דוח מבקר המדינה

הגנת הסייבר בעבודה מרחוק בעיתות שגרה וחירום

▪ סיוון התשפ"ו ▪ מאי 2026 ▪

הגנת הסייבר בעבודה מרחוק בעיתות שגרה וחירום

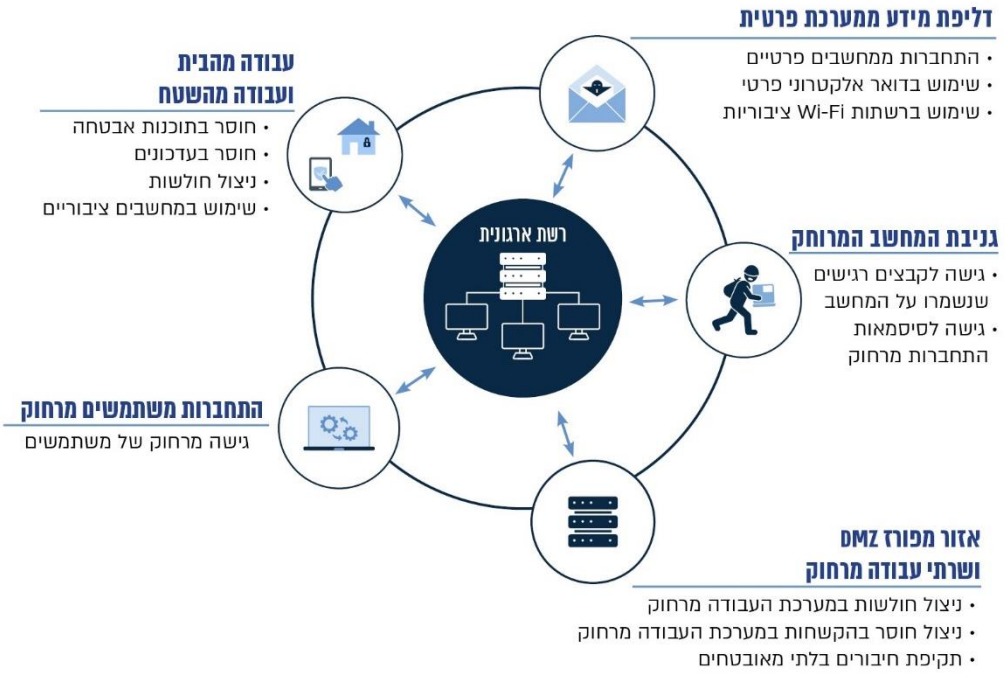
מבוא

"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[1], ומרבית[2] הגופים בשירות המדינה עובדים כך. מדובר במאות אלפי[3] עובדים במגזר הציבורי ובהם משרדי הממשלה, מערכת החינוך הממשלתית, מערכת הבריאות הממשלתית, גופי הביטחון, חברות ממשלתיות, שלטון מקומי ותאגידים.

תרשים 1: **עבודה מרחוק - מתארי תקיפה ואיומים אפשריים**



הוכן בידי משרד מבקר המדינה.

---

1 הנחיות נציב שירות המדינה מס' 3.6 בנושא "גמישות תעסוקתית - עבודה מרחוק וביצוע שעות נוספות מרחוק" (עדכון אחרון מיום 21.9.22).

2 עם זאת, הנחיית הנציב קובעת כי התאמות וחריגות להנחיה יינתנו במידת הצורך על ידי הממונים במערכות הרלוונטיות. כך למשל, במשטרת ישראל וכב"ה השוטרים ולוחמי האש המבצעיים עובדים מרחוק מהשטח, בעוד שלעובדים המינהליים עובדים מרחוק מהבית יום בשבוע.

3 https://www.gov.il/BlobFolder/reports/salary-superior-report-public-body-2021-2022-main/he/salary-supervisor-reports_salary-superior-report-public-body-2021-2022-full-version.pdf

לארגון המאפשר לעובדיו לעבוד מרחוק נשקפים איומי סייבר מועצמים, עקב הגדלת משטח התקיפה ופתיחת האפשרות ברשת התקשורת של החברה להתחבר למערכותיה מרחוק.

בשנים האחרונות התרחשו אירועי סייבר בארגונים באמצעות ניצול חולשות אבטחה במערכות העבודה מרחוק, למשל:

- **Fox Kitten:** בשנת 2021 נחשפה פעילות של קבוצת תקיפה איראנית אשר מכונה בשם זה[4]: במתקפת סייבר אשר נמשכה כשנתיים הצליחו האיראנים לחדור לרשתות מחשוב של מספר רב של חברות בישראל, בין השאר באמצעות ניצול של חולשות בשרתים המשמשים לעבודה מרחוק; בשנת 2019 נחשף קמפיין נוסף[5] איראני שבמסגרתו הותקפו במהלך שלוש שנים עשרות ארגונים בישראל ובעולם בתחומי המחשוב, התקשורת, האנרגיה, התעופה, הממשל והביטחון, ונוצלו לרעה חולשות בשירותים המשמשים לעבודה מרחוק.

- **פריצה לבית החולים הלל יפה[6]:** באוקטובר 2021 ניצל פורץ חולשה בתוכנת גישה מרחוק שהותקנה בבית החולים לצורך עבודה מרחוק, החדיר כופרה[7] למחשבי הארגון וגרם לפגיעה בפעילות בית החולים[8]. הפגיעה נמשכה יותר מחודש, והנזק בגינה נאמד בכ-36 מיליון ש"ח[9].

- **Change Healthcare Breach[10]:** בפברואר 2024, בפריצה המוגדרת כפריצה הנרחבת ביותר לארגוני בריאות בארה"ב, תוקפים ניצלו מזהי גישה גנובים של עובד שאפשרו עבודה מרחוק, התקינו כופרה במחשבי הארגון, גנבו מידע, הצפינו מחשבים וגרמו לשיבוש משמעותי בפעילות.

לנוכח האמור לעיל ניכרת חשיבות ההגנה על פעילות העבודה מרחוק בארגונים, ומתחדד הצורך בבחינה מעמיקה ויסודית של היבטי האבטחה בסביבת עבודה זו. במלחמת חרבות ברזל הוצבו אתגרי סייבר נוספים, מאחר שעלה חשש שתוקפים ינסו לנצל את המצב הביטחוני, שבגינו עובדים רבים נאלצו לעבוד מרחוק בכך שיגבירו את הפעילות העוינת במרחב הקיברנטי.

<u>פעולות הביקורת</u>

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

---

4 סקירה של INSS המכון למחקרי ביטחון לאומי - https://www.inss.org.il/he/wp-content/uploads/sites/2/2022/01/%D7%A4%D7%A8%D7%A1%D7%95%D7%9D-%D7%9E%D7%99%D7%95%D7%97%D7%93-020122.pdf

5 סקירה של חברת ClearSky אודות קמפיין ריגול איראני - www.clearskysec.com/fox-kitten

6 מאמר מכלכליסט אודות תקיפת הסייבר על הלל יפה - www.calcalist.co.il/calcalistech/article/h1pxfrrsk

7 נוזקה (תוכנה זדונית) שמטרתה למנוע מבעלי המידע או מפעילי המערכת גישה לנתונים, לקבצים או למערכות המידע הארגוניות, לרוב באמצעות הצפנה של המידע או נעילת המערכת. לאחר חסימת הגישה, התוקפים דורשים תשלום כופר בתמורה לשחזור הגישה או למסירת מפתח הפענוח, ולעיתים מלווים זאת באיום נוסף, כגון לפרסום מידע רגיש שנגנב.

