

מבקר המדינה | דוח מיוחד: התמודדות מדינת ישראל עם
משבר הקורונה | התשפ"א-2021



החטיבה לביקורת משרדי ממשלה
ומוסדות שלטון

**ההיערכות התקשובית
של משרדי הממשלה
לעבודה מרחוק ויישומה
במשבר הקורונה**



ההערכות התקשובית של משרדי הממשלה לעבודה מרחוק ויישומה במשבר הקורונה

רקע

שוק העבודה עומד בפני אתגרים רבים, לרבות ההערכות לשוק עבודה משתנה וגמיש, שיושפע בין היתר משינויים טכנולוגיים ודיגיטליים. אחד השינויים שיאפיינו את שוק העבודה בעתיד, וכבר מאפיין אותו בתקופת הקורונה, הוא עבודה באמצעות התחברות מרחוק למערכות הממוחשבות של הארגון (עבודה מרחוק). לעבודה מרחוק יש תועלות בתחומים שונים, כגון צמצום זיהום האוויר ממקורות תחבורתיים, הקלת העומס בכבישים ושיפור ההנגשה של מקומות העבודה לאוכלוסיות שהיו מודרות מהם בגלל קשיי נגישות. לצד זה העבודה מרחוק מציבה מגוון אתגרים לעובדים ולמעסיקים, כגון צמצום האינטראקציה החברתית בין עובדים בארגון וקושי של המעביד לפקח על העובד.

נתוני מפתח

48%

מכלל עובדי משרדי הממשלה קיבלו אישור לעבוד מהבית במאי 2020

כ-4%

מהמועסקים בישראל לפני פרוץ משבר הקורונה עבדו מהבית (לפי נתונים לשנת 2018), וזאת לעומת 5.4% מהמועסקים במדינות האיחוד האירופי (לפי נתונים לשנת 2019)

כ-40,000

עובדים מועסקים במשרדי הממשלה וביחידות הסמך

כ-2,500

מחשבים ניידים היו חסרים למשרדי הממשלה ובתי החולים הממשלתיים בתחילת משבר הקורונה (מרץ 2020)

13%

משעות העבודה במאי 2020 התבצעו מהבית

51% - 57%

מהעובדים החיוניים במשרדי הממשלה עבדו מהבית בתקופת החירום¹



5	48%	51%
משרדים (מתוך 36) ציינו כי בעבר התרחש בהם אירוע סייבר באמצעות ממשק החיבור מרחוק	הגידול שחל במספר אירועי הסייבר שניטר המרכז הארצי לניהול אירועי סייבר (CERT) בשנת 2020 (שבה התרחשו 3,662 אירועי סייבר) לעומת מספרם בשנת 2019 (שבה התרחשו 2,443 אירועים)	שיעור הנשים במשרדי הממשלה שאושר להן לעבוד מהבית במאי 2020 לעומת 43% מהגברים במשרדי הממשלה

פעולות הביקורת

בחודשים מאי 2020 - פברואר 2021 בדק משרד מבקר המדינה היבטים הנוגעים להיערכות התקשובית של משרדי ממשלה לעבודה מרחוק וליישומה בתקופת משבר הקורונה. הביקורת נעשתה ברשות התקשוב הממשלתי (להלן - רשות התקשוב). בדיקות השלמה נעשו בחמישה משרדי ממשלה: במשרד הפנים, במשרד התחבורה והבטיחות בדרכים, במשרד המדע והטכנולוגיה, במשרד המשפטים ובמשרד להגנת הסביבה; וכן בנציבות שירות המדינה, במשרד האוצר ובמערך הסייבר הלאומי במשרד ראש הממשלה.

תמונת המצב העולה מן הביקורת



גיבוש מדיניות תקשובית לעבודה מרחוק: רשות התקשוב פרסמה כמה הנחיות העוסקות בנושא גישה מרחוק שמתמקדות בעיקר בהיבטים של אבטחת מידע והמשכיות עסקית, אולם הנחיות אלה אינן בגדר מדיניות כוללת בנושא העבודה מרחוק, וחסרה בהן התייחסות למגוון היבטים בתחום התקשוב, כגון: התשתיות והציוד הנדרשים לעובדים לשם עבודה מיטבית; השירותים הממשלתיים הפרונטליים אשר ניתן לתת במסגרת העבודה מרחוק (ואלו שלא); החלופות האפשריות ליישום מודל עבודה זה ותפקידו של הענן במסגרת העבודה מרחוק.

תוכנית להמשכיות עסקית: הועלה כי נכון לנובמבר 2020, 21 (57%) מ-37 משרדי ממשלה שנבדקו טרם גיבשו תוכנית המשכיות עסקית להבטחת המשך תפקודו התקין של הארגון; אשר לחמשת משרדי הממשלה שנבדקו פרטנית בביקורת - הועלה כי משרד התחבורה ומשרד המדע טרם השלימו את גיבושה של תוכנית ההמשכיות העסקית, וכי למשרד הפנים, משרד המשפטים והמשרד להגנת הסביבה היו באותו המועד תוכניות



להמשכיות עסקית, אך רק אחת מהן - של משרד המשפטים - עסקה בין היתר בנושא העבודה מרחוק.

היבטי תשתית: מניתוח נתוני רשות התקשוב עולה כלהלן: עם פרוץ המשבר במרץ 2020 ציינו 19 (45%) מ-42 משרדי הממשלה שיש לכלל העובדים הזקוקים לחיבור מרחוק מחשב נייד או נייד (או כל אמצעי חיבור אחר) המאפשר להם חיבור מרחוק, 22 (52%) מהמשרדים ציינו שלא היו להם די מחשבים כדי שיוכלו להקצות מחשב כאמור לרשות כלל העובדים הנזקקים לחיבור מרחוק, ומשרד אחד לא השיב על השאלה; 19 (45%) מהמשרדים ציינו כי המערכות שלהם עמדו בעומס ואיפשרו עבודה תקינה ורציפה מרחוק, שניים (4%) מהמשרדים ציינו שהמערכות שלהם לא עמדו בעומס, ויתר המשרדים לא השיבו על שאלה זו או ציינו כי הם נמצאים בתהליכי היערכות כדי שיוכלו להשלים את המחסור בציד ובתשתיות באופן שיאפשר לכלל העובדים שנדרשים לעבוד מרחוק לעשות כן. באותו המועד היו חסרים במשרדי הממשלה ובתי החולים הממשלתיים כ-2,500 מחשבים ניידים. המשרדים נקטו מגוון פעולות כדי להרחיב את היקף העבודה מרחוק, למשל הושמשו מחשבים ישנים שנועדו לגריטה, הוקצו מחשבים ברוטציה בין עובדים ובוצעו התאמות במחשבים פרטיים של העובדים. יצוין כי כמה חודשים לאחר פרוץ המשבר חל שיפור ביכולתם של המשרדים לתמוך באופן העבודה האמור.

הטמעת בקורות להבטחת גישה מאובטחת מרחוק: על מנת למזער את הסיכונים הטמונים בעבודה מרחוק יש להטמיע בקורות שונות שיאפשרו הגנה על המידע, ניטור פעולות חריגות ותייעוד. מניתוח נתוני יח"ב (היחידה להגנת הסייבר בממשלה) עולה כי נכון לדצמבר 2020, למעט משרד אחד, כל משרדי הממשלה האחרים שנבדקו (35 משרדים) עומדים בבקורות שיה"ב קבעה כי הן בגדר תנאי סף להתחברות מאובטחת מרחוק. עם זאת, נמצאו פערים ביישומן של בקורות נוספות: ב-15 (41%) מהמשרדים שנבדקו לא מתבצעים זיהוי ואימות של המכשירים שמהם מתבצעת ההזדהות מרחוק; בעשרה (27%) מהמשרדים בעת חיבור המחשב לרשת לא מתבצע וידוא כי מותקנת בו תוכנת אנטי-וירוס; בשלושה (8%) מהמשרדים אין הגבלה בנוגע למספר החיבורים המותרים בו-זמנית של משתמש יחיד; בחמישה (14%) מהמשרדים הגישה למערכות המשרד לא מתבצעת אך ורק באמצעות רכיב ייעודי מוקשח; בעשרה (27%) מהמשרדים אין הגבלת גישה לכתובות IP מישראל בלבד, ובשלושה (8%) מהמשרדים מערכות החיבור מרחוק אינן מחוברות למערכת ניטור. כמו כן, ניתוח הנתונים העלה כי באחד המשרדים לא הוטמעו ארבע מהבקורות הנוספות, ובשלושה משרדים לא הוטמעו שלוש מהבקורות הנוספות.

עמידה בתקן ISO 27001: עלה כי בפברואר 2021 שישה מ-40 המשרדים המונחים על ידי יח"ב עדיין אינם עומדים בתקן ISO 27001, הגם שלפי החלטת הממשלה הם היו אמורים לעמוד בו כבר בפברואר 2020.

ביצוע מבדקי חדירה: נמצא כי במסגרת הבקורות שיה"ב מקיימת על משרדי הממשלה היא מבצעת מבדקי חדירות לבדיקת המוגנות של הארגון, אולם היא לא ביצעה מבדקי חדירות בהיבט של עבודה מרחוק.



שימוש בתוכנות מסרים מיידיים: הועלה כי משרדי הממשלה נאלצים להשתמש בתוכנות מסרים מיידיים מסחריות, בעיקר לנוכח היעדרו של תחליף מאובטח ואיכותי לתוכנות אלה. הדבר גורם לחשיפה של המידע הארגוני ומגדיל במידה ניכרת את נגישותו של מידע זה לגורמים בלתי מורשים ולמזיקים; המידע השמור במכשיר אינו מוגן ואינו מנוהל, ולכן הוא חשוף לכל נזקה פשוטה. בשנת 2020 בחנה יה"ב את האפשרות לספק למשרדי הממשלה מערכת מסרים מיידיים ממשלתית מאובטחת ומוצפנת מקצה לקצה, אולם פיתוח יישום זה לא קודם.

חויית המשתמש - העובדים: ממצאי הסקרים שבוצעו בתקופת החירום ובתקופת העבודה לפי הוראות התו הסגול³ מלמדים כי כשליש מהעובדים דיווחו שנתקלו בתקלות בחיבור מרחוק. עוד עולה מהממצאים כי יש צורך בקיום הדרכות לעובדים, על מנת לשפר את יכולת העבודה מרחוק ולהבטיח כי העבודה תתבצע ביעילות.



עם פרוץ משבר הקורונה, במרץ 2020, הייתה במשרדי הממשלה התשתית הנדרשת להתחברות מרחוק - 95% מהמשרדים ציינו כי הייתה גישה מרחוק לתשתיות ולמערכות התפעוליות אשר נדרשות לעובדים לשם המשך עבודה תקינה ורציפה. הפערים שהועלו נגעו בעיקר לצורך להרחיב את התשתיות ולהגדיל את מספר אמצעי החיבור מרחוק כדי לספק את הצרכים הנדרשים למספר הולך וגדל של עובדים מרחוק. ביולי 2020, כמה חודשים לאחר פרוץ המשבר, כבר חל שיפור ביכולתם של משרדי הממשלה לתמוך באופן העבודה האמור. משרד מבקר המדינה מציין לחיוב את ההתקדמות שחלה בהיערכות המשרדים לעבודה מרחוק ואת הבקרה שביצעה רשות התקשוב בנושא.

עיקרי המלצות הביקורת

מומלץ כי רשות התקשוב תגבש מדיניות תקשובית בנושא העבודה מרחוק, לאחר מיפוי של המצב הקיים, ניתוח צרכים והגדרה של המצב הרצוי, תוך זיהוי אתגרים והזדמנויות לטווח הקרוב והרחוק. מדיניות זו תשמש את משרדי הממשלה בבואם לבחון ולגבש מדיניות לטווח הארוך בנושא העבודה מרחוק ועשויה גם לסייע בידי נציבות שירות המדינה ומשרד האוצר לבחון את היתכנות היישום של מודל העבודה מרחוק באופן נרחב יותר בשירות המדינה.

מומלץ כי הגורמים הממשלתיים הרלוונטיים, ובכללם, משרד האוצר, רשות המסים, זרוע עבודה במשרד העבודה, הרווחה והשירותים החברתיים והמוסד לביטוח לאומי, יבחנו, בשיתוף ובתיאום עם משרד המשפטים, את הצורך בהסדרת היבטים הנוגעים למעבר שוק העבודה לעבודה מרחוק וליצירת תנאים המאפשרים את הרחבת העבודה מרחוק בכלל המשק. במסגרת הסדרת הנושא יש לתת את הדעת על סוגיות שונות, ובהן עיגון הזכויות

3 תיקון 7 לתקנות שעת חירום (הגבלת מספר העובדים במקום עבודה לשם צמצום התפשטות נגיף הקורונה החדש) התש"ף-2020, החלטת הממשלה 5037 (2.5.20).



והחובות של העובד והמעסיק, הכדאיות הכלכלית והחברתית של מודל עבודה זה והשפעותיו על מגזרי תעסוקה שונים.

על 21 משרדי הממשלה שטרם השלימו את גיבוש התוכנית להמשכיות עסקית להשלימה בהתאם להנחיות יה"ב; מומלץ כי רשות התקשוב תעקוב אחר יישום ההנחיה הייעודית שפורסמה בנובמבר 2020 בדבר היערכות להמשכיות עסקית ותפקודית במצב חירום, ובכלל זה בצורך במתן גישה מרחוק בזמן משבר.

מומלץ כי משרדי הממשלה ימשיכו לבסס בעיתות שגרה את התשתיות הנדרשות לעבודה מרחוק באופן שיבטיח מענה שלם וגמיש גם במצבי חירום שבהם יידרש לאפשר עבודה מרחוק יציבה ומאובטחת להיקף רחב יותר של עובדים ויגבשו תוכנית רכש שתספק את כל הצרכים הנדרשים לכך, בהתאם למדיניות שיקבעו המשרדים. מהלך זה נדרש במיוחד במשרדים שבהם נעשה שימוש בפתרונות זמניים על מנת לתת מענה מיידי במהלך משבר הקורונה.

לנוכח הרחבת היקף העבודה מרחוק בתקופת משבר הקורונה והתבונה כי העבודה מרחוק עשויה להיות חלק משגרת העבודה בעתיד, ולנוכח הסיכונים הטמונים במודל עבודה זה, מומלץ כי יה"ב תמשיך לפעול מול המשרדים על מנת שיעמדו בכלל בקרות אבטחת המידע המצוינות בהנחיותיה; תנחה את משרדי הממשלה להשלים את ביצועו של סקר סיכונים עדכני אשר במסגרתו הם יבחנו אילו שינויים חלו באופן עבודתם (עבודה מרחוק, שילוב מערכות חדשות, שינויים טכנולוגיים, שינויים בתהליכים עסקיים) ולבצע מבדקי חדירות שבמסגרתן ייבחן אף נושא החיבור מרחוק; תשלים את פיתוחה של מערכת מסרים ממשלתית ותטמיע את השימוש בה בהקדם.

מומלץ כי נציבות שירות המדינה תבחן בשיתוף משרדי הממשלה באילו נסיבות ניתן לבצע את העבודה מרחוק ברמת אפקטיביות מספקת יחסית לאפקטיביות של העבודה המבוצעת מהמשרד; וכן מומלץ לבחון אם כלי הבקרה שנקבעו בהנחיות נציבות שירות המדינה בתקופת הקורונה מספקים, ואם יש מקום לפתח כלים נוספים שייתנו מענה יעיל ונוח לעניין זה. כמו כן, מומלץ כי הגורמים הבוחנים את ההיתכנות של יישום נרחב יותר של מודל עבודה מרחוק בשירות המדינה - בנציבות שירות המדינה ובמשרד האוצר - יבחנו בין היתר גם את ההיבט הנוגע לסביבת העבודה בבית, תוך מתן הדעת על הצידוד הנדרש לעובד לשם ביצוע עבודתו מרחוק (כגון - חיבור אינטרנט מהיר, מחשב נייד או נייד, כיסא ארגונומי, מקלדת, אוזניות ומצלמות).

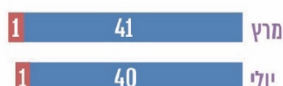


מידת המוכנות של משרדי הממשלה לעבודה מרחוק, לפי מספר המשרדים שהשיבו על כל אחת מהשאלות שבסקר, מרץ ויולי 2020

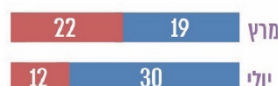
כן - לא - בתהליך -



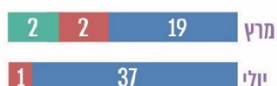
האם המערכות התפעוליות הנדרשות לעובדים אלו נגישות מרחוק?



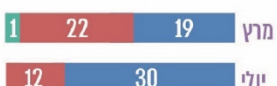
האם לכל העובדים הזקוקים לחיבור מרחוק יש מחשב נייד/נייח (או כל אמצעי חיבור אחר) המאפשר חיבור מרחוק?



האם המערכות עמדו בעומס ואיפשרו עבודה תקינה ורציפה?



האם בוצע ניסוי חיבור מרחוק בעומס?



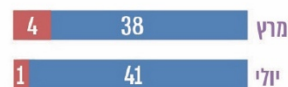
האם המערכות והתשתיות הדרושות של ה-IT נגישות מרחוק (שרתי ניהול, תקשורת, אחסון וכ"ב)?



האם בוצע ניסוי לבחינת יכולת תמיכה מרחוק (סיסטם)?



האם מוקד התמיכה של אגף טכנולוגיות דיגיטליות ומידע מסוגל לתת מענה מרחוק?





סיכום

משבר הקורונה הוא משבר עולמי מהבחינה הרפואית, הכלכלית והחברתית, אך הוא גם פותח פתח להזדמנויות. הסדרה לטווח הארוך של העבודה מרחוק לצד עבודה מהמשרד היא הזדמנות ליצור מציאות חדשה שתאפשר את ניצול היתרונות הגלומים במתכונת עבודה זו, תוך התמודדות עם האתגרים שהיא מציבה. הסדרה זו תאפשר למשרדי הממשלה לשפר את היערכותם להמשכיות תפקודית כדי שיוכלו להמשיך לספק שירותים ביעילות ובאופן המיטבי לאזרחי המדינה בעיתות שגרה וחירום, בפרט נוכח הצורך בהמשך ההתמודדות עם מגפת הקורונה וכהיערכות לאתגרים סביבתיים וגלובליים עתידיים.



ההיערכות התקשובית של משרדי הממשלה לעבודה מרחוק ויישומה במשבר הקורונה

מבוא

שוק העבודה עומד בפני אתגרים רבים, לרבות היערכות לשוק עבודה משתנה וגמיש, שיושפע בין היתר משינויים טכנולוגיים ודיגיטליים. אחד השינויים שיאפיינו את שוק העבודה העתידי, ומאפיינים את העבודה בתקופת הקורונה, הוא עבודה באמצעות התחברות מרחוק למערכות הממוחשבות של הארגון (להלן - עבודה מרחוק). במסגרת זו, עובדים רשאים לבצע על בסיס קבוע מטלות שוטפות מרחוק (מהבית או מכל אתר אחר שאינו משמש מקום העבודה המרכזי).

עבודה מרחוק: תועלות, חסרונות ואתגרים: לעבודה מרחוק יש כמה תועלות בתחומים שונים. עם זאת, היא מציבה מגוון אתגרים לעובדים ולמעסיקים. להלן כמה דוגמאות לתועלות, לחסרונות ולאתגרים הכרוכים בעבודה מרחוק:



תרשים 1: דוגמאות לתועלות, חסרונות ואתגרים הטמונים בעבודה מרחוק

תועלות בעבודה מרחוק

-  **תועלת סביבתית**
צמצום זיהום אוויר ממקורות תחבורתיים
-  **תועלת כלכלית**
הקטנת נזקי גודש בתחבורה, הגדלת הפריזון במשק
-  **תועלת חברתית**
העסקת אוכלוסיות שהיו מודרות משוק העבודה בגלל קשיי נגישות (כגון - אנשים עם מוגבלויות, אנשים המתגוררים בפריפריה)
-  **תועלת למעסיק**
חיסכון במשאבים, הפחתת הגורמים המסיחים
-  **תועלת לעובד**
חיסכון בזמן ובהוצאות נסיעה, עלייה בשביעות הרצון, יכולת לאזן בין משפחה לעבודה, שיפור באיכות החיים
-  **תועלת במצבי חירום**
שמירה על רציפות תפקודית במצבי חירום בהם יש מגבלות על הגעה למקום העבודה

חסרונות ואתגרים בעבודה מרחוק

-  **קשיים בבקרה**
קושי בפיקוח על עובדים
-  **בידוד חברתי**
צמצום האינטראקציה החברתית בין עובדים שמתקיימת כאשר הם נמצאים במשרד; היעדר ממשקים בין-אישיים; תחושת בדידות; פגיעה בעבודת הצוות
-  **מדיניות סלקטיבית והעמקת פערים**
היכולת לעבוד מרחוק מוגבלת לתחומים ספציפיים ודורשת משאבים מתאימים. הנהלים מהאפשרות לעבוד מרחוק הם בעיקר העובדים החזקים יותר בשוק העבודה (בעלי השכלה גבוהה ועובדים עם רמות שכר גבוהות). העובדים החלשים יותר בשוק העבודה מועסקים לרוב במשרות שאינן ניתנות לביצוע מרחוק
-  **טשטוש הגבולות וההפרדה בין שעות העבודה לשעות הפנאי**
גלישה לעבודה בשעות לא שגרתיות
-  **סיכוני אבטחת מידע והגנת הפרטיות**
גישה מרחוק מעצימה את הסיכונים עקב קושי בשליטה על פעילות מחוץ לחצרות הארגון, הדבר בא לידי ביטוי באיומים כגון התחזות, ציטוט לתעבורה, זליגת מידע



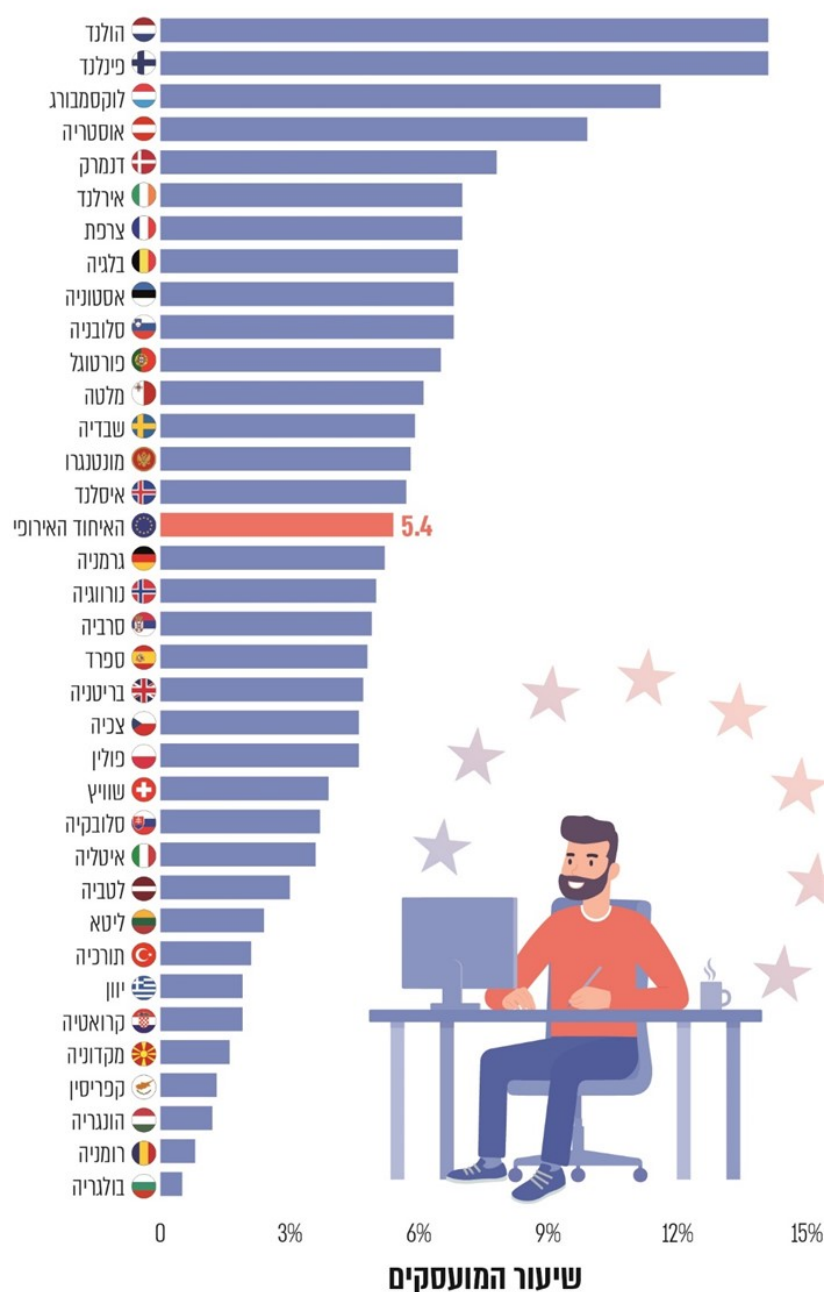
בהקשר התחבורתי והסביבתי, עבודה מרחוק היא אחד הכלים שיש בהם כדי להקל את העומס בכבישים באמצעות צמצום הנסיעות. על פי נתונים שפרסם משרד האוצר בדוח מפרברואר 2020⁴, כ-60% מהעובדים במשק בישראל מגיעים למקום העבודה ברכבם הפרטי; בתחום זה חלה מגמת עלייה מהירה מקצב הגידול בתשתיות, והדבר גורם להתמשכות זמן הנסיעה לעבודה, להתמעטות שעות הפנאי וכן לפגיעה באיכות החיים של התושבים ובפריון העבודה. בדוח צוין כי "מגמות אלו מביאות לאי-מיצוי הפוטנציאל של התוצר המקומי הגולמי ושל ההכנסות ממסים, לזיהום אוויר ולמפגעי רעש". לפי נתוני הדוח, הנזק הכלכלי הנגרם מעומסי התנועה בישראל מוערך בעשרות מיליארדי דולרים וצפוי להחמיר.

עבודה מרחוק בעולם: במדינות רבות בעולם מיושמת כיום מדיניות המעודדת עבודה מרחוק. לדוגמה, בארה"ב, בהתאם לחוק ממשלתי⁵, כל הסוכנויות הממשלתיות מחויבות לגבש תוכניות ליישום עבודה מרחוק ולעודד את השימוש בה. בשנת 2010 העביר הקונגרס האמריקני החלטה להגדלת היקף העבודה מרחוק במשרדים ובסוכנויות ממשלתיות, והנתונים לשנת 2018 מעידים כי 22% מהעובדים במוסדות האמורים עבדו בגישה מרחוק לפחות בחלק מהזמן⁶. באיחוד האירופי נחתם בשנת 2002 הסכם מסגרת בין ארגוני הגג של המעסיקים והעובדים להסדרת נושא העבודה מרחוק⁷. אימוץ ההסכם לא התבצע באופן זהה בכל מדינות האיחוד (בחלק מהן הוא התקבל כהסכם וולונטרי, באחרות כהסכם בפיקוח המדינה, ויש מדינות שבהן הוא הוסדר באמצעות חקיקה). להלן נתונים לשנת 2019 על שיעור המועסקים שעבדו מרחוק בדרך כלל במדינות האיחוד האירופי⁸:

- | | |
|---|---|
| 4 | משרד האוצר, אגף השכר והסכמי עבודה, דין וחשבון על הוצאות השכר בשירות המדינה וגופי הביטחון לשנת 2018 (פברואר 2020). |
| 5 | The Telework Enhancement Act of 2010 |
| 6 | Status of Telework in the Federal Government - Report to Congress, Fiscal Year 2018 OPM.GOV MARCH 2020 |
| 7 | European cross-sector social partners, <i>framework agreement on telework</i> 2002 |
| 8 | https://ec.europa.eu/eurostat/web/products-eurostat-news/-/DDN-20200424-1 |
- באיחוד האירופי חברות 27 מדינות. בריטניה עזבה את האיחוד ב- 31.1.20.



תרשים 2: שיעור המועסקים (באחוזים) שבדרך כלל עובדים מהבית, במדינות שונות באיחוד האירופי, 2019:



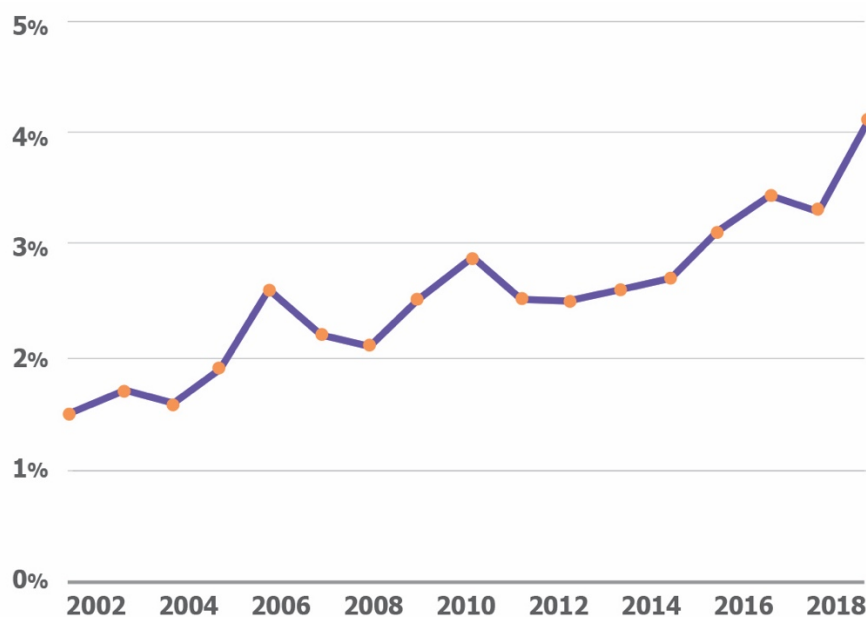
המקור: נתוני האיחוד האירופי בעיבוד משרד מבקר המדינה.



כעולה מהתרשים, בשנת 2019, לפי נתוני האיחוד האירופי, 5.4% מהמועסקים במדינות האיחוד האירופי (שהיו בגילאי 15-64), עבדו בדרך כלל מהבית.

עבודה מרחוק בישראל (טרם משבר הקורונה): בשנים האחרונות חל גידול בשיעור העובדים מרחוק במדינות שונות. מגמה זו ניכרת גם בישראל - בין השנים 2005 ל-2018 חל גידול בשיעור העבודה מרחוק בישראל, מכ-2% בשנת 2008 לכ-4% בשנת 2018:

תרשים 3: שיעור העובדים מהבית מקרב העובדים בישראל, 2002-2018:



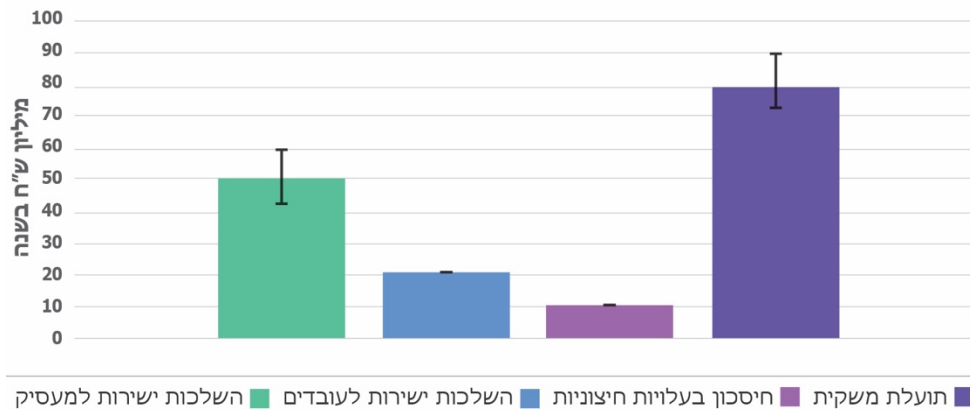
המקור: אגף השכר והסכמי עבודה במשרד האוצר, **דוח על הוצאות השכר בשירות המדינה וגופי הביטחון לשנת 2018** (פברואר 2020).

מחקר בנושא הפחתת השימוש ברכבים פרטיים בקרב המגזר הציבורי שבוצע עבור המשרד להגנת הסביבה בדצמבר 2018 בחן בין היתר את התועלת הצפויה בעבודה מרחוק בקרב שירות המדינה⁹. האומדן שבוצע התייחס להשלכות ישירות למעסיק: חיסכון בהוצאות המשרדים, חיסכון בעלויות חנייה, תועלת מעלייה בפרודוקטיביות; להשלכות ישירות לעובדים: חיסכון בעלויות נסיעה (לרבות עלויות דלקים), חיסכון בזמני הגעה; ולחיסכון בעלויות חיצוניות מזיהום אוויר, גודש, רעש ותאונות דרכים. האומדן העלה כי מתן אפשרות לכ-22% מקרב עובדי שירות המדינה לעבוד 15% משעות התקן שלהם בבית יביא לחיסכון למשק של כ-80 מיליון ש"ח בשנה, כמתואר בתרשים להלן:

9 אקוטרירדס בע"מ (הוכן עבור המשרד להגנת הסביבה), **הפחתת השימוש ברכבים פרטיים בקרב המגזר הציבורי**, (דצמבר 2018), עמ' 44-51.



תרשים 4: סיכום כלל התועלת נטו הצפויה מיישום עבודה מרחוק בקרב עובדי שירות המדינה בישראל



- האומדן מתבסס על מתן אפשרות ל- 22% מקרב עובדי שירות המדינה לעבוד 15% משעות התקן שלהם בבית.

המקור: אקווריידס בע"מ (הוכן עבור המשרד להגנת הסביבה), הפחתת השימוש ברכבים פרטיים בקרב המגזר הציבורי, (דצמבר 2018).

במחקר צוין כי פוטנציאל התועלת מיישום אפשרות העבודה מרחוק בקרב כלל עובדי המגזר הציבורי עומד על כ- 850 מיליון ש"ח בשנה.

בשנים עברו היקף העבודה מרחוק של עובדי משרדי הממשלה היה מצומצם יחסית. משרדי הממשלה איפשרו לעובדים לעבוד מרחוק בתנאים מסוימים. במסגרת זו הופעלו במשרדי הממשלה מודלים מסוימים לעבודה מרחוק¹⁰, כגון מודל המיושם ברשות הפטנטים שבמסגרתו בוחני פטנטים מבצעים את עבודתם מרחוק כיומיים בשבוע, זאת בהמשך לפיילוט מבוקר שיושם ברשות הפטנטים¹¹. כמו כן, במסגרת יישום המלצות דוח הוועדה לקידום נשים בשירות המדינה (ועדת שטאובר)¹², וכדי לסייע בהשגת השוויון המגדרי מיושם בשירות המדינה החל משנת 2016 מודל, במסגרת פיילוט, המאפשר עבודה של שעות נוספות מהבית לעובדים במשרת הורה העומדים בכמה תנאים (יצוין כי הוא אינו מחליף את ההגעה הפיזית למקום העבודה בשעות הרגילות).

