשוב והתקשורת; קביעת עקרונות להגנת המידע בכל הנוגע לכוח האדם, לרבות עובדי חברות חיצוניות; ניהול וסיווג של נכסים; טיפול באירועי סייבר; פיתוח ורכש; ניהול המשכיות תפקודית בעת חירום; וגיבוש תוכנית עבודה ותקציב בתחומי הגנת הסייבר.

לפי הנחיות הגופים המאסדרים, יש לאשרר את מדיניות הגנת הסייבר אחת לשנתיים או מוקדם יותר אם יש צורך מיוחד בכך (כגון עקב שינויים מהותיים במערך המחשוב או במערך הארגוני של המשרד הממשלתי). בנוגע למידע מסווג נקבע בהנחיות כי המדיניות תאושר בידי מנכ"ל המשרד הממשלתי או מי שהוא הסמיך לכך ותתוקף אחת לשלוש שנים.

בעת הביקורת היו בידי משרד רה"ם שני מסמכי מדיניות להגנת המידע: (א) מסמך מדיניות שגיבש אגף טד"ם, שעסק הלכה למעשה במידע בלמ"ס (להלן - מדיניות המידע הבלמ"ס). המסמך אושר בידי הוועדה למידע בלמ"ס במשרד רה"ם בנובמבר 2018, ובסיכום דיון הוועדה מנובמבר 2022 נרשם כי הוועדה תאשר את המדיניות; (ב) מסמך מדיניות שגיבש אגף ביטחון וחירום בשנת 2020, שעסק באבטחת המידע המסווג והגנת המידע ברשתות המסווגות; המסמך עודכן בשנת 2022.

1. **מדיניות לאבטחת המידע הבלמ"ס:** בשנים 2019 - 2023 חלו שינויים במשרד רה"ם, ובכלל זה בתחום אחריותו לניהול מערכות המידע של משרדים אחרים, לרבות אבטחת המידע שבהם. למשל, עקב שינוי ארגוני שביצע המשרד בשנת 2019, הוקמה חטיבת הגנת המידע באגף ביטחון וחירום, והוטלה עליה האחריות לאבטחת המידע המסווג של המשרד; במאי 2020 הוקמו, במסגרת הקמת הממשלה ה-35 משרד ראש הממשלה החלופי, המשרד לחיזוק וקידום קהילתי, משרד הדיגיטל הלאומי ומשרד ההתיישבות, ומשרד רה"ם קיבל את האחריות לניהול מערכות המידע שלהם ולאבטחת המידע שבמערכות אלה; בדצמבר 2022 הוקמו במסגרת הקמת הממשלה ה-37 המשרד לקידום מעמד האישה, משרד התפוצות והמאבק באנטישמיות, משרד ההתיישבות והמשימות הלאומיות ומשרד הנגב, הגליל והחוסן הלאומי, ומשרד רה"ם קיבל את האחריות לניהול מערכות המידע שלהם ולאבטחת המידע שבמערכות אלה.

נמצא כי מסמך מדיניות המידע הבלמ"ס של משרד רה"ם שאושר בנובמבר 2018 לא עודכן ולא תוקף במשך ארבע שנים וחצי, כנדרש בהנחיות הגופים המאסדרים. זאת אף על פי שבשנים האלה חלו שינויים ארגוניים ניכרים, ובכלל זה קבלת אחריות של משרד רה"ם לטיפול בתחומי טכנולוגיות המידע ואבטחת המידע בעוד משרדי ממשלה ויחידות סמך[3].

2. **מסמך המדיניות לאבטחת המידע המסווג: מסמך זה כלל חמישה משבעת תחומי הפעולה העיקריים הנדרשים על פי הנחיות הגופים המאסדרים - הסדרת הסמכויות**

[3] משרד הנגב, הגליל והחוסן הלאומי, המשרד לשיתוף פעולה אזורי, משרד המורשת, משרד ירושלים ומסורת ישראל, משרד המודיעין, המשרד לנושאים לעניינים אסטרטגיים, המשרד לקידום מעמד האישה, משרד התפוצות והמאבק באנטישמיות, משרד ההתיישבות והמשימות הלאומיות, משרד סגן שר במשרד רה"ם, המל"ל, רשות השירות הלאומי - אזרחי ולשכת הפרסום הממשלתית.

והתפקידים בארגון בהיבטי הגנת הסייבר; הגדרת התמיכה הניהולית והקצאת המשאבים; הצגת הסיכונים בתחום הגנת הסייבר להנהלה והדרכים לצמצומם; הגדרת עקרונות לתוכנית כשירות מקצועית של בעלי התפקידים בתחום הגנת הסייבר; והיערכות לטיפול באירועים חריגים.

ואולם נמצא כי מסמך המדיניות לאבטחת המידע המסווג לא כלל את תחומי הפעולה האלה, הנדרשים אף הם על פי הנחיות הגופים המאסדרים: הגדרת עקרונות פיקוח ובקרה על יישום ההנחיות; הגדרת האחריות האישית של העובדים; והעקרונות לטיפול בעובד אשר יחרוג מהנדרש בהנחיות. כמו כן, ממסמכי משרד רה"ם עולה כי המדיניות לאבטחת המידע המסווג בשנים האלה לא אושרה בידי מנכ"ל המשרד, כנדרש על פי ההנחיות.

מומלץ שאגף טד"ם יגבש הצעה למדיניות מעודכנת לאבטחת המידע הבלמ"ס במשרד רה"ם, לנוכח השינויים שחלו במשרד רה"ם ובתחומי אחריותו; יביא את הצעתו לבחינה ולאישור של הוועדה למידע בלמ"ס; ויקפיד על עדכון ואשרור של המדיניות אחת לשנתיים לפחות, כנדרש בהנחיות הגופים המאסדרים. עוד מומלץ שמנכ"ל משרד רה"ם יפעל לגיבוש מדיניות תקפה להגנת המידע המסווג של המשרד ולתיקופה, כנדרש בהנחיות.

משרד רה"ם ציין בתשובתו כי החל לפעול לתיקון הליקויים, ובכלל זה קבע את הגורם האחראי לביצוע ההמלצה האמורה ולוח זמנים לביצועה.

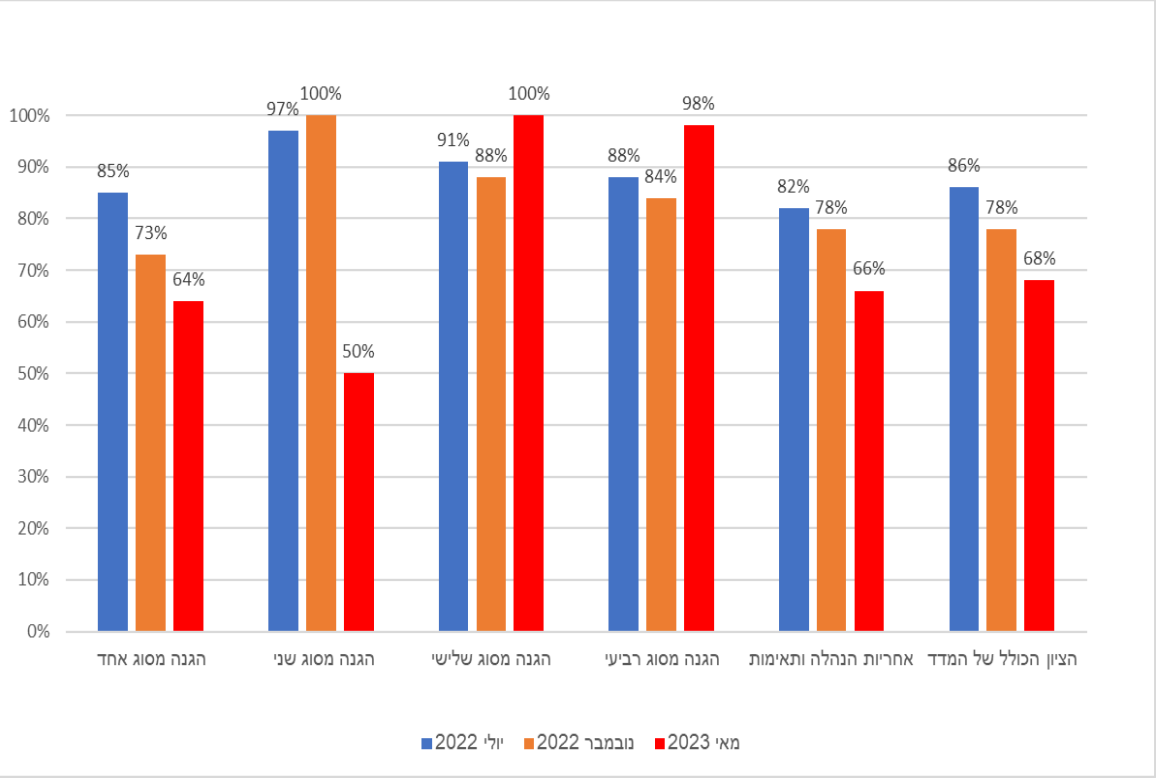
<u>בקרה על יישום הגנת הסייבר במשרד רה"ם</u>

אחד מתפקידיה העיקריים של ועדת ההיגוי במשרד ממשלתי הוא לבצע בקרה ניהולית על יישום הגנת הסייבר במשרד. הבקרה הניהולית נדרשת לאיתור פערים במרכיבים שונים של רמת ההגנה בסייבר וטיפול בהם.