8 יצוין כי בגין אירוע זה מסרה הרשות להגנת הפרטיות שהיא ניהלה הליך פיקוח, ובסופו נקבע כי בית החולים הפר את הוראות סעיף 17 לחוק הגנת הפרטיות ואת תקנות 5(ג), 5(ד), 8(א), 9(א),9(ב) ו-14(ג) לתקנות הגנת הפרטיות (אבטחת מידע).

9 מאמר מגלובס אודות תקיפות סייבר על מערכת הבריאות- www.globes.co.il/news/article.aspx?did=1001438399

10 מאמר מאתר CRN (ארה"ב) אודות תקיפת הסייבר על חברת שירותי הבריאות UnitedHealth - www.crn.com/news/security/2024/unitedhealth-compromised-citrix-credentials-behind-change-healthcare-hack

מרחוק, אבטחת המשאבים הארגוניים בגישה מרחוק, מדיניות ונהלים לגבי עבודה מרחוק ועבודה בשעת חירום. הביקורת נעשתה ברשות הארצית לכבאות והצלה (להלן - כב"ה), במשטרת ישראל, בהנהלת בתי המשפט, במשרד הכלכלה והתעשייה - במערך הדיגיטל הלאומי (להלן - מערך הדיגיטל) לרבות ביחידה להגנת הסייבר בממשלה (להלן - יה"ב), במשרד ראש הממשלה - במערך הסייבר הלאומי (להלן - מס"ל) ובמשרד המשפטים - ברשות להגנת הפרטיות. יצוין כי חלק מהממצאים בדוח מסומנים בסיווג 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 (להלן - היחידה המגזרית) בכל שלבי מבדק החדירה: החל בתכנון המבדק, עבור דרך ביצועו, תהליך הצגת הממצאים ונקיטת פעולות לשיפור התהליכים הקיימים ולטיפול 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).

אסדרה והנחיה בנושא עבודה מרחוק

<u>גופים אסדרתיים מדינתיים בתחום הגנת הסייבר - רקע</u>

המחוקק התייחס לתחום אבטחת המידע והגנת הסייבר בחוק להסדרת הביטחון בגופים ציבוריים, התשנ"ח-1998 (להלן - החוק להסדרת הביטחון), בחוק הגנת הפרטיות, התשמ"א-1981 (להלן - חוק הגנת הפרטיות), ובתקנות הגנת הפרטיות (אבטחת מידע), התשע"ז-2017 (להלן - תקנות אבטחת מידע). כמו כן הממשלה קיבלה כמה החלטות העוסקות בתחום זה[11]. בהתאם להחלטות הממשלה ולהוראות הדין בנושא, הנחיית תחום אבטחת הסייבר מוטלת על כמה גורמים. להלן רשימת הגופים האסדרתיים המדינתיים העיקריים בתחום הסייבר שאליהם מתייחס הדוח:

מערך הסייבר הלאומי: גוף ממשלתי שאמון על הגנת מרחב הסייבר הלאומי ופועל ברמת המדינה לחיזוק תמידי של רמת ההגנה של הגופים במשק והאזרחים, לטיפול בתקיפות סייבר וסילוקן ולהיערכות לשעת חירום[12]. בהתאם לחוק להסדרת הביטחון אחראי מס"ל להנחיית מרבית הגופים שהוגדרו כתשתיות מדינה קריטיות (להלן - גופי תמ"ק) ולבקרה עליהם. בהתאם להחלטת הממשלה 2443 הוא אחראי להנחיה מקצועית של יחידות הסייבר המגזריות ושל יה"ב ומשכך נדרש לבצע בקרה על יישום הנחיותיו ליחידות. בנוסף מפרסם מס"ל הנחיות שונות למשק שהן בגדר המלצה, לדוגמה: תורת ההגנה 2.0 (להלן - תורת ההגנה) - מדריך יישומי להגנת הסייבר בארגון. מס"ל הוקם במשרד רה"ם וכפוף ישירות לראש הממשלה.

---

11 החלטת הממשלה 2443, "קידום אסדרה לאומית והובלה ממשלתית בהגנת הסייבר" (15.2.15), החלטת הממשלה 3611, "קידום היכולת הלאומית במרחב הקיברנטי" (7.8.11), החלטת הממשלה 2444, "קידום ההיערכות הלאומית להגנת הסייבר" (15.2.15), החלטת ממשלה 219, "בחינת רגולציה חכמה בסייבר וכללים והסמכות למתן הנחיות בזמן תקיפת סייבר שעודנה בעיצומה תוך שקילת שיקולים כלכליים" (1.8.21).

12 מתוך אתר המרשתת של מערך הסייבר - www.gov.il/he/pages/newabout

היחידה להגנת הסייבר בממשלה במערך הדיגיטל הלאומי: יחידת הכוונה והנחיה מקצועית בתחום הגנת הסייבר עבור משרדי הממשלה ויחידות הסמך[13]. היחידה הוקמה על פי החלטת הממשלה 2443 מפברואר 2015. היא כפופה ארגונית למערך הדיגיטל (בעבר רשות התקשוב הממשלתי) ופועלת בהנחיה מקצועית של מס"ל. מערך הדיגיטל כפוף למשרד הכלכלה והתעשייה.

יחידות הסייבר המגזריות: כיום שמונה יחידות סייבר מגזריות פועלות במסגרת משרדי ממשלה לשיפור הגנת הסייבר במגזרי המשק השונים (מגזר הבריאות, מגזר התחבורה, מגזר האנרגיה, מגזר המים, מגזר הגנת הסביבה, מגזר התקשורת, המגזר הפיננסי והמגזר לביטחון לאומי). היחידות הוקמו בהתאם להחלטת הממשלה 2443 מפברואר 2015, שהטילה על המנכ"לים של משרדי הממשלה לקדם את הטיפול בהיערכות לאיומי סייבר במסגרת המגזר שבו הם פועלים, על ידי הקמת יחידות להכוונה מגזרית והכנת עבודת מטה לבחינת התיקונים והשינויים המשפטיים הנדרשים כדי שתהיה להן הסמכות הנדרשת להנחות בתחום הסייבר את הגופים במגזר. היחידות כפופות מהבחינה הארגונית למשרד הממשלתי שאליו הן שייכות ופועלות בהנחיה מקצועית של מס"ל. אחת מהן היא יחידת הסייבר המגזרית של המשרד לביטחון לאומי, והיא מנחה גופים ויחידות סמך האמונים על אכיפת החוק ועל שמירת הסדר הציבורי והביטחון הלאומי.

הרשות להגנת הפרטיות: הרשות להגנת הפרטיות היא מאסדרת של כלל המשק ומופקדת על הגנת הזכות לפרטיות ובכלל זה הגנה על המידע האישי במאגרי מידע דיגיטליים בישראל. לשם כך הרשות מוסמכת לבצע אכיפה מינהלית ואכיפה פלילית על כלל המחזיקים במאגרי מידע (גופים פרטיים וגופים ציבוריים כאחד), בהתאם להוראות חוק הגנת הפרטיות ותקנותיו. לצורך הפקת תמונת מצב מגזרית בנוגע לעמידה בהוראות החוק והתקנות ולצורך איתור כשלים הטעונים אסדרה קיים בידי הרשות מנעד של כלים, ובהם הכלי של פיקוח רוחב, הנעשה בעיקר במגזרים שיש בהם סיכון גבוה לפגיעה בפרטיות. הרשות להגנת הפרטיות היא יחידה במשרד המשפטים והיא עצמאית ובלתי תלויה בהפעלת סמכויותיה[14].