10 משרד האוצר, אגף השכר והסכמי עבודה, **דין וחשבון על הוצאות השכר של הגופים הציבוריים לשנת 2018** (יוני 2020).

11 רשות הפטנטים שבמשרד המשפטים ביצעה בשנת 2012 פיילוט להעסקת בוחני פטנטים מרחוק כדי לשפר את יכולתה לגייס עובדים. בשנת 2014 הוחלט למסד את נושא העבודה מרחוק כהסדר קבוע ברשות הפטנטים.

12 דוח הוועדה לקידום נשים בשירות המדינה בראשות דלית שטאובר (2014).



מדינת ישראל טרם גיבשה מדיניות ממשלתית כוללת בנושא העבודה מרחוק בשירות המדינה, על כל היבטיו של הנושא והמשתמע ממנו. היתכנות של הרחבת היקף היישום של המודל לעבודה מרחוק בשירות המדינה נמצאת בבחינה בצוות משותף של אגף השכר והסכמי עבודה במשרד האוצר ואגף בכיר לתכנון, אסטרטגיה ומדיניות בנציבות שירות המדינה.

עבודה מרחוק בארץ ובעולם בתקופת משבר הקורונה: חשיבות היכולת לעבוד מרחוק גוברת במצבי חירום כגון - מלחמה, רעידת אדמה, פנדמיה (מגפה עולמית), שרפה נרחבת, אירוע מזג אוויר חריג, מתקפות סייבר - שעלולים להקשות על העובדים להגיע למקום עבודתם.

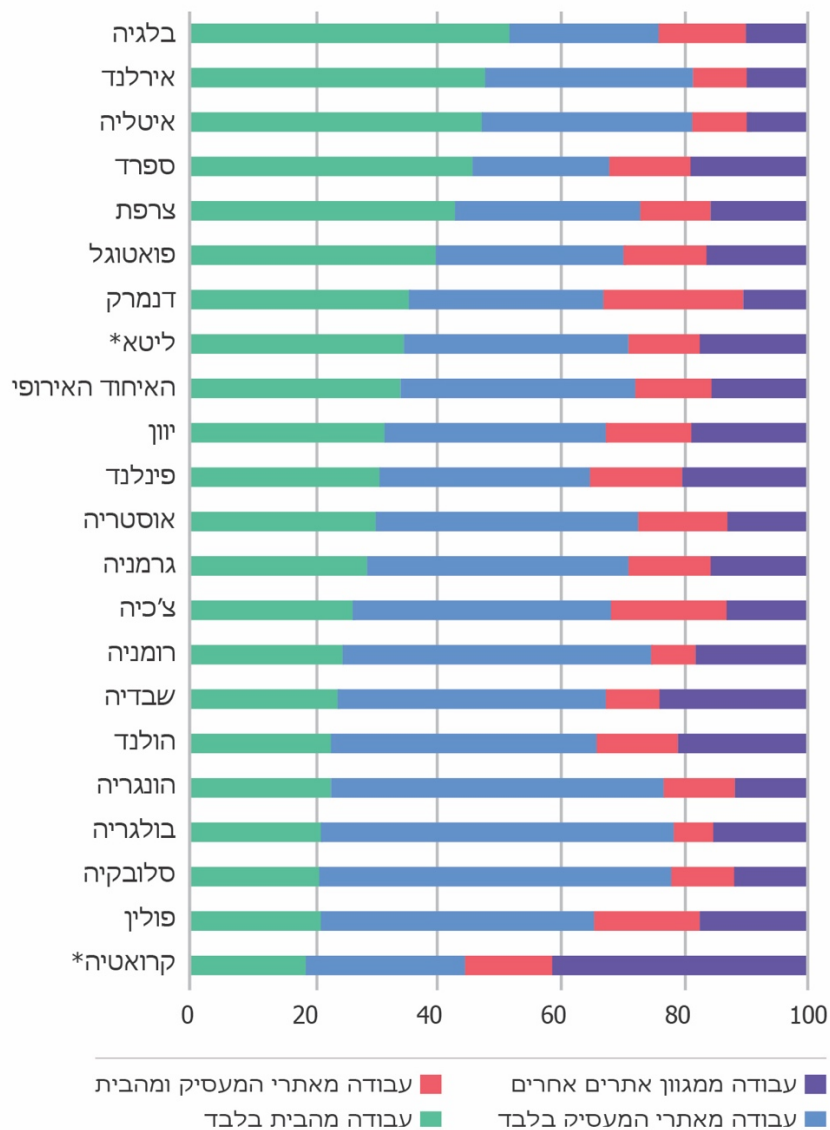
בסוף דצמבר 2019 התפרץ בסין נגיף הקורונה (SARS-COV-2), שגורם למחלת COVID-19 (מחלת הקורונה). מאמצע פברואר 2020 התפשט הנגיף למדינות רבות, וב-11.3.20 הכריז ארגון הבריאות העולמי על המחלה כמגפה עולמית (פנדמיה). בהתאם לכך מדינות שונות, לרבות ישראל, קבעו הוראות הנוגעות בין היתר לשמירה על ריחוק חברתי. בעקבות כך ארגונים שונים, ובכלל זה משרדי ממשלה, נדרשו לאפשר לעובדיהם עבודה בחיבור מרחוק, כדי להבטיח רציפות תפקודית ומתן שירותים לאזרחים תוך שמירה על אבטחת המידע הנדרשת.

הנתונים מלמדים כי במהלך משבר הקורונה היקף העבודה מרחוק גדל במידה ניכרת במדינות שונות. סקרים שבוצעו במדינות האיחוד האירופי מלמדים כי ביולי 2020 כמעט מחצית (48%) מהעובדים שילבו בין עבודה מהבית לבין עבודה מאתרי המעסיק (כגון מהמשרד) וכשליש (34%) מהעובדים ביצעו את כל עבודתם מהבית¹³.

להלן נתונים על התפלגות העבודה מהבית או מאתרי המעסיק בתקופת מגפת הקורונה במדינות האיחוד האירופי:



תרשים 5: מועסקים - מקום ביצוע העבודה במהלך מגפת הקורונה, במדינות האיחוד האירופי, (באחוזים)



הערות שהובאו במקור - האיחוד האירופי:

* מהימנות נמוכה.

לא הוצגו תוצאות לגבי כמה מדינות שהנתונים שלהן לא היו מבוססים על מספר מספק של מקרים לצורך הפקת תוצאות סטטיסטיות מהימנות. מדינות אלה הן: קפריסין, אסטוניה, לטביה.

המקור: Living, working and COVID-19, COVID-19 series, Publications Office of the European Union, Luxembourg, 28 September 2020



גם בישראל, על רקע התפרצות נגיף הקורונה, ובפרט עם כניסתן לתוקף של תקנות שעת חירום בדבר הגבלת מספר העובדים במקום העבודה, גדל מספר העובדים מרחוק¹⁴. מנתוני הלמ"ס מאפריל 2020¹⁵ עולה כי 38% מהעסקים דיווחו כי הם מאפשרים עבודה מהבית (רובם עסקים בענפי ההיי-טק, השירותים הפיננסיים ושירותים מקצועיים וטכניים); כ-47% מבין העסקים שאפשרו עבודה מהבית דיווחו כי היא אפקטיבית "במידה רבה" ו"רבה מאוד".

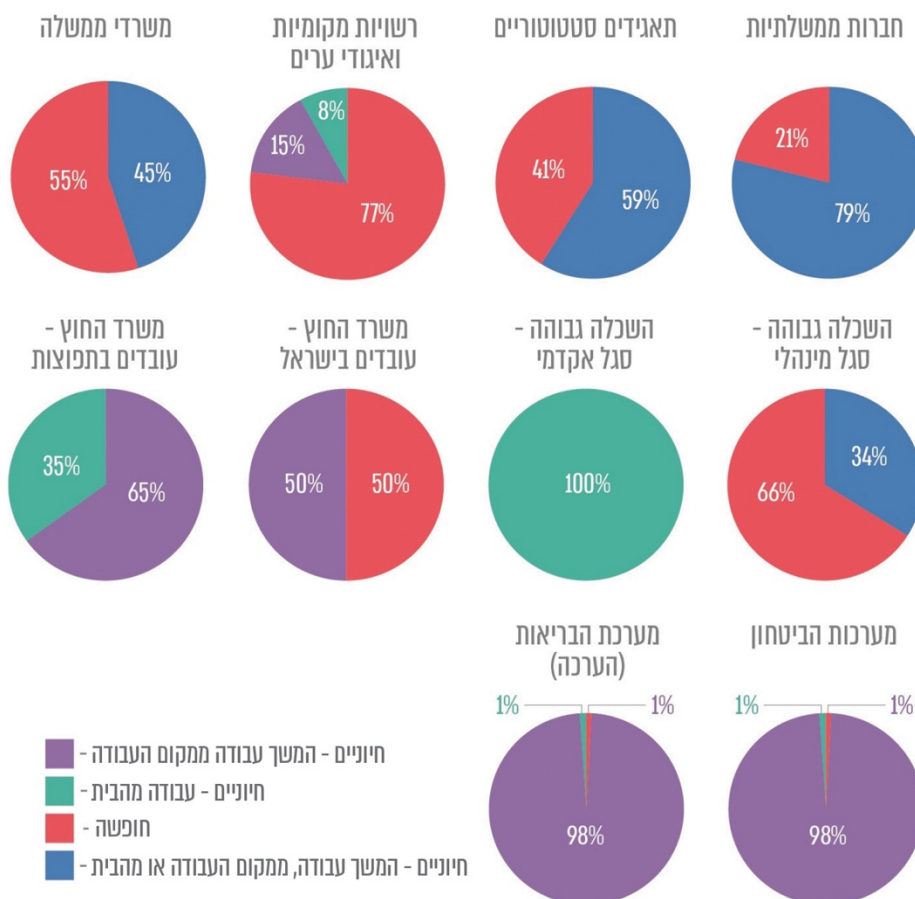
המגזר הציבורי בישראל (המונה כ-730 אלף עובדים)¹⁶, ובכלל זאת משרדי הממשלה, נערך אף הוא למתכונת חירום ובמסגרת זו למעבר של חלק מהעובדים לפלטפורמה של עבודה מהבית. בתחילת המשבר, מ-22 במרץ 2020 עד 30 באפריל אותה שנה, העבודה בוצעה באמצעות מצבת כוח אדם מצומצמת אשר הוגדרה כחיונית (להלן - תקופת החירום)¹⁷. בהמשך, בתחילת מאי 2020, בוטלה החלוקה לעובדים חיוניים ושאינם חיוניים, ועובדי משרדי הממשלה שבו לעבודתם, על פי הגבלות שנקבעו בהוראות התו הסגול¹⁸ (להלן - תקופת הוראות התו הסגול) באופן המשלב בין עבודה מן המשרד לבין עבודה מרחוק.

ביוני 2020 פרסם משרד האוצר ממצאים של סקר שביצע בנוגע לעבודת המגזר הציבורי בתקופת החירום (בחודשים מרץ-אפריל 2020), לפי תת-מגזרים¹⁹:

- 14 תקנות שעת חירום (הגבלת מספר העובדים במקום העבודה לשם התפשטות נגיף הקורונה החדש), התש"פ-2020.
- 15 הלשכה המרכזית לסטטיסטיקה, **ממצאי סקר מצב העסקים בעת התפשטות נגיף הקורונה**, (אפריל 2020).
- 16 המגזר הציבורי בישראל מורכב מעובדי שירות המדינה (משרדי ממשלה, בתי חולים ממשלתיים ומערכת החינוך הממשלתית), גופי הביטחון, תאגידים שהוקמו בחוק, רשויות מקומיות, גופים נתמכים וחברות ממשלתיות. אוכלוסייה זו של גופים מתוקצבים באופן ישיר ונתמכים באופן עקיף מונה יחד כ-730,000 עובדים. הממונה על השכר במשרד האוצר אמון על פיקוח על השכר שלהם. לצד קבוצה זו, יש עובדים נוספים במגזר הציבורי שאינם כפופים לסמכותו של הממונה על השכר: שופטים, עובדי הכנסת ונבחרי ציבור ששכרם נקבע בוועדת הכספים בכנסת, ועובדי משרד מבקר המדינה. מקור: משרד האוצר, אגף השכר והסכמי עבודה, דין וחשבון על הוצאות השכר בשירות המדינה ועובדי גופי הביטחון, לשנת 2019 (2021), עמ' 12.
- 17 יצוין כי ב-19.4.20 אושר על פי החלטת הממשלה 4996 להחליף 25% מעובדי המשרד החיוניים בעובדים אחרים. בהמשך, ב-25.4.20, תוקנו התקנות לשעת חירום באופן שמכסת העובדים החיוניים לתקופת החירום גדלה מ-35% ל-45% מעובדי המשרד. כמו כן, ניתנה למשרדים האפשרות לשנות את הרכב העובדים הנכללים ברשימת העובדים החיוניים.
- 18 תיקון 7 לתקנות שעת חירום (הגבלת מספר העובדים במקום עבודה לשם צמצום התפשטות נגיף הקורונה החדש) התש"פ-2020, החלטת הממשלה 5037 (2.5.20).
- 19 אגף שכר והסכמי עבודה - משרד האוצר, **דין וחשבון על הוצאות השכר של הגופים הציבוריים לשנת 2018** (יוני 2020), עמ' 15.



תרשים 6: המשך עבודה או יציאה לחופשה במגזר הציבורי במהלך תקופת החירום, מרץ-אפריל 2020



המקור: נתוני אגף שכר והסכמי עבודה - משרד האוצר, מתוך **דין וחשבון על הוצאות השכר של הגופים הציבוריים לשנת 2018**, (יוני 2020), בעיבוד משרד מבקר המדינה.



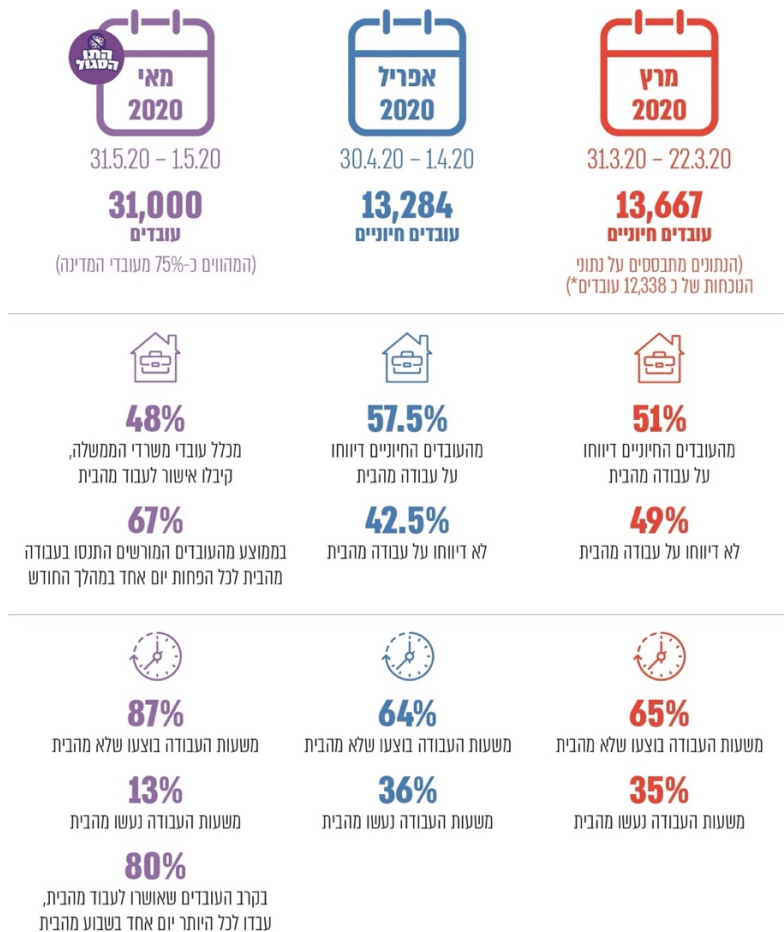
לסקטורים שונים במגזר הציבורי יש צרכים ומאפיינים שונים, דבר המשליך על יכולתם לעבוד מרחוק. מהנתונים עולה כי היו קיימים הבדלים ניכרים בין סקטורים בתוך המגזר הציבורי בכל הנוגע לשיעור העובדים שהוגדרו חיוניים בתקופת החירום (מרץ - אפריל 2020) וכן בנוגע לשיעור העובדים מהבית. כך למשל עובדי מערכת הביטחון ומערכת הבריאות²⁰ הוגדרו ברובם המוחלט כעובדים חיוניים ועבדו במקום עבודתם (ולא מהבית); הסגל האקדמי במערכת ההשכלה הגבוהה הוגדר כולו כחיוני ועבד מהבית, בעוד הסגל המינהלי במוסדות להשכלה גבוהה הוצא בחלקו לחופשה (66%). במשרדי הממשלה 55% מהעובדים הוצאו לחופשה ו-45% מהעובדים עבדו תוך שילוב בין עבודה מהבית לבין עבודה מהמשרד.

במשרדי הממשלה ויחידות הסמך מועסקים כ-40,000 עובדים²¹. העבודה מרחוק במשרדי הממשלה וביחידות הסמך בתקופת משבר הקורונה התבצעה בהתבסס על הנחיות נציב שירות המדינה והממונה על השכר המפרטות, בין היתר, את התנאים לאישור עבודה מהבית²². נתוני נציבות שירות המדינה, כפי שפורסמו בכמה דוחות²³, מלמדים כי שיעור ניכר מהעובדים התנסו בעבודה מרחוק במהלך משבר הקורונה (הן בתקופת החירום והן בתקופת העבודה לפי הוראות התו הסגול):

- 20 יצוין כי בתקנות לשעת חירום הוחרגה מערכת הבריאות הממשלתית באופן שמגבלת ההגעה למקום העבודה לא חלה על בתי החולים.
- 21 נציבות שירות המדינה, **דוח חמישי - "תמונת מצב - עבודת עובדי המדינה בהתאם להוראות 'התו הסגול'" - עבודת עובדי המדינה מהבית בחודש מאי 2020** (יולי 2020), עמ' 2.
- 22 נציב שירות המדינה והממונה על השכר והסכמי עבודה במשרד האוצר, **הנחיה לעבודת עובדי המדינה במתכונת חירום** (מרץ 2020); נציב שירות המדינה והממונה על השכר והסכמי עבודה במשרד האוצר, **הנחיה בדבר עבודה מהבית - מעבר לעבודה בהתאם להוראות התו הסגול** (1.5.20).
- 23 נציבות שירות המדינה, **דוח שלישי - תמונת מצב הון אנושי בשירות המדינה - עבודת עובדי המדינה מהבית בתקופת הקורונה**, (מאי 2020); **דוח רביעי - תמונת מצב הון אנושי בשירות המדינה - עבודת עובדי המדינה מהבית בחודש אפריל 2020** (יוני 2020) **דוח חמישי - תמונת מצב בהתאם להוראות "התו הסגול" - עבודת עובדי המדינה מהבית בחודש מאי 2020** (יולי 2020).



תרשים 7: היקף העבודה מרחוק במשרדי הממשלה במהלך תקופת החירום (22.3.20 - 30.4.20) ובמאי 2020 - עבודה לפי הוראות התו הסגול



מקור: נתוני נציבות שירות המדינה בדוחות שונים, בעיבוד משרד מבקר המדינה.

* נציבות שירות המדינה ציינה כי מסיבות טכניות, מתוך כלל דיווחי הנוכחות של העובדים החיוניים שעבדו במרץ 2020 נשלפו דיווחי הנוכחות של כ-12,338 עובדים, ובהתבסס על כך הוצגו הנתונים שמופיעים בתרשים.

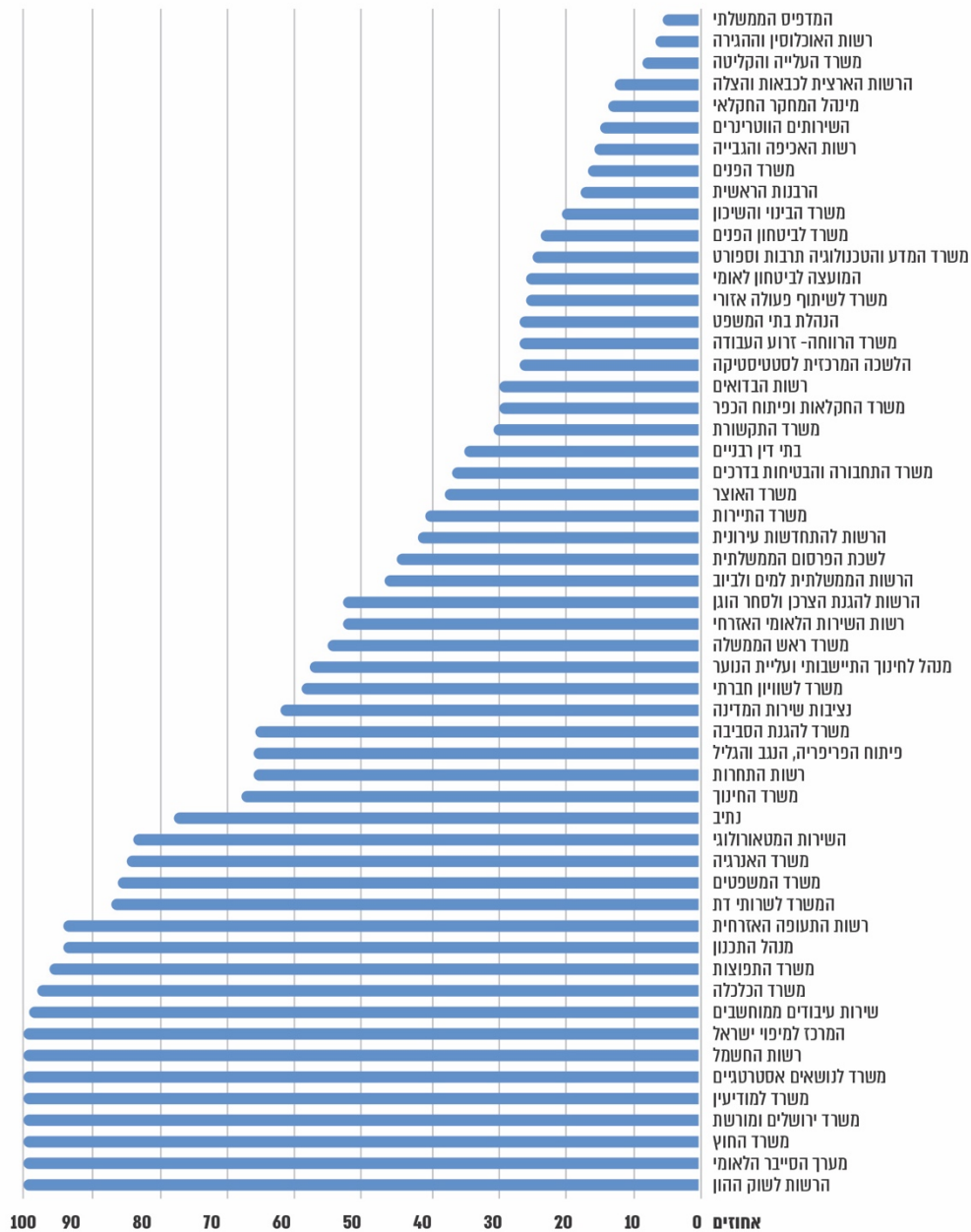
הערה כללית: נתוני נציבות שירות המדינה מתבססים על נתונים שנשלפו ממערכת הנוכחות במרכז"ה, ועל כך אינם כוללים את נתוני רשות המיסים - מכס ומע"מ ומס הכנסה ואת נתוני זרוע הרווחה במשרד העבודה, הרווחה והשירותים החברתיים, זאת מכיוון שמשרדים אלה אינם מדווחים על נוכחות במערכת מרכז"ה (מערכת רוחבית כוללת במשרדי הממשלה - לניהול רכש, כוח אדם ומשאבים לוגיסטיים)



מנתוני נציבות שירות המדינה עולה כי בתקופת החירום כ-51%-57% מהעובדים החיוניים במשרדי הממשלה עבדו מהבית, כאשר בחודש אפריל 2020 חלה עלייה של 6% בשיעור העובדים מהבית לעומת שמונת ימי העבודה בחודש מרץ 2020. עם זאת, על אף הגידול בשיעור העובדים החיוניים שהתנסו בעבודה מהבית, נראה כי לא היה שינוי בחלוקת העבודה בין הבית למשרד. מהנתונים עולה עוד כי במהלך חודש מאי 2020, בו העבודה במשרדי הממשלה התבצעה על בסיס הוראות התו הסגול, 48% מכלל עובדי משרדי הממשלה קיבלו אישור לעבוד מהבית (80% מהם עבדו עד יום אחד מהבית) וכי 13% משעות העבודה נעשו מהבית.



תרשים 8: נתוני נציבות שירות המדינה אודות שיעור העובדים המורשים לעבוד מרחוק, בחלוקה למשרדים, בחודש מאי 2020

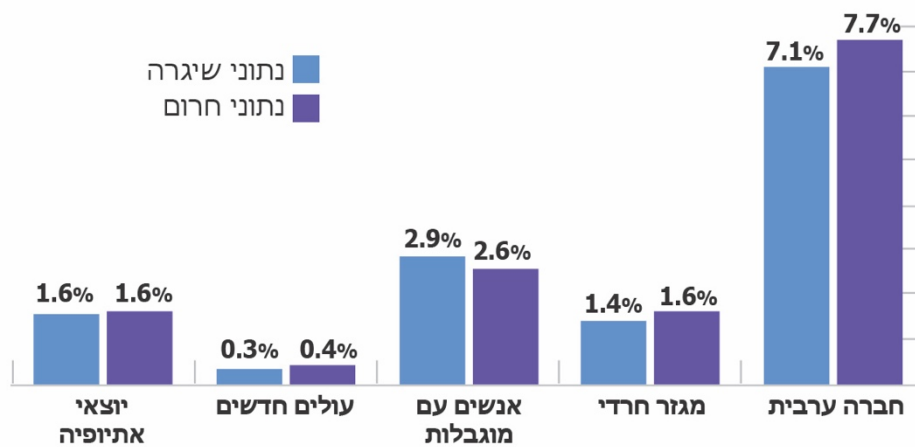


מקור: דוח חמישי - תמונת מצב בהתאם להוראות "התו הסגול" - עבודת עובדי המדינה מהבית בחודש מאי 2020 (יולי 2020).



גיוון תעסוקתי בתקופת הקורונה - נציבות שירות המדינה מסרה למשרד מבקר המדינה כי בתקופת החירום נקטה צעדים לשמירת הגיוון התעסוקתי, בהם פרסום הנחיית נציב שירות המדינה, באפריל 2020, בדבר ייצוג מגוון קבוצות באוכלוסייה הישראלית במוקדי קבלת ההחלטות בתקופת משבר²⁴. להלן נתונים אודות העסקת עובדים מרקע מגוון בתקופת החירום בהשוואה לתקופת שגרה²⁵:

תרשים 9: ייצוג עובדים חיוניים מרקע מגוון בשירות המדינה בזמן משבר הקורונה, ינואר - מרץ 2020²⁶



מקור: נציבות שירות המדינה, **מגוונים את שירות המדינה - דוח גיוון וייצוג בשירות המדינה לשנת תשע"ח-תשע"ט**, (מאי 2020), עמ' 14 - 17.

מהתרשים עולה כי מקרב העובדים שהוגדרו חיוניים - ייצוגם של עובדים מרקע מגוון בתקופת החירום היה דומה לייצוגם בשגרה.

היקף העבודה מרחוק לפי מגדר: מנתוני נציבות שירות המדינה בנוגע לעבודת העובדים החיוניים במהלך חודש אפריל עולה כי בין העובדים שניצלו את האפשרות לעבוד מהבית היו יותר נשים בצורה משמעותית, וכי מקרב הגברים היו עובדים רבים שלא ניצלו את האפשרות, הגם שחלקם עמדו בכללים שמאפשרים עבודה מהבית.

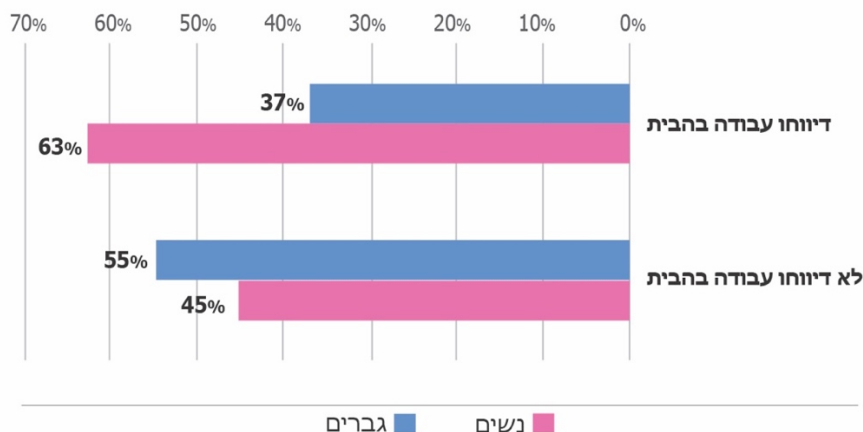
24 נציבות שירות המדינה, **הנחיה 03.23 של נציב שירות המדינה: ייצוג המגוון הישראלי במוקדי קבלת ההחלטות** (אפריל 2020).

25 נציבות שירות המדינה, **מגוונים את שירות המדינה - דוח גיוון וייצוג בשירות המדינה לשנת תשע"ח-תשע"ט**, (מאי 2020), עמ' 14 - 17.

26 שם, עמ' 15.



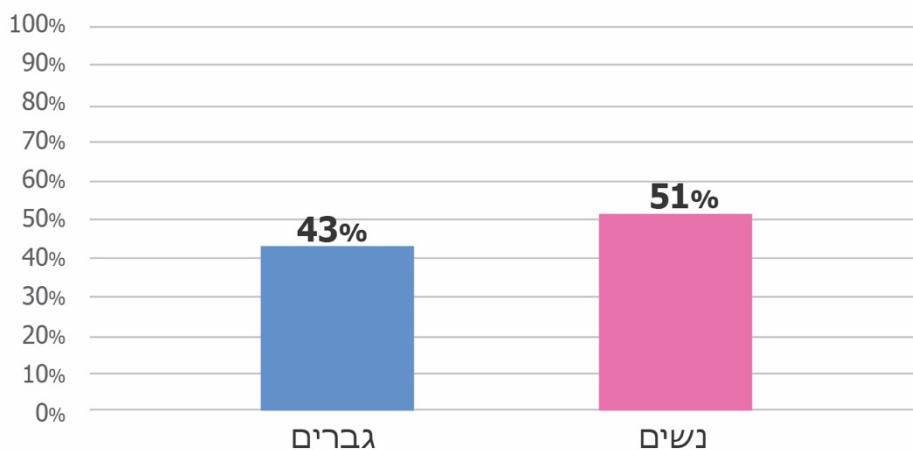
תרשים 10: התפלגות מגדרית בדיווחי העבודה מהבית, אפריל 2020



מקור: דוח רביעי - תמונת מצב הון אנושי בשירות המדינה - עבודת עובדי המדינה מהבית בחודש אפריל 2020 (יוני 2020).

באשר לעבודה במהלך חודש מאי, בו העבודה מרחוק נעשתה בהתאם להוראות התו הסגול, מנתוני נציבות שירות מדינה עולה כי שיעור הנשים שאושרו לעבודה מהבית היה גדול משיעור הגברים, וחלקה של העבודה מהבית מתוך כלל שעות העבודה היה גדול יותר בקרב נשים אלה (כ-29% לעומת 21% בקרב העובדים הגברים).

תרשים 11: שיעור המורשים לעבודה מהבית בחלוקה מגדרית, מאי 2020



מקור: דוח חמישי - תמונת מצב בהתאם להוראות "התו הסגול" - עבודת עובדי המדינה מהבית בחודש מאי 2020 (יולי 2020).



עבודה מרחוק - היבטים תקשוביים: בהיבט התקשובי, המעבר לעבודה מרחוק במשרדי הממשלה דורש בין היתר קביעת מדיניות ונהלים, הקצאת תשתיות ופתרונות טכנולוגיים שיאפשרו לעובד חיבור לרשת המשרדית ומתן אפשרות עבודה מרחוק, תוך שמירה על רמת אבטחת המידע הנדרשת. זאת כדי לאפשר את המשכיות העבודה, מתן שירותים לאזרחים ולעסקים וכן תמיכה בשירותים ממשלתיים דיגיטליים בערוצים שונים.

תרשים 12: עולם העבודה מרחוק - היבטים תקשוביים



יצוין כי אחד הגורמים שיש לו השפעה ניכרת על יכולת העבודה מרחוק הוא פריסת תשתיות תקשורת, ובפרט תשתיות מתקדמות - תשתיות פס רחב. פריסת תשתיות מתקדמות ואיכותיות מגדילה את האפשרות לעבוד מהבית או ממקום מרוחק מהמשרד. לפי נתוני משרד התקשורת²⁷, נכון לאפריל 2020 נפרשו רשתות סיבים אופטיים המשמשות כ-25% ממשקי הבית בישראל.

משבר הקורונה הביא להרחבת היקף העבודה מרחוק ולהעלאת תובנות לפיהן העבודה מרחוק צפויה להתרחב בשנים הבאות²⁸; בספרות המקצועית צוין כי העבודה מרחוק אינה רק כלי להתמודדות עם משבר חולף או עם מצב חירום זמני, למעשה העבודה מרחוק תהפוך להיות

27 דוח הצוות הבין-משרדי לבחינת מדיניות פריסת תשתיות תקשורת אולטרה רחבות-פס ניידות במדינת ישראל, יולי 2020.

28 OECD, Productivity gains from teleworking in the post COVID-19 era: how can public policies make it happen? (2020)



חלק מהשגרה בעולם העבודה העתידי. מציאות עתידית זו מכונה במחקרים "השגרה החדשה" (The Next Normal)²⁹. דבר זה יבוא לידי ביטוי, בדרך זו או אחרת, גם בשירות הציבורי בישראל.

פעולות הביקורת

בחודשים מאי 2020 - פברואר 2021 בדק משרד מבקר המדינה היבטים הנוגעים להיערכות התקשובית של משרדי ממשלה לעבודה מרחוק ויישומה בתקופת משבר הקורונה. הביקורת נעשתה ברשות התקשוב הממשלתי שבמשרד הדיגיטל הלאומי. בדיקות השלמה נעשו בחמישה משרדי ממשלה: במשרד הפנים, במשרד התחבורה והבטיחות בדרכים (להלן - משרד התחבורה), במשרד המדע והטכנולוגיה (להלן - משרד המדע)³⁰, במשרד המשפטים ובמשרד להגנת הסביבה - (להלן - המשרדים שנבדקו פרטנית בביקורת); בנציבות שירות המדינה, במשרד האוצר ובמערך הסייבר הלאומי במשרד ראש הממשלה (להלן - מערך הסייבר הלאומי).