לשם ביצוע בקרה ניהולית פיתחה יה"ב בדצמבר 2018 "מבדק ציון איכות למשרד ממשלתי" (להלן - מדד יה"ב). מדד יה"ב כולל מאות שאלות הנוגעות לפעולות בקרה שהמשרד הממשלתי נדרש לבצע בתחום הגנת הסייבר, והמשרד הממשלתי נדרש להשיב עליהן באופן שוטף ובהתאם לקידום המשימות שבאחריותו. מדד יה"ב נועד לאפשר לקבל בכל עת סיכום של רמת ההגנה על הסייבר, לפי חמישה רבדים עיקריים, ביניהם אחריות הנהלה ותאימות. לכל רובד ניתן ציון באחוזים, המחושב על פי תשובות המשרד הממשלתי לכל השאלות שרלוונטיות לאותו רובד. בשנת 2021 כלל מדד יה"ב 246 שאלות, ולאחר מכן צומצם ל-176 שאלות. בשנים 2021 ו-2022 משרד רה"ם מילא את השאלון המורחב הנדרש לצורך חישוב מדד יה"ב, והחל מתחילת שנת 2023 מילא את השאלון המצומצם שנדרש באותה עת לצורך חישוב המדד.

1. בתרשים שלהלן יוצגו סיכומי מדד יה"ב של משרד רה"ם בשלושת המועדים האלה: יולי 2022, נובמבר 2022 ומאי 2023.

תרשים 2 : **סיכומי מדד יה"ב של משרד רה"ם, יולי 2022, נובמבר 2022 ומאי 2023**



המקור : מדד יה"ב, על פי נתוני אגף טד"ם במשרד רה"ם.

מהתרשים עולה כי בתוך פחות משנה, מיולי 2022 עד למאי 2023, חלה ירידה בציון הכולל של מדד יה"ב במשרד רה"ם מ-86% ל-68%. הירידה בציון הכולל שניתן למשרד רה"ם נובעת מירידה חדה בהערכת התפקוד של המשרד, בין השאר בתחום אחריות, הנהלה ותאימות (מ-82% ל-66%). בתקופה זו חלה עלייה בציון של שני תחומי הגנה.

2. בדיון הוועדה למידע בלמ"ס שהתקיים במאי 2023, בראשות מנכ"ל משרד רה"ם, הוצגו הציונים של כל אחד מחמשת רובדי ההגנה על הסייבר וכן הציון הכולל של המדד במשרד במאי 2023 - 68%. ציון זה נמוך יחסית מציונים כוללים קודמים, כמתואר בתרשים שלעיל, ונחשב על פי יה"ב לציון שאינו מעיד על רמת הגנה גבוהה[4]. זאת בשעה שעל פי מדד יה"ב ביולי 2022, הציון הכולל היה 86% ושיקף רמת הגנה גבוהה.

נתוני מדד יה"ב שהוצגו לוועדה למידע בלמ"ס במאי 2023 שיקפו ירידה בציון הכולל של המדד ממאי 2023, לעומת הציון הכולל של המדד מנובמבר 2022 (78% ל-68%), וכן שיקפו ירידה חדה בשלושה מרובדי הבקרה, כאמור. על פי סיכום דיון הוועדה, היא לא העלתה שאלות ולא ביקשה לקבל מידע המסביר את פשר הירידה הניכרת ברמת ההגנה על הסייבר במשרד רה"ם, כפי שהיא משתקפת ממדד יה"ב, ולמעשה לא עסקה בממצאי מדד יה"ב. יודגש כי חבר הוועדה המשמש נציג יה"ב בה השתתף בדיון.

אחד מתפקידיה העיקריים של ועדת ההיגוי הוא לבצע בקרה ניהולית על יישום הגנת הסייבר במשרד הממשלתי, לצורך איתור פערים במרכיבים שונים של רמת ההגנה בסייבר וטיפול בהם. יוצא אפוא כי הוועדה למידע בלמ"ס, בראשות מנכ"ל משרד רה"ם, אשר שימשה כוועדת היגוי, לא ביצעה את אחד מתפקידיה העיקריים - ביצוע בקרה ניהולית, באמצעות הכלי שנבנה לצורך זה - מדד יה"ב.

4 רמות ההגנה מדורגות בסקאלה של 1-5, כאשר הציון הנדרש כדי לעמוד ברמה 5 הוא 80%.

מומלץ כי הוועדה למידע בלמ"ס תעקוב אחר ממצאי מדד יה"ב והשינויים שחלו בהם משנה לשנה, ובאמצעות מעקב זה תאתר פערים המחייבים טיפול, במטרה לבסס רמה גבוהה של הגנה על הסייבר במשרד רה"ם. עוד מומלץ כי יה"ב, שנציגה חבר בוועדה, תיזום גם היא דיון של הוועדה בממצאי מדד יה"ב.

משרד רה"ם ציין בתשובתו כי החל לפעול לתיקון הליקויים, ובכלל זה קבע את הגורם האחראי לביצוע ההמלצה האמורה ולוח זמנים לביצועה.

תקציב משרד רה"ם לתחום טכנולוגיות המידע

התקציב של משרד ממשלתי מפורט בהתאם להוראות חוק יסודות התקציב, התשמ"ה-1985. סעיף תקציב מעיד בדרך כלל על המשרד הממשלתי האחראי לו. סעיף התקציב נחלק לתחומי פעולה, וכל תחום פעולה המוקצה לעניין מסוים נחלק לפי הצורך לתוכניות, המוקצות כל אחת לעניין מסוים. לאחר שהכנסת מאשרת את חוק התקציב השנתי, קובע שר האוצר פירוט נוסף של התוכניות בתקנות תקציב. משרד ממשלתי רשאי לקיים חלוקה של תקנה ל"מרכזי קרנות". נתוני התקציב של משרדי הממשלה, לרבות יחידות הסמך שלהם, מרוכזים במערכת ממוחשבת רוחבית כוללת המכונה מרכב"ה.

בהחלטה 2443 הוטל על המנכ"לים של משרדי הממשלה להקצות תקציב ייעודי להגנת הסייבר, ולהסדיר את מבנה התקציב השנתי של המשרדים כך שלכל הפחות 8% מתקציב תחום טכנולוגיית המידע יופנה להגנת הסייבר. אחד מתפקידי ועדת ההיגוי, על פי הנחיות הגופים המאסדרים, הוא לוודא שיוקצו די משאבים להגנת הסייבר.

משרד מבקר המדינה בדק באמצעות נתוני התקציב של משרד רה"ם ושל יחידות הסמך שלו וכן באמצעות נתוני המערכת הממוחשבת של משרד האוצר (להלן - מערכת נתוני התקציב), את תקציב משרד רה"ם לתחום טכנולוגיות מידע בכל אחת מהשנים 2018 - 2023 ("תקציב מקורי" שהוקצה לצורך זה בתחילת שנת התקציב; "תקציב על שינוייו", הכולל את התקציב המקורי ואת תוספות התקציב שניתנו במהלך השנה; ו"ביצוע התקציב כולל התחייבויות", שכולל את ההוצאה בפועל מהתקציב, לרבות התחייבות המשרד להוצאה בעתיד). כן נבדקו נתוני משרד רה"ם בדבר התקציב שהוקצה להגנת הסייבר.

1. משרד רה"ם אחראי כאמור לניהול מערכות המידע ולהגנת הסייבר ב-13 משרדי ממשלה ויחידות סמך, מלבד המשרד עצמו. נכון לשנת 2023, התקציב של משרד רה"ם לתחום טכנולוגיות המידע כולל את תקציב המשרד עצמו וכן את התקציבים של משרד התפוצות והמשרד לקידום מעמד האישה. תקציב משרד רה"ם אינו כולל את התקציבים לתחום טכנולוגיות המידע של הגופים האלה: ארכיון המדינה, שהוא יחידה במשרד רה"ם; לשכת הפרסום הממשלתית והמל"ל, שהן יחידות סמך של משרד רה"ם; המשרד למודיעין; המשרד לנושאים אסטרטגיים; משרד ירושלים ומסורת ישראל; ורשות השירות הלאומי-אזרחי, שהיא יחידת סמך של משרד ההתיישבות.

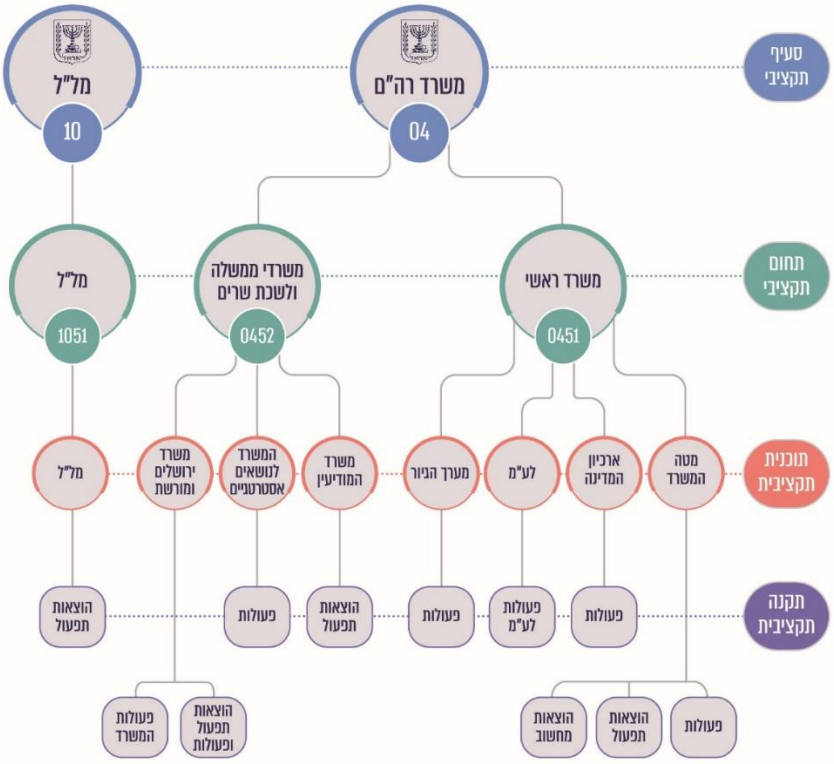
   במערכת מרכב"ה יש נתונים על התקציב לתחום טכנולוגיות המידע במשרד רה"ם, ללא הבחנה בין התקציב להגנת הסייבר לבין התקציב למטרות אחרות. כלומר, אי אפשר לנתח, על פי נתוני מרכב"ה, את החלק של תקציב הגנת הסייבר מתוך התקציב הכולל לתחום טכנולוגיות המידע.