<u>הגופים שנבדקו בביקורת</u>

גופי ביטחון לאומי

שני הגופים העיקריים שנבדקו בביקורת הם משטרת ישראל (להלן - המשטרה) וכב"ה, שניים מגופי החירום המרכזיים במדינת ישראל, הפועלים באופן שוטף למתן מענה מהיר ויעיל על אירועים מבצעיים, פליליים וביטחוניים - הן בעיתות שגרה והן בעיתות חירום. חשיבות שגרת העבודה הרציפה והתקינה של גופים אלה אף מתעצמת בהתרחש מחוללי חירום[15], גם כאלו שאינם בהכרח אירועי סייבר באופן מובהק, אולם להבדיל מרוב הגופים הציבוריים, עבור ארגונים אלו ההבחנה בין עת שגרה לעת חירום אינה מהותית מבחינת אופן תפעולם, שכן עבודת חירום היא ליבת פעילותם גם בימי שגרה.

מערכות העבודה מרחוק הן כיום רכיב קריטי בתפקודו של מערך הביטחון הלאומי, ובכלל זה של המשטרה וכב"ה.

הרשות הארצית לכבאות והצלה: ארגון הכבאות וההצלה הרשמי של מדינת ישראל, אשר יש בו כ-4,000 עובדים וכ-3,500 מתנדבים, ושתפקידיו הם כיבוי שריפות, מניעת דליקות, חילוץ והצלה של לכודים, טיפול באירועי חומרים מסוכנים והצלת נפש ורכוש. הרשות הוקמה כרשות ממלכתית ארצית במשרד לביטחון הפנים (כיום המשרד לביטחון לאומי) מכוח חוק הרשות

---

13 מלבד משרד הביטחון והגופים המיוחדים שפורטו בהחלטה 3611 ומלבד הפעולות של גופים אלה באמצעות משרדי הממשלה במסגרת תפקידם.

14 בהתאם לסעיף 1 בתוספת הראשונה לחוק הגנת הפרטיות, שמעגן את עצמאותה של הרשות.

15 במסמך "תפיסה לאומית בסייבר להיערכות ולניהול מצבי משבר" שפרסם מערך הסייבר הלאומי מוגדר מחולל חירום (Emergency Trigger) כך: "מהלך מלחמתי, תופעת טבע, משבר סייבר, פעולת טרור, תקלה וכיו"ב, שרמת הסיכון הטמונה בו מוערכת כעלולה לחולל מצב חירום".

הארצית לכבאות והצלה, התשע"ב-2012. מערך הכבאות פרוס בשבעה מחוזות, בכ-150 אתרים ברחבי הארץ, מהם 126 תחנות כיבוי, ומפעיל כ-600 כבאיות.

מערכת העבודה מרחוק בכב"ה מאפשרת עבודה מרחוק לעובדי כב"ה. כב"ה מונחית על ידי יחידת הסייבר המגזרית של המשרד לביטחון לאומי.

משטרת ישראל: המשטרה אמונה על אכיפת החוק ועל שמירת הסדר הציבורי וביטחון הפנים של המדינה. נכון לשנת 2022 משרתים בה כ-32,000 שוטרים. העבודה מרחוק במשטרה מתאפיינת בעיקר בעבודה מן השטח ובמידה פחותה מהבית.

משטרת ישראל היא אחד מחמשת הגופים שלגביהם נקבע בהחלטת הממשלה 3611[16] שההחלטה לא תחול עליהם. היא בעלת שיקול דעת עצמאי בתחום הגנת הסייבר, ולכן לדברי המשטרה היא מאמצת את הנחיות מס"ל בכל פעם שהיא מוצאת זאת לנכון ובמקומות הנדרשים אף מחמירה ביחס להנחיות האמורות. אין מדובר באימוץ כולל ומקיף של ההנחיות אלא באימוץ הנחיות שנמצאו רלוונטיות ונדרשות בהתאם לתרחישי האיום. מדור אבטחת מידע וסייבר הוא היחידה המשטרתית שמנחה את הארגון בתחום אבטחת מידע, והיחידה לביטחון מידע (יחב"ם) מנחה בתחום ביטחון המידע.

לדעת משרד מבקר המדינה, ככלל, החלטה של גוף בדבר אימוץ הנחיות של מאסדר מדינתי, כולן או חלקן, גם אם היא נעשית באופן וולונטרי, הינה מהלך שמחייב 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.

גופים נוספים שנבדקו במטלה

הנהלת בתי משפט (להלן - הב"ה): מערכת בתי המשפט בישראל מורכבת מבית המשפט העליון, מבתי המשפט המחוזיים, מבתי משפט השלום וממערך בתי הדין לעבודה. במערכת בתי המשפט, שעל הניהול והארגון המינהליים שלה מופקדת הנהלת בתי המשפט, יש כ-5,500 עובדים, מתוכם כ-900 שופטים ורשמים ועוד יותר מ-2,000 עובדים בצוות השיפוטי, הפרוסים בכ-50 אתרים ברחבי הארץ. העבודה מרחוק מבוססת על פתרון, אשר נרכשו עבורו אלפי רישיונות התחברות. העבודה מרחוק באמצעות מערכת זו מבוצעת ממספר רב של מחשבים ניידים ארגוניים. קיים פתרון נוסף לעבודה מרחוק שמשמש חלק מעובדי הגוף. הב"ה אינה נכללת בהחלטה 2443 לעניין חובת ההנחיה של יה"ב, אך בשנת 2016 קיבלה על עצמה "הנחיה מרצון" על ידי יה"ב.

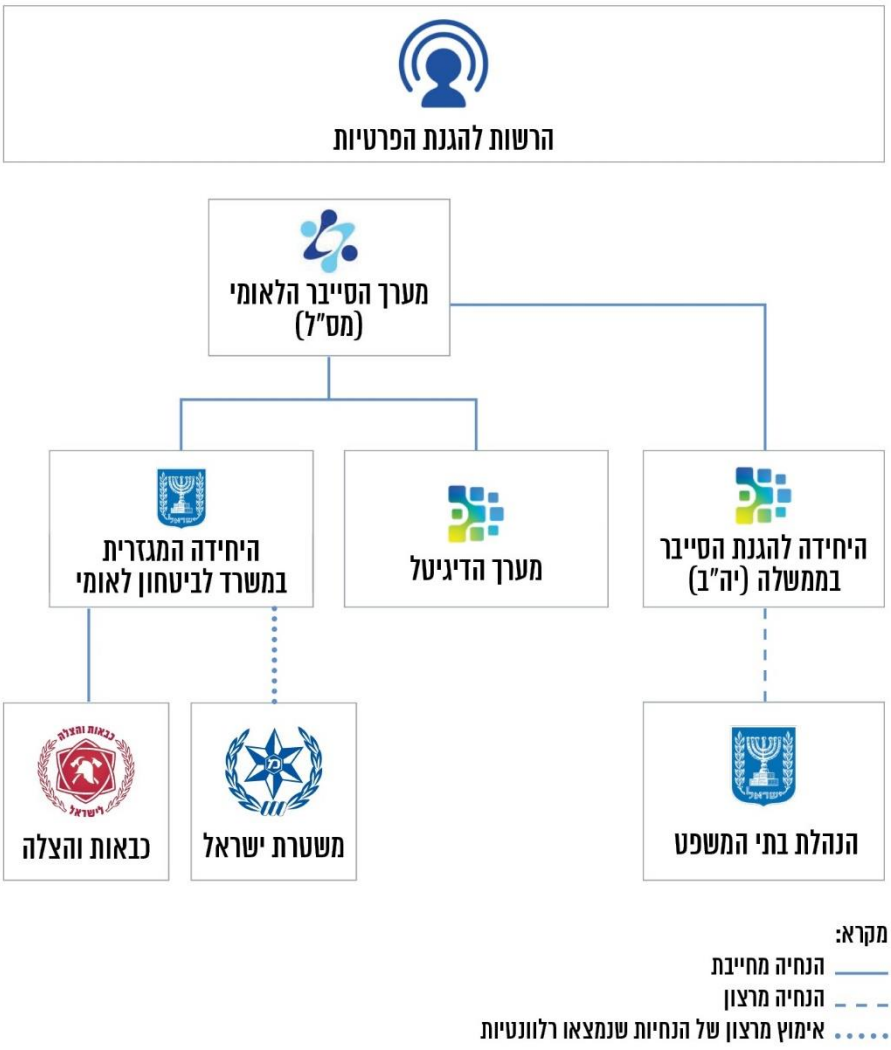
מערך הדיגיטל: הגוף האמון על קידום מהפכת הדיגיטל במגזר הציבורי. המערך כפוף לשר הכלכלה והתעשייה, משמש גוף המטה הטכנולוגי של משרדי הממשלה והגופים הציבוריים ופועל לשיפור הממשק והשירות הממשלתי עבור התושבים והעסקים בישראל[17]. מערך הדיגיטל מוגדר כגוף תמ"ק, ועל כן מונחה על ידי מס"ל בתחום הסייבר. במערך כ-600 עובדים, ולכולם הוקצו מחשבים ניידים ארגוניים אשר משמשים אותם לעבודה מרחוק באמצעות מערכת העבודה מרחוק המרכזית הקיימת במשרד. כאמור, במערך הדיגיטל פועלת יחידת יה"ב, שאחראית להנחיה מחייבת של כל משרדי הממשלה ויחידות הסמך בתחום הסייבר.