הביקורת בוצעה בתקופת משבר הקורונה על מנת להציג את תמונת המצב לגבי היערכות משרדי הממשלה לעבודה בגישה מרחוק במשבר הקורונה, לשקף אילו פערים היו קיימים עם פרוץ המשבר ואילו צעדים ננקטו כדי לגשר על אותם פערים. זאת כדי לעמוד על פעולות נוספות שיש לשקול במסגרת ההיערכות לעבודה מרחוק בטווח הארוך, בשים לב למגמות שיאפיינו את שוק העבודה העתידי ולצורך להיות ערוכים למשברים נוספים שיחייבו עבודה מרחוק בהיקף משמעותי.

גיבוש מדיניות תקשובית לעבודה מרחוק

בשנים האחרונות הולכת ומתרחבת מתכונת העבודה מרחוק במדינות שונות ובכלל זה בישראל, לרבות במשרדי הממשלה וביחידות הסמך. כדי להבטיח יכולת עבודה מרחוק, יש להיערך לכך הן באמצעות גיבוש מדיניות, הנחיות ונהלים לעבודה מרחוק והן באמצעות הקמת תשתית שתאפשר עבודה מרחוק ותתמוך בכך.

בהחלטת הממשלה משנת 2014³¹ נקבע כי רשות התקשוב תנחה את אגפי מערכות המידע במשרדי הממשלה ויחידות הסמך, תקדם משילות בתחום התקשוב בממשלה, תטמיע מתודולוגיות וסטנדרטים רוחביים ותפעל לפיתוח תשתיות, מערכות ושירותים לייעול עבודת הממשלה ולהנגשת מידע ושירותים ממשלתיים לציבור. כמו כן, נקבע כי הרשות תקדם את מאמצי ההגנה על תשתיות ומערכות של המידע הממשלתי ותפעל לפיתוח ההון האנושי בתחום התקשוב בממשלה. נכון לאוגוסט 2020 רשות התקשוב מנחה 48 משרדי ממשלה ויחידות סמך (להלן - משרדי ממשלה)³².

29 McKinsey&Company, A dual cybersecurity mindset for the next normal (2020)

30 יצוין כי האגף לטכנולוגיות דיגיטליות ומידע משותף למשרד המדע והטכנולוגיה ולמשרד התרבות והספורט.

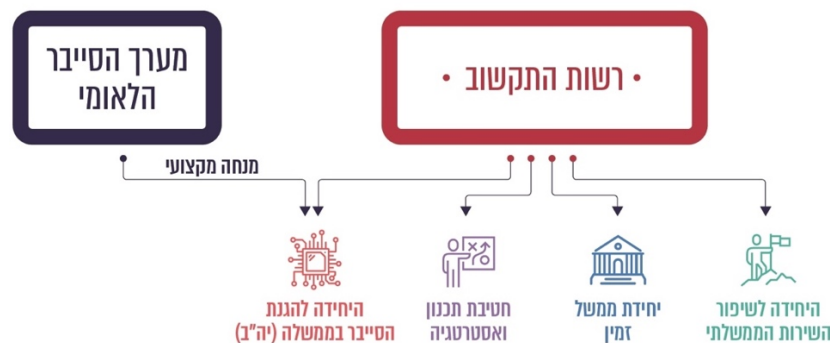
31 החלטת הממשלה 2097 של הממשלה ה-33, "הרחבת תחומי פעילות התקשוב הממשלתי, עידוד חדשנות במגזר הציבורי וקידום המיזם הלאומי 'ישראל דיגיטלית'" (10.10.14).

32 לגבי רשימת משרדי הממשלה ויחידות הסמך הכפופים לסמכות רשות התקשוב הממשלתי ראו: משרד הדיגיטל הלאומי, רשות התקשוב הממשלתי, מבט על פעילות 2020, עמ' 288.



בשנת 2015 הוקמה מתוקף החלטת ממשלה³³ היחידה להגנת הסייבר בממשלה (להלן - יה"ב) בכפיפות לראש רשות התקשוב ובהנחיה מקצועית של מערך הסייבר הלאומי³⁴. היחידה נועדה להיות גוף הכוונה והנחיה מקצועית בתחום הגנת הסייבר עבור כל משרדי הממשלה ויחידות הסמך, ובין תפקידיה - גיבוש מדיניות ארגונית, שיטות עבודה ונהלים³⁵.

תרשים 13: מבנה רשות התקשוב



כפי שיפורט להלן, רשות התקשוב פרסמה במהלך השנים כמה הנחיות העוסקות בנושא גישה מאובטחת מרחוק. הנחיות אלה עודכנו במהלך משבר הקורונה ואף פורסמו כמה הנחיות חדשות העוסקות בין היתר בנושא זה. עם זאת הנחיות אלה אינן נותנת מענה לכלל ההיבטים התקשוביים הכרוכים בעבודה מרחוק. להלן פרטים:

במשך השנים רשות התקשוב עסקה בנושא הגישה מרחוק ופרסמה כמה הנחיות הנוגעות בהיבטי אבטחת מידע וסייבר בגישה מרחוק. כך למשל, הנחיית מסגרת להגנת הסייבר בממשלה³⁶ משנת 2016 קבעה כי הגישה מרחוק לרשת הארגונית תאומת באמצעות מנגנוני הזדהות חזקה (MFA / 2FA)³⁷, ושיש לשלב מנגנוני הצפנה במערכות המשרד, במקרים שונים בהם הצפנת מידע רגיש הנשמר על גבי מחשבים ניידים והצפנת התקשורת בשירותי תקשורת רגילים,

33 החלטת הממשלה 2443 של הממשלה ה-33, "קידום אסדרה לאומית והובלה ממשלתית בהגנת הסייבר" (15.02.15).

34 מערך הסייבר הלאומי פועל לפי החוק להסדרת הביטחון בגופים ציבוריים, התשנ"ח-1998, וכן לפי החלטות ממשלה בתחום הגנת הסייבר, לקידום ההגנה על תפקודו התקין בעיתות שגרה וחירום של מרחב הסייבר האזרחי בישראל, מגיבוש מדיניות ובניין כוח טכנולוגי ועד הגנה מבצעית. כמו כן, בהתאם לחוק, האחראיות להנחיית גופים אשר להם מערכות ממוחשבות חיוניות (להלן - גופי תמ"ק) הוטלה על המערך.

35 נכון לפברואר 2021 יה"ב מנחה 40 משרדי ממשלה ויחידות סמך.

36 הנחיית מסגרת להגנת הסייבר בממשלה, רשות התקשוב הממשלתית, תאריך הוצאה: 1.9.2016, תאריך עדכון: 12.03.2020 (הנחיה מספר 5.2).

37 גורם אימות (Authentication Factor) הוא מידע ו/או תהליך שנועד לצורך אימות או תיקוף (verification) של זהות המשתמש. 2FA - Two Factor Authentication / MFA - Multi-Factor Authentication: תהליך אשר במסגרתו נעשה שימוש בשניים או יותר גורמי אימות (Authentication Factor), אשר מקורם מקטגוריות שונות. לדוגמה: שימוש בסיסמה אישית (משהו שהמשתמש יודע), מאפיין ביומטרי (משהו שהמשתמש הינו).



כגון גישה מרחוק לרשת; הנחייה בנושא EMM / MDM³⁸ למשרדי הממשלה³⁹ משנת 2015 קובעת הוראות באשר לניהול אבטחת המידע במכשירים ניידים (כגון טלפונים חכמים ומחשבי לוח (טאבלטים)) המסונכרנים מול רשת המשרד והתקנת מערכת ניהול ושליטה מרחוק בעלת יכולת ניטור; והנחיה בנושא הקשחת עמדות קצה⁴⁰ משנת 2018 קובעת הוראות בדבר ביצוע הקשחה של עמדות קצה ובכללם מחשבים ניידים (כגון הצפנת מחשבים ניידים כחלק ממכלול האמצעים למניעת דלף מידע ממשלתי במקרים של אובדן או גניבת מחשב נייד). בנוסף לכך, ישנה התייחסות לנושא הגישה מרחוק גם במסגרת ההנחיה העוסקת בניהול יעיל של מערך אבטחת המידע ומזעור איומי הסייבר אשר מקורם בשרשרת האספקה (ספקים)⁴¹.

לאחר פרוץ המשבר והרחבת היקף העבודה מרחוק עודכנו חלק מההנחיות האמורות ופורסמו הנחיות חדשות בנוגע לגישה מרחוק, ובהן הנחיה בנושא גישה מרחוק שמטרתה להנחות את משרדי הממשלה בדבר קביעת מדיניות לגבי גישה מאובטחת מרחוק לרשת הפנים-ארגונית ולמערכות המידע של המשרד⁴², הנחיות הנוגעות להמשכיות העסקית והנחיות בדבר שימוש מאובטח במערכות המשמשות לשיחות וידאו⁴³.

בשנים האחרונות משרדי הממשלה מאפשרים עבודה מרחוק במידה זו או אחרת, והוטמעה פלטפורמה תקשובית התומכת בכך. הועלה כי רשות התקשוב פרסמה כמה הנחיות העוסקות בנושא גישה מרחוק שמתמקדות בעיקרן בהיבטים של אבטחת מידע והמשכיות עסקית, אולם הנחיות אלה אינן מהוות מדיניות כוללת בנושא העבודה מרחוק שנותנת מענה למגוון ההיבטים הקשורים להסדרת הנושא מבחינה תקשובית. המציאות של הרחבת היקף העבודה מרחוק לצד ההתקדמות הטכנולוגית והתובנה כי העבודה מרחוק עתידה להיות נדבך מרכזי בעולם העבודה העתידי, מחייבת הסדרה צופה פני עתיד. בכלל זה יש להתייחס לחלופות האפשריות לשם יישום מודל העבודה מרחוק והערכת העלות של כל אחת מהחלופות, לצד הסיכונים הטמונים בכל אחת מהן; לתשתיות והציוד הנדרש לעובדים לשם עבודה מיטבית; לסוגיית השירותים הממשלתיים הפרונטאליים אשר ניתן לבצע בעבודה מרחוק (ואלו שלא); ולמקומו של הענן בעבודה מרחוק.

- 38 Enterprise Mobility Management - EMM ; Mobile Device Management - MDM.
- 39 ההנחיה: EMM / MDM למשרדי הממשלה, יה"ב - רשות התקשוב הממשלתי, תאריך הוצאה: 9.2.2015, תאריך עדכון: 30.3.20.
- 40 ההנחיה: הקשחת עמדות קצה, יה"ב - רשות התקשוב הממשלתי, תאריך הוצאה: 25.12.18, תאריך עדכון: 3.6.19.
- 41 ההנחיה: שרשרת האספקה, יה"ב - רשות התקשוב הממשלתי, תאריך הוצאה: 3.11.19.
- 42 יה"ב - רשות התקשוב הממשלתי, **ההנחיה: גישה מרחוק**, תאריך הוצאה: 12.3.20, תאריך עדכון: 19.7.20.
- 43 יה"ב - רשות התקשוב הממשלתי, **ההנחיה: שימוש מאובטח במערכת Webex**, תאריך הוצאה: 25.3.20, תאריך עדכון: 28.7.20; ההנחיה: שימוש מאובטח במערכת Teams הממשלתית, תאריך הוצאה: 10.5.20, תאריך עדכון: 28.7.20; ההנחיה: שימוש מאובטח במערכת Zoom, תאריך הוצאה: 25.3.20, תאריך עדכון: 28.7.20.



מומלץ כי רשות התקשוב תגבש מדיניות תקשובית אחודה לכלל משרדי הממשלה בנושא העבודה מרחוק, לאחר מיפוי של המצב הקיים, קיום הליך הפקת לקחים עם כל המגזרים ובעלי התפקידים הרלוונטיים במשרדים השונים, ניתוח צרכים והגדרה של המצב הרצוי, תוך זיהוי אתגרים והזדמנויות לטווח הקרוב והרחוק. כמו כן, מוצע להגדיר חלופות שונות למימוש המדיניות שיתנו מענה למשרדי ממשלה שונים מבחינת היקף ואופי פעילותם, לרבות הערכת העלויות הכרוכות במימוש כל אחת מהחלופות⁴⁴.

גיבוש מדיניות תקשובית בנושא העבודה מרחוק תשמש את משרדי הממשלה בבואם לבחון ולגבש מדיניות באופן פרטני בנושא עבודה מרחוק והיא עשויה גם להוות תשומה לנציבות שירות המדינה ולמשרד האוצר הבוחנים את היתכנות היישום של מודל העבודה מרחוק באופן נרחב יותר בשירות המדינה, ולסייע להם בקבלת ההחלטות לגבי התכנון לטווח הקצר והארוך, לרבות בנושא הקצאת המשאבים ובחינת הכדאיות הכלכלית (עלות-תועלת) של צעד זה.

עוד מומלץ כי אגף שכר והסכמי עבודה במשרד האוצר ונציבות שירות המדינה ישלימו את הבחינה הנעשית לגיבוש מדיניות ממשלתית כוללת בעניין העבודה מרחוק בשרות המדינה ובכלל השרות הציבורי ויפעלו ליישומה וכי בהתאם למדיניות התקשובית בנושא עבודה מרחוק שתגובש יתנו אגף התקציבים במשרד האוצר והמשרדים השונים דעתם לצורך בהקצאת אמצעים ומשאבים ליישום מודל העבודה מרחוק, לרכישת תשתיות מחשוביות נדרשות לשם יישומה ולאחזקתן.

אגף השכר והסכמי העבודה במשרד האוצר מסר באפריל 2021 כי התפשטות מגפת הקורונה בישראל וההגבלות שחלו על פעילות משרדי הממשלה והמשק הביאו להאצת עבודת הצוות המשותף עם נציבות שירות המדינה וכן להרחבה ניכרת של האפשרות לעבודה מרחוק במשרדי הממשלה בתקופת החירום. תקופה זו שימשה ללמידה מעמיקה של הנושא ולביצוע מחקרים וסקרים בקרב עובדים ומנהלים. אגף השכר והסכמי העבודה מסר עוד כי הצוות העוסק בנושא פועל על מנת לגבש מודל לעבודה מרחוק בעיתות שגרה תוך התחשבות במאפיינים הייחודיים של עיתות שגרה, למאפייני העבודה והפעילות הייחודיים הקיימים במשרדי הממשלה השונים ולמסקנות שעלו ונלמדו במהלך השנה האחרונה.

בראייה צופה פני עתיד, מומלץ כי הגורמים הממשלתיים הרלוונטיים, ובכללם, משרד האוצר, רשות המסים, זרוע עבודה במשרד העבודה, הרווחה והשירותים החברתיים והמוסד לביטוח לאומי, יבחנו בשיתוף ובתיאום עם משרד המשפטים, את הצורך בהסדרת היבטים הנוגעים למעבר שוק העבודה לעבודה מרחוק וליצירת תנאים מאפשרים להרחבת העבודה מרחוק בכלל המשק. במסגרת הסדרת הנושא יש לתת את הדעת לסוגיות שונות, בהן עיגון הזכויות והחובות של העובד והמעסיק, הכדאיות הכלכלית והחברתית של מודל עבודה זה והשלכותיו על מגזרי תעסוקה שונים.

44 כך משרד ממשלתי יוכל לבחון אם הוא מעוניין לקדם לדוגמה מימוש של עבודה מרחוק תוך שימוש בתחנות עגינה ומה העלות הכרוכה בתהליך זה בהשוואה לחלופות אחרות.



רשות המסים מסרה בתשובתה מאפריל 2021 כי היא נערכת לקראת ההשפעות השונות של משבר הקורונה, בכל ההיבטים של עולם המס ובכלל זה בנושא העבודה מהבית.

בתשובת המוסד לביטוח לאומי מאפריל 2021 צוין כי משבר הקורונה הוביל לשינויים בדפוס התעסוקה לרבות מבחינת העבודה מהבית. לשינויים אלו השפעות מהותיות בהיבטים שונים, לרבות במישור יחסי עובד ומעסיק. המוסד הוסיף כי בדיקת יחסי עובד - מעסיק נעשית בהתאם ל"מבחן המעורב"⁴⁵ שנקבע בפסיקות בתי הדין לעבודה, וכי אין כל מניעה משפטית לכך שמבוטח יוכר כעובד שכיר גם אם העבודה מתבצעת בבית. הביטוח הלאומי ציין כי הוא מכיר זה שנים רבות במודל העסקה כזה, עוד לפני מגפת הקורונה, ולא נדרשת היערכות מיוחדת לכך (למעט במקרים של קרבה משפחתית בין העובד למעסיק, שבהם נדרשת בחינה של היבטים שונים). המוסד לביטוח לאומי ציין כי עובר למשבר הקורונה, הוא הכיר בתביעות נפגעי עבודה, בעיקר עצמאיים, שעבדו בביתם. המוסד ציין עוד כי הוא פעל כבדרך שגרה לעדכון מידעים, החלטות, נתונים, הנחיות והבהרות באתרי המרשתת (האינטרנט) והפייסבוק, לטובת חשיפת המידע לציבור הרחב.

במאי 2021 מסר משרד העבודה, הרווחה והשירותים החברתיים כי זרוע העבודה במשרד החלה בבחינת הסוגיה של עבודה מרחוק עוד בטרם התפרצות משבר הקורונה, בשל ההבנה כי השינויים בעולם העבודה מאפשרים צורת עבודה זו. במסגרת כך, הזרוע מקדמת פיילוט במשותף עם תב"ת-ג'וינט ישראל, בכדי לאתר את הכלים הנדרשים לעידוד עבודה מרחוק בקרב ארגונים ואוכלוסיות. המשרד הוסיף כי לצד זאת, זרוע העבודה בוחנת את הצורך בשינויי חקיקה נדרשים, וכי במהלך משבר הקורונה פרסמה הזרוע גילוי דעת באשר לאופן היישום של עבודה מהבית בהיעדר אסדרה ייעודית לנושא. עוד צוין על ידו כי בהמשך לכך, ובהתאם להנחיית השר, נוסחה טיוטה ראשונית של תזכיר חוק המאסדר את אופן העבודה מהבית, במקום בו יש הסכמה של המעסיק והעובד. המשרד ציין כי ימשיך לקדם את עבודת המטה מול הגורמים הרלוונטיים על בסיס טיוטה זו, וכי גורמי המקצוע סבורים כי יש לאסדר את אופן העבודה מרחוק, בכדי שהדעת תינתן למורכבות הטמונה בצורת עבודה זו, כגון - היבטי פרטיות, איזון בית-עבודה, שינויי ההוצאות למעסיק ולעובד ועוד.

⁴⁵ קיומם של יחסי עבודה נבחנים באמצעות ה"מבחן המעורב" המשלב כמה מבחנים - המבחן העיקרי הוא מבחן ההשתלבות, ואליו נלווים כמה מבחני משנה. מבחן ההשתלבות בוחן את מידת ההשתלבות של העובד במקום העבודה; עד כמה הוא מהווה חלק אינטגרלי מהפעילות של העסק או פעילות משלימה; ואם הוא נותן שירות חיצוני.



תוכנית להמשכיות עסקית

לשם הבטחת הרציפות התפקודית והתפעולית של ארגון בעיתות משבר, אסון או חירום נדרש שתהיה לו תוכנית להמשכיות עסקית (BCP - Business Continuity Plan) (להלן גם - תוכנית להמשכיות תפקודית). תוכנית כזו מתייחסת לפעולות שעל הארגון לבצע כדי להבטיח זמינות משאבים קריטיים והמשך פעילותן של תשתיות נחוצות כדי שיוכל להמשיך לתפקד בתרחישי ייחוס שונים⁴⁶. כל ארגון מחויב, במסגרת ניהול הסיכונים שלו, לתכנן כיצד להיערך להתמודדות עם מצבי קיצון. גורמי הסיכון שעלולים לפגוע בארגון הם, לדוגמה, אסונות טבע (רעידות אדמה, הצפות, סופות), אירועי לוחמה (למשל פגיעת טילים או פיגועי טרור), פגיעה בכוח אדם (מגפות), ופגיעות המבוססות על טכנולוגיה (לוחמה אלקטרונית המכוונת נגד מערכות תוכנה, מערכות תקשורת, לוחמת סייבר).

תרשים 14: דוגמאות למצבי חירום



46 להרחבה בעניין זה ראו גם: תקן 24001 "מערכות ניהול חוסן תפקודי של ארגון (מנחת"א)", ותקן 22301 "מערכת ניהול המשכיות עסקית".



קיומה של תוכנית המשכיות עסקית במשרדי הממשלה

תוכנית ההמשכיות העסקית והתפקודית של המשרד צריכה להיקבע בהתאם להנחיות הגורמים המוסמכים לעניין תפקוד במצבי חירום. השירותים והתהליכים העסקיים והתפקודיים של משרדי הממשלה מושתתים, בין היתר, על טכנולוגיות דיגיטליות. על כן, במסגרת גיבוש תוכנית ההמשכיות העסקית יש להביא בחשבון גם היבטי תקשורת. לכל תרחיש ייחוס עלולות להיות השפעות שונות על השירותים והתהליכים המושתתים על מערכות מידע (תשתיות פיזיות, תשתיות מחשוב, כוח אדם קריטי, ספקים ועוד).

בשנת 2016 פרסמה יה"ב הנחיית מסגרת להגנת הסייבר בממשלה⁴⁷, העוסקת, בין היתר, בניהול המשכיות תפקודית של מערכות המידע⁴⁸. בהנחיה נקבע שיש להגדיר את העקרונות שיאפשרו המשך פעילות של מערכות התקשורת החיוניות של המשרד בעת חירום, ובכלל זה להגדיר את המערכות והתהליכים החיוניים להמשך פעילות המשרד ואת משך הזמן הדרוש להתאוששותם; לזהות את האסונות והכשלים העלולים לפגוע בפעילותו של המשרד, ולהעריך את השפעותיהם.

עוד נקבע בהנחיה כי יש לגבש תוכנית להמשכיות תפקודית (Business Continuity Plan), אשר תכלול גם תוכנית להתאוששות מאסון (Disaster Recovery Plan), בהתבסס על הערכת סיכונים נאותה המפרטת את כלל האמצעים שיש לנקוט בעקבות אירוע חירום המסכן את פעילותו התקינה של המשרד. בהנחיה צוין כי "היערכות להמשכיות תפקודית נועדה לסכל הפרעות לפעילות השוטפת של המשרד ולהגן על נתונים מפני הרס, שיבוש, מחיקה וכדומה, הנגרמים בהשפעת מקרי כשל מהותיים או מקרי אסון (שריפה, הצפה, מלחמה, אסונות טבע וכדומה) במערכות התקשורת הפיזיות והלוגיות של המשרד".

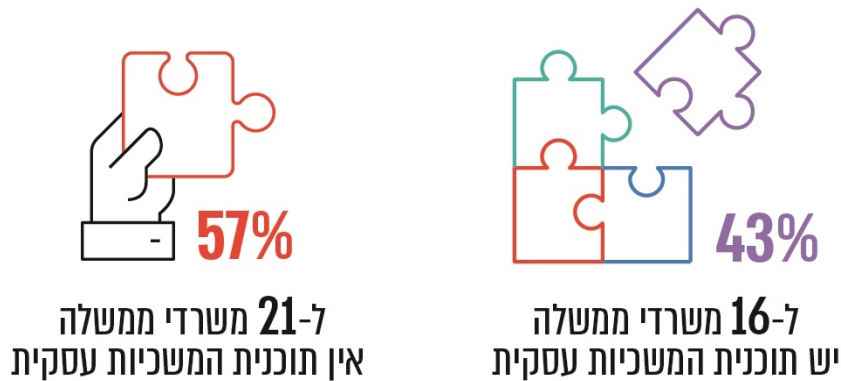
תורת ההגנה לסייבר בארגון⁴⁹, שהוציא מערך הסייבר הלאומי, עוסקת אף היא בצורך בגיבוש תוכנית המשכיות עסקית כדי למזער את הנזק הנגרם בהתרחש אירוע חמור בהיבטי הגנת סייבר ולצורך בקיום בחינה עיתית לשם צמצום פערים בין המצב הרצוי לבין המצוי ולצורך תיקון ליקויים שהתגלו⁵⁰.

בנובמבר 2020 מסרה יחידת יה"ב למשרד מבקר המדינה נתונים בנוגע לגיבוש תוכניות להמשכיות עסקית על ידי משרדי הממשלה. המידע שהועבר נוגע ל-37 משרדי ממשלה:

- | | |
|----|---|
| 47 | רשות התקשורת הממשלית, הנחיית מסגרת להגנת הסייבר בממשלה , תאריך הוצאה: 1.9.2016, תאריך עדכון: 12.03.2020 (הנחיה 5.2). |
| 48 | סעיף 13 בהנחיה. |
| 49 | מערכת הסייבר הלאומי, תורת ההגנה בסייבר לארגון , גרסה 1.0 (אפריל 2018). |
| 50 | שם, (עמ' 142 - 149). |



תרשים 15: **גיבוש תוכניות המשכיות עסקית על ידי משרדי ממשלה, לפי נתוני יה"ב המעודכנים ל-2.11.20:**



נתוני יחידת יה"ב נכון לנובמבר 2020, בעיבוד משרד מבקר המדינה

מנתוני יה"ב עולה כי נכון לנובמבר 2020, 21 (57%) מ-37 משרדי ממשלה טרם גיבשו תוכנית המשכיות עסקית.

יכולת השרידות של הארגון בשעת אסון תלויה בתכנון המקדים של הארגון ובאופן הטיפול שניתן לנושא בעיתות שגרה. ישנה חשיבות שתהיה לארגון תוכנית המשכיות עסקית כדי להבטיח את הרציפות התפקודית והתפעולית של הארגון בעיתות חירום וגם כדי למנוע פגיעה באמון הציבור.

על 21 משרדי הממשלה שטרם השלימו את גיבוש התוכנית להמשכיות עסקית להשלימה בהתאם להנחיות יה"ב.

המשכיות עסקית - עבודה מרחוק

לכל משרד ממשלתי יש אחריות בתחום שהוא מופקד עליו, ומחובתו להיערך מבעוד מועד להקצות את המשאבים והתקציבים הנדרשים על מנת שגם במצב חירום יוכל להמשיך למלא את התחייבויותיו לאספקת מוצרים ושירותים. אחת הדרכים להבטיח את המשך תפקודו התקין של הארגון היא היערכות למתכונת של עבודה מרחוק.

התוכנית הלאומית לפנדמיה של שפעת ("נחשול בריא"), המפרטת את העקרונות הלאומיים להיערכות מוקדמת להתמודדות עם מגפה, כוללת בין היתר התייחסות לנושא העבודה מרחוק כחלק מהבטחת המשכיות התפקודית של ארגונים⁵¹. בין היתר מצוין בתוכנית כי במסגרת ההיערכות למגפה יש להגדיר ולקבוע סדרי עדיפויות לשירותים חיוניים שהארגון מחויב לספק

51 משרד הביטחון, "נחשול בריא" - תוכנית ההיערכות הלאומית לתרחיש פנדמיה של שפעת (התוכנית במעמד טיוטה), משרד הביטחון, פברואר 2018.



לאזרחים בכל מצב; לתכנן את פעילות הארגון בהנחה שייעדרו עד 45% מהעובדים למשך שבוע עד שבועיים; לבחון את האפשרות שהארגון יעבוד בלוח זמנים גמיש ותוך הקניית גמישות תפעולית לעניין אופן עבודתם של העובדים; לעודד "עבודה מרחוק" תוך שימוש בטכנולוגיות מחשב ותקשורת במצבים שבהם מתכונת עבודה זו רלוונטית וישימה ובחינת האפשרות לשינוי אופן העבודה ממגע "פנים מול פנים" לשירות הניתן מרחוק, לרבות באמצעות קביעת נהלים מתאימים. התוכנית הלאומית מונה אסטרטגיות פעולה שיבטיחו המשכיות תפקודית של הארגון, בהן בחינת ישימות האפשרות של "עבודה מרחוק" ופיתוח תוכנית למימוש ההחלטה, אם תתקבל החלטה בעניין.

גם גופי פיקוח שונים החלו לחייב ארגונים במגזרם להתוות מסגרת עבודה כוללת לניהול המשכיות עסקית, ובמסגרתה לעסוק, בין היתר, בנושא הגישה מרחוק. למשל, המפקח על הבנקים פרסם הוראות בנושא בשנת 2017⁵², ובמסגרתן צוין כי בעת גיבוש תוכנית ההמשכיות העסקית, על התאגיד הבנקאי לתת את הדעת על כל מרכיבי הטכנולוגיה הנדרשים לשם שמירת הרציפות העסקית או לאישוש הפעילות. עוד צוין בהוראות כי נוהלי עבודה לגישה מרחוק יהיו חלק מתוכנית ההמשכיות העסקית, שכן באירועי חירום מסוימים לא תתאפשר גישה למתקני הבנק, ולכן עלול להיות צורך במתן גישה מרחוק לעובדים או לנותני שירותים חיצוניים. על פי ההוראות, מדיניות הגישה מרחוק צריכה לקבל את אישור ההנהלה הבכירה ולהביא בחשבון סיכונים הכרוכים במדיניות ולהפעיל מנגנוני בקרה ואבטחת מידע הולמים.

בדומה לכך, הממונה על שוק ההון, ביטוח וחיסכון, פרסם בשנת 2013 הוראות ולפיהן גופים מוסדיים נדרשים לגבש תוכנית המשכיות עסקית שתבטיח תפקוד רציף ותקין במצב חירום⁵³. בהוראות צוין, בין היתר, כי על הגוף המוסדי לקבוע נוהלי עבודה לגישה מרחוק במצב חירום לתשתיות IT שאותן הגדיר כתשתיות קריטיות, הן של עובדים והן של נותני שירותים חיצוניים. עוד צוין בהוראות כי במסגרת מדיניות הגישה מרחוק יידונו הסיכונים הכרוכים בה וקיום מנגנוני בקרה ואבטחת מידע מתאימים.

בשנת 2016 פרסמה יה"ב הנחיית מסגרת להגנת הסייבר, שכללה בין היתר הוראות הנוגעות להמשכיות עסקית, שהתייחסו בעיקר להיבטים הנוגעים להמשך הפעילות של מערכות התקשוב החיוניות של המשרד, ולא נכללה בהן התייחסות ספציפית לצורך בהבטחת המשכיות התפקודית של משרדי הממשלה במצבי חירום, בין היתר באמצעות מתן גישה מרחוק.

במהלך משבר הקורונה, במרץ 2020 ובנובמבר 2020, פרסמה רשות התקשוב הנחיות ייעודיות העוסקות בהמשכיות עסקית, אשר נתנו, בין היתר, מענה לנושא הגישה מרחוק.

משרד מבקר המדינה בחן במהלך החודשים אוגוסט - דצמבר 2020 מול משרדי ממשלה שנבדקו פרטנית בביקורת אם יש להם תוכנית המשכיות עסקית ואם היא כוללת התייחסות לנושא הגישה מרחוק. להלן ממצאי הבחינה האמורה:

52 בנק ישראל, **הוראות ניהול בנקאי תקין, "ניהול המשכיות עסקית"** (אפריל 2017)

53 הממונה על שוק ההון, ביטוח וחיסכון, **הוראות חוזר גופים מוסדיים 11-9-2013, "ניהול המשכיות עסקית בגופים מוסדיים"** (אוגוסט 2013).



תרשים 16: תוכניות המשכיות עסקית במשרדי הממשלה שנבדקו פרטנית בביקורת

קיימת תוכנית המשכיות עסקית	נושא העבודה מרחוק כלול בתוכנית	
		משרד הפנים
		משרד התחבורה*
		משרד המשפטים
		משרד המדע
		המשרד להגנת הסביבה

* קיימת טיוטת תוכנית המשכיות עסקית שטרם אושרה.

הועלה כי משרד התחבורה ומשרד המדע טרם השלימו את גיבושה של תוכנית ההמשכיות העסקית. באשר לשלושת המשרדים הנוספים שנבחנו - משרד הפנים, משרד המשפטים והמשרד להגנת הסביבה - הועלה כי יש להם תוכניות להמשכיות עסקית, אולם רק אחת מהן, של משרד המשפטים, כללה התייחסות לנושא העבודה מרחוק.

להלן התייחסות המשרדים לממצאים שעלו:

משרד הפנים מסר למשרד מבקר המדינה באוגוסט 2020 כי בעקבות התפרצות משבר הקורונה והרחבת היקף העבודה מרחוק מבוצעת פעילות לעדכון ולתיקוף של התוכנית בהתאם לכך, בהובלת אגף הביטחון בשיתוף משאבי אנוש ומערכות מידע.

משרד התחבורה מסר למשרד מבקר המדינה בנובמבר 2020 כי אגף החירום במשרד התחבורה משמש גורם אחראי ומתכלל לכלל תחומי מערך התחבורה, ובכלל זאת לגופים שהם חברות ממשלתיות שלהן תוכניות התאוששות עסקית פנימית. עוד מסר משרד התחבורה כי בשנתיים האחרונות (2018 - 2020) הוא פעל לגיבוש ולאפיון של תפיסה חדשה לעניין מצבי חירום, לעדכון ולריענון של נהלים, להכנת תיק אב (אוגדן חירום) ובכלל זה לעדכון של תרחיש הייחוס ותוכניות המענה ולקיום הדרכות ותרגילים. המשרד הוסיף כי לנוכח המציאות הנוכחית נקטע ביצוע עבודת המטה לגיבוש ולהטמעה של התפיסה ולקבלת אישור רשמי מאגפי המשרד ומהנהלת



המשרד לגבי התפיסה, ולכן מסמך בעניין זה הוא עדיין במעמד טיוטה. המשרד צירף לתגובתו את טיוטת המסמך (אוגדן אב להיערכות ומענה בחירום של מערך התחבורה). הטיוטה עוסקת, בין היתר, בנושא עבודה מרחוק.

באפריל 2021 מסר משרד התחבורה שתוכנית ההמשכיות העסקית גובשה, אך עדיין לא אושרה סופית וטרם הוטמעה היות שנדרשים שינויים מקיפים בתוכנית לנוכח לקחי תקופת הקורונה. המשרד הוסיף כי הוא ערוך מהבחינה הטכנולוגית להבטחת הרציפות התפקודית והתפעולית בעת חירום, וכי במסגרת זו מותקנות במשרד שתי מערכות לגישה מאובטחת מרחוק של שני יצרנים שונים המגבות זו את זו, והגישה למערכות מתבצעת על בסיס שני קווי מרשתת של שתי ספקיות שונות כדי להבטיח את שרידות המערכות.

המשרד להגנת הסביבה מסר למשרד מבקר המדינה בדצמבר 2020 כי תוכנית ההמשכיות העסקית הקיימת עוסקת בהיערכות להתאוששות לאחר אסון באמצעות קיומו של אתר גיבוי (DR); היא אינה עוסקת בנושא של עבודה מהבית.