   מהאמור לעיל עולה כי מנתוני מרכב"ה אי אפשר לדעת מה הוא מכלול התקציב של משרד רה"ם לתחום טכנולוגיות המידע וכמה ממנו מיועד להגנת הסייבר, ולפיכך אי אפשר לדעת אם משרד רה"ם מקצה 8% ממכלול התקציב לתחום טכנולוגיות המידע להגנת הסייבר, כנדרש.

2. התקציב לתחום טכנולוגיות המידע של משרד רה"ם נכלל בשני סעיפי תקציב: תקציב משרד רה"ם (04) ותקציב המל"ל (10). סעיף התקציב של משרד רה"ם נחלק לתחומי פעולה, ובהם

תחום המשרד הראשי (0451) ותחום משרדי ממשלה ולשכות שרים (0452), הכולל משרדי ממשלה שניהול תחומים מסוימים בהם הוא באחריות משרד רה"ם, כגון משרד המודיעין והמשרד לנושאים אסטרטגיים. תחום המשרד הראשי מחולק למטה המשרד וליחידות אחרות במשרד - ארכיון המדינה, לשכת העיתונות הממשלתית (להלן - לע"מ) ומערך הגיור. תחת תוכנית מטה המשרד מצויה תקנת התקציב העיקרית של משרד רה"ם לתחום טכנולוגיות המידע - "הוצאות מחשוב". לצד תקנה זו, קיימות תקנות תקציב נוספות שבאמצעותן ממומנות הוצאות מחשוב של המשרד (תקנת "פעולות" ותקנת "הוצאות תפעול"). גם תחת כל אחת מהתוכניות המיועדות לתקציבי ארכיון המדינה, לע"מ ומערך הגיור יש תקנות המכונות "פעולות", והן משמשות גם למימון הוצאות מחשוב. המערך התקציבי המתואר לעיל מוצג בתרשים שלהלן:

תרשים 3: **מערך תקציבי טכנולוגיות המידע בגופים שבאחריות משרד רה"ם, 2022**



המקור: נתוני משרד האוצר.

מהתרשים עולה כי התקציב של משרד רה"ם לתחום טכנולוגיות המידע פרוס על פני 11 תקנות תקציביות (כולל תקנה בתקציב המל"ל). אחת מהן מיועדת להוצאות מחשוב, והשאר מיועדות ל"פעולות" או ל"הוצאות תפעול". משכך תקציב טכנולוגיות המידע בשנים 2018 - 2023 על פי נתוני משרד רה"ם (63 מיליון ש"ח) קטן מהתקציב בפועל (73 מיליון ש"ח), כפי שמשתקף מנתוני מרכב"ה (לרבות תקנות המיועדות לפעולות ולהוצאות תפעול כלליות)[5].

אגף תקציבים במשרד האוצר ציין בתשובתו כי משרד רה"ם רשאי לפתוח מגוון מרכזי קרנות ולסווג באמצעותם את ההוצאה להגנת הסייבר בנפרד מהוצאות מחשוב אחרות.

---

5 לפי נתוני מרכב"ה לשנת 2022, ממרכז קרנות "אגף מערכות מידע של משרד רה"ם" חויבו התקנות האלה: תקנת הוצאות תפעול בתקציב המשרד למודיעין בסך כ-1.5 מיליון ש"ח; תקנת פעולות בתקציב המשרד לנושאים אסטרטגיים בסך כ-140,000 ש"ח; ותקנות תפעול ופעולות, ופעולות המשרד בתקציב משרד ירושלים ומורשת בסך 692,000 ש"ח.

רישום ההוצאות של משרד רה"ם בתחום טכנולוגיות המידע בתקנות תקציביות שונות, ובהן תקנות שמיועדות להוצאות שונות, לא רק בתחום זה, מקשה את איגום הנתונים בדבר תקציב המשרד בתחום טכנולוגיות המידע, ואף פוגע ביכולת ועדת ההיגוי לוודא שהמשרד הקצה די משאבים לצורך הגנת הסייבר.

3. בשנים 2018 - 2023 אגף טד"ם לא הציג לוועדת ההיגוי למידע בלמ"ס את פירוט התקציב להגנת הסייבר, והסתפק באמירה שמשרד רה"ם עומד בשיעור הנדרש של התקציב להגנת הסייבר מכלל התקציב לתחום טכנולוגיות המידע (8%)[6]. על פי סיכומי הוועדה בשנים האמורות, הוועדה לא העלתה שאלות בנוגע לתקציב, קיבלה את המסקנות שהוצגו לה ללא עוררין ולא עמדה על הצגת נתונים מלאים, כדי שתוכל לוודא שהוקצו די משאבים להגנת הסייבר - 8% לפחות מהתקציב לתחום טכנולוגיות המידע.

בשנים 2018 - 2023 ועדת ההיגוי למידע בלמ"ס לא וידאה שהוקצו די משאבים להגנת הסייבר, על פי הנדרש בהחלטת הממשלה: בשנים 2020 ו-2021 הוועדה לא עסקה בנושא מכיוון שלא קיימה דיונים, וביתר השנים הוועדה הסתפקה בדיווח כללי שהוצג לפניה, ולפיו משרד רה"ם עומד בדרישת ההקצאה להגנת הסייבר, ולא דרשה להציג לפניה נתונים כספיים כדי לוודא שהדיווח מדויק.

4. בלוח שלהלן מוצגים נתוני משרד רה"ם על תקנת התקציב "הוצאות מחשוב", שהיא כאמור התקנה המרכזית של מטה משרד רה"ם לתחום טכנולוגיות המידע, בשנים 2018 - 2023 (עד יוני 2023), על פי מערכת נתוני התקציב ונתוני אגף טד"ם: התקציב המקורי, התקציב על שינוייו וביצוע התקציב כולל התחייבויות. לצורך הניתוח מובאים בלוח גם נתונים שאגף טד"ם ריכז לבקשת משרד מבקר המדינה על התקציב שהוקצה להגנת הסייבר. נתונים אלה של משרד רה"ם כוללים כאמור רק חלק מהתקציבים שעומדים לרשות אגף טד"ם.

לוח 1: **תקציב תקנת "הוצאות מחשוב" של מטה משרד רה"ם בשנים 2018 - 2023 (עד יוני 2023), באלפי ש"ח**

	תקציב טכנולוגיות המידע המקורי	תקציב טכנולוגיות המידע על שינוייו	ביצוע התקציב כולל התחייבויות	שיעור ביצוע התקציב על שינוייו (מעוגל)	התקציב שהוקצה להגנת הסייבר	שיעור תקציב הגנת הסייבר מתקציב טכנולוגיות המידע על שינוייו
2018	25,000	49,361	49,200	100%	7,070	14%
2019	25,000	55,367	56,836	103%	7,163	13%
2020	30,000	60,967	60,960	100%	5,891	10%
2021	33,227	56,080	56,060	100%	7,811	14%
2022	32,833	63,284	53,282	84%	8,612	14%
2023	33,745	72,101	68,528	95%	7,345	10%

המקור: נתוני משרד האוצר ונתוני אגף טד"ם במשרד רה"ם.

א. מהלוח עולה כי בכל אחת משש השנים שנבדקו קיבל משרד רה"ם במהלך השנה תוספות תקציב ניכרות לתקנת התקציב "הוצאות מחשוב": 97% בשנת 2018; 121% בשנת 2019; 103% בשנת 2020; 69% בשנת 2021; 93% בשנת 2022; 114% בשנת 2023 (עד יוני 2023). נתוני הביצוע של משרד רה"ם בתקנה זו, המפורטים בלוח, מלמדים על

6 בנובמבר 2018 לא הוצגו כלל נתוני תקציב, ונמסר לחברי הוועדה כי משרד רה"ם עומד בדרישה של הקצאת 8% מסך התקציב בתחום טכנולוגיות המידע להגנת הסייבר; באוגוסט 2019 הוצגו לחברי הוועדה נתונים חלקיים על התקציב להגנת הסייבר; בשנים 2020 - 2021 הוועדה לא קיימה כאמור דיונים, ולא הוצגו לפניה נתוני תקציב; בנובמבר 2022 ובמאי 2023 הוצגו לוועדה נתונים כוללים על התקציב להגנת הסייבר, ונמסר לחברי הוועדה כי משרד רה"ם "מוציא... כ-11%" מהתקציב בתחום טכנולוגיות המידע להגנת הסייבר. על פי משרד רה"ם, הוא ריכז נתונים על התקציב להגנת הסייבר מרשימות שערך, שלא באמצעות מערכת נתוני התקציב.

ניצול מלא של התקציב בשנים 2018 - 2021 וניצול כמעט מלא של התקציב בשנים 2022 - 2023 (עד יוני 2023).