---

16 החלטת ממשלה 3611 קידום היכולת הלאומית במרחב הקיברנטי.

17 מתוך אתר האינטרנט של מערך הדיגיטל הלאומי - https://www.gov.il/he/pages/about-national-digital-agency.

תרשים 2: **מדרג האסדרה של הגופים שנבדקו בביקורת**



הוכן בידי משרד מבקר המדינה.

<u>הנחיות הגופים האסדרתיים המדינתיים בתחום אבטחת העבודה מרחוק</u>

במסגרת הביקורת נבדקו ההנחיות האלה בנושא אבטחת העבודה מרחוק:

1. **הרשות להגנת הפרטיות:** "דגשים למנהלים ועובדים בהפעלת מדיניות עבודה מרחוק אל מול הרשת הארגונית"[18], פורסם ב-24.3.20. נוסף על מסמך זה פרסמה הרשות מסמכים העוסקים בהתמודדות עם היבטים שונים של הגנת הפרטיות ואבטחת המידע בהקשר הרחב של עבודה מרחוק[19].

2. **מערך הסייבר הלאומי:** "הנחייה לחיבור משתמשים מרחוק לרשת הארגונית בגופי תמ"ק", "המלצה לחיבור משתמשים מרחוק לרשת הארגונית ביחידות המגזריות" - פורסמו לאחר פרוץ מלחמת חרבות ברזל, ב-9.10.23.

---

18 הרשות להגנת הפרטיות - "דגשים בהפעלת מדיניות עבודה מרחוק אל מול הרשת הארגונית" - www.gov.il/he/pages/corona_work

19 הגנת הפרטיות במתן שירותי רפואה מרחוק; הגנה על פרטיות בהעברת מידע רפואי באמצעים דיגיטליים; היבטי פרטיות במעקב אחרי עובדים בעבודה מרחוק; הגנת פרטיות תלמידים בלמידה מקוונת מרחוק.

3. היחידה להגנת הסייבר בממשלה - יה"ב: "גישה מרחוק" - פורסמה ב-12.3.20.

נמצא כי הרשות להגנת הפרטיות פרסמה בשנת 2020 - בעקבות התפשטות נגיף הקורונה - מסמך דגשים לעבודה מרחוק[20] שלא התעדכן מאז, ולכן כולל המלצות על שימוש בפתרונות אבטחת מידע שאינם עדכניים (כמו אנטי-וירוס) או פרוטוקולי הצפנה (כמו WPA2 ל-Wi-Fi).

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

משרד מבקר המדינה בדק את הבקרות המוגדרות בהנחיות של מס"ל כלפי גופי תמ"ק והיחידות המגזריות (הכוללות גם את יה"ב), שרלוונטיות בביקורת זו עבור מערך הדיגיטל, המשטרה וכב"ה, וכן את הנחיות יה"ב, שרלוונטיות עבור הב"ה, והשווה ביניהן.

נמצא כי אין תאימות בין הנחיות מס"ל בנושא עבודה מרחוק לאלו של יה"ב, אף שיה"ב מונחית על ידי מס"ל.

בתשובת מס"ל מאוקטובר 2025 (להלן - תשובת מס"ל) נמסר כי הנחיות מס"ל הן הנחיות כלליות שמופצות לכלל גופי המשק וגופי התמ"ק. קיימת שונות גדולה בין המגזרים והגופים השונים, ולפיכך ההנחיה קובעת כללים רחבים עם יכולת גמישות לביצוע התאמות לכל מגזר. לנוכח זאת, לא מן הנמנע שיהיו פערים בין ההנחיות של מס"ל לבין ההנחיות של כל יחידה מגזרית ושל יה"ב בפרט. בנספח ד' בהחלטה 2443 נקבע כי היחידות המגזריות יפעלו בהנחיה המקצועית של מס"ל, ועם זאת כל יחידה מגזרית תנחה את המגזר שבאחריותה בהתאם למאפייניו הספציפיים.

בהתייחס לתשובת מס"ל משרד מבקר המדינה מעיר כי הבקרות הנכללות בהנחיית יה"ב בנושא עבודה מרחוק עוסקות בנושאים מערכתיים שרלוונטיים לכלל המגזרים. לכן מומלץ כי מס"ל ישקול לכלול הנחיות בנושאים אלו גם בהנחיותיו המופנות לכלל המגזרים.

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.

בתשובת מערך הדיגיטל מאוקטובר 2025 (להלן - תשובת מערך הדיגיטל) נמסר כי הוא יבחן בשיתוף עם מס"ל את אחידות ההנחיה.

<u>פעולות הפיקוח של הגופים האסדרתיים המדינתיים</u>

מס"ל

בהתאם לחוק להסדרת הביטחון אחראי מס"ל להנחיית מרבית גופי התמ"ק, ולבקרה עליהם, בהם מערך הדיגיטל, אשר סיפק במהלך חלק מתקופת הביקורת את תשתית העבודה מרחוק ל-17 משרדי ממשלה.

כאמור, ההנחיה שחלה על מערך הדיגיטל היא הנחיית מס"ל מאוקטובר 2023 בנושא חיבור משתמשים מרחוק לרשת הארגונית. בחודשים מרץ עד מאי 2024 בדק מס"ל את פערי ההקשחות בתשתית העבודה מרחוק של כלי י"ג במערך הדיגיטל, אשר איפשר באותה עת עבודה מרחוק למשרדי ממשלה רבים. הבדיקה כללה מבדק חדירה כדי לזהות פרצות אבטחה בתשתית העבודה

[20] "דגשים למנהלים ועובדים בהפעלת מדיניות עבודה מרחוק אל מול הרשת הארגונית" - https://www.gov.il/BlobFolder/reports/corona_work/he/CORONA_%D6%B9WORK_%D6%B9PRIVACY.pdf

מרחוק. במבדק נמצאו פערים בהקשחת ממשק העבודה מרחוק, אשר מקילים על תוקף להתחבר לממשקים ברשתות המשרדים, ובפרט ברשת מערך הדיגיטל.

נמצא כי מאוקטובר 2023, מועד פרסום ההנחיה לחיבור משתמשים מרחוק לרשת הארגונית בגופי תמ"ק, 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.

בתשובת מס"ל נמסר כי מבדק החדירה שביצע מייתר לדעתו את הבדיקה של יישום ההנחיה, שכן במסגרת מבדק זה נבחן גם תחום העבודה מרחוק.