בדצמבר 2020 מסר משרד המדע למשרד מבקר המדינה כי אין ברשותו מסמך תוכנית המשכיות עסקית מעודכן וחתום על ידי ההנהלה, וכי בתוכנית העבודה לשנת 2021 (רבעון ראשון) של אגף ביטחון, חירום וסייבר נכללת הכנת התוכנית; ובמסגרתה יתקיימו פגישות עם כלל האגפים ויתבצע מיפוי התהליכים. עוד נמסר כי אי קיומה של תוכנית המשכיות עסקית מאושרת יעלה כפער בפני ההנהלה בישיבת ועדת ההיגוי שאמורה להתכנס בחודש זה. באפריל 2021 מסר משרד המדע כי בדצמבר 2020 הוא אישר בוועדת ההיגוי לסייבר תוכנית עבודה לאגף הסייבר, ובכלל זה היערכות לגיבוי תוכנית המשכיות עסקית. המשרד מסר כי בכוונתו להשלים את גיבוש התוכנית במהלך 2021.

על משרד התחבורה ומשרד המדע להשלים את גיבוש התוכנית להמשכיות עסקית אשר תכלול את נושא העבודה מרחוק ולתקף תכניות אלו למול הנהלות המשרדים. עוד מומלץ כי משרד הפנים והמשרד להגנת הסביבה יבצעו עדכון לתוכנית ההמשכיות העסקית הקיימת שלהם, כך שזו תכלול בין היתר התייחסות גם להיבטים הנוגעים לעבודה מרחוק.

המשכיות עסקית - משבר הקורונה

ב-9.3.20 פרסמה רשות התקשוב הנחיה ייעודית הנוגעת לצורך בהמשכיות עסקית בתקופת הקורונה⁵⁴. בהנחיה צוין כי מטרתה להורות למשרדי הממשלה וליחידות הסמך להיערך להמשכיות עבודה רציפה ולמתן שירותים חיוניים לציבור. ההנחיה מפרטת את הפעולות המקדימות הנדרשות מהמשרדים על מנת למפות את הפונקציות והצרכים החיוניים למשרד, את הכלים העומדים לרשות המשרדים על מנת לאפשר התחברות מרחוק לרשת המשרד ואת הדרך לרכוש אותם, ואת הכלים החלופיים המאפשרים קיום פגישות דיגיטליות.

בהנחיה צוין שעל מנהלי אגפי טכנולוגיות ומידע (להלן - מנמ"רים) בכל משרדי הממשלה ויחידות הסמך לבצע מיפוי מסודר של משרדם, ובכלל זה של מספר העובדים במשרד, מספר העובדים שעומדים לרשותם מחשבים ניידים המאפשרים חיבור מרחוק, מספר עובדים שנדרש

54 "היערכות אגפי טכנולוגיות דיגיטליות ומידע לרציפות עסקית - אירוע הקורונה", הנחיה: 1.1.23.



לחבר מרחוק ובזמנית למערכות המידע של המשרד במקרה חירום, מספר עובדים המחוברים לדואר האלקטרוני הארגוני באמצעות מכשיר סלולרי ורשימה של מערכות תפעוליות שנדרשות בחיבור מרחוק. זאת כדי לזהות את הפערים הקיימים ולפתח תוכנית פעולה ותוכנית רכש על מנת לצמצם אותם.

בנוסף, ההנחיה כוללת התייחסות לכך שיחידת ממשל זמין ברשות התקשוב הממשלתי (להלן גם - ממשל זמין) מעמידה לרשות משרדי הממשלה פתרון לחיבור מרחוק של מחשב נייד והזדהות לצורך חיבור מרחוק בעזרת כרטיס חכם; עוד יש התייחסות לכך שמשרדי ממשלה סוברניים ליישם פתרונות אחרים לחיבור מרחוק וכי רשות התקשוב תפעל לגיבוש פתרון ממשלתי לגישור על הפערים בין הצרכים לבין היישום אם אכן יימצאו פערים כאלו במשרדי ממשלה.

ב- 18.11.20 פורסמה הנחיה ייעודית נוספת בנושא "היערכות להמשכיות עסקית ותפקודית במצב חירום". צוין כי הנחיה זו מיועדת להשלים את תוכנית ההמשכיות העסקית והתפקודית של משרד ממשלתי למצב חירום, שמובילים אגפי החירום במשרד, אם אכן הוכנה בו תוכנית כזאת. עוד צוין בהנחיה כי מטרתה להגביר את המודעות של הנהלות המשרדים, אגפי החירום ואגפי טכנולוגיות דיגיטליות ומידע למידת ההיערכות של מערכי התקשוב במשרדים להמשכיות עסקית ותפקודית בעת התממשות איום על המשרד, שעלול לגרום נזק מלא או חלקי לתפקוד המשרד, ולהשבתה, חלקית או מלאה, של שירותים ותהליכים עסקיים ותפקודיים. ההנחיה קובעת כי על המנמ"רים, בתיאום עם אגף החירום במשרד, לבצע לצורך ניהול נושא ההמשכיות העסקית כמה פעולות, ובהן: מיפוי תרחישי הייחוס, ניתוח הסיכונים שאליהם האגף חשוף במקרה של התממשות תרחיש ייחוס, קביעת יעדי שירות למצב חירום, פיתוח תוכנית להמשכיות עסקית ותפקודית והטמעתה.

זאת ועוד, ההנחיה מגדירה אילו נושאים צריכים להיכלל בתוכנית ההמשכיות העסקית של המשרד, ובכלל זה נושא הגישה מרחוק. בעניין זה נקבע כי על אגפי טכנולוגיות דיגיטליות ומידע לספק כלים טכנולוגיים להקמת ממשקי תקשורת שיפעלו במצב חירום ויאפשרו קשר רציף וסדיר עם גורמים בעלי עניין שונים (עובדים, אזרחים, ספקים וכו'). עוד נקבע בעניין זה שהאגף יקבע נוהלי עבודה לגישה מרחוק במצב חירום לתשתיות ולמערכות שהגדיר כקריטיות, הן של עובדים והן של נותני שירותים חיצוניים, וכי מדיניות הגישה מרחוק תעסוק בסיכונים הכרוכים בה ובהסדרת מנגנוני בקרה ואבטחת מידע מתאימים.

עוד נקבע בהנחיה כי על האגף לבחון אחת לשנה לפחות, או בעת שחל שינוי ניכר בסביבת הפעילות והסיכונים, את תרחישי הייחוס, את יעדי השירות בעת חירום, את ניהול הסיכונים, את מסגרת העבודה הכללית ואת התוכנית להמשכיות עסקית ותפקודית הנקבעת לפיהם. כמו כן צוין כי על האגף להקצות משאבים להבטחת המשכיות העסקית והתפקודית, לרבות בתקציב השוטף ובתקציב השקעה, כנדרש לתמיכה בתהליכים עסקיים ותפקודיים בהתאם לאסטרטגיה וליעדי המשרד.

משבר הקורונה חידד את התובנה כי היכולת לעבוד מרחוק היא תנאי הכרחי להבטחת הרציפות התפקודית של גופים ציבוריים.



מן האמור עולה כי ל-21 משרדי ממשלה (מתוך 37) אין תוכנית המשכיות עסקית, וכי בחמשת המשרדים שבדק משרד מבקר המדינה באופן פרטני - גם לאלו שהיו תכניות ההמשכיות העסקית, הרי שהן לא כללו בהכרח התייחסות לצורך למתן גישה מרחוק בזמן משבר. על משרדי הממשלה, להם תפקיד מרכזי בעת שגרה ובפרט במצבי חירום, לגבש תוכנית המשכיות עסקית שתבטיח תפקוד שוטף ותקין במצב חירום.

פרסום ההנחיה הייעודית בדבר היערכות להמשכיות עסקית ותפקודית במצב חירום על ידי רשות התקשוב בנובמבר 2020 היא צעד חשוב להבטחת ההיערכות להתמודדות עם מצבי חירום, ובפרט בנוגע להיבטי התקשוב הקשורים לכך. על משרדי הממשלה לפעול ליישום ההנחיה האמורה. מומלץ כי רשות התקשוב תעקוב אחר יישומה.

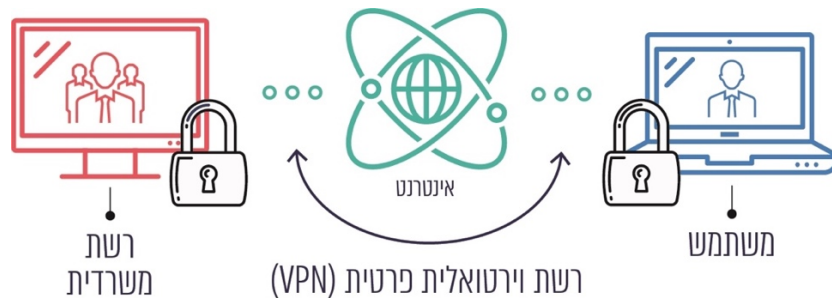


העבודה מרחוק במהלך משבר הקורונה - תמונת המצב

היבטי תשתית

עבודה מרחוק דורשת בין היתר קיומם של תשתיות ופתרונות טכנולוגיים שיאפשרו גישה מרחוק תוך שמירה על רמת אבטחת המידע הנדרשת, ובכלל זה קיומה של התשתית הנדרשת מבחינת חומרה, תוכנה, הקצאת מחשבים ניידים וציוד קצה נלווה, אפליקציות וכלים המסייעים לעבודה מרחוק וכן שירותי תמיכה.

תרשים 17: יישום מודל העבודה מרחוק



חלק ממשרדי הממשלה הקימו יכולות חיבור מרחוק עצמאיות וחלק משתמשים בשירות הגישה מרחוק של ממשל זמין. נכון לדצמבר 2020 משתמשים בשירות זה של ממשל זמין 19 משרדי ממשלה.

לצד זאת פרסם מינהל הרכש הממשלתי⁵⁵ מכרזים מרכזיים⁵⁶ שמטרתם לספק צרכים הנוגעים לעבודה בגישה מרחוק ולאבטחת המידע במסגרתה: כגון מכרז מרכזי לאספקת מחשבים, לרבות מחשבים ניידים, למשרדי הממשלה; ומכרז לאספקת מערכות ניהול ואבטחת המכשירים הניידים עבור משרדי הממשלה. אחד מכלי העזר הנוספים שעומד לרשות משרדי ממשלה הוא הסכם מחירים מרביים⁵⁷ שפורסם עבור מוצר שנועד לאפשר גישה מאובטחת מרחוק⁵⁸.

55 מינהל הרכש הממשלתי הוא גוף מטה בחטיבת משרדים כלכליים באגף החשב הכללי. תפקידיו העיקריים הם להתוות את מדיניות הרכש הממשלתית, ליצור התקשרויות מרכזיות עבור משרדי הממשלה ויחידות הסמך, להקים תשתיות דיגיטליות לביצוע תהליכי רכש וקדם רכש, וכן לסייע לגופים הממשלתיים בביצוע ויישום מדיניות הרכש במשרדם. מקור: <https://mr.gov.il/ilgstorefront/he/about>

56 מכרז מרכזי הוא מכרז הנערך מטעם החש"ל בעבור המשרדים הממשלתיים.

57 הסכם מחירים מרביים הוא כלי עזר למשרד ואינו מחייב את משרדי הממשלה להתקשרות זו או אחרת עם היצרן או הספק.

58 בעניין זה ראו: <https://mr.gov.il/ilgstorefront/en/p/4000521039>



משרד מבקר המדינה בדק את מידת היערכותם של משרדי הממשלה מהבחינה התקשובית לעבודה מרחוק לאורך משבר הקורונה במטרה לקבל תמונת מצב כוללת לגבי היערכות המשרדים לעבודה מרחוק. נוסף על כך, בדק משרד מבקר המדינה את מידת ההיערכות לעבודה מרחוק של כמה משרדים באופן פרטני, לרבות פעולות שביצעו על מנת להתמודד עם הצורך בהרחבת היקף העבודה מרחוק בתוך פרק זמן קצר. להלן פירוט:

תמונת מצב כוללת של משרדי הממשלה

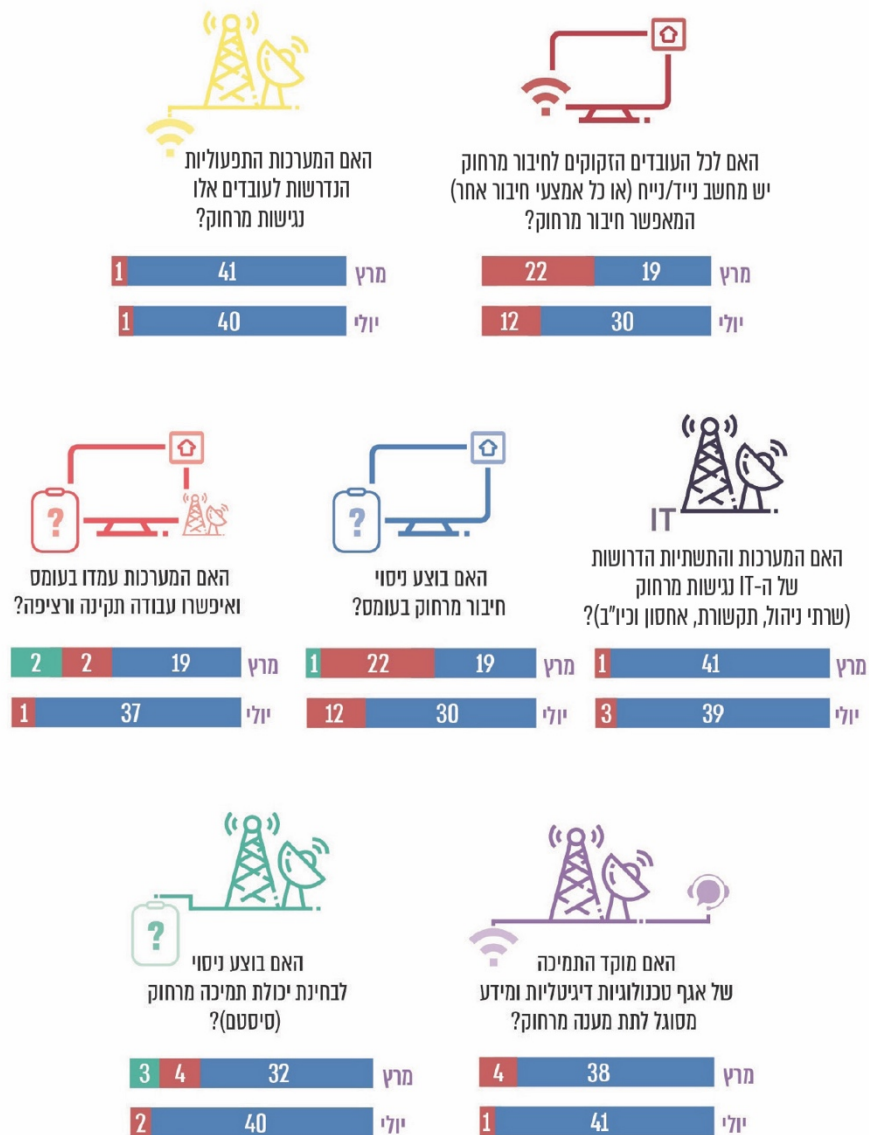
עם פרוץ המשבר, ב-17.3.20, ביצעה רשות התקשוב מיפוי מול משרדי הממשלה כדי לעמוד על מידת המוכנות של המשרדים לעבודה מרחוק, ובכלל זה לעמוד על יכולתם של העובדים שהוגדרו כחיוניים לעבוד מרחוק ולזהות בעיות ופערים שיש לתת להם מענה. המיפוי כלל כמה שאלות שהמשרדים נדרשו להשיב עליהן. בהמשך, ב-19.7.20, ביצעה רשות התקשוב מיפוי נוסף כדי להבין אילו פערים נותרו ולבחון את מידת היערכותם של משרדי הממשלה לעבודה מרחוק במקרה של סגר נוסף (באשר לחוויית המשתמש ראו להלן בפרק שעניינו: חוויית המשתמש - העובדים).

רשות התקשוב שלחה למשרד מבקר המדינה את קובצי המיפוי האמורים. משרד מבקר המדינה ניתח את קובצי המיפוי במטרה לבחון את תמונת המצב שהועלתה בשתי נקודות זמן - במרץ 2020 וביוני 2020. בניתוח שבוצע נכללו 42 משרדי ממשלה שמילאו את שני הסקרים (יצוין כי חלקם לא השיבו על כל השאלות). להלן תמונת המצב המצטיירת מניתוח הקבצים:



תרשים 18: תמונת המצב הכוללת- מידת המוכנות של המשרדים לעבודה מרחוק, לפי מספר המשרדים שהשיבו על כל אחת מהשאלות שבסקר, מרץ ויולי 2020

כן - לא - בתהליך -



נתוני רשות התקשוב, בניתוח ועיבוד משרד מבקר המדינה.



מהתרחשים עולה כי עם פרוץ משבר הקורונה, במרץ 2020, הייתה במשרדי הממשלה התשתית הנדרשת להתחברות מרחוק - 95% מהמשרדים ציינו כי הייתה גישה מרחוק לתשתיות ולמערכות התפעוליות אשר נדרשות לעובדים לשם המשך עבודה תקינה ורציפה. הפערים שהועלו נגעו בעיקר לצורך להרחיב את התשתיות ולהגדיל את מספר אמצעי החיבור מרחוק כדי לספק את הצרכים הנדרשים למספר הולך וגדל של עובדים מרחוק: 19 (45%) מ-42 משרדי הממשלה ציינו כי יש לכל העובדים הזקוקים לחיבור מרחוק מחשב נייד או נייד (או כל אמצעי חיבור אחר) המאפשר להם חיבור מרחוק, 22 (52%) מהמשרדים ציינו כי לא היו להם מספיק מחשבים כדי להעמיד מחשב כאמור לרשות כלל העובדים הנזקקים לחיבור מרחוק, משרד אחד לא השיב על השאלה; 19 (45%) מהמשרדים ציינו כי המערכות שלהם עמדו בעומס ואפשרו עבודה תקינה ורציפה מרחוק, שניים (4%) מהמשרדים ציינו שהמערכות שלהם לא עמדו בעומס, יתר המשרדים לא השיבו על שאלה זו או ציינו כי הם נמצאים בתהליכי היערכות כדי שיוכלו למלא את החוסרים בנוגע לצידוד ותשתיות באופן שיאפשר לכלל העובדים שנדרשים לעבוד מרחוק לעשות כן. יובהר כי בתקופת החירום נדרשו רק עובדים שהוגדרו חיוניים להמשיך לעבוד, חלקם נדרש לעבוד מהמשרד וחלקם יכול היה לעבוד גם מרחוק.

כשם שעולה מהתרחשים, בחלוף כמה חודשים מפרוץ המשבר, ביולי 2020, חל שיפור ביכולתם של משרדי הממשלה לתמוך באופן העבודה האמור - הפערים שנמצאו בהם במרץ 2020 צומצמו מאז במידה ניכרת. בין היתר עולה, כי 30 (71%) מ-42 משרדים ציינו כי לכל העובדים שנדרש להם חיבור מרחוק יש מחשב נייד או נייד (או כל אמצעי חיבור אחר) המאפשר להם חיבור מרחוק, ו-37 (88%) מהמשרדים ציינו כי המערכות שלהם עמדו בעומס ואיפשרו עבודה תקינה ורציפה מרחוק.

מגמת השיפור בהיערכות באה לידי ביטוי גם בתכלול של סטטוס היערכות המשרדים בשני המועדים, מרץ ויולי 2020, שביצעה רשות התקשוב. להלן הממצאים בנושא:

תרשים 19: סטטוס היערכות המשרדים לעבודה מרחוק, מרץ ויולי 2020



המקור: נתוני רשות התקשוב בעיבוד משרד מבקר המדינה.



הרחבת היקף העבודה מרחוק במשרדי הממשלה במהלך משבר הקורונה נעשתה בתוך פרק זמן קצר מאוד. במרץ 2020 נמצאו פערים מסוימים בהיערכותם לעבודה מרחוק וביכולתם לתת מענה לכלל העובדים הנדרשים לכך, פערים אשר הצטמצמו ביולי 2020 (בהתאמה): 17% לעומת 40% דיווחו כי השלימו את ההיערכות לעבודה מרחוק; 64% לעומת 60% דיווחו שהם נמצאים בשלבי היערכות ו-19% לעומת 0 דיווחו שההיערכות שלהם מתעכבת.

משרד מבקר המדינה מציין לחיוב את ההתקדמות שחלה בהיערכות המשרדים לעבודה מרחוק ואת הבקרה שביצעה רשות התקשוב בנושא. מומלץ כי המשרדים יעקבו באופן שוטף אחר יכולתם לעבוד מרחוק וכי רשות התקשוב תמשיך לבחון באופן עיתי את מידת ההיערכות של המשרדים לעבודה מרחוק, על מנת לוודא כי ביכולתם לבצע במצבים שונים.

פעולות שבוצעו להשלמת ההיערכות לעבודה מרחוק

לשם צמצום הפערים שהועלו ובמסגרת השלמת ההיערכות לעבודה מרחוק לתקופה ממושכת נדרשו משרדי הממשלה לבצע פעולות שונות, ובהן רכש של מחשבים ניידים, הגדלת מספר רישיונות החיבור מרחוק, הרחבת תשתיות התקשורת (רוחב הפס), רכישת "קוראי כרטיסים", רכישת מצלמות רשת וציוד נוסף. מבדיקת משרד מבקר המדינה עולה כי בחלק מהפעולות סייעה רשות התקשוב למשרדי הממשלה. במסגרת זו, ומאסמכתאות שהועברו למשרד מבקר המדינה עולה כי רשות התקשוב קיימה באופן עיתי ישיבות עם המנמ"רים של משרדי הממשלה על מנת לעמוד על הפערים והחסמים הפוגעים בהיערכות לעבודה מרחוק ולסייע בגיבוש פתרונות להתמודד עמם במידת האפשר. יצוין כי משיחות שקיים משרד מבקר המדינה עם המשרדים שנבדקו פרטנית בביקורת עלה כי הישיבות העיתיות לצד שיח לא פורמלי ושיתוף פעולה בין המנמ"רים לבין עצמם קידם את יכולת המשרדים להתמודד עם הצרכים שעלו. להלן פרטים על הפעולות שנעשו בתחום זה:

רכש מחשבים ניידים בתקופת החירום

עם פרוץ המשבר ביצעה רשות התקשוב מיפוי של תמונת המצב מול משרדי הממשלה על מנת לעמוד על הפערים הקיימים בהיערכות לעבודה מרחוק ולסייע בצמצומם. אחד הפערים שהועלו נגע למחסור במחשבים ניידים - במסגרת המעבר לעבודה מרחוק נדרשו משרדי הממשלה לספק מספר גדול יותר של מחשבים ניידים לעובדים החיוניים. רשות התקשוב בדקה בסקר שביצעה במרץ 2020 לכמה עובדים יש מחשבים ניידים המאפשרים חיבור מרחוק ולכמה עובדים נדרש חיבור מרחוק - על פי הגדרת היחידות המקצועיות. הבדיקה האמורה העלתה כי יש מחסור בכ-1,500 מחשבים ניידים.

בהמשך לכך, ב-15.3.20 התקיים דיון בוועדת מכרזים מרכזיים למחשוב וטכנולוגיה במשרד האוצר למתן פטור מחובת מכרז לרכישת מחשבים ניידים עקב התפשטות נגיף הקורונה. הדיון עסק במחשבים הניידים הדרושים לכלל משרדי הממשלה, יחידות הסמך ובתי החולים הממשלתיים. בפרוטוקול הדיון צוין כי מנתוני רשות התקשוב וכן מפניות שהתקבלו במינהל הרכש עולה כי יש צורך מידי בכ-2,500 מחשבים ניידים. עוד צוין בפרוטוקול הדיון כי מבדיקה שביצע צוות מקצועי עלה כי מלאי המחשבים בישראל מוגבל מאוד, וזאת נוכח היערכות כלל



הגורמים במשק לעבודה מהבית. הצוות המקצועי פנה למגוון רחב של ספקים ויצרנים, ולמועד זה המלאי המצטבר של המחשבים אצל הספקים שאליהם פנו הסתכם בכ-2,000 בלבד. "לאור האמור, נוכח הנסיבות המיוחדות והנדירות של התפרצות נגיף הקורונה והצורך להיערכות לעבודה מהבית בזמן קצר ככל הניתן ממליץ הצוות המקצועי לאשר התקשרויות לרכישת מחשבים ניידים ללא מכרז". הוועדה החליטה לאשר את הבקשה בכפוף לכמה תנאים: האישור יוגבל ל-2,500 מחשבים ניידים; לא תאושר רכישה של מחשב נייד בסכום גדול מ-1,700 דולר לפני מע"ם; האישור יהיה בתוקף עד 30.4.20 או עד שהספקים הזוכים במכרז יחדשו את המלאי של המחשבים בתצורות הזוכות במכרז המרכזי, לפי המוקדם בהם; הזמנות המשרדים תהיינה טעונות אישור של מנהל הרכש; היקף כל ההתקשרויות לא יעלה על סך כ-15 מיליון ש"ח כולל מע"ם.

בהמשך לכך, ב-16.3.20 המליצה ועדת הפטור של משרד האוצר לשר האוצר על מתן פטור מחובת מכרז לרכישת מחשבים ניידים, בתנאים האמורים לעיל. ב-19.3.20 אישר שר האוצר דאג את ביצוע ההתקשרות האמורה בפטור ממכרז.

מנתוני מינהל הרכש, שהועברו למשרד מבקר המדינה בדצמבר 2020, עולה כי בהתבסס על הפטור האמור נרכשו 1,997 מחשבים עבור 47 גופים, בעלות כוללת של כ-7 מיליון ש"ח (כולל מע"ם).

מבירור שקיים משרד מבקר המדינה עם המשרדים שנבדקו בביקורת באופן פרטני עולה כי המשרדים רכשו מחשבים ניידים גם שלא במסגרת הפטור ממכרז האמור אלא על ידי התקשרויות שביצעו בעצמם באופן עצמאי בהתבסס על המכרז המרכזי לאספקת מחשבים למשרדי הממשלה⁵⁹.

הספקת שירותי מחשוב למשרדי הממשלה

שירותי המחשוב בממשלה מבוצעים באמצעות נותני שירותים העובדים מטעם ספקי שירות שזכו במכרז מרכזי⁶⁰. בהתאם להוראות המכרז, הספקת השירותים על ידי נותני השירותים מתבצעת באתרי הממשלה בכל רחבי הארץ או כפי שיקבע המזמין. כמו כן, נקבע בהוראה כי אין חובה שנותני השירותים יוצבו דרך קבע באתר המשרד מקבל השירות, וכי ניתן יהיה לספק את שירותי המחשוב מאתר הספק או מכל מקום אחר אשר יאשר המזמין ויאפשר את מתן השירות למשרד.

ב-16.3.20 הוציא מנהל מינהל הרכש הממשלתי אישור למשרדי הממשלה ולפיו במצב של מעבר למשק בשעת חירום, מנכ"ל המשרדים רשאים לאשר לספקים הרלוונטיים לתת בתקופה זו שירות מרחוק למשרדי הממשלה בתחומים המאפשרים מתן שירות במתכונת זו, דוגמת שירותי פיתוח תוכנה, תפעול תשתיות ותמיכת משתמשים, וזאת באמצעות נותני השירותים העובדים מטעם ספקים אלה. בהודעה הובהר עוד כי יש לאפשר פעילות זו בהתבסס על שיקול דעת ובאופן מתוכנן במקומות שבהם הדבר אפשרי וניתן לפיקוח ובקרה, וכי צעד זה יאפשר את קידום משימות הממשלה לצד הפחתת הפגיעה בפעילות במשק.

59 מכרז מרכזי מספר 18-2017, "אספקת מחשבים עבור משרדי הממשלה". יצוין כי המשרדים מחויבים בביצוע רכישת המחשבים אך ורק מהספקים הזוכים במכרז, בהתייחס לצורכיהם ולמחירי התצורות.

60 מכרז מרכזי 1-2009 לאספקת שירותי מחשוב בתחומי טכנולוגיות המידע למשרדי הממשלה.



פעולות ממשל זמין

יחידת ממשל זמין מבצעת ייזום, פיתוח ותפעול של תשתיות ופתרונות טכנולוגיים מאובטחים לצורך פעילות שוטפת של משרדי הממשלה ויחידות הסמך. היחידה מעניקה שני שירותים או מוצרים: שירותים רוחביים הניתנים לכלל משרדי הממשלה. שירותים אלו מחויבים בהשתתפות כספית של משרדי הממשלה; שירותים או מוצרים הניתנים על פי הצורך של משרדי הממשלה ובהתאם לשיקול דעתם אם לצורך שירותים אלו מממשל זמין או לאו. התשלום שמשלם מקבל השירות לממשל זמין תמורת שירותים אלה נקבע בהתאם לסיכום עמה. בין היתר, היחידה מספקת למשרדי ממשלה הרוכשים את שירותיה כלים מאובטחים לעבודה מרחוק, כגון שירות גישה מרחוק (מוצר המאפשר גישה מרחוק לרשת הארגונית באמצעות חיבור מאובטח ומוצפן) ושירות סנכרון סלולרי (מוצר המאפשר גישה מאובטחת לרכיבי הדואר האלקטרוני, ליומן, ליישומים ארגוניים ולשרת הקבצים). לצד אלו, היחידה אף מספקת מוצרי מדף אינטרנטיים המתאימים לקיום פגישות וירטואליות ושיחות ועידה⁶¹.

נכון לדצמבר 2020 משתמשים 19 משרדי ממשלה בשירות הגישה מרחוק של ממשל זמין ו-25 משרדים מחוברים לשירות סנכרון סלולרי של ממשל זמין.

משרד מבקר המדינה פנה לממשל זמין על מנת לבחון את הפעולות שנעשו על ידו במסגרת ההתמודדות עם משבר הקורונה והצורך בהרחבת היקף העבודה מרחוק. בספטמבר ובדצמבר 2020 מסר ממשל זמין למשרד מבקר המדינה כי במסגרת ההיערכות של רשות התקשוב, וכדי לתת מענה מיטבי למשרדי הממשלה ולאפשר להם רציפות עבודה, יחידת ממשל זמין ביצעה פעולות רבות בעלות כוללת של כ-15.8 מיליון ש"ח. בין הפעולות העיקריות שביצעה: עיבוי תשתיות החומרה (שרתים, זיכרון, מעבדים וכדומה) - תוספת של כ-40%; העלאת קצב התעבורה מול כל ספקיות האינטרנט בעוד 1 ג'יגה; הגדלת קו ה-IPVPN⁶² הראשי מול כל המשרדים מ-1 ג'יגה ל-2 ג'יגה; הוספת רישיונות גישה מרחוק - קודם למשבר הקורונה היו כ-300 רישיונות לכלל המשרדים, לאחר פרוץ המשבר הוגדל מספר הרישיונות באופן שיאפשר עבודה של 2,500 משתמשים בו זמנית; הוספת מערכי אחסון - קודם למשבר הקורונה מערך האחסון היה בנפח של כ-2 טרה (TERA), כיום מערך האחסון הוא בנפח של כ-10 TERA; הגדלת צוות המומחים בתחום התקשורת והבקרה של ממשל זמין; הפעלת צוות התמיכה בכל שעות היממה (24/7).

כמו כן, ממשל זמין ציין כי איפשר למשרדים שהיו מעוניינים בכך לקבל דוח יומי על שימוש המשתמשים במוצרי גישה מרחוק; נוספה אפשרות לחיבור מרחוק באמצעות שימוש בסיסמה חד-פעמית (OTP)⁶³ - כדי שניתן יהיה לסייע למשתמשים במקרים שבהם נחסם הכרטיס החכם או פג תוקפו; וניתנה למשרדים האפשרות להוסיף משתמשים או להפחית את מספרם בהתאם לצורך (אחת לחודש). ממשל זמין ציין עוד כי פעל מול הספק להחיל את עלות הרישוי בעקבות הגידול במספר המשתמשים במוצר.

61 כגון - WEBEX, TEAMS, ZOOM.

62 IPVPN (IP Based Virtual Private Network) - רשת תקשורת וירטואלית מאובטחת הבנויה על גבי תשתית האינטרנט הציבורית.

63 One-Time Password: מוצר המשמש להזדהות חזקה, ע"י קוד שמתחלף כל כמה שניות, דבר המאפשר כניסה מאובטחת לארגון ולאפליקציות שונות.



ממשל זמין הוסיף כי לנוכח הפעילות האמורה, הוא לא נדרש לנקוט פעולות מיוחדות נוספות לשם התמודדות עם הסגר השני, למעט הוספת רישיונות או משאבים בהתאם לקצב גידול המשתמשים, וכי התשתיות של ממשל זמין הוקמו באופן המאפשר להגדיל את היקף המשאבים בהתאם לצורך. ממשל זמין הוסיף כי אחת התובנות מתקופה זו היא שנדרש לאפשר גם לספקים לעבוד מרחוק (כחלופה להגעה פיזית ליחידה על מנת לטפל בשרתים), וכי הם פועלים לתת מענה לכך.

היערכותם לעבודה מרחוק של משרדי הממשלה שנבדקו פרטנית

כדי לאפשר עבודה בחיבור מרחוק למספר גדול והולך של עובדים לאחר פרוץ משבר הקורונה נדרשו משרדי הממשלה לבצע רכישות של ציוד ולהרחיב את תשתיות התקשורת שלהם. משרד מבקר המדינה בדק עם חמשת המשרדים שנבדקו פרטנית בביקורת זו כיצד נערך כל אחד מהם לכך, באלו פעולות נקט ומה היו החסמים והקשיים שעיינום הם נאלצו להתמודד, ולהלן יובאו עיקרי הדברים שהועלו:

משרד המשפטים	במשרד כ-6,500 עובדים⁶⁴. בתחילת המשבר, במרץ 2020, לכל העובדים שהוגדרו כעובדים חיוניים הייתה יכולת עבודה מרחוק. בהמשך, וכדי לאפשר רציפות תפקודית נרחבת יותר הורחבה יכולת ההתחברות מרחוק, ובמסגרת זו: סופקו כ-400 מחשבים ניידים נוספים מתוך מאגר מחשבים שהיו מיועדים לגריטה (לפני משבר הקורונה היו כ-2,800, ובמועד סיום הביקורת מספרם 3,200); שודרגה תשתית החיבור מרחוק; נרכשו רישיונות לתמיכה בחיבור של כ-3,225 עובדים בו זמנית; הופעל ערוץ התחברות נוסף מאתר הגיבוי לשם איון עומסים ושיפור איכות החיבור לעובדים; סופקו כרטיסי SIM על מנת לאפשר עבודה מרחוק לעובדים ללא חיבור אינטרנט בבית; הורחבה אופציה המאפשרת עבודה מאובטחת מרחוק מכל מחשב וניתנה אפשרות לקבלת ציוד משרדי משלים לעבודה מהבית (כגון - מסכים, מקלדות). ההצטיידות להרחבת היקף העבודה מרחוק מומנה על חשבון תקציב שהוקצה במקור לפעילויות אחרות של המשרד שנכללו בתוכנית העבודה (לפני פרוץ משבר הקורונה). אשר לתקלות שבהן נתקלו עובדים שהתחברו מרחוק: המשרד ציין כי בשבוע הראשון של המשבר הוטל עומס גדול על קווי התקשורת, והדבר גרם לרמת חיבור ירודה למשרד, עד להשלמת שדרוג התשתית למצבה הנוכחי. עוד ציין המשרד כי עומסים ותקלות בתשתיות ספקי האינטרנט הארציים השפיעו גם הם על יכולת העבודה מרחוק.
--------------	--

64 העובדים במשרד המשפטים כוללים בין היתר עובדי מדינה, מתמחים, סטודנטים ועובדי קבלן.