מהנתונים האלה עולה כי התקציב שתכנן משרד רה"ם לתחום טכנולוגיות המידע בתקנת התקציב "הוצאות מחשוב" בכל אחת משש השנים (התקציב המקורי, שנע בין 25 מיליון ש"ח ל-33.7 מיליון ש"ח), לא שיקף את צורכי המשרד, כפי שבאו לידי ביטוי בביצוע התקציב (בין 49.2 מיליון ש"ח בשנה ל-68.5 מיליון ש"ח בשנה), ולא שיקף את התקציב שהוקצה לו בפועל (בין 49.3 מיליון ש"ח בשנה ל-72.1 מיליון ש"ח בשנה). עקב כך קיבל המשרד תוספות תקציב שברוב השנים האמורות הכפילו את תקציביו, ואף יותר מכך, ואלה נוצלו כמעט במלואן.

ב. עוד עולה מהלוח כי על פי נתוני משרד רה"ם, הוא הקצה להגנת הסייבר בין 10% ל-14% מהתקציב לתחום טכנולוגיות המידע. ואולם כאמור, נתונים אלו אינם כוללים את נתוני התקציב לתחום טכנולוגיות המידע ולהגנת הסייבר של כלל היחידות שנמצאות באחריות אגף טד"ם במשרד רה"ם.

על משרד רה"ם לפעול לתיקון הליקויים שעלו בניהול התקציב בתחום טכנולוגיות המידע, לרבות התקציב להגנת המידע, ובכלל זה לרכז נתונים על כלל התקציבים שעומדים לרשות המשרד לצורך ניהול טכנולוגיות המידע בכל הגופים שהוא אחראי להם, וכן לנהל רישום תקציבי נפרד של תקציבים המופנים להגנת הסייבר. זאת כדי שיהיו בידי משרד רה"ם נתונים מלאים על התקציב בתחום טכנולוגיות המידע בכל המשרדים והיחידות שמקבלים ממנו שירותים בתחום זה, וכדי שיהיה אפשר לבדוק, על פי הרישום במערכת מרכב"ה, אם משרד רה"ם עומד בדרישה העולה מהחלטת הממשלה - להקצות לצורכי הגנת המידע 8% לפחות מהתקציב לתחום טכנולוגיות המידע. נוסף על כך, מומלץ שהמשרד יגבש מדי שנה בשנה, בהתאם לצרכיו, את דרישותיו לגבי תקציב ניהול טכנולוגיות המידע, כדי לצמצם את הצורך בתוספות תקציב ניכרות במהלך השנה.

משרד רה"ם ציין בתשובתו כי החל לפעול לתיקון הליקויים, ובכלל זה קבע את הגורם האחראי לביצוע ההמלצה האמורה ולוח זמנים לביצועה. אגף תקציבים במשרד האוצר ציין בתשובתו כי מאחר ששיעור הביצוע של התקציב במשרד רה"ם בשנים האחרונות הוא נמוך יחסית[7], יהיה נכון לבחון את התקציב גם על פי שיעור ביצועו בפועל, שהיה נמוך בשנים 2018 - 2023.

סקרי הערכת סיכונים

סקר הערכת סיכונים (להלן - סקר סיכונים) הוא תהליך שיטתי שמטרתו לזהות נכסים, תהליכי מידע ואיומים הנשקפים להם, להעריך את הסיכון הנובע מהאיומים ולזהות את הבקרות הנדרשות לצמצום הסיכונים, תוך התחשבות בסבירות ההתממשות ובנזק הפוטנציאלי עקב כך. בכל הנוגע לעולם הסייבר ומערכות המידע, הסיכון שנדרש להעריך בסקר סיכונים מוגדר כאפשרות לחשיפת נכסי המידע או לפגיעה וגרימת נזק לנכסי המידע, עקב ניצול פגיעות או חולשה הקיימות בנכסי המידע. נכסי המידע של משרד רה"ם הם המידע, מערכות המחשוב המעבדות ומאחסנות אותו, רכיבי התקשורת שמעבירים אותו, האמצעים וציוד המחשב שעליו הוא מושתת. בתרשים שלהלן מוצגים השלבים הכלולים בסקר הערכת הסיכונים לגבי נכסי המידע, אשר עשויים לגרום נזק לתפקודו התקין של המשרד.

[7] ראו גם בלוח לעיל - שיעור תקציב הגנת הסייבר מתקציב טכנולוגיות המידע על שינוייו.

תרשים 4: **השלבים בביצוע של סקר הערכת סיכונים**

על פי הנחיות הגופים המאסדרים, בעיבוד משרד מבקר המדינה.

על פי הנחיות הגופים המאסדרים, על משרד ממשלתי לבצע סקר סיכונים במערכות המידע שלו לכל הפחות אחת ל-36 חודשים ולתקף את ממצאי הסקר לפחות אחת ל-18 חודשים. סקר הסיכונים יהיה עבור המשרד בסיס לבניית תוכנית עבודה רב-שנתית ושנתית. במקרים מיוחדים, כגון שינוי ניכר בסביבה הטכנולוגית או בתהליכי העבודה, על המשרד לבצע סקר סיכונים נוסף. האחריות לייזום סקרי הסיכונים מוטלת על מנהל מערכות המידע במשרד.

להלן סקרי הסיכונים שערך משרד רה"ם משנת 2017 ועד למועד סיום הביקורת. בשנת 2017 ביצע משרד רה"ם סקר סיכונים לגבי מערכות המידע שלו ברשת הבלמ"ס. בסקר מופו 26 תהליכי עבודה ונכסי מידע, וכן בוצעו השלבים הנדרשים בסקר סיכונים על פי הנחיות הגופים המאסדרים. נוסף על כך ביצע המשרד משנת 2018 סקרי סיכונים ל-11 מערכות מידע חדשות שפותחו, תוך התייחסות לסיכוני אבטחת מידע רוחביים הנוגעים לפיתוח מערכות מידע חדשות, כגון חשש לדליפת מידע וגישה של גורמים לא מורשים למערכת המידע עקב מנגנוני הזדהות חלשים.

בשנת 2023 ערך משרד רה"ם סקר סיכונים של הרשת הבלמ"ס. מסיכום הסקר עולה כי מופו 28 סיכונים עיקריים של פגיעויות ואיומים על אבטחת המידע ברשת הבלמ"ס; נבדקה רמת ההגנה שיושמה בפועל בארכיון המדינה, שהוא יחידה מיחידות המשרד; מופו מערכות ההגנה והבקרות העיקריות הקיימות ברשת; נותח הפער בין רמת ההגנה הנדרשת לפי מדיניות המשרד ונוהלי המשרד לבין זו הקיימת בפועל; הוגדרה רמת הסיכונים השיוריים[8], וגובשו המלצות לטיפול בהם.

נמצא כי משרד רה"ם ערך סקר סיכונים כולל בשנת 2017 וכן ערך סקרי סיכונים ממוקדים במערכות מידע שפותחו לאחר מכן. בשנת 2023 המשרד ערך סקר סיכונים חלקי: הוא לא מיפה תהליכי עבודה ונכסי מידע ולא העריך את המידה שבה הם קריטיים לפעילותו; מיפה באופן חלקי מערכות הגנה ובקרה קיימות; ומיפה פגיעויות ואיומים, אך לא בפירוט לגבי כל נכס מידע; קבע רמת הגנה נדרשת על נכסי מידע וניתח את הפער בין רמת ההגנה הנדרשת לרמת ההגנה בפועל רק באופן כללי, ולא בפירוט לגבי כל נכס מידע. יוצא אפוא כי משרד רה"ם ביצע סקר סיכונים שלא על פי הנדרש בהנחיות הגופים המאסדרים.

מומלץ שמשרד רה"ם יפעל לביצוע סקרי סיכונים ותיקופם, כנדרש בהנחיות הגופים המאסדרים.

משרד רה"ם ציין בתשובתו כי החל לפעול לתיקון הליקויים, ובכלל זה קבע את הגורם האחראי לביצוע ההמלצה האמורה ולוח זמנים לביצועה. שב"כ ציין בתשובתו כי ביצע בינואר 2019 ביקורת סקר סיכונים לגבי הרשת המסווגת של משרד רה"ם, ובכוונתו לבצע סקרי סיכונים ברשתות מסווגות.

8 הסיכון השיורי מוגדר כסיכון שנותר לאחר התחשבות בבקרות הקיימות נכון למועד ביצוע הסקר. זאת בשונה מהסיכון השורשי, שהוא הסיכון המובנה הנובע מעצם קיום הפעילות, ללא קיומן של בקרות כלל.

איוש כמה תפקידי ליבה על ידי מנהל אגף טד"ם

על פי חוזר נש"ם מיוני 2011, על משרד ממשלתי לאייש ארבעה תפקידי ליבה באגף מערכות מידע בעובדי מדינה בלבד. ארבעת התפקידים הם **מנהל אגף בכיר מערכות מידע** (להלן - מנמ"ר), המופקד על מכלול שירותי טכנולוגיות המידע והמחשוב של המשרד, ובין תפקידיו ליזום תוכניות עבודה וליישמן, לתכנן ולנהל את התקציב בתחום טכנולוגיות המידע וליזום רכש ופיתוח של חומרה ותוכנה על פי צורכי המשרד; **מנהל תחום בכיר יישומים**, המופקד על ניהול היישומים באגף מערכות מידע, לרבות פיתוח, יישום והטמעה של הפרויקטים הממוחשבים של המשרד; **מנהל תחום בכיר טכנולוגיות ופיתוח** (להלן - מנהל טכנולוגיות), האחראי לתכנון, לתפעול ולתחזוקה של הטכנולוגיות במערכות המשרד, לרבות בחינת טכנולוגיות חדשות ואחריות לשרידות המערכות; **מנהל תחום (יישום אבטחת מידע)**, המופקד על יישום מדיניות אבטחת המידע במערכות המידע, ובין תפקידיו ליווי פרויקטים בתחום המחשוב בכל הנוגע לאבטחת מידע, הכנת תוכנית עבודה שנתית לתחום אבטחת המידע ובקרה על פעילויות ממוחשבות, לשם מניעת פרצות במערכות המחשוב. כאמור, הממשלה החליטה בשנת 2015 למנות בכל אחד ממשרדי הממשלה ממונה על הגנת הסייבר, שיהיה אחראי בין היתר לגיבוש מדיניות הגנת הסייבר, בניית מתווה תוכנית העבודה להגנת הסייבר וגיבוש מתווה לתוכנית התקציבית לטיפול בהגנת הסייבר.

