דוח מבקר המדינה

הגנת הסייבר בעבודה מרחוק בעיתות שגרה וחירום

▪ סיוון התשפ"ו ▪ מאי 2026

הגנת הסייבר בעבודה מרחוק בעיתות שגרה וחירום

תקציר

רקע

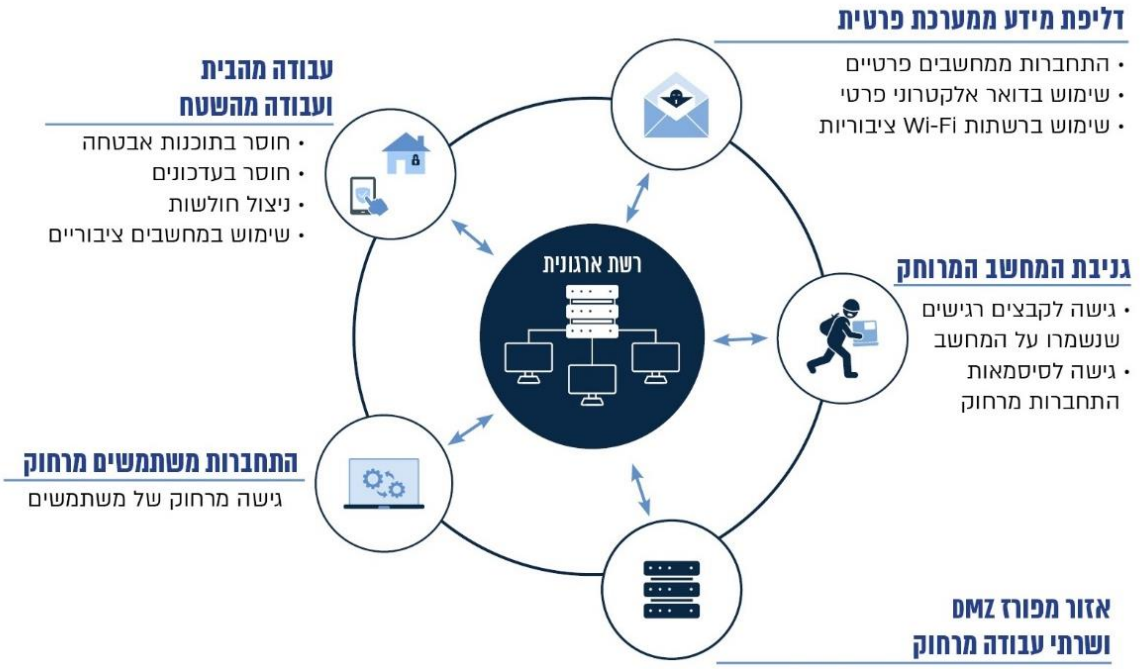
"עבודה מרחוק" מתבצעת בכמה מתווים: עבודה המתבצעת בדרך כלל מבית המגורים של העובד או ממקום אחר תוך שימוש בטכנולוגיית מידע ותקשורת ולא מהאתר של המעסיק (מקום העבודה); התחברות של עובדי שטח למערכות הארגון. בעידן הטכנולוגי עבודה מרחוק הפכה לחלק בלתי נפרד מתפקוד המשק. עבודה מרחוק מאפשרת גמישות תפעולית (כגון לעובדים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

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

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

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

עבודה מרחוק - מתארי תקיפה ואיומים אפשריים



הוכן בידי משרד מבקר המדינה.

נתוני מפתח

מאות אלפי

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

עשרה חודשים

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

0

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

אלפי

מחשבים ניידים וטאבלטים של המשטרה משמשים לעבודה מרחוק

במאות

כבאיות יש ללוחמי האש גישה לעבודה מרחוק מהשטח

פעולות הביקורת

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

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

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

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

ועדת המשנה של הוועדה לענייני ביקורת המדינה של הכנסת החליטה שלא להניח על שולחן הכנסת ולא לפרסם חלקים מפרק זה לשם שמירה על ביטחון המדינה, בהתאם לסעיף 17(א) לחוק מבקר המדינה, התשי"ח-1958 (נוסח משולב).

תמונת המצב העולה מן הביקורת

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

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

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

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

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

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

הגנת הסייבר בעבודה מרחוק בכב"ה

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

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

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

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

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

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

הגנת הסייבר בעבודה מרחוק במשטרה

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

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

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

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

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

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

הגנת הסייבר בעבודה מרחוק בהנהלת בתי המשפט

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

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

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

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

עיקרי המלצות הביקורת

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

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

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

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

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

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

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

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

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

הגנת הסייבר בעבודה מרחוק בכב"ה

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

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

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

הגנת הסייבר בעבודה מרחוק במשטרה

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

הגנת הסייבר בעבודה מרחוק בהנהלת בתי המשפט

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

סיכום

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

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

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

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

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

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