משרד המדע

במשרד 130 עובדים. כלל עובדי המשרד יכולים להתחבר למשרד מרחוק בו-זמנית. עם תחילת המשבר המשרד נדרש לרכוש ציוד כדי לתמוך בעבודה מרחוק של העובדים וכן להרחיב את תשתיות התקשורת שלו. במסגרת זו: נרכשו מחשבים ניידים; נרכשו דיסקים שאפשרו החזרת מחשבים מגריטה ושדרוג מחשבים קיימים; שודרגה תשתית תעבורת הנתונים (רוחב פס); נרכש מודול איזון עומסים; נרכשו "קוראי כרטיסים"; נרכשו מצלמות רשת ורמקולים ובוצעו הדרכות לעובדים בנושא חיבור מרחוק ושימוש במערכות וידאו דיגיטליות. כמו כן, עובדים אשר הצהירו כי יש להם מחשב פרטי המאפשר עבודה מרחוק קיבלו ציוד משלים במידת הצורך (למשל, קורא כרטיסים למחשב פרטי). יתר העובדים קיבלו מחשבים ניידים מהמשרד. הפעולות מומנו מהתקציב השוטף של אגף מערכות מידע. מסגרת התקציב שהוקצתה לטובת הנושא עמדה על כ-300 אלף ש"ח.

אשר לתקלות, המשרד ציין כי מקורן היה בעיקר עומסים ותקלות בתשתיות ספקי האינטרנט הארציים וחוסר ידע של העובדים לגבי עבודה מרחוק ושימוש בכלים השונים, וכי הוא טיפל בכך באמצעות הדרכת העובדים.

משרד הפנים

במשרד כ-600 עובדים, ולכ-150 מהם היו מחשבים ניידים שסיפק להם המשרד עוד קודם לפרוץ המשבר. בתחילת המשבר כ-190 מהעובדים הוגדרו עובדים חיוניים (בהמשך מספרם גדל לכ-210), וחסרו להם כ-50 מחשבים ניידים. במסגרת ההיערכות להרחבת היקף העבודה מרחוק ביצע המשרד כמה פעולות, ובהן: רכש של 30 מחשבים ניידים; המרת "חדר הדרכה נייד" של המשרד כדי שניתן יהיה לספק את המחשבים הניידים שבו לעובדים; רכש רישיונות נוספים לגישה מרחוק; שדרוג תשתיות התקשורת. בהמשך, כדי לעמוד בהוראות התו הסגול, נרכשו עוד כ-50 מחשבים, וכל שני עובדים עשו רוטציה ביניהם⁶⁵. מימון הפעולות בוצע בחלקו מהתקציב השוטף ובחלקו מתקציב ייעודי שהוקצה לשם כך. הוקצתה תוספת של כ-400 אלף ש"ח ומהתקציב השוטף עוד כ-600 אלף ש"ח.

אשר לתקלות, המשרד ציין כי הנפוצות שבהן נגעו לחוסר עדכון של תוכנת אנטי-וירוס ולצורך בביצוע עדכונים, לתקלות ברשת האינטרנט הביתית ולחוסר ידע של המשתמשים בהפעלת ההתחברות מרחוק.

65 מלבד אלו שהיה להם מחשב נייד קבוע עוד קודם למשבר הקורונה.



משרד התחבורה

במשרד כ-1,000 עובדים. במסגרת ההיערכות לעבודה בחיבור מרחוק - המשרד ביצע רכש של מחשבים ניידים והרחבה של רישיונות החיבור מרחוק באופן שכ-500 עובדים יכולים לעבוד מרחוק בו-זמנית. הפעולות מומנו מהתקציב השוטף של אגף טכנולוגיות דיגיטליות ומידע של המשרד, על חשבון פעולות פיתוח שתכנן האגף, אשר ביצען נדחה. המשרד ציין כי נראה שנדרש להקצות תקציב נוסף גם בשנים הקרובות על מנת להעביר חלקים גדולים מהעובדים לעבודה עם מחשבים ניידים וכי נעשית על ידו בחינה תקציבית ומחשובית באשר למעבר לעבודה עם תחנות עגינה.

המשרד ציין כי הבעיה העיקרית שהקשתה עליו לפעול בסגר הראשון הייתה חוסר היכולת לספק שירות ומענה טלפוני מרחוק כתחליף לקבלת קהל פרונטלית. המשרד עדכן כי חל שינוי בעניין זה, וכי הוא החל לתת מגוון של שירותים באמצעות שיחה טלפונית, תוך אימות זהותו של הפונה בדרכים שונות⁶⁶. נכון לאוקטובר 2020, התקיימו כ-3,500 שיחות שירות ביום שהחליפו שירות פרונטלי.

אשר לתקלות, המשרד ציין כי רובן היו קשורות לצורך בשחזור סיסמה או לתשתית האינטרנט הביתית או לעומס על הרשת הסלולרית (לחלק מהמחשבים הוקצה סים עבור גלישה).

המשרד להגנת הסביבה

במשרד כ-750 עובדים. לפני משבר הקורונה היו לכ-400 עובדים מחשבים ניידים שסיפק להם המשרד (כמו כן אפשר לבצע חיבור מאובטח מרחוק גם ללא מחשב נייד לכ-40 עובדים). במהלך משבר הקורונה נעשו כמה פעולות כדי לאפשר עבודה מרחוק, בכלל זה: רכש של כ-50 מחשבים ניידים; שדרוג תשתיות התקשורת (רוחב פס); הגדלת מספר רישיונות החיבור מרחוק באופן שכ-400 עובדים יכולים להתחבר בו זמנית (קודם לכן יכלו להתחבר בו-זמנית רק 100 עובדים); רכש רכיב ניתוב עומסים; הקצאת כרטיסי סים, מצלמות ואוזניות. נכון לנובמבר 2020 יש בארגון כ-610 מחשבים ניידים. פעולות אלה ממונו מתקציב ייעודי על סך של כ-400 אלף ש"ח שהקצה המשרד לטובת הנושא בעקבות המשבר.

אשר לתקלות, המשרד ציין כי בתחילה היו בעיות בהתחברות מהבית עקב עומס מתחברים ופניות רבות למוקד התמיכה, וכי על מנת להתמודד עם כך בוצעו איוון עומסים בהקשר של המתחברים מרחוק ועיבוי של מוקד התמיכה, לרבות פתיחת מוקד ערב באופן חד-פעמי.

66 התנאי למתן שירות טלפוני הוא אימות זהות הפונה באופן ודאי באמצעות שימוש בשלושה פרטי מידע מתוך חמשת פריטי המידע האלה: שם פרטי ושם משפחה; מספר זהות; מספר רישיון נהיגה; תאריך הוצאת רישיון נהיגה; מספר רכב (לבעלי רכב).



מתשובות המשרדים שהועברו לידי משרד מבקר המדינה במהלך הביקורת עולה כי הם נקטו מגוון פעולות כדי להרחיב את היקף העבודה מרחוק ולאפשר עבודה תקינה ורציפה. למשל, נרכשו מחשבים והושמשו מחשבים ניידים ישנים שהיו מיועדים לגריטה, הורחבו תשתיות התקשורת ותשתיות הגישה מרחוק ונרכש ציוד נלווה. הפעולות האמורות ננקטו בתוך זמן קצר, וחלקן מומנו על חשבון תקציבים שהוקצו במקור לפעילויות אחרות שהמשרדים תכננו לבצע בשנת 2020. לצד זאת, המשרדים נתקלו בתקלות שעיקרן נבע מעומס על מערכות ההתחברות מרחוק, מבעיות ברשת האינטרנט הארצית ומחוסר ידע של העובדים כיצד לעבוד מרחוק.

משרד מבקר המדינה מציין לחיוב את פעולות ההיערכות האמורות. לנוכח תמונת המצב המצטיירת מהממצאים, וכדי להבטיח היערכות סדורה של משרדי הממשלה לעבודה מרחוק בתרחישים שונים ובטווח הארוך, מומלץ כי כל אחד מהמשרדים יבצע הליך של הפקת לקחים ובהתבסס על כך תוכן תוכנית עבודה סדורה שתפרט אילו כלים וצעים יש לנקוט על מנת להבטיח את המענה השלם והדרוש כפי שיוגדר לצורך התמודדות עם תרחישים שונים. כמו כן מוצע כי יבוצעו הדרכות עיתיות לעובדים בנושא עבודה מרחוק ושימוש בכלים המאפשרים זאת ויקבע מנגנון לקבלת משוב מהעובדים.

עוד מומלץ כי המשרדים יבחנו הצורך בתקצוב הפעולות שנדחו וכן יגבשו תוכנית להצטיידות במחשבים חדשים לשם עבודה מרחוק, בהתאם למדיניות שתקבע על ידם. מהלך זה נדרש במיוחד במשרדים בהם נעשה שימוש בפתרונות זמניים על מנת לתת מענה מידי לצרכים שעלו במהלך משבר הקורונה, כגון: שימוש במחשבים ישנים שנועדו לגריטה, הקצאת מחשבים ברוטציה בין שני עובדים, שימוש במחשבי חדר הדרכה או התאמות שבוצעו במחשבים פרטיים של העובדים.

משרד המשפטים מסר למשרד מבקר המדינה באפריל 2021 כי הוא ביצע משוב על העבודה בתקופת חירום, לרבות העבודה מהבית, תוך התמקדות באיכות המענה התקשובי. על המשוב ענו כ-1,800 (יותר מ-40%) מעובדי המדינה במשרד. עוד מסר המשרד כי הוא קיים הדרכות הנוגעות לעבודה מהבית הן בהיבט של אוריינות דיגיטלית והן בהיבטים הנוגעים ליעילות ולאפקטיביות של עבודה מהבית ולאבטחת מידע, בכלל זה נשלחה לכלל עובדי המשרד לומדה לפעילות בטוחה במרחב הסייבר. המשרד הוסיף כי בכוונתו לשוב ולקבל משוב על עבודה מהבית תוך התמקדות בהיבטים הטכנולוגיים.

בתשובת משרד המדע מאפריל 2021 נאמר כי המשרד קיים תהליך הפקת לקחים בתחילת שנת 2021, וכי הלקחים האמורים באו לידי ביטוי בתוכניות העבודה של האגפים הרלוונטיים.

משרד התחבורה מסר בתשובתו מאפריל 2021 כי בשנים 2020 ו-2021 בוצעו הדרכות אבטחת מידע לעובדי המשרד, אשר כללו נושאים כלליים ובהם נושא החיבור מרחוק.





מתמונת המצב שתוארה לעיל, ובהתבסס על מידע שהתקבל בפגישות והתכתבויות שקיים משרד מבקר המדינה עם מנמ"רים במשרדי הממשלה שנבדקו בביקורת פרטנית, עלו כמה תובנות והמלצות, כמפורט להלן: (א) תשתית העבודה מרחוק שהייתה קיימת בשגרה עוד טרם פרוץ משבר הקורונה, היוותה תשתית יסודית שתמכה ביכולתם של המשרדים להרחיב את היקף העבודה מרחוק בתוך טווח זמן קצר עם תחילתו של המשבר. מומלץ להמשיך לבסס בעיתות שגרה את התשתיות הנדרשות לעבודה מרחוק באופן שיבטיח מענה שלם וגמיש גם במצבי חירום שבהם יידרש לספק אפשרות של עבודה מרחוק יציבה ומאובטחת להיקף רחב יותר של עובדים; במסגרת זו יש לבחון מה העבודה הנדרשת מעובדים חיוניים במצבי חירום והאם ניתן לבצעה בעבודה מרחוק. ככל שניתן לבצעה מרחוק, מומלץ להעמיד לרשותם תשתית מחשובית שתאפשר זאת (ב) עלה כי חלק ניכר מהעובדים לא התנסו בעבודה מרחוק קודם למשבר הקורונה ולכן חוו קשיי הסתגלות. מומלץ לבצע הדרכה והכשרה מבעוד מועד לכלל העובדים באשר למיומנויות הנדרשות להם לשם עבודה מרחוק, לרבות בנוגע לשימוש בפתרונות טכנולוגיים נוספים לצורך כך (כגון שימוש בתוכנות שונות לביצוע שיחות וידאו דיגיטליות), לקבוע מנגנון לקבלת משוב מהעובדים ולהסדיר תוכנית הדרכה רציפה ומוקד לסיוע לעובדים בהתמודדות עם תקלות; (ג) הועלה כי חלק מהמשרדים נתקלו בקשיים בהקצאת תקציבים לטובת יישום מודל העבודה מרחוק. מומלץ לגבש תוכנית הפעלה בחירום שתאפשר מתן מענה לנסיבות חריגות בהיבט של המשאבים (תקציב, התקשרויות, כוח אדם, פעילות ספקים ועוד); (ד) במהלך משבר הקורונה נעשו פעולות שונות לקידום שירותים דיגיטליים חלופיים לשירות פרונטלי (כגון במשרד התחבורה). מדובר בפעולות משמעותיות שיש להמשיך ולבסס באופן שוטף. מומלץ לגבש תפיסת הפעלה ממשלתית רוחבית בנוגע לשירותים הדורשים מענה קהל פרונטלי, תוך התחשבות בתשתית הנדרשת לשם הסבת השירות לדיגיטלי ולשם מתן מענה מקצה לקצה, בהתרחש אירועים שונים; (ה) הועלה כי שיתוף ידע בין המנמ"רים, הן שיח פורמלי באמצעות הערכות המצב העתיות שקיימה רשות התקשוב, והן שיח בלתי פורמלי, שקיימו המנמ"רים אחד עם השני, סייע בהתמודדות עם האתגרים שהתעוררו בעקבות משבר הקורונה. מומלץ להמשיך ולבסס את הערוצים לשיתוף בידע כדי שניתן יהיה להפעילם בעיתות שגרה וחירום.

היבטי אבטחת מידע והגנת סייבר בעבודה מרחוק

פעילותם התקינה של משרדי הממשלה מושפעת מרמת הסודיות, השלמות, הזמינות והשרידות של המידע, מערכות המחשוב המעבדות והמאחסנות אותו ותשתית התקשורת. כמו בכל ארגון גם במשרדי הממשלה נשקפת סכנה של זליגת המידע הנמצא במערכות המידע שלהם או של תקיפות המכוונות לגנוב מידע, לשבש אותו או לפגוע בו. פגיעה במידע עלולה לגרום לנזקים תפעוליים, טכנולוגיים וכספיים הקשורים לביטחון ולשלום של אדם או של הציבור, וכן לגרום לפגיעה בצנעת הפרט של אזרחי המדינה, לפגיעה במוניטין ובתדמית של המשרדים והמדינה.



אבטחת מידע משמעה כלל הפעולות והאמצעים שארגון נוקט ומיישם כדי להבטיח כי המידע יהיה מוגן מפני פגיעה, חשיפה ושינוי במזיד או בשוגג, באופן שישמרו הזמינות, המהימנות, הסודיות והשלמות של המידע.

מרחב הסייבר הוא מרחב וירטואלי ופיזי הנחלק לשלושה רבדים מרכזיים: רובד פיזי - כלל רכיבי המחשוב והתקשורת; רובד לוגי: הקודים המפעילים את רכיבי המחשוב וקובעים כיצד יפעלו; רובד אנושי: כלל המשתמשים ברשת.

הגנת סייבר היא כלל הפעולות המתבצעות והכלים המיושמים בכל שלושת הרבדים (הפיזי, הלוגי והאנושי) כדי להגן על נכסי הסייבר⁶⁷ במשרד, לרבות הפעולות שנעשות למניעה, להתמודדות ולטיפול בתקיפה או באיום סייבר, ולצמצום הנזק שנגרם כתוצאה מכך.

הגנת סייבר כוללת ביצוע פעולות לאבטחת המידע, בין היתר תוך שימוש בכלים כדי למנוע כניסת "נזקות"⁶⁸ למערכת המידע ולאתר כאלה שכבר חדרו אליה, ניטור של המידע העובר ברשת והפעלת אמצעי הגנה כדי למנוע פגיעה במערכות ובמידע.

סיכונים הכרוכים בעבודה מרחוק

עבודה מרחוק ומתן גישה מרחוק לרשת הפנימית ולמערכות המידע של הארגון מעצימה את האיומים הנשקפים לו עקב קושי בשליטה על פעילות מחוץ לחצרותיו. חולשה או היעדר של הגנות פיזיות ולוגיות מספקות של עמדות קצה המתחברות מרחוק לארגון מגדילות את הסיכונים לפגיעה במידע.

כמה מהסיכונים הנשקפים לארגון שקשורים לעבודה מרחוק הם ציתות לתעבורת המידע ברשת התקשורת, התחזות, יכולת גישה למידע של גורם שאינו מורשה לכך, זליגת מידע, חוסר יכולת אכיפה של מדיניות אבטחה ארגונית; גישה מרחוק באמצעות מכשיר לא מאובטח; גנבה או אובדן של מחשב או מכשיר נייד המכיל חומר רגיש ואפשרות גישה באמצעותו לרשת הארגונית. גם שימוש בתוכנות השתלטות מרחוק לשם מתן תמיכה למשתמשים עלולה לחשוף את הארגון לתקיפות סייבר. סיכון נוסף הנקשר לעבודה מרחוק נוגע להוצאת המחשב מרשת המשרד והחזרתו לרשת⁶⁹. פעולה זו עלולה לגרום לכך שהמחשב יחזור לארגון כשאינו "נקי" בגלל שאמצעי ההגנה על המחשב מופחתים בעת הימצאותו מחוץ לרשת הארגונית⁷⁰.

שימוש בפלטפורמות פגישות וידאו דיגיטליות המאפשרות קיום פגישות מרחוק⁷¹ כרוך אף הוא בכמה סיכונים. למערכות אלו מגוון יכולות, ובהן ניהול משימות, העברת קבצים, שליטה מרחוק והקלטת שיחות בענן. בין האיומים הנלווים לכך - חשיפת מטה-דאטה (כגון מידע על נושא הפגישה, המשתתפים, כתובות הדואר האלקטרוני שלהם, נתונים טכנולוגיים כגון כתובת ה-

67 נכס סייבר - מערכת מחשב שתפקודה התקין נדרש לשם הבטחת רציפות התפקוד של המשרד.

68 נזקה - שם כולל לכל סוגי התוכנות שנועדו להזיק למערכת, לחדור אליה או להפריע לפעולתה.

69 כגון במקרים של שימוש במחשבים ניידים ותחנות עגינה במשרד.

70 יצוין כי יש בנמצא בקורות המפצות על כך, כמו כלים שיקפחו על המחשב ויודאו שרמת האבטחה שלו אינה נפגעת עקב הוצאתו מחוץ לכותלי הארגון.

71 כגון - WEBEX, TEAMS, ZOOM.

IP⁷²); זיהוי לא מוקפד של כל משתתף⁷³; אפשרות להשתתפות בפגישה של משתתפים סמויים⁷⁴; העברת קבצים ללא פיקוח; הקלטת שיחות וידאו בענן ושימוש בפגישה או בפלטפורמה כבסיס לתקיפה. כמו כן, הגורם השלישי (בעל הפלטפורמה) מקבל אחריות לאבטחת המידע⁷⁵.

איום נוסף שעשוי לבוא לידי ביטוי, בין היתר, במסגרת מתן גישה מרחוק נקשר למימוש תקיפת סייבר באמצעות "הנדסה חברתית" (Social Engineering) - ניצול תכונות פסיכולוגיות אנושיות לשם הונאה, שכנוע והתחזות, הגורמים לאדם לציית מרצון לבקשת התוקף ולמסור לידי מידע אישי על עצמו או על ארגונו. הנדסה חברתית יכולה להתבצע באמצעות טכנולוגיות מגוונות כגון שיחת טלפון, דואר אלקטרוני והודעות טקסט. התוקף יכול להתחזות לכל דמות שתשרת את מטרותיו, לדוגמה לעובד הנדרש לחיבור מרחוק לשם ביצוע עבודתו.

הסיכונים הטמונים בעבודה מרחוק עלולים להביא לפגיעה בכמה היבטים:

תרשים 20: הסיכונים הטמונים בעבודה מרחוק



- 72 כתובת IP (Internet Protocol) - כתובת המוצגת בתבנית מספרית המשמשת לזיהוי נקודות קצה, כגון מחשב, מדפסת וכו'.
- 73 לא מתבצע אימות של זהות המשתתפים מעבר לקבלת הצהרותיהם.
- 74 המשתתפים בפגישה מנוהלים על ידי הפלטפורמה, ולכן ייתכן שמשתתפים שאינם מוצגים בפלטפורמה משתתפים בפגישה בפועל.
- 75 להרחבה בעניין זה ראו: מערך הסייבר הלאומי, **סיכונים מרכזיים בעת עבודה עם פלטפורמות פגישות וידאו דיגיטליות**, (מרץ 2020).



מערך הסייבר הלאומי מסר למשרד מבקר המדינה בדצמבר 2020 ובאפריל 2021 כי עקב התפרצות משבר הקורונה, רמת הסיכון עלתה במידה ניכרת, בין השאר בשל גידול חד בהיקף העבודה מרחוק במגזר הציבורי והפרטי, הרחבת הפעילות בזירה הדיגיטלית ותהליכי דיגיטציה מואצים של שירותים ציבוריים ופרטיים; זאת ללא הכנה מספקת ולעיתים תוך התפשרות על רמת האבטחה. המערך הוסיף כי שינויים אלו הביאו להגדלה ניכרת של משטח התקיפה וכן יצרו הזדמנויות רבות לאיומים במרחב הסייבר והגדילו את מגוון האיומים הללו. המחשבים הניידים והמכשירים החכמים מאחסנים מידע רב ועלולים לשמש "שער כניסה" פוטנציאלי עבור תוקפים אשר מטרתם לנצל ולאתר הזדמנויות וחולשות, בייחוד במצבים כאלו. המערך עמד על הסיכונים ודרכי ההתמודדות עימם בכמה פרסומים והנחיות שהוציא בנושא חיבור ועבודה מרחוק.⁷⁶

הגדלת היקף העבודה מרחוק בתקופת הקורונה העצימה את הסיכונים השונים שטומנת בחובה העבודה מרחוק ומתן גישה מרחוק לרשת הממוחשבת הפנימית ולמערכות המידע של המשרד והדבר דורש היערכות מתאימה ובקורות מונעות.

לאור זאת וכפי שיפורט להלן, מומלץ כי י"ב תנחה את המשרדים השונים בכל הנוגע להתמודדותם עם רמת הסיכון שגדלה בתקופת משבר הקורונה בשל המעבר לעבודה מרחוק וכי המשרדים יפעלו להגברת הבקורות בשל התעצמות הסיכונים ויшлиמו הצטיידות נדרשת, לצד תגבור הפעולות השוטפות להקטנת סיכונים.

אירועי סייבר בתקופת משבר הקורונה

לפי פרסומי מערך הסייבר הלאומי, במהלך משבר הקורונה זוהו במדינות שונות אינדיקציות רבות למתקפות סייבר המכוונות כלפי בתי חולים, מעבדות לאומיות, ממשלות ואזרחים תוך ניצול הבהלה העולמית כדי לבצע מתקפות דיוג⁷⁷, מניעת שירות, כופרה⁷⁸ ועוד. המערך הוציא כמה התרעות ודיווחים בעניין זה המלמדים על גידול בהיקף מתקפות הסייבר.⁷⁹

76 מערך הסייבר הלאומי פרסם כ-20 מדריכים והמלצות רלוונטיות בנושא המציאות המשתנה, המיועדים לקהלי היעד השונים (מעסקים ועד אזרחים פרטיים). ראו למשל פרסומי מערך הסייבר הלאומי: **איומים מרכזיים בעת עבודה באמצעות פלטפורמות תמיכת משתמשים מרחוק** (22.7.20); **המלצות הגנה לארגונים ועסקים לעבודה מהבית בעקבות התפשטות נגיף הקורונה** (11.3.20); **המלצות הגנה לנתבים ביתיים** (אפריל 2020); **סיכונים מרכזיים בעת עבודה עם פלטפורמות פגישות וידאו דיגיטליות** (מרץ 2020).

77 דיוג (פשינג) הוא אופן התקפה מסוג הנדסה חברתית, ובו עבריין הסייבר מתחזה לגוף אמין תוך שהוא מבקש מהקורבן פרטי מידע רגיש. דיוג עשוי להתבצע באמצעות שליחה של קישור לאתר מתחזה, או שליחת הודעה בדואר האלקטרוני, הודעת טקסט, הודעת ווטסאפ וכו'.

78 כופרה (Ransomware) היא נזקה המשמשת לסחית המשתמש באמצעות הגבלת גישה לקבצים או למשאבים, למטרת קבלת תשלום כספי.

79 בעניין זה ראו: <https://www.gov.il/he/departments/publications/reports/daily>

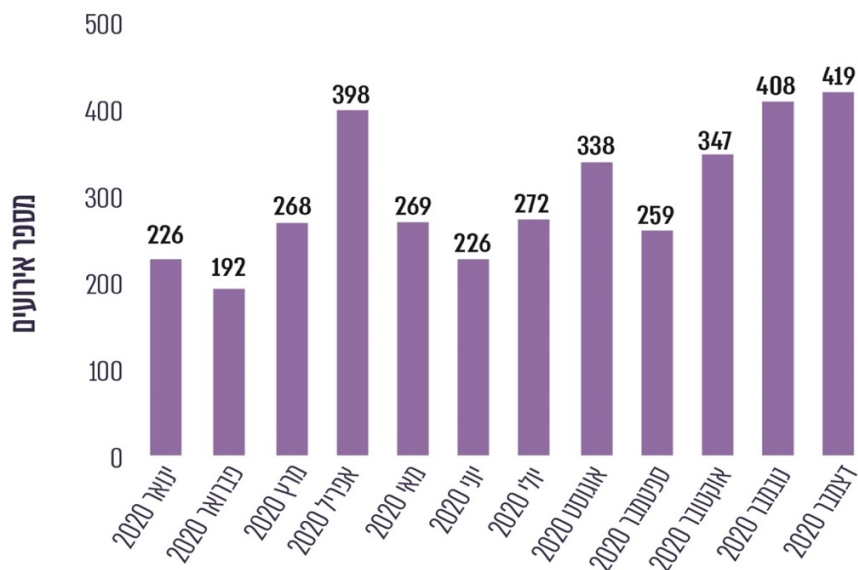


במערך הסייבר הלאומי פועל המרכז הארצי לניהול אירועי סייבר (CERT)⁸⁰, המטפל באירועי סייבר במרחב האזרחי של מדינת ישראל (להלן - ה-CERT הלאומי). אל המרכז מתנקזים דיווחים ומידע מהארץ וממדינות אחרות על ניסיונות לביצוע מתקפות סייבר או על חשדות לביצוען.

בדצמבר 2020 מסר מערך הסייבר הלאומי למשרד מבקר המדינה כי המספר וההיקף של האירועים שנצפו בשנת 2020 גדולים מאשר בשנה הקודמת ועמד על 3,326 אירועים. עוד נמסר על ידו כי עם פרוץ המשבר ובמסגרת התקנות לשעת חירום⁸¹ הוחרגה פעילות מערך הסייבר הלאומי לאור תפקידו הייחודי בהגנה על המרחב הקיברנטי. כמו-כן, המערך פעל להחרגתן של חברות הגנת הסייבר ואבטחת מידע בתקנות לשעת חירום, כך שפעילותן של החברות תוגדר כפעילות חיונית והן ימשיכו לפעול כסדרן.

להלן יוצגו נתוני מערך הסייבר הלאומי על אירועי הסייבר שהתרחשו בשנת 2020 ונוטרו על ידי ה-CERT הלאומי, וכן נתונים אודות אירועי הסייבר שהתרחשו בשנת 2019 לעומת שנת 2020:

תרשים 21: אירועי סייבר שנוטרו על ידי ה-CERT הלאומי, ינואר 2020 - דצמבר 2020



מקור: נתוני מערך הסייבר הלאומי בעיבוד משרד מבקר המדינה.

* הנתונים האמורים אינם כוללים נתונים על אחת המערכות שהעלתה הרבה דיווחי שווא ולכן הוחלט להוציאה משימוש; הנתונים משקפים אירועים בלבד ולא מספר דיווחים ופניות (עשויות להתקבל כמה פניות על כל אירוע).

80 Computer Emergency Response Team.

81 תקנות לשעת חירום (הגבלת מספר העובדים במקום העבודה לשם צמצום התפשטות נגיף הקורונה החדש), תש"ף-2020.



תרשים 22: אירועי סייבר שניטר ה-CERT הלאומי, 2019 ו-2020*



מקור: נתוני מערך הסייבר הלאומי בעיבוד משרד מבקר המדינה.

- * הנתונים המוצגים אינם כוללים פרטים על אירועי פריצה לרשתות חברתיות (כ-5,500 אירועים בשנת 2020).
- * יצוין כי בשנת 2020 אסף מערך הסייבר הלאומי נתונים גם על קמפיינים ודיווחים [קמפיין מוגדר כאירוע גדול עם הרבה דיווחים, דיווח מוגדר כפנייה נוספת (מאדם/ארגון) על אירוע סייבר שכבר נפתח]. בשנת 2020 היו 4 קמפיינים והתקבלו 733 דיווחים.

מרחב הסייבר נתון כל העת לאיומים ולתקיפות. מהנתונים האמורים עולה כי היקף אירועי הסייבר שהתרחשו בשנת 2020 גדול בכ-48% מהיקף האירועים שהתרחשו בשנת 2019. דהיינו, במהלך משבר הקורונה גברו האיומים על מרחב הסייבר במידה ניכרת. מערך הסייבר הלאומי מסר למשרד מבקר המדינה בדצמבר 2020, כי אין בידו מידע שבאמצעותו ניתן לבחון כמה מהאירועים האמורים, נובע באופן ישיר בגין עבודה מרחוק.

במסגרת ה-CERT הלאומי פועל ה-SOC הממשלתי - מרכז שליטה ובקרה שמגבש תמונת מצב ממשלתית שוטפת בהיבטי הגנת הסייבר ומעדכן את הגופים המנטרים (משרדי הממשלה ויחידות הסמך) על אירועי סייבר (או על חשד לאירועים אלה) הנובעים ממערכות ההגנה והמערכות התפעוליות בארגון.

לפי הנתונים המעודכנים לאוקטובר 2020 מחוברים ל-SOC הממשלתי 38 משרדי ממשלה, שבעה משרדים עדיין אינם מחוברים אליו, ועל פי תוכנית העבודה הם יחוברו אליו בשנת 2021. נוכח חשיבות הנושא, יש להבטיח כי חיבור משרדי הממשלה ל-SOC הממשלתי יעשה בהתאם לתוכנית העבודה וללוחות הזמנים שנקבעו בה.

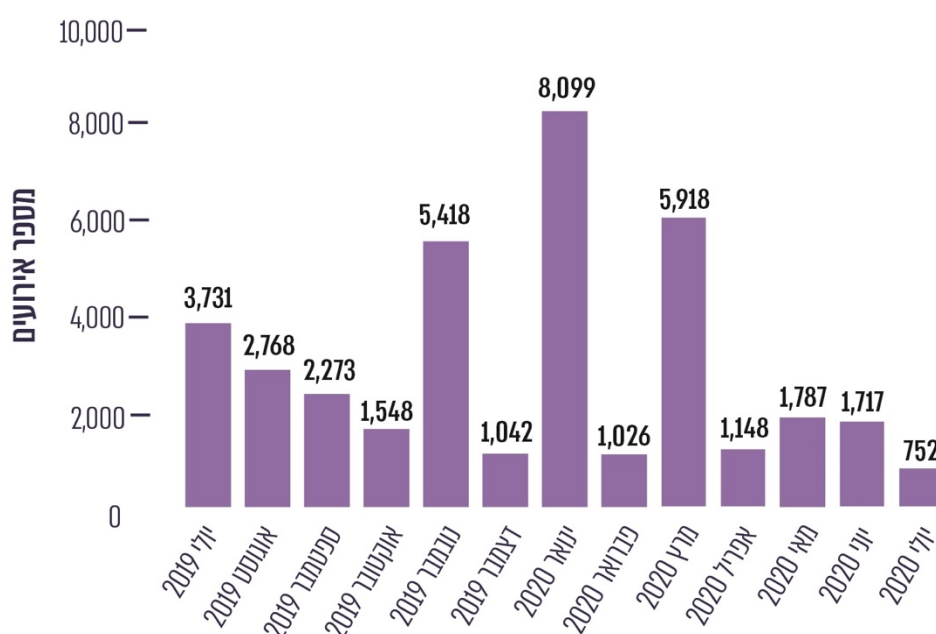
אירועי הסייבר שמרוכזים על ידי ה-SOC הממשלתי כוללים: (1) דיווח מהמשרד - כפי שמצוין בהנחיה; (2) דיווח מודיעיני - ממקורות גלויים (רשתות חברתיות וכו') או ממקורות שאינם גלויים; (3) ניטור על ידי מערכת לניתוח אירועי אבטחת מידע המרכזת דיווחים ממערכות המחשוב השונות (להלן - מערכת ה-SIEM⁸²) המותקנת במשרדי הממשלה. ה-SOC הממשלתי בוחן לגבי כל אחד מהאירועים המנטרים על ידי המערכת אם מדובר בתקלה תפעולית, בפעולה



זיומה לא סטנדרטית שלא דווחה טרם התרחשותה על ידי המשרד, ב- False positive (חיובי כוזב) או באירוע סייבר.

באוגוסט 2020 העבירה יה"ב למשרד מבקר המדינה נתונים על האירועים שנוטרו במערכת ה-SIEM, מיולי 2019 עד יולי 2020:

תרשים 23: אירועים שנוטרו על ידי מערכת ה-SIEM, יולי 2019 - יולי 2020



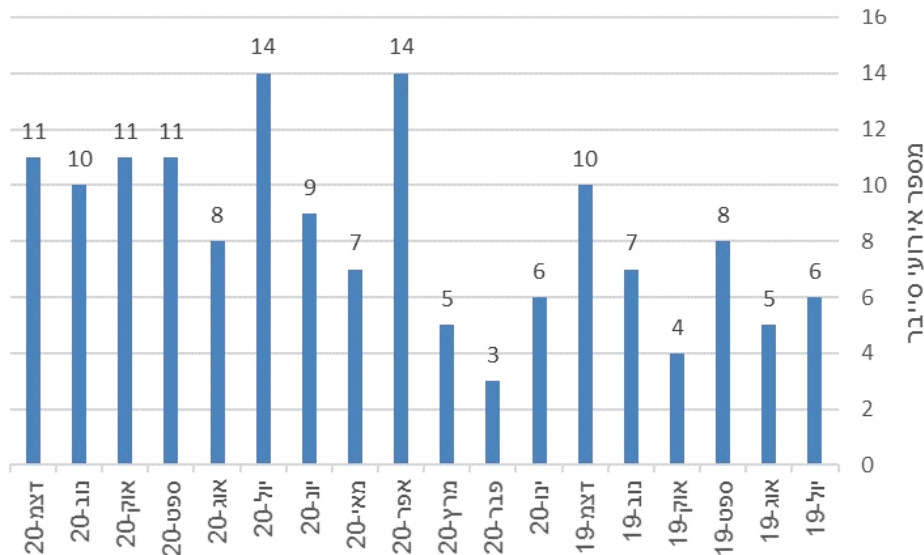
מקור: נתוני יה"ב בעיבוד משרד מבקר המדינה.

