דוח מבקר המדינה | תמוז התשפ"ד | יולי 2024

משרד ראש הממשלה

הגנה על המידע הממוחשב במשרד ראש הממשלה

הגנה על המידע הממוחשב במשרד ראש הממשלה

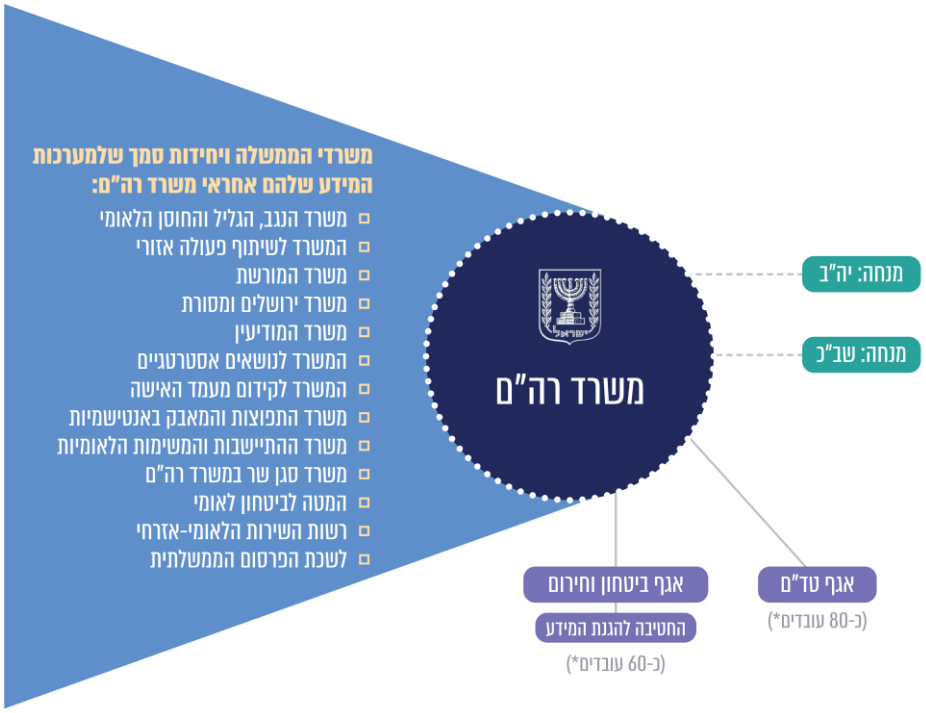
רקע

משרד ראש הממשלה אמון על מימוש התפיסה המדינית, הכלכלית, החברתית והניהולית של ראש הממשלה והממשלה בנושאים המרכזיים שעל סדר יומה. המשרד מספק שירותי ניהול מערכות מידע והגנה על המידע שבהן ל-13 מיחידות הסמך שלו ולמשרדי ממשלה נוספים. המטה לביטחון לאומי (המל"ל) הוא יחידת סמך של משרד רה"ם, המשמש גוף מטה לראש הממשלה ולממשלה בענייני החוץ והביטחון של ישראל. 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 זה, לרבות דליפת המידע, שיבושו או פגיעה בזמינותו, עלולה לגרום לנזק ממושך חמור מאוד לביטחון מדינת ישראל או למערכותיה החיוניות, על אחת כמה וכמה בעיתות מלחמה, כאשר כמות תקיפות הסייבר עולה. ההגנה הנדרשת על המידע המסווג שבידי משרד רה"ם היא ברמה הגבוהה ביותר.

משרד רה"ם מונחה בכל הנוגע להגנה על המידע על-ידי גורמים מאסדרים בהתאם לתורת ההגנה שקבע המאסדר הרלוונטי ביחס לכל אחת מהרשתות. גורמי המקצוע במשרד רה"ם האמונים על הגנת המידע שבו הם אגף בכיר טכנולוגיות דיגיטליות ומידע (אגף טד"ם), שאחראי לתחום טכנולוגיות המידע ולהגנת המידע הבלתי מסווג והחטיבה להגנת המידע באגף ביטחון וחירום, שאחראית להגנת המידע המסווג.

המבנה הארגוני הכללי של תחומי טכנולוגיות דיגיטליות והגנת המידע במשרד רה"ם, המשרדים ויחידות הסמך של מערכות 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 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.