נמצא כי מנהל אגף טד"ם משמש גם הממונה על הגנת הסייבר של משרד רה"ם. בשנים 2018, 2019 ו-2022 שימש מנהל אגף טד"ם כממלא מקום יו"ר ועדת ההיגוי - הוועדה למידע בלמ"ס וניהל כממלא מקום את דיוני הוועדה באותן שנים. משנת 2021 מנהל האגף משמש גם מנהל הטכנולוגיות של המשרד (כמפורט להלן). יוצא אפוא כי במשך שנתיים וחצי מנהל אגף טד"ם ממלא למעשה שלושה מחמישה תפקידים מרכזיים בתחום טכנולוגיות המידע במשרד רה"ם[9], ונוסף על כך, בחלק מהתקופה הוא שימש גם ממלא מקום יו"ר הוועדה למידע בלמ"ס.

מצב שבו מנהל אגף טד"ם ממלא למעשה שלושה מתפקידי הניהול הבכירים באגף עלול לפגוע בביצוע המשימות שבאחריותו. יתר על כן, ניהול אגף טד"ם, תוך ביצוע משימות של בעל תפקיד ליבה באגף - אחראי אבטחת מידע, עלול לפגוע ביכולת הפיקוח והבקרה על משימות בתחום אבטחת המידע.

ארכיון המדינה הוא יחידה במשרד רה"ם, ומנוהל בו הארכיון הממלכתי של מדינת ישראל. על פי מסמכי משרד רה"ם, משנת 2021 (לכל המאוחר) ועד אמצע שנת 2023 שימש מנהל הטכנולוגיות באגף טד"ם, הלכה למעשה, גם מנהל אגף מערכות מידע בארכיון המדינה. משרד רה"ם לא הסדיר בתקופה הזו בתקן המשרד את פיצול משרתו של מנהל הטכנולוגיות, וממסמכי המשרד אי אפשר לדעת כיצד מתחלקת המשרה בין שני התפקידים. ביוני 2023 אישרה נציבות שירות המדינה, לבקשת משרד רה"ם, את העברת המשרה שבה כיהן מנהל הטכנולוגיות לארכיון המדינה. במשך כחצי שנה, מיוני 2023 ועד למועד הבירור האחרון שערך משרד מבקר המדינה בנובמבר 2023, משרת מנהל הטכנולוגיות לא אוישה. משרד רה"ם מסר למשרד מבקר המדינה כי מנהל אגף טד"ם הודיע שישמש גם מנהל הטכנולוגיות של המשרד.

נציבות שירות המדינה, אשר קבעה את הכללים שלפיהם משרד ממשלתי נדרש לאייש ארבעה תפקידי ליבה, ובהם תפקיד מנהל הטכנולוגיות, אישרה למשרד רה"ם לוותר על משרה זו ולהעביר אותה לארכיון המדינה. במסמכי משרד רה"ם והנציבות לא צוינו נימוקי הנציבות להחלטה לוותר על משרת מנהל טכנולוגיות במשרד רה"ם.

לנוכח הכללים שקבעה נש"ם והחשיבות שהיא ראתה באיוש ארבעת תפקידי הליבה האמורים באגף מערכות מידע בעובדי מדינה, מומלץ כי משרד רה"ם יפעל ליצירת משרה של מנהל טכנולוגיות במשרד ולאיושה וכן יפעל לאיוש משרת הממונה על הגנת הסייבר.

---

[9] בשנים 2018 - 2022 הוא מילא, נוסף על תפקידו, גם את תפקיד אחראי אבטחת המידע, ומשנת 2021 ועד אוגוסט 2023 מילא גם את תפקיד מנהל הטכנולוגיות באגף טד"ם.

משרד רה"ם ציין בתשובתו כי פרסם בינואר 2024 מכרז לאיוש תפקיד מנהל הטכנולוגיות באגף טד"ם, וכי החל בהליך למינוי הממונה על הגנת הסייבר באגף זה.

☆

בשנת 2015 החליטה הממשלה על שורה של פעולות יסודיות בכל אחד ממשרדי הממשלה, כדי לשפר את רמת ההגנה במרחב הסייבר בתחומים שבאחריותם. הביקורת העלתה ליקויים בהיבטים השונים של ניהול-העל בתחום טכנולוגיות המידע במשרד רה"ם: הוועדה למידע בלמ"ס והוועדה למידע מסווג פעלו בהיקף מצומצם מהנדרש, ובין השאר עלו ליקויים באופן שבו מילאו את תפקידיהן - לעדכן את המדיניות המשרדית בתחום טכנולוגיות המידע; לאשר את תוכניות העבודה השנתיות; לבקר את יישום הפעולות הנדרשות להגנת הסייבר; לוודא שיוקצו משאבים להגנת המידע, על פי הנדרש בהחלטת הממשלה; ולבצע סקרי סיכונים ולתקפם בתדירות הנדרשת.

מומלץ שמנכ"ל משרד רה"ם יפעל לתיקון הליקויים שעלו בביקורת, ובכלל זה, יקפיד שוועדת ההיגוי להגנת הסייבר תפעל בהתאם לנדרש על פי החלטת הממשלה ותוודא שיובאו לפניה נתונים מרוכזים על כלל התקציבים שעומדים לרשות המשרד לצורך ניהול טכנולוגיות המידע והגנת הסייבר בכל הגופים שלהם אחראי אגף טד"ם; יקפיד על ביצוע סקרי סיכונים ותיקופם ויוודא כי תחום טכנולוגיות המידע במשרד ינוהל גם בהתאם לנדרש בהחלטת הממשלה משנת 2015.

הזדהות משתמשים וניהול הרשאות

ההגנה הלוגית[10] 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. כאשר הגנה לוגית 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[11] 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[12].

<u>הזדהות משתמשים במערכות הממוחשבות</u>

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

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.

---

10 הגנה המשתמשת בתוכנות ובנתונים כדי להגן על הזמינות, השלמות והסודיות של הנתונים והתהליכים הממוחשבים.

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

12 אימות זהות המשתמש נעשה באמצעות נתון מיוחד הנוגע לאדם המזדהה, למשל באמצעות השוואת הסיסמה שהוא הזין לסיסמתו במאגר הסיסמאות של הארגון.

הגופים המאסדרים קבעו כללים בנוגע לתדירות החלפת סיסמאות, בהבחנה בין קבוצות משתמשים שונות.

אמצעי הזדהות לצורך כניסה לרשת

הכניסה לרשתות של משרד רה"ם אינה עומדת בכללים הנדרשים על פי הנחיית הגופים המאסדרים. כן נמצא כי ההגדרות הלוגיות שקבע משרד רה"ם בעניין סיסמתם של משתמשים מסוגים שונים אינן עולות בקנה אחד עם ההנחיות.

☆

מערך ההזדהות המיושם בעת הגישה למערכות הארגון נועד לוודא כי הגישה למערכת מידע, לרכיב תקשורת או למידע מוגבלת למורשים בלבד, וכן למנוע מגורמים עוינים להשיג גישה לרשתות הארגון. כאשר מדובר במערכות רגישות, דוגמת מערכות המידע במשרד רה"ם, 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 ויישם משרד רה"ם, המאפשר גישה לרשתות של משרד רה"ם. הליקויים היו בין השאר בנוגע להחלפה עיתית של סיסמאות הגישה לרשתות, ועלו בנוגע לחשבונות של משתמשים בקבוצות שונות. ליקויים אלה במשרד רה"ם, פוגעים ברמת ההגנה של המערכות, מסכנים שלא לצורך את השלמות, הסודיות והזמינות של המידע האצור בהן ומחייבים תיקון מיידי.

על משרד רה"ם ליישם מנגנון המספק את ההגנה הנדרשת בעת הכניסה לרשתות המשרד, להתאים את הדרישות הלוגיות בעת הכניסה לרשתות לנדרש על פי הנחיות הגופים המאסדרים וליישם את כלל ההנחיות שנקבעו בנושא בעת הכניסה לרשתות, בשים לב להבחנה שבין קבוצות המשתמשים השונות. על משרד רה"ם גם לוודא כי בכל החשבונות הפעילים ברשתות המשרד תוחלף הסיסמה בתדירות הנדרשת.

ניהול הרשאות גישה למערכות הממוחשבות

על פי הנחיות הגופים המאסדרים, 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. בהנחיות 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 מתן מספר ההרשאות המזערי הנדרש לצורך ביצוע העבודה (least privilege). מטרת הנחיות הגופים המאסדרים היא להקשות על תוקפים פוטנציאליים לתקוף את הרשת באמצעות חשבונות המשתמשים המורשים לגשת אליה.

משרד רה"ם אינו מנהל כראוי את הרשאות הגישה לרשתות הממוחשבות שלו. כאמור, נמצאו ליקויים במערך ההזדהות שקבע ויישם משרד רה"ם, המאפשרים גישה לרשתות של משרד רה"ם, לרבות בנוגע להחלפה עיתית של סיסמאות הגישה לרשתות שלא על פי הנדרש בנוהל המשרדי. ליקויים כאלה עלו בנוגע לחשבונות של משתמשים בקבוצות שונות. ליקויים אלה במשרד רה"ם, פוגעים ברמת ההגנה של המערכות ומסכנים שלא לצורך את השלמות, הסודיות והזמינות של המידע האצור ברשתות המשרד ומחייבים תיקון מיידי.