בהתייחס לתשובת מס"ל מעיר משרד מבקר המדינה כי מבדק החדירה שביצע מס"ל לא בחן נושאים מהותיים הנכללים בהנחייתו בנושא העבודה מרחוק. 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.

יה"ב

בהחלטת הממשלה 2443 הוגדר כי תפקידה של יה"ב הוא, בין השאר, לעשות בקרה על ביצוע הדרישות המקצועיות במשרדי ממשלה ויחידות סמך בהתאם להכוונה ולהנחיה שלה[21].

הנחיית יה"ב בנושא ניהול סיכוני סייבר מחייבת את משרדי הממשלה לבצע סקר סיכונים לפחות אחת ל-36 חודשים ולתקף אותו מדי 18 חודשים, וזאת לפי תבנית בדיקה אחודה ושמה "מדד יה"ב", שכוללת חמש בקרות בנושא גישה מרחוק.

כאמור, המשרדים מחויבים ליישם את ההנחיה הייעודית בנושא עבודה מרחוק, שכוללת 45 בקרות ברמת פירוט טכנית גבוהה המגדירות את הנדרש בתהליך ההתחברות המאובטח. יה"ב אינה אוכפת הנחיה זו מאז 2020 בשל משאביה המוגבלים ואי-יכולתה לפקח על יישום כל הנחיותיה (על המשרדים חלות עשרות הנחיות בנושאים שונים).

נמצא כי ממרץ 2020, מועד פרסום ההנחיה לגישה מרחוק, יה"ב לא ביצעה בקרה על אופן יישום ההנחיה במשרדי הממשלה המונחים על ידה. עוד נמצא כי 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.

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

בתשובת מערך הדיגיטל נמסר כי לנוכח ממצאי הביקורת החל תחום הבקרה לבצע בשנה האחרונה בקרות ממוקדות לגישה מרחוק שבהן נבחן לעומק יישום הנחיה לגישה מרחוק: יה"ב בדקה את תשתית החיבור מרחוק שהיא מספקת למשרדים ויחידות סמך וכן ביצעה בקרה יזומה במספר משרדי ממשלה שמשתמשים בכלים שונים הנכללים בתשתית של מערך הדיגיטל.

---

[21] החלטת ממשלה 2443, "קידום אסדרה לאומית והובלה ממשלתית בהגנת הסייבר" (15.2.15), נספח ה' סעיף 3ב.

היחידה המגזרית של המשרד לביטחון לאומי

כאמור, ההנחיה שחלה על כב"ה היא הנחיית מס"ל לעבודה מרחוק.

נמצא כי 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.

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.

בתשובת המשרד לביטחון לאומי מנובמבר 2025 נמסר כי לנוכח ממצאי הביקורת תיתן היחידה קדימות לביקורת ייעודית בנושא, בתיאום עם כב"ה.

<u>הפעולות להבטחת אי-שימוש של גופים בכלים החשופים לפגיעות אבטחת מידע[22]</u>

על פי חוק חובת המכרזים, התשנ"ב-1992, כלל גופי המדינה מחויבים בעריכת מכרז פומבי לצורך ביצוע עסקה בטובין או במקרקעין או לביצוע עבודה או לצורך רכישת שירותים. בתקנות חובת המכרזים, התשנ"ג-1993, נקבעה אפשרות להתקשרות באמצעות "מכרז מרכזי" - מכרז המתבצע מטעם החשב הכללי עבור המשרדים.

להלן הכלים הטכנולוגיים שמאפשרים עבודה מרחוק שמשרדים יכולים לבחור בהם מתוך המכרזים המרכזיים הקיימים:

1. **מכרז א':** המכרז כלל מוצר עיקרי ומוצרים נוספים של החברה, בהם כאלה המאפשרים עבודה מרחוק אשר רכישתם אפשרית כתוספת והרחבה למוצר. במכרז זה לא נכללו דרישות אבטחה ייעודיות להיבטי עבודה מרחוק. במוצר התגלו בשנים האחרונות כמה פרצות ברמות סיכון קריטיות. יה"ב ביצעה הוכחת היתכנות (POC)[23] של המוצר כדי לבחון אם הוא מתאים לצרכיה, אולם נמצאו בו פערי אבטחת מידע משמעותיים, הוא לא עמד בדרישותיה ועקב כך לא הוטמע במערך הדיגיטל ככלי לעבודה מרחוק.

2. **מכרז ב':** במכרז זכתה חברה שבמודול העבודה מרחוק של המוצר שהיא מספקת התגלתה לפני מספר שנים פרצת אבטחה קריטית שבגינה בוצעו ברחבי העולם תקיפות רבות של המוצר. במכרז זה היו דרישות אבטחה ייעודיות להיבטי עבודה מרחוק.

3. **הסכם מחירים מרביים:** הסכם התקשרות עם חברה ג', הכולל מחירי רישיונות בלבד ולא נכללות בו דרישות אבטחה. במודול העבודה מרחוק של מוצר זה, התגלו כמה פגיעויות משמעותיות בבדיקת חדירה שבוצעה בגוף מסוים לפני מספר שנים. כמו כן לפני מספר שנים התגלתה פגיעות קריטית במוצר.

4. **מכרז מרכזי ייעודי למערכת גישה מאובטחת לעבודה מרחוק:** החל מאפריל 2022 מינהל הרכש בשיתוף מס"ל ומערך הדיגיטל ביצעו מכרז מרכזי ייעודי לתחום

---

22 **חולשה** במערכת מחשוב - בתוכנה, בחומרה, בתצורה או בתהליך - שיכולה להיות מנוצלת על ידי תוקף כדי לגרום נזק, לקבל גישה לא מורשית או לשבש את פעולת המערכת.

23 תהליך שבו הארגון בוחן מוצר או פתרון מסחרי כדי **לוודא שהוא מתאים לצרכים, לתהליכים ולתשתיות של הארגון** - כדי להחליט אם לרכוש ולהטמיע אותו.

העבודה מרחוק. הזוכה במכרז זה הוכרז בפברואר 2025. במכרז זה נכללות דרישות אבטחת מידע להיבטי עבודה מרחוק.

תמונת מצב בנוגע לשימוש משרדי ממשלה בפתרונות עבודה מרחוק

עד ינואר 2025 ניהל ותחזק מערך הדיגיטל את התשתית המדינתית לעבודה מרחוק ששימשה מלבדו גם 17 משרדי הממשלה. לצורך כך התקשר המערך לפני כמה שנים בפטור ממכרז עם ספק יחיד לרכישת כלי י״ג, שהוא מוצר רוחבי לעבודה מרחוק, כדי לספקו למשרדים. בשנים האחרונות התגלו במוצר פגיעויות רבות, שבגינן בוצעו מתקפות סייבר רבות ומשמעותיות בארץ ובעולם. ב-17.3.24 הנחה מס״ל את מערך הדיגיטל להחליף את המוצר עקב מספר רב של חולשות שנמצאו בו. כאמור, באותה העת תהליך ביצוע המכרז לרכש כלי ייעודי לעבודה מרחוק היה בעיצומו, וטרם פורסם הזוכה בו. בעקבות זאת החליט מערך הדיגיטל להחליף את כלי י״ג ולצאת לרכש חירום של כלי י״ח.

באוגוסט 2024 נמסר ממערך הדיגיטל כי כלי י״ח כבר פרוס ויוכל להחליף את כלי י״ג בכלל המשרדים בתוך 3 - 5 חודשים.