כפי שעולה מהתרשים, בין יולי 2019 ליולי 2020 ניטרה מערכת ה-SIEM ב-SOC הממשלתית מדי חודש אלפי אירועים במשרדי הממשלה.

בפברואר 2021 העבירה יה"ב למשרד מבקר המדינה נתונים אודות האירועים שהתבררו בסופו של דבר כ"אירועי סייבר" במשרדי הממשלה, במהלך החודשים יולי 2019 - דצמבר 2020 (כולל):



תרשים 24: אירועי סייבר במשרדי הממשלה, יולי 2019 - דצמבר 2020



בדצמבר 2020 ביצעה יה"ב מיפוי בנושא גישה מרחוק בקרב משרדי הממשלה. מניתוח הנתונים עולה כי חמישה (14%) מ-36 משרדים ציינו כי בעבר התרחש בהם אירוע סייבר באמצעות ממשק החיבור מרחוק.

יה"ב מסרה למשרד מבקר המדינה בדצמבר 2020 בנוגע לאותם אירועי סייבר שעליהם דיווחו המשרדים ושנמצאו כקשורים לגישה מרחוק כי התוקפים ניצלו חולשה (נקודות תורפה / פערי אבטחת מידע אותם ניתן לנצל בכדי לפגוע במערכות המשרד) באחת המערכות המשמשות חלק מהמשרדים לגישה מאובטחת מרחוק, וכי לאחר שהיצרן דיווח על החולשה עודכנה גרסת המערכת. עוד ציינה יה"ב כי אירועים אלו השפיעו על משתמשים מועטים ולא פגיעה מהותית בנכסי משרדים, בתפקוד מערכות הליבה שלהם או בשירותים שהם מספקים לציבור.

משרד מבקר המדינה בירר גם עם המשרדים שנבדקו בביקורת הפרטנית אם התרחשו אצלם אירועי אבטחת מידע הנוגעים לנושא העבודה מרחוק. משרד אחד השיב כי התרחש אצלו אירוע אבטחת מידע ובמסגרתו עובד שעזב את המשרד גרם לנציג מוקד שירות - תוך שימוש בהנדסה חברתית - לחדש את יכולת החיבור שלו למערכות המשרד, ובעקבות כך התחבר אליהן באופן לא מורשה. המשרד ציין שהנמשא הועבר למשטרה לצורך המשך טיפול במישור הפלילי, וכי בוצע במשרד הליך הפקת לקחים בעניין, ובמסגרתו בוצעו הדרכות וננקטו פעולות טכנולוגיות כדי שאירוע מסוג זה לא יישנה. משרד נוסף ציין כי בוצעו ניסיונות תקיפה על מערכת ההתחברות מרחוק שלו, אולם ניסיונות אלו לא צלחו מכיוון שמערכות המידע שלו מוגנות בהתאם להנחיות מערך הסייבר הלאומי ויה"ב; וכי ההתראות על ניסיונות התקיפה הגיעו למשרד מה-SOC הממשלתי.



הדברים האמורים מלמדים על סיכוני אבטחת מידע והגנת סייבר הכרוכים בעבודה באמצעות חיבור מרחוק ועל החשיבות בהטמעה של בקורות ונקיטת צעדים לצמצום הסיכונים. מומלץ כי יה"ב בשיתוף המשרדים שבעבר התרחש בהם אירוע סייבר באמצעות ממשק החיבור מרחוק, יבצעו תהליך הפקת לקחים מהאירועים ויפעלו לתקן את הנדרש כדי למנוע הישנות האירועים. כן מומלץ לעדכן את כלל המשרדים בממצאי תחקירים אלו.

משרד מבקר המדינה בדק את ההנחיות הנוגעות להבטחת גישה מאובטחת מרחוק ואת פעולות הבקרה שננקטו לשם יישומן. להלן פרטים:

בקות להבטחת גישה מאובטחת מרחוק

על מנת למזער את הסיכונים הכרוכים במתן גישה מרחוק למערכות המידע של המשרד יש להטמיע בקורות שונות שיבטיחו הגנה על המידע במסגרת עבודה מרחוק, ניטור פעולות חריגות ותיעוד שלהן.

בהתאם לחוק להסדרת הביטחון בגופים ציבוריים, התשנ"ח-1998, האחריות להנחיית גופים המשתמשים במערכות ממוחשבות חיוניות - תשתית מדינה קריטית (להלן - גופי תמ"ק) מוטלת על מערך הסייבר הלאומי. יה"ב משמש גוף הכוונה והנחיה מקצועית בתחום הגנת הסייבר עבור כלל משרדי הממשלה ויחידות הסמך, למעט הגופים המיוחדים. נכון לפברואר 2021 יה"ב מנחה 40 גופים (משרדי ממשלה ויחידות סמך).

ההוראות הנוגעות לגישה מאובטחת מרחוק מעוגנות ב"תורת ההגנה בסייבר לארגון"⁸³ (להלן - מסמך תורת ההגנה) שפרסם מערך הסייבר הלאומי באפריל 2018; בתקן ISO 27001 המגדיר עקרונות להקמה, לניהול ולתחזוקה של מערכת אבטחת מידע המתאימה לארגון (להלן - תקן ISO 27001)⁸⁴ ובהנחיות יה"ב⁸⁵.

על פי מסמך תורת ההגנה, על הארגונים להטמיע בקורות מסוימות בעת גישה מרחוק, בכלל זאת נקבע במסמך כי - נדרשת מדיניות העוסקת בחיבור מרחוק אשר מגדירה את מגבלות השימוש בהתחברות מרחוק למשאבי הארגון וכן נדרש שימוש במערכות אשר מספקות גישה מאובטחת מרחוק למשאבי הארגון; נדרש כי עובדי הארגון וספקיו יתחברו מרחוק תוך שימוש בתווך תקשורת מוצפן⁸⁶; יש לנטר התחברויות מרחוק; יש לנתב את כל ההתחברויות מרחוק באמצעות מספר מוגדר של נקודות בקרת גישה מנוהלות (הפחתת מספר נקודות בקרת הגישה מצמצם את משטח התקיפה); יש לאסור את ההתחברות מרחוק למערכת לצורך ניהולה, וכן יש להגביל גישה למערכת מרשתות שאינן מנוהלות על ידי הארגון; יש להגן על חיבור למערכת

83 המסמך מגדיר שיטה סדורה שבאמצעותה יכיר הארגון את הסיכונים הרלוונטיים לו, יגבש פתרון להגנה מפניהם ויממש תוכנית להפחתתם.

84 מכון התקנים הישראלי, ת"י 27001 טכניקות אבטחה - מערכות לניהול אבטחת מידע - דרישות (ינואר 2014).

85 היבטים נוספים הנוגעים לאבטחת המידע מעוגנים בתקנות הגנת הפרטיות (אבטחת מידע), התשע"ז-2017.

86 אחת הדרכים היא שימוש ברשת וירטואלית פרטית (VPN - Virtual Private Network) אשר מקשרת בין מערכות הארגון באופן המונע התערבות זרה בתוכן המידע המועבר או את חשיפתו והצפנת המידע בה.



מרשת אלחוטית באמצעות אימות זהותם של משתמשים ואימות של מכשירים מהם מתבצע החיבור, שימוש בהצפנה והגדרת הגבלות שימוש (מטרת הבקרה היא למנוע שימוש לא לגיטימי ולא מזהה ברשת האלחוטית); יש להטמיע הצפנה מלאה של המידע המאוחסן על מכשירים ניידים על מנת להגן על סודיות המידע ושלמותו; יש לאסור על התחברות למערכת רגישה באמצעות מכשירים ניידים; יש ליישם הזדהות מרחוק רק במסגרת שימוש בשני אמצעי זיהוי לפחות; יש לזהות ולאמת באופן ייחודי מכשירים שמהם מתבצעת ההתחברות למערכות המידע של הארגון.

הנחיות יה"ב עוסקות אף הן בנושא הגישה מרחוק, תוך שימת דגש על הצורך בהזדהות חזקה ובהצפנת התעבורה: למשל, הנחיית מסגרת להגנת הסייבר בממשלה⁸⁷ משנת 2016 (להלן - הנחיית המסגרת או הנחיית המסגרת להגנת הסייבר) קבעה כי הגישה מרחוק לרשת הארגונית תאומת באמצעות מנגנוני הזדהות חזקה (MFA או 2FA)⁸⁸, ושיש לשלב מנגנוני הצפנה במערכות המשרד במקרים שונים, ביניהם הצפנה של מידע רגיש הנשמר על גבי מחשבים ניידים וכן הצפנה של התקשורת בשירותי תקשורת רגישים, כגון גישה מרחוק לרשת; הנחיה בנושא EMM / MDM⁸⁹ למשרדי הממשלה משנת 2015⁹⁰ קובעת הוראות בנוגע לניהול אבטחת המידע במכשירים ניידים (כגון טלפונים חכמים ומחשבי לוח - טאבלטים) המסונכרנים מול רשת המשרד והתקנת מערכת ניהול ושלטיה מרחוק בעלת יכולת ניטור; והנחיה בנושא הקשחת עמדות קצה⁹¹ משנת 2018 קובעת הוראות בדבר הקשחת עמדות קצה ובכללן מחשבים ניידים (כגון הצפנת מחשבים ניידים כחלק ממכלול האמצעים למניעת דלף מידע ממשלתי בעת אובדן או גניבה של מחשב נייד). כמו כן, יש הנחיה העוסקת בנושא הגישה מרחוק בהיבט של ניהול יעיל של מערך אבטחת המידע ומזעור איומי הסייבר אשר מקורם בשרשרת האספקה (ספקים)⁹².

לאחר פרוץ משבר הקורונה עודכנו חלק מההנחיות האמורות ואף פורסמו כמה הנחיות נוספות. בין היתר פורסמו הנחיות בדבר שימוש מאובטח במערכות המשמשות לשיחות וידאו⁹³ הקובעות כי אין להעביר מידע מסווג או רגיש באמצעות תוכנות ענן המשמשות לשיחת וידאו, וכי יש להשתמש במערכות אלו תוך חסימת האפשרויות האלה בעת השימוש בתוכנה: העברת קבצים, הקלטת השיחה ואפשרות מתן שליטה מרחוק.

- 87 רשות התקשוב הממשלתי, **הנחיית מסגרת להגנת הסייבר בממשלה**, תאריך הוצאה: 1.9.16, תאריך עדכון: 12.3.20 (הנחיה 5.2).
- 88 גורם אימות (Authentication Factor) הוא מידע ואו תהליך המשמש לאימות או לתיקוף (verification) של זהות המשתמש. 2FA - Two Factor Authentication / MFA - Multi-Factor Authentication: תהליך אשר במסגרתו נעשה שימוש בשניים או יותר גורמי אימות (Authentication Factor), אשר מקורם בקטגוריות שונות. לדוגמה: שימוש בססמה אישית (מידע הידוע למשתמש בלבד), מאפיין ביומטרי (תכונה פיזית של המשתמש).
- 89 EMM - Enterprise Mobility Management; MDM - Mobile Device Management.
- 90 **יה"ב - רשות התקשוב הממשלתי**, ההנחיה: EMM / MDM למשרדי הממשלה, תאריך הוצאה: 9.2.15, תאריך עדכון: 30.3.20.
- 91 **יה"ב - רשות התקשוב הממשלתי**, ההנחיה: **הקשחת עמדות קצה**, תאריך הוצאה: 25.12.18, תאריך עדכון: 11.8.20.
- 92 **יה"ב - רשות התקשוב הממשלתי**, ההנחיה: **שרשרת האספקה**, תאריך הוצאה: 3.11.19.
- 93 **יה"ב - רשות התקשוב הממשלתי**, ההנחיה: **שימוש מאובטח במערכת Webex**, תאריך הוצאה: 25.3.20, תאריך עדכון: 28.7.20; **ההנחיה: שימוש מאובטח במערכת Teams הממשלתית**, תאריך הוצאה: 10.5.20, תאריך עדכון: 28.7.20; **ההנחיה: שימוש מאובטח במערכת Zoom**, תאריך הוצאה: 25.3.20, תאריך עדכון: 28.7.20.



כמו כן, עם פרוץ המשבר, במרץ 2020, פורסמה הנחייה ייעודית בנושא גישה מרחוק. ההנחיה נועדה לתת למשרדי הממשלה הוראות מפורטות יותר בדבר קביעת מדיניות לעניין גישה מאובטחת מרחוק לרשת הפנים-ארגונית ולמערכות המידע של המשרד⁹⁴ (להלן - ההנחיה). יצוין כי ההנחיה כוללת גם הוראות שנכללו בהנחיות קודמות של י"ב.

בהנחיה צוין כי כדי למלא צרכים משתנים כגון עבודה מהבית וגמישות במודל ההעסקה מתעורר הצורך במתן גישה מרחוק לרשת הפנימית ולמערכות המידע של המשרד. דבר זה מצריך הנחיות אבטחת מידע להגנה על מערכות הארגון עקב הסיכון הכרוך במתן גישה מרחוק. בהנחיה נקבע כי תחנות העבודה שיאפשרו גישה מחוץ לרשת המשרד יסופקו על ידי המשרד לאחר הקשחת מערכת ההפעלה והצפנת הכוננים במחשבים הניידים, וכי אפשרות נוספת היא שימוש בסביבת עבודה ייעודית שהוגדרה על ידי המשרד לצורך גישה מרחוק. אשר לתהליך ההתחברות, בהנחיה צוין כי בממשל זמין קיים שירות חיבור מרחוק אשר מומלץ להשתמש בו כדי לאפשר גישה מרחוק, וכי על משרדים שאינם משתמשים בשירות זה לעמוד בכמה תנאים, ובהם: על תווך הגישה להיות מוצפן; על המשרד לממש תצורת הזדהות חזקה (MFA, 2FA) על מנת לאפשר גישה מרחוק; יש לזהות ולאמת באופן ייחודי מכשירים שמהם מתבצעת ההתחברות; לאחר תהליך הזדהות חזקה אין לאפשר גישה ישירה לשרתי הארגון, הגישה למערכות המשרד תתבצע אך ורק באמצעות רכיב ייעודי מוקשח (כגון שרת טרמינל); יש להימנע ככל האפשר מחיבור באמצעות רשתות אינטרנט ציבוריות, כגון "אינטרנט קפה" ורשתות שדה תעופה; בעת חיבור מחשב לרשת המשרד יש לוודא כי מותקנת בו תוכנת אנטי-וירוס; יש להגביל את הרשאות המשתמשים למינימום ההכרחי; בשל רגישות הגבוהה של מערכות גישה מרחוק, יש לוודא ביצוע עדכונים למוצרים שמשמשים בהם לגרסה העדכנית ביותר⁹⁵; יש להגביל את מספר החיבורים המותרים בו-זמנית למשתמש יחיד⁹⁶; יש לוודא כי ניטור מערכות החיבור מרחוק מתבצע בהתאם למדיניות המשרד⁹⁷; יש להגביל גישה מכתובות IP⁹⁸ מישראל בלבד, למעט במקרים חריגים שייקבעו על פי מדיניות המשרד; יש לדווח ל-SOC הממשלתי על כל אירוע חריג.

מנהל יחידת י"ב מסר למשרד מבקר המדינה בנובמבר 2020 בנוגע להנחיה האמורה כי הדרישות להצפנה ולהזדהות חזקה הן בבחינת תנאי סף להתחברות מרחוק ונכללו עוד קודם לכן בהנחיית המסגרת, וכי יתר התנאים הם בבחינת בקורות נוספות על דרישות המינימום. בקורות אלו נועדו לתת מענה בארכיטקטורה מסוימת של גישה מרחוק ואף במקרים שבהם מתגלות חולשות במערכות הגישה מרחוק שמבצעות הצפנת תעבורה או הזדהות חזקה. עוד מסר מנהל יחידת י"ב כי הגמישות שניתנה למשרדים להחליט בנוגע לפתרונות גישה מרחוק נעשתה

94 י"ב - רשות התקשוב הממשלתי, **ההנחיה: גישה מרחוק**, תאריך הוצאה: 12.3.20, תאריך עדכון: 19.7.20.

95 בעניין זה ראו: י"ב - רשות התקשוב הממשלתי, **הנחיה 5.15 - מדיניות עדכון מערכות מידע בממשלה** (ינואר 2018). בהנחיה צוין כי ככלל, תוכנה חשופה לפגיעות מסיבות שונות, בהן דרישות אבטחת מידע לא מספקות בכל שלבי הפיתוח, גילוי חולשות חדשות במערכות מידע ופרוטוקולי תקשורת, וכי יש לבצע בדיקת עדכניות גרסה עיתיות בארגון. עוד צוין כי לאחר פרסום חולשה, התוקפים מנצלים את פרסומה לתקיפת גופים אשר עדיין לא עדכנו גרסה ולא יישמו בקורות מפצות או תיקוני אבטחה.

96 מטרת הבקרה הינה לזהות התחברות משני מקומות שונים באמצעות אותם פרטי הזדהות. תרחיש כזה עלול להוות אינדיקציה לשימוש לא מורשה בחשבון המשתמש.

97 ניטור אוטומטי של חיבורים מרחוק מאפשר לארגונים לזהות התקפות סייבר, ובנוסף מאפשר לוודא ציות לנהלי הגישה מרחוק באמצעות בקרה על פעילויות המתבצעות במהלך החיבור המרחוק.

98 כתובת IP (Internet Protocol) - כתובת המוצגת בתבנית מספרית המשמשת לזיהוי נקודות קצה, כגון מחשב, מדפסת וכונן.



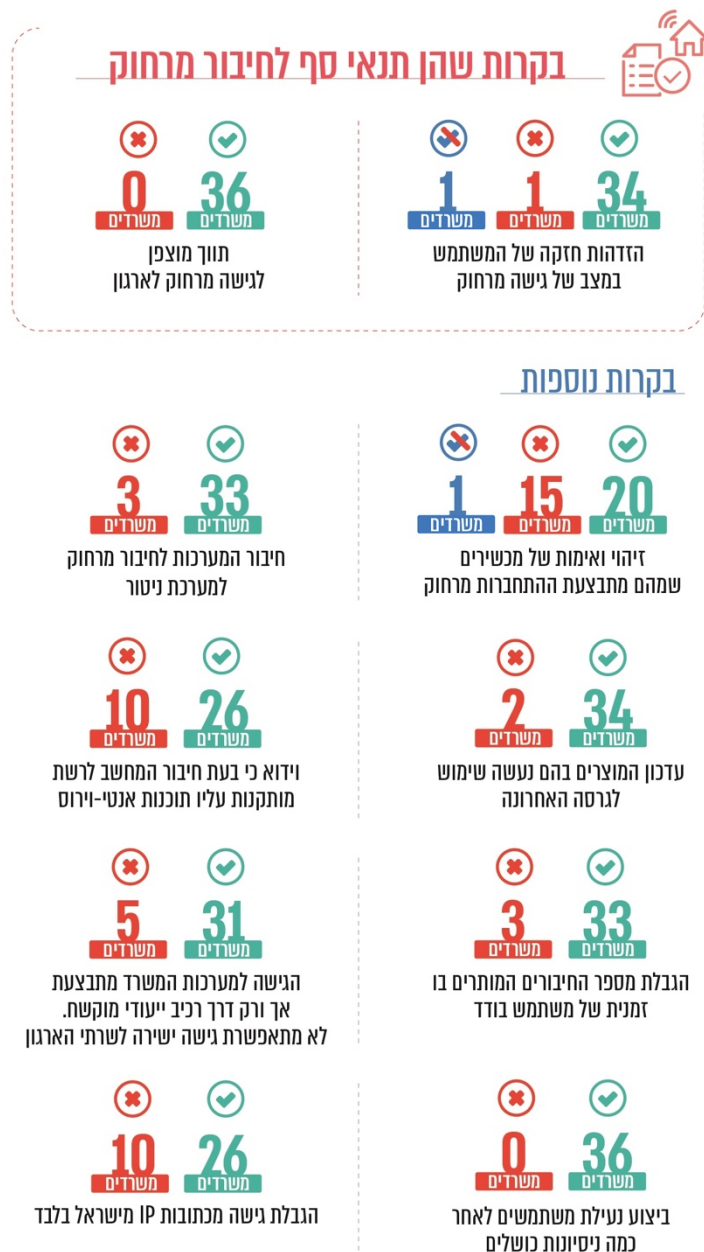
בראייה של מענה נכון לצרכים השונים במשרדי הממשלה תוך שמירה על הגדרות בסיסיות של אבטחה. למשל, בהנחיה צוין כי "תחנות העבודה שיאפשרו גישה מחוץ לרשת המשרד יסופקו ע"י המשרד לאחר הקשחת מערכת ההפעלה והצפנת הכוננים במחשבים ניידים. אפשרות נוספת הנה שימוש בסביבת עבודה ייעודית שהוגדרה ע"י המשרד לצורך גישה מרחוק". מנהל יה"ב הבהיר כי האפשרות הנוספת נועדה לצורך שימוש בפתרונות שונים ומאובטחים המאפשרים עבודה עם מחשבים שלא סופקו על ידי המשרד על ידי חיבור לסביבה המספקת חציצה מלאה בין המחשב המרוחק לסביבת העבודה המשרדית. מנהל יחידת יה"ב מסר עוד כי לשם הצגת הפתרונות המובילים במגזר הממשלתי התקיים בספטמבר 2020 פורום יה"ב ובו הציגו שלושה משרדים את הפתרונות השונים והמאובטחים שהם מיישמים.

בדצמבר 2020 ביצעה יחידת יה"ב מיפוי מול משרדי הממשלה בנוגע לבקורות המוטמעות אצלם בנושא גישה מרחוק. המיפוי שבוצע כלל 36 משרדים, שעשרה מהם משתמשים בשירותי ממשל זמין לחיבור מרחוק העומד בכל הבקורות הנדרשות⁹⁹. משרד מבקר המדינה ניתח את נתוני המיפוי. יצוין כי משרדים אשר יחידת יה"ב ציינה כי יש להם בקרה מפצה נספרו ככאלה שמיישמים את הבקרה. להלן יוצגו ממצאי הבחינה:

99 במשרד אחד מדובר בחיבור חלקי של חלק מהעובדים דרך ממשל זמין.



תרשים 25: מידת עמידתם של משרדי הממשלה בבקורות הגישה מרחוק, נכון לדצמבר 2020



מקור: נתוני יה"ב בעיבוד משרד מבקר המדינה.



ניתוח הנתונים מלמד כי למעט משרד אחד, כל משרדי הממשלה האחרים עומדים בבקורות שהגדירה יה"ב כי הן בגדר תנאי סף להתחברות מאובטחת מרחוק¹⁰⁰. בקורות אלו מהוות מרכיב משמעותי בהבטחת גישה מאובטחת מרחוק. עם זאת, תמונת המצב שעולה בנוגע לבקורות הנוספות, שנועדו לדברי יה"ב, לתת מענה בארכיטקטורה מסוימת של גישה מרחוק ואם מתגלות חולשות במערכות הגישה מרחוק שמבצעות הצפנת תעבורה או הזדהות חזקה, מלמדת שיש פערים מסוימים באופן שחלקן לא מיושם: ב-15 (41%) מהמשרדים שנבדקו לא מתבצעים זיהוי ואימות של המכשירים שמהם מתבצעת ההזדהות מרחוק; בעשרה (27%) מהמשרדים בעת חיבור המחשב לרשת לא מתבצע וידוא כי מותקנת עליו תוכנת אנטי-וירוס; בשלושה (8%) מהמשרדים אין הגבלה בנוגע למספר החיבורים המותרים בו-זמנית של משתמש יחיד; בחמישה (14%) מהמשרדים הגישה למערכות המשרד לא מתבצעת אך ורק באמצעות רכיב ייעודי מוקדש; בעשרה (27%) מהמשרדים אין הגבלת גישה לכתובות IP מישראל בלבד, ובשלושה (8%) מהמשרדים מערכות החיבור מרחוק אינן מחוברות למערכת ניטור. כמו כן, ניתוח הנתונים האמורים מלמד כי באחד המשרדים לא הוטמעו ארבע מהבקורות הנוספות, ובשלושה משרדים לא הוטמעו שלוש מהבקורות הנוספות.

במיפוי האמור, שבוצע בקרב 36 משרדי הממשלה, המשרדים ציינו מדוע הם לא מיישמים את הבקורות האמורות. להלן פירוט הסיבות שציינו המשרדים באשר לבקורות בהם נמצאו הפערים המשמעותיים:

הבקרה	הסיבות שציינו המשרדים לא-ביצועה
זיהוי ואימות של מכשירים שמהם מתבצעת התחברות מרחוק	ארבעה משרדים ציינו כי הנושא נכלל בתוכנית העבודה לשנת 2021. שני משרדים ציינו כי מדובר בהחלטה ארגונית. שני משרדים ציינו כי מדובר באלפי מחשבים המתחברים מהבית ועל כן אין יכולת יישום. שני משרדים ציינו כי הנושא ייבחן במסגרת תוכנית העבודה לשנת 2021. שני משרדים ציינו כי הדבר נובע ממגבלות המוצר שבו הם משתמשים. משרד אחד ציין כי הבקרה לא מיושמת בשל חוסר תקציב. משרד אחד ציין כי הבקרה נמצאת בתהליך הטמעה. משרד אחד ציין כי הנושא יועבר לאישור ההנהלה.
הגבלת גישה מכתובות IP מישראל בלבד	ארבעה משרדים ציינו כי יבחנו את ביצוע ההגבלה. שני משרדים ציינו כי הבקרה נמצאת בתהליך הטמעה. משרד אחד ציין כי בשירותים רגישים הוא מגביל את כתובות ה-IP מישראל. משרד אחד ציין כי הנושא ייכלל בתוכנית העבודה של שנת 2021.

100 במשרד נוסף צוין כי העמידה בבקורות הייתה חלקית היות שהגישה לחלק מהמערכות לא התבצעה על בסיס הזדהות חזקה.



הבקרה	הסיבות שצינו המשרדים לא-ביצועה
	משרד אחד ציין כי יש לו סניפים בחו"ל ועל כן יש צורך בגישה, וכי הגישה ממדינות עוינות נחסמת. משרד אחד ציין כי מדובר בהחלטה ארגונית.
וידוא כי בעת חיבור המחשב לרשת מותקנות עליו תוכנות אנטי-וירוס	שני משרדים ציינו כי מדובר באלפי מחשבים המתחברים מהבית ועל כן אין יכולת ליישום הבקרה. שני משרדים ציינו כי הדבר גרם להם לבעיות תפעוליות, וכי הנושא ייבדק שנית. שני משרדים ציינו כי הרכיב לא הוטמע בשל חוסר תקציב. משרד אחד ציין כי הבקרה נמצאת בתהליך הטמעה. משרד אחד ציין כי חשיבות הנושא הובהרה וייבחנו ביצועה. משרד אחד ציין כי הנושא נכלל בתוכנית העבודה לשנת 2021. משרד אחד ציין כי הדבר נובע ממגבלות המוצר שבו הוא משתמש.
הגישה למערכות המשרד מתבצעת אך ורק דרך רכיב ייעודי מוקשח. לא מתאפשרת גישה ישירה למערכות הארגון	שני משרדים ציינו כי מדובר בהחלטה ארגונית. משרד אחד ציין כי הנושא נכלל בתוכנית העבודה שלו לשנת 2021. משרד אחד ציין כי אין לו סביבה/שרת המותאמים לצורך זה, וכי הנושא ייבחנו בתוכנית העבודה לשנת 2021. משרד אחד ציין כי אין לו סביבה/שרת לצורך זה

יה"ב מסרה למשרד מבקר המדינה בנובמבר ובדצמבר 2020 כי באופן רוחבי, המשרדים עומדים בשתי הבקורות בעלות החשיבות הרבה ביותר - הזדהות חזקה וגישה בתווך מוצפן. יה"ב הדגישה כי יתר התנאים בהנחיה שפורסמה בעקבות ההיערכות לתקופת הקורונה נועדו להציג למשרדים באופן מרוכז את יישום החיבור מרחוק באמצעות ממשל זמין, ובכלל זה להציג להם בקורות נוספות על דרישות המינימום.

יה"ב הוסיפה הבהרות הנוגעות לכמה בקורות: אשר לבקרה הקובעת כי יש להגביל גישה מכתובות IP לכתובות מישראל בלבד צוין כי יש משרדים שנדרשים לספק גישה זו עבור עובדים השוהים בחו"ל. עוד צוין בעניין זה כי ניתן לשנות כתובות IP באופן שהתוקף יכול לתקוף ממקום אחד ובפועל להציג את עצמו ממקום אחר; אשר לבקרה הנוגעת להגבלת מספר החיבורים המותרים בו-זמנית של משתמש יחיד צוין כי לעיתים משרד רוצה לאפשר כמה חיבורים לאותו משתמש כדי שיוכל לבצע תמיכה מכמה מחשבים בו-זמנית; ואשר לבקרה שנועדה לוודא כי לא מתאפשרת למשתמש גישה ישירה לשרתי הארגון, ציינה יה"ב כי "גישה ישירה למשרד ממחשב משרדי מנוהל מהווה חשיפה מסוימת למשרד אך יכולה להיחשב לסיכון סביר. גם במחשבים שמתחברים דרך ממשל זמין קיים סיכון של מחשב שיוצא וחוזר לארגון ומתחבר לרשת באופן ישיר עם חזרתו לארגון". יה"ב הוסיפה כי הגמישות שניתנה למשרדים לפתרונות גישה מרחוק נעשתה בראיה של מענה נכון לצרכים השונים במשרדי הממשלה, בהתאם לארכיטקטורה הקיימת בכל משרד ותוך שמירה על הגדרות בסיסיות של אבטחה - הצפנת התעבורה והזדהות חזקה.



עוד מסרה יה"ב כי היא פועלת באמצעות שיח שוטף עם ממוני הגנת הסייבר ומנהלי אבטחת המידע בהתאם למענים ולארכיטקטורות השונות שבכל משרד, וכי הפערים שהועלו נמצאים בטיפולם של המשרדים.

משרד מבקר המדינה מציין את פעולות יה"ב אל מול המשרדים. התובנה כי היקף העבודה מרחוק יתרחב ככל הנראה בשנים הבאות ויכלול בשגרת העבודה השוטפת מחדדת את הצורך בהטמעתן של כל הבקורות הנדרשות, זאת על מנת להבטיח כי מעטפת ההגנה תהיה מיטבית. מומלץ כי יה"ב תמשיך לפעול מול המשרדים על מנת שיעמדו בכלל הבקורות הנוספות המצוינות בהנחיות, בדגש על משרדים שאינם עומדים בכל הבקורות. הדבר הכרחי במיוחד לנוכח ההתראות המתפרסמות מדי פעם בפעם בנוגע לחולשות (נקודות תורפה או פערי אבטחת מידע אותם ניתן לנצל בכדי לפגוע במערכות המשרד) שמתגלות במערכות האמורות. חולשות אלו עלולות לאפשר לתוקפים להשיג גישה לרשת הארגונית ולבצע גניבת מידע ותקיפות כופרה¹⁰¹.

עבודה מרחוק - גופים בעלי תשתיות קריטיות

אשר לפעילות גופי תמ"ק, מערך הסייבר הלאומי מסר למשרד מבקר המדינה בדצמבר 2020 כי עם התפשטות משבר הקורונה פעל אגף תמ"ק במערך לבצע אפיון והנחיה ייעודית לכל גוף המוגדר כתשתית קריטית בדגש על עבודה מרחוק, במסגרת זו גם הוקם צוות ייעודי לנושא שגיבש מתודולוגיית עבודה וארכיטקטורה ייחודית לעבודה מרחוק בגופי תמ"ק. עוד מסר המערך כי בוצעו בקרה ופיקוח על פתיחה וניהול של הרשאות משתמשים לעבודה מרחוק.

מערך הסייבר מסר למשרד מבקר המדינה מסמכים המשקפים את הפעולות שביצע מול גופי התמ"ק בתחום העבודה מרחוק. מהחומר המתועד עולה כי האישור שנתן לעבודה מרחוק אינו אישור גורף, אלא אישורים נקודתיים בכפוף לעמידה בהנחיות שניתנו להם. עוד עולה כי חלק מהאישורים תקפים רק עד מועד סיום משבר הקורונה.

משבר הקורונה הצריך לגבש בתוך פרק זמן קצר מענה לצורך בעבודה מרחוק גם בגופי התמ"ק. נוכח התובנה כי היקף העבודה מרחוק עשוי להתרחב בשנים הבאות, וכן על מנת להיערך מבעוד מועד למצבי חירום שונים, מומלץ כי מערך הסייבר הלאומי יבצע בחינה של אפשרות העבודה מרחוק בגופים אלה, ובהתבסס עליה יגובשו עקרונות וכללים לעבודה מרחוק שניתן יהיה ליישם בעיתות שגרה וחירום. במסגרת זו מומלץ לבחון פעולה פרטנית מול כל אחד מגופי התמ"ק על מנת להתאים לו את ההגנות הנדרשות לאור היקף פעילותו ומאפייניה.

עמידה בתקן ISO 27001

תקן ISO 27001 כולל בין היתר הוראות הנוגעות לגישה מאובטחת מרחוק. לדוגמה, בתקן נקבע כי יאומצו מדיניות ואמצעי אבטחה תומכים על מנת לנהל את הסיכונים המוצגים בעת שימוש

101 כופרה (Ransomware) היא נזקה המשמשת לסחיטת המשתמש באמצעות הגבלת גישה לקבצים או למשאבים, למטרת קבלת תשלום כספי.



במכשירים ניידים; מדיניות ואמצעי אבטחה תומכים ייושמו על מנת להגן על מידע שיש אליו גישה, עיבוד או אחסון ממקומות מרוחקים; גישה למערכות ואפליקציות תתאפשר אך ורק באמצעות הליך התחברות מאובטח; יש להשתמש בבקורות הצפנה על מנת להגן על המידע.

אשר לעמידה של משרדי הממשלה וגופיה בתקני אבטחת מידע ארגוניים, נקבע בהחלטת ממשלה מפברואר 2015¹⁰² כי על משרדי הממשלה לקבל הסמכה לתקן ISO 27001: על מטה המשרד ומחוזות המשרד - בתוך שנתיים, ועל גופים אחרים במשרד - בתוך חמש שנים לכל היותר.

מנתוני יחידת יה"ב המעודכנים לפברואר 2021 עולה כי מבין 40 משרדי ממשלה המונחים על ידה, 34 משרדים מוסמכים לתקן ISO 27001, ואילו שישה משרדים אינם מוסמכים לתקן, הגם שחלף המועד שנקבע בהחלטת הממשלה (פברואר 2020).