נתוני מפתח

רמת הגנה נמוכה
הרשתות המסווגות של משרד רה"ם הן ברמת הגנה נמוכה ביחס לרמה הנדרשת

כ-49 מיליון
ניסיונות להתקפה על שירות החיבור מרחוק במשרד רה"ם בחודשים ינואר-מאי 2023 בלבד

עשרות
משתמשים פעילים ברשת מסווגת של משרד רה"ם נכנסו לרשת, שלא על פי ההגדרות הלוגיות שקבע משרד רה"ם

פעולות הביקורת

בחודשים מרץ עד אוגוסט 2023 ביצע משרד מבקר המדינה ביקורת בנושא ההגנה על המידע הממוחשב המצוי בעיקר ברשתות המחשוב 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 גרסאות 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.

תמונת המצב העולה מן הביקורת

ניהול-העל של הגנת המידע

- **ניהול ועדות ההיגוי ותדירות הדיונים** - ועדת ההיגוי להגנת הסייבר נדרשת לפעול לשיפור רמת הגנת הסייבר של המשרד הממשלתי ולביצוע בקרה ניהולית על יישום הגנת הסייבר במשרד. הביקורת העלתה שורה של ליקויים בקשר לתפקודן של ועדות ההיגוי במשרד רה"ם: ועדת ההיגוי להגנה על מידע בלמ"ס לא התכנסה בתדירות הנדרשת בשנים 2018 - 2022; תפקיד יו"ר הוועדה לא אויש בשנת 2020; בשנים 2020 – 2022 לא עמד בראש הוועדה מנכ"ל משרד רה"ם, כנדרש בהחלטת הממשלה. ועדות ההיגוי למידע בלמ"ס ולמידע מסווג לא מילאו את תפקידן כנדרש בכל הנוגע להליך הבחינה והאישור של תוכניות העבודה השנתיות בשנים 2019 - 2022.

- **גיבוש מדיניות הגנת הסייבר ועריכת סקרי סיכונים** - המדיניות של משרד רה"ם לגבי הגנה על המידע הבלמ"ס אושרה בנובמבר 2018 ולא עודכנה ותוקפה במשך ארבע שנים וחצי, כנדרש בהנחיות הגופים המאסדרים, אף על פי שבשנים האלה חלו שינויים ארגוניים ניכרים - הוקמה חטיבת הגנת המידע באגף ביטחון וחירום, ומשרד רה"ם קיבל את האחריות לניהול מערכות המידע ואבטחת המידע בעוד משרדי ממשלה. מדיניות הגנת המידע לא כללה את כל תחומי הפעולה הנדרשים ואף לא אושרה על ידי מנכ"ל המשרד, כנדרש בהנחיות הגופים המאסדרים. משרד רה"ם ביצע סקר סיכונים שלא על פי הנדרש בהנחיות.

- **בקרה על יישום הגנת הסייבר במשרד** - ועדת ההיגוי לא עסקה בממצאי המדד שגיבש יה"ב (הבוחן בקרה ניהולית של המשרד הממשלתי בתחום הגנת הסייבר), כנדרש, אף על פי שנתוני המדד שיקפו ירידה בציון הכולל של משרד רה"ם (מ-86% ל-68%), וכן שיקפו ירידה חדה בשלושה מרובדי הבקרה: אחריות הנהלה ותאימות ושני רבדי הגנה נוספים.

- **תקציב משרד רה"ם לטכנולוגיות מידע** - ביצוע תקציב משרד רה"ם לתחום טכנולוגיות המידע בתקנת "הוצאות מחשוב" נע בשנים 2018 - 2023 מכ-49 מיליון ש"ח ועד כ-68 מיליון ש"ח בשנה. נמצא כי מנתוני מערכת מרכב"ה אי אפשר לדעת מה הוא מכלול התקציב של משרד רה"ם לתחום טכנולוגיות המידע וכמה ממנו מיועד להגנת הסייבר, ולפיכך לא ניתן לדעת אם משרד רה"ם מקצה 8% מתקציב זה להגנת הסייבר, כנדרש בהחלטת הממשלה. עוד נמצא כי רישום הוצאות המשרד בתחום זה ב-11 תקנות תקציביות שונות מקשה את איגום הנתונים של המשרד ואף פוגע ביכולת ועדת ההיגוי לוודא שהמשרד הקצה די משאבים לצורך הגנת הסייבר. בשנים 2018 - 2023 ועדת ההיגוי למידע בלמ"ס לא וידאה שהוקצו די משאבים להגנת הסייבר, כנדרש בהחלטת הממשלה.