בנובמבר 2024 נמסר ממערך הדיגיטל כי מכרז מרכזי ייעודי לעבודה מרחוק פורסם כמה חודשים לפני כן, וכי המערך הפסיק את הפריסה של כלי י״ח כדי שלא לפגוע במכרז והחליט להמשיך את השימוש בכלי י״ג כפתרון התשתית המרכזי עד להכרזה על הזוכה במכרז. עד ינואר 2025 הומלץ בהנחיית יה״ב להשתמש בכלי י״ג לגישה מרחוק למרות הפגיעויות הרבות שנמצאו במוצר לאורך השנים האחרונות, אשר חלקן נוצלו לביצוע מתקפות סייבר בארץ ובעולם.

בתחילת שנת 2025 פורסמה פגיעות קריטית חדשה בכלי י״ג ובוצעו מתקפות סייבר על תשתית מערך הדיגיטל שבהן נוצלה פגיעות זו, ועקב כך החליט מערך הדיגיטל להפסיק את השימוש בכלי י״ג ואת השירות למשרדים באמצעות מערכת זו. בהמשך להערכת מצב משותפת של מס״ל ומערך הדיגיטל שהתקיימה ב-11.1.25 הנחה מס״ל את מערך הדיגיטל שלא לחבר בחזרה משרדים לכלי י״ג, וב-17.1.25 פרסמו מס״ל ויה״ב הנחיה משותפת ובה הנחו את כלל הגופים הממשלתיים להפסיק באופן מיידי וגורף את השימוש בכלי י״ג ולעבור לשימוש במוצרים העומדים בהנחיות יה״ב ומס״ל. בפברואר 2025 הוכרז הזוכה במכרז הייעודי המרכזי, ובמקביל עדכנה יה״ב את הנחייתה בנושא גישה מרחוק, והיא כוללת כיום הנחיות מפורטות בנושא תהליך ההתחברות אל המוצר, אולם לא ניתנה למשרדים המלצה לעבור להשתמש בו, והם יכולים לבחור בכל אחד מהכלים שקיימים במכרזים השונים.

לוח 1: **התפלגות השימוש בטכנולוגיות עבודה מרחוק לפני האירוע בכלי י״ג ואחריו**

	אוקטובר 2024	נובמבר 2025		
המוצר	**מספר המשרדים**	**מספר המשרדים**	**דרישות האבטחה במכרז**	**מסגרת הרכישה**
כלי י״ד	9	20	לא נכללו	חלק ממכרז מרכזי
כלי י״ב	0	10	נכללו	הזוכה במכרז הייעודי
כלי ט״ו	6	6	נכללו	חלק ממכרז מרכזי
כלי י׳	2	3	לא נכללו	חלק מהסכם מחירים מרכזי
כלי י״א	0	3	לא נכללו	חלק מהסכם מחירים מרכזי
כלי ט״ז	0	1	לא נכללו	ללא מכרז או הסכם מרכזי
כלי י״ט	0	1	לא נכללו	ללא מכרז או הסכם מרכזי
כלי י״ג	31	0	לא נכללו	
סה״כ	**48**	**44**		

על פי ממצאי הביקורת של משרד מבקר המדינה מתוך מסמכים שסופקו על ידי מערך הדיגיטל.

מהלוח "התפלגות השימוש בטכנולוגיית עבודה מרחוק לפני ואחרי האירוע בכלי י"ג עולה כי 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. רק בינואר 2025 נפסק השימוש במוצר. יצוין כי מערך הדיגיטל נערך להחלפת כלי י"ג באמצעות התקשרות רכש חדשה לאחר קבלת ההנחיה ממס"ל להפסיק את השימוש במוצר זה, אולם לא הנחה את המשרדים להפסיק את השימוש בו ולעבור למוצר חליפי שהיה זמין לרכישה באמצעות אחד מן המכרזים המרכזיים הקיימים.

בתשובת מערך הדיגיטל נמסר כי לאורך התקופה הם עדכנו באופן מיידי כל פגיעות שפורסמה בכלי י"ג.

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 ללא מתן פתרון מצד היצרן בטווח זמן קצר, יפרסמו מס"ל ויה"ב הנחיה רלוונטית בסמיכות לאירוע ויוודאו מול מינהל הרכש שיש הלימה למחויבות החוזית שבהסכמי המכרז המרכזי.

מערך הדיגיטל מסר בתשובתו כי ההמלצה מקובלת עליו, וכי הוא מקיים שיח עם מינהל הרכש כדי לקבל התראות ממוקדות ישירות מהיצרן בכל פעם שמתגלות במוצרים חולשות שעלולות להשפיע על עבודת הממשלה. עוד נמסר כי יה"ב אינה נותנת הנחיות לשימוש במוצר ספציפי אלא ליישום דרישות אבטחת מידע טכנולוגיות, וכי היא מעודדת מעבר לטכנולוגיות Zero Trust, אשר מספקות מענה נוסף מעבר לחיבור מאובטח מרחוק.

בתשובת מס"ל נמסר כי ההמלצה מקובלת עליו.

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.

יישום ההנחיות בתחום העבודה מרחוק על ידי הגופים שנבדקו בביקורת - תמונת מצב

<u>מדיניות ונהלים בעניין עבודה מרחוק</u>

מדיניות לעבודה מרחוק היא נדבך מרכזי בשמירה על אבטחת מידע בסביבה שבה גם לעובדים ששוהים מחוץ למשרד הפיזי יש גישה למשאבי הארגון. מדיניות ברורה מגדירה את הכלים, הנהלים ואמצעי ההגנה הנדרשים כדי למנוע פריצות, זליגות נתונים או שימוש לא מורשה במשאבי הארגון. בהיעדר מדיניות כזו, הארגון חושף את עצמו לסיכונים משמעותיים, כגון גישה לא מאובטחת לרשתות, שימוש במכשירים שאינם מוגנים ותקלות שעלולות לפגוע במוניטין ובתפקוד העסקי.

בהנחיית מס"ל נקבע כי יש לקבוע ולאשר מדיניות ארגונית ונהלים לעבודה מרחוק באמצעות תשתיות המחשוב הארגוניות. כמו כן, מטרתה של ההנחיה של יה"ב היא להנחות את קהל היעד בדבר קביעת מדיניות לגישה מאובטחת מרחוק לרשת הפנים-ארגונית ולמערכות המידע של המשרד.

כב"ה, המשטרה והב"ה

במסמך מדיניות אבטחת המידע של כב"ה לא מוזכר כלל נושא העבודה מרחוק. יש לארגון נוהל עבודה מרחוק, אולם נוהל זה אינו עוסק בבקרות רבות שבהנחיית מס"ל בנושא עבודה מרחוק נקבע כי יש לבצען - הנחיה אשר מחייבת את הארגון - וגם אין בו הפניה אל ההנחיה.

במסמך המדיניות של המשטרה לא מוזכר נושא העבודה מרחוק, אף שהוא חלק מרכזי בעבודת המשטרה.

להב"ה יש מסמך מדיניות גישה מרחוק וכן נוהל גישה מרחוק למשתמשים. עם זאת, בנוהל חסרות בקרות אשר נדרשות בהנחיית יה"ב בנושא עבודה מרחוק אשר הארגון אימץ, וגם אין בו הפניה אל ההנחיה.

נמצא כי מסמכי מדיניות אבטחת המידע של כב"ה והמשטרה אינם עוסקים בנושא העבודה מרחוק. עוד נמצא כי בנוהלי העבודה מרחוק בכב"ה חסרות בקרות מסוימות שנכללות בהנחיית מס"ל; כמו כן, בנוהלי העבודה מרחוק בהב"ה חסרות בקרות מסוימות שנכללות בהנחיית יה"ב.

בתשובת המשטרה מפברואר 2026 נמסר כי אין היא רואה את העבודה מרחוק כתת-נושא ייחודי המצריך התייחסות פרטנית במסמך המדיניות. כמו כן, ישנה התייחסות יחב"מית פרטנית לנושא האבטחה והשמירה הפיסית על המכשירים לאור העובדה שמדובר באמצעי נייד.