מלבד הרשאת גישה לרשת, ניתנות לעובד גם הרשאות שהוגדרו לקבוצות העבודה שאליהן הוא משתייך. ברשת מסויימת שנבחנה אותרו קבוצות הרשאה שכבר אינן רלוונטיות, כגון קבוצה שיוחדה לצוות של שר ללא תיק לשעבר שסיים את תפקידו לפני למעלה מעשור וכן עשרות קבוצות "כפולות" בעלות שם זהה, שבכל אחת מהן חברים משתמשים אחרים. למשרד רה"ם אין מידע מרוכז בדבר תוכנה וענייניה של כל קבוצת הרשאה.

הגדרת מועד תפוגה לחשבונות מסייעת לניהול תקין של מערך ההרשאות ומאפשרת שליטה ובקרה על הרשאות שניתנו. נמצא כי משרד רה"ם קבע תאריכי תפוגה רק לחלק מהחשבונות של המשתמשים הפעילים ברשתות (בין 19% ל-62% מהחשבונות ברשתות שנבחנו). אותרו חשבונות שהוגדר לגביהם מועד פקיעת תוקף, אולם הם נותרו במצב "פעיל" (enable) גם לאחר אותו מועד (בין 6% ל-40% מהחשבונות ברשתות שנבחנו). כן נמצאו חשבונות משתמשים שלגביהם נקבעו מועדי פקיעת תוקף רחוקים ובלתי רלוונטיים, בין שנת 2033 לשנת 2071.

ברשת מסויימת במשרד רה"ם שנבחנה לא בוצעה בקרה על ההרשאות של קבוצות משתמשים ועל מתן הרשאות לעובדים, כנדרש בהנחיות הגופים המאסדרים, במשך שלוש שנים וחצי, מתחילת שנת 2020 ועד אוגוסט 2023.

משרד רה"ם מאפשר גישה לרשתות גם באמצעות חשבונות שלא נעשה בהם שימוש (בין 18% ל-43% מהחשבונות ברשתות שנבחנו נותרו פעילים (enable) במועד הבדיקה, אף שהיו צריכים להינעל בשל אי-השימוש בהם). המשרד מאפשר גישה כאמור גם באמצעות חשבונות של עובדים שסיימו זה מכבר את עבודתם במשרד. הותרת אפשרות הגישה לרשתות באמצעות חשבונות אלה מאפשרת לגורמים לא מורשים - פנימיים או חיצוניים - לצפות במידע ולהשתמש בו, ולפיכך מהווה סיכון מהותי למידע האצור ברשתות.

ממצאי הביקורת העלו חשד שעובדים לשעבר השתמשו בחשבונותיהם לאחר סיום העסקתם, או שגורמים אחרים, במשרד או מחוצה לו, השתמשו בחשבונות עובדים שהעסקתם הסתיימה, תוך שהם נחשפים למידע המצוי ברשתות משרד רה"ם שלא היו אמורים להיחשף אליו ומסוגלים לבצע פעולות שאינם אמורים לבצע. בין היתר נעשה שימוש בחשבונו של שר לשעבר ובחשבונו על בעל תפקיד בכיר במשרד רה"ם, שסיימו את כהונתם זה מכבר. חשדות אלה מחייבים בדיקת עומק ממצה של כל אחד מהמקרים שעלו, כדי לאמת או לשלול כל אחד מהחשדות.

☆

ממצאי הביקורת מעלים כי משרד רה"ם אינו מנהל כראוי את הרשאות הגישה לרשתות הממוחשבות שלו. בכלל זה, משרד רה"ם מאפשר גישה לרשתות גם באמצעות חשבונות שלא נעשה בהם שימוש במשך תקופה ארוכה, ואף באמצעות חשבונות של עובדים שסיימו זה מכבר את עבודתם במשרד. הותרת אפשרות הגישה לרשתות באמצעות חשבונות אלה מאפשרת לגורמים לא מורשים - פנימיים או חיצוניים - לצפות במידע ולהשתמש בו, ולפיכך היא מהווה סיכון מהותי למידע האצור ברשתות.

ממצאי הביקורת העלו חשד לשימוש בחשבונות של עובדים לשעבר לאחר סיום העסקתם. חשדות אלה מחייבים בדיקת עומק ממצה של כל אחד מהמקרים שעלו, כדי לאמת או לשלול כל אחד מהחשדות.

על משרד רה"ם, בשיתוף השב"כ, לבצע בדיקות עומק כאמור ולפעול בהתאם לממצאיהן, וכן לבצע בדיקות רוחביות בכל רשתות המשרד, כדי להבטיח שכל המקרים שעלה מהם חשד כאמור נבדקו היטב.

נוסף על כך, על משרד רה"ם לבטל הרשאות של עובדים עם סיום העסקתם במשרד והרשאות בחשבונות שלא נעשה בהם שימוש; ולוודא העברת החשבונות למצב לא פעיל (disable). כן

מומלץ שמשרד רה"ם ינפיק, במסגרת הבקרות שעליו לערוך, "דוח חריגים" שיאפשר לאתר מצבים המשקפים חריגה מניהול תקין של מערך הגישה לרשתות המשרד, כגון חשבונות שנותרו פעילים (enable) אף שהעובדים שלהם משויכים החשבונות כבר סיימו את העסקתם במשרד, והתחברות לרשת באמצעות חשבונות כאלה או חשבונות שלא נעשה בהם שימוש.

משרד רה"ם ציין בתשובתו כי החל לפעול לתיקון הליקויים, ובכלל זה קבע את הגורם האחראי לביצוע ההמלצות האמורות ולוח זמנים לביצוען.

ניטור מערכות ברשת מסוימת שנבחנה

על פי הנחיות הגופים המאסדרים, איסוף וניתוח של מידע על פעולות הנעשות במערכות ממוחשבות ועל אירועים שמתחוללים בהן מאפשרים לחשוף ניסיונות לביצוע פעולות לא מורשות במערכות, לזהות מתקפות על המערכות ולסייע בתהליך ההתאוששות מהן. איסוף וניתוח של פעולות ואירועים כאלה יכול שיתבצע בזמן אמת, באמצעות כלים ממוחשבים לאיתור פעולות חריגות, או בדיעבד, באמצעות ניתוח נתונים על פעולות שנעשו. תנאי מקדים לביצוע פעילות זיהוי הוא איסוף מידע רלוונטי. כמו כן, על פי ההנחיות, יש לאסוף מידע כאמור באופן שיטתי באמצעות מערך ניטור, שתכליתו איסוף המידע הרב המוזרם מרכיבי המערכת הממוחשבת, סינונו וגיבוש תובנות מעשיות כבסיס לתגובה ותיקון ככל שנדרש. הניטור מתחיל במידע שנצבר בקובצי LOG על פעולות שהתרחשו ברכיב מסוים של המערכת ואירועים שהתחוללו בו. קובצי ה-LOG נאספים מרכיבים שונים באמצעות מערכת SIEM (System Information Event Manager) ומנותחים על פי חוקים והגדרות שנקבעו למערכת, ומערכת SIEM מתריעה על אירועים חריגים בהתאם לחוקים שהוגדרו. למשל, ניתן להגדיר במערכת זו כי יש להתריע על כל מצב שבו עובד מנסה להיכנס לתיקייה שאינו מורשה להיכנס אליה. המידע המעובד בידי מערכת SIEM, לרבות התרעות המתקבלות בהתאם לחוקים שהוגדרו, מוצג במרכז הגנת המידע של הארגון, המכונה SOC (Security Operation Center). צוות ה-SOC נדרש בין היתר לזהות אירועים חריגים שנוטרו, לבצע חקירה ראשונית בעניינם ולפעול בהתאם לממצאיה.

בנוהלי משרד רה"ם פורטו דרכי הפעולה לניטור, ניתוח ומתן התרעות כאמור. למשל, יש לתחקר אירועי סייבר שזוהו בידי מערכת SIEM ולעקוב אחר אירועים חריגים. במקרה של אירוע סייבר יש לאסוף נתונים על האירוע, ובכלל זה על מקורו (פנימי או חיצוני, חומרה או תוכנה); לזהות את המערכות המעורבות בו; לזהות את ההשפעה הפוטנציאלית של האירוע על שלמותן של מערכות המידע, סודיותן וזמינותן; ולעדכן את סטטוס האירוע עד גמר הטיפול.

תפעול יעיל של SOC כולל אפוא שלושה נדבכים עיקריים: (א) חיבור כל רכיבי המערכות הממוחשבות של הארגון למערכת SIEM; (ב) הגדרת חוקים שלפיהם תנתח מערכת SIEM את המידע בקובצי ה-LOG ותייצר התרעות ל-SOC; (ג) טיפול בהתרעות שהתקבלו ב-SOC. יצוין כי במשרד רה"ם פעלו בתקופת הביקורת שני מערכי ניטור. הביקורת בדקה את פעילות ה-SOC ברשת מסוימת.

ניטור פעולות ברשת מאפשר לחשוף ניסיונות לביצוע פעולות לא מורשות במערכות, לזהות מתקפות עליהן ולסייע בתהליך ההתאוששות מאירועי פגיעה באבטחת המידע. נמצא כי משרד רה"ם לא הפעיל את מערך הניטור ברשת מסויימת שנבחנה כנדרש: חלק מרכיבי הרשת לא חוברו למערכת הניטור המשרדית (SIEM), ורכיבים אחרים לא הפיקו קובצי LOG; ועלה חשש שהמשרד לא קבע כללים מספקים למערך הניטור, לרבות קביעת המקרים שעליהם המערכת תתריע. בשל כל אלה הצטמצמה יכולת המשרד בין השאר לזהות מתקפות על המערכות ולהתאושש מהן היטב ובמהירות.