- **איוש כמה תפקידי ליבה על ידי מנהל אגף טד"ם -** משנת 2021, ולפחות עד אמצע שנת 2023 מנהל אגף טד"ם מילא למעשה שלושה מחמישה תפקידים מרכזיים בתחום טכנולוגיות המידע במשרד רה"ם, ונוסף על כך, בשנים 2018, 2019, 2022 הוא שימש גם ממלא מקום יו"ר ועדת ההיגוי להגנה על מידע בלמ"ס. מצב זה עלול לפגוע בביצוע המשימות שבאחריותו. יתר על כן, ניהול אגף טד"ם, תוך ביצוע משימות של אחראי אבטחת מידע, עלול לפגוע ביכולת הפיקוח והבקרה על משימות בתחום אבטחת המידע. נציבות שירות המדינה אישרה למשרד רה"ם לוותר על אחת המשרות - מנהל הטכנולוגיות של המשרד - בלי לנמק זאת.

הזדהות משתמשים וניהול הרשאות

- **אמצעי הזדהות לצורך כניסה לרשת** - הכניסה לרשתות של משרד רה"ם אינה עומדת בכללים הנדרשים 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.

- **ניהול הרשאות גישה לרשתות** - משרד רה"ם אינו מנהל כראוי את הרשאות הגישה לרשתות הממוחשבות שלו. 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.

- **ניהול קבוצות הרשאה ברשת מסויימת שנבחנה** - 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 ועניינה של כל קבוצת הרשאה.

- **קביעת מועדי תפוגה לחשבונות** - 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.

- **ביצוע בקרות במערך ניהול המשתמשים** - 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.

- **מתן גישה לרשתות לחשבונות שאינם פעילים** - 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.

- **חשד לשימוש לא מורשה בחשבונות לאחר סיום העסקה** - 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.

ניטור מערכות ברשת מסויימת שנבחנה

- 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.

עדכניות הגרסאות של מערכות ההפעלה והתוכנה

- **מערכות המצויות לאחר סוף מחזור חייהן**

  - ברשת מסויימת שנבחנה במשרד רה"ם אותרו שרתים ומספר רכיבי תקשורת שמצויים לאחר מועד סוף התמיכה, ולכן הם חשופים לפגיעויות שהתגלו בהן. 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% - 27% מהשרתים ברשתות שנבחנו). שרתים אלה חשופים לפגיעויות שיתגלו במערכת ההפעלה שלהם, והשימוש בהם הוא בניגוד להנחיות הגופים המאסדרים.

- **התקנת עדכוני אבטחה -** 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).

הגנה על המידע ברשתות מסווגות ביטחונית

- **רמת ההגנה על המידע ברשתות מסווגות במשרד רה"ם** - רמת ההגנה על המידע ברשתות האלה 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.

- **ההגנה על המידע ברשת מסווגת מסוימת שנבחנה** - במשך יותר משנה וחצי, מהמועד שבו מסרה חטיבת הגנת המידע את ממצאי בדיקתה לגבי אבטחת המידע

המצוי ברשת המסווגת שנבחנה ועד למועד סיום הביקורת, לא תוקנו ליקויים מהותיים שעלו בבדיקה. עקב כך רשת זו עודנה חשופה לסיכונים הנובעים מאותם ליקויים.

- **בדיקת חוסן והתקנת אמצעי הגנה באותה רשת מסווגת מסוימת** - משרד רה"ם לא עשה מבדק חדירה לרשת המסווגת הזו, כנדרש, במשך שש שנים לפחות (בשנים 2018 - 2023).
- **מניעת דלף מידע** - משרד רה"ם לא התקין ברשת המסווגת המסוימת אמצעי הגנה שהתקין ברשת מסווגת אחרת.

משרד מבקר המדינה מציין לחיוב את תגובת משרד רה"ם על ממצאי הביקורת: משרד רה"ם השיב כי המלצות משרד מבקר המדינה אוגדו בידי אגף טד"ם, נקבעו גורמים אחראים ליישומן או להעמקת הבדיקה של הממצאים שבבסיס ההמלצות, וכן נקבע לוח זמנים להשלמת יישום ההמלצות והבדיקות בהתאם לרמת הדחיפות שיוחסה להן. המשרד ציין כי הגורמים הרלוונטיים במשרד רתומים לנושא ומחויבים לקידומו.