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 כב"ה והב"ה לעדכן את מסמכי המדיניות והנהלים שלהם באופן שהם יכללו את הבקרות הנדרשות בהנחיות הגופים האסדרתיים הרלוונטיים עבורם (מס"ל ויה"ב). על יה"ב והיחידה המגזרית במשרד לביטחון לאומי לוודא כי מסמכי המדיניות והנהלים לעבודה מרחוק של הגופים הכפופים להנחייתם תואמים להנחיות.

בתשובת כב"ה מאוקטובר 2025 (להלן - תשובת כב"ה) נמסר כי הליקוי תוקן: נכתבו שני נהלים חדשים.

בתשובת הב"ה מספטמבר 2025 נמסר כי הליקוי תוקן: עודכנו כלל הבקרות הרלוונטיות להב"ה במסמכי המדיניות, בנהלים ובהנחיות.

בתשובת מערך הדיגיטל נמסר כי במהלך הביקורת, ב-3.7.25, ביצעה יה"ב בקרה על החיבור מרחוק בהב"ה.

נושאים טכנולוגיים בעבודה מרחוק

בחלק זה של הדוח 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.

על הגופים השונים שבהם נמצאו פערים לטפל בהם.

ניהול סיכוני עבודה מרחוק

בהנחיית מס״ל מוגדר כי על הנהלת הארגון לבצע הערכת סיכונים ובהתבסס עליה לקבוע משמעויות אבטחתיות וזאת עוד לפני שייקבע מהי תצורת העבודה המומלצת. כמו כן צוין בהנחיה כי יש לוודא שהערכת הסיכונים כוללת התייחסות פרטנית לדרישות חוק, לרגולציה ולדרישות עסקיות. בהנחיית יה״ב מוגדר כי בעת מתן אישור לעבודה מרחוק יש להגדיר וליישם תהליך של הערכת סיכוני סייבר, בהתאם למתאר הסיכונים של המשרד, לרמת החשיפה של יעדי ההגנה לאיומים ולבקרות ההגנה המיושמות במשרד.

כב״ה

בכב״ה אין סקר סיכונים עדכני. הסקר האחרון, שביצעה חברה חיצונית בשנת 2019, אינו מתוקף, ועל כן מבחינת אגף הביטחון של הארגון אינו רלוונטי כיום, גם לגבי מערכות ותהליכי העבודה מרחוק.

נמצא כי כב״ה לא ביצעה הערכת סיכונים לגבי תהליך הגישה מרחוק, וזאת בניגוד להנחיית מס״ל, בה מוגדר כי על הנהלת הארגון לבצע הערכת סיכונים ובהתבסס עליה לקבוע משמעויות אבטחתיות. נוכח זאת קיים חשש כי הסיכונים שכרוכים בתהליך הגישה מרחוק לא יובאו בחשבון ולא יינקטו הצעדים הנדרשים להפחתת סיכונים אלו.

על כב״ה לוודא כי תהליכי הערכת הסיכונים שמבוצעים כוללים התייחסות לתהליך העבודה מרחוק, בהתאם להנחיות מס״ל. עוד מומלץ כי גופי האסדרה (יה״ב והיחידה המגזרית של המשרד לביטחון לאומי) יוודאו כי תהליכי הערכת סיכונים בגופים הכפופים להנחייתם כוללים התייחסות לתהליכי העבודה מרחוק ולמערכות המשמשות לכך.

המשטרה

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

מבדקי חדירה למערכות עבודה מרחוק

בהנחיית יה״ב בנושא גישה מרחוק נכללת בקרה שלפיה נדרש לבצע מבדקי חדירה תקופתיים כדי לבדוק את מידת ההתאמה בין רמת ההגנה המוגדרת לבין רמת ההגנה המיושמת בפועל.

בהנחיה של מס״ל בנושא עבודה מרחוק נכללת בקרה המנחה לבצע בדיקת חדירה לפתרון הטכנולוגי המשמש לעבודה מרחוק. בבקרה נוספת נדרש לבצע סריקת פגיעויות ופורטים תקופתית.

היחידה המגזרית של המשרד לביטחון לאומי ביצעה ביוני 2020 מבדק חוסן תשתיתי ברשת של כב״ה, אולם המבדק לא כלל מבדק חדירה ייעודי לפתרונות הגישה מרחוק. גם מבדק שבוצע עבור כב״ה בנובמבר 2023 לא היה ייעודי למערכות הגישה מרחוק, אולם נמצאו בו גם פערים במערכות העבודה מרחוק. באפריל 2025 בוצע במסגרת הביקורת מבדק חדירה במערכת העבודה מרחוק.

בבדיקת חדירה שבוצעה במשטרה בתחילת שנת 2025 נמצאו פערי אבטחה. מבדק החדירה הקודם במערכת בוצע בשנת 2017.

נמצא כי בכב״ה לא בוצעו מבדקי חדירה למערכת העבודה מרחוק עד אפריל 2025 (המבדק שבוצע על ידי הביקורת), וכי המשטרה ביצעה מבדק חדירה במערכת הטכנולוגית המשמשת לעבודה מרחוק במהלך הביקורת בתחילת שנת 2025, מבדק שבו נמצאו פערים, כשמונה שנים לאחר 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 לא מודע לחולשות שבמערכותיו.

על כב״ה לבצע מבדקי חדירה עיתיים וייעודיים במערכות העבודה מרחוק, בהתאם להנחיית מס״ל.

בתשובת כב״ה נמסר כי הליקוי תוקן: היא הזמינה מספר מבדקי חדירה.

על המשטרה לבצע מבדקי חדירה עיתיים וייעודיים במערכת העבודה מרחוק בהתאם להנחיית מס״ל.

בתשובת המשטרה נמסר כי היא מבצעת באופן עיתי מבדקי חדירה.

<u>המשכיות עסקית ורציפות תפקודית</u>

מעטפת ההגנה של הארגון אינה מונעת לחלוטין את התרחשותם של אירועים חריגים, ולכן שמירה על הרציפות התפקודית של הגוף חיונית כדי שלגוף תהיה יכולת להמשיך לספק את השירותים החיוניים בשעת משבר ולמזער את הנזקים שעלולים להיגרם בגינו. לצורך כך, ולפי נורמות מקובלות[24], על הארגון להיערך למשבר מראש, ובכלל זה עליו לגבש, לתקף ולתרגל תוכנית המשכיות עסקית (BCP - Business Continuity Plan). התוכנית מגדירה תוכנית פעולה לניהול של התהליכים העסקיים הקריטיים בארגון ולמערכות המידע התומכות בהם לצורך התאוששות באופן מלא או חלקי, בפרק זמן מוגדר וברמת שירות מוגדרת, בהתאם למדיניות הארגון. כמו כן, על הארגון לוודא שיש לו יכולת שחזור מהירה של תשתיות מערכות המידע העולה בקנה אחד עם יעדי הארגון, וכן עליו להיערך מבחינת תשתיות חלופיות באתרים חליפיים, ובכלל זה בהיבטי זמינות וַתירות.

לצורך הבטחת הרציפות התפקודית, על הארגון לוודא שעומדים לרשותו הנדבכים האלה:

1. **מדיניות המשכיות עסקית (BCP):** גיבוש מדיניות המשכיות עסקית (לרבות קביעת מדד מקובל לכל שירות ויעדי הגנה התומכים בו) ותיקופה לפחות אחת לשנה.

2. **תוכנית התאוששות מאסון:** גיבוש תוכנית התאוששות מאסון (DRP - Disaster Recovery Plan), תיקופה לפחות אחת לשנה ותרגולה באופן עיתי.