המשרד לא קבע תקן למשך הטיפול בהתרעות ברשת המסויימת שנבחנה. כמו כן, עלה חשש לפגיעה באבטחת המידע עקב איוש חלקי של עמדת ה-SOC ששירתה את אותה הרשת, בפרט בנוגע להתרעות ברמת חומרה גבוהה.

☆

איסוף וניתוח של מידע על פעולות הנעשות במערכות ממוחשבות ועל אירועים שמתחוללים בהן, מאפשרים לחשוף ניסיונות לביצוע פעולות לא מורשות במערכות, לזהות מתקפות עליהן ולסייע בתהליך ההתאוששות מאירועי פגיעה באבטחת המידע. לצורך זה נדרש, על פי הנחיות הגופים המאסדרים, לאסוף מידע באופן שיטתי באמצעות מערך ניטור: לאסוף קובצי LOG ממאות רכיביה של הרשת באמצעות מערכת SIEM ולנתחם על פי כללים שנקבעו לכך, כדי להתריע לפני הגורמים המופקדים על ה-SOC על אירועים חריגים, לבצע חקירה בעניין האירועים החריגים ולפעול בהתאם לממצאיה.

נמצא כי משרד רה"ם לא הפעיל את מערך הניטור ברשת מסויימת שנבחנה, כנדרש: חלק מרכיבי הרשת לא חוברו ל-SIEM, ורכיבים אחרים לא הפיקו קובצי LOG; עלה חשש שמשרד רה"ם לא קבע כללים מספקים במערך הניטור, בנוגע למקרים שעליהם המערכת תתריע; משרד רה"ם לא קבע תקן למשך הטיפול בהתרעות של מערך הניטור על פגיעה לכאורה באבטחת המידע; וכמו כן, עלה חשש לפגיעה באבטחת המידע עקב איוש חלקי של עמדת ה-SOC, בפרט בנוגע להתרעות ברמת חומרה גבוהה. בשל כל אלה הצטמצמה יכולת המשרד לזהות פעולות לא מורשות שנעשו במערכות סמוך לאחר ביצוען, לזהות מתקפות על המערכות ולהתאושש מהן היטב ובמהירות.

לאחר סיום הביקורת מסר משרד רה"ם כי הוא פועל לאיחוד ה-SOC, כדי שישרת את כל רשתות המשרד.

על משרד רה"ם לפעול להשלמת הפעילות לגבי מערך הניטור של הרשת המסויימת שנבחנה: לחבר את כל רכיביה ל-SIEM, לוודא שכל הרכיבים מפיקים קובצי LOG ולקבוע כללים לניתוח המידע שמתקבל. כמו כן, מומלץ שמשרד רה"ם יקבע תקן למשך הטיפול בהתרעות של מערך הניטור ויאייש את עמדת ה-SOC באופן שמבטיח טיפול יעיל בהתרעות.

בתשובת משרד רה"ם ממרץ 2024 צוין כי איחוד ה-SOC האמור בוצע, כי המרכז האחוד מאויש 24 שעות ביממה בכל ימות השבוע, וכי נקבע תקן לגבי משך הטיפול בהתרעות של מערך הניטור. כמו כן החלה עבודת טיוב, בשיתוף ה-SOC-G, להעלאת שיעור מערכות המשרד המנוטרות.

עדכניות הגרסאות של מערכות הפעלה ותוכנה

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

מרשם הפגיעויות הלאומי האמריקאי (NVD - National Vulnerability Database) של המוסד הלאומי לתקינה וטכנולוגיה בארצות הברית (NIST - National Institute of Standards and Technology), מרכז מידע על פגיעויות המתגלות ברכיבי מערכות מידע ומזהה כל פגיעות מדווחת

באמצעות מספר סידורי חד-ערכי (CVE ID[13]). הפגיעויות המתגלות מתועדות ונרשמות. היות שהשפעתן של הפגיעויות על רכיבי מערכות המידע אינה זהה, קובע ה-NVD לכל פגיעות דירוג (CVSS - Common Vulnerability Scoring System) המתאר את דרגת החומרה האיכותנית של הפגיעות בסולם של 1 - 10; דירוג CVSS 7.0 - 8.9 משקף דרגת חומרה גבוהה, ודירוג של 9.0 - 10.0 משקף דרגת חומרה קריטית. ככלל, עם התגלותה של חולשה חדשה פועל היצרן לפתח עדכון לתוכנה ("טלאי") שהתקנתו במערכת אמורה להתמודד עם החולשה שהתגלתה ולאיינה. הימנעות מהתקנת עדכוני האבטחה חושפת את רכיבי מערכות המידע שלא עודכנו לפגיעויות קריטיות, לרבות כאלו שנעשה בהם שימוש מוכח על ידי תוקפי סייבר ברחבי העולם. לדוגמה, במאי 2019 פרסם יצרן של מוצרי אבטחת מידע עדכון אבטחה להתמודדות עם פגיעות קריטית שהתגלתה באחד ממוצריו. כעבור כשנתיים, בספטמבר 2021, מצאה הרשות האוסטרלית הממשלתית לאבטחת מידע כי במקרה שבו לא בוצע אותו עדכון, הפגיעות נוצלה במערכת של ישות אוסטרלית.

לפיכך נקבעו בתקנות הגנת הפרטיות (אבטחת מידע), התשע"ז-2017, ובהנחיות הגופים המאסדרים הוראות בדבר הצורך לשמור על עדכניות מערכות הארגון והוראות האוסרות להשתמש בגרסאות מערכת שהגיעו לסוף תקופת התמיכה שלהם. עוד נקבע בהנחיות כי יש לפעול להחלפת רכיבים קיימים המצויים לקראת סוף תמיכת היצרן בהם.

ברשת מסויימת שנבחנה במשרד רה"ם אותרו שרתים ומספר רכיבי תקשורת שמצויים לאחר מועד סוף התמיכה, ולכן הם חשופים לפגיעויות שהתגלו בהם. שימוש משרד רה"ם ברכיבים אלה הוא בניגוד להנחיות הגופים המאסדרים וכפי הנראה, לא ניתן מענה אבטחתי מתאים לרכיבים אלה, כך שהשימוש בהם נעשה גם בניגוד לתקנות הגנת הפרטיות (אבטחת מידע), התשע"ז-2017.

ברשתות שנבחנו פועלים שרתים ומספר רכיבי תקשורת שבהם מותקנת מערכת הפעלה מגרסה מסוימת, שמועד תום מחזור החיים שלה עבר זה מכבר (בין 17% ל-27% מהשרתים ברשתות שנבחנו). שרתים אלה חשופים לפגיעויות שיתגלו במערכת ההפעלה שלהם, והשימוש בהם הוא בניגוד להנחיות הגופים המאסדרים.

משרד רה"ם לא הקפיד על התקנת העדכונים הנדרשים במערכות הפעלה של שרתים במועד, ועקב כך נותרו מערכות המידע של המשרד חשופות לפגיעויות שונות, לרבות פגיעויות שנעשה בהן שימוש תדיר על ידי תוקפי סייבר ברחבי העולם. בחלק ניכר מהשרתים יש איחור של שישה חודשים לפחות בהתקנת עדכוני אבטחה קריטיים, נכון למועד הבדיקה (יולי 2023).

☆

לצורך הגנת השרתים במשרד רה"ם יש להתקין במערכות ההפעלה שלהם את עדכוני האבטחה שמפרסם היצרן מעת לעת. בהתאם לכך, נקבעו בהנחיות הגופים המאסדרים כללים מפורטים בדבר תהליך התקנת עדכוני האבטחה ומועד התקנתם, כדי להבטיח הגנה על רכיבי מערכות המידע מפני פגיעויות קריטיות, לרבות פגיעויות שנעשה בהם שימוש מוכח על ידי תוקפי סייבר ברחבי העולם. משרד רה"ם מחזיק במאות שרתים שבהם הותקנה מערכת הפעלה של Windows, ונדרש לבצע בהם כעשרה עדכונים קריטיים בממוצע בשנה וכן עדכונים נוספים, על פי פרסומי היצרן. ממצאי הביקורת העלו כי משרד רה"ם לא הקפיד על התקנת העדכונים הנדרשים במערכות ההפעלה במועד, וכי בחלק ניכר מהשרתים יש איחור ניכר בהתקנת עדכוני אבטחה קריטיים, נכון למועד הבדיקה (יולי 2023). כן הועלה כי משרד רה"ם לא התקין עדכוני אבטחה בגרסאות התוכנה של שרתים מסוג מסוים. עקב כך נותרו מערכות המידע של המשרד חשופות לפגיעויות שונות, לרבות פגיעויות שנעשה בהן שימוש תדיר על ידי תוקפי סייבר ברחבי

[13] Common Vulnerabilities and Exposures.

העולם. הסיכון הטמון בחשיפה זו הומחש כאמור במקרה שאירע באוסטרליה בשנת 2021, עת נפגעה מערכת של ישות אוסטרלית, מכיוון שלא הותקן בה עדכון אבטחה מסוים.

על משרד רה"ם להקפיד על התקנת עדכוני אבטחה בהתאם להוראות היצרן, ולוודא עמידה בהנחיות הגופים המאסדרים.

משרד רה"ם ציין בתשובתו כי החל לפעול לתיקון הליקויים, ובכלל זה קבע את הגורם האחראי לביצוע ההמלצה האמורה ולוח זמנים לביצועה.