מנהל יחידת יה"ב מסר למשרד מבקר המדינה בנובמבר 2020 כי אף שהסמכה לתקן מעלה בין היתר צורך לתת את הדעת על תהליכים, נהלים ובקורות הנוגעים לגישה מרחוק, משרדים שטרם הוסמכו לא יהיו בהכרח בעמדה פגיעה יותר בנוגע לחיבור מרחוק ממשרדים שכן הוסמכו. הדבר בא לידי ביטוי בכמה גורמים ובהם אופן יישום החיבור מרחוק של המשרד, רמת המוכנות שלו באבטחת מידע הכוללת נהלים, תהליכים וכוח אדם מיומן אשר תומך בארכיטקטורת המשרד להתחברות מרחוק.

על משרדי הממשלה שטרם השלימו את תהליך ההסמכה לתקן ISO 27001 להשלימו, בשים לב לכך שהמועד האחרון להשלמתו חלף.

ביצוע סקרי סיכונים

על פי מסמך תורת ההגנה של מערך הסייבר הלאומי, על הארגונים לבצע תהליך ניהול והערכה של סיכונים סייבר. זהו תהליך מחזורי, שיש לבצעו כאשר סביבת הסייבר של הארגון משתנה - הן בתוך הארגון (קליטת מערכות חדשות, שינויים טכנולוגיים, שינוי בתהליכים עסקיים וכד') והן מחוץ לארגון (שינוי מתמיד של מרחב האיומים בסייבר על הארגון). על פי תורת ההגנה, בניהול הסיכונים הארגון נדרש לזהות את יעדי ההגנה, להגדיר מה הן הבקורות הנדרשות על מנת להגן עליהם ולפתח תוכנית עבודה מתאימה.

הנחיות רשות התקשוב קובעות עקרונות לניהול סיכונים בתחומי התקשוב, לרבות סיכונים פרויקטים, סיכונים תפעוליים וסיכונים מערכות מידע¹⁰³. הנחיות בתחום סיכונים אבטחת מידע ניתנות על ידי יה"ב. רשות התקשוב מתווה את המתודולוגיה לניהול סיכונים התקשוב ולצדה כלי לניהול - בנק יעדים ובנק סיכונים ותגובות לצורך הכנת סקר סיכונים תקשוב. כל משרד ראוי

102 החלטת הממשלה 2443, "קידום אסדרה לאומית והובלה ממשלתית בהגנת הסייבר" (15.2.15).

103 רשות התקשוב, הנחיה 1.3.01 - עקרונות לניהול סיכונים תקשוב במשרדי הממשלה, (1.11.2018); רשות התקשוב, הנחיה 1.3.03 - גיבוש וניהול תכניות טיפול לסיכונים תקשוב, (1.12.2018); רשות התקשוב, הנחיה 1.3.02 - ביצוע סקר סיכונים תקשוב במשרדי הממשלה, (1.11.2017); רשות התקשוב, בנקי סיכונים, פעולות ויעדים לניהול סיכונים ICT.



להוסיף יעדים, סיכונים ותגובות שאינם מופיעים בבנק בהתאם לפעילותו הייחודית ובהתבסס על אירועי כשל שהתממשו או כמעט התממשו אצלו. באשר לעדכון מסמך מיפוי הסיכונים ותחזוקתו צוין בהנחיות כי יש לבחון באופן שוטף את עדכניות מפת סיכוני התקשוב ולעדכנה בהתאם לצורך במקרים הבאים: בעת יישום פעילויות, פרויקטים ומערכות חדשים; במקרים של שינוי ארגוני, שינוי פעילות, שינוי במצבת הנכסים (תשתיות, מערכות) או שינוי במסגרת הפעילות של פרויקטים; כתוצאה מאירועי כשל, מקרים בהם סיכון תקשוב התממש או נמנע סמוך להתממשותו וכתוצאה מכך נגרם נזק או כמעט ונגרם נזק; ולאחר שיפור תגובות קיימות והטמעת תגובות מומלצות במסגרת תוכנית טיפול.

בהנחיית יה"ב¹⁰⁴ נקבע כי על משרד ממשלתי לבצע סקר סיכוני סייבר על מנת לספק תמונת מצב עדכנית של מכלול הסיכונים שהוא מתמודד איתם. סקר סיכונים הוא תהליך שמטרתו זיהוי האיומים, הערכת הסיכון הנשקף בגינם וזיהוי הבקורות הנדרשות לצמצום הסיכונים, תוך התחשבות בסבירות ההתממשות והנזק הפוטנציאלי הכרוך בכך. עוד נקבע בהנחיה כי סקר הסיכונים יתקיים בתדירות של אחת ל-36 חודשים לפחות ויתוקף לפחות אחת ל-18 חודשים, וכי במקרים מיוחדים, למשל בעת שחל שינוי ניכר בסביבה הטכנולוגית או שינוי תהליכי, יבוצע סקר סיכונים נוסף.

בפברואר 2021 מסרה יה"ב למשרד מבקר המדינה כי ההסמכה לתקן ISO27001 מבטיחה כי הגוף מנהל סקר סיכונים קבוע כחלק מההסמכה לתקן ותחזוקתו השנתית. כאמור, נכון למועד זה 34 גופים (מתוך 40 גופים המונחים על ידה) מוסמכים לתקן זה ומקיימים סקרי סיכונים בהתאם.

ביצוע סקר סיכונים מעודכן לנוכח משבר הקורונה

במרץ 2020 פרסמה כאמור יה"ב הנחיה ייעודית למשרדים בנושא גישה מרחוק הכוללת הוראות הנוגעות לאבטחת מידע להגנה על מערכות הארגון עקב הסיכון הנוגע לגישה מרחוק. בהנחיה צוין בין היתר כי בעת מתן אישור לחיבור מרחוק יש להגדיר וליישם תהליך של הערכת סיכוני סייבר בהתאם למתאר הסיכונים של המשרד, ברמת החשיפה של יעדי ההגנה של האיומים ובקורות ההגנה המיושמות במשרד.

משרד מבקר המדינה בדק עם יה"ב אם לנוכח הגידול במספרן של מתקפות הסייבר ולנוכח הרחבת היקף העבודה מרחוק יש מקום שכל משרד יבצע עדכון של סקר הסיכונים שלו שישקף, בין היתר, את הסיכונים הכרוכים במתן גישה מרחוק למערכות המידע שלו:

מנהל יחידת יה"ב מסר למשרד מבקר המדינה בנובמבר 2020 כי בסקרי הסיכונים שמבוצעים במשרדי הממשלה כבר קיימת התייחסות לנושא הגישה מרחוק, הסיכונים הנוגעים לכך והבקורות הנדרשות. דהיינו, נושא העבודה מרחוק הובא בחשבון, גם אם לא בהיקף נרחב.

משרד מבקר המדינה בחן סוגיה זו גם עם המשרדים שנבדקו פרטנית בביקורת. להלן הממצאים שעלו מתשובותיהם:

104 היחידה להגנת הסייבר בממשלה, הנחיה 5.3 - ניהול סיכוני סייבר במשרדי ממשלה (10.7.17, עודכנה ב-2018).



1. משרד התחבורה מסר באפריל 2021 כי בשנת 2020 בוצע סקר למדד יח"ב¹⁰⁵, ובמסגרתו נבחן גם נושא החיבור מרחוק לרשת הארגונית. מהסקר עלה כי המשרד עומד בבקורות שנקבעו בנושא הגישה מרחוק.
2. משרד הפנים ביצע סקר סיכונים סייבר בשנת 2018, אשר במסגרתו נבחנו בין היתר סיכונים הנוגעים לגישה מרחוק. הסקר העלה ממצא המצביע על פער באבטחת המידע בנוגע לגישה מרחוק. בתשובתו המשרד העביר את תוכנית העבודה לשנת 2019 שנעשתה לשם טיפול בפער שהועלה, ומסר כי הוא נערך לביצוע סקר מחודש.
3. משרד המשפטים מסר למשרד מבקר המדינה בתשובותיו בנובמבר 2020 ומאפריל 2021 כי לפני פרוץ משבר הקורונה, בשנת 2017, הוא ביצע סקר סיכונים שעסק בין היתר גם בסיכונים הנוגעים לעבודה בחיבור מרחוק, וכי במהלך משבר הקורונה, ביולי 2020, ביצע סקר סיכונים לעמידה במדד יח"ב. הסקר משנת 2020 העלה כי קיים פער באשר לאחת הבקורות הנוגעות לנושא הגישה מרחוק. המשרד הוסיף כי הרחבת היקף העבודה מרחוק משפיעה על היקף החשיפה הקשור במספר המשתמשים והמחשבים של המשרד השוהים מחוצה לו, ועל כן הגביר את תשומת הלב והדחיפות לגבי טיפול בתחזוקה הנוגעת לאבטחת מידע של רכיבי המערכת. עוד מסר משרד המשפטים כי במהלך משבר הקורונה בוצעו סקרים בנוגע למערכות המידע ולשינויים שיש לבצע במערכות או בתצורות העבודה (כגון יצירת סביבת עבודה מאובטחת בענן לחיבור עובדים), וכי סקר סיכונים נוסף מתוכנן להתבצע בשנת 2021.
4. המשרד להגנת הסביבה מסר למשרד מבקר המדינה בנובמבר 2020 כי באפריל אותה שנה יועץ חיצוני ביצע עבור המשרד סקר תשתיתי חיצוני בדגש על תוֹר מוצפן לגישה מרחוק לארגון. הסקר העלה ממצאים, בעלי רמות הסתברות וחומרה שונים, המלמדים על פערים באבטחת המידע בגישה מרחוק. עוד מסר המשרד כי הוא מבצע באופן שוטף סקרי סיכונים ובדיקות חוסן או חדירה בהיבטים התשתיתיים והאפליקטיביים, וכי הסקר הבא מתוכנן לביצוע באפריל 2021.
5. משרד המדע והטכנולוגיה מסר למשרד מבקר המדינה באוקטובר 2020 ובאפריל 2021 כי בסקרי סיכונים שבוצעו אצלו בשנת 2017 ובשנת 2019 הייתה התייחסות, בין היתר, לנושא החיבור מרחוק וכי הוא מבצע סקרי סיכונים באופן שוטף ובהתאם להנחיות יח"ב. המשרד מסר למשרד מבקר המדינה את ממצאי הסקר שבוצע בינואר 2019, שבמסגרתו הועלו ממצאים המלמדים על פערים באבטחת הגישה מרחוק, שלושה מהם ברמת סיכון גבוהה. הפערים ברמה גבוהה טופלו באופן מיידי והפערים ברמה הבינונית טופלו תוך כשבוע ימים. המשרד הוסיף כי בשנת 2019 התקיימו במשרד תהליכים לקבלת תקן ISO27001, וכי בדצמבר 2019 הוא קיבל אישור ולפיו הוא עומד בתקן ובבקורות הנדרשות במסגרתו. כמו כן ציין המשרד כי אישור העמידה בתקן תוקף מחדש בדצמבר 2020, וכי במסגרת תוכנית העבודה של אגף הביטחון והחירום לשנת 2021 יבוצע סקר סיכונים מעודכן.

105 מדד יח"ב בוחן את רמות ההגנה של המשרד ברבדים שונים ואת מידת עמידתם של המשרדים בבקורות מוגדרות, והוא עשוי לשמש סקר סיכונים.



הגדלת היקף העבודה מרחוק בקרב משרדי הממשלה בתקופת משבר הקורונה, והטמעה מהירה בטווח זמן קצר, של טכנולוגיות ויישומים שלא בהכרח היו קיימים קודם אצל משרדי הממשלה, עשויה להוות שינוי של מרחב האיומים בסייבר.

עלה כי בשניים מתוך חמשת המשרדים שנבדקו סקרי הסיכונים נערכו לפני שנת 2020 וכי הסקרים שנערכו העלו, בארבעה מתוך חמשת המשרדים, פערים בדרגות חומרה שונות, בנושא אבטחת המידע בגישה מרחוק.

נוכח זאת מומלץ כי יה"ב תנחה את משרדי הממשלה, לרבות אלו שכבר התייחסו לנושא הגישה מרחוק בסקרי הסיכונים שביצעו, להשלים סקר סיכונים עדכני אשר במסגרתו יבחנו אלו שינויים חלו באופן עבודתם (עבודה מרחוק, הכנסת מערכות חדשות, שינויים טכנולוגיים, שינויים בתהליכים עסקיים) והאם שינויים אלה מחייבים התאמה של סקר הסיכונים למציאות החדשה, במטרה לעמוד על הפערים והפעולות הנדרשות לשם צמצומם.

כמו כן, מומלץ כי יה"ב תבחן את העולה מסקרי הסיכונים האמורים על מנת לעמוד על סיכונים רוחביים בנושא, לבחון מה הפעולות שיש לנקוט בעניינם ולשקפם למשרדי הממשלה.

מבדקי חדירה

אחד הכלים לבחינת האפקטיביות של הבקורות ושל רמת מוגנות הארגון הוא ביצוע מבדקי חדירה¹⁰⁶ שנועדו לדמות תקיפה חיצונית או פנימית על מערכות המחשוב של הארגון, כדי לאתגר את מערכות האבטחה בארגון ולאתר פרצות אבטחה וסיכונים פוטנציאליים.

בתורת ההגנה של הארגון נקבע כי יש לבצע מבדקים עיתיים בנוגע לחדירות למערכות, וכי יש למנות גורם עצמאי או בלתי-תלוי לביצועם. גם בהנחיית המסגרת להגנת הסייבר בממשלה¹⁰⁷ נקבע כי יבוצעו מבחני חדירה תקופתיים.

ביצוע מבדקי חדירה על ידי המשרדים

משרד מבקר המדינה בירר בדצמבר 2020 עם המשרדים שנבדקו בביקורת אם הם ביצעו בדיקות חדירה בהיבט של עבודה מרחוק. להלן פרטים:

1. משרד המדע מסר כי מבדק חדירות, אשר כלל בין היתר את ממשק העבודה מרחוק, בוצע בינואר 2019. עוד מסר כי המבדק העלה ארבע חולשות אבטחה, וכי בשלוש טיפל באופן מיידי ובאחת טיפל בתוך כמה ימים.

106 Penetration tests.

107 היחידה להגנת הסייבר בממשלה, הנחיה 5.2 - הנחיית מסגרת להגנת הסייבר בממשלה (תאריך הוצאה: 1.9.16, תאריך עדכון: 3.9.20).



2. משרד התחבורה מסר בדצמבר 2020 כי לא קיים בדיקות חדירה ייעודיות בהיבט של חיבור מרחוק אך ביצע הקשחות רבות בנושא.
3. משרד הפנים מסר כי לא ביצע מבדקי חדירות בהיבט של עבודה מרחוק. זאת, היות שהוא מחובר דרך ממשל זמין והם מספקים את הנדרש מבחינת אבטחת מידע.
4. משרד המשפטים מסר כי ביצע בדיקות חדירות לעבודה מרחוק לפני כמה שנים, וכי בתקופה האחרונה לא נעשתה בדיקה בעניין זה.
5. המשרד להגנת הסביבה מסר למשרד מבקר המדינה בינואר 2021 כי ביצע מבדקי חדירות עבור התחברות מרחוק באפריל 2020. עוד מסר בתשובתו כי בימים אלו מבוצע במשרד מבדק חדירה נוסף בקשר לחיבור מרחוק.

מומלץ כי משרדי התחבורה, המשפטים, המדע והפנים ישלימו עריכת בדיקות חדירות עדכניות, שיתייחסו להיבט של חיבור מרחוק.

משרד מבקר המדינה מדגיש בפני משרד הפנים כי שימוש בשירותי ממשל זמין אינו מייתר את הצורך בביצוע בדיקות חדירות על ידי המשרד עצמו, תוך מתן דגש לעמדות הקצה דרכם מתחברים לשירות. משכך ראוי כי משרד הפנים יידרש לנושא.

בתשובתו מאפריל 2021 מסר משרד המשפטים כי הוא מקבל את ההמלצה וביצע בדיקות חדירה למערכות; משרד הפנים מסר בתשובתו מאותו החודש כי ייערך לביצוע בדיקות חדירה במהלך שנת 2021.

משרד המדע מסר בתשובתו מאפריל 2021 כי מבדקי חדירה מתבצעים במשרד באופן שוטף, וכי מספר המבדקים המבוצעים, אופיים וסוגם נקבעים בהתאם לתוכנית עבודה ולניתוח סבירות התרחישים האפשריים לפגיעה. המשרד כלל בתשובתו פירוט על מבדקי החדירה שהתבצעו במשרד בשנים 2018 - 2020.

משרד התחבורה מסר באפריל 2021 כי הוא מבצע באופן שוטף בדיקות חדירות למערכות, וכי בשנת 2020 בוצע מבדק חדירות תשתיתי. המשרד הוסיף כי "הבדיקה אומנם לא מדמה חיבור מרחוק לרשת המשרדית אך עם זאת מדמה מצב בו תוקף נמצא בתוך הרשת". כמו כן ציין המשרד כי המוצר המותקן לחיבור מרחוק הוא המוצר המוביל בתעשייה, וכי היצרן מקיים באופן שוטף בדיקות מקיפות בעניינו.

מבדקי חדירה נועדו להעריך את רמת החשיפה של הארגון או של המערכות בו ולקבל תמונת מצב מהימנה החושפת נקודות תורפה פוטנציאליות. לנוכח הרחבת היקף העבודה מרחוק בתקופת משבר הקורונה והתובנה כי העבודה מרחוק עשויה להיות חלק משגרת העבודה בעתיד, מומלץ כי י"ב תנחה את כלל המשרדים ויחידות הסמך, לרבות אלו המשתמשים בשירותי ממשל זמין, לבצע בתדירות נדרשת מבדקי חדירות וכי במסגרת מבדקי החדירות שהם מבצעים ייבחן אף נושא החיבור מרחוק. עוד מומלץ כי י"ב תעקוב אחר יישום הנחייתה.



ביצוע מבדקי חדירה על ידי יה"ב

בהחלטת הממשלה שבה הוסדרה הקמת יה"ב¹⁰⁸ נקבע כי ייעוד היחידה הוא הכוונה והנחיה מקצועית בתחום הגנת הסייבר עבור כלל משרדי הממשלה ויחידות הסמך. בהחלטה אף נמנו תפקידי יה"ב, ובהם: הכוונה והנחיה בתחומים שונים; בקרה על המשרדים והיחידות כדי לוודא שהם ממלאים את הדרישות המקצועיות, בהתאם להכוונה ולהנחיה; יזום פעילות רוחבית ומימושה; וקביעת תהליכי שיתוף מידע בין משרדי הממשלה.

נמצא כי במסגרת הבקורות שיה"ב מקיימת על משרדי הממשלה היא מבצעת מבדקי חדירות אולם היא לא ביצעה מבדקי חדירה למשרדי הממשלה בהיבט של עבודה מרחוק. נוכח חשיבות הנושא, ראוי כי יה"ב תבצע מבדקי חדירה אף בהקשר זה.

שימוש בחשבון הדואר האלקטרוני הפרטי וביישומנים להעברת מידע ארגוני

השימוש בסביבה הביתית במסגרת העבודה מרחוק וחסמים ותקלות טכניות במערכות התקשורת הביתיות או במערכות הארגוניות עלול להביא עובדים לעשות שימוש בנתיבי העברת מידע עוקפים כגון דואר אלקטרוני פרטי (כגון GMAIL) או בתוכנות מסרים מיידיים (כגון WhatsApp) להעברת מידע ארגוני. שימוש זה טומן בחובו סיכונים אבטחת מידע וסייבר, ועלול לחשוף מידע ארגוני לגורמים שאינם מורשים לכך. שימוש זה עלול אף להביא לאיבוד מידע ארגוני ולהיעדר תיעוד של מידע ומסמכים ברשת הארגונית.

שימוש בדואר האלקטרוני

הגלישה באינטרנט והשימוש בדואר האלקטרוני הפרטי במסגרת העבודה הם נקודת תורפה בכל הנוגע לאבטחת מידע וסייבר בארגון בשל היותם כר תקיפה נרחב עבור גורמים חיצוניים לארגון.

לשם צמצום אפשרות הפגיעה בתשתיות הדואר האלקטרוני של המשרדים ולנוכח הניסיונות לשיבוש פעילות המשרדים, להחזרת פוגענים וליירוט דואר אלקטרוני ממשלתי, נקבע בהנחיית יה"ב משנת 2014¹⁰⁹ כי יש לנתב את תעבורת הדואר האלקטרוני בין הרשויות הממשלתיות באמצעות שירותי יחידת ממשל זמין. בהנחיה צוין כי יחידת ממשל זמין מפעילה מדיניות הכוללת שירותי סינון, ניטור ובדיקה של הדואר האלקטרוני שנשלח אל הלקוח, זיהוי וחסיתה של דואר זבל, הפעלת מערכת אנטי-וירוס ייעודית לתעבורה של הדואר האלקטרוני והפעלת מערכות נוספות המבצעות בדיקה וניטור של קבצים שמצורפים להודעות הדואר האלקטרוני.

108 החלטת הממשלה 2443 (15.2.15).

109 יה"ב - רשות התקשוב הממשלתי, הנחיה 5.6: שער דואר אלקטרוני ממשלתי, תאריך הוצאה: 5.1.14 תאריך עדכון: 1.10.17.



בנובמבר 2020 פורסמה הנחיה נוספת¹¹⁰ ובה נכללה שנית ההוראה כי יש לנתב את תעבורת הדואר האלקטרוני במשרדי הממשלה באמצעות שירותי יחידת ממשל זמין. כמו כן נקבעו בהנחיה הבקורות ורמת האבטחה הנדרשת ממשרדי ממשלה שיבחרו שלא להשתמש בשירותי הדואר האלקטרוני שמספקת יחידת ממשל זמין.

לפי נתוני יחידת ממשל זמין המעודכנים לדצמבר 2020, 36 גופים מנתבים את תעבורת הדואר האלקטרוני שלהם באמצעות שירותיה. מדובר בכ-43,630 תיבות דואר פעילות.

לצד זאת, לשם צמצום הסיכונים האמורים נדרשים המשרדים להשתמש במערכות למניעת דלף מידע¹¹¹. בתורת ההגנה של מערך הסייבר הלאומי נקבע כי על המשרדים לטפל בהעברת מידע לא מורשית שעלולה להתבצע באמצעות תיקיות משותפות, דואר אלקטרוני, מדיה נתיקה וכו' ואף למנוע תופעה זו, וכי הדבר ניתן ליישום באמצעות שימוש בטכנולוגיות למניעת דלף מידע שמנטרות פעולות אלה, מתריעות עליהן ומונעות אותן.

עוד צוין בתורת ההגנה כי תרבות של הגנת סייבר בארגון חשובה לצמצום סיכוני התקיפה של הארגון. עובדי הארגון מהווים עבור תוקפי סייבר אמצעי משמעותי שדרכו ניתן לנסות לחדור לארגון ולשלבש את פעילותו, ולכן הדרכות בקרב העובדים והגברת מודעותם לסיכוני סייבר הן כלי ארגוני חשוב להתמודד עם סיכונים אלו. הארגון נדרש לקיים בקרב העובדים הדרכות בנושא הגנת הסייבר בכל הדרגים ובאופן עיתי - הן הדרכות כלליות שמטרתן להגביר את המודעות והן הדרכות ספציפיות לבעלי תפקידים רגישים ונושאי משרה - ולקיים תרגולים שוטפים בנושא.

גם בהנחיית המסגרת להגנת הסייבר בממשלה שפרסמה יה"ב נקבע כי כל עובד יהיה אחראי באופן אישי להגנה על המידע שאליו הוא נחשף במהלך עבודתו ולכלל המידע הנמצא בחזקתו, לרבות כזה אשר נשלח או הועבר אליו על ידי גורם אחר, וכי יש לקיים הדרכות בקרב העובדים כדי להבטיח כי הם ערים לסיכוני סייבר וכי בידם כלים ליישום המדיניות שקבע המשרד בעניין זה.

אשר לשימוש של עובדים בכלי דואר פרטיים, עם פרוץ משבר הקורונה פורסמה כאמור במרץ 2020 הנחיה ייעודית בנושא גישה מרחוק. בין היתר נקבע בהנחיה זו כי יש למנוע העברת מידע רגיש¹¹² במערכות העברת מידע חיצוניות כגון Gmail ו-OneDrive¹¹³.

בדצמבר 2020 כתבה נציבות שירות המדינה למשרד מבקר המדינה בעניין זה כי בנציבות "עבודה ממיל פרטי, הינה בניגוד לכללים, ואם היא מתבצעת, אזי היא מתבצעת על דעת העובד בלבד". עוד מסרה כי חל איסור לשמור חומרים משרדיים בכווננים בענן הציבורי (כגון Google Drive). גם במקרה זה, אם הדבר נעשה - הוא נעשה בניגוד לכללים. בנוהל פנימי של הנציבות מפברואר 2019 צוין כי "חל איסור מוחלט להשתמש בתיבת דוא"ל פרטית... לצרכי עבודה. שימוש בדוא"ל

110 רשות התקשוב הממשלתי, **הנחיה 1.1.25 - שירות גלישה באינטרנט ודואר אלקטרוני בממשלה**, 15.11.20.

111 מערכת למניעת דלף מידע (Data Loss Prevention Software - DLP) - המערכת מנטרת נתונים בהתאם למדיניות ולחוקים שנקבעו מראש, מדווחת על דליפה של מידע רגיש בתוך הארגון ומחוצה לו (כגון ניטור לפי מילות מפתח מסוימות והיקף קבצים) ופועלת למניעתה.

112 מידע רגיש - מידע אשר פגיעה בסודיותו, או בשלמותו או בזמינותו עלולה לפגוע בניהול התקין של המשרד הממשלתי או של גופים אחרים. ראו: יה"ב - רשות התקשוב הממשלתי, **הנחיה 5.1: מדיניות הגנת הסייבר בממשלה** (2016), סעיף 4.15.

113 יה"ב - רשות התקשוב הממשלתי, **הנחיה 5.24: גישה מרחוק**, תאריך הוצאה: 12.3.20.



פרטי מהווה סכנה הן מבחינת היבטי אבטחת המידע והן מבחינת אובדן מידע יקר ערך, אשר לא יתועד במערכות הארגוניות".

בהתאם להנחיה שהוציאה יה"ב במרץ 2020, יש למנוע העברת מידע ארגוני רגיש תוך שימוש בחשבון הדואר האלקטרוני הפרטי, זאת לנוכח הסיכונים הכרוכים בהיבטי אבטחת מידע והגנת הסייבר הנוגעים לשימוש בתוכנות דואר אלה. על מנת לוודא כי העובדים ערים להנחיה זו ולסיכונים הכרוכים בשימוש בחשבון הדואר האלקטרוני הפרטי, מומלץ כי יושם דגש על כך הן במסגרת ההדרכות העיתיות המתקיימות במשרדים בנושא אבטחת מידע וסייבר והן במסגרת ההנחיות והנהלים הפנימיים שמוציא כל משרד לעובדיו.

עוד מומלץ כי כלל המשרדים וגופי הסמך יונחו לקיים בקורות אודות יישום הנחיית יה"ב ממרץ 2020 בדבר שימוש עובדיהם בדואר אלקטרוני פרטי. נוסף על כך, יש לוודא כי המשרדים שאינם מנתבים את תעבורת הדואר האלקטרוני שלהם דרך ממשל זמין, מקיימים את כל הבקורות הנדרשות בהתאם להנחית יה"ב מנובמבר 2020.

שימוש בתוכנות מסרים מידיים

בשנים האחרונות התרחב היקף השימוש בתוכנות מסרים מידיים בציבור¹¹⁴, והן הפכו גם לכלי עבודה המאפשר קיום שיח בקלות, העברת טקסטים, הודעות קוליות ומסמכים לצד ניהול שיחות קול ווידאו. השימוש במדיה זו מהווה חלק משמעותי של התקשורת הארגונית גם בהתרחש מצבי חירום כגון אסונות טבע, מגיפה התקפות טרור ומלחמות ועוד, בהם נוצרת מציאות המחייבת בין היתר מודל של עבודה מרחוק לשם הבטחת הרציפות התפקודית של הארגון.

לנוכח השימוש ההולך וגובר בתוכנות אלה, לרבות במגזר הממשלתי, ולאור פניות רבות שהגיעו אליה באשר לשימוש בתוכנות אלה וסיווג המידע המועבר בהן, בחנה יה"ב את האפשרות לספק למשרדי הממשלה מערכת צ'אט ממשלתית מאובטחת ומוצפנת מקצה לקצה. במסמך של יה"ב מיולי 2020 תוארה המערכת שנבחנה וצוין כי היא נבדקה במשך מספר חודשים באחד ממשרדי הממשלה. כרקע להצגת המערכת צוינו הסיבות לנחיצותה. להלן:

- כיום כלל משרדי הממשלה נאלצים להשתמש בתוכנות מסרים מידיים מסחרית בעיקר לנוכח העובדה שאין לכך תחליף מאובטח ואיכותי. הדבר יוצר חשיפה של המידע הארגוני ומגדיל במידה ניכרת את נגישותו של מידע זה לגורמים בלתי מורשים ולמזיקים.
- עקב השימוש בתוכנות אלו המידע הארגוני נמצא בידי גוף חיצוני עסקי (דבר שלא מאפשר שליטה במפתחות ההצפנה), ולרוב תוכן השיחות אף מגובה בענן ציבורי ומכאן שהמידע חשוף לגורמים חיצוניים ולתקיפה.
- המידע השמור במכשיר אינו מוגן ואינו מנוהל, ולכן חשוף לכל נזקה פשוטה.

114 למשל, WhatsApp פרסמה בפברואר 2020 כי לפי נתונים המעודכנים לאותו המועד התוכנה תומכת ביותר משני מיליארד משתמשים בכל העולם. <https://blog.whatsapp.com/two-billion-users-connecting-the-world-privately>



בסיכום המסמך נכתב בין היתר כי על פי ממצאי הבדיקה המערכת מטפלת בהצלחה באיומים של דלף מידע שנגרם עקב העברת מידע רגיש באמצעות תוכנות שאינן רגישות; היא מאפשרת ניהול ידע ארגוני ובקרה על המידע; יש לחבר את כל משרדי הממשלה למערכת על מנת שהם יוכלו לקיים שיח ביניהם וכן להעביר זה לזה מידע באופן מאובטח; יש להתאים את חווית המשתמש לחוויית המשתמש בתוכנות מסרים מיידיים אחרות ועל כן יש להמשיך עם הפיתוח של התכונות החסרות. עלות הפיתוח הוערכה במסמך בכ-150,000 ש"ח. במסמך הומלץ להמשיך בהטמעת המערכת.

יה"ב בחנה במהלך שנת 2020 את האפשרות לספק למשרדי הממשלה מערכת מסרים מידיים ממשלתית מאובטחת ומוצפנת מקצה לקצה, אולם פיתוח יישום זה לא קודם. נוכח הסיכונים הכרוכים בשימוש בתוכנות מסרים מידיים וכן נוכח השימוש ההולך וגובר בכלי זה, מומלץ כי יה"ב תשלים את פיתוחה של מערכת מסרים ממשלתית ותטמיע את השימוש בה בהקדם וכי תוציא הנחיה ייעודית בנושא השימוש בתוכנות מסרים מידיים שתבהיר את הסיכונים הטמונים בהן ותעמוד על ההגבלות הנדרשות בעניין זה, לרבות באשר לסיווג המידע המועבר בהן.

עוד מומלץ כי משרדי הממשלה יבצעו הדרכת עובדים בנושא כדי להעלות את מודעות העובדים לסכנות הטמונות בשימוש בתוכנות מסרים מידיים ולצורך להקפיד שלא יועבר מידע משרדי, ובפרט מידע רגיש, באמצעות תוכנות מסרים אלו.



חויית המשתמשים - העובדים

אחד הכלים המאפשרים הערכה של מודל העבודה מרחוק בתקופת הקורונה ואיתור של הבעיות העיקריות במודל עבודה זה הוא ביצוע סקר משתמשים בקרב העובדים. במהלך משבר הקורונה נציבות שירות המדינה ומשרד האוצר ביצעו סקרים בנושא העבודה מרחוק בקרב עובדי המגזר הציבורי, ובכללם עובדי שירות המדינה. להלן פרטים:

עבודה מרחוק במהלך תקופת החירום - עובדים חיוניים

1. **סקר נציבות שירות המדינה:** כאמור, בתקופת החירום (מרץ-אפריל 2020) הורשו לעבוד רק עובדים שהוגדרו כחיוניים. לפי נתוני נציבות שירות המדינה עבדו בתקופה זו כ-13,000 עובדים, כמחציתם עבדו לפחות יום מלא אחד מהבית, מהם כשני שלישים עבדו מהבית במחצית ימי העבודה או יותר מכך¹¹⁵.

בתחילת אפריל 2020 ביצעה נציבות שירות המדינה סקר בקרב כלל העובדים החיוניים בשירות המדינה בנוגע לעבודה מהבית בתקופת משבר הקורונה. מטרת הסקר הייתה לבדוק את עמדותיהם של העובדים והמנהלים לגבי העבודה מרחוק באותה העת, ולזהות בעיות וצרכים (להלן - סקר נציבות שירות המדינה הראשון). את הסקר מילאו כ-2,600 עובדים ומנהלים¹¹⁶.

אחד הממצאים המרכזיים שהועלו בסקר נגע לקושי להתחבר מרחוק למערכות המחשב של המשרדים. העובדים נשאלו אם הם חוו קשיים בהתחברות מרחוק לתוכנות משרדיות בתקופה זו. כ-31% מהם ציינו שחוו קשיים בהתחברות. כמו כן, העובדים נשאלו אילו אמצעים יוכלו לסייע להם לשפר את יעילותם בעבודה מהבית בתקופה זו. כ-24.6% מהם ציינו כי הדרכה ומתן תמיכה טכנית באמצעות כלים טכנולוגיים לעבודה מרחוק יסייעו בכך.

לנוכח הממצאים האמורים המליצה נציבות שירות המדינה "להקדיש את מירב המאמצים לשיפור יכולתם של העובדים להתחבר מרחוק למערכות המשרד, בכדי לאפשר עבודה יעילה מהבית. במקביל למתן פתרונות נקודתיים בטווח המיידי, יש לפעול לפתרון בעיות אלו באופן קבוע, בכדי לאפשר עבודה יעילה מהבית גם במקרה של גל תחלואה שני, או כל תרחיש חירום אחר".

2. **סקר משרד האוצר:** אגף השכר והסכמי עבודה, בשיתוף אגף בכיר לתכנון אסטרטגי ומדיניות בנש"ם, הפיץ אף הוא סקר בקרב עובדי המגזר הציבורי לבחינת אלמנטים שונים שקשורים במעבר לעבודה מרחוק ומשפיעים על יעילותה. הסקר הופץ בתקופת מתכונת החירום שנכנסה לתוקפה ב-22.3.20 ונמשכה עד 30.4.20 (להלן - סקר משרד האוצר הראשון). את הסקר מילאו 3,448 עובדים ומנהלים מכלל המגזר הציבורי (גופי

115 משרדי הממשלה ויחידות הסמך הממשלתיות, נציבות שירות המדינה, **תמונת מצב - הון אנושי בשירות המדינה, דוח שלישי - עבודת עובדי המדינה מהבית בתקופת הקורונה** (חודש מרץ), (6.5.20).