עיקרי המלצות הביקורת

- על משרד רה"ם לבצע את הפעולות הדרושות לעמידה ברמת ההגנה הנדרשת ברשתות במשרד, בהתאם להנחיות הגופים המאסדרים.
- על משרד רה"ם למנות ועדות היגוי להגנת הסייבר בראשות מנכ"ל המשרד, ולכנסן בתדירות הנדרשת. מומלץ כי ועדות ההיגוי במשרד רה"ם ידונו בתוכניות העבודה לאבטחת המידע במשרד מדי שנה בשנה, יקבלו החלטות אם לאשרן ויתעדו את ההחלטות בסיכומי הדיונים. עוד מומלץ כי מדיניות מעודכנת לאבטחת המידע הבלמ"ס תובא לבחינה ואישור של ועדת ההיגוי, כנדרש.
- על משרד רה"ם לרכז נתונים על כלל התקציבים שעומדים לרשות המשרד לצורך ניהול טכנולוגיות המידע בכל הגופים שלהם הוא אחראי, וכן לנהל רישום תקציבי נפרד של תקציבים המופנים להגנת הסייבר. מומלץ שהמשרד יגבש את דרישותיו לתקציב ניהול טכנולוגיות המידע בהתאם לצרכיו מדי שנה בשנה, כדי לצמצם את הצורך בתוספות תקציב ניכרות במהלך השנה.
- על משרד רה"ם ליישם מנגנון המספק את ההגנה הנדרשת בעת הכניסה לרשתות המשרד, להתאים את הדרישות הלוגיות בעת הכניסה לרשתות לנדרש וליישמן. על משרד רה"ם לוודא כי בכל החשבונות הפעילים ברשתות המשרד תוחלף הסיסמה בתדירות הנדרשת.
- מומלץ כי משרד רה"ם יעדכן את קבוצות המשתמשים שיצר ברשת מסויימת שנבחנה וימחק קבוצות שאין בהן צורך; יקבע תאריך תפוגה לכל חשבונות העובדים הזמניים במשרד; יגבש מדיניות לגבי תאריכי תפוגה של חשבונות של עובדים קבועים; יוודא שבעלי

חשבונות שתוקפם פג לא יהיו מורשים לגשת לרשת; ויבסס מערך בקרה אפקטיבי להבטחת ניהול תקין של הרשאות הגישה ברשתות.

- על משרד רה"ם לבטל הרשאות של עובדים עם סיום העסקתם במשרד; לבטל הרשאות בחשבונות שלא נעשה בהם שימוש ולוודא שהחשבונות האלה יועברו למצב "לא פעיל" (disable). כן מומלץ שמשרד רה"ם ינפיק "דוח חריגים" שיאפשר לאתר מצבים המשקפים חריגה מניהול תקין של מערך הגישה לרשתות המשרד.
- על משרד רה"ם, בשיתוף השב"כ, לבצע בדיקות עומק לבחינת החשד לשימוש בחשבונותיהם של עובדים לאחר סיום העסקתם, לבצע בדיקות רוחביות בכל רשתות המשרד ולפעול בהתאם לממצאיהן.
- על משרד רה"ם לפעול להשלמת הפעילות לגבי מערך הניטור ברשת מסויימת 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.
- על משרד רה"ם לוודא כי לא נעשה שימוש במוצרים לאחר תום מחזור החיים שלהם, ולהקפיד על התקנת עדכוני אבטחה בהתאם להוראות היצרן.
- על משרד רה"ם לפעול לתיקון הליקויים הנוגעים לאבטחת המידע ברשת מסווגת מסוימת שנבחנה, לוודא את הגנת המידע ברשת, וכן לבצע מבדקי חדירה לרשת הזו בהתאם לנדרש ולפעול בהתאם לממצאיהם.
- על משרד רה"ם לנקוט בכל הפעולות הדרושות לשם התמודדות עם דליפת מידע מיעדי ההגנה שלו.
- על הגופים המאסדרים האמונים על הנחיית משרד רה"ם בכל הנוגע לאבטחת המידע ברשתות המשרד, לוודא שמשרד רה"ם יפעל כנדרש לתיקון הליקויים שעלו בביקורת.

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.