הגנה על המידע ברשתות המסווגות ביטחונית

רמת ההגנה על המידע ברשתות מסווגות במשרד רה"ם נמוכה מרמת ההגנה הנדרשת, ואינה עומדת בדרישות הגורם המאסדר. זאת, אף שמשרד רה"ם הוא יעד המצוי באיום תמידי ברמת חומרה קריטית. הותרת רשתות מסווגות של המשרד ברמת הגנה נמוכה כאמור עלולה להביא לפגיעה מהותית במדינת ישראל בהיבטים מדיניים, ביטחוניים, כלכליים ותדמיתיים.

☆

משרד רה"ם הוא יעד המצוי באיום תמידי ברמת חומרה קריטית, ורמת הגנה לא מספקת על רשתות מסווגות שבו עלולה להביא לפגיעה מהותית במדינת ישראל בהיבטים מדיניים, ביטחוניים, כלכליים ותדמיתיים.

על משרד רה"ם לבצע בהקדם את הפעולות הדרושות לעמידה ברמת ההגנה המירבית, כמתחייב מרמת איום הייחוס שהוגדרה לו.

משרד רה"ם ציין בתשובתו כי החל לפעול לתיקון הליקויים, ובכלל זה קבע את הגורם האחראי לביצוע ההמלצה האמורה ולוח זמנים לביצועה.

<u>ההגנה על המידע ברשת מסוימת שנבחנה</u>

בנובמבר 2021 בדקו חטיבת הגנת המידע ואגף טד"ם את מידת העמידה של רשת מסוימת במשרד רה"ם בהנחיות הגופים המאסדרים. בינואר 2022 מסרה חטיבת הגנת המידע את ממצאיה לגבי הליקויים שהעלתה בבדיקה זו וכן בסקר סיכונים שביצעה, המחייבים תיקון.

נמצא כי במשך יותר משנה וחצי, מהמועד שבו מסרה חטיבת הגנת המידע את ממצאי הבדיקה שערכה עם אגף טד"ם לגבי אבטחת המידע המצוי ברשת המסוימת, ועד למועד סיום הביקורת, לא תוקנו ליקויים מהותיים שעלו בבדיקה שעשתה חטיבת הגנת המידע. עקב כך הרשת הזו עודנה חשופה לסיכונים הנובעים מאותם ליקויים.

על משרד רה"ם לפעול לתיקון הליקויים שנמצאו הנוגעים לאבטחת המידע ברשת הזו ולוודא את השלמות, הבטיחות והסודיות של המידע ברשת.

משרד רה"ם ציין בתשובתו כי החל לפעול לתיקון הליקויים, ובכלל זה קבע את הגורם האחראי לביצוע ההמלצה האמורה ולוח זמנים לביצועה.

<u>ביצוע מבדק חדירה באותה רשת מסוימת</u>

מבדק חדירה (Penetration Test - PT) הוא הליך שבו מתבצעת תקיפה מבוקרת ומתוכננת של מערכות ממוחשבות בארגון, כדי לאתר חולשות הקיימות בהן. בהנחיות הגופים המאסדרים נקבע כי יש לבצע מבדק חדירה לרכיביה של כל מערכת מסווגת אחת לתקופה שנקבעה בהנחיות.

נמצא כי במשך שש שנים לפחות, בשנים 2018 - 2023, משרד רה"ם לא עשה מבדק חדירה לרשת המסוימת הזו.

על משרד רה"ם לבצע מבדקי חדירה לרשת האמורה בהתאם לנדרש ולפעול על פי ממצאיהם.

משרד רה"ם ציין בתשובתו כי החל לפעול לתיקון הליקויים, ובכלל זה קבע את הגורם האחראי לביצוע ההמלצה האמורה ולוח זמנים לביצועה.

התקנת אמצעי הגנה ברשת המסוימת

על פי הנחיות הגופים המאסדרים, יש להתקין ברשת אמצעי הגנה, כדי להקשות על תוקף לבצע פעולות ברשת וכן לזהות פעולות תקיפה (או פעולות הכנה לתקיפה) המתבצעות בה.

הבדיקה העלתה כי משרד רה"ם לא התקין ברשת המסוימת אמצעי הגנה שהתקין ברשת אחרת.

מומלץ כי משרד רה"ם יפעל להתקנת אמצעי ההגנה שבידי משרד רה"ם גם ברשת המסוימת.

משרד רה"ם ציין בתשובתו כי החל לפעול לתיקון הליקויים, ובכלל זה קבע את הגורם האחראי לביצוע ההמלצה האמורה ולוח זמנים לביצועה.

מניעת דליפת מידע

דליפת מידע עלולה להתבצע במגוון מתווים, לרבות בדרך של חיבור התקני קצה (דוגמת הֶחסֶן נייד) למערכות הממוחשבות והעתקת החומר האצור בהן וכן בדרך של הדפסת חומר מתוך המערכות ושימוש לא מורשה בעותק קשיח שהודפס.

על פי הנחיות הגופים המאסדרים, תורת ההגנה בסייבר ונוהל מדיניות הניטור של משרד רה"ם, יש לוודא כי הוטמעו במערכות הארגון מנגנונים טכנולוגיים ואחרים, לשם התמודדות עם דליפת מידע מיעדי ההגנה שלו, לרבות מנגנונים המאפשרים לחסום הוצאה של קבצים מחוץ לרשת הארגונית. כמו כן, יש לנטר את הדפסת המסמכים מרשתות ובמידת הצורך להגביל את כמות החומר.

DLP (Data Loss Prevention Software) היא מערכת המיועדת למנוע דליפת מידע מהארגון. בין היתר יכולה המערכת להתריע על חיבור התקני קצה לא מורשים למערכות הארגון וכן לנטר ולמנוע הדפסה בהיקף גדול של מידע ומסמכים מהרשתות המסווגות.

נמצא כי משרד רה"ם לא נקט בכל הפעולות המתחייבות מהוראות הגופים המאסדרים בנוגע למניעת דליפת מידע.

על משרד רה"ם לנקוט בכל הפעולות הדרושות לשם התמודדות עם דליפת מידע מיעדי ההגנה שלו.

משרד רה"ם ציין בתשובתו כי החל לפעול לתיקון הליקויים, ובכלל זה קבע את הגורם האחראי לביצוע ההמלצה האמורה ולוח זמנים לביצועה.

סיכום

משרד רה"ם עוסק בתכנון ויישום של מדיניות הממשלה וראש הממשלה בנושאים המרכזיים שעל סדר יומה של הממשלה. במשרד רה"ם מותקנות מערכות מידע שמשמשות מערכים רגישים, לרבות לשכת ראש הממשלה, מזכירות הממשלה, המזכירות הצבאית של ראש הממשלה ומערך ההסברה הלאומי. במסגרת המשרד פועל גם גוף מטה לראש הממשלה

ולממשלה בענייני החוץ והביטחון של ישראל. הביקורת העלתה ליקויים בהיבטים שונים של ניהול-העל בנוגע להגנת המידע במשרד רה"ם, לרבות בנוגע לסדרי עבודתן של ועדות היגוי להגנת הסייבר שפעלו במשרד ולניהול תקציבי טכנולוגיות המידע של המשרד.

במערכות הממוחשבות במשרד רה"ם אצור מידע רב, לרבות מידע רגיש ומידע ברמת סודיות גבוהה ביותר. ההגנה הנדרשת על המידע המסווג היא ברמה הגבוהה ביותר. הועלה כי רמת ההגנה על רשתות שבמשרד רה"ם נמוכה מהנדרש. רמת הגנה שאינה מספקת עלולה להביא לפגיעה מהותית במדינת ישראל בהיבטים מדיניים, ביטחוניים, כלכליים ותדמיתיים.

נמצאו ליקויים בניהול הרשאות הגישה של משרד רה"ם למערכות הממוחשבות שלו; משרד רה"ם לא הפעיל כנדרש את מערך הניטור באחת הרשתות ועקב כך הצטמצמה יכולתו לזהות מתקפות על המערכות ולהתאושש מהן היטב ובמהירות; המשרד לא הקפיד על התקנת עדכונים נדרשים של מערכות שונות, ובכלל זה מערכות ההפעלה בשרתיו, ועקב כך נותרו מערכות מידע חשופות לפגיעויות שונות, לרבות פגיעויות שנעשה בהן שימוש תדיר על ידי תוקפי סייבר ברחבי העולם.

משרד מבקר המדינה מציין לחיוב את תגובת משרד רה"ם על ממצאי הביקורת: משרד רה"ם השיב כי המלצות משרד מבקר המדינה רוכזו בידי אגף טד"ם; נקבעו הגורמים האחראים ליישומן או להעמקת הבדיקה של הממצאים העומדים בבסיס ההמלצות; וכן נקבע לוח זמנים להשלמת יישום ההמלצות והבדיקות, על פי רמת הדחיפות שלהן. משרד רה"ם ציין כי הגורמים הרלוונטיים במשרד רתומים לנושא ומחויבים לקידומו. אגף ביטחון וחירום מסר כי בשנת 2024 יחל בפעולות לפיקוח ובקרה על רשתות מידע שאינו מסווג, בהיבטי רציפות תפקודית ודלף מידע.

האחריות לתיקון הליקויים שעלו בביקורת בנוגע לניהול טכנולוגיות המידע של משרד רה"ם ואבטחת המידע הממוחשב שבו מוטלת על מנכ"ל משרד רה"ם, העומד גם בראש ועדת ההיגוי להגנת הסייבר. על משרד רה"ם לפעול לתיקון הליקויים שעלו בביקורת, כמפורט בדוח זה.

על שב"כ ויחידת יה"ב במערך הדיגיטל הלאומי, האמונים על הנחיית משרד רה"ם בכל הנוגע לאבטחת המידע, לוודא שמשרד רה"ם יפעל כנדרש לתיקון הליקויים שעלו בביקורת.

משרד מבקר המדינה
ונציב תלונות הציבור