116 נציבות שירות המדינה - אגף בכיר אסטרטגיה ומדיניות, משרד האוצר - אגף השכר והסכמי עבודה, **תוצאות סקר עבודה מהבית בתקופת משבר הקורונה בשירות המדינה**, (מאי 2020).



שירות המדינה, תאגידים שלטון מקומי, חברות ממשלתיות, חינוך והשכלה גבוהה) שהוגדרו כעובדים חיוניים בתקופה זו.

להלן יוצגו ממצאים מהסקר: מחצית העובדים מהבית דיווחו כי הם משלבים בין עבודה מהמשרד לבין עבודה מהבית, וכמחצית העובדים דיווחו על ביצוע העבודה מהבית בלבד; כ-93% מהעובדים דיווחו כי החיבור מרחוק למשאבי המשרד חיוני עבורם; כ-28% מהעובדים דיווחו על קשיים טכניים בהתחברות מרחוק למשאבי המשרד; כ-23% מהעובדים ציינו כי הדרכות ותמיכה טכנית בכלים טכנולוגיים עשויים לשפר את יעילות העבודה מרחוק.

הסקרים מלמדים כי במהלך תקופת החירום (מרץ-אפריל 2020) קרוב לשליש מהעובדים החיוניים שהשתתפו בסקרים של נציבות שירות המדינה ושל משרד האוצר דיווחו על קשיים טכניים בהתחברות מרחוק, כרבע מעובדים אלה סברו שמתן הדרכה ותמיכה טכנית היו עשויים לשפר את עבודתם מרחוק.

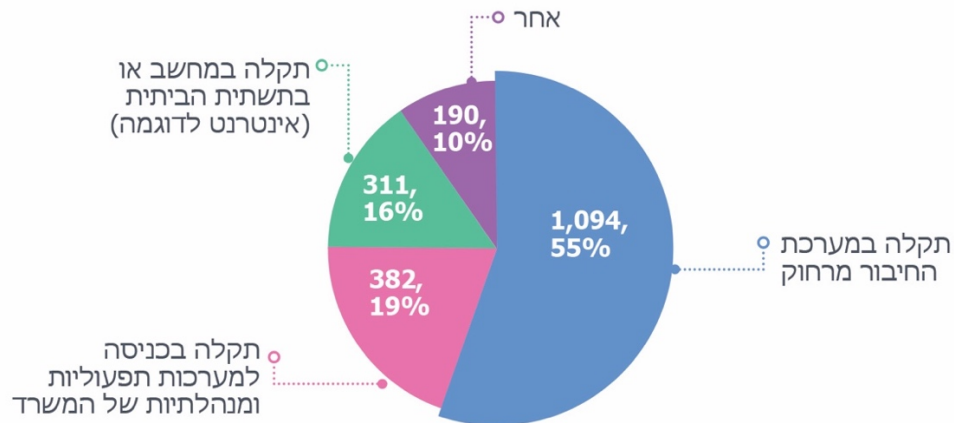
עבודה מרחוק במהלך תקופת הוראות התו הסגול

במהלך שנת 2020 ביצעה נציבות שירות המדינה סקר נוסף בקרב עובדי שירות המדינה - סקר בנושא העבודה מרחוק שמתייחס לעבודה במהלך מאי 2020 (להלן - סקר נציבות שירות המדינה השני). את הסקר מילאו כ-7,000 עובדים. לבקשת רשות התקשוב, נכללו בסקר זה גם שאלות שנגעו לקושי הטכני שהעלו עובדים לגבי התחברות מרחוק למערכות המחשוב של המשרדים (ממצאי הסקר עדיין לא פורסמו באופן רשמי). רשות התקשוב ונציבות שירות המדינה העבירו למשרד מבקר המדינה את ניתוח הנתונים שביצעה רשות התקשוב לסקר האמור.

מתוצאות הניתוח שביצעה רשות התקשוב עולה כי כ-28% מכלל המשיבים על הסקר השני של נציבות שירות המדינה דיווחו שהם נתקלו בתקלות טכניות במהלך העבודה מרחוק. להלן התפלגות התקלות המדווחות על פי סוגיהן:



תרשים 26: התפלגות התקלות על פי סוגיהן - לפי דיווחי המשיבים

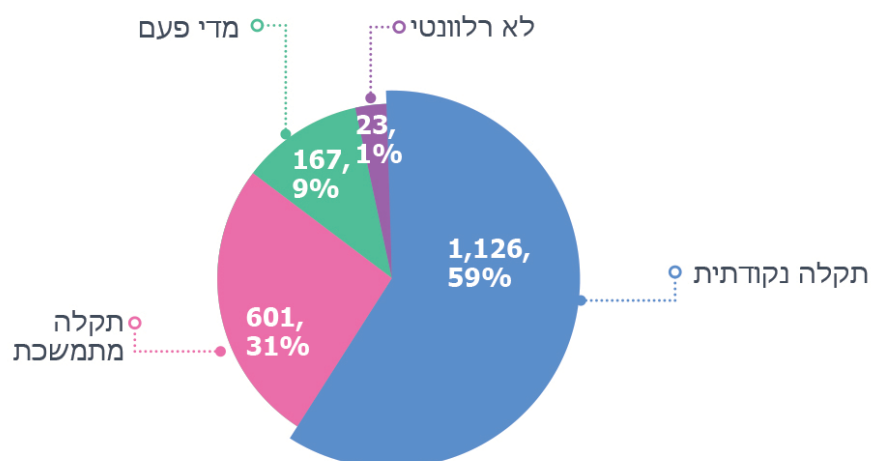


נתוני רשות התקשוב, בעיבוד משרד מבקר המדינה.

מהנתונים האמורים עולה כי כ-55% מהעובדים שדיווחו על תקלות טכניות בעבודה מרחוק (ששיעורם כ-16% מכלל המשיבים על הסקר) נתקלו בבעיות במערכות החיבור מרחוק, כ-19% דיווחו על תקלות בגישה למערכות תפעוליות ו-16% דיווחו על תקלות שמקורן בתשתית הביתית או בציוד הקצה.

בנוגע למשך זמן התקלה הועלו הממצאים האלה:

תרשים 27: משך התקלה



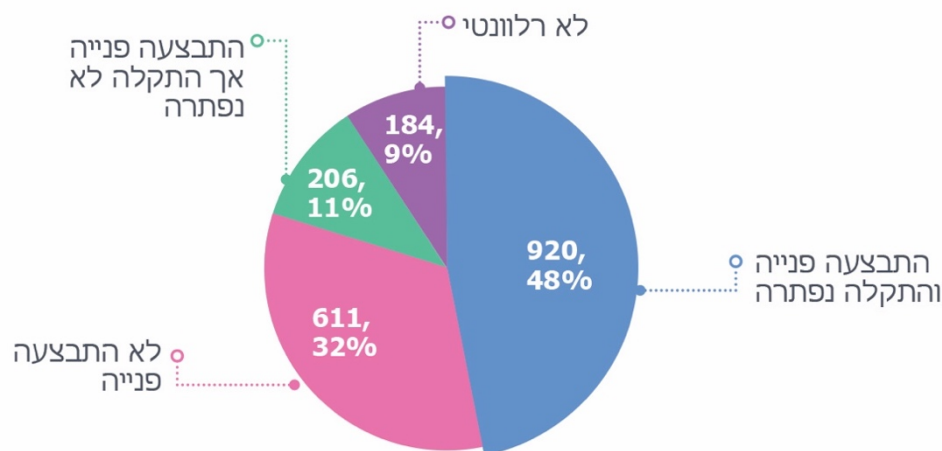
המקור: נתוני רשות התקשוב.



עולה כי 31% מהמשיבים שדיווחו על תקלה טכנית (ששיעורם כ-8% מכלל המשיבים על הסקר) ציינו כי היה מדובר בתקלה מתמשכת (שאינה נקודתית חד פעמית), וכי כ-59% ציינו שמדובר היה בתקלה נקודתית.

היבט נוסף שנבחן נוגע לפנייה למוקד התמיכה של המשרד:

תרשים 28: האם נעשתה פניה למוקד התמיכה והמענה שניתן



המקור: נתוני רשות התקשוב.

הממצאים מלמדים כי 48% מהמשיבים שדיווחו על תקלה ציינו כי היא נפתרה לאחר פנייה לאגף טכנולוגיות דיגיטליות ומידע במשרדם; 32% כלל לא דיווחו לאגף האמור על התקלה, ו-11% ציינו כי התקלה לא נפתרה גם לאחר פנייה לאגף.

אשר לממצאי הסקר השני, רשות התקשוב מסרה למשרד מבקר המדינה ביולי 2020 כי רק מקצת מהתקלות היו תקלות מתמשכות ואף פחות תקלות לא תוקנו על ידי אגפי טכנולוגיות דיגיטליות ומידע במשרדים. מכאן שבתום תקופת ההסתגלות וההיערכות, שלווה בתקלות התחלתיות, אין קושי ניכר במישור הרוחבי בנוגע לתשתיות הטכנולוגיות לעבודה מרחוק. עוד מסרה הרשות כי היא פועלת פרטנית מול משרדים או גופים שבהם היה או עדיין קיים שיעור חריג של קשיים טכנולוגיים, על מנת לבחון את מקור התקלות ולסייע לתיקונן.

בתשובת נציבות שירות המדינה מאפריל 2021 צוין כי במהלך תקופת החירום הופעלו כמה מנגנוני בקרה אשר נוצרו אד-הוק ולא באופן מתוכנן ושיטתי (כגון - סקרים, בדיקת נתוני נוכחות ושיחות רקע עם סמנכ"לים ומנכ"לים). הנציבות הוסיפה כי אגף הבקרה בנציבות שירות המדינה מרכז את נושא הבקרה לתקופת השגרה והציג תוכנית בקרה אשר תביא בחשבון את מכלול ההיבטים העיקריים של עבודה מהבית.



תוצאות הסקרים שבוצעו בתקופת החירום ובתקופת העבודה לפי הוראות התו הסגול מלמדות כי קרוב לשליש מהעובדים דיווחו על תקלות בחיבור מרחוק. עוד עולה מהתוצאות כי יש צורך בקיום הדרכות לעובדים, על מנת לשפר את יכולת העבודה מרחוק ולהבטיח כי העבודה תתבצע ביעילות. יצוין כי גם הבחינה שביצע משרד מבקר המדינה מול חמשת המשרדים שנבדקו בביקורת זו באופן פרטני העלתה ממצאים דומים באשר לצורך בקיום הדרכות לעובדים. מומלץ לבצע הדרכה והכשרה מבעוד מועד לכלל העובדים באשר למיומנויות הנדרשות להם לשם עבודה מרחוק, לרבות בנוגע לשימוש בפתרונות טכנולוגיים נוספים לצורך כך. עוד מומלץ כי המשרדים יעבירו משוב עיתי לשם בקרה בקרב כלל עובדיהם על מנת לעמוד על פערים הנוגעים לתשתיות העבודה מרחוק.

מוצע כי רשות התקשוב תעביר את ממצאי הסקר שנעשה בתקופת הוראות התו הסגול לידיעת משרדי הממשלה (כל אחד וממצאיו), כדי שאלו ימפו את הקשיים והבעיות שהועלו בכל הנוגע לכל אחד מהם ויפעלו לתת להם מענה במידת הצורך. מיפוי הקשיים והבעיות המרכזיות שבהם נתקלו העובדים במהלך עבודתם מרחוק עשוי אף לסייע לזהות את הדגשים הנחוצים במסגרת ההדרכה לעובדים.

כמו כן, מוצע לקיים בקרות מעקב אל מול משתמשים שונים - עובדים, מנהלים, משרדים שנדרשים לעבודה בחומר מסווג וכיו"ב על מנת לעמוד על הקשיים הקיימים בנושא ועל הדרוש שיפור.

שינוי סביבת העבודה הפיזית - עבודה מהבית

היבט נוסף בחוויית המשתמש נוגע לסביבת העבודה, המשפיעה על היכולת לעבוד באופן יעיל ואפקטיבי. משבר הקורונה והמעבר לעבודה מרחוק - דהיינו מעבר לעבודה מהבית, הביא עימו גם שינוי בסביבת העבודה הפיזית.

אגף השכר והסכמי עבודה במשרד האוצר, בשיתוף אגף בכיר לתכנון אסטרטגי ומדיניות בנציבות שירות המדינה, הפיצו סקר נוסף בתקופה שבה הוחלו הנחיות התו הסגול (להלן - סקר משרד האוצר השני). הנחיות אלו נכנסו לתוקפן ב-1.5.20, ובמסגרתן הוקנתה לכל גוף האוטונומיה לקבוע את אופן העבודה מרחוק של העובדים בו. את הסקר, שבוצע בתחילת יוני 2020, מילאו 9,767 עובדים ומנהלים מכלל המגזר הציבורי, לרבות משירות המדינה. מטרת הסקר הייתה לבחון אילו גורמים משפיעים על אפקטיביות העבודה מרחוק, ובין היתר נבחן אף נושא סביבת העבודה בבית.

על פי ממצאי הסקר כ-17% מהעובדים דיווחו כי גם אנשים אחרים משתמשים במחשב המשמש אותם לעבודה מהבית; כ-84% מהעובדים ציינו כי במידה רבה עמדת העבודה שבביתם קבועה ומסודרת; כ-67% מהעובדים ציינו כי יתרון משמעותי של המשרד על פני הבית הוא המפגש החברתי המתקיים בו; כ-60% מהעובדים ציינו כי יתרון נוסף של עבודה במשרד על פני עבודה מהבית הוא נגישות למשאבים הדרושים לביצוע העבודה.



מהאמור עולה כי נודעת חשיבות לנגישות המשאבים הדרושים לביצוע העבודה גם בעת העבודה מרחוק ולהתאמת סביבת העבודה בבית העובד. נוכח זאת, מומלץ כי הגורמים הבוחנים את ההיתכנות של יישום נרחב יותר של מודל עבודה מרחוק בשירות המדינה - בנציבות שירות המדינה ובמשרד האוצר - יבחנו בין היתר גם היבט זה, תוך מתן הדעת על הצידוד הנדרש לעובד לשם ביצוע עבודתו מרחוק (כגון - חיבור אינטרנט מהיר, מחשב נייד או נייד, כיסא ארגונומי, מקלדת, אוזניות ומצלמות). יש בכך כדי להבטיח שהעבודה לא תיפגע בשל היעדר ציוד בסיסי, וכן כדי להשרות על העובד את התחושה שרווחתו חשובה למשרד.

נציבות שירות המדינה מסרה בתשובתה מאפריל 2021 כי במסגרת השיח שהיא מקיימת בנושא עם אגף השכר במשרד האוצר נדונים גם היבטים אלה, וכי נושא זה יידרש להיות מסוכם כחלק מהסדרה כוללת.

ניהול העבודה מרחוק

לעבודה מרחוק יש כאמור מגוון תכליות. לצד זאת, העבודה מרחוק מציבה אתגרים שונים, ובהם ביצוע העבודה באופן יעיל ואפקטיבי.

מטרת העבודה מהבית במשרדי הממשלה וביחידות הסמך בתקופת משבר הקורונה היא המשכיות תפקודית של משרדי הממשלה תוך שמירה על בריאות הציבור, וזאת בהתבסס על הנחיות נציב שירות המדינה והממונה על השכר. בין היתר, פורטו בהנחיות התנאים לאישור עבודה מהבית¹¹⁷:

¹¹⁷ נציב שירות המדינה והממונה על השכר והסכמי עבודה במשרד האוצר, **הנחיה לעבודת עובדי המדינה במתכונת חירום** (מרץ 2020); נציב שירות המדינה והממונה על השכר והסכמי עבודה במשרד האוצר, **הנחיה בדבר עבודה מהבית - לעבודה בהתאם להוראות התו הסגול** (1.5.20).



תרשים 29: התנאים המצטברים הנדרשים לאישור עבודה מהבית – שירות המדינה



מקור: הנחיית נציב שירות המדינה בעיבוד משרד מבקר המדינה.

* תנאי זה נוסף בהנחיה מעודכנת של נציב שירות המדינה והממונה על השכר והסכמי עבודה במשרד האוצר בדבר עבודה מהבית - לעבודה בהתאם להוראות התו הסגול מ-1.5.20.

בהנחיה שפורסמה במאי 2020¹¹⁸ נקבעו כמה הוראות. בכלל זאת נקבע כי עובד שקיבל אישור לעבודה מהבית ידווח במערכת הנוכחות על שעות העבודה שבהן עבד בפועל, וכי במסגרת הדיווח יידרש העובד בשלב זה לדווח במערכת הנוכחות במפורט על המטלות שביצע במהלך היום. כמו כן נקבע כי בשלב הבא יידרש העובד לצרף למערכת הנוכחות טופס דיווח יומי אשר יפרט את פעולותיו ותפוקותיו במהלך יום העבודה מהבית, כי הנחיות מפורטות בעניין זה יועברו בהמשך; וכי יגובשו כלים הנוגעים לדיווח על-ידי העובד כדי לעודד עבודה מבוססת תפוקות.

ביוני 2020 פורסמו הנחיות מעודכנות לשירות המדינה¹¹⁹. בהנחיות הודגש כי כעיקרון, מקום העבודה של העובד הוא במשרד. עם זאת, האחראים במשרד רשאים להמשיך לאשר עבודה מהבית לעובדים העומדים בתנאים המצטברים לאישור מתכונת זו של עבודה, וזאת במידתיות הראויה. עוד הודגש בהנחיה כי "מבדיקה מדגמית שערכנו נדרשת הקפדה יתרה על דיווח המטלות שביצעו העובדים. הסמנכ"לים מתבקשים להקפיד על יישום האמור" (ההדגשה במקור).

118 נציב שירות המדינה והממונה על השכר והסכמי עבודה במשרד האוצר, הנחיה מעודכנת בדבר עבודה מהבית - לעבודה בהתאם להוראות התו הסגול (1.5.20).

119 נציב שירות המדינה, הנחיות מעודכנות לשירות המדינה בעקבות התגברות התחלואה (24.6.20).



אשר ליישום ההנחיות האמורות נציבות שירות המדינה מסרה בדצמבר 2020 למשרד מבקר המדינה כי על מנת שעובדים יוכלו לדווח על המטלות שביצעו במהלך העבודה מהבית, בוצעו כמה התאמות במערכת דיווח הנוכחות, ובהן - החובה להוסיף פירוט לדיווח העבודה מהבית וגם ביטול מגבלת התווים בשדה הדיווח. בעקבות התאמות אלה, ניכר כי אופן הדיווח איפשר הן לעובדים לדווח באופן פשוט ויעיל על המשימות שביצעו, והן למנהלים לבצע בקרה על העבודה הנעשית מהבית. אשר על כן, וגם על מנת למנוע קשיים בדיווח, הוחלט כי אין צורך בטופס דיווח נוסף.

נציבות שירות המדינה הוסיפה כי מעבר לכך, חלק מהמשרדים הכינו טפסים משרדיים המותאמים למאפיינים ולמשימות ייחודיים של המשרד, ובאמצעותם המנהלים הישירים מבצעים מעקב ובקרה בעניין עבודת העובדים מהבית.

הנציבות ציינה כי לאורך כל התקופה היא התדיינה עם אגף השכר ועם סמנכ"ל ההון האנושי וסוכם בין כל הגורמים כי בשל המאפיינים המיוחדים של כל משרד ומשרד ובשל הצורך להקנות גמישות מחד גיסא ולאפשר עמידה בהנחיות מאידך גיסא לא יוכן טופס "אחיד". נכון להיום על העובד למלא הצהרה בנוגע לעבודה מהבית אחת לחודש. בד בבד, וככלי עזר בלבד, הופץ טופס דיווח תפוקות ומשימות של נציבות שירות המדינה למעוניינים בכך. כמו כן, פורסמו המלצות וסקירות על אופני דיווח וכלי דיווח (יישומונים, שימוש ב-OUTLOOK, דיווח במערכת מרכז"ה) ככלי עזר למשרדים.

ההמלצות וסקירות על אופני דיווח וכלי דיווח מתפרסמות באתר אינטרנט¹²⁰ (מגזר ציבורי - מחוברים - אתר הכלים לעבודה מרחוק) שהוקם על ידי נציבות שירות המדינה, בשיתוף ישראל דיגיטלית¹²¹, רשות התקשוב וג'וינט אלכא¹²². בין היתר, ניתן למצוא באתר מידע על מעבר לעבודה על פי תפוקות ומידע על כלים לניהול משימות. נוסף על כך פועלת קהילת הפייסבוק "המגזר הציבורי - מחוברים יחד מרחוק"¹²³, ובה משתפים החברים תובנות שונות.

מומלץ כי נציבות שירות המדינה תבחן בשיתוף עם משרדי ממשלה שונים באם יש מקום להציג באתר האמור גם דוגמאות לכלים שפותחו בהם, על מנת שמשרדים אחרים יוכלו ללמוד מניסיונם. עוד מומלץ כי נציבות שירות המדינה תבחן אם יש מקום לעשות שימוש בכלים שיאפשרו לבצע ניתוח של מאפייני העבודה מרחוק כגון באמצעות קידוד המשימות והעיסוקים השונים.

¹²⁰ https://govextra.gov.il/digitalisrael/projects/telecommuting?utm_source=go.gov.il&utm_medium=referral

¹²¹ ראו מבקר המדינה, דוח שנתי 70 (2020), "המשרד לשוויון חברתי - 'המים הלאומי' ישראל דיגיטלית", עמ' 1511 - 1589. במועד הביקורת הנוכחית "ישראל דיגיטלית" פעלה במסגרת משרד הדיגיטל הלאומי.

¹²² ג'וינט-אלכא: פיתוח פתרונות לקידום יעילות ומועילות המערכות הציבוריות.

¹²³ <https://www.facebook.com/groups/206036797419636/>



נושא ניהול העובדים מרחוק נבחן גם במסגרת הסקרים שביצעו נציבות שירות המדינה ומשרד האוצר:

1. סקר נציבות שירות המדינה הראשון, שבוצע כאמור בתקופת החירום (מרץ-אפריל 2020), בחן מהו טיב הקשר עם הממונה הישיר וכיצד מתבצעת הבקרה על העובדים. ממצאי הסקר העלו כי רובם המוחלט (84.7%) של העובדים שמילאו את הסקר ציינו כי הם נמצאים בקשר ישיר יומי עם הממונה הישיר. אשר לדיווח על העבודה שנעשתה הועלו הממצאים האלה: האמצעי הנפוץ ביותר המשמש לבקרה של מנהלים על עובדיהם הוא דיווח או שיחה שגרתית וקבועה (38.8% מהעובדים), אך רק כ-21% מהעובדים נדרשו לדווח במערכת ייעודית על ביצועיהם או לחלופין התפוקות שלהם נמדדות ישירות (כגון מספר הפניות בהן טיפל העובד). היבט נוסף שנבחן בסקר נוגע לשביעות הרצון מהעבודה בבית. רובם המכריע של המנהלים (84.3%) הביעו רצון משמעותי להגדיל את תדירות העבודה מהבית של העובדים הכפופים להם גם בימי שגרה, בהשוואה לנתון מקביל של 92.0% בקרב העובדים עצמם המעוניינים בתדירות גבוהה יותר של עבודה מהבית עם החזרה לשגרה. לצד שביעות הרצון, 20% בקירוב מהמשיבים ציינו כי נוכחות הילדים בבית פוגעת בעבודתם במידה רבה. בנוסף, 40% בקירוב מהמשיבים דיווחו כי העבודה מהבית מסייעת להם מאוד בהיותה מסיחה את דעתם מהמזב. הנציבות ציינה בסקר כי עובדים, שתפוקותיהם נמדדו ודווחו במפורט, היו שבעי רצון יותר מכלל היבטי העבודה מהבית יחסית לשאר העובדים. הנציבות ציינה כי, מסיבה זו, בין היתר, היא קבעה החל ב-1.5.20 כי חובה על עובד מהבית למלא טופס דיווח יומי. עוד ציינה הנציבות כי "מהסקר עולה הצורך במדידת תפוקות העובדים ע"י הממונים, ובעבודה על פי תוכנית עבודה מפורטת יותר מכפי שנהוגה בשגרה".

בהתבסס על ממצאי הסקר גיבשה נציבות שירות המדינה כמה המלצות, ובהן: לעודד מנהלים ועובדים לקבוע יעדים יומיים ושבועיים מדידים - מתכונת עבודה זו תסייע להגברת האפקטיביות בכל תרחיש, אך בעבודה מהבית תפקידה חיוני ביותר; לעודד מנהלים לקבוע יעדים המבוססים על תפוקות ולא על תשומות; לעודד מנהלים לקבוע שיחות קבועות ותכופות עם עובדיהם, שבהן יידונו תפוקות העובד בימים שקדמו לשיחה ויעדי העובד בימים שלאחריה.

2. סקר משרד האוצר השני, שבחן את העבודה בתקופה שבה הוחלו הוראות התו הסגול (בתחילת יוני 2020), בחן בין היתר את שביעות הרצון מהעבודה מרחוק ואת יעילות העבודה מהבית. ממצאי הסקר העלו כי 92% מהמנהלים דיווחו על שביעות רצון גבוהה ממידת עמידתם של העובדים מהבית ביעדיהם בתקופה זו; 78% מהמנהלים הביעו נכונות גבוהה להגדלת שיעור העבודה מהבית של עובדיהם עם החזרה לשגרה. אשר לתפוקות העבודה וליעילותה, התגלה מתאם חיובי בין מדידת תפוקות העובד ובין שביעות הרצון של העובד מהעבודה בבית ומביצועיו בכלל; עובדים שביצעיהם נמדדים באופן כלשהו דיווחו על ניהול יעיל יותר מצד הממונה לעומת עובדים שביצעיהם אינם נמדדים; נמצא מתאם חיובי מובהק בין אופן עבודה הכולל תכנון וסדר לבין שביעות רצון העובדים מהבית מעמידתם ביעדים; נמצא מתאם חזק בין קלות התקשורת עם העובדים מהבית ליכולת הממונה לעקוב אחר ביצועי העובדים מהבית. בעניין זה צוין כי ממצא זה מעיד שהדרכות טכנולוגיות למנהלים ולעובדים, לצד סיוע בפתרונות טכניים שונים, כגון שיפור יכולת התקשורת, יכולים לעזור למנהלים לעקוב אחר ביצועי העובדים ולאפשר בכך עבודה אפקטיבית יותר מהבית.



משרד מבקר המדינה בחן היבט זה גם בקרב חמשת משרדי הממשלה שנבדקו פרטנית בביקורת. במסגרת זו המשרדים נשאלו אם הם משתמשים באמצעים טכנולוגיים או בחנו פיתוח כלי משרדי ממוחשב שיתמוך בפיקוח על עבודה מרחוק.

מתשובות המשרדים שנבדקו בביקורת עולה כי הם פועלים בהתאם להנחיות נציבות שירות המדינה - העובדים מדווחים על שעות עבודה מהבית ועל משימות שביצעו במהלך יום העבודה באמצעות מערכת הנוכחות; ומנהליהם הישירים נדרשים לבדוק את הדיווחים ולאשר אותם. המשרדים ציינו כי מהבחינה הטכנית ניתן לעקוב אחר שעות החיבור מרחוק, אולם היבט זה אינו משקף נאמנה את כלל העבודה שנעשת. המשרדים גם עמדו על ההבדל בין ביצוע עבודה הניתנת לכימות ולבקרה (כגון - טיפול בפניות) לבין משימות שביצוען יכול להיבדק רק באופן עיתי (פעם ברבעון, בחציון או בשנה). כמה משרדים ציינו שהם פיתחו, לצד הדיווחים האמורים, כלים משלהם לדיווח על עבודה מהבית. להלן פרטים:

משרד המדע מסר למשרד מבקר המדינה בנובמבר 2020 כי לנוכח מגבלת המקום הפנוי לדיווח במערכת הנוכחות, והיעדר האפשרות למעקב יומי פשוט, הוא פיתח מערכת המאפשרת ביצוע פעילויות אלה: דיווח של העובד למנהל על פעילות שבוצעה; צפייה של העובד בכלל הדיווחים שמסר למנהל; משלוח מכתב אלקטרוני למנהל ובו מתוארת פעילות שנוספה; אפשרות שהמנהל יבחן את הדיווח ויקבע אם לאשר; משלוח מכתב אלקטרוני לעובד ולמנהל ובו תיעוד של אישור הדיווח. להלן דוגמא למערכת שפיתח משרד המדע:

תרשים 30: דוגמא לדיווח עבודה מהבית - משרד המדע

דיווח עבודה מהבית

☐ *	יחידה
	שם העובד
	שם המנהל
17/11/2020	תאריך
*	משעה
*	עד שעה
*	פירוט משימות
	הערות



משרד התחבורה מסר למשרד מבקר המדינה בנובמבר 2020 כי העובד מחויב בסיום יום עבודה מהבית לפרט את המטלות שביצע, הן באמצעות מערכת הנוכחות והן באמצעות דיווח נוכחות יומי ביישומון שפותח, וכי חלק מהמטלות מוגדרות על ידי המנהל וחלקן מוגדרות על ידי העובד מתוקף אחריותו ועצמאותו. המשרד הוסיף כי עבודה מהבית, לרבות דיווחי הביצוע, מושתתת על אמינות ברמה הגבוהה ביותר, על עצמאות העובד ועל אחריות אישית שלו, וכי על כך מתבסס המנהל.

יצוין כי ביוני 2020 נשלח לנציב שירות המדינה ולממונה על השכר במשרד האוצר מכתב שעליו חתומים יותר מ-800 מנהלות ומנהלים בשירות הציבורי במשרדי הממשלה ובשלטון המקומי. הפונים ציינו במכתבם כי בתקופת משבר הקורונה הם גילו את היתרונות הרבים הגלומים בעבודה מהבית, וכי בעולם העבודה מתחוללים שינויים ניכרים בתקופה זו, המחייבים בחינה מחדש של הגמשת הרגלי העבודה ובכלל זה עבודה מהבית. הפונים ציינו כי הם מבקשים "לשמר במידה את הצלחת הניסוי שנכפה עלינו, ולאפשר מסגרת גמישה לעבודה מהבית עבור מנהלי ועובדי השירות הציבורי".

בתקופת הקורונה נדרש מעבר מהיר לעבודה מהבית בהיקפים נרחבים, ואחת הסיבות העיקריות לכך הייתה שמירה על בריאות הציבור. בהתאם למגמות המסתמנות בארץ ובעולם, לא מן הנמנע שהעבודה מהבית תהפוך בעתיד הקרוב לדבר מקובל אף בעיתות שגרה. על מנת לוודא שהעבודה אינה נפגעת כאשר היא מבוצעת מרחוק, מומלץ כי נציבות שירות המדינה תבחן בשיתוף משרדי הממשלה באילו נסיבות ניתן לבצע מהבית ברמת אפקטיביות מספקת יחסית לאפקטיביות של העבודה המבוצעת מהמשרד; כן מומלץ לבחון מבעוד מועד אם כלי הבקרה שנקבעו בהנחיות נציבות שירות המדינה בתקופת הקורונה מספקים, ואם יש מקום לפתח כלים נוספים שייתנו מענה יעיל ונוח לעניין זה; חשוב להמשיך לבצע מחקרים שיסייעו להבנת הנושא ולזיהוי הפעולות הנדרשות לשם הבטחת האפקטיביות של העבודה מרחוק. מציאת האיזון בין אפקטיביות העבודה מהבית לבין התכליות שהיא נועדה לקדם תאפשר תכנון מיטבי של העבודה מהבית בהווה ובעתיד.

באפריל 2021 מסרה נציבות שירות המדינה למשרד מבקר המדינה כי אגף הבקרה בנציבות האמון, בין היתר, על בקרת העבודה מרחוק הציג תוכנית לבקרה בנושא בתקופת השגרה אשר תכלול היבטים מרכזיים של עבודה מהבית וכי הוא עדיין מבצע עבודת מטה לגיבוש כלים טכנולוגיים תומכי בקרה.



סיכום

משבר הקורונה הביא לכך שארגונים שונים, ובכלל זה משרדי ממשלה, נדרשו לאפשר עבודה מרחוק כדי להבטיח רציפות תפקודית ומתן שירותים לאזרחים תוך שמירה על אבטחת המידע הנדרשת. בהיבט זה, המשבר משמש זרז להתפתחות של תהליכים הצפויים בשוק העבודה העתידי.

לעבודה מרחוק יש מגוון תועלות, ובהן הפחתת נזקי גודש התחבורה וצמצום זיהום האוויר, הגדלת הפריזון, צמצום סכנת התפשטות מחלות מדבקות, קידום שוויון הזדמנויות, חיסכון במשאבים, תועלת במצבי חירום ואפשרות איזון בין חיים אישיים לעבודה. עם זאת, היא מציבה אתגרים לעובדים ולמעסיקים, בכלל זה סיכוני אבטחת מידע, קושי בפקוח על עובדים, צמצום האינטראקציה החברתית בין העובדים, פגיעה בעבודת הצוות, והגדלת פערים בין עובדים שאופי עבודתם מאפשר לבצעה גם מרחוק לבין עובדים שאינם יכולים ליהנות מהיתרונות הכרוכים בכך.

דוח זה בחן היבטים תקשוביים הנוגעים לעבודה מרחוק בתקופת הקורונה. התובנה כי היקף העבודה מרחוק יתרחב ככל הנראה בשנים הבאות ויהיה חלק משגרת העבודה השוטפת מחדדת את הצורך בגיבוש מדיניות תקשובית בתחום. מדיניות זו עשויה לשמש תשומה לגורמים שונים בממשלה הבוחנים את היתכנות יישום מודל של עבודה מרחוק באופן נרחב יותר בשירות המדינה. על המשרדים להבטיח כי יעמדו לרשותם תשתיות תקשוב שיקנו להם גמישות מבחינת היקף העובדים הנדרשים לעבוד מרחוק; להבטיח כי הם יוכלו להעמיד לרשות העובדים תמיכה טכנית והדרכה מספקות כדי לאפשר להם להתגבר על קשיים שהם נתקלים בהם בעת התחברות מרחוק. כל זאת, תוך יישום בקרות אבטחת המידע הנדרשות והעמדת גישה מאובטחת מרחוק, שתיתן מענה לסיכונים הטמונים בכך.

משבר הקורונה הוא משבר עולמי מהבחינה הרפואית, הכלכלית והחברתית, אך הוא גם פותח פתח להזדמנויות. הסדרה לטווח הארוך של העבודה מרחוק לצד עבודה מהמשרד היא הזדמנות ליצור מציאות חדשה שתאפשר את ניצול היתרונות הגלומים במתכונת עבודה זו, תוך התמודדות עם האתגרים שהיא מציבה. הסדרה זו תאפשר למשרדי הממשלה לשפר את היערכותם להמשכיות תפקודית כדי שיוכלו להמשיך לספק שירותים ביעילות ובאופן המיטבי לאזרחי המדינה בעיתות שגרה וחירום, בפרט נוכח הצורך בהמשך ההתמודדות עם מגפת הקורונה וכהיערכות לאתגרים סביבתיים וגלובליים עתידיים.