3. **אתר גיבוי (DR - Disaster Recovery):** קיומו של אתר DR נגיש בעת חירום, הנותן מענה על הצרכים של הגוף כפי שבאים לידי ביטוי במדיניות ההמשכיות העסקית; תרגול מעבר לאתר הגיבוי אחת לשנה (של כלל הצוותים העוסקים בהקמתו ובתפעולו), הפקת לקחים ויישומם.

4. **מערך גיבוי:** מערך לגיבוי של נתונים ושל מערכות מחשוב ותקשורת התומכים ביעדים עסקיים, התואם את צורכי הגוף מבחינת ההמשכיות העסקית בהתאם למדיניות ההמשכיות העסקית; בדיקת תקינות הגיבוי והיכולת לשחזור תקין.

הנחיית מס״ל בנושא עבודה מרחוק דורשת היערכות עם נוהל מקרים ותגובות לאירוע, וכן תרגול עיתי של אירועים אלו.

---

[24] תורת ההגנה 2.0, ISO 27001, NIST 800-53.

המשטרה וכב"ה

מהמשטרה נמסר כי היא לא קבעה לעצמה מדיניות לעניין העבודה בעיתות חירום ולא הגדירה מהם צרכיה בתקופות אלה, ועל כן לא ניתן לומר מהו הפער בציוד הארגוני שיידרש לתמיכה בעבודה מרחוק בשעת חירום.

נמצא כי למשטרה ולכב"ה אין תוכנית המשכיות עסקית (BCP), ועל כן, בין השאר, אין ביכולתן להגדיר את הפערים בציוד ובתשתיות 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 וידאה, הגדירה ואישרה מדיניות ואסטרטגיה בנושא המשכיות עסקית (BCP).

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

נמצא כי נוהלי העבודה מרחוק של כב"ה אינם כוללים פירוט של מקרים ותגובות לאירועי סייבר הקשורים לעבודה מרחוק, בניגוד להנחיית מס"ל, הדורשת היערכות עם נוהל מקרים ותגובות לאירוע.

מומלץ כי המשטרה וכב"ה יגבשו ויאשרו תוכנית המשכיות עסקית הכוללת התייחסות להתאוששות המערך הטכנולוגי של הארגון ולעבודה מרחוק בעיתות חירום, כנדרש על פי תורת ההגנה.

בתשובת המשטרה מינואר 2026 נמסר כי מסמך BCP טכנולוגי נמצא בימים אלו בשלבי כתיבה מתקדמים.

בתשובת כב"ה נמסר כי בכוונתה לתקן את הליקוי עד סוף שנת 2025: היא ביצעה הזמנה מחברה מלווה להכנת תוכנית ההמשכיות העסקית.

על כב"ה לבצע תרגולים עיתיים של ההמשכיות העסקית של התשתיות הטכנולוגיות שמאפשרות חיבור ועבודה מרחוק, בהתאם להנחיית מס"ל.

על המשטרה לבצע תרגולים עיתיים של ההמשכיות העסקית של התשתיות הטכנולוגיות שמאפשרות חיבור ועבודה מרחוק, בהתאם להנחיית מס"ל.
בתשובת המשטרה נמסר כי ההמלצה לביצוע תרגולים עיתיים מקובלת עליה.

כב"ה

בכב"ה מאות רבות של מחשבים ניידים המשמשים לעבודה מרחוק. עם זאת, בכב"ה תשתית העבודה מרחוק (כלי י') הקיימת תומכת במאות בודדות של משתמשים בו-זמנית, בשל מגבלות מספר הרישיונות הקיים ויכולות השרתים בתשתית מערכת העבודה מרחוק. בשני אירועי חירום בשנים האחרונות - בעת מגפת הקורונה ובתחילת מלחמת חרבות ברזל - הגיעה המערכת למקסימום הניצולת שלה (Maximum utilization), ועל כן התאפשרה במגפת הקורונה עבודה מרחוק לעובדים נוספים באמצעות מערכת י"ג, נוסף על כלי י', באופן שמספר החיבורים בו זמנית לעבודה מרחוק הורחב. בדצמבר 2024 כב"ה השביתה את מערכת י"ג עקב חולשת אבטחה שנמצאה בגרסה שהייתה מותקנת בארגון וכן עקב ההודעה של היצרן ולפיה הוא אינו תומך עוד בגרסה (ועל כן אין אפשרות לעדכנה ולסגור חולשה זו).

נמצא כי בכב"ה מספר הרישיונות לעבודה מרחוק וכן תשתית שרתי מערכת העבודה מרחוק לא סיפקו מענה הולם בעיתות חירום כמו מגפת הקורונה ותחילת מלחמת חרבות ברזל, מכיוון שבעיתות אלה נדרשה עבודה מרחוק בהיקפים גדולים יותר מאשר בעת שגרה. על כן בתקופות

אלה היה צורך לבצע פעולות נקודתיות לגידול בכמות המשתמשים ביחס לימי שגרה. עוד נמצא כי נכון למועד סיום הביקורת כב"ה לא יכלה לבצע פעולות לגידול נרחב בכמות המשתמשים: היא אינה ערוכה לרכש של שרתים נוספים או של מחשבים ניידים למערכת העבודה מרחוק בעיתות חירום, בניגוד לנדרש על פי תורת ההגנה.

מומלץ כי כב"ה תגדיר את הצרכים הטכנולוגיים הנדרשים (תשתיות מחשוב, מחשבים ניידים וכו') וכן את גורמי כוח האדם הרלוונטיים בארגון שנדרשים לעבוד מרחוק בשעת חירום. עוד מומלץ כי כב"ה תרכוש רישיונות, שרתים ומחשבים ניידים חדשים בהתאם להגדרת צרכים זו.

משרד מבקר המדינה מציין לחיוב את כב"ה על ההחלטה להשבית את מערכת י"ג הארגונית לעבודה מרחוק בדצמבר 2024 עם היוודע על חולשת אבטחה קריטית שהתגלתה בה. פעולה זו בוצעה כחודש לפני מתקפת הסייבר על מערכות י"ג של מערך הדיגיטל ומשרדים נוספים, אשר בעקבותיה הושבתה העבודה מרחוק במשרדים רבים לתקופה של כמה שבועות.

רציפות תפקודית בהיבטים טכנולוגיים

הרציפות התפקודית בהיבטים טכנולוגיים בהקשר של עבודה מרחוק מבוססת על שני מרכיבים עיקריים: יתירות ברמת התשתית לעבודה מרחוק ויתירות ברמת תשתית התקשורת. היתירות נדרשת עבור אירועים כמו עומס חריג שאינו צפוי, מתקפות סייבר או תקלות.

בכב"ה ובמשטרה נמצאו פערים בחלק מהנושאים שנבדקו.

על כב"ה ועל המשטרה לפעול בהתאם להמלצות המבקר.

מבדק חדירה בכב"ה - בוצע על ידי משרד מבקר המדינה

סקר הערכת פגיעויות ומבדק חדירה ברשת כב"ה

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.

משרד מבקר המדינה מציין לחיוב את שיתוף הפעולה עם כב"ה בכל שלבי מבדק החוסן: החל בתכנונו, המשך בביצועו, בתהליך הצגת הממצאים ובנכונות לשפר את התהליכים הקיימים וכלה בטיפול בחלק מהליקויים שנמצאו בתוך זמן קצר ביותר.

כב"ה פעל לתיקון הליקויים החל משלב ביצוע המבדק.

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[25] לעובדי מדינה לעבוד יום בשבוע מהבית, ומרבית הגופים בשירות המדינה עובדים כך).

[25] בהתאם ליכולת לבצע את התפקיד מרחוק